International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 02.02.2018 Published : 28.02.2018

MESSAGE VERIFICATION AND SOURCE PRIVACY IN WSN

R.SathiyaPriya, R.Priyanka, K.Lalitha
Department of Computer Science and Engineering
Dhanalakshmi Srinivasan Institute of Technology, Samayapuram, T.N, India

ABSTRACT

The efficient message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks. For this reason, many message authentication schemes have been developed, based on either symmetric key cryptosystems or parallel cryptosystems. Most of them, however, have the limitations of high complex and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To solve these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial based scheme: when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial. In this paper, we propose a scalable authentication scheme based on elliptic curve cryptography. While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, our scheme can also provide message source privacy.

KEYWORDS: Message Verification, Source Anonymity, Signature-Based Scheme, Multiple Authentication Code Based Scheme, Wireless Sensor Networks.

INTRODUCTION

The recent progress on elliptic curve cryptography (ECC) shows that the public key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience since public-key based approaches have a simple and clean key management. In this project propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified Elgamal signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive chosen message attacks in the random oracle model. 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. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Every forwarder on the routing path should be able to verify the authenticity and

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 24.02.2018 Published : 27.02.2018

integrity of the messages upon reception. In this project propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, this scheme can also provide message source privacy. Both theoretical analysis and simulation results demonstrate that proposed scheme is more efficient than the polynomial-based approach in terms of computational and communication overhead under comparable security levels while providing message source privacy. Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless sensor networks (WSNs). These schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. The symmetric-key based approach requires 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 shared key is used by the sender to generate a message authentication code (MAC) for each transmitted message. However, for this method, the authenticity and 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 intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks.

To solve the scalability problem, a secret polynomial based message authentication scheme was introduced. The idea of this scheme is similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. This approach offers information-theoretic security of the shared secret key when the number of messages transmitted is less than the threshold. The intermediate nodes verify the authenticity of the message through a 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. An alternative solution was proposed in to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial. The idea is to add random noise, also called a perturbation factor, to the polynomial so that the coefficients of the polynomial cannot be easily solved. However, a recent study shows that random noise can be completely removed from the polynomial 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. One of the limitations of the public-key based scheme is the high computational overhead. The recent progress on elliptic curve cryptography (ECC) shows that the public key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience since public-key based approaches have a simple and clean key management. The rest of this paper is organized as follows: Section 2 discusses the related work, with a focus on polynomial-based schemes. Section 3 describes the system model. Section 4 describes an overview of the proposed scheme. Key management and

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 24.02.2018 Published : 27.02.2018

compromised node detection are provided in Section 5.Performance Analysis described in Section 6. We conclude in Section 7.

II RELATED WORK

In [1], [2], symmetric key and hash-based authentication schemes were proposed for WSNs. 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 [5] 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 a delay in message authentication and the delay increases as the network scale-up.

A secret polynomial based message authentication scheme was introduced in [3]. 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 intruder to reconstruct the secret polynomial, a random noise, also called a perturbation factor, was added to the polynomial in [4] to thwart the adversary from computing the coefficient of the polynomial. However, the added perturbation factor can be completely removed using error-correcting code techniques [6].

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 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 [9]. The existing anonymous communication protocols are largely stemmed from either mixnet [11] or DC-net [12]. A mixnet provides anonymity via packet re-shuffling through a set of mix servers (with at least one being trusted). In a mixnet, a sender encrypts an outgoing message, and the ID of the recipient, using the public key of the mix. The mix accumulates a batch of encrypted messages, decrypts and reorders these messages, and forwards them to the recipients. Since mixnet-like protocols rely on the statistical properties of the background traffic, they cannot provide provable anonymity. DC-net [12], is an anonymous multi-party computation scheme. Some pairs of participants are required to share

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 24.02.2018 Published : 27.02.2018

secret keys. DC-net provides perfect (information-theoretic) sender 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. Recently, message sender anonymity based on ring signatures was introduced. This approach enables the message sender to generate a source anonymous message.

III SYSTEM MODEL

In this section, we present the system model, the wireless sensor networks are assumed to consist of a large number of sensor hop nodes. Assume that each sensor hop node knows its relative location in the sensor domain and is capable of communicating with its neighbouring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. Assume there is a security service 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 SAMA, MES, and Public Key Cryptographic Systems.

