# Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things

Mahalle, Parikshit N.; Anggorojati, Bayu; Prasad, Neeli R.; Prasad, Ramjee

*Published in:*
Journal of Cyber Security and Mobility

*Publication date:*
2013

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

# Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things

Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad

*Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark;*
*e-mail: {pnm, ba, np, prasad}@es.aau.dk*

Received 15 September 2012; Accepted 17 February 2013

## Abstract

In the last few years the Internet of Things (IoT) has seen widespread application and can be found in each field. Authentication and access control are important and critical functionalities in the context of IoT to enable secure communication between devices. Mobility, dynamic network topology and weak physical security of low power devices in IoT networks are possible sources for security vulnerabilities. It is promising to make an authentication and access control attack resistant and lightweight in a resource constrained and distributed IoT environment. This paper presents the Identity Authentication and Capability based Access Control (IACAC) model with protocol evaluation and performance analysis. To protect IoT from man-in-the-middle, replay and denial of service (Dos) attacks, the concept of capability for access control is introduced. The novelty of this model is that, it presents an integrated approach of authentication and access control for IoT devices. The results of other related study have also been analyzed to validate and support our findings. Finally, the proposed protocol is evaluated by using security protocol verification tool and verification results shows that IACAC is secure against aforementioned attacks. This paper also discusses performance analysis of the protocol in terms of computational time compared to other

*Journal of Cyber Security and Mobility,* Vol. 1, 309–348.

existing solutions. Furthermore, this paper addresses challenges in IoT and security attacks are modelled with the use cases to give an actual view of IoT networks.

**Keywords:** access control, authentication, capability, Internet of Things.

## 1 Introduction

In the Internet of Things (IoT) [1, 2], every virtual and physical entity is communicable, addressable and is accessible through the Internet. These virtual and physical entities produce seamless communication and seamless service collaborating with users and other devices creating service oriented networks. The IoT is an emerging paradigm and makes the world of computing fully ubiquitous creating UbiComp, a term initially coined by Mark Weiser [3]. Due to rapid development in Radio Frequency Identification (RFID) [4] technology, Wireless Sensor Networks (WSN), actuators and mobile communication, it is possible to realize the IoT due to ubiquitous interactions between things and devices in an "anytime, anywhere and anything" form.

Any "thing" with sensing, communication and computation capability helps us to realize the IoT vision and there are many application areas possible due to these smart thing or objects. These IoT applications are categorized in four domains in [5]:

- Personal and Home – includes individual homes [6].
- Enterprise – includes scales of community [7].
- Utilities – includes national and regional scales [8].
- Mobile – includes IoT applications spread across multi-domain due to distributed connectivity and scale [9].

An example application area is intelligent home environment (personal) which mainly consists of places full of things that will interact with each other at different levels. There are different kinds of sensors and devices that use heterogeneous technologies; low bandwidth meshes networking based (such as ZigBee and Z-Wave) or other high bandwidth demanding (such as Bluetooth, WiFi, 4G or UWB) providing $24 \times 7$ monitoring or entertainment services. Other application area includes nomadic access to services where accessible services are discovered according to the user's identity and profile with the help of a mobile device. eHealth is the most important application of IoT, where sensors, actuators, RFID tags, etc., are applied in the health sector to facilitate ease of life service across geographic and time barriers.

The main challenges in these application areas are to ensure that ubiquitous access to services and monitoring data is granted to identities that fulfil the access control rules for identity management, heterogeneous device interaction, authorization, mutual authentication and secure delegation from a mobile device, and the secure data access. Securing user interactions with IoT is essential if the notion of "things everywhere" is to succeed. In such a scenario, security and privacy are two key challenges [10] that will determine the success or failure of a connected world.

The remainder of this paper is organized as follows: Section 2 presents the technological challenges and security challenges that need to be addressed to realize the notion of IoT. Section 3 presents the related works in authentication and access control. Threat analysis and attack modelling is presented in Section 4. Section 5 presents the proposed scheme for mutual authentication and access control. Evaluation of the proposed scheme using protocol verification tool and performance analysis is presented in Section 6. Finally, Section 7 concludes the paper with future work.

## 2 Challenges

As outlined in the scenarios and the applications above, it is clear that we are transforming from an Internet of computers to the Internet of things with device to device communication. In order to make the IoT services available at low cost with a large number of devices communicating to each other, there are many challenges to overcome. These challenges are divided into two categories in this paper as:

- *Technological challenges* – These challenges are related to underlined wireless technologies, energy, scalability, distributed and dynamic nature of IoT and ubiquitous interactions.
- *Security challenges* – These challenges are related to security services like authentication, privacy, trustworthiness and confidentiality. Security challenges also include heterogeneous communication and end-to-end security.

### 2.1 Technological Challenges

- *Wireless Communication*: IoT significantly uses convergence of established wireless technologies such as GSM, UMTS, Wi-Fi, Bluetooth and WPAN. These underlined wireless technologies use different stand-

ards and have different communication bandwidth requirement. This convergence also creates serious interoperability issues.

- *Scalability*: Unbounded number of devices creates the larger scope and scalability in IoT than conventional communication networks. IoT covers large application areas like a home environment where number of devices are relatively small in number to a factory or building that has a large number of devices offering multiple services to the users. IPV6 is one attempt to accommodate as many numbers of devices and things in IoT.
- *Energy*: IoT consist of constrained objects which do not have enough power, memory and computation capabilities. Designing lightweight protocols for IoT which minimize energy consumption is very important as compared to conventional protocols running on devices with sufficient resources.
- *Distributed and Dynamic Nature*: In IoT, things can interact with other things at any time, from anywhere and in any way independent of the location. As the IoT networks are distributed in nature, designing protocols for them is a challenging task. The objects interact dynamically and hence appropriate services for the objects must be automatically identified. In addition to this, the mobility/roaming of the objects is another important challenge.
- *Identification*: In the IoT, things include variety of objects like computers, sensor nodes, people, vehicles, medicines, books, etc. These things should be uniquely identified for the addressing capabilities and for providing a means to communicate with each other. After verifying the identities of things, we call these uniquely identified things as objects. Different identity schemes have been proposed for the IoT and it is predicted that it is dubious to have common identification schemes globally. Identification schemes like RFID Object Identifier, EPCglobal, Short-OID and Near Field Communications Forum, IPV4, IPV6 and E.164 have been studied in the literature. These addressing methods/principles are highly depends on the underlined access technology, thus it is challenging to have many different addressing protocols for varied underline access technologies.

## 2.2 Security Challenges

- *Privacy*: Privacy is one of the most sensitive areas in the context of IoT. In IoT, all objects are connected to the Internet and they communicate

with each other over the Internet. Hence the privacy issue is critical. As the Internet gets diversified with new types of devices and heterogeneous networks, IoT users and devices have to access the digital world with wide range of methods and protocols. Further, as ownership of these devices by the users does not exist, the issue of privacy is aggravated.

- *Identity Management*: Due to the scale of economics in the IoT, unbounded numbers of things or objects are involved in accessing IoT networks and communicating with each other. Hence, efficient and lightweight identity management schemes are required. In addition to this, the distributed nature of IoT makes this problem more challenging.
- *Trust*: Trust is an essential and integral factor to consider when implementing IoT. In an uncertain IoT environment, trust plays an important role in establishing secure communication between things. There should be an effective mechanism to define trust in a dynamic and collaborative IoT environment. It is also important to provide context aware trust management for varied IoT applications.
- *End-to-End Security*: End-to-end security measures between IoT devices and Internet hosts are equally important. Applying cryptographic schemes for encryption and authentication codes to a packet is not sufficient for the resource constrained IoT. Hence future research is required into efficient end-to-end security measures between IoT and the Internet.
- *Authentication and Access Control*: Authentication is identity establishment between communicating parties. Authentication and access control is important to establish secure communication between multiple devices and services. Interoperability and backward compatibility are the two key issues to be addressed. For example, in Wi-Fi roaming, devices use UMTS at the core networks.
- *Attack Resistant Security Solution*: Due to diversity of devices and end users, there should be attack resistant and lightweight security solutions. All the devices in IoT have low memory and limited computation resources, thus they are vulnerable to resource enervation attack. When the devices join and commissioned into the network, keying material, security and domain parameters could be eavesdropped. Possible external attacks like denial of service attack, flood attack, etc., on device and mitigation plan to address these attacks is another big challenge.

## 3 Related Works

There is ongoing research in the field of authentication and access control. This section presents state of the art in authentication and access control.

### 3.1 Authentication

There is much research done in the area of securing IoT. There is closely related work done in the MAGNET project [11, 12] where security associations take place with increased communication overhead and authentication is left unaddressed. The authors presented a distributed access control solution based on security profiles but attack resistance is not explored. In [13, 14], the authors have presented an ECC based authentication protocol but the major disadvantage is that it is not Denial of Service (DoS) attack resistant. As there are billions of devices in IoT, resistance to DoS attack is of vital importance. In [15], the author addressed the problem of secure communication and authentication based on a shared key and is applicable to limited location and cannot be used for wide area. It addresses peer to peer authentication but cannot be extended to a resource constrained environment.

There has been lot of debate about which of the cryptographic primitives like public key or private key is suitable for the IoT. Most of the research has mainly focused in areas like WSN and applications like healthcare and smart home. Many security mechanisms have been proposed based on private key cryptographic primitives due to fast computation and energy efficiency. Scalability problem and memory requirement to store keys makes it inefficient for heterogeneous devices in IoT.

A public key cryptography based solution overcomes these challenges because of its high scalability, low memory requirements and no requirement of key pre-distribution infrastructure. In [16], the author presented ECC based mutual authentication protocol for IoT using hash functions. Mutual authentication is achieved between terminal node and platform using secret key cryptosystem introducing the problem of key management and storage. Self-certified keys cryptosystem based distributed user authentication scheme for WSN is presented in [17], where only user nodes are authenticated. However, this is not lightweight solution for IoT. In [18], the author presented an authentication with parameter passing during the handshake. The handshake process is time consuming and based on symmetric key cryptography with more memory requirement for large prime numbers. Efficient identification and authentication is presented in [19] and is based on the signal properties of the node but it is not suitable for mobile nodes. The direction of the signal

is considered as a parameter for node authentication but it takes more time to decide the signal direction with more memory and computations involved. In [20], cluster based authentication is proposed which is most suited for the futuristic IoT, but an attacker can get hold of the distribution of system key pairs and cluster key. Generation of random numbers and signatures creates considerable computational overhead consuming memory resources.

