Secure Authentication Framework in Wireless Sensor Networks

Rumana Akhtar
Part-time faculty
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology,
Dhaka, Bangladesh

Abdullah Al-Mahmud
Assistant Professor,
Department of Computer Science and Engineering
Ahsanullah University of Science and Technology,
Dhaka, Bangladesh

ABSTRACT
The nodes in the wireless sensor networks collect data from their environment. Sometimes these data are valuable for the networks and also confidential. So it is important to prevent unauthorized access of those data. The preventive measure can be done through the authentication. In this paper, we propose an authentication framework that authenticates both the users of the network and sensor nodes based on the Identity-Based Signature (IBS) scheme. IBS uses the ECC (Elliptic Curve Cryptography) based digital signature algorithm (DSA) to sign a message and verify the signature on a message for a wireless sensor networks. This authentication framework register a new user and sensor node, authenticate a user and sensor node, and finally establishes a session key between sensor nodes and between sensor node and the user depends on the authenticating parties. Node and user revocation is handled in this authentication framework. Finally we made a comparison with other existing security solutions in wireless sensor networks and able to make a conclusion that the protocol provides confidentiality and integrity of the 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, ECC, Authentication, IBS.

1. INTRODUCTION
The sensor nodes in the WSN 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 or users in the network over the wireless connection medium. The collected data is valuable for the network. In some case the data are confidential and are only visible to those nodes or users who have proper subscription on the data. So the security in sensor networks is a vital issue to protect the data. In WSN different applications require different security solution. In some applications, some outsider entity may feel interest to get access the data and also modify the data. If they success to gain access the data as well as modify the data then the integrity and confidentiality of the data will be violated. So it is important to protect sensor data from any sort of unauthorized access. So a secure authentication framework is important to protect the data from unauthorized access as well as to maintain the data confidentiality, data integrity and access control of data.

The authentication in WSN can be divided into three categories [1] - base station authentication, sensor node authentication and user authentication. The base station authentication is similar as the traditional network authentication system. One base station is authenticated by other base stations in the network to make their communication secure. There are many research already been done in this context of the base station authentication [1, 3]. Sensor node authentication can be done by other sensor nodes, base station or both. On the other hand the users in the wireless sensor network are authenticated by the sensor nodes or the base station. Actually the process of the authentication of users or nodes depends on the designed protocol.

Generally a system requires to perform three important functions for the whole authentication process such as registration, authentication, and session key establishment; to provide the access on data [1]. The authentication ensures that the only authorize user can get access on the data. After an authentication, session key is established to make their future communication more secure. The user in the wireless sensor networks may uses their mobile device like PDA to connect with the network.

In general, the authentication process can be done in two ways [1] - centralized and distributed authentication. In centralized authentication system, all the entity will be 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 framework 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 a secure and efficient identity-based authentication framework that authenticates both the sensor nodes and users in wireless sensor network. This authentication process helps to protect the data of a sensor node from illegitimate access, overcome the existing problems in authentication of sensor networks and also preserve the security issues of the nodes.

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 ***ó*** of the entity i on the message ***m***.

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

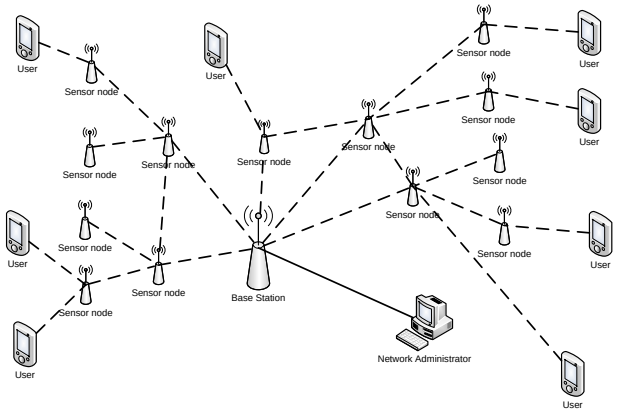

Figure 1: A typical network architecture for the proposed protocol.

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 an user A
SIDA	Identity of a sensor node 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/sensor node A
ó	Signature of the user/sensor node
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 $\boldsymbol{DID_i}$ of all users i. All users i store their identity ***UIDi,*** private key $\boldsymbol{DID_i}$ and system parameter ***P*** before their deployment.
4. BS registers all valid sensor nodes and uses its private key ***SKPKG*** to generate the private key $\boldsymbol{DID_i}$ 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). On the other hand when a sensor node *A* register with the BS. BS keeps its' record by storing the dataset (***SIDA***, ***TS).*** The BS broadcast the data set that contains the registration information of the node A, immediately after the registration. Here the BS send the dataset like (***H1(SIDA), TS***). Hash value of node identity or user identity is used to reduce the memory requirement of the sensor node. Nodes which are deployed already in the network get only the updated registration information of nodes from the BS. Upon receiving the broadcast information from the BS, all nodes will send acknowledgement using their own identity to the BS. [8] If any node does not receive the broadcast message, it will keep silent. When the base station knows about the lost message, it immediately resends the message again. The broadcast message contains the sending timestamp of BS. So a receiving node can identify the message whether it is a resent message or new message. As a result only those nodes will update their database who did not received the message before. BS only responsible to generate the private key of the nodes or users but base station never stores the secret key of users or nodes to own.

