Interaction between users and IoT clusters

Moving towards an Internet of People, Things and Services (IoPTS)

Shinde, Gitanjali; Olesen, Henning

Published in:
Proceedings of WWRF Meeting 34

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
Shinde, G., & Olesen, H. (2015). Interaction between users and IoT clusters: Moving towards an Internet of People, Things and Services (IoPTS). In *Proceedings of WWRF Meeting 34: Santa Clara, CA, USA, Apr. 2015*

Interaction between users and IoT clusters: Moving towards an Internet of People, Things and Services (IoPTS)

Gitanjali Shinde and Henning Olesen
Center for Communication, Media and Information Technologies (CMI)
Aalborg University Copenhagen
DK-2450 Copenhagen SV, Denmark
gis@es.aau.dk, olesen@cmi.aau.dk

***Abstract*—The Internet of Things (IoT) is paving the way for a vast number of objects in our environment to react, respond and work autonomously as and when required and as per their capability, role and position. They will be able to announce and offer their services to the users, and together this will enable the vision of an "Internet of People, Things and Services" (IoPTS). Application areas for IoT include smart cities, smart homes, environmental control, security & emergency, retail, logistics, industrial control, smart farming, and e-Health. All the IoT objects are organized in clusters, which have a logical relationship with each other and are part of an overall IoT architecture. Defining the cluster and the seamless user-cluster communication are the challenges of the IoPTS. In this work, we present the detailed scenarios and discuss the requirements and functionalities for the cluster framework that is needed to realize IoPTS. In particular, we focus on the interaction between the users and the IoT clusters, where the user profile (role, privileges, and preferences) should be matched with the services offered by the IoT cluster, including the initial set-up, access control, authentication, and authorization.**

***Keywords*—Personal Network, Internet of things, Cluster Formation, service discovery, User Preference, User Privilege.**

I. Introduction

In the IoT paradigm, a vast number of objects around us are interconnected to each other over the Internet. Objects are not only Smartphone but also any electrical/non-electrical devices around us, termed as IoT objects. Most of the IoT objects have limited or no processing power, limited memory, and limited battery life. In the near future, IoT will be deployed in the large scale[1]. Application areas for IoT include smart cities[2], smart homes, environmental control, security & emergency, retail, logistics, industrial control, smart farming, and e-Health [3].

To realize such applications, the IoT objects around us sense and collect data, process, and analyze the data and submit the results to the cluster head and the external parts of the architecture. Every IoT device is not capable of processing the data and taking action depending on sensed data hence there is need for selecting some devices as the head device that performs the data processing and forward data to external architecture/cloud or perform appropriate action. In the IoT, Communication takes place using a number of wired or (short-range) wireless technologies such as Bluetooth Low Energy, ZigBee, NFC, Z-Wave, WiFi, and RFID [4]. The IoT has come out of its infancy, and it is the next revolutionary technology that embeds Internet into all the things around us[5]. According to the Wireless World Research Forum (WWRF): “7 trillion wireless devices serving 7 billion people by 2017 [6]. Concisely, in the near future IoT objects will be able to announce and offer their services to the users, and together this will enable the vision of an "Internet of People, Things and Services" (IoPTS). In the rapid evolution of IoPTS, the participation of devices in the communication networks is increased significantly, and user interception decreased in the same manner.

IoPTS offers the flexibility and services to the end user, however comes with challenges, how to organize large number of devices in the group/cluster? How should these clusters be defined, and how can users interact with them? Mobility is the mandatory subset of IoPTS as people can interact with and use services from objects irrespective of his/her location. How to resolve the mobility issue? Some devices user could carry with him/her how to form its cluster and how to interact with other stationary cluster (Cluster of stationary devices). In the scale of IoPTS, everything around us is capable of sensing and reacting depending on the application domain so huge number of devices will be part of the communication network. Hence, organizing this large number of devices is the basic challenge of IoPTS. Clustering resolves many more critical issues that arise due to deploying huge number of devices in a flat topology.

