Proceedings of the Pakistan Academy of Sciences:
A. Physical and Computational Sciences 53 (3): 293–307 (2016)
Copyright © Pakistan Academy of Sciences
ISSN: 2518-4245 (print), 2518-4253 (online)

Pakistan Academy of Sciences

Research Article

A Novel Light Weight and Automatic Authentication based on Centralized Approach for Pervasive Environment

Muhammad Nawaz Khan[a,*], and Muhammad Nazir[b]

Department of Computing, Shaheed Zulfikar Ali Bhutto Institute of Science & Technology (SZABIST), Islamabad, Pakistan

Abstract: Today is the age of hyper-connectivity, no standalone system ever exist. Now each device has the processing and communicating capabilities. Pervasive computing brings all these devices into a uniform layer for ease of use and for providing on fly services. In pervasive environments, smart devices communicate each other to provide pervasive services according to the user modes and contexts. To construct an ad hoc and un-structure network of heterogeneous entities and to standardize all different technologies into a uniform solution, many technical and functional challenges are need to be addressed. With dissimilar nature and distributed control over the resources in unfriendly situation the pervasive environments always in trouble due to lack of proper security system. For consistent dynamic flow of services in an ad hoc pervasive network, the authentication of users, devices, services and process are critical. Here in this research work we proposed “A novel light weight and automatic authentication scheme based on centralized approach for pervasive environment”. In this approach a central base station is responsible for providing resources and implementing security policy for all entities. Public Keys, Public key Certificates, Nonce, IDs and time stamps are parameters used in the proposed scheme. The new scheme is validated and analyzed in a simulator in the presence of attacker. The proposed model is designed to prevent most sophisticated DoS attacks and man in middle attacks.

Keywords: Pervasive computing, context awareness, ambient intelligence, middle ware, embedded devices, ad hoc network, man in middle, DoS.

1. INTRODUCTION

Pervasive or ubiquitous computing means that all objects in our surrounding are become so intelligent that they understand the context and behaves according to the situations. Physical spaces, mobile devices and building infrastructures interact with each other and provide services according to the context. The omnipresence of chip-based smart devices with hybrid network enables us to interact and use all the available services in a uniform way. Billions of smart devices make out environment more interactive, attractive and user friendly. Pervasive is now termed as Internet of Things (IoTs) because services are available for everyone, everywhere and any time without knowing the underlying infrastructure [1, 2]. The Mark Weiser was the pioneer in giving the idea of pervasive computing in 1991 [3, 4] and now with the emergence of the miniaturization in devices and sensor technology enable us to construct pervasive environments, where services are available at everywhere, at any time for any one. The interactive spaces and smart dust make our environment more accessible and convenient. Services are available anywhere, anytime for everyone with a zero-click. Users even did not know about the nature of the software, platform and services while achieve the service as he wished.

Pervasive computing declines time and space by providing on fly services which ultimately lead to reduce the cost for the offered services. User can use other user resources without hesitation if the service is reachable in the same premises. Pervasive computing changed the traditional dull computing into more interactive computing. Now every device is embedded with microprocessor, memory and with communicating facility. These

Received, April 2016; Accepted, August 2016

*Corresponding author: E-mail: nawazpk805@gmail.coma, nazir@szabist-isb.edu.pkb

smart devices reflect the current circumstances according to the user moods and conditions. It can remember crucial moments because they have memory, they show context sensitive behavior because they have sensors and they are responsive because they have communications links. It provides a new apparition of computing where computing will be disappear into specialized invisible computers. In simple words these ubiquitous personal assistance will be the integral part of human environment. As stated by Moor law [5] , that after every eighteen months the processing and storage capacities shall be increased in double. The figure.1 shows the trend that how technology makes available pervasive computing.

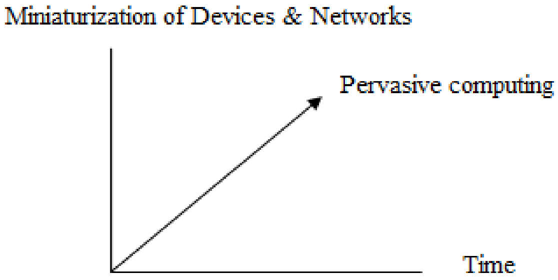

Fig. 1. Trend in pervasive computing.

Traditional computing approach is dull and passive where all burdens on a user with single machine for single user as in system centric approach. While pervasive environments are user centric where all burdens is on the surrounding smart devices. In user centric approach, the portable and embedded devices communicate each other and behave according to the context. Hardware and software resources are arranged into a resource channel in cascading. Resources are arranged in such a uniform layer that they operate themselves automatically according to the context. The framework bring all the nearby resources (hard ware & software) to a platform where services are available everywhere, for everyone, any time. The pervasive computing will subsist in our lives everywhere and that's why MIT called its pervasive project "Oxygen" [6] .When devices came under such framework, a single system can use a bunch of resources at a time which cannot possible for standalone system. Figure 2; show the basic of pervasive computing paradigm.

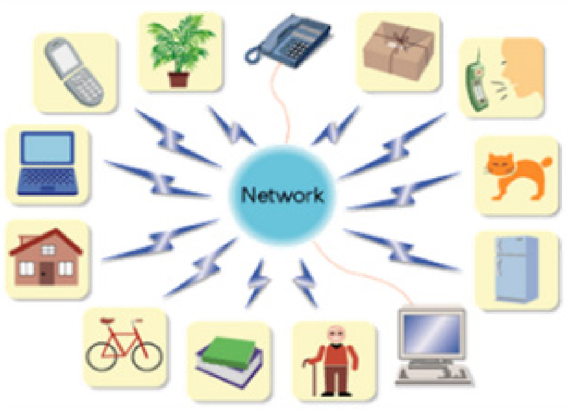

Fig. 2. Pervasive environment paradigm.

For real pervasive environment many technical and functional challenges need to be resolved. But the impromptu and diverse nature of pervasive network with partial resources and frosty environment leads to the inherent weakness of security. Traditional wired and wireless networks are secured with strong administrative policies with most dedicated devices like firewalling and Intrusion Detection Systems. But a network with different channels and with different devices having no defined infrastructure, these mechanisms are infeasible. For better accessibility and good availability of resources, authentication of all entities always desired. A new light weight and portable scheme is always needed to fulfill the requirements of the authentication of all entities including users, devices, services and process.

2. RELATED WORK

Here the first scheme is discussed about providing end to end authentication of users, devices and services [7]. The proposed system is based on Globus Grid Security Infrastructure (GGSI) [8] in which users are authenticated but machines and related services do not. In GGSI extensive use of proxies while here the system works without proxies. PKI based certificates and CA play main roles in authentication. Commonly used key is 256-bits. The Fat browser use APIs with WS protocols for security purpose [7]. The SAML credentials are uses for authorization of entities and XML provided exchange of information. It cans prevention of many variants of Man-in-the-Middle (MITM) attacks. The service based architecture, bilateral authentication and cascading process in authentication are the main steps in this model. Authentication for every entity creates latency and overhead in the system. The browser compatibility on user side is another problem [1].

