INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

# SCALABLE MESSAGE AUTHENTICATION SCHEME BASED ON ECC IN WIRELESS SENSOR NETWORKS

**Ms. S.Banumathi[#1],Ms. P. Pappathi[#2], Ms.M. Muthumalar[#3], Mr. J.Joepaul[*4]**

*[#]Student,[*]Assistant Professor*
*Department of Applied Electronics*
*Chandy college of engineering*
*Tutucorin(T.N) India*
banumathi592@gmail.com,pappathi91@gmail.com, malaramula@gmail.com,jeanvillavan@gmail.com

**Abstract:-** Message Authentication scheme have been proposed in the past for protecting communication Authenticity and integrity 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. While Symmetric Key schemes are efficient in processing time for sensor networks, they generally require complicated key management, which may create large memory and communication overhead. On the contrary, Public Key based Schemes have simple and clean key management. Most of them however have following limitations: Computation and Communication overhead, no resilience to a large number of node compromises, lack of scalability. To solve this problem, a secret Polynomial based Message Authentication scheme was introduced. This scheme is similar to a threshold secret sharing, where the threshold value is 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 and the system is completely broken. In this paper, we propose a Novel and efficient Source Anonymous Message Authentication scheme based on ECC 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. The main challenges is that authenticity must be guaranteed even when only the sender of the data is trusted and scheme needs to scale to potentially millions of receivers. Proposed scheme is more efficient than the polynomial-based scheme in terms of computational overhead, delivery ratio and message delay

**Keywords:-**Hop-by-hop message authentication,public-key cryptography,message authentication,source privacy, wireless sensor networks(WSNs).

## *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 approachesand 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 mes- sages transmitted is less than the threshold. The intermedi- ate nodes verify the authenticity of the message through a polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the poly- nomial can be fully recovered and the system is completely broken.An alternative solution was proposed in  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 mes- sage generated using the sender's private key. Every intermediate forwarder and the final receiver can authen- ticate 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 sim- ple 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 con- serve the sensor power. While achieving compromise- resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold prob- lem. Both theoretical analysis and simulation results dem- onstrate that our proposed scheme is more efficient than the polynomial-based algorithms under comparable secu- rity levels.

## *II . SYSTEM DESIGN AND MODULES*

### *a) Source Anonymous Message Authentication Scheme*

An unconditionally secure and efficient Source Anonymous Message Authentication (SAMA) scheme based on the optimal Modified ElGamal Signature (MES) scheme on Elliptic Curves is introduced. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model.

The major contribution is first to develop a source anonymous message authentication on elliptic curves that can provide an unconditional source anonymity. Secondly, offering efficient hop by hop message authentication for WSN without threshold limitation. Thirdly, an efficient key management framework is introduced to ensure isolation of compromised nodes.

Our scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to con- serve 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 ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms. A variant developed at NSA and known as the Digital Signature Algorithm is much more widely used. There are several other variants. The ElGamal signature scheme allows a third-party to confirm the authenticity of a message sent over an insecure channel. The modified ElGamal signature scheme consists of the following three algorithms:

- **Key Generation Algorithm**

Let "p" be a large prime and "g" be a generator of $Z^*p$. Both p and g are made public. For a random private key x€$Z_P$, the public key y is computed from

y=$g^k$ mod p.

- ***Signature Algorithm***

The MES can also have many variants. For the purpose of efficiency, we will describe the variant, called optimal scheme. To sign a message m, one chooses a random k€$Z^*_{p-1}$, then computes the exponentiation r= $g^k$ mod p and solves s from:

s = r x h (m, r) + k mod (P -1),

where h is a one-way hash function. The signature of message "m" is defined as the pair (r, s).

- ***Verification algorithm***

The verifier checks whether the signature equation $g^s = ry^{rh(m,r)}$mod p: If the equality holds true, then the verifier accepts the signature, and rejects otherwise.The major contributions of this paper are the following:

1. We develop a Source Anonymous Message Authentication Code (SAMAC) on elliptic curves that can provide unconditional source anonymity.
2. We offer an efficient hop-by-hop message Authentication mechanism for WSNs without the threshold limitation.
3. We devise network implementation criteria on source node privacy protection in WSNs.
4. We propose an efficient key management framework to ensure isolation of the compromised nodes.
5. We provide extensive simulation results under ns-2 on multiple security levels.

