www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 5 May 2018, Page No. 23896-23900
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i5.04

Message Validation in Wireless Sensor Network

Shruti Amburle[1], Vaishali Khairnar[2]

[1]ME Student of Information Technology Department, Terna Engineer College, Nerul, Navi Mumbai, India
[2]HOD of Information Technology Department, Terna Engineer College, Nerul, Navi Mumbai, India

Abstract: Message authentication is one of the most efficient way to keep the data safe from unauthorized access and corrupted messages which is 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. Many schemes have the restrictions of high computational and communication transparency and deficient in the scalability 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 higher processing time determined by the degree of the polynomial when the number of messages transmitted is larger, the adversary can fully recover the polynomial.

This system allows the intermediate nodes authentication to transmit a larger number of messages without suffering with the time complexity problem. It is basically design to authenticate the message in network while transferring. Here we will utilize the elliptic curve polynomial y2 = (x3 + ax + b) mod p and comparison will be done between transmission with and without security mechanism of signatures. To prove that our approach is better than Polynomial based scheme we compare result between Elgamal signature analyses with ECC polynomial signature analysis.

Index terms: Hop by Hop Message Authentication, Digital Signature, elliptic curve polynomial, ECC polynomial signature analysis.

1.INTRODUCTION

In signature based message validation with source privacy in wireless sensor network, were authentication is effective way to protect from unauthorized users effected messages from being send through in wireless sensor networks. Most of the system used for message authentication will suffer from limitations of high overhead, lack of ability, to node attacks and threshold problem. Message authentication has a main role in discomforting the unauthorized and effected messages from being sent in networks to save the energy. Many of validation systems have been implemented to protect message and confirmation for wireless sensor networks. The symmetric key based approach has complicated key management and lacks of ways. It is not affected by the attacks since the message sender and the receiver have to share a secret key. The sender generates a key uses shared key to message authentication code for each transmitted message. The accuracy and reliability of message can authenticated only by the node using shared secret key, which is generally shared by a group of sensor nodes. An attacker can easily access the key by occupying a single sensor node. So, it will does not work in multicast networks.

To get the bottom of the problem, a secret based for the message authentication system was proposed. The method is similar to a threshold secret sharing, where it is determined by the degree of the value. This offers information security of the shared secret key when the number of messages transmitted is less than the threshold.

the public-key based method, each message is transmitted along with the digital signature of the message produced 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 precincts of the public key based method is the high computational overhead.
Message authentication is effective way to avoid illegal and
corrupted messages from being sent in wireless sensor networks (WSNs).So, many message authentication plan have been build up, based on either symmetric-key cryptosystems or public-key cryptosystems. In this paper, we propose a scalable authentication scheme based on elliptic curve cryptography (ECC) which again provide message source privacy.

Objectives:

- To develop a signature based message authentication on elliptic curves that can provide unconditional source anonymity.
- To propose an efficient midway node authentication mechanism for WSNs without the threshold limitation.
- To the devise network implementation criteria on source node privacy protection in WSNs.

2. RELATED WORK

The System which permits the sender to send a message to the receiver end such that if the modified message will almost detected by Receiver that termed as message authentication. We can also say that message authentication is data origin authenticity. The survey has been described as follows.
Paper [1] gives Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. Here the major issue of security is in wide level sensor network. In widespread sensor network detecting and removal of fake reports injected by compromised node is a greater challenge. It get the 80% to 90 % fake data by a compromised node. [2] An ideal hop-by-hop authentication scheme is implemented.
Theses can be achieve by clustering g certain group of nodes for interested area and we can also create a base station in a secure location to gather the data.
A new message authentication approach[3] which accept a polynomial-based technique to simultaneously accomplish the goals of lightweight, resilience to a large number of node compromises, immediate authentication, scalability, and non-repudiation. Extensive analysis and experiments have also been conducted to evaluate the scheme in terms of security properties and system overhead.
A new signature system is propose the Diffie - Hellman key distribution scheme that achieves a public key cryptosystem[4].
The paper [5] gives recent progress of elliptic curve cryptography (ECC) implementation on sensors motivates us to design a public-key scheme and compare its performance with the symmetric-key counterparts. This paper builds the user access control on commercial off-the-shelf sensor devices as a case study to show that the public-key scheme can be more advantageous in terms of the memory usage, message complexity, and security resilience.
By Keeping confidential who sends which messages, in a world where any physical transmission can be traced to its origin, seems impossible. The [6] unconditionally or cryptographically secure system, depending on whether it is based on one-time-use keys or on public keys, respectively. A protocol is described which allows to send and receive messages anonymously using an arbitrary communication network [7], and it is proved to be unconditionally secure. [8] It provides a bridge between cryptographic theory and cryptographic practice. In the paradigm we suggest, a practical protocol P is produced by first devising and proving correct a protocol PR for the random oracle model, and then replacing oracle accesses by the computation of an “appropriately chosen” function h.

