ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 2 February 2015, Page No. 10485-10488

Efficient Validation and Source Aloofness in Wireless Sensor Networks

Priya.G.S[1], Muthulakshmi.B[2]

[1]Post Graduate Student, Department of Computer Science Engineering
A.V.C. College Of Engineering, Tamil Nadu, India
Priya2421@gmail.com

[2]Assistant Professor, Department Of Computer Science Engineering
A.V.C. College Of Engineering, Tamil Nadu, India
Kavithakamalan240101@gmail.com

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 key management techniques have been developed for message authentication, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of the authentication schemes have the limitations of security, in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. The polynomial schemes have the weekness to build in threshold value determined by the degree of the polynomial. In the proposed system, a scalable authentication scheme is SAMA based Modified Elgamal Signature (MES). It enabling intermediate nodes authentication and 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.***

Keywords: ***Hop-by-Hop authentication, source privacy, simulation, distributed algorithms, Wireless sensor Networks (WSN), decentralized control.***

1. Introduction

Message authentication plays a major role in prevent the message from unauthorized access in the wireless sensor networks. For this reason many authentication scheme have been developed, these schemes can divided into two categories: public-key cryptosystems and symmetric-key cryptosystems. The symmetric-key based approach sender, receiver and intermediate node share the common key. So the key management is not secure in the symmetric-key based approach. The shared key is used by the sender to generate a message authentication code (MAC) for each forwarded message. So the intruder can compromise the key by compromising the single node in the sensor network. In addition, this symmetric-key cryptosystems is not safe for large scale sensor networks. In the public-key cryptosystems, each message is forwarded along with the message signature of the transmitted message generated using the source private key. Each intermediate node and the final receiver can authenticate the message using the source public key. The proposed system is implemented by public-key cryptosystem. It has more advantages in terms of security, memory usage, and security resilience, since public-key based approaches have simple and clean key management. In the proposed system a scalable secure and efficient source anonymous message authentication (SAMA) based on Modified ElGamal Signature (MES) schemes on elliptic curves. This MES scheme is secure against adaptive chosen-message so that all corrupted message can be detected and dropped to conserve the sensor power. So the proposed system provides intermediate node security, in addition this scheme can also provide message source privacy.

2. Existing System

A polynomial based message authentication scheme was used in the existing system for message authentication. This scheme is similar to a threshold secret sharing, where the threshold is found by the degree of the polynomial. This approach offers security of the shared secret key when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken. The key management also not secure in this system, intermediate node authentication also not available in this system and it is not a scalable authentication scheme.

3. Planned System

A proposed system is the scalable secure and efficient source anonymous message authentication (SAMA) scheme based on the Modified ElGamal Signature (MES) scheme on ECC. By using SAMA source privacy is provided. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor node. Each and every intermediate node check the message authentication code (MAC) with source private key. The intermediate node authentication is mainly focused in the proposed system. In

addition, it can also provide message source privacy by using SAMA.

3.1 Planned System Technique

The wireless sensor networks are assumed to consist of a large number of sensor nodes.

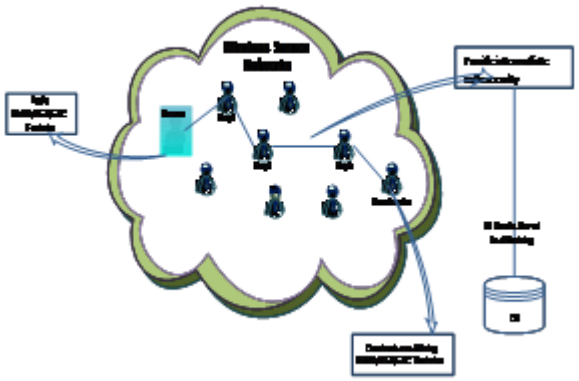

Figure1. The Planned Framework

Fig.1. shows the proposed system framework. Assume that there is a source is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised, because that the source is hidden from sensor network by using SAMA algorithm. In addition, intermediate node authentication also available by using optimal MES algorithm.

4. Implementation

4.1 Creation Of Nodes

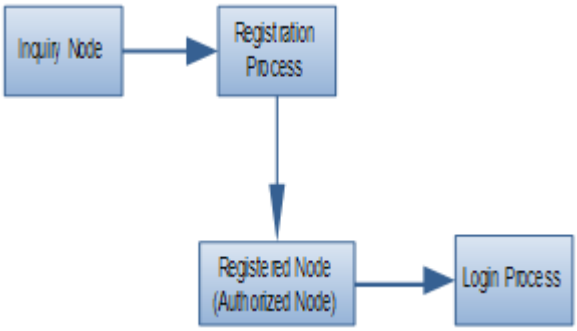

Figure2. Creation Of Nodes

Each and every message transferred node register the personal information with the security server. Fig.2 shows is a node creation process diagram. Every node verify with the security server. After to verification and confirmation the node will be created. Each and every hop verify with the security server during the message transformation. so the authorized node only can transmit the message to the next node.

