ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient Approach for Node-to-Node Message Authentication and Source Privacy in WSN's

Swetha.N
M.Tech Student,
Department of Computer Science and Engineering,
Kuppam Engineering College,
Kuppam-517 425, A.P, India.

A.Anantha Bipin
Assistant Professor,
Department of Computer Science and Engineering,
Kuppam Engineering College,
Kuppam-517 425, A.P, India.

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 paper, we 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, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, wireless sensor networks (WSNs), distributed algorithm, decentralized control.

1. 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. 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 to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.The major contributions of this paper are the following:

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

2. EXISTING SYSTEM :

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 OF EXISTING SYSTEM:

•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.

3. 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.

3.1.PROPOSED SYSTEM ARCHITECTURE:

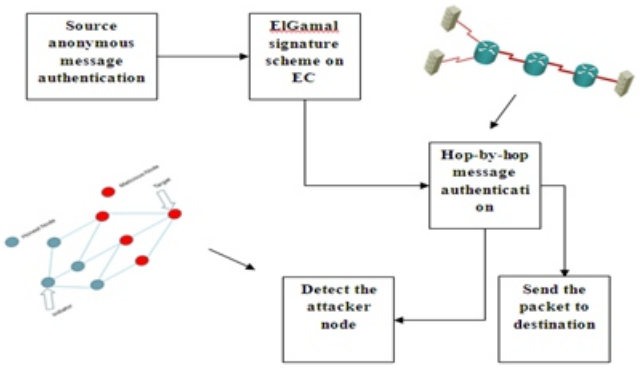

Fig-1: Architecture of Proposed system

ADVANTAGES OF PROPOSED SYSTEM:

» 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

4.IMPLEMENTATION OF PROPOSED SYSTEM:

The framework of our proposed system has the accompanying modules alongside the following prerequisites.

•Network Configuration
•Source Anonymous Message Authentication (SAMA)

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•Hop-by-hop message authentication
•Performance Evaluation

Network Configuration:

Sensor nodes are randomly distributed in the sensing field. In this project we are using wireless sensor network. In this network, the nodes are static and fixed. The sensor nodes are sense the information and then send to the server. If the source node sends the packet, it will send through the intermediate node. The nodes are communicates only within the communication range. So, we have to find the node's communication range.

Source Anonymous Message Authentication (SAMA):

In this project, we propose the Source Anonymous Message Authentication scheme (SAMA) for secure message sending. The proposed scheme allows any node to transmit an unlimited number of messages without suffering from threshold problem.

We are using ElGamal signature for message authentication. In this scheme enables the nodes to authenticate the message so that all corrupted message can be detected and dropped. We develop the SAMA code on elliptic curves that can provide unconditional source anonymity. We propose an efficient key management framework to ensure isolation of the compromised nodes.

Hop-by-Hop Message Authentication:

In this project, we also propose hop-by-hop message authentication scheme for protect the data. We are using ElGmal signature for message authenticate. Along this signature we can provide the secure for data packet and also using the signature we can detect the adversaries. The message receiver should be able to verify whether the message sent by the authorized node and also verify the message has been modified by the adversaries.

Every forwarder can verify the message is authenticated or not. If the forwarder detect the intruder or find the message has been modified, forwarder will drop the packet or change the routing path. Along this proposed scheme, we can get accurate data without modifying and also can easily detect the adversaries.

Performance Evaluation:

In this section, we can evaluate the performance of simulation. We are using the xgraph for evaluate the performance. We use some evaluation metrics: Packet delivery ratio – it is the ratio of the number of packet received at destination and number of packet sent by the source, End-to-End delay - the average time taken for a packet to be transmitted from source to destination, Energy level – number of energy consumed when the data should be transmitted.

5. CONCLUSION:

In this paper, 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] 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

[5] 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.

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

[7] 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.

[8] 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.

[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," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

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

[11] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.

[12] D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

[13] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology," http://dud.inf.tu-dresden.de/ literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.

[14] A. Pfitzmann and M. Waidner, "Networks without User Observability— Design Options.," Proc. Advances in Cryptology (EUROCRYPT), vol. 219, pp. 245-253, 1985.

[15] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transaction," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

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

[17] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361- 396, 2000.

[18] 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.

[19] 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.

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