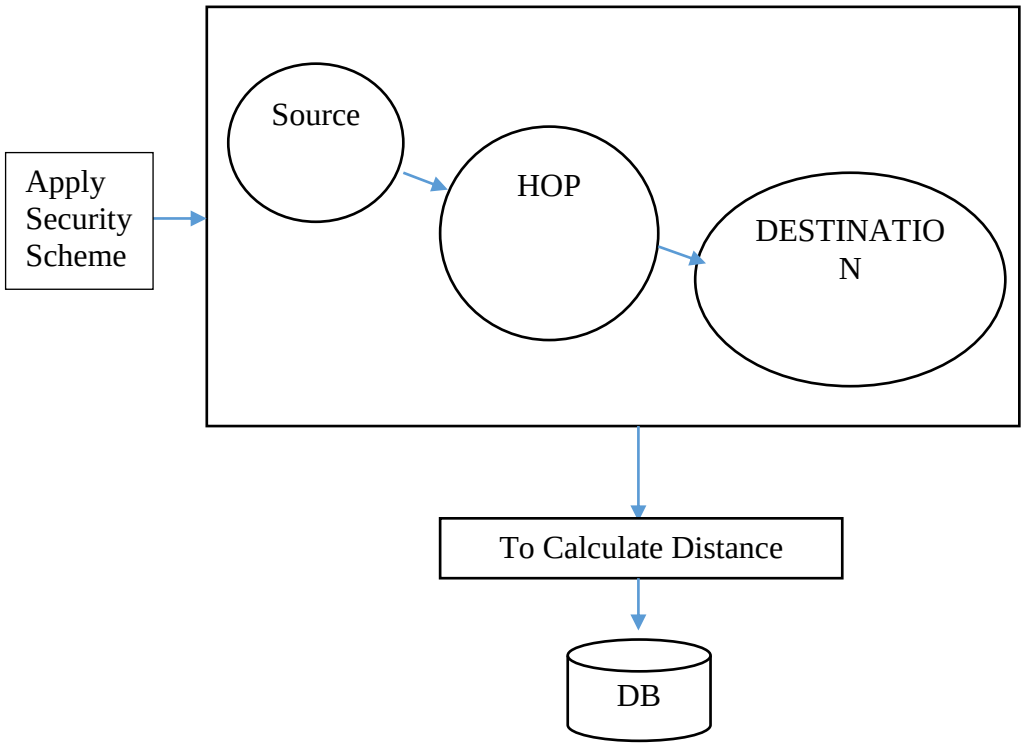

Fig. 1 : System Diagram

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 24.02.2018 Published : 27.02.2018

IV PROPOSED SCHEMES OVERVIEW

Our scheme involves the following six phases:

1. In the Node Deployment phase, an inquiry node to register the personal information, after to verify and confirm, after to continue the login process.

2. In the Source Anonymous Message Authentication Phase, using an unconditionally secure and efficient source anonymous message authentication scheme (SAMA). The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m.

3. In the Modified ElGamal Signature (MES) phase, the optimal Modified Elgamal Signature (MES) scheme on elliptic curves. This MES scheme is to generate signature dynamically and then, This MES scheme is secure against adaptive chosen-message attacks in the random oracle model. 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.

4. In the Crypto System Encryption phase, assume that all sensor information will be delivered to a sink node, which can be co-located with the SS. When 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 untampered when a bad or meaningless message is received by the sink node, the source node is viewed as compromised.

5. In the Packet Arrivalling Performance Using Doomsday Algorithm, efficiently to make and monitoring packet arriving performance, these packet arriving performance at each and every round of the packet.

6. To Improve Sending Packet Ratio Speed involves, transmission size, bandwidth could be a limiting factor. Data compression can be used to reduce the amount of data to be transmitted. Displaying a picture or image can result in transmitting tens of thousands of bytes (48K in this case) compared with transmitting six bytes. Finally, this contribution efficiently improves Sending packet speed.

V KEY MANAGEMENT AND COMPROMISED NODE DETECTION

A) Key Management Key management is one of the major issues for secret-key based authentication schemes. It is especially true for large scale WSNs. These schemes are provided node authentication, they can only provide end-to-end node authentication using the secret key shared between the two nodes, which implies that only the receiver can verify the authenticity of the messages enroot. In addition to performance-improvement, enabling intermediate node

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 24.02.2018 Published : 27.02.2018

authentication to provide hop-by-hop intermediate node authentication is an important research task.

B) Compromised Node Detection When a message is received by the sink node, the source is hidden in an AS. Since the SAMA scheme guarantees that the message integrity is untampered when a bad or meaningless message is received by the sink node, the source node is viewed as compromised. If the compromised source node only transmits one message, it would be very difficult for the node to be identified without additional network traffic information.

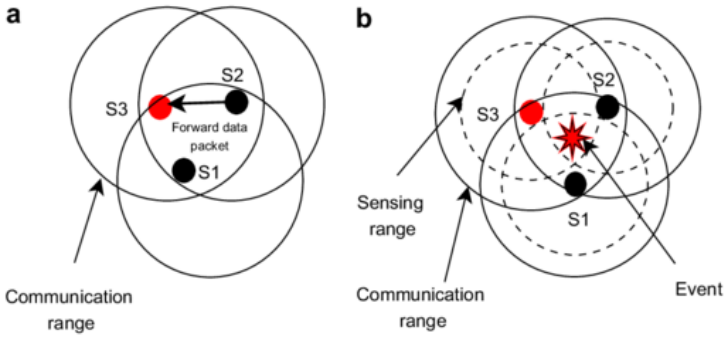

Figure 2: Compromised Node Detection

VI PERFORMANCE ANALYSIS

In this section, we will evaluate our proposed authentication scheme through both theoretical analysis and simulation demonstrations. We will compare our proposed scheme with the bivariate polynomial-based symmetric-key scheme described in [3], [4]. A fair comparison between our proposed scheme and the scheme proposed in [4] should be performed with n ¼ 1.

