Secure Sensor Node Authentication in Wireless Sensor Networks

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

Rumana Akhtar
Masters Student, ICT,
The Royal Institute of Technology(KTH),
Stockholm, Sweden

ABSTRACT
Wireless sensor networks are usually installed in rough environments and sometime when the traditional network fails to deploy on that environments. The nodes in the network collect data and information from its environment. These data are moves from one node to another. All the data are not publicly accessible; some of them contain confidential and valuable information which only be accessible through a proper secure mechanism between two communicating parties. A secure authentication scheme can solve this problem to access the confidential data and protect the unauthorized access. In this research paper, we propose a secure sensor node authentication protocol. The protocol uses an identity-based signature (IBS) algorithm where Elliptic Curve Cryptography (ECC) based the digital signature algorithm (DSA) is used to generate a signature on a message and verify a signature on the message within the network. The successful authentication process in this protocol consists a new node registration, node authentication and finally a session key establish between two parties that make their future communication secure. In the WSN, the sensor nodes are installed in a place where the intruder may easily get access on the node. So a compromised node revocation is also an important issue which is handled in this protocol. To provide the proper security metric, the protocol also analyzed through some conventional security solutions. The protocol ensures the confidentiality and the integrity of the data, provides improved communicational and computational performance and also achieves the energy efficiency due to the usage of more efficient ECC based DSA algorithm than RSA.

KEYWORDS: WSN, Sensor node, Security, Authentication, DSA, IBS, ECC.

1. INTRODUCTION
Sensor nodes are spatially distributed to sense and monitor the physical changes throughout the environment to collect the data. The nodes also collect data from its surrounding nodes and the environments. These collected data are transmitted from one node to other through the wireless medium. Sometimes nodes are requested data from other nodes, in some cases the collected data of a node may be confidential and only visible to the authenticated nodes. Different application required different security requirements. Some time, the unauthenticated nodes in the network or outsider nodes may feel interest on the data collected by a sensor node. If that entity capable to gain access the data and be able to alter the data then the data integrity could be violated. So it is more important to stop the unauthorized access of data. In other way all the authenticated nodes do not have same right to access the data from a node. Every node may have their own security privileges that they can apply to gain access of data. Sometime it is important to hide some data from some group of the nodes in the network. So a secure node authentication protocol is important to ensure data confidentiality, integrity and also the access control on the data.

Mainly the authentication of WSN can be divided into two categories [3] - base station authentication and sensor node authentication. Besides of these two categories there is another authentication mechanism which is used in the WSN for user authentication. The principle of the base station authentication is similar as the traditional network authentication solution. 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 [3, 12]. Sensor node authentication can be done by other nodes, base station or both. How the node will be authenticated, it depends on the designed protocol.

Sensor nodes in the network are collecting data from their environment. Some time the data may be confidential. So the request and access on those data can only be done by the authenticated nodes. The authentication of sensor nodes can be done in two ways - using distributed authentication system or centralized authentication system. A centralized authentication system authenticates a node by the central entity (base station) of the network. As the base station is more powerful entity having capability to do the complex operations, so it is much easier and simpler to implement. But this system has some drawbacks. First of all it has the single-point of failure which leads to malfunction the network completely if the base station fails. Secondly the nodes surrounding the base station will be more busy to send authentication requests of nodes to the base station and their response to the node as a result these nodes will lose their power quickly. Thirdly the base station may suffer DoS (Denial of service) attack that also makes a problem in the operation of the network. In distributed authentication system, the node will be authenticated by the surrounding nodes. This system makes less traffic congestion and also reduce the communication overhead of the network.

The goal of this research is to propose an efficient secure sensor nodes authentication protocol in wireless sensor networks that provide the proper protection on data from unauthorized access and also overcome the existing problems in the node authentication of the sensor networks. Finally the proposed node authentication protocol will be analyzed through the theoretical analysis and also compare it with the existing protocols.

2. CRYPTOGRAPHY PRIMITIVES
Identity-Based Signature (IBS) [2] algorithm is used in this proposed protocol. IBS scheme uses ECC (Elliptic Curve Cryptography) which is based on DSA (Digital Signature Algorithm) to sign a message and verify the signature in the message. There are many RSA based IBS scheme are available

but the main problem in these IBS scheme is the size of the signature. Signature based on RSA is comparatively larger that increase the size of the message. On the other hand the RSA signature verification is more efficient than ECC [13]. As the WSN is resource constraint network so it is desirable the size of message becomes smaller. For this reason ECC is good choice to sign a message and verify the signature on the message.