Mobility is very important aspect of mobile and wireless communication and essentially in the context of IoT. With the heterogeneous network topologies like Wi-Fi, LTE and WiMax, authenticated service delivery with proper access control in place on the fly is a big challenge. Wireless Internet Service Provider roaming (WISPr) [21, 22] is an architecture, which proposes detailed specifications for allowing inter-operator roaming for Wi-Fi clients. Roaming functionalities in the vendor devices is based on the IANA Private Enterprise Number (PEN). WISPr enables users for roaming between different wireless Internet service providers. WISPr uses Remote Authentication Dial in User Service (RADIUS) [23] to provide centralized authentication and authorization. Analysis and security vulnerabilities of RADIUS have been discussed in [24] due to its centralized nature. Extensible Authentication Protocol (EAP) [25] is authentication framework being used in Wi-Fi. Security assessments of EAP have been discussed in [26] and explored many weakness points. Especially EAP do not address mutual authentication and not resistant to replay attack [26]. Key replication and replay attack on Authenticated Key Agreement (AKA) have been presented in [27] which clearly shows that there is even an identity is associated with AKA, it is prone to attack. Comparative studies on authentication and key agreement methods for 802.11 wireless LANs is presented in [28]. Weaknesses and security assessment of various authentication methods in the context of wireless networks is very well presented in [28]. General requirements for authentication and key agreement are classified into three mutually exclusive sets as: mandatory, recommended and additional requirements. A multi-layer agreement protocol is also proposed in [28]. This state of the art in mobile and Wi-Fi environment clearly shows that there is a need of flexible and secure authentication scheme.

State of the art evaluation is shown in Table 1. Related work is summarized based on the parameters like mutual authentication, lightweight solution, resistant to attacks, distributed nature and access control solution. Recent related work in the area of authentication for IoT is considered for the evaluation and is presented below.

Table 1 State of the art evaluation summary.

| Solutions | Parameters | | | | | | |
|---|---|---|---|---|---|---|---|
| | Mutual Authentication | Lightweight Solution | Attack Resistant | | | Distributed Nature | Access Control |
| | | | Dos | Man in middle | Replay | | |
| Ubiquitous Access Control in MAGNET [11, 12] | No | No | No | No | No | Yes | Yes |
| ECC based Authentication in RFID [13, 14] | Yes | Yes | No | No | No | Yes | No |
| Authentication in Ad-hoc Wireless Networks [15] | No | No | Yes | Yes | Yes | No | No |
| Authentication in IoT [16] | Yes | Yes | No | Yes | Yes | Yes | No |
| Authentication in WSN [17] | No | No | No | No | No | Yes | No |
| Progressive Authentication in Ad-hoc Networks [18] | Yes | Yes | No | Yes | Yes | No | No |
| Peer Identification and Authentication [19] | Yes | No | No | No | No | Yes | No |
| Authentication in Ad-hoc Networks [20] | Yes | No | No | No | No | Yes | No |

From Table 1, it is clear that not all existing solutions for authentication fulfil each and every requirement for IoT. The NO block in Table 1 represents the respective feature unavailability in the corresponding solution. Evaluation summary of the state of the art shows that all existing authentication solution in Wi-Fi environment and in the context of IoT do not address all the requirements like attack resistant, mobility and lightweight solution and mutual authentication.

## 3.2 Access Control

Controlling access to information or resources is usually done by defining access control rules, which decide who is allowed to access what and who is not. These rules take different forms such as RBACs, ACLs, policies, and so on. Before the development of standards based policy languages, interoperability was a major concern. It was with the emergence of the XACML proposal

[29], defined by OASIS, that identity management developers started thinking about how to make use of such standards based languages to define the set of policies, and to provide more standard solutions. In the IoT world, such standards based solutions are imperative due the distributed nature of the problem. XACML includes an XACML delegation profile in order to support administrative and dynamic delegation. The purpose of this profile is to specify how to express permissions about the right to issue policies and to verify issued policies against these permissions. This profile led to an identity federation scenario, is the key element upon the management of delegation policies. At the moment there is not a solution to define the relationship among the involved institution in a service interaction, neither a way to combine the decision taken by different organizations. There is currently no standard proposal related with the establishment of agreement at organization, federation or other trust domains levels. Examples of this kind of policies could be common information representation format, security requirements, levels of trusts, etc. This policy can be taken as a starting point for the definition of a negotiation mechanism about capabilities and policies, independently of the kind of entity involved on it. Policy and Charging Control (PCC) in LTE enables centralized mechanism for charging control and service-aware quality of service. PCC operates in S9 interface and consist of Policy and Charging Rule Function (PCRF) which controls the policies dynamically based on subscriptions and sessions between home PCRF and visited PCRF. Consider the scenarios of heterogeneous home M2M network in IoT based on LTE/4G. In this scenario, home gateway proactively and adaptively interacts with the surrounding radios in order to connect to home network and in turn to the external networks. Security policies protect the home M2M network from possible external attack via trusted access control and networked encryption technique.

Although XACML was the starting point towards the definition of standard policies, it is only focused on the resource access control type of policy. More or less at the same time, other kind of policies emerged to cover specific aspects for identity management, for example P3P [30], to define online privacy release information policies between end users and services. Current systems have incorporated these kinds of standard policies in some way, for example Shibboleth [31] and Liberty Alliance [32] providing definition of access control policies by means of XACML. However, there is a need to define policies in a standard way in the next generation of policy-driven systems when distributed scenarios in the IoT domain are considered.

It is equally important to discuss the state of the art in access control solutions. Traditionally, access control is represented by Access Control Matrix (ACM), in which the column of ACM is basically a list of objects or resources to be accessed and the row is a list of subjects or whoever wants to access the resource. From this ACM, two traditional access control models exist, i.e. Access Control List (ACL) and capability based access control. Many scientists [33, 34] have made comparisons between ACL and capability based access control and the conclusion is that ACL suffers from a confused deputy problem and other security threats while it is not the case in the capability based access control. Moreover, ACL is not scalable being centralized in nature and also it is prone to single point of failure. It cannot support different level of granularity and revocation is time consuming with lack of security. However, several drawbacks have been identified in applying the original concept of capability based model into access control model as it is to IoT. Gong [35] pointed out two major drawbacks of classical capability based model namely the capability propagation and revocation, and provide solutions to them by proposing a so called Secure Identity based Capability System (ICAP). Yet, Gong [35] did not clearly describe the security policy that is used in the capability creation and propagation. It also did not consider context information in making access control decision upon access request from a subject or user.

Nowadays Internet and web based applications are widely used and different types of access control models have appeared, such as Role Based Access Control (RBAC), Context Aware Access Control (CWAC), Policy Based Access Control, etc. Among others, RBAC is considered to be the most famous access control method in terms of the usage and implementation. In [36–42] extensions of the RBAC model are presented. As mentioned in [34], the RBAC model is essentially a variation of identity based access control to which ACL is sometimes referred, which seeks to address the burdens of client identification. Therefore, the RBAC model is still vulnerable to confused deputy problem as is the case with an ACL based model. Moreover, due to the role based structure in RBAC, it is not a generic model. As access permissions to the entities can be assigned through roles only, it has limited granularity. Scalability and delegation is critical in RBAC and it is not time efficient for micro level access. In [37], the authors presented General Temporal RBAC (GTRBAC), a RBAC based model that capable in expressing a wide range of temporal constraints, in particular periodic as well as duration constraints on roles, user-role assignments, and role-permission assignments. An example of GTRBAC's usage in the real world application is in defining access rights

to employees in a company who work based on shifts, e.g. morning, afternoon, and night shift, and also for people who work on short term contracts, and many others. However, it is not able to describe the limitation of any context other than periodic or time duration. Bhatti et al. [38] addressed the issues in XACML as well as GTRBAC with emphasize in formal definition of context, and introduction of trust model with RBAC and XML main features. However, the scope is only limited to web service environments and hence not really suitable to the IoT. Privacy aware RBAC is presented in [39] and compared with XACML but its application to IoT is unclear.

In [40–42], the authors addressed the issue of role and/or permission delegation based on the RBAC model. However, unlike Barka and Sandhu [40, 41], Hasebe et al. [42] considered delegation of roles and permissions in a cross-domain environment by using capability, and thus it is called Capability RBAC (CRBAC) model. The main idea of CRBAC is essentially similar to what has been proposed in [35], i.e. by using capability transfer or propagation in order to delegate roles or permissions. However, the main aim of using capability is limited to delegation only, thus it does not exploit the capability fully. Moreover, explanation of the revocation of delegation or capability transfer was not discussed, plus other drawbacks related to [39] and RBAC as described earlier are also applicable here.

In CWAC [43], the surrounding context of the subject and/or object is considered to provide access. Scalability is again a problem with CWAC. Delegation and revocation is not supported completely in CWAC. In CRBAC [44], context is integrated with RBAC dynamically. Context is defined as characterization of surrounding entities for performing appropriate actions. Improper association of context and role results in scalability and time inefficiency. Further, the delegation is not simple due to context dependency. There are many examples like context aware patient information system and context aware music player where applying role based access control is a cumbersome process.

Comparison of these access control models is shown in Table 2. Comparison is based on functional parameters such as generic nature, scalability, granularity, delegation, time efficiency, and security.

State of the art for authentication and access control shows that there is no integrated protocol for authentication and access control. The objective is to achieve mutual identity establishment, i.e. authentication and once authenticated, access control will take place. This paper proposes a new method of authentication of devices and access control for the IoT resources using public key approach with scalability and less memory requirements. The most

Table 2 Comparison of different access control models.

| Models | Generic | Scalable | Granular | Delegation | Time Efficient | Security |
|---|---|---|---|---|---|---|
| ACL | Yes | No | No | No | No | No |
| RBAC | No | No | Yes | Yes | No | No |
| CWAC | Yes | No | Yes | No | No | No |
| CRBAC | Yes | No | Yes | Yes | No | No |
| CCAAC | Yes | Yes | Yes | Yes | Yes | Yes |

important design issue of IoT is the mobility of heterogeneous devices and proposed scheme works efficiently for this need.

## 4 Threats and Attacks Modelling

An important endeavour of this paper is to model the activities of IoT attacks to understand the sequence of actions taking place when the attacks are happening. The modelling of the security attacks helps to understand an actual view of the IoT networks and enable us to decide the mitigation plans.

In the IoT, the possible communications are device to device, human to device and human to human giving connection between heterogeneous entities or networks. Figure 1 presents general use case of IoT, where MobileEntity(x): A mobile device represents an entity, i.e. any device in the network which communicates with other entities of same type or of different type via Internet or direct. MobileEntity 1, 2, 3 represent three different and most probable scenarios in the system of communication. Use Cases are self-explanatory and attackers are at the top of the diagram.

- *Man-in-the-Middle Attack*: When the devices are commissioned into a network, keying material,security and domain parameters could be eavesdropped. Keying material can reveal the secret key between devices and authenticity of the communication channel could be compromised. Man-in-the-middle attack is one type of eavesdropping possible in the commissioning phase of devices to IoT. The key establishment protocol is vulnerable to man-in-the-middle attack and can compromise device authentication as devices usually do not have prior knowledge about each other. As device authentication involves exchange of device identities, identity theft is possible due to man-in-the-middle attack. Sample use case for man-in-the-middle attack is shown in Figure 2.

