ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Providing Hop by Hop Message Authentication and Source Privacy in Wireless Sensor Networks

Malashree

P.G. Student, Department of CSE, SDIT College of Engineering, Mangalore, India

Abstract: Message authentication is an effective mechanism, used to authenticate the messages in wireless sensor networks (WSNs). Wireless Sensor Network consists of a large number of sensor nodes. Each sensor node knows its location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. Many message authentication schemes are based on either symmetric-key cryptosystems or public-key cryptosystems. An existing system like polynomial based scheme authenticate the message based on threshold value, this is a problem of existing system because only limited number messages are authenticated. Proposing a new Source Anonymous Message authentication (SAMA) is a scalable authentication scheme based on elliptic curve cryptography (ECC) is used to allow any node to transmit and authenticate an unlimited number of messages without suffering the threshold problem and provides message source privacy.

Keywords: Hop by hop message Authentication, elliptic curve cryptography, WSN, SAMA, MES.

I. INTRODUCTION

In hop by hop message authentication with source privacy in wireless sensor network, were authentication is effective way to protect from unauthorized users effected messages from being send through in wireless sensor networks. Many message authentication schemes have been used to protect messages but these authentication schemes have the limitations of high overhead, lack of ability, to node attacks and threshold problem. Message authentication has a main role in thwarting unauthorized and effected messages from being sent in networks to save the energy. Many authentication processes have been implemented to provide message authenticity and verification for wireless sensor networks. The symmetric-key based approach has complicated key management and lacks of ways. It is not taken to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The sender uses shared key to generate a message authentication code for each transmitted message. The authenticity and integrity of message can verified only by the node using shared secret key, which is generally shared by a group of sensor nodes. An attacker can easily access the key by occupying a single sensor node. So, It will does not work in multicast networks.

In order to solve the problem, a secret based for the message authentication scheme was introduced. The method is similar to a threshold secret sharing, where it is determined by the degree of the value. This offers information security of the shared secret key when the number of messages transmitted is less than the threshold. The middle nodes verify the authenticity of the message. If the transmitted messages are larger than the threshold, can be fully recovered. For the public-key based method, each message is transmitted along with the digital signature of the message produced using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. One of the restrictions of the public key based method is the high computational overhead.

In this project we propose an unconditionally source anonymous g message authentication scheme (SAMA), which uses Modified New variant ElGamal signature Scheme (MNES). This MNES scheme is secure against adaptive chosen-message attacks in the random oracle model [10]. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based algorithms under comparable security levels.

The major contributions of this paper are the following:

1) We develop a source anonymous message authentication code on elliptic curves that can provide
2) Unconditional source anonymity.
3) We offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation.
4) We devise network implementation criteria on source node privacy protection in WSNs.
5) We propose an efficient key management framework to ensure isolation of the compromised nodes.
6) We provide extensive simulation results under ns-2 and TelosB on multiple security levels.

A. EXISTING SYSTEM

The symmetric key based approach has complex key management, lacks of scalability and is not resilient to

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

large numbers of node compromise attacks, reason being need of sharing secret key between message sender and receiver. Here sender uses the shared secret key to generate the message authentication code (MAC) for each transmitting message. The authenticity and integrity of messages can verify only by the node using the shared secret key, which is generally shared by a group of sensor nodes. Because of this, an attacker can easily compromise the key by capturing a single sensor node, so this method doesn't work in multi cast networks. To address this problem, a secret polynomial based message authentication scheme has been introduced; however this scheme and its extensions (Perturbation factor) all have the weakness of built in threshold problem determined by the degree of the polynomial.

For the public key based approach, the sender transmits each message along with the digital signature of the message generated by using the sender's private key. The sender's public key is used by every intermediate forwarder and the final receiver to authenticate and verify the transmitted message but the limitation of the public key based scheme is the high computational overhead, So to overcome these limitation, the progress on the elliptic curve cryptography (ECC) shows that public key schemes can have more benefits in terms of security resilience, computational complexity, memory uses. As per this we can find out that, public key based approaches have a simple and clean key management than the symmetric key based approaches.

