International Journal of Advance Research and Innovation
Vol. 3(2), Apr-Jun 2015, pp. 49-53
Doi: 10.51976/ijari.321512

Article Info
Received: 05 Apr 2015 | Revised Submission: 30 Apr 2015 | Accepted: 20 May 2015 | Available Online: 15 Jun 2015

Effectively Secure Data Retrieving for Using Three Different Level Security

Sathiya Priya. R and V. Gokulakrishnan***

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.*

1.0 Introduction

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 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).

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.

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

**Corresponding Author: Department of Computer Science Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India (E-mail: sathyapriyacse89@gmail.com)*
***Department of Computer Science Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India*

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.

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 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.

Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). 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.

2.0 Related Work

2.1 Signature-based scheme

As the most natural approach, the public key cryptography may be applied to generate digital signatures for message authentication. However, adopting this approach to resource constrained wireless sensor networks may either (i) results in high computational cost or (ii) requires special hardware supports. proposed approach only involves simple arithmetic operations (i.e., polynomial evaluations over a finite field) and low-cost hash functions; hence, it has much lower overhead (i.e., a few milliseconds in authentication and tens of milliseconds in verification).

2.2 Multiple authentication code-based scheme

Some researchers proposed to use hash functions to produce multiple authentication codes to authenticate messages. These schemes are more efficient than the approach based on public key cryptography. However, because each secret key is shared by multiple nodes these schemes become ineffective or even useless if a large number of nodes are compromised. Moreover, these schemes cannot achieve non-repudiation. proposed approach is also computationally efficient. Different from these schemes, proposed approach can tolerate a large number of node compromises and can achieve non-repudiation. TESLA and its variants.

Assuming time synchronization among nodes as well as the sharing of initial secrets between authenticators and verifiers, the TESLA scheme and its variants can perform delayed authentication in the presence of a large number of colluding malicious nodes. In some scenarios, especially when the network size is large, it is hard to determine the bound of normal delay, and this can be exploited by the adversary to launch denial of service attacks. Moreover, these schemes repel asynchronous interaction between the source and the destination/verifier.

3.0 System Analysis

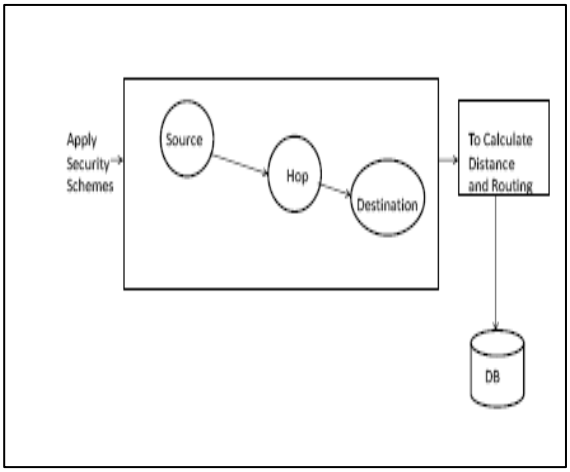
In this paper, propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise resiliency, flexible-time authentication and source identity protection, scheme does not have the threshold problem. Both theoretical analysis and simulation results demonstrate that proposed scheme is more efficient than the polynomial-based algorithms under comparable security levels.

The major contributions of this work are the following develop a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation. These device network implementation criteria on source node privacy protection in WSNs. propose an efficient key management framework to ensure isolation of the compromised nodes. In this provide extensive simulation results under ns-2 and TELOSB on multiple security levels. To the best of the 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 of algorithm makes the scheme suitable for decentralized networks. This 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 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 at Hop-by-hop message authentication.

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 server 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 Architecture Diagram



3.1 Node deployment

Node Deployment is the first phase of the proposed system. In this phase used to register the personal information. After to verify and confirm the inquiry node continue the login process.

3.2 Source anonymous message authentication (SAMA)

In this method for using an unconditionally secure and efficient source (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.

3.3 Modified ElGamal signature (MES)

The optimal Modified Elgamal Signature (MES) scheme applied on elliptic curves. This MES scheme is to generatesignature 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 sothat all corrupted message can be detected and dropped to conserve the sensor power.

3.4 Crypto system encryption scheme

In this scheme, 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 un tampered, when a bad or meaningless message is received by the sink node, the source node is viewed as compromised.

3.5 Packet arrival performance using doomsday algorithm

In this method using Doomsday Algorithm efficiently to make and monitoring packet arrival performance, these packet arrival performance at each and every round of the packet. Doomsday calculation is effectively calculating the number of days between any given date in the base year and the same date in the current year, and then taking the remainder modulo 7.

When both dates come after the leap day (if any), the difference is just 365y plus y/4. Doomsday algorithm is a way of calculating the day of the week of a given date. It provides a perpetual calendar because the Gregorian calendar moves in cycles of 400.

3.6 To improve sending packet ratio speed

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 coefficiently improve Sending packet speed.

4.0 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 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, 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] M. Albrecht, C. Gentry, S. Halevi, J. Katz, Attacking Cryptographic Schemes Based on ‘Perturbation Polynomials, 2009, http://eprint.iacr.org/.

[2] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, Perfectly-Secure Key Distribution for Dynamic Conferences, Advances in Cryptology (Crypto ’92), 1992, 471-486

[3] D. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Comm. ACM, 24(2), 1981, 84-88

[4] D. Chaum, The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability, J. Cryptology, 1(1), 1988, 65-75

[5] T. A. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. Information Theory, IT-31(4), 1985, 469-472

[6] L. Harn, Y. Xu, Design of Generalized ElGamal Type Digital Signature Schemes Based on Discrete Logarithm, Electronics Letters, 30(24), 2025-2026

[7] K. Nyberg, R. A. Rueppel, Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem, Advances in Cryptology (EUROCRYPT), 950, 1995, 182-193

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

[9] A. Pfitzmann, M. Hansen, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology, http://dud.inf.tu dresden.de/literature/Anon_ Terminology_v0.31.pdf, 2008

[10] A. Pfitzmann, M. Waidner, Networks without User Observability—Design Options, Advances in Cryptology (EUROCRYPT), 219, 1985, 245-253

[11] D. Pointcheval, J. Stern, Security Proofs for Signature Schemes, Advances in Cryptology (EUROCRYPT), 387-398

[12] D. Pointcheval, J. Stern, Security Arguments for Digital Signatures and Blind Signatures, J. Cryptology, 13(3), 2000, 361- 396

[13] M. Reiter, A. Rubin, Crowds: Anonymity for Web Transaction, ACM Trans. Information and System Security, 1(1), 1998, 66-92

[14] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Comm. ACM, 21(2), 1978, 120-126

[15] R. Rivest, A. Shamir, Y. Tauman, How to Leak a Secret, Advances in Cryptology (ASIACRYPT), 2001

[16] M. Waidner, Unconditional Sender and Recipient Untraceability in Spite of Active Attacks, Advances in Cryptology (EUROCRYPT), 1989, 302-319

[17] H. Wang, S. Sheng, C. Tan, 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), 11-18

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

[19] W. Zhang, N. Subramanian, G. Wang, Lightweight and Compromise-Resilient Message Authentication in Sensor Networks, IEEE INFOCOM, 2008

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