International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-2, May 2015
ISSN: 2395-3470
www.ijseas.com

"An Overview On Authentication In Wireless Sensor Networks"

[1] S.Shalini, [2]M.S.Bonshia Binu
[1] II M.E CSE, [2] Assistant Professor
Department of Computer Science and Engineering,
Ponjesly College of Engineering,
Nagercoil, 629001, India.
shalinishamini92@gmail.com, binubonshia1988@yahoo.com

ABSTRACT

Message authentication is one of the most effective ways to stop corrupted and unauthorized messages are inserted into the Wireless Sensor Networks (WSNs). This Message authentication schemes developed based on the symmetric-key or asymmetric-key cryptosystems. Many of them, have the constraints of high computational and communication overhead due to lack of scalability and resilience to node compromise attacks. In this paper, proposing a security model for providing the authentication on messages that helps to preserve confidentiality and integrity of transmitted message. The key idea of this technique is to provide the unconditional security using the authentication algorithm. This paper discusses various types of authentication, attacks, security goals, and etc. Furthermore, it discusses the authentication technique such as SAMA, public-key cryptosystem.

Keywords- Authentication, symmetric-key cryptosystems, public-key cryptosystem, Wireless Sensor Networks(WSNs), Attacks.

1. INTRODUCTION

Message authentication scheme carry out a key role to preventing unauthorized and corrupted messages from being forwarded in sensor networks. So that, many authentication schemes have been planned in literature to give message authenticity and integrity verification for wireless sensor networks(WSNs) [1]-[6].These approaches have can largely be divided into two categories: public-key based approaches and symmetric-key based approaches.

The symmetric-key based approach needs complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The sender generate a Message Authentication Code (MAC) for each transmitted message by using the shared key. However, for this basis, the authenticity and integrity of the message can only be checked by the node with the secret key, which is usually shared by a group of sensor nodes. An intruder can compromise the key by confining a single sensor node. This method does not applicable for multicast network.

For a public-key based approach, each message is transmitted along with the digital signature of the message which is generated using the sender's private-key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public-key [7], [8]. The drawbacks of the public-key based approach is the high computational overhead.

2. SECURITY TERMS

The security terms such as encryption, and decryption etc. Encryption is used to hiding the original data which is not visible to the unauthorized users. Decryption is reverse process of encryption. Strength of the method depends on secrecy of the key used. There are two keys are used: Public-key and private-key. The public-key is also known as asymmetric-key or two-way-key. Private-key use the same key for both encryption and decryption. Public-key use the different keys for encryption and decryption. William Stallings [11] explained in detail about the commonly used security terms. Some of the security terms are defined in the following:

2.1 Authentication: This will verify the identity of the user whether the message is sent by the node that is claimed.

2.2 Confidentiality: This will protect the secrecy of the information and does not allow unauthorized users to access the another information.

2.3 Integrity: This will verify the originality of information. The information is unaltered or not modified.

2.4 Identity and Location Privacy: The opponent cannot determine the message sender's identity and location by analyzing the message contents.

2.5 Efficiency: This should be efficient in terms of both computational and communication overhead.

3. AUTHENTICATION TYPES

Authentication is the process by which it check whether the message is sent by a node that is claimed. In other words, the adversaries cannot act as an innocent node and inject fake messages into the network. The following are the types of authentication.

3.1 Unicast Authentication

Unicast authentication provide the assertion of origin integrity when the message is distributed from one sender to one receiver. Message authentication code is produced by the sender of the message by using a secret key, which is used to guarantee origin integrity.

3.2 Broadcast Authentication

Broadcast authentication is also known as multicast authentication. It guarentees that multiple recipients of the message can authenticate its origin integrity. If using message authentication code to make sure broadcast authentication, all recipients of the message must share the symmetric key.

4. TYPES OF ATTACKS

Sensor networks are mostly vulnerable to several types of attacks. Attacks can be performed by variety of ways such as, Sybil attacks, Denial of service attacks, Node replication attacks, Privacy violation by attacks, Traffic analysis attacks and so on.

4.1 Sybil Attacks

The Sybil attack is described as a "malicious device illegitimately taking on multiple identities". It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. In addition to defeating distributed data storage systems, the Sybil attack is also effective

against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection.

4.2 Denial of Service Attacks

The Denial of service attacks on wireless sensor networks is jamming a node or set of nodes. The jamming of a network can come in two forms:

- Constant jamming
- Intermittent jamming

Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently. Denial of service Attacks can also be made on the link layer itself. One possibility is that an attacker may simply intentionally violate the communication protocol and continually transmit messages in an attempt to generate collisions. Using this denial of service technique it would be possible for an attacker to simply deplete a sensor node's power supply by forcing too many retransmissions or perform any detection.

4.3 Node Replication Attacks

Abstractly, a node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by replicating the node ID of an existing sensor node. If a node replicated in this fashion then, it can severely disrupt a sensor network's performance: packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, not authenticated etc. If an attacker can gain physical access to the entire network, he can copy cryptographic keys to the replicated sensor and can also insert the replicated node into strategic points in the network.