4.2 Source Anonymous Message Authentication

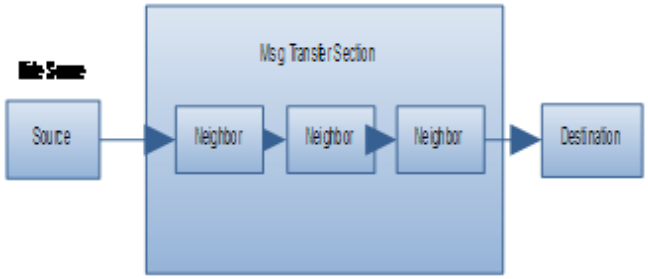

Figure.3.Source Anonymous Message Authentication

The fig.3 shows is a Source Anonymous Message Authentication(SAMA) The main idea is that for each message is send from the source, so using the SAMA provide hidden security for source .here source is hidden from the all those node from the network. So the message is kept secret through by this security scheme.

4.3 Modified Elgamal Signature(MES)

The Fig.4 shows is an optimal modified Elgamal signature (MES) scheme on elliptic curves.

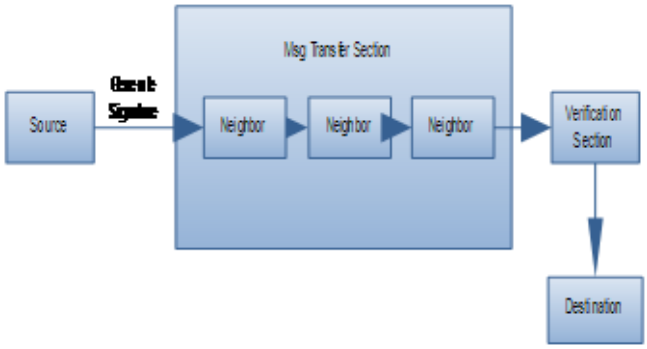

Figure.4.Modified Elgamal Signature

This MES scheme is to generate signature dynamically for intermediate node verification. Each and every intermediate node verify that message signature by the sender private key. This MES scheme is secure against intermediate node attacks in the Wireless Sensor Networks (WSN). This scheme enables the intermediate nodes to authenticate the message so that unauthenticated message can be detected and dropped in the network.

4.4 Compromised Node Detection

Compromised node detection is the important implementation system as shown in fig.5, when a message is received by the sink node, the message source is hidden by SAMA. Since the SAMA scheme guarantees that the message privacy, when a unauthorized message is received by the sink node, the source node is find through the security.

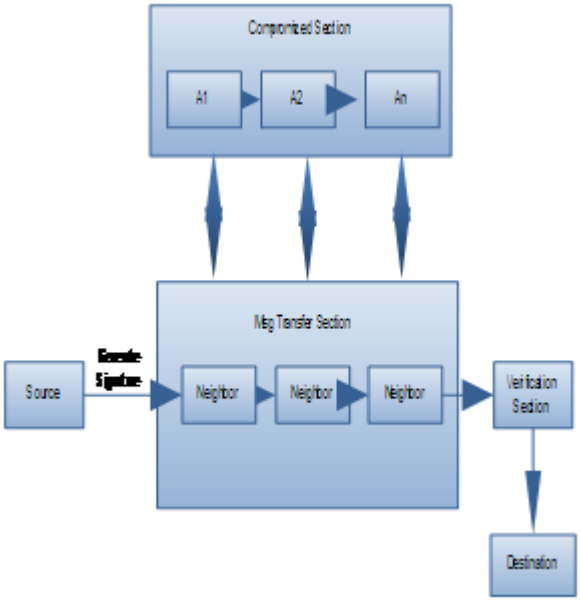

Figure.5.Compromised Node Detection

5. Performance Analysis

This proposed research work was implemented by NS2 Network Simulation Tool. Both theoretical and simulation results show that, the proposed scheme is more efficient than the existing system in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

5.1 Theoretical Analysis

Key management is one of the main issues for message authentication techniques. For this reason many of these schemes are designed to provide message authentication. In these shared key scheme sender and receiver only used those keys and receiver only aware about that message authentication. This means that no intermediate node can authenticate the message general. In the proposed system allows to intermediate node authentication by optimal MES scheme, and also provide message source privacy by SAMA algorithm. So the proposed system has demonstrated that the public-key based schemes have more advantages in terms of memory usage, message complexity, and security, since public-key based approaches have a simple and clean key management.

5.2 Implementation Results

Efficient message authentication scheme is evaluated the proposed systems algorithm by ns2 network simulator. Fig.6 and fig.7 shows packet delivery ratio and energy consumptions of the proposed method over other existing methods.