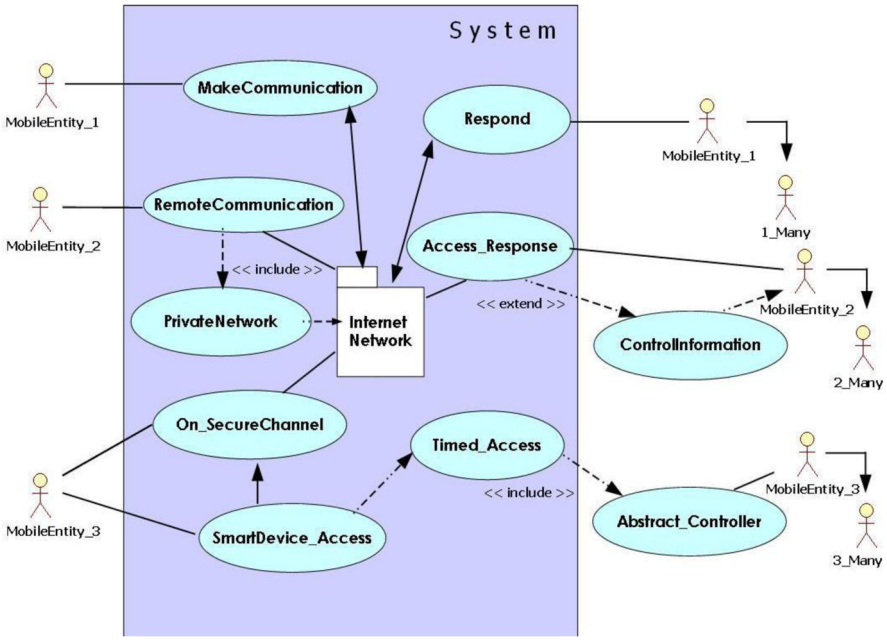


Figure 1 IoT use case.

- *Denial of Service Attack*: All the devices in IoT have low memory and limited computation resources, thus they are vulnerable to resource enervation attack. Attackers can send messages or requests to specific device so as to consume their resources. This attack is more daunting in IoT since attacker might be single in number and resource constrained devices are large in numbers. DoS attack is also possible due to man-in-the-middle attack. Sample use case of DoS in IoT scenario is shown in Figure 2.
- *Replay Attack*: During the exchange of identity related information or other credentials in IoT, this information can be spoofed, altered or replayed to repel network traffic. This causes a very serious replay attack. Replay attack is essentially one form of active man-in-the-middle attack. Our solution prevents replay attacks by maintaining the freshness of random number, for example by using time stamp or nonce by including Message Authentication Code (MAC) as well. A sample use case is shown in Figure 2.

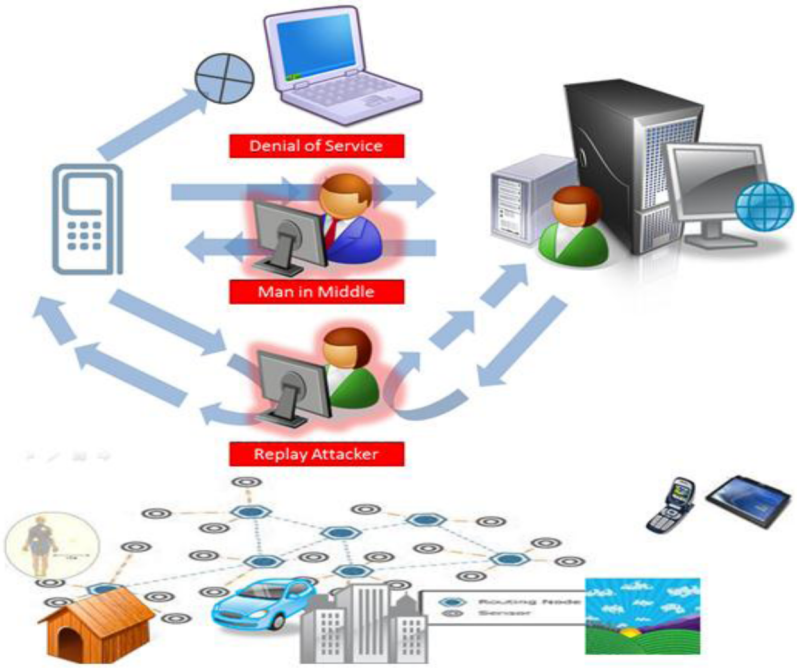


Figure 2 IoT security attacks modelling.

For this purpose, authentication and access control are main security issues which are to be addressed. This paper presents an integrated lightweight solution for authentication and access control with the protocol evaluation.

## 5 Proposed IACAC Model

As stated earlier, mobility is very important aspect of wireless communication and essentially in the context of IoT. With the heterogeneous network topologies like Wi-Fi, LTE and WiMax, authenticated service delivery with proper access control is major problem to be addressed. Wireless Internet Service Provider roaming (WISPr) [21, 22] and RADIUS [23] are the existing solutions to provide centralized authentication and authorization in Wi-Fi. Related work in security analysis [24–28] shows that there is a need of attack resistant and integrated approach for authentication and access control. Security flaws of authentication and access control protocols have been studied in [45] in the context of mobile communication. Required goals for

authentication protocols between mobile entities and fixed networks have been presented in [46], which includes mutual authentication, confidentiality and the attack resistance. Hybrid cryptography based authentication scheme is presented in [47], which is prone to attack on key share and replay attack. Aziz and Diffie [48] proposed mobile authentication and key agreement protocol based on public key cryptography, but it is prone to impersonation attack [49]. The Wong–Chan mobile authentication protocol [50] is vulnerable to DoS attack where malicious initiator can disturb the execution of protocol through bogus request. This makes the Wong–Chan scheme not suitable for resource constrained environment.

This paper presents an Identity Authentication and Capability based Access Control (IACAC) scheme for the IoT to replace the existing schemes. IACAC is compatible with underline access technologies like Bluetooth, 4G, WiMax and Wi-Fi. IACAC presented in this paper is implemented in a Wi-Fi environment and the performance results are discussed in next sections.

The algorithm presented in this paper addresses both authentication and access control which are divided into three parts:

- Secret key generation based on Elliptical Curve Cryptography-Diffie Hellman algorithm (ECCDH),
- Identity establishment,
- Capability creation for access control.

### 5.1 Secret Key Generation Based on ECCDH and Identity Establishment for Authentication

There is considerable interest in ECC for IoT security [51]. It has advantages of small key size and low computation overhead. It uses public key cryptography approach based on elliptic curve on finite fields. ECCDH [51] is a symmetric key agreement protocol that allows two devices that have no prior knowledge about each other to establish a shared secret key which can be used in any security algorithm. Using this public parameter and own private parameter, these parties can calculate the shared secret. Any third party, who does not have access to the private details of each device, cannot calculate the shared secret from available public information. All devices joining IoT share key pairs during the bootstrapping. The IACAC scheme presented in this paper is also applicable to security bootstrapping. Security bootstrapping is the process by which devices join the IoT with respect to location and time. It includes device authentication along with credential transfer. Protocol uses one or more trusted Key Distribution Center (KDC) to generate domain paramet-

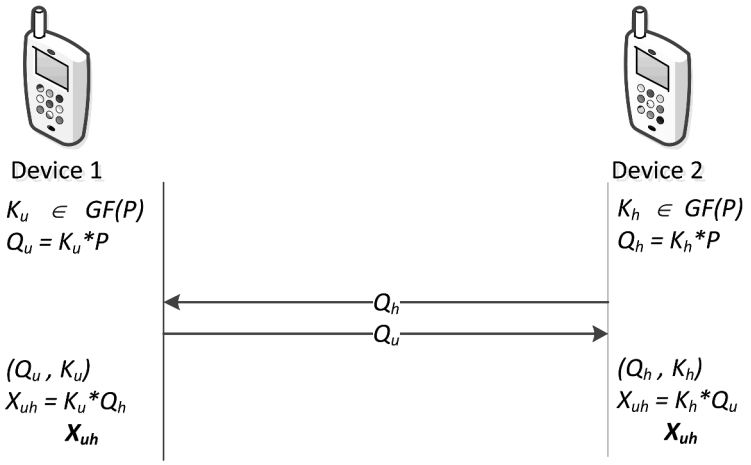


Figure 3 ECCDH for establishing shared secret key.

ers and other security material and important part is this KDC is not required to be online always. Initially KDC randomly selects particular elliptic curve over finite field $GF(p)$ where $p$ is a prime and makes base point $P$ with large order $q$ (where $q$ is also prime). KDC then picks random $x \in GF(p)$ as a private key and publishes corresponding public key $Q = x \times P$. KDC generates random number $Ki \in GF(p)$ as a private key for device $i$ and generates corresponding public key $Q_i = Ki \times P$. The key pair $\{Q_i, K_i\}$ is given to device $i$. With the increasing number of devices, KDC can generate an ECC key pair based on base point $P$ for any number of devices as it is rich in terms of resources as compared to other devices in IoT. These ECC key pairs will be used to share common secret key for secure communication using ECCDH and is explained below. Steps of aforementioned ECCDH are shown presented in Figure 3.

The assumption here is that ECC is running at trusted KDC. There is an agreement on system based point $P$ and generate $(Q_u, K_u)$ and $(Q_h, K_h)$ pairs where $Q_u$ is the Public key of Device 1; $K_u$ is the secret key of Device 1; $Q_h$ is the public key of Device 2; and $K_h$ is the secret key of Device 2. Furthermore, $P$ is large prime number over $GF(P)$ and generations of above keys are shown in Figure 3.

No parameter is disclosed in this process of establishing a shared secret key other than domain parameter $P$ and public keys. In this paper, we consider sensor nodes as a device, because the functionalities and operational

principle of wireless sensor networks makes it an appropriate and mandatory candidate of the IoT.