A) Theoretical Analysis

Key management is one of the major issues for secret-key based authentication schemes. This is especially true for large scale WSNs. While many of these schemes are designed to provide node authentication, they can only provide end-to-end node authentication using the secret key shared between the two nodes, which implies that only the receiver can verify the authenticity of the messages en route. This means that no intermediate node can authenticate the message in general. The intermediate nodes may have to forward a manipulated message for many hops before the message can finally be authenticated and dropped by the receiving node. This not only consumes extra sensor power but also increases the network collision and decreases the message delivery ratio.

In addition to performance-improvement, enabling intermediate node authentication will thwart adversaries from performing denial-of-service attacks through message manipulation to deplete

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 24.02.2018 Published : 27.02.2018

the energy and communication resources of the wireless network. Therefore, developing a protocol that can provide hop-by-hop intermediate node authentication is an important research task. The public-key based schemes were generally considered as not preferred, mainly due to their high computational overhead. However, our research demonstrates that it is not always true, especially for elliptic curve public-key cryptosystems.

In addition, in the bivariate polynomial-based scheme, there is only one base station that can send messages. All the other nodes can only act as intermediate nodes or receivers. This property makes the base station easy to attack and severely narrows the applicability of this scheme. In fact, the major traffic in WSNs is packet delivery from the sensor nodes to the sink node. In this scheme enables every node to transmit the message to the sink node as a message initiator. The recent progress on ECC has demonstrated that the public-key based schemes have more advantages in terms of memory usage, message complexity, and security resilience since public-key based approaches have a simple and clean key management [9].

B) Experimental Results

In this section, we implement the bivariate polynomial based scheme and our proposed scheme in a real-world comparison. The comparison is based on comparable security levels. The bivariate polynomial-based scheme is a symmetric key based implementation, while our scheme is based on ECC. This requires us to determine the comparable key sizes. If we choose the key size to be l for the symmetric key cryptosystem, then the key size for our proposed ECC should be 2l according to [22], which is much shorter than the traditional public-key cryptosystem. This progress facilitates the implementation of the authentication scheme using ECC.

In our simulation setting, we choose five security levels, which are indicated by the symmetric-key sizes l: 24, 32, 40, 64, and 80 bits, respectively. The comparable key sizes of our scheme are 48, 64, 80, 128, and 160 bits, respectively. We also need to determine dx and dy for the bivariate polynomial-based scheme, and the n for our scheme. In our simulation, we select dx equal tody and choose three values for them: 80, 100, and 150. We assume that WSNs do not contain more than 216 nodes in our simulation, which is reasonably large. For size n of the AS, we choose three values in the simulation: 10, 15 and 20. We will compare the computational overhead, communication overhead, delivery ratio, energy consumption, transmission delay, and memory consumption of our proposed scheme with the bivariate polynomial-based scheme. For a public-key based authentication scheme, the computational overhead is one of the most important performance measurements. So we first performed a simulation to measure the processing time. The simulations were carried out in 16-bit, 4MHz TelosB mote.

VII CONCLUSION

A Novel and efficient source anonymous message authentication scheme based on elliptic curve cryptography (ECC). While ensuring message sender privacy, SAMA can be applied to any

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018
Pages 95-102 | Cosmos Impact Factor (Germany): 5.195
Received: 24.02.2018 Published : 27.02.2018

message to provide message content authenticity. To provide hop-by-hop message authentication without the weakness of the Built-in the threshold of the polynomial based scheme, then propose a hop-by-hop message authentication scheme based on the SAMA.To improve the sending packet ratio speed and to maintain packet delivery timing accuracy, finally to reduce packet delay performance. The scheme has very limited flexibility and very high complexity.

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] W.Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, 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] 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. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.
[7] A.Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology," http://dud.inf.tu-dresden.de/ literatureAnon_Terminology_v0.31.pdf, Feb. 2008.
[8] D.Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.
[9] K.Nyberg and R.A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem," Proc. Advances in Cryptology (EUROCRYPT), vol. 950, pp. 182-193, 1995.
[10] R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Advances in Cryptology (ASIACRYPT), 2001.
[11] M.Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. ACM First Conf.Computer and Comm. Security (CCS "93), pp. 62-73, 1993.
[12] L.Harn and Y. Xu, "Design of Generalized ElGamal Type Digital Signature Schemes Based on Discrete Logarithm," Electronics Letters, vol.30, no. 24, pp. 2025-2026, 1994