In this proposed protocol the base station of the network acts as a PKG (Private Key Generator). IBS algorithm is a set of four different algorithms such as system setup, key extraction, signature generation and signature verification [1, 2]. A short description of these four algorithms is given below.

System setup: Master entity (Base station) uses this algorithm. The input of this algorithm is a security parameter ***k*** and the outputs are public system parameters ***P*** and a master secret key ***SKPKG***. The BS keeps the master secret key ***SKPKG*** to itself and distributes the public system parameter ***P*** to all.

Key Extraction: This algorithm is run by the BS to generate the secret key of the sensor nodes. The inputs of this algorithm are the public system parameter ***P***, a master secret key ***SKPKG*** of the BS and the identity of sensor node (***SIDA*** for node A). The output is the secret key of the sensor node ***DIDA*** (secret key for sensor node with id ***SIDA***). The BS then transfers the secret key of the sensor node to the node through a secure channel.

Signature generation: This algorithm is used to generate the signature of the message. The inputs of this algorithm are a message ***m*** which is to be sign and the private key of the node *A* ***DIDA*** who will sign the message. The output of this algorithm is a signature ***S*** on the message ***m*** of the node *A*.

Signature verification: This algorithm is used to verify the signature on the message. The inputs of this algorithm are the message ***m***, a signature ***S*** of the message, identity of the sensor node and the public system parameters ***P***. The output of this algorithm is accepted or rejected. If the signature ***S*** on the message ***m*** for the sensor node is valid then the output will be accepted and rejected otherwise.

3. ASSUMPTION

This research has presented a secure sensor node authentication in wireless sensor network. Here a wireless sensor network consisting an administrator, one or more BS, a large number of nodes, and many users, are considered. The administrator of the network plays some important roles within the network such as – preload the identity of the nodes. The administrator and base station are directly connected with each other. In any change in the network the administrator always inform the update to the base station. The base station (BS) acts as a Private Key Generator (PKG). PKG is responsible to generate the private key for all the nodes and the users in the network. The sensor node are authenticated by other sensor nodes surrounding of it and then can access the data from the network.

The architecture of the network for the proposed secure authentication protocol is shown in the figure below. The architecture is based on the hybrid network topology. Here the users are connected with the sensor nodes, the sensor nodes are connected with other sensor nodes or with the base station, the base station of this network is connected with other base stations via wired communication medium. Wireless communication medium is used to connect the users, sensor nodes and base station in the network. Wired medium is used to connect the network administrator with the base station.

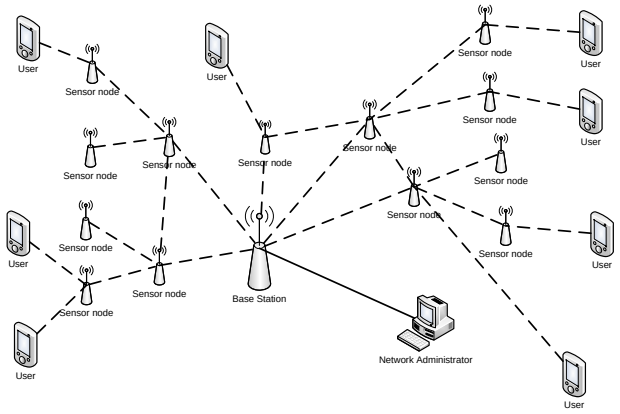

Figure 1: A typical network architecture for the proposed protocol.

4. PROPOSED PROTOCOL

The proposed authentication protocol use some symbols. The meaning of these symbols used in this chapter is given in the following table.

Table 1: Description of different symbols used in this proposed protocol.

Symbol	Meaning
SIDA	Identity of sensor node A
DID_A	Secret key of sensor node A
UIDA	Identity of user A
UPKA	Private Key of user A
R	Authentication request message
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 PKG (base station)
m	Message
BSPK	Public key of the BS
P	Public system parameters
S	Signature of the user
TS	Sending time stamp
TC	Current time stamp
K_{AB}	Common shared secret between node A and B on node A
TK	Ephemeral key
ΔT	Maximum communication delay
SK	Session key
χ	Key derivation function

The proposed secure sensor node authentication protocol in WSNs is working in three different steps which have been presented in this section below.