A SAMA consists of the following two algorithms

1. Generate (m;$Q_1, Q_2, \ldots Q_n$). Given a message "m" and the public keys $Q_1, Q_2 \ldots Q_n$of the AS.S = {$A_1, A_2, \ldots A_n$ }, the actual message sender$A_t$; 1 ≤ t ≤ n, produces an anonymous message S(m) using its own private key$d_t$.
2. Verify S (m). Given a message m and an anonymous message S(m), which includes the public keys of all members in the AS, a verifier can determine whether S(m) is generated by a member in the AS.

***b) MES Scheme on Elliptic Curves***

Let p > 3 be an odd prime. An elliptic curve E is defined by an equation of the form:

E: $y^2 = x^3 + ax + b \bmod p$

*i.* ***Signature Generation Algorithm***

1. Select a random integer $k_A$ , $11 \leq k_A \leq N-1$
2. Calculate $r = x_A \bmod N$, where $(x_A, y_A) = k_A G$ . If r=0, go back to step 1.
3. Calculate $h_A \leftarrow$h (m r)
4. Calculate s= r $d_A h_A + k_A \bmod N$. If s=0, go back to step 2
5. The signature is the pair (r, s).

***ii. Signature Verification Algorithm***

Step 1: Verify that r and s are integers in [1, N-1]. If not the signature is invalid.

Step 2: Calculate $h_A \leftarrow$h (m, r)

Step 3: Calculate (x1, x2) = s G-r$h_A Q_A \bmod N$

Step 4: The signature is valid if r-x1 mod N, invalid otherwise.

### c) *SAMA on Elliptic Curves*

#### i. *Authentication Generating Algorithm*

Step: 1 Select a random and pair wise different $k_i$ for each $1 \leq i \leq n-1, i \neq t$ and compute $r_i$ from $(r_i, y_i) = k_i G$
Step2: choose a random $k_i \in Z_p$ and compute $r_t$ from $(r_i, y_i) = k_i G$ -$\sum_{i \neq t} r_i h_i Q_i$ such that $r_t \neq 0$
Step 3: Compute s= $k_t + \sum_{i \neq t} k_i + r_t d_t h_t \ mod \ N$
The SAMA of the message m is defined as

S (m) = (m, S $r_1, y_1 \ldots \ldots, r_n, y_n, s$)

#### ii. *Verification of SAMA*

Step 1: Verify that $r_i, y_i, i = 1 \ldots \ldots n$ and s are integers in [1,N-1]. If not, the signature is invalid.
Step 2: Calculate $h_i \overset{l}{\leftarrow} h(m, r_i$
Step 3: Calculate (x0, y0) = s G-$\sum_{i \neq t} r_i h_i Q_i$
Step 4: The signature is valid if the first coordinate of $\sum_i (r_i y_i$ ) equals x0, invalid otherwise.

## III *RELATED WORK*

### A. *Network Initialisation*

The WSNs are assumed to consist of a large number of sensor nodes. We assume 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.

### B. *Anonymous Set*

Some basic criteria for the selection of the AS can be described as follows:

To provide message source privacy, the message source needs to select the AS to include nodes from all directions of the source node. In particular, the AS should include nodes from the opposite direction of the successor node. In this way, even the immediate successor node will not be able to distinguish the message source node from the forwarder based on the message that it receives. Though the message source node can select any node in the AS, some nodes in the AS may not be able to add any ambiguity to the message source node. For instance, the nodes that are apparently impossible or very unlikely to be included in the AS based on the geographic routing. Therefore, these nodes are not appropriate candidates for the AS. They should be excluded from the AS for energy efficiency.

To balance the source privacy and efficiency, we should try to select the nodes to be within a predefined distance range from the routing path. We recommend selecting an AS from the nodes in a band that covers the active routing path. However, the AS does not have to include all the nodes in the routing path.

The AS does not have to include all nodes in that range, nor does it have to include all the nodes in the active routing path. In fact, if all nodes are included in the AS, then this may help the adversary to identity the possible routing path and find the source node.

### C. *Key Management & 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 an AS 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 process in order to save the precious sensor power.

***Compromised Node Detection***

We assume that all sensor information will be delivered to a sink node, which can be collocated with the SS. As described in Section 5, when 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 untampered, when a bad or meaningless message is received by 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.

### *D. Security Analysis*

SAMA can ensure unconditional source anonymity, we have to prove that:

1) For anybody other than the members of S, the probability to successfully identify the real sender is 1/n.

