Context-Aware Privacy Protection Framework for Wireless Sensor Networks

Mitzeva, Anelia Ivanova

Publication date:
2009

Document Version
Early version, also known as pre-print

Aalborg University, Center for TeleInFrastruktur (CTIF)

"Context-Aware Privacy Protection Framework for Wireless Sensor Networks"

By

Anelia Mitseva, M.Sc.

PhD Dissertation

To be presented to the International Doctoral School of Technology and Science
Aalborg University

Aalborg University

To be defended on date

Supervisors:

Dr. Neeli R. Prasad

Prof. Dr. Ramjee Prasad

Anelia Mitseva
Aalborg University
Center for TeleInFrastruktur (CTIF)
Niels Jernes Vej 12
9220 Aalborg, Denmark

Abstract

Wireless sensor networks (WSNs) are expected to be one of the key enabling technologies in the near future. Ubiquitous intelligent sensing environments have a promising potential to enhance the everyday life of the citizens, bringing important social benefits for each person and for the society as a whole. Example application space of this new technology is the pervasive health and elderly care. Successful integration of pervasive health care systems in the everyday life of elderly, patients, their relatives and their carers - in terms of selection of appropriate means for security and privacy protection - may only be achieved if the systems offer tools for flexible, adaptable and individualised services which at the same time leave the end-user to be in control of taking the decision for revealing sensitive information according to a specific situation and context. This touches both technological aspects such as ensuring confidentiality, data integrity and freshness, trust establishment in pervasive healthcare environments, as well as privacy of communication, data and location.

Substantial research has contributed to progress in this field. However, before the wide acceptance of such services and systems, the integration of wireless sensor networks with different network systems gives rise to many research challenges to ensure security, privacy and trust in the overall architecture. Part of the challenges to overcome are due to requirements for reliable services, low network latency, low packet loss, robust data and image transmission, and the great need for safe, secure, and dependable operation. For pervasive health care services using wireless sensor networks and body sensor networks, ensuring security and privacy is a quite complex task because of the need for power efficiency, the need for solutions which fit in very low memory, solutions for heterogeneous devices, need for unobtrusive operation, and last but not least - the need for solutions which are adaptable and flexible enough in order to be applicable to many services. Moreover, there is a need of empowering end-users with flexible personalised controls for their personal data collected, processed and communicated via the sensors.

The security and privacy protecting mechanisms must be non-obtrusive and context-aware to support the daily private and professional life of the persons. Since the devices/nodes used by patients and medical professionals will have diverse capabilities, many of them with very limited resources, an important question is the implication of the security and privacy solutions on the overall system performance and the costs of integrating the protocols and mechanisms.

The goal is to design an adaptive security and privacy framework that provides the respective services under the constraints of code size, CPU, and memory size. The solution adopted in this PhD thesis to provide privacy protection for WSNs is based on application-aware adaptive security management and context-aware controlled information disclosure, capable of providing three different security levels that best match with the actual needs of the scenarios, without overloading the constrained devices. Starting point of the work is thorough analysis of security threats and vulnerabilities to which such systems could be exposed to. Based on the specific security, privacy, user and service requirements, valid for the pervasive health care applications, threat model is defined (including threats coming from context provision), security risk assessment is performed and overall mitigation plan to countermeasure the threats is proposed. Further in the thesis, suitable countermeasure solutions for a subset of the threats are proposed – namely, threats to unauthorised access, revealing confidential data and revealing user's identity and location.

The privacy protection framework is integrated within the generic security framework. Suitable protocols and mechanisms are identified, which when combined according to the framework form a complete toolbox solution which fits the architecture of Beyond 3G environments.

This thesis proposes novel flexible privacy protection framework suitable for diverse set of pervasive health and elderly care applications; describes evaluation frames for it and investigates the cost of privacy protection. Evaluation of the influence of the context complexity and policy-based management is also presented. Performance evaluation results demonstrate the feasibility and estimate the benefits of the adaptive security and context-aware privacy for pervasive health care scenarios. The evaluation should aid the designers of pervasive

systems with integrated wireless sensor networks in understanding how to exploit context, policies and profiling in order to protect privacy; how to find the most relevant design; how to access the performance of the solution.

More precisely, the major contributions of this thesis are:

- Analysis of the security and privacy requirements of the scenarios of tele-health and tele-care, including also the requirements for the relevant context
- Full threat analysis of pervasive health care scenarios with definition of threat model and mitigation plan for WSNs for pervasive health and elderly care application spaces
- Definition of generic adaptive security management framework for WSNs in pervasive health care scenarios
- Definition of context-aware privacy protection framework for WSNs in pervasive health care scenarios, integrated within adaptive security management framework
- Proposal of context-enhanced controlled information disclosure mechanism
- Proposal of adaptive security protocol suit for confidentiality for WSNs in pervasive health care scenarios

Dansk Resumé

Acknowledgments

Table of Content

List of Figures

List of Tables

Chapter 1 – Introduction

1.1 General Framework

As the average age of the population is increasing in most of the European countries, the percentage of many chronic diseases is increasing too. WHO has predicted that in 2030, the reasons for highest death rate will due to cancer, ischemic heart disease and cerebrovascular disease. The number of cases will be increasing with time. [1]
At the same time, the shortage of qualified personnel to take care of patients and elderly posses many challenges for the health and social systems in many European countries.

Health and primary care providers must use the resources most effectively and save costs, and at the same time keeping the same living standard as of today and even improving the quality of healthcare services. Therefore it is in many cases an option to treat/monitor as many patients as possible at their home and to prolong the time which an elderly person lives independently at home. Hence, many governments are now focusing to find technological systems for supporting the chronically ill and the elderly to live as independently as possible and to help elderly and patients to be treated and/or after cared safely at their own homes.
In this respect the application of pervasive computing in telemedicine and tele-care and development of an ambient intelligence for healthcare and wellness management in the patient's home is the appropriate choice [2] [3]. In parallel, the use of pervasive systems for patients at hospital provides many opportunities for cheaper and effective treatment.

Pervasive healthcare is in this respect an emerging cross-disciplinary domain, focusing on the research and developments of pervasive and ubiquitous wireless technologies in order to improve the quality of health-care, care for elderly and wellness. We are currently witnessing first trials of pilots of services integrating wireless communications in patients and elderly care by the evolution of new generations of embedded wireless devices, which facilitates reliable, comprehensive, and high-standard health and elderly care. Particularly, developments in wireless infrastructure, such as wireless sensor networks and body-area networks or pervasive health-monitoring systems, have proved beneficial to deliver telemedicine services regardless of a patient or elderly physical location [4][5].

However, before the wide acceptance of such services and systems, there still exist many challenges to overcome due to requirements for reliable services, low network latency, low packet loss, robust data and image transmission, and the great need for safe, secure, and dependable operation [6]. In all these applications and services, the data which will be monitored, communicated, stored, requested, will be of very sensitive and private value for the end –user [7]. In order to avoid dehumanising and stigmatising the user, the privacy and ethical aspects and the end-user values must be paid great attention to and incorporated in the design approach [8]. This is especially true for designing pervasive healthcare applications, where the 'complexity of users' is increasingly sensitive. The end-users must be also aware and informed that certain pieces of sensitive information must be revealed, collected and accessed by others. By considering measures for privacy protection of the human values in the design process, designers and developers can create pervasive health applications that better fit the end-user needs and desires. This will further reduce the risk of resistance to this new technology.

Designing of such systems with privacy and ethical care in mind must solve security, privacy and social issues of ubiquitous systems; issues for data integrity and privacy protection; security auditing; authentication and identity management; access controls, etc.

Additionally, successful integration of Pervasive Health and Social Care Systems in the everyday life of elderly, patients, their relatives and their carers - in terms of selection of appropriate means for security and privacy protection - may only be achieved if the systems offer tools for flexible, adaptable and individualised services which at the same time leave the end-user to be in control of taking the decision for revealing sensitive information according to a specific situation and context. This touches both technological aspects such as ensuring

confidentiality, data integrity and freshness, trust establishment in pervasive healthcare environments, as well as privacy of communication, data and location.

Looking at possible network architectures which could support pervasive health care services, the focus is on Beyond 3G environments. Their characteristics are heterogeneous devices, inter-working of different communication paradigms, heterogeneous wireless interfaces, hierarchical network organisation and data aggregation [9]. They are potentially highly dynamic, with frequent changes of topology, with mobility at all levels of hierarchy in the forms of node and network mobility. In some of the levels of these environments, the devices are power, energy and memory constraint. The applications are user and service oriented and to provide unobtrusive end-user services, they rely heavily on context data from the surroundings. These specifics call for flexible and context-aware solutions.

1.2 Reference network and system architecture

Addressing the requirements of ubiquitous sensing and networking, the EU-funded project CRUISE [10] proposed the Hybrid Hierarchical Architecture (HHA) [11], see Figure 1 as a common framework for the research towards integrating WSNs with existing networks. HHA has been proposed as a reference network architecture which can support the vision for the development of ubiquitous sensorised environments. This type of architecture is a response to the need of integrating WSNs with existing communication technologies in many emerging application spaces. It integrates devices with heterogeneous capabilities and constraints, in particular concerning energy, memory, processing power, programmability, deployment, mobility, and wireless interfaces [12] [13]. In this novel architecture, the network edge must migrate towards the objects of the physical world and sensors and actuators which access it and provide data for the users. This includes simple devices such as passive RFIDs and active sensors which can organise within ad hoc networks and deploy mechanisms to exploit density and locality of the data. The data aggregated within WSN patches are accessed by wireless stationary or mobile devices which in order to communicate themselves may either use ad hoc communication or cellular network. Short description of HHA is presented later in Section 2.1 of this thesis.

As a result of the joint work, CRUISE project identified related open issues concerning energy efficiency, scalability, mobility, security, privacy and trust, middleware design, and fundamental theoretical constraints and integrated research efforts to make a progress in these areas. One of the open research issues was the need for system architecture, that could be context capturing framework that enables the convergence of many input modalities, mainly focussing on energy efficient WSNs that are multisensory in their composition, heterogeneous in their networking, either mobile (e.g. Body Sensor Network) or integrated in the environment e.g. from single sensors to a big number of sensors collecting information about the environment, a person or an object. This has been investigated in the EU-funded project e-SENSE [14] – Capturing Ambient Intelligence for Mobile Communications through Wireless Sensor Networks. The aim of e-SENSE was to enable context rich information availability (for user, social and environment) by means of multi-sensory intelligent wireless sensor networks that have hybrid mobile and fixed characteristics and thus provide the enabling technology to develop Ambient Intelligent Mobile Systems beyond 3G. Key research issues were energy efficiency; ultra low power and bandwidth efficient air-interfaces; security, privacy and trust; distributed resource management for wireless sensors; self growing, robust, and scalable wireless sensor networks.
In e-SENSE, flexible protocol stack architecture for WSNs was designed, which allows the incorporation of novel connectivity, management, and middleware concepts into the e-SENSE system including flexible security management. This architecture provides the advanced support functionality and high adaptability required for a wide range of application and deployment scenarios. The flexible protocol stack comprises of application, middleware, management and connectivity subsystems (Figure 1) which are presented in more details later in Section 4.5.

These two concepts are complementary to each other - CRUISE HHA is a network architecture that can be built using the e-SENSE system architecture. ***As this thesis has been carried out as a part of work done in these two projects and in relation to these two points of gravity, the work presented in this thesis will be put into the perspective of HHA and the flexible protocol stack with a general objective of the work to define how context-***

aware security and privacy services could be provided within the overall network architecture, in a way that covers the security needs of WSNs medical scenarios and the dynamic nature of context changes.

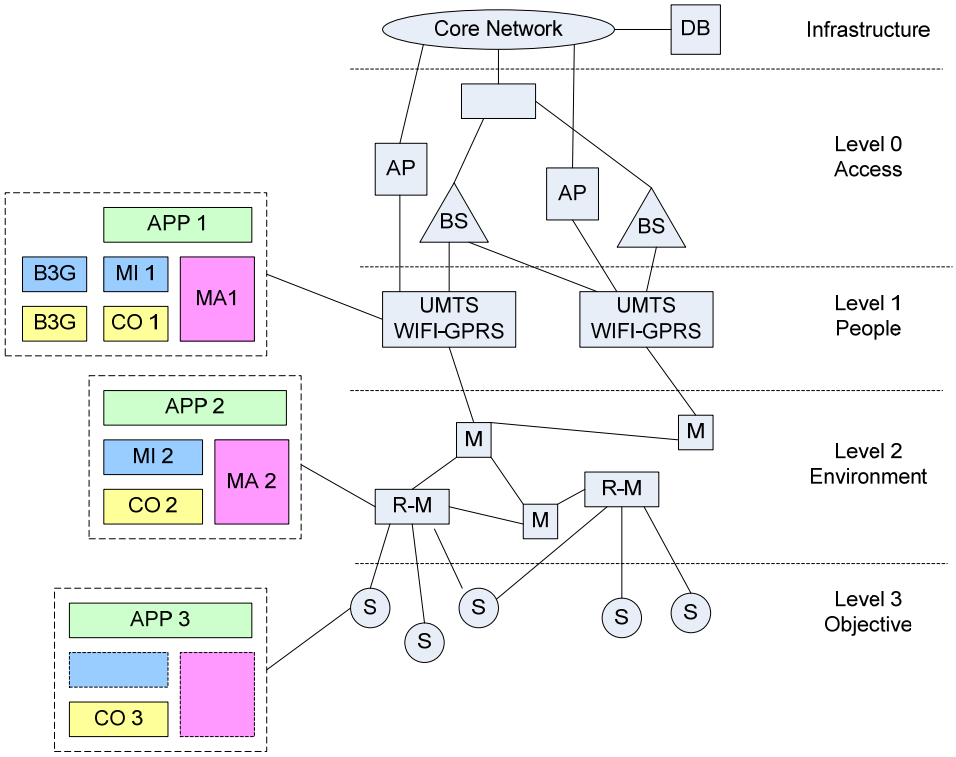


Figure 1: Hybrid Hierarchical Architecture introduced by CRUISE project and flexible protocol stack introduced by e-SENSE project

Legend: APP: Application Subsystem, MI: Middleware Subsystem, MA: Management Subsystem, CO: Connectivity Subsystem, B3G: Beyond 3G Component, DB: Data Base, AP: Access Point, BS: Base Station, M: Mote, R-M: Reader + Mote, S: Smart Tag

1.3 Thesis Motivation

However, for pervasive health care services using WSNs and body sensor networks (BSNs), ensuring security and privacy is a quite complex task for several reasons:

- Power efficiency – both the WSN and BSNs have very scarce power sources. The mobile terminals are also power limited.
- Heterogeneous devices – the pervasive systems will rely on integration of heterogeneous devices such as end-sensor nodes, aggregators, mobile terminals, smart phones, laptop and desktop computers with very diverse memory, power, and computation capabilities.
- The question of trust - There will be different services and different service providers. How the user will know which provider to trust?
- Unobtrusive operation – in order to be more user-friendly and intuitive and not to require a lot of interaction, the applications become more complex. However, this complexity must be hidden for the end-user. One way to achieve this is for the system to use available context information and take certain decisions on behalf of the user.
- User's control over disclosure of own sensitive data - Once released and (maybe) stored in different places, it is very difficult for the users to have control over to whom this data might be released at a later time or linked with their data from other services.
- The solutions must be adaptable and flexible enough in order to be applicable to many services.

Not much work has been done in most of the listed above points. These facts lead to the rationale to this thesis, namely proposing *enhancing privacy protection with context-awareness for WSNs in pervasive health care*, which focal points are to enable the systems to provide

- the best privacy protection for the end-users and their sensitive data, and the conditions in which they use a service unobtrusively and with minimum user interaction
- privacy protection services strictly necessary for what is needed for the healthcare service, the application, the groups of the end-users
- the most optimal level of security and privacy vs energy efficiency and memory usage

The following paragraphs present examples of scenarios for pervasive health and elderly care and highlight the above mentioned challenges.

1.4 Example scenarios for pervasive health and elderly care using WSN and BSN

The idea with the use of WSN and BSNs for pervasive health and elderly care is to support the medical, emergency or elderly care teams in the care for the patients in the hospital or in the after-care when they are recovering at home, to help the elderly persons to perform their daily activities independently and safely at home, to support the care-givers more efficiently to take care for their clients and last but not least to help the relatives to be informed all the time what is happening with their loved ones. All that diversity of services is linked to different types of end-user groups, each of them with a set of requirements for privacy protection, which in most of the cases are diverse. These will be exemplified in the following three examples:

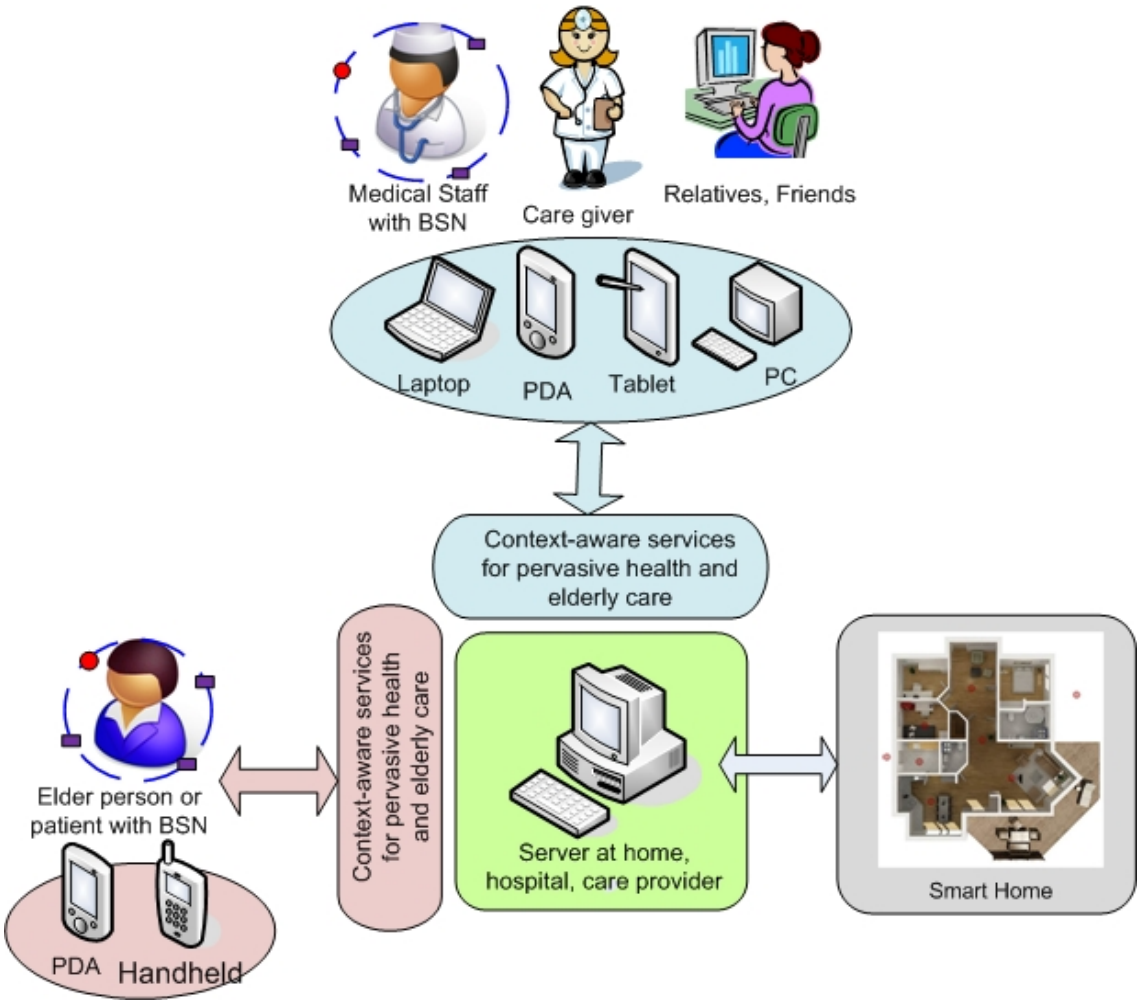


Figure 2: Overall picture for pervasive health and elderly care scenarios

Scenario for monitoring of patients at hospital

This is a "trivial" health care scenario - involves the use of sensors to capture the physiological status of patients with BSN, additional information from the sensors in the environment (locating patients, equipment, staff). The types of data taken into account are patients' related information, hospital administrative information, knowledge based information. The patients' related information includes pieces of data such as medical history, current medications, diagnosis, allergies, food plan, administrative data such as names, address, the closest relatives to be contacted in case some important and life-saving decisions must be taken on behalf of the patient, insurance scheme, social security number, etc. In case of emergency, if special equipment is necessary, the doctor must be informed by the system where this equipment at the moment is; or in case help of a specialised doctor is needed, the system must check where the back-up doctor is, is he available at the moment, and is it the needed specialist.
All these different pieces of information must be accessible to strictly defined medical groups. In case the information is very sensitive for the patient, it might be required that, the access to some parts of it happens only with the user involvement. If not, the system must self react based on pre-defined access rules and taking the current context into account.

For this to happen, the system must be configured to:

- Transmit confidentially the measured vital health status of the patient
- Define for each part of the patient's data which is the medical group authorised to access it
- Map a requesting party to a list of groups authorised to see a certain piece of information
- Check for the position of equipment and send notification or show the shortest path to get this equipment
- Check for a name of a specialised doctor in the hospital database, find the position of this doctor, check for his availability in the administrative system of the hospital

Scenario for elderly care - monitoring of behaviour and activities of daily living

Another scenario where the use of sensors helps in the care for elderly is behaviour and activities monitoring. It is about individual behaviour monitoring and the autonomous detection of critical long-term deviations. Here the home of the elderly is equipped with sensors in the floor, in the walls, in the kitchen equipment, in the bed which help to detect if any anomaly of person's behaviour occurs or the person is fallen down. Such system substitutes direct monitoring of persons with cameras, which in many cases is seen as going too far in protecting the privacy and dignity of elderly.
In this situation, if it is considered that one group of social-care personnel receives and sees collective information for all clients, the anonymity of the persons' identities and even addresses must be protected. If alarming event occurs and a care person must be sent to the home, only this person must know the exact address of the client in need.
Apart from this basic privacy protection, the clients must be sure that information for their patterns of behaviour will not be released to somebody who wants to use the time period when they are not at home to make robbery.

Here the system must use

- Suitable approaches for modelling context knowledge (user-/environment-oriented)
- Mechanism for data anonymity
- Mechanism to check if the party requesting address information is only the one authorised to access it

Scenario of integration of medical and social care (doctors and care-givers interaction)

In this scenario the elderly patients is at home under continuous care. They have a chronic disease and visit periodically the hospital or their general practitioner (GP) but in their daily life they are cared by social services. Here health related data are captured via BSN and the sensors from the home in the patient's home. The collected and interpreted patient's data can be used to give feedback about and to support medication intake, exercise regime, visits to the hospital or to the GP.
The user-groups here are the patients, health professionals, social-care staff and secondary users (e.g. relatives, friends). In order to be most efficient, the hospital, medical and social-care systems must communicate with each other sharing the information for the patient.
For the elderly persons themselves would not be possible to manage all coming requests for different pieces of their private information from different parties. The system must do it on their behalf once they or their relatives or the administrator of the service have specified it in the setup phase.

From a system point of view a number of things must be considered in order to protect the users as they want:

- The measured vital health status of the patient must be transmitted confidentially
- The medical and social staff must be able to coordinate their actions for a certain person only based on the minimum necessary data without knowing the rest of the privacy information for the user
- On request, the systems must provide exactly this piece of sensitive data which the requesting party is authorised to see – for example medications and latest medical results can be accessible to the GP, while the schedule of visits to GP must be accessible to the primary care-giver too. And this without intervention by the users. However they or their relatives must be able to see who and when has accessed the data.
- Security level of the BSN must be managed to save energy – for example lowest level when the user is at home and highest level when the user is in a public place. The system must "detect" where the user is and to have mechanisms to change the security level.

1.5 Goal of the Thesis and Problems Defined

Achieving a wireless pervasive system using heterogeneous devices (WSN, BSN, mobile terminals, smart phones, etc), which protects against *all possible* security and privacy threats and risks and at the same time does not use a lot of resources, is a very challenging task, even almost impossible to achieve. Therefore the work discussed in this thesis provides solutions to only a certain aspects of privacy.

The thesis proposes a framework that is capable of protecting all information which is considered private and sensible for the users who live surrounded by ubiquitous sensorised environments, by adapting to the changing context and using the minimum possible resources, and at the same time being unobtrusive in supporting their daily tasks.

The privacy objectives are defined as follows:

- **Maintaining *information confidentiality*,** i.e. to prevent any disclosure or manipulation of the message content to any other party
- **Maintaining *information privacy***, i.e. to prevent any disclosure of personal data or information directly related to the individual to a medical service or application without the user's prior approval or knowledge.
- **Maintaining *context privacy***, i.e. to prevent any disclosure of identifiable information related to the context in which the user is using the medical service and from which indirect information for the user could be extracted.

There are four main questions that this thesis seeks to answer, namely:

1. How to define a security and privacy framework which protect against the security threats and attacks most likely to happen and easiest to perform for the scenarios in question and does not waist system resources to protect against all possible threats and vulnerabilities at the highest level? That means – what is the threat model for pervasive heath carer system using WSNs?
    - Who are the main user groups which will be using this system, what are their assets

- What security and privacy requirements are valid for the reference medical-care scenarios
- What type of context information for the users' devices, users' environment could be used to threaten their privacy
- Which could be the access points to the system to materialise an attack and via which threat scenarios this could be materialised

2. How to define a security and privacy framework which provides exactly the necessary level of protection for a specific scenario and how flexibility and adaptivity could prevent waist of system resources
    - How could flexibility and adaptivity be achieved in the framework
    - Which privacy services and mechanisms could be made flexible
    - How to define deferent security levels which satisfy the diversity of the cases in which the pervasive healthcare systems will be used

3. How can privacy protection framework be extended so that it may use knowledge about the context to work autonomously without putting the burden to the user and be adaptive to the dynamic change of the context?
    - What type of context could be considered relevant to be fed into the system
    - What is the most efficient rule model to be used to combine context, conditions, decisions, actions
    - What number of rules and context attributes could be considered for the different categories of devices
    - What security protocols and mechanisms could form suitable security protocol suit having adaptivity and flexibility features for potential power savings

4. What is the cost of adding desirable features such as context-awareness and adaptivity to the privacy protection mechanisms for WSNs? In particular with respect to
    - Time to find the most appropriate privacy protection rule which is valid to the current context
    - Introduced delay from the privacy protection
    - Gain in efficiency if a proactive approach is used in reply to the dynamic nature of context changes
    - Power savings coming from the use of different security levels via suitable security protocol suit

Throughout the presented work these four questions remain the focal points of the thesis. These questions are divided into three main topics addressed in the thesis:

Threat model for WSNs in pervasive health care scenarios and overall mitigation plan:
Providing full security and privacy protection is costly for any system, because it introduces additional computations, communications and delays and makes the systems more complex. One standard solution ensuring the highest levels of security for all possible scenarios would be very costly. The challenge here is to define the threat model and based on risk management analysis, to draw up the overall mitigation plan to protect against most possible threats:

- Analysing threats and vulnerabilities for the discussed scenarios
- Analysing the specific security and privacy requirements derived from the scenarios
- Defining detailed threat model for the pervasive health care systems which considers the main actors, assets, their values, vulnerabilities, etc
- Proposal of a mitigation plan for the identified security and privacy threats and risks with mechanisms which fit into the system restrictions

Adaptive and context-aware privacy protection framework:
The development of a generic security management framework and security and privacy mechanisms capable to react on change of the context and at the same time achieving the best trade off between the security and privacy requirements and the optimal system performance. The challenges that are being addressed on this topic are:

- Introducing flexibility and adaptivity features in the generic security management framework
- Analysing and mapping different security levels to everyday situations in the discussed scenarios

- Proposing the building blocks of the generic security management framework and their interactions with the other entities of the system
- Defining the context attributes to be used to enhance the work of the security management and proposing context monitoring algorithm
- Defining suitable security protocol suit and privacy mechanisms for the different levels of security and privacy protection as a recommendation to the system designers
- Proposing generic context-ware privacy protection framework which fulfils the scenario requirements and is flexible enough in order to fit the requirements of the scenarios
- Proposing context-enhanced controlled information disclosure mechanism and adaptive security protocol suit

Performance evaluation:
A proof of concept test bed used for performance evaluation of different metrics related to the cost of the context-aware privacy protection and investigation of possible energy savings from the adaptive security concept. The main purpose of the evaluation through a practical implementation is

- To validate that the proposed concept for adaptive security and enhanced privacy protection holds promise for pervasive care scenarios
- To get estimation of gained energy savings when applying different security levels in typical everyday settings
- To obtain idea of how the applied context-awareness and adaptivity to the privacy protection impacts the performance parameters in terms of delay and complexity
- To provide the system designers with some practical directions for applying the proposed framework and mechanisms

1.6 Original contributions

Several original contributions have been studied and are presented in this thesis - solutions applicable for WSNs to countermeasure a subset of privacy threats to which pervasive health care systems could be exposed. In particular:

- Analysis of the security and privacy requirements of the scenarios of tele-health and tele-care, including also the requirements for relevant context
- Full threat analysis of pervasive health care scenarios with definition of threat model and mitigation plan for WSNs for pervasive health and elderly care application spaces
- Definition of generic adaptive security management framework for WSNs in pervasive health care scenarios which allows for the optimal energy and memory trade-off between the requirements and system restrictions and allows for personalisation and user friendliness
- Definition of context-aware privacy protection framework for WSNs in pervasive health care scenarios, integrated within adaptive security management framework
- Proposal of context-enhanced controlled information disclosure mechanism which can be tailored according the needs of all user groups and diverse set of scenarios
- Proposal of adaptive security protocol suit for confidentiality for WSNs in pervasive health care scenarios to provide different security levels and to comply with the heavy restrictions for power and memory of the end-sensor nodes without compromising the security

1.7 Thesis Outline

The rest of the thesis is divided in six chapters:

Chapter 2 presents the vision for the development of ubiquitous sensorised environments and introduces wireless sensor networks (WSNs) as the enablers of this vision. Further it presents the reference network architecture which can support such a vision – The Hybrid Hierarchical Architecture (HHA) and some related applications. It continues with overview of the major security and privacy threats and risks for WSNs. It further identifies the security, trust and privacy issues for WSNs coming from the specifics of HHA and it discusses the open research issues to be solved before the wide acceptance of WSNs. It further explains the implications which security, privacy and trust have on HHA. It finishes with review of the current approaches for solving these open issues and identification of research gaps.

Chapter 3 begins with short description of the main pervasive health care services using WSNs or BSNs and selects one reference scenario which will be investigated throughout this thesis, namely – the pervasive health and elderly care application space. Further the security, privacy and trust requirements derived from the scenarios are presented. The main aspects of Chapter 3 are the security threats analysis for health care applications with WSNs and definition of threat model which are one of the original contributions in this thesis. Risk management and overall mitigation plan are further presented.

Chapter 4 is one of the most important focal points of this thesis where other contribution is presented in details – The Adaptive Context-Aware Privacy Protection (ACAPP) Framework for WSNs as part of a generic adaptive security management framework. It starts with motivation for such a framework and presentation of the privacy objectives in this thesis. It presents the key features of this framework and how it is integrated in an overall Adaptive Security Framework. The main functionality and building blocks of the ACAPP Framework are further explained. Furthermore it is explained, how the security management and the context monitoring could be applied.

Chapter 5 presents the proposed context-aware and adaptive privacy protection mechanisms – for controlled information disclosure and security protocol suit providing adaptive confidentiality. Further, the applicability of ACAPP Framework to the reference scenarios is presented. In the end, the discussed mechanisms are compared with existing solutions.

Chapter 6 is the analysis and evaluation chapter. The proposed ACAPP Framework and mechanisms are first theoretically analysed. After that they are evaluated - starting with presentation of the evaluation goals and continuing with the results of the performed evaluation. It presents the costs of the privacy protection having features such as adaptivity, context-awareness and security management. It further evaluates the security management and the power savings from applying the adaptive security protocol suit.

The last Chapter 7 gives the overall conclusions and directions for future work.

References

[1] Lauren Davis, **WHO Predicts How We Will Die in 2030**, Nov 29 2008, http://io9.com/5100009/who-predicts-how-we-will-die-in-2030

[2] C. Lin, R. Lee, C. Hsiao, **A pervasive health monitoring service system based on ubiquitous network technology**, International Journal of Medical Informatics, Volume 77, Issue 7, Pages 461-469

[3] **TELEMEDICINE MEDICAL SERVICES - Biennial Report to the Texas Legislature** - Health and Human Services Commission, December 2008,

http://www.hhsc.state.tx.us/reports/TelemedicineMedicalServicesBiennialReport_December2008.pdf

[4] M. Tounsi, B. Qureshi, **A Bluetooth-enabled mobile intelligent remote healthcare monitoring system: analysis and design issues**, International Journal of Healthcare Technology and Management 2008 - Vol. 9, No.5/6 pp. 473 – 484

[5] Upkar Varshney, **Pervasive Healthcare and Wireless Health Monitoring**, Mobile Networks and Applications Journal, Publisher Springer Netherlands, Issue Volume 12, Numbers 2-3 / June, 2007, DOI 10.1007/s11036-007-0017-1, Pages 113-127

[6] **Challenges and Issues, Special Issue on Telehealthcare System Implementation**, International Journal of Healthcare Technology and Management (IJHTM), Volume 9 - Issue 5/6 – 2008

[7] Krishna K. Venkatasubramanian, Sandeep K. S. Gupta, **Security for Pervasive Health Monitoring Sensor Applications**, Fourth International Conference on Intelligent Sensing and Information Processing, 2006. ICISIP 2006. Publication Date: Oct. 15 2006-Dec. 18 2006 Bangalore, pp. 197-202. ISBN: 1-4244-0612-9, DOI: 10.1109/ICISIP.2006.4286096, Current Version Published: 2007-08-08, http://impact.asu.edu/publication/ICISIP2006.pdf

[8] Costanza-Sheedy, **A review of the legal and regulatory issues in telehealth and telenursing**, Journal on Telemed and Telecare 6(Supplement 1): 196; doi: 10.1258/1357633001934654, 2000; 6: 196

[9] Triantafyllidis, A.; Koutkias, V.; Chouvarda, I.; Maglaveras, N, **An open and reconfigurable Wireless Sensor Network for pervasive health monitoring**, Second International Conference on Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Volume , Issue , Jan. 30 2008-Feb. 1 2008 Page(s):112 – 115; DOI 10.1109/PCTHEALTH.2008.4571044

[10] Cruise website: www.ist-cruise.eu

[11] CRUISE Del 210.1 "**Sensor Networks Architecture Concept**", November 2006

[12] G. J. Pottie and W. J. Kaiser, "**Wireless Integrated Network Sensors**", Commun. ACM, vol. 43, no.5, May 2000, pp. 551-58

[13] **GENI: Global Environment for Network Innovations**, Technical Document on Overview- Wireless, Mobile and Sensor Networks, GDD-06-14

[14] e-Sense website: www.e-sense.eu

Chapter 2 – Background and State of the Art for Security and Privacy in WSNs

The aim of Chapter 2 is to set the scene for the discussions which will follow in this report. Namely, to present the vision for the development of ubiquitous sensorised environments and to introduce wireless sensor networks (WSNs) as enablers of this vision. Further it presents the reference network architecture which can support such a vision – The Hybrid Hierarchical Architecture (HHA) and some applications which could be supported by it. The other focus in this part is to provide short overview of the major security and privacy threats and risks for WSNs. It further identifies the security, trust and privacy issues for WSNs coming from the specifics of HHA and it discusses the open research issues to be solved before the wide acceptance of WSNs. It explains the implications which security, privacy and trust services have on HHA. It finishes with review of the current approaches for solving these open issues and identification of research gaps.

2.1. Introduction for WSNs

In this section it will be presented the vision for development of ubiquitous sensor networks and a reference network architecture by which the vision can be implemented, together with a short overview of the applications which can be supported by this architecture.

Vision for the development of ubiquitous sensor networks

The vision of the ubiquitous networks which integrates people and things [1] [2] is steadily coming into realisation within the maturing environment characterised on the one hand with the technological advances in wireless technology, hardware platforms, software architectures, networking concepts and data processing methods, and on the other hand, with attractive application opportunities.

In this global picture, the WSNs enhanced with the actuator capabilities materialise the interface between the people and the environment and establish a context for assisted living and emergency measures, intelligent production and transport, and environmental monitoring. In the long run, with the growing number of new applications, the ubiquitous networks will have to integrate the unprecedented amount of different types of communicating, sensing and actuating devices imposing significant constraints on the scalability of the mechanisms for network organisation, and data handling. European and International research communities have realised that this long term vision requires a novel hierarchical network architecture to integrate devices with heterogeneous capabilities and constraints, in particular concerning energy, memory, processing power, programmability, deployment, mobility, and wireless interfaces [3] [4]. In this novel architecture, the network edge must migrate towards the objects of the physical world and sensors and actuators which access it and provide data for the users. This includes simple devices such as passive RFIDs and active sensors which can organise within ad hoc networks and deploy mechanisms to exploit density and locality of the data. The data aggregated within WSN patches are accessed by wireless stationary or mobile devices which in order to communicate themselves may either use ad hoc communication or cellular network.

It is obvious that the research issues related to WSN self-organisation and data-centric operation needs partial refocusing with the inclusion of WSNs in this holistic hierarchical network architecture. The simple model of a single sink network must be replaced with already studied multi-sink model, however with a novel set of energy and topology optimisation requirements stemming from the fact that network control and information aggregation, storage and retrieval can span different levels of architecture and detached geographic locations. In particular mobility, which is immanent to almost all WSN applications, including mobility of objects and events, sensor nodes, relay nodes, data harvesters, and end-users, provides a fertile ground for novel approaches towards network self-organisation and data processing. Addressing the requirements of ubiquitous sensing and networking, the EU Project CRUISE [5] [7] proposed the Hybrid Hierarchical Architecture [6] [10] as a common framework for the research, and identified related open issues concerning energy efficiency, scalability, mobility, security, privacy and trust, middleware design, and fundamental theoretical constraints. This Hybrid Hierarchical Architecture will be the reference architecture for the proposed in this PhD report solutions for security and privacy for WSNs.

Overview of Hybrid Hierarchical Architecture

Hybrid Hierarchical Architecture is composed of four levels (Figure 2) [6] [10]. At *level 0*, referred to as access level, radio *access points*, for example fixed stations covering the area through Radio Access Networks – RANs - using air interface standards like e.g. GPRS or UMTS or WiFi, provide access to mobile terminals, denoted here as *gateways* carried by people (*level 1 - people*). These mobile devices can connect through a different air interface, e.g. ZigBee, or Bluetooth, to wireless nodes *(level 2 - environment*), with limited energy and processing capabilities, which are distributed in the *environment* and provide information taken from it. These wireless nodes, which may be sensor nodes (SNs), or beacons (providing localisation data) access the fixed network only through the gateways. Moreover they interact through possibly different air interfaces with tiny devices, e.g. smart tags, or very-low-cost sensors, which are part of movable *objects* such as books and tickets (*level 3 - objects).*

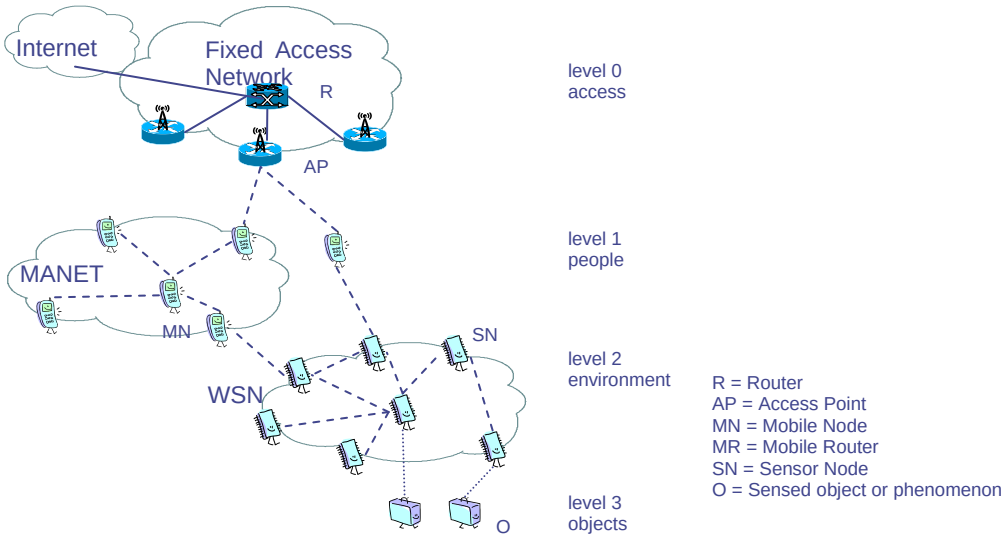


Figure 3: Hybrid Hierarchical Architecture [6], [8]

The proposed architecture is:

- **Hierarchical,** in terms of network organisation and data aggregation. Data will follow the hierarchy from the SNs to the mobile gateway and then to the access points (called as base stations in the cellular systems). Sensor nodes (level two – environment) can also be organised in hierarchical structures (i.e. tree-based topologies) including even lower level of radio nodes, like smart tags remotely read by the SNs.
- **Hybrid**, in terms of inter-working of different communication paradigms, routing domains, and addressing realms in different parts of the network. The mobile gateways link air interfaces based on different technologies: while WSN use self-organising infrastructure-less short-range low-cost types of radio standards, the transport networks are often based on complex centralised infrastructure-based standards like UMTS. The gateway should therefore be able to bridge very different types of networks.
- **Heterogeneous,** in terms of supported wireless interfaces. Different radio interface technologies are used in the different sub-parts of the network: low-power short-range standards in the WSN, such as e.g. IEEE 802.15.4 or Bluetooth, and cellular systems like GPRS or UMTS to connect the mobile gateways to the wired networks.

HHA applies to potentially **highly dynamic** networks with frequent changes of topology owing to the mobility at all levels of hierarchy in the forms of node mobility and network mobility. For example, mobile nodes in the role of sink nodes at level 1 may move with respect to the access points in the fixed network at level 0 – either individually or as members of a mobile network (e.g., MANET or MONET). Simultaneously, they may also move with respect to a network of sensors at level 2. Mobility may appear across levels and administrative domains, or

within a single domain among nodes that run a common routing or data dissemination protocol (e.g., in a MANET or among sensors in a WSN).

Short overview of the application spaces for WSNs in HHA

HHA can support a certain type of applications such as smart homes, healthcare and elderly care, environment and habitat monitoring, asset tracking, etc. In these applications spaces, WSNs will lead to more effectiveness, cost reduction and increased quality of life. These applications are briefly describe below:

Environmental Monitoring

WSNs in environment and habitat monitoring are expected to find wide applicability since they can be easily deployed in large areas and capture the spatial and temporal state of the monitored environment. Of relevance here is event detection and localisation where an event can be the outbreak of a forest fire, a release of a toxic substance in the drinking water reservoir [3], etc. A sensor field is deployed over a large area and nodes measure various signals (e.g. temperature or pollutant concentration). The main problem is to use the measurements to decide the existence of an event and locate its source.

Logistics Management

Atomisation of goods, new value chains, just-in-time production, globalisation and further developments in logistics require new technical solutions. WSNs and advanced communication will allow better surveillance of goods and even enable decentralised decision taking at the transport good, as for example investigated in the framework of the Collaborative Research Center 637 funded by the German Research Foundation. Sensors and RFID tags can be placed in the transport vehicles, as well as on the goods.

Emergency Management

In Emergency Management, e.g. fire-fighting and emergency aid after disasters, emergency forces cannot assume the presence of any communication infrastructure, but sensor information from different locations could improve their work. In a disaster scenario, the same technology would enable medics to more effectively care for large number of casualties. An integration of WSNs with fire-fighters is demonstrated in [4] - the focus is on the use of WSNs to directly support the fire-fighter when entering a building under fire.

Health and Elderly Care

In the medical and elderly care, outfitting care subjects or clients with tiny, wearable wireless sensors forming a Body Sensor Network (BSN) would allow medical or care teams to monitor the status of their patients or clients (either at hospital or at home). In this case, the BSN transmits the current readings of vital signs (heart beat rate, body temperature, blood glucose, etc) to the hospital or care-giver database. Medical staffs, emergency teams, general practitioners can then access the data when needed. In addition to that, with the ageing population in Europe, the costs for the health and elderly care will increase significantly [9] and in order the current living standard to be maintained, ICT integrated with WSNs will find very broad applicability. At the same time, in all these applications and scenarios in discussion, providing secure systems which preserve the privacy of the individuals, is of a major concern for acceptance of this technology. Solving the security and privacy issues in these applications is very challenging and posses a number of not solved for the time being research issues.

As it can be seen from the short overview, these applications are very diverse - have different needs in terms of: large/small scale deployment; interference-free / interference-prone environment; velocity required for the information; passive nodes /actuators, also diverse security and privacy requirements which in many of the cases are just opposite to each other. It is obvious that the security and privacy solutions for them must be customised and application-dependent. One standard solution will not be as effective and cost-appropriate as more tailor-made solutions applicable to a certain category of applications. This tailor-made approach was the motivation to investigate more closely the specific security and privacy requirements and the security threats for a set of reference applications using WSNs and for the different levels of HHA. This investigation is presented in Section 3.2. But before that, in the following paragraph security threats and attacks for WSNs are briefly summarised.

Summary of Section 2.1

In this chapter the vision for development of ubiquitous sensor networks was presented and the Hybrid Hierarchical Architecture with four levels as the reference architecture which can support this vision. Among the different types of applications which can be accommodated within HHA, the ones for health and elderly care will be investigated throughout this thesis. The motivation to select these reference applications was threefold – the prognosis for ageing population in Europe; the prospect for cost savings and increased quality of life when using WSNs for health and elderly care and numerous business opportunities; the number of un-solved security and privacy issues related to the use of this technology.

2.2. Major security threats and attacks for WSNs

In this chapter major security threats and attacks for WSNs will be presented. The focus will be on the threats to communication links, to routing protocols, to data aggregation, attacks on traffic analysis, threats to localisation, time synchronisation, reprogramming and information sharing. All these threats and attacks are considered to be major ones for WSNs [11].

Very schematic, the general architecture for WSN can be depicted in the following Figure 4. This architecture will be kept in mind when the major security threats and attacks will be presented in the rest of the chapter.

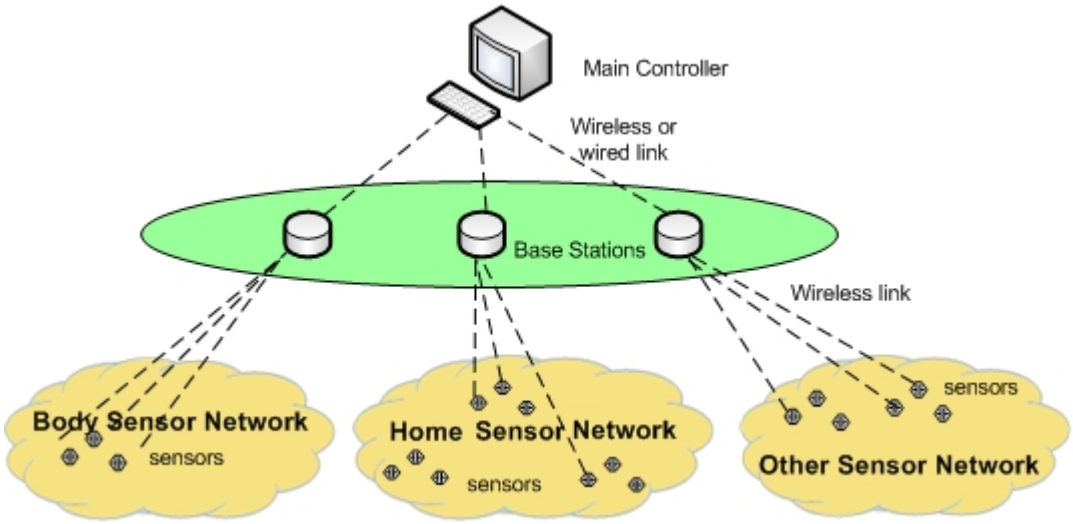


Figure 4: Hierarchical topology of a sensor network

All the sensor nodes are able to collect data and transmit it to the sink which sends information to the task manager node via Internet or satellite. Sensors are able to transmit and send data to all others. Of course, depending on the applications, there are modifications of this general architecture.

2.2.1. Threats to communication links

These threats could affect the confidentiality, integrity or availability of information by manipulating communications between WSN nodes.
Passive **eavesdropping** on communications between the WSN components to learn sensitive information is one of the simplest forms of attack. In WSNs communications, an adversary can gain access to private information by monitoring transmissions between nodes.
Masquerade or **impersonation** of a node can be used by an adversary to fool a node by sending sensitive information to an adversary's node that is pretending to be a legitimate node. Such an attack can also be used by an adversary to send illegitimate information by pretending to be a legitimate sending node.

Compromise of a node by an adversary can be used in the same ways as masquerade or impersonation. However, this attack eliminates encryption effectiveness for any communications directed through the compromised node.
With a **man-in-the-middle** attack, an adversary seeking (unauthorised) access to a node belonging to the SN inserts himself "in between" two authorised devices. Communications between the two devices are intercepted and manipulated. In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement.
Interference from deliberate **jamming** due to malicious nodes using the same frequency band can be used by an adversary to affect the availability of information. Jammers interfere with the radio frequencies the network nodes are using. Even sporadic jamming can be enough to cause disruption.
Denial-of-service (DoS) attacks can be used by an adversary to prevent nodes communicating, and thus affect the availability of information. Examples include flooding attacks and, in particular, battery exhaustion attacks (also called “sleep deprivation torture” attacks). DoS is produced by the unintentional failure of nodes or malicious action.

2.2.2. Threats to routing protocols

Attacks on routing protocols in WSNs can be particularly effective with relatively modest required effort. The general aim is either to completely disrupt routing like a DoS attack or to route traffic via a so-called "sinkhole" for eavesdropping, selective forwarding etc… Current WSN routing protocols do not consider security, and even though many have been designed for fault-tolerance, they do provide protection against random faults rather then against an active attacker. Security for routing in ad-hoc networks has been well studied, however, solutions here cannot be applied directly to WSNs. This is because they are too expensive (in terms of computation or communication) and solve a typical problem for ad-hoc networks - that ad-hoc network routing requires complete routing tables, not just routes from multiple sources to a sink as it is the case in WSNs.
Spoofing or altering routing messages can be used to divert traffic via an adversary's node. A special type of such attacks is the so-called "**Black hole**" attack. This is a type of DoS attack where the routing messages are disrupted in order to cause traffic to be diverted to a non-existent node or into infinite loops.
Routing can be diverted using so-called "**wormholes**" between two compromised nodes in order to capture traffic from widely dispersed areas. The idea is that the two compromised nodes can be linked with high-powered antennas and thus create a very attractive route compared to using the ordinary WSN links.
“**Sybil**" attacks are where a compromised node is able to assume multiple identities in order to compromise fault-tolerance mechanisms or to create sinkholes in geographic routing protocols.

2.2.3. Threats to data aggregation

In order to minimise communications in a WSN, data is normally aggregated at nodes along the path to the sink from the source nodes. Because of this, by compromising a node near to the sink, a large amount of the data being generated in the WSN can be affected, and therefore, this is particularly attractive for an adversary.
Attacks on data aggregation rely on an adversary compromising a node. This compromised node can then be used to **eavesdrop on aggregated data**, or to **add to, delete, replay or modify aggregated data**.

2.2.4. Traffic analysis attacks

Traffic analysis in WSNs can reveal sensitive information due to the unusual patterns of traffic in that kind of networks. This can work even if encryption is used to make communications unreadable. In addition, several applications of WSNs involve monitoring and tracking of people. In this case, traffic analysis can compromise the privacy of these people.
In WSNs where traffic flows between one or more sources and a single sink, an attacker can identify these by either **observing** the information directly, or simply following or **backtracking** the route. It may be possible to **infer events**. For example, just the existence of traffic in a WSN at a particular time could be used to infer the occurrence of a particular event (e.g. a particular condition has been observed by a sensor node causing it to relay this information to the sink). It may also be possible to **link events**, even if their precise details cannot be inferred. For example, the existence of traffic from multiple nodes at the same time could be used to infer that these nodes are monitoring the same conditions. A special case of this is **linking identities through matching pseudonyms**, which can be used to identify a person and defeat pseudonymity.

2.2.5. Threats to localisation

There are four aspects to location security:

- Securely reporting a location. This is mainly a data communications security issue which has been covered above.
- Location privacy. This is preventing observers from learning the position of nodes, which has also been covered above.
- Secure localisation. This is allowing a node to correctly identify its location.
- Location verification. This is allowing other nodes to correctly identify the position of a node (or more correctly, to verify it).

Attacks on localisation and location verification can be achieved through a **malicious node disrupting position identification and/or reporting**. The aim of the adversary is to give the nodes in the WSN a false indication of its, or their, position, which, for example, may lead to incorrect information being sent to the sink (e.g. an event reported with an incorrect location) or could be used to disrupt routing protocols.

2.2.6. Threats to time synchronisation

Time synchronisation is a fundamental requirement for WSNs to enable them to communicate effectively and efficiently. By disrupting time synchronisation, an adversary could cause denial of service, or incorrect timings of events to be reported to the sink.
The main means of defending against attacks on time synchronisation is the use of cryptographic communications security protocols. However, **jamming communications and/or relaying packets** (with an additional delay) can be an effective means of disrupting current time synchronisation protocols even with this protection.

2.2.7. Threats to reprogramming

WSNs may need to be reprogrammed periodically, perhaps to re-purpose the sensor, to send code patches or to update entire modules. The amount of data which needs to be sent to achieve this can range from quite small, for patches for example, up to very large, for entire modules or libraries. Being able to disrupt reprogramming of sensor nodes could be particularly attractive to an adversary. In the worst-case, this could allow the attacker to take complete control of all nodes, and this can even be done in such way as to be undetectable (except, perhaps, through inconsistencies with external data and observations).
Reprogramming could be disrupted by an adversary in several ways. The adversary could attack the WSN directly by a **man-in-the-middle** attack (i.e. adding to, deleting, replying or modifying communications), **masquerading/impersonating** the sender of the code update or **compromising the sending node**. The adversary could also try to impersonate the source of the code update, through either **masquerade/impersonation of the WSN manager** or even **masquerade/impersonation of the writer of the code**.

2.2.8. Threats to information sharing

In almost all of the literature on WSN security, security is considered from the point of view of one identified individual or organisation controlling the whole of the WSN and all of its information. This is the individual or organisation which controls the sink, or sinks, and receives all the information from the WSN. From this point of view, all information within the WSN has the same security ‘classification’ and all nodes have the same ‘clearance’ or permissions. Therefore, no access control for data is required within the WSN other than to ensure that only legitimate nodes can see it. In more sophisticated applications of WSNs, including those considered in this PhD report, multiple WSNs may need to share information to achieve a particular goal. These WSNs may be controlled by different individuals and organisations with different policies regarding their information, and therefore controlled release of information between these networks becomes an issue. **Inappropriate release of information** to adversaries (or equivalently un-trusted or partially trusted WSNs) may occur, allowing the adversary access to sensitive information. Other potential attacks include **eavesdropping**, **masquerading/impersonating** legitimate WSN gateways or nodes or **compromising gateways or nodes**. These are the same as the equivalent attacks on communication links, however, in this case the links are between WSNs rather than within them. Therefore, the analysis of these threats will be almost identical, but solutions to any resulting security requirements may need to be different.

The following Figure 5 summarises the security threats and attacks for WSNs and depicts where in the architecture these threats or attacks can appear.

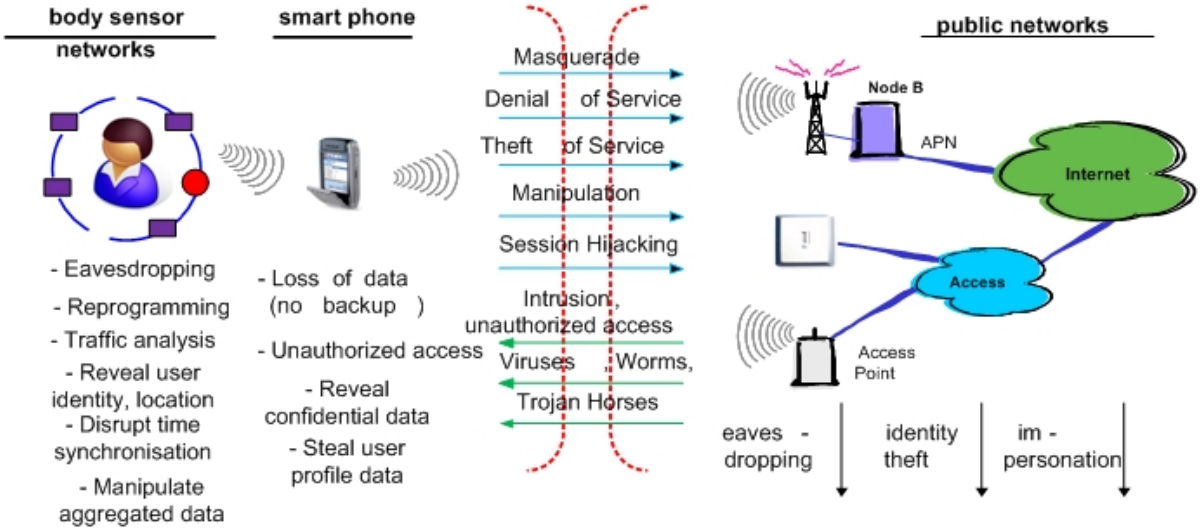


Figure 5: Security threats and attacks for WSNs

For a more detailed investigation on the security threats and attacks for the discussed in this report reference scenario, please refer to Section 3.3.

