IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Hop-By-Hop Message Authentication and Source Privacy in Wireless Sensor Networks

Mrs.C.Theebendra[1], S.Prema[2]

Assistant Professor, Department of Computer Science,

Vivekanandha College of Arts and Sciences for Women(Autonomous) Elayampalayam, Tiruchengode, India[1]

Research Scholar, Department of Computer Science,

Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, India[2]

Abstract: Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address 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: when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial. In this project, propose a scalable authentication scheme based on elliptic curve cryptography (ECC). 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. Both theoretical analysis and simulation results demonstrate that our 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.

Keywords: Hop by Hop authentication, Wireless Sensor Networks.

I. INTRODUCTION

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 in. 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 a 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 the 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. In this paper, we 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

Copyright to IJARCCE

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

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 (SAMAC) on elliptic curves that can provide unconditional source anonymity.
2.We offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation.
3. We devise network implementation criteria on source node privacy protection in WSNs.
4. We propose an efficient key management framework to ensure isolation of the compromised nodes.
5. We provide extensive simulation results under ns-2 and TelosB on multiple security levels. To the best of our knowledge, this is the first scheme that provides hop-by-hop node authentication without the threshold limitation, and has performance better than the symmetric-key based schemes. The distributed nature ofour algorithm makes the scheme suitable for decentralized networks.

II. TERMINOLOGY AND PRELIMINARY

We will briefly describe the terminology and the cryptographic tools that will be used in this.

2.1Terminology

Privacy is sometimes referred to as anonymity. Communication anonymity in information management has been discussed in a number of previous works. It generally refers to the state of being unidentifiable within a set of subjects. This set is called the AS. Sender anonymity means that a particular message is not linkable to any sender, and no message is linkable to a particular sender.

We will start with the definition of the unconditionally secure SAMA.

A SAMA consists of the following two algorithms:

Generate (m; Q1; Q2; . . . ; Qn). Given a message m and the public keys Q1; Q2; . . . ; Qn of the AS S ¼ fA1; A2; . . . ; Ang, the actual message sender At; 1 _ t _ n, produces an anonymous message Some using its own private key dt.

At; 1_ t _ n, produces an anonymous message Some using its own private key dt.

Given a message m and an anonymous message Same, which includes the public keys of all members in the AS, a verifier can determine whether Some is generated by a member in the AS. The security requirements for SAMA include:

Sender ambiguity. 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 AS.

Unforgetability. An anonymous message scheme is unforgetable if no adversary, given the public keys of all members of the AS and the anonymous messages m_1; m_2; . . . ; m_n adaptively chosen by the adversary, can produce in polynomial time a new valid anony-mous message with non-negligible probability.

III. RELATED WORK

In, 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 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. A secret polynomial based message authentication scheme was introduced in.

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 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. 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. The existing anonymous communication protocols are largely stemmed from either mixnet or DC-net. 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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

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.

IV. PROBLEM STATEMENT

A. *Exiting Model*

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.Computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management.

Disadvantages:High computational and communication overhead.Lack of scalability and resilience to node compromise attacks.Polynomial-based scheme have the weakness of a built-in threshold determined by the degree of the polynomial.

B. Proposed System

We propose an unconditionally secure and efficient 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.The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS.In our scheme, the entire SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA alike. In addition, our design enables the SAMA to be verified through a single equation without individually verifying the signatures.

Advantages:

A novel and efficient SAMA based on 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 built- in threshold of the polynomial-based scheme, we then proposed 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.

V. SERVER CLIENT MODULE

Client – Server computing is distributed access. Server accepts requests for data from client and returns the result to the client. By separating data from the computation processing, the compute server's processing capabilities can be optimized. Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system.

VI. KEY MANAGEMENT AND DEFINITION

In our scheme, we assume that there is an SS whose responsibilities include public-key storage and distribution in the WSNs. We assume that the SS will never be compromised. However, after deployment, the sensor node may be captured and compromised by the attackers. Once compromised, all information stored in the sensor node will be accessible to the attackers. We further assume that the compromised node will not be able to create new public keys that can be accepted by the SS. For efficiency, each public key will have a short identity. The length of the identity is based on the scale of the WSNs.

VII. SYMMETRIC KEY AND CRYPTOSYSTEM

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.

VIII. PUBLIC-KEY CRYPTOSYSTEM

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 [7], [8]. 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.

IX. HOP-BY-HOP AUTHENTICATION

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.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

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 of both computational and communication overhead.

X. ANALYSIS AND EXPERIMENTAL RESULTS

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. A fair comparison between our proposed scheme and the scheme proposed in [4] should be performed with n ¼

The appropriate selection of an AS plays a key role in message source privacy, since the actual message source node will be hidden in the AS. In this section, we will discuss techniques that can prevent the adversaries from tracking the message source through the AS analysis in combination with local traffic analysis. Before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice. This set should include itself, together with some other nodes.