## 5.2 Protocol for Identity Authentication

### 5.2.1 One Way Authentication

One way authentication authenticates Device 1 to Device 2 and is explained below. As per above ECCDH, both Device 1 and Device 2 have $X_{uh}$ as a common secret key. Device 1 selects $r \in GF(P)$ which will be used to create session key. $T_u$ is generated as a time stamp by Device 1. It is assumed that synchronization is taken care using appropriate mechanism. The secret key is created by Device 1 as $L = h(X_{uh} \oplus T_u)$. Then Device 1 encrypts $r$ with secret key $L$ as $R = E_L(r)$ and encrypts $T_u$ by $X_{uh}$ as $T_{us} = EX_{uh}(T_u)$. After this Device 1 builds a Message Authentication Code (MAC) value as $\text{MAC}_1 = \text{MAC}(X_{uh}, R \| \text{ICAP}_1)$ where $\text{ICAP}_1$ is a data structure representing an identity based capability for this Device 1 giving access rigts. Details about ICAP are given in the same section below. Now Device 1 sends the following parameters to Device 2 directly or through gateway node/coordination node or access point as $(R, T_{us}, \text{MAC}_1)$. Device 2 generates its current time stamp as $T$ current and Device 2 will decrypt $T_{us}$ to get $T_u$ and compare it with $T_{\text{current}}$. If $T_{\text{current}} > T_u$, it is valid. Now Device 2 calculates $L$ and decrypts $R$ to get $r$. Device 2 also calculates the $\text{MAC}_1'$ and it will verify this with the $\text{MAC}_1$ received from Device 1. If valid, then Device 1 is authentic to Device 2. Device 1 also matches the $\text{ICAP}_1$ received with $\text{ICAP}_2$ stored at Device 2. If Device 2 gets a match with $R$, $\text{MAC}_1$, $T_{us}$, then Device 1 is authenticated to Device 2. This protocol is presented in Figure 4.

### 5.2.2 Mutual Authentication

This part of authentication authenticates Device 2 to Device 1, and is explained in Figure 5. Device 2 builds a MAC as $\text{MAC}_2 = \text{MAC}(r \| \text{ICAP}_2)$ and also encrypts $r$ with $X_{uh}$ as $R' = EX_{uh}(r)$. Device 2 sends $(R', \text{MAC}_2)$ to Device 1. Device 1 verifies $\text{MAC}_2$ and decrypts $R'$ and compares received $r$ with this $r$ (denoted as $r'$ and $r''$ in Figure 5). If a match is found, Device 2 is also authenticated to Device 1 and communication and access will be granted based on the $\text{ICAP}_2$. This protocol achieves both mutual authentication along with capability based access control in secure way.

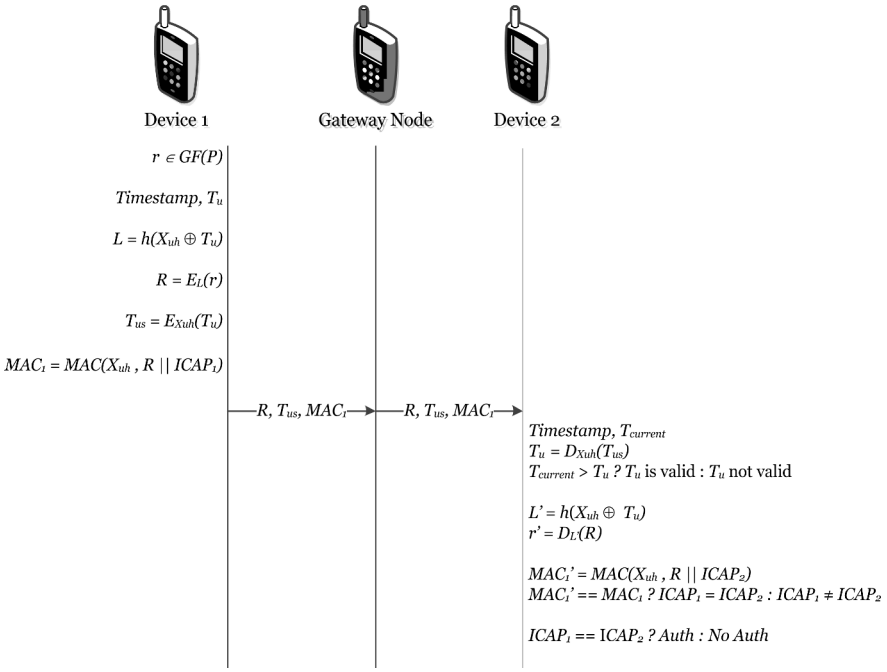


Figure 4 One way authentication protocol.

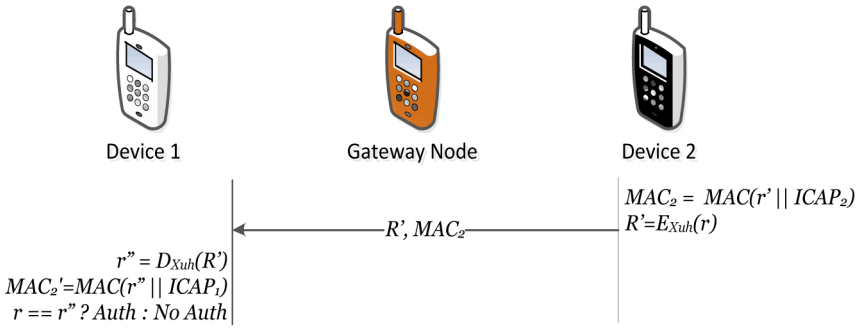


Figure 5 Protocol for mutual authentication.

### 5.2.3 Capability Creation for Access Control

Conceptually, a capability is a token that gives permission to access device. A capability is implemented as a data structure that contains two items of information: a unique device identifier and access rights. A capability structure is presented in Figure 6. For simplicity, it is sufficient to examine the

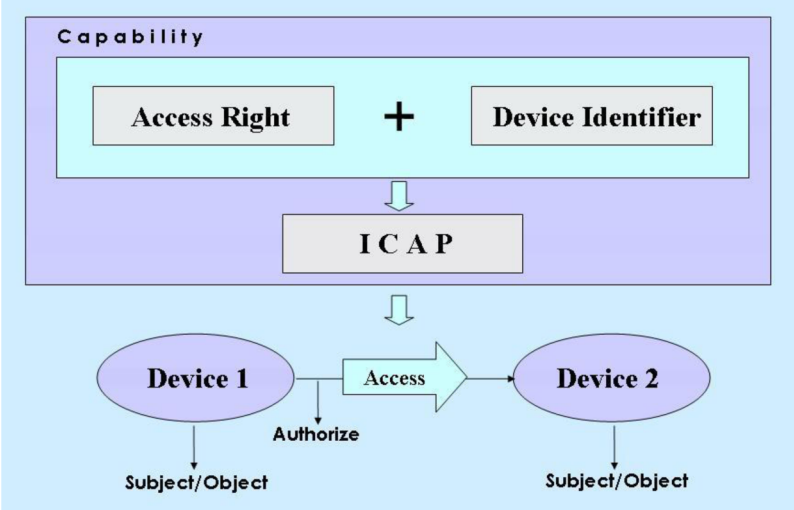


Figure 6 Capability structure.

case where a capability describes a set of access rights for the device. The device which may also contain security attributes such as access rights or other access control information. The ICAP [35] was essentially extending the capability system concept, in which the capability is used by any user or subject that wants to get access to a certain device or resource.

If the capability that is presented by the subject matches with the capability that is stored in the device or an entity that manages the device, access is granted. However, unlike the classical capability based system, ICAP introduced the identity of subject or user in its operation. In this way, it claimed to reduce the number of capabilities stored in the so-called "Object Server", "Gateway" or "Access Point" and thus offers more scalability. Moreover, it has better control in capability propagation which provides more efficient access later on. The ICAP structure and how capability is used for access control is shown in Figure 6. ICAP is represented as

$$\text{ICAP} = (\text{ID}, \text{AR}, \text{Rnd}) \tag{1}$$

where ID presents the device identifier; AR the set of access rights for the device with device identifier as ID; and Rnd the random number to prevent forgery and is a result of one way hash function as: $\text{Rnd} = f(\text{ID}, \text{AR})$. In IACAC, access rights are sent in the form of a MAC value in the authentication process. Implementation works in two stages. First, the devices are

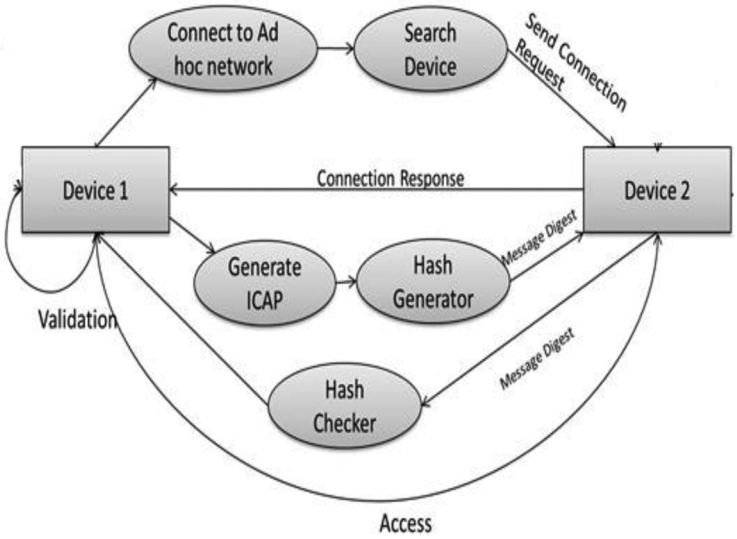


Figure 7 High level functioning of CAC.

connected with each other through the use of an access point and then the capability based access is allowed to the other device through Capability based Access Control (CAC). Each communication that is to be established is verified by its capability access. Only after the capability verification the devices are able to communicate with each other. Any device wants to communicate with other device is able to initiate the communication by sending the request to a specific device. The second stage is to verify whether that requesting device is having the capability to communicate with called device. This access right gets checked using the capability of that device which is associated with every device. For sending capability message digest using SHA-1 is generated for each device as stated earlier and the remote device will check its validity using SHA-1. Figure 7 depicts high level functioning of CAC.

The complete CAC scheme is presented in Figure 8. Figure 8 shows access based on CAC between two Wi-Fi devices. In this paper, we treat all devices as subjects and resources to be accessed as objects. In this implementation of CAC, file is considered as object for access. Access rights (AR) is given as

$$\text{AR} \in \{\text{Read, Write, NULL}\} \tag{2}$$

AR can either be {Read}, {Write}, {Read, Write} or {NULL}. If AR = {NULL}, the permission to access particular object is not allowed. Once the capability is verified against forgery, both devices are able to perform an operation as specified in capability and access is granted. As any device can perform only those operations as specified in capability, principle of least privilege is supported to a large extent.

## 6 IACAC Evaluation and Analysis

### 6.1 Protocol Evaluation

The evaluation will focus on identity authentication in terms of one way and mutual as the most important processes in the authentication. The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [52] based on the Dolev–Yao model [53] is used for model and protocol verification. We implement the aforementioned protocol in stages. The first stage of protocol authenticates Device 1 to Device 2, i.e. one way authentication, and the second stage is for mutual authentication, i.e. authenticates Device 2 to Device 1. The verification results are described below.