4.1 System initialization

Base station acts as a private key generator. During this phase the base station start-up then initializes all of its parameters, register all sensor nodes and the users, and inform the network about the registration of the new nodes or users by broadcasting

a list of registered users or nodes to the network. The step by step functions that performed by the BS are following-

1. Base station (BS) generates its' own private (***SKPKG***) and public key (***PKPKG***).
2. BS now sets the public system parameter ***P*** which also consists its' own public key ***PKPKG.***
3. BS registers all valid nodes. As BS is the private key generator, so it generates the private key of the nodes (private key DID_i for node i). The sensor nodes then stores their own identity ***SIDi*** along with their private key ***DIDi,*** and public system parameter ***P*** into their own memory before the deployment of the nodes in the network.
4. BS also registers all valid users and generates their private keys (private key UPK_i for user i). The user then stores their own identity ***UIDi*** along with their private key UPK_i, and public system parameter ***P*** into their own memory before the deployment of the nodes in the network.
5. 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 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. [7] If any node does not receive the broadcast message, it will keep silent. When the base station knows about the lost message, it immediately resend 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 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 is needed to be authenticated by other nodes or BS. The authentication is necessary to make further communication (request to access some data, send a 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. The sensor node A generates an authentication request message R and signs it using the signature generation algorithm of the IBS. The node A now send this authentication request message along with the signature S, its own identity SID_A, and the time stamp TS. The time stamp TS is the sending time stamp that ensure to avoid the reply attack.

Step 2. 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 ΔT 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 3. 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 4. The sensor node A now do same verification in step 2.

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 ΔT 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 unsuccessful then the authentication will be rejected otherwise authentication successfully completed.