3. PROPOSED SYSTEM

Message authentication is efficient ways to prevent unauthorized and corrupted messages from being forwarded in wireless sensor networks. Due to this , many message authentication schemes have been build up, based on either symmetric-key cryptosystems or public-key cryptosystems. In, we propose scheme based on elliptic curve cryptography (ECC).

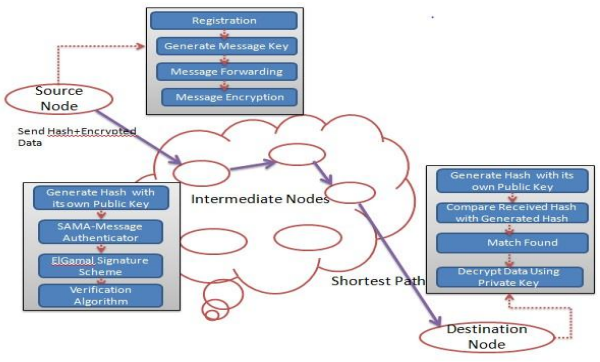

Fig.1 -Architecture diagram Of Proposed System

It is an secure and efficient source anonymous message authentication (SAMA) system based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This system allow the intermediate nodes to validate the message so that all corrupted message can be detected and fall to conserve the sensor power. It needs to develop a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. Then offer an efficient message authentication mechanism at each stage for WSNs without the threshold limitation.

The wireless sensor networks consist of a large number of sensor nodes. And each sensor node is well- known with its location in the sensor field and is able to communicate with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. In this project 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. but the sensor nodes after deployment compromised by aggressor. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the SS and other nodes.

Two types of attacks launched by the adversaries:

1) Passive attacks: Through passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis.

2**) Active attacks:** Active attacks can only be launched fromthe sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised nodes, including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages.

Design goals:

1) **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.
2) **Message reliability**: The message receiver can verified whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.
3) **Hop-by-hop message authentication:** Every intermediate node on the path should be able to confirm the authenticity and integrity of the messages upon reception.
4) **Identity and location privacy**: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.
5) **Efficiency:** The scheme should be efficient in terms both computational and communication overhead.

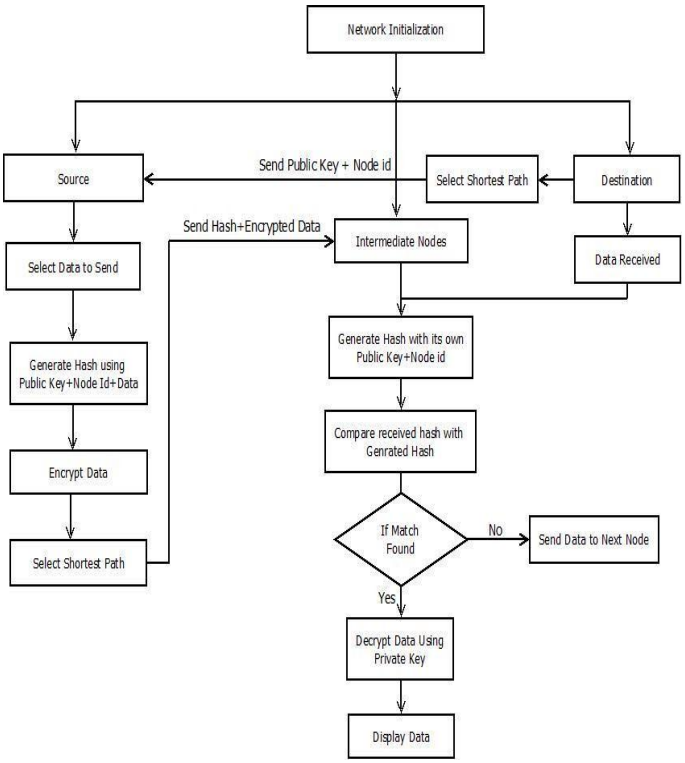

Figure2-System Workflow

4. PROPOSED METHOD Technique Used

1. Source Anonymous Message Authentication (SAMA) on Elliptic curves

A SAMA technique does not have the threshold problem. Unlimited numbers of messages are authenticated. SAMA isa secure and efficient mechanism. Generates a source anonymous message authenticator for the message m. The message generation is based on the MES scheme on Elliptic curves. An elliptic curve E is defined by an equation of the form:

$E : y^2=x^3 +ax + b \bmod p;$ ------- ------- (1)

1. Considering a base point elliptic curve.
2. Assuming the private key of sender node.
3. Calculate public key of sender.
4. The message is to be hashed and left bit of hash functions are converting into binary format.
5. Finding the signature of message.