4.2 Authentication

In this section we present the authentication framework that includes the sensor node authentication and user authentication.

4.2.1 Sensor node authentication

At first a sensor node downloads its own identity through a secure channel from the network administrator then the node is registered by the BS. After a successful registration of a sensor node, now the node needs to be authenticated by other nodes or BS. The authentication is necessary to make further communication (request to access some data, send an emergency report etc.) within the network. After completion of the successful authentication procedure, the both parties will generate their session key. The generation process of the session key has described in the following part of this protocol. The step by step authentication procedure is given below. Here sensor node A send authentication request and sensor node B or the BS authenticates the node A.

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

Step 2. Sensor node A sign an authentication request message R which include **TS**, ***TK*** and ***SIDA;*** and sends it to the sensor nodes surrounding the node for the authentication. The node 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. Upon sending the authentication request message R, the nodes or BS surrounding of the requesting node A will receive and response after some verifications on the receiving message.

a. The receiving node or BS first check its registration list to make sure that the node is already registered.
b. If the node is already registered then it checks whether the receiving authentication message is replayed message or fresh message. The received message has the sending timestamp TS. This timestamp is compared with the current timestamp. If the difference between current timestamp TC and sending timestamp TS is greater than the maximum communication delay $\boldsymbol{\Delta T}$ then the received message is a replayed message (authentication request will be rejected) otherwise go to the next step for further verification.
c. The node or BS now verify the received signature S of the node A by the signature verification algorithm of IBS. If the signature verification is unsuccessful then the authentication will be rejected otherwise go to the next step.

Step 4. To mutually authenticated by each other the receiving node or BS now sends its own signature message that include the identity of the node SIDB or BS and sending timestamp TS to the sensor node A.

Step 5. The sensor node A now do same verification in step 3.

a. The node A first check its registration list to make sure that the node sent the signed message is already registered.
b. If the node is already registered then it checks whether the receiving signed message is replayed message or fresh message. The received message has the sending timestamp TS. This timestamp is compared with the current timestamp. If the difference between current timestamp TC and sending timestamp TS is greater than the maximum communication delay $\boldsymbol{\Delta T}$ then the received signed message is a replayed message (mutual authentication will not successful) otherwise go to the next step for further verification.
c. The node A now verify the received signature S of the node B or BS by the signature verification algorithm of IBS. If the signature verification is successfully pass then the node A computes the shared common secret $\boldsymbol{K_{AB}}$ using the algorithm ID-based One-pass Authenticated Key Establishment described in [6] and sends it to the node B.

Step 6. After receiving the common share secret from node A, sensor node B also computes the common shared secret $\boldsymbol{K_{BA}}$ using the same algorithm. If the $\boldsymbol{K_{AB} = K_{BA}}$ 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.

4.2.2 User authentication

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.

4.2.3 User 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.

4.3 Update of the network information

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

4.4 User or node revocation

The node or 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]. There are different ways to revoke an entity from the networks.

Sensor node may be compromised due to the physical access on the node, key discloser etc. Here neighbor-ship based detection [2] algorithm is used to detect a compromised node. Nodes in the network are placed in such a way that the signal power level within any two neighbor will keep in a certain limit. This power level is used to detect a compromised node. All nodes periodically monitor their neighbor about their proper existence in the network. When a node try to monitor another node, it asks its' neighbor node about the existence in the network and

the monitee node replay that he is alive. Now the receiving node checks the power level of the received signal. If the power level exceeds the max threshold of power or goes beyond a minimum threshold of power then the receiving node suspects that the node has been compromised and immediately informs the BS about that compromised node. Now the BS will verify the information about that compromised node. If the node is really compromised then BS places that node in the list of the compromised node and immediately broadcast the information of compromised node in the network. All the entities in the network make update their list of compromised nodes. If a compromised node make a request to the network, the entity can easily verify whether the node is compromised or not by checking the list of compromised nodes. If the node is compromised then the entity rejects the request of that node.

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.

Every entity in the network has its own access time, which is defined by the BS during the time of registration. When the BS computes the secret key of that entity, it uses the expiration of access time of the entity as a parameter. So after the expiration, the secret key will not be valid and if the node or user places a signed request to other then the receiving node will verify the signature and the signature verification will not pass as its access time has been expired. As a result it is not possible for any entity to be authenticated for the communication after its expiration.