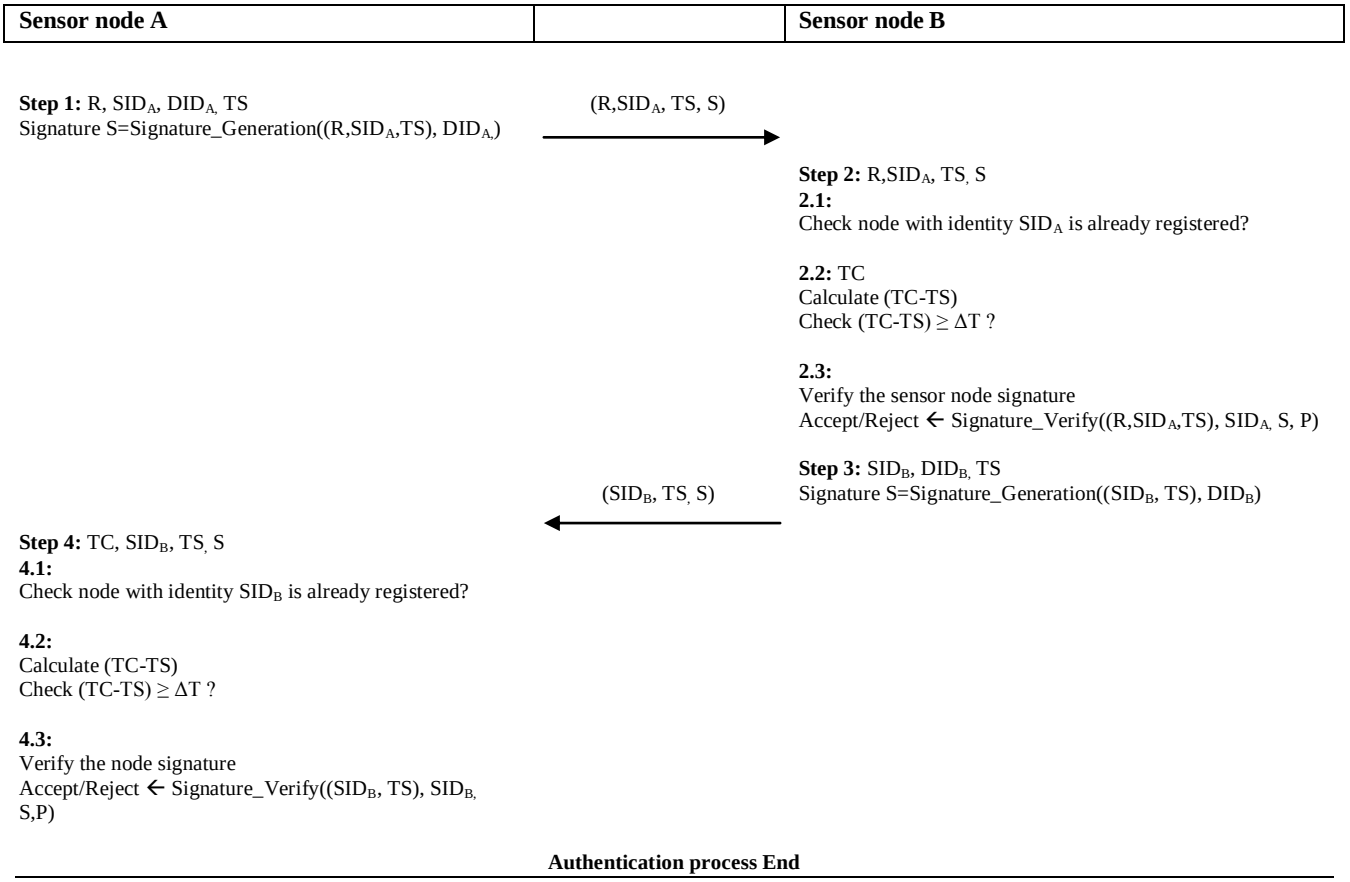

Figure 2: Authentication process of sensor node A with node B.

4.3 Session key establishment

The sensor node is authenticated by other sensor node or the BS. They are now capable to communicate with each other. For making their future communication more secure, need to establish the session key between them. In this context the key management protocol plays important role to secure exchange of the session key between these two communicating parties. This authentication protocol uses the one-pass key establishment [5] to establish the session key. The process of the session key establishment is given below. .

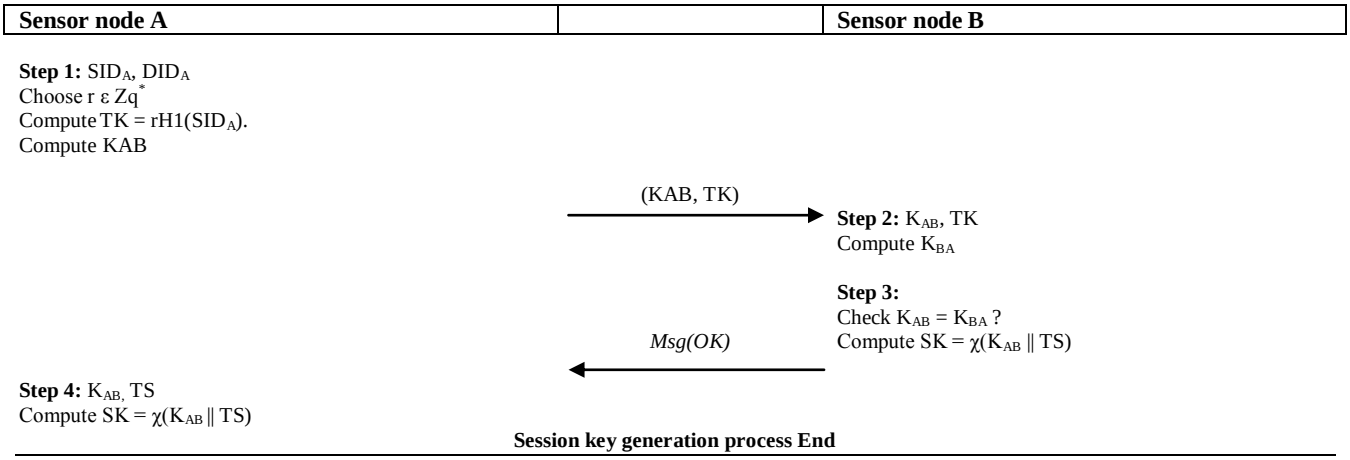

Figure 3: Session Key establishment process between nodes A and B.

Step 1. Sensor node **A** select a random number **r ε Zq*** then the node will generate a temporary key ***TK*** as ***TK*** = ***rH1***(***SIDA***). The node now generate a common share secret K_{AB} using the One-pass Authenticated Key Establishment algorithm described in [5] and then send K_{AB} and TK to the sensor node B or BS.

Step 2. Receiving entity sensor node B or BS also generates the common share secret K_{BA} and check whether K_{AB} and K_{BA} is equal or not.

