# Hop-byHop Message Authentication and Source privacy in Wireless Sensor Networks

G.Lalithambal
PG scholar, Department of CSE
Moogambigai College of Engineering

M.Flora Mary
Associate Professor, Department of CSE
Moogambigai College of Engineering

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

## I. 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 in. 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. 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. In this paper, 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.

## II. PROBLEM DEFINITION

Cloud could possess each user's private key, it can easily finish the re-signing task for existing users without asking them to download and re-sign blocks. However, since the cloud is not in the same trusted domain with each user in the group, outsourcing every user's private key to the cloud would introduce significant security issues. we need to consider is that the re-computation of any signature during user revocation should not affect the most attractive property of

public auditing data integrity publicly without retrieving the entire data. Therefore, how to efficiently reduce the significant burden to existing users introduced by user revocation, and still allow a public verifier to check the integrity of shared data without downloading the entire data from the cloud, is a challenging task.

## III. SYSTEM ANALYSIS

In existing system, 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. 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.

A secret polynomial based message authentication scheme was introduced in. The idea of this scheme is similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. 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. Demerits of this approach are lack of scalability, Node compromise attacks, High computational overhead and threshold problem.

## IV. SYSTEM DESIGN

Fig 1.Shows the system Architecture and its functionalities and Fig 2 shows the data flow diagram .This model proposes 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. This system provides more merits such as compromise-resiliency, flexible-time authentication, source identity protection and this scheme does not have the threshold problem.

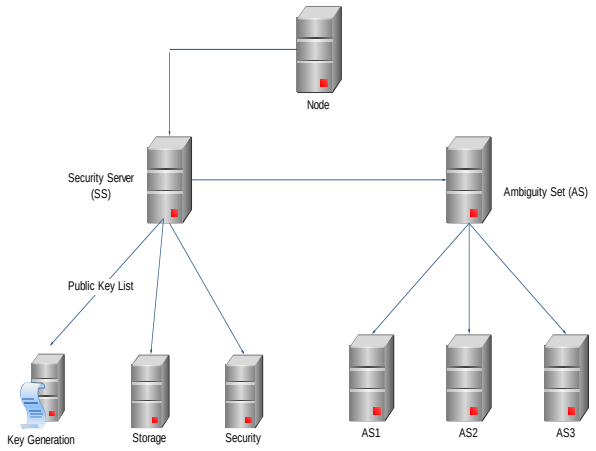


Fig .1. Software Archietecture

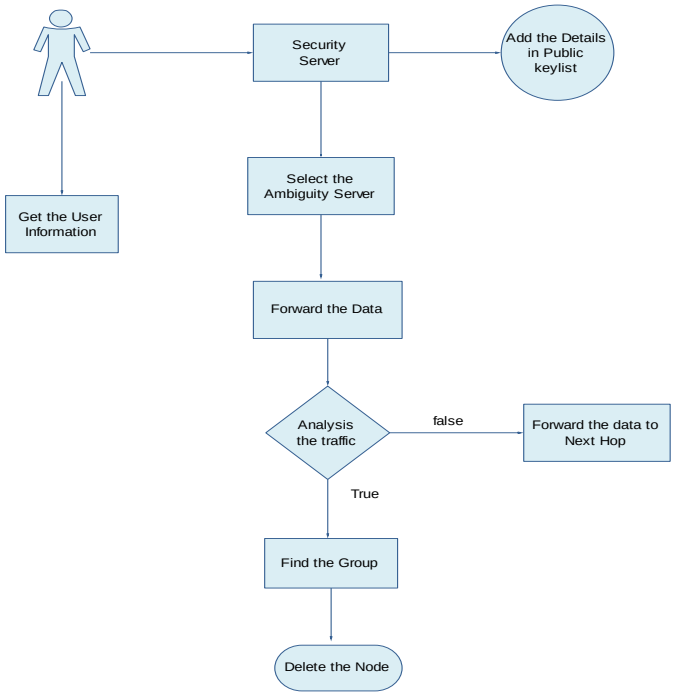


Fig. 2. Dataflow diagram

## IV. PROPOSED MODEL

This system consists of following modules 1.Network Construction 2. Security server Process 3. Secure Packet Forwarding4. Analysis Message Authentication 5. Compromised Node Detection.

*A.Node Creation*

Fig 3 shows the node creation, construct a Node Creation. Node is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and ip address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user.

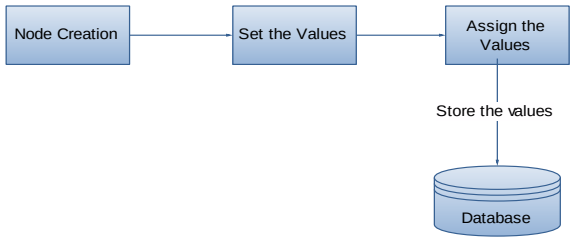


Fig .3. Node creation

*B. Security Server Process*

Fig 4 shows the security server process, in this process it is assumed that each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. We assume there is a security server (SS) that is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised.

