Source Anonymous Message Authentication and Source Privacy using ECC in Wireless Sensor Network

[1]Ms.Anisha Viswan, [2]Ms.T.Poongodi, [3]Ms.Ranjima P,[4]Ms.Minimol Mathew

[1,3,4]PG Scholar,[2]Assistant Professor,
[1,2,3,4]Computer Science and Engineering, PPG Institute of Technology,Coimbatore,641035,India

***Abstract*— The unauthorized and corrupted messages being forwarded in the wireless sensor networks (WSN) can be prevented by using the message authentication. For this many conventional methods have been developed, they are symmetric key and public key cryptosystem. But they have their own limitations of high computational overhead, communicational overhead and lack of scalability. To overcome these problems a polynomial based scheme was developed but they have the limitations with the threshold value ie, the number of messages transmitted should be less than the threshold value .In this paper ,we propose a source anonymous message authentication scheme based on elliptic curve cryptography which enables intermediate authentication. By this scheme any node can transmit an unlimited number of messages without threshold problem and also provide message source privacy.**

***Key words*-Authentication, Public key cryptography, Symmetric key cryptography, Source privacy**

I. INTRODUCTION

Message authentication plays a key role in preventing unauthorized and corrupted messages from being forwarded in WSN to save the precious sensor energy. Message authentication scheme can be divided into two categories those are symmetric-key based approaches and public key based approaches.

The symmetric-key based approach needs complex key management and having scalability problem and is not resilient to node compromise attacks as same key is shared between sender and receiver. By capturing a single node an intruder can easily compromise the key and it does not work in multicast networks.

A secret polynomial based message authentication scheme was introduced to solve the scalability problem which is based on the information, security provided by sharing the threshold where threshold means degree of the polynomial. The intermediate nodes use the polynomial evaluation to verify the authenticity of the message. However, the number of messages transmitted is larger than the threshold, the polynomial can be easily discovered and the system is completely broken.

In the public key based approach, each message has to be sent along with the digital signature of the message generated using the sender's private key. Each intermediate forwarder and final receiver can perform the authentication of the message using sender's public key. But it has the limitation of 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 and it also having a simple and clean key management.

In this paper, we propose a secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. By this every intermediate nodes can authenticate the message so that all the unauthorized and corrupted messages can be detected and dropped to conserve the sensor power. And this scheme does not have any threshold problem; any node can transmit an unlimited number of messages.

II. PROPOSED METHOD

A. Goals

- Message authentication: Each message receiver should be able to verify whether a received message is sent by the node that is claimed. The adversaries cannot act as an innocent node.
- Message integrity: Each message receiver should be able to verify whether the message has been modified by the adversaries.
- Hop-by-hop message authentication: Every intermediate node along the routing path should be able to verify the authenticity and integrity of the message.
- Identity and location privacy: By analyzing message content, the adversaries cannot identify the message ID and location.
- Node compromise resilience: It should be resilient to node compromise attacks.
- Efficiency: The proposed scheme should be efficient in terms of both computational and communication overhead.

B. Source Anonymous Message Authentication Scheme on Elliptic Curve

For each message m to be released, the message sender generates a source anonymous message authenticator for the message m.This generation is depends on the MES scheme on the elliptic curves. Each ring member in the ring signature is required to compute a forgery signature for other members in the AS. The SAMA generation requires only three steps, that links all the non-senders and the message sender to the SAMA.SAMA can be verified through a single equation without individually verifying the signatures.

C. Algorithms used

1. The SAMA consists of mainly two algorithms:

- Generate $(m,Q_1,Q_2,\dots,Q_n)$: Given a message m and the public keys $Q_1,Q_2,\dots,Q_n$ of the AS (ambiguity set) S = f$\{A_1,A_2, \dots ,A_n\}$, the actual message sender At,$1 \leq t \leq n$, produces an anonymous message S(m) using its own private key d_t.
- 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.

2. The Modified ElGamal Signature scheme consists of mainly 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 $x \epsilon Z_p$, the public key y is computed from
  $y= g^x$ mod p.
- Signature algorithm: One chooses a random $k \epsilon Z_{p-1}$, then computes the exponentiation $r = g^k$ mod p and solves s from s = rxh (m, r) + k mod (p-1), where h is a one-way hash function. The signature of message m is (r,s).
- Verification algorithm: The verifier checks the signature equation $g^s = ry^{rh}(m, r)$ mod p: If it holds equality, then the verifier accepts the signature, otherwise reject it.