Another scheme is based on critically analysis of Turkanovi et al. scheme [9]. In which first the scheme is investigated for man in the middle and stolen smart card attacks. Much vulnerability is found out and based on the same weakness; the scheme is updated for resistance to such types of attacks. The scheme is useful because it used only symmetric techniques of cryptography. It uses XOR operation and hashes which is very simple and light weight for such low energy network. All entities are authenticated by a systematic method of protection of passwords, many choices for new passwords, dynamic addition of other entities and quickly changing passwords policy. The performance analysis in BAN-Logic and with AVISPA simulation tool of the improved scheme is better and more efficient to its successor [10].

A lightweight and low power authentication scheme has proposed for authentication of devices and services [11]. They deploy "Generic Bootstrapping Architecture (GBA)" [12] of "3rd Generation partnership Project (3GPP) of mobile technology for authentication of participating entities. The scheme is useful for global mobility of such pervasive devices but it produces extra overhead in terms of IP address pool and calculating of hashes for IPs. The authors claim analysis of scheme is energy efficient but scheme have narrow scope in low energy devices [11].

Low level authentication scheme "Aggregated Proof based Hierarchical Authentication scheme (APHA)" is based on U2IoT architecture in hierarchical method. The two protocols used light weight methods for calculating dynamic hashed for authentication, confidentiality and integrity. It uses chaotic maps and direct paths methods for ensuring authentication of data [13]. APHA mainly described in three phases; first, aggregated proofs are collected for unidentified network traffic in both directions. Second, for mutual authentication of chaotic maps, homomorphism and path descriptor apply combine. Third, different levels of trust are defined and named for hierarchical authentication of data and devices. APHA is good for data integrity and confidentiality but the scheme is not recommended for authentication of entities including devices, services, channels and users in pervasive environment [13].

Another light weight authentication scheme server-client based architecture has proposed [14]. Physical objects are authenticated and verified its status "Constrained Application Protocol". In first phase, the requester and provider entities are authenticated each other. In second phase, only those services are provide that only specified certain conditions in the request. The first phase authenticates heterogeneous devices with different specification, architecture and data rates. The second phase minimizes resources usage by only fulfilling the specific request. The scheme is looking good against some specific attacks like eaves-dropping and key fabrication but not recommended for resource exhaustion and denial of service attacks [14].

Table 1. The symbols used in system.

BS	Base Station
N_A	Node-A
N_B	Node-B
N_N	Node-N (any node/entity)
Cer_A	Certificate of Node-A
Cer_B	Certificate of Node-B
$RrgreqSer_S$	Registration request for service
PU_{BS}	Public key of base station
E	Encryption
D	Decryption
$Time_{1\ldots n}$	Specific time for message request
$Time_{expire}$	Time on which certificate expired
$Time_{stamp}$	Time when certificate issued
ID_A	Identity of Node-A
ID_B	Identity of Node-B
PU_A	Public key of Node-A
PU_B	Public key of Node-B
$Services_N$	Some specific service
Req	Request for a service
Specs	Specification of the request type (network & supporting technologies)
N_1	Nonce at time T1
N_2	Nonce at time T2
Dev_i	Device List having (i) number of devices
$Serv_i$	Services List having (i) number of service
$Task_i$	Any task
Req_i	Request for resource
Dev_s	Specific Device
$Serv_s$	Specific service
MiM	Main In Middle

An automatic authentication scheme has proposed based isolated zero knowledge approach [15]. Sending messages are used for authentication between legitimate nodes based on secret session keys. The bulky data are shared between authenticated nodes in broadcast manner. For public key exchange many case scenarios are discussed. For analysis, the system is implemented in "Android Open Source Project" reveals that it is light weight authentication with minimum utilization of resources with high level of security.

The scheme is useful for abrupt and dynamic networks but prior knowledge for communicating entities make it hurdle for pervasive environments [15].

Very faster and more efficient authentication mechanism which works on short encrypted and authentic messages is explained in [3]. A short random string is appended to the plaintext message before encryption. A single one time key is used and many other schemes have discussed based on Message Authentication Codes (MACs) [16] and radio frequency identification (RFIDs) [17]. The Lima and three theorems are nicely is explained. The small message size and small modular further minimize the amount of processing data, which increase system efficiency. Due to the light-weighted modular multiplication, the hardware implementation is efficient as compared sophisticated cryptographic operations [17]. The proposed scheme is recommended for short messages are used but not for bulk data [17]. Here another system based master key proposed for novel authentication. This master combined all digital keys for authentication. The same master key is responsible for starting authentication and for the selection of other keys on the basis of code words with locks. The taxonomy and choices for master key creation nicely explain for achieving good usability, authentication and security of the users. Exchange code in master key support key locks automatically without user interventions. The master key maintains the security by applying key locks interaction and keeps the authentication secret. Master key scheme does not sustain multiple groups of key owners [18].

A new approach for authentication in ad hoc and wireless environment are studied and analyzed with assessment [19]. Only authenticated devices are the part of network, therefore, if user password and other credentials are stolen, network resources are still confined [19]. Threat model for physical device authentication include Bluetooth specification, Radio Frequency Identification (RFID) tags based attacks and the vulnerabilities of key based sensors network. The IEEE 802.1X framework [20], 802.16 Case [21], Trusted Computing Solution (TCG) [22] and many other authentication schemes [23] are discussed. The main focus here is on correct identification of devices without revealing user's credential [19]. The paper also spotlights some points about 4 G pervasive environments [19]. In pervasive and ad hoc network system, the devices are resource restricted in processing power, memory, communication and software support [24]. Most of these devices are portable, hand held and light weight. Robustness and dependability are difficult in such heterogeneous and multiplatform environment [24]. The system is divided into network security and system security. Field Programmable Gate Arrays [25] and Suggested Application specific integrated circuits [26] with their low-cost, low-power and easily deployment, are better option for light-weighted cryptographic algorithms. Reducing the input key, number of rounds and processing bit for specific system does not increase system efficiency [24].

One of the schemes suggested for light-weight authentication key agreement protocol for authentication based on of a user behavior. The Elliptic Curve-based Secure Authenticated Key Agreement protocol (EC-SAKA) [27] provides basis and Diffi-Hellman key based protocol make the system more resistant against malicious users. The 3-pass scheme for authentication generates a common secret key with collaboration to an elliptic curve-based digital signature [28]. The demand and expiry approach is used for minimum resource utilization. The system is focus on metric values rather than the underlying network. For judgment the human behavior, a technical approach is used based on number of control messages exchanged and the total number of actions for specific events [28].

Another scheme for Privacy-Preserving Location proof Updating System (APPLAUS) [29] is suggested, in which mobile entities correlate each other by using Bluetooth. Mobile entities verify their location by updating pseudonyms periodically with location servers. The APPLAUS structure with different entities (prover, witness, Location Proof Server, CA) in the environment and their interaction with each other are also explain [29]. The simulation results also show power consumption and the proof exchange latency for APPLAUS. The performance evaluation has been done with three metrics (overhead ratio, proof delivery ratio and average delay). The location is verified from both parties with updated pseudonyms for avoid intruders [29].

