An authentication framework for wireless sensor networks using Signature Based Algorithm

Sneh Vyas[1] Prof. Sharnil Pandya[2]

Abstract—Authentication in Wireless Sensor Networks (WSNs) is a challenging process. Providing authentication for the Nodes in WSN is a vital issue in Secure Group communication among WSNs. Massive group of tiny sensor Nodes forms WSNs and these are placed in open, unattended milieu. Due to this reason, Nodes in WSN can endure exclusive encounters. WSNs are more vulnerable to active and passive attacks than wired ones due to their broadcasting nature, limitations in resources and unrestrained environments. However, security will be a significant factor for their complete implementation. In this proposal, a new approach has been introduced to achieve secure authentication among Nodes in WSNs.

Keywords— Authentication, DSA, ECC, Framework, IBS

I. INTRODUCTION

The Sensor nodes are spatially distributed to sense and monitor the physical changes throughout the environment to collect the data. The nodes also process data from its surrounding nodes and the environments. These process 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. Sometime 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.

II. PROPOSED IDEA FOR AUTHENTICATION IN WSN IN DETAIL

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

A. *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

B. *MSKBS*

The BS keeps the master secret key **MSKBS** to itself and distributes the public system parameter **P** to all.

C. *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 **MSKBS** 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.

D. *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.

E. *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.

F. *System Initial Setup Procedure:*

The step by step functions that performed by the BS are following-

1) Base station (BS) generates its' own private (**MSKBS**) and public key (**PKBS**).

2) BS now sets the public system parameter P which also consists its' own public key **PKBS.**

3) BS registers all valid nodes. As BS is the private key generator, so it generates the private key of the nodes (private key DIDi 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

4) Own memory before the deployment of the nodes in the network.

5) BS also registers all valid users and generates their private keys (private key UPKi for user i). The user then stores their own identity UIDi along with their private key UPKi, and public system parameter P into their own memory before the deployment of the nodes in the network.

6) 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 sends the dataset like (H (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. 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.

– *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 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. 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 SIDA, 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 checks 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 does 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.

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

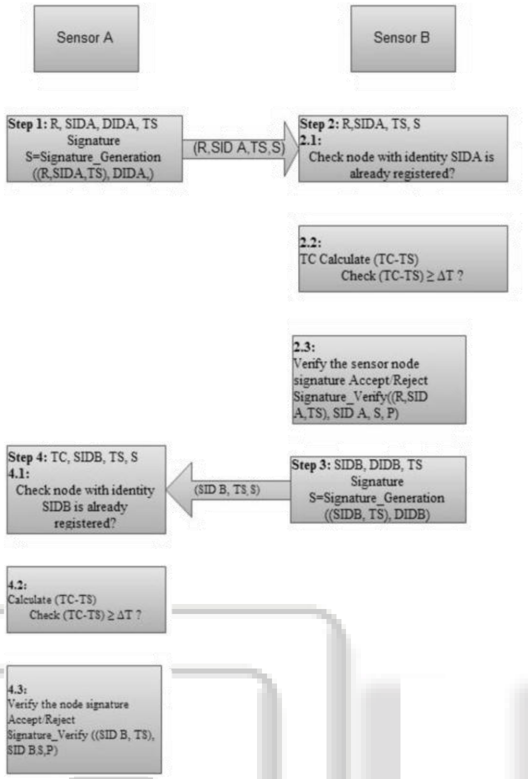
Sensor A
Sensor B
Step 1: R, SIDA, DIDA, TS Signature S=Signature_Generation ((R,SIDA,TS), DIDA,)
(R,SID A,TS,S)
Step 2: R,SIDA, TS, S
2.1: Check node with identity SIDA is already registered?
2.2: TC Calculate (TC-TS) Check (TC-TS) ≥ ΔT ?
2.3: Verify the sensor node signature Accept/Reject Signature_Verify((R,SID A,TS), SID A, S, P)
Step 3: SIDB, DIDB, TS Signature S=Signature_Generation ((SIDB, TS), DIDB)
(SID B, TS,S)
Step 4: TC, SIDB, TS, S
4.1: Check node with identity SIDB is already registered?
4.2: Calculate (TC-TS) Check (TC-TS) ≥ ΔT ?
4.3: Verify the node signature Accept/Reject Signature_Verify ((SID B, TS), SID B,S,P)

Fig. 1: Authentication process of sensor node A with node B.

III. 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[1] to establish the session key. The process of the session key establishment is given below.

Symbol	Meaning
MSKBS	Master Secret Key For Base Station
SIDA	Identity of sensor node for node A
DIDA	Secret key for sensor node A
PKBS	Public Key For Base Station
UIDA	Identity of user A
UPKA	Private Key of user A
R	Authentication request message
BS	Base station
H	One-way hash function
||	Concatenation
k	Security parameter
P	Public system parameters
S	Signature of the user
TS	Sending time stamp
TC	Current time stamp
KAB	Common shared secret between node A and B on node A
TK	Ephemeral key
ΔT	Maximum communication delay
SK	Session key
λ	Key derivation function

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

Step 2. Receiving entity sensor node B or BS also generates the common share secret KBA and check whether KAB and KBA is equal or not.

Step 3. If equal then the node B computes its session key SK = λ (KAB || TS) using the key derivation function λ. TS is the current timestamp of the sensor node B or BS. Sensor node B or BS send an 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 computes 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.

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.

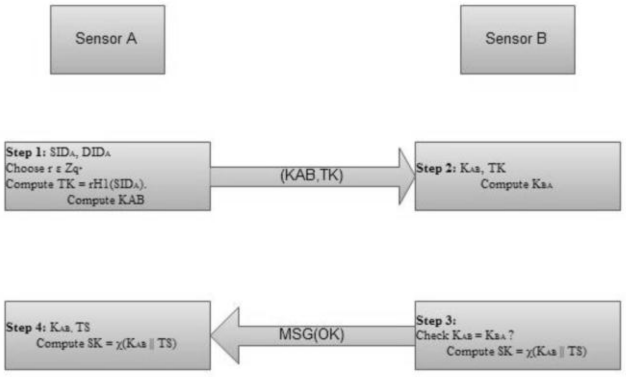
Sensor A
Sensor B
Step 1: SID_A, DID_A Choose r ε Zq* Compute TK = rH1(SID_A). Compute KAB
(KAB,TK)
Step 2: K_{AB}, TK Compute K_{BA}
Step 3: Check K_{AB} = K_{BA} ? Compute SK = χ(K_{AB} || TS)
MSG(OK)
Step 4: K_{AB}, TS Compute SK = χ(K_{AB} || TS)

Figure 2: Session Key establishment process between nodes A and B.

IV. 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.

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.