D. Hop-by-hop authentication

An unconditionally secure and efficient SAMA, the main idea is that for each message m to be released the message sender can generate a source anonymous message authenticator for the message m and it should be based on the MES scheme on elliptic curves. Each ring member in the ring signature is required to compute a forgery signature for other members in the AS. The entire SAMA generation requires only three steps that link all non-senders and the message sender to the SAMA. The SAMA can be verified through a single equation without individually verifying the signatures.

E. Symmetric-key cryptosystem

Each symmetric authentication key is shared by a group of sensor nodes so that the intruder can compromise the key by capturing a single sensor node. Then, these schemes are not resilient to node compromise attacks. One type of symmetric-key scheme needs synchronization among nodes. This also includes TESLA and its variants, can also provide message sender authentication. It requires initial time synchronization, but it is not easily applicable in large scale WSNs. They also introduce delay in message authentication, and it increases with the network scales up.

A secret polynomial based message authentication scheme provides information theoretic security as similar to a threshold secret sharing ideas, where the threshold means degree of the polynomial. If the number of messages transmitted is below the threshold, the intermediate node can verify the authenticity of the message through polynomial evaluation. However, the number of messages transmitted is larger than the threshold, the polynomial can be easily discovered and the system is completely broken.

F. Public-key cryptosystem

The public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Each intermediate forwarder and final receiver can perform the authentication of the message using sender's public key. 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 and it also having a simple and clean key management.

Public-key cryptosystem scheme has assumed that there is an SS whose responsibilities include public-key storage and distribution in the WSNs. Assume that the SS will never be compromised. After deployment, the sensor node may be captured and compromised by the attackers. Once compromised, all information stored in the sensor node will be accessible to the attackers. Further assume that the compromised node will not be able to create new public keys that can be accepted by the SS. Each public key will have a short identity for the efficiency and it is based on the scale of the WSNs.

G. Source privacy

The actual message source node will be hidden in the AS, so the appropriate selection of the AS plays a key role in message source privacy. It discuss the techniques that can prevent the adversaries from tracking the message source through the AS analysis in combination with local traffic analysis. The message source node selects an AS from the public key list in the SS as its choice before a message is transmitted. This set also contains sensor node and some other nodes. When an adversary receives a message, he can possibly find the direction or the real node of the previous hop. If the adversary is unable to monitor the traffic of the previous hop, then he is unable to distinguish whether the previous node is the actual source node or a forwarder node. A sufficient diversity is created in the selection of the AS so that it is infeasible for the adversary to find the message source based on the selection of the AS itself.

H. Multi-key Generation

ACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. By this we understand the extra resources that are required with the introduction of digital signature in WSNs. To address this concern, both schemes have been implemented. The goal is to find the most optimal solution for using digital signature in WSNs.

Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption multiple key pairs. Having knowledge of multiple key, say the encryption key, is not sufficient enough to determine the other key - the decryption key. For this, the encryption key can be made public and the decryption key is held only by the party wishing to receive encrypted messages (hence the name public/private key cryptography). Anyone can not use the public key for others public keys and to encrypt a message, only for recipient can decrypt it.

The mathematical relationship between the public/private key pair permits a general rule: any message encrypted with one key for one slot of the pair can be successfully decrypted only with that key's counterpart. The encryption using public key means, the slot by slot decryption can be done using the private key only. The converse is also true - to encrypt with the private key means you can decrypt only with the public key.

