Identity-based Authentication and Access Control in Wireless Sensor Networks

Abdullah Al-Mahmud
Masters Student, ICT,
The Royal Institute of Technology(KTH),
Stockholm, Sweden

Matei Ciobanu Morogan
Lecturer, Department of Computer and System Science,
The Royal Institute of Technology(KTH),
Stockholm, Sweden

ABSTRACT

The application and usage of the wireless sensor network is rapidly growing. Wireless sensor networks are normally deployed into the unattended environment where the intended user can get access of the network. The sensor nodes collect data from this environment. If the data are valuable and confidential then some security measures are needed to protect the data from the unauthorized access. In this paper, I propose an identity-based user authentication and access control protocol based on the Identity-Based Signature (IBS) scheme where the ECC (Elliptic Curve Cryptography) based digital signature algorithm (DSA) is used for signing a message and verifying a message for a wireless sensor networks. This protocol accomplishes the registration of a new user, authentication of a user, session key establishment between sensor node and the user; and finally grants the appropriate data access to the user. User revocation is also handled in this proposed protocol. Compared with other conventional security solutions, this protocol provides confidentiality and integrity of the sensor data; and also achieves better computational, communicational performance and energy efficiency due to the use of more efficient IBS algorithms based on ECC than those based on RSA.

KEYWORDS: WSN, Security, Authentication, Access control, IBS.

1. INTRODUCTION

The sensor nodes in the sensor networks sense or monitor the environmental and physical changes to collect data. It also collects data from its neighbor nodes and its surrounding environment. These data are communicated to the other nodes over the wireless connection. The data that are collected by the sensor node may be confidential and in some cases the data is only visible to the authenticated users. The security in sensor networks varies from application to application. In some applications, some outsider users may also feel interest to modify the data that are collected by the sensor node. If they success to modify the data then the integrity of data may be violated. So it is important to protect data from the unauthorized access. Another way, all authenticated users do not have the right to access all kinds of information from a node. Every user has their own privileges to the access the data from the network. Some information may need to hidden from some users. So a secure authentication and access control protocol may help to ensure these three important issues data confidentiality, data integrity and access control of data.

Wireless sensor networks authentication can be classified into three categories [1] such as base station authentication, sensor node authentication, and user authentication. The base station authentication in WSN is same as the traditional networks where the base station are registered and authenticated by other base stations. The base station authentication has been addressed deeply in many research papers [2, 3]. The sensor node authentication can be done by the base station and other sensor nodes. When a sensor node broadcasts its authentication request in the network, the sensor nodes and base station authenticate that node. The authentication protocol decides how a node will authenticate in the network.

Generally a system need to do four important functions such as user registration, user authentication, session key establishment and access control; to provide the access on data to the outsider users[1]. The user authentication ensures the only subscribe user can get access on the data. Session key establishment ensures the secure exchange of data including the user request and response. Access control ensures that the user only get access on those data to which the user is permitted. User may connect to the network with his or her mobile device like PDA. To get access the network user must need to authenticate to the entity with in the network. User may authenticated by the base station, sensor nodes or both which is based on the protocol. Normally authentication can be done in two ways [1] - centralized and distributed authentication. In centralized user authentication system, the users are authenticated by the base station. This system is very simple and easy to implement because the base station is a powerful device which can perform lots of complex cryptography functionalities. But the system has some problems. First the system has a single point of failure; that means if the base station fails then the overall system will not work. Second sensor node closed to the base station will more busy to forward the request and response; and reduce quickly their energy. Third it may affect the DoS attack. So a distributed approach will help to solve the problem in centralized approach. The proposed protocol is a distributed approach which will reduce the traffic congestion and transmission overhead within the network.

The aim of this research is to propose an efficient identity-based authentication and access control protocol in wireless sensor network that helps to protect the data of a sensor node from illegitimate access, overcome the existing problems in authentication as well as access control of sensor networks and also preserve the security issues of the nodes. Finally the proposed protocol should be analyzed through the implementation (simulation) and theoretical analysis.