#### 6.1.1 Evaluation Procedure

In order to carry out the evaluation using AVISPA some assumptions are made. Both devices have already obtained ECC based shared key using Diffie–Hellman (ECCDH). As stated earlier, assumption here is that KDC is secure and trusted. Complete protocol evaluation is presented in the following model:

$$D_1 \rightarrow D_2 : [R, T_{us}, \mathrm{MAC}_1]; [\{r\}_L, \{T_u\}\_X_{uh}, \mathrm{RND}_1]$$

$$D_1 \leftarrow D_2 : [R', \mathrm{MAC}_2]; [\{r\}\_X_{uh}, \mathrm{RND}_2]$$

where $D_1$ is Device 1; $D_2$ is Device 2; { }_ presents a symbol of encryption; $T_u$ is the timestamp generated as a nonce; $X_{uh}$ is a shared key between $D_1$ and $D_2$ using ECCDH; $r$ is some value $x \in GF(p)$; $\mathrm{RND}_1$ is the MAC value of $X_{uh}$, $R$ and $\mathrm{ICAP}_1$ where ICAP is the result of a one way hash function $f$(Device_ID, Access Rights, Rnd), Rnd is a random number generated to prevent forgery; $\mathrm{RND}_2$ is the MAC value of $r$ and $\mathrm{ICAP}_2$; and $L$ presents the result of one way hash function (XOR of $X_{uh}$ and $T_u$).

Besides this, the Dolev–Yao intruder model has been introduced in the evaluation. The intruder is assumed to have knowledge of the following:

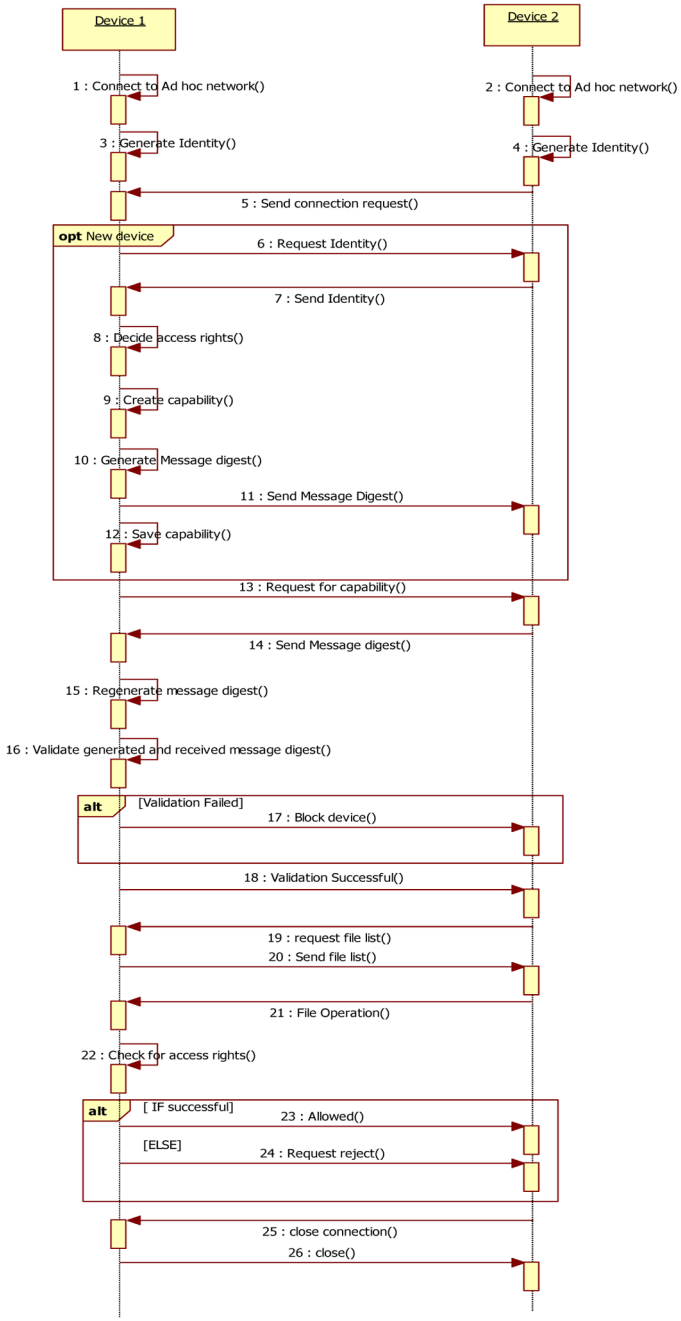


Figure 8 Proposed CAC scheme for IoT.

- ID: Device identifier,
- $f(\,)$: Knowledge of one way hash function.

### 6.1.2 Evaluation Results

The goal of evaluation is to verify protocol for attacks mentioned above and ensures mutual authentication along with the access control.

*Mutual authentication*: $X_{uh}$ is shared securely between $D_1$ and $D_2$, and $r$ is provided by trusted KDC to both the devices. Consequently, $D_1$ is authenticated to $D_2$ as only $D_2$ can decrypt $R$ and $T_{us}$. Also MAC can be calculated only by $D_2$ and $D_2$ is sending the encrypted $r$ to authenticate it to $D_1$. Verification results show that secure mutual authentication is achieved.

*Man-in-the-middle attack*: In case of authentication, even there is a man-in-the-middle attack on $R$, $T_{us}$, $\text{MAC}_1$ parameters; the attacker will not reveal any information. AVISPA shows that authentication protocol is free from attacks. For access control, man-in-the-middle attacks happen when an attacker eavesdrop the ID and ICAP transmitted, and then a masquerade attack happens when the attacker uses the stolen ID and CAP. The key to preventing a masquerade attack from the stolen CAP is to use an ID to validate the correct device. If the attacker manages to steal the ID, the attack is prevented by applying public key cryptography to ID, assuming that the authentication process has been done before access control. In this way, although the attacker gets the ICAP which is not encrypted, the capability validity check will return an exception because the one way hash function, $f$(ID, AR, Rnd) will return a different result than the one presented in the CAP, without a correct ID.

Another type of man-in-the-middle attack is replay attack. Adversary can intercept the message sent out from $D_1$. However, it is not possible in IACAC because it can easily detect by verifying timestamp $T_u$. If $T_u$ is older than the predefined threshold value, it is invalid and has been used. If $T_u$ is changed, $\text{MAC}_1 = \text{MAC}(X_{uh}, R \| \text{ICAP}_1)$ is not valid and consistent. For access control, IACAC prevents the replay attack by maintaining the freshness of Rnd, for example by using timestamp or nonce by including MAC as well. Even if the attacker manages to compromise the solution and gets the ICAP, it cannot use the same capability next time because the validity will be expired.

*DoS attack*: Upon receiving the message from $D_1$, $D_2$ first checks the validity of the timestamp. If it is not valid, then $D_2$ discards the message. Otherwise, it computes a $\text{MAC}_2$ value to compare with the received value. DoS happens when an attacker accesses a particular resource massively and simultaneously by using the same or different IDs. It is easy to control access using one ID because the system is able to maintain the session, thus the

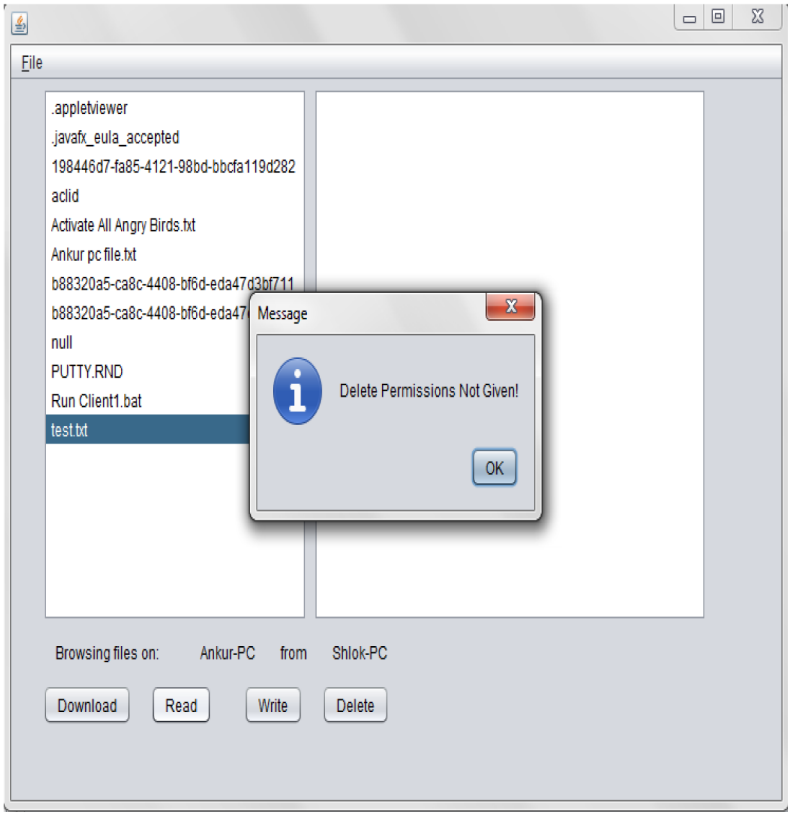


Figure 9 Snapshot showing principle of least privilege.

access of the same ID to the same resource can be restricted to only one session at a time. The potential of DoS attacks from multiple IDs can be prevented in the capability propagation process. Therefore, a DoS attack can be prevented or at least minimized.

*Principle of Least Privilege*: Security analysis shows that CAC has greater support for principle of least privilege due to the use of capabilities and hence it limits the damage when the protection is partially compromised. As access rights are encapsulated in the process of capability creation, even attacker or intruder is trying to modify these access rights, capability verification and comparison process returns false and access is denied. Access control schemes purely based on the role, context and ACL [44] has not addressed the principle of least privilege which is an important feature of the access

control solution. A sample snapshot as in Figure 9 shows that even one device is trying to perform delete operation which is not included in its capability, delete operation is denied achieving the principle of least privilege.

## 6.2 Performance Analysis

### 6.2.1 IACAC

The security level of protocol presented in this paper depends on the type of MAC algorithm, encryption algorithm and security level of ECC signature. We propose to use RC5 stream cipher for encryption, which takes 0.26 ms on Mica2 motes [54–56]. RC5 is notable for its simplicity for resource constrained devices such as IoT and its flexibility due to the built in variability. Heavy use of data independent rotations and mixture of different operations provides strong security to RC5 [57]. We propose to use SHA-1 as one way hash function which takes 3.63 ms on Mica2 motes and it is computationally expensive to find text which matches given hash and also it is difficult to two different texts which produces the same hash [54–56]. To generate the MAC value, we propose CBC-MAC which has advantage of small key size and small number of block cipher invocations and takes 3.12 ms on Mica2 motes [55]. The time required to generate random number is 0.44 ms and ECC to perform point multiplication which takes 800 ms on Mica2 motes [55, 56]. In IACAC protocol as the message length is fixed, CBC-MAC is most secure [58]. It is clear from these values that maximum time is required for ECC point multiplication. In IACAC, point multiplication is taking place at KDC and as KDC is powerful device, computational overhead is trivial as compared to the sensors. We denote the computational time required for each operation by device in IoT by following notation:

- $D_H$ is the time to perform one way hash function SHA-1;
- $D_{\text{MAC}}$ is the time to generate Mac value by CBC-MAC;
- $D_{\text{RC5}}$ is the time to perform encryption and decryption by RC5;
- $D_{\text{MUL}}$ is the time to perform ECC point multiplication; and
- $R$ is the time for random number generation.

