Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 12, No. 2, (2021),
ISSN : **1906-9685**

Journal of Nonlinear Analysis and Optimization : Theory & Applications
Editors-in-Chief :

IMPORTANCE OF SOURCE PRIVACY AND HOP-BY-HOP MESSAGE AUTHENTICATION IN WIRELESS SENSOR NETWORKS

[#1]Mr.SHANIGARAPU NAVEEN KUMAR, *Assistant Professor*
[#2]Mr.CHADA SAMPATH REDDY, *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT

Message authentication is a powerful tool for preventing the transmission of tainted or unlawful data in wireless sensor networks (WSN). As a result, a plethora of public- and symmetric-key based message authentication protocols have emerged. Most of these systems, however, suffer from significant processing and communication lags and struggle to deal with tasks that need a considerable amount of resources. At the node level, they are also simple to hack. A novel polynomial-based approach was implemented to address these concerns. If more than that amount of messages are sent, the enemy will recover the entire polynomial. In this research, we present an approach to scalable authentication using elliptic curve cryptography (ECC). Our proposed approach simplifies the authentication process for intermediary nodes. This solves the cutoff issue, allowing any node to send an infinite number of messages. Furthermore, our approach guarantees the confidentiality of communication senders. We found that our method required less time and effort in computation and discussion than the polynomial-based method. The sender's anonymity is safeguarded with the message's contents.

Keywords—Wireless Sensor Networks(WSN),Elliptic curve cryptography(ECC)Source Anonymous Message Authentication(SAMA)

INTRODUCTION

In order to prevent the transmission of unauthorized or altered communications across networks, message authentication is required. As a result, numerous identification systems have been developed to facilitate the verification of the authenticity of data transmitted across wireless sensor networks (WSNs). These systems can be categorized into two major groups: those that employ public keys and those that employ symmetric keys. Since the sender and receiver both need to know the same secret key, symmetric-key methods are difficult to administer, lack scalability, and are vulnerable to several node compromise attempts. Each transmitted message is accompanied by a message authentication code (MAC) generated by the sender using the shared key. However, the message can only be verified as genuine and reliable by the node in possession of the secret key, which is often shared among a group of sensor nodes. A single compromised sensor node is all it takes to unlock all the doors. The use of several networks further hinders the performance of this technology. A cryptographic approach to validating secret messages using polynomials was developed to address the issue of scalability. The degree of the polynomial determines the threshold, making this system similar to a threshold secret sharing mechanism. This approach ensures the information-theoretic security of a shared secret key as long as the number of messages sent remains below a particular threshold. The intermediary nodes do a polynomial evaluation to verify the authenticity of the message. Once the total number of messages delivered surpasses the threshold, the polynomial can be entirely restored, and the system is irreparably broken. A new system was implemented to thwart the intruder's attempts to determine the polynomial's coefficients. The objective is to make it more difficult to determine the coefficients of the equation by introducing a random disturbance, often known as random noise. However, recent research demonstrates that error-correcting code techniques can eliminate the noise in the polynomial entirely. Each communication delivered with the public-key method is accompanied by a digital signature generated with the sender's private key. The authenticity of the message can be confirmed at each step of the chain of transmission by using the sender's public key. The proposal has certain issues, one of which being the strain it will place on computers. Public key approaches can be more secure, take up less memory, and be harder to crack, as demonstrated by recent developments in elliptic curve cryptography (ECC). Key management for public-key methods is straightforward and effective. Our source anonymous message authentication (SAMA) mechanism is robust and secure. The best modified El Gamal signature (MES) technique for elliptic curves serves as the foundation for this system. Adaptive chosen-message attacks in the context of the random oracle concept are useless against the Message Encryption Scheme (MES). Our solution optimizes sensor resources by allowing intermediate nodes to verify the message. All the unwanted correspondence can be quickly located and removed in this way. Our method is resistant to compromise, has adjustable time for verification, and ensures the safety of the source's identity. When compared to polynomial-based algorithms, which provide a similar level of security, our proposed system performed better in theoretical and simulated tests.

PROBLEM DEFINITION

The cloud stores every user's private key, allowing it to instantly re-sign blocks for current users, sparing them the time and effort of doing it themselves. Since the cloud is not in everyone's trusted area, it would be extremely risky to store private keys there. When a user's access is revoked, other users should be able to verify the data's accuracy without having to download the entire set. It's challenging to find a middle ground that helps affected current users without requiring them to download the entire dataset from the cloud and allows a public verifier to verify the accuracy of shared data..