2. CRYPTOGRAPHY PRIMITIVES

The proposed protocol is based on the Identity-Based Signature (IBS) [4] scheme where the ECC (Elliptic Curve Cryptography) based on digital signature algorithm (DSA) is used for the signing a message and verifying the signature. There are many IBS scheme available based on the RSA algorithm. The RSA signature is relatively larger in size which increases the size of the message. However the verification procedure of RSA signature is more efficient than ECC [5]. The signature based on ECC is very important to sign and verify the message in WSN because in WSN the smaller size of the message is desired due to the resource constraint network.

The base station works as a PKG (Private Key Generator). IBS is a collection of four different algorithms such as system setup, key extraction, signature generation and signature verification [4]. The brief description of these algorithms is shown below-

2.1 System setup: This algorithm is run by the master entity (BS) which takes a security parameter ***k*** as input and generates a master secret key ***SKPKG*** and public system parameters ***P*** as output. The BS publishes the public system parameter for all and keeps the master secret key to itself.

2.2 Key Extract: The BS uses this algorithm to generate the private key of the users and sensor nodes. This algorithm takes system parameter ***P***, a master secret key ***SKPKG*** of the BS and the identity of the user (***UIDA*** for user A) or sensor node (***SIDB*** for node B) as inputs and generates the private key ***DIDA*** associated with the identity of the user **UIDA** or ***DIDB*** associated with the identity of the sensor node ***SIDB*** as output. The private key of the user then transfer to the user through a secure channel.

2.3 Signature generation: This algorithm takes a message ***m*** and the private key of the entity i ***DIDi*** as inputs and generates a signature ***б*** of the entity i on the message ***m***.

2.4 Signature verification: This algorithm takes a message ***m***, identity of the entity, a signature ***б*** and system parameters ***P*** as inputs. The output of this algorithm is accepted if the signature ***б*** on the message ***m*** is valid for the entity and reject otherwise.

3. ASSUMPTION

In this research, a wireless sensor network that consists a network administrator, one or more base stations, a large number of sensor nodes and many users have been considered. The network administrator preloads the identity of the users/sensor nodes and places the user in a group of the access structure according to the role of the user in the network. The access structure defines what type of the data a user can access from the network. For any update the administrator always inform the base station. Base station plays the role of the private key generator (PKG), from where all the sensor nodes and users will take their respective private key. Sensor nodes authenticate the user and grant the access of the data that a user requested.

A typical network architecture of the proposed protocol is shown in the figure 1. The architecture is used the hybrid network topology consisting one base station, a network administrator, large number of sensor nodes and many users. Users are connected locally by the sensor nodes using their own device like PDA. Sensor nodes are connected directly to the base station or through the other sensor nodes. All sensor nodes and users are connected to the network by the wireless communication medium. The network administrator is directly connected with the base station using the wired communication medium. Bass station may be connected with other base stations by using the wired connection.

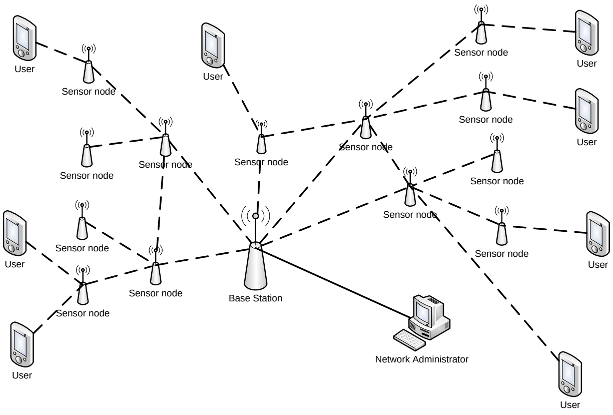


Figure 1: A typical network architecture for the proposed protocol.

4. PROPOSED PROTOCOL

In this proposed protocol, user authentication and access control will present. This part will discuss with the protocol itself. The following table 1 contains the description of the symbols used in this protocol.

Table 1: Description of the symbols used in this protocol.