2.2.9. Summary of Section 2.2

The briefly presented in this chapter security threats and attacks show the scale of the problem. Proposing effective and appropriate solutions to all of them takes a serious amount of efforts. Therefore, in this thesis, the focus will be on solving part of the security and privacy issues - mainly on proposing solutions for protecting privacy. This will be countermeasures against threats to information sharing and communication links. From the depicted on Figure 5 security threats and attacks – reveal user identity, location; reveal confidential data; steal user profile data; unauthorised access. However, the knowledge about the presented in this section major security and privacy threats will be used to build up the threat model for WSN in medical scenario and to draw up a mitigation plan (Section 3.3.2).

2.3.Identification of security, trust and privacy issues for WSN in HHA

This section starts with discussion of security, privacy and trust problems for the reference architecture [10][11][12]. Further, open research issues for security, privacy and trust for the reference architecture are investigated. The implications which security, privacy and trust mechanisms have on the systems design of HHA are discussed too. The last focus of this section is the current approaches for solving security and privacy problems in WSN. In the end, the presented current approaches for solving the major security and privacy problems in WSNs are summarised and their pros and cons presented.

Security is a very important issue that needs to be considered in all HHA scenarios and applications. The nature of the wireless nodes in level 2 and the smart objects in level 3 poses additional challenges when looking at security, privacy and trust solutions. Therefore authentication, encryption, key establishment, secure routing, intrusion detection, secure data aggregation and secure service discovery, privacy and trust establishment are the main security features that are addressed in this section. They are viewed through aspects like network architecture,

threats and attacks, number of supported nodes, sink/gateway functionalities, and limitations posed by battery-operated wireless devices.
The main constraint for the security services for the battery-operated wireless devices in level 2 and 3 is the need for low power consumption. Since it is difficult to achieve low power by using SSL or similar technologies on devices like sensors and tags, low-level security protocols are considered. The latter exposes also the need for gateway security. The primary goal is to provide an infrastructure, where important data can travel through any medium that may not be secure, either this is a wireless node or a telecom network. For HHA, the goal is to provide security services to inter-connecting wireless networks and especially their inter-working with various access networks.
In the next paragraph list of the major security threats for WSNs in HHA are provided. Much more detailed threat analysis and mitigation plan for the referenced category is presented in Section 3.3.

2.3.1. Security Threat and Attacks in HHA

Threats and Attacks relevant for all levels

The goals of an attacker may be to prevent a network from functioning, to make it function incorrectly, or to acquire confidential information from the network. In the HHA, the following basic types of attacks [13] are relevant to all levels having wireless nodes, but the probability, nature, and impact of the attacks vary between levels. Even though the major security threats and attacks were presented in Section 2.2, here they are revisited again but from the point of view of HHA.

- Passive and active attacks on confidentiality and authentication. Examples of such attacks are listed below:
    - eavesdropping,
    - packet replay attacks, and
    - modification or spoofing of packets (e.g. through man-in-the-middle attacks).
- Attacks on network availability (DoS attacks) at different layers of the protocol stack (see also [14])
    - physical layer: jamming, tampering
    - link layer: collision, exhaustion called “sleep deprivation torture”, unfairness (misbehaviour)
    - network layer: some of the possible attacks are spoofed, altered or replayed routing information, selective forwarding, hello flood attacks.
    - transport layer: flooding, de-synchronisation
- Stealthy attacks against service integrity
    - making the network accept false data

In the following paragraphs, the factors that affect on how the threats may materialise at levels 1 and 2 in the HHA are elaborated.

Security Threats and Attacks in Level 1 (people)

The nodes at layer 1 are carried by people. So, the security measures are largely at the user’s discretion, which exposes the risks of false configurations or even intentional intrusion. Preservation of privacy is of great concern, especially when identity is needed for authentication or service personalisation. In MANETs, the problems with the broadcast nature of the medium are exacerbated by the distribution of control. Further, in multi-hop topologies, it is easy to eavesdrop and change routing. The mobility of nodes and networks sets challenges to seamless operation and thus blurs the boundary between the normal and anomalous function of the network.

Security Threats and Attacks in Level 2 (environment)

The threats and the forms of attacks that are specific to sensor nodes residing at level 2 are partially the same as those for level 1. However, in many application scenarios, WSNs have peculiar characteristics, which have an influence on the vulnerabilities and on the feasible counter measures:

- Sensor nodes are severely resource-constrained (in terms of computing power, memory, bandwidth, and available energy).
    - the network topology may frequently change due to node failure (possibly also due to mobility)
    - strong cryptographic protection with long keys or with using asymmetric algorithms is not feasible
    - an attacker may be much more powerful (e.g. a laptop) than the sensors nodes
- The nodes are vulnerable to physical attack and easy to capture
    - it is difficult to distinguish between a stolen node and a node that has run out of batteries
    - tamper resistance is difficult to achieve
    - losing a node might be recoverable through redundancy
- The nodes are supported by sink or relay nodes that reside at level 1 (people). This means that –
    - the data mostly originates from the sensors and traverses towards the sinks
    - nodes typically need to process the data along the route, e.g. for aggregation purposes (instead of simply forwarding it)
    - a sink may become a single point of failure (and thus also an attractive target of attacks)
    - due to the nature of communications, jamming (DoS) is a more likely attack than misbehaviour (attempt to obtain performance benefits)

Level 2 (environment) nodes may communicate with low-cost RFID systems (at level 3-objects), which may lack all security features.

2.3.2. Open research issues for security, privacy and trust in HHA

When examining the open security, privacy and trust issues, it is worth mentioning that the most important characteristics of HHA which cause the research challenges are:

- hybrid nature of the architecture due to interaction between different networks with different security services and trust establishment policies,
- large number of nodes in level 2 (environment) and objects in level 3 which might themselves be hierarchically organised,
- the nodes in the levels 2 (environment) and 3 (objects), even though with different resource constraints, are still very limited in computation capabilities,
- the sinks in level 1 (people) are mobile terminals.

In the following paragraphs the most important open issues coming from the specifics of HHA are discussed. The focus is first on issues which reside at level 2 (environment) and 3 (objects).

Data Origin Authentication and Encryption

Scalability issues due to large number of nodes

When level 2 (environment) has large number of nodes, it is a vital question how the authentication is done when not every node will have a unique ID. Open issues are how to select suitable cryptographic functions and protocols and how the keys are distributed in an efficient manner.

In [15] a localised algorithm for key establishment between a sensor node and a sink node suitable for sensor network deployment is proposed. The protocol provides security against a large number of attacks and guarantees that data securely reaches the sink node in an energy efficient manner. However, this method could be not very safe when the number of nodes is very large because if the authentication process is too long an adversary can compromise a sensor node during this process. So, it is important to investigate a faster authentication process.
Another approach is taken in [16] - the security architecture for medium and large scale WSNs proposed by the authors follows the probabilistic security paradigm for authentication and re-recognition; key pre-distribution - in a toolbox of security-aware components. The proposed Zero Common Knowledge (ZCK) protocol is an authentication protocol that establishes well-defined pair-wise security associations between entities in the absence of a common security infrastructure or pre-shared secrets. For key pre-distribution they suggest Topology Aware Group Keying (TAGK).

Variety of security mechanism due to different resource constraints

The mechanisms used for encryption differ according to the security needs and computational capabilities of the nodes. Due to the seriously limited system resources in level 2 (environment), security solutions applied in traditional networks cannot be directly applied. The goal of designing security mechanisms for level 2 (environment) is to provide energy-saving encryption function, supporting more suitable network security protocol and secure routing algorithm.
Few encryption algorithms are suitable for sensor networks with harsh resource constraints. Comparison of four different encryption functions (SEAL, RC4, RC5, and TEA) is done in [17] to evaluate their suitability for sensor nodes. Energy comparison and suitability for WSNs of TEA and RC5 is done in [18]. The authors observed that TEA uses less memory (static and automatic) than RC5 does because RC5 uses an expanded key table while TEA does not. The conclusion is that TEA uses lower amount of energy compared RC5 and Schneier's implementation of RC5.

Key Management and (Re-)authentication

In Section 2.1 it is described that the movement in HHA may consist of host mobility, network mobility, or node mobility within a sensor network. In a scenario with mobile nodes, there is the need for secure mobility because the distributed nature of a mobile and wireless environment makes it vulnerable to adversary malicious attacks. Especially, mobility puts stress on the distribution of key material that the nodes need for security functions (e.g. for message authentication). That basically means reiterating the authorisation, authentication and accounting procedures. This becomes problematic when high terminal number and density lead to longer paths. In this scenario a research issue is investigating the possibility of using decentralised re-authentication techniques based on symmetric key encryption that are secure, fast and energy-aware and to speed up the authentication phase when in presence of mobile nodes. In the presence of mobility, links are constantly falling and rising, a procedure or renegotiation of keys must be developed in a time and energy sensitive way.
Distributed authentication protocols and threshold cryptography algorithms must be evaluated to reach support for re-authentication in mobile WSNs. At the edge of an access network re-authentication can be accelerated with context transfer between access points (e.g. by using [19]). Within MANETs and WSNs, one approach is to distribute the authentication protocol by using threshold cryptography (e.g. [20]).
On other side, having mobile objects to track with the sensors introduces some different kind of impact over the security of the network. While the key agreement and access control of the network is unchanged, some higher level problems arise. As an example, in [21] the problem of the panda-hunter is described, in which the sensor network should be able to trace the movement of a moving source (the panda), without revealing it to some unauthorized attacker (the hunter). It can be seen that source-location privacy and other forms of anonymity are considered higher level problems, but they can be helped bringing them down to lower levels with a correct protocol choice or design.
Security is affected also by the kind of mobility the roaming object has. While [22] is based on the possibility of having a highly controllable mobility, this is not always possible. If the path of the moving object is predictable, this can help re-authentication, as described in [23] for wireless mesh networks. If the node moves on a predictable pattern, even if it is not always the same (in that case key caching can be used) the nodes on the path can proactively move credentials one to the other in order to proceed the arrival of the roaming node. This is particularly useful for moving sinks that might move in fixed directions (roads). If the movement pattern is

random, then such a prediction cannot be done and moving credentials will have as a consequence, the increased risk of delivering some sensitive keying material to some insider attacker.

Secure Routing

In level 2 (environment), the challenges to make the routing secure come from the fact that the communication is wireless, the nodes have limited capabilities, but the attackers can use powerful laptops. Another aspect of sensor networks that complicates the design of a secure routing protocol is in-network aggregation. Here to guarantee message availability is not enough. In-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages. The secure routing protocols have to be robust against many attacks, also node-capture attacks; to prevent injection of incorrect routing information, selective forwarding, etc [24]. Some approach proposed for large scale WSN does not need public key. Tokens are proposed to be sent to sensor nodes and they are pre-loaded. Those Tokens are used to substitute the public key and different events use different tokens.

Intrusion Detection

In the sensor networks from level 2 (environment), many potential sources of faulty packets exist. The source may be benign, such as a malfunctioning sensor reporting impossible data, or the source may be malicious - an outside attacker performing a denial-of-service by injecting garbage data, or a compromised node triggering false alarms or misleading data. A challenge here is how to remove or isolate the nodes which are possible sources of faulty packets. As a possible solution, Sensor Node Traceback Scheme (SNTS) to trace malicious packets into the network is proposed in [25].
At the same time reliable and timely detection of deviation from legitimate protocol operation is recognised as a prerequisite for ensuring efficient use of resources and minimising performance losses [26]. The basic feature of attack and misbehaviour strategies is that they are entirely unpredictable. The random nature of protocol operation together with the inherent difficulty of monitoring in the open and highly volatile wireless medium poses significant challenges.

Secure Data Aggregation

As mentioned in Section 2.1 for hierarchical data processing, data regarding context from lower levels (level 2-environment and level – objects) in the network will be produced in huge quantities in the future, posing gigantic problems in network scalability. By increasing the number of sensor nodes, the amount of information gathered at the sink becomes excessive with respect to its communication capacity either towards the transport network if it is a gateway or towards the WSN. A security encryption scheme requests the transmission of extra bits that means additional processing, memory and battery power consumption. This might require the use of relevant in-network data processing techniques such as data aggregation or distributed and collaborative signal processing, which increase the need for large computing capabilities at the sensor nodes. In [27] a series of techniques to support a large number of senders broadcast authentication capabilities from compromised senders using the μTESLA broadcast authentication protocol as a building block are developed. These techniques use multiple μTESLA instances with different parameters to provide additional capabilities related to broadcast authentication.
In addition, more heterogeneous data is being collected. A challenge here is the data aggregation and reduction of context data within sensor networks from level 2 (environment) which also influences the secure data aggregation. It is an open question how to efficiently store the past data and authenticator, as well as the challenge that the verifier either needs to compute many one-way functions for deriving the current key of a node or that the verifier needs to store one key per node.

Secure Context and Service Discovery

Some applications and services in HHA will heavily rely on collecting information from the context provided by level 2 (environment) and 3 (objects) and analysing it in order to intelligently support the end-users in their daily interactions with context-aware applications. However, the provision and the aggregation of context information from motes and objects introduce some security threats and vulnerabilities which have to be carefully analysed.

For example how one can be sure that the information for some physical parameters of the environment has not been intentionally altered by an attacker. Trustworthiness of the context and service providers has to be evaluated [28]. One approach is comparison of the data from other sources using redundancy. Suitable models for threats coming from context delivery and methodology for threat analysis have to be designed in parallel with the advances in the HHA context-aware systems. There is a need for a general secure context management architecture framework which can successfully prevent attacks coming from context.

Privacy and Anonymity

In the application areas with heavy user involvement, like smart house and health and elderly-care (Section 1.4), the subjects of the collected data from the level 2 (environment) nodes are directly real persons as the end-users. The communication within and out of the WSNs, possibly contains sensitive data related to them. It is a privacy requirement to keep this data confidential and privacy of other information, related to the communications like the identities of the commutating parties, the frequency of the communications and the size of the messages, the time and the location, etc, is not to be revealed. Even revealing context information for the user's handheld device from level 1 (people) such as CPU usage, battery power, free memory, etc can also be used to derive information of where and how a user is using a device [29].
For maintaining the privacy of the users themselves, their anonymity has to be ensured – the users should be able to use resources or services without being distinguished from other users and without disclosing the user's identity and/or location to third parties but at the same time the means of accountability should be provided.
The proposed solutions should ensure privacy in a way that:

- Information privacy is maintained, i.e. to prevent the disclosure of personal information to attackers by giving away information only to trusted entities.
- Anonymity of the users for distinct scenarios is preserved, i.e. preserving their "state of being not identifiable within a set of subjects" **Fejl! Henvisningskilde ikke fundet.**. Anonymity affects also location privacy, because as long as a user or a node is anonymous, location privacy is provided.
- Location privacy of a node is maintained, i.e. to deny an attacker the knowledge of a node's current and past location.
- Trust is established with respect to the confidential treatment of private information by a peer, as a basis for controlled disclosure of information.

Trust Establishment

While HHA has an advantage to solve partially the scalability issues of the traditional large WSNs, it imposes more challenges on the trust establishment concepts. From the open issues which come from the interplay between different levels, it can be mentioned more specifically, transitivity of trust – e.g. how a level 1 (people) node that authenticates with level 0 (access) gets authorised to communicate to level 2 mote (environment). Another important question here is how the policy negotiation will be done when different policies meet from level 0-access, level 1-people, and level 2-environment.

2.3.3. Security, Privacy and Trust Implications on HHA

The solutions to be proposed for the briefly summarised security, privacy and trust open questions listed in the above paragraph, will influence the overall design of frameworks, protocols and mechanism for HHA. Security, privacy and trust services will have implications on a number of aspects of the HHA, the major listed below:

- topologies – if level 2 (environment) itself has multi-hop topology, the security services will lead to additional node to node simple authentication and authorisation mechanisms in the communication process. Mobility capabilities in level 1- people and level 2 (environment) will lead to the necessity of additional mechanisms for fast authentication and key management. For applications with multiple sinks, this will lead to more complex models for the point of trust. In the applications where level 2

(environment) and 3 nodes (objects) are very large number, scalable and power-efficient solutions for key establishment and authentication are required.

- protocol architecture – in general the incorporation of the security services will increase the overhead, delay and complexity of all layers the security requirements. It will also increase the complexity of the routing protocols with embedded security functionality.
- middleware – the need to protect privacy of user data, user identity, location, presence will lead to introduction of mechanisms for privacy, trust, pseudonimity and anonymity which of course will have their costs.
- trust establishment - need of strong trust establishment mechanisms which take into account the fact that any mobile terminal from level 1 (people) might play the role of data fusion centre and process the data gathered from the SNs from level 2 (environment) and objects from level 3

2.3.4. Current approaches for solving security and privacy problems in WSNs

Following the short summary of the major threats and attacks for WSNs, presented in Section 2.2, this section deals with the recent developments for security and privacy in WSN and the current approaches to counteract the threats with focus on the health and care scenarios. It is assessed how suitable these approaches are for the pervasive health scenarios and identify where gaps exist in the current state-of-the-art.

Solutions for Security of the Communication links – confidentiality, authentication, key establishment, etc

Key establishment

Cryptographic keys are usually required in WSNs in order to provide some of the basic security functionality. In particular, they are needed in order to provide confidentiality and integrity protection to the communications within WSNs, the threats to which have been identified as high risk for the pervasive health scenarios.

Depending on the application scenario, shared keys may need to be established between all neighbouring nodes, any pair of neighbouring nodes, nodes and ‘cluster heads’, nodes and the sink (or sinks), or other configurations. However, a typical requirement is for any pair of neighbouring nodes to be able to establish a shared key. The desirable features for such key establishment are:

- Sensor nodes should be able to establish keys with other nodes using only preconfigured information.
- It may not be possible to know beforehand which sensors will be located where, and therefore the key establishment should be possible regardless of which nodes end up being neighbours.
- The preconfigured information in each node should be as different as possible from other nodes, otherwise compromising one node could lead to compromise of the entire WSN.
- Key establishment should require minimal storage, memory and processing power as well as minimal communication.
- It should be possible for sensors to establish keys with new nodes introduced anytime time after the initial deployment.

The traditional way of meeting these requirements would be to use public key cryptography, however, the use of symmetric keys may also be possible. Some methods are discussed in the following paragraphs.

Key establishment using preconfigured public/private keys

The traditional way of solving the key establishment problem would be each sensor node to be set up with a unique private key before deployment. The associated public key would be signed by a recognised authority (e.g. the owner of the WSN), and the obtained certificate, together with the authority's trusted public key, would also be preconfigured into the node. After deployment, nodes wishing to establish keys between each other would simply swap their certificates, verify the validity of the certificates with the authority's trusted public key, and then exchange symmetric keys with each other using one of the available protocols (e.g. Diffie-Hellman).

The main problem with this approach is the amount of processing power required for the algorithms used, which generally makes it infeasible. However, as noted previously, it can be possible to do this in some cases. In addition, various optimisations have been worked on which make use of the likely, or imposed, structure of the

WSN after deployment. For example, protocols can be designed so that more powerful 'cluster-head' nodes have to do the bulk of the processing.

Therefore, depending on the application scenario, the use of public key cryptography in this way may be possible. However, it is also true that if its use can possibly be avoided, then it should be.

Key establishment using preconfigured symmetric keys

If neighbouring nodes already share a common symmetric key, then the use of computationally expensive public key cryptography can be avoided. However, this is complicated by the fact that when reconfiguring keys into sensor nodes, the topology may not be known i.e. which nodes will be neighbours after deployment. A naive approach would be to give every node the same symmetric key, which would guarantee that neighbours would share the same key. However, in this case the compromise of one node will reveal the keys for the entire WSN. As compromise of the nodes is a high risk in WSNs, this situation should be avoided.

The main approach described in the literature to this problem is the use of 'random key pre-distribution schemes'. The idea is that each node is preconfigured with a randomly chosen set of keys from some larger key space. The aim is that two neighbouring nodes will then share at least one of these keys after deployment with a certain probability. The theory for this has been worked out, and practical schemes are available. However, the main problem with them is that they do not scale to very large sensor networks.

In summary, many methods are available for key establishment and this is a well studied area. Therefore, it should be possible to provide keys for pervasive health scenarios in a suitable way with existing techniques.

Nodes Compromise

As said before it is very easy to gain access to a node and to control it because usually they are in accessible areas. A compromised node may exist in the form of a subverted sensor node or it can be a more powerful device with more capabilities. When a node is compromised, the adversary is already inside the WSN and has access to the node key, which means it is very important to detect this intrusion as quickly as possible because he has all the means to a disrupt or paralyse the network or even to steal secrets. The most common attack is the flooding of messages to the base station which will cause a DoS due to large amount of data to process. Of course this is related with the hacker intentions, if he wants to steal secrets or to mislead the network he should not paralyse it.

There are several proposed solutions to face this problem. Some of them are the following:

- **The use of redundancy** [31]– redundancy means the use of several nodes in order to obtain redundant information. With this "extra" data it is possible to check if a node is sending misleading information which would cause its immediate detection. This technique works very well if it is adjusted with a good comparison algorithm. The drawback of redundancy is related with economic issues. It is in the best interest of all parties to have the cheapest sensor network possible, so by adding more sensors than it is actually needed, it will compromise the budget. Another objection for this solution is that when one of the main parts of the pervasive health care systems is BSN, it is not possible to keep adding many sensors to the person's body - this solution is not very suitable.
- **Code attestation** [32] – the use of code attestation enables the possibility to validate the code running on each sensor because the code running on a malicious node must be different from that on a legitimate node. By verifying their memory content compromised nodes can be detected. Code attestation can be achieved through software or hardware. This technique needs more research, the direction will be the design of software or hardware capable of verifying the codes within the sensors without consuming much resources.
- **A Voting System [32]** – since it is desirable to detect and revoke compromised nodes as quickly as possible, a proposed solution is the use of a distributed voting system. The strategy of this system is to have the nodes which are working well to vote against those who are misbehaving. If a sufficient number of votes against a node which is giving misleading data (either by malfunction or compromised) all the others nodes will refuse to communicate with it. This technique has an obvious flaw, the malicious nodes can also vote which of course will try to deceive the network by voting on the nodes that are behaving properly. A solution to this situation is to limit the number of votes which node can make. By doing so the hacker will not have sufficient votes to misinform the network. However, here the same comment as for the use of the redundancy applies.

- **Secure Localisation [32]** – this technique is an important base in sensor networks. A sensor node can accurately determine its geographic coordinates in any environment, therefore if a malicious node tries to claim a false position it will be immediately detected. This method will also be very useful against the wormhole attack or the Sybil attack.
- **Tamper-resistant [32]** – using this kind of technology on the sensor nodes is very expensive and it should not be forgotten that the goal is to have a network as cheap as possible; therefore this solution is not very suitable.

Eavesdrop on the networks radio frequency

As mentioned before the use of a wireless communication system has its natural weakness. The network communicates through radio waves which can be captured by foreign antennas. Once the attacker has caught the network's signal he may try to read it. The best solution against this problem is the use of cryptographic primitives [32]. The use of more robust cryptographic techniques is limited by the sensor nodes processing capabilities and energy consumption. However, more research in the asymmetric cryptography or the elliptic curve cryptography [31] may bring new solutions more resistant to these kinds of attacks. It must be kept in mind that if the attacker is allowed to listen to the network's communication for a long period of time, he may be able to collect enough data to decipher the code. The cryptographic code (keys) should be changed between short periods of time (depending on the level of security desired).

Jamming

Basically the attacker sends an impulse with enough power to overcome the network's signal. The results of a successful jamming attack will cause temporally breakdown of the system. The usual defence against this situation is frequency hopping and spread spectrum communication [32]. Although they are not 100% effective, they will force the attacker to use much more energy to cause temporary malfunction of the discussed system (DoS).

Packet injection

The name of this attack already explains by itself, the hacker will insert in the network several streams of bits in order to overload the system causing temporally DoS. The solution for this problem resides on the use of authentication [32]. Trough this technique a node will be able to verify the origin of a packet and ensure its data integrity. This method works perfectly unless a node is captured, i.e. the attacker has access to the key used by the node and so he is able to use it for transmitting authenticated messages.

DoS - Disabled sensor nodes / node failures/energy depletion

All electronic devices have a certain probability of failure or malfunction. This is especially valid for the pervasive health and care applications, since in BSNs the sensors must be small and will be attached to the body of a person, meaning that they will be under constant risk of falling or folding. Or they are just out of battery. If it is WSN with many nodes, according to the level of security wanted for the network and the accessibility of nodes, it may be useful to use redundancy, i.e., the use of more than one sensor to collect the same or approximately equal data. However, this is totally not applicable for applications with BSNs placed on the person's body where there are just a few sensors. So, this threat is very realistic for the reference scenario but extra nodes could not be used. The only way to reduce somehow the impact of it, is to have a good monitoring and notification mechanism for lower battery level or for node malfunctioning.

Solutions for Data Aggregation

From the threat analysis which will be presented in Section 3.3, it could be seen that attacks on data aggregation in WSN have been identified as a high risk for the health and care scenarios.

Proposed mechanisms to protect against data aggregation threats are mainly against node compromise. In summary, this is an area that has received little research attention to date, and is particularly important for the reference scenarios.

Solutions for Traffic analysis

From the threat analysis which will be presented in Section 3.3, it could be seen that traffic analysis attacks in WSN have been identified as a moderate risk for the health care scenarios.

Where such attacks affect privacy, potential countermeasures are covered in the next paragraphs. Some other options are discussed below.

In WSNs where traffic flows between one or more sources and a single sink, an attacker can identify them by simply following or back-tracking the route. In [33], several ideas for how to protect against this are given. These include:

- Multi-Parent Routing. Here, a packet is randomly sent to a node closer to the sink.
- Random Walk. With this technique, packets are usually sent to a node closer to the sink using Multi-Parent Routing, however, they are also occasionally sent to any random neighbour.
- Fractal Propagation. This is an enhancement of Random Walk where fake packets are created and forwarded in random directions to further hide the true direction of real traffic.

Further enhancements of the above methods are also possible, such as in [34]where Random Walks from the sources are combined with partial routing trees from the sink to provide similar protection but with improved routing efficiency.

In summary, some techniques to prevent traffic analysis are known, and it is not a major consideration for the scenario considered in this report. Therefore, further research here is not a pressing requirement for us.

Solutions for Localisation

Attacks on localisation in WSN have been identified as a moderate risk for the discussed scenarios.

Methods for secure localisation and location verification are mainly physical in their nature, relying on measurements about received radio signals. "Verifiable Multilateration" [35] is such a technique, which uses measurements on ‘time of flight’ of RF signals to determine distance to other nodes. This is combined with triangulation to determine position. To prevent malicious nodes from disrupting the protocol, a cryptographic 'blind commitment' protocol is used to ensure that nodes can only increase their claimed distances. These increases can then be detected through distance measurements with legitimate nodes. The technique can work with locator beacons, whose positions are fixed and known, or in a completely decentralised WSN. However, it does require accurate timing on the sensor nodes (at a nanosecond level).

A slightly different technique is used by SeRLoc [36]. This makes use of directional antennas on sensor nodes to enable them to determine a rough direction for locator beacons, whose positions are fixed and known. A "centre of gravity" technique is then used by each node to estimate their position. This is much simpler than Verifiable Multilateration as accurate timing is not required. However, locator beacons must be used and the technique cannot be used in completely decentralised WSNs. In addition, there is a relatively complex security model, which is needed to protect the broadcasts from the locator beacons.

In summary, some techniques to prevent attacks on localisation are known, and, like traffic analysis, it is not a major consideration for the health care scenarios. Therefore, further research here is not a pressing requirement.

Solutions for Time Synchronisation

Attacks on time synchronisation in WSNs have been identified as a high risk for the health care scenarios.

In [37] these issues are addressed with modifications to existing protocols and the definition of new ones that can protect against these attacks. The coverage seems fairly comprehensive, but there might be scope to provide some improvements.

Solutions for Reprogramming

Attacks on reprogramming in WSN have been identified as a high risk for the pervasive health care scenarios.

Secure reprogramming is only really a problem for large and geographically dispersed WSNs, where the sensor network itself has to be used to distribute the updates. This causes significant problems for authentication in the presence of compromised nodes. There are some proposed solutions to this problem, such as [38] and [39] which make use of so-called "stream signatures", and use one or both of hash chains or hash trees. Approaches based on hash chains require packets to be received in the correct order, which can be hard to achieve in unreliable WSNs. Hash trees relax this requirement, but introduce their own problems due to a relatively complex setup stage. Therefore, finding a good solution for large code downloads appears to be an open problem.

In summary, secure reprogramming is highly important for the discussed scenarios, and although some proposals have been made for how to do this, these are in general only partial solutions. Therefore, further research is required here.

Solutions for Trust Establishment

The trust establishment frameworks which have been proposed for ad hoc and sensor networks can be classified into two categories, namely certificate-based and behaviour-based. This is done according to their scope, purpose and type of evidence that trust evaluation is based on [40]. Certificate-based frameworks aim at defining mechanisms for pre-deployment knowledge on the trust relationships within the network, usually represented by certificates, to be spread, maintained and managed either independently or cooperatively by the nodes. Trust decisions are mainly based on the provision of a valid certificate, which proves that the target node is considered as trusted either by a certification authority or by other nodes that the issuer trusts. In behaviour-based frameworks, each node performs trust evaluation based on continuous monitoring of the behaviour of its neighbours, in order to evaluate how cooperative they are. Trust is evaluated both independently by each node, based on using the statistical data that is being continuously accumulated, and cooperatively through sharing recommendations and spreading reputation.

The main challenge confronted by certificate-based frameworks for ad hoc networks is the lack of pre-established infrastructure, which hinders the use of on-line certification authorities. In the framework proposed in [41], trust is represented by certificates signed by off-line certification authorities, whose public keys the trustors maintain locally in order to verify the signatures. Hubaux et al. [42] propose a distributed public key management scheme, where trust is evaluated using certificate chains similarly to the ”web of trust” approach of the PGP model, with the difference that each node maintains locally a subset of the trust graph. In the mobile certification authority framework, presented by Yi and Kravets [43], secret sharing mechanisms are used to distribute trust to an aggregation of nodes that can collaboratively provide certification authority services. The distributed trust establishment framework proposed by Eschenauer et al. [44] takes a broader view on the inputs required for trust decisions by accepting as trust evidence not only certificates and public keys, but also information like identities, locations, or independent security assessments.

Trust in behaviour-based frameworks is formulated as a combination of the direct trust value to the target node, which is evaluated independently by the trust issuer based on previous interactions and network traffic monitoring metrics, and the indirect trust value derived from the recommendations of neighbouring nodes. In the reputation-based framework for sensor networks [45], a watchdog mechanism is used for monitoring the behaviour of neighbouring nodes in terms of data forwarding and raw sensing data consistency, and a Bayesian formulation is proposed for representing node reputation and trust evolution. Huang et al. [46] developed a trust evaluation model targeted for sensor networks, where the Dempster-Shafer Theory of Evidence is proposed for combining recommendations. Confidence values are assigned along with the recommendations in [47] where trust and confidence values are mapped in a trustworthiness composite metric, and [48] where the trust inference problem is formulated as a shortest path problem on a weighted directed graph and theory of semirings is being used.

However, both the behaviour-based and the certificate-based frameworks that have been proposed are better targeted for ad hoc than for sensor networks. The main reasons are that they do not exploit the pre-deployment knowledge that will usually be available in sensor network deployments, and they do not allow for pre-established, stable trust relationships. None of the behaviour-based frameworks includes any bias with respect to the identity of the node under evaluation. From the certificate-based frameworks, this requirement could be satisfied by the framework proposed in [44] through introducing identity related bias in the trust metrics and policies of the nodes, and [42] through appropriate selection of the locally stored subsets of the trust graph. Moreover, the computational complexity of the certificate-based and the energy requirements of the behaviour-

based trust evaluation frameworks raise concerns related to their applicability on resource constrained sensor nodes. The former category uses asymmetric cryptography which is considered as too expensive for sensor nodes. The frameworks in the latter category are resource consuming in terms of computation, memory and energy, since they require the radio on each node to be continuously on, and the trust values of the neighbouring nodes to be stored and continuously updated as interactions occur.

Solutions for Secure Profile Management

A success factor for ubiquitous sensorised systems and the services they could offer is their personalisation, i.e. the ability to take into account user's preferences, presence information, location, etc in order to support the users and to enhance their experience. Therefore, for a better service, in scenarios like pervasive health care, it might happen that the user would have to reveal personal information to basically non-trusted third parties. In order to meet these apparently contradictory requirements, the system has to integrate privacy and identity management mechanisms while at the same time preserving trust and privacy and offering user-friendly navigation of available services and improved user experience. The scenarios discussed in this PhD report are user-privacy sensitive and differ at the level of processing and revealing confidential and private data for the persons. In some cases the user seeks full anonymity (for identity, location), in others, a certain part of the private information (medical history, health status, medications, address, social security number) may be available to specific and strictly defined categories of persons specified by the users themselves. Here comes the need of offering the user to have and manage several virtual identities and roles supported by profile management mechanisms. End-users or network administrator can specify different sets of rules for different identities and/or identity levels and for different levels of privacy.

Therefore, it is of key importance to develop a conceptual structure of user profiles for WSNs, which is flexible, scalable, dynamic, supports conditional access control, and can be smoothly integrated with available context information. Currently the technical means for the realisation of personalised services and context-aware services and applications are the user profiles and context modelling. The working group of IETF, the rich presence information RPI, defines a structure and a transport mechanism for presence information. Ideas for distributed profiles with a single point of access can be found in the 3GPP generic user profile work. One of the chosen approaches is that the policy framework has to be in place to control the exchange of profile and context information. Policies advertised by external applications declare the parts of profile and the context needed by that service. Only a matching of such a policy with the internal user privacy rules will lead to the exposure of the required profile data [49].

However, even though some proposals for profile management exist, the building of user profiles and context profiles requires a standardised and extensible framework.

Solutions for Privacy Protection

Controlled disclosure of personal information

Policy-based approaches with end-user involvement in defining the policies, are another side of access control methods that allow a user to specify the policy specifying who is able to access their location information and sensitive data and with what accuracy. This is done with the help of an agent responsible for policy enforcement. Examples of these approaches have been already described in the beginning of this section. However, more work is needed here to design flexible systems by which the end-user or the administrator can easily configure new features and add new pieces of personal information depending on the goal of the services.

Privacy of context information related to persons

The design of pervasive health services closely relies on information from the context, fed to the management subsystem, in order to smartly support the end-users in their daily interactions with the context-aware services and applications. However, the provision of context information introduces some security threats and vulnerabilities as discussed in Section 2.3.

Privacy issues related to the access of user information are becoming increasingly important following the movement toward ubiquitous environments and devices acting on behalf of the user. As in the pervasive health application scenarios, sensitive private information for the end-user (for example doctor, medical staff, patient, social or home care staff, etc), such as names, address, health status, medical history, has to be revealed in order the user to take advantage of context-aware services. The key issue here is the development of automated privacy protection mechanism to control how, when and to whom a user's sensitive information has to be disclosed. Such mechanism could have predefined user preferences and a policy module. The goal is to give the end-users the power to easily manage their own privacy without being an expert in the domain. Main features of such mechanism are policy based access control, pessimistic and optimistic approaches for access control, hierarchical privacy rules, mixed-initiative interaction as presented in [50].

The authors of [50] define a privacy service for protecting context information in context-aware environments that grants or denies access to a very limited set of context data based on predefined policies. The approach focuses on developing means to define and use tailored policies for their frameworks adapted to their use case – collaborative mobile service. Existing approaches rely on the minimisation of the data disclosed and taking decisions with policy engine. The user is mainly involved for making final high-level decisions and for giving consent to data processing.

As the context-aware applications and services will use more and more diverse type of context information, provided by different parties, suitable threat models coming from context and methodology for threat analysis have to be designed in parallel with the advances in the context-aware systems. More work in direction of context modelling and security threats resulting from providing the context is necessary. More work is also needed in the development of user-friendly and intuitive mechanisms for controlled information disclosure of any context information related to the user.
In addition to that, performance evaluation for the system complexity (for example depending on the number of rules and the number of considered context attributed) is a necessity.

Location Privacy

Finally, for location privacy for people, techniques can be divided into those that try to hide people's identity or any identifiable information, those that try to reduce data precision and policy-based techniques that restrict data access.

Hiding a person's identity is covered by anonymity and pseudonymity techniques. Work such as [51], [52] and [53] is aimed at adapting ideas from anonymous communication networks (specifically 'mixnets') to location privacy. The variable quality approach, where a centralised location server adjusts the accuracy of the given location such that the given area holds enough nodes to provide anonymity has been proposed by Gruteser in [52] and refined by Beresford in [51]. Here, the idea of a 'mixzone' is introduced, which is used to prevent linking between movements of a particular person, even if they are using different pseudonyms over time. The basic idea is that if many people enter a particular location over a certain time period, and many people leave it over the next, then it is difficult to link individuals between those who entered and those who left (as long as their pseudonyms change). How these mixzones are created, differs between the different papers, with some opting for fixed areas and others allowing the mixzones to be dynamically resized to maintain a consistent level of privacy.

The concept of a silence period between pseudonym changes for increasing location privacy has been introduced by Huang et al in [54] and further examined in the context of vehicular applications sending frequent beacons by Sampigetaya et al [55]. The authors state an increase in location privacy using the silence period. They measure the privacy in terms of the average anonymity set and the maximum tracking time.

In [56] Bessler and Jorns propose an extension to the Parley X architecture [57] to let users create own pseudonyms. Further they propose a pseudonym creation scheme – PRIVES – that can be used to create similar pseudonyms at different locations with only a single key exchange. The chain of pseudonyms is created using a combination of HMAC and SHA.

In [52], privacy is further enhanced by the ability to add noise to location and time information. For example, responses to requests can be delayed to give less accurate information about where a person is at a particular time.

The following Table 1 summarises the presented current approaches for solving some of the security and privacy issues and presents their pros and cons.

Possible Threats	**Proposed Solutions**	Pros	**Cons**
Compromised Base Station	Complete shutdown		Lost of data and the network is offline
Compromised nodes	Redundancy (the use of several nodes in order to obtain redundant information);	Extra data to work with. More protection against node failures and it is easier to implement multipath routing	Economic issues; In some cases must be used a limited number of sensors (sensors implemented in someone's body to monitor health)
	Code Attestation (permits to validate the code running on each sensor) [32];	Can be achieved either by software or hardware.	It must be kept in mind the computational limitations of sensor nodes. Needs more research;
	Voting System (allows the detection of compromised nodes in a timely fashion) [32]	Easy to implement	A compromised node can also vote (limit the number of votes for each node);
	Secure Localization (allows the detection of a malicious sensor node because it cannot claim a false position to the infrastructure) [32]	Ability to locate sensor nodes. Very useful for applications related to movement. Prevents numerous attacks.	Needs more research;
	Tamper-resistant hardware	Ability to store keys.	Too expensive and does not provide a high level of security
Eavesdrop on the networks radio frequency or packet injection	Cryptographic primitives;	Allows confidentially during the transmission of messages.	If there is a compromised node it has the secret key to decipher messages; Research the use of asymmetric cryptography; Research elliptic curve cryptography
	Authentication (μTESLA) [58]	Ability to establish secure links. μTESLA - especially design for WSN and doesn't require much energy	A compromised node may have the means to authenticate itself. The failure of nodes has not been considered.
	TinySec solution [31]	Incurs only an additional 5%-10% for performance overhead.	Need a secure and efficient key-distribution mechanism allowing simple key establishment for large-scale network;
Disabled sensor nodes/ node failures	Redundancy	Extra data to work with. More protection against node failures and it is easier to implement multipath routing	Economic issues; In some cases a limited number of sensors must be used (sensors implemented in someone's body to monitor health)

Denial of Service (DoS) (due to jamming and packet injection)	Achieve graceful degradation using time synchronization protocol;	Very efficient	Difficult to implement Needs more research;
	Jamming – use spread spectrum communication;	Ability to hide the message in the channel noise	The need for a large bandwidth;
	Secure Routing [31];		The existing protocols are not especially made for WSN; Needs more research;
The Sybil Attack	To leverage the key predistribution process [32]	Nodes can verify each other's identity	If there is a compromised node the adversary may have access to the key. If the network has numerous nodes the number of keys is too high.
Miscellaneous Attacks against Routing	Multipath routing [32]	Effective against DoS	The need to have alternative paths
Spreading bogus, routing information, creating sinkholes or wormholes and Hello flooding	Geographic routing protocols [59]; Limit the number of neighbours allowed [59];	Easy to implement	They are not 100% effective; Needs more research
Stealthy Attacks against Service Integrity	SIA [60]		Usage of many different keys.
Intrusion	The use of secure groups [31]	It is a decentralized solution for intrusion detection.	Needs more research, and it must be kept in mind that a solution is needed that is full distributed and inexpensive in terms of communication, energy and memory requirements;
Control the amount of data	Secured data aggregation [31] (the sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station)	Less data is transmitted to the base station;	All aggregation locations must be secured;
Unauthorised access	Access control policies – policy -based and role-based. [50], multi-party and heirerchical access control [61]		They are not instantaneously imposed. Require profiling and definition of parties which are authorised to access certain data
Threats to reveal node identity	Use of pseudonyms by different pseudonym creation schemes [56]		Additional computational cost to calculate new pseudonym. Pseudonyms of a group of nodes must be changed in the "correct" moment and this requires communication overhead

Reprogramming	Use of so-called streamed signatures and use of one or both hash chains or hash trees [38], [39]		Require packets to be receieved in the correct order, which can be hard to achieve in unreliable WSNs
Disrupt Time Synchronisation	Use of cryptographic communication secirity protocols [37]		Even with this protection, jamming communications and/or relaying packets could disrupt the current time synchronisation protocols
Reveal location	SeRLoc [36]– use of directional antennas on sensor nodes to enable them to determine a rough direction for locator beacons, whose positions are fixed and known	Simpler solution - accurate timing is not required;	Locator beacons must be used and the technique cannot be used in completely decentralised WSNs
Threats to Trust establishment	Certificate-based and behaviour-based trust establishmetn solutions [40]		Mainly proposed for ad-hoc networks and do not exploit pre-deployment knowledge that is available for sensor networks. Computational complexty of Certificate-based solutions. Energy requirements for behaviour-based solution

Table 1: Possible security and privacy threats and comparison of proposed solutions

2.3.5. Summary of Section 2.3

In this section the discussion was on the identification of the security, privacy and trust issues for WSNs in the framework of HHA. The focus was on the security threats and attacks on level 1 (people) and level 2 (environment) as the ones most relevant for the scope of this PhD report.
Further, the advantages and disadvantages of current solutions to the listed security, privacy and trust research problems were presented.
In short, considering pervasive healthcare applications, there is a pressing need for more research in a number of areas. Suitable for WSNs solutions are needed for services like privacy and anonymity and trust establishment, secure context and service discovery, secure data aggregation, trustworthiness of provided context data.

2.4. Summary of Chapter 2

In this chapter the vision for development of ubiquitous sensor networks which integrates people and things was presented. In the long run, with the growing number of new applications, the ubiquitous networks will have to integrate the unprecedented amount of different types of communicating, sensing and actuating devices imposing significant constraints on the scalability of the mechanisms for network organisation, and data handling. this long term vision requires a novel hierarchical network architecture to integrate devices with heterogeneous capabilities and constraints, in particular concerning energy, memory, processing power, programmability, deployment, mobility, and wireless interfaces. In this novel architecture, the network edge must migrate towards the objects of the physical world and sensors and actuators which access it and provide data for the users. This includes simple devices such as passive RFIDs and active sensors which can organise within ad hoc networks and deploy mechanisms to exploit density and locality of the data. The data aggregated within WSN patches are accessed by wireless stationary or mobile devices which in order to communicate themselves may either use ad hoc

communication or cellular network. The Hybrid Hierarchical Architecture (HHA) with four levels could be the reference architecture which can support this vision - *level 0 - access, level 1 – people, level 2 – environment, level 3 - objects*. The WSNs are accommodated in *level 2 – environment.*
Among the different types of applications which can be accommodated within HHA, the ones for health and elderly care will be investigated throughout this thesis. The motivation to select these reference applications was threefold – the prognosis for ageing population in Europe; the prospect for cost savings and increased quality of life when using WSNs for health and elderly care and numerous business opportunities; the number of un-solved security and privacy issues related to the use of this technology.

The briefly presented in this chapter a list of security threats and attacks show the scale of the problem. There are a number of issued which have not been yet solved successfully. In short, considering pervasive healthcare applications, there is a pressing need for more research and suitable for WSNs solutions are needed for secure context and service discovery; secure data aggregation; privacy and anonymity and tryst establishment.
Proposing effective and appropriate solutions to all of the security threats and attacks takes a serious amount of efforts. Therefore, in this thesis, the focus will be on solving part of the security and privacy issues on level 1 (people) and level 2 (environment) as the ones most relevant - mainly on proposing solutions for protecting privacy. This will be countermeasures against threats to information sharing and communication links – reveal user identity, reveal user or user's device location; reveal confidential data; steal user profile data; unauthorised access. Solutions to these threats will be some of the main contributions in this PhD thesis.
Further, the advantages and disadvantages of current solutions to the listed security, privacy and trust research problems were presented.

References

[1] Th. Arampatzis and J. Lygeros, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", in *Proc. of the 13th Mediterranean Conference on Control and Automation,* Limassol, Cyprus, June 27-29, 2005, pp719-724

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, Aug. 2002, pp. 102–114

[3] M. P. Michaelides and C. G. Panayiotou, "Event detection using sensor networks," *45th IEEE Conference on Decision and Control*, December 2006, pp. 6784-6789

[4] A. Timm-Giel, K. Kuladinithi, P. Hofmann, and C. Görg, "Wireless and Ad Hoc Communications Supporting the Firefighter", *in Proc. of 15th IST Mobile and Wireless Summit*, Mykonos, Greece, 4-8 June 2006

[5] R. Chandra, C. Fetzer, and K. Hogstedt, "Adaptive Topology Discovery in Hybrid Wireless Networks", Proceedings of *Informatics, 1st International Conference on Ad-hoc Networks and Wireless*, Toronto, Vol. 16, September 20-22, 2002, pp 1-16

[6] R. Verdone, V. Corvino, and J. Orriss, "A Hierarchical Hybrid Network Model", *in Proc. of IEE 3G&Beyond*, London, UK, Nov. 7-9, 2005

[7] Mitseva, M.Imine, N.R.Prasad, **"CRUISE Project - Network Initiative for Creating Ubiquitous Intelligent Sensing environments",** in Proceedings of The 15th IST Mobile & Wireless Communications Summit, 4-8 June 2006, Myconos, Greece

[8] Anelia Mitseva, Tapio Suihko, Radosveta Sokullu, Slobodanka Tomic, Maria Marchitti, Neeli R. Prasad "**Mobility Framework for Wireless Sensor Networks: CRUISE Approach**" in Proc. Of CRUISE Worksop at VTC 07 Spring, 25 April 07, Dublin, Ireland

[9] ICT & Ageing, European Study on Users, Markets and Technologies, Preliminary Findings, empirica & WRC 10/2008, October 2008

[10] CRUISE Del 210.1 **"Sensor Networks Architecture Concept"**, November 2006

[11] CRUISE Del 230.1 **"Key Issues Related to Mobility and Security in Sensor Networks",** September 2006

[12] CRUISE Del 230.2 "**Mobility and Security Framework for WSNs",** December 2006

[13] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks", *IEEE Communications Surveys*, 8(2):2–23, 2006

[14] A. D. Wood and J. A. Stankovic, "Denial of Service in sensor networks", *IEEE Computer*, vol.35, no.10, pp.54-62, October 2002

[15] Tassos Dimitriou, I. Krontiris and F. Nikakis. "A Localized, Distributed Protocol for Secure Information Exchange in Sensor Networks", in Proc. of the 5th IEEE International Workshop on. Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks, WMAN 05

[16] Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA, "Security Solutions for Wireless Sensor Networks", NEC Technical Journal, Vol.1, No.3/2006, www.ist- ubisecsens.org/publications/SecuritySolutionsWSN.pdf

[17] Related-Key Cryptanalysis of 3-WAY. Biham-DES, CAST, DES-X, NewDES, RC2, and TEA

[18] Y. W. Law, S. Dulman, S. Etalle, P. Havinga, " Assessing Security-Critical Energy-Efficient Sensor Networks", in Proc. of the 18th IFIP International Information Security Conference , May 2003

[19] J. Loughney, Ed., M. Nahkjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol", IETF RFC 4067, July 2005

[20] L. Zhou and Z. J. Haas, "Securing ad hoc networks", *IEEE Network*, Vol. 13, No. 6, 1999

[21] Pandurang Kamat, Yanyong Zhang et Al. "Enhancing Source-Location Privacy in Sensor Network Routing", In Proc. of the 25th IEEE International Conference on Distributed Computing Systems (ICSCS 05)

[22] Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan, “Mobility Helps Security in Ad Hoc Networks”, MobiHoc’03, June 1–3, 2003

[23] A. Mishra, M. H. Shin, j. Nick L. Petroni, T. C. Clancy, and W. A. Arbaugh, “Proactive key distribution using neighbor graphs,” *IEEE Wireless Communications*, 2004

[24] Chris Karlof, David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, *Ad Hoc Networks* 1 (2003), p. 293–315

[25] Damon Smith, Ryan Mahon, Swathi Koundinya, Shubhashri Panicker, ”SNTS: Sensor Node Traceback Scheme”, in Proc. of ACM WiSe 2004, October 1, 2004

[26] S. Radosavac, J.S. Baras and I. Koutsopoulos, “A framework for MAC layer misbehavior detection in wireless networks’’, in Proc. of ACM Workshop on Wireless Security, 2005. Available in http:www.inf.uth.gr/~jordan

[27] Przydatek, Song, Perrig, “SIA-Secure information aggregation in sensor networks”, in Proc. of the First ACM International Conference on Embedded Networked Sensor Systems (SenSys 2003)

[28] Sven Lachmund, Frank Fransen, Eddy Olk, “Context-Awareness, Security and Trust”, in Proc. of WPMC 2005, Aalborg, Denmark

[29] Vagner Sacramento, Markus Endler, Fernando Ney Nascimento, “A Privacy Service for Context-aware Mobile Computing”, in Proc. of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) pp. 182-193

[30] A. R. Beresford and F. Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing, Volume 2, Issue 1, January 2003, pages 46-55

[31] A. Perrig, J. Stankovic, and D. Wagner, “**Security in Wireless Sensor Networks**”, ACM June 2004/ vol. 47 No6

[32] E. Shi and A. Perrig, “**Designing Secure Sensor Networks**”, IEEE December 2004

[33] J. Deng et al., Countermeasures against Traffic Analysis Attacks in Wireless Sensor Networks, Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SECURECOMM 2005, IEEE, 5-9 September 2005, pages 113-126

[34] C. Ozturk et al., Source-Location Privacy in Energy-Constrained Sensor Network Routing, Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM Press, 2004, pages 88-93

[35] S. Capkun and J.-P. Hubaux, Secure Positioning in Wireless Networks, IEEE Journal on Selected Areas in Communications, Volume 24, Issue 2, February 2006, pages 221-232

[36] L. Lazos and R. Poovendran, SeRLoc: Robust Localisation for Wireless Sensor Networks, ACM Transactions on Sensor Networks, Volume 1, Number 1, August 2005, Pages 73-100

[37] S. Ganeriwal et al., Secure Time Synchronisation Service for Sensor Networks, Proceedings of the Fourth ACM Workshop on Wireless Security, International Conference on Mobile Computing and Networking, ACM press, 2005, Pages 97-106

[38] P. Lanigan et al., Sluice: Secure Dissemination of Code Updates in Sensor Networks, Proceedings of the 26th IEEE International Conference On Distributed Computing Systems (ICDCS ’06), July 2006, pages 53-62

[39] J. Deng et al., Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, Proceedings of the Fifth International Conference on Information Processing in Sensor Networks (IPSN '06), IEEE, April 2006, pages 292-300

[40] E. Aivaloglou, E., Gritzalis, S., Skianis, C.: Trust establishment in ad-hoc and sensor networks. In: Proceedings of CRITIS’06 1st International Workshop on Critical Information Infrastructure Security, LNCS 4347. (2006) 179–194

[41] Davis, C.R.: A localized trust management scheme for ad hoc networks. In: 3rd International Conference on Networking (ICN’04). (2004) 671–675

[42] Hubaux, J.P., Butty´an, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: MobiHoc ’01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, New York, NY, USA, ACM Press (2001) 146–155

[43] Yi, S., Kravets, R.: Moca: Mobile certificate authority for wireless ad hoc networks. In: Proceedings of 2nd Annual PKI Research Workshop. (2003)

[44] Eschenauer, L., Gligor, V.D., Baras, J.S.: On trust establishment in mobile ad-hoc networks. In: Security Protocols Workshop. (2002) 47–66

[45] Ganeriwal, S., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN'04), ACM Press (2004) 66–77

[46] Huang, L., Li, L., Tan, Q.: Behavior-based trust in wireless sensor network. In: APWeb Workshops, Springer Berlin (2006) 214–223

[47] Zouridaki, C., Mark, B.L., Hejmo, M., Thomas, R.K.: Robust cooperative trust establishment for manets. In: SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, New York, NY, USA, ACM Press (2006) 23–34

[48] Theodorakopoulos, G., Baras, J.S.: Trust evaluation in ad-hoc networks. In: Workshop on Wireless Security. (2004) 1–10

[49] Henning Olesen et al, Scenario Construction and Personalization of PN Services based on User Profiles and Context Information, in Proc. of IST Mobile and Wireless Summit, Myconos, 2006

[50] Vagner Sacramento, et al. "A Privacy Service for Context-aware Mobile Computing". First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), pp. 182-193

[51] A. R. Beresford and F. Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing, Volume 2, Issue 1, January 2003, pages 46-55

[52] M. Gruteser and D. Grunwald, Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking, Proceedings of First International Conference on Mobile Systems, Applications, and Services (MobiSys'03) (May 2003), pages 31-42.

[53] M. Gruteser et al., Privacy-Aware Location Sensor Networks, 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX) -- 2003.

[54] L. Huang, K. Matsuura, et al. "Enhancing wireless location privacy using silent period". In Proceedings of Wireless Communications and Networking Conference, volume 2, pages 1187–1192, 2005.

[55] L. Huang, K. Sampigethaya, et al.: "Providing location privacy for VANET". In Proceedings of Escar 2005, 2005.

[56] Sandford Bessler, Oliver Jorns, "A Privacy Enhanced Service Architecture for Mobile Users," In Proceedings of PERCOMW, pp. 125-129, Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05), 2005.

[57] The Parlay Group, URL: http://www.parlay.org, accessed 2. Sept. 2004

[58] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. Tygar, "**SPINS: Security Protocols for Sensor Networks**"

[59] C. Karlof and D. Wagner, "**Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures**", Proc 1st IEEE, Wksp. Sensor Network Protocols and Applications, May 2003.

[60] B. Przydatek, "**SIA: Secure Information Aggregation in Sensor Networks**", Proc. 1st ACM Int'l. Conf. Embedded Networked Sensor Sys., Nov. 2003, pp 255-65.

[61] Eskeland, S.; Oleshchuk, V., **Hierarchical Multi-Party Key Agreement for Wireless Networks,** Third International Symposium on Information Assurance and Security, 2007. IAS 2007. Volume , Issue , 29-31 Aug. 2007 Page(s):39 – 43, Digital Object Identifier 10.1109/IAS.2007.82

Chapter 3
3. Health Care Applications for WSNs - their security and privacy requirements and threat and vulnerability model

The aim of Chapter 3 is first to shortly describe examples of pervasive health care services using WSNs or BSNs and to select one application space which will be investigated throughout this thesis, namely – the pervasive health and elderly care application space. The second aim of this chapter is to present the security, privacy and trust requirements derived from the scenarios – this analysis is one of the contributions in this thesis. The third and main aim of Chapter 3 is to analyse the security threats for health care applications with WSNs. Threat model and mitigation plan are further presented. The security threats analysis, definition of threat model and presenting mitigation plan are one of the major contributions in this thesis.

3.1. Description of Pervasive Health Services and Use Cases

In this section details for Pervasive Health Services are provided, seen from point of view of user requirements, information flow, used devices and technologies and end-user groups (main actors) and relevant context attributes. All these points will be revisited in Section 3.3 where they play an important role in the threat analysis.

In the medical care, outfitting care subjects with tiny, wearable wireless sensors forming a Body Sensor Network (BSN) would allow medical teams to monitor the status of their patients (either at hospital or at home). The same technology could be used for rehabilitation of a patient at home or to monitor the health status of an early discharged patient or just the physical status of an elderly person. In this case, the BSN transmits the current readings of vital signs (heart beat rate, body temperature, blood glucose, etc) to the hospital or home-care database. Medical staffs, emergency teams, general practitioners, home or social care staff can then access the data when needed. Such application space is depicted on Figure 6.

