International Journal of scientific research and management (IJSRM)
||Volume||3||Issue||2||Pages|| 2067-2072||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Authentication Techniques in Wireless Sensor Networks : A Survey

M. Mary Madura Selvam[1] and R. Jensi[2]

[1]Final Year PG, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, India.
marymenon24@gmail.com
[2]AP – CSE, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, India.
jensi.ramakrishnan@gmail.com

ABSTRACT

A wireless Sensor Network (WSN) consists of a large number of sensor nodes mostly deployed in places where monitoring thenodes is highly tougher. The most commonly used authentication techniques are public key cryptography or private keycryptography. In some networks a node will be selected as cluster head which will be communicating with the base stationthrough a trusted server, In such cases the nodes has to be authenticated to ensure the security. Authentication ensures the nodalsecurity in a network. In sensor networks, confidentiality, integrity, authenticity, non repudiation and compromise node are mainfeatures to take care off. In this paper, the various authentication techniques in Wireless Sensor Networks and its methodologiesare discussed.

KEYWORDS

Wireless Sensor Networks, Authentication, Authentication Techniques, Security of WSNs.

1. INTRODUCTION

Most of the sensor networks are dependent on some specific application. Sensor networks are mostly deployed for the collection of real time data in remote areas as said in [1]. The sensor networks are most suited for monitoring or some surveillance applications. Some of the sensor network applications are wildlife monitoring, traffic monitoring, smart homes, quality control in industries, fire response in forests, military command. In the above said applications most of them are deployed in a remote environment. The major area which uses the WSNs is military and medical applications, in such fields prevention of false data stated in [2], [3], [4] entering into the network is important. Adversary detection and attacking is the main aim of the securing a Wireless Sensor Network.

The initial step towards protecting a network is to verify the identity of users. The method of verifying an identity of a user is called as user authentication. Verification using the passwords is not so adequate because access to the resources is possible, if the password is known. Hence a change over from ancient authentication techniques to advanced authentication methods has to be used.

2. AUTHENTICATION OVERVIEW

Authentication provides a correctness of messages by a process of identifying its source by some authentication technique. The main issues of security in a network are the following:

1. Authenticity – destination of a message can check the identity of the source.
2. Confidentiality – content is accessed only by authorized nodes.
3. Integrity – checking for content modification during transmission of message.

The security measures in a Wireless Sensor Network said in [5] include the following:

1.Availability – network services are available at needed time.

2.Authorization – only authorized users/nodes send messages, Authentication, Confidentiality, Integrity.

3.Non-repudiation – node cannot stop sending an already sent message, Scalability.

2.1. Authentication Phase

The authentication phase as quoted in [9], is shown in figure 2.1.1, is invoked when user wants to perform some query to or tries to access some data from the network. The phase is further divided into Login and Verification phases.

1) Login Phase: User enters her/his identity and password. The system checks for the identity and password with the stored ones in it. If the entered *identity and password* is correct then the user is authenticated.

2) Verification Phase: Upon receiving the login request at time *T*, the node authenticates User and Validate the user at time *T*.

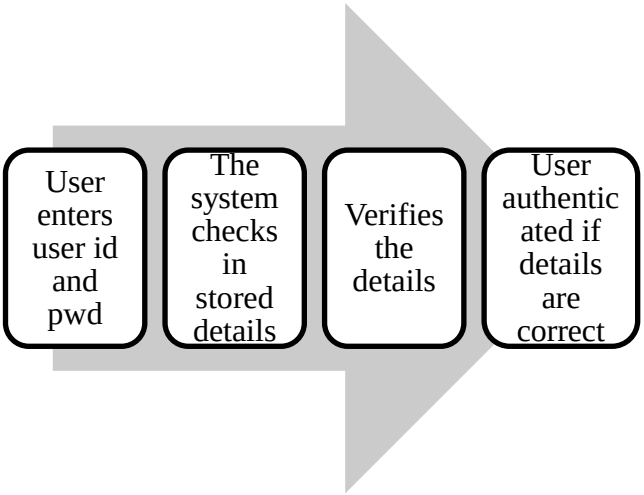

Figure 2.1.1 – Authentication Phase

2.2. Need for Authentication

The process of authentication is mainly needed in order to maintain privacy, integrity and false data injection into network. The alteration of message is possible during the transmission of message in a network, so authentication is needed in order to stop alteration of messages.

The node in a network can be compromised by the adversary and they can make any alteration in the message being forwarded to the sink or base station or an additional data can be added over the data being transferred, in order to prevent this authentication is needed and hence the techniques.