A scheme known as "trustworthy authentication" based on trustworthy behavior of the genuine entity is defined [30]. The typical procedure consists of eight steps, main components are trustworthiness record and local trustworthy certificate with mentioned parameters and higher level trustworthy certificate with pre-define requirements. This approach is better for environment where most of the nodes are transportable and network links are effervescent. For clear autonomy the mobile users develop a trust for resources and vice versa [30].

Here in this paper, suggested two-step QR-Auth, 2D barcode authentication for entities with minimum user interaction [31]. The system consumes the visual QR-Codes in arbitrary alphanumeric data. Authorization Delegation and One-Time Password Generation are explained at packet level. In systematic and sequential way the protocol collects the sample images, transforms these images into bits and uses it as a proof of authentication [31]. The use of the system is easy due to visual rather strict and complicated password schemes. The proposed scheme shows resistance for main in middle and denial of service attacks. The visual channel is considered to be suspect for intruders, other credentials are considered to be secure [31].

A scheme known as "Secure Ubiquitous Authentication Protocols (SUAP) [32]" for efficient authentication is suggested. SUAP is a hybrid of "low-cost authentication protocol (LCAP) [33]" and "one-way hash-based LCAP (OHLCAP) [34]". The new scheme removes major drawbacks and combines the advantages of both the schemes. The random numbers and hashing value is used for encrypting the key for the protection RFID system. The threat model for RFID system consist of information leakage, traceability and location privacy, impersonation and replay attack and denial of service (DoS) attack [32]. The LCAP is explained in six steps while in OHLCAP the static identifier, a secret and one way hashed function is used. These protocols work on challenge–response method with low cost, hashed address indexing and one way functions [32].

It is self organizing scheme based on audio sampling. Which authenticate devices when they are in a specific acoustic area [35]. Recording phase, feature extraction phase, feature exchange phase and verification phase are discussed. To avoid and prevent the attacks, the feature extraction is not an arbitrary process. Because in those cases, the attacker can records the environmental sound samples and can analyzes about the auditory skin tone for a specific region [35]. The system also analyzes other relevant things which improve the system efficiency like computation cost and energy cost.

This paper argued some challenges about authentication based on formal and graphical system [35]. In the first part, cryptographic protocols or graphical language is used while in the second part, the logic is used for reasoning about the authentication protocols [35]. The payload consists with the potential identities rather than sender or receiver identities. Protocol Derivation Logic (PDL) [36] is actually the new description of Compositional Protocol Logic (CPL) [37]. In proximity authentication, a fresh nonce is used to prevent replay attacks. Proximity verification is done with the help of time channels, time channel response, specifying timed channels in PDL and with security goals of proximity authentication [35]. PDL to distance bounding is explained with a detail description of Distance bounding protocols and with Brands-Chaum Protocol [38].

Another authentication scheme is based on enhancement of the work of Lee, Batina and Verbauwhede [39] [40]. On the basis of this analysis, two of the protocols show strong privacy and third one has weak privacy preserving. A searching protocol is also offered in which a server querying a specific tag with efficiency. In first part, three previous approaches (Lee, Batina and Verbauwhede) are re-new for authentication for privacy preserving. In second part, a searching protocol has discussed based on a novel approach and working on querying a particular tag [39].

The Revised Elliptic Curve Based Randomized Access Control (EC-RAC) protocol is also explained with Randomized Schnorr Protocol [41]. Hui and their co-workers suggest new scheme for distributed authentication [42]. A trust pervasive model illustrates trust relationship among hosts based on distributed applications. Instead of the trusted third party (TTP) for reliability and security, here they distribute the services based on threshold cryptography [43]. The agent owner create signature by signing task. The agent is dispatch into pervasive network and search for a specific offer. When find an acceptable offer, it sign with TTP. Two proxy keys (prA and skA) are used for signing process [42].

A proposal is used for the protection of original digital content authentication from copyright infringement. It protects intellectual property from modification or fraudulent use of digital contents. It limits the access privileges by setting the scope of content usage [44]. The mechanism proves the authenticity for extraction and by comparison original and targeted contents. System efficiently used in offline mode for verification of the contents. Some implementations are pixel based and histogram based comparison, entropy Based Comparison Mechanism and comparison based which focus on border icon in a specific area. Also include a brief overview of frame similarity extraction algorithm. Proposed scheme is properly analyzed by applying different techniques [44].

3. CENTRALIZED APPROACH: A NEW SCHEME

We proposed a centralized approach for real time authentication in pervasive environments. Instead of mesh and dull pervasive environment, the centralized approach is more useful and efficient. Centralized approach provides a central point for connection establishment and central policy implementation. In previous approaches, the device first search for a specific service (hardware/ software) in dull passion, where every device works an independent entity in a passive manner. So if more than a dozen devices in environment and all of them are in requesting phase. Then the environment becomes interlocked and the system performance would be degraded.

4. PROBLEMS WITH EARLIER APPROACHES

4.1 Unintelligent Network

In previous approaches, most of the time, devices connect each other in a dull passion. If the required service is available with required specification then the service is availed. But if the requested entity have not compatible with provider entity then all the process is worthless. Such type of system has no idea that how to provide services on a uniform layer for hybrid network of different devices.

4.2 Latency and Delay

Devices in earlier approaches are communicated to each other concurrently for same or different services. If the multiple devices need one request which is already occupied by another one or many request generate for many services on same time, then the network experience delay in response. This delay leads to create latency in the network and finally packet results.

4.3 Hybrid Network

Earlier approaches have no support for heterogeneity between networks. Different devices have different network support. So if the requester belongs to one network and provider belongs to another, they cannot communicate. For smooth communication between different network devices, a mechanism is needed.

4.4 Binding and Resuming of a Service

What will happen if the service provider is down or fail during service consumption? From where the requester get the same service and from which point the service need to be resumed? Another scenario, if the requester needs two service and these services located on different location with devices. Then who will bind both of them for requester? For binding and resuming, a mechanism is always desired.

5. THREAT MODEL

Pervasive computing is, in fact, an ad hoc and unstructured network of different device with different network support. Compared to its predecessor ad hoc network, it has more security threats. And as newer area the pervasive networks is not so mature to prevent all attacks deployed on ad hoc network. Here we discuss the most sophisticated denial of services (DoS) and man in middle (MiM) attacks. We designed our scheme keeping in view the structure of ad hoc pervasive network with respect to these attacks.

5.1 Denial of Services (DoS)

In this attack, the attacker makes an attempt to prevent the legitimate users from availing the services. In our model, when a single user sends too many request to the base station for serving their requirements. The base station verifies the node identity and signs a certificate for it and sends it back. All this process tack time and too many requests can cause the base station for denial of service for another user. Another form of this attack is when a user occupies a service for all time and another user waiting for it.

5.2 Man in Middle (MiM)

In MiM attack, a malicious node intercepts the traffic between two communicating entities without their intensions. The man in the middle captured the packets, open it and may be changed or not and resend it for destination. Sometime the packets are captured and resend it again and again. This is variation in MiM and known as replay attack.