Symbol	Meaning
UIDA	Identity of user A
BS	Base station
H1	One-way hash function
||	Concatenation
k	Security parameter
SKPKG	Master secret key of the PKG (base station)
PKPKG	Public key of the BS
P	Public system parameters
DID_A	Private key of the user A
б	Signature of the user
TS	Time stamp
TK	Ephemeral key
ΔT	Maximum communication delay
SK	Session key
χ	Key derivation function
α	Access structure
g	Group identity of the user in the access structure that defines the set of right of the user

The proposed authentication and access control protocol works in three different steps, are described in the following sections.

4.1 System initialization

BS is the private key generator (PKG). During this initialization phase, BS initializes itself first then it registers all sensor nodes and users; and also broadcast the register users and sensor nodes list in the network. In this phase, BS performs the following functions:

1. BS chooses a master secret key ***SKPKG*** for its own and computes its public key ***PKPKG***.
2. Base station set the public system parameter ***P*** that includes the user data access structure ***α*** and public key of the base station ***PKPKG.***
3. BS registers all valid users and uses its private key ***SKPKG*** to generate the private key ***DID_i*** of all users i. All users i store their identity ***UIDi,*** private key ***DID_i*** and system parameter ***P*** before their deployment.
4. BS also registers all valid sensor nodes and uses its private key ***SKPKG*** to generate the private key ***DID_i*** of all sensor nodes i. Every sensor nodes i stores their identity ***SIDi***, corresponding private key ***DIDi*** and system parameter ***P*** before their deployment.
5. When a user A register with the BS. BS stores the dataset (***UIDA***, ***TS, g***) in its registered user database list where ***g*** is the group identity of the user in the access structure that defines the set of right of the user A and also broadcast the registration information of user A by sending the dataset (H1(UIDA), TS, g). Sensor node stores the hash value of the user identity instead of the identity which reduces the node storage content. BS does similar process for a sensor node. BS never keeps the private key of the users to itself.

4.2 User authentication and session key establishment

After a user successfully register with the BS, the user may wish to communicate in the network. Before to communicate or access the data from the network, the user must need to authenticate to the sensor nodes where the user wants to communicate or access data. After completion of successful authentication both (sensor node and user) parties establish their session key. Session key ensures that the future communication between the user and the sensor node will be secure. Key exchange protocol is very important to secure exchange of the session key between two parties. In this proposed protocol one-pass key establishment [6] is used for the session key establishment. User authentication and session key establishment are in the same phase because it reduces the numbers of message exchange during the key establishment phase. The authentication and session key establishment process between a user A and a sensor node B is given below-

Step 1. User A choose a random number r ε Zq^* and compute the ephemeral key ***TK*** as ***TK*** = ***rH1***(***UIDA***). ***TK*** will be used in step 6 by the sensor node to generate the common secret ***K_{BA}*** for competing the successfully authentication.

Step 2. User A sign an authentication request message R which include **TS**, ***TK*** and ***UIDA;*** and sends it to the sensor nodes surrounding the user for the authentication. The user uses the signature generation algorithm of IBS to sign the message. To avoid the replay attack the user send the sending timestamp ***TS*** with the signed message.

Step 3. The sensor nodes surrounding the user receive the authentication request message R from the user. Now the receiving node performs three checking on the received request.

- At first the node checks whether the user is already registered or not from the registration history of the user that the node received from the BS. If the user is not in the list then sends a *Msg(REJECT_LOGIN)* and stops all communication to the user otherwise go to the next step.
- Second the node checks the ***TS*** of the request message whether it is newly generated message or a replayed request message. Here the user consider the maximum communication delay ***ΔT***. Assume the current time stamp is ***T***. If (T-TS) ≥ ΔT then the message is a replayed message and the node sends a Msg(REJECT_LOGIN) and stops all communication to the user otherwise go to the next step.
- Third the nodes now verify the signature of the user using the signature verification algorithm in the IBS. If the signature is not valid then the node sends a Msg(REJECT_LOGIN) and stops all further communications to the user otherwise go to the step 4.