Step 3. If equal then the node B computes it's session key $SK = \chi(K_{AB} || TS)$ using the key derivation function χ. TS is the current timestamp of the sensor node B or BS. Sensor node **B** or **BS** send a OK message to the node **A** to confirm the common shared secret key and session key has been computed.

Step 4. Sensor node **A** now compute its own session key using the same key derivation function. The session key ***SK*** between both communicating parties is ready to encrypt all future message

4.4 Update of the node information

BS always gives the up-to-date information to the network. When a new node registered into the BS, the BS immediately sends the information about the registration of that node to the network and all of the entities updated their list of registered nodes. BS informs the network immediately because when a sensor node registers with the BS, it might be try to communicate with the network by sending the authentication request. To make the authentication successful the authenticating entity must need the registration information of that node before the authentication. The BS also keep a compromised nodes list. When a node compromised and BS gets this information from the network, it immediately puts the node into the compromised nodes list and then passes the list into the network which ensures the proper security of the network.

4.5 Sensor node revocation

A sensor node may be revoked due to some predicted or unpredicted reasons. Some of them are violation of network access policy, discloser of the private key, expiration of the subscription etc.[6] This proposed protocol has considered two different reasons to revoke a sensor node from the network.

Sensor node may be compromised due to the physical access on the node, key discloser etc. Here neighborship-based detection [8] 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 entire 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.

During the time of registration, BS defined the expiration time of a node. So, all of the entities within the network have their own expiration time of access. When the base station generates the private key of a node it uses the access time duration of the node as a parameter. So if the private key of a node expire then the signature verification will not pass the request.

5. ANALYSIS OF THE PROTOCOL

The analysis of the proposed protocol is carried out based on two main terms - security and efficiency. Security and efficiency is opposite from each other. If we are thinking about the better security then we cannot guarantee the proper level of efficiency and vice versa. So it is more important to equalize these two terms using some kinds of agreement.

5.1 Security Analysis

In every research the analysis on security is an important part. This proposed protocol has also been analyzed to achieve the proper level of security. The achieved securities in this proposed protocol according to some fundamental terms of security are given below.

5.1.1 Mutual authentication

Considering the proposed authentication protocol, two authenticating parties are authenticated mutually by each other where the nodes confirm the authentication through their signature verification process. Here the nodes are authenticated only if the node has a valid private key. All the sensor nodes and users get their private key from the base station (PKG) by presenting their own identity which they get from the administrator. A sensor node having a valid private key is able to sign a message. The node then sends the message along with the signature to the other sensor nodes for authentication. The receiving node verifies the signature through the signature verification process. If the verification process passes then the receiving node will send its own identity along with the signature to the sending node. Sending node now do the same as the receiving node that means it also verify the receiving node's signature through the signature verification process. If verification process passes then it ensures that both parties know each other. Mutual authentication does not permit of impersonating the nodes to send false data to the others. So the both communicating parties are well known about the correctness of the received data.

5.1.2 Integrity

The message integrity is ensured through the verification process of the signature. The communicating parties send their message along with their signature on the message. If a message altered during the transmission then the signature verification process never pass. As a result, the receiving node can easily make a decision whether a message violate its' integrity or not.

5.1.3 Confidentiality

The sensor nodes are collecting data. All data are not publicly accessible by others. Some of them are confidential. To access those data, all the entities need to go through the authentication process to verify its' identity to access the data. Confidential data never disclose to others without proper authentication on other word the data only disclose to those entities who have valid permission to access the data.

5.1.4 Availability

Distributed mechanism is applied to do the authentication where the nodes are authenticated by other node locally. Local authentication does not take more time and the requesting entities do not need to wait for a long time to get access on the data. In this authentication protocol base station does not mostly involve in the authentication process. The nodes which are very near to the BS may be authenticated by the BS otherwise the nodes are authenticated by the other surrounding nodes. Mainly the sensor node is authenticated by other surrounding sensor nodes so the DoS attack will not effect on the node authentication process. So the requesting data will be available sooner to the node.

5.1.5 Session key agreement

Session key agreement ensures that the future communication between two communicating parties will be more secure. In this proposed authentication protocol, after a successful authentication both parties compute their own session key for future use by using their own shared secret key.

