SECURED APPROACH FOR AUTHENTICATION OF MESSAGES IN WIRELESS SENSOR NETWORKS

Tejaswini B S[1], Praneetha G N[2], Bhavatarini N[3], Kavyashree K[4], Chaithra B M[5]

[1,2,3,4,5]*Assistant Professor, Dept. of Information Science & Engineering, Sapthagiri College of Engineering, Karnataka, India*

---***---

ABSTRACT: *Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects false data into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes. Standard authentication mechanisms cannot prevent this attack if the adversary has compromised one or a small number of sensor nodes. Message authentication is one of the prominent techniques to mitigate unauthorized and malicious access from being forwarded in wireless sensor networks (WSNs). In this paper, an efficient and robust authentication approach is introduced that is designed based on Elliptic curve cryptography.*

Keywords: **Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy**

1. INTRODUCTION

Message authentication is defined as the way of detecting at the receiver side wheather the message sent by the sender has been modified or not while travelling across transmission medium. Message authentication protects the integrity of the message. The special characteristics of Wireless sensor is the absence of infrastructure. And they also have limited bandwidth, energy constraints, and low computational capabilities. Inspite all these limitations wireless sensor networks have wide range of applications in military, medical field etc.

Since the node is deployed in a hostile environment the security becomes the major constraint in WSN. The WSN can be easily hacked by an attacker and he can gather all the private information which is present. In many cases it is sufficient to secure data transfer between the sensor nodes and the base station. In particular, the base station must be able to ensure that the received message was sent by specific sensor node and not modified while transferring. Many WSN applications needs strong and light weight authentication schemes to secure data from unauthorised users. To overcome all security issue many different scheme that had been discover. Some schemes detects the compromised node , detects the injected false message in the network or giving special authorization to the sender or receiver, Encryption of decryption is the most often used scheme for providing the security. Message authentication prevents the unofficial and corrupted message in WSN. It is a short piece of information used to authenticate a message and to provide integrity and authenticity to the message. Symmetric key cryptosystems or public-key cryptosystems are the various schemes that are proposed to provide authenticity and integrity of the message. These schemes have limitations such as high computational and communication overhead, lack of scalability, node compromise attacks. Many data gathering protocols are proposed in order to gather data from various nodes in a secure manner and there are various merits and demerits in each of them [2]. To implement Data gathering technique at the Base station authors have used iSense Modular Wireless Sensor Hardware and Software System of Coalesenses product [3].

2. PROBLEM STATEMENT

Purpose of the project is to provide intermediate node authentication without the threshold limitation, and to perform better than the symmetric-key based schemes. The distributed nature of algorithm makes the scheme suitable for decentralized networks.

Important purposes are as follows:

- To develop a source anonymous message authentication code [5] (SAMAC) on elliptic curves that can provide unconditional source anonymity.
- To offer an efficient intermediate node authentication mechanism for WSNs without the threshold limitation.
- To the devise network implementation criteria on source node privacy protection in WSNs.

3. PROPOSED SYSTEM:

The proposed work presents the new scheme of authentication scheme in WSN, though conventional cryptographic scheme used in WSN are not that efficient but the proposed work use multi-hop authentication scheme [3]. This modified scheme used is more efficient in authentication scheme such that the false or impersonator nodes participating cannot generate their own public key.

In this scheme the sender anonymity or the particular message is not linkable to any sender or the particular sender. The algorithms in the proposed work use signature generation and verification. In order to facilitate optimal security of the proposed model, the following are the product functions:

- The framework should work for all the participating nodes in the sensor network.
- The proposed project work should have an efficient and secure use of unique cryptographic key for performing message embedding and extraction process [1].
- The product utilizes Elliptical Curve Cryptography [4] for scalable authentication and the work also contributes message source privacy.
- The product also uses an unconditionally secure and efficient source anonymous message authentication scheme, based on elliptic curves.
- It enables the intermediate nodes to authenticate the message so that all corrupted packets can be dropped to conserve sensor power.