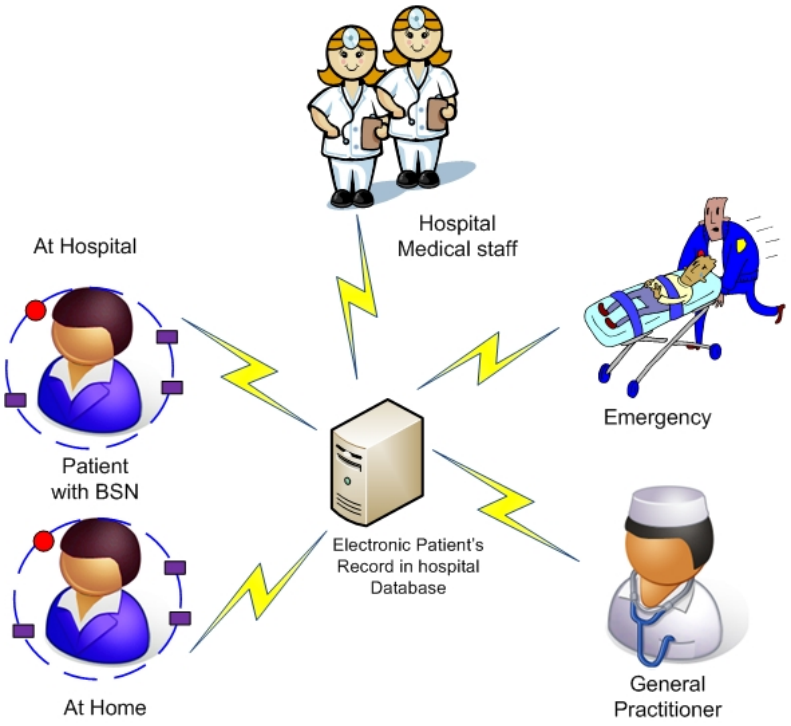


Figure 6: Pervasive Health Care of a patient [1] [2]

3.1.1. Use cases for Pervasive Health Care Services

The use cases for the Pervasive Health Care application space could be numerous [3] but the most important ones are summarised to:

- **Wireless Hospital**. This scenario involves the use of sensors to capture the physiological status of patients, physician's physiological data, medical staff's physiological data, additional information from the sensors in the environment (locating patients, equipment, staff). The types of data taken into account are patient related information, administrative information, knowledge based information. The Wireless Hospital use case can be split in two scenarios:
  - Night Shift Assistant: a nurse usually spends the night shift at a room in a different part of the hospital and is responsible for several wards at a time. Then, the medical status of the patients is monitored, together with environment information for the patient's room. In these scenarios, communicating vital patient's data is very critical regarding privacy and has to be highly reliable to infer critical health conditions.
  - Backup Shift Assistant: in this scenario, a young doctor on shift at the hospital, gets support from the back-up shift senior doctor who might be out of the hospital, but not so far. Here, wireless transmission of vital data over long distances takes place; localisation functionalities, navigation and instant messaging are involved.
- **Residential Health Monitoring**. In this scenario health related data are captured via BSN and the sensors from the environment in the patient's home. The actors here are patients, health professionals and secondary users (e.g. relatives, friends). The collected and interpreted patient's data can be used to give feedback about and to support medication intake and exercise regime. This use case considers two scenarios:
  - Acute Patient Monitoring: this scenario depicts a warning system for critical vital data assessed at home, featuring online wireless vital data transfer for long distances, localisation functionalities and messaging service for relatives.
  - Continuous Care – monitoring the status of the patient at home, when he is in a rehabilitation process.
- **Emergency Coordination**. This scenario includes communication among rescue staff in case of emergency in order to improve the organisation of emergency response. The communication, which is mainly between emergency physicians and rescue transports, is mission critical and requires intelligent emergency coordination via WSNs.

3.1.2. Selection of a reference scenario

"Backup Shift Assistant" from Wireless Hospital use case

The proposed adaptive security and privacy protection framework is designed in such a way to be applicable to a number of application spaces as mentioned in Section 1.4. However, in order to exemplify its functionality, analysis and evaluation, later in this PhD report there will be a reference to only one scenario, namely *Backup Shift Assistant from the Wireless Hospital use case.* This scenario is depicted on Figure 7 and described in the paragraph below:

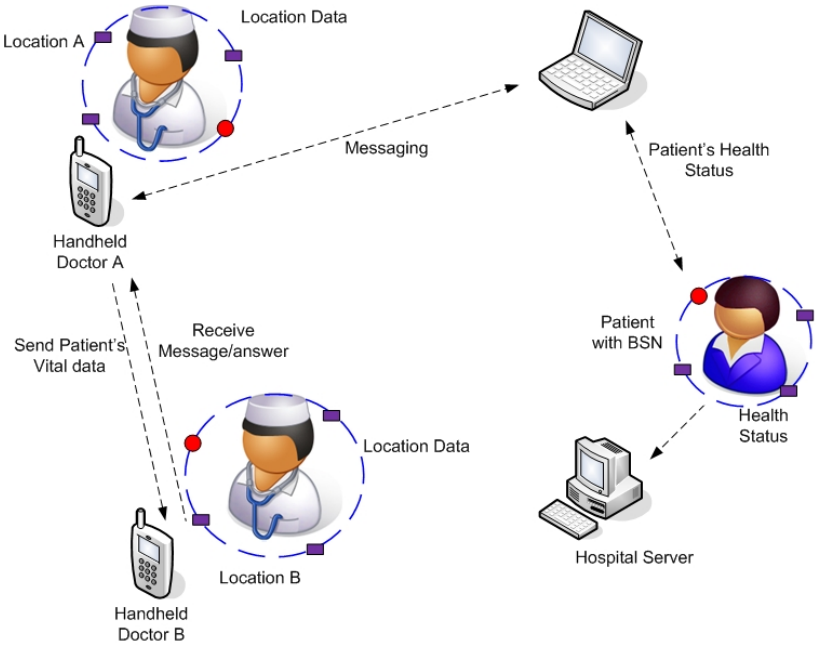


Figure 7: Illustration of the "Backup shift assistant" scenario [3]

At any hospital, the physicians differ in their age and work experience. Today Doctor A, a very young doctor, is on duty when a severe patient condition comes up. He is yet inexperienced and does not feel comfortable with handling the situation by himself. Since the patient's condition is critical, he decides to contact the next experienced colleague available in the hospital or at home. Doctor A sends an instant message to the closest available physician Doctor B, who is doing administrative duties in another building of the hospital. The physician quickly gives feedback via instant message that he will support Doctor A and receives Doctor A's location and navigation information for the fastest route on his handheld. Doctor A also sends him the vital data of the patient to inform him for the patient medical condition. Doctor A is relived when the older physician Doctor B arrives. Together they stabilise the patient's condition.

Characteristics of the reference scenario – Back-up shift assistant
The characteristics of the reference scenario in terms of user requirements, information flow, user sensitive data, communicated context data, are presented below.

3.1.3. User Requirements

The reference scenario described above involves the wireless transmission of vital data over long distances, localisation functionalities, navigation and instant messaging, which are integrated and used in an intelligent information exchange application. Here, especially the medical personnel, is mobile. Besides patients' BSN, the BSN is applied on the physicians to infer their health status and location (e.g., operating theatre, office, out of the hospital). The sensors for both physicians and patients need to be easily accessible and replaceable for maintenance. For the sensors from the environment (for example in the hospital rooms, the corridors, the operating theatre, etc), maintenance is minimal but should be carried out frequently. Vital patients' data, their identity, medical history as well as physicians' health data is very critical regarding privacy. The vital patient's data has to be highly reliable because it communicates critical health conditions, whereas the physicians' location data reliability and privacy should be moderate. Both the functionality provided by integrated data transfer as well as the functionality provided by the instant messaging is similar to traditional methods and therefore not complex. The data integration, however, is complex. The environment in which the sensors are deployed is safe and invariable.

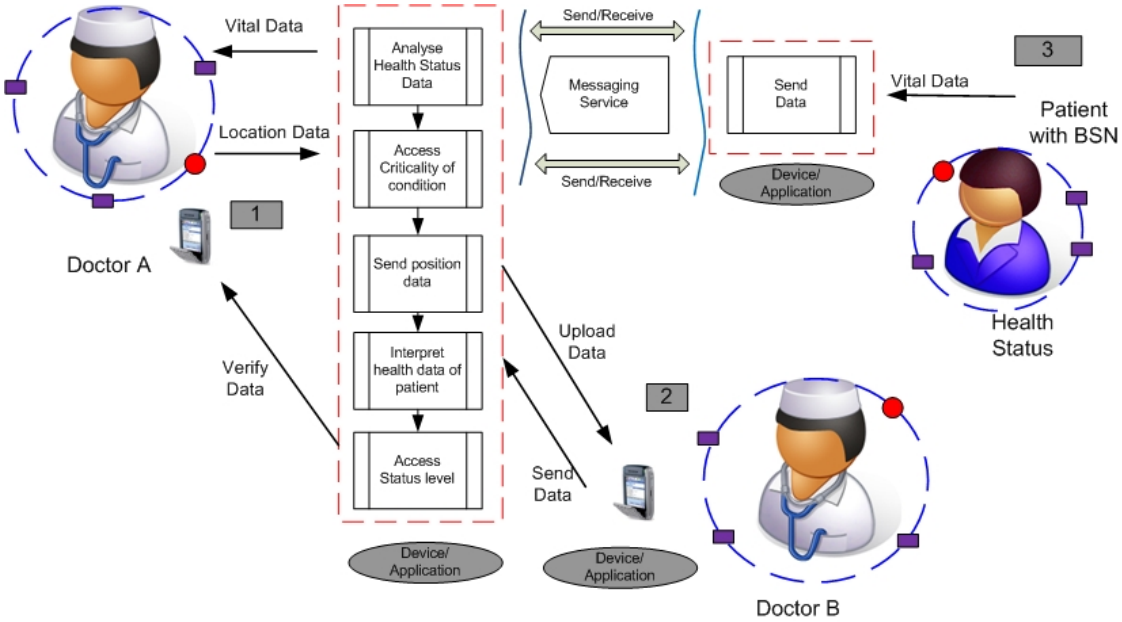


Figure 8: Information flow diagram of the "Backup shift assistant" scenario [3]

3.1.4. Information Flow

After registering in the database, Doctor A receives and analyses patients' vital data on a mobile device **(1)**. Doctor A localises the back-up colleague (Doctor B) that is available working at his office and triggers a data transfer to him for professional support **(2)**. Doctor B receives the information on a PDA-like device which can be used for communication and navigation. After logging in the monitoring and diagnosis application Doctor B receives vital data from the patient's BSN **(3)**.

3.1.5. Devices, involved technologies, description of the actors

As later in this chapter it will be discussed about threat analysis of the reference scenario, of importance for this is the system description from point of view of the used devices, involved technologies, actors, main goals. These are summarised in the Table 2 below:

System characteristics	Description
Reference scenario	Back-up shift assistant
Main Actors	Patient (primer) Doctor (primer) Other Medical staff (secondary) Network administrator (secondary) Hospital administration (secondary) Service providers (other)
Main goals of the system	Measuring and communicating vital signs of persons; Locating and communicating the position of persons, devices Communication among the medical staff Communicating physical parameters of the environment in the hospital room
Devices to be used	A few wireless end-sensors and a coordinator node forming BSN Several wireless sensors from the environment (hospital room and building) Mobile terminal (smart mobile phone) for the medical staff

	Hospital computers/terminals Hospital server
Communication Technologies	Wireless communication - BT (IEEE802.15.1), IEEE 802.15.3, IEEE 802.15.4, IEEE802.11b, IEEE802.11g, IEEE802.11a Interconnecting – Internet, WLAN

Table 2: System characteristics

3.1.6. Context attributes directly provided by the sensor networks

In the following Table 3, the context attributes which play role in the functionality of the security and privacy framework are presented. They are the context attributes typical for the reference scenario and are provided by the body sensor networks of the subjects or by the environmental WSNs.

Context Name	Information Required	When required	Number of users	Environment
Vital Functions (patient)	Physiological information	All the time	1-100	Indoor
Vital Functions (doctor A or B)	Physiological information	All the time	1-10	Indoor/Outdoor
Indoor Location (patient)	Location	All the time	1-100	Indoor
Indoor-Outdoor Location (doctor A or B)	Indoor-Outdoor Location	All the time	1-10	Indoor/Outdoor
Environmental information	Physical information	All the time	1-100	Indoor
Indoor Location of hospital equipment	Location	All the time	1-100	Indoor

Table 3: Data which is subject to measurement and communication

Figure 9 shows the information flow of the reference scenario and the context information that is required by each device to decide how each message exchange will be protected and how the privacy of the user will be preserved. Table 4 summarises the high-level context information, its type and if it is of a sensitive value for the user. A distinction is made between ‘static’ and ‘dynamic’ context data [1]. Static context data changes only infrequently, and could be manually configured (e.g. Doctor’s A and B current role). Dynamic context data can change at any time, and is usually automatically detected (e.g. the patient’s vital functions, location).

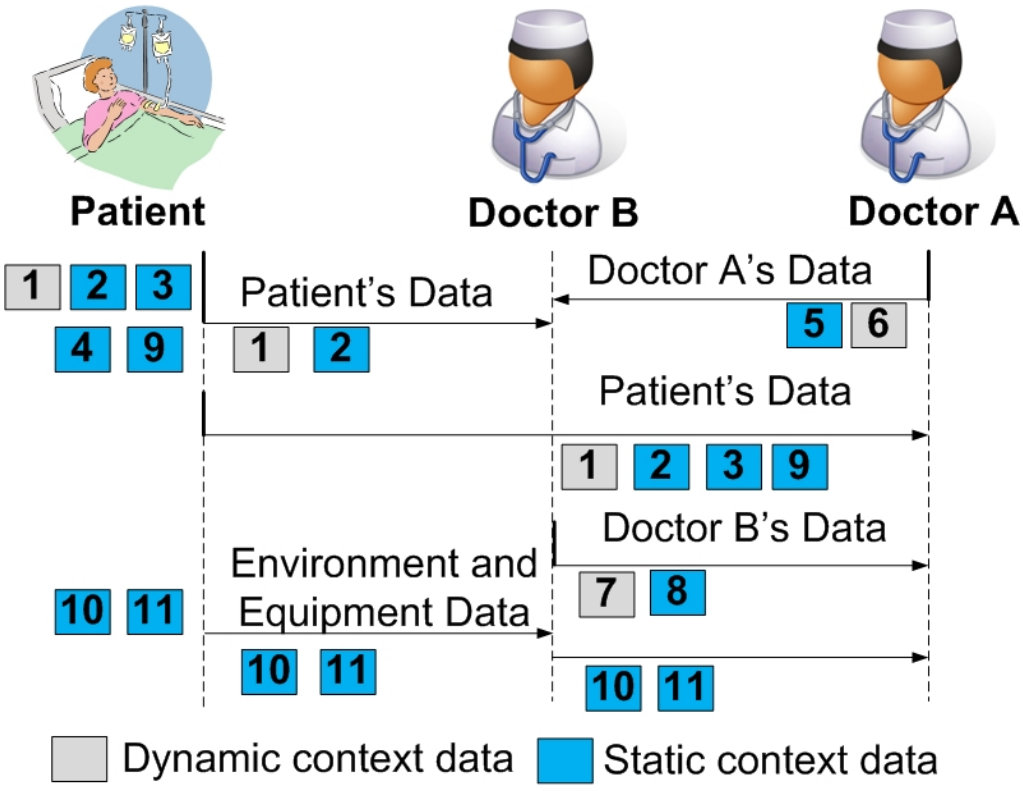


Figure 9: Types of communicated context data [4] [5]

The following Table 4 presents the communicated context data and if it needs privacy protection:

Communicated context data	Type of communicated context data	Privacy protection needed
1- Patient's medical data	Dynamic	Yes
2 - Patient's Indoor Location	Static	Yes
3 - Patient's ID	Static	Yes
4 - Type of service	Static	no
5 - Doctor's A Indoor Location	Static	Yes
6 - Doctor's A ID	Dynamic	Yes
7 - Doctor's B Indoor Location	Dynamic	Yes
8 - Doctor's B ID	Static	Yes
9- Patient's medical history	Static	Yes
10 - Data for the physical environment in the room	Static	yes
11- Indoor Location of hospital equipment	Static	No

Table 4: Communicated context data and its characteristics

3.1.7. Summary of Section 3.1

In this chapter the reference scenario is selected – namely, "Back-up shift assistant" scenario which provides support for professional communication. The characteristics of the system with respect to the reference scenario were presented, from point of view of user requirements, information flow, main actors, used devices and technologies, used context attributes directly provided by the sensor networks. Context attributes directly provided by the sensor networks were defined as: vital functions of patient and medical staff, indoor/outdoor location of the actors, physical information from the environment. Further, the communicated context data have been defined and

if it needs privacy protection or not. The communicated context data is identified as 11 contexts relevant for the reference scenario and 9 of these contexts need privacy protection.

3.2. Security, privacy and trust requirements derived from the scenarios

The initial focus in this section is the security and privacy objectives for the discussed system. Further the focus is on the security, privacy and trust requirements derived from the scenarios presented in the previous chapter. Since the context-awareness plays important role in this thesis, in the end of this chapter the security requirements for the context data are discussed too. This analysis is one of the contributions in this thesis.

3.2.1. Security and Privacy Objectives for the system

The security and privacy system of a certain application can be described to fulfil specific objectives and have specific functionality. Similar to the common criteria [10], in this section, it is distinguished between security and privacy **objectives** and security and privacy **requirements**. *Security objectives* define what the security system must achieve to counter a certain threat. They can be *preventive or reactive*. A preventive objective prevents a threat from occurring; reactive objectives imply that a system shall detect and correct potential threats. Privacy objectives define what the system must achieve in order to protect privacy data and all aspects of privacy of a person. These objectives summarise what the user and developer expect from the security and privacy system.

Security and privacy requirements define the functionality that is necessary to implement the required security and privacy objectives. The security and privacy system can therefore be specified in terms of what functions it provides.

Looking at the security objectives more closely, it should be noted that they are also related to trust establishment and privacy protection [6]:

- *Security* aims at, broadly speaking, ensuring that the data which is communicated is not modified, deleted or damaged. In other words, the data which is sent by the sender, must be the same data, received or stored at the end point.
- *Trust establishment* aims at preventing any false data to be injected into the system by different means or to be released to parties which should not be trusted. Trust can be established into nodes, into a piece of data, into a service, or any other element that needs to be accessed or used by a sensor node.
- *Privacy protection* aims at preventing the disclosure of private or sensitive information, location information, and identification data to an attacker. For example, this may be realised using access control mechanisms, changing pseudonyms, cloaking of data by reducing its precision.

Trust establishment
According to Avizienis [7], trust is *accepted dependence*. Hence, the security system must provide mechanisms that make applications accept a certain level of dependence on a piece of data (or a service, or an entity in general).
Trust can be either in the *source of data*, or in the *data itself*. Certification, for example, usually certifies that a node is sending out valid data. The receiving nodes often do not check if the data is indeed valid but simply trust the certificate (if it can be validated). Approaches including trust in the source typically require cryptography to ensure the well-known security objectives *integrity, authenticity and non-repudiation*. In order to be able to bind trust to a node, *node identification* is an important issue for these approaches as well.
On the other hand, checking the *plausibility of data* can be independent from the sending node. Independent from any knowledge about the sender, the content itself is evaluated and ignored if it is invalid. This requires semantic knowledge about the received data, knowledge about the current context, and knowledge about the history of the context.

Privacy Protection

Traditionally, privacy protection in general contains protection of the *identity* of a user and the *data* of the user. While protecting the identity of a user is relatively straightforward, and can be achieved by pseudonymous systems, the protection of user and context data is more difficult.

With the development and implementation of pervasive and ubiquitous systems, some context information must be also protected in order the user to be able to use some services anonymously. Social concerns from autonomous cooperative objects have been expressed in [8] for privacy, data protection and building trust. This is because current developments in computing direct towards the collection and processing of an increasing quantity of personal data and, what is more, are in search of new qualities of data (e.g. biometric identifiers extracted from the human body or very intimate data displaying emotions and thoughts). In networked ubiquitous computing environments data might be collected of even very simple and insignificant incidents that might be never forgotten by the hardware memories of huge databases, they could be combined, sorted and reinvented by sophisticated algorithms and transferred at a global scale to other entities for further processing for unknown purposes. This process is related to data-mining, data surveillance ("dataveillance) and data-profiling. All these electronically available pieces of information form the so-called "electronic shadow" [9] of a person and a personal profile could be created. This may expose the persons to many security threats and intrude their privacy. It becomes more and more difficult for the end-users to protect their privacy and make informed decisions when they need to provide some sensitive data.

Therefore in this thesis the security objectives for privacy protection of a "traditional secure system" is extended with privacy protection for context data, directly or indirectly related to the user, based on which sensitive information for the subject could be inferred. In the work presented in this report, the privacy protection is further extended to preserve the privacy of the context in which the users currently are or the context in which users use a service.

Concerning user data, the distinction must be made between *core (system) data* and *application specific data*. The first are required by the core system to work, e.g. location data and will be received by all nodes listening to the channel. The latter may have specific authorisations and roles that are attached to the network nodes.

In the following Table 5, the security objectives for trust establishment and privacy protection are summarised. The threats which can threaten these objectives are also listed.

Security and Privacy Objective	**Short Description**	**Countered Threats**
Availability	The system provides its services, i.e. correct sensor data even in the case of a locally mounted DoS attack.	Disrupt Communication, Disable Sensors, Disable Processing, Impair Transceiver
Access Control	The system provides the means to assign the use of resources only to authorised users.	Unauthorised Access to data
Non-Repudiation	A node can be held responsible for a sent message.	DoS Inject False Message
Freshness	Messages must be checked for their freshness, i.e. to have recently been sent by the originator.	Replay Messages
Ensure time synchronisation	Time synchronisation is a fundamental requirement for WSNs to enable them to communicate effectively and efficiently. By disrupting time synchronisation, an adversary could cause denial of service, or incorrect timings of events to be reported to the sink or the coordinator node. It is especially important for the medical applications.	DoS Incorrect timing of events Jamming communication Relay packets
Detect Malicious Nodes	Nodes that behave in a malicious way can be detected and excluded from the environment.	DoS Inject False Message
Exclude Malicious Nodes	The environment can exclude nodes that have been detected to be malicious.	Inappropriate release of information to adversaries

Auditability	It is possible to log and audit security relevant data to detect new threats and security violations.	DoS Inject False Message
Maintain confidentiality of the communication (links, data)	The system must ensure confidentiality of the communication links and the communicated data. Confidentiality might be easily violated with simple and quite cheap equipments. Besides, the attacker does not need to be an expert hacker to be able to perform it.	Eavesdropping Masquerade/ Impersonation Node compromise
Maintain data integrity	The system must ensure that the data is not corrupted, changed or modified. Attacks will lead to data corruption that can turn into wrong requests and then wrong operations thus likely affecting users' vital functions.	Man-in-the-middle Masquerade/ Impersonation Node compromise
Prevent reprogramming	The system must exclude possibility of reprogramming. Such attacks in the healthcare application would either be to disrupt communications so that the network services would appear unreliable or to gain access to sensitive information collected for patients and/or medical or emergency staff.	Node compromise Man-in-the-middle Masquerade/ Impersonation of sender in communications Masquerade/Impersonation of WSN manager Masquerade/Impersonation of code originator
Ensure security of the aggregated data	In order to minimise communications in a WSN, data is normally aggregated at nodes along the path to the sink from the source nodes. Because of this, the goal is to prevent compromising a node near to the sink, since a large amount of the data being generated in the WSN can be affected.	Node compromise Eavesdrop on aggregated data Add, delete, replay, modify aggregated data
Ensure confidentiality of the communication traffic	Confidentiality of the communication traffic in WSNs is important in order to prevent revealing sensitive information due to the unusual patterns of traffic in that kind of networks. Traffic analysis is possible even if encryption is used to make communications unreadable. In addition, several applications of WSNs involve monitoring and tracking of people. In this case, traffic analysis can compromise different aspect of the privacy of these people.	Traffic analysis Direct observing the information Following or backtracking the route Inferring events Linking events Linking identities through matching pseudonyms Inferring location Inferring identities
Controlling release of information	In more sophisticated applications of WSNs, including those for pervasive healthcare services, multiple WSNs may need to share information to achieve a particular goal. These WSNs may be controlled by different individuals and organisations with different policies regarding their information, and therefore controlled release of information between these networks becomes an issue. The goal here is to prevent inappropriate release of information to adversaries (or equivalently untrusted or partially trusted WSNs) may occur, allowing the adversary access to sensitive information.	Inappropriate release of information to adversaries (or equivalently non-trusted or partially trusted WSNs) Eavesdropping Masquerading/impersonation Compromising gateways or nodes
Maintain location	The goal is to prevent an observer from	Track subjects current location

privacy	learning the position of nodes/people.	Track subjects movements
Maintain user anonymity	If users anonymity is ensured, they can use diverse pervasive services while their privacy is protected	Reveal node/user's identity
Maintain the privacy of the context in which the users are	The current context in which the users are using a service, device, system or part of it can reveal some private or sensitive information, or their behaviour.	Infer privacy data for the user from context information
Trusted Administrator	The administrator is trusted to correctly assign access control rules.	Inappropriate release of information to adversaries (or equivalently non-trusted or partially trusted WSNs)

Table 5: Security Objectives for Trust Establishment and Privacy Protection

3.2.2. Security, privacy and trust requirements for the system

While the security objectives specify the overall objectives of the security system to counter threats, in this section it is outlined the functionality to achieve these objectives. The list is based on the Common Criteria [10], which is an international standard for the development of secure systems. The Common Criteria define the following classes of functionality[1] (cites from [10]):

- *Security Audit* "involves recognising, recording, storing, and analysing information related to security relevant activities". Intrusion detection, for example is security audit functionality.
- *Communication* functionality in terms of the common criteria defines two classes of communication: non-repudiation of sending or non-repudiation of receiving messages. Note that protection of integrity, authenticity and confidentiality are subsumed under the user data protection.
- *Cryptography Support* is concerned with the management of keys and their use in cryptographic operations.
- *User data protection* defines a set of functions to protect the unauthorised access to user data, in particular the definitions of access control rules. *Confidentiality and secrecy* of the collected and communicated data entails ensuring that information is accessible only to those authorised to have access, and providing assurance that the information processed by a system is protected against intentional or unintentional unauthorised access by individuals, processes or devices. *Integrity* of the data that is sensed, processed or aggregated is a measure of its reliability. It entails protection against unauthorised data modification, insertion, substitution or deletion. It includes providing the means for assuring data freshness. *Authorisation* for accessing data or network resources entails providing the means to control access and approve actions by authenticated entities.
- *Identification and authentication* contains the set of functions to "establish and verify a claimed user identity". *Authentication* of the originator and recipient of messages entails providing the means for verification of network identities, and is a prerequisite for covering the other security requirements.
- *Security Management* defines the attributes, roles and functions of the security system itself.
- *Privacy* defines privacy preserving functionality. Note that in terms of the Common Criteria, privacy only concerns the protection of the identity of the users (and not their data and the context in which they are using a service, as assumed throughout this report).
- *Protection of the [security functions]*[2] defines functions to protect important data (like key material) and functions (like key distribution) of the security system.

[1] Note that the Common Criteria also define assurance levels, which is out of scope of this document.

[2] The common criteria call the security functions *TSF: Target of Evaluation Security Functions.*

- *Resource Utilisation* functions define how the availability of the system can be protected, e.g. by prioritising resources and by being fault tolerant.
- *Trusted Path/channels* define the function to establish a secure communication channel with an identified communication partner.
- As described in Section 2.1, HHA have diversity of nodes with respect to memory, computation, communication capabilities and roles. Depending on the scenario and role of each node in the network, the information it communicates has different security requirements. In the wireless hospital use case described in Section 3.1.1 for example, information for the current health status and patient's medical history is communicated, while in other use cases, other type of sensitive information (for example the current location of the back-up shift assistant) is essential. The first case generates information whose correctness and freshness is crucial, thus requiring strong integrity protection. The second case generates information with high confidentiality needs, because it is related to the privacy of the medical staff. Detailed risk analysis will show further in this chapter that the diversity which exists in the scenarios of the application spaces influences the risks and consequently the security needs of the nodes. This will be presented in the following subsections.
- The adaptive security framework must of course cover the general security requirements through security protocols and mechanisms. From the above listed requirements, in the following sections will be analysed more closely the ones related to *privacy, confidentiality and secrecy, data integrity and freshness, authentication and authorisation [3]*.

Scope of the proposed security and privacy solution

In order to identify the set of requirements that the security and privacy framework must cover for secure deployments, it is important to define the scope of the security solution. The assumptions here are that data handling practices and privacy policies of legitimate deployments are enforced and supervised by some regulatory framework. In order for the users to take full advantage of the services that can be offered by legitimate deployments, it is necessary to build some level of trust, which can not be accomplished using sorely technical means, i. e. the users have to trust that the organisations responsible for the deployments are complying with regulations (e.g. for data handling practices) in order to use the services offered. Moreover, it is assumed that the security and privacy solution should cover the communications between the nodes of sensor networks and between nodes and gateways to other networks.
The communication scope for which each requirement should be fulfilled to counteract each threat is also identified. In order, for example, to counteract threats against data confidentiality, the mechanisms for authentication, authorisation and confidentiality need to be applied for both the communications within the nodes of the network and the communications with gateway nodes of trusted subscribed networks. The communication scopes are:

- Communication within the nodes of the network (denoted here as IN)
- Communication with nodes of trusted subscribed networks (denoted here as SUB)
- Occasional communication with nodes of unknown networks (denoted here as UN)

The following Table 6 presents the scope of the threats and general security requirements. Only the relevant threats are listed.

Threats	Confidentiality	Integrity	Authentication	Authorisation
Threats to confidentiality	IN, SUB		IN, SUB	IN, SUB
Threats to integrity		IN, SUB	IN, SUB	IN, SUB
Threats to data aggregation	IN	IN	IN	IN
Threats to localisation and time synchronisation		IN	IN	IN
Threats to reprogramming		IN, SUB	IN, SUB	IN, SUB
Threats to information	UN		UN	UN

sharing				

Table 6: Scope of threats and general security requirements

3.2.3. Trust Requirements for the Pervasive Health Care

The requirement for trust management mechanisms is set because within the scope of future ubiquitous systems, communications between highly heterogeneous and dynamic networks need to be secured. Moreover, sensor networks depend on the distributed cooperation among network nodes, and the evaluation and establishment of trust relationships within the network could serve as the basis for decisions on security issues and network activities. In general, the problem of formulating evaluation rules and policies, representing trust evidence, and evaluating and managing trust relationships is referred to as the trust management problem.

The trust establishment process which needs to be defined as part of the security framework includes the specification of valid types of evidence, and its generation, distribution, collection and evaluation. Trust evaluation is performed by applying context-specific rules, metrics and policies on the trust evidence. The result of the process is the trust relation between the trustor and the trustee, usually represented as a certificate or as a numeric value, either discrete or in a continuous range. The trust relation, along with other aspects like the associated transaction risk, could be used by the trustor as the basis for decisions on cooperation with the trustee. Trust relations can be revoked on the basis of newly obtained evidence. Trust is transitive if it can be extended beyond the two parties between whom it was established, allowing for the building-up of trust paths between entities that have not directly participated in a process of trust evaluation.

Trust evidence, which forms the basis for establishing trust relations, can be characterised as stable and long-term, if the evaluation metrics and mechanisms used for obtaining it do not change without notification. Within the scope of discussed medical applications, even trust relationships can be stable and long-term. Some sensor nodes, for example the nodes of a BSN, will be clustered by deployment and the trust relationships within the predefined cluster do not need to be continuously under evaluation. The characteristics required for the trust establishment mechanisms within the security framework are:

- Support for pre-established and stable trust relationships
- Provide adaptive and flexible mechanisms for trust evaluation between nodes of heterogeneous deployments
- Support trust revocation in a controlled manner

The following Table 7 presents the scope of the threats and the trust requirements. Only the relevant threats are listed.

Threats	**Pre-established**	**Trust evaluation**	**Revocation**
Threats to confidentiality	IN, SUB	IN, SUB	IN, SUB
Threats to integrity	IN, SUB	IN, SUB	IN, SUB
Threats to data aggregation	IN	IN	IN
Threats to localisation and time synchronisation	IN	IN	IN
Threats to reprogramming	IN, SUB		
Threats to information sharing		UN	UN

Table 7: Scope of the threats and trust requirements

3.2.4. Privacy Requirements for the Pervasive Health Care

Preserving the privacy of the individuals, acting within an information system generally entails keeping their personal information confidential and accessible only to authorised parties. Especially for sensor networks,

however, ensuring the confidentiality of the data does not suffice. For example, confidentiality of the messages content would not protect from tracking the relative location of a BSN and from it – of the real end-users. The additional requirements that are set are:

- Provision of mechanisms for controlled data disclosure based on rules and policies. Those mechanisms should operate according to the data sensitivity level and the data abstraction level, and protect from information induction through sensed data correlation.
- Protection of the identity of the nodes related to users through anonymity and pseudonymity mechanisms.
- Provision of user's notice and choice mechanisms to be applied when a user-related device has user interaction capabilities. The responsibility of those mechanisms is to provide awareness to the users whose data for or the environment surrounding them is being collected. They also have to empower the users to control, by making informed decisions, what personal data will be disclosed and which of the network pseudonyms representing them should be used.

Anonymity description and requirements

Anonymity mechanisms can ensure that users may use a resource or a service without being distinguished from other users and without disclosing their identity to third parties. Anonymity is defined as "the state of not being identifiable within a set of subjects, referred to as the anonymity set" **Fejl! Henvisningskilde ikke fundet.**. With respect to acting entities, the anonymity set consists of the subjects who might cause an action. With respect to addressees (subjects being addressed), the anonymity set consists of the subjects who might be addressed. It is thus a requirement for anonymity mechanisms to be context-aware. [12]

As long as the users are anonymous, they could disclose any personal data, such as the location, that can be considered as essential in future ubiquitous sensor networks. Considering a user's location as personal data, as long as no identifying information is attached to the location, i.e., the user is anonymous, the privacy of the user is protected. As in many network settings the use of identifiers is integral part and often necessary for correct operation of most applications, the goal is to make these identifiers temporary and change them to prevent the collection of too many information about a node that – in the long run – will help identifying it. In addition, changing identifiers in the right situation helps to break the connection to any identifying information that – purposefully or not – have been provided to the peer. Like this, the users can maintain control of the information that can be associated to them.

In order for anonymity to be achieved, the data communicated in the sensor network needs either to be depersonalised or pseudonymised with respect to the identity of the sender, in cases that a legitimate network service requires user identification. Pseudonymity is the use of pseudonyms as IDs **Fejl! Henvisningskilde ikke fundet.**. Pseudonyms with different scopes can be used for each communication, from node pseudonyms to transaction pseudonyms, for achieving different levels of long-term unlinkability. In general, anonymity is stronger the more often and independently the pseudonyms are selected or produced.

In addition, the potential impact of the pseudonym change is also important. Situations that allow a direct mapping of the pseudonym to the node, for example by restricted space identification, may require a pseudonym change shortly before and after this situation, in order to limit the amount of available information about the traces for the identified user. Following this, an important question which is investigated in the research literature is for the trade-off between how often the pseudonyms are changed and the achieved anonymity level on one side, and the application requirements on the other side. Having in mind the resource constrained sensor nodes and the cost to compute a new pseudonym, in comparison with the standard approach when the pseudonyms are changed periodically, it is of importance the suitable moment when a pseudonym must be changed [12]. Thus the node must have mechanism to evaluate the current context in order to decide when the most suitable time to change the pseudonym is, in order to avoid energy waste.

The following Table 8 presents the scope of the threats and the privacy requirements. Only the relevant threats are listed.

Threats	**Controlled data disclosure**	**Protection of the identity of the nodes**	**Notice and choice**
Threats to confidentiality	IN, SUB	IN, SUB	SUB

Threats to data aggregation	IN	IN	
Threats to information sharing	UN	UN	UN

Table 8: Scope of the threats and privacy requirements

3.2.5. Security requirements for context data for the Pervasive Health Care

For the three scenarios discussed in the previous section, the high-level context elements have been described. They are used in order to analyse in more detail the requirements that the proposed in this report security framework must cover, because they classify both the diverse characteristics and roles of the devices, and the types of information that are captured and communicated. Based on the security needs, the integrity needs and the sensitivity of the data, along with the capabilities of the communicating parties, the context elements are used in order to identify and characterise the security requirements.

The following two tables include an evaluation of the security requirements for the context elements. The aim towards the evaluation of the context elements is twofold. Firstly, it will assist on the understanding of the various security requirements that the security framework needs to fulfil. Secondly, it will provide the basis for the security framework adaptation and configuration guidelines that will be formulated in Section 5.5.2. These guidelines will assist later in the applying the security framework to the scenario, the role of each node in the network and the context attribute it belongs to.

The Table 9 contains the security, privacy and trust requirements described in the previous subsections:

Types	**Requirements**
General security requirements	Confidentiality (CO)
	Integrity – Freshness (IF)
	Authentication (AT)
	Authorisation (AS)
Trust requirements	Pre-established trust (PT)
	Adaptive trust negotiation (AT)
	Trust revocation (RT)
Privacy requirements	Controlled data disclosure (CP)
	Identity management (IP)
	Notice and choice (NC)

Table 9: Type of security, privacy and trust requirements for context data

For each context element, it is indicated if the security requirement applies (Yes/No), and at what degree (S: Strong, M: Medium, W: Weak) the requirement is estimated to be important. For example, when Strong is used for the Integrity requirement, it indicates both that the integrity of the information is considered critical and that the device capabilities are such so that the requirement can be fulfilled. When used for Identity management, "Strong" means that pseudonyms with high degree of un-linkability should be used.
In Table 10 the security requirements associated to the contexts are presented [3]. Given the high sensitiveness of the treated data in the healthcare scenario, only the Movement of a person context is assigned with lower security and privacy requirements than the other contexts.

	Comm. Scope	**CO**	**IF**	**AT**	**AS**	**PT**	**AT**	**RT**	**CP**	**IP**	**NC**
Indoor Location	SUB	S	S	S	S	S	S	S	S	S	S
	UN	W	N	W	W	W	W	W	W	W	W
	IN	S	S	S	S	S	S	S	S	S	N
	SUB	S	S	S	S	S	S	S	S	S	S
Outdoor	SUB	S	S	S	S	S	S	S	S	S	S

Location	UN	W	N	W	W	W	W	W	W	W	W
	IN	S	S	S	S	S	S	S	S	S	N
	SUB	S	S	S	S	S	S	S	S	S	S
Vital Functions	IN	S	S	S	S	S	S	S	S	S	N
	SUB	S	S	S	S	S	S	S	S	S	S
	UN	W	N	W	W	W	W	W	W	W	W

Table 10: Security, privacy and trust requirements associated to the context attributes

3.2.6. Summary of Section 3.2

This section presented one of the original contributions of this thesis – the security, privacy and trust requirements for the reference scenario, including the requirements for the context data. In order to build a pervasive system which exactly protects the security, privacy and trust aspects to the most efficiency, the exact requirements for security, privacy and trust which are valid for the reference scenario were investigated. To do that, the security, privacy and trust objectives were presented in a table form providing short descriptions of the objectives. The security and privacy objectives were further mapped to possible threats for which these objectives provide countermeasures. Since the security threats are related to different parts of the architecture and to different scopes of the communication, the scope of the threats for security, privacy and trust was mapped to the three types of the communications which are discussed in this report – namely, communication within the nodes of the network; communication with nodes of trusted subscribed networks and occasional communication with nodes of unknown networks.
As explained previously, the context plays an important role in the proposed in this thesis solutions. Communication of context data in the reference scenario (indoor/outdoor location, vital signs) also has security, privacy and trust requirements. They have been evaluated in the end of the chapter and assigned Strong, Medium or Weak classification.

3.3. Threats analysis for WSNs in Pervasive Health Care scenarios

This section first describes the threat analysis methodology which will be used in order to analyse the security threats, risks and vulnerabilities when pervasive systems with WSNs have been developed. Then eight steps will be followed in the detailed analysis – starting from describing the system, then identifying the assets and mapping them, defining the threat model, and in the end - determining the risks and proposing mitigation plan. The presented in this section material is one of the contributions in this thesis.

The described scenarios for the pervasive health care involve gathering and communicating data related to the medical staff physiological conditions, to patients' physiological conditions, personal information, medical history, and patient's activity, location of hospital equipment and physical parameters of the environment. This type of data is sensitive because of privacy concerns, especially when it can be combined with information about the actual identities or physical location of patients and medical staff. Attacks against availability, data integrity, confidentiality, privacy of patient sensitive information and location anonymity are considered likely and their impact would be high, since the services offered in most of the scenarios are considered critical.
In general, attacks on the pervasive health care scenarios will target specific individuals (patients, medical or emergency staff). The aim of the attacks would be the collection of sensitive user information, health status, medication list, medical history or location information for large sets of users, which can be used for making harm to an individual. The benefits to the attacker would thus be measured in terms of financial gain, even though sometimes the assets are abstract and it is difficult to set a value. Attacks against specific individuals could be invoked for activities monitoring, blackmail purposes or initiated by insurance companies.
Another type of attack in the pervasive health care application space and specifically on the emergency coordination, could be attacks aiming at disrupting the effective coordination of a rescue activity.
In order to make detailed analysis on the security threats for the pervasive health care scenarios, in Tables 2 and 3 it was presented all use cases, the business benefits, the type of information which is subject to communication and pieces of information which could be subject to attacks. In this table Electronic Patient Record (EPR) consists

of: medical history, diagnose, medications, chronic diseases, allergies, previous treatments and current health status of a patient. The description of the systems and the use cases is actually the initial step in the threat analysis. All the steps in the threat analysis which must be followed, will be presented in the next paragraphs.

3.3.1. Threat analysis methodology

The threat analysis is a formal process identifying, documenting and mitigating the security threats and vulnerability of a system. Following the threat analysis methodology, proposed in [14] **Fejl! Henvisningskilde ikke fundet.**, in this subsection the threats and vulnerabilities for the reference scenarios will be discussed and mitigation measures will be proposed. The threat analysis process is divided in three stages – threats modelling, assets mapping and building the mitigation plan.
Threat modelling is a method of assessing and documenting the security risk associated with an application that involves also understanding the goals of an adversary in attacking a system based on the assets of interest. This allows to enumerate the threats and also to discover the vulnerabilities. Enumerating threats and vulnerabilities creates the threat and vulnerability profiles for a system, describing all the potential attacks and all valid attack paths. Briefly speaking, **the resulted threat model** has the following components: A list of threat profiles, a list of vulnerability profiles, a list of threat scenarios, a list of use cases. This phase can help to identify both the security strengths and weaknesses of the system [14] [16]. To begin with, the system has to be understood completely, this means to know the goals, the actors and the devices involved. Then, the next step is the assets mapping. Here, everything that could be damaged or violated must be identified. Asset mapping involves identifying and documenting the tangible and intangible resources of the system and identify the related entry points of the system. The assets value is used as the basis for calculating threat risks and for prioritising countermeasures, assets need to be prioritised. In some cases the value of assets is less intuitive especially when they are abstract.
The third stage of the threat analysis is building a mitigation plan, namely selecting from the list of all the proposed countermeasures, the most effective combination. This involves determining threats, determining vulnerabilities, analysing risks. The risk management helps to balance between what is acceptable and what is possible. From the threat and vulnerability list it is possible to extract the information about which threat pose the highest risk value. The aspects, which have to be taken into account to assess the risk, are the impact, the damage to the assets when the threat would materialise, the size of the vulnerabilities and the likelihood that the threat will try to materialise.
The result of this analysis is a set of countermeasures that might mitigate the threats identified. Since the implementation of all the proposed countermeasures is, in most of the cases, impractical due to limitation of budget, time and resources, the goal of a beneficial threats analysis process is to propose the set of the most cost-effective countermeasures against the identified threat.

In [14], eight steps have been proposed for the threat analysis:

Step 1 – Description of the system: network overview and use cases
Step 2 – Analyse the technical background of the use cases
Step 3 – Identify Assets
Step 4 – Determining Threats and defining threat scenarios
Step 5 – Determining Vulnerabilities
Step 6 – Asset Mapping
Step 7 – Risk Management
Step 8 – Mitigation Plan

In the following sections, this methodology will be applied for the threat analysis.

The result of this exercise will be a detailed threat analysis for WSNs in Pervasive Health Care applications with a thorough threat model. This will be one of the main contributions of this PhD report since to the best of our knowledge, only general threat analysis has been published until now in the literature and not specific for pervasive tele-care scenarios. [17]

3.3.2. Applying the threat analysis methodology

Step 1 – Description of the system: network overview and use cases

In the Section 3.1.5, the reference scenarios and use cases have been discussed, identifying the envisaged services, their goals, the users (the actors) and the used devices. They are summarised in Table 11. The primary actor in the Pervasive Health Care Applications using WSNs is the person using the WSNs – medical staff, hospital administration and patient. Other actors related to pervasive healthcare services could be patients family, relatives and friends, network providers, service providers, insurance companies, others parties requesting information or services, anyone who the user sends a message or anyone who sends a message to the user, etc. In this discussions the focus is mainly on **the medical staff, hospital administration and patient since they are the primary end-users.**

Scenarios	Goal of the scenario	Actors and confidential information to be exchanged	Main Technical Functionalities
Wireless Hospital	Simplifying the procedure for medical staff, speed up and improve the accuracy of the diagnose and treatment	Medical staff – current physiological data, calendars, number of patients, current location, personal profile Hospital administration - administrative information, number and location of equipment, number of patients Patients - identity, social security number, EPR, location, personal profile	TF1 - Measure vital signs TF2 - Communicate vital signs TF3 - Message Notification TF4 - Request current vital signs of a person TF5 - Define position of a person/equipment TF6 - Request position of a person/equipment TF7 - Alert notification TF11- Request data from user profile TF12 - Request data from EPR TF13 - Request data from calendars
Residential Health Monitoring	Enabling the patients to maintain their life outside the hospital	Patients - identity, social security number, EPR, current location, personal profile	TF1 - Measure vital signs TF2 - Communicate vital signs TF4 - Request current vital signs of a person TF5 - Define position of a person TF6 - Request position of a person TF7 - Alert notification TF12 - Request data from EPR
Emergency Coordination	Supporting the rescue staff, emergency physicians, rescue transport, intelligent emergency coordination	Hospital administration - availability of the medical equipment, available medications, location of the accidents, location of the rescue team, number of casualties Patients - identity, social security number, EPR, current location, personal profile	TF8 - Define and communicate position of a team TF9 - Request position of a team TF2 - Communicate patient's vital signs TF10 - Communication among teams

Table 11: Goal of the scenarios and technical functionalities

Step 2 – Analyse the technical background of the use cases

The system overview is a description of the static parts of the system and contains a list of requirements, the system architecture, the system environment, a list of technologies being used and a list of things which require security attention. Description of the reference scenario and information flow diagram together with list of security and privacy requirements is presented in Section 3.1. Here a picture for the system architecture is added and a list of main things which require security attention which could be used by an adversary as attack entry points to the system.

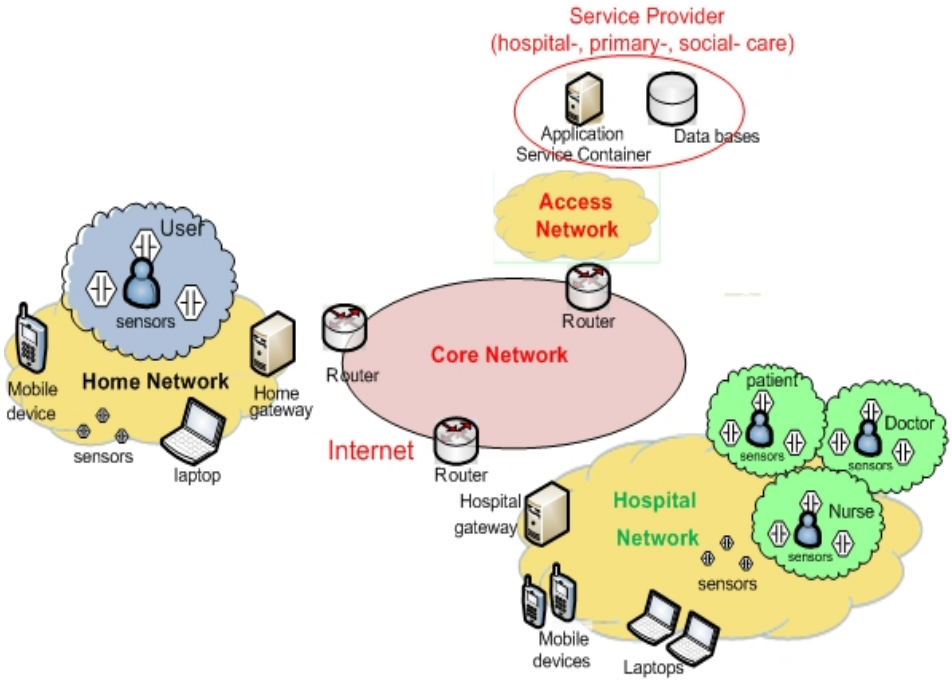


Figure 10: System architecture for pervasive health care scenarios

List of the most important Entry Points (EP) to the system which are specific for the Wireless hospital use cases is presented in the following Table 12:

Entry Point ID	Name	Description
EP1	Wireless radio link	All wireless radio links should provide fair MAC schemes. Also wireless links can be weak, because potentially, anyone can pickup the signal, as it is broadcast in every direction
EP2	Establish a secure link	The first thing two nodes must do before they can establish a secure link, is to communicate with each other over an **insecure link**. This communication must establish a secured link. The way how this insecure communication happens is very important for the system security
EP3	Sensitive data stored in personal devices	End user's sensitive data stored in personal devices must be protected such that no disclosure of data is allowed without permission of the user
EP4	Sensitive data stored in hospital server	End user's sensitive data stored in hospital server must be protected in such a way that only authorised persons can access it or it must be encrypted and even if an unauthorised access happened, the sensitive data will not be revealed.
EP5	Take over the role of the WSNs coordinator in case of energy shortage	Every coordinator of WSN, should have a power check. Before running out of power the device should send a message to the rest of the cluster that someone has to take-over the functionalities. This message should be sent, such that there is enough time for the cluster to relocate the functionalities to other nodes. If this is not done (thus, when the device

		loses power before take-over), it is then possible for another (hostile) device to take its place, without the rest of the network noticing. A usual take-over should be done by authentication of the two nodes: the old and the new one.
EP6	Malicious node	If an attacker compromises a node, he could later use this node to either disrupt communication or steal data
EP7	Any place in close proximity of WSNs where an attacker could hide	In this situation, an attacker could use more powerful device to jam the communication
EP8	Direct psychical access to sensor node	If there is no good access control policies in a hospital, an adversary could enter the hospital and physically damage a sensor node
EP9	Context information provided by untrustworthy providers	In the pervasive health care applications, in some situations, the systems decisions depend on provision of context information by external providers. If the provided context information is wrong, this might lead to discloser of sensitive data to non-trusted parties

Table 12: Description of entry points for pervasive health care scenarios

Step 3 – Identify Assets and Step 6 – Assets Mapping

In this stage everything which can be damaged or violated in the network is listed, specifying to which actor the assets have a certain personal and sensitive value. The assets could be representing content or context, related to security and privacy and physical assets. For the sake of simplicity, only the general categories are enumerated, without specifying the number of asset for each specific actor.
In step 6, the value of each asset must be identified and prioritised. Even though giving a value to some of the assets, related to a person, is a very subjective process, here suggestion for evaluation is given based on the perception of the author. The assets are mapped to three values - defined as – High, Medium, Low.

Assets ID	List of Assets	Type of actor	Value of the asset
Physical assets			
AS1	Sensors which are part of BSN	Patient, doctor, medical staff	H
AS2	Sensors which are part of the environment	Hospital administration	L
AS3	Mobile terminal	Doctor or medical staff	H
AS4	Hospital server	Hospital administration	H
Assets related to security			
AS5	User ID and credentials	Patient, doctor, medical staff, administration	H
AS6	Passwords and secret keys	Patient, doctor, medical staff, hospital administration	H
AS7	User profile	Patient, doctor, medical staff, hospital administration	H
AS8	List of trusted devices and their access rights	Patient, doctor, medical staff, hospital administration	H
Assets related to privacy			
AS9	Mobile terminal's "identity" (to whom a certain smart phone or PDA belongs)	Doctor or medical staff	H
AS10	Vital Functions of a person (for a patient - part of EPR)	Patient, doctor, medical staff	H
AS11	Location of a person	Patient, doctor, medical staff	H
AS12	Location of a device or equipment	Hospital administration	M
AS13	Person's ID (for a patient - part of EPR)	Patient, doctor, medical staff	H
AS14	Personal information stored in the user profile (names, address, bank account, social security number, friends, family)	Patient, doctor, medical staff	H

AS15	Medical history of a patient (part of EPR)	Patient	H
AS16	Movement pattern or history of a person	Patient, doctor, medical staff	M
AS17	Environmental information	Hospital administration	L

Table 13: List and importance of assets

Definition of the threat model for WSNs in Pervasive Health Care Applications

Step 4 – Determining threats and defining threat scenarios

In the Table 5 in Section 3.2 the major security and privacy objectives in the Pervasive Health Care scenarios and the threats which can violate these objectives are described. This information is necessary for the later stage, when the threats profiles will be built.

From these objectives, it can be seen that the major functional component for these applications will be

- *User Data Protection*, in order to be able to define the rules of access. These may be simple in terms of being part of the network, or more complex as to who may read which parts of the medical record of a particular person.
- *Cryptography Support*, in order to manage the keys within the network and carry out cryptographic operations. Keys may need to be selected such that the access rules are enforced; key management techniques must be chosen such that they fit the needs for the sensor networks.
- *Security Audit* may be relevant in order to track back security violations, in particular, where sensible user data are disseminated, e.g. in the medical scenario. For sensible audit data, *Identification and Authentication* may be necessary. In general, security audit may include lower level intrusion detection schemes and appropriate reactions, but this is not mandatory for this application.

When building threat profiles, an important question to be answered is – "How the intruder can materialise a specific threat?" To answer this question, threat scenarios are also provided as part of the threat profile. Threat scenarios of the pervasive health care are presented in the following paragraph.

Threat scenarios

After determining the security and privacy threats, the possible threat scenarios (TS) must be identified. These scenarios show how the threat materialises, in other words how the system is compromised. The threat scenario should contain all the actions which can possibly happen. An attack tree is a good way to describe and investigate threat scenarios. The determination of entry points, e.g. the points in the network where the threat-source enters or interacts for the first time with the network, is part of building threat scenarios. For simplicity sake the threat scenarios from the highest level of the attack tree are shown here, giving their ID too.

1st level	**2nd level**
TS1 - the sensor is destroyed	TS1.1 - physically destroyed by a person
	TS1.2 - chemically destroyed if some chemicals are in the environment
	TS1.3 - destroyed if something happens in parts of the building
TS2 - adversary listens to the wireless channel	TS2.1 - unauthorised monitoring of communication
	TS2.2 - the message is not encrypted
TS3 - The attacker assumes the identity of a trusted entity	TS3.1 – the attacker steals somehow identity information
	TS3.2 - the attacker overhears or eavesdrops identity information
TS4 - attacker gets access to data he is not authorised to access	TS4.1 - attackers has obtained and uses user's password
	TS4.2 - access to the data is not protected with a password

TS5- attacker changes the message	TS5.1 - attacker may modify parts of the message
	TS5.2 - an attacker may delete part of the message
TS6 - the attacker obtains confidential information from external source	TS6.1 - The attacker buys the information
	TS6.2 - The attacker blackmails somebody who can provide the confidential information
TS7 - The attacker has different pieces of information	TS7.1 - The attacker has access to information which is stored at different places
	TS7.2 - Some pieces of the information are not protected with access control
	TS7.3 - Some pieces of the information are not encrypted
TS8 - Attackers reveals user's/node's identity	TS8.1 - The user is not anonymous
	TS8.2 - Pseudonyms are used but they are long-term and the identity is revealed
TS9 - information is released to inappropriate party	TS9.1 - Information is sent by mistake
	TS9.2 - Not updated list of parties with authorised access
TS10 - Malicious node uses the same frequency band	
TS11 - Attacker observes traffic information directly	TS11.1 - Attacker follows the route
	TS11.2 - Attacker backtracks the route
TS12 - Attacker infers events by the fact that there exist communication in certain periods	TS12.1 - The attacker can see communication in different parts of the network
TS13 - Sleep deprivation attack	
TS14 - Flooding the network	
TS15 - Malicious node disrupts position identification	
TS16 - Attacker disrupts time synchronisation	
TS17 - Adversary impersonates the source of the code update	TS17.1 - Masquerade the WSN manager
	TS17.2 Impersonate the writer of the code

Table 14: Threat scenarios

To build the threat profiles (Table 15), for each of it a number of characteristics must be described – ID, name, classification, the source of the threat, the assets involved and the entry point to the system. The threat sources could be natural, human or environmental. The classification in the table is made based on the type of the objective – security or privacy.
The following Table 16 presents the threat profiles, grouped by type. More detailed classification of the major threats for the Pervasive Health Care scenarios is presented in Step 7 – Risk Assessment.