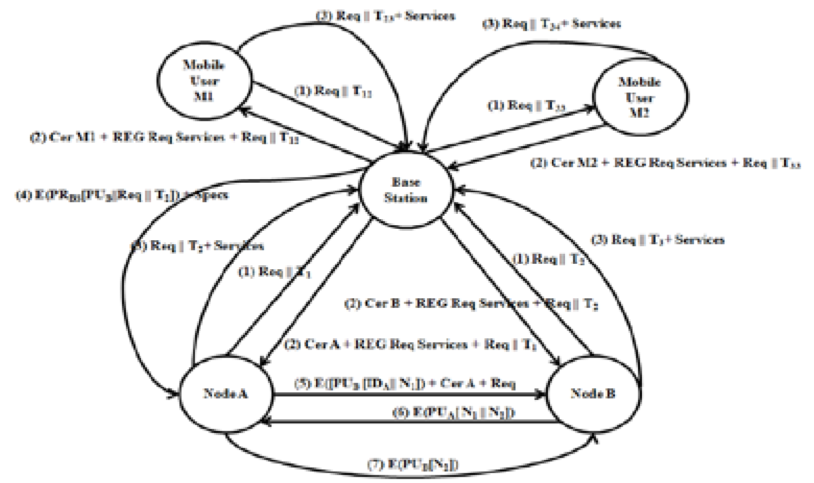
(3) Req || T_{11}+ Services
(3) Req || T_{24}+ Services
Mobile User M1
(1) Req || T_{11}
(1) Req || T_{22}
Mobile User M2
(2) Cer M1 + REG Req Services + Req || T_{12}
(2) Cer M2 + REG Req Services + Req || T_{33}
Base Station
(4) E(PR$_{BS}$[PU$_B$||Req || T_1]) + Specs
(3) Req || T_2+ Services
(3) Req || T_1+ Services
(1) Req || T_1
(1) Req || T_2
(2) Cer B + REG Req Services + Req || T_2
(2) Cer A + REG Req Services + Req || T_1
Node A
Node B
(5) E([PU$_B$ [ID$_A$|| N_1]) + Cer A + Req
(6) E(PU$_A$[N_1 || N_2])
(7) E(PU$_B$[N_2])

Fig. 3. The system architecture.

6. SYSTEM REQUIREMENTS

Central point (Base Station): Our proposed system is mainly focused on a central Base Station (BS) where all services are registered and policies are implemented. The Base station play a vital role in system performance and it shall increase system efficiency.

6.1 Hybrid Topology

Our system implementation need hybrid of both static and mobile entities with heterogeneous network supports. The central point has support of all the networks. All entities communicate to the base station. The base station provides all network support.

6.2 Two Types of Node

Our system implementation needs two types of nodes. The blind node which is only provides services and well defines nodes which provide and use the services.

6.3 Two Type of ID are Defined

If node is dull node (with very little memory & processing), the base station is responsible for all activities including key creation, distribution etc. While the well defines nodes can react in more intelligent way for key creation etc.

6.4 Two and More Networks

A base station would be providing the connecting point for different entities belongs to different networks.

7. THE BASE STATION: A CENTRAL POSITION

The base station is a central position where the entire all the devices are registered with their services with their privilege. The BS works like a central server where all devices first to authenticate itself and register their services. The BS also central place where all decisions are made and security policy are implemented. When new user came for appetites its need for a specific service, it makes a connection to the BS. The BS provides a list of services including network services. In figure-3, the overall structure with BS at the center and the basic architecture.

8. SYSTEM ARCHITECTURE

In the proposed architecture, all devices in pervasive environment should enroll with the BS and its services. The BS registers the devices and its services for controlling and accessing the registered services. The BS allows the requesting devices for using these registered services. In figure-4, all the static and incoming mobile entities registered its services with the BS.

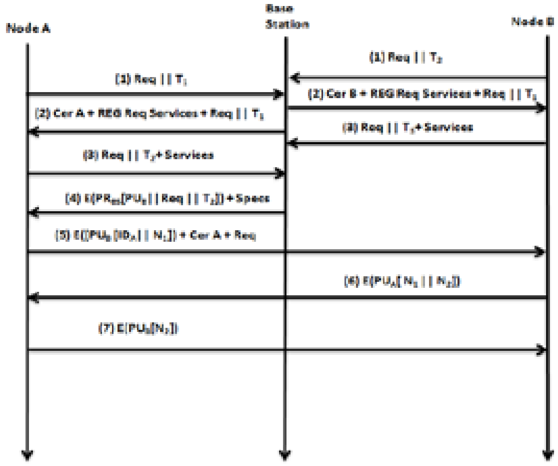
Node A
Base Station
Node B
(1) Req || T_2
(1) Req || T_1
(2) Cer B + REG Req Services + Req || T_1
(2) Cer A + REG Req Services + Req || T_1
(3) Req || T_1+ Services
(3) Req || T_2+ Services
(4) E(PR$_{BS}$[PU$_B$|| Req || T_2]) + Specs
(5) E([PU$_B$ [ID$_A$ || N_1]) + Cer A + Req
(6) E(PU$_A$[N_1 || N_2])
(7) E(PU$_B$[N_2])

Fig. 4. The BS registered the devices with the services.

In figure.4, the node "A" required a specific service; it shall request the Base Station (BS). The node "A" wants a service for example it need a high resolution screen. The BS provides a list of devices having resolution screens. The BS fist search for the screen and on the basis of ontology's, a list of devices having this services are authenticated and registered with list of instructions. Node "A" sends a request in time T1 for the BS.

$$N_A \rightarrow BS\ (Time_1 \parallel Request_A)$$

The Base Station receives the message and time of request and types of request. As the BS have already a list of services with list of privileges and the level of authenticity.

Now the BS provides the identity certificate for Node-A, and also ask for registration of services plus sending its original request to avoid main in meddle and replay attacks. The receiving of the original request, enable Node-A, to match this corresponding earlier request and to verify that the original request was not altered before reception by the BS. This guaranteed the message integrity and prevents replay attack.

$$BS \rightarrow N_A\ (Cer_A + RrgreqSer_S + Request_A \parallel Time_1)$$

$$:: \ Cer_A = E\ (PR_{BS},\ [Time_{stamp} \parallel ID_A \parallel PU_A \parallel Time_{expire}]\ )$$

A then pass this certificate to any other, who reads and verifies:

$$D(PU_{BS}, Cer_A) = D(PU_{BS}, E\ (PR_{BS}, [Time_{stamp} \parallel ID_A \parallel PU_A \parallel Time_{\ expire}]))$$

$$= [Time_{stamp} \parallel ID_A \parallel PU_A \parallel Time_{\ expire}\ ]$$

If Node-A have any service for which it welling to provide, they first enlist it with the BS before used other device service.

$$N_A \rightarrow BS\ (Services_N + Time_2 \parallel Request_A)$$

In the same way other entities also register its services with BS. And from the same the BS also knows that which entity required which service and on which device that service available.

$$N_B \rightarrow BS\ (Time_2 \parallel Request_B)$$

$$BS \rightarrow N_B\ (Cer_B + RrgreqSer_S + Request_B \parallel Time_1)$$

$$N_B \rightarrow BS\ (Services_N + Time_3 \parallel Request_B)$$

……………………………………

……………………………………

$$N_N \rightarrow BS\ (Time_n \parallel Request_N)$$

$$BS \rightarrow N_N\ (Cer_N + RrgreqSer_S + Request_N \parallel Time_n)$$

$$N_N \rightarrow BS\ (Services_{N+1} + Time_{n+1} \parallel Request_N)$$

The BS knows about all the nodes with their services and also about their request for the specific services.BS is the only place where traffic been diverted from one place to another. After passing some initial important messages for basic trust, the BS leave the communication between the nodes and remain un-active for a while.