Step 4. Sensor node B now sends its' own identity SIDB along with its signature to the user for authentication.

Step 5. After receiving the identity from the sensor node, first the user checks whether the message is replied or not then the user verifies the signature of the sensor node. If the verification successful then computes the shared common secret ***K_{AB}*** using the algorithm ID-based One-pass Authenticated Key Establishment described in [6] and sends it to the node.

Step 6. Sensor node also computes the common shared secret ***K_{BA}*** using the same algorithm. If the ***K_{AB} = K_{BA}*** then the authentication successful.

Step 7. Both parties now compute the session key ***SK*** using the key derivation function ***χ*** as ***SK*** = ***$\chi(K_{AB} \| TS)$***. Now the ***SK*** is ready to encrypt all messages between two communicating parties.

4.3 Data access

The user initiates the request to access the data and the sensor nodes verifies the user whether the user have such privilege or not. User may request the data access before the authentication of the user, and then the user will authenticate first then get access the data according to the privileges of the user. If a user is already authenticated and have a valid session then the data access request verify only whether the user have such privileges or not that the user requested. The steps to allow the access of data are following-

1. User A generates a request to access data from the sensor node B.
2. If the user is already authenticated by the node B and has a valid session then the node B will check whether the user is authorized to perform the requested action, from the access structure that node B received from the BS otherwise start from the authentication phase.
3. If the user has the privilege to access the data that he requested then the node will send a response that includes the requested data to the user otherwise Msg(NO_ACCESS) will send to the user.

4.4 Update of the user information

BS always provides up-to-date information to the entities in the network. When a new user is added into the network, BS immediately informs the network about the presence of the user because after registration with the BS, the user may send authentication request to the sensor nodes for further communication to the network. BS maintains a list of compromised users. When a user compromised and BS gets information about the compromised user, it puts that user into the compromised users list and passes it to the network to preserve the security for the networks.

4.5 User revocation

User revocation can be due to different expected and unexpected reasons, e.g., expiration of the subscription, network access policy violation, group changing, secret key exposure, etc. [7]. In this proposed protocol, two different reasons have been considered for user revocation.

Every user has an access time, is defined by the BS during the time of registration. When the BS computes the secret key of the user, it uses the expiration of access time of the user as a parameter. So after the expiration of the secret key if the user places a signed request to a node then the node will verify the signature and the signature verification will not pass. As a result the user will not be authenticated for the communication.

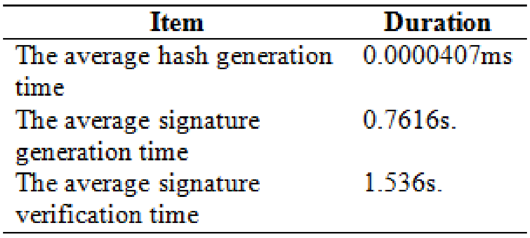
User may be compromised. When the BS gets information about the compromised user, it then put the user into the list of compromised users which the BS passes periodically to the network. Sensor nodes store the list of compromised users. When a compromised user places a request to the node for accessing the network then the node checks whether the user is compromised or not. If the user is in the compromised users list then the node does not pass the request of the user.

5. SIMULATION RESULTS

Some main feature of the proposed protocol has been simulated by the Network simulator 2 (NS2) where the programming part is done by the programming language C++ where some cryptographic operations are performed by some third party library such as crypto++ [8], minisip [9], Posix [10], OpenSSL [11].

The proposed protocol has been simulated and the results that I have been found from the simulation are shown in Table 2.

Table 2: Simulation results



Item	Duration
The average hash generation time	0.0000407ms
The average signature generation time	0.7616s.
The average signature verification time	1.536s.

6. ANALYSIS OF THE PROTOCOL

The terms security and efficiency is opposite from each other. If we consider strong security then the efficiency will be decrease and on the other hand if we want high efficiency then we cannot guaranteed the security. So it is very important to balance these two within an agreement. This chapter analyses the proposed authentication and access control protocol in terms of security and efficiency.