Thre at ID	Threat Name	Classification	Source of the threat	Assets involved	Entry point	Threat scenario
Threats to communication links and data integrity						
1	Disrupt Communication	Security	Human, natural	AS10,11,12,13, 14,15,16,17	EP6,7	TS5
2	Disable Sensors	Security	Human, natural, environment	AS1, 2	EP8	TS1
3	Disable Processing	Security	Human, natural, environment	AS10,11,12,13, 14,15,16,17	EP8	TS3, TS17
4	Impair	Security	Human,	AS10,11,12,13,	EP8	TS1

	Transceiver		natural	14,15,16,17		
5	DoS	Security	human	AS10,17	EP5,6	TS13,14
6	Inject False Message	Security	human	AS10,11,12,13, 14,15,16,17	EP1, 6,7	TS10, 3
7	Man-in-the-middle	Security	human	AS10,17	EP6	TS3
Threats to traffic analysis and confidentiality of the communicated data						
8	Eavesdropping	Security	human	AS10,11,12,13, 14,15,16,17	EP1, 7	TS10, TS7.3, TS2, TS2.1
9	Masquerade/ Impersonation	Security	human	AS10,11,12,13, 14,15,16,17	EP6	TS3
10	Node compromise	Security	human	AS10,11,12,13, 14,15,16,17	EP5,6	TS3
11	Add, delete, modify aggregated data	Security	human	AS10,17	EP5,6	TS3,4
12	Inferring location, identities, events	Privacy	Human	AS11,12,13,16	EP1, EP3	TS12, TS12.1, TS7, TS7.1, TS7.2, TS7.3
13	Linking location, identities, events	Privacy	human	AS11,12,13,16	EP1,3	TS12, TS12.1, TS7, TS7.1, TS7.2, TS7.3
Threats to information sharing						
14	Unauthorised Access to data	Security and privacy	human	AS9,10,11,12,1 3,14,15,16,17	EP2,3	TS6, TS6.1, TS6.2
15	Inappropriate release of information to adversaries	Privacy	human	AS9,10,11,12,1 3,14,15,16,17	EP6, 7	TS3, TS9
16	Compromised gateways or nodes	Privacy	human	AS10,17	EP6,8	TS3,4
17	Infer privacy data for the user from context information	Privacy	human	AS11,12,13,16	EP1,7	TS7.2, TS7.3, TS8
Threats to localisation						
18	Track subject's current location	Security	human	AS11,12	EP1,6,7	TS8,9,12, 15
19	Track subject's movements	Privacy	human	AS11,12	EP1,6,7	TS8,9,12, 15
20	Reveal node/ user's identity	Privacy	human	AS13	EP6, 3,1,2	TS8,12
Threats to reprogramming						
21	Reprogramming	Security	human	AS5,6,7,8	EP6,8	TS17, 3
Threats to time synchronisation and freshness						
22	Disrupt time synchronisation	Security	human	AS10	EP1,6	TS5, 10
23	Communication of old massages	Security	human	AS10	EP1,6	TS16
24	Replay message	Security	human	AS10	EP6	TS16
25	Jamming the	Security	human	AS10	EP7	TS10

	communication					
26	Incorrect timing of events	Security	human	AS10, 11,12,16	EP7,6	TS5

Table 15: Threat profiles

Step 5 – Determining Vulnerabilities

After the threat profiles were built, it is now analysed which of the listed threats could be exploited by threat sources through vulnerabilities. The vulnerabilities will show the security and privacy weaknesses of the system which might be realised as attacks.
Vulnerability (V) is a flaw in the network, which can be exploited when a threat materialises. It should be also known which threats exploit the vulnerability. In order to make the mitigation of vulnerabilities more convenient for the security designer, each vulnerability is mapped to a fundamental threat by which it is exploited and the technical functionality during which the vulnerability could be exploited.
Here it is also built vulnerability profiles list, with ID, name, threat scenario, the fundamental threat, the technical functionality and the weakness index. The weakness index can be: *critical, potentially critical, not critical.*
The threat scenarios for the whole system analysed in the previous paragraphs are numerous. For each of them, a number of vulnerabilities exist, thus giving a long list. In the Table 16, where the list is presented, the focus is on those, related mainly to privacy and which are related to the human nature of the end-user. *This is because even though many security measures could be technically implemented in the system, via expensive design efforts, despite of the limited sensor node resource, still, the negligence of the end-user itself may lead to serious privacy breaches. With this list, the intention is to raise awareness for this fact since the pervasive heath care applications will deal with sensitive private data and the users must be informed and they must not neglect the actions which could protect it.*

Vulnerability ID	**Name**	**Exploited by Threat scenario**	**Fundamental threat**	**Technical functionality**	**Weakness index**
Related to human factor					
V1	Low password/credential complexity	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V2	Removed password/credentials by the user	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V3	User stores password/credentials to an easily accessible place	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V4	User mobile terminal could be stolen	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF11	Potentially critical
V5	Users are not sufficiently informed about privacy risks	TS3, TS9	THR15 - Inappropriate release of information to adversaries	TF11	Potentially critical
V6	Users are not sufficiently educated to use security and privacy measures	TS7.2, TS7.3, TS8	THR17 - Infer privacy data for the user from context information	TF11	critical
V7	User does not log-off the system after use	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V8	Password system is not	TS6, TS6.1,	THR14	TF4, TF6,	critical

	user-friendly and is complex and the user does not use it	TS6.2	Unauthorised access	TF9, TF11, TF12, TF13	
V9	Users gives their password/credentials to other persons	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V10	Exposing user's personal information to many institutions and companies	TS12, TS12.1, TS7, TS7.1, TS7.2, TS7.3	THR12, 13 - Inferring and linking location, identities, events	TF11, TF12, TF13	Potentially critical
V11	User has secrets, which can be used to blackmail him	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	Potentially critical
V12	Gullible user	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	Potentially critical
V13	Inattentive user	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	Potentially critical
V14	Impatient user	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	Potentially critical
Related to security design flaws					
V15	Sensitive data not encrypted	TS10, TS7.3, TS2, TS2.1	THR8 - Eavesdropping	TF2, TF3, TF7, TF8, TF10	Critical
V16	Sensitive user data accessed without user's agreement	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V17	Insufficient message encryption	TS10, TS7.3, TS2, TS2.1	THR8 - Eavesdropping	TF2, TF3, TF7, TF8, TF10	Potentially critical
V18	No password/credentials where there should be	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V19	All information related to credentials is sent in one message	TS10, TS7.3, TS2, TS2.1	THR8 - Eavesdropping	TF2, TF3, TF7, TF8, TF10	Potentially critical
V20	Administrator could assign wrong privileges	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
V21	The number of tries to enter the password is unlimited	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	critical
Related to policies and laws					
V22	Privacy laws can be easily violated	TS3, TS9	THR15 - Inappropriate release of information to adversaries	TF4, TF6, TF9, TF11, TF12, TF13	Potentially critical
V23	Weak policy protection and detection	TS3, TS9	THR15 - Inappropriate release of information to adversaries	TF4, TF6, TF9, TF11, TF12, TF13	Potentially critical
V24	Unauthorised people can	TS10, TS7.3,	THR8 -	TF2, TF3,	Potentially

	come close enough to overhear the channel	TS2, TS2.1	Eavesdropping	TF7, TF8, TF10	y Critical
V25	An intruder device is (physically) able to enter the network premises	TS10, TS7.3, TS2, TS2.1	THR8 - Eavesdropping	TF2, TF3, TF7, TF8, TF10	Potentiall y Critical
V26	The password is the only required credential for access (single-point failure)	TS6, TS6.1, TS6.2	THR14 Unauthorised access	TF4, TF6, TF9, TF11, TF12, TF13	Critical
V27	Private information is freely available or easy to access	TS12, TS12.1, TS7, TS7.1, TS7.2, TS7.3	THR12, 13 - Inferring and linking location, identities, events	TF12	Potentiall y critical
Related to trust					
V28	Insufficient user or device credibility check	TS3, TS9	THR15 - Inappropriate release of information to adversaries	TF2, TF3, TF7, TF8, TF10	Potentiall y critical
V29	Insufficient check on the trustworthiness of the service by the user device	TS3, TS9	THR15 - Inappropriate release of information to adversaries	TF2, TF3, TF7, TF8, TF10	critical
V30	Trust-lists on different devices are not synchronised	TS3, TS9	THR15 - Inappropriate release of information to adversaries	TF2, TF3, TF7, TF8, TF10	critical
V31	The device doesn't have a black list of untrustable services, devices	TS3, TS9	THR15 - Inappropriate release of information to adversaries	TF2, TF3, TF7, TF8, TF10	critical

Table 16: Vulnerability profiles

Step 7 - Risk Analysis and Management

A standard qualitative risk analysis based on impact and likelihood is used to assign risk levels to each threat.
The **impact** of the threat is an assessment of the consequences of a successful attack, and is based on factors such as the amount and importance of the compromised information, and the economic cost of the attack and of any recovery actions required from it.
The **likelihood** of the threat is an assessment of the probability of a successful attack, or equivalently the frequency with which successful attacks based on this threat are expected to occur. This assessment is based on several factors including the type, skill level and motivation of attackers, the ease of mounting the attack, availability and cost of any special equipment required, the existence and number of vulnerabilities that may make successful attacks easier, and the likelihood and consequences of the attacker being caught. The impact and likelihood are combined using Table 17 to obtain the overall **risk** level of the threat [3]. In Table 17 and the remainder of this document, the following key is used for impact, likelihood and risk levels:

	Impact		
	L=Low	**M=Medium**	**H=High**

Likelihood				
	L	L	L	M
	M	L	M	H
	H	M	H	H

Table 17: Calculating risk level from impact and likelihood

The risk level will be used in the following paragraphs in order to decide whether any security requirements, or countermeasures, are required to counter the threat. Generally speaking, threats with a low risk can either be ignored or only require minimal protection against. Threats with a medium risk need to be addressed to a reasonable degree of thoroughness, but direct and indirect costs of the security requirements should not be excessive. Threats with a high risk need to be thoroughly addressed with strong security requirements.

Threats to communication links

Threats to Confidentiality

Very sensitive data are exchanged in a healthcare scenario: patients' information as ID, EPR and location are transmitted on the communication link as well as medical staff's information (IDs that might be related to their functions and rights, location and physiological data).

All in all, in this scenario threats to communications links can be considered as the most dangerous ones as an important property as confidentiality might be easily violated with simple and quite cheap equipments. Besides, the attacker does not need to be an expert hacker to be able to perform it.

Threats	**Wireless Hospital**						**Residential Health Monitoring**						**Emergency Coordination**		
	Night Shift Assistant			**Backup Shift Assistant**			**Acute Patient Monitoring**			**Continuous Care**					
	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**
Eavesdropping	*H*	*H*	***H***	*H*	*H*	***H***	*H*	*H*	***H***	*H*	*H*	***H***	*H*	*H*	***H***
Masquerade/ Impersonation	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***
Node compromise	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***

Table 18: Threats to confidentiality in Pervasive Health Care scenarios

Threats to Integrity

Integrity loss is another major threat in medical care applications that might lead to serious damages to the users' safety if the attack is successful. The impact in all the medical application space and for all the threats has to be considered high, as in case of success, attacks will lead to data corruption that can turn into wrong requests and then wrong operations thus likely affecting users' vital functions.
The likelihood is considered to be medium for all the mentioned scenarios and all the threats, as these threats are slightly more difficult to be performed; corruption of data in this scenario is not the first aim of an attacker. The combination of these likelihood and impact leads to have a high risk associated to all the use cases.

Threat	**Wireless Hospital**	**Residential Health Monitoring**	**Emergency**

	Night Shift Assistant			Backup Shift Assistant			Acute Patient Monitoring			Continuous Care			Coordination		
	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**
Man-in-the-middle	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***
Masquerade/ Impersonation	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***H***
Node compromise	*H*	*M*	***H***	*H*	*M*	***H***	*H*	*M*	***M***	*H*	*M*	***M***	*H*	*M*	***H***

Table 19: Threats to integrity in Pervasive Health Care scenarios

Threats to reprogramming

The aim of reprogramming attacks in the pervasive heath care application space would be either to disrupt communications so that the network services would appear unreliable or to gain access to sensitive information collected for patients and/or medical or emergency staff. Since the services offered to the end-users are considered critical, it is likely that reprogramming attacks would aim to modify data or to inject false data into the network. In most of the use cases the impact of reprogramming attacks would be medium or high.

Threat	**Wireless Hospital**						**Residential Health Monitoring**						**Emergency Coordination**		
	Night Shift Assistant			**Backup Shift Assistant**			**Acute Patient Monitoring**			**Continuous Care**					
	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**	Im	Li	**Ri**
Man-in-the-middle	*H*	*M*	***H***	*H*	*M*	***H***	*M*	*L*	***L***	*M*	*L*	***L***	*H*	*M*	***H***
Masquerade/ Impersonation of sender in communications	*H*	*M*	***H***	*H*	*M*	***H***	*M*	*L*	***L***	*M*	*L*	***L***	*H*	*M*	***H***
Node compromise	*H*	*L*	***M***	*H*	*L*	***M***	*H*	*L*	***M***	*H*	*L*	***M***	*H*	*L*	***M***
Masquerade/Impersonation of WSN manager	*H*	*M*	***H***	*H*	*M*	***H***	*M*	*L*	***L***	*M*	*L*	***L***	*H*	*M*	***H***
Masquerade/Impersonation of code originator	*H*	*M*	***H***	*H*	*M*	***H***	*M*	*L*	***L***	*M*	*L*	***L***	*H*	*M*	***H***

Table 20: Threats to reprogramming in Pervasive Health Care scenarios

Step 8 – Mitigation Plan

After the presented very detailed analysis of the threats and vulnerabilities of the system, this section is now concluded with discussing a mitigation plan. This mitigation plan is a set of countermeasures that might mitigate the threats identified.

Proposing countermeasures for all identified threats for WSNs in medical related scenarios gives a big number of security, privacy and trust establishment protocols and algorithms. Many of the current existing solutions presented in Section 2.3.4 could be considered. However, in many of the cases these solutions do not give the full protection, have themselves some weaknesses and may not be very suitable for resource-restricted nodes. It is because of this consideration that the presented below mitigation plan with protocols and algorithms which is considered suitable for WSNs and for the applications in question. The mitigation plan is based on the discussed system, security, privacy and trust requirements for the reference scenario. Since one of the major distinctive characteristics of the work proposed with this PhD thesis is allowing for flexibility in the security and privacy

protection, in the mitigation plan different options for countermeasures are presented which might be used in different combinations, depending on the exact system set-up, sensor node parameters, user requirements, etc. Exactly what combinations of mechanisms and algorithms could be used to ensure flexibility, will be discussed later in this thesis, in Section 5.1.
The implementation of all the proposed above countermeasures is, in most of the cases, impractical due to limitation of budget, cost, time and resources. Additionally, the goal in this PhD report is to provide measures to a set of very specific objectives, defined in the beginning in Section 3.2.1. So, to focus the proposed mitigation plan to reply to the security, privacy and user-friendliness objectives, a set of countermeasures in the form of adaptive, context-aware security and privacy framework for WSNs in pervasive HealthCare applications are proposed. This proposed generic framework is designed in such a way to answer all the listed in this section requirements. Since till now the research community has published some partial solutions to countermeasure, some of the discussed threats and a complete solution is out of the scope of this report.

In the next sections the focus is on the following identified threats:

- **Violate *information privacy***, i.e. any disclosure of personal data or information directly related to the individual using a medical service or application without the user's prior approval or knowledge.
- **Violate *confidentiality of the communication,*** i.e. any disclosure of personal data or information to non-trusted parties.
- **Violate *context privacy***, i.e. any disclosure of identifiable information related to the context in which the user is using the medical service and from which indirect information for the user could be extracted.

The following Table 21 presents the proposed mitigation plan.

Threats and Vulnerabilities	Preventive approaches	Specific Mitigation Options
Violation of Security Aspects		
THR9 - Masquerade/ Impersonation THR10 – Node compromise THR15 - Inappropriate release of information to adversaries	Authentication mechanisms **Fejl! Henvisningskilde ikke fundet.**	Authentication based on the identities claimed by nodes or use of symmetric network and group keys Pairwise authentication using symmetric link keys and μTESLA for source authentication Authentication through Elliptic Curve digital signatures
THR8 – Eavesdropping THR12 – Inferring events, identities, location THR13 – Linking events, identities, location	Encryption mechanisms	Optional Encryption RC5 (CTR mode) 32 bits block length, 6 rounds & 24-bit key RC5 (CTR mode) 32 bits block length, 12 rounds & 40-bit key Asymmetric encryption
THR6 - Inject False Message THR7 – Man-in-the-middle THR11 – Add, delete, modify aggregated data	Integrity protection mechanisms **Fejl! Henvisningskilde ikke fundet.**	Optional integrity protection 0/32 bit integrity 32/64 bit integrity 64/128 bit integrity
THR23 – Communication of old messages THR24 – Replay message THR26 – Incorrect timing of events	Mechanisms to ensure Freshness **Fejl! Henvisningskilde ikke fundet.**	Optional freshness Relative freshness through message sequence numbers Strong freshness through timestamps
Violation of Privacy Aspects		
THR14 - Unauthorised access to data THR16 - Infer privacy data for the user from context information	Controlled information disclosure **Fejl! Henvisningskilde ikke fundet.**	policy – based role – based
THR20 - Reveal node/user's identity	Mechanisms to ensure node anonymity **Fejl! Henvisningskilde ikke fundet.**	pseudonym creation schemes group formation to increase the silence periods capability-based privacy-preserving

		scheme
THR14 - Unauthorised access to data THR15 - Inappropriate release of information to non-trusted parties	Mechanisms for controlled data access; including hierarchical and multi-party access control [24]	hierarchical team-based access control secure multi-party access control
THR18 - Track subject's current location THR19 - Track subject's movements	Mechanisms to ensure location anonymity **Fejl! Henvisningskilde ikke fundet.**	data cloaking mix-zones mix-contexts

Table 21: Mitigation plan

Furthermore, some specific State-of-the Art mechanisms for context-aware controlled information disclosure and adaptive confidentiality will be proposed to prevent that these threats materialise. Together with the above presented threat analysis, threat model and mitigation plan for medical applications with WSNs and with adaptive, context-aware generic privacy protection framework for WSNs in medical scenarios, they are one of the main contributions of this PhD report.

3.3.3. Summary of Section 3.3

This chapter presented one of the main contributions of this thesis – namely thorough security threat and vulnerability analysis, leading to definition of thereat model for pervasive tele-care applications, identification of security risks, risk management and proposal of overall mitigation plan. First, threat analysis methodology was shortly presented consisting of eight main steps. These steps were followed to reach to the final stage. Initially the system was described in terms of scenarios and their goals, main actors in the scenarios and the confidential information which is exchanged during system operation. For each of the main scenarios, main technical functionalities of the system were listed. After that information flow diagram was used to list the security and privacy requirements for the use scenarios. Possible entry points to the system were identified and described which could be used by an adversary to initiate an attack or exploit system vulnerability. After that for each category of main actor, list of assets were identified and value each asset has been defined. The assets were mapped to High, Medium or Low values.

The next step was to determine a list of threats for each security and privacy objective and to define threat scenarios, with the aim to build threat model. The threat scenarios were presented as attack tree, but for the simplicity sake only the first two levels of the tree were presented. The next step was to build threat profiles with threat ID, threat name, type, source of the threat, assets involved, entry point and threat scenario via which an attacker can enter the system or the network. The same approach was further used to build vulnerability profiles – listing vulnerability ID, name, exploited by threat scenario, fundamental threat, technical functionality and weakness index. Risk analysis and risk management for the major threats for the reference scenario were after that proposed.

In the end of the section, overall mitigation plan for the threats for pervasive health applications was presented. Since a complete solution to all threats is out of scope of this report, in the next chapters solutions will be proposed to a subset of the identified threats. However, for the proposed privacy protection framework, for some of the major threats, some suitable existing mechanism will be identified in Section 5.

3.4. Summary of Chapter 3

In order one communication system to be protected against security, privacy and trust attacks and vulnerabilities, the respective requirements must be analysed and fed into a threat and vulnerability model. The goal is to draw up a mitigation plan to overcome these threats and vulnerabilities. Briefly speaking, this is what has been presented in Chapter 3. This process started with detailed analysis of the reference scenario and the use cases and with description of the system (who the main actors are, the devices used, the information flow, context attributes, etc.). Then, the exact security, privacy and trust requirements were drawn up, used as a basis for identification of the major security threats and vulnerabilities. The pervasive health care system was looked at different perspectives – from the main actors and the material and non-material assets for them, to access points which could be used by an attacker to enter the systems, to threat scenarios by which a threat could be materialised, and

in the end solutions by which these threats could be prevented. The proposed solutions are considering the trade off of what is possible to be done and what is realistically and economically feasible. This threat model and mitigation plan could be followed step by step by system designers when they build pervasive health care system which is security protected and protects the privacy of the groups of the end-users.

References

[1] Anelia Mitseva, Mohamad Imine, Neeli .R. Prasad, **"Context-Aware Privacy Protection with Profile Management",** In proceedings of WMASH 2006 (The fourth ACM international Workshop on Wireless Mobile Applications and Services on WLAN Hotspots), pp. 53-62 (ACM Press), September 29, 2006, Los Angeles, USA in conjunction with MobiCOM 2006

[2] Anelia Mitseva, Petia Todorova, Ramon Aguero, Ana Garcia Armada, Christos Panayiotou, Andreas Timm-Giel, Leonardo Maccari, Neeli R. Prasad, **"CRUISE research activities towards Ubiquitous Intelligent Sensing Environments",** IEEE Wireless Communications Magazine, August 2008, Vol.15 No.4, SI on Security in Ad Hoc and Sensor Networks; Wireless Sensor Networks, pp. 52- 59, 1536-1284/08/$25.00 © 2008 IEEE

[3] e-SENSE Del 2.3.1, **"e-SENSE Security Framework**", December 2007

[4] Mitseva, Anelia; Gerlach, Matthias; Prasad, Neeli R. **Privacy Protection Mechanisms for Hybrid Hierarchical Wireless Sensor Networks.** In Proc. of 4th International Symposium on Wireless Communication Systems, Trondheim, 2007. ISWCS 2007. IEEE, 2007. pp. 332-336

[5] Aivaloglou, E.; Mitseva, Anelia; Skianis, C.; Gritzalis, S.; Waller, A.; Prasad, Neeli R.., **Scalable Security Management for Wireless Sensor Networks for Medical Scenarios,** In Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007, pp. 1014-1018, Dec 2007, India

[6] CRUISE Del 230.2, "**Mobility and Security Framework for WSNs",** December 2006

[7] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. **Basic concepts and taxonomy of dependable and secure computing**. IEEE Transactions on dependable and secure computing, 1(1):11–33, January 2004

[8] Workshop report on "**Social Aspects of Cooperating Objects Technologies**", International Workshop of the Coordination Action Embedded WiSeNts (IST-004400), November 1-2, 2006, Technical University Berlin

[9] Hildebrandt, Mireille; Serge Gutwirth (2008) (in English). **Profiling the European Citizen: Cross Disciplinary Perspectives**. Dordrecht: Springer. ISBN 978-1-4020-6913-0

[10] Common Criteria for Information Technology Security Evaluation - **Part2: Security functional requirements**, http://www.commoncriteriaportal.org 2005. http://www.commoncriteriaportal.org.

[11] A. R. Beresford and F. Stajano. **"Location privacy in pervasive computing**". *IEEE Pervasive Computing*, pages 46–55, 2003

[12] Anelia Mitseva, Matthias Gerlach, Christian Räck, Neeli R. Prasad, **"Context-aware Adaptive Privacy Protection for Wireless Sensor Networks"**, in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1032-1036, San Diego, USA, Sept 2006

[13] SAS: A Simple Anonymity Scheme for Clustered Wireless Sensor Networks, http://www.zdnetasia.com/itlibrary/networking-and-communications/0,3800009948,41100281p,00.htm

[14] Neeli Rashmi Prasad, **Threat Model Framework and Methodology for Personal Networks (PNs),** WILLOPAN 2007

[15] A. Stango, D. M. Kyriazanos, N. Prasad, **"A Threat Analysis Methodology for Security Evaluation and Enhancement Planning"**, to appear in SECURWARE 2009, June 18-23, 2009 - Athens/Vouliagmeni, Greece

[16] F. Swiderki, W. Snyder, **"Threat Modelling**", Microsoft Press 2004

[17] Sokullu, Radosveta; Korkmaz, Ilker; Dagdeviren, Orhan; Mitseva, Anelia; Prasad, Neeli R., **An Investigation on IEEE 802.15.4 MAC Layer Attacks,** In Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007, pp. 1019-1023, Dec 2007, India

[18] Sven Lachmund, Frank Fransen, Eddy Olk, "**Context-Awareness, Security and Trust**", In proceedings of WPMC 2005, September 2005, Aalborg, Denmark

[19] Venkatasubramanian, K.K.; Venkatasubramanian; Banerjee, A.; Gupta, S.K.S., **EKG-based key agreement in Body Sensor Networks,** IEEE INFOCOM Workshops 2008, Volume , Issue , 13-18 April 2008 Page(s):1 – 6, Digital Object Identifier 10.1109/INFOCOM.2008.4544608

[20] Giani, A.; Roosta, T.; Sastry, S, **Integrity checker for wireless sensor networks in health care applications,** Second International Conference on Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008, Volume , Issue , Jan. 30 2008-Feb. 1 2008 Page(s):135 – 138, Digital Object Identifier 10.1109/PCTHEALTH.2008.4571051

[21] Yi-Ying Zhang; Wen-Cheng Yang; Kee-Bum Kim; Min-Yu Cui; Myong-Soon Park; A Rekey-Boosted Security Protocol in Hierarchical Wireless Sensor Network; International Conference on Multimedia and Ubiquitous Engineering, 2008. MUE 2008; Volume , Issue , 24-26 April 2008, Page(s):57 - 61, Digital Object Identifier 10.1109/MUE.2008.10

[22] Stefan Schmidt, Holger Krahn, Stefan Fischer, and Dietmar Watjen, **A Security Architecture for Mobile Wireless Sensor Networks,** Springer-Verlag Berlin Heidelberg 2005, C. Castelluccia et al. (Eds.): ESAS 2004, LNCS 3313, pp. 166–177, 2005

[23] Yi Ouyang, Zhengyi Le, Yurong Xu, Nikos Triandopoulos, Sheng Zhang, James Ford and Fillia Makedon, **Providing Anonymity in Wireless Sensor Networks**, ICPS'07 : IEEE International Conference on Pervasive Services July 15 - 20, 2007, Istanbul, Turkey

[24] Eskeland, S.; Oleshchuk, V., **Hierarchical Multi-Party Key Agreement for Wireless Networks,** Third International Symposium on Information Assurance and Security, 2007. IAS 2007. Volume , Issue , 29-31 Aug. 2007 Page(s):39 – 43, Digital Object Identifier 10.1109/IAS.2007.82

[25] M. Gruteser and D. Grunwald, **Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking**, Proceedings of First International Conference on Mobile Systems, Applications, and Services (MobiSys'03) (May 2003), pages 31-42

Chapter 4 - Presentation of Adaptive Context-Aware Privacy Protection Framework

This chapter presents the Adaptive Context-Aware Privacy Protection (ACAPP) Framework. Initially the motivation for this proposal is presented. System specific requirements and privacy objectives are further presented. Next section describes how the ACAPP framework is integrated in the Security Manager, also explaining the information flow among the building blocks. After that, the proposed privacy protection mechanisms are presented. How the proposed concepts and mechanisms could be applied in the reference scenarios is explained further. This part is concluded with comparison of this proposal with existing solutions.

4. Proposed Adaptive Context-Aware Privacy Protection Framework

The main focus of this chapter is to present one of the main gravity points in this thesis – namely, the proposed Adaptive Context-Aware Privacy Protection Framework (ACAPP), starting with list of its key features. The main building blocks of the framework are described, together with how it is integrated in context-aware security management. The importance of the context-awareness is discussed in order to make the framework more optimal and suitable for the reference scenarios. In the end, it is described how the security management and context monitoring could be applied in practice.

4.1. Motivation for proposing The Adaptive Context-Aware Privacy Protection Framework

The principal distinctive aspect of ubiquitous sensorised environments using the reference HHA is the heterogeneity of the various access systems that will be combined into a common, flexible and seamless platform to complement each other in an optimum way for different application and service requirements [1]. Ubiquitous sensorised environments and future mobile environments will provide a framework for adequate connectivity for data delivery. On top of the connectivity, open architectures and platforms for service control and delivery will allow a wealth of communication services and applications to be offered to users and businesses [2]. The integration of ubiquitous WSNs in future mobile systems could be obtained by providing a toolbox approach [3]. Such a toolbox approach is necessary in order to satisfy the diverse requirements from different sensor network applications and scenarios.

At the same time, the specifics of HHA as reference network architecture raise new research issues for privacy and trust establishment:

- the *hybrid nature* of the architecture due to interaction between different networks with different security and privacy services and trust establishment policies,
- the *large number of nodes* in level 2 (environment) and objects in level 3 which might themselves be hierarchically organised,
- the nodes in the levels 2 (environment) and 3 (objects), even though with different resource constraints, are still *very limited in computation capabilities*, and
- the sinks in level 1(people) are *mobile terminals*.

The security of the data and the communications (which leads to integrity) are essential requirements for the end applications and services to be reliable, while the protection of the privacy of the end users is essential for their adoption. Privacy concerns arise mainly because different types of sensor networks may be deployed for different purposes and will have different levels of trust. Hence, the diverse security, trust and privacy requirements of the applications, services and nodes impose the need for an adaptive, scalable and flexible security and privacy framework.

In the HHA, diversity comes also from the fact that the nodes from certain levels have various computational, memory and power capabilities and different roles in the network (for example gateway, coordinator, end-node).

This calls for scalable, adaptive and general enough approaches for privacy protection and trust establishment in the HHA. As pointed out previously in Section 2.3, from the diverse set of security issues in the levels 1 (people), 2 (environment), and 3 (objects) of the HHA, the ones related to security, privacy and context-awareness are discussed in this thesis.

All these essentials call for flexible, scalable and adaptable solutions, and are the motivation for proposing the following core properties of the security and privacy framework:

- *Flexibility and Scalability*
- *Context-awareness*
- *Adaptability*

These core properties will be discussed in more detail in the following sections. But before that, here their definitions are presented:

- *Flexibility and Scalability* – reconfigurable framework to provide the most suitable levels of security and privacy functionality for different node architectures, hardware limitations, user requirements, and application spaces. Essentially, different versions of the framework can be deployed for the network components, providing varying levels of security and privacy protection functionality.
- *Context-awareness* - the ability of the privacy protection framework and mechanisms to react on change in the context in such a way that they provide the best privacy protection for the users and their sensitive information while minimising the user distractions.
- *Adaptability* – ensuring that the system works at the best of its capability, taking into account the trade-off among device constraints, change in context and different users' preferences. Essentially, the security protocols and primitives that are used for each communication after the network deployment are selected according to the context of the communication.

4.2. System specific requirements for the security and privacy framework

In order to support the requirements of future applications that may emerge with the integration of WSNs in ubiquitous systems, flexible architectures are required. Such architectures, for example the e-SENSE architecture **Fejl! Henvisningskilde ikke fundet.**, introduce the desired flexibility. The overall architectural framework must:

- be *flexible enough* to allow a system to be configured for various application environments based on the selection of appropriate protocols and service functions
- provide relevant infrastructure within the system to allow *more efficient operation* of protocols through *cross layer interaction*
- allow the WSNs system *to adapt* its behaviour according to change in context
- offer *enhanced support functionality* required for many applications

To support the features listed in above for the overall architecture, the integrated security and privacy framework should comply with the following system specific requirements:

- **Power efficiency:** one of the most important constraints in WSNs is the low power consumption requirements. In fact, being wireless sensor nodes limited in computational capacity, memory and power, and being the power sources generally irreplaceable, their lifetime is strictly related to the power consumption. The long life time of such networks depends crucially on the wise and frugal use of energy. Additionally, the support for security, privacy and trust mechanisms in general increases the communication overhead. This justifies the need of an adaptive and flexible security framework which aims at preserving energy.

- **Adaptability:** to ensure that the system works at its best possible, taking into account the trade-off between device constraints, which changes with the time, the changes of the context (e.g. service or location) and the different user's preferences. Adaptive variations are needed in order that the systems continue functioning as programmed by the end-user as well as they meet the computational demands and power consumption. Essentially, the security protocols and primitives which are used for each communication after the network deployment are selected according to the context of the communication.
- **Flexibility and Scalability:** the framework should be reconfigurable and scalable in order to provide the best suitable levels of security, trust and privacy functionality for different node architectures, hardware limitations, end-user requirements, and application spaces. Essentially, different versions of the framework to be deployed for the network components, providing varying levels of security functionality.
- **Profile-based:** in order to make use of available context information and to allow for personalisation of the ubiquitous systems, descriptive profiles should be used. These profiles could be related to the nodes, the context, the end-user, etc…
- **Policy-based:** the framework must accommodate very diverse scenarios having different requirements with security, privacy and trust. The goal is to help the overall system to work with minimum intervention from an administrator, industry expert, medical staff or end-user. Therefore, decisions must be taken based on beforehand agreed policies and rules.
- **Support for mobility: i**n most of the application spaces, different types of mobility exist. For instance, this might be a mobility of the entire BSN attached to a person's body with respect to sensors in the environment or only a mobility of some of the sensors within BSN. Support for mobility in this discussion must be considered as information for node location (and from here, person location) and the change in context when a node moves. Mobility will influence the work of the following mechanisms:
    - Trust establishment – like mechanisms for mobile nodes to establish trust relationships when entering an environment with unknown nodes
    - Re-authentication – like fast and energy-efficient re-authentication mechanisms
    - Privacy protection – like different policies for disclosing sensitive information based on the current location of the source of the sensitive data, the location of the requesting party, type of requested data, etc…
    - Definition of different security levels according to the location of the nodes
- **Requirement for Graphical User Interface:** in the pervasive healthcare, the end-user must be able to interact with the system via simple and intuitive GUI, in order to select and modify preferences, settings and rules. The parameters modified by the user might concern privacy protection mechanism (as the users might be able to select the most suited privacy level according to their personal preferences), security level and trust establishment.
- **Pre-defined settings and policies:** some settings and policies must be pre-defined. This means that as soon as the node enters the network, according to the context information and to the information provided by the network administrator or the end-users themselves, default settings are assigned. These will help the system to operate without intervention and to adapt to the changing contexts.

4.3. Privacy objectives for the selected scenarios

In Section 3.3, where the threat model was described, the security and privacy objectives for the system were briefly presented. In the following paragraphs, privacy objectives for the reference scenario are elaborated in more details.

As outlined in [5], the success of the end-user acceptance in pervasive health scenarios depends on the provision of appropriate privacy mechanisms and ensuring flexibility and easiness of use in the end-user control over these mechanisms.
The reference scenario was described in Section 3.1.2. Here more details from point of view of HHA are provided. In a hospital, patients are equipped with BSN with a coordinator node (in level 2) measuring their physical status. The data collected from BSN is transmitted to the hospital database via mobile terminals carried by frequently passing by medical staff (nodes in level 1). The medical staffs are also equipped with BSNs to detect their overall status. The coordinator node (CN) in the BSN and the mobile terminals are fully functional nodes (FFN) while the end sensor nodes (EN) from the BSN are very limited in resources. At the same time, from the sensors in the environment, information for the position of the medical personnel or the patients can be provided. Data for the medical personnel can be sent to their colleagues on shift to perform collaborative tasks or in case of emergency. In home settings, information for the patient can be sent to care providers. An obvious concern in these scenarios is privacy in a number of aspects.
Privacy in this discussion is broadly defined as the possibility for the user to have control over the disclosure of privacy sensitive information. Important question is for example "who sends what type of data to whom and when and who can access it". Privacy can be violated by for example revealing sensitive information or user's identity to non-trusted parties, by tracing user's location or monitoring the history of user's behaviour. The threats for privacy were discussed in more details in Section 3.3.2.

The privacy of the users could be enforced by following public privacy regulations and the user's control over the disclosure of all their private sensitive information. The context information is either directly related to the person or to objects the user can interact with or to situations or environments (Tables 3, 4). All of this data can reveal to a certain degree, directly or indirectly, private aspects of the user.

- *Identifying information* can be used to trace a node or device and following from this, to recognise or identify the user (in the discussed scenario medical staff or patient) and could also contain additional information about the surrounding environment, the state of an object belonging to the person, or an object under the control of the user from which privacy attributes of the person might be inferred.
- *Personal data* are those data that are directly related to the health status of a person and other personal information such as address, social security number, etc. Both identifying information and personal data are assets for the user (Table 13) and might have different privacy values to the user and hence require *different levels of protection*.

Countermeasures for these threats will seek to disclose personal data only to trustworthy parties, to keep the user sensitive data confidential, to provide the minimum required node-, user- or context- identifiable information, to ensure control when private information must be revealed even to trusted parties in accordance with the user preferences.

The privacy objectives discussed in this thesis are:

- **Maintaining *information confidentiality,*** i.e. to prevent any disclosure or manipulation of the message content to any other party
- **Maintaining *information privacy***, i.e. to prevent any disclosure of personal data or information directly related to the individual to a medical service or application without the user's prior approval or knowledge.
- **Maintaining *context privacy***, i.e. to prevent any disclosure of identifiable information related to the context in which the user is using the medical service and from which indirect information for the user could be extracted.

Briefly speaking, in relation with the discussed application spaces, the privacy of a person can be ensured by:

- For location - changing pseudonyms with different time duration and blurred location information (When the exact location is known, there are different methods how the information could be blurred before sending. Location accuracy parameter provides indications for the range of blurring.)
- For the ID – use of a pseudonym instead of the ID of the node
- For personal information – controlled revealing of only the minimum set of user sensitive data with which the current application can work (with the help of rules and profiles) and controlled data access to the personal information of the end-user once it is accumulated and stored somewhere else.

The following Table 22 gives overview of possible approaches for ensuring privacy.

Privacy Aspects And Approaches	
controlled information disclosure	• policy – based • role – based
controlled data access	• hierarchical team-based access control • secure multi-party access control
node anonymity	• pseudonym creation schemes • group formation to increase the silence periods • capability-based privacy-preserving scheme
location anonymity	• data cloaking • mix-zones • mix-contexts

Table 22: Possible approaches for ensuring privacy

As access control and controlled information disclosure are some of the major points of gravity for this PhD thesis, in the next paragraphs they will be briefly introduced.

Access control is the ability to permit or deny the use of a particular resource by a particular entity.
In computer security, access control includes authentication, authorisation and audit. It also includes measures such as physical devices, including biometric scans, digital signatures, encryption, passwords, secret keys.
Access control models usually fall into one of two classes: those based on capabilities and those based on access control lists (ACLs). In a capability-based model, holding an unforgeable reference or *capability* to an object provides access to the object; access is conveyed to another party by transmitting such a capability over a secure channel. In an ACL-based model, a subject's access to an object depends on whether its identity is on a list associated with the object.
Both capability-based and ACL-based models have mechanisms to allow access rights to be granted to all members of a *group* of subjects.

Access control systems provide the essential services of *identification and authentication* (*I&A*), *authorisation*, and *accountability* where:

- identification and authentication determine who can log on to a system
- authorisation determines what a subject can do;
- accountability identifies what a subject (or all subjects associated with a user) did.

Information disclosure means the giving out of information, either voluntarily or to be in compliance with legal regulations or workplace rules. Controlled information disclosure is when subjects have suitable tools/mechanisms which give them abilities to control the release of private information they consider sensitive. There are several ways to achieve this. Both ways have some advantages and disadvantages and could be used in different scenarios and depending on the security and privacy requirements for the system.

One way to achieve this is by pre-defining rules for: Which groups of subjects can have access to information; what pieces of information could be accessed by the group; what types of permissions are granted to the group or a single subject (read or write the content). In this way the access rights are given in advance and the end-user is not involved in the time of accessing the information.

Other way for controlled information disclosure is when the end-user is directly involved in granting the requestor the permission to access the content every time a request for information comes. Technically this could be implemented by schemes for secure multi-party access control or hierarchical team-based access control. In this second option the end-user is really in control of who accesses what piece of data. The disadvantage is that the end-user is disturbed. This option could be used for very sensitive information.

Access control techniques are sometimes categorised as either discretionary or non-discretionary. The three most widely recognised models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC and RBAC are both non-discretionary.

4.4. Key features of the proposed adaptive security and privacy framework

4.4.1. Context-awareness

In this discussion, the focus is on the privacy mechanisms and the integrated context-awareness and personalisation. Since context and context-awareness play very important role in this proposal, here the important points regarding context are revisited in the following paragraph.

Exploiting Context
Entity of context could be person, place, physical or computational object that is considered relevant for the interaction. In this proposal, it is distinguished between *identifying information* and *personal data,* both of them considered as contexts.

- *Context information* could be considered any information about the users, their activities, their health status, also coming from their BSN, their other devices, the surrounding environment. Table 4 provides more details on contexts in the view of the reference scenario.
- *Context attributes* describe a snapshot of the current context from the status of all relevant interacting entities.
- *Context assessment entity* - collects all low level context attributes (such as GPS coordinates, time, physical parameters, health parameters, service type, number of neighbouring nodes, etc) and defines higher level context attributes (for example location, domain, user role, presence, etc) which then are fed to the user's system to take intelligent decisions based on predefined rules. More details on the context attributes are provided in Section 5.3.2.
- *Context-awareness* in this discussion is the ability of the privacy protection mechanisms to react on change in the context in such a way that it provides the best privacy protection for the users and their sensitive information while minimising the user distractions.
- *Context-aware privacy* is the application of the privacy protecting mechanisms which adjusts to the context of all entities and make decisions accordingly.

For the sake of this discussion, context information is divided into context attributes linked with the users' side and their devices, called *internal context attributes (ICA)*, and context attributes provided by external entities, for example location service and application, called *external context attributes (ECA)*. ICA contain attributes for the user's device - CPU usage, battery power, free memory (which according to [7] should also be a subject to access control), communications media and also context directly connected with the users themselves like a current health status provided by BSN. ECA are all attributes provided from external parties - the location, the service, the application, etc...
For the ECA, the user's system should receive *trusted* information for location and context from the external services. The question for the trustworthiness of the location and context information is another very important and challenging issue which is out of the scope of this thesis. Threats coming from context were described in Section 3.3.2. Trusted location and context information should be used by the users' devices to assist users in their interaction and making intelligent decisions, preferably acting on user's behalf based on predefined scenario settings and preferences. Based on information provided by the surrounding WSNs from the environments, the user has to be informed with the help of their devices that they are in the area of a certain service of interest to the users. For example location-based service could be at the reception in the entrance of a hospital – the pervasive system automatically registered the user to the receptions and notifies the doctor with whom he/she has appointment. Going further, in more sophisticated systems, trusted location and context information should be used to predict users' needs and offer them appropriate available services based on patterns of their behaviour.

4.4.2. Policy-and Profile-based Management

For ensuring minimum intervention of the end-user and systems flexibility for the diverse nodes in HHA, the context attributes are analysed with the help of predefined policies. Subject of the policies and rules are low-level context attributes and these rules are defined as *low-level rules*. The rules concerning high-level contexts are defined as *high-level rules*. Context-reasoning supports definition of high-level rules using high-level context information from the current context and low-level rules (for example coordinates into a meaningful for the end-user and for the system location). In this way, the context-aware system is "aware" of the current system state. This further is stored as current status of the system, the user and the environment. The system automatically defines *Scenario* based on primer context parameters: the current location and role of the end-user (as a source of USD – User Sensitive Data) and the role and location of the requesting party (the node with which trust relationship must be established). The decisions are taken as dependent on *current scenario.* A more complex Rule Agent implemented on a FFN may consider perhaps up to a hundred of rules applicable to a current scenario.

4.4.3. Default settings

In their everyday life, the users have different roles and usually have certain places where these roles are applicable. For example, they are employee at the office, family member at home, trainee at the fitness center, patient at the hospital. In this proposal certain scenarios are defined based on most frequent everyday situations. One of the functionality of the privacy protection framework is to protect user's privacy based on these roles, without the need of user's intervention all the time. This could be obtained by introducing default settings in the system. Appropriate templates could help the user to set up these default settings. Assigning privacy flags (PF) for filtering all pieces of the sensitive information helps the autonomous behaviour of the users and their devices. PFs indicate how the user wants this data to be handled and revealed by the privacy protection mechanism. The PFs presented in Section 5.2.2 are also the tool to give the control in the hands of the user. The default disclosure of the user's sensitive information is "never disclose" (pessimistic approach).
In this proposal, the sensitive user data is grouped by domains and could have different level of granularity and a hierarchical structure. The highest level is defined as "data abstractions". In some cases, request comes only for the highest level of granularity. Therefore, there are templates also for the data abstractions based on different domains and for the low-level of granularity of the user sensitive information. For example the template for data abstraction "Address" is a container for the parts of the address (Figure 20). The user only needs to change, if necessary, the default value of the PF for each of these data and data abstractions.
Templates for scenarios are also provided
The user is able to change and update all the information in the user profiles and to create new roles. The scenarios can be changed too and new scenarios created.

4.4.4. Scalability and Flexibility of the framework

Definitions for flexibility and scalability were presented in Section 4.1.
To provide them, both the framework as a whole but also its main components must support these features. Specifically for the privacy framework, the privacy protection mechanisms must be scalable – that means that the respective modules of the framework must be also scalable (i.e. having extended, scaled-down and lightest versions) and must "fit" in all types of nodes and the system must handle them without e.g. the processing burden exceeds the resources.
In the following paragraph scalability and flexibility are further defined for the three aspects of privacy on which the focus of the proposal is:

<u>For the information and context privacy</u>
Scalability of the context-aware privacy protection is defined as a set of maximum number of context attributes and rules which can be processed by a node belonging to a certain resource class:

- *Maximum number of different context attributes* directly related to the health status of the user and the surrounding environment which are included in the conditions for the policy-based privacy protections

- *Maximum number of different Low and High level rules,* necessary for building up the reasoning to support the privacy protection of the users' medical data and their lifestyle and any other necessary information, defined as sensitive by the users themselves

Different number of rules are applied for diverse nodes (gateway, coordinator, end node) based on their capabilities. Scalability is also ensured from the possibility to select this version of the privacy protection framework which best corresponds to the role of the node in the network and its capabilities as explained in Section 4.6.1.

Flexibility is defined in terms of:
- The rules, policies and profiles support the work of both health professionals and health care subjects
- Provision of personalized control for different levels of privacy protection

For the information confidentiality
Flexibility is defined in terms of:
- Different values of the parameters of the algorithms providing confidentiality

These will be explained in details in Section 5.1.

Overall, the security and privacy protection framework ensures that the properties of flexibility, scalability, adaptivity and context-awareness are satisfied both in the overall framework and in each component.

4.5. Privacy Protection Framework as part of The Adaptive Security Framework

Privacy protection mechanisms for Hybrid Hierarchical WSNs have been discussed in [8]. Preventing unauthorised access is coupled with privacy policies that define who may receive and use what type of data and for what purposes. The provided personal sensitive information must comply with general privacy policies based on legislation on one hand and rules set-up by the individual on other hand. The end-users themselves can have the option to define which of the context information about them they feel to be sensitive. Hence, controlled information and information filtering before disclosure, is necessary.
The protocol stack for level 2 (environment) HHA nodes could be divided into four logical subsystems - connectivity, middleware, management, and application, designed to facilitate cross-layer optimisation. Each subsystem comprises various protocol entities, which offer services at various access points to other subsystems, and can be combined in a number of ways to configure the protocol stack according to the sensor node's role and application requirements. the Application Subsystem, hosting one or several sensor applications, the Middleware Subsystem, providing data transfer services for the transport of the application data packets, the Connectivity Subsystem, consisting of functions required for operating the physical layer, the medium access control, and the network and transport layer, and the Management Subsystem, responsible for the configuration and initialisation of the stack. The proposed security framework is implemented by a cross layer Security Manager, positioned in the Management Subsystem of the flexible protocol stack [10], depicted in Figure 11. The Security Manager is cross-layer and context-aware, given that context information is made available from other network entities from the context layer, such as for example location entity, and from the application subsystem. Its main components are Profile and Rules Agent; Security, Privacy Agent, Trust Agents, Entity with Privacy and Trust Mechanism and a Small Data Store. To satisfy the flexibility property, as mentioned in Section 4.4.4, a toolbox approach is taken for the Security Manager, which is designed to be configurable regarding the modules that it contains. For privacy protection, Profile and Rules Agent, Privacy Agent, Privacy Safeguard mechanisms and the Small Data Store interact as shown on Figure 12. The flexible security protocol for ensuring confidentiality is situated in the Connectivity subsystem.
Since part of the context information could be considered sensitive for the users, they have the option to indicate with the help of the Privacy Flags (PF) how this data will be treated. It must be noted however, that the users must be also informed in advance which types of personal data and node identifiers can be used for identification as well, depending on the available context information. The users must be aware for the need of a trade off because

the smart systems and the context-aware applications, in order to function properly, need some sensitive information which must be revealed by the users following the minimisation approach.

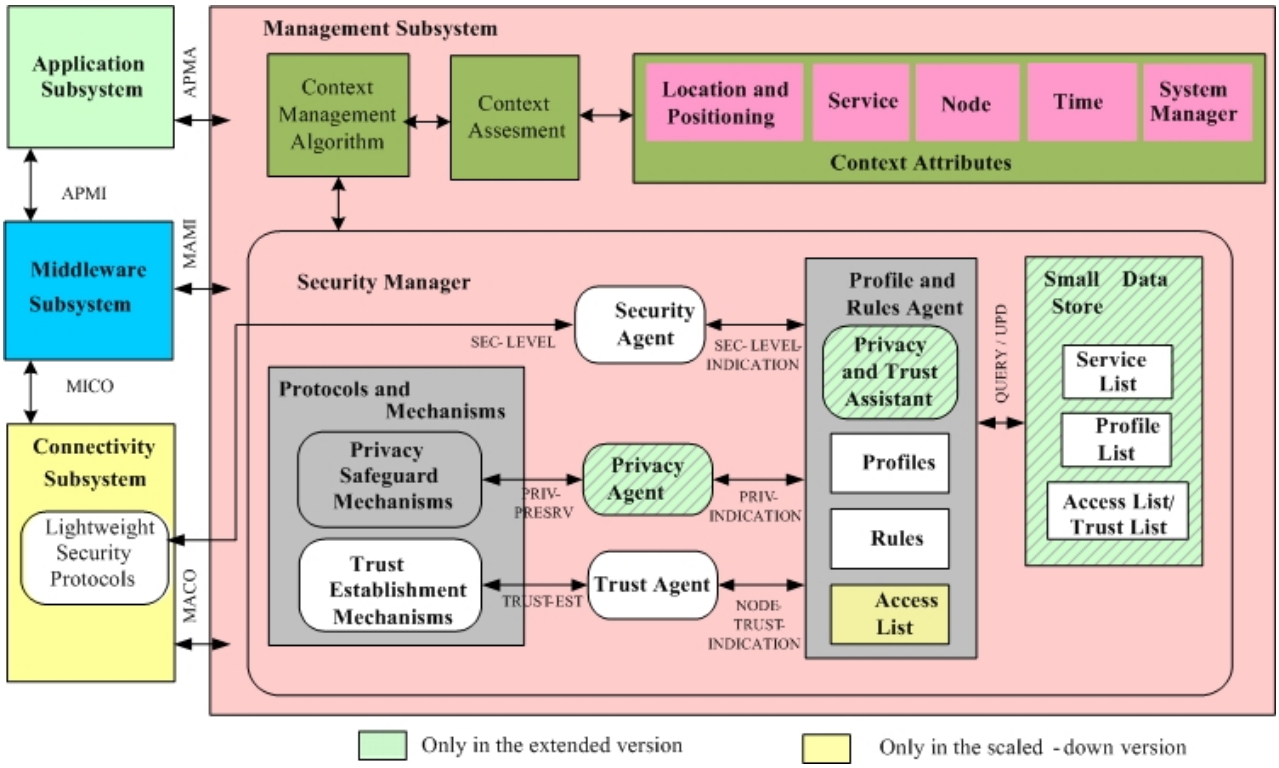


Figure 11: Generic Adaptive Security Framework within the FLEXIBLE PROTOCOL stack– Scaled-down and Extended Versions

4.6. Building blocks of the Security Manager

The *Protocols and Mechanisms* component is the most fundamental, since it is the one required for all types of nodes in the network. It contains the security primitives necessary to implement several security protocols in a way that is transparent to the layers above it in the protocol stack. The adaptivity of the security mechanisms is ensured by the *Security Agent*, responsible for determining the most suitable security mechanisms and protocols for every message exchange. Decisions on the cooperation of nodes are based on their trust status, provided by the *Trust Agent*, while the *Trust Establishment Mechanisms* block is responsible for determining the trust status for unknown nodes. The *Context Monitoring Algorithm* and the *Context* Assessment Entity have the goal to monitor very important context parameters from the network, from its own systems itself in order to detect if the system is in danger. In case of a security risk, the Security Manager takes appropriate actions as defined in the table with countermeasures. The *Privacy Agent* is responsible for determining if and in what form data should be disclosed, and for invoking the *Privacy Safeguard Mechanisms,* which interfere with the data by filtering it before any disclosure, by allowing or forbidding it, or by pseudonymising it. The *Privacy and Trust Assistant* is an application support component, existing only in user-related full-function nodes (for example a smart phone or PDA) and provides the interface between the user and the device for the configuration of data privacy policies and trust relationships.

The *Profiles and Rules Agent* interfaces with the Security, Privacy and Trust Agents for the exchange of security, privacy and trust definitions respectively. The Profiles and Rules Agent sends requests to the *Small Data Store* to get or modify (if required) the Security Level, Trust Level, and profile information that are stored in the respective lists entities. The context information that can lead to reconfigurations comes from S*ervice and Node Discovery*, *Location and Positioning* and the *Applications*.

Within the protocol stack implemented in any end-sensor node, cluster head or gateway, the Security Manager interfaces with various layers. The Security Agent interfaces with the connectivity layers for the configuration of the Protocols and Mechanisms component. The Trust Agent interfaces with the connectivity layers for the exchange of security protocol messages with peer nodes, and for the establishment of trust relationships. The Security Manager also offers its services to other layers of the protocol stack. Security requirements can come from the application layer. Privacy policies and trust relationships could be obtained directly from the user with the help of the Privacy and Trust Assistant.

The extended version of the security framework applies to the coordinator and gateway nodes as well as to simple nodes without very harsh memory, battery and computational constraints (Figure 11). The scaled-down version residing in a sensor node from the BSN, because of the very limited power, memory and computational capabilities, only performs a specific security mechanism as requested by the Security Manager in the handheld device. In addition to the components that might be omitted, others allow for lighter versions to be deployed, in order to provide only a subset of the services defined. Nodes might be equipped with a subset of the mechanisms defined, depending on their computational capabilities, their role in the network and their communication needs. In Figure 11, the two versions presented (scaled-down and full) are not strict regarding their components, since some components are customisable. Since the components are themselves customisable, this essentially enables many more than two versions to be deployed (i.e. additional intermediate versions). More details for these versions of the framework are presented in the next Section.

In the following paragraph, the main communication flow among the building blocks is briefly described and depicted on Figure 12.
The SERV-QUERY(parameters) is a request, sent by the Profiles and Rules Agent to the Service List, regarding service. The Profiles and Rules Agent can request, with this same primitive but using different parameters, either just getting the Security Level or changing the Security Level associated to the service. SERV-UPD is the response to the SERV-QUERY. It can carry either the Security Level information or just the notification that the Security Level has been changed.
The TRUST-QUERY(parameters) primitive is a request, sent by the Profiles and Rules Agent to the Access List/Trust List. Similar to the SERV-QUERY (parameters), the Profiles and Rules Agent can request either getting the Trust Level or changing the Trust Level associated to the node ID. TRUST-UPD is the response to the TRUST-QUERY. It can carry either the Trust Level information or the notification that the Trust Level has been changed in the Access List/ Trust List.
The PROF-QUERY(parameters) is issued towards the Profile List. The Profile List provides the profile for the corresponding node/user through the PROF-UPD primitive.
The primitive SEC-LEVEL-INDICATION sends to the Security Agent all the information that the Profiles and Rules Agent gets from the List and the Rule Module and is relevant to determine the Security Level.
The primitive SEC-LEVEL sends the Security Level for the corresponding node/user to the Security Protocol entity.
The primitive PRIV-INDICATION allows the exchange of privacy information between the Privacy Agent and the Profiles and Rules Agent.
The primitive PRIV-PRESRV sends the privacy (and pseudonym) information to the Privacy Protection Mechanism entity.
NODE-TRUST-INDICATION primitive allows the exchange of trust information between the Trust Agent and Profiles and Rules Agent.
The primitive TRUST-EST sends the trust information to the Trust Establishment Mechanisms.