When an adversary receives a message, he can possibly find the direction of the previous hop, or even the real node of the previous hop. However, the adversary is unable to distinguish whether the previous node is the actual source node or simply a forwarder node if the adversary is unable to monitor the traffic of the previous hop. Therefore the selection of the AS should create sufficient diversity so that it is infeasible for the adversary to find the message source based on the selection of the AS itself.

Some basic criteria for the selection of the AS can be described as follows: To provide message source privacy, the message source needs to select the AS to include nodes from all directions of the source node. In particular, the AS should include nodes from the opposite direction of the successor node. In this way, even the immediate successor node will not be able to distinguish the message source node from the forwarder based on the message that it receives.

Though the message source node can select any node in the AS, some nodes in the AS may not be able to add any ambiguity to the message source node. For instance, the nodes that are apparently impossible or very unlikely to be included in the AS based on the geographic routing. Therefore, these nodes are not appropriate candidates for the AS. They should be excluded from the AS for energy efficiency.

To balance the source privacy and efficiency, we should try to select the nodes to be within a predefined distance range from the routing path. We recommend selecting an AS from the nodes in a band that covers the active routing path. However, the ASdoes not have to include all the nodes in the routing path.The AS does not have to include all nodes in that range, nor does it have to include all the nodes in the active routing path. In fact, if all nodes are included in the AS, then this may help the adversary to identity the possible routing path and find the source node.

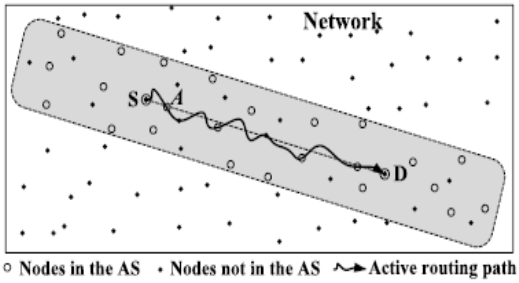

Fig 1Anonymous set selection in active routing.

As an example, suppose we want to transmit a packet from source node S to destination node D in Fig. 1. We select the AS to include only nodes marked with , while nodes marked as will not be included in the AS. Of all these nodes, some of them are on the active routing path while others are not. However, all these nodes are located within the shaded band area surrounding the active routing path. Suppose node A is compromised, unless node A collaborates with other nodes and can fully monitor the traffic of the source node S, it will not be able to determine whether S is the source node, or simply a forwarder. Similar analysis is also true for other nodes. Any node in the active routing path can verify the contents' authenticity and integrity. However, anybody who receives a packet in the transmission can possibly exclude some of the nodes in the WSNs as the possible source node. Inclusion of these nodes in the AS will not increase the source privacy. Nevertheless, the more the nodes included in the AS are, the higher the energy cost will be.

Therefore, the selection of the AS has to be done with care so that the energy cost and the source privacy can both be optimized. In addition, to balance the power consumption between authenticity and integrity verification, and the possibility that corrupted messages are being forwarded, the verification service may not have to take place in every hop; instead, it may be configured to take place in every other hop, for instance.

As a special scenario, we assume that all sensor information will be delivered to a sink node, which can be collocated with the SS. As described in Section 5, 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. 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.

DOI 10.17148/IJARCCE.2016.5251

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

However, when a compromised node transmits more than one message, the sink node can narrow the possible compromised nodes down to a very small set. As shown in Fig. 2, we use the circle to represent an AS. When only one message is transmitted, the sink node can only obtain the information that the source node will be in a set, say AS1. When the compromised source node transmits two messages, the sink node will be able to narrow the source node down to the set with both vertical lines and horizontal lines. When the compromised source node transmits three messages, the source node will be further narrowed down to the shaded area. Therefore, if the sink node keeps tracking the compromised message, there is a high probability that the compromised node can be isolated.

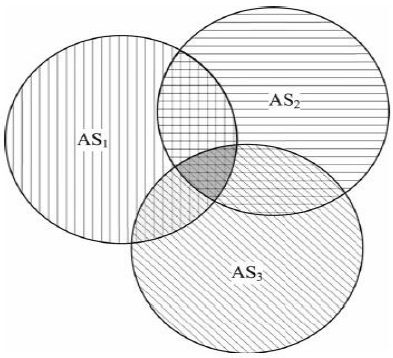

Fig. 2. Compromised node detection.

XI. CONCLUSION

In this project, we first proposed a novel and efficient SAMA based on 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 built in threshold of the polynomial-based scheme, we then proposed 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 bivariate polynomial-based scheme through simulations using ns-2 and TelosB. Both theoretical and simulation results show that, in comparable scenarios, our 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] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.
[2] "Cryptographic Key Length Recommendation," http://www.keylength.com/en/3/, 2013.
[3] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.
[4] 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.

BIOGRAPHIES

Mrs.C.THEEBENDRA Assistant Professor, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women(Autonomous)Elayampalayam, Tiruchengode.

S.PREMA Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous) Elayampalayam, Tiruchengode.