II. Need of Clustering

In order to make IoPTS a reality, there is a need of organizing IoT objects in clusters, which have some logical relationship with each other and are part of an overall IoT architecture. The clusters may be static or dynamic, depending on how they are formed and defined, and each cluster will have a cluster head, which communicates with gateways, servers or cloud services. The cluster head is also responsible for announcing the services of the cluster and managing

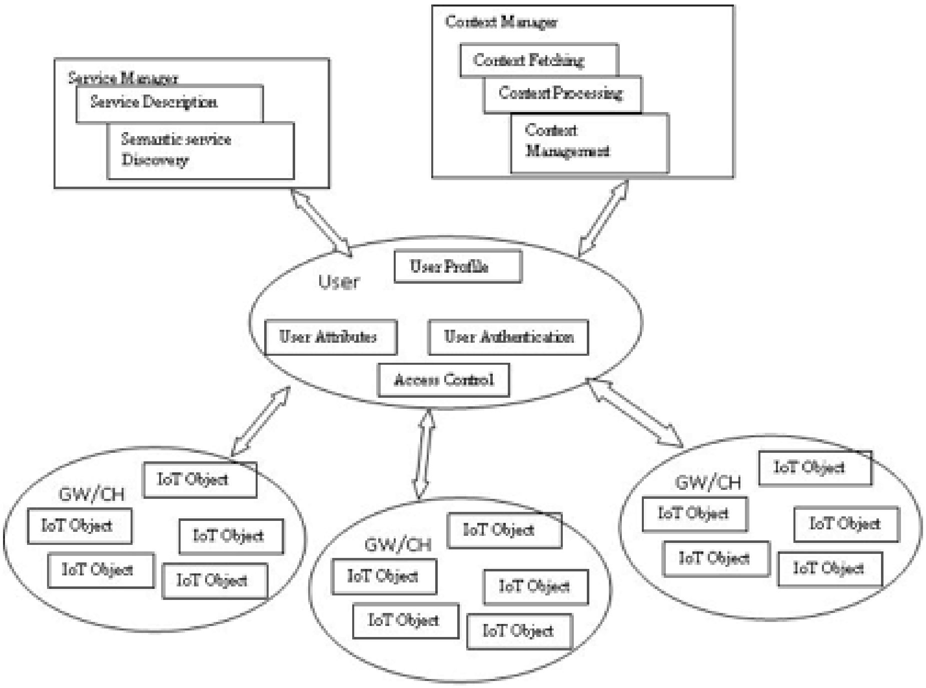

Fig. 1. Interaction between user and cluster.

authentication and access control on behalf of the cluster. Cluster formation is the process of discovering neighboring node and setting communication link between nodes. In the next section of the paper, a few use cases are discussed that explains how a logical connection is required to form a cluster. For example, in the scenario 1 the devices in each room may form one cluster, in the scenario 5, the products in each floor of a shopping mall may form a cluster. Hence forming clusters based on the logical relation between IoT devices and selecting cluster head is the main challenge of IoPTS.

Every device of the cluster provides a few services to the user. Ideally to get access to these services user must be in the transmission range of the cluster. To support mobility, there is a need for a framework that provides services to the user irrespective of location. This invokes the concept of personal network (PN) [7]. The EU projects MAGNET and MAGNET Beyond [8] developed the concepts of "Personal networks" (PN) and "Personal Network federations" (PN-F). The Personal Network seamlessly links together the user's Personal Area Network (PAN) in the immediate vicinity with other (remote) clusters of relevance to the user, and two or more users can form a PN Federation, sharing some of their resources for a limited time in a controlled manner to carry out some joint task.

A PN is the interconnection of local and geographically distributed personal devices that are organized in clusters providing personalized services. The PN uses any existing wired/wireless technology to communicate [7]. In the personal network, a large number of devices are communicating with each other.