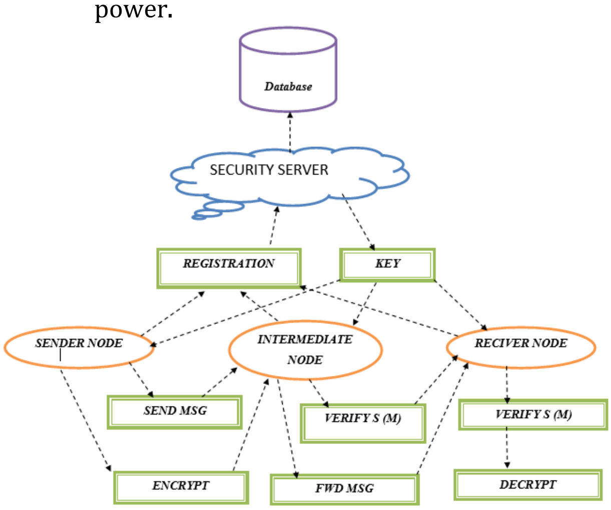

Fig 1: System Architecture

The system architecture of the proposed system is highlighted in Figure 2. The following are the assumptions of the proposed system:

- The basic assumption of the project work is that sensor Network consists of large number of sensor nodes.
- Each node can be data source or data sink and capable of communicating with its neighbour nodes directly.
- Another assumption is that the user is expected to use the standard encryption algorithm in a most secure system and network.

The following functional requirements provides a high level overview of the proposed authentication based WSN framework, in which the common activities, processes, and the products are described in relation to how they create, use, and modify information. Functional requirements of proposed system are specified as follows:

- Effective design of a message with public keys and indexing of actual message sender, and maintaining anonymity with private keys.
- Consideration of Sender ambiguity and Unforgeability for the proposed algorithm.
- The proposed system allows the user to deploy many number of sensor nodes and hop by hop authentication of sensor nodes by using Elliptical Curve Cryptography.
- The system also considers both passive and active attacks and compromised nodes cannot create new public key.
- The proposed system uses sender anonymity i.e. there will be no linkable of message to other senders.
- The proposed system also deploys the signature generation and verification on sensor nodes.
- The proposed system efficiently gives the multi-hop authentication for sensor nodes and the compromised nodes can be evaluated.

4. Design Goals

Proposed authentication scheme aims at achieving the following goals:

- **Node 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.
- **Message integrity:** The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.
- **Intermediate node authentication:** Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.
- **Identity and location privacy:** The adversaries cannot determine the message sender's ID and

location by analyzing the message contents or the local traffic.

- **Efficiency:** The scheme should be efficient in terms of both computational and communication overhead.

5. CONCLUSIONS

Message authentication schemes are used to improving the security in wireless sensor Networks. An efficient Source anonymous message authentication scheme based on ECC.To provide message content authenticity. This is Intermediate hop by hop message authentication. An intermediate nodes are authenticate and allow to transmit a message, does not have the threshold problem that is unlimited number of messages are verified compare than polynomial based scheme Proposed scheme is more efficient than the bivariate polynomial-based scheme such as memory and security.

REFERENCES

[1] Jian Li, Yun Li, Jian Ren, Senior Member, IEEE, and Jie Wu, Fellow, IEEE,"Hop-by-Hop Message Authentication and Source Privacy in WirelessSensor Networks", ieee transactions on parallel and distributed systems, vol. 25, no. 5, may 2014

[2] Bhat Geetalaxmi Jayram , D. V. Ashoka," Merits and Demerits of Existing Energy Efficient Data Gathering Techniques for Wireless Sensor Networks", International Journal of Computer Applications (0975-8887),Vol. 66, Issue 9, pp 15-22,March 2013.

[3] Bhat Geetalaxmi Jayram , D. V. Ashoka," Intelligent data gathering in distributed wireless sensor environment-A Real Scenario", International Journal of Scientific & Engineering Research(2229-5518), Vol. 5, Issue 2,pp 789-794, , March 2013, .

[4]http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[5] M. Bellare and P. Rogaway, "Random oracles are protocols," in Proc. CCS'93, 1993, pp. 62-73. practical: A paradigm for designing efficient