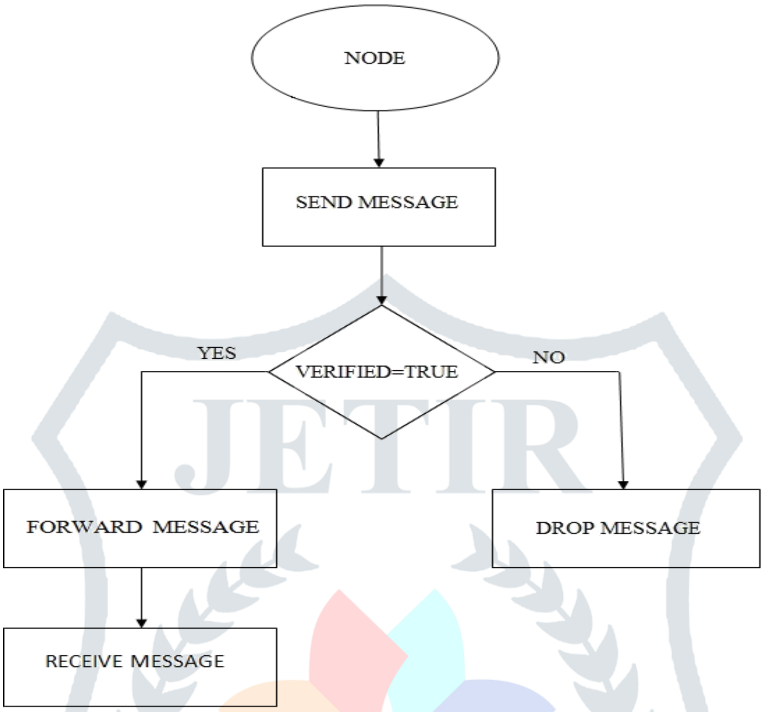

Fig 2.1 Flow diagram

III. PERFORMANCE EVALUATION

For evaluating the performance of the proposed scheme, compare it with the some existing techniques using NS-2 simulator. The polynomial-based scheme is based on symmetric key and the proposed scheme is based on ECC. The key size for the symmetric key cryptosystem is *l*, while for the proposed ECC is 2*l*, which is much shorter than the traditional public-key cryptosystem. This progress helps the implementation of the authentication scheme using ECC.

The ECC scheme is compared against polynomial based scheme and it provides positive results. The schemes should be comparing against delay, energy consumption, delivery-ratio and communication overhead .Delay is the additional amount of time taken for the delivery of the packet than the normal. Packet delivery ratio is the ratio between the numbers of delivered data packet to the destination. Sending a payload of data over a communication network requires sending more than just the desired payload data, itself. This makes communication overhead in wireless sensor network. The proposed scheme is efficient in terms of delay, energy consumption, deliver ratio and the communication overhead than the polynomial scheme.