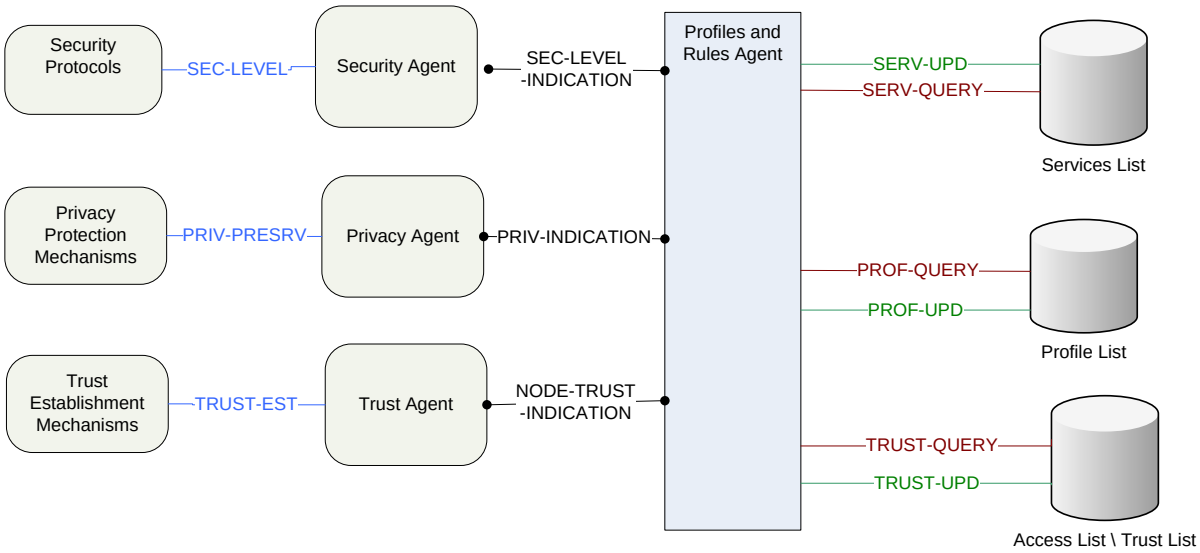


Figure 12: Main communication flow – interaction among the building blocks

Further in this report all the building blocks of this Security and Privacy Framework will be discussed in more or less details, except the Trust Agent and Trust Establishment Mechanisms, which are out of the scope of this work.

4.6.1. Ensuring Adaptability and Flexibility in the Security Management Framework

Adaptability is supported by the proposed security framework in several ways.

- Firstly, with the help of the **Security Agent**, Security Levels are assigned for each communication (Table 23), which determines the security mechanisms that are applied, according to its security needs. For example, in the use case for continuous home care, where a BSN is attached to the patient's body and communicates data via a handheld device which acts as a gateway, the *Low* Security Level could be assigned when the patients are at home and the *High* level when they are in public places.
- Secondly, adaptability is supported by the representation and establishment of various trust relationships between communicating parties by the **Trust Agent**.
- Finally, the **Privacy Agent** is responsible for determining if data should be disclosed, and if it should be provided anonymously according to the data sensitivity and according to the scenario and application requirements. Privacy level flags indicate how the user wants the data in question to be handled and revealed by the Privacy Agent.

The definition of Security, Tryst and Privacy levels are presented in Table 23 **Fejl! Henvisningskilde ikke fundet.**.

Parameters	How Adaptability and Flexibility is Ensured
Security Levels	*Low* – provides non-privileged services and allows exchange of non-sensitive data
	Medium – provides limited protection, even if the data exchanged within the WSN is not necessarily sensitive
	High – provides privileged access to service and/or exchange of highly sensitive data.
Trust Status	*Unknown* – devices that enter the network and request access to some service for the first time
	Untrusted – devices that are not allowed to access the network for any reason even if they have previously been granted access

	Trusted – devices that have previously established a trust relationship and already share a trust key with the WSN
Privacy Level Flags	*"Always give"* – give data without asking the user for confirmation
	"Check with the Profile Agent" – check device profile for exception list and priority rules from Rules Agent before giving the data
	"Ask the user" – ask the user before handling sensitive data
	"Never give" – never disclose the sensitive data

Table 23: Ensuring Adaptability and Flexibility

As described in the Section 4.6.1, *flexibility* is ensured by enabling the role, capabilities and security needs of each node in the network to define the subset of Security Manager components which reside in the node. Below is explained what is meant by different versions of the Security Manager.

Extended version of the proposed framework: The main components described below refer to fully functional node (FFN) and a gateway node. Security Manager consists in this case of the Profiles and Rules Agent, the Security Agent, the Privacy Agent, the Trust Agent, the Protocols and Mechanisms, the table with the countermeasures and the small Data Store, which are positioned in different logical parts of the flexible architecture.

Scaled-down version: The Security Manager as depicted in Figure 11 contains the **superset** of the building blocks that a node may be equipped with. It is assumed that the Security Manager will operate as described in nodes that have enough computational capabilities, are cluster heads or gateways and can be subjects to regular maintenance. According to the role (node/cluster head/gateway, strictly defined long-term role/highly mobile) and constraints of each node in the network, it may be equipped with a **scaled-down version** of the Security Manager. If the reference scenario is taken as an example, the extended version of the security framework resides in the handheld user device, while the end sensor nodes from the BSN have the scaled-down version. The Security Manager residing in the handheld is responsible for defining the level of security and trust services for the communications with the BSN on one side and with external networks on the other side. It also gives the end-user possibility to set up rules for disclosing sensitive information to other networks and different requesting parties and for anonymisation of data. The scaled-down version residing in a sensor node from the BSN, because of the very limited power, memory and computational capabilities, only performs a specific security mechanism as requested by the security mechanism in the handheld device.

Lighter version: Except from the components that might be omitted, the other ones allow for lighter versions to be deployed, in order to provide only a subset of the services defined. The Security Protocols and Mechanisms component may support only a subset of the security levels. For highly constrained nodes with strictly defined role, one security level may suffice for its communications with the cluster head. Moreover, the Trust Establishment Mechanisms are required for nodes that, during the network lifecycle and without reconfiguration, will need to communicate with nodes different from those they were initially configured to trust. Nodes might be equipped with a subset of the mechanisms defined, depending on their computational capabilities, their role in the network and their communication needs.

The components that might be omitted or might provide only a subset of the services described are:

- The Security Protocols may support only a subset of the security levels. For highly constrained nodes with strictly defined role, one security level may suffice for its communications with the cluster head.
- A more simple information flow will be defined for within the Security Agent for nodes that are configured to support only one security level.
- The Privacy Protection Mechanisms are required only for nodes that act as communication points with service providers and gather personal or corporate sensitive information.
- The Privacy Agent may be omitted for nodes which according to their role do not require privacy protection or anonymity

- The Trust Establishment Mechanisms are required for nodes that, during the network lifecycle and without reconfiguration, will need to communicate with nodes other than those they were initially configured to trust. Nodes might also be equipped with a subset of the mechanisms defined.
- The Trust Data Store may include only an access list together with an indication on the other nodes supported security levels. The more sophisticated version of the trust database is required for nodes that have highly diverse communication needs.
- The Graphical User Interface (GUI) is optional. It will only exist in devices that can support it, are related to a human user and may require reconfigurations.

4.7. The importance of context-awareness

Having in mind the different reference scenarios and the application of BSN in them, the security and privacy framework presented above is valid for any kind of environment. However some modifications might be done in order to optimise the system.
If the patient is in a public place, it is not surprising that in this scenario the system will face major interference problems; therefore authentication and encryption are two vital requirements, as described in Section 3.2.
On the other hand, if the patient is at home or in the office, there is no need for such robust mechanisms, the energy consumption of the sensors could be reduced by choosing lighter encryption techniques and protocols.
In order to introduce this automatic adaptability, two important types of context are required: the recognizing of location and the detection/recognizing of current profile. They are important because it is needed tools to obtain data from the surrounding environment to determine if the users (and respectively the BSN) are in a trusted or non trusted environment and if they are alone or not. Then, based on this context information, Security Manager is able to choose the best security and privacy level for the network.
However, location and current profile is not the only context information used by the system. Other types of contexts are necessary. They are presented in the following paragraphs.

The context model in this report represents three classes of real world objects (person, location, node) and 2 classes of conceptual objects that characterise pervasive healthcare contextual environment (*scenario* – current user role, requesting party identity and their locations; *event* – for the health status of a person - normal, pre-emergency, emergency).
Low-level context attributes (LLCA) is basic contextual information which is directly measured by sensors, as in [5] – raw context data obtained from various sources, in heterogeneous formats (in this discussion readings from the body sensors, coordinates, physical parameters of the environment). From them, information for the user's state and the surroundings can be deduced (for example meaningful location, user role), forming *high-level context attributes (HLCA)*.
The *Context assessment entity* collects all low-level context attributes and defines high-level context attributes and this allows the ACAPP framework to take intelligent decisions based on predefined rules.
The Context assessment entity notifies the Profile and Rules Agent to update all relevant context attributes in the context profile when they are changed. ICA is updated within the user's device and ECA are updated each time when they are provided from external entities. Some relevant examples of association of LLCA with HLCA mentioned in Section 3.1 are provided in Table 24.

	Low Level Context Attributes	**Higher Level Context Attributes**
Person (the end-user)	Exact location, physical parameters measured from BSN	User role, location of source, mood, Scenario, direction, speed
Selected Service	Domain, time period for communication, Exact Location, time stamp, Requesting party identity, service provider	destination role, location of destination, Scenario, trustworthiness
Environment	Exact location, number of neighbouring nodes, communication medium, distance from other nodes	Presence, anonymity level, transmitting power

User's device	time stamp, battery level, CPU usage, memory usage, IP address, bandwidth	Device mode (sleep/wake), transmitting power
Node	battery level, processor usage, memory usage	Device mode (sleep/wake), transmitting power
Scenario	Source ID, Source location, destination ID, destination location	User Role at certain location
Location	Physical coordinates	Meaningful location for the user – home, office, hospital, gym
Measurements from end-sensor nodes	Oxygen, heart rate, glucose	Events for health status – normal, pre-emergency, emergency

Table 24: Context Attributes

4.8. Applying Security Management and Context Monitoring

One of the contributions presented in this PhD thesis is the adaptability feature of the security and privacy framework, including the need to have a mechanism to change levels of some of the security and privacy parameters according to the location of WSN and to the interaction with the surrounding environment. Having this in mind, the Security Manager comes into play as a cross-layer entity in the flexible protocol stack (Section 4.6). The Security Manager with different versions of it, suitable for variety of types of nodes (end-sensor, aggregator, coordinator node). In order to function properly, The Security Manager needs to "monitor" the change in the context as explained previously in Section 4.6.1. This is done with a dedicated algorithm, called Context Monitoring Algorithm (CMA) which is another contirbution of this thesis. In the following paragraphs the responsabilities of CMA are described.

The Security Manager tackles all security and privacy issues regarding the WSNs behaviour. One of its tasks is to analyse the network's activities w.r.t. security and this is performded with CMA. CMA is responsible to track and analyse the network's status, anomalies and context information. According to the data provided by this algorithm, the Security Manager is able to determine a corresponding reaction to maintain the network's integrity and functionalities by changing if necessary the security level.

The following Figure 13 shows the reactions of the Security Manager, if security attacks took place:

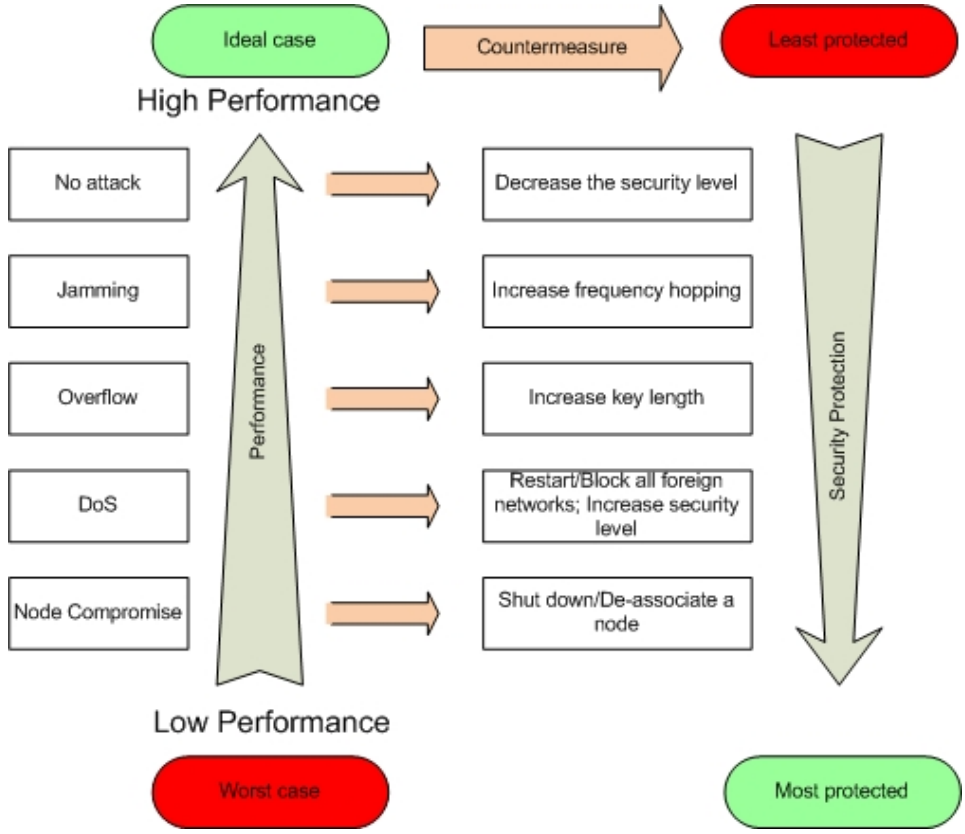


Figure 13: Trade off among security protection and performance (Detection – Reaction in the BSN)

In technical terms, one of the tasks of CMA is to broadcast requests and analyses traffic. The broadcast requests are mainly used to request the sensor nodes' batteries status. The traffic analyses is vital to determine if the nodes are working properly and if the system is under attack. In order to achieve these goals an initial estimation of the number of messages that the aggregator should receive in a period of time, should be done. However, to perform this task correctly, the Security Manager needs to know from the beginning how many sensors the network has and what their characteristics (freshness and update) are. The information is provided to the Security Manager by the CMA.
Another important task of CMA is to track the baterry status of the end-sensor nodes in the whole BSN and according to the remaining battery level, to take approprite actions.

In the following paragraphs some of the most important procedures performed by the Security Manager are explained:

Procedure against security attack:
In the BSN, the detection of possible attack is managed by the CMA, running by the Security Manager. To detect an attack, the CMA needs to know the typical attacks and how they affect the network. When an attack is identified, the Security Manager looks into the table of countermeasures. In case of a determined attack it may order the network, via the coordinator node, to accomplish a specific technique to increase the level of security (like example strong authentication or encryption). Actually, it is the coordinator node that puts in action the orders of the Security Manager towards the end-sensor nodes. The sensor nodes change then their security level. More details for these procedures are provided in Section 5.5.

Procedure against low battery:
The tracking of the battery level is done by the Context Monitoring Algorithm via the Security Manager in the BSN. If the battery power drops to a certain level, via the GUI (The Privacy and Trust Assistant) the user is directly informed for the level and which procedure is launched. For example, the Security Manager can determine if the data is saved on a mobile device and if this back-up device continues to manage the network.

The countermeasures initiated by the Security Manager in reply to different threats and risks, are presented in the following Table 25:

	Readings	SECURITY MANAGER		
		Warnings	Actions	Level of security
Context Monitoring Algorithm	Batteries status	Three warnings: below 40% below 20% below 10% (critical warning)	Display the warning in the mobile device	Below 20% the level of security may be decreased to save energy
	Compare the number of estimated messages received during a determined period of time (1 minute)	below the expected – report sensor malfunction	Find which sensor is not working properly, display it on the mobile device and send the information to the user's hospital database	No changes
		above expected – intrusion detected	The keys are compromised! Revoke the keys. Ask for ID and Pre-distributed key, change new keys	Increase the level of security (if possible)
	Scan for specific attack	CRC errors - possible jamming or interference	Increase frequency hopping or change channel on the affected node(s)	No changes
	Scan for specific attack	Aggregator being overflowed with data - DoS	Revoke all keys, reboot system (takes at least 8 sec. times the number of sensor nodes)	Increase the level of security (if possible)
		Node sending more data than expected – Node compromised	Revoke its key, report to the user (display) and hospital database	Increase the level of security (if possible)
		Eavesdrop	Impossible to detect because there is no change in the network's behaviour	No changes

Table 25: Security Manager and Context Monitoring Algorithm

The following Figure 14 depicts the functionality of CMA [9].

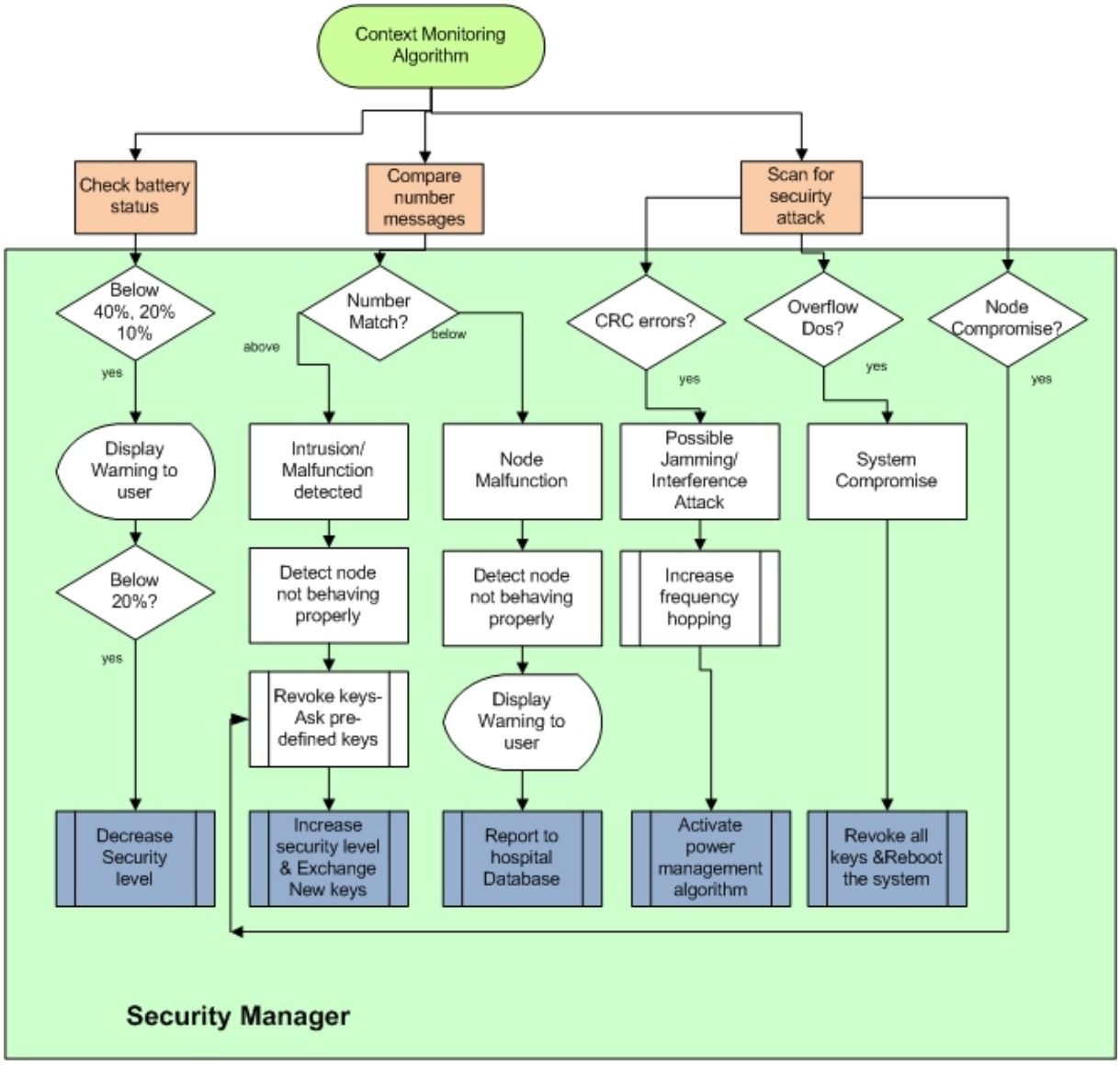


Figure 14: The functionality of the Context Monitoring Algorithm

4.9. Summary of Chapter 4

This Chapter 4 presented the motivation for proposing the context-aware privacy protection mechanisms integrated within security management framework. Its distinctive features are flexibility and scalability, context-awareness and adaptability. The major part of its components is placed in the management subsystem and some other parts in the connectivity and the application subsystem.

The system requirements are for power efficiency, adaptability, flexibility and scalability, profile-based, policy-based, need to support mobility, need for GUI and predefined settings and policies.

The privacy objectives which are to be preserved by the proposal in this PhD report are maintaining information confidentiality, information privacy and context privacy.

The main components of the security framework are the block for protocols and mechanisms, the security, privacy and Trust, Profiles and Rules Agent and the small data store. Context information is provided to the Security Manager by other entities of the management subsystem forming the context assessment entity. Important role for enhancing the functionality of the systems is the context-awareness. The component responsible for it is the context monitoring algorithm which monitors the battery status and scans for specific attacks. In case some anomalies are detected, it takes appropriate actions based on a table with countermeasures.

Interaction among the main building blocks and the main communication flow is further presented.
To ensure adaptability and flexibility, different security levels, trust status and privacy level flags were introduced. Extended, scaled-down and lighter versions of the overall security framework were defined for different classes and roles of sensor nodes.

References

[1] Young Kyun Kim, Ramjee Prasad, "4G Roadmap and Emerging Communication Technologies", Artech House Publishers, ISBN 1-58053-931-9, 2006

[2] K. Knightson, N. Morita, T. Towle; NGN architecture: generic principles, functional architecture, and implementation; IEEE Communications Magazine, Issue 10, October 2005, pp. 49- 56

[3] Gluhak, M. Presser, Z. Shelby, P. Scotton, W. Schott and P. Chevillat, "e-SENSE Reference Model for Sensor Networks in B3G Mobile Communication Systems", 15th IST Mobile and Wireless Communications Summit 2006, Myconos, Greece, 4-8 June 2006

[4] A. Mitseva, E. Aivaloglou, M. A. Marchitti1, Neeli R. Prasad, C. Skianis, S. Gritzalis, A. Waller, Timothy Baugé, Sarah Pennington, **"(Towards) Adaptive Security for Convergent Wireless Sensor Networks",** WIRELESS COMMUNICATIONS AND MOBILE COMPUTING:, SI on Quality of Service and Security in Wireless and Mobile Networks, 29 Sept 2008

[5] Robert Steele, Chris Secombe, Wayne Brookes. Using Wireless Sensor Networks for Aged Care: The Patient's Perspective, In Proceedings of *Pervasive Health Conference, Nov-Dec. 2006*

[6] Sven Lachmund, Frank Fransen, Eddy Olk, "Context-Awareness, Security and Trust", *In proceedings of WPMC 2005, September 2005, Aalborg, Denmark*

[7] Vagner Sacramento, Markus Endler, Fernando Ney Nascimento. A Privacy Service for Context-aware Mobile Computing. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pp. 182-193.

[8] Anelia Mitseva, Matthias Gerlach, Christian Räck, Neeli R. Prasad, **"Context-aware Adaptive Privacy Protection for Wireless Sensor Networks**", in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1032-1036, San Diego, USA, Sept 2006

[9] Ricardo José S. Rodrigues, Mathieu David, Dimitri Loire, Anelia Mitseva, Neeli R. Prasad, **"Adaptive Security Management for Body Sensor Networks in Medical Scenario"**, in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1037-1041, San Diego, USA, Sept 2006

[10] A. Mitseva, E. Aivaloglou, M. A. Marchitti1, Neeli R. Prasad, C. Skianis, S. Gritzalis, A. Waller, Timothy Baugé, Sarah Pennington, **"(Towards) Adaptive Security for Convergent Wireless Sensor Networks",** WIRELESS COMMUNICATIONS AND MOBILE COMPUTING:, SI on Quality of Service and Security in Wireless and Mobile Networks, 29 Sept 2008

[11] Anelia Mitseva, Satya A. Wardana, Neeli R. Prasad, **"Context-Aware Privacy Protection for Wireless Sensor Networks in Hybrid Hierarchical Architecture"** – IEEE IWCMC 2008, Wireless Sensor Networks Symposium, Creta Island, Greece, August 2008, 978-1-4244-2202-9/08/$25.00 © 2008 IEEE

Chapter 5 - Proposed Privacy Protection Mechanisms and their applicability

In this chapter another main contribution of this thesis is presented in details – namely, the proposed privacy protection mechanisms. First, a shot review of existing mechanisms is made and their suitability for WSNs discussed. Then, the proposed security protocol suit for adaptive confidentiality is described. Second, the context-aware mechanism for controlled information disclosure is presented. Since the access control is based on profiles and rules, other important blocks of the framework are then described in details – the Profile and Rules Agent, with the defined profiles of user, context, application, scenario. It is also discussed how scalability and power-efficiency is ensured. In the end, the applicability of the proposed mechanisms to the reference scenario for outdoor, home and hospital locations was exemplified and the mechanisms were compared with some existing solutions.

5. Proposed Privacy Protection Mechanisms and their applicability

To remind, the ACAPP Framework aims to ensure *information confidentiality, information privacy and context privacy*, as presented in Section 3.2.1. All these aspects of privacy protection are guaranteed using different mechanisms. Which is the most appropriate mechanism to be applied? – It depends on the Privacy Agent. These mechanisms will be described further in Sections 5.1 and 5.2.
In the Mitigation Plan presented as the final stage from the threat analysis, countermeasures for the most dangerous security attacks were presented (Table 21). However, here in the beginning of this section definitions of some of the security primitives which will be later discussed are briefly presented:

Authentication:
The broadcast nature of the transmission medium makes information more vulnerable than in wired applications. Thus, security mechanisms such as encryption and authentication are essential to protect information transfers.
Authentication and Access Control process have 2 different sides: initial entity authentication (creating security associations) and authentication for sessions (which is based on keys, established during initial authentication).
Access control procedures heavily depend on an initial entity authentication phase in which a node entering the network has to set up some keying material with its neighbours that will be used to enforce cryptography and a data authentication at link layer. These keys can be obtained in different ways based on the entity authentication phase. Initial authentication between a sensor and a network often requires that the administrator participates and introduces sensors to each others. For instance, administrators may utilise a centralised server (by typing a sensor specific password to the server) or authenticate sensors in distributed manner (the administrator may keep sensors close each other in order to change keys using short range radio e.g. Near Field Technology). Different initial authentication schemes are more trustworthy than others.

Encryption:
This is the procedure that guarantees secrecy of the data exchanged. Any encryption algorithm depends on some key, and keys are normally generated during authentication phase, so the two phases are strictly connected.
Few encryption algorithms are suitable for sensor networks with harsh resource constraints. According to the comparison performed in [1], TEA is the most perfect encryption algorithm to minimize memory footprint and maximize speed;
SEAL is a very fast stream cipher optimized for machines with a 32-bit word size and plenty of RAM. Although encryption process is relative faster than RC5, the key setup process of SEAL requires several kilobytes of RAM space and rather intensive computation.
RC4 is widely used in many applications, under certain circumstances it has been proven to be insecure [2], but whenever correctly deployed it is used in robust protocols such as TLS or TKIP (into IEEE 802.11i).

Integrity:

In information security, integrity means that data cannot be modified without authorisation.
Integrity, together with confidentiality and availability is one of the core principles of information security, also known as CIA Triad.

Availability
For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Data integrity is a term used in computer science and telecommunications that can mean ensuring data is "whole" or complete, the condition in which data are identically maintained during any operation (such as transfer, storage or retrieval), the preservation of data for their intended use. Generally speaking, data integrity is the assurance that data is consistent and correct.
Often such integrity is ensured by use of a number referred to as a Message Integrity Code (MIC) or Message Authentication Code (MAC).
In plain words, integrity can be compromised through:

- Malicious altering, such as an attacker altering content
- Accidental altering, such as a transmission error, or a hard disk crash

An attacker can perform a wide variety of attacks aimed to alter data exchanged over insecure networks. These have been discussed in Section 3.3. Again, countermeasures are based on the use of some form of secure integrity code based on shared keys generated during network access.

5.1. Algorithms for ensuring confidentiality and their suitability

The focus in this subsection is to discuss existing algorithms for confidentiality and authentication from the perspective of their suitability for WSNs and for the selected reference scenarios and how they could be enhanced with context-awareness and flexibility features in order to be applied in the ACAPP framework.

5.1.1. Confidentiality

Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorised to have access". In other words, confidentiality is the property of preventing disclosure of information to unauthorised individuals or systems.

Confidentiality is ensured with Encryption and Authentication Algorithms. First the discussion will be about RC5 and AES algorithms and then The Diffie-Hellman Algorithm (DHA) and The Elliptical Curve Cryptography (ECC) will be discussed.

Discussion on the RC5 and AES Algorithms

Strength
The **RC5 algorithm** is recognised by the cryptographic community to be a secure algorithm. The only way to break a secure algorithm is to try every possible key on a sequence of encrypted data, known as the brute force attack. As the length of the key increases, the number of possible keys increases exponentially. For example, a 56-bits key as 2^{56} possible keys, and if it is assumed that a computer can compute a million key per second, it will take approximately 2,258 years to a single attacker to find the correct key. A 64-bits key will take the same attacker more than 585,000 years [3].
The **AES** encryption process, based on the **Rijndael** algorithm is currently the most secure algorithm implemented. In addition to its incredible strength, it is light enough to be implemented in smart card located in 3G mobile phones and PDA. As a comparison with the RC5 described above, if a computer would be able to solve

a 56-bits key encrypted data with RC5 algorithm in 1 sec, it would need 149,000 billions of years to find the correct key…

Variable Parameters
The RC5 has the particularity to be modulated according to the user wishes to improve the security or the performance. In this way several parameters could be set. The conventional notation for any RC5 algorithm is RC5-***w*/*r*/*b*** where:

- **w** is the *word size* in bits. It represents the length of the data blocks of plaintext and ciphertext treated. The most common size is 32 bits, but 16 and 64 bits are also available. RC5 encrypts two-word blocks, which means that plaintext and ciphertext are 2*w*-bits long each.
- **r** is the number of rounds. The tolerable values are 0 to 255 rounds. The expanded key table ***S*** contains t = 2(r+1) words.
- **b** is the length of the secret key ***K*** in bytes. The number of bytes of the key could be chosen between 0 and 255. As shown in the previous paragraph, a 56-bit key is more than enough to guarantee sufficient security in this particular case.

However, the assumption is that the shorter the lengths are and the smaller the number of rounds is, the weaker the algorithm is.

The AES algorithm is based on variable key lengths which are 128, 192 and 256 bits used to encrypt 128-bits blocks of data. The Rijndael algorithm allowed more data blocks sizes that were not adopted in the AES standard. As it can be seen, even if the AES algorithm is much more secure than the RC5, it remains less flexible for the security and privacy objectives defined in this report.

Algorithms
The **RC5** algorithm is divided into three parts:

- A key expansion algorithm, used to create additional keys from the main key.
- An encryption algorithm
- A decryption algorithm

The encryption process is based on only three basic operations: additions, exclusive-or (XOR), and rotation.

The **AES** algorithm is a more complex. Every 128-bits data blocks are divided in 4 blocks.
To these blocks, 4 operations are made:

- A byte substitution. Each byte is replaced by a different, thanks to a S-Box (a table of substitution).
- A shift in rows. In each rows of the small blocks, bytes are shifted by 0, 1, 2 or 3 places.
- A mixing in columns. Each column vectors of 4 bytes are multiplied by a 4x4 matrix.
- A XOR addition with a sub-key. The sub-keys are defined by a key expansion algorithm, as for the RC5.

These four operations are duplicated as many times as the number of rounds the algorithm is defined, except for the last round, where the mixing in column step is avoided.

Advantages of the AES algorithm
AES is currently the most secured algorithm implemented. Its robustness would allow it to go through years without being solved, at least for a couple of years. It is quite easy to implement on any type of hardware and software since it only uses simple operations.

Disadvantages of the AES algorithm
The strength of this algorithm is its substitution table. It gives it a higher level of security than the RC5 for example. However, one of the constraints in sensor motes is the memory size, and it is not possible to add such a table (which should be dynamic) in the motes. Moreover, the encryption process, although simple, would use resources and consume batteries faster than the RC5.

Short discussion

The conclusion is that for the proposed system, comaprisn AES with RC5, even the 64-bits RC5 algorithm, despite of the fact that is breakable, seems to be much more secure than the privacy levels to be reached. Moreover, the RC5 algorithm allows much more customisation than the AES algorithm.
Thus, the use of the RC5 algorithm is considered a good compromise between security, adaptability and performance.

Proposed Adaptive Confidentiality

The proposed ACAPP framework is adaptive w.r.t. its building blocks and w.r.t the algortums and mechanisms, which in their turn have possibility to be flexible.
In the following subsection one of the security algorithms which is enhanced with flexibility is described – namely the proposed mechanism by which adaptive confidentiality is ensured in ACAPP.

Adaptive Parameters for RC5

The assumptions
The RC5-32/12/8 (64-bits key) algorithm has been solved by a group of volunteers which has joined the power of more than 40,000 2Ghz computers for a period of 1,757 days to find the correct key[33]. From this sum of operations, some assumptions are defined to find some suitable parameters to take into account in the adaptive security system.
The simulations were performed considering the parameters of MICA2dot sensor nodes, that have 8-bits / 4Mhz processors. This implies that:

- To solve the same problem (RC5-32/12/8) with a **single node**, it would take more than 140 billions of days.
- If the number of rounds was divided by 2, the computational time was also divided by 2, but it was kept a sufficient level of encryption. Estimated time to solve the key: 70 billions of days.
- If the length of the block of plaintext was changed, it would affect neither the security nor the processing time, so this paramewter would not be changed.
- If the length of the key was reduced, the computational time would be divided by 2 for each bit removed. It would only remove 8 bits per 8 bits and it would give the following results :

    - 70 billions / 2^8 = 273 millions of days for a 56-bit key
    - 70 billions / 2^{16} = 1 million of days for a 48-bits key
    - 70 billions / 2^{24} = 4,172 days for a 40-bits key
    - 70 billions / 2^{32} = 16 days for a 32-bits key
    - 70 billions / 2^{40} = 1,5 hours for a 24-bits key

In an ideal case, a single sensor node could be able to solve a RC5-32/6/3, in only 1,5 hours. However, it would imply that:

- The sensor node would have compute at the maximum of its capabilities during all this time, and may be out of batteries before finding the right key.
- The assumption is that the sensor node would be able to do such a computation.
- The assumption is that there is not any new key exchange between the nodes and the aggregator.

Definition of the different levels of confidentiality
In the following paragraph the line of thought when defining the confidentiality levels is present.

For trusted environment, which is considered to be the home environment, as defined in Section 4.6.1, the security requirements are lower, thus leading to less computations. This lower level of security is sufficient to provide satisfactory performance and higher batteries lifetime. In such a scenario, a MICA2dot sensor node of the network could be able to process its encryption algorithm in less than 0,35 ms, according to the simulation results.
Thus, the consideration is that the RC5-32/6/3 algorithm is suitable for the trusted environments.
Starting from this point, the encryption process by modifying the two parameters is increased (number of rounds and key length) to define the medium and high levels of security, to be applied in a contolled and public environments respectively. In this way, the length of the key is set to 40 bits, which would require a computational

effort of 2 days to a computer, if the number of round is still fixed at 6. This is defined as the medium level of security, which would be used in a hospital scenario.
To define the high level of security, the number of rounds is modified from the medium level of security from 6 to 12, which should double the computational process to solve the key (approximately 4 days). However, if these parameters seem to have some easy breakpoints, the key exchange process is taken into account, which occurs at a frequency higher than daily.

The different levels of confidentiality with their RC5 parameters are summarised in the following table:

Confidentiality Levels	Block Length	Number of rounds	Key length
Low	32 bits	6	24 bits
Medium	32 bits	6	40 bits
High	32 bits	12	40 bits

Table 26: RC5 parameters providing different levels of confidentiality

5.1.2. Algorithms for authorisation and their suitability

Broadly speaking, authorisation determines what a subject can do on the system. When a subject is authorised to perform an action for a system, it is usually the case that the subject has the permission to "read" (R) or "write" (W). Read could be to read content; Write could be to change content.

In this section The Diffie-Hellman Algorithm (DHA) and The Elliptical Curve Cryptography (ECC) are discussed.

The Diffie-Hellman Algorithm

This algorithm is used for the authentication process that consists of the keys exchange. The particularity of this algorithm is that both nodes own a secret number that is never revealed in the network. Both combined, this two numbers provide the encryption key that is exactly the same for the two nodes, that is the reason it is called the symmetric key. The following example depicts the concept:
Node A and Node B want to exchange vital information that no one would be able to intercept and decrypt. They first have to generate an encryption key.

The Algorithm

- First, they will define two numbers **p** & **g**.
  - p is a large prime number (> 512 bits)
  - g is called the "base" or "generator"

- Second, they will both define their own secret number.
  - Node A choose **a**
  - Node B choose **b**

- Third, they will compute their public number.
  - Node A will compute $\mathbf{x = g^a \bmod p}$
  - Node B will compute $\mathbf{y = g^b \bmod p}$

- Fourth, they will exchange their public number.
  - Node A knows **p, g, a, x, y**
  - Node B knows **p, g, b, x, y**

- Fifth, they will compute the encryption key.
  - Node A will compute $\mathbf{k_a = y^a \bmod p = (g^b \bmod p)^a \bmod p}$

  = gba mod p

- Node B will compute $\mathbf{k_b} = \mathbf{x}^{\mathbf{b}} \bmod \mathbf{p} = (\mathbf{g}^{\mathbf{a}} \bmod \mathbf{p})^{\mathbf{b}} \bmod \mathbf{p}$
  $= \mathbf{g}^{\mathbf{ab}} \bmod \mathbf{p}$

The encryption key is ka = kb = k.

Possible attacks

It is assumed now that adversary C wants to decrypt information sent by both Node A and Node B. Then he has to listen to the network to get $\mathbf{g}^{\mathbf{a}}$ and $\mathbf{g}^{\mathbf{b}}$ since they are emitted in a public medium. In this case, it is supposed that adversary A also knows the value of g. However, to find the values **a** and **b** he will have to compute a discrete logarithm of $\mathbf{g}^{\mathbf{a}}$ and $\mathbf{g}^{\mathbf{b}}$ which is currently impossible with big values of **p**.

An alternative is called "man in the middle" attack. In this case, Adversary C will be between Node A and Node B. He will get the value $\mathbf{g}^{\mathbf{a}}$ from Node A and send the value $\mathbf{g}^{\mathbf{a'}}$ to Node B. In the same manner, he will get the value $\mathbf{g}^{\mathbf{b}}$ from Node B and send the value $\mathbf{g}^{\mathbf{b'}}$ to Node A. Node A and Node B will both think they have the same encryption key whereas Node A will have $\mathbf{g}^{\mathbf{ab'}}$ and Node B $\mathbf{g}^{\mathbf{a'b}}$. Thus, Adversary C will be able to decrypt all the messages that come from both sides.

Possible Counter-Measures

To avoid this kind of attack, two solutions are possible:

- The signature of the exchanged values with the use of a couple of asymmetric keys certified by a trusted third party.
- The exchange of the values **x** and **y** in Station-to-Station protocol.

The Elliptical Curve Cryptography (ECC)

Unfortunately the Diffie-Hellman procedure, just by itself, requires some processor and memory resources which for a normal computer are insignificant but for a sensor node the case is very different. The problem sensor nodes have to face is the computation of heavy exponential mathematical expressions as shown in section 5.4.1.3. Therefore in the proposed framework the use of **Elliptic Curve Diffie-Hellman** as the best suitable authentication procedure for WSN to be used. With the use of elliptic curves there is no longer need to work with heavy exponential equations. Instead the work is with the well known elliptical curve equation in a (x, y) Cartesian coordinate system.

The elliptical curve equations

Applied to real numbers for simplicity, they are defined by the following formula:

Equation (1) $$y^2 = x^3 + ax + b$$

Where a and b are real numbers.

The property of the elliptical curves is the non singularity of the curve, which means that the curve never crosses itself. Moreover, if two points P and Q on the curve are taken, a third point R could be defined that correspond to P+Q, which could be represented as the third intersection point of the curve when a line is drawn that goes through P and Q.

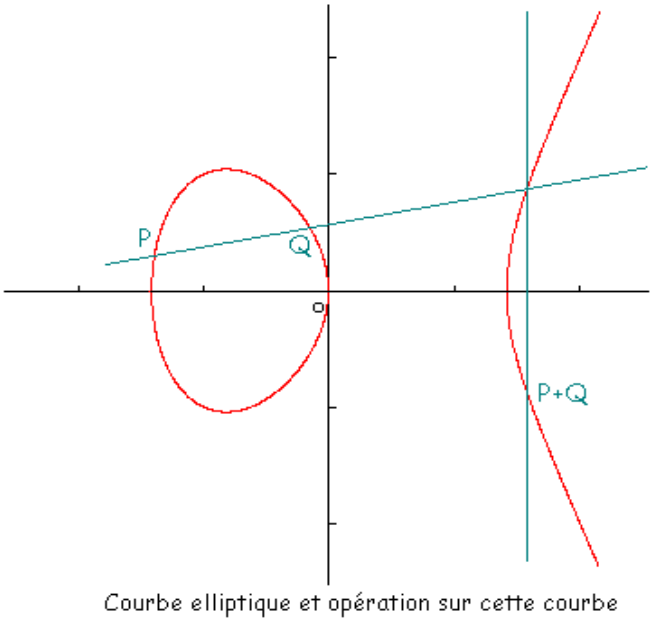


Figure 15: An elliptical curve representation [4]

From the points $P(x_1,y_1)$ and $Q(x_2,y_2)$, it is possible to find the coordinates of the point R with the following formulas [5]:

Equation (2) $$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

Equation (3) $$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

Application to the cryptography

The main operation in elliptical curve cryptographic schemes is point multiplication. This operation presents the most desired properties in cryptography, i.e. the forward operation is quite simple but its inverse is very difficult. The main characteristics of Diffie-Hellman still persist in this method.

Point multiplication is done by calculating Q=kP, where k is an integer and P is a point on the elliptic curve defined in the prime field. Scalar multiplication is performed through a combination of point additions and point doublings, e.g. $9P = 2(2(2P)) + P$. Each curve has a specially designated point G, called the base point, chosen such that a large fraction of the elliptic curve points are multiples of it.

The elliptical curve equation has been implemented in the Diffie-Hellman algorithm for higher robustness against attackers. In the previous example, instead of choosing **p** and **g**, Node A and Node B would have made their choice on an elliptical curve equation and a point P on the curve. Node A and Node B both choose a real value $\mathbf{k_a}$ and $\mathbf{k_b}$, and send the product with P to the other party. Node B will get $\mathbf{k_aP}$ from Node A, which will get $\mathbf{k_bP}$ in return.

Both nodes can compute $\mathbf{k_a(k_bP) = k_b\ (k_aP) = k_ak_bP}$ which is a point on the curve and the encryption key. Once again, to break the encryption key, the attacker will have to solve the elliptic curve discrete logarithm problem (ECDLP), i.e. to find k given P and Q=kP. This calculation is computationally intractable for large values of k.

So far the best known attack against ECC is called the Pollard's rho attack [6]. Pollard's rho attack belongs to the class of collision search attacks, which achieve better performance than brute force attacks. However, as the field size increases, it has been proven that Pollard's rho attack gets more difficult as $\frac{(\pi \times n)^{1/2}}{2}$ where n represents the group size, which is exponential to the key size.

Therefore the conclusion is that for big group sizes this attack will take a long time to break ECC. Since the best known algorithm to attack ECC runs more slowly than the best known algorithm to attack other cryptosystems, ECC can offer equivalent security with smaller key sizes.

As an example a 160-bit ECC key provides the same level of security as a 1024-bit RSA key [7]. This is the main reason why ECC is so attractive for small devices with lower energy and processing capabilities.

5.1.3. Proposed Security Protocol Suite: Combining RC5 and Elliptic Curve -Diffie-Hellman

In order to provide flexibility and adaptivity feature for confidentiality and authorisation algorithm, suitabale for small devices with very limited energy and computationals capabilites such as sensor nodes and the neccesary level of security, the posibility of combining RC5 and Elliptic Curve Diffie-Hellman will be investigated in order to propose suitable for the discussed systems secrty protocol suite.

As described before, RC5 is not sufficient to provide us a high level of security, therefore the Elliptic Curve Diffie-Hellman key exchange protocol is added to sthrengthen the weeknesses.

The applicability of this protocol to WSN is expalined below:
Since the available channel for the sensors to communicate with the aggregator may be eavesdropped by a third party, there is the need to use the proposed protocol siute. In order for the two parties (end node sensors on one side and aggregators or coordinators on other side) to obtain their keys, some domain parameters have to be agreed upon. In this case (p,a,b,G,n,h) should be exchanged between them. Therefore they can compute the same key K.
Through this process another problem arises. How it is sure that the aggregator/sensor is communicating with the right sensor/aggregator? Is should not be forgetten that although the sensor's range is limited, in some situations the aggregator may capture incoming signals from sensors which are not part of the network. This situation might easily occur if someone seats next to a person and they both have BSNs.
To investigate this possible scenario, the following solution is proposed: Instead of using the key K obtained by the Elliptic Curve Diffie-Hellman, an extra operation is performed that will create a K' which will use the sensor node's ID. Since the sensor node's ID should never be sent without being encrypted because it could be eavesdrop and then easily cloned, the recommendation is that after obtaining the key K both the sensor and the aggregator should perform an XOR operation between the key K and the node's ID. In order for this procedure to work properly the aggregator has to know all the sensors IDs but that was already assumed before. However since the aggregator does not know with which sensor it is communicating, in the worst case it may have to do this XOR operation the same number of times as the number of sensors. According to the simulation results, this process wastes energy and some latency problems might occur, therefore there was the need to come up with a more time efficient solution. Since the goal of BSN in the medical scenario is to treat the vital information first, the use of flags after the encrypted messages is studied.

The idea of adding a vital informaiton flag (VIF) does not compromise the required security level. Below it is explained how VIF works:
Two numbers are defined. The first number is on a single bit, defined as **1** for vital information and **0** for non-vital information.
The second number is on a byte: from **0** to **N**, where N represent the number of the end-sensor node, defined when the BSN is designed. Both information would be stored in the end -ensor nodes and the aggregator.

Vital / Non-Vital parameter	Number of the node	Encryption Key	Information registred in…
0	0000 0001	Key 1	Node 1 , aggregator
1	0000 0010	Key 2	Node 2 , aggregator
1	0000 0011	Key 3	Node 3 , aggregator
0	0000 0100	Key 4	Node 4 , aggregator

Table 27: Information about vital/non-vital node

Then, both numbers could be integrated in the frame before the encrypted message:

Authentication Numbers		Encrypted Message
0	0000 0001	0010 1010 1101 0101 0110 0010 0111 0001 0001 …

Table 28: Example of encrypted message

Discussion
If an attacker gets the frame, he would be able to read the numbers, but it couldn't use them to decrypt the message as they are fully independent from the encryption algorithm. Once the aggregator receives the message, it directly knows which node it comes from and can decrypt it with the right key. With this solution latency is no longer a problem because priority messages could be identified and also the aggregator only has to find the right key in its table, which is a process very fast and doesn't consume much energy. One problem with this solution is eavesdropping, since the flags and the number of the node are not encrypted, the adversary may have access to this information. Therefore he is able to determine from which sensor a certain message came from. However the adversary cannot easily identify the kind of sensor (if it is the heart rate sensor or the breathing rate sensor, etc). Therefore he cannot predetermine the content of the message.

5.1.4. Summary of Section 5.1

In this section it was discussed how confidentiality with flexibility feature could be achieved. Two algorithms have been analysed – *RC5 and AES. Even* if the AES algorithm is more secure than the RC5, it remains less flexible for the security and privacy objectives defined in this report. Moreover, the encryption process with AES, although simple, would use resources and consume batteries faster than the RC5. Therefore, RC5 was selected and on Table 5 it was shown how, via a combination of its parameters, different levels of confidentiality were defined.
Another part of the confidentiality is the authorisation process. The suitability of The Diffie-Hellman Algorithm (DHA) and Elliptical Curve Cryptography (ECC) for authentication was discussed in this section.
Unfortunately the Diffie-Hellman procedure, just by itself, is quite haeavy for the resourse contsrained sensor nodes. This is bacuase of the heavy exponential mathematical expressions. To avoud this resosurce consuming process, in the proposed framework the use of **Elliptic Curve-Diffie-Hellman** is taken as a more suitable authentication procedure for WSN based on the elliptical curve equation in a (x, y) Cartesian coordinate system.
Taking into account all the presented in the above paragraphs, it is concluded that the proposed security protocol suit *(*RC5 combined with the Elliptic Curve - Diffie-Hellman) will ensure the privacy which is needed for the reference scenario even in the lowest security level with the goal of energy savings and extended battery lifetime.
The results from the evaluation of the proposed security protocol suit will be presented in Section 6.3.

5.2. The Proposed Context-Aware Mechanism for Controlled Information Disclosure

In the pervasive health-care scenarios, personal data is being accumulated and communicated, which raises privacy concerns, as explained in Section 1.3. Apart from that, some other node or communication identifiers might be used by an attacker to infer additional information (location, identity) which can intrude the privacy of the sender (Section 3.3.2).
In this section the focus of the discussion is on how enhancing controlled information disclosure with context-awareness could better protect the privacy of the end-user in pervasive telehealth and telecare systems with WSNs.

5.2.1. Exchange of privacy primitives

A request for user data triggers a series of actions in the Security Manager. This request is processed from the application subsystem, via the management subsystem, to the connectivity subsystems of the sender and receiver's side. Figure 16 shows how the privacy primitives are exchanged within these subsystems. Upon receiving the request for a privacy service from the application subsystem APMA–PRIVACY.req, the management subsystem defines the necessary privacy indications and requests with MACO–PRIVACY.req to provide them for the current transmission. Confirmations to the management and applications subsystems are sent back with MACO–PRIVACY.cnf and APMA–PRIVACY.cnf.

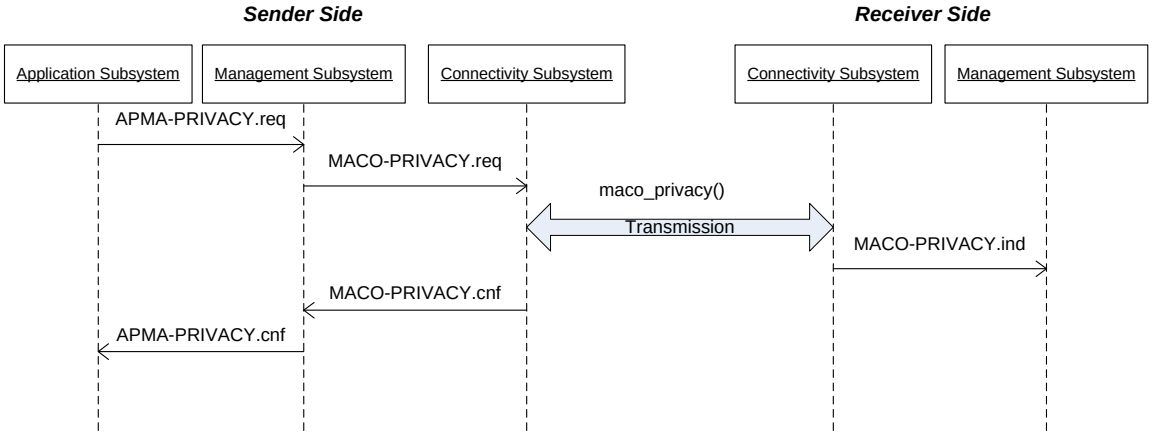


Figure 16: How the privacy primitives are exchanged

5.2.2. Block for privacy protection mechanisms

The access to the data is filtered through the Privacy Safeguard which is part of the privacy protection mechanisms. The privacy safeguard mechanism shown on Figure 17 is responsible for taking decisions concerning controlled information disclosure for data subject to control, with the help of assigned privacy flags.
In the following paragraphs, the proposed context-aware mechanism for controlled information disclosure is explained. It is called Privacy Safeguard (PS). Its main purpose is to filter privacy information (user-sensitive, context and any other node identifiable information) when a request for information comes.

Every personal data for the end-user or confidential corporate data, subject to policy for controlled information disclosure, it is supposed to have its own privacy flag that can be set up in the process of the default setup or later by the user or by the network administrator prior to any usage (with the help of the privacy and trust assistant – via GUI). The privacy flag implements the policy of how this particular piece of sensitive data must be treated before disclosing [8].

The main service offered by the Privacy Safeguard Mechanism is *getFilteredSourceData*: returns the allowed user sensitive data according to the privacy flag. The query is processed according to this rule: if the flag is "Always", the expected data value is returned; if it is "Never", and empty value is returned, if it is "Ask", the user is explicitly asked whether the query can be processed. If it is "Check the profile", the policy for data disclosure is checked for the user profile. This is depicted in the following Figure 17.

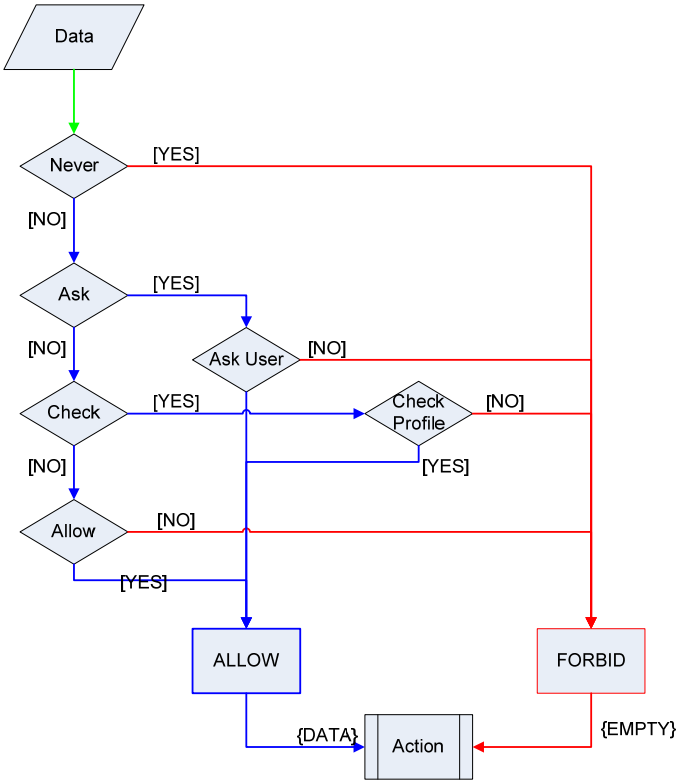


Figure 17: Privacy Safeguard Mechanism [8]

5.2.3. Anonymity

For the privacy protection process to be complete, another important aspect must be mentioned – ensuring anonymity, also the types of mechanisms used to create the pseudonyms.

Anonymity mechanisms can ensure that users may use a resource or a service without being distinguished from other users and without disclosing their identities to third parties. Anonymity is defined as "the state of not being identifiable within a set of subjects", referred to as the anonymity set [9]. With respect to acting entities, the anonymity set consists of the subjects who might cause an action. With respect to addressees (subjects being addressed), the anonymity set consists of the subjects who might be addressed. To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes. It is thus a requirement for anonymity mechanisms to be context-aware.

As long as the users are anonymous, they could disclose any personal data, such as the location, that can be considered as essential in future ubiquitous sensor networks. Considering a user's location as personal data, as long as no identifying information is attached to the location, i.e., the user is anonymous, the privacy of the user is protected. As in many network settings the use of identifiers is integral part and often necessary for correct operation of most applications, the goal is to make these identifiers temporary and change them to prevent the collection of too many information about a node that – in the long run – will help identifying it. In addition, changing identifiers in the right situation helps to break the connection to any identifying information that – purposefully or not – have been provided to the peer. Like this, the user can maintain control of the information that can be associated to her.

In order for anonymity to be achieved, the data communicated in the sensor network needs either to be depersonalised or pseudonymised with respect to the identity of the sender, in cases that a legitimate network service requires user identification. Pseudonymity is the use of pseudonyms instead of ID [10]. Pseudonyms with different scopes and duration can be used for each communication, from node pseudonyms to transaction pseudonyms, for achieving different levels of long-term unlinkability. In general, anonymity is stronger the more often and independently the pseudonyms are selected. But this has of course its costs - in some approaches for achieving anonymity, this requires additional communication and computation efforts.

In addition, the potential impact of the pseudonym change is also important. Situations that allow a direct mapping of the pseudonym to the node, for example by restricted space identification may require a pseudonym change shortly before and after this situation, in order to limit the amount of available information about the traces for the identified user. Following this, an important question which is investigated in the literature is for the trade-off between how often the pseudonyms are changed and the achieved anonymity level on one side, and the application requirements on the other side. Having in mind the resource constrained sensor nodes and the cost to compute a new pseudonym, in comparison with the standard approach when the pseudonyms are changed periodically. It is of importance the suitable moment when a pseudonym must be changed. Thus the node must have mechanism to evaluate the current context in order to decide when the most suitable time to change the pseudonym is, in order to avoid energy waste. For this purpose, a *Pseudonym Manager* could be introduced in ACAPP to create or change pseudonyms, as shown on Figure 18. The mechanism itself by which pseudonyms are created and by which the life-time of the pseudonyms are defined, could be part of the block of the Privacy Mechanisms. However, proposal of mechanism for improving anonymity is out of the scope of this PhD thesis. More information for anonymity mechanisms can be found in [11].