Disadvantages:

- In these schemes, each symmetric authentication key is shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. Therefore, these schemes are not resilient to node compromise attacks. Another type of symmetric-key scheme requires synchronization among nodes.
- These schemes, including tesla and its variants, can also provide message sender authentication. However, this scheme requires initial time synchronization, which is not easy to be implemented in large scale WSNs. In addition, they also introduce delay in message authentication, and the delay increases as the network scales up.
- In polynomial scheme only limited number of messages can be transmitted.

II. PROBLEM STATEMENT

Purpose of the project is to provide intermediate node authentication without the threshold limitation, and to perform better than the symmetric-key based schemes. The distributed nature of algorithm makes the scheme suitable for decentralized networks.

Important purposes are as follows:

1) To develop a source anonymous message authentication code [12] (SAMAC) on elliptic curves that can provide unconditional source anonymity.
2) To offer an efficient intermediate node authentication mechanism for WSNs without the threshold limitation.
3) To the devise network implementation criteria on source node privacy protection in WSNs.

III. PROPOSED SYSTEM

An unconditional secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise-resiliency, flexible-time authentication and source identity protection. In this it needs develop a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. Then offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation. Then propose an efficient key management framework to ensure isolation of the compromised nodes.

The wireless sensor networks are assumed to consist of a large number of sensor nodes. Assume that each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. In this project there is a security server (SS) that is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the SS and other nodes.

Based on the above assumptions, this paper considers two types of attacks launched by the adversaries:

1) Passive attacks: Through passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis.
2) Active attacks: Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised nodes, including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages.

Design goals:

Proposed authentication scheme aims at achieving the following goals:

- Message authentication: The message receiver should be able to verify whether a received message is sent

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

by the node that is claimed, or by a node in a particular group. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.

- Message integrity: The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.
- Hop-by-hop message authentication: Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.
- Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.
- Efficiency: The scheme should be efficient in terms both computational and communication overhead.

A. Source Anonymous Message Authentication (SAMA) on Elliptic curves

SAMA techniques does not have the threshold problem. unlimited number of messages are authenticated. SAMA is a secure and efficient mechanism. Generates a source anonymous message authenticator for the message m. The message generation is based on the MES scheme on Elliptic curves. An elliptic curve E is defined by an equation of the form:

$E : y^2=x^3 +ax + b \bmod p;$

1. Considering a base point elliptic curve.
2. Assuming the private key of sender node.
3. Calculate public key of sender.
4. The message is to be hashed and left bit of hash functions are converting into binary format.
5. Finding the signature of message.

B. Modified ElGamal Signature Scheme

Authentication generation algorithm: Sender node is send the message to be transmitted to receiver node. (SAMA):A SAMA consists of the following these steps:

1. Receiver node receiving the hashed message.
2. Left most bit of the hash is taken in decimal format.
3. If it receives same key means allow to transform and access that message.

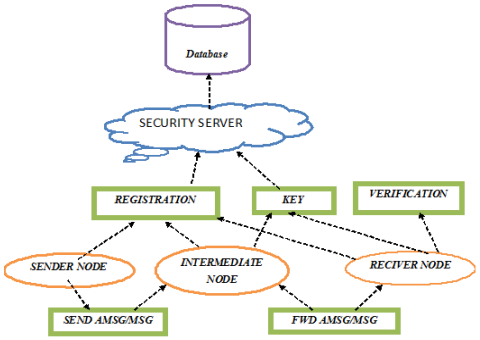

Figure 1: Proposed Architecture diagram

IV. CONCLUSION

In this Project, we first proposed a novel and efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC). While ensuring message sender privacy, SAMA can be applied to any message to provide message content authenticity.To provide hop by hop message authentication without the weakness of the threshold of the polynomial-based scheme, we then propose a hop-by-hop message authentication scheme based on the SAMA. When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification. We compared our proposed scheme with the polynomial-based scheme through simulations usingns-2 and TelosB. Both theoretical and simulation results show that, in comparable scenarios, our proposed scheme is more efficient than the polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

REFERENCES

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

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

[3]. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U.Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. Advances in Cryptology (Crypto '92), pp. 471-486, Apr. 1992.[4] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEEINFOCOM, Apr. 2008.

[4]. A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy, May 2000.

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

[6]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[7]. T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[8]. H. Wang, S. Sheng, C. Tan, and Q. Li, "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. Dis- tributed Computing Systems (ICDCS), pp. 11-18, 2008.

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