Now after these three initial important messages with the BS, the BS responding with

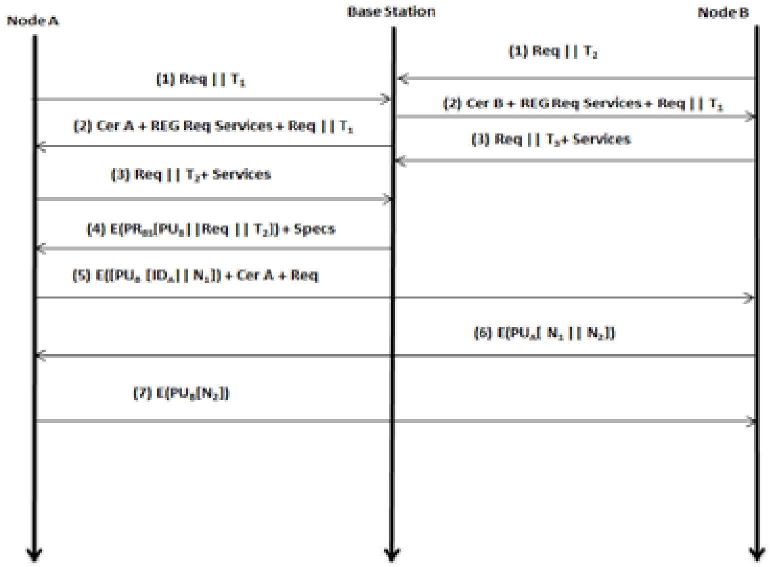
Node A
Base Station
Node B
(1) Req | | T_2
(1) Req | | T_1
(2) Cer B + REG Req Services + Req | | T_1
(2) Cer A + REG Req Services + Req | | T_1
(3) Req | | T_3+ Services
(3) Req | | T_2+ Services
(4) E(PR_{BS}[PU_B| |Req | | T_2]) + Specs
(5) E([PU_B [ID_A| | N_1]) + Cer A + Req
(6) E[PU_A[N_1 | | N_2])
(7) E(PU_B[N_2])

Fig. 5. Node-A and Node-B authenticate with BS.

properly identified entities for that specific service. Consider the Figure-5, in which two entities Node-A and Node-B develop a trust and they authenticate with BS.

After the third message from the Node-A to BS, the BS responds with the encrypted same request and public key of Node-B, having the requested service and also included the specifications of the same device. Specification tells the requested node about the system description including network and platform and also tells about the policy and access rights.

$$BS \rightarrow N_A \ (E\ (PR_{BS}[PU_B||Req \ || \ T_2]) + Specs)$$

After receiving this message the Node-A, know the identity of the Node-B (PU_B), the type of request and all this encrypted by the "PR_{BS}" (Private Key) of BS. So the Node-A decrypt it with "PU_{BS}". Now Node-A knows about the other entities having the service and also clarify the access of these resources by the BS.

Now Node-A sends a message directly for Node-B, after analyzing and decrypting above message. The message moves directly from Node-A to Node-B without the involvement of BS.

$$N_A \rightarrow N_B \ \ (E([PU_B\ [ID_A||\ N_1]) + Cer\ A + Req)$$

Now Node-B receives the message having "Cer_A" (Certificate of Node-A), request type and "ID_A" identity of Node-A, who is requesting for a service and unique nonce "N_1". The ID_A and N_1 are encrypted by "PU_B" (Public Key of Node-B). Nonces are used to identify this transaction uniquely. The message prove many things including the identity of the requesting node and certificate of Node-A, which prove the authenticity of the node and can verify from BS. The nonce avoids the main in the middle (replay attack) attacks and encryption with public key ensures the encryption of the message. The Node-B can verify the identity or authenticity of the Node-A, from the BS.

Now the public keys have been securely delivered to both node "A" and "B". At this point, the identities (public keys) of both are delivered and verify and now able to start secure exchange. However, some additional steps are required. Now node "B" responds against the request of node "A" with nonce (N_1) and new generated nonce (N_2), encrypted with "A" public key (PU_A). Nonce (N_1) assured node "A" that response is come from "B".

Now the Node-B responds with a verify message for completing the trust level. The Node-B sends an encrypted message having nonce "N_1" and nonce "N_2" encrypted with the "PU_A" (Public key of Node-A).

$$N_B \rightarrow N_A \ \ (E(PU_A[\ N_1\ ||\ N_2])\ )$$

The encrypted message verifies the authentication as well as encryption and only the corresponding Node-A can decrypt it with its private key. The nonce verifies that messages are not replay or duplicate.

The Node-A, sends the last message before the actual use of the service on the Node-B. Now Node-A return nonce (N_2) to Node-B, is encrypted by public key of "B" (PU_B) which assured that corresponding is Node-A.

$$N_A \rightarrow N_B \ \ (E\ (PU_B\ [N_2])\ )$$

Hence, seven messages are required for complete understanding and conformation of messages between them. The initial four messages are used rarely because when these messages are received, the nodes save the public keys for future use and the technique is known as "caching".

9. SECURITY ANALYSIS

Here we discuss the proposed system with proper prevention of some most dedicated attacks. We analyze the scheme in the presence of some attacks.

9.1 Base Station has Overall Policy

The base station is a central point where all decisions are made and all policies are implemented. It is the base station which periodically checks the status of the resource. If resource is remains for more than one entity a specific time, the BS disconnected the session and updates the status of the device in device list (Dev_i). So if another device waiting for the same resource, it should be made available for them.

9.2 Unauthorized Access of Resources

The Base station implements the security policy and the whole network of different devices follow the same policy for using and offering the resources. Every notation and symbol has a proper meaning with proper resistance against some attack. The unauthorized accesses to resources are prevented by valid certificates (Cer_N). Any one wants to use the resource; it first goes for BS to gain the attention for resources. The BS authenticates the requesting node by issuing proper certificate. Those nodes having no certificate should not authorize to use the resource. In the diagram 3, the first three messages between requesting node and base station ensure the identity for authorization.

9.3 No one can Spoof

Every entity has a pre-define certificate and a proper identity before it becomes a part of pervasive network. The identity and certificate of a node is properly defined and this mechanism prevents all type of spoofing attacks. The messages are communicated between entities in a proper mechanism and messages are communicate securely between base station and nodes. No one can pretend the identities of the other nodes for impersonation.

9.4 No Replay Attack

The time stamp and nonce in every request ensure time sequences and unique transaction for each message respectively. These parameters (time stamp &nonce) prevent any attempt for impersonation and base station know the time and sequence of the messages. The base station can discarded those messages which are sent by node again and again for illegal operation at the base station.

