International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 5, May 2015)

Preserving Source Privacy And Massage Authentication In WSN

using elliptic curve cryptography

Sandeep Awale
Dept. Of Telecommunication
Dayananda Sagar College of Engineering.
Bangalore, Karnataka, India
awalesandeep@gmail.com

Dr. A Sreenivasan
Prof. & PG Director
Dayananda Sagar College of Engineering.
Bangalore, Karnataka, India

***Abstract*—Message authentication is the most effective way to thwart unauthorized and corrupted messages being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, In this paper, it proposes a scalable authentication scheme based on elliptic curve cryptography (ECC). Where all the intermediate nodes do the authentication, the proposed scheme allows any node to transmit and receive an unlimited number of messages without the limitation of threshold problem. In addition, this scheme also provides message source anonymity.**

***Keywords*— Source Privacy, elliptic curve cryptography, SAMA.**

I. INTRODUCTION

A typical wireless sensor node consists of sensing, computing, communication, actuation, and power components. These components are integrated on a single or multiple boards, and packaged in a few cubic inches. A WSN usually consists of ten to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing. WSNs can be deployed on a global scale for environmental monitoring, over a battle field for military surveillance , in factories for condition based maintenance, in buildings for infrastructure health monitoring, or even in medical field for patient monitoring system.

In a typical WSN scenario, A user can retrieve information of interest from the WSN by injecting queries and collecting results from the base station, which act as an interface between the user and the network. So WSNs can be considered as a distributed database. The WSN will be will be connected to the Internet, by which global information sharing becomes feasible.

Message authentication is the most effective way in thwarting the unauthorized and corrupted messages from being transmitted in networks so as to save the precious sensor energy. For this reason, there are many authentication schemes present in literature to provide message authentication in WSN. These schemes can be classified into two categories. Public-key and symmetric-key based approaches.

The symmetric-key based scheme requires complex key management, lacks of scalability, and it is not resilient to large numbers of node compromise attacks since the message sender and the receiver both share a secret key. The shared key is used by the sender and it generates a message authentication code (MAC) for each transmitted message. However, in this method, the authenticity and the integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An attacker can compromise the key by attacking a single sensor node. But this method does not work in multicast networks.

To solve this scalability issue, the secret polynomial based message authentication scheme was introduced in this system. In this scheme the idea is similar to a threshold secret sharing, This scheme offers information-theoretic security of the shared secret key when the number of messages transmitted is less than the threshold value, Where the threshold is determined by the degree of the polynomial. The intermediate nodes do verify the authenticity of the message through a polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial based scheme fails in authentication.

An alternative solution was proposed to this system to thwart the attacker from recovering the polynomial by computing the coefficients of the polynomial. The idea is to add the random noise, also called as perturbation factor, to the polynomial so that the coefficients of the polynomial cannot be easily solved. However, the study shows that the random noise can be completely removed from the polynomial using error-correcting code techniques.

In the public-key based scheme, The message is transmitted along with the digital signature generated for the message using the sender's private key. Every intermediate node and the destined receiver can do authentication of the message using the sender's public key. The limitation of the public key based scheme is that it has high computational overhead.But the recent studies on elliptic curve cryptography shows that the public-key schemes is more advantageous in terms of memory usage, computational complexity, and security

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 5, May 2015)

resilience, since public-key based scheme have a simple and clean key management.

In this paper, it proposes an SAMA scheme which is unconditionally more secure and efficient source anonymous message authentication scheme, based on the optimal modified ElGamal signature scheme on elliptic curves. This scheme enables the intermediate nodes to do authentication, so that all corrupted message can be detected and dropped to save the sensor energy. While achieving compromise-resiliency, flexible-time authentication and source privacy protection, this scheme does not have the problem of threshold.

II. PROPOSED BLOCK DIAGRAM

Here, the source will send the encrypted message or information file to the nearest node and the keys are exchanged between the source, nodes and the destination node. The intermediate node receive message and do authentication and pass it to the nearest node and here also the authentication takes place. And if the message is uncorrupted then it is sent to destined receiver. If the message is corrupted then filtering is done and then passed to the destination node.

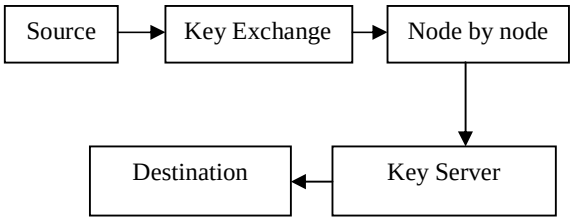

Figure1: Block diagram of proposed system.

In this system, proposed a scalable authentication scheme based on elliptic curve cryptography. While enabling intermediate nodes to do authentication, this scheme allows any node to transmit an unlimited number of messages without the problem of threshold. In this a source anonymous message authentication code (SAMAC) on elliptic curves that provides unconditional source anonymity through node by node message authentication scheme. In order to evaluate the existing message authentication, SAMAC acts resilient to both active and passive attack.

III. RELATED WORK

In the existing system, hash based and symmetric key authentication schemes were proposed for WSNs. In this scheme, each symmetric authentication key is shared by a group of nodes. An attacker can compromise the key by attacking a single sensor node. Therefore, this scheme is not resilient to node compromise attacks. Another scheme is symmetric-key scheme which requires synchronization among nodes. This scheme, including TESLA and its variants 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.