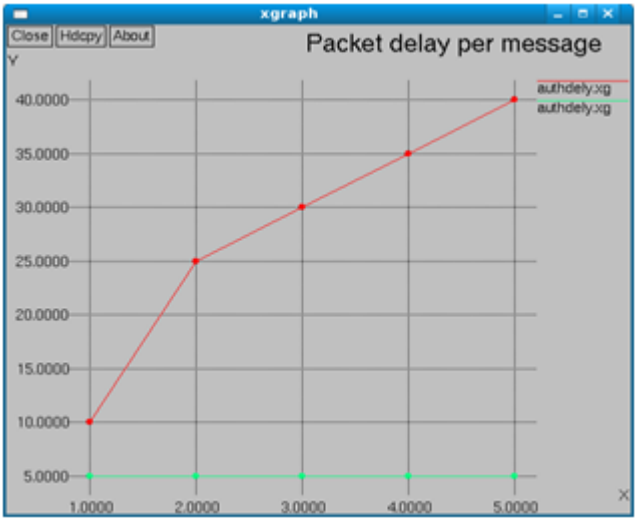

Figure.6. Packet Delivery Ratio

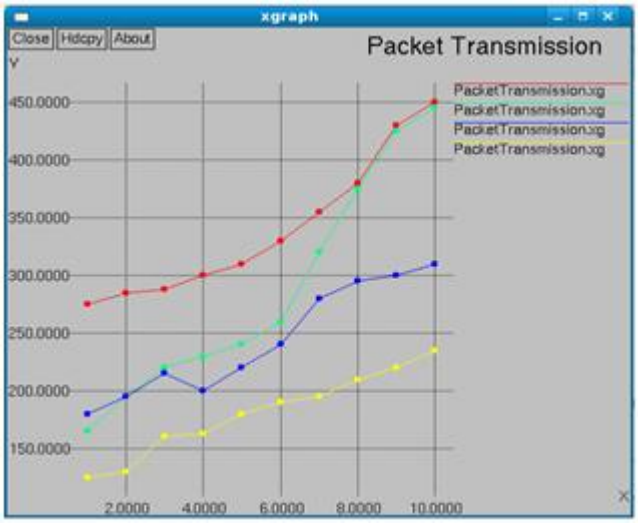

Figure.7.Energy Consumption

6. Conclusion

A novel and efficient SAMA based on ECC. While ensuring message sender privacy, SAMA can be applied to any message to provide message source privacy.amd also provide hop-by-hop authentication by using optimal MES. The efficiency of the proposed scheme can check through simulations using ns-2. Both theoretical and simulation results show that the proposed scheme is more efficient than the polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

REFERENCES

[1] Albrecht, M., Gentry, C., Halevi, S., & Katz, J. (2009, November). Attacking cryptographic schemes based on perturbation polynomials. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 1-10). ACM.s

[2] Bellare, M., &Rogaway, P. (1993, December). Random oracles are practical: A paradigm for designing efficient protocols. In Proceedings of the 1st ACM conference on

Computer and communications security (pp. 62-73).ACM.
[3] Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., & Yung, M. (1993, January). Perfectly-secure key distribution for dynamic conferences. InAdvances in cryptology—CRYPTO'92 (pp. 471-486).Springer Berlin Heidelberg.
[4] Chaum, D. (1988). The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of cryptology, 1(1), 65-75.
[5] Chaum, D. (2003). Untraceable electronic mail, return addresses and digital pseudonyms. In Secure Electronic Voting (pp. 211-219). Springer US.
[6] ElGamal, T. (1985, January). A public key cryptosystem and a signature scheme based on discrete logarithms.In Advances in Cryptology (pp. 10-18).Springer Berlin Heidelberg.
[7] Perrig, A., Canetti, R., Tygar, J. D., & Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels.In Security and Privacy, 2000.S&P 2000.Proceedings. 2000 IEEE Symposium on (pp. 56-73). IEEE.
[8] Pointcheval, D., & Stern, J. (1996, January). Security proofs for signature schemes. In Advances in Cryptology—EUROCRYPT'96 (pp. 387-398). Springer Berlin Heidelberg.
[9] Rivest, R. L., Shamir, A., &Adleman, L. (1983). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 26(1), 96-99.
[10] Wang, H., Sheng, B., Tan, C. C., & Li, Q. (2008, June). Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control. In Distributed Computing Systems, 2008.ICDCS'08. The 28th International Conference on (pp. 11-18). IEEE.
[11] Ye, F., Luo, H., Lu, S., & Zhang, L. (2005). Statistical en-route filtering of injected false data in sensor networks. Selected Areas in Communications, IEEE Journal on, 23(4), 839-850.
[12] Zhang, W., Subramanian, N., & Wang, G. (2008, April). Lightweight and compromise-resilient message authentication in sensor networks.In INFOCOM 2008.The 27th Conference on Computer Communications.IEEE.