9.5 Main in the Middle Attacks (MiM)

The MiM attack is prevented by using IDs, nonce, certificate and keys related in each transaction. The encrypted messages create secure transactions of message between base station and nodes and between nodes to nodes.

10. SERVICES SELECTION ALGORITHM

The following algorithm determines available devices and also resolves the required service request if available.

Algorithm 1: Devices discovery and services selection: DevSelServSel (Dev_i, $Serv_i$, $Task_i$,Req_i,)

```
1:  Base Station (BS) has a list of Devices ($Dev_i$) with list of Services ($\text{Serv}_i$).
    Let BS: =$\{Dev_1 + Serv_1 * Dev_2 + Serv_1 + Serv_2* Dev_3 + Serv_4* Dev_5 + Serv_5* Dev_6 + Serv_8*\ldots\ldots\ldots\ldots*Dev_n + Serv_{n+1}\}$
2:  Sort List of Devices ($Dev_i$) according to time and frequent use (quality of device)
    Let sorted List: = $\{Dev_2 + Serv_1 + Serv_2* Dev5 + Serv_5 *\ldots\ldots\ldots\ldots\ldots\ldots.\}$
3:  Request($Req_i$) for a specific Device ($Dev_i$) or Service ($Serv_i$)
    Let the ($Req_s$):= $\{Dev_s + Serv_{s1} + Serv_{s2}\}$
3:  Checkforeach device in the List($Dev_i$)
    For i: =$Dev_1$ to $Dev_n$Do
4:  Check for each service in the List ($Serv_i$)
    For j: = ($Serv_1$) to ($Serv_n$)Do
5:  Check if the request is fulfill for specific ($\text{Req}_s$)
    IFfit {($Req_i$)== ($Dev_i$)AND ($Req_i$)== ($Serv_i$)}
    Else Go to Exit
5:  Check the status of the device ($Dev_i$) and service ($Serv_i$)
    IF  {($Dev_i$)|| ($Serv_i$)== Buzzy}
    Else Go to Exit
6:  Selection of specific ($Dev_s$) or ($Serv_s$)
    Select {($Req_s$) ➔ ($Dev_s$)AND ($Req_s$)➔($Serv_s$)}
7:  Check the Authenticity of devices ($Dev_s$)
    For each selected Device ($Dev_s$)and Service ($Serv_s$)
    IF (Authentic == Successful)
    Else Go to Exit
8:  Check the Authorization
    For each Device ($Dev_i$)and Service ($Serv_i$)
    IF (Authorized == Successful)
    Else Go to Exit
9:  Connection Granted
10: End IF
11: End For
12: End IF
13: End For
14: End IF
15: End IF
16: End IF
```

11. THE DATA FLOW DIAGRAM

The algorithm clearly mentions the main step of the overall system. In following data flow diagram, the device makes a request for connection with the other nodes for services. The

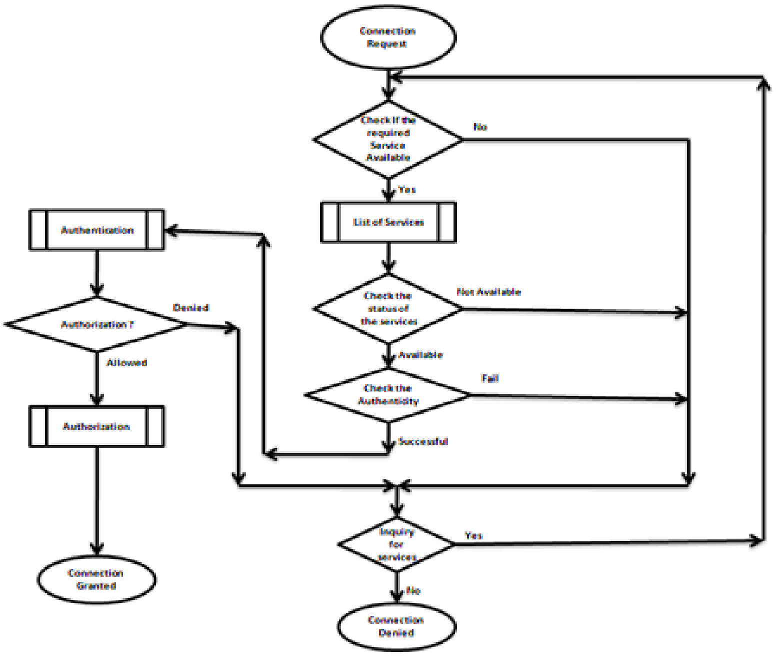

Fig. 6. The data flow diagram.

base station checks the policy implemented on the network entities, if satisfied, the connection is granted. In figure-6, show the overall flow of control from requesting phase to granted phase. When the requester is make a request for connection to the network for required services. The base station checks the required service in the service list with its specification and availability. If the service is not available then request is satisfied with no availability of service. And if the service is available, it is provided a list of that service. The list tells the requester about the number of availability and specifications. After that the status of the service is checked, either it busy or not and also its priority on user level. If the service is available then check it authenticity. And if the authenticity is satisfied then the algorithm checks the authorization of the requester for the specific request. If the authorization is also satisfied then the connection for a request is granted. Figure-6, show the overall data flow model.

12. ANALYSIS OF THE SYSTEM

For performance evaluation of our proposed novel light weight and centralized scheme, we use NS-2 (v-2.35) network simulator. The terrain is about (600 x 600) meters with randomly deployed nodes and a dedicated BS. The transmission range of the BS is 400 meters while other nodes have the range of 250 meters only. Some nodes are stationary while some in motion. The environment is check with different number of nodes from 5 to 50. Moving nodes move randomly in the same topological space with a speed 1,5,10,15,20,25 and 30 m/s with simulation pause time is fixed to 25 seconds. The network is established with IEEE 802.11 at data link and physical layers. The AODV (Ad-hoc On-Demand Distance Vector) protocol is implemented on network layer and with CBR (continuous bit rate) traffic over UDP link on transport layer. With 0.2 Mbps packets transmission rate, 512 bytes packet size and 200 seconds is simulation time with average transmission for flow is 2 bytes per second. The key size is 512 bit and the same model is used for uniformity in simulation. The cbrgen is used for constructing linking patterns while setdest is used for creating mobility model.

Average end to end delay: The time experienced by data packets when transmitted by CBR source for its corresponding CBR receiver. Average end to end delay includes all types of delay in the network like delay in buffering, acquisition delay and even processing delay at nodes. From simulation results in figure-7, indicates the end to end delay between two nodes without base station. End to end delay increases in the presence of a malicious node. When the malicious node working as in middle to gain the messages access and also gain authorization.