Building on these ideas, we believe that users in the future IoPTS world will have a "Personal cluster", most likely centered on their Smartphone or another smart device. This would act as a "hub", to which other personal devices and objects could be connected, such as smart watches, body sensors, or medical sensors. Hence, there is a need of efficient cluster management.

Some key concepts regarding personal clusters are as follows [7]:

- PN Cluster: collection of collocated devices in the personal network e.g. home cluster, office cluster, vehicle cluster, e-health cluster, etc.
- Personal device: Personal device is the device that owned by the user. User has all access rights of that device.
- Foreign device: Device owned by another user.

Thinking ahead, a large number of PN around us will offer services, how to filter the services that the user requires? And services should be granted only to authorized users, how to apply authentication and authorization with such resource constrained devices? Most of the IoPTS communication will happen through existing wireless technologies and wireless communications, which are more prone to security attacks. Hence, to support privacy, user authentication must be done with minimal disclosure of personal information. Concisely, a semantic service discovery framework is required to announce the services offered by the cluster, as well as authentication and access control policies with minimal personal information disclosure from the user side. Requirements of the user-cluster interaction are depicted in Fig 1. The cluster of IoT devices is formed depends on the logical relationship between them e.g. Location. Every cluster selects one device as cluster head that responsible for the announcement of services. Cluster head is also responsible for authentication and access control to allow foreign device to access offered services. The service manager module offers the service to the user depends on user's attributes and priority. Fig.1 shows the framework requirement for realizing IoPTS.

III. Related work

Parallel to MAGNET and MAGNET Beyond[8], a number of related projects were running under the EU 6thFramework Programme, e.g. Personal Distributed Environment (PDE), Ambient Networks (AN), Security for Heterogeneous Access in Mobile Networks (SHAMAN), Power Aware Communications For Wireless Optimized Personal Area Network (PACWOMAN), Mynet , P2P Universal Computing Consortium (PUCC), Mobile Grouped Devices(MOPED), Service Platform for Innovative Communication Environment (SPICE) and Global RFID-related Activities and Standardization (CASAGRAS).

The PDE project [9]aimed to provide a solution to interconnect user's personal devices. The devices may be near to the user or geographically distributed far from the user. Every device is connected to the PDE server and updates its location, capabilities and services to the device management entity (DME). The user can access the service provided by any device through the PDE server. However in PDE privacy and context awareness are not addressed.

AN [10]aimed to develop network solutions for mobile and wireless systems beyond 3Gand provide on-demand connection to any network available, depending on user requirements. The SHAMAN project aimed to provide security and trust framework for PANs [11],[12]. The security model depends on the trust between device and owner. The trust model implemented depends on the personal certificate authority that runs on the user device using the public-private key pairs. PACWOMAN [13]was dealing with WPANs and ad hoc networking. PACWOMAN differentiated the need of data rate for sensors and low powered devices. The project aimed to create three different networking spaces: PAN, community network and WAN. To provide seamless communication between geographically distributed personal devices PACWOMAN worked on the link layer and medium access layer for PAN.

However, the requirements of IoPTS such as naming, service management, security, trust management privacy and the context awareness were not addressed by these projects.

PUCC [14]addressed the seamless peer-to-peer communication between networked devices and the communication between IP networks and non-IP networks. It also developed a service integration and discovery framework. The Mynet project [15]aimed to provide a simple and secure overlay network for personal networks, based on a trust model and social connectivity. It proposed a personal namespace for the user to access his/her devices irrespective of location.

The MOPED project [16]provided a communication framework for personal devices, using a single IP address to access all personal devices. A proxy node is selected, and an IP address is assigned to it. The proxy node maintains the information of all personal devices and provides the communication link between them. MOPED supported mobility, addressing and routing, but it is not applicable to IOPTS as security, privacy and context awareness were not addressed.

The SPICE [17]provided a framework for mobile services, combining several technologies such as context awareness, semantic middleware, and service brokering. It proposed a four-layered architecture: Capabilities and Enablers Layer, Component Services Layer, Knowledge Layer, and the Value Added Services (VAS) Layer. In the SPICE project a single sign-on approach is used for authentication.