SYSTEM ANALYSIS

Because the sender and the recipient of a message need to exchange a secret key, the existing technique necessitates careful key management, is incapable of scaling, and is vulnerable to numerous forms of hacking. The sender creates the message with the help of the shared key. Each communication delivered with the public-key method is accompanied by a digital signature generated with the sender's private key. The authenticity of the message can be confirmed at each step of the chain of transmission by using the sender's public key. The approach suffers greatly from the fact that it necessitates a lot of computer processing time. Polynomial-based authentication of private conversations was provided. The degree of the polynomial determines the threshold, making this system similar to a threshold secret sharing mechanism. The intermediary nodes do a polynomial evaluation to verify the authenticity of the message. Once the total number of messages delivered surpasses the threshold, the polynomial can be applied.

Snapshot 2. Even though the dataflow map is normal again, the system is currently unusable. Some issues with this approach include its inability to scale, its susceptibility to node compromise attacks, its high computational demands, and the threshold problem.

.SYSTEM DESIGN

The data flow layout is depicted in Figure 2, and the system's construction and operation are shown in Figure 1. Using this technique, we can securely and efficiently verify messages with unknown origins. To make it applicable to elliptic curves, the best modified ElGamal signature (MES) technique is employed. In the random oracle model, adaptive chosen-message attacks are useless against the MES utilized here. Our solution optimizes sensor resources by allowing intermediate nodes to verify the message. All the unwanted correspondence can be quickly located and removed in this way. Our approach sidesteps the threshold issue while maintaining confidentiality of the source, imperviousness to tampering, and flexibility across time scales. Strong security against compromise, flexible temporal identification, protection of source identity, and elimination of the threshold problem are only a few of the benefits of this method.

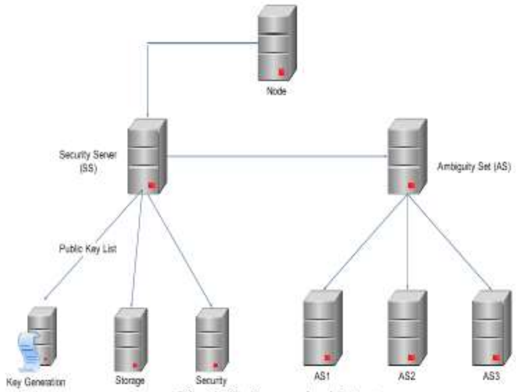


Fig .1. Software Archietecture

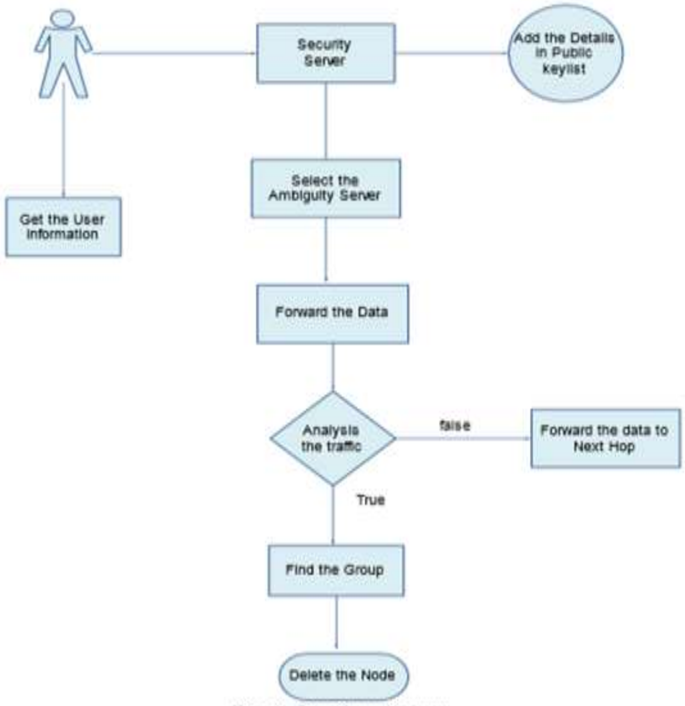


Fig. 2. Dataflow diagram

PROPOSED MODEL

The components of this system are as follows: 1) The network architecture How to authenticate communications in the security server and send encrypted packets. Locating Compromised Network Nodes, 5.

Node Creation

The construction of a node is depicted in Figure 3. The user-provided node IDs and connections are used to construct the node. Each node's IP address and port number are also obtained. The user agrees that this node may be selected as the target for outbound links.