6.1 Security Analysis

The security analysis is an important part in the research. Some basic terms according to the achieved security are given below:

6.1.1 Mutual authentication

The proposed protocol authenticates only those users who have a valid secret key. Both the user and sensor node are mutually authenticated by each other through the signature verification process. User gets his secret key from the PKG by showing its identity. User with a valid secret key can sign a message and send the message with its signature to the nodes for authentication and the node verifies the user signature. If the signature of the user is valid then the node also sends its' own identity to the user for authentication. User verifies the signature of that node. So both parties know each other. Mutual authentication allows for avoiding impersonating the sensor nodes in order to send fake data to the user. So the users are confirmed about the accuracy of the received data.

6.1.2 Integrity

Integrity of the message can be ensured by verifying the signature. When a user sent a message, it includes the signature of the user into the message. If any changes made during the transmission of the message then the signature verification does not pass. So the receiver can detect the integrity violation through the signature verification of the user.

6.1.3 Confidentiality

Sensor node collects data from their environment. These data moves among different nodes and sometimes outsider users feel interest to access or modify the data. To get access the data every user must go through the authentication and access control procedure. And the data only discloses to those users who have valid subscription to access those data.

6.1.4 Availability

Users are authenticated locally by the sensor nodes. So the authentication procedure does not take more time and the users do not need to wait longer to access the data. In this proposed protocol, the BS only involves in the system initialization phase and other two phase authentication and access control are done by the sensor nodes. So the denial of service (DoS) attack which is mainly effect on the BS will not affect into the authentication and access control. As a result the data will be available upon request from the sensor node to the user.

6.1.5 Session key agreement

After the successful authentication, the user and the sensor node computes their own session key using their common shared secret key. The session key ensures that the future communication between the user and the sensor node will be secure.

6.2 Vulnerability analysis

Wireless sensor networks are vulnerable to attacks. During the authentication and access control the network may suffer different kind of attacks. The proposed protocol are avoiding or minimizing the attacks given below.

6.2.1 Active attack

The proposed protocol is based on the identity-based signature (IBS) scheme which provides the strong authentication. The signature using IBS scheme is generated by the secret key of the signer. So it is quite impossible for any illegal users to sign or change a message sent by a valid user. If any change made by the illegal users on a valid message then the signature verification procedure must detect the modification and does not pass the verification. So attackers can never success to falsify the system.

6.2.2 Reply attack

When a user sent a message to the sensor nodes, it includes the sending timestamp with the message. After receiving the message the node can easily check whether the message is newly generated message or a replayed message. If the node identifies the message is a replayed message then the node will reject the authentication.

6.2.3 Node capture attack

In wireless sensor networks, it is very easy to take physical control over a sensor node. The elimination of this kind of attack is very difficult in WSN because the WSN deploy in such an environment where an attacker has direct physical access on the network. The proposed protocol cannot eliminate the node capture attacks completely but it can minimize the number of capture nodes. The sensor nodes in this protocol use the asymmetric key. So every node has their own key which is used to calculate the message authentication code (MAC) for a message. If an attacker gain control over a sensor node then the attacker cannot impersonate it to the other nodes. On the other hand the revocation process helps to make inactive a capture node for the future communication with others.

6.2.4 Denial of service (DoS) attack

The intruder may attack the BS by sending continuous fake requests. In the proposed protocol, the involvement of the BS is not so much into the authentication process. BS has only involved into the initialization phase otherwise the respective nodes perform all the required functionalities for the authentication and data access for a user that helps to avoid the DoS attack. User broadcast the authentication request to the sensor nodes. If a node is blocked by the attacker then other nodes will response to the user request. So the attackers cannot prevent the network to provide the service to the users.