The CASAGRAS [18]aimed to provide the relation and framework for RFID with the IoT. In particular, the objective of CASAGRAS was to provide requirements, regulations and standardization of RFID for realizing the IoT.

The frameworks discussed above contain many promising features, but they have not yet been applied in an IoPTS setting.

IV. USER REQUIREMENTS AND SCENARIOS

In the following, different types of scenarios will be discussed, describing the need for organizing a large number of devices in the cluster and the need for context-aware service discovery. The detailed scenarios also explain the requirement of a strong authentication and access control mechanism with minimal personal information disclosure.

A. Home Management

Control of home equipment such as air conditioners, refrigerators, washing machines, etc., which helps to reduce energy bills and to control functions in the environment.

In this scenario one or more clusters of devices should be formed in the home, each cluster having a cluster head. Every sensor/device in the home can collect data and forward them to the cluster head, which then analyzes the data, performs appropriate actions or upload the data to the cloud. If there are more clusters in the home, the cluster head may be connected to an intermediate gateway, which will handle the common functionality. The owner of the home can retrieve data from the cloud and take appropriate actions. The cluster head can control the environment of the home depending e.g. on the weather and the timing, when the owner enters the home. In the morning a person may return from gym/jogging to the home, and he might get the message that bathtub is already prepared for him to take a bath. Depending on the timing and the weather different music modes could be set. When the person is in the gym, unusual changes in his heartbeat could be sent to his physician with the help of his Smartphone, human implantable sensor devices like the AppleWatch. Strong access control mechanism is required, so only the family physician could get the medical information.

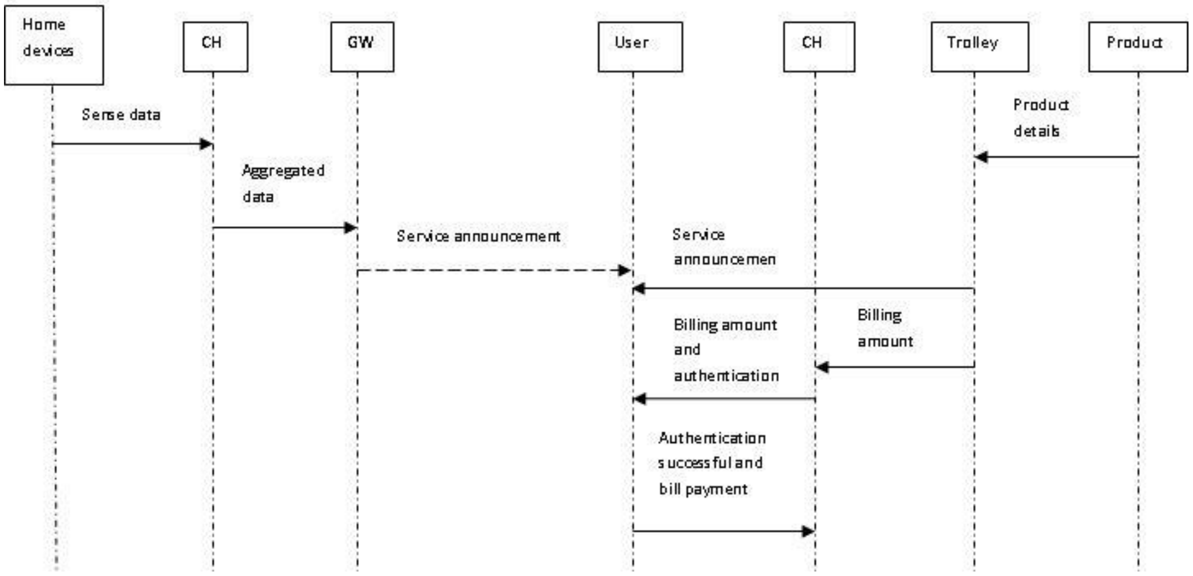

Fig. 2 Shopping Mall Scenario

The scenario requires clustering of the home devices, authentication mechanisms to use the services offered by the home cluster(s), and a context-aware service discovery mechanism to select services depending on user profile and requirements. Depending on the type of user (owner of the home, kids, maid, family, friends or other visitors) different access control policies should be maintained by the cluster head(s).