Modified ElGamal Signature Scheme

Authentication generation algorithm: Sender node is sending the message to be transmitted to receiver node. (SAMA):

ASAMA consists of the following these steps:

1. Receiver node receiving the hashed message.
2. Left most bit of the hash is taken in decimal format.
3. If it receives same key means allow to transform and access that message.

5. RESULT

Comparision of Power Consumption of Existing vs Proposed (Elgamal vs ECDH)

Sr.No	Algorithm Name	Key Size	Time for Encryption	Key Size	Time For Decryption	Load ON CPU Existing	Load ON CPU Proposed	Power Existing (Elgamal)	Power Proposed (ECDH)
1	ElGamalNoneNoPadding	128	606.471594	128	364.8132	0.01	0.01	0.0085	0.0085
2	ElGamalNoneNoPadding	256	7591.376139	256	722.8163	0.03	0.02	0.0255	0.017
3	ElGamalNoneNoPadding	256	3434.470392	256	712.7761	0.029	0.02	0.02465	0.017
4	ElGamalNoneNoPadding	512	3842.313039	512	1084.9362	0.04	0.03	0.034	0.0255
5	ElGamalNoneNoPadding	1024	548461.4504	1024	1984.5031	0.05	0.04	0.0425	0.034

Table1:Comparison Of Power Consumption

Authentication is given to each hop fo forwarding the message from source to the destination through in the wireless sensor systems. Source node creates the authentication keys and signature in the WSN's, information from the source node finds the most efficient shortest way to reach the destination.

The communication and computational overhead and power consumption is greatly reduced in the system compared to the other existing system.Table 1 shows the comparrison of power usage between proposed system and existing system.

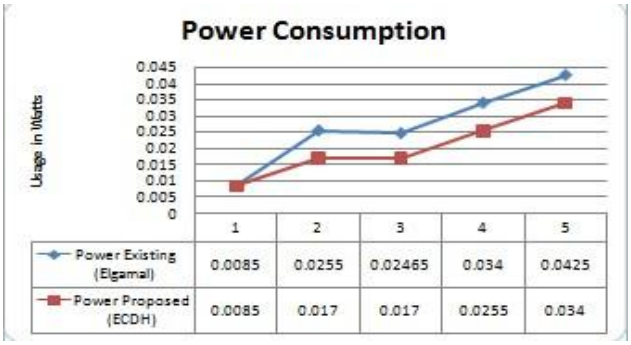

Fig 3-Power Consumption Graph

5. CONCLUSIONS

We propose an efficient signature based message authentication system. While ensuring message sender privacy, SAMA can be applied to any message to provide message content authenticity. To provide hop-by-hop message authentication with advances we built in threshold of the polynomial-based scheme, and gives a hop-by-hop message authentication scheme based on the SAMA.

The system transfer data from source to destination while performing authentication at each hop, and detect compromised nodes in the system if any This system better than other scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

REFERENCES

[1] D. X. Song, D.Wagner, and A. Perrig. "Practical techniques for searches on encrypted data."In Proceedings of the 2000 IEEE Symposium on Security and Privacy, Berkeley, CA, USA,May 2000.

[2] Y. Hwang and P. Lee, "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-User System," Pairing, vol. 4575, pp. 2-22, 2007.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou. "Privacy- preserving multi-keyword ranked search over encrypted cloud data." In Proceedings of the 30th IEEE International Conference on Computer Communications, Shanghai, China, Apr. 2011.

[4] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order- preserving symmetric encryption," in Proceedings of Eurocrypt'09, volume 5479 of LNCS. Springer, 2009.

[5] Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou"Secure Ranked Keyword

Search over Encrypted Cloud Data" In International Conference on Distributed Computing Systems, Chicago, 2010

[6] T. Moataz and A. Shikfa. "Boolean symmetric searchable encryption." In Proceedings of the8th ACM SIGSAC Symposium on Information, Computer and Communications Security,Hangzhou, China, May 2013.

[7] D. Boneh and B. Waters. "Conjunctive, subset, and range queries on encrypted data." InProceedings of the 4th IACR Theory of Cryptography Conference, Amsterdam, The Netherlands, Feb. 2007.