Table 3 shows the comparison of computational time for the above-mentioned protocol. The IACAC protocol for mutual authentication and access control for the IoT devices takes less time (14.28 ms) as compared to other protocol compared in this paper. Key point to note here is that none of the work has addressed the issue of authentication and access control as an integrated solution for IoT. Total computational time for of the proposed

Table 3 Computational time for an IACAC scheme.

| Scheme | IACAC | HBQ [59] | IoT_Auth [16] |
|---|---|---|---|
| Auth. Time | $2D_H + 2D_{MAC} + 2D_{RC5}$ | $2D_H + 2D_{MAC} + D_{RC5} + 3D_{MUL}$ | $R + D_H + 2D_{MUL}$ |
| Total | $2D_H + 2D_{MAC} + 2D_{RC5}$ | $2D_H + 2D_{MAC} + D_{RC5} + 3D_{MUL}$ | $R + D_H + 2D_{MUL}$ |
| Total time | 14.02 ms | 2413.76ms | 1604.07ms |

scheme, HBQ [59] and mutual authentication for IoT (IoT_Auth) [16] is shown in Table 3. IoT_Auth scheme requires $R + D_H + 2D_{\text{MUL}}$ time for mutual authentication which comes approximately 1604.07 ms. The HBQ scheme takes $2D_H + 2D_{\text{MAC}} + D_{\text{RC5}} + 3D_{\text{MUL}}$ total time for authentication which is approximately 2,413.76 ms. Key point to note here is that both schemes do not address access control after authentication. IACAC takes only $D_H + 2D_{\text{MAC}} + 2D_{\text{RC5}}$ which takes only 14.02 ms which is much better than the other two schemes analyzed in this paper. In IACAC, the $2D_H$ factor is introduced which comprises time required by one way hash function in authentication as well as in ICAP to calculate Rnd.

### 6.2.2 CAC

The performances of independent CAC have also been analyzed to validate and support our findings. The CAC implementation consists of the capability creation, object selection once capabilities are verified and denying access if there no match found for capability. In this paper, files are treated as objects and operations are performed as mentioned in capabilities. Operations are Read, Write, Read and Write, or NULL operations as explained earlier.

As stated earlier, the CAC scheme is implemented in Wi-Fi for Laptop devices. To check the performance of CAC in terms of Access Time (AT), different laptop devices of same configuration are used and AT is averaged for all devices. In this paper, AT is a function of latency and is defined as

$$\text{Access Time (AT)} = f(L) \tag{3}$$

where $L$ is latency of access and defined as an overhead in terms of computational time to access right resource on right device. The unit of AT is milliseconds (ms). For measurement, we took the scenario as the two devices (Laptops) are connected via access point. AT defined in equation (3) is the time required to access one device to other in one way. Since WLAN is used and traffic can affect the access delay, multiple measurements are required

Table 4 Performance comparison of AT.

| Scheme ⟶ | CAC | CRBAC[44] |
|---|---|---|
| AT in (ms) | 364 | 410 |

to consider for evaluation. The three measurement runs have been taken for calculating the access time. Two devices are discoverable to each other by the Jgroups [60]. JGroups is a reliable group communication toolkit implemented in Java. It is based on IP multicast, and also provide reliable group membership, lossless transmission of a message to all recipients, message ordering. As reliability requirement varies from application to application, JGroups provides a flexible protocol stack architecture that gives flexibility to users to put together custom-tailored stacks, ranging from unreliable but fast to highly reliable but slower stacks. There are two cases for the performance measure, first is access with capability and second without using capability. In both cases we considered the same common modules, as device discovery and file browsing.

Table 4 shows the performance comparison of CAC, AT without capability and CRBAC [44]. In this paper, we also implemented CRBAC scheme to check its performance with CAC scheme presented. In [44], programming framework is presented to model CRBAC. Same programming framework is implemented in Wi-Fi to get context aware role based access control for laptop devices. As per the framework presented in the paper, context management and access control are brought and implemented together to get role based access control. Performance in terms of AT in milliseconds (ms) is measured for CRBAC [44] access control scheme and it shows that CAC works better as compared to CRBAC. CAC take average AT of 364 ms and AT without capability take 173 ms. Table 4 shows that the CAC scheme takes extra 191 ms but it provides secure access to devices by avoiding tampering or forgery of capability with the help of one way hash function. CAC access is also attack resistant from replay and man-in-the-middle attack. The CRBAC scheme takes 410 ms to access the device, which is more than the CAC scheme. In the CRBAC context dependent role based access is granted but the access is not secure. It can be concluded from Table 4 that the CAC scheme gives secure access control with better performance in terms of AT.

Moreover, in a distributed context, like IoT, CAC provides many advantages over traditional or consolidated approaches due to its flexibility, better

support for least privilege principle and avoidance for replay attack and man-in-the-middle attack. The chosen approach for the access control based on the capability concept, and in particular the CAC scheme, is considered in order to cope with the scalability of IoT system since it is well suited for providing access control in distributed systems. Besides a proposed access control model which provides scalability and flexibility, the main contribution of this paper also includes a secure access control mechanism that have been tested with a security protocol verification tool. To provide complete security solution to the identity management in IoT, authentication and access control are two important security measures.

Furthermore, there are few challenges to implement IACAC in mobile environment. Access delegation method with security considerations based on capability based context aware access control scheme intended for federated IoT networks is presented in [61]. In [61], capability propagation incorporating context in federated IoT environment with scalability and flexibility for distributed systems is presented. Authority delegation for mobile and federated environments is challenging due to dynamic and distributed nature. Another issue is that, it is necessary to have an established trust relationship between all entities prior to delegation. IACAC is completely compatible with the state of the art and it has been tested in Wi-Fi environment as discussed in the evaluation part of this paper. As the IACAC is addressing device to device authentication and access control, it is compatible in the user equipment and network elements being a lightweight and flexible in nature. Backward compatibility with the legacy network should not be the issue with the availability of high and powerful resources. In a mobile environment, mobility management is an interesting issue to deal with. The A interface which is an interface between mobile switching service switching centre and base station system which support many application part and Direct Transfer Application Part (DTAP) is one of them. Mobility management is one of the functionality of DTAP. There are many mobility management messages which are exchanged for identity establishment and access control (AUTHENT_REJ, AUTHENT_REQ). As physical layer of the A interface is 2 Mbps digital connection and DTAP deals with the exchange of layer 3 messages, no major adaptations are required to make IACAC functional.

As presented in [62], wireless communication and evolution is being faced by many constraints. These constraints are regulatory constraints like operating rules on the communication device, pre-decision on the frequency bands. Layered design of the communication protocol introduces architectural constraints which is important for proliferation. Other constraints are

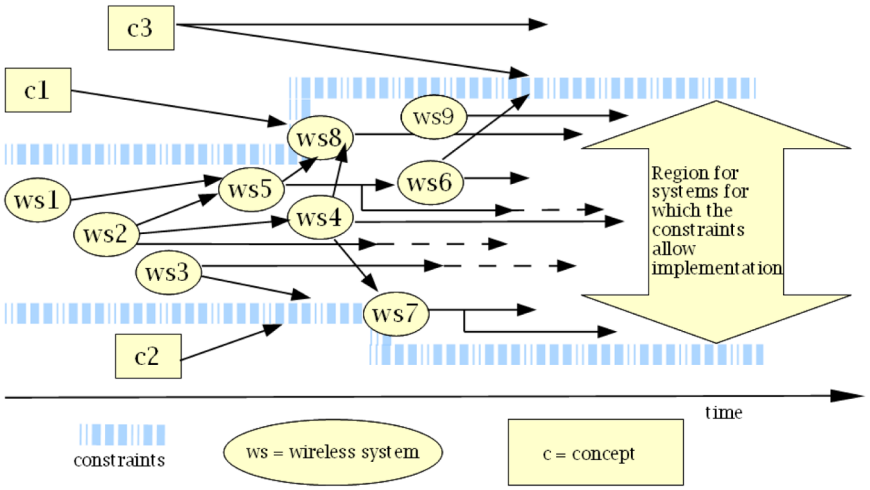


Figure 10 Wireless System Evolution [62].

standardization constraints in which particular communication protocol is developed and operated. The backward compatibility also needs many refinements and technological improvements for new standards. There are also market and social constraints deals with the new applications and the requirements from communication systems. Figure 9 depicts the outline of the evolution in wireless communications. As shown in the figure, ws1 and ws2 get converged and system ws5 is emerged. When ws4 is evolved, it is not feasible to implement concept c2 due to heavy constraints as discussed above, but due to increasing requirements (by ws3 also) the constraints are refined to change and ws7 is evolved. Over the period of time, some of the wireless communication systems become obsolete. Example of this obsolete system is shown in the Figure this happens for ws2. Important point to make a note here is that the constraints do not allow the concept c3 to be implemented over the period of time frame as depicted in Figure 10.

Similar to a global Internet scenario, interoperability and Internet working is ensured by following OSI stack but still there are many exceptions due to unpredictable nature of wireless interface. This makes more difficult to guarantee expected quality of service in resource constrained IoT and next generation networks. Backward compatibility to legacy networks is a challenge due to lack of cross layer coordination which is a need of today in order to get performance improvement. Other interoperability and Internet working

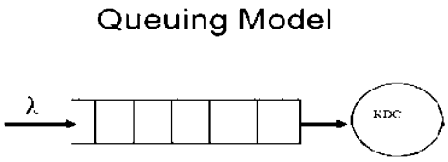


Figure 11 IACAC queuing model.

issues are architecture design and multi-traffic environment. To address these ensuing issues, more research is needed.

### 6.2.3 Proposed Mathematical Model for IACAC Queuing Analysis

The proposed IACAC model consists of a trusted third party which is responsible for distributing the ECC parameters to devices trying to communicate to each other. Devices approaching to KDC for service are managed in queue. Figure 11 shows the system, where $\lambda$ is the arrival rate of devices. The inter-arrival time for devices is exponentially distributed. Thus arrival rate follows the poisons arrival process. Our system can be modelled with an M/D/1 queuing model with a constant service rate and one server. To evaluate the system performance, we model the sojourn time, that is, the total time spent by the device in the system.

The expectation of waiting time for devices in the queue can be as

$$E[W_q] = N_q \times E[S] + E[R] \tag{4}$$

where $N_q$ is the mean number of devices in queue; $E[S]$ is the service time of KDC; and $E[R]$ is the residual time. Thus using Little's formula [63], the mean queue length is given as

$$N_q = \lambda \cdot E[W_q] \tag{5}$$

Therefore,

$$E[W_q] = \frac{E[R]}{1 - \rho_{\text{KDC}}}$$

where the utilization of KDC is given as

$$\rho_{\text{KDC}} = \lambda \cdot E[S]$$

The residual time $R_i$ is the service time remaining to the customer being served when the $i$th device arrives at queue. Figure 12 shows the residual time in queue at time $t$.