B. *Enterprise*

Sensors have always been an integral part of the factory setup for security, automation, climate control, etc. It will eventually be replaced by a wireless system giving the flexibility to make changes to the setup whenever required. It is nothing but an IoT subnet dedicated to factory maintenance. In this scenario, a few clusters could be constructed depending on deployment area of the WSN. Secure communication is required between the sensor clusters and the enterprise server(s). The sensed data will again be forwarded to the cluster head(s) and further to the company server or to the cloud. The enterprise may have branches at different locations, and. some applications may require analysis of the information from sensors of each branch to take further action. The traditional web service approach is not applicable the scale of IoT, and a RESTful approach may be required to interact with each object. Depending on the relevant user profiles (project manager, project member, other staff, or visitors) different access policies and authentication mechanisms should be applied.

C. *Car cluster*

The user wants to access services provided by a car cluster. In this scenario, cluster formation of the devices/sensors in the car is needed. Depending on the user profile (car owner, car driver) different services of the car could be provided, and different authentication and access control mechanisms will be required.

D. *Looking after elderly people or kids*

A trusted user wants to monitor an elderly person's or a kid's health, irrespective of the user's location. In this scenario the communication between the personal cluster of the elderly person or kid and that of the user is required. On the Smartphone, the trusted user may get notifications on any unfavorable change in the health conditions. If desired, the Smartphone may suggest the nearest physician and simultaneously send the health record to the family physician through cloud services. The information should be given only to authorized persons; hence strong authentication and access control mechanism will be required.

E. *Supermarket*

The user is walking around in the supermarket. The user's shopping trolley vibrates and displays a message: "There is no milk in your fridge". The user's fridge has identified that there is no milk and has sent a message to user phone. The phone knows that the user is in the supermarket. The user trolley knows that the user right now is next to the milk fridge and has recommended the user to buy milk. After purchasing, the trolley may calculate the amount the user needs to pay and send the amount information to the counter. Interaction between the user's home cluster and the shopping mall cluster is depicted in Fig.2.

This scenario requires cluster formation of the home devices and the shopping mall devices. The home cluster should forward the info about fridge to the user's Smartphone, but the Smartphone should only provide an alert to the user when it is relevant and appropriate, e.g. when the user is leaving office or is at/near shopping mall. Context-aware service discovery should be done. Access control mechanisms and user profile management are also required in this scenario.

F. Hospital

A person has been admitted at the hospital due to a heart disease. An internal heart monitor implanted into the person's arm constantly monitors his heart rate and detects changes. If there is a critical change in heart rate, it sends a message to the physician and updates the health record stored at the hospital database. Accordingly, the physician can monitor and update the recovery plan. The health record should only be accessed by the authorized physician. Different access policies should be applied to the hospital staff depending on their role, i.e. physician, nurse, and other staff. Communication between the user's personal cluster and the hospital infrastructure is required.

G. Cab service

The user needs to go out of office for a meeting. In the PN scenario the user doesn't need to call a cab. The user's Google calendar updates the entry of meeting on the user's phone. Depending on the user's preferences and profile the Smartphone informs the office that user is leaving for the meeting. Again depending on user preferences, a self-driving Google cab may arrive at the front gate. This scenario requires communication between the user's PAN, the office cluster, and the car cluster. Context-aware service discovery and user profile management are required to take the appropriate action depending on the user's schedule. Strong authentication and authorization mechanisms are required to access and communicate with office database as the Smartphone makes an entry when the user is leaving. The user's location should not be disclosed to others.