By inserting the replicated nodes at network particular points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether. The node replication attack is quite simple, an attacker seeks to add a sensor node to an existing sensor network by replicating the node ID (Identity) of an existing sensor node in the wireless sensor network.

4.4 Privacy Violation by Attacks

Some of the more common attacks against sensor privacy are described in the following;

- Monitor and Eavesdropping
- Traffic Analysis
- Camouflage

Monitor and Eavesdropping. By listening to the data, the adversary could easily identify the communication contents.

Traffic Analysis. Traffic analysis typically combines with monitoring and eavesdropping. By increasing the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity.

Camouflage. Adversaries can insert their node or compromise the nodes in the sensor network. After that these nodes can masquerade as a normal node to attract the packets, then misroute the packets, e.g. forward the packets to the nodes conducting the privacy analysis.

4.5 Traffic Analysis Attacks

Wireless sensor networks are normally composed of many low-power

sensors nodes. That communicating with a few relatively robust and powerful base stations. It is not abnormal, therefore, the data to be gathered by the individual nodes where it is ultimately routed to the base station. Often, for an adversary to effectively render the network useless, the attacker can simply hinder the base station. The WSNs are vulnerable to a number of attacks at all layers of the TCP/IP protocol stack, there may be other types of attacks possible which are not yet identified. Securing a WSN against all these attacks may be a quite challenging task.

5. SECURITY MODEL IN WIRELES SENSOR NETWORKS

5.1 Public-key Cryptosystem Based Security Model

This public-key cryptosystem is the authentication scheme, which is developed for preventing the unauthorized messages and corrupted messages inserted into the wireless sensor network to save the sensor power. In which each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public-key [7],[8]. The recent progress on Elliptic Curve Cryptography (ECC) shows the public-key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, and etc since public-key based approaches have a simple and clean key management [9].

ECC used in the security development field of information security. It requires low operating cost for sensor network. This ECC used for digital signature generation and key exchange and also used for classified as well as unclassified national security systems. It provide strong security for the information when transmitting from source node to destination node in the wireless sensor network.

5.2 Source Anonymous Message Authentication (SAMA)

The source anonymous message authentication scheme is the unconditionally secure and efficient authentication scheme based on the optimal Modified ELGamal Signature (MES) scheme on elliptic curves. The MES scheme is secure against adaptive chosen-message attacks in the random oracle model [10]. The SAMA scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. The SAMA has the following security requirements.

5.2.1 Sender Ambiquity

The probability that a verifier successfully determines the real sender of the anonymous message is exactly 1=n, where n is the total number of members in the network.

5.2.2 Unforgeability

An anonymous message scheme is unforgeable if no adversary, given the public-keys of all members of the anonymous set.

6. CONCLUSION

This paper presented the various types of authentication, attacks, security goals, and etc. This paper propose a novel and efficient SAMA based on ECC. This SAMA can be applied to any message

contents to provide authentication on message. And also it provide hop-by-hop message authentication when the message is transmitted from one node to another. This will identify the compromised node, when applied to wireless sensor networks with fixed sensor node. This scheme is more efficient in terms of computational overhead, energy consumption, delivery ratio.

7. REFERENCES

1. Ye F., Lou H., Lu S., and Zhang L. (Mar-2004) 'Statistical En-Route Filtering of Injected False Data in Sensor Networks', Proc. IEEE INFOCOM.

2. Zhu S., Setia S., Jajodia S. and Ning P. (2004) 'An Interleaved Hop-By-Hop Authentication Scheme for Filtering False Data in Sensor Networks', Proc. IEEE Symp. Security and Privacy.

3. Blundo C., De Santis A., Herzberg A., Kutten S., Vaccaro U. and Yung M. (Apr-1992) 'Perfectly-Secure Key Distribution for Dynamic Conferences', Proc. Advances in Cryptology (Crypto '92), pp. 471-486.

4. Zhang W., Subramanian N. and Wang G. (Apr.2008) 'Lightweight and Compromise-Resilient Message Authentication in Sensor Networks', Proc. IEEE INFOCOM.

5. Perrig A., Canetti R., Tygar J. and Song D. (May-2000) 'Efficient Authentication and Signing of Multicast Streams over Lossy Channels', Proc. IEEE Symp. Security and Privacy.

6. Albrecht M., Gentry C., Halevi S. and Katz J. (2009) 'Attacking Cryptographic Schemes Based on Perturbation Polynomials', Report 2009/098, http://eprint.iacr.org/.

7. Rivest R., Shamir A. and Adleman L. (1978) 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems', Comm. ACM, vol. 21, no. 2, pp. 120-126.

8. ElGamal T.A. (July-1985) 'A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms', IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472.

9. Wang H., Sheng S., Tan C. and Li Q. (2008) 'Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control', Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18.

10. Pointcheval D. and Stern J. (1996) 'Security Proofs for Signature Schemes', Proc. Advances in Cryptology (EUROCRYPT), pp. 387-398.

11. William Stallings, 'Cryptography and Network Security Principles and Practices, Fourth Edition', 2006