2) Anybody from S can generate SAMAs. SAMA is secure against existential forgery under adaptive chosen message attacks in the random oracle model. The security of our result is based on ECC, which assumes that the computation of discrete logarithms on elliptic curves is computationally infeasible. In other words, no efficient algorithms are known for non-quantum computers.

### *E. Performance Analysis*

In this section, we will evaluate our proposed authentication scheme through both theoretical analysis and simulation demonstrations. Key management is one of the major issues for secret-key based authentication schemes. This is especially true for large scale WSNs.

While many of these schemes are designed to provide node authentication, they can only provide end-to-end node authentication using the secret key shared between the two nodes, which implies that only the receiver can verify the authenticity of the messages en-route. This means that no intermediate node can authenticate the message in general. The intermediate nodes may have to forward a manipulated message for many hops before the message can finally be authenticated and dropped by the receiving node.

## *III SIMULATION RESULTS*

***Performance evaluation***

To evaluate the performance of the method, the developed system is compared with various performance metrics. The performance metrics are like delivery ratio, message delay and message overhead.

***Comparative study***

. To analysis the performance of the developed system, it is compared with various performance metrics. This is shown in the below tables, and to know the working of the developed system, it is compared with different methods. The comparison with different methods is shown below.

We will compare the computational overhead, communication overhead, delivery ratio, transmission delay of our proposed scheme with the bivariate polynomial-based scheme.In this section we implement the bivariate polynomial based scheme and our proposed scheme in a real world comparison. The comparison is based on comparable security level.

### *a. Delivery Ratio*

The ratio of the number of delivered data packet to the destination is known as packet delivery ratio. This illustrates the level of delivered data to the destination.

$$Packet\ Delivery\ ratio = \frac{\sum Number\ of\ Packet\ Received}{\sum Number\ of\ Packet\ Send}$$

Table 1. Comparison of Delivery Ratio with Various methods

| No. Of Nodes | Polynomial | SAMA |
|---|---|---|
| 5 | 84.16 | 98.16 |
| 10 | 83.26 | 97.46 |
| 15 | 85.49 | 97.28 |
| 20 | 84.79 | 96.13 |
| 25 | 85.34 | 97.23 |

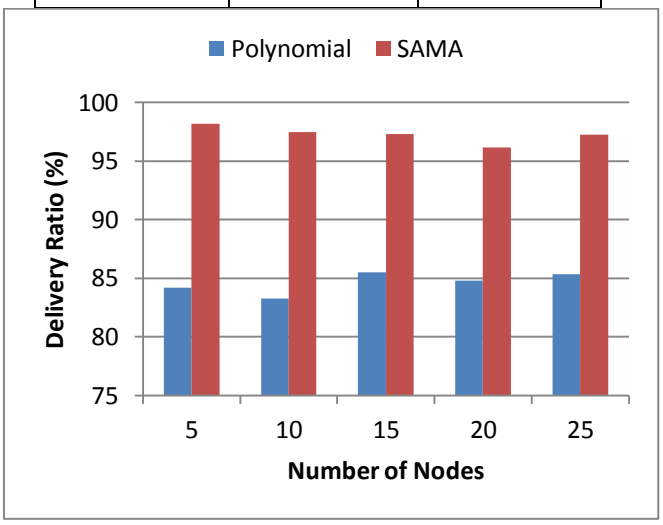


Fig 1.Comparison of Delivery Ratio

***b. Message Delay***

The average time taken by a data packet to arrive in the destination is known as end to end delay. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$$Message\ Delay = \frac{\sum(Arrive\ Time - Send\ Time)}{\sum Number\ of\ Connections}$$

Table 2. Comparison of Message Delay with Various methods

| No. Of Nodes | Polynomial | SAMA |
|---|---|---|
| 5 | 6.49 | 0.09 |
| 10 | 6.23 | 0.46 |
| 15 | 5.49 | 0.98 |
| 20 | 6.39 | 1.23 |
| 25 | 6.82 | 1.56 |

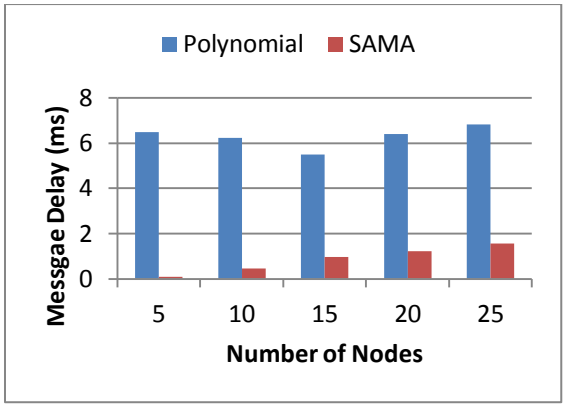


Fig 2. Comparison of Message Delay

### *c. Message Overhead*

In computer science, the routing overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. It can also be calculated as the difference between the actual or fixed values and the absorbed values.