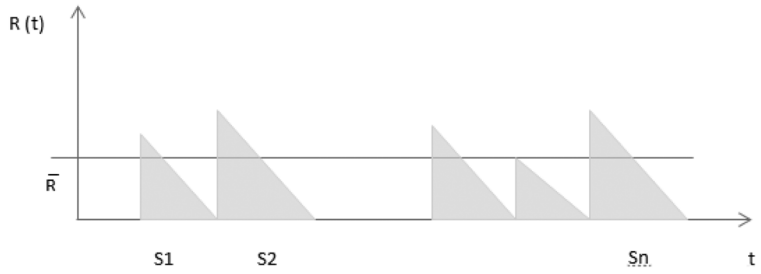


Figure 12 Residual time in queue.

The mean residual time can be calculated by dividing the sum of areas of triangles by the length of interval and is derived as follows:

$$\begin{aligned} E[R] &= \frac{1}{t}\int_0^t R(t)dt = \frac{1}{t}\sum_{i=1}^{n}\frac{1}{2}[S_i^2] \\ &= \frac{n}{t}\cdot\frac{1}{n}\sum_{i=1}^{n}\frac{1}{2}[S_i^2] \\ \frac{n}{t} &\to \lambda \quad \sum_{i=1}^{n}\frac{1}{2}[S_i^2] \to \frac{1}{2}E[S^2] \\ E[R] &= \frac{\lambda\cdot E[S^2]}{2} \\ E[W_q] &= \frac{\lambda\cdot E[S^2]}{2(1-\rho_{\mathrm{KDC}})} \end{aligned} \tag{6}$$

Now, the total time spent by a device in the system (the sojourn time) is

$$\begin{aligned} E[T] &= E[W_q] + E[S] \\ E[T] &= \frac{\lambda\cdot E[S^2]}{2(1-\rho_{\mathrm{KDC}})} + E[S] \end{aligned} \tag{7}$$

The total service time comprises of two factors: expectation $E[S]$ and variance $V[S]$. The variance is the difference between the mean of squares of the values and square of mean of values. Therefore $V[S]$ is given as

$$V[S] = E[S^2] - E[S]^2 \tag{8}$$

For the M/D/1 system, as the service time is constant, variance $V[S] = 0$ and results into $E[S^2] = E[S]^2$. Thus,

$$E[T] = \frac{\lambda \cdot E[S]^2}{2(1 - \rho_{\text{KDC}})} + E[S]$$

$$E[T] = \left(1 + \frac{\rho_{\text{KDC}}}{2(1 - \rho_{\text{KDC}})}\right) \cdot E[S] \tag{9}$$

By Little's formula, the mean queue length, the mean number of devices in queue is given by

$$N_q = \lambda \cdot E[W_q]$$

$$N_q = \frac{\lambda 2 \cdot E[S]^2}{2(1 - \rho_{\text{KDC}})}$$

$$N_q = \frac{\rho_{\text{KDC}}^2}{2(1 - \rho_{\text{KDC}})} \tag{10}$$

Thus, from equations (4) to (10), it can be concluded that the total time spent by a device in system is the function of the service time $E[S]$ and the utilization of KDC, $\rho_{\text{KDC}}$. The mean queue length and the utilization are proportional to each other. If the number of devices in queue increases, the utilization of KDC also increases. For further improvement in the utilization of KDC, we can pipeline the services of KDC. The services provided by KDC can be divided in three stages. This will lead to service of three devices at a time. As shown in Figure 13, the server device will get serviced from server S1 and will enter the queue for server S2 and so on.

Thus a network of set of single servers in series is formed. The input for each queue except for the first is the output of the previous queue. The input to the first queue is Poisson. If the service time of each queue is constant and the waiting lines are infinite, the output of each queue is a Poisson stream statistically identical to the input. When this stream is fed into the next queue, the delays at the second queue are the same as if the original traffic had bypassed the first queue and fed directly into the second queue. Thus the queues are independent and may be analysed one at a time. Therefore the

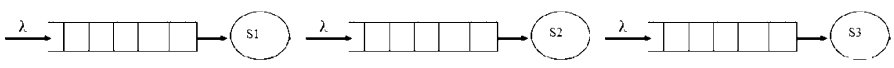


Figure 13 Proposed pipelining of the KDC services.

waiting time for a device in complete system will be the sum of waiting time for devices at each subsystem and is shown as

$$T = \sum E[T_i]$$

$$T = \sum_{i=1}^{3} \left(1 + \frac{\rho_i}{2(1-\rho_i)}\right) \cdot E[S_i] \tag{11}$$

where $\rho_i$ is the utilization of server $S_i$ and $E[S_i]$ is the service time of server $S_i$.

## 7 Conclusions and Future Work

A distributed, lightweight and attack resistant solution are the mandatory properties for the security solution in IoT and puts resilient challenges for authentication and access control of devices. This paper presents an efficient and secure ECC based integrated authentication and access control protocol. This paper also presents a mutual authentication protocol and integrated with novel and secure approach of CAC for access control in IoT along with the implementation results. Furthermore, this paper presents comparative analysis of different authentication and access control schemes for IoT. Comparison in terms of computational time shows that IACAC scheme is efficient as compared to other solution. The protocol is also analyzed for the performance and security point of view for different possible attacks in IoT scenario. Protocol evaluation shows that it can defy attacks like DoS, man-in-the-middle and replay attacks efficiently and effectively. The paper also presents protocol verification using AVISPA tool which proves that the IACAC protocol is also efficient in terms of key sharing and authentication. Finally, we also presented a mathematical model for improving queuing analysis of IACAC.

The future plan is to put this protocol in place with RFID middleware architecture for identity management in IoT. Future work will involve specification as well as security evaluation of the CAC propagation and revocation in order to have a complete model of CAC scheme. Another interesting aspect will be to define and devise a lightweight version of CAC for resource constrained devices in IoT like sensor nodes. Complete interoperability and Internet working is still an open research area to take this research further.

## References

[1] ITU-T Internet Reports, Internet of Things, November 2005.
[2] E. Zouganeli and I. E. Svinnset. Connected objects and the Internet of Things – A paradigm shift, Photonics in Switching 2009, September 2009.
[3] M. Weiser, The computer for the 21st century, Scientific American, 265: 66–75, 1991.
[4] S. Sarma, D. L. Brock, and K. Ashton. The networked physical world. TR MIT-AUTOIDWH-001, MIT Auto-ID Center, 2000.
[5] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Technical Report CLOUDS-TR-2012-2, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, 29 June 2012.
[6] Xiaodong Lin, Rongxing Lu, Xuemin Shen, Y. Nemoto, and N. Kato. Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems. IEEE Journal on Selected Areas in Communications, 27(4): 365–378, May 2009.
[7] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo. A survey on facilities for experimental Internet of Things Research. IEEE Commun. Mag., 49: 58–67, 2011.
[8] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. Souza, and V. Trifa. SOA-based integration of the internet of things in enterprise services. In Proceedings of IEEE ICWS 2009, Los Angeles, Ca, USA, July 2009.
[9] I. F. Akyildiz, J. Xie, and S. Mohanty. A survey on mobility management in next generation All-IP based wireless systems. IEEE Wireless Communications Magazine, 11(4):16–28, 2004.
[10] C. Mayer. Security and privacy challenges in the IoT. WowKivs, Electronic Communications of the EASST, Volume 17, Germany, 2009.
[11] R. Prasad. My personal Adaptive Global NET (MAGNET). Signals and Communication Technology Book, Springer, The Netherlands, 2010.
[12] D. M. Kyriazanos, G. I. Stassinopoulos, and N. R. Prasad. Ubiquitous access control and policy management in personal networks. In Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1–6, July 2006.
[13] Michael Braun, Erwin Hess, and Bernd Meyer. Using elliptic curves on RFID tags. International Journal of Computer Science and Network Security, 8(2), 2008.
[14] Sheikh Iqbal Ahamed, Farzana Rahman, and Endadul Hoque. ERAP: ECC based RFID authentication protocol. In 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2008.
[15] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In Network and Distributed Systems Security Symposium (NDSS), February 2002.
[16] Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long, and Ting Hu. A novel mutual authentication scheme for Internet of Things. In Proceedings of 2011 IEEE International Conference on Modelling, Identification and Control (ICMIC), pp. 563–566, 26–29 June 2011.
[17] C. Jiang, B. Li, and H. Xu. An efficient scheme for user authentication in wireless sensor networks. In 21st International Conference on Advanced Information Networking and Applications Workshops, pp. 438–442, 2007.

[18] R. R. S. Verma, D. O'Mahony, and H. Tewari. Progressive authentication in ad hoc networks. In Proceedings of the Fifth European Wireless Conference, February 2004.
[19] T. Suen and A. Yasinsac. Ad hoc network security: Peer identification and authentication using signal properties. In Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop (IAW'05), pp. 432–433, 15–17 June 2005.
[20] L. Venkatraman and D. P. Agrawal. A novel authentication scheme for ad hoc networks. In Wireless Communications and Networking Conference (WCNC2000), vol.3, pp. 1268–1273. IEEE, 2000.
[21] B. Bing. Emerging Technologies in Wireless LANs – Theory, Design and Deployment. Cambridge University Press, 2008.
[22] Best Current Practices for WISP Roaming, WiFi Alliance, 2003.
[23] RFC 2865, Remote Authentication Dial in User Service (RADIUS).
[24] Jian Feng. Analysis, implementation and extensions of RADIUS protocol. In International Conference on Networking and Digital Society (ICNDS'09), vol.1, pp. 154–157, 30–31 May 2009.
[25] RFC 5247, Extensible Authentication Protocol (EAP) Key Management Framework, August 2008.
[26] A. M. El-Nagar, A. A. El-Hafez, and A. Elhnawy. A novel EAP – Moderate weight Extensible Authentication Protocol. In IEEE Seventh International Conference on Computer Engineering (ICENCO2011), pp. -1-6, 27–28 December 2011.
[27] Wei Yuan, Liang Hu, Hong-tu Li, Kuo Zhao, Jiang-feng Chu, and Yuyu Sun. Key replicating attack on an identity-based three-party authenticated key agreement protocol. In IEEE International Conference on Network Computing and Information Security (NCIS), vol. 2, pp. 249–253, 14–15 May 2011.
[28] Jun Lei, Xiaoming Fu, Dieter Hogrefe, and Jianrong Tan. Comparative studies on authentication and key exchange methods for 802.11 wireless LAN. Computers & Security, 26(5): 401–409, August 2007.
[29] OASIS.eXtensible Access Control Markup Language (XACML) Version 3.0, Working Draft 8, February 2009.
[30] W3C Platform for Privacy Project: http://www.w3.org/privacy/.
[31] The Shibboleth project: www.shibboleth.net.
[32] The Liberty Alliance Project: www.projectliberty.org.
[33] Ravi S. Sandhu. The typed access matrix model. In Proceedings of the IEEE Symposium on Security and Privacy. IEEE CS Press, 1992.
[34] T. Close. ACLs don't. HP Laboratories Technical Report,February 2009.
[35] L. Gong. A secure identity-based capability system. In Proceedings of 1989 IEEE Symposium on Security and Privacy, Oakland, CA, May. IEEE Computer Society Press, Los Alamitos, 1989.
[36] Ravi S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. IEEE Computer, 29(2): 38–47, February 1996.
[37] J. B. D. Joshi, E. Bertino, U.Latif, and A. Ghafoor. A generalized temporal role-based access control model. IEEE Transactions on Knowledge and Data Engineering, 17(1): 4–23, January 2005.
[38] R. Bhatti, E. Bertino, and A. Ghafoor. A trust-based context-aware access control model for web-services. Distributed and Parallel Databases, 18(1), July 2005.