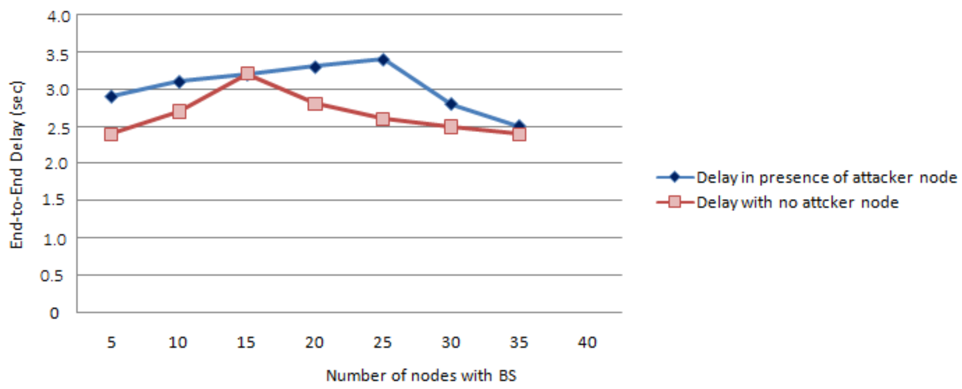

Fig. 7. End to end delay.

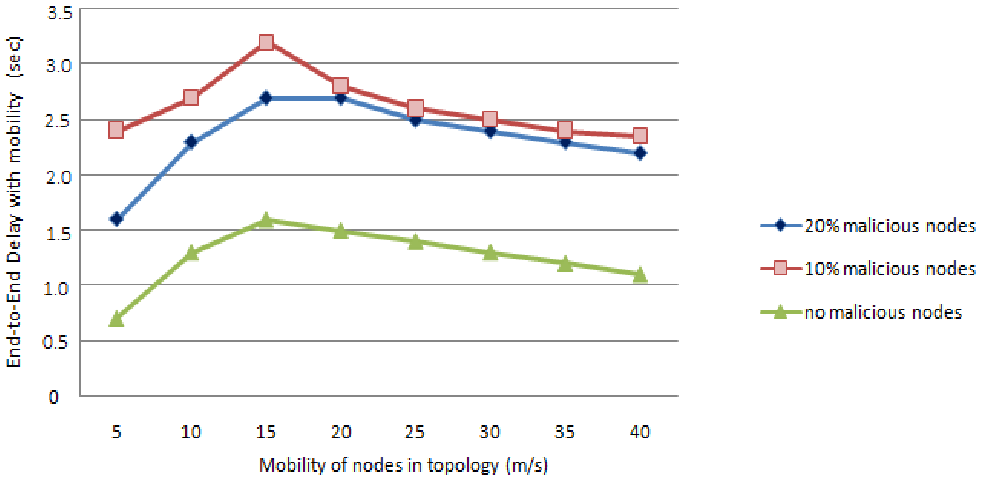

Fig. 8. End to end delay with mobility.

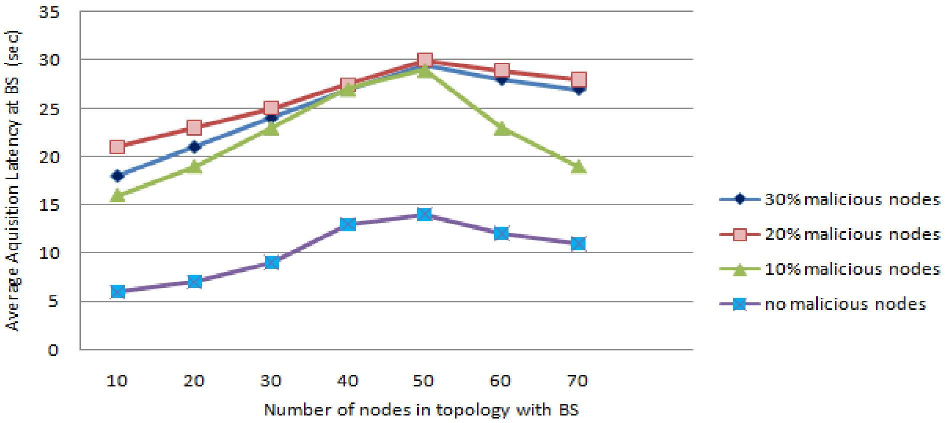

Fig. 9. The average acquisition delay.

Average end to end delay with mobile nodes: We also analyzed the proposed scheme with mobile and static nodes. The figure is, in fact, the results of the static nodes network analysis. In figure-8, the scheme managed mobile nodes with the presence of malicious nodes. The results clarify when the number of malicious nodes increase (15%), the system will experienced more delay as compared to the network having less amount (5%) of malicious nodes. The 5% malicious nodes have delay at certain level but the carve 10% and 15% of malicious nodes overlap each other, show that after a certain level the system performance degrade when the malicious nodes increases.

Average acquisition latency: This is the amount of time experienced when a node first request for a service, search it, content to base station and find the service on a specific device. In fact, it is the average delay experienced by node when request for a service available in the same premises. In figure-9, the average acquisition delay increases moderately when the number of malicious nodes increases. With increasing the number of genuine and malicious nodes, the base station feels more load for serving certificate and related security policies. But after certain level (30 nodes), carve tends to lower because the congestion feels at the base station been resolved.

13. CONCLUSION

Traditional computing have changed by real time and embedded devices by providing on the fly services. These embedded and smart devices have greater impact on our daily lives. Now services are available everywhere, every time and for everyone. These devices use its processing and communicating capabilities and conduct itself according to the user mood and circumstances. These devices communicate each other and construct an ad hoc and unstructured network of heterogonous devices. For better quality of services, these devices should communicate in such a way to provide services to end user in a uniform way. In such hybrid network, the authentications of all entities are important including devices, services, users and process. Here we proposed a novel lightweight, portable and centralized scheme based on symmetric security approach. The communicating entities ensure its authentication with the base station before the availability of a service. The base station is a central point with controlling the overall network entities. The base station checks the level of authenticity and specification of both devices before they make the connection. In our research we implement a security policy on ad hoc and hybrid network in NS-2. We analyzed our scheme in the presence of malicious nodes and we conclude that the system is properly worked and it is securing the resources from an attacker.

14. REFERENCES

1. Brush. A., J. Hong & J. Scott, Pervasive computing Moves in, *IEEE Pervasive Computing* 15: 14-15 (2016).
2. Carteron. A, C. Consel & N. Volanschi. Improving the Reliability of Pervasive Computing Applications By Continuous Checking of Sensor Readings. In: *IEEE International Conference on Ubiquitous Intelligence and Computing,* Toulouse, France (2016).
3. Weiser. M, The computer for the 21st century. *Scientific American* 265: 94-104 (1991).
4. Huang. A.C., B.C. Ling & S. Ponnekanti. Pervasive Computing: What is it good for. In: *Proceedings of the 1st ACM International Workshop on Data Engineering for Wireless and Mobile Access,* p. 84-91 (1999).
5. McKernan. K.J. The Chloroplast Genome Hidden in Plain Sight, Open Access Publishing and Anti-fragile Distributed Data Sources. *Mitochondrial DNA,* p. 1-2 (2015).
6. Rudolph. L. Project Oxygen: Pervasive, Human-Centric Computing, an initial experience. In: *International Conference on Advanced Information Systems Engineering,* p. 1-12 (2001).
7. Ceesay. E.N., C. Chandersekaran & W.R. Simpson. An Authentication Model for Delegation, Attribution and Least Privilege. In: *Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments*. p. 30 (2010).
8. Foster. I., C. Kesselman, G. Tsudik & S.A. Tuecke. Security Architecture for Computational Grids. In: *Proceedings of the 5th ACM Conference on Computer and Communications Security*. p. 83-92 (1998).
9. Turkanovi. M., B. T. Brumen & M. Holbl. A Novel User Authentication and Key Agreement Scheme for Heterogeneous Ad hoc Wireless Sensor Networks based on Internet of Things Notion. In: *Ad Hoc Networks,* 20, p. 96-112 (2014).
10. Farash. M.S., M. Turkanovia, S. Kumari & M. Holbl. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things

environment. In: *Ad Hoc Networks,* 36, P 152-176 (2016).