2.3. Authentication Types

The authentication process is mainly of two main types. They are open system authentication and shared key authentication.

2.3.1. Open System Authentication

The open system authentication process includes a simple username and a password verification, in which an open usage of the key between the sender and the receiver occurs. This is simple mode of authentication between the client and the server. The access is provided by a server which verifies the username and the password and authenticates it and gives the access to the client, which request for the access.

To the server, which is connecting junction, any number of server and clients can be connected and authenticated and made to communicate with the client over the secured communication link, created by the process of open shared authentication process. The process involved in open system authentication is shown in figure 2.3.1.1.

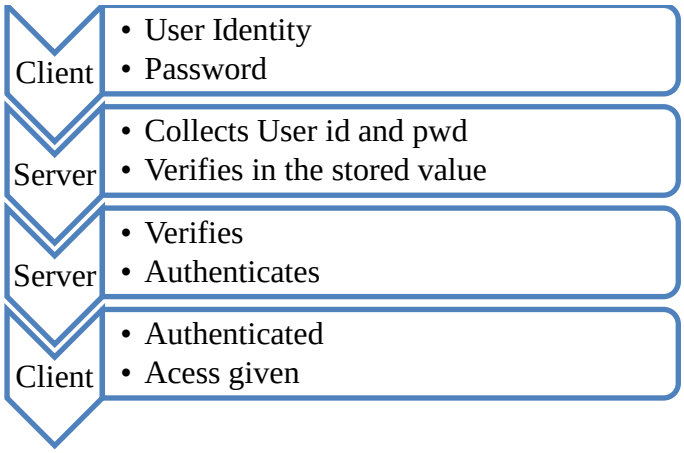

Figure 2.3.1.1 – Open System Authentication Process

2.3.2. Shared Key Authentication

The Shared Key Authentication is shown in figure 2.3.2.1. This technique is also called as public key cryptography. The node sends an authentication request to the server. The server sends challenge text to the station. The station uses it's configured 64-bit or 128-bit default key to encrypt the challenge text, and it sends the encrypted text to the server.

The server decrypts the encrypted text using its configured key that corresponds to the station's default key. The server compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the server and the station share the same key, and the server authenticates the station.

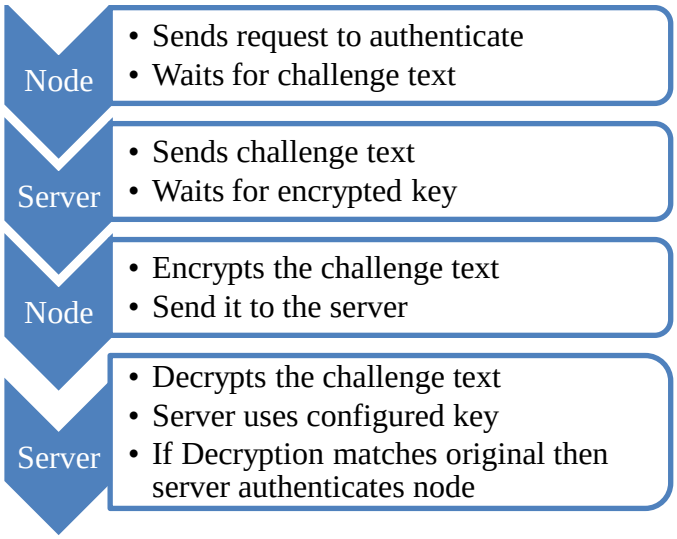

Figure 2.3.2.1 – Shared Key Authentication Process

2.3.3. Message Authentication Code

A message authentication code (MAC) is a symmetric cryptographic mechanism that takes a *k*-bit secret key and a message as input, and outputs an *l*-bit authentication tag. To exchange authentication messages, a sender and receiver must share the same secret key.

Using the secret key, the sender computes the message's authentication tag (or MAC) and appends it to the message. To verify the authenticity of a message, the receiver computes the message's MAC with the secret key and compares it to the original MAC appended with the message.

A MAC achieves authenticity for point-to-point communications because a receiver knows that a message with the correct MAC must have been generated either by itself or by the sender.

3. WIRELESS SENSOR NETWORKS

Wireless Sensor networks (WSNs) is a spatially distributed autonomous sensor to monitor the physical or environmental conditions such as temperature, sound, pressure etc., and to cooperatively pass their data through the network to a main location which may be a base station or a monitoring station. The WSN is built by a few to even thousands of sensor node where each node is connected to one or several sensors.

