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

Enabling Intermediate Nodes Authentication Scheme Based on Elliptic Curve Cryptography in Wireless Sensor Networks

Ms. Zohra Binte Sailan[1], Ms. Syeda Nusrath Fatima[2], Khaderbi Shaik [3]

[1]PG Scholar, Dept of CN, Shadan Womens College of Engineering and Technology, Hyderabad, TS, India.
[2]Assistant Professor, Department of CSE, Shadan Womens College of Engineering and Technology, Hyderabad, TS, India.
[3]HOD, Department of CN, Shadan Womens College of Engineering and Technology, Hyderabad, TS, India.

Abstract:

In hop by hop message authentication with source privacy in wireless sensor network, were authentication is effective way to protect from unauthorized users effected messages from being send through in wireless sensor networks. Many message authentication schemes have been used to protect messages but these authentication schemes have the limitations of high overhead, lack of ability, to node attacks and threshold problem. Message authentication has a main role in thwarting unauthorized and effected messages from being sent in networks to save the energy. Many authentication processes have been implemented to provide message authenticity and verification for wireless sensor networks. The symmetric-key based approach has complicated key management and lacks of ways. It is not taken to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The sender uses shared key to generate a message authentication code for each transmitted message. The authenticity and integrity of the message can verified only by the node using shared secret key, which is generally shared by a group of sensor nodes. An attacker can easily access the key by occupying a single sensor node. So, It will does not work in multicast networks. In order to solve the problem, Proposing a new Source Anonymous Message authentication (SAMA) is a scalable authentication scheme based on elliptic curve cryptography (ECC) is used to allow any node to transmit and authenticate an unlimited number of messages without suffering the threshold problem and provides message source privacy. In addition, our scheme can also provide message source privacy. The middle nodes verify the authenticity of the message. If the transmitted messages are larger than the threshold, can be fully recovered.

Keywords:

Hop by hop message Authentication, elliptic curve cryptography, WSN, SAMA, MES;

INTRODUCTION:

Wireless sensor networks:- Wireless sensor networks simplify the compilation and scrutiny of information from multiple locations. The term wireless sensor network (WSN) illustrates an association among miniaturized embedded communication devices that supervise and evaluate their surrounding environment. The network is composed of many minute nodes sometimes referred to as motes. A node is made up of the sensor(s), the microcontroller, the radio communication component, and a power source. Wireless sensor nodes range in size from a few millimeters to the size of a handheld computer. Apart from of size, sensor nodes share general constraints.

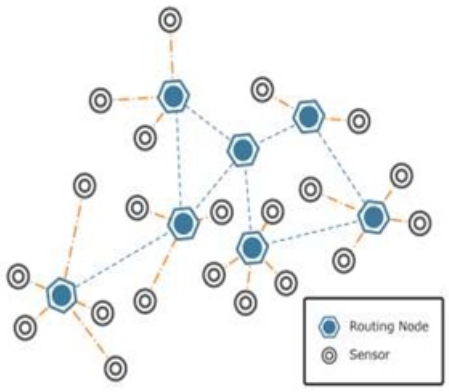

Fig: wireless sensor network environment.

In hop by hop message authentication with source privacy in wireless sensor network, were authentication is effective way to protect from unauthorized users effected messages from being send through in wireless sensor networks. Many message authentication schemes have been used to protect messages but these authentication schemes have the limitations of high overhead, lack of ability, to node attacks and threshold problem. Message authentication has a main role in thwarting unauthorized and effected messages from being sent in networks to save the energy. Many authentication processes have been implemented to provide message authenticity and verification for wireless sensor networks.

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

The symmetric key based approach has complicated key management and lacks of ways. It is not taken to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The sender uses shared key to generate a message authentication code for each transmitted message. The authenticity and integrity of message can verified only by the node using shared secret key, which is generally shared by a group of sensor nodes. An attacker can easily access the key by occupying a single sensor node. So, It will does not work in multicast networks. In order to solve the problem, a secret based for the message authentication scheme was introduced. The method is similar to a threshold secret sharing, where it is determined by the degree of the value. This offers information security of the shared secret key when the number of messages transmitted is less than the threshold. The middle nodes verify the authenticity of the message.

If the transmitted messages are larger than the threshold, can be fully recovered. For the public-key based method, each message is transmitted along with the digital signature of the message produced 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 restrictions of the public key based method is the high computational overhead. In this project we propose an unconditionally source anonymous g message authentication scheme (SAMA), which uses Modified New variant ElGamal signature Scheme (MNES).

This MNES scheme is secure against adaptive chosen-message attacks in the random oracle model . 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 the proposed system 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.

RELATED WORK:

Proposed authentication scheme aims at achieving the following goals:

Security in WSN:

Security risks in wireless sensor networks contain threats to the confidentiality, integrity, and availability of the system. Security methods used on the Internet are not simply adaptable to sensor networks because of the limited resources of the sensors and the ad-hoc feature of the networks. The adoption of competent algorithms to alleviate security risks has not kept pace with the rate of miniaturization. This section underscores the challenges of securing sensor network communications and demonstrates general attacks against sensor networks.

Security Goals:

Security assessments of any application spotlight on the five fundamental tenets of data security: confidentiality, origin integrity, data integrity, non-repudiation, and availability. The definitions used in this subsection are derived. Confidentiality means the camouflage of information from unauthorized entities. Mechanisms used to accomplish confidentiality include access control mechanisms and cryptography. Cryptography scrambles, or encrypts, information to produce cipher text inarticulate to any unauthorized viewer. The data can be made understandable to an authorized viewer who knows the secret key. Semantic security entails a stronger assurance of confidentiality. Semantic security needs that repeated encryption of a message M would yield unique cipher text each round.