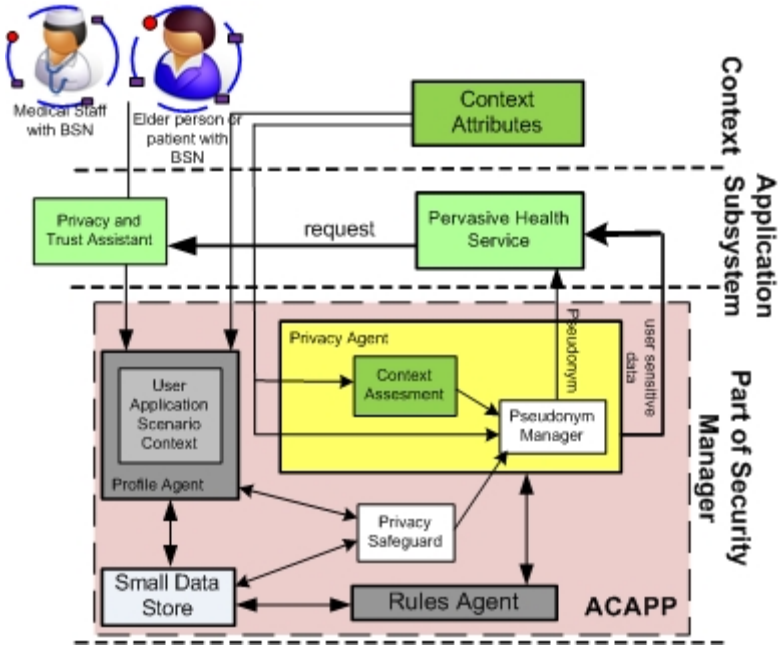


Figure 18: Component Model of Privacy Protection Framework

5.2.4. Interaction among the entities

The Profile Agent handles profiles of the user, of the context, of the application, and of the situation. To define the current user role, the context is taken into account. Scenarios are also defined - for the most common situations of the user's daily life based on information for the role and location of the user and role and location of the party requesting the sensitive user data. This was presented in Table 24 (HLCA). The small Data store holds user profiles descriptions of important preferences and characteristics; role categories; security, privacy and trust policies, priority rules, the access rights and different policies. It gives the user personalisation options of having a number of profiles based on different roles - employee, parent, patient, etc. In each of the profiles, security and privacy preferences of the user are defined. The Adaptive Privacy Protection block takes the context, the situation, the anonymity level, trust level, and privacy preferences as input to decide how to protect the privacy of the user. The PS filters with privacy flags all the private and personal data from being disclosed to any outside party without prior approval or knowledge of the user. Rules for revealing private information and access policies are handled by the Rule Agent. Figure 19 presents the interaction flow for controlled information disclosure when a request for user data comes.

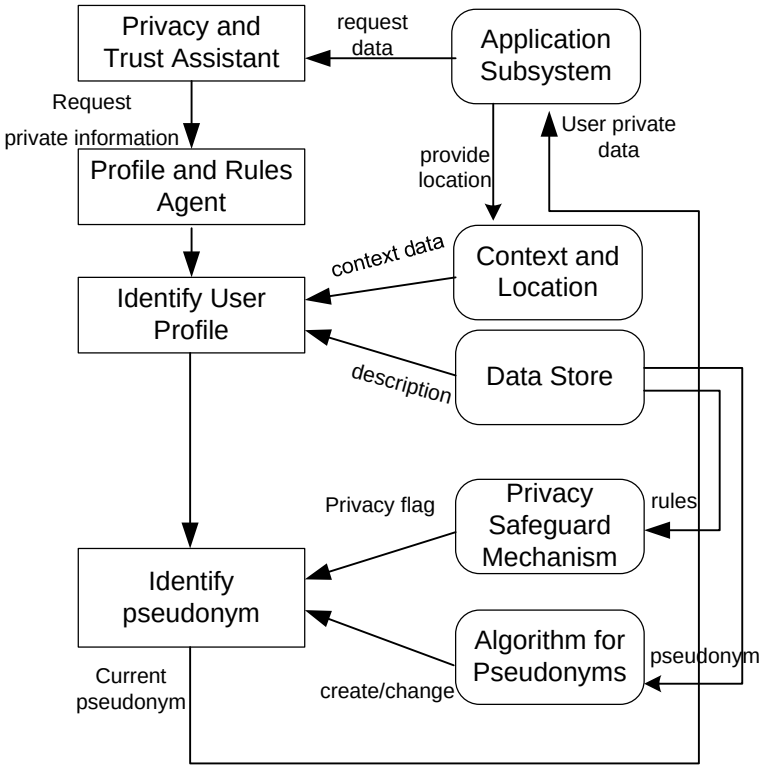


Figure 19: Interaction flow for controlled information disclosure [11]

5.2.5. Data Abstractions

To decrease the delay introduced by the context-aware privacy protection, all sensitive data, aimed at being communicated, can be grouped into data abstractions. In this case, the filtering is done on the level of the data abstractions. For deeper level of granularity, each data abstraction consists of more detailed sensitive data. Each data abstraction and data has its own PF which can be set up (default setup) prior to any usage. Figure 20 gives a brief overview of the data abstractions for a patient in the reference hospital scenario. Data abstractions are introduced with the aim of reducing the power cost and the response time in the communications which do not require protection of low granularity sensitive data.

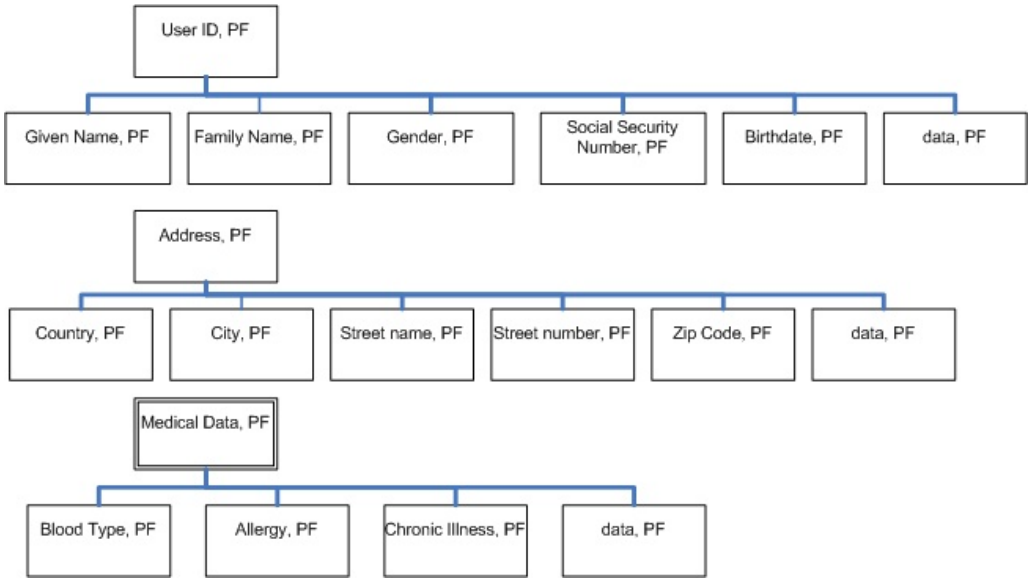


Figure 20: Data abstractions [8]

5.2.6. Summary of Section 5.2

In this section it was shown how the privacy primitives are exchanged among the application, management and connectivity subsystems among the sender and the receiver. Then, the main blocks of the privacy protection were presented with the respective services. The mechanism ensuring personalisation and flexibly in the controlled access is the Privacy Safeguard with a number of options for filtering of the data - “Always”, “Never”, explicitly “Ask” the user and “Check the user profile”. Filtering of the data depends on the data granularity. However, to achieve faster filtering, data abstractions for thematic groups of personal data have been proposed. This could be used when the request for data is with less granularity.
If anonymity provision is one of the scenario and user requirements, Pseudonym Manager Block could be introduced, which handles the creation of pseudonyms and defines the exact moment to change them.

5.3. Profile and Rules Agent

As described in the previous section, the filtering of the user data before any disclosure is based on pre-defined user roles and rules for revealing information, for actions to be taken in case of emergency, etc.
The approach taken in this work for controlled information disclosure is a mix between the role- and policy-based. Therefore, the Profile and Rules Agent plays a major role in the privacy protection framework.
The Profile and Rules Agent has several sub-modules: Profiles for objects (devices, persons and their roles), Profile of Context, Application/Service Profile and Scenario Profile.
The profiles are described in the Profiles and Rules Agent in xml format; each field of the user profile has its own privacy flag which, by default, is set up to “Never” but it can be changed by the user in any moment via GUI. The user data which privacy flag is different from “Always” are considered sensitive. Each profile has a template that basically is an empty profile.
The actions that can be taken by the Profile and Rules Agent are loading data from the Data Store, updating and deleting the whole profiles as well as only part of the profile.

The most important services that the Profile and Rules Agent provides are:
getCurrentRole(), getCurrentLocation(), getCurrentContextAttributes(), getCurrentApplicationTypeParameters().

5.3.1. User Profiles

In the User Profile there is information defined for user roles and corresponding location of the requesting party based on the most common daily activities.

For more advanced users or the network administrator, it is possible to load a profile template, save a profile as a new user, update own user profile or delete it with the help of the Privacy and Trust Assistant (via GUI). These actions are respectively taken up through the commands *LoadUserProfileTemplate(), saveNewUserProfile(), updateUserProfile(), deleteUserProfile()*

Each field of user data has its own SET and GET set of actions which are listed below:

- *getUserID, setUserID, getUserIDFlag, setUserIDFlag, getFirstName, setFirstName, getLastName, setLastName.*

The PF management interface is used to setup and update the PFs.

- *getXPrivacyFlag*: gets the PF of user sensitive data from the user profile. In this case X is the policy protected data
- *setXPrivacyFlags*: sets the PF for a certain user sensitive data X.

In particular for the reference scenarios described in Section 3.1.2, the user (e.g. the patient) can request to see his vital functions information, while, in case the users are doctors, they might request to know the vital functions of the patients as well as location information through the following service queries: *getData, setData, getDataFlag, setDataFlag, getVitalFunctions, getLocationInformation,* and so on.

The system is also able to define the current role of the person-based context information for the current GPS coordinates or relative indoor location and then map it to a meaningful location for the person using the following set of services: setXRole, getXRole, getXRoleFlag, setXRoleFlag. Examples of descriptive roles for the reference scenario are: patient, family member, friend, doctor, nurse. There are also services to get and set PFs for controlled information disclosure regarding the current role.
The core user roles with the corresponding locations implemented are UserAtHome(Parent, home), UserAtWork(Employee, office), UserAtHospital(Patient, Hospital), UserInCar(Driver, Car), UserHobby(GolfPlayer, GolfClub).
An important question is how exactly the system defines which the current user profile is, after considering the current parameters of some context attributes. This is presented in Table 29.

GPS interval	**Source_Location**	**Source_Role, Probability**
((x1,y1), (x2,y2))	**Location_Name**	**Role_Name, P**
((xhm1,yhm1), (xhm2,yhm2))	Home	User, 1; Parent, 0.9; Spouse, 0.8; Child, 0.5; Patient, 0.5; Employee, 0.3; Friend, 0.3
((xof1,yof1), (xof2,yof2))	Office	User, 1; Parent, 0.7; Spouse, 0.8; Child, 0.1; Patient, 0.2; Employee, 0.9; Friend, 0.2
((xhs1,yhs1), (xhs2,yhs2))	Hospital	User, 1; Parent, 0.7; Spouse, 0.8; Child, 0.2; Patient, 0.9; Employee, 0.1; Friend, 0.1
	Public (out of other locations)	User, 1; Parent, 0.7; Spouse, 0.8; Child, 0.4 Patient, 0.2; Employee, 0.1; Friend, 0.6

Table 29: Selection of the current user role

Additional services are:

- get and set additional policy protected data with PFs (through the services *setNewPrivacyData, getNewPrivacyData, setNewPrivacyDataFlag, getNewPrivacyDataFlag*)
- there might be some others

In Table 4 the sensitive data which needs privacy protection was presented. The profiles, the user roles, the locations and the user sensitive data (USD), and the values defined for them, are presented in Table 30.

Context	Values
Source_Role (SR)	Patient, Spouse, Family member, Employee, Friend, User
Destination_Role (DR)	Doctor, Family member, Boss, Friend, Spouse, Child, Unknown,
Location (L)	Home, Office, Hospital, Car, Public, Unknown,
User sensitive data (USD) General Categories	User Identity (*GivenName, FamilyName, Gender…),* Medical history, Medical data*(BloodType, Allergy, ChronicIllness…),* Social security number, Address *(Country, City, StreetName…),* Telephone , Location

Table 30: Defined values for user roles and user sensitive information

Examples of predefined rules for disclosure of USD for the medical scenario are presented in Table 31.

5.3.2. Context Profile

The Context Profile deals with the context attributes and extracts the current context attributes from the context profile. It is responsible for providing context information as accurate as the system can deliver it. The contexts which are taken into consideration within the pervasive healthcare applications of all the considered scenarios in this PhD thesis are: Vital Function, Indoor Location, Outdoor Location, Environment physical parameters, available hospital equipment. (Table 4)

The location of an object (this could be an end-device, a person, etc…) is actually very important information which is treated with more specific queries. The system sets or gets the location (together with the PF for controlling the information disclosure) through the commands: *getXLocation, setXLocation, getXLocationFlag, setXLocationFlag* where X is indicating the source (the object) and the possibility for revealing the location.

Examples of meaningful location values could be provided with different accuracy and area: hospital, room in a hospital, home, etc.

Beside, the system or the end-user might be interested in a more accurate or specific information about the location, like for example the GPS coordinates or indoor location, the name of the room where the user is located, the name of the building, the name of the street, the name of the city or the country: *getXLocationAccuracy, setXLocationAccuracy, setXLocationAccuracyFlag, getXLocationAccuracyFlag.*

The assumption here is that "raw information" which represents context attributes is provided to the management subsystem. Further, for the work of the privacy protection framework, this raw context data is then "translated" into meaningful input information which must be fed into the privacy protection mechanisms via suitable predefined rules and policies. The component which takes care of the mapping of context attributes to meaningful policies is the Rule Agent, as explained in Section 5.2.2.

To remind, the current context information could be dynamic or relatively static, as presented on Figure 9 and Table 4, and is used for the ACAPP mechanisms to work properly.

5.3.3. Application/Service Profile

This profile describes the application/service type and features the provided services.

The application type, according to the scenarios described previously in this document, can be for example Enhanced Professional Communication, Emergency Localisation for the pervasive healthcare applications.

The service profile is considered to be part of the context. The service profile contains information for the types of the following parameters: the requesting party, the requesting location, the domain types (medical, entertainment, sport, etc…), interaction type (one-one/one-many), location accuracy requested (different levels of granularity – exact GPS coordinates, room, building, street), requested identifiable user parameter (ID, exact user name, pseudonym, label name), service duration (short, medium, long).

ServiceName = f (RequestorID, RequestorLocation, DomainType, InteractionType, LocationAccuracyLevel, UserParameter, TimeDuration).

If a patient visits the hospital for a visit for example, at the reception, a registering service will automatically register the patient on his/her entrance. The registering service is defined as (CityHospital, Registrator, HospitalregsitrationDesk, Medical, One2One, HospitalBuilding, LabelName, short).
According to the chosen application type, different parameters are relevant and likely to be treated by privacy mechanisms, for example in the reference scenario, the location of the patient and the doctor are important and vital signs of the patient and location of the doctor are important and assumed to be sensitive information. They are subject to controlled information disclosure.
It is also important to specify the duration of the expected communication for the given application, if the type of application is long term or short term. This is also linked to evaluation of how often the pseudonym needs to be changed, in case the location privacy of a person is required to be protected.

The services related to the Application/Service Profile are:

- *getApplicationType*(): it returns the type of the application
- *getApplicationTypeParameters(): it* returns the important parameters of the application type

5.3.4. Profile for Scenario

For the scenario to be defined, the role and location of the requesting party should be identified. In the user profiles descriptions in the Profile Agent, the user describes the most probable requesting party role called DestinationRoleName linked with the role of the destination DestinationRole (DR) and the location of the requesting party DestinationLocation (DL), as explained in Section 5.3. Respectively Source Role (SR) and Source Location (SL). Examples for most probably destination roles: FamilyAtHome(Family member, home), BossAtWork(Boss, office), DoctorAtHospital(Doctor, Hospital), MedicalStaffAtHospital(Nurse, Hospital). The user has the option to create new destination roles. Working assumption is that the requesting party identity and location are provided by the trustworthy service provider and this information is used in the creation of the current scenario.
In the Scenarios Profiles (stored in the small Data Store), a list of most common scenarios for the daily life of the user is stored. The number of possible roles of source is r_s; number of possible roles of destination is r_d; number of possible locations of source is l_s; number of possible locations of destination is l_d. The number of all possible scenario combinations based on SR, SL, DR, DL is

Equation (4) $$l_s * l_d * r_s * r_d = N.$$

The current scenario profile is
ScenarioName(SourceRoleValue, SourceLocationValue, DestinationRoleValue, DestinationLocationValue, ProbabilityValue, ScenarioFlagValue).

To illustrate the gain when using scenario profiles for most common daily situations, when there are 4 different SRs, 4 different DRs, 4 different SLs and 5 different DLs, then N=320. After analysis, only the realistic ones are taken into account by setting their ProbabilityValue=1. In one of the implemented set of scenarios, the realistic number Nr is approximately 86 out of 320, (Nr / N =27%). ScenarioFlagValue is assigned in the setup stage by the users themselves and the values are (A-Always give | R-Ask User | N-Never give). This flag is used in cases when the result for the rule for providing or not sensitive information depends only on the current scenario. This is done also with the goal to decrease continuous the user involvement and to reduce the daily in the communication.

Example of current scenario is PatientDoctorAtHospital (UserAtHospital, DoctorAtHospital, 1, Always). For each realistic scenario a LabelName of the user is defined by the user herself which can then acts as (that also can be linked to) a long-/short-term pseudonym. For example, as mentioned before, the registration service in the hospital, the LabelName is created when the first time user is registered in the hospital and it is used in all the necessary communications/EPR access to keep the anonymity of the patient [8].

5.3.5. Rules Management

In the Profile and Rules Agent, the profiles of nodes, services, applications, users and situations are managed. Default profiles exist too. From them, the profiles of the user can be modified, updated and deleted. It must be underlined that this version of the Profiles and Rules Agent, which is more complex, should be considered for implementation in devices with higher capabilities only. Simpler and less complex policies with a minimal set of rules are applied to end-sensor nodes with limited capabilities. As described in Section 4.5, the Profile Module of the Profile and Rules Agent in a full functional device contains the following profiles: Node/Device Profiles, User Profiles, Service/Application Profiles, Context Profiles. Examples of user profiles and roles (source role), location, user sensitive data, are presented in Table 31.
Although the rules are predefined, there is always the choice for the user to change part of the rules for disclosing information.

The Rule Module processes the rules for filtering the sensitive user data. Each rule is function of the scenario (it could be any of the relations for the source, for the destination or both), the context attributes, conditions to be satisfied, USD, results and actions.

Rule = f (input, condition, user sensitive data, result, action)

The conditions are expressed as a logical function.

Result is the PF value for the USD: A - Always give; C - Check profile; R – Ask User; N - Never give.
The action for the USD is taken based on the PF value and it can be: Give data - Check profile - Ask user for permission - Never give data.

Rule ID	Destination_ Location	Destination _Role	Source_ Location	Current Source Role	Rule for revealing user data
t01	Hospital	Doctor	Home	Patient	Always (medical status), never for the rest of data
t02	Hospital	Doctor	Hospital	Patient	Always (medical status), Always (medical history), Ask user (address) Never for the rest of data
t03	Home	Spouse	Hospital	Patient	Always (current location) Always (medical status)
m01	Office	Boss	Home	Employee	Never (medical status), Never (medical history) Never (current location)
m02	Office	Boss	Office	Employee	Never (medical status), Never (medical history) Always (current location)
r01	Home	Child	Office	Parent	Always (current location)
r02	Home	Child	Hospital	Patient	Always (current location)
p01	Home	Spouse	Office	Spouse	Always (current location) Always (medical status)
s01	Public	Unknown	Home	User	Never for all data
s02	Public	Unknown	Public	User	Never for all data

Table 31: Examples of possible predefined rules

Some relevant examples of lower level rules for the medical scenario describe the behaviour of the SR and the DR are provided below. The Source Role represents the party who requests the disclosure of data or information. In the following, two cases were described:

"Rule A" explains what happens when a patient (destination) outside of hospital asks for the location of her/his doctor (source of information): since the doctor sets her/his PF for location data to "Never" when the doctor is out of working shift and patient is asking for it, this information cannot be disclosed.
"Rule B" is instead a rule for an emergency: it defines when the doctor should take action according to the heartbeat rate of the patient. If the heartbeat rate goes above a certain threshold (TH), then an action is needed.

Rule A: If DR=patient and DL=not_in_hospital, USD_requested=SR_location, SR=doctor and Time_doctor=out_of_shift then privacyflag(location data) = N
Action A = the location of the doctor will not be revealed and for providing any other user sensitive data, the user will be asked explicitly via GUI

Rule B: If SR=patient and SL=hospital, USD_requested=SR_hearthbeatrate, DR=doctor then privacyflag(data) = A
Action B = IF (USD_requested < TH) THEN (patient status is good → no action) ELSE (Patient status is not good → DR takes action)

More examples of high-level rules, applied to the information flow of the backup shift assistant scenario are given in Table 32 as in [11].

Context data	Rule Agent – Example of context-aware rules
Patient's medical data	Release to doctor and nurse on current shift only
Patient's Indoor Location	Show to doctor and nurse on current shift only
Patient's ID	Show to doctor only
Type of service	If service = hospital service, trust level= trusted
Doctor's Indoor Location	Show to nurse on shift only
Doctor's ID	Show to nurse on shift only
Nurse's Indoor Location	Show to doctor on shift only
Nurse's ID	Show to doctor on shift only
Colleague's Location	If location is public and remaining energy in all nodes is higher than $E_{threshold}$, set security level to high, otherwise set to low

Table 32: High level context information and respective rules

Selection of applicable rule

Explanation of how applicable rules are selected is given in the flowchart in Figure 21. In this case, several assumptions have been made:

- BSN consists of a coordinator node (CN) and a limited number of end nodes (EN). These nodes are known in advance from the setup phase. Starting from this assumption, the trust establishment procedure in the flowchart is not considered.
- The coordinator node moves with the end nodes.
- Malicious nodes' attacks are not considered.

Doctor A, who is at the hospital during nightshift, asks for location information of the back-up assistant - colleague on shift Doctor B who is at home at the moment. The privacy protection framework in the handheld device of Doctor B receives the request for USD (location). Then current destination location CDL = hospital; current destination role CDR = colleague; current source role CSR = doctor; current source location CSL = home. The predefined rule for Doctor B's location is "Provide my current location if the colleague on shift asks from the hospital and my current role is doctor". When a request for USD comes, context information for the current user location, current time of the day is already provided to the Security Manager by entities from the context assessment.
To remind, the assumption is that user roles and locations based on the everyday life of the person are defined in the configuration phase. Also in this phase rules for high and low-level context are defined by an authorised person together with the rules for personal information depending on the application.

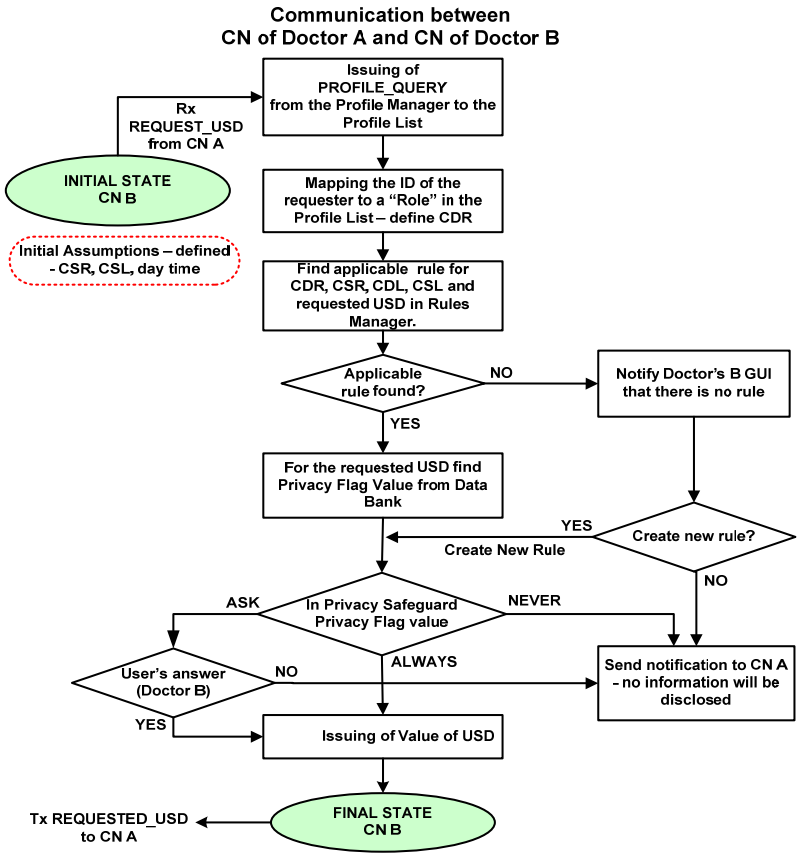


Figure 21: Selection of applicable profiles and rules

5.3.6. Summary of Section 5.3

The approach taken in this work for controlled information disclosure is a mix between the role- and policy-based. Therefore, the Profile and Rules Agent plays a major role in the privacy protection framework.
The proposed profiles are for objects (devices, persons and their roles), context, application/service and scenario. Each profile has a template that basically is an empty profile.
The system is also able to define the current role of the person-based context information for the current GPS coordinates or relative indoor location and then map it to a meaningful location for the person. Examples of descriptive roles for the reference scenario are: patient, family member, friend, doctor, nurse.
The profile for the Context is for Vital Function, Indoor Location, Outdoor Location, and Environment.
The application type could be for example Enhanced Professional Communication, Emergency Localisation for the pervasive healthcare applications.
The service profile is considered to be part of the context. It contains information for the types of the following parameters: the requesting party, the requesting location, the domain types (medical, entertainment, sport, etc…), interaction type (one-one/one-many), location accuracy requested (different levels of granularity – exact GPS coordinates, room, building, street), requested identifiable user parameter (ID, exact user name, pseudonym, label name), service duration (short, medium, long).
In the Scenarios Profiles, a list of most common scenarios for the daily life of the user is stored. The scenario is defined as a combination of Role and Location of the source and destination of the data.
Last but not least, the Rule Agent is an important component of the privacy protection framework. Each rule is function of the scenario, the context attributes, conditions to be satisfied, USD, results and actions. There are rules for low and high level context data. This controlled information disclosure mechanism considers the current scenario and context in order to find the applicable rule for disclosure. How the applicable rule could be selected is presented on Figure 21.

For the different categories of nodes, as presented in Section 4.6.1, different versions of the Profile and Rules Agent are applied. The most complex agents are for full-functional nodes.

5.4. Addressing scalability and power efficiency

5.4.1. For information and context privacy

How much memory and power resources are necessary for the controlled information disclosure mechanism depend on the required level of granularity in the implemented versions of the profiles and rules. Scalability is ensured with the options to implement very simple rule engine with 10-50 applicable rules and which consider 3-6 context attributes in resource constrained nodes. For the gateway and coordinator nodes which have more important role in policy negotiations and which must consider more complex context, rule engine with 200 rules and 20 current context attributes might be envisaged. However, even in this case, using compression of the data will reduce the memory needed but will increase slightly the energy consumption and the response time.
Power efficiency will depend highly on the specific scenario and on the desired user preferences too - if the users would like to have protection of their personal data and if they would like to have their anonymity and location privacy ensured.
In these aspects, ensuring anonymity, location privacy and pseudonyms creation are the processes which will require most computation and communication overhead. Moreover, the location privacy solutions in many cases require cooperative behaviour which also leads to increased communication overhead.

5.4.2. For information confidentiality

Several factors may affect the benefits achieved in practice by the introduction of the flexibility property in the confidentiality algorithm. One of them is the processing versus communication power. In previous studies, it has been shown that energy costs of data transmission far outweigh the costs of computation (e.g. [12]). For the suggested method of varying the number of rounds and key size for RC5 encryption, this may have some effect on the computation cost but will have no effect on the data transmission costs. Therefore, the benefit may not be of very big significance in practice. Another issue is that many scenarios require integrity more than encryption protection, and therefore in practice nodes may have to constantly apply integrity protection, but may sometimes not have to use encryption. Adding integrity protection increases the message size by more than encryption and may even require more computation (e.g. 5.9μJ/byte for SHA-1 compared to 1.62μJ/byte for AES encryption as measured in [12]. Therefore, the benefit of being able to switch encryption on and off may be insignificant compared to the overall cost caused by having to use integrity protection at all times. This is presented in [13].

5.4.3. Summary of Section 5.4

To summarise, the framework is *flexible* in order to allow for different versions of it to be deployed for a coordinator or gateway node and a small sensor node, given that they have both different hardware limitations, and communication and security requirements. The framework is *adaptable* in order to allow for different protocols and primitives to be applied after deployment for the communications within the nodes of a BSN, and the communications between cluster heads and gateways.
For information and context privacy, scalability is ensured with the options to implement very simple rule engine with 10-50 applicable rules and which consider 3-6 context attributes in resource constrained nodes. For the gateway and coordinator nodes which have more important role in policy negotiations and which must consider more complex context, rule engine with 200 rules and 20 current context attributes might be envisaged. If ensuring anonymity, location privacy and pseudonyms is a scenario and user requirement, this will lead to less power-efficiency since this will require most computation and communication overhead.
For information confidentiality, for the suggested method of varying the number of rounds and key size for RC5 encryption, may have some effect on the computation cost but will have no effect on the data transmission costs.

Bigger effect could be achieved if encryption is switched on and off if acceptable from the scenario and user requirements.

5.5. Applicability to the reference scenarios

In the previous chapter, the ACAPP framework and its components were described in detail. The goal of this section is to give examples of how the proposed concepts and mechanisms could be applied in practice. First, the interaction of BSN with foreign networks is described. Three cases will be considered: BSN in a public place, in home and in a hospital. Further, the configuration guidelines for the Rule Agent are followed and the reactivity of the Security Manager to change of context is described in order to provide working examples for two applications.

In accordance with the example scenarios selected to demonstrate the ACAPP Framework, example configurations for the security framework will be provided for:

- A BSN of the reference scenario (backup shift assistant) - rules for health status and for notification
- A BSN of the reference scenario (backup shift assistant) - rules for localisation

5.5.1. Interaction of BSNs with foreign networks

In Section 3.2, the scope of the proposed solution was presented. One of the communication scopes was with nodes of trusted subscribed networks or occasional communication with nodes of unknown networks.
In the following paragraphs it will be shown how the Security Manager functions in these two communication scopes.

Case 1: Outdoor scenario (In a public place)

This is the case when there is communication with nodes of unknown networks. It is the scenario which is exposed to most security threats as presented in Section 3.3. Interference is a possible threat not only from the same type of sensors but also from all other available wireless services and networks. Confidentiality is a major requirement too. It is assumed that the network is always in this case and it only can be changed if a connection is established successfully with another network.
This is a typical scenario that requires high level of security. The management of the security parameters by the Security Manager is presented in the following Figure 22.

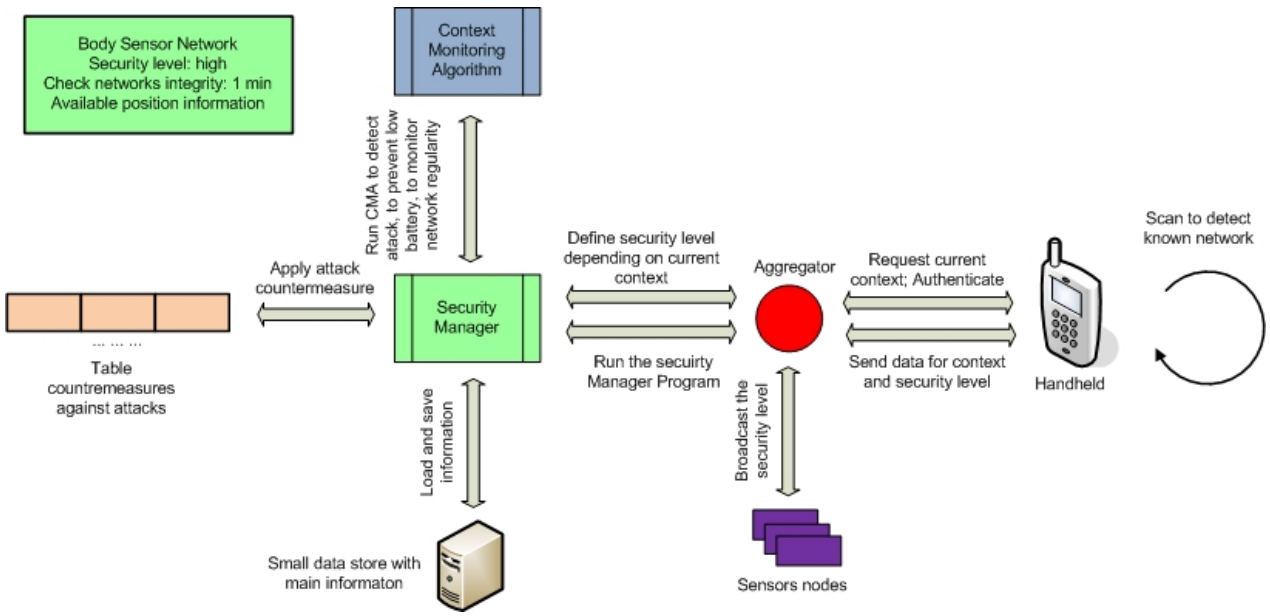


Figure 22: Outdoor Scenario (In a public place)

Case 2: Home scenario

This is the case when there is communication with nodes of trusted subscribed networks.

It is the scenario exposed to least security threats because it is a controlled environment. Confidentiality is not a main concern here between those who live in the house (assuming a family house). Authentication for each user can be done easily because they are few, in a family house typically about 5 people or even less. Taking all these factors into account for this type of location, low level of security for the BSN is selected.

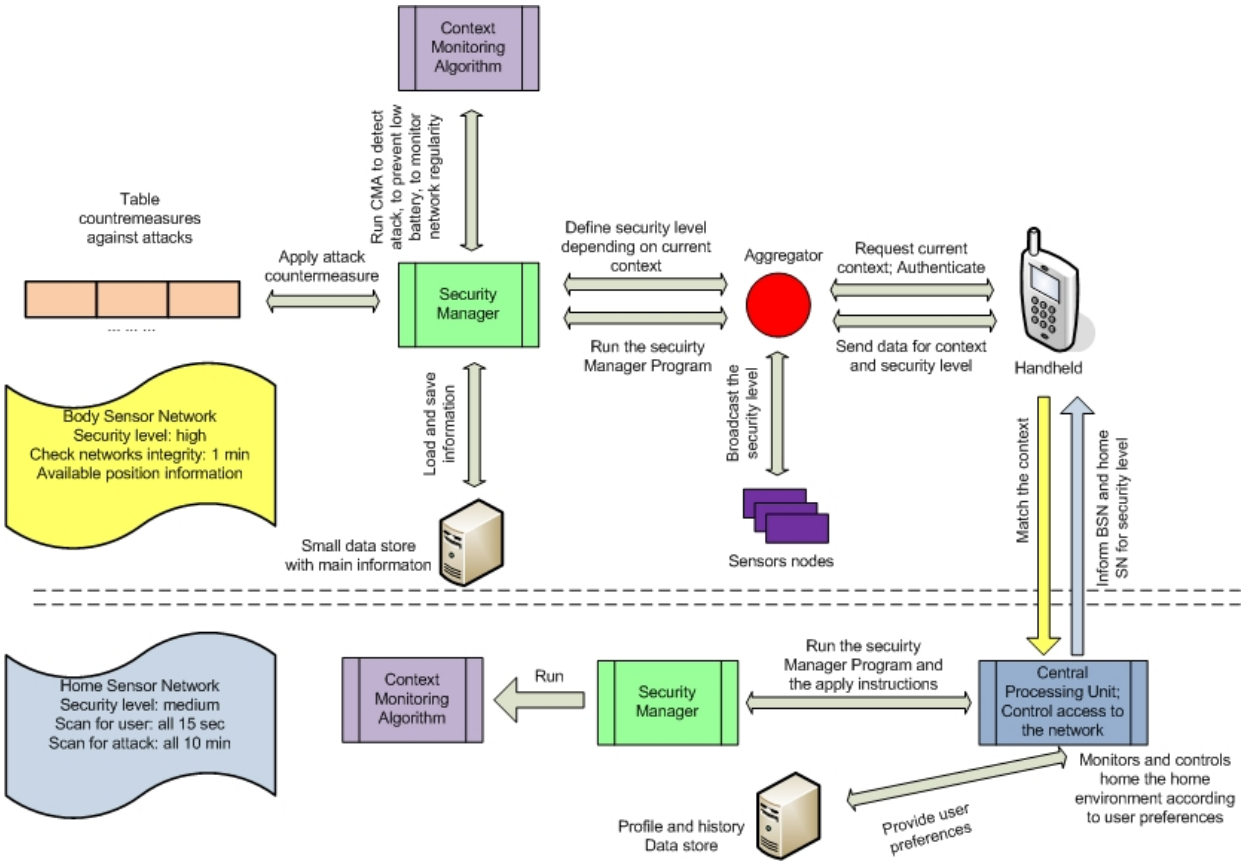


Figure 23: Home Scenario

The office scenario can be seen as staying in a "foreign house", i.e. the users are still in a trusted environment but now the environment is only partially controlled by them. In this scenario the system uses the medium level of security. The use of the office network to provide an alternative for the mobile phone may also be applied, in case of shortage of battery power for example.

Case 3: Hospital scenario

This is the case when there is communication with nodes of trusted subscribed networks too.

The Hospital scenario has an interesting particularity; in this case many BSNs will be near each other, which may cause problems regarding authentication procedures and interference. Having this in mind, it is proposed the use of the medium level of security to be used. The Power Management Algorithm of the end-sensor nodes will have a very important task in this scenario. It has to control precisely the transmitting signal power of the sensor nodes so that interferences may not occur.

In this scenario there might be the need to add more sensors to the existing BSN. This task should only be done by the hospital staff and with extreme caution because the keys will be exchanged for the first time and it is necessary to make sure it is performed with the right sensors. The figure would be the same as above for the home

environment, except that instead of Home sensor network on the right side, it is the Hospital sensor network with assumptions: the security level is high; scanning for attack: all 5 min; scanning for user: all 5 sec.

Other scenarios could be analysed with more details but it is considered that these three scenarios allow for a good representation. However, some other ubiquitous networks can interact with the BSN, for example the patient's car network. In this case, the patient's vehicle can be used to improve the transmission/reception quality and there could also be some interaction between the body and the BSN. In the case when while driving, the patient suffers some kind of attack, the BSN could deliver this information to the car's processing unit, which in return would activate an emergency procedure, e.g. turning on the emergency lights or decreasing the car's speed to a complete stop, etc.

5.5.2. Configuration of the Profiles and Rules for providing adaptability

In Section5.3, the profiles for nodes/devices, user, scenario and context, and services have been defined. In a pre-deployment phase, the devices are loaded with a set of pre-defined profiles and rules, corresponding to multiple policies, which allow the initialisation of the device as soon as it joins a network, making it possible the insertion of it in any type of network.
Once the device has been deployed, it needs to be guaranteed the adaptability of the policies in the different situations which might arise, as the security protocol, and hence primitives, are selected according to the context of the communication, taking into account the trade-off among device constraints and context itself, as well as user's preferences.

In this section the profiles and rules that the Privacy and Security Agent use for providing adaptability, after the network deployment, are given. These rules are necessary in order to decide which security level to apply depending on the context and to help the system to operate without intervention and to adapt to the changing contexts. There are groups of rules corresponding to different context events, for example – health status rules, notification rules. More details are provided in the rest of this section.

Backup Shift Assistant Scenario – rules for health status and for notification

Health Status Rules
Among all the possible contexts, the following three context events are considered: "normal", "pre-emergency" and "emergency" which describe the health status of the patient. The measurements from the different body sensors provide summarised picture of the collective information for health status. It is possible to define them through four parameters (thresholds) for each context data presented in Section 5.3.2: two thresholds are used for delineating when the patient is in an emergency case (above U-ETH, or below L-ETH), and the four of them are used instead to define the "pre-emergency" case, as depicted in Figure 24.
It is assumed that for the "normal" context, the initial security levels for all the security services are high, as if that the end-user is in public place. This is Case A as described in the previous section.

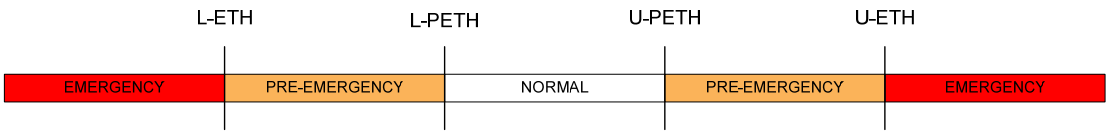


Figure 24: Rules for definition of the health status of the patient

In the following Table 33, rules for determining the security levels accordingly to the change of context are given:

	Initial security levels				Final security levels			
Security services / Change of context	A	E	I	F	A	E	I	F

Normal→pre-emergency	H	H	H	H	H	M	H	M
Normal → emergency	H	H	H	H	H	L	H	L
Pre-emergency → normal	H	M	H	M	H	H	H	H
Pre-emergency → emergency	H	M	H	M	H	L	H	L
Emergency→ normal	H	L	H	L	H	H	H	H
Emergency→pre-emergency	H	L	H	L	H	M	H	M

Table 33: Determining the security levels according to the change of health status

Notification rules

"Notification rules" are rules that, based on the context information, notify a certain category of person (medical staff, family or both) of the present heath situation of the user/patient. In the following Figure 25, it is showed which category is alerted in case an emergency or pre-emergency situation happens.

Figure 25: Rules for notification based on health status of end-user

Battery Level Rules

Further need of notification rules arises when the battery level is reducing, as depicted in the following Figure 26. In this case, the battery level, and not the status of the patient, represents the context information. This case has been mentioned in Section 4.8 where the Context Management Algorithm was described.

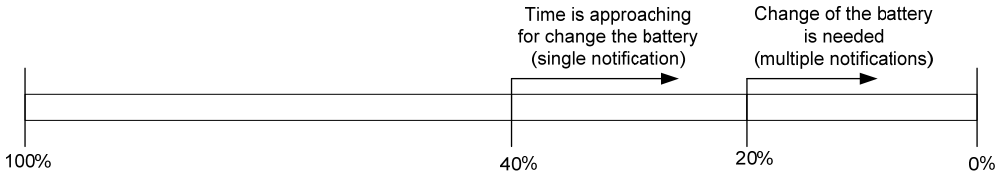


Figure 26: Rules for notification based on status of battery

Examples of other privacy rules (low and high level) for medical staff are presented in Section 5.3.5.

Backup Shift Assistant Scenario – rules for localisation

In the previous section, for the backup shift assistant scenario, it is described low level rules for the notification of the status of the user/patient, as well as basic rules that show how the security service are changing according to the change of the status of the patient. These rules are still valid in the case of change of localisation, in the Backup Assistant scenario. Furthermore, rules concerning the localisation of the user must be added, in order to have the medical staff and the user's family aware of user's location when it is required.

When the health status of the patients is "normal", the security levels of the security services change according to their location as depicted in the following Figure 27. In this case the context information is a combination of the health status and the user's location.

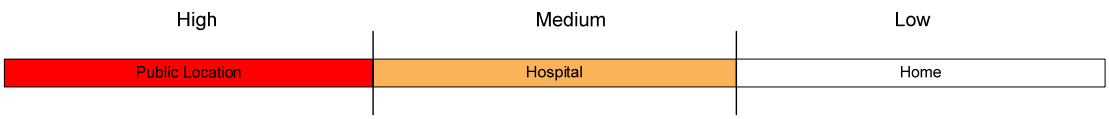


Figure 27: Rules for security levels depending on different locations

High level rules are a combination of low level rules as explained in the following examples:

IF {“location=public” AND “time=evening” AND “context=pre-emergency”} THEN {“notify the relative of the position of the user”}

IF {“location=hospital” AND “time=night” AND “context= emergency”} THEN {“notify the doctor for the health status of the patient”}

Flow charts for change of Security Level

The following flowchart (Figure 28) explains how the security level in the coordinator node (CN) from a BSN is changing based on a change in context (in this case the context is location and it is changing from home to public). Figure 29 explains the change in the security level in the end-node (EN).

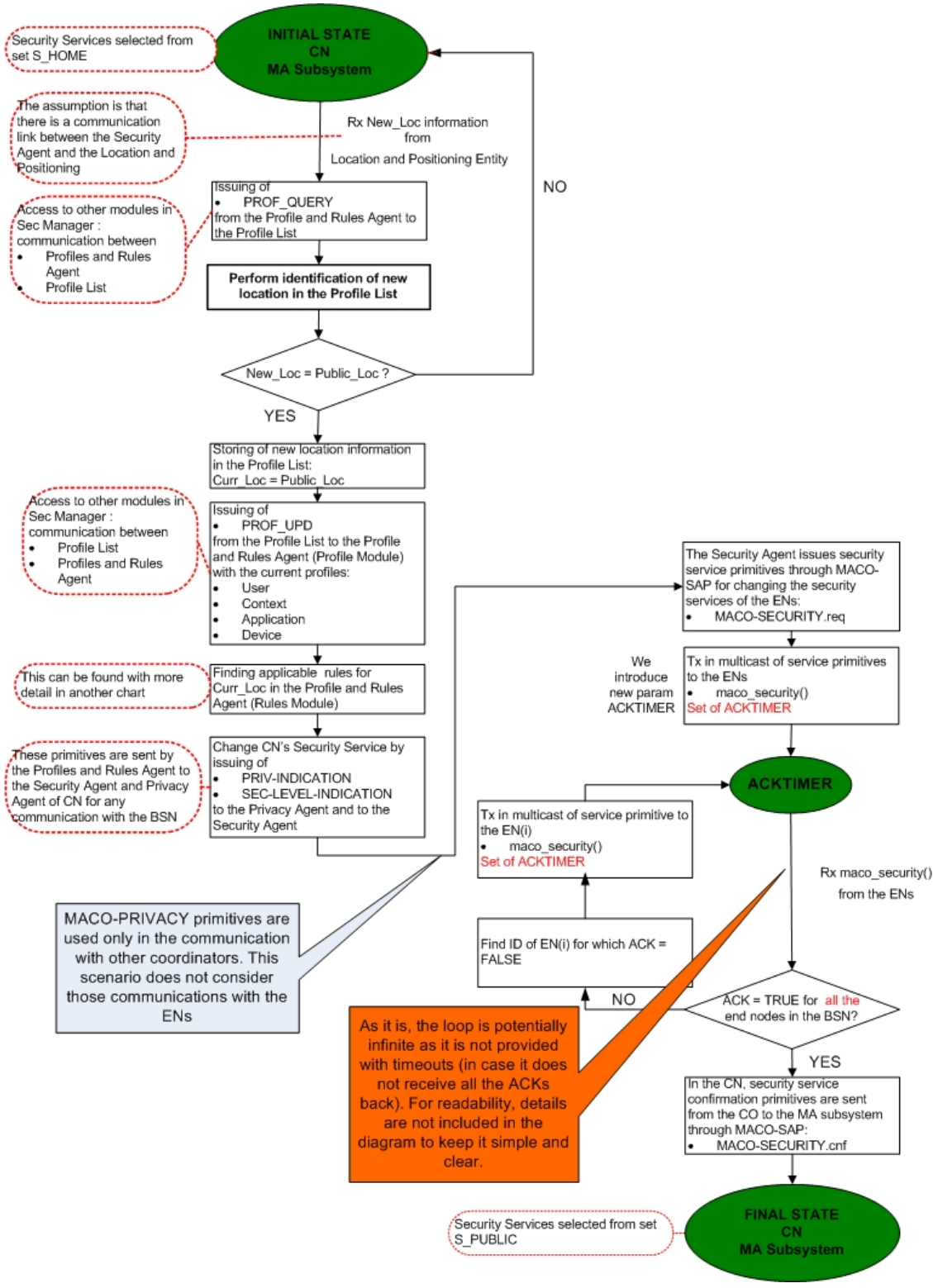


Figure 28: Change of security level in the coordinator node from a BSN based on a change in context

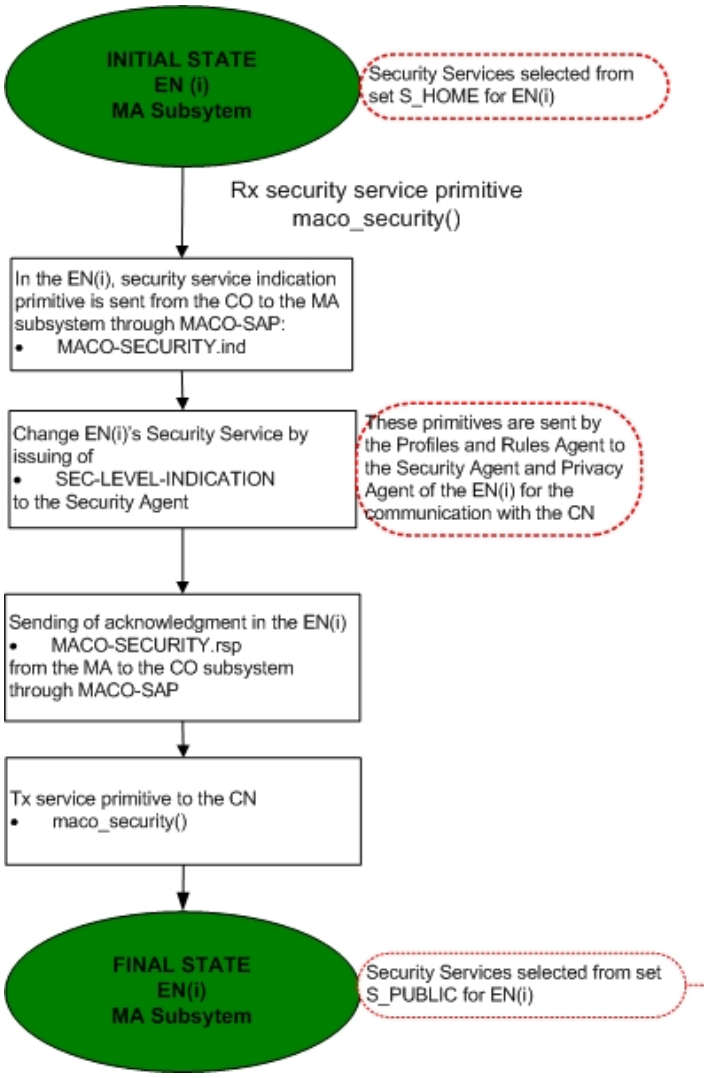


Figure 29: Change in the security level in the end-node from a BSN based on a change in context

5.5.3. Summary of Section 5.5

To show how the security and privacy framework could be applied in practise, examples for outdoor, home and hospital scenario were presented. It was explained in detail the behaviour of the Security Manager when a change of one the context attributes is happening – namely, change in location.
Furthermore, configuration examples for the profiles and rules for the reference scenario were presented – for health status, for determining security levels when the health status of the end user changes and when the location changes. In the end of the section, it was shown how the security level is changed in the different subsystems of both in the coordinator and the end-sensor node.

5.6. Comparison with existing solutions

The focus of this section is to position the proposed solutions in this thesis with existing ones. The Security Manager is compared with SPINS and CodeBlue. The privacy protection framework is compared with PRIVES and with a privacy service for collaborative application using mobile phone. In the end, the profiling is compared with existing initiatives.

So far SPINS [14] is the most used protocol for security in sensor networks, therefore a comparison between the Security Manager and SPINS is the best way to present the innovations brought with the proposed here security protocol suite.
SPINS and the Security Manager rely on RC5 for the encryption/decryption process, however in SPINS the key is generated through random numbers based on a MAC function, while in the Security Manager this key is obtained with the ECC. This also implies that in SPINS all keys depend on a secret master key while in the proposed security protocol suite all keys are independent and uncorrelated.

Table 34 presents the main characteristics of these two protocols:

	SPINS	**Security Manager**
Encryption/decryption algorithm	RC5 in CTR mode	RC5 in CTR mode
Authentication procedure	MAC function	ECC-DH
Freshness	Weak freshness provided by the CTR encryption	Weak freshness provided by the CTR encryption
Strong freshness	Use of nonces	Not implemented
Adaptability	No	Yes
Low Overhead	Yes	Yes
Reduced latency (Use of flags)	No	Yes
O.S.	TinyOS	TinyOS
Broadcasting	µTESLA	No specific protocol
Power management	No	Yes

Table 34: SPINS vs Security Manager

As it is possible to see from the Table 34, several new features were added, specially the adaptability and power management and a new authentication procedure was developed in order to ensure an improved security. With the use of flags a new mechanism to fight latency was introduced, which is important for communicating of measurement of vital signs.
The ECC-DH requires more computational time than the MAC function which means that the proposed security protocol suit spends more energy in the authentication procedure. However, since this process is only performed every 4 hours and with the energy saved from the adaptability and power management features, the whole mechanism fully compensates this event.
Detailed analysis of the proposed security protocol suit and performance evaluation is presented in Part D of this report.

5.6.1. CodeBlue and the Security Manager

CodeBlue [15][16] is a project which uses WSNs for medical care, such as pro-hospital, in-hospital emergency care, disaster response and stroke patient rehabilitation. Comparison between the proposed security protocol suit and the requirements/characteristics of CodeBlue follows in the next paragraphs.
Regarding vital information, CodeBlue and some of its references [17] recommend a sample rate of one second. The proposal in this report has a standard sample rate of 10 seconds for vital sensors. However two additional sample frequencies could be introduced without major modifications. Having the possibility to get a sample every 5 seconds or every second, clearly satisfies that recommendation.

Let us imagine that a doctor wishes to monitor the patient's heart rate every second because the patient is in a critical state. The doctor only has to send this instruction to the patient's aggregator node which will then send a request to the specific sensor node to increase its sample rate. The aggregator also has the task to alert the CMA that the sensor in question will send a larger number of messages then previously expected (the number doubles for a 5 seconds sample rate and is multiplied by 10 for a single second sample rate). In this way, the whole system adapts itself to the new circumstances. It should be kept in mind that the 10 seconds was stipulated having in mind the increase of the sensor nodes' lifetime (regarding energy consumption). It is also possible that the increase of the sample rate in the case of emergency is pre-defined in the Rule Agent. In this situation it is not

even necessary that the doctor sends a special request for this to the coordinator node, this will be done automatically. These rule settings could be done in the "emergency" rule group.
Regarding emergency responses, a new feature is introduced in the protocol suit. While the exchanging key procedure is running, an emergency situation should imply a response. To face this situation flags are used, i.e. all the bits are set to "1" if an emergency is detected. In this way, the aggregator easily detects a top priority message and overrides any other procedures that are still running.
Another significant difference between the proposal here and CodeBlue relies on tracking issues. In this proposal the GPS location is only sent when it is detected an abnormal situation either of the patient or the network. In CodeBlue this information is sent every 15min, no matter what. Seen from the point of view of the proposed privacy framework this violates the patient's privacy and stimulates an adversary to hack the system in order to easily track the patient's movement (location). The solution from this report does not endanger the patients and it keeps their privacy intact.

This current proposal clearly satisfies the requirements imposed by the medical scenarios even in emergency cases and once more proves itself as a good alternative to existing protocols.

5.6.2. Privacy Frameworks

Related work addresses complete architectures as well as domain specific privacy solutions.
In [18] the authors propose a pre-configurable policy-based framework for protecting and sharing private data for automotive telematics. Similarly, but for protecting context information in context-aware environments, the authors of [19] define a privacy service that grants or denies access to the context data based on predefined policies. Both approaches focus on developing means to define and use tailored policies for their frameworks adapted to the respective use case.
In [20] Bessler and Jorns propose an extension to the Parley X architecture [21] to let users create own pseudonyms. Further they propose a pseudonym creation scheme – PRIVES – that can be used to create similar pseudonyms at different locations with only a single key exchange. The chain of pseudonyms is created using a combination of HMAC and SHA.
Within the PRIME project, architecture is developed to support private use of the Internet across Europe. As outlined in [22], the system architecture incorporates novel cryptographic protocols, sophisticated security protocols, and artificial intelligence algorithms for privacy protection for the digital world.

5.6.3. Existing Initiatives for Profiling

The OSGi™ [23] specifications define a standardised, component oriented, computing environment for networked services. Adding an OSGi Service Platform to a networked device (embedded as well as servers), adds the capability to manage the life cycle of the software components in the device from anywhere in the network. OSGI's User Admin Services use database with user information (private and public) for authentication and authorisation purposes.
UPnP [24] enables simple and robust connectivity among stand-alone devices and PCs from many different vendors. There are standardised service descriptions for the Device Security and Security Console.
Although OSGI and UPnP provides means to not only deal with, but also to handle profiles for devices' and services', they do not provide any direct means to manipulates users' profiles, where essentially the entire user's sensitive data can be located. In particular if the users' sensitive data is separate of any of the devices' or services' profiles, there are no means for the system (OSGI and UPnP) to make decision concerning their protection (security, privacy and anonymity) without direct specific request from the user.
The Rights Expression Language, MPEG REL [25], is intended to provide flexible, interoperable mechanisms to support transparent and augmented use of digital resources in publishing, distributing, and consuming of digital movies, digital music, electronic books, broadcasting, interactive games, computer software and other creations in digital form, in a way that protects digital content and honours the rights, conditions, and fees specified for digital contents. Also it provides a flexible interoperable mechanism to ensure personal data is processed in accordance with individual rights and to meet the requirement for Users to be able to express their rights and interests in a way that addresses issues of privacy and use of personal data.