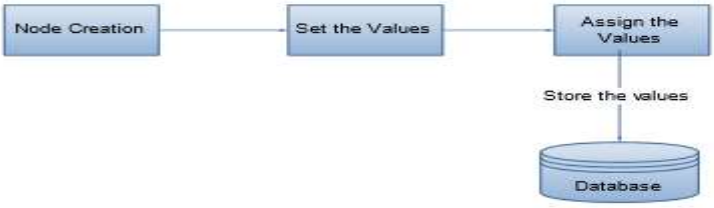


Fig .3. Node creation

Security Server Process

Figure 4 depicts the security server's internal workings. It is believed that all sensor nodes have accurate localization data and can use geographic routing to establish direct connections with other nodes in the same general area. Messages sent over the network travel several nodes before arriving at their destination. Many believe that the SS is accountable for creating, storing, and disseminating all network-wide security policies. This computer is completely unbreakable.

Fig .1. Software Architecture

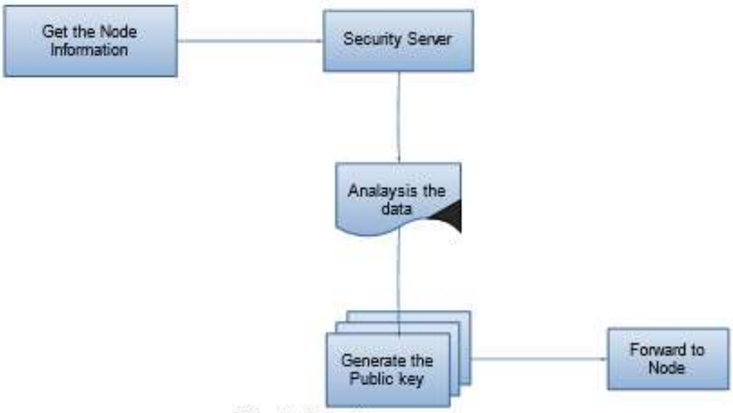
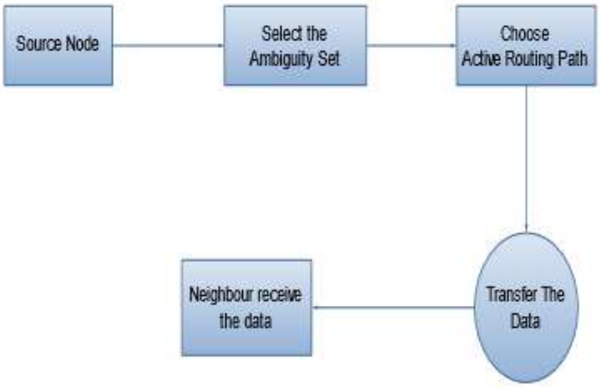


Fig .4. Security server process

Secure Packet Forwarding

As shown in Figure 5, it is crucial that each relay along the route verify the legitimacy of messages upon receipt.



.Compromised Node Detection

The location of a compromised node can be determined as shown in Figure 7. When a compromised node is discovered, the SS can remove its public key from the list of public keys. The node's short identifier can also be broadcast across the sensor network. Any sensor node that relies on a previously stored public key to select an Autonomous System (AS) can now receive new keys. To maximize energy efficiency, you should cut ties with the authentication server (AS) that hosts the compromised node as soon as its public key is made public or removed from the public key list.

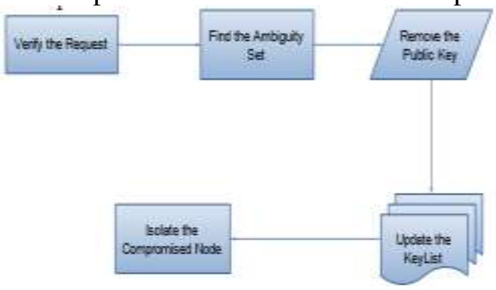


Fig. 7. Compromised Node Detection

6. CONCLUSION

The proposed method, called Source Anonymous Message Authentication (SAMA), uses elliptic curve encryption to conceal the identities of message senders. SAMA can be used to verify the accuracy of a message before it is sent. Then, we demonstrate the SAMA technique's applicability in a hop-by-hop message authentication mechanism. Hop-by-hop message authentication is made possible without the fundamental drawback of the polynomial-based method. This research also discusses other methods for detecting compromised nodes in Wireless Sensor Networks (WSNs) using stationary sink nodes.

REFERENCES

1. 1.F. Ye, H. Lou, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” in *IEEE INFOCOM*, March 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,” in *IEEESymposium on Security and Privacy*, 2004.
3. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and
4. 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.
5. W. Zhang, N. Subramanian, and G. Wang, “Lightweight and compromiseresilient message authentication in sensor networks,” in *IEEE INFOCOM*, Phoenix, AZ., April 15-17 2008.
6. 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.
7. M. Albrecht, C. Gentry, S. Halevi, and J. Katz, “Attacking cryptographic schemes based on ”perturbation polynomials”,” Cryptology ePrint Archive, Report 2009/098, 2009,