Data integrity and authentication:

In wireless sensor networks, the need for integrity surpasses all other security goals. Data integrity and authentication create a foundation for a highly available and trustworthy network.

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

While many authentication schemes have been conceived for wireless sensor networks, none of them is a panacea. Algorithms for unicast message authentication, for example, do not meet the requirements for authenticating broadcast messages.

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.

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• both computational and communication overhead.

PROBLEM DEFINITION:

Problem of the system is to define 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. 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.

EXISTING SYSTEM:

In the existing system, 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.So 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 this system. 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 this system 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.

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

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 existing anonymous communication protocols are largely stemmed from either mix net or DC-net. A mix net provides anonymity via packet re-shuffling through a set of mix servers (with at least one being trusted). In a mix net, 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 mix net-like protocols rely on the statistical properties of the background traffic, they cannot provide provable anonymity. DC-net is an anonymous multi-party computation scheme. Some pairs of the participants are required to share 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.

PROPOSED SYSTEM:

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 against adaptive chosen-message attacks in the random oracle model. 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.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 of our algorithm makes the scheme suitable for decentralized networks.

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.

IMPLEMENTATION:

Node Deployment:

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

Sama 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.

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. This can be done through the verification of public key. ACK is replied to previous hop node if authentication is successful.

Compromised Node Detection Process:

If 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 unhampered, when a bad or meaningless message is received by

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

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. 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.

Key Server Management:

Key server is a certificate authority server, which is responsible for message authentication. The key server verifies the information and authenticates the user. This could be a kind of data encryption and decryption process. This is achieved through diffiehellman key exchange algorithm.

CONCLUSION:

In this Project, we first proposed a novel and efficient source anonymous message authentication scheme (SAMA) 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 threshold of the polynomial-based scheme, we then propose 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. Our 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]. Jian Li Yun Li Jian Ren Jie Wu, ―Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks‖, IEEE Transactions On Parallel And Distributed Systems, pp 1-10, 2013 .

[2]. Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman, ―Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)‖, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012, pp 96-101.

[3]. Harsh Kumar Verma, Ravindra Kumar Singh, ―Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms‖, International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012, pp 1-7 .

[4]. M. Albrecht, C. Gentry, S. Halevi, and J. Katz, ―Attacking cryptographic schemes based on ‖perturbation polynomials‖,‖ Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org.

[5]. Dunfan Ye,DaoliGong,WeiWang ―Application of Wreless Sensor Networks in Environmental Monitoring‖, 2009 2nd International Conference on Power Electronics and Intelligent Transportation System.

[6]. Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi ―Application of Wireless Sensor Networks in Energy Automation‖, Sustainable Power Generation and Supply, 2009. Supergen ’09. International conference .

[7]. 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,‖ in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[8]. Ian F. Akylidiz, Fellow IEEE, Tommaso Melodia, Member IEEE, and Kaushik R. Chowdhury, Student Member IEEE ―Wireless Multimedia Sensor Networks: Applications and Testbeds‖, Proceedings of the IEEE. Vol. 96, No. 10, October 2008.

[9]. W. Zhang, N. Subramanian, and G. Wang, ―Lightweight and compromise resilient message authentication in sensor networks,‖ in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[10]. Raymond Sbrusch, ―Authenticated Messaging In Wireless Sensor Networks Used For Surveillance‖, Thesis, The University Of Houston-Clear Lake, May, 2008.

[11]. Chung-Kuo Chang, J. Marc Overhage, Jeffrey Huang ―An Application of Sensor Networks for Syndromic Surveillance‖ 2005 IEEE .

[12]. F. Ye, H. Lou, S. Lu, and L. Zhang, ―Statistical enroute filtering of injected false data in sensor networks,‖ in IEEE INFOCOM, March 2004.

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

[13]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, ―An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks,‖ in IEEE Symposium on Security and Privacy, 2004.

[14]. A. Perrig, R. Canetti, J. Tygar, and D. Song, ―Efficient authentication and signing of multicast streams over lossy channels,‖ in IEEE Symposium on Security and Privacy, May 2000.

[15]. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, ―Perfectly-secure key distribution for dynamic conferences,‖ in Advances in Cryptology - Crypto'92, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[16]. T. A. ElGamal, ―A public-key cryptosystem and a signature scheme based on discrete logarithms,‖ IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[17]. R. Rivest, A. Shamir, and L. Adleman, ―A method for obtaining digital signatures and public-key cryptosystems, ‖ Communications. of the Assoc. of Comp. Mach., vol. 21, no. 2, pp. 120–126, 1978.

Author's Details:

Ms.Zohra Binte Sailan Has Completed Her Intermediate in Mathematics, Physics and Chemistry, She Has Completed Her B.Tech. in Computer Science & Engineering From Shadan College of Engineering and Technology, Peerancheru, JNTU University, Hyderabad. Presently, She is Pursuing Her Masters in Computer Networks From Shadan Women's College of Engineering And Technology, Khairatabad, Hyderabad, T.S, India

Ms.Syeda Nusrath Fatima, Has Completed Her B.Tech (Information Technology) From Osmania University,and M.Tech (Computer Science & Engineering) From Jntuh. She Has 4 Years of Experience In Teaching Field She is Working as Assistant Professor, Department Of CSE, in Shadan Women's College of Engineering And Technology.

Ms.Khaderbi Shaik, HOD, Department Of CN, Shadan Women's College of Engineering and Technology, Hyderabad, Ts, India