5.2 Vulnerability analysis

Wireless networks specially the wireless sensor networks are vulnerable to different types of attacks. During the process of authentication this networks may undergo through the various types of attacks. All of the attacks are not avoidable. The attacks that are not avoidable are minimized in the proposed protocol. Some of the attacks that may be suffered by the sensor networks during the authentication are given below.

5.2.1 Active attack

Identity-based signature (IBS) algorithm is used in this proposed authentication protocol that ensures the strong authentication. The signature generation algorithm in IBS generates the signature of signer using his own private key. Private key always kept by own. So it is quite impossible for any illegitimate entity (hacker) to generate a signature for a valid node or make any changes on the message sent by a valid node. If any changes made by an illegal entity then it must be detected through the signature verification procedure of IBS. IBS never passes any alteration on message made by illegal entity. As a result an attacker will never successful to make the system fool.

5.2.2 Reply attack

All the messages send between the communication parties include a sending timestamp on the message. The benefit to add a sending timestamp on message is to find out whether the receiving message is fresh or a replayed message. When a receiving node receives a message, it compares the sending timestamp of the message with the receiving timestamp. If the difference between these two timestamps greater than the maximum communication delay then the message is replayed message and the authentication process will be terminated. So the replay attack cannot be able falsify the system.

5.2.3 Node capture attack

Wireless sensor networks install in such an environment where it is very easy for an attacker to take physical control on a node over the network. So the network may suffer to the node capture attack which is very difficult to eliminate. But it is possible to minimize this kind of attack. The proposed authentication protocol does also not be able to eliminate completely this kind of attack but the protocol is able to minimize this attack. In this protocol, all nodes are placed in a designated position in such a way that the signal power level within any two neighbor will keep in a certain limit. If it is not maintained then it can be suspected that the node has been captured and compromised. This protocol also used asymmetric key algorithm where every individual node has its own private key. This private key is used to generate the message authentication code (MAC) on their message. One other benefit of using asymmetric key is - if an attacker is able to take the control of a sensor node then the attacker cannot be able to imitate the attack to other nodes in the network. Node revocation also used to stop function the compromised node. So the captured node will be inactive to communicate with others in future.

5.2.4 Denial of service (DoS) attack

Mostly the denial of service (DoS) attack occurs in wireless networks when an attacker succeeds to make the BS busy by sending continuous false request. In this proposed protocol, the BS does not involve more in the authentication process. Most of the time node authentication is done by the other nodes surrounding of that node. BS is involved in the first step (initialization) of the authentication and all other steps are done by the sensor nodes. When a sensor node broadcasts an authentication request to the network, any nodes surrounding that node may response for the request. So if the attacker blocked a node, it does not make any problem in the authentication process because other nodes may response the authentication request. So the attacker does not able to block the network by blocking the BS or other nodes. As a result DoS attack never succeeds in this protocol.

5.3 Energy efficiency

Energy and security is related to each other. More security requirements required more energy that means if we want to provide more security the nodes in the network will reduce their energy rapidly. The authentication procedure requires cryptography operations which require more energy to perform. All the entities within the network require more or less performing cryptography operations. As WSN is a resource constraint network having limited energy, so the optimum use of energy is an important issue in this network. In this proposed most of the cryptograph operations which require more energy is performed by the BS. BS generates the private keys that use in the cryptography operation in a node and distributes all the keys to the nodes for their future use. The nodes are only singing the message and verifying the signature. So it can be said that the energy efficiency might be possible to achieved through the implementation of this protocol.

After a successful authentication the both nodes generates their own session key for future use. During a valid session a node does not need to do the authentication in every step to access the data from the network. Authentication only require once prior to generate the session key. So the communicating nodes do not need to loss their energy by verifying the signature every time.

When a user registered with the BS, it broadcast the hash value of the nodes identity to the network instead of broadcasting the identity of the node 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. So the proposed authentication protocol expenses less energy than other existing authentication protocols.

The sensor nodes in the network operate into two states- active and idle. The nodes perform various types of operations such as data transmission, data receiving etc. in the active state. Whereas the node goes sleep in the idle state and save their energy. Both the states are required equally in a node to do the proper functioning of the network. But it is not desirable to stay for long time in idle or in active state. The requirement of energy in active state is more because of performing different function including cryptography operations. On the other hand the nodes in the idle state save their energy but long time in idle state lead to decrease the performance of the network. So it is very important to deal these two states properly to ensure the good performance of the network [4]. Cryptography operations require more energy but the requirement of this kind of operation varies application to application.