11. Sethi. M., P. Kortoasi, M. Di Francesco & T. Aura. Secure and low-power authentication for resource-constrained device. In: *Internet of Things (IOT), 2015 5th International Conference on the Internet of Things (IOT),* p. 30-36 (2015).
12. Sher. M. & T. Magedanz. Secure access to IP multimedia services using generic bootstrapping architecture (GBA) for 3G & beyond mobile networks. In: *Proceedings of the 2nd ACM International Workshop on Quality of Service & Security for Wireless and Mobile Networks,* p. 17-24 (2006).
13. Ning. H., H. Liu & L.T. Yang. Aggregated-Proof based Hierarchical Authentication Scheme for Internet of Things. In: *IEEE Transactions on Parallel and Distributed Systems,* 26. p. 657-667 (2015).
14. Jan. M.A, P. Nanda, X. He, Z. Tan & R.P. Liu. A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment. In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. p. 205-211 (2014).
15. Marta-n-Fern A¡ndez. F, P. Caballero-Gil & C. N. Caballero-Gil. Authentication Based on Non-Interactive Zero-Knowledge Proofs for Internet of Things. In: *Sensors,* 16, P 75 (2016).
16. Wang. X., L.Y. Yin & H. Yu. Finding collisions in the full SHA-1. In: *Annual International Cryptology Conference*, p. 17-36 (2005).
17. Juels. A. RFID security and Privacy: A Research Survey. In: *IEEE journal on selected areas in communications,* 24. P 381-394 (2006).
18. Zhu. F., M.W. Mutka & L.M. Ni. Private Entity Authentication for Pervasive Computing Environments. In: *IJ Network Security,* 14: p. 86-100 (2012).
19. Kambourakis. G., S. Gritzalis. & J.H. Park. Device Authentication in Wireless and Pervasive Environments. In: *Intelligent Automation & Soft Computing,* 16: p. 399-418 (2010).
20. Bahl. P., A. Adya, J. Padhye & A. Walman. Reconsidering Wireless Systems with Multiple Radios. In: *ACM SIGCOMM Computer Communication Review,* 34, P 39-46, (2004)
21. Committee. I.L. M.S. IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed bands and Corrigendum 1. In: *IEEE Std 802.16-2004/Cor 1-2005, (*2006).
22. Group. T, TCG Specification Architecture Overview Revision 1.2. (2004).
23. Wen. H.A, C.L. Lin & T. Hwang. Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients. In: *Computers & Security,* 25: p. 106-113 (2006).
24. Rekha. R. N & M. Prasad Babu. On some security issues in pervasive computing-light weight cryptography. *International Journal on Computer Science and Engineering,* 4: 267 (2012).
25. Betz. V, J. Rose & A. Marquardt. In: *Architecture and CAD for Deep-submicron FPGAs* 497. Springer Science & Business Media (2012).
26. Landis. D. Programmable Logic and Application Specific integrated Circuits. (1999).
27. Abi-Char. P.E, A. Mhamed & E.H. Bachar. A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications. In: *The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007),* p. 235-240 (2007).
28. El Husseini. A, A. Mac hamed, B.E. Hassan & M. Mokhtari. A novel trust-based authentication scheme for low-resource devices in smart environments. *Procedia Computer Science,* 5: 362-369 (2011).
29. Zhu. Z. & G. Cao. Applaus: A privacy-preserving location proof updating system for location-based services. In: *INFOCOM, 2011 Proceedings IEEE,* p. 1889-1897 (2011).
30. Batyuk. L., S. L. Camtepe & S. Albayrak. Multi-device key management using visual side channels in pervasive computing environments. In: *International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA),* p. 207-214 (2011).
31. Morshed. M.M, A. Atkins & H. Yu. Secure ubiquitous authentication protocols for RFID Systems. *EURASIP Journal on Wireless Communications and Networking.* p. 1-13 (2012).
32. Lee. S.L., Y.L. Hwang, D.H. Lee & J.I. Lim. Efficient authentication for low-cost RFID systems. In *International Conference on Computational Science and Its Applications,* p. 619-627 (2005).
33. Choi. E.Y, S.M. Lee & D. H. Lee. Efficient RFID authentication protocol for ubiquitous computing environment. In: *International Conference on Embedded and Ubiquitous Computing,* p. 945-954 (2005).
34. Morshed. M.M, A. Atkins & H. Yu. Privacy and security protection of RFID data in E-passport. In: *5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA),* p. 1-7 (2011).
35. Kim. S.J & S.K. Gupta. Audio-based Self-organizing Authentication for Pervasive Computing: A cyber-physical approach. In: *2009*

International Conference on Parallel Processing Workshops, p. 362-369 (2009).

36. Datta. A, A. Derek, J.C. Mitchell & D. Pavlovic. A derivation system for security protocols and its logical formalization. In: *Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE,* p. 109-125 (2003).
37. Brands. S. & D. Chaum. Distance-bounding protocols. In: *Workshop on the Theory and Application of Cryptographic Techniques,* p. 344-359 (1993).
38. Lee. Y.K, L. Batina, D. SingelAae & I. Verbauwhede. Low-cost untraceable authentication protocols for RFID. In: *Proceedings of the Third ACM Conference on Wireless Network Security,* p. 55-64 (2010).
39. Lee. Y.K, L. Batina & I. Verbauwhede. Untraceable RFID authentication protocols: Revision of EC-RAC. In: *2009 IEEE International Conference on RFID*. p. 178-185 (2009).
40. Schnorr. C.P. Efficient Identification and signatures for smart cards. In: *Conference on the Theory and Application of Cryptology,* p. 239-252 (1989).
41. Liu. H. & C.M. Zhang. Research on Use of Distributed Authentication in Pervasive Computing. In: *2006 First International Symposium on Pervasive Computing and Applications* (2006).
42. Desmedt. Y.D. Threshold Cryptography. In: *European Transactions on Telecommunications,* 5: p. 449-458 (1994).
43. Jang. E.G, B.S. Koh & Y.R. Choi. An Authentication Mechanism of Digital Contents in Pervasive Computing Environment. In: *International Conference on Information Security and Assurance, 2008. ISA 2008,* p. 527-533 (2008).
44. Eskicioglu. A.M & E.J. Delp. An Overview of Multimedia Content Protection in Consumer Electronics Devices. *Signal Processing: Image Communication,* 16: p. 681-699 (2001).