H. Collaborative work

A company may have several divisions and depending on the application requirement the team members of a project may need to access information/resources of any division. When a team member visits another division, he must get access to the information/resources. Clustering of company devices and personal devices is required in this scenario. Further, different access policies and authentication mechanisms are required depending on different user roles, i.e. project manager, team leader, team member, and supplementary staff. When the team member comes back to his division, his personal cluster should seamlessly connect with the office cluster.

I. At the airport

The user enters the airport, gets an alert on his smart device showing the different services available at the airport, e.g., a map of the airport, the current waiting times in the security check area, airline services etc. At the check-in desk, another alert informs him that due to the technical snag his flight is delayed by a couple of hours, and lunch e-vouchers are provided by airlines. After reaching his destination, he may require guidelines for sightseeing, shopping and food facilities. Different clusters of devices at destination premises may assist in providing such guidelines depending on the user interests and preferences. The scenario requires clustering of devices at airport, devices at the destination premises and the user's personal devices. Context-aware service discovery is required to get offers depending on the user profile and attributes. The user should only be notified about the waiting for the flight he planned to take up. The lunch e-vouchers and details of the flight should be revealed to authorized person only. The user's personal information, i.e. his location and travel plans, should not be disclosed.

J. Summary

Table 1 summarizes the user profiles and requirements for scenarios discussed in this section.

TABLE I. USER PROFILES AND REQUIREMENTS

Scenario	**User Role / Profile**	**User Requirements**
A	Home Owner	Get notifications from all devices, access to all devices for usage, can switch on/off all devices, and can change the operating modes of devices.
	Kid/ Children	Access to limited devices depending on age group, i.e. no or limited access to electronic equipment.
	Family or Friends	Can't change the operating modes of few devices. Access to limited devices depending on privacy/security i.e. laptop, mobile, PDA.
	Guest	Access to very few devices. (Less than a family / friend profile)
B	Owner	Access to all devices/sensor/resources, can analyze data from all sensors deployed in the enterprise. Set default parameters to sensors
	Project Manager (PM)	Access to devices/resources/sensors of application that is assigned to him. Can modify parameters of few sensors
	Project Member	Limited access rights
C	Car owner	Access to all devices/sensor services in the car. Can check pressure, fuel leakage, fuel level, car location, can change the speed limit. Play songs that are stored at the home computer.
	Car driver	Restricted access rights i.e. can't change speed limits and can't switch off the GPS
D	User	Can access and monitor the health record.
	Physician	Access to health record, can modify recovery plan
E	User	Access to all devices at home, restricted access to devices at the shopping mall
	Worker at Shopping Mall	Access to all devices at mall, can modify the operating mode of devices at mall, can modify the database(price change, discount prize)
F	Physician	Access to health record, can modify recovery plan
	Nurse	Can view health record but couldn't modify the recovery plan
G	User	Access to office database, can modify the

		schedule of meeting
H	Team Member of the same division	Access to all devices and can modify the device parameters, database as per application requirement
	Team Member of different division	Limited access to devices and database.
I	Traveler	Access to map of the airport, waiting time, gate numbers
	Officers at the airport	Access to sensors/devices, database and can modify the database.

From the above scenarios, it can be concluded that structured organization of IoT devices (clusters) and selection of cluster head are basic requirements for IoPTS. Following are some of the key requirements of the cluster framework of IoPTS:

- The cluster formation must consider heterogeneity, as in the world of IoPTS thousands of heterogeneous devices will be communicating with each other.
- The clustering algorithm must identify own nodes and foreign nodes.
- The cluster must support mobility.
- Cluster communication must be secured.
- Cluster head selection should be done on the basis of logical connection between devices as well as processing capability and energy of the node.
- Strong authentication and authorization mechanism should be managed by the cluster head to grant the access to service offered by the cluster.
- Context-aware service discovery and profile / role management should be provided.