3.1. Traffics in Wireless Sensor Networks

Traffic is the communication between any two or more nodes in a wireless sensor network. There are basically three main types of traffics in WSNs as said in [6]:

1. Many to one: In this method many sensor nodes communicate with a single node, this single node may be a base station.
2. One to one: Here a single sensor node communicates with a single node over a network.
3. Local Communication: The nearby neighbor sends messages to the adjacent nodes to discover the association [7].

3.2. Attacks in a Wireless Sensor Networks

The two main types of attacks said in [5] in any type of networks are mainly:

1. Outsider attacks.
2. Insider attacks.
3. Replay attacks (replay an old message).
4. Impersonation attacks (pretend to be the client or server).
5. Reflection attacks (bounce the authentication messages elsewhere).
6. Steal the client/server authentication database.

The outsider attack involves the attacks of nodes that have not compromised any other nodes of the network. In particular they do not know any details about the network but may inject an additional data or a false data can be included into the network.

The insider attack is launched by any node that is being compromised and may know some details of the network because a node is already being compromised.

Replay attacks is more common in most of the network where a node may be compromised by an adversary but couldn't access further over the network, in such cases the node sends a replay of the old message to the sink, which may lead to a critic.

The impersonation attacks involve the pretending of a node to be a client or a server and act as a client/server. In this impersonation, a client or server can pretend to be anyone in the network.

4. AUTHENTICATION TECHNIQUES

4.1 Bloom Filters

The Statistical Enroute Filtering works in three main steps which help to detect and drop the false data packets at the earliest. They are mentioned below:

1. A report is generated which is legitimate and it carries several MACs generated by all the nodes in the form of bloom filters to the destination.
2. The incorrect false MACs are detected in en-route.
3. The sink checks the correctness of the MACs and drops incorrect one.

4.2 Interleaved hop by hop

- *Node initialization and deployment phase:* The main server loads each and every node with a unique id, and also some necessary keying values that allow the node to establish pair wise keys with all the association nodes.

- *Association Discovery:* In the association discovery step, each node detects the association nodes. The process of association discovery is started by the base station.

- *Report Endorsement:* The nodes generate a legitimate report when an event of interest occurs. Every node of the participating network computes two MACs (Message Authentication Code) over an event, one for the Base Station (BS) and the other is for the upper association. The nodes send the report to the Cluster Head (CH). The CH collects all the MACs from the network. This collection is made into a report and forwarded to the BS.

- *En-Route Filtering:* In the en-route filtering checks the MAC computed by the association of nodes at lower level and if the verification succeeds, then attaches a new MAC with upper association. Finally the report is forwarded to base station (BS).

- *Base Station Verification Phase:* The BS verifies for the report that has been received. If the BS detects endorsed nodes then it accepts the report else rejects it.

4.3 ID based scheme

ID-based Online/Offline Signature (IBOOS) Schemes: ID-based online/offline signature schemes are suitable for the proposed sensor broadcast authentication scheme. An IBOOS scheme in [14] presents a method to convert any underlying signature scheme into an online/offline signature scheme. The Offline signature in this scheme can be securely re-used to sign more than one message. This signature scheme is proved to be existentially not forgeable. Its security depends on Discrete Logarithm Problem.

Unlike in [14], an IBOOS scheme presented in [15] provides a direct online/offline signature scheme, which does not require another underlying signature scheme.

4.4 Hop by hop authentication

The hop by hop authentication uses an authentication process in every hop of its message sending. Here the elliptic curve cryptography has been used for the signature generation and verification. The hop by hop technique uses the Modified Elgamal Signature (MES) for the process of signature creation and verification. It uses Source Anonymous Message Authentication (SAMA) for securing the source location.

5 RELATED WORK

- *Statistical En-route filtering* as said by Fan Ye, Haiyun Luo, Songwu Lu, Lixia Zhang in [1]. The Statistical En-route filtering (SEF) mainly focus on the node compromise attack and its prevention since it will affect the entire networks performance. In SEF the amount of reliability on a single node is limited and the security is based on a collection of reports from a number of nodes.

The goals that can be achieved by using SEF are as follows:

- Early detecting and dropping of false data reports.
- Low computation and communication overhead.

- *Interleaved hop by hop scheme* as discussed by Sencun Zhu, Sanjeev Setia, Sushil Jajodia, Peng Ning in [11]. The scheme used in interleaved hop by hop technique.

An example where t = 3. BS(base station),CH(cluster head). Nodes connected with an arc are associated, one closer to BS is the upper associated node and other is the lower associated node.