The Web Ontology Language (OWL) [26] is designed for use by applications that need to process the content of information instead of just presenting information to humans. OWL can be used to explicitly represent the meaning of terms in vocabularies and the relationships between those terms. The ability of the Semantic Web to link information from multiple sources is a desirable and powerful feature that can be used in many applications [27]. However, the capability to merge data from multiple sources, combined with the inferential power of OWL, does have potential for abuse. Users of OWL *should be alert to the potential privacy implications*. A number of organizations are addressing these issues with a variety of security and preference solutions. See for example SAML [28] and P3P [29].

5.6.4. Summary of Section 5.6

In this section, comparison of the Security Manager with SPINS, CodeBlue, other privacy frameworks and profiling initiatives was presented.
The difference with SPINS is in the authentication procedure - the Security Manager uses a security protocol suit which is a combination of ECC-DH while SPINS uses MAC function. Security Manager has adaptability and reduced latency features. Adaptability is very important for the pervasive application space which allows applicability for diverse scenarios. Reducing latency is vital for transmission of health status parameters.
CodeBlue is a system for emergency response, with recommended sampling rate of 1 sec. Since the pervasive health care systems will have main goals to help rehabilitation at home or just transmitting health status to care personnel, in this proposal sampling rate of 10 sec is used, which gives possibility for power and battery savings. However, in case of emergency, there is always the option the doctor to request sample rate of 1 sec as in CodeBlue project. Another difference is that in CodeBlue project, GPS location is sent every 15 min, which according to the presented in this PhD report threat analysis, violates the location privacy of the treated subject.

5.7. Summary of Chapter 5

This Chapter 5 presented in details the proposed privacy protection mechanisms. As for adaptive confidentiality, the proposed security protocol suit uses RC5 and DHA-ECC. Variation of parameters of RC5 defines deferent levels of confidentiality. To avoid the heavy computation of DHA, ECC was proposed for the key exchange.
The main operation in elliptical curve cryptographic schemes is point multiplication. This operation presents the most desired properties in cryptography, i.e. the forward operation is quite simple but its inverse is very difficult. The main characteristics of Diffie-Hellman still persist in this method.
Second, the context-aware mechanism for controlled information disclosure was presented. To allow for personalisation and context-awareness, the access control is based on a combination of profiles and rules. The access control itself is filtering of user sensitive data before any disclosure and this is done with the help of the Privacy Safeguard. Other important block of the framework was described – the Profile and Rules Agent, with the defined profiles of user, context, application, scenario. The framework allows for scalability and power-efficiency.
In the end, the applicability of the proposed mechanisms to the reference scenario for outdoor, home and hospital locations was exemplified. The mechanisms were compared with some existing solutions - SPINS, CodeBlue, other privacy frameworks and profiling initiatives.

References

[1] X. Luo, K. Zheng, Y. Pan, and Z. Wu, Encryption Algorithms Comparisons for Wireless Networked Sensors, IEEE International Conference on Systems, Man and Cybernetics, Volume 2, October 2004

[2] S. Fluhrer, I. Mantin, and A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, Eighth Annual Workshop on Selected Areas in Cryptography, Springer, 2001.

[3] http://www.dns-ny.com/encrypt.htm

[4] http://www.bibmath.net/crypto/complements/courbelliptique.php3

[5] The elliptical curves, http://www.bibmath.net/crypto/complements/courbelliptique.php3

[6] Hans Eberle, Vipul Gupta, Sheueling Chang, Nils Gura, "**Securing the Web with the Next-Generation Public-Key Cryptosystem"**, Sun Microsystems Laboratories, SNRC Industry Seminar, October 14, 2003.

[7] Sheueling Chang, Hans Eberle, Vipul Gupta, Nils Gura, "**Elliptic Curve Cryptography – How it Works"**, Sun Microsystems Laboratories

[8] Anelia Mitseva, Mohamad Imine, Neeli .R. Prasad, **"Context-Aware Privacy Protection with Profile Management",** In proceedings of WMASH 2006 (The fourth ACM international Workshop on Wireless Mobile Applications and Services on WLAN Hotspots), pp. 53-62 (ACM Press), September 29, 2006, Los Angeles, USA in conjunction with MobiCOM 2006

[9] A. R. Beresford and F. Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing, Volume 2, Issue 1, January 2003, pages 46-55.

[10] Andreas Pfitzmann and Marit Hansen: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Version v0.27, February 2006.

[11] Mitseva, Anelia; Gerlach, Matthias; Prasad, Neeli R. **Privacy Protection Mechanisms for Hybrid Hierarchical Wireless Sensor Networks.** In Proc. of 4th International Symposium on Wireless Communication Systems, Trondheim, 2007. ISWCS 2007. IEEE, 2007. pp. 332-336

[12] E. Aivaloglou, S. Gritzalis, C. Skianis, "Towards a flexible trust establishment framework for sensor networks", Telecommunication Systems Modeling, Analysis, Design and Management 35 (3-4), Springer, 2007, pp. 207-213

[13] Aivaloglou, E.; Mitseva, Anelia; Skianis, C.; Gritzalis, S.; Waller, A.; Prasad, Neeli R.., **Scalable Security Management for Wireless Sensor Networks for Medical Scenarios,** In Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007, pp. 1014-1018, Dec 2007, India

[14] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. Tygar, "**SPINS: Security Protocols for Sensor Networks**"

[15] Anu Bhargava and Mike Zoltowski, "Sensors and Wireless Communication for Medical Care".

[16] **Detection classification, and tracking of targets**, IEEE Signal Processing Mag., vol. 19, pp.17-29, March 2002.

[17] Th. Arampatzis, J. Lygeros, S. Manesis **"A survey of Applications of Wireless Sensors and Wireless Sensor Networks"**. In proceedings of the 13th Mediterranean Conference on Control and Automation, Limasso, Cyprus, June 27-29, 2005.

[18] Sastry Duri, et al. "Data protection and data sharing in telematics, Mobile Networks and Applications", Volume 9 Issue 6, December 2004.

[19] Vagner Sacramento, et al. "A Privacy Service for Context-aware Mobile Computing". First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), pp. 182-193.

[20] Sandford Bessler, Oliver Jorns, "A Privacy Enhanced Service Architecture for Mobile Users," In Proceedings of PERCOMW, pp. 125-129, Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05), 2005.

[21] *The Parlay Group*, URL: http://www.parlay.org, accessed 2. Sept. 2004.

[22] Jan Camenisch, et al. “Privacy and identity management for everyone”. Workshop On Digital Identity Management, Proceedings of the 2005 workshop on Digital identity management.

[23] OSGi Alliance, http://www.osgi.org/

[24] UPnP™ Forum, http://www.upnp.org/

[25] REL: http://www.contentguard.com/MPEGREL_home.asp

[26] OWL, http://www.w3.org/TR/owl-features/

[27] Integration Applications: http://www.w3.org/2002/07/swint

[28] SAML: http://www.oasis-open.org/committees/security/charter.php

[29] The platform for privacy preferences 1.0 (P3P1.0): http://www.w3.org/TR/P3P/

Chapter 6
6. Analysis and Evaluation

The main goal of Chapter 6 is to present the analysis for the proposed work. It further discusses the evaluation of the ACAPP Framework and the proposed mechanisms, starting with presentation of the evaluation goals and continuing with the results of the performed evaluation. It presents the costs of the privacy protection enhanced with adaptivity, context-awareness and security management. It further evaluates the security management and the adaptive confidentiality.

6.1. Analysis of the proposed framework and mechanisms

In the following subsections it is analysed how the introduced adaptive and flexibility features influence the functionality of the proposed adaptive framework and the presented in this PhD thesis mechanisms. The adaptivity feature of the security framework will be first analysed. Then this proposal is compared with some existing solutions. Further, the context-awareness in the privacy protection framework will be discussed. In the end of this section factors which might influence the savings and the efficiency from the adaptive security and the context-aware privacy protection will be analysed.

6.1.1. Adaptive Security

The following Table 35 gives overview of the parameters and features which have been discussed in the previous sections. It presents the aim with maintaining them and what the specifics and measures are. The most important from them is considered to be power consumption, security adaptiveness and a number of extra features.

Parameter/Feature	Aim	Specifics/Measures
Power Consumption	To preserve the maximum of battery level, several measures could be taken	- reduction of the transmission power - adaptation of the security level - reduction of the number of the sent message
Identification Delay	The first time the user or the administrator configures the network and the profiles of devices manually. Next time this is done automatically	The use of access control list is a simple way for this.
Transmission Adaptiveness	For best system performance, the system needs to do a smart transmission of data from one network to another	It takes about 10 sec for the aggregator node to collect data. After that it does an intelligent filtering. If the information is vital/important, it transmits directly. Else it transmits with an interval of several minutes
Security Adaptiveness	To maintain the integrity of the system, specific requirements are defined depending on the type of security attack	General case ->Attack detected ->Increase Security Intrusion detected->Revoke the keys; Request for ID and Pre-distributed key Jamming or interference->Increase frequency hopping Overflow->Revoke all keys, reboot the system DoS attack-> Restart/Block all foreign networks; Increase the security level Compromise of a node-> Shutdown/Revoke the key's user; provide feedback to the user on the display and update the database

Extra features	Optimisation: Creation of a back up solution	The control could be taken by a PDA or a laptop in case the coordinator node is out of battery
Extra features	Security: the choice of the algorithm is important in order to manage the authentication and the integrity of the system to protect the privacy of the user	The proposed security protocol suit ECC-DH&RC5
Extra features	Reactivity: warn the user or a medical personnel as soon as an anomaly is detected	Implementation of a warning algorithm

Table 35: Analysis of important parameters of the adaptive security and privacy framework and some extra features

Comparison of the proposed adaptive security protocol suit with SPINS was presented in Section 5.6.
Several new features were introduced with the presented proposal, specifically the adaptability and power management and a new authentication procedure was developed in order to ensure an improved confidentiality. With the use of flags a new mechanism to fight against latency was introduced, which is an important option for measuring and communicating vital health signals. In this respect it could be considered that the proposed mechanism for adaptive confidentiality to be an evolution of the SPINS protocol.
The proposed here protocol suit is applicable for a diverse applications than SPINS since it flexible and can be easily adapted, a connection with a trusted network is done automatically (after the first session), the users may create their own profile in order to increase the interaction between networks and also they may be warned of some critical events and it provides optimal functionality for the current combination of situation, context and environment.
However, The ECC-DH requires more computational time than the MAC function which means that WSNs using this proposal will spend more energy in the authentication procedure. However since this process is only performed every four hours and with the energy saved from the adaptability and power management features, the mechanism compensates this event.

6.1.2. Vulnerabilities according to the security levels

From the presented in Section 4.8 Security Manager it could be observed that by decreasing the level of security the protection of the network is reduced. But what exactly does that mean? Does the whole network become more vulnerable?
In the following paragraphs it is analysed to which attacks the network is more susceptible when the level of security decreases. However, it must be underlined that the level of security is only decreased because it is assumed that the users are in a trusted environment, i.e. there is another system to detect intrusions.

When the level of security is changed, two parameters change: the key length in the ECC-DH and the number of rounds in the RC5 algorithm. By decreasing those parameters the network is more vulnerable to all attacks related to compromised keys such as:

- Packet injection (malicious packets);
- Sinkhole attacks (if the adversary is able to impersonate the aggregator);
- Denial of Service;

It is not easy to predict and even more difficult is to quantify which attack is more likely to occur. However the goal in this section is to try to estimate the probability of each attack, having in mind two factors: the time it takes to break the key and the easiness to implement such an attack.

From the three possible attacks presented above, the easiest one is the Denial of Service (DoS). Although the proposed security protocol suit prepares the system to count the number of messages of a certain sensor and to

check if they correspond to the expected number, this procedure is only done once a minute for vital sensors. Between these periods the adversary is free to send all the packets at once, i.e. the aggregator node receives in one moment what it was supposed to receive in one minute. If only one key is compromised this may not be a big problem. However if more keys are compromised, then the aggregator may be overflowed with packets, causing DoS. For simplicity and in order to study the worst case it is assumed here that the compromise of one sensor is enough to cause DoS.
The packet injection is intimately related with DoS but in this case the focus is specifically to malicious packets. This attack is more challenging than the DoS because the aggregator node (through the Security Manager) expects a certain type and size of message from each sensor. Therefore, the adversary needs to have enough expertise to deceive the aggregator and make it accept a packet which contains a malicious code (virus).

The hardest attack to perform is certainly the Sinkhole attack. The adversary has to break all the keys and then impersonate the aggregator, i.e. he has to gather enough resources to create signal at least as strong as the one provided by the real aggregator. If the adversary successfully achieves these requirements he is able to lure all the traffic to it and then it only needs to send deceiving information to the real aggregator to make it believe everything is working properly. This is by far the worst scenario possible. The adversary has access to all the information inside the compromised network.

In order to quantify the probability of success of these attacks, "weights" are estimated which relate to the time it takes to break the key and how easy it is to perform the attack.
The total probability is calculated by the product of the probability to break the key and the probability to succeed of each attack:

Equation (5) $$P_T = P_{key} \times P_{attack}$$

The following Table 36 and the chart from Figure 30 present the evaluation:

	Probability to succeed an attack			**Total Probability (succesfull attack) * (Key breaking)**		
Attack Type	Low level	Medium level	High level	Low level	Medium level	High level
DoS	0.8	0.8	0.8	0.4	0.12	8.E-03
Packet Injection	0.5	0.5	0.5	0.25	0.075	5.E-03
Sinkhole	0.1	0.03	0.002	0.05	0.0045	2.E-05
break key (P_{Key})	0.5	0.15	0.01			

Table 36: Analysis of the System Vulnerabilities

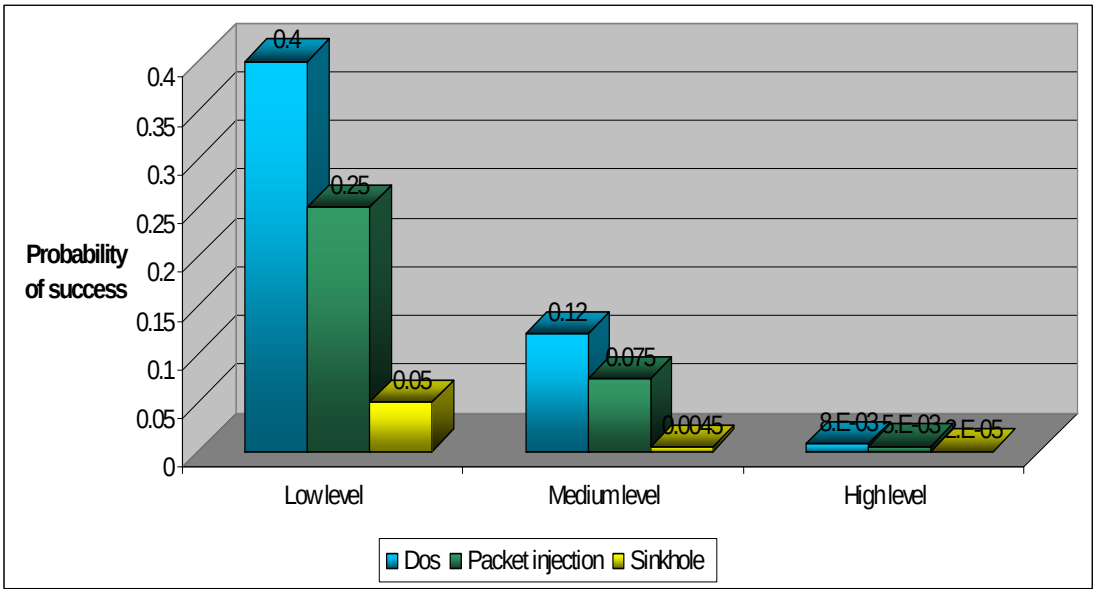


Figure 30: Probability of success for the three attacks in each level of security

As it is possible to see from Figure 30, in the high level of security these attacks do not present a threat. However in the low level of security caution must be taken because the probability to succeed one of these attacks is significant. ***From this analysis could be concluded that the user or the administrator must carefully choose which places should be considered as trusted, when setting up the system***.

It should be underlined once more that these results do not take into account the level of trust of the user's location. The purpose of this section is to present the vulnerabilities of the system regarding the security parameters of each level of security. Also these values are a rough estimation based on the characteristics of the attacks and the time to break the key.

6.1.3. Privacy Protection and Context-awareness

In many design situations where the user directly interacts with the systems, the KISS principle (Keep it simple stupid) is considered. But with respect to implementing the privacy safeguard, breaking the KISS principle might be worthwhile, because even with increased complexity, this will give the control in the hands of the end-user and will increase the users' satisfaction and their confidence in using pervasive systems. And this is to fulfil one of the main user requirements listed in Section 3.2 and therefore it is expected that the user will be more willing to pay for the offered services.
At the same time, fulfilling the requirement for pre-defined rules is essential to reduce the setup and labour maintenance costs.
Adaptability is ensured with the services offered to the end-user or the network administrator to create new profiles and rules, to edit or delete existing ones.
Another important factor to be considered is the processing vs. communication costs. In the privacy protection, when the privacy safeguard mechanism for controlled information disclosure is discussed, it does not influence the communication overhead. It is more the internal processing, on which the power is spent. On the contrary, providing pseudonymity and anonymity makes influence on the computation and transmission because of the cost of computing and communicating a new pseudonym or estimating the current anonymity level.

In the reference scenario, very diverse context information is considered as input to the policies and rules for the privacy protection mechanism. For example, the considered context on one hand is directly related to the end-users and supporting them in their interaction with the flexible system. On the other hand – context data for the applications and for the environment are also necessary. They are all essential for the privacy mechanisms and the Rule Module to work properly. The more context attributes are considered, the more reactive and autonomous the

system could be. But this of course comes with the cost of increased complexity. The vulnerability and uncertainty coming from providing the context from a third party, must be also kept in mind.

Previous studies [1] have shown evaluation of a context-aware privacy service for mobile computing considering some context linked to the end-user's mobile device. However, when evaluating such a complex flexible system as the one proposed in this report which considers applications with sometimes opposite requirements, it is obvious that the number of the context attributes taken into account will increase significantly. This will lead to expanding the number of the rules applicable for certain scenarios. On the other side, since the deployed end-sensor nodes will also have very different set of memory and computational characteristics in comparison with the coordinator and gateway nodes, the number of rules and context attributes must be scaled-down for these resource constrained nodes.
In order to address the scalability requirement, the influence of the complexity of the context attributes in the work of the Privacy Agent as part of the security services, must be evaluated in terms of response time vs number of context attributes; response time vs number of applicable rules; memory requirements for different sets of rules. Furthermore, it is good to perform a comparative evaluation of different number of context attributes and different number of applicable rules. The main challenge here will be to simulate the context in a realistic way. All these evaluations are presented in the next subsections and could serve as a guideline when designing scalable versions of the Privacy Agent.

6.1.4. Factors influencing the savings from the adaptive security and privacy framework

In Section 4.5 an adaptive and flexible security framework for WSNs has been described that allows for the provision of sophisticated, unobtrusive, context-aware applications and services. Memory, storage space and processing power are severely limited on some nodes, and this has been addressed by allowing the framework's components to be simplified or even left out according to each individual node's capabilities and roles. For example, the simplest nodes could implement policies as 'if-then-else' statements, whereas more capable nodes requiring sophisticated policy management can implement policy databases, and even expert systems. Battery lifetime can be an issue for some nodes, and this is particularly affected by communications overhead. This overhead will be increased by the need to send trust management messages, and perhaps to distribute policy updates. Such messages will be infrequent. However, future work will need to look at their impact and potential optimisation. Having said that, the adaptability that the framework provides, may lead to significant savings in battery power. Without this adaptability, the standard security approach often provides the highest level at all times to protect data. In practice, several factors may affect the benefits from the security framework achieved. Some of the relevant factors for the lightweight security mechanisms could be [3]:

- Processing versus communication - For the suggested method of varying the number of rounds and key size for RC5 encryption, this may have some effect on the computation cost but will have no effect on the data transmission costs. Another issue is that many scenarios require integrity more than encryption protection, and therefore in practice nodes may have to constantly apply integrity protection, but may sometimes not have to use encryption.
- Cost of other functionality on the node - The computation and data transmission costs of performing security are just some of the costs incurred by wireless sensor nodes.
- Overheads from security management - Frequent security level changes and trust evaluation operations incur communication overheads, while privacy safeguard mechanisms incur processing overheads. On the other hand, the security parameters may be communicated by piggy-backing on other messages, which will reduce some of the costs.
- Implementation cost – The complexity and cost for the configuration of the Security Manager components can be high for deployments with a large number of highly diverse nodes but it is expected to be low for BSNs with just a couple of end-sensor nodes .
- Required lifetime of nodes and difficulty in replacement - Security Manager's functionality may be preferred for nodes that cannot receive regular maintenance or cannot be replaced.

- Dynamicity of scenario - Mobile nodes need the extended Security Manager version in order to adapt within a dynamic environment, with the received benefits depending on the frequency of environment changes.

6.1.5. Summary of Section 6.1

From the analysis presented in this chapter could be seen that the proposed adaptive security framework and the security protocol suit could be seen as evolution of SPINS with the power management, the extra adaptivity features and suitability for a bigger number of scenarios.
In this thesis different security levels have been proposed to achieve power savings – low, medium, high with a corresponding set of suitable mechanisms. The lower the security is, the bigger the vulnerability of the system is. With low security level, the possibility to succeed DoS attack or packet injection is not neglectable, as seen from the analysis. Usually the low security level could be applied when the persons is in trusted environments. However, it was noted that the trusted environment must be carefully selected.
Overall, introducing privacy protection framework and context-awareness requires to some extent involvement of the user. It enhances the functionality with offering pre-defined profiles and features but it might be complicated for some groups of users (for example very old persons or disabled) if they want to change the initial settings. Another perspective is that the users must make informed decisions and this could be difficult if they are not aware of the threats for privacy.
Finally, some of the factors influencing negatively the savings introduced from the adaptive security and privacy framework could be implementation costs, overheads from the security management when frequent security level changes are needed. Furthermore, if anonymity is a requirement, calculation of new pseudonym increases the computation costs.

6.2. Performance evaluation for the proposed privacy protection and context awareness

This is one of the final chapters of this thesis. Here it is presented the performance evaluation of the proposed adaptive context-aware privacy protection framework starting with definition of the evaluation parameters and the aims and the methodology of the evaluation and then the chapter is finished with the results themselves.

6.2.1. Evaluation parameters

In the flexible architecture of the ubiquitous systems, the nodes from BSN and the environment have diverse computational, memory and power capabilities and different roles in the network (such as gateway, coordinator, end node) as described in Section 4.6.1. The privacy protection mechanisms for the applications spaces with heavy end-user involvement, described in Section 5.2, must be scalable (i.e. having extended, scaled-down and lightest versions) and "fit" in the different types of nodes where necessary and the system must handle them without e.g. the processing burden exceeds the resources. Therefore, to evaluate the *scalability* of the context-aware privacy protection, a set of maximum number of context attributes and rules have been defined, which can be processed by a node belonging to a certain resource class:

- *Maximum number of different context attributes* directly related to a certain application space, the status of the user and the surrounding environment – all these are included in the conditions for the policy-based privacy protection
- *Maximum number of different Low and High level rules,* necessary for building up the reasoning to support the privacy protection of the users' private data and their lifestyle and any other necessary information, defined as sensitive by the user themselves

To remind*, Flexibility* is defined in terms of

- The rules, policies and profiles support the work of all involved parties – in the reference scenario, these are both health professionals and care subjects
- Provision of personalised control for different levels of privacy protection

6.2.2. Privacy Protection Simulator

The test bed for the Privacy Protection and Rule Management Simulator was Pentium 4 - 2.4 GHz with memory of 512 MB using Java in Windows XP environment. The demo program for the GUI was also written in Java. The GUI consisted of two main windows which represented User side and Requester side. Figure 31 below shows a snapshot of the demo program – the user and requestor window.

There are three buttons on the window of the requesting party to simulate a scenario:

- RESET button - It is used to reset the display.
- DISPLAY button

  It is used to display the requested user profiles after sent by the user.

  If the corresponding flag for particular user profiles are *never*, then the information will not appear.
- REQUEST button - It is used to send the requested user profiles to the user

The User Window displays the requested user profiles with their corresponding flags. It also shows the requester and his location. *The Current Rule ID* form shows the ID rule for particular scenario (in this case is Pt01, which indicate *Doctor* in *Hospital* is asking for user profiles of *Patient* who is at *Home*.

There are two buttons on the User Window:

- REFRESH button - It is used to display the current requests
- REPLY button - It is used to send the requested user profiles

In case there are some user profiles which have *Ask*, a new window will appear to ask the user whether those user profiles are allowed to be revealed to the requester, as illustrated in the Figure 31 above. The figure shows that for user profile *full_name* have *Ask* flag, thus a new window appears to ask the user whether it is allowed to be revealed.

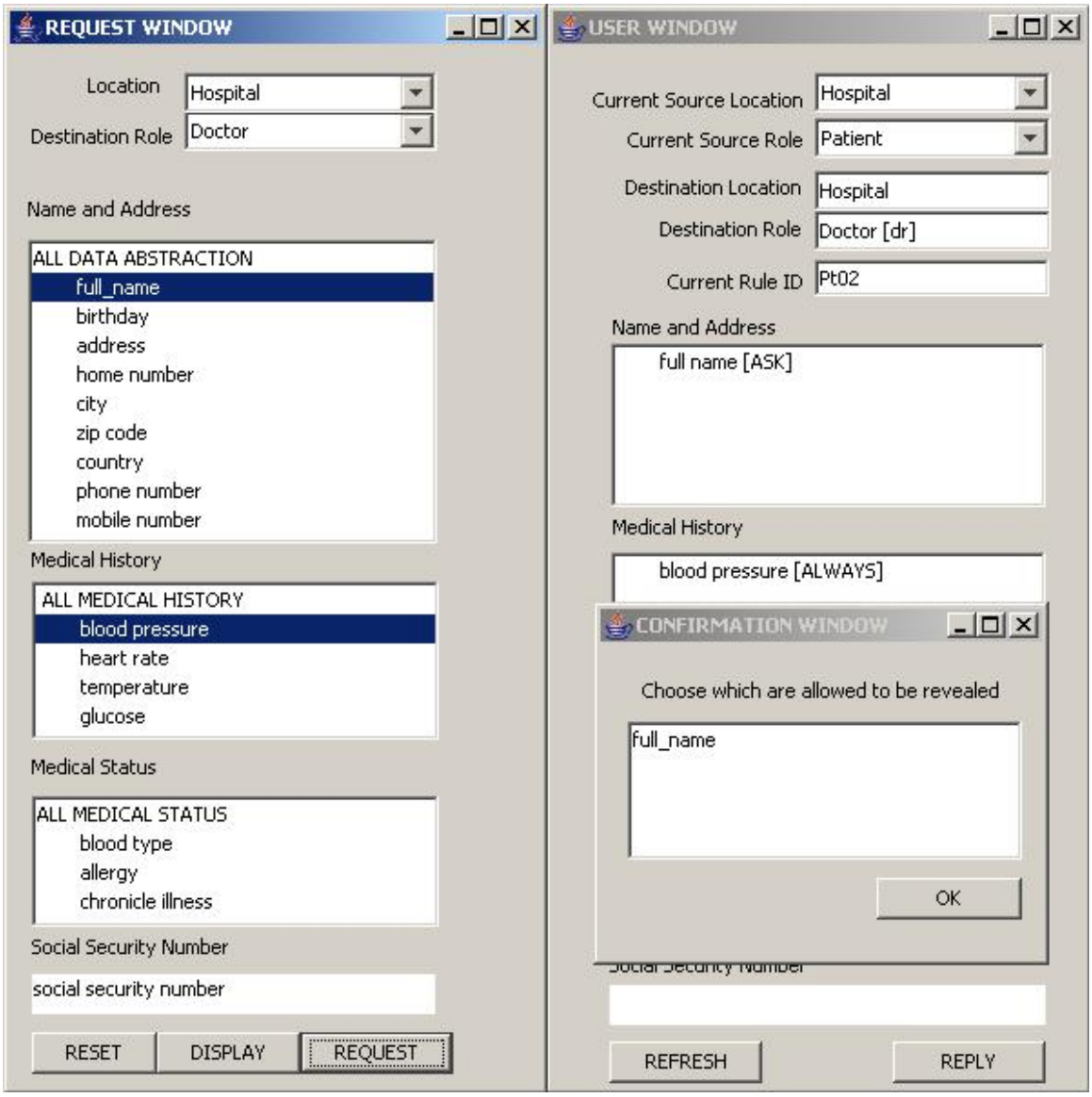


Figure 31: GUI for Privacy Protection Simulator

6.2.3. Aims and Methodology

In order to adapt the ubiquitous system for a specific service in a specific set-up, it is desirable that the system designers have clear frames and guidelines about the possibilities and the limits of the systems they want to build and/or to set-up. Important decisions for a trade-off in resource-limited nodes could be taken through selecting only vital rules and context attributes as explained in Section 5.3.5, which represented the ones related to functions of the system vital for the end-user. A bottom-up approach could be followed: once the system set-up ensures these vital functionalities, additional features covering less vital functionality could be build-up if the resource class of the node allows this.
Two main aspects of the assessment of the scalable context-aware privacy protection are in focus:

Aspect A - the influence of the complexity and granularity of the context information on the performance of the Rule Agent is considered and
Aspect B - the evaluation of the implication of the Privacy Safeguard mechanism is investigated.

As said, aspect A concerns the rule analysis. The main factors which influence the decision-taking depend on:

- How efficient the model of the rules is
- The percentage distribution of rules for low vs. high-level context attributes
- The relationship among attribute granularity, rule complexity, response time
- The overall number of rules and distribution of rules per requested user sensitive data

When it comes to the influence of the complexity of context, important parameters are the overall number of considered context attributes, the average number of context attributes per scenario, the average number of context attributes per rule.
As for the Aspect B, the main performance parameter of concern is the delay (or the response time) caused by the filtering: the difference depends on if the USD, subject to filtering, is on the high-level or it is on finer-grained level (attribute granularity, where for each grain of attribute data there can be a different rule).
All the above mentioned evaluation parameters are essential to find out which the optimal complexity of the Rule Agent is and optimal number of context attributes to be considered for designing scalable and flexible systems, as well as for setting each possible particular set-up.
Indirectly, the format of the rules and the way they are accessed and stored influence the memory usage. Example of how the memory can be affected: "Are the stored rules compressed or not?"; "How many bites/bytes are needed to store each rule or all the rules?"; "Do the coding/decoding of the rules affect the time response?"

The proposal in this report is based on the belief that in order to decrease the delay caused by processing a request for USD and to reduce the influence of the dynamic context change, only applicable rules must be processed. *Applicable rules* (APLR) are defined as a subset "S" of *all the possible rules* for a certain domain, based on everyday activities and common logic (ALLR). The subset "S" takes into consideration certain well defined but limited number of *context attributes* (CATR) where each attribute have a well defined granularity. More detailed examples of such rules are provided in Section 5.3.5.
The proposed approach for the context-awareness is proactive – and the mechanism evaluates the current context and identifies the corresponding subset "S" of most probable applicable rules which apply for the current situation. Then, when a query for USD comes, the number of rules to be searched has been already reduced since only the applicable rules for the current context are selected beforehand. In the examples of the rules which have been defined, the higher the number of context attributes and their granularity has been considered, the lower the number of applicable rules related to the total number of possible rules, normally is. This is because a smaller number of rules have conditions that allow incorporating many contexts.
The considered use case is the back-up shift assistant from the wireless hospital. In the simulations, four situations based on SL (source location) are defined with 200 meaningful rules, with the following percentage distribution per location:

- 23% for home
- 31% for office
- 30% for hospital
- 16% for public places

For this investigation, location is selected since the rules for this low-level context attribute are linked to the rules for high-level context (for example current source role, current situation). Additionally, Figure 32 presents the distribution of applicable rules per requested USD, seen from the patient's perspective in the mentioned reference scenario.
The context awareness of the privacy protection the simulations depends on 10 context attributes directly related to the current status of the individual. They are considered the most important context information for the care of the subjects: DL (destination location), DR (destination role), SL (source location),

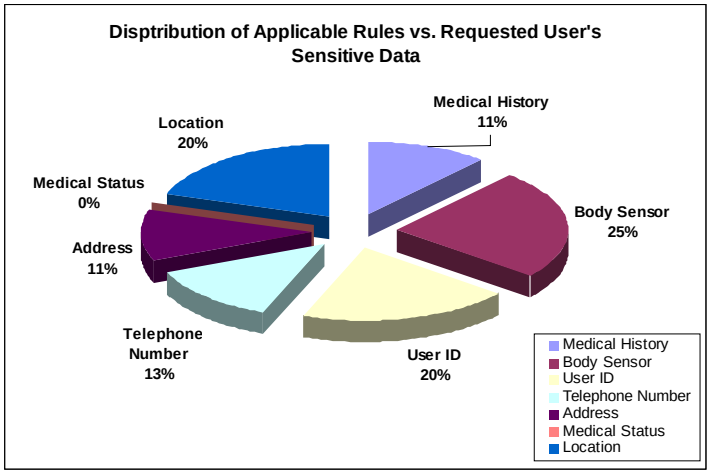


Figure 32: Percentage Distribution of applicable rules per user sensitive data

CSR (current source role), DAY (day of the week), TIME (time of the day), DEV.TYPE (type of sensor node), DEV.READING (reading of the sensor node), DEV.BATTERY (battery status of the sensor node), EVENT (overall status of the person: normal, emergency, pre-emergency).

In the simulations, the investigation is made respectively with

Cases	Number of context attributes	Types of context attributes
Case A	the first three context attributes	DL (destination location), DR (destination role), SL (source location)
Case B	the first six context attributes	DL (destination location), DR (destination role), SL (source location), CSR (current source role), DAY (day of the week), TIME (time of the day)
Case C	all ten context attributes	DL (destination location), DR (destination role), SL (source location), CSR (current source role), DAY (day of the week), TIME (time of the day), DEV.TYPE (type of sensor node), DEV.READING (reading of the sensor node), DEV.BATTERY (battery status of the sensor node), EVENT (overall status of the person: normal, emergency, pre-emergency).

Table 37: Types of context attributes considered in the simulations

6.2.4. Cost of the controlled information disclosure

The evaluation of the context-aware privacy protection is done via:

- The Rule Agent – evaluation of: rule distributions; time to process the rules; finding the most appropriate rule for a certain scenario
- Introduced delay from the privacy safeguard algorithm, which is defined as the time necessary to filter the requested USD
- Efficiency of the proactive approach in reply to the dynamic nature of context changes – reducing the delay when a subset S of the rules relevant only for the current context are extracted.

The performance of the privacy protection for scalable versions of the Rule Agent was evaluated. Rule distribution is shown in Figure 32. The *Response time* in this discussion is defined as the time from placing the request for the USD until it is filtered by the privacy safeguard; requested data is found and ready to be processed further according to the decisions from the privacy protection. Simulation scenarios for 50, 100, 150 and 200 APLR and 3, 6 and 10 numbers of CATR have been tested.

To optimise the performance, the subset S of the applicable rules depending on the current context (state of the system, the subject, location and environment), could be efficiently re- allocated and accessible in the memory, so that the response time is decreased.

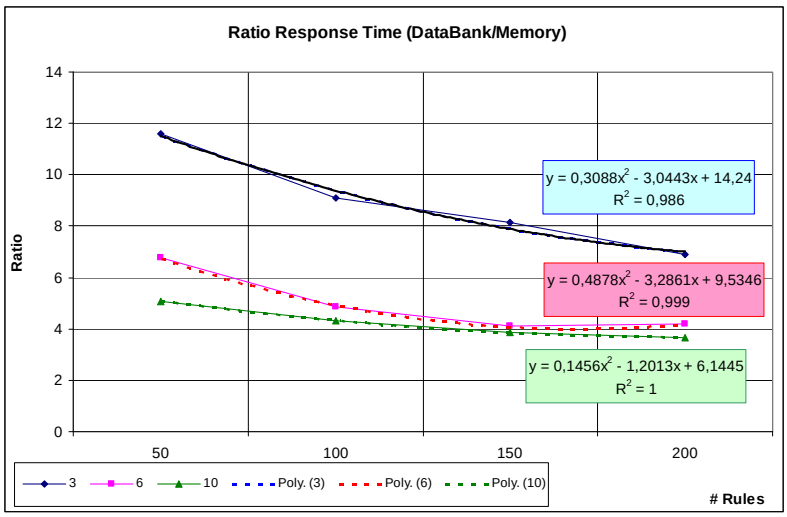
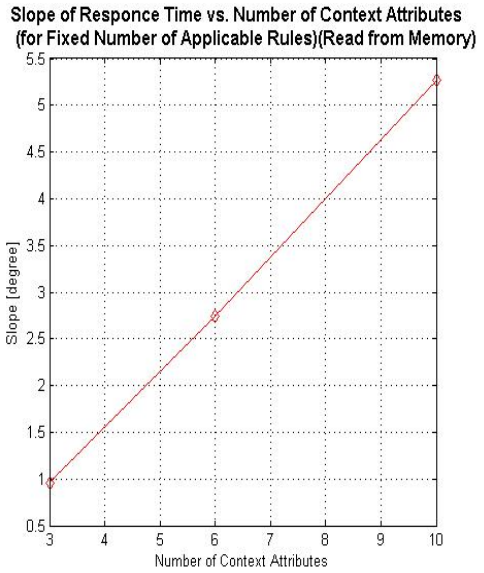


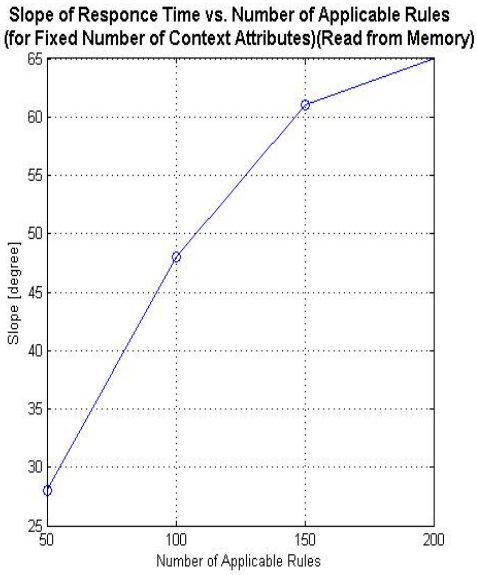
Figure 33: Ratio of the response time - read from file vs. read from memory [6]

How efficient is this optimisation in terms of reduction of the response time is investigated with a ratio *R= (read access DataStore/read access memory).* The difference is in the value of the response time: when *all* the rules are stored in a file in the Small Data Store and all of them are searched or when only the applicable rules for current context are stored in the memory. The limit asymptote of the curves of ratio R of 6 and 10 context attributes (Figure 33) is around the value 4 for more than 120 applicable rules and no significant difference exists between the two cases. In the contrary, there is a ratio R asymptote limit of value 7 in the case of a curve of 3 attributes and 200 rules.

Figure 34 a) illustrates how the response time for different number of APLR depends on the semantic richness of the context while Figure 34 b) shows its dependence on the number of the applicable rules. The slope gives view of how fast the increase of the response time is with respect to the increase of the number of CATR or the number of APLR.



a)



b)

Figure 34: Slope of Response Time vs. Number of Context Attributes (a) and vs. Number of Applicable Rules (b) [6] [7]

6.2.5. Summary of Section 6.2

The performance evaluation for the privacy protection and context-awareness was performed with two aspects in mind: to evaluate the influence of the complexity and granularity of the context information on the performance of the Rule Agent and to evaluate the implication of introducing the Privacy Safeguard mechanism.
The first aspect concerns the rule analysis. The main factors which influence the decision-taking depend on the efficiency of the rule model; the percentage distribution of rules for low vs. high-level context attributes; the relationship among attribute granularity, rule complexity, response time; the overall number of rules and distribution of rules per requested user sensitive data. For the second aspect, the most important evaluation parameter is the delay caused by the filtering.
The simulations have shown that having proactive approach for selection of a set of applicable rules in reply to the dynamic nature of context changes, optimises the performance and reduces the delay from the filtering. The results show that there is no big difference in the ratio of read from data store in comparison to read from memory, when six and ten context attributes are use and with over 120 rules. The slope of the response time vs number of context attributes (up to 10 attributes) is linear.

6.3. Performance evaluation for the security management and adaptive confidentiality

In this chapter performance evaluation for the security management and for the adaptive confidentiality is presented. First the evaluation parameters are listed; then the assumptions are presented and further down the gains in power savings and the cost of the proposed solution are presented.

6.3.1. Evaluation Parameters

The performance evaluation of the security management and adaptive confidentiality is done against the following parameters:

- Processing time
- Message frequency
- Power savings
- Memory usage
- Trade off between energy savings and security levels

These parameters have been selected because they are of special concern for sensor nodes with very limited power, memory and processing capabilities. Message frequency plays also important role since the more messages are transmitted, the more power is consumed. It is of interest to see what the maximum message frequency period is which is acceptable for the pervasive health-care applications. Last but not least, the different security levels were introduced in order to save power. Investigation of the trade-off between security levels and energy savings could show what could be expected in terms of prolonged battery time when lower security levels are applied.

6.3.2. Security Management Simulator

The GUI of the Security Manager Simulator purpose is to provide a user friendly tool to replicate the procedures it have been proposed so far for some typical events that may occur in wireless sensor networks in the discussed reference scenarios.

The program was written in C++ and with Borland's C++ builder which allows the use of a Win32 application. Part of the code used in this application (the RC5 and ECC) was based on The Security Simulator **Fejl! Henvisningskilde ikke fundet.**.
The main goal of this simulator was to show the adaptability of the proposed theoretical solution. It should be clear for the user that the level of security is dynamic, which also means that both the authentication and encryption mechanisms are adjustable according to the context. Since this is a simulation tool, there is no a real interaction between the SCM (Security Manager Simulator) and the sensor nodes.
With the help of this program the period of time each procedure takes could also be measured. This information is extremely important to have an idea of what will be the computational time if these procedures were done in the sensors. Which actions are triggered when the user presses the buttons of the interface, is shown on Figure 35.

For the test bed, a computer with the following properties has been used:

- Processor Frequency : 540 MHz
- Processing unit : 32 bits

In the real case, the sensor nodes taken into account are the MICA2dot with the following properties:

- Processor Frequency : 4 MHz
- Processing unit : 8 bits

Security Manager Simulator has the following key features:

- Ability to change the authentication parameters to increase/decrease the key length;
- Possibility to change the block length and the number of rounds in the RC5 algorithm;
- Possibility to use the RC5 for both authentication and encryption procedures;
- Tracks the time each process takes for further analysis;
- Displays all the actions/reactions of the Security Manager;
- Presents examples of encrypted/decrypted messages.

Functionalities of the simulator
In the following paragraphs it is explained what procedures are possible to be simulated with this tool. Since there is no real communication with sensors, therefore some of the functionalities within this program rely on the generation of random numbers. Through the following sections some assumptions are made:

Power Management

On the Action Window there are three buttons which belong to the Power Management section. These buttons represent the energy left in the sensor nodes' battery. In a real time application these context attributes are fed to the context assessment entity and by the Monitoring Algorithm which has the task to request it to the sensor nodes. In this case it is possible to choose 40%, 20% or 10% of battery life time.
If the 40% button is pressed, the Security Manager has to react, i.e. it has to detect the current status and report it to the user (through a mobile device's GUI – The privacy and Trust Assistant) so that the user has the knowledge of the current situation of the sensor nodes' energy. In this case there is the recommendation to schedule an appointment to fix the battery problem which is displayed on the user's window.
For the 20% and the 10% buttons, one key extra procedure exists. In these cases the level of security is decreased and for the 10% the low level of security is forced. The reason to impose the change in the security level is justified by the reduction of the computational time necessary for the authentication and encryption procedures, as it is possible to demonstrate with the alert window.

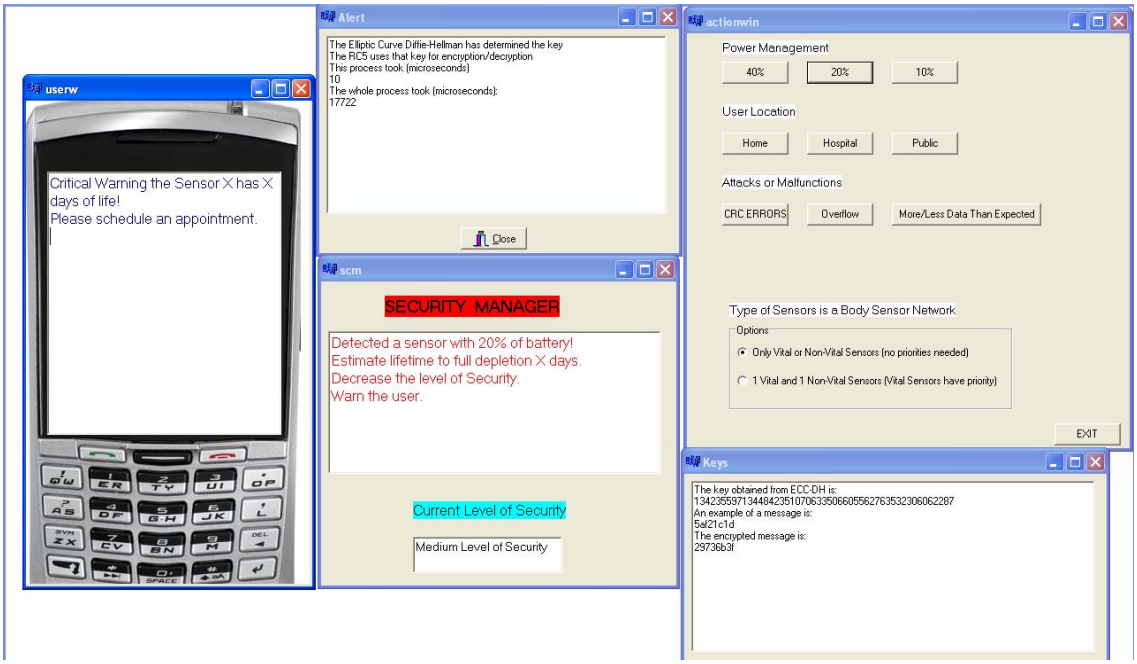


Figure 35: Security Management Simulator [4]

The User Location

This section of the simulator is dedicated to networks that "go along with the user" such as Body Sensor Networks. As it was proposed the level of security changes according to the level of trust some locations may offer. In this case low level of security is defined for the home scenario, the medium level for the hospital scenario and the high level for public places. These levels may be overrun with the power management instructions, i.e. if the batteries are at 10%, the low level of security could be forced. However if an attack is detected the level changes automatically to high. This is the best option because, even is the batteries are running out, it is not wise to keep the low level of security if the network is being a fragile target to an adversary. It msut be reminded that the user should never let the batteries reach such low levels of energy, therefore the "10% situation" must be a rare event. By default the system will always start with the high level of security.

For the home scenario, a message is shown on the GUI of the mobile device to alert the user that his home was detected, the security settings were changed and it opens the possibility for the BSN and the home network to interact. Then the user has to decide if he wants his BSN to connect to the home network. This option is only to avoid the situations when the user will only be at home for a very short period of time, e.g. to pick up something he forgot. For these cases it is not wise to change all the key just for a few minutes because that would imply to run the authentication procedure which is far more consuming then encrypt/decrypt messages using high level of security.

Attacks or Malfunctions

This is to simulate the response of the Security Manager program against the most common attacks a network may be victim of.

CRC Errors

Nowadays the use of wireless communications is quite common and since the spectrum is limited, interferences may become a major problem. Also jamming is a very common attack given that is very easy to do it. Since in the simulator program there is no a real communication with sensors, it is difficult to simulate this situation. The only thing done here is to use all the channels available in the sensor nodes (typically 20). If the aggregator/sensor

detects that the message has too many errors (incoherent data) it may be requested to change its channel until the problem is solved. To remind, this procedure uses code schemes to detect such errors.

Overflow
If an adversary is able to "get the aggregator's attention", i.e. if he is able to obtain a valid key that allows him to communicate freely with the aggregator, overflow or DoS is just one easy step away. Since the adversary was expert enough to "open a door" to get into the aggregator all key may be compromised. Therefore in this situation the countermeasure is the revocation of all keys and assigning new ones giving priority to the vital sensors (use of flags) and change the level of security to high. If the problem persists then the best option is to report this situation to the user and the hospital database in order to schedule reparation as soon as possible.

More/less data than expected
This is another attack/malfunction that it is not easy to simulate because the simulator does not use real sensors. The simulation relies on random numbers. In a real application the aggregator has a table with all the keys and the expected number of messages for each sensor during a certain period of time. If by some reason the aggregator receives more/less messages then expected, a malfunction is detected and it is easy to trace the source. The fisrt countermeasure would be to revoke the sensor key and renew it. If this process succeeds, it means the sensor is most likely to be working and it was compromised. If not, then the sensor is malfunctioning and this situation should be reported to the user and the hospital database.

6.3.3. Assumptions

To remind, for the test bed simulations a computer with 540 MHz was used and for the sensors, the parameters of MICA2dot have been considered with Processor Frequency 4 MHz.
For simplicity, it is assumed that there is a linear relation between the two processing units, which means that the MICA2dot sensor node is considered to be exactly 540 times less fast than the computer.

Since the only device that would have to deal with the flags is the aggregator node, the priority flag for the vital sensors in the authentication process would not be taken into account regarding battery consuming. Indeed, the aggregator has higher processing capabilities and higher batteries (however battery is not a really relevant issue for the aggregator node). Moreover, the purpose of the flags is to fight the latency because the goal is the messages from the vital sensors to be processed first. There is no power saving here, just priorities to make sure the system works properly and that the minimum number of messages are lost.

In the results described in the following part, it is assumed that the gain in processing time is equivalent to the gain of battery lifetime. In fact, in the sensor node, the processing unit is the only block of the device that consumes batteries. Memory is a passive block that is used by the processing unit and cannot work alone. The radio resources are not taken into account here because that is related with the frequency of the messages.
For example, if there is a gain of 16% of the processing time compared to the worst case, the assumption is that it is equivalent to a gain of 16% in the batteries lifetime, still compared to the consumption of batteries in the worst case. However, it does not directly mean that 16% of the total batteries lifetime will be saved in reality.

6.3.4. Gain in processing time and message frequency

First, the results as obtained on the computer during the simulation are displayed, and then the amount of time required to do the same operation with a MICA2dot sensor node is computed [4]. The values given for the time elapsed are defined as the mean values of 20 samples to be closer to real case.

		Security level		
		Low	Medium	High
	Key length	24	40	48
Computer:	Time elapsed for 1 key			
		9459	13980	14961

540 MHz - 32 bits processing unit	determination (in µsec)			
	Time Elapsed for 1 encryption (in µsec)	10	12	13
MICA2dot Sensor Node : 4 MHz - 8 bits processing unit	Time Elapsed for 1 key determination (in sec)	5,11	7,55	8,08
	Time Elapsed for 1 encryption (in sec)	0,0054	0,00648	0,00702

Table 38: Time elapsed for each level of security

Then, the time elapsed to process all the message encryptions and key determinations in one day could be computed, both for vital and non-vital sensors. The following Table 39 presents the results for one vital sensor:

For 1 vital sensor	**Security level**		
	Low	Medium	High
Message			
Message frequency (every X sec)	10	10	10
Number of messages encrypted in 1 hour	360	360	360
Processing Time in 1 hour	0:00:01	0:00:02	0:00:02
% of processing in 1 hour	0,03%	0,06%	0,06%
Processing Time for the message encryptions in 1 day	**0:00:46**	**0:00:55**	**0:01:00**
Key			
Key determination frequency (hh:mm:ss)	4:00:00	4:00:00	4:00:00
Processing Time to determine a key (hh:mm:ss)	0:00:05	0:00:07	0:00:08
Processing Time for the keys determination in 1 day	**0:00:30**	**0:00:45**	**0:00:48**
Full Processing Time in 1 day (hh:mm:ss)	**0:01:16**	**0:01:40**	**0:01:48**

Table 39: Time elapsed for each level of security - for 1 vital sensor

The following Table 40 presents the results for one non-vital sensor.

For 1 non-vital sensor	**Security level**		
	Low	Medium	High
Message			
Message frequency (every X sec)	60	60	60
Number of messages encrypted in 1 hour	60	60	60
Processing Time in 1 hour	0:00:00	0:00:00	0:00:00
% of processing in 1 hour	**0,0%**	**0,00%**	**0,00%**
Processing Time for the message encryptions in 1 day	**0:00:07**	**0:00:09**	**0:00:10**
Key			
Key determination frequency (hh:mm:ss)	4:00:00	4:00:00	4:00:00
Processing Time to determine a key (hh:mm:ss)	0:00:05	0:00:07	0:00:08
Processing Time for the keys determination in 1 day	**0:00:30**	**0:00:45**	**0:00:48**
Full Processing Time in 1 day (hh:mm:ss)	**0:00:37**	**0:00:54**	**0:00:58**

Table 40: Time elapsed for each level of security - for 1 non-vital sensor

The values for vital and non-vital sensor are linearly linked since the only parameter that changes is the message frequency. From this statement, in order to get a better idea of the power saving, taking into account the impact of the message encryption process, the results will be only focused on the vital sensors in the examples that will follow.

The results above do not show the gain of battery lifetime using the different levels of security, which is interesting to know. The highest level of security is taken into account as a reference; it is assumed there is no adaptive security in others solutions researched before, in order to advance the benefits of the adaptability of the discussed system.

1st case: always in low level of security [4]

Case 1: low level	Security level			
Vital Sensor	Low	Medium	High	Total
% of use	100,0	0,0	0,0	100,0
Time of working	24:00:00	0:00:00	0:00:00	
Processing Time	0:01:16	0:00:00	0:00:00	**0:01:16**
Time of working (if always high level)				**0:01:48**
Gain in processing time				**0:00:32**
% of power saved compared to high level of security				**30%**

Table 41: Case 1: low level

As seen from Table 41 above, this is the best case possible seen from poitn of view of time savings. It is assumed that the persons who wear the BSN stay the whole day in a trusted environment (their house on weekends, for example), it can be saved up to 30% of the battery lifetime during all the day.

2nd case: always in medium level of security [4]

Case 2: medium level	Security level			
Vital Sensor	Low	Medium	High	Total
% of use	0,0	100,0	0,0	100,0
Time of working	0:00:00	24:00:00	0:00:00	
Processing Time	0:00:00	0:01:37	0:00:00	**0:01:37**
Time of working (if always high level)				**0:01:48**
Gain in processing time				**0:00:11**
% of power saved compared to high level of security				**10%**

Table 42: Case 2: medium level

As seen from Table 42 above, if the end-users spend all the time in places where it is possible to use medium security level, it can be saved up to 10% of the battery lifetime during all the day.

3rd case: A typical day [4]

The assumption in this case is that the persons spend 50% of their time in places where low secrity level coul be allpied (for example 12 hours staying at home), 35% in places where medium security level could be applied (for example in the office for the working hours) and 10% (the rest) in public places.

Case 3: Typical day	**Security level**			
Vital Sensor	Low	Medium	High	Total
% of use	55,0	35,0	10,0	100,0
Time of working	13:12:00	8:24:00	2:24:00	

Processing Time	0:00:40	0:00:33	0:00:14	**0:01:28**
Time of working (if always high level)				**0:01:48**
Gain in processing time				**0:00:20**
% of power saved compared to high level of security				**19%**

Table 43: Case 3: Typical day

As seen from Table 43 above, for a typical day, it can be saved up to 19% of the battery lifetime during all the day.

6.3.5. Power savings

In the paragraphs to follow, the power savings of applying the adaptive security are analysed.

Low level of security

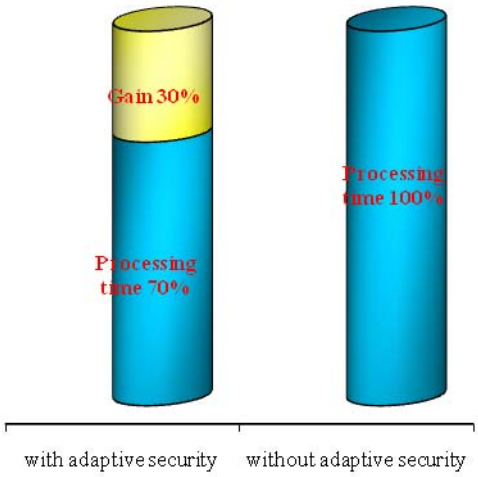


Figure 36: Power saving in low level of security

This case allows for biggest saving of the battery lifetime (up to 30%) but provides low security level in trusted environment. This is a typical case of a patient spending time at home.

Medium level of security

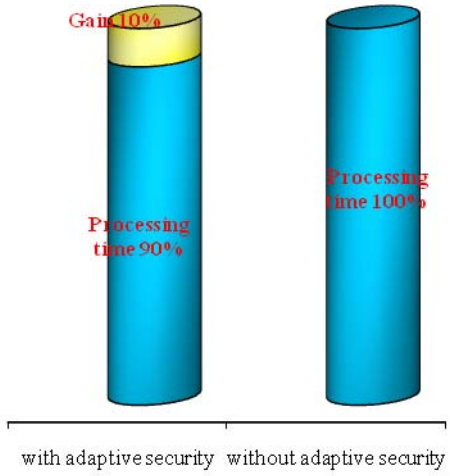


Figure 37: Power saving in medium level of security

This case allows a small saving of the battery lifetime and guarantees a sufficient security in partially trusted environment. This is a typical case of a patient in a hospital lying on his bed all the day. This level saves up to 10% of the battery lifetime.