5. 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.

5.1 Security Analysis

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

5.1.1 Mutual authentication

The proposed protocol authenticates only those users or nodes that have a valid secret key. All the authenticating parties (user-node or node -node) are mutually authenticated by each other through the signature verification process. Sensor node or user in the network gets their secret key from the PKG by showing its identity which is given by the administrator. User or node with a valid secret key can sign a message and send the message with its signature to other nodes for authentication and the receiving node verifies the signature of the requesting user or node. If the signature is valid then the node also sends its' own identity to the requesting entity for authentication. The requesting entity now 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 or sensor node. So the both communicating parties are confirmed about the accuracy of the received data.

5.1.2 Integrity

Integrity of the message can be ensured by verifying the signature. When a sensor node or user sent a message, it includes the signature of its own 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 sending entity.

5.1.3 Confidentiality

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

5.1.4 Availability

Users or sensor nodes are authenticated locally by the sensor nodes. So the authentication procedure does not take more time and the requesting user or node does 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 procedure. As a result the data will be available upon request from the sensor node.

5.1.5 Session key agreement

After the successful authentication, both communicating parties compute their own session key using their common shared secret key. This session key ensures that the future communication between those parties will be secure.

5.2 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.

5.2.1 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 user or node to sign or make any change on a message sent by a valid user or node. If any change made by any illegal entity 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.

5.2.2 Reply attack

The authentication request message includes the sending timestamp of the sender. 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.

5.2.3 Node capture attack

In wireless sensor networks, it is very easy to take physical control over a sensor node or a user. 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 its 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.

5.2.4 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 a sensor node that helps to avoid the DoS attack. Requesting entity broadcast the authentication request to the network. If a node is blocked by an attacker then other nodes will response to the authentication request. So the attackers cannot prevent the network to provide the service.

5.3 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 or node already authenticated and has a valid session with the node then the node or user does not wait for the authentication to get access of the data. During a valid session between a user and a sensor node or a sensor node and a sensor node, a user or node 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 other parties.

Register user or sensor node list contain the hash identity of the registered user or node other than the identity itself. The storage requirement of the hashed identity requires less memory than the original identity and the operation that perform on the hash value require less energy than on the original identity of the node or user. So the proposed authentication protocol expenses less energy to do the manipulation with the identity.

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 [9]. 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.

5.4 Comparison with existing protocols

The table 2 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 2: Comparison of security properties with existing protocols.

	Benenson et al. [12]	Banerjee et al. [13]	Jiang et al. [14]	Roberto et al. [11]	Tseng et al. [10]	Proposed protocol
Authentication	One-way	One-way	One-way	One-way	One-way	Mutual
Access control	Not maintain	Not maintain	Not maintain	Not available	Not maintain	Maintain
Session-key agreement	Not available	Not available	Not available	Not available	Not available	Available
Data Confidentiality	Not maintain	Not maintain	Not maintain	Not maintain	Not maintain	Maintain
Data Integrity	Not maintain	Not maintain	Not maintain	Not maintain	Not maintain	Maintain

Infrastructure	Public key infrastructure (PKI)	No	Key distribution center (KDC)	No	No	No
Cryptographic technique	PKI based on ECC	Symmetric	Self-certified key (SCK)	Symmetric	XOR and hash	Identity-based signature
Scalability	Yes	No	Yes	No	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	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	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	Avoidance of Node capture attack	Efficiency	Efficiency

6. CONCLUSION

The main contribution of this research is to provide an authentication framework for the sensor nodes and the user in wireless sensor networks. Through the authentication only the registered users or sensor nodes are authenticated and get access the data from the network. So any entity who does not have valid identity will not be authenticated or not able to falsify the system. An identity-based signature (IBS) has been used in this authentication procedure. After a successful authentication both the user and node or node and node compute their own session keys to secure their future communication.

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 proposed authentication framework is analyzed through the theoretical analysis. This protocol also compares with some other existing protocol and is found that our proposed protocol is better than others based on different security parameters like security, energy consumption, efficiency, durability etc.. We have plan in future to justify our findings in the practical environment.

7. 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] Hui Song, Liang Xie, Sencun Zhu and Guohong Cao (2007), "Sensor Node Compromise Detection: The Location Perspective" IWCMC '07 Proceedings of the 2007 international conference on Wireless communications and mobile computing.

[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] M. Durvy, C. Fragouli and P. Thiran (2007),"Towards Reliable Broadcasting using ACKs", Information Theory, 2007. ISIT 2007. IEEE International Symposium, page 1156 – 1160

[9] 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.

[10] 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

[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.