$$Message\ Overhead = \frac{Actual\ Values}{Absorbed\ Values}$$

Table 3. Comparison of Message Overhead with Various methods

| No. Of Nodes | Polynomial | SAMA |
|---|---|---|
| 5 | 1.9 | 0.09 |
| 10 | 2 | 0.19 |
| 15 | 2.1 | 0.24 |
| 20 | 2.5 | 0.41 |
| 25 | 3.6 | 0.45 |

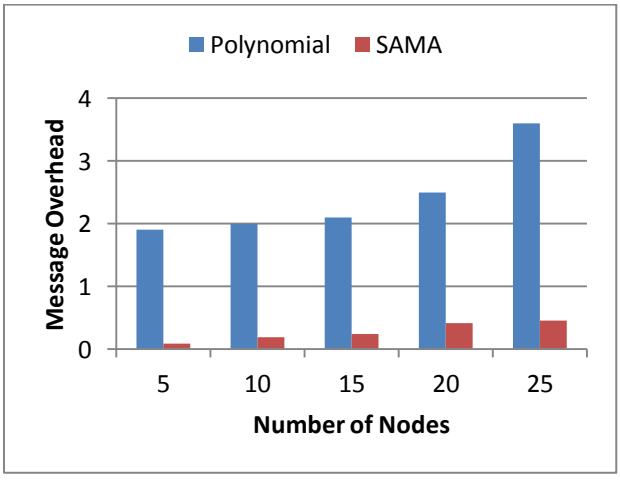


Fig 3. Comparison of Message Overhead

The above tables and figure shows the performance of the developed system which is compared with the existing methods, with the performance metrics of delivery ratio, message delay and message overhead.

## *CONCLUSION*

This work proposed to design the secure base an unconditionally secure and efficient Source Anonymous Message Authentication (SAMA) scheme based on the optimal Modified ElGamal Signature (MES) scheme on elliptic curves. From this, the AS is selected and the privacy is applied at the source point. Then the key is managed and the nodes are detected. By this an unlimited number of messages can be transmitted without any threshold problem. From the experimental results, the method used in this paper shows better results in all the performance metrics, than the existing method. Thus, the proposed method provides more ways to transmit the message without any problem and SAMA 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. Message Authentication has always been a major threat to the security in Wireless Sensor Networks (WSN).An efficient Source Anonymous Message Authentication scheme based on ECC 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. SAMA based on ECC compared it against other popular mechanisms in different scenarios through simulations and TelosB. Simulations results indicate that it greatly increases the effort of an attacker, but it requires proper models for every application. 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] Abror Abduvaliev, Sung young Lee and Young-Koo Lee (2009) "Simple Hash Based Message Authentication Scheme for Wireless Sensor Networks" Communication and information technology.

[2] Haodong Wang, Bo Sheng, Chiu C. Tan, Qun Li (2008) "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 System (ICDCS), pp.11-18.

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

[4] Pointcheval. D and Stern. J, (2000) "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 950, pp.182-193.

[5] Rivest. R, Shamir and Adleman. L (1978) "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol.21, no. 2, pp. 120-126.

[6] Ramesh kumar. M, Suresh Gnana Dhass. C (2012) "A Security of Wireless Sensor Networks and Analysis on Efficient Broadcast Authentication" International Journal of Advanced Research in Computer Science and Software Engineering.

[7] Ramesh kumar. M, Suresh Gnana Dhass. C (2012) "Design an Enhanced Certificate Based Authentication Protocol for Wireless Sensor Networks" International Journal of Advanced Research in Computer Science and Software Engineering.

[8] Swati Verma1, and Birendra Kumar Sharma (2011) "A New Digital Signature Scheme Based on Two Hard Problems" Int. J. Pure Appl. Sci. Technol., International Journal of Pure and Applied Sciences and Technology.

[9] Victor. R, Shen. L, Yu Fang Chung, Tzer Shyong Chen and Yu An Lin (2011) "A Blind Signature Based On Discrete Logarithm Problem" International Journal of Innovative Computing.

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