V. Conclusion

Due to economics of scale in the future IoPTS, structured organization of devices is a big challenge. In order to address the user requirements and functionalities we have analyzed a number of scenarios. In particular, we focus on the interaction between the users and the IoT clusters, where the user profile (role, privileges, and preferences) should be matched with the services offered by the IoT cluster, including the initial set-up, access control, authentication, and authorization. In the literature a lot of work has been done on Personal Networks (PNs), however the proposed mechanisms have yet not applied to IoPTS settings. There is a need for a clustering framework that provides seamless communication between the user's Personal Cluster and diverse clusters of devices. To access the services offered by a cluster there is a need for a service architecture that can match user requirements, profile and privileges to access the available services.

References

[1] "IERC-European Research Cluster on the Internet of Things." [Online]. Available: http://www.internet-of-things-research.eu/about_iot.htm. [Accessed: 16-Mar-2015].

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, Feb. 2014.

[3] "Internet of Things (IoT): A vision, architectural elements, and future directions - Internet-of-Things-Vision-Future2013.pdf." [Online]. Available: http://www.buyya.com/papers/Internet-of-Things-Vision-Future2013.pdf. [Accessed: 03-Mar-2015].

[4] "TheInternetofThings-BerlinERIN.dvi - The Internet of Things.pdf." [Online]. Available: http://www.theinternetofthings.eu/sites/default/files/%5Buser-name%5D/The%20Internet%20of%20Things.pdf. [Accessed: 03-Mar-2015].

[5] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: Vision amp; challenges," in 2013 IEEE TENCON Spring Conference, 2013, pp. 218–222.

[6] M. A. Uusitalo, "Global Vision for the Future Wireless World from the WWRF," IEEE Veh. Technol. Mag., vol. 1, no. 2, pp. 4–8, 2006.

[7] M. Jacobsson, I. Niemegeers, and S. H. de Groot, Personal Networks: Wireless Networking for Personal Devices. John Wiley & Sons, 2011.

[8] R. Prasad, My personal Adaptive Global NET (MAGNET). Springer Science & Business Media, 2009.

[9] S. K. Goo, J. M. Irvine, and R. C. Atkinson, "Personal distributed environment securing the dynamic service platforms beyond 3G," in 3G Mobile Communication Technologies, 2003. 3G 2003. 4th International Conference on (Conf. Publ. No. 494), 2003, pp. 18–22.

[10] M. Vorwerk, S. Schuetz, R. Aguero, J. Choque, S. Schmid, M. Kleis, M. Kampmann, and M. Erkoc, "Ambient networks in practice instant media services for users on the move," in 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006, 2006, p. 2 pp.–238.

[11] "Microsoft Word - D13_V1.doc - D13_V1.pdf." [Online]. Available: http://www.isrc.rhul.ac.uk/shaman/docs/D13_V1.pdf. [Accessed: 03-Mar-2015].

[14] N. Ishikawa, "PUCC Activities on Overlay Networking Protocols and Metadata for Controlling and Managing Home Networks and Appliances," Proc. IEEE, vol. 101, no. 11, pp. 2355–2366, Nov. 2013.

[15] D. N. Kalofonos, Z. Antoniou, F. D. Reynolds, M. Van-Kleek, J. Strauss, and P. Wisner, "MyNet: A Platform for Secure P2P Personal and Social Networking Services," in Sixth Annual IEEE International Conference on Pervasive Computing and Communications, 2008. PerCom 2008, 2008, pp. 135–146.

[16] "The MOPED Project | MOBIUS." [Online]. Available: http://mobius.cs.uiuc.edu/research/moped. [Accessed: 03-Mar-2015].

[17] "FP6 IST Project Spice." [Online]. Available: http://www.ist-spice.org/. [Accessed: 17-Mar-2015].

[18] "CSA for Global RFID-related Activities and Standardisation (CASAGRAS2) | CASAGRAS2 - INTERNET OF THINGS." [Online]. Available: http://www.iot-casagras.org/. [Accessed: 17-Mar-2015].