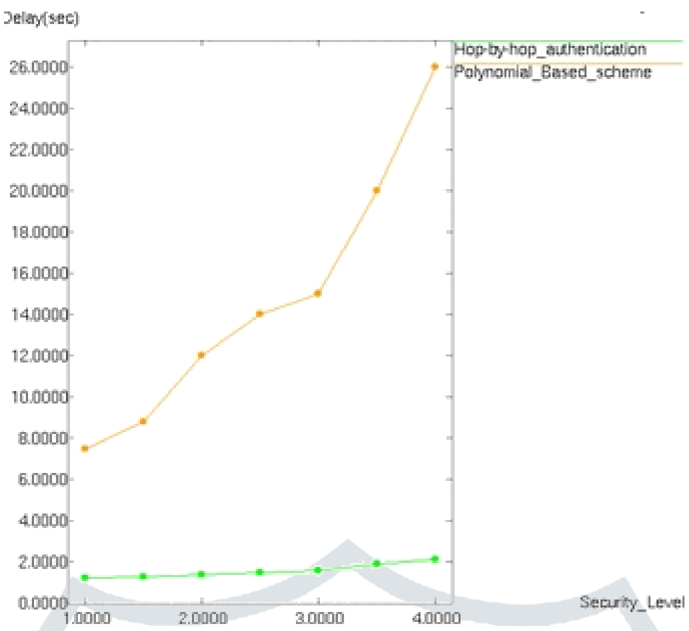

Fig 3.1 Delay

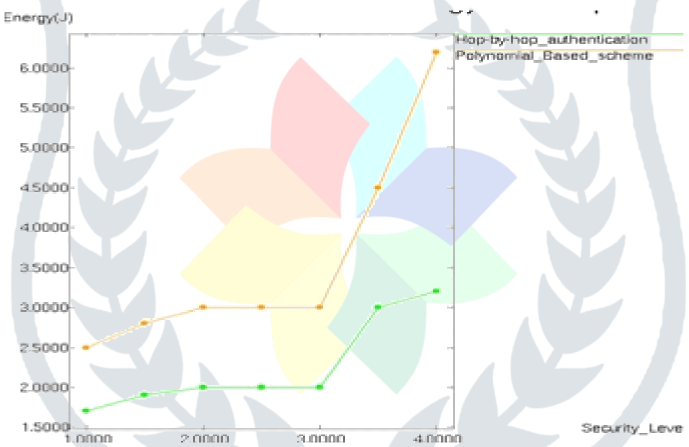

Fig 3.2 Energy consumption

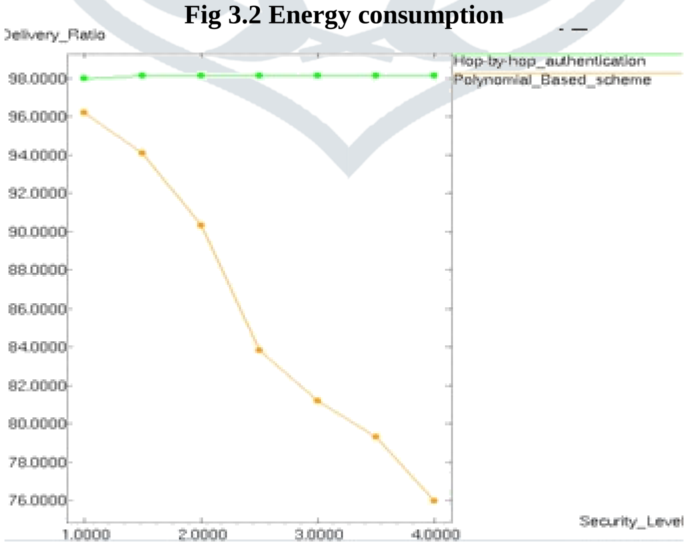

Fig 3.3 Delivery ratio

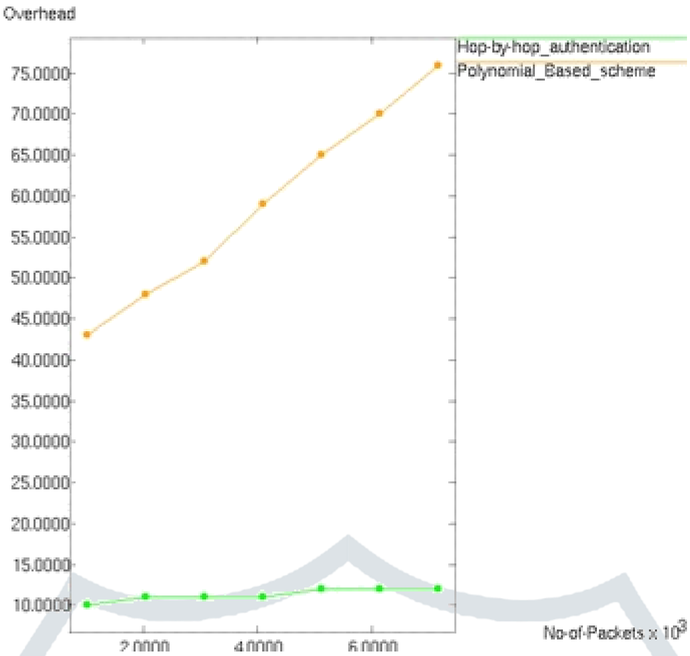

Fig 3.4 Communication overhead

IV. CONCLUSION

The message authentication is used to prevent the unauthorized and corrupted messages being forwarded in the WSN.A novel and efficient SAMA based on ECC can be applied to any message to provide message content authenticity. It provides hop-by-hop message authentication without the weakness of the built in threshold of the polynomial-based scheme. Our scheme not only has efficiency in authentication but also can provide extra source privacy. The proposed scheme is compared with the bivariate polynomial-based scheme through simulations using ns-2. Our proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of delay, energy consumption, delivery ratio and communication overhead.

REFERENCES

[1] Jian Li, Jian Ren, Yun Li Senior Member, IEEE, & Jie Wu, Fellow, IEEE, “Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks,” IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 5, May 2014

[2] F. Ye, H. Lou, S. Lu, & L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” Proc. IEEE INFOCOM, Mar. 2004.

[3] Perrig, R. Canetti, J. Tygar, & D. Song, “Efficient Authentication and Signing of Multicast Streams over Lossy Channels,” Proc. IEEE Symp. Security and Privacy May 2000.

[4] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, & M. Yung, “Perfectly-Secure Key Distribution for Dynamic Conferences,” Proc. Advances in Cryptology (Crypto ’92), pp. 471-486, Apr. 1992.

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

[6] T.A. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[7] S.Jajodia,P.Ning,S.Setia&, S. Zhu, “An Interleaved Hop-By-Hop Authentication Scheme for Filtering False Data in Sensor Networks,” Proc. IEEE Symp. Security and Privacy, 2004.

[8] D. Pointcheval & J. Stern, “Security Proofs for Signature Schemes,” Proc. Advances in Cryptology (EUROCRYPT), pp. 387-398, 1996.

[9] M. Waidner, “Unconditional Sender and Recipient Untraceability in Spite of Active Attacks,” Proc. Advances in Cryptology (EUROCRYPT), pp. 302-319, 1989.