Message Authentication And Source Privacy using ECC in WSN

Chitrashree Kurtkoti
Department of Computer Science & Engineering
M.V.J College of Engineering
Bangalore, India

S. Pramela Devi
Department of Computer Science & Engineering
M.V.J College of Engineering
Bangalore, India

***Abstract*—In order to thwart unauthorised and corrupted messages from being forwarded in wireless sensor networks (WSN) we can make use of message authentication which is very effective way. In this regard many symmetric and public key cryptographic systems have been developed which suffered in their own limitations. Recently developed polynomial-based scheme also reported the limitation in its threshold value, as number of messages to be transferred should not cross the threshold limit. In this paper we propose a scalable authentication scheme based on Elliptic Curve Cryptography (ECC).Here our scheme enables intermediate nodes authentication and does not suffer with any threshold limit problem also provide message source privacy.**

Keywords—Hop by Hop authentication, Anonymous message, source privacy, ECC.

I. INTRODUCTION

Message authentication plays significant role in thwarting unauthorized and corrupted messages from being forwarded in WSNs in order to save precious sensor energy[2]. For this purpose many authentication schemes have been proposed those are symmetric-key based and public-key based approaches[6].

Symmetric-key based approach needs complex key management system and suffers from scalability issue and is not resilient to large node compromised attacks as same key is shared between sender and receiver of the message[3].

In order to solve scalability problem the secret polynomial based scheme was introduced. In this threshold is determined by the degree of the polynomial. The intermediate nodes verify authenticity by polynomial evaluation. However the number of messages transmitted is greater than threshold, polynomial can be fully recovered and the system is fully broken[1].

For public-key based scheme each message has to be sent along with digital signature generated using the sender's private key[4]. Every intermediate forwarder nodes can perform message authentication using their public keys. However scheme suffers with 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[5].

In this paper we propose secure and efficient source anonymous message authentication scheme (SAMA) and Modified ElGamal Signature scheme (MES) based on elliptic curve cryptography. Our proposed scheme make it possible for every intermediate nodes to authenticate incoming messages so that unauthorized and corrupted messages can be deleted and dropped in order to save the precious sensor energy. And the scheme does not have any threshold limit problem; the sensor nodes can send any number of messages.

II. THE PROPOSED METHOD

The proposed method aims to achieve at the following goals.

1. Message authentication: Each message receiver should be able to verify whether a received message is sent from the node that is claimed.
2. Message integrity: Each receiver node of message should be able to verify whether the message is altered en-route by the adversaries.
3. Hop by bop message authentication: Every intermediate node along the path is able to verify message authentication and integrity.
4. Identity and location privacy: The adversaries cannot determine the information of the message sender like sender's ID and location by analyzing the content of the message.

The proposed method includes the following steps.

1. Security server model.

2. Registration of nodes to security server.

3. Anonymous message generation by nodes.

4. Verification of message authenticity.

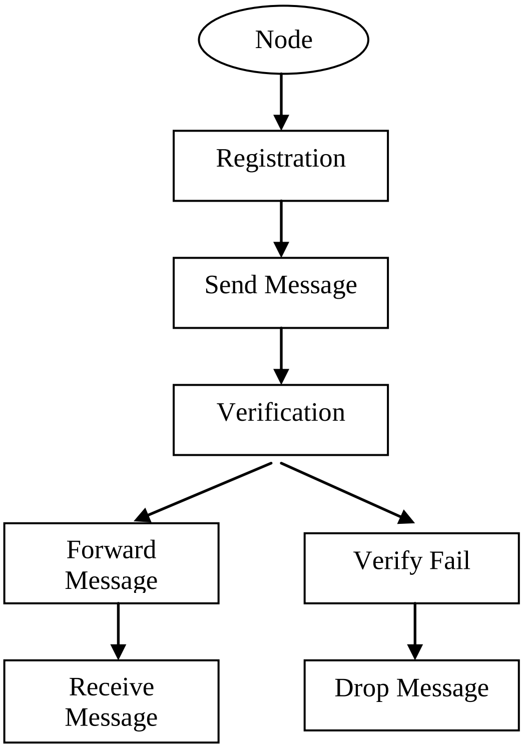

Fig1. Flow diagram of message transmission

A. *Security server model:*

- The wireless sensor network is assumed to be consisting of number of sensor nodes. Here our proposed method assumes that each sensor node know about its current location and can communicate with the neighbour nodes in the network.
- We assume there is security server in the network and each sensor node can register to it. Security server is responsible for generation of security parameters for each sensor node.

B. *Registration of nodes to security server:*

- Every sensor node can register to the security server with node name and its port number.
- Security server will generate keys for respective nodes and maintains the log of node profile.

C. *Anonymous message generation and vrification.[1]*

- Every node in the network will generate one anonymous message by using some code or byte of string from original message before sending original message to the other node.
- We have used here the secure anonymous message authentication (*SAMA*) scheme include following algorithms.
- Generate (m, Q1, Q2, Q3, Q4..): Given message m and public keys Q1, Q2, Q3, Q4…of security server log AS S={ A1, A2, A3, A4..}, the actual message sender **A**t, 1 ≤ t ≤ n ,produces an anonymous message S(m) using its own private key.
- Verify S(m): Given a message m and anonymous message S(m), which includes public keys of all members in the log AS, a verifier can determine whether S(m) is generated by member in AS.

D. *Verification of message authenticity.[1]*

- For verification of message authenticity we are using Modified ElGamal Signature scheme (MES) which is based on Elliptic Curve Cryptography (ECC).
- Modified ElGamal Signature scheme (MES) uses following three algorithms.
- Key generation algorithm: Let p be a large number and g be a generator of Ƶ*p. Both p and g are made public. For a random private key x € Ƶp., the public key y is computed by $y = g^x$ mod p.
- Signature algorithm: To sign a message one choose a random K € Ƶ*p-1, then computes the exponential $r = g^k$ mod p and solves s from:
- s = r x h (m, r) + k mod p-1. Where h is one way hash function. The signature of the message m is defined as pair of (r, s).
- Verification algorithm: Verifier checks whether the signature equation g^s = r$y^{rh(m,r)}$ mod p. If equality holds signature is accepted otherwise rejected.

III. ANALYSIS

The proposed algorithm uses Modified ElGamal Signature scheme to generate keys, signature and for verification. So it is expected when the message is forwarded in network by using the proposed scheme the efficiency is greater in terms of computational overhead, energy consumption and delivery ratio than the polynomial based approach.

IV. CONCLUSION

The proposed scheme provides very efficient level of security. It is very much difficult for the intruder or attacker to hack the message because of the security server which maintains the log of registered node profile and key information. And it is highly impossible for the attacker to compromise security server hence the method prevents node compromised attacks. The method SAMA provide message authentication at every hop in network which uses ECC. The method also provides the message source privacy so message found to be not from the intended sender immediately message is dropped[1].

REFERENCES

1. Jian Li Department of Electrical & Computer Engineering, Michigan State University, East Lansing, Yun Li SPD Department, Microsoft, Redmond ,Jian Ren Jie Department of Computer & Information Sciences, Temple University, Philadelphia .”Hop by hop message authentication and source privacy in wireless sensor networks”, in IEEE 2013.
2. 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..
3. 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.
4. William Stallings, “Cryptography and Network Security”, 3rd Edition.
5. Willium Stallings,”Network Security Essentials” , 2nd Edition.
6. Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, 4th Edition.