6.3 Energy efficiency

More security requires more energy. So if we want more security then the node will decrease it energy rapidly. Cryptography operation consumes more energy. Within a network all the entities perform some kind (more or less) of cryptographic operations. WSN is a resource constraint network which has limited energy. In WSN application more cryptographic operations on sensor nodes are not suitable. The BS and user device has more energy and executing capabilities. So executions of cryptographic operations on these two devices are not a problem. In the proposed protocol, most of the cryptographic operations have performed by the BS and the user device. BS performs the cryptographic key generation and distribution for all the nodes and users. The user generates the digital signature for itself to send a signed message to the sensor nodes and also verifies the signature of the sensor node. So energy efficiency can be achieved by implementing this proposed protocol.

Every data access request does not need to go through the authentication procedure. If a user already authenticated and has a valid session with the node then the user does not wait for the authentication to get access of the data. During a valid session between a user and a sensor node, a user is authenticated only once (at the beginning of the session) to the sensor node. So the node does not need to expense extra energy to verify the signature of the user.

After successful registration of a user, BS sent the hash value of the user identity instead of the user identity itself to the sensor nodes. Sensor nodes store this value for further use. Hash value takes less memory space than the user identity and the operation performing with the identity takes more energy than the hash value. So the proposed protocol spends less energy than other existing protocols.

Sensor nodes operate into the active and idle state. In the active state they do the processing such as transmit data, receive data etc. In the idle state they save their energy. Long time in active or in idle state is not desirable. If a node is in active state for a long time then it reduce its energy very quickly. On the other hand long idle time makes the performance of the network poor though the node saves more energy. So the dealing with the active and idle state is very important to increase the life time of a sensor nodes as well as the performance of the networks [16]. The consumption of the energy in active state depends on the operations that a node performs in the state. Moreover the operations like sending data, receiving data are taking constant energy but the other operation like cryptography operation consumes more energy which also varies from application to application.

6.4 Comparison with existing protocols

The table 3 is shown in the next page, has provided a comparison study of the proposed protocol with the other related protocol found in the literature. According the comparison table, it can be said that the proposed protocol provides the mutual authentication, where the authentication in all related protocols is one-way. This protocol maintains the access control mechanism to access the data. It has session key agreement which ensure the future communication will be secure. It maintains the data confidentiality and data integrity. It does not need any prior infrastructure. IBS is used to perform the cryptography operations. It has the scalability properties which makes the proposed protocol more flexible. The target of the query is a set of sensor nodes surrounding the user. So if a node denies providing the services to the user then the user will get services from other sensor nodes without any interruption. During the analysis of this proposed protocol, I did not find any vulnerability and the main advantage of this proposed protocol is the efficiency which is mentioned in the analysis section in this chapter.

Table 3: Comparison of security properties with existing protocols.

	Benenson et al. [12]	Banerjee et al. [13]	Jiang et al. [14]	Tseng et al. [15]	Proposed protocol
Authentication	One-way	One-way	One-way	One-way	Mutual
Access control	Not maintain	Not maintain	Not maintain	Not maintain	Maintain
Session-key agreement	Not available	Not available	Not available	Not available	Available
Data Confidentiality	Not maintain	Not maintain	Not maintain	Not maintain	Maintain
Data Integrity	Not maintain	Not maintain	Not maintain	Not maintain	Maintain
Infrastructure	Public key	No	Key distribution	No	No

	infrastructure (PKI)		center (KDC)		
Cryptographic technique	PKI based on ECC	Symmetric	Self-certified key (SCK)	XOR and hash	Identity-based signature
Scalability	Yes	No	Yes	Yes	Yes
Target of the query	Single sensor node	Set of sensor nodes within the range of the user	Set of sensor nodes within the range of the user	Single sensor node	Set of sensor nodes within the range of the user
Vulnerability	Possibility of Denial of service (DoS) attack	Computation and communication overhead	Computation and communication overhead	Node synchronization required	None found
Main advantage	Avoidance of Node capture attack	Avoidance of Node capture attack	Avoidance of Node capture attack	Efficiency	Efficiency

7. CONCLUSION

The main contribution of this research is the user authentication and access control in wireless sensor networks. In the authentication part, only the registered users are authenticated by the sensor nodes. On the other hand all authenticated user does not have the same access right on the sensor data. The access control part makes the decision that which user will get what kind of access on the data. So a user without a valid identity will not be authenticated and also an authenticated user will not get the requested access without having the proper access right. An identity-based signature (IBS) has been used in this authentication and access control protocol. When a user is authenticated by a sensor node, the user and the sensor node both computes their session keys to secure their future communication. The evaluation through the simulation of the proposed protocol ensures that the protocol is energy efficient and secure. The other advantage of this proposed protocol is the reusability of the IBS. When a new improved and more secure IBS scheme will available, the new IBS scheme can easily substitute the old IBS scheme which makes better performance and security of the proposed protocol.