Typical day

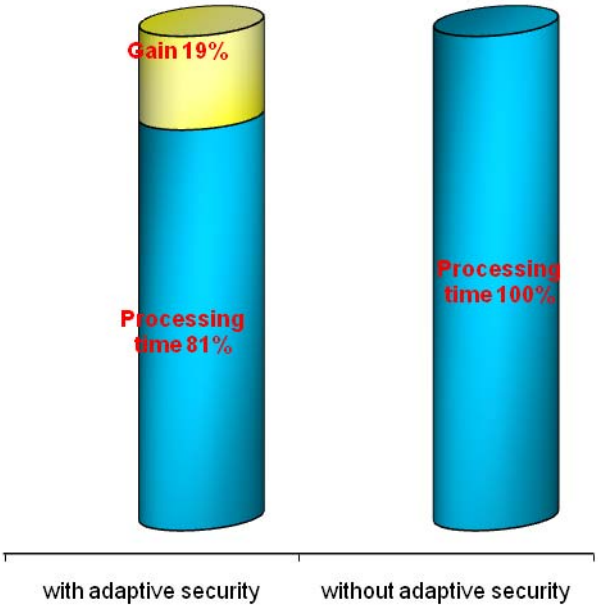


Figure 38: Power saving during a typical day

This is the most interesting case since it represents a typical day of a working person. It is assumed that the person is almost 13 hours at home (morning, evening and night), almost 8,5 hours in work environment (work office, canteen, etc.) and 2,5 hours in public places (transport, shopping, etc.). For a typical working day, the network is able to save almost 20% of its batteries lifetime.

Influence of the sampling rate on the power savings

There are some parameters of the BSN which the doctor or the network administrator could influence. Those parameters are the sampling rate of the messages sent by the nodes to the aggregator, and the sampling rate of the key exchange process. For the vital sensors, it has been defined the messages sampling rate in such a way to avoid loss of messages. Indeed, the key exchange protocol takes at max 8 sec (in high level of security), and since messages are sent every 10 seconds, all the messages could be delivered. **If the messages sampling rate is increased, some messages could be lost, each time there is change of the keys.**

The key exchange sampling rate has been defined to prevent attackers to enter the system. However, this sample rate could allow an attacker to enter the network, if it is in the "supposed trusted place" since it requires only 1,5 hours to break the key with a single node. But it has been previously assumed that the possibility of an attacker in the trusted place without being seen by the end-user (e.g. an intruder in a house) is very small. The second reason for the choice of this sample rate is a battery consuming issue. In fact, the most battery consuming process is the key exchange protocol, and if this sample rate is increased to 1,4 hours (avoiding any intrusion in this way), the lifetime of the sensor node batteries will be dramatically decreased. The following Figure 39 presents a graph for the same case as a typical day presented in the previous section to depict this situation.

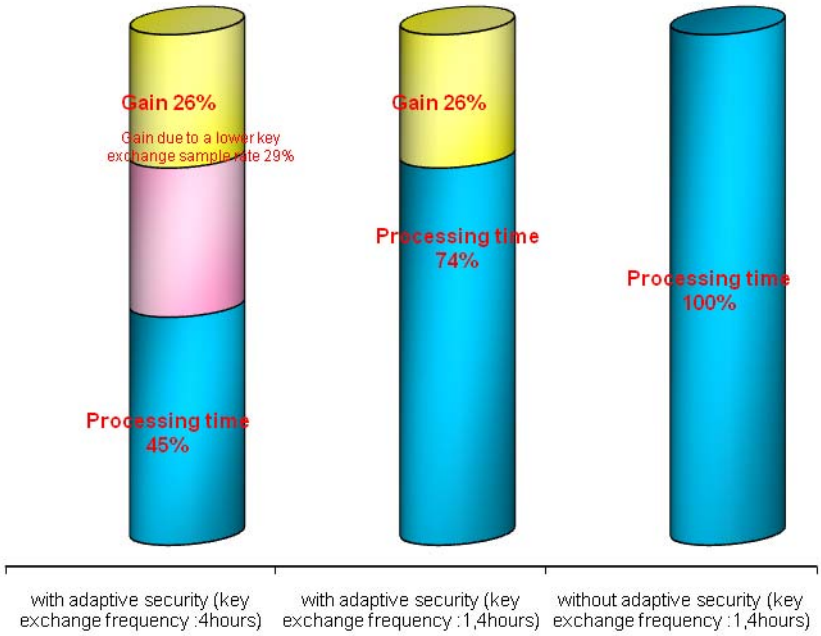


Figure 39: Power saving depending on the key exchange sampling rate [5]

As seen from the Figure 39, even if batteries could be saved thanks to the adaptive security algorithm, in case of a higher sample rate, it consumes 29% more batteries than with the use of a lower sample rate.

In case of a patient in critical state, the doctor would have constant monitoring of the patient which implies a higher messages sampling rate (i.e. 1 message every second). This will obviously impact the battery consuming. To simulate this scenario, it is considered that the patient is laid up in hospital the whole day. Figure 40 presents the results of such a case.

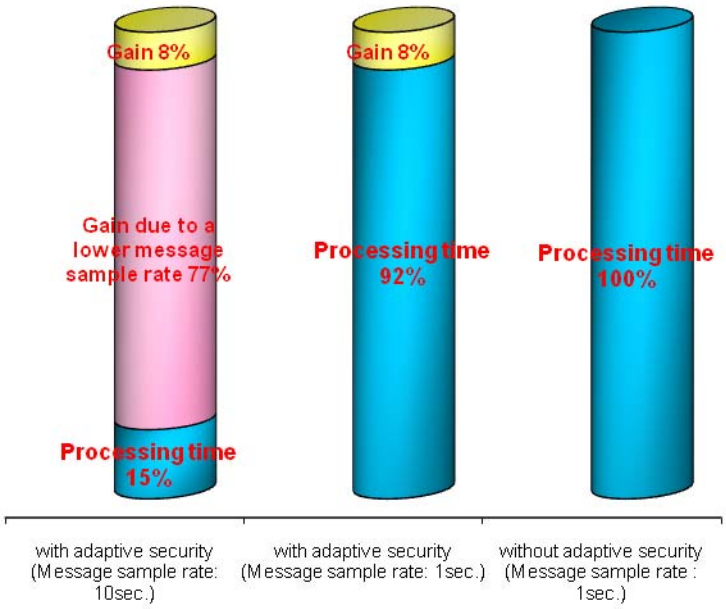


Figure 40: Power saving depending on the message sampling rate

As can be seen from Figure 40, the additional power consumed by this increase of the message sampling rate is huge. **With such a high sampling rate, the sensor nodes will consume almost 6 times more energy than in the normal case of monitoring.**

6.3.6. Trade off between energy savings and security levels

The sample rates of the BSN must be taken into account and modified with care. As shown in Figures 39 and 40, a high sampling rate implies a huge loss of battery lifetime. Moreover, an increase in the message sampling rate will automatically involve a loss of messages during the key exchange process, **except if a buffer is used to save messages during this process.** (This could a topic for study in future works). In addition, the bigger the increase of the key exchange sampling rate is, the bigger the loss of messages would be.

The three cases presented are some assumptions and they show that the batteries lifetime saving mainly depends on the behaviour of the user. If the users are more often in public places (work outside their office for example) the power saved would be less. To see the impact of the level of security on the battery consumption and the security issue regarding the time needed to break a key, the following Figure 41 must be referred to.

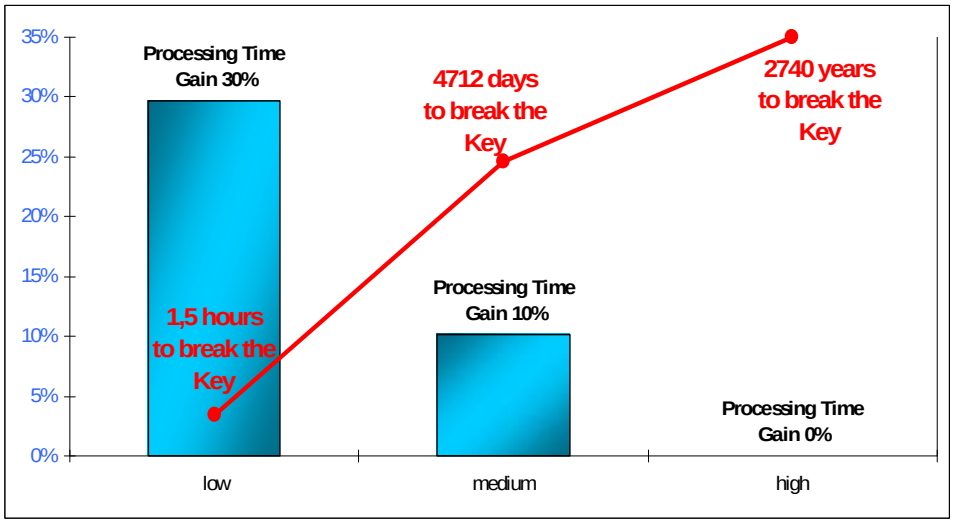


Figure 41: Evolution of the processing time and security aspect depending on the level of security [5]

As it is possible to see from Figure 41, there is a clear trade off between energy saving (processing time gain) and the provision of security (time to break the key). ***For the trusted scenario (low level of security) the security is not a main concern. Therefore a lot of energy could be saved. In the medium level of security a compromise between energy and security is obtained, although in this case the security provision is more relevant.***

If the number of sensor nodes is increased, it will not affect the behaviour of the sensor nodes themselves, but the aggregator would have to compute much more in the same amount of time. However, since the aggregator has much higher processing capabilities than a single sensor node, it would not affect the global performance of the BSN.

6.3.7. Memory Usage

Another main concern during the development of the proposed security protocol suit was the required memory to run the whole protocol suit. This issue is even more important than the computational time because the sensors have a small amount of available memory. Looking at the processor capabilities, it might be used at its maximum performance as long as there is energy in the batteries. However the memory cannot be increased unlimited according to the growing needs. The proposed security protocol suit has to satisfy the current characteristics of the available devices in the moment.

The proposed adaptive confidentiality protocol uses two main algorithms, the RC5 and the ECC-DH which are responsible for the memory needs.

The RC5 algorithm is known for its light memory storage. To be more precise and the real amount of required memory has been calculated [2]:

The main Code (about 2Kbytes);
Buffer, equivalent to one data block (8 Bytes);
Encryption Key (variable length);
Expanded Round Key (8 Bytes for each round);
Initialisation Vector (8 Bytes, only in CBC mode).

Looking now at the ECC-DH algorithm [2]:

Key generator public key (2×128 Bytes);
Partial Key (128 Bytes);
Identity (40 Bytes);

Secret Key (128 Bytes);
Tate Pairing result (128 Bytes).

Applying this knowledge to the proposed protocol suit, Figure 42 presents its comparison with AES:

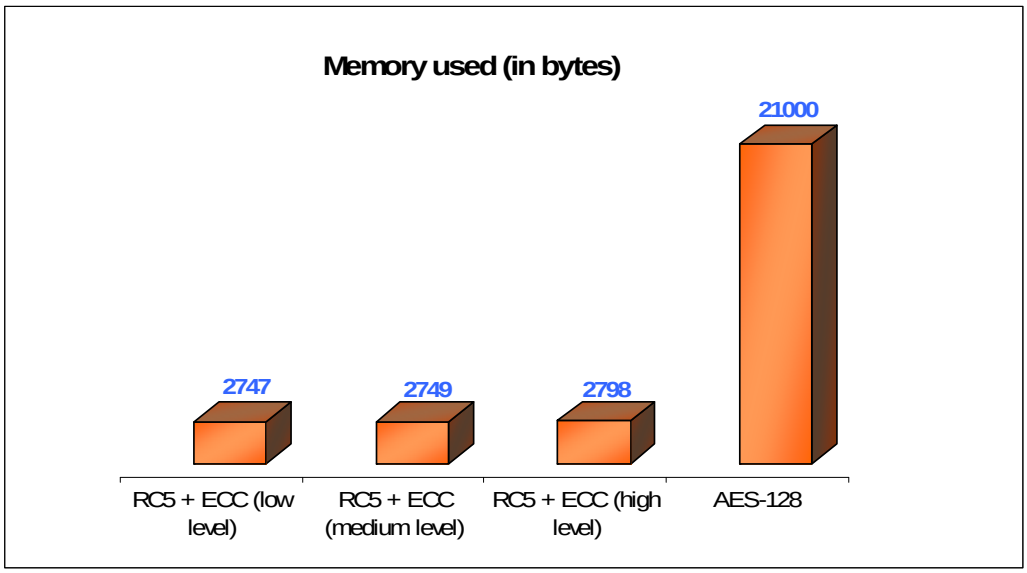


Figure 42: Memory Allocation for each level of Security and AES

As it can be seen in the highest level of security, the proposed protocol suit uses almost 3kB, which is an extremely suitable result for the current sensor nodes, limited to 8KB of memories (MICA2.). The difference between the three levels of security resides on the adaptability of the RC5. For comparison reasons it is added the memory required for AES-128 [2] which is around 21kB. ***The AES requires seven times more memory than the RC5+ECC. Once more, this result justifies the reason why RC5+ECC has been chosen in this proposal instead of AES.***

With these results it is concluded that the proposed security protocol suit satisfies the hardware constraints of the sensor nodes.

6.3.8. Summary of Section 6.3

From the simulation could be seen that with low security level it can be saved up to 30% of the battery lifetime during all the day. A typical day, when most of the time a person is in office and during the evening and the night he/she is at home, would save around 20% of the battery life time.

Power savings for medium level of security could give approximately 10% and the higher power savings could be in low level of security – approximately 30%.

Regarding memory usage, the proposed protocol suit uses almost 3kB, which is a suitable result for the current sensor nodes, limited to 8KB of memories (MICA2.). The difference between the three levels of security resides on the adaptability of the RC5. For comparison, the AES requires seven times more memory than the RC5+ECC. Once more, this result justifies the reason why RC5+ECC have been chosen in this proposal instead of AES.

Further, the simulations have shown that there is a clear trade off between energy saving (processing time gain) and the provision of security (time to break the key). For the trusted scenario (low level of security) the security is not a main concern therefore a lot of energy could be saved. In the medium level of security a compromise between energy and security is obtained, although in this case the security provision is more relevant.

However an open door must be left for future applications. Technology grows at a quick pace and what seems fit and secure today, might be inadequate and weak tomorrow. It is believed that soon new sensors will be available with much bigger capacities. The answer to the question: “Which is the most suitable encryption protocol?” would not be the same as today. However it must be kept in mind that the proposed framework was developed to allow an easy change of the key length, among others parameters, in order to increase its security. Even with better sensors, RC5 could still be promising to guarantee security for pervasive tele-care applications.

6.4. Summary of Chapter 6

The main goal of Chapter 6 was to analyse and evaluate from different points of view the proposed concept and mechanisms for context-awareness and adaptability for ensuring privacy in pervasive telehealth and telecare scenarios. It further discussed the evaluation of the ACAPP Framework, starting with presentation of the evaluation goals and continuing with the results of the performed evaluation. It presented the costs of the privacy protection enhanced with adaptivity, context-awareness and security management. It also evaluated the security management and the adaptive confidentiality for memory usage and power-savings.
From the analysis it could be concluded that the proposed adaptive security framework and the security protocol suit could be seen as evolution of SPINS with some extra features- the power management and the adaptivity features and suitability for a bigger number of scenarios.
Three security levels have been considered. Usually the low security level could be applied when the persons are in trusted environments. However, the trusted environment must be carefully selected.
From the simulation could be seen that with low security level it can be saved up to 30% of the battery lifetime during all the day. A typical day, when most of the time the persons are in office and during the evening and the night they are at home, would save around 20% of the battery life time.

Regarding memory usage, the proposed protocol suit uses almost 3kB, which is a suitable result for the current sensor nodes, limited to 8KB of memories (MICA2.). The difference between the three levels of security resides on the adaptability of the RC5. For comparison, the AES requires seven times more memory than the RC5+ECC and this justifies the choice of RC5 instead of AES. Further, the simulations have shown that there is a clear trade off between energy saving (processing time gain) and the provision of security (time to break the key).

However it must be kept in mind that the proposed framework was developed to allow an easy change of the key length, among others parameters, in order to increase its security. Even with better sensors, RC5 could still be promising to guarantee security for pervasive tele-care applications.

The performance evaluation for the privacy protection and context-awareness was performed with two aspects in mind: to evaluate the influence of the complexity and granularity of the context information on the performance of the Rule Agent and to evaluate the implication of introducing the Privacy Safeguard mechanism. The simulations have shown that having proactive approach for selection of a set of applicable rules in reply to the dynamic nature of context changes, optimises the performance and reduces the delay from the filtering.
On the user side, introducing privacy protection framework and context-awareness requires to some extent involvement of the user and for some user groups this could be a challenge. Sometimes the users must also make informed decisions for protecting their privacy and this could be difficult if they are not aware of the threats for privacy. That means that there must be overall efforts to educate the end-users of pervasive telehealth and telecare services.

References

[1] Vagner Sacramento, et al. "A Privacy Service for Context-aware Mobile Computing". First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), pp. 182-193.

[2] Neeli R. Prasad, "**Adaptive Security for Heterogeneous Networks**", PhD Thesis, April 2004

[3] eSENSE Delivarable 2.3.1 **"e-SENSE Security Framework**", December 2007

[4] Ricardo Jose S. Rodrigues, Mathieu David, Dimitri Loire, "**Adaptive Security for Wireless Sensor Networks**", Master Thesis, Aalborg University, June 2006

[5] Ricardo José S. Rodrigues, Mathieu David, Dimitri Loire, Anelia Mitseva, Neeli R. Prasad, **"Adaptive Security Management for Body Sensor Networks in Medical Scenario"**, in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1037-1041, San Diego, USA, Sept 2006.

[6] Anelia Mitseva, Satya A. Wardana, Neeli R. Prasad, **"Context-Aware Privacy Protection for Wireless Sensor Networks in Hybrid Hierarchical Architecture"** – IEEE IWCMC 2008, Wireless Sensor Networks Symposium, Creta Island, Greece, August 2008, 978-1-4244-2202-9/08/$25.00 © 2008 IEEE

[7] A. Mitseva, E. Aivaloglou, M. A. Marchitti1, Neeli R. Prasad, C. Skianis, S. Gritzalis, A. Waller, Timothy Baugé, Sarah Pennington, **"(Towards) Adaptive Security for Convergent Wireless Sensor Networks",** WIRELESS COMMUNICATIONS AND MOBILE COMPUTING:, SI on Quality of Service and Security in Wireless and Mobile Networks, 29 Sept 2008

Chapter 7
7. Conclusions and directions for future work

In this final chapter 7 of the thesis the final conclusions will be presented - for the proposed solution for privacy protection and for the adaptive confidentiality. Further, overall conclusions for the presented concept for adaptive security will be drawn. The chapter is finished with drafting directions for future work.

7.1. Conclusions for Privacy Protection and Context-awareness

In this section, it is presented preliminary assessment of the scalable and flexible context-aware controlled information disclosure for BSN, integrated within hybrid hierarchical architectures in pervasive health care scenarios.
To compare the preliminary findings from the presented in the previous chapters work, it is referred to [1] where real-time context information is used to aid in system decision-making for general purpose applications. One of the conclusions in [1] for their context-aware system was that context reasoning causes a perceivable delay (about one second), which sometimes matters to users. The context-aware privacy protection mechanism proposed in this security management framework for flexible architecture differs in the model of the rules, the proactive approach for selection of a rule subset, and it results in a minor delay.
Some evaluation of a privacy service can be found in [2]. In their paper, the application is in collaborative mobile services without WSNs integration and considering only a limited number of contexts. From comparing the collaborative service presented in [2] with the context-aware privacy protection investigated in this report, it must be noted that the proposed here policy framework is scalable and targeted to support different stakeholders in a set of application spaces, also providing set-up and design guidelines.
After proposing flexible and scalable privacy protection framework in Chapter 5, in Section 6.2 it was also presented proper evaluation goals and performance metrics to assess the pros and cons of context-aware rule-management solution targeted to protect privacy of users, when using sensor nodes and handheld devices with diverse performance capabilities, residing in level 1 (people) and 2 (environment) nodes of hybrid hierarchical architecture. The evaluation should aid the designers of medical and care systems with integrated WSNs in understanding how to exploit context, policies and profiling in order to protect privacy; how to find the most relevant design; how to access the performance of the solution.
Additional performance parameters, such as for example memory cost and influence of the period of the context changes, have to be further considered. Furthermore, optimisation approaches (i.e. compression) to reduce the memory usage, and how they influence the efficiency of the privacy framework, need to be investigated.
At the same time, in some of the situations, the end-user will need to interact with the privacy protection. This is in the cases when explicit request regarding certain sensitive data must be provided and only for this type of explicit request the user needs to decide on case per case basis. This might not be very convenient for any situations in which the user is requested the data or it could be challenging for some elderly users. Therefore, special attention for user-friendliness must be paid and especially for elderly persons. Future direction of work is usability testing of the privacy protection service.

7.2. Conclusions for the proposed adaptive security protocol suit

When analysing the existing solutions, a weakness in the current protocols for key exchange regarding the authentication procedure has been identified. This was the motivation to propose a new solution – security protocol suit based on the ECC and the Diffie-Hellman protocol. With the use of the ECC, it is not only increased the protection against a very common attack (eavesdropping), but this is also done using smaller keys than any other known algorithm.

In accordance with the simulation results, the RC5 continues to impose itself as the right encryption/decryption algorithm for these computational and energy constrained nodes because it is fast, efficient, light and not easily breakable.
The introduction of flags in the transmitted messages proved to be an efficient solution against latency (the most vital information is always treated first) and it allows the detection of emergency situations (which have top priority).
From the analysis presented in Section 6.1, it became visible that in the low level of security, disregarding the fact the network is in a trusted place, the probability of the network being compromised is significant. This fact has to be taken into account when defining which places should be considered as trusted.
In the previous section it was demonstrated that the adaptability of the proposed security protocol suit increases the sensor nodes' lifetime. The conclusion was that in the average case it could be saved up to 20% of energy with the assumption that these savings will come from applying the adaptive confidentiality only.
For comparison, study on the benefits from using adaptive security has been investigated in [3]. In that work the benefits of the adaptability property on battery power consumption were quantified through a prototype implementation on sensor hardware (on Crossbow Mica2 motes - www.xbow.com). The aim of the performance evaluation was to quantify the difference in energy consumption between having and not having the ability to adapt the Security Level. A simplified version of the framework has been deployed, with the security mechanisms being implemented using TinySec and the Security Levels being represented by the TinySec transmit modes. Low, Medium and High security levels were characterised by no encryption or integrity protection, integrity protection only, and both encryption and integrity protection respectively. This was the main difference with the evaluation done in this Phd report. The main conclusion drawn from the experimental evaluation in [3] is that the power savings from the adaptability property depend on the proportion of the total time spent in each Security Level during network operation, and the frequency of Security Level changes, i.e. to the number of configuration messages that are required.
A careful study on the influence of the sampling rate of the sensors and the medical requirements for BSNs, made us realise that changing the keys every four hours brings the best compromise between energy saving and latency.
With this proposal the user's behaviour is intimately connected to the security parameters. However the user has the option of interacting with the network status through several warnings for low battery which are displayed on the mobile device. The user is also given the power to override some of the Security Manager instructions, as wished, to stay on a higher level of security than necessary.
The use of a Context Monitoring Algorithm provides the ability to keep track of the network status and to ensure a quick response if a malfunction or an attack is detected.
It could be argued that the Context Monitoring Algorithm and Security Manager, combined with the Power Management feature provide a reasonable security energy-efficient solution for WSNs in pervasive health care applications.
Based on the presented calculations it can be concluded that the full implementation of the proposed protocol suit satisfies the memory constraints of the current sensors. In the highest level of security the proposed here solution uses 3kB of memory which still leaves room for 1kB for other implementations.
Another new feature proposed and implemented is the connection with foreign trusted networks in order to optimise and increase the functionalities of both networks. With this current proposal the process is done automatically (after the first session) without compromising the security of the networks in question.

7.3. Overall conclusions for this thesis and future work

The general objective of this thesis was to define how context-aware privacy management services integrated in an adaptive security management framework, can be provided within flexible protocol stack, in a way that effectively covers the diverse security and privacy needs of realistic pervasive health and elderly care scenarios. This has been achieved through the definition of an adaptive privacy framework, integrated in the overall scalable security management framework which is able to make use of suitable privacy mechanisms to continually select and perform the most appropriate level of security and privacy according to the current context. The framework provides a number of options designed to make it suitable for different applicable scenarios and to provide adaptability within these scenarios. Table 44 summarises the proposal to address the security and privacy considerations that were identified through the requirements analysis (Section 3.2).

	Mechanisms	Flexibility and Configurability	Adaptability
Security services	Various sets of mechanisms for authentication, encryption, integrity and freshness	For each node, selection of sets of mechanisms for the Security Levels according to the scenario and the node security requirements	Selection of appropriate Security Level for each communication according to node profile, the applicable rules and the current context information
Privacy services	Mechanisms for privacy protection and controlled information disclosure according to user/application/service profile and current context	For each node, privacy protection components are included according to node privacy requirements	Controlled information disclosure decisions depend on the node profile, the applicable rules and the current context information

Table 44: Overview of the proposal for flexible security framework

This PhD report proposes solutions to a number of privacy protection threats – reveal user identity, reveal user location, un-authorised access and reveal confidential data. Figure 43 shows where the proposed solutions fit in the identified threats for WSNs.

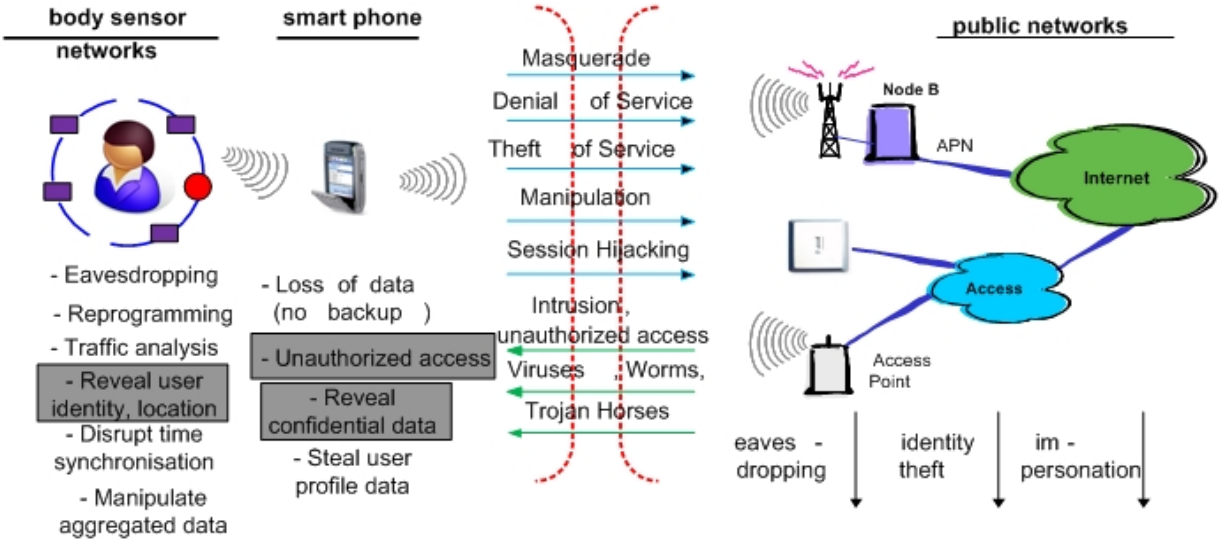


Figure 43: Proposed solutions to a subset of the identified threats for WSNs in pervasive health care scenarios

Overall, it has been shown that the proposed framework enables diverse applications and their associated security and privacy requirements to be supported in the heterogeneous network topologies that WSNs will need to integrate within real-world scenarios. It has been also demonstrated how it could be integrated into a flexible architecture. For tailoring the framework to deploying the system, configuration guidelines (check) were given (Section 5.5.2), and worked examples for several applications were described.

The adaptability introduced in the security framework aims to achieve significant savings in resources and flexibility. Without flexibility, the standard security approach often provides the highest possible level of protection to all data which costs a lot. By only providing the security and privacy requirements that are strictly necessary according to the application needs, user and environmental context etc., significant processing and

communications overhead can be saved. The framework enables self-reliance and minimises the need for maintenance by providing functionality for self-configuration of nodes according to their individual context and defined policies. In addition, the use of policies means that changes of requirements can be met rapidly without affecting implementations on the nodes (policies define "what" is needed and not "how" it is achieved, which is up to the nodes themselves). The actual level of these benefits will need to be validated in practice, as will the effect of the usual sensor network constraints. An initial evaluation of the proposed framework has been undertaken against the security and privacy requirements identified in Section 3.2 and the overall system requirements and constraints. ***This has shown that the framework holds promise, but that the potential benefits are affected by many complicated factors that are difficult to assess and are often highly application-specific***.

Further evaluation of the proposed adaptable security protocol suit and the context-aware controlled information disclosure concluded the following:

The estimated power consumption in the three cases explained in Section 5.5.1 based on the ability of the security framework to change the current security level of nodes in WSN, and hence the algorithms employed, according to change in context, suggests that there is potential in the proposed adaptive security framework but the savings in resources are dependent on the scenario. The expected power savings are dependent on the rate of changing the security level and the proportion of time spent in each security level. Scenarios that use the 'Low' security level for a large proportion of the time and that change security levels infrequently have the potential to benefit most, such as case A – user at home scenario. For the discussed three cases as long as the rate of changing the security level is relatively low, it is expected that the proposed solution provides power savings. It is unlikely that the security level will need to change very frequently and so the framework is likely to conserve battery power for these scenarios. Due to the necessary simplifications of the prototype, the work carried out does not give direct validation of the adaptive security framework. In particular, it should be noted that the sensor nodes are also performing other functionality that may have a greater effect on the power consumed by the node than the security framework, and may offer greater potential for power savings. These, and other external factors presented in Section 6.1, may affect the overall significance of the power savings achieved by the adaptable security framework for the reference scenarios. However, the work carried out does provide evidence that there is potential in this idea and that further in-depth validation may be worthwhile for many other scenarios outside the medical domain.

In particular, the key benefit is that with the context-aware and adaptivity feature for security management, the privacy protection framework only provides the security and privacy requirements that are strictly necessary according to the application needs, environmental context, etc. and in this way significant security and privacy processing and communications overhead can be saved. Moreover, the additional processing that the framework entails will add some delays, but for WSN nodes this is unlikely to be significant as they are infrequent communicators rather than high bandwidth users. This could be more of an issue for gateways, as they are natural points of aggregation. Future work will investigate how much of an issue the power is in practice for gateways and whether any optimisations are possible.

The preliminary evaluation of the context-aware privacy protection mechanisms and the complexity of the context assessment have been done for 50, 100, 150 and 200 applicable rules and 3, 6 and 10 number of context attributes. Since the rules could be read from the data store or from a valid subset proactively stored in the memory, there is no significant difference in the ratio read from data store vs. read from memory with 6 and 10 context instances for over 120 applicable rules. The memory usage for compressed and uncompressed implementation of the Rule Agent shows that the gain is bigger with higher number of context attributes – gain of 70% with 10 context attributes. The proposed model of rules and the proactive approach for selection of a valid rule subset lead to a delay much less than 1 sec (where 1 sec is a limit which sometimes matters to users). Additional performance parameters, such as for example memory cost and influence of how often the context changes, have to be further investigated.

Finally, the framework provides increased functionality for users, but at the potential cost of increased complexity for their interactions. The effects of this depend on how users need to interact with the system, and could be minimised with 'user–centric' design of interfaces and pre-defined configurations. In addition, the use of policies can be argued to simplify user interactions by allowing them to manage from a central point and concentrate on "what" is needed rather than "how" it is achieved. In other words, they are isolated from the complexities of implementations and can concentrate on what their requirements are. Further, usability testing of the whole system with real end-users under realistic conditions could greatly help the validation and broad acceptance of the presented context-aware privacy protection framework for WSNs.

7.4. Summary of Chapter 7

This final chapter 7 presented the conclusions for the proposed privacy protection framework, the adaptive security protocol suit and the overall concept for context –awareness and adaptivity of the security and privacy services for pervasive telehealth and telecare scenarios. An initial evaluation of the proposed framework has been undertaken against the security and privacy requirements strictly necessary for the reference scenario and the overall system constraints.

The estimated power consumption in the three investigated cases based on the ability of the security framework to change the current security level of nodes in WSN, and hence the algorithms employed, according to change in context, suggests that there is a potential in the proposed adaptive security framework but the savings in resources are dependent on the scenario. The expected power savings are namely dependent on the rate of changing the security level and the proportion of time spent in each security level. Scenarios that use the 'Low' security level for a large proportion of the time and that change security levels infrequently have the potential to benefit most, such as user at home scenario. For the discussed three cases as long as the rate of changing the security level is less than twice a minute, it is expected that the proposed solution provides power savings. In reality it is unlikely that the security level will need to change this frequently and so the framework is likely to conserve battery power for these scenarios.

This has shown that the framework holds promise, but that the potential benefits are affected by many complicated factors that are difficult to assess and are often highly application-specific. In particular, the key benefit is that with the context-aware and adaptivity feature for security management, the privacy protection framework only provides the security and privacy requirements that are strictly necessary according to the application needs, environmental context, etc. and in this way significant security and privacy processing and communications overhead can be saved.

These, and some other external factors, may affect the overall significance of the power savings achieved by the adaptable security framework for the reference scenario. However, the work carried out does provide evidence that the framework holds promise and that further in-depth validation may be worthwhile for many other scenarios under the medical and care domain, also outside this domain.

Finally, the framework provides increased functionality for users, but at the potential cost of increased complexity for their interactions. The effects of this depend on how users need to interact with the system, and could be minimised with 'user–centric' design of interfaces and pre-defined configurations.

Direction for future work is validation in practice of the actual level of the above mentioned benefits, as will the effect of the usual sensor network constraints. Further, usability testing of the whole system with real end-users under realistic conditions could greatly help the validation and broad acceptance of the presented context-aware privacy protection framework for WSNs.

References

[1] Wang, X.; Dong, J.S.; Chin, C.Y.; Hettiarachchi, S.R.; Zhang, D.; Semantic Space: An Infrastructure for Smart Spaces, *Pervasive Computing, IEEE,* Volume 3, Issue 3, July-Sept. 2004 Page(s):32 - 39

[2] Vagner Sacramento, et al. "A Privacy Service for Context-aware Mobile Computing". First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), pp. 182-193.

[3] A. Mitseva, E. Aivaloglou, M. A. Marchitti1, Neeli R. Prasad, C. Skianis, S. Gritzalis, A. Waller, Timothy Baugé, Sarah Pennington, **"(Towards) Adaptive Security for Convergent Wireless Sensor Networks",** WIRELESS COMMUNICATIONS AND MOBILE COMPUTING:, SI on Quality of Service and Security in Wireless and Mobile Networks, 29 Sept 2008

Appendix A - List of Publications

Journals

1. Anelia Mitseva, Petia Todorova, Ramon Aguero, Ana Garcia Armada, Christos Panayiotou, Andreas Timm-Giel, Leonardo Maccari, Neeli R. Prasad, **"CRUISE research activities towards Ubiquitous Intelligent Sensing Environments",** IEEE Wireless Communications Magazine, August 2008, Vol.15 No.4, SI on Security in Ad Hoc and Sensor Networks; Wireless Sensor Networks, pp. 52- 59, 1536-1284/08/$25.00 © 2008 IEEE

This paper has been cited in one work:

- A survey on wireless sensor networks deployment; Z Bojkovic, B Bakmaz - WSEAS TRANSACTIONS on COMMUNICATIONS, 2008

2. A. Mitseva, E. Aivaloglou, M. A. Marchitti1, Neeli R. Prasad, C. Skianis, S. Gritzalis, A. Waller, Timothy Baugé, Sarah Pennington, **"(Towards) Adaptive Security for Convergent Wireless Sensor Networks",** WIRELESS COMMUNICATIONS AND MOBILE COMPUTING:, SI on Quality of Service and Security in Wireless and Mobile Networks, published online on 29 Sept 2008, DOI 10.1002/wcm.678

3. Gabriele Kotsis, Anelia Mitseva and Neeli R. Prasad, "**The CRUISE Project - Network Initiative for Creating Ubiquitous Intelligent Sensing Environments",** ERCIM News No.65, April 2006, pp.39-40

Conferences

4. Anelia Mitseva, Matthias Gerlach, Christian Räck, Neeli R. Prasad, **"Context-aware Adaptive Privacy Protection for Wireless Sensor Networks**", in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1032-1036, San Diego, USA, Sept 2006

5. Ricardo José S. Rodrigues, Mathieu David, Dimitri Loire, Anelia Mitseva, Neeli R. Prasad, **"Adaptive Security Management for Body Sensor Networks in Medical Scenario"**, in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1037-1041, San Diego, USA, Sept 2006.

6. Anelia Mitseva, Mohamad Imine, Neeli .R. Prasad, **"Context-Aware Privacy Protection with Profile Management",** In proceedings of WMASH 2006 (The fourth ACM international Workshop on Wireless Mobile Applications and Services on WLAN Hotspots), pp. 53-62 (ACM Press), September 29, 2006, Los Angeles, USA in conjunction with MobiCOM 2006; SESSION: AAA, security and privacy; Year of Publication: 2006 ; ISBN:1-59593-470-7

This paper has been citied in 4 external works:

- Usability Improvements for WLAN Access, K Karvonen, J Lindqvist - Lecture Notes in Computer Science, 2007 – Springer
- Patient's privacy protection with anonymous access to medical services; D Weerasinghe, K Elmufti, M Rajarajan, V Rakocevic – School of Engineering and Mathematical Sciences, City University, Northampton Square, London, EC1V 0HB, UK. Pervasive Computing Technologies for Healthcare, 2008 - ieeexplore.ieee.org
- Resource Discovery in Ubiquitous Health Care; G Pallapa, S Das, Dept. of Comput. Sci. & Eng., Univ. of Texas at Arlington, Arlington, TX; - Advanced Information Networking and Applications Workshops, …, 2007, AINAW'07 - ieeexplore.ieee.org; 21-23 May 2007
- D2.1 – Requirements of methods, languages, algorithms, and tools to modeling and management of context. Project MUSIC - Self-Adapting Applications for Mobile Users in Ubiquitous Computing Environments; P Rigole, PA Ruiz, PH Meland, N Paspallis, S … - ist-music.eu

7. A. Mitseva, M.Imine, N.R.Prasad, **"CRUISE Project - Network Initiative for Creating Ubiquitous Intelligent Sensing environments",** in Proceedings of The 15th IST Mobile & Wireless Communications Summit, 4-8 June 2006, Myconos, Greece

8. Anelia Mitseva, Tapio Suihko, Radosveta Sokullu, Slobodanka Tomic, Maria Marchitti, Neeli R. Prasad "**Mobility Framework for Wireless Sensor Networks: CRUISE Approach**" in Proc. Of CRUISE Worksop at VTC 07 Spring, 25 April 07, Dublin, Ireland

9. Anelia Mitseva, Matthias Gerlach, Neeli R. Prasad. **"Privacy Protection Mechanisms for Hybrid Hierarchical Wireless Sensor Networks".** In Proc. of IEEE International Symposium on Wireless Communication Systems (ISWCS) 2007, 17-19 Oct 2007, pp. 332-336, Trondheim, Norway, DOI 10.1109/ISWCS.2007.4392356

10. Aivaloglou, E.; Mitseva, Anelia; Skianis, C.; Gritzalis, S.; Waller, A.; Prasad, Neeli R.., **Scalable Security Management for Wireless Sensor Networks for Medical Scenarios,** In Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007, pp. 1014-1018, Dec 2007, India

11. Sokullu, Radosveta; Korkmaz, Ilker; Dagdeviren, Orhan; Mitseva, Anelia; Prasad, Neeli R., **An Investigation on IEEE 802.15.4 MAC Layer Attacks,** In Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007, pp. 1019-1023, Dec 2007, India

12. Anelia Mitseva, Satya A. Wardana, Neeli R. Prasad, **"Context-Aware Privacy Protection for Wireless Sensor Networks in Hybrid Hierarchical Architecture"** – IEEE IWCMC 2008, Wireless Sensor Networks Symposium, Creta Island, Greece, 6-8 August 2008, pp. 773-778 © 2008 IEEE, ISBN: 978-1-4244-2201-2; INSPEC Accession Number: 10152730; Digital Object Identifier: 10.1109/IWCMC.2008.134

Public Technical Reports

13. CRUISE Del 210.1 **"Sensor Networks Architecture Concept"**, Section 6, November 2006

14. CRUISE Del 230.1 **"Key Issues Related to Mobility and Security in Sensor Networks",** September 2006

15. CRUISE Del 230.2 "**Mobility and Security Framework for WSNs",** December 2006

16. e-SENSE Del 2.2.1 "**Initial e-Sense system architecture"**, Section 5, November 2006

17. e-SENSE Del 2.3.1 **"e-SENSE Security Framework**", December 2007

Successful EU Project Proposals

CRUISE – EU FP6 Network of Excellence – Jan 2006- Dec 2007 – Creating Ubiquitous Sensorised Environments

Major contributions and leading role for the preparation and implementation of this project , - technical contributions for proposal writing, consortium composition, negotiations with EC for the contract, technical manager of the project, Work Package Leader of Cluster C on Security and Mobility for WSNs, major contributions to the deliverables from Cluster C

ISISEMD – EU ICT PSP Pilot Project – March 2009 – Sept 2011 – Intelligent system for independent living of elderly with cognitive problems or mild dementia

Major contributions and leading role for the preparation of this project proposal - technical contributions for proposal writing, consortium composition, negotiations with EC for the contract, scientific contact person from the project's side with the EC, Work Package Leader for Pilot Operation and Evaluation

EAGER NetWIC – EU project under AsiaLink Programme - 01 April 2003 – 31 March 2006 - Euro-Asian Network for Strengthening Graduate Education and Research in Wireless Communications

Major contributions and leading role for the preparation of this project proposal - technical contributions for proposal writing, negotiations with EC for the contract, Project Manager during the project implementation, main responsible for all project deliverables and reports.

Appendix B – Matrix with Publications

Publication	S 2.1	S 2.2	S 2.3	S 3.1	S 3.2	S 3.3	S 4.0	S 5.1-5.4	S 5.6	S 5.7	S 6.1	S 6.2	S 6.3	S 7.0
Anelia Mitseva, Matthias Gerlach, Christian Räck, Neeli R. Prasad, **"Context-aware Adaptive Privacy Protection for Wireless Sensor Networks**", in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1032-1036, San Diego, USA, Sept 2006	1			X	X		X	X		X	X	X		X
Ricardo José S. Rodrigues, Mathieu David, Dimitri Loire, Anelia Mitseva, Neeli R. Prasad, **"Adaptive Security Management for Body Sensor Networks in Medical Scenario"**, in Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications, WPMC 2006, pp. 1037-1041, San Diego, USA, Sept 2006.				X			X	X		X	X		X	X
Anelia Mitseva, Mohamad Imine, Neeli .R. Prasad, **"Context-Aware Privacy Protection with Profile Management",** In proceedings of WMASH 2006 (The fourth ACM international Workshop on Wireless Mobile Applications and Services on WLAN Hotspots), pp. 53-62 (ACM Press), September 29, 2006, Los Angeles, USA in conjunction with MobiCOM 2006 SESSION: AAA, security and privacy; Year of Publication: 2006 ; ISBN:1-59593-470-7				X	X		X	X		X	X			X
Mitseva, M.Imine, N.R.Prasad, **"CRUISE Project - Network Initiative for Creating Ubiquitous Intelligent Sensing environments",** in Proceedings of The 15th IST Mobile & Wireless Communications Summit, 4-8 June 2006, Myconos, Greece	X													
Anelia Mitseva, Tapio Suihko, Radosveta Sokullu, Slobodanka Tomic, Maria Marchitti, Neeli R. Prasad "**Mobility Framework for Wireless Sensor Networks: CRUISE Approach**" in Proc. Of CRUISE Worksop at VTC 07 Spring, 25 April 07, Dublin, Ireland	X				X									X
Anelia Mitseva, Matthias Gerlach, Neeli R. Prasad. **"Privacy Protection Mechanisms for Hybrid Hierarchical Wireless Sensor Networks".** In Proc. of IEEE International Symposium on Wireless Communication Systems (ISWCS) 2007, 17-19 Oct 2007, pp. 332-336, Trondheim, Norway, DOI 10.1109/ISWCS.2007.4392356			X		X		X			X	X	X		X
Anelia Mitseva, Petia Todorova, Ramon Aguero, Ana Garcia Armada, Christos Panayiotou, Andreas Timm-Giel, Leonardo Maccari, Neeli R. Prasad, **"CRUISE research activities towards Ubiquitous Intelligent Sensing Environments",** IEEE Wireless Communications Magazine, August 2008, Vol.15 No.4, SI on Security in Ad Hoc and Sensor Networks;	X													

Wireless Sensor Networks, pp. 52- 59, 1536-1284/08/$25.00 © 2008 IEEE														
Gabriele Kotsis, Anelia Mitseva and Neeli R. Prasad, "**The CRUISE Project - Network Initiative for Creating Ubiquitous Intelligent Sensing Environments",** ERCIM News No.65, April 2006, pp.39-40	X													
Aivaloglou, E.; Mitseva, Anelia; Skianis, C.; Gritzalis, S.; Waller, A.; Prasad, Neeli R.., **Scalable Security Management for Wireless Sensor Networks for Medical Scenarios,** In Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007, pp. 1014-1018, Dec 2007, India				X	X		X	X		X	X	X	X	X
Sokullu, Radosveta; Korkmaz, Ilker; Dagdeviren, Orhan; Mitseva, Anelia; Prasad, Neeli R., **An Investigation on IEEE 802.15.4 MAC Layer Attacks,** In Proceedings of The 10th International Symposium on Wireless Personal Multimedia Communications (WPMC) 2007, pp. 1019-1023, Dec 2007, India			X	X	X	X							X	X
A. Mitseva, E. Aivaloglou, M. A. Marchitti1, Neeli R. Prasad, C. Skianis, S. Gritzalis, A. Waller, Timothy Baugé, Sarah Pennington, **"(Towards) Adaptive Security for Convergent Wireless Sensor Networks",** WIRELESS COMMUNICATIONS AND MOBILE COMPUTING:, SI on Quality of Service and Security in Wireless and Mobile Networks, published online on 29 Sept 2008, DOI 10.1002/wcm.678				X	X	X	X	X		X	X	X	X	X
Anelia Mitseva, Satya A. Wardana, Neeli R. Prasad, **"Context-Aware Privacy Protection for Wireless Sensor Networks in Hybrid Hierarchical Architecture"** – IEEE IWCMC 2008, Wireless Sensor Networks Symposium, Creta Island, Greece, 6-8 August 2008, pp. 773-778 © 2008 IEEE, ISBN: 978-1-4244-2201-2; INSPEC Accession Number: 10152730 Digital Object Identifier: 10.1109/IWCMC.2008.134				X			X	X		X	X	X		X
CRUISE Del 210.1 **"Sensor Networks Architecture Concept"**, Section 6, November 2006	X		X											
CRUISE Del 230.1 **"Key Issues Related to Mobility and Security in Sensor Networks",** September 2006		X			X									
CRUISE Del 230.2 "**Mobility and Security Framework for WSNs",** December 2006		X			X	X	X	X						X
e-SENSE Del 2.2.1 "**Initial e-Sense system architecture"**, Section 5, November 2006					X									
e-SENSE Del 2.3.1 **"e-SENSE Security Framework**", December 2007		X	X	X	X	X	X	X	X		X	X	X	X
	S 2.1	**S 2.2**	**S 2.3**	**S 3.1**	**S 3.2**	**S 3.3**	**S 4.0**	**S 5.1-5.4**	**S 5.6**	**S 5.7**	**S 6.1**	**S 6.2**	**S 6.3**	**S 7.0**

Appendix C – CV

CURRICULUM VITAE

PERSONAL CHARACTERISTICS

- Result oriented and systematic;
- Capable of work in a team and independently
- Strong communication, supervision and teaching abilities;
- Highly motivated and hard working
- Efficient, easy to adapt and learn new things

EDUCATION

02/2000 - 06/2001	Master of Science in Engineering, Intelligent Multimedia, **Aalborg University (Denmark)**, finished with excellent results; Education based on Problem/Project Based learning Relevant Courses -**Object Oriented Programming and JAVA, HCI and Design of Multi modal systems, Multi Modal Interaction (HCI-2)**
09/1999 - 01/2000	Exchange semester, Master's Degree Course in Computer-Based Systems, **Technical University of Denmark, Lyngby**
09/1986 - 06/1991	Master in Electronics and Automation Engineering**, Technical University of Sofia, Bulgaria**

PROFESSIONAL EXPERIENCE

05/2008 **–** *now* — ***Project Manager***
North of Denmark EU-Office, *Aalborg, Denmark*

EU Pilot Project ISISEMD under the programme ICT PSP – Intelligent System for independent living and self-care of seniors with cognitive problems or mild dementia
I played a major role in preparation of the project proposal and communication with the 12 partners and the negotiations with the European Commission. Since the project start in March 2009, I am Work Package leader of the work package for Pilot Operation, Maintenance and Evaluation. I am also contributing to the tasks for definition of user and system requirements and Security, Privacy requirements and Ethical Issues and Dissemination.

07/2004- 04/2008 — ***Assistant Research Professor***
Technical Manager of International project CRUISE
System Development
CTIF - Center For TeleInfrastruktur (Networking and Security Section), Aalborg University, Denmark

EU FP6 Project CRUISE Network of Excellence (Creating Ubiquitous Sensorised Environments) – starting from the project proposal in Spring 2006, the project negotiations in autumn 2006, project start in Jan 2006 and project end Dec 2007.
My role was Technical Manager of the project with 32 partners and Work Package leader of Cluster C on Security and Privacy for WSNs. The major work in Cluster C was to develop Security and Mobility framework for WSNs and to disseminate the results of the work to workshops, conferences and in articles. The work started with review of state of the art for security solutions for WSNs and identification of research gaps.

EU FP6 Integrated Project eSENSE – mid 2005 - Dec 2007 – Convergence of wireless sensor networks with mobile handheld terminals
My role was Task leader for Task 2.3 – Security framework. The goal was to design and implement software solution of context-aware privacy protection module for WSN which is part of adaptive security

framework. I started with investigating the state of the art in this area. Then defined the system, security and usability requirements for protecting the privacy of the users. Further I proposed the concept of this privacy protection module and designed the system main components. Described the functionality of the main components and defined the interfaces with the other subsystems. I prepared detailed specification of the module and I supervised a student to implement Windows demo application for proof of concept – it is coded in C++, XML and Java. Analysis of the solution was performed in terms of energy evaluation, latency, complexity of the context information. Articles were published to disseminate the results.

07/2001- 06/2004 ***Research Assistant***
Technical Manager of International projects NEXWAY and EAGER Netwic
CTIF - Center For TeleInfrastruktur (Networking and Security Section), Aalborg University, Denmark

EU FP5 Project NEXWAY – Network of Excellence in Wireless Communication Applications
My role was Technical Manager of the project with 27 partners. I was responsible to contribute to all project activities as representative of Aalborg University; to prepare technical and financial reports; to prepare and lead the review team during the project annual and final reviews.

EU Project ***EAGER Netwic under Asia Link Programme – with three European and two Asian partners.***
My role was Technical Manager of the project. I was responsible to contribute to all project activities as representative of Aalborg University; to prepare technical and financial reporting; to disseminate the project activities

Project GUI for Network IP Simulator – 2001 till the end of 2003
In this project the goal was designing, implementing, software and usability testing of GUI for Network IP Simulator. This simulator was internal software product for the WING Lab in CTIF where I was working at that moment. It was used for research on mobility for the new at that moment IPv6 protocol. The goal of the GUI was to give the researchers possibility to define their scenarios for the simulations. I analyzed the requirements, designed the concept and implemented the GUI partially in Borland C++ and in Visual Basic. GUI was Windows-based application with multiple windows and drop-and drag functionality to draw the network for each scenario - the mobile nodes and the hosting node. It had also communication with a small database implemented in WS Access. The GUI included both the input and output of the simulator. The design was according to the principles of HCI and user friendliness.

05/2000 - 05/2001 ***Software Developer***
Rohde-Schwarz Technology Center, Aalborg, Denmark
The project was to develop a concept for Man-Machine Interface, to design and implement a prototype for more enhanced handset for a cordless phone. First I started with testing of the MMI of the handset which was under development at that moment in the company. Then I prepared the vision for the menu structure and the way of the user interaction with the handset. The structure of the menu was hierarchical, with small animated icons and jug-wheel in addition to the keyboard which for that time was quite a new concept. Then I implemented the prototype using Rapid Plus Fast prototyping tool. I planned and described **usability testing** for evaluation of this prototype.

09/1997 - 08/1999 ***Teacher*** in Information Technologies
Secondary Information Technology School, Sofia, Bulgaria
- **Motivated students** to achieve good results
- Maintained the **computer lab**

ACHIEVEMENTS

02/2000 **Scholarship** received from Danish Ministry of Education and Nokia during my Master's study at the Aalborg University

12/2002 **Financial award** received from the Faculty of Aalborg University for valuable contribution and active participation in the preparation of MAGNET project proposal funded by the European Commission

From Spring 2002/ Till Spring 2009	**Successful project proposals** - Coordinated and contributed in the initiation, organization, writing and negotiations of 23 big international projects, funded by the European Commission (CRUISE, EAGER NetWIC and ISISEMD)

COMPUTER SKILLS

General tools: Borland C++ Builder, Visual Basic, XML, Java, Eclipse, MS Visual Studio, Access, MS Windows; MS Office; MS Project, Visio

Specialised - Rapid Plus Fast prototyping tool, VHDL (for Computer System architecture), SLM (Structural Meta Language Programming)

Knowledge about: OOP, Design, prototyping and evaluation of software applications according to the principles of intuitiveness, user friendliness and usability; Wireless Sensor Networks; RFID, Use Cases, UI/MMI design; Security and Privacy services, Context-aware Services;

OTHER EXPERIENCES

Knowledge about East European way of work and cultural understanding for the **Slavic countries**

09/1997 - 08/1999	***Private tutor*** *in English and Computer Skills for High School Students and Adults,* Sofia, Bulgaria
01/1994 - 08/1997	***CAD Operator*** *(full time), Computer Company*, Sofia, Bulgaria
01/1993 - 12/1993	***Secretarial support*** (part time job), Sofia, Bulgaria

RELEVANT COURSES

06/2007	***Code Camp for Context Prototyping***, Nokia course, Aalborg University
02/2007	***Coaching; Mediation; Visual Mind Mapping, MS Project 2003,*** IDA courses
08/2005	***Mobile Phones Programming,*** ELITE course, Aalborg University
09/2004	***Project Leadership Course***, Aalborg Handelsskole

LANGUAGES

• English	Professional
• Danish	Advanced
• Russian	Intermediate
• French	Beginner
• Bulgarian	Native

MEMBERSHIP

10/2006-Present	IDA and Netværk for kvindelige ingeniører

INTERESTS AND HOBBIES

During my free time I clear my mind when doing open air activities; recharge with Cycling and Fitness (I am **non-smoker**); maintain my network of friends and colleagues when I meet them in the town or at home. Gather new experiences from short travels in Europe.

Appendix D - List of Abbreviations

WSN	Wireless sensor network
CRUISE project	Creating ubiquitous intelligent sensorised environments
e-SENSE project	Capturing Ambient Intelligence for Mobile Communications through Wireless Sensor Networks
HHA	Hybrid hierarchical architecture
BSN	Body sensor network
SN	Sensor node
DoS	Denial of service
SSL	Secure Sockets Layer
MANET	Mobile ad hoc network
RFID	Radio frequency identification
ID	Identification
ZCK	Zero common knowledge protocol
TAGK	Topology aware group keying
SEAL	Software-Optimized Encryption Algorithm
RC4	Rivest Cipher 4, also called “Ron's Code”
TEA	Tiny Encryption Algorithm
SNTS	Sensor node trace back scheme
µTESLA	Micro version of the TESLA protocol; TESLA is Timed, efficient, streaming, loss-tolerant authentication
RF	Radio frequency
PGP model	Pretty Good Privacy Trust model
RPI	Rich presence information
3GPP	3rd Generation Partnership Project
HMAC	Keyed-Hash Message Authentication Code (HMAC or KHMAC), is a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.
SHA	Secure Hash Algorithm. The SHA hash functions are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
MN	Mobile node
CPU	Central processing unit
ICA	Internal context attributes
ECA	External context attributes
USD	User sensitive data
LLCA	Low level context attributes
HLCA	High level context attributes
GUI	Graphical user interface
IP	Internet protocol
CMA	Context management algorithm
RAM	Random access memory
TLS	Transport Layer Security, successor to Secure Sockets Layer (SSL)
TKIP	Temporal Key Integrity Protocol - a security protocol used in

	the IEEE 802.11 wireless networking standard
DHA	Diffie-Hellman Algorithm
ECC	Elliptic curve cryptography
PDA	Personal digital assistant
AES	Advanced Encryption Standard
XOR	Logical Operation eXclusive OR
ECDLP	Elliptic Curve Discrete Logarithm Problem
RSA	Algorithm for public key-cryptography (from the names of Ron Rivest, Adi Shamir, and Leonard Adleman at MIT)
VIF	Vital information flag
DL	Destination location
DR	Destination role
SL	Source location
SR	Source role
CN	Coordinator node
EN	End-sensor node
EPR	Electronic patient record
GP	General practitioner
APLR	Applicable rules
ALLR	All possible rules
CATR	Context attributes