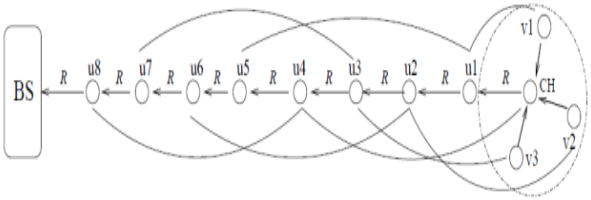

Figure 4.2.1 – Association Finding with a cluster head [11]

An example BS hello step where t = 3. u_i is an en-route node. v1; v2; v3 are cluster nodes. (M) is the content of the beaconing message. Note that u_i may be an en-route node for multiple paths and CH may also be an en-route node for another cluster.

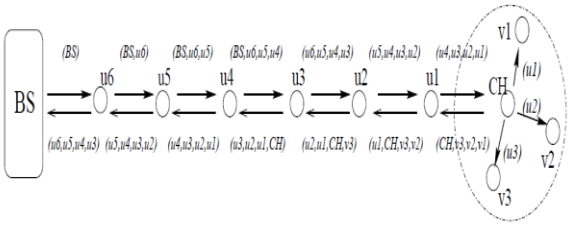

Figure 4.2.2 – Sending of hello packets from base station to cluster head [11]

- *Light Weight Message Authentication in WSN* Wensheng Zhang, Nalin and Guiling Wang [5]:

Scheme-I as discussed in [5]*: A Basic Bivariate Polynomial-Based Scheme for Authenticating Messages Sent by the Base Station:* Initial step is the process of initializing the Security Server and the BS. Over finite field F_q, the security server randomly picks a secret bivariate polynomial. Then, the security server preloads the base station with f(x, y) and a secure one-way hash function h(.), which could be MD5, SHA, etc. The steps involved in light weight message authentication [12] is,

a) Initialization of Sensor Nodes.

b) Message Sending at the Base Station.

c) *Message Verification at Sensor Nodes.*

Scheme-II [5]: A Perturbed Bivariate Polynomial-Based Scheme for Authenticating Messages Sent by the Base Station

Firstly, when the base station sends out a message m, its authentication function ,then it is perturbed, after the perturbation, even an intruder has collected more messages, it cannot obtain any exact shares of function.

Secondly, when the security server distributes verification functions to sensor nodes, these functions shall not be exact shares of function, but perturbed ones. This way, even the adversary has compromised more sensor nodes, they cannot obtain any exact share of function.

- *Authentication Framework* as said by X. Cao, W. Kou, L. Dang, and B. Zhao in [12]

ID-based Signature (IBS) Schemes: ID-based signature schemes are suitable for the user authentication scheme. IMBAS has been said in [12] describes an IBS scheme which is actually an improvement over BNN-IBS as discussed in [13] to reduce signature size. Security of this signature scheme depends on Elliptic Curve Discrete Logarithm Problem.

- *Hop by hop authentication* as said by Jian Li, Yun Li, Jian Ren and Jie Wu [16] The survey on the papers referred shows that there are several authentication techniques in which each technique has its own advantages and disadvantages, over which the hop by hop authentication said by Jian Li, Yun Li, Jian Ren and Jie Wu in [16] is the most secure method for authentication process. Here the Elliptic Curve Cryptography is used for the signature generation and verification algorithm by using the two main techniques. One is MES (Modified ElGamal Signature) and the other is SAMA (Source Anonymous Message Authentication). These are the techniques which are used in recent authentication process, which overcomes all the above said ideas.

The detailed comparison table is below:

Paper Referred	Technique Used	Possible Attacks (if any)	Performance Measure	Advantages (Disadvantages if any *)
Fan Ye, Haiyun Luo, Songwu Lu, Lixia Zhang [1]	Bloom Filters.	Node compromise attack.	Low computation and communication overhead.	Early detecting and dropping of false data reports.
Sencun Zhu, Sanjeev Setia, Sushil Jajodia, Peng Ning [11]	Interleaved hop by hop.	Impersonation attack	Authentication done only by the verification of a Base station.	En-route filter for multiple paths is possible.
Wensheng Zhang, Nalin and Guiling Wang [5]	Scheme – 1 Bivariate Polynomial using MD5, SHA.	Polynomial attack.	One way hash function.	Hash Function can be generated easily.
Wensheng Zhang, Nalin and Guiling Wang [5]	Scheme – 2 Perturbed Bivariate Polynomial using MD5, SHA.	Polynomial attack.	Many hash function.	High Complexity is a main disadvantage.
X. Cao, W. Kou, L. Dang, and B. Zhao	ID based scheme.	Logarithmic Problem.	The elliptic curve discrete logarithm.	Non forgeable.
Jian Li, Yun Li, Jian Ren and Jie Wu.	Scalable authentication based on Elliptic Curve Cryptography.	Node resilient attack and compromise attack.	Reduced Threshold.	Less computation and communication overhead.