5.4 Comparison with existing protocols

The table (Table 2) shown in the next page describes a comparison study of the proposed protocol with the existing protocol. The comparison is based on the different security and performance metrics. The proposed protocol provides mutual authentication. It has the session key agreement. This protocol maintains the data confidentiality and integrity in the network and there is no need of any prior infrastructure. Identity-based signature (IBS) algorithm is used to do the cryptography operations. The protocol does not restrict the network in size, it is easily expandable. The target of the authentication request message is a set of nodes surrounding of the requesting node. During the analysis, there is no vulnerability is found in this protocol. And finally the main advantage of this protocol is the efficiency.

Table 2: Comparison of security properties with existing protocols.

Item	Banerjee et al. [11]	Jiang et al. [9]	Tseng et al.[10]	Proposed protocol
Authentication	One-way	One-way	One-way	Mutual
Session-key agreement	Not available	Not available	Not available	Available
Data Confidentiality	Not maintain	Not maintain	Not maintain	Maintain
Data Integrity	Not maintain	Not maintain	Not maintain	Maintain
Infrastructure	No	Key distribution center (KDC)	No	No
Cryptographic technique	Symmetric	Self-certified key (SCK)	XOR and hash	Identity-based signature
Scalability	No	Yes	Yes	Yes
Target of the query	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 node
Vulnerability	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	Efficiency	Efficiency

6. CONCLUSION

The main purpose of this research is to propose a secure sensor node authentication protocol for wireless sensor networks. The architecture of the proposed protocol consist a network administrator, a base station, large number of sensor nodes and many users. Administrator preloads the identity of the nodes or users and informs the BS. BS registers the nodes and users; and also generates the private key of all nodes or users in the network. After registration of a node by the BS, the node will now capable to send authentication request to the network and the node surrounding of requesting node will perform the authentication. Only the registered node will get permission for authentication and data access; and also a node having a valid identity will not be able to do the registration.

An identity-based signature (IBS) algorithm is used in this proposed authentication protocol. The requesting node sends an authentication request along with the signature of the node on the message. Signature generation algorithm of IBS is used to generate the signature on the message. On the other hand the receiving node verifies the signature using signature verification algorithm of IBS. If the signature verification passed then the authentication is successful. After a successful authentication the communication parties compute their own session key to secure their future communication.

The assessment through the analysis, it ensures that the protocol node authentication protocol is more secure and energy efficient. One more important characteristics of this protocol is the reusability of IBS. If a new better version of IBS algorithm available then the protocol can easily substitute the old IBS with the new one. The new IBS may provide better performance and make more secure the protocol.

The sensor network is resource constraint network having limited power. The main source of the power is the battery (AA type). More security requires more energy. As the security is main attention in this proposed protocol, so it is very important to do the proper balancing of the security and power so that the network will run for longer time without any interruption of power.

The protocol is proposed and analyzed through the theoretical analysis. It is also important to assure whether the protocol is good for the practical environment. So our works in future will be finding out more concrete solution for the node capture attack and implementing the overall protocol to monitor the actual effect in the real environment in terms of different parameters like security, energy consumption, efficiency, durability etc.

7. REFERENCES

[1] 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, modeling and simulation (ISMS), pp 374-379.

[2] H. Jin, H. Debiao and C. Jianhua(2010), "An Identity Based Digital Signature from ECDSA", Second International Workshop on Education Technology and Computer Science (ETCS), pp 627 - 630.

[3] R. Yasmin, E. Ritter, and G. Wang(July 2010), "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures", 10th International Conference on Computer and Information Technology (CIT).

[4] N. A. Pantazis, D. J. Vergados, D. D. Vergados and C. Douligeris(March 2009), "Energy efficiency in wireless sensor networks using sleep mode TDMA scheduling", Elsevier Science Publishers B. V.

[5] M. C. Gorantla, C. Boyd, and J. M. Gonz_alez Nieto(2008), "ID- based One-pass Authenticated Key Establishment", AISC.

[6] W. Ren, K. Ren, W. Lou and Y. Zhang(2008), "Efficient User Revocation for Privacy-aware PKI", 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness.

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

[8] 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.

[9] 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.

[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] Roberto Di Pietro, Luigi V. Mancini and Alessandro Mei (2006), "Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks", Springer Science + Business Media, LLC 2006

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

[13] 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.