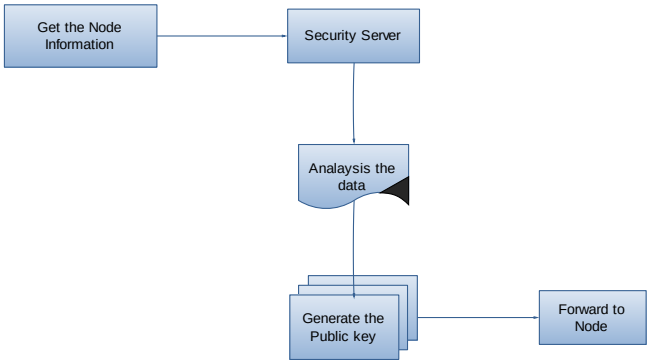


Fig .4. Security server process

*C.Secure Packet Forwarding*

Fig 5 shows the server packer forwarding, every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.

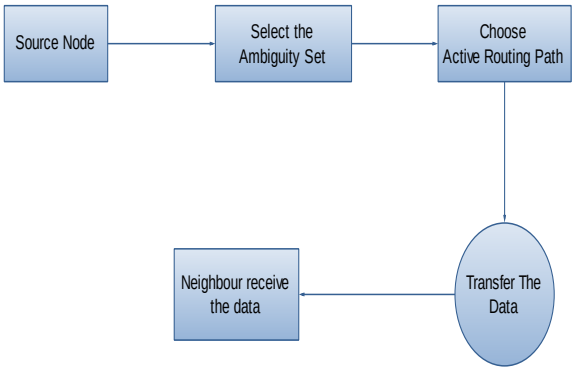


Fig .5.Secure packet forwarding

*D.Analysis Message Authentication*

Fig 6 shows Analysis 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.

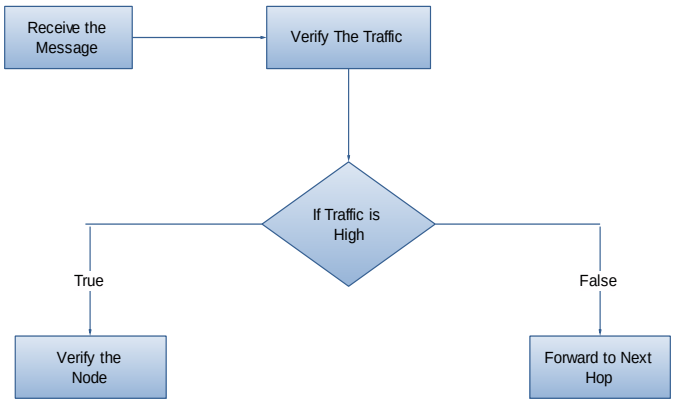


Fig. 6. Analysis Message Authentication

*E.Compromised Node Detection*

Fig 7 shows the Compromised node detection, When a node has been identified as compromised, the SS can remove its public key from its public key list. It can also broadcast the node's short identity to the entire sensor domain so that any sensor node that uses the stored public key for anAS selection can update its key list. Once the public key of a node has been removed from the public key list, and/or broadcasted, any message with the AS containing the compromised node should be dropped without any processing order to save the precious sensor power.

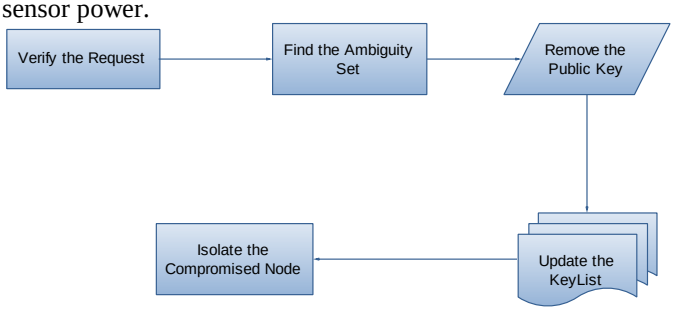


Fig. 7. Compromised Node Detection

## V CONCLUSION

The proposed novel and efficient source anonymous message authentication based on elliptic curve cryptography ensures 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 propose a hop-by-hop message authentication scheme based on the SAMA. When applied to WSNs with fixed sink nodes, it is also discussed various possible techniques for compromised node identification.

## REFERENCES

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 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.

4. W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromiseresilient message authentication in sensor networks," in *IEEE INFOCOM*, Phoenix, AZ., April 15-17 2008.

5. 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.

6. 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/.