Table 1. Comparison of various parameters in the papers' surveyed

5. CONCLUSION

This paper is about a study on the authentication techniques in Wireless Sensor Networks. The survey starts with an introduction to the authentication, WSN and the various authentication techniques and finally a study on several papers on authentication. The Wireless Sensor Network which is deployed in the remote areas has to be monitored from a remote base station for which the process of authentication is more important in order to secure all the nodes from all sorts of attack. A public key cryptography using the Elliptic Curve Algorithm, in which techniques like Modified ElGamal Signature(MES) and Source Anonymous Message Authentication(SAMA) has been used for a better hop by hop authentication process. More research has to be carried on hop by hop authentication in Wireless Sensor Network, through which the nodes and messages can be secured.

REFERENCES

1. *"Statistical En-route Filtering of Injected False Data in Sensor Networks"* Fan Ye, Haiyun Luo, Songwu Lu, Lixia Zhang UCLA Computer Science Department, Los Angeles, CA 900095.
2. V. Wen, A. Perrig, and R. Szewczyk, *"SPINS: Security Suite for Sensor Networks,"* in ACM MOIBCOM, 2001.
3. L. Eschenauer and V. D. Gligor, *"A Key-Management Scheme for Distributed Sensor Networks,"* in ACM CCS, 2002.
4. H. Chan, A. Perrig, and D. Song *"Random Key Predistribution Schemes for Sensor Networks,"* in IEEE Symposium on Security and Privacy, 2003.
5. *"Lightweight and Compromise-Resilient Message Authentication in Sensor Networks"* Wensheng Zhang and Nalin Subramanian Department of Computer Science Iowa State University Ames, IA 50011, Guiling Wang Department of Computer Science New Jersey Institute of Technology Newark, NJ 07102.
6. *"Kerberos Authentication in Wireless Sensor Networks"*, Qasim Siddique Foundation University, Islamabad, Pakistan.
7. *"An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks"*, Sencun Zhu1 Sanjeev Setia1 Sushil Jajodia1, Center for Secure Information Systems George Mason University Fairfax.
8. *"An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks",* Shang-Ming Chang Shiuhpyng Shieh Warren W. Lin, National Chiao Tung University / University of California, Berkeley, Chih-Ming Hsieh, Institute for Information Industry.
9. *"Two-Factor User Authentication in Wireless Sensor Networks"*, Manik Lal Das, Member, IEEE.
10. *"Multi-User Broadcast Authentication in Wireless Sensor Networks"*, Kui Ren, Member, IEEE, Shucheng Yu, Student Member, IEEE, Wenjing Lou, *Senior Member, IEEE*, and Yanchao Zhang, Member, IEEE.
11. *"An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks",* Sencun Zhu, Sanjeev Setia, Sushil Jajodia, Center for Secure Information Systems George Mason University, Fairfax, Peng Ning, Computer Science Department North Carolina State University, Raleigh.
12. X. Cao, W. Kou, L. Dang, and B. Zhao, *"IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks,"* Computer Communications, vol. 31, no. 4, pp. 659 – 667, 2008.
13. M. Bellare, C. Namprempre, and G. Neven, *"Security proofs for identity-based identification and signature schemes,"* in Proc. EUROCRYPT '04. Springer-Verlag, 2004, pp. 268–286.
14. Q. Ren, Y. Mu, and W. Susilo, *"Mitigating phishing with ID-based online/offline authentication,"* in Proc. Australasian conference on Information Security, AISC '08, pp. 59–64.
15. S. Xu, Y. Mu, and W. Susilo, *"Efficient authentication scheme for routing in mobile ad hoc networks,"* in Proc. EUC '05 Workshops, ser. LNCS, vol. 3823. Springer, 2005, pp. 854–863.
16. *"Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks"*, Jian Li, Yun Li, Jian Ren, Senior Member, IEEE, and Jie Wu, Fellow, IEEE.

Authors

M. Mary Madura Selvam received her B.Tech (CSE) in 2012 from Anna University and pursuing M.E (CSE) in Dr. Sivanthi Aditanar College of Engineering, Tiruchendur. Her area of interest is Network Security in Wireless Sensor Networks and she is also an active student member of CSI.

R.Jensi received the B.E (CSE) and M.E (CSE) in 2003 and 2010, respectively. Her research areas include data mining, text mining especially text clustering, natural language processing and semantic analysis. She is currently pursuing Ph.D(CSE) in Manomanium Sundaranar University , Tirunelveli. She is a member of ISTE.