A secret polynomial based message authentication scheme was introduced in this system. This scheme offers information-theoretic security with ideas similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken. To increase the threshold and the complexity for the attacker to reconstruct the secret polynomial, a random noise, called as perturbation factor is added to the polynomial in the system to thwart the adversary from computing the coefficient of the polynomial. The added perturbation factor is completely removed using error-correcting code techniques.

For the public-key based approach, 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. The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience, since public-key based approaches have a simple and clean key management.

The existing anonymous communication protocols are largely stemmed from either mix net or DC-net. A mix net provides anonymity via packet re-shuffling through a set of mix servers. In the mix net, the sender encrypts the outgoing message, and the ID of the receiver, using the public key of the mix. The mix accumulates a batch of encrypted messages, decrypts and re-orders the messages, and forwards them to the receiver. Since mix net-like protocols rely on the statistical properties of the background traffic, mix-net cannot provide provable anonymity. DC-net is an anonymous multi-party computation scheme. Some pairs of the participants are required to share secret keys. DC-net provides perfect source anonymity without requiring trusted servers. However, in DC-net, only one user can send at a time, so it takes additional bandwidth to handle collision and contention.

IV. ALGORITHMS

A. Generation of HMAC

The keyed hash message authentication code (HMAC) is a specific technique for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with the secret cryptographic key. With any MAC, it is used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as SHA1 is used in the calculation of an HMAC,

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 5, May 2015)

the resulting MAC algorithm is termed as HMACSHA1.It is calculated as shown. We use either i-padding or o-padding.

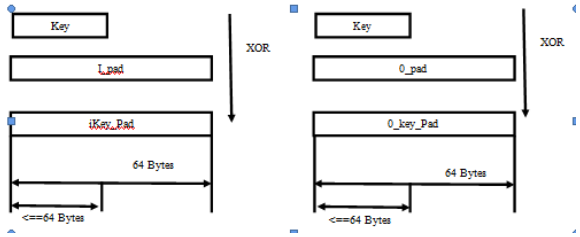

Figure 2: Generation of Hmac.

B. SAMA

The SAMA consists of the following algorithm. Generating (m,Q1,Q2,….Qn) :the given massage m and public keys Q1,Q2…Qn of AS S={A1,A2,…An}, the massage sender At,1<=t<=n, generates the anonymous massage S(m) using its own private key dt. The S(m) includes public key of all members in AS, the verifier determines ehether S(m) is generated by a member of AS or not.

C. Modified Elgamal Signature Scheme

The modified elgamal signature scheme consist of three algorithms

- Generation of key: let p be the prime and g be the generator of Zp. Here both p and g are public.For a private key x ,if it belongs to Zp, then the public key y is computed by $y=g^x \text{mod} p$.
- Generation of signature : For the massage m, choose a random k belongs Z_{p-1} and calculate $r = g^k \text{mod } p$ and solve for s, h is HMAC.

  $S=rxh(m,r)+k \text{ mod } (p-1)$
- The signature is defined by (r,s)
- Algorithm for verification: the verifier checks whether $g^x = ry^{rh(m,r)} \text{mod } p$. If equality is true, then the verifier accepts the signature, else rejects.

V. IMPLIMENTATION

The implementation procedure includes the following steps

A. Node Deployment

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

B. SAMA Message authentication

The message receiver should be able to verify whether a received message is sent 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.

C. Hop-by-hop message authentication

Every intermediate node on the routing path should be able to verify the authenticity and integrity of the messages upon receiving. This is done by the verification of public key. ACK is replied to previous node if authentication is successful.

D. Compromised Node Detection Process

If a message is received by the sink node, the message source is hidden in an AS. Since the SAMA scheme guarantees that the message integrity is unhampered, when a corrupted or meaningless message is received by the sink node, the source node is viewed as compromised. If the compromised source node transmits only one message, it will be very difficult for the node to be identified without the help of additional network traffic information. When a compromised node transmits more than one message, the sink node can narrow the possible compromised nodes down to a very small set.Key server management. Key server is a certificate authority server, which is responsible for message authentication. The key server verifies the information and authenticates the user. This is a kind of data encryption and decryption process. It is achieved through diffie Hellman key exchange algorithm.

VI. CONCLUSION

In this paper, It proposed a novel and an efficient source anonymous message authentication (SAMA) scheme based on elliptic curve cryptography (ECC). It ensures message sender privacy, SAMA scheme can be applied to any message to provide message content authenticity. To provide node-by-node message authentication without the problem of the built in threshold of the polynomial-based scheme, propose a node-by-node message authentication method based on the SAMA. We also discussed possible techniques for compromised node identification. This proposed scheme is more efficient than the bivariate 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,” in IEEE INFOCOM, March 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,” in IEEE Symposium on 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,” in Advances in Cryptology - Crypto’92, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[4] W. Zhang, N. Subramanian, and G. Wang, “Lightweight and compromiseresilient message authentication in sensor networks,” in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[5] A. Perrig, R. Canetti, J. Tygar, and D. Song, “Efficient authentication and signing of multicast streams over lossy channels,” in IEEE Symposium on Security and Privacy, May 2000.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009.

[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications. of the Assoc.of Comp. Mach., vol. 21, no. 2, pp. 120–126, 1978.

[8] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory,vol. 31, no. 4, pp. 469–472, 1985.

[9] 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," in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[10] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 1070, 1996, pp. 387–398.

[11] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84–88, February 1981.

[12] A. Pfitzmann and M. Waidner, "Networks without user observability–design options." in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 219, 1985, pp. 245–253.