[39] Q. Ni, A. Trombetta, E. Bertino, and J. Lobo. Privacy-aware role based access control. In Proceedings of the 12th ACM Symposium on Access Control Models and Technologies (SACMAT'07), 2007.
[40] E. Barka and R. Sandhu. A role-based delegation model and some extensions. In Proceedings of the 23rd National Information Systems Security Conference, 2000.
[41] E. Barka and R. Sandhu. Role-based delegation model/hierarchical roles. In Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04), 2004.
[42] K. Hasebe, M. Mabuchi, and A. Matsushita. Capability-based delegation model in RBAC. In Proceedings of the 15th ACM Symposium on Access Control Models and Technologies (SACMAT'10). ACM, 2010.
[43] Y. G. Kim, C. J. Mon, D. Jeong, J. O. Lee, C. Y. Song, and D. K. Baik. Context-aware access control mechanism for ubiquitous applications. In Advances in Web Intelligence, LNCS, Vol. 3528, pp. 236–242. Springer, Heidelberg, 2005.
[44] D. Kulkarni and A. Tripathi. Context-aware role-based access control in pervasive computing systems. In SACMAT'08, Estes Park, CO, 11–13 June 2008.
[45] Kyungah Shim and Young-Ran Lee. Security flaws in authentication and key establishment protocols for mobile communications. Applied Mathematics and Computation, 169(1): 62–74, October 2005.
[46] G. Horn, K. M. Martin, and C. J. Mitchell. Authentication protocols for mobile network environment value added services. IEEE Transactions on Vehicular Technology, 51(2): 383–392, 2002.
[47] M. J. Beller, L. F. Chang, and Y. Yacobi. Privacy and authentication on a portable communications system. IEEE Journal on Selected Areas in Communications, 11: 821–829, 1993.
[48] C. Boyd and A. Mathuria. Key establishment protocols for Secure Mobile communications: A selective survey. In Information Security and Privacy, ACISP 98, LNCS, Vol. 1438, pp. 344–355. Springer, Heidelberg, 1998.
[49] A. Aziz and W. Diffie. Privacy and authentication for wireless local area networks. IEEE Personal Communications, 1: 25–31, 1994.
[50] D. S. Wong and A. H. Chan. Efficient and mutually authenticated key exchange for low power mobile device. In Advances in Cryptology – Asiarcypt01, LNCS, Vol. 2248, pp. 272–289. Springer-Verlag, Heidelberg, 2001.
[51] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48: 203–209, 1987.
[52] Avispa – A tool for Automated Validation of Internet Security Protocols. http://www.avispa-project.org.
[53] D. Dolev and A. C.-C. Yao. On the security of public key protocols. In FOCS, pp. 350–357. IEEE, 1981.
[54] R. Chakravorty. A programmable service architecture for mobile medical care. In 4th IEEE International Conference on Pervasive Computing and Communications, 2006.
[55] C. Karlof, N. Sastry, and D. Wagner. Tinysec: Link layer security architecture for wireless sensor networks. In SensSys, ACM Conference on Embedded Networked Sensor Systems, 2004.
[56] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz. Comparing elliptic curve cryptography and RSA on 8-it CPUs. In CHES 2004, LNCS, Vol. 3156, pp. 119–132, Springer, Heidelberg, 2004.

[57] Y. L. Yin. The RC5 encryption algorithm: Two years on. CryptoBytes, 3(2), Winter 1997.
[58] M. Bellare, J. Killan, and P. Rogaway. The security of cipher block chaining. In Y. Desmedt (Ed.), CRYPTO 1994. LNCS, Vol. 839, pp. 341–358. Springer, Heidelberg, 1994.
[59] H. Wang, B. Sheng, and Q. Li. Elliptic curve cryptography based access control in sensor networks. Int. J. Security and Networks, 1(3/4): 127–137, 2006.
[60] Bela Ban. Adding group communication to Java in a non-intrusive way using the ensemble toolkit. Technical Report, Dept. of Computer Science, Cornell University, November 1997.
[61] Bayu Anggorojati, Parikshit N. Mahalle, Neeli R. Prasad, and Ramjee Prasad. Capability-based access control delegation model on the federated IoT network. In IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC2012), Taipei, Taiwan, September 24–27, pp. 604–608, 2012.
[62] Petar Popovski. On designing future communication systems: Some clean-slate perspectives. In R. Prasad, S. Dixit, R. Nee, and T. Ojanpera (Eds.), Globalization of Mobile and Wireless Communications, pp. 129–143. Springer Science+Business Media, 2011.
[63] Alberto Leon-Garcia. Probability, Statistics, and Random Processes for Electrical Engineering (3rd ed.). Prentice Hall, 2008.

## Biographies

**Parikshit N. Mahalle** is IEEE member, ACM member, Life member ISTE and graduated in Computer Engineering from Amravati University, Maharashtra, India in 2000 and received Master in Computer Engineering from Pune University in 2007. From 2000 to 2005, he was working as lecturer in Vishwakarma Institute of technology, Pune, India. From August 2005, he wass working as an Assistant Professor in Department of Computer Engineering, STES's Smt. Kashibai Navale College of Engineering, and Pune, India. Currently he is pursuing his Ph.D. in wireless communication

at Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark. He has published 25 papers at national and international level. He has authored five books on subjects like Data Structures, Theory of Computations and Programming Languages. He is also the recipient of "Best Faculty Award" by STES and Cognizant Technologies Solutions. His research interests are Algorithms, IoT, Identity Management and Security.

**Bayu Anggorojati** is currently pursuing his PhD at Center for TeleInFrastruktur (CTIF), Aalborg University. His main research interest is in access control for RFID system and IoT. During the period of his PhD work, he has been involved in several projects, especially the EC projects, such as ASPIRE, ISISEMD, LIFE2.0, and BETaaS.

**Neeli Rashmi Prasad**, Ph.D., IEEE Senior Member, Director, Center For TeleInfrastructure USA (CTIF-USA), Princeton, USA. She is also Head of Research and Coordinator of Themantic area Network without Borders,

Center for TeleInfrastruktur (CTIF) headoffice, Aalborg University, Aalborg, Denmark.

She is leading IoT Testbed at Easy Life Lab (IoT/M2M and eHealth) and Secure Cognitive radio network testbed at S-Cogito Lab (Network Management, Security, Planning , etc.). She received her Ph.D. from University of Rome "Tor Vergata", Rome, Italy, in the field of "adaptive security for wireless heterogeneous networks" in 2004 and M.Sc. (Ir.) degree in Electrical Engineering from Delft University of Technology, the Netherlands, in the field of "Indoor Wireless Communications using Slotted ISMA Protocols" in 1997.

She has over 15 years of management and research experience both in industry and academia. She has gained a large and strong experience into the administrative and project coordination of EU-funded and Industrial research projects. She joined Libertel (now Vodafone NL), The Netherlands in 1997. Until May 2001, she worked at Wireless LANs in Wireless Communications and Networking Division of Lucent Technologie, the Netherlands. From June 2001 to July 2003, she was with T-Mobile Netherlands, the Netherlands. Subsequently, from July 2003 to April 2004, at PCOM:I3, Aalborg, Denmark. She has been involved in a number of EU-funded R&D projects, including FP7 CP Betaas for M2M & Cloud, FP7 IP ISISEMD ICt for Demetia, FP7 IP ASPIRE RFID and Middleware, FP7 IP FUTON Wired-Wireless Convergence, FP6 IP eSENSE WSNs, FP6 NoE CRUISE WSNs, FP6 IP MAGNET and FP6 IP Magnet Beyond Secure Personal Networks/Future Internet as the latest ones. She is currently the project coordinator of the FP7 CIP-PSP LIFE 2.0 and IST IP ASPIRE and was project coordinator of FP6 NoE CRUISE. She was also the leader of EC Cluster for Mesh and Sensor Networks and is Counselor of IEEE Student Branch, Aalborg. Her current research interests are in the area of IoT & M2M, Cloud, identity management, mobility and network management; practical radio resource management; security, privacy and trust. Experience in other fields includes physical layer techniques, policy based management, short-range communications. She has published over 160 publications ranging from top journals, international conferences and chapters in books. She is and has been in the organization and TPC member of several international conferences. She is the co-editor is chief of *Journal for Cyber Security and Mobility* by River Publishers and associate editor of *Social Media and Social Networking* by Springer.

**Ramjee Prasad (R)** is currently the Director of the Center for TeleInfrastruktur (CTIF) at Aalborg University (AAU), Denmark and Professor, Wireless Information Multimedia Communication Chair. He is the Founding Chairman of the Global ICT Standardisation Forum for India (GISFI: www.gisfi.org) established in 2009. GISFI has the purpose of increasing the collaboration between European, Indian, Japanese, North-American, and other worldwide standardization activities in the area of Information and Communication Technology (ICT) and related application areas. He was the Founding Chairman of the HERMES Partnership – a network of leading independent European research centres established in 1997, of which he is now the Honorary Chair.

Ramjee Prasad is the founding editor-in-chief of the Springer *International Journal on Wireless Personal Communications*. He is a member of the editorial board of several other renowned international journals, including those of River Publishers. He is a member of the Steering, Advisory, and Technical Program committees of many renowned annual international conferences, including Wireless Personal Multimedia Communications Symposium (WPMC) and Wireless VITAE. He is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE), USA, the Institution of Electronics and Telecommunications Engineers (IETE), India, the Institution of Engineering and Technology (IET), UK, and a member of the Netherlands Electronics and Radio Society (NERG) and the Danish Engineering Society (IDA). He is also a Knight ("Ridder") of the Order of Dannebrog (2010), a distinguishment awarded by the Queen of Denmark.