The WSN run by the power of the battery (AA type). As security was the main concern to the design of this protocol, and if we demand more security then it takes more power which lead to limit the battery life of the sensor nodes. So it is important to balance the security with the power that the network runs longer without any power failure.

The main parts of the proposed protocol have been simulated and presented into the results section in this paper which assures that the protocol would be possible in its practical environment. So our future works would be standardize all the module for future implementation and also implement in the real environment to observe the real impact in terms of security, energy consumption, efficiency, durability etc.

REFERENCES

[1] Rehana Yasmin, Eike Ritter, and Guilin Wang (July 2010), An Authentication Framework forWireless Sensor Networks using Identity-Based Signatures, 10th International Conference on Computer and Information Technology (CIT).

[2] X. Cao, W. Kou, L. Dang, and B. Zhao (2008), IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks, Computer Communications 31(4), pp 659 – 667.

[3] D. Liu and P. Ning (2004), Multilevel mTESLA: Broadcast authentication for distributed sensor networks, ACM Trans. Embed. Comput. Syst. 3(4), pp 800–836.

[4] Hu Jin, He Debiao and Chen Jianhua (2010), An Identity Based Digital Signature from ECDSA, Second International Workshop on Education Technology and Computer Science (ETCS), pp 627 - 630.

[5] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz (2004), Comparing

Elliptic Curve Cryptography and RSA on 8-bit CPUs, CHES, pp 119–132.

[6] M. Choudary Gorantla, Colin Boyd, and Juan Manuel Gonz_alez Nieto (2008), ID- based One-pass Authenticated Key Establishment, AISC.

[7] Wei Ren, Kui Ren, Wenjing Lou and Yanchao Zhang (2008), Efficient User Revocation for Privacy-aware PKI, 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness.

[8] Wei Dai (September 2010), Crypto++ Library 5.6.1, Ibiblio-The Public's Library and Digital Archive

[9] Erik Eliasson (May 2006), Secure Internet Telephony: Design, Implementation, and Performance Measurements, TRITA-ICT/ECS AVH 06:04

[10] A. Molana, A. Vina, and R. Juanes (1994), An open Posix.4 based architecture for real time intelligent control, Second international IEEE conference on intelligent systems engineering, pp 378-388.

[11] M. Halil-Hani, V. P. Nambiar, M. N. Marsono (2010), Hardware acceleration of OpenSSL cryptography functions for high-performance internet security, International IEEE conference on intelligent systems, modelling and simulation (ISMS), pp 374-379.

[12] Z. Benenson, F. Gartner and D. Kesdogan (2004), User authentication in sensor networks

[13] S. BaneIjee and D. Mukhopadhyay (2006), Symmetric key based authentication querying in wireless sensor networks, First international conference on Integrated internet ad hoc and sensor networks.

[14] C. Jiang, B. Li and H. Xu (2007), An efficient scheme for user authentication in wireless sensor networks, 21st

International Conference on Advanced Information Networking and Applications Workshops, pp 438 - 442.

[15] H.-R. Tseng, R.H. Jan and W. Yang (2007), An improved dynamic user authentication scheme for wireless sensor networks, Global Telecommunications Conference, pp 986 - 990

[16] Nikolaos A.Pantazis, Dimitrios J. Vergados, Dimitrios D. Vergados and Christos Douligeris (March 2009), Energy efficiency in wireless sensor networks using sleep mode TDMA scheduling, Elsevier Science Publishers B. V.