International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 7, July - 2013

A Robust Message Authentication Scheme In Multihop WSN Using Elliptical Curve Cryptography And Elgamal Signature

Mrs. Manjusha
Asst. Prof: Dept of Computer Science and Engg.
Nagarjuna College of Engineering
Bangalore, India

Ms. Laxmi B. Rananavare
Associate Prof:
Dept of Computer Science and Engg. Reva ITM,
Bangalore, 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 and ElGamal Signature Scheme.

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

I. INTRODUCTION

Consider a military application of sensor networks for reconnaissance of the opposing forces. Suppose we want to monitor the activities of the opposing forces, e.g., tank movements, ship arrivals or departures, and other relevant events. To achieve this goal, we can deploy a cluster of sensor nodes around each area of interest. We can then deploy a base station in a secure location to control the sensors and collect data reported by the sensors. To facilitate data collection in such a network, sensor nodes on a path from an area of interest to the base station can relay the data to the base station. The unattended nature of the deployed sensor network lends itself to several attacks by the adversary, including physical destruction of sensor nodes, security attacks on the routing and data link protocols, and resource consumption attacks launched to deplete the limited energy resources of the sensor nodes. Unattended sensor node deployment also makes another attack easier: an adversary may compromise several sensor nodes, and then use the compromised nodes to inject false data into the network. This attack falls in the category of *insider attacks*. Standard authentication mechanisms are not sufficient to prevent such insider attacks, since the adversary knows all the keying material possessed by the compromised nodes. We note that this attack can be launched against many sensor network applications, though we have only given a military scenario

In this paper, we propose an unconditionally secure and efficient source anonymous message authentication scheme, based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against no-message attacks and adaptive chosen-message attacks in the random oracle model. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted packets can be dropped to conserve 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. To the best of our knowledge, this is the first scheme that provides hop-by-hop node authentication without the threshold limitation, while having performance better than the symmetric-key based schemes. The distributed nature of our algorithms makes these schemes suitable for decentralized networks. The major contributions of this paper include: (i) we develop a source anonymous message authentication scheme on elliptic curves that can provide unconditional source anonymity; (ii) we offer an efficient hop-by-hop message authentication mechanism without the threshold limitation; (iii) we devise network implementation criteria on source node privacy protection in WSNs; (iv) we provide extensive simulation results under Matlab on multiple security levels.

In the proposed research paper, we highlight a message authentication technique using Elliptical curve cryptography and ElGamal digital signature scheme. In section 2 we give an overview of related work which identifies all the major research work being done in this area. Section 3 highlights proposed system followed by Implementation in Section 4.

Section-5 discusses about results and finally in section 5 we make some concluding remarks.

II. RELATED WORK

Investigating the problems and the research works for the message authentication and source privacy in the network, the following schemes have been found:

- C. Blundo et al [1] introduced a secret polynomial-based message authentication scheme. This scheme offers information theoretic security with ideas similar to a threshold secret sharing scheme, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation.
    - Limitations: Whenever the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system becomes completely broken.
- W. Zhang et al [2] enhanced the work done by C Blundo et al for increasing the threshold and the complexity for the intruders to break the secret polynomial and the perturbation factor.
    - Limitations: The added perturbation factor can be completely removed using error-correcting code techniques.
- H. Wang et al [3] compare the symmetric-key and public-key based security schemes in sensor networks and the result illustrates that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience since public-key-based approaches have simple and clean key management.
- R. Rivest et al [4] introduced message sender anonymity which is based on ring signatures. This approach enables the message sender to generate a source-anonymous message signature with content authenticity assurance. The original scheme has very limited flexibility and very high complexity. Moreover, the original paper only focuses on the cryptographic algorithm, and the relevant network issues were left unaddressed.
    - Limitations: The original scheme has very limited flexibility and very high complexity. Moreover, the original paper only focuses on the cryptographic algorithm, and the relevant network issues were left unaddressed.

Although the continuous efforts made for getting one potential scheme for the message authentication in the wireless communication network have been proposed but still few factors are to be resolved so as to accomplish the highly potent solution for message authentication and source privacy in the wireless communication network.

III. 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 using modified ElGamal signature [5] scheme for elliptic curves. 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.
- The product utilizes Elliptical Curve Cryptography [6] 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 the optimal modified ElGamal signature scheme on elliptic curves.
- It enables the intermediate nodes to authenticate the message so that all corrupted packets can be dropped to conserve sensor power.

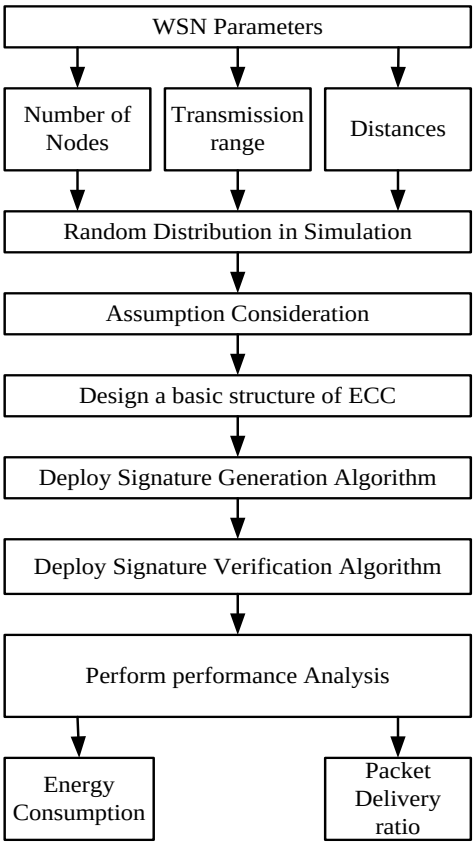

Figure 1: System Architecture of the proposed project

The system architecture of the proposed system is highlighted in Figure 1. 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 neighbor 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.
- Design of ElGamal signature scheme.
- Before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice. This set should include itself, together with some other nodes.
- 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 modified ElGamal signature scheme on elliptic curves for secure and efficient source authentication of nodes.
- 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.

IV. IMPLEMENTATION

The proposed system is implemented in 32 bit Windows OS with 2.84 GHz Intel core-i3 processor using Matlab as programming tool. An interface description for short is a specification used for describing a software component's interface. IDLs are commonly used in remote procedure call software. The interface initially considers a design of novel and efficient source anonymous message authentication scheme based on elliptic curve cryptography. While ensuring message sender privacy, the framework can be applied to any messages to provide hop-by-hop message content authenticity without the weakness of the built-in threshold of the polynomial-based scheme. In these cases the machines at either end of the "link" may be using different operating systems and computer languages. Interface Description offer a bridge between the two different systems. The project work is basically the software solution with no dependency on any specialized hardware devices. But still for the proper design of the hardware interface, the user needs to assure about the presence of proper windows 32-bit OS specifically of XP type of min 1GB of RAM. Matlab environment software needs to be installed for the proper operation of the framework application.

Algorithm: Multi-Hop Authentication in WSN

Input: WSN parameters

Output: data aggregation with multi-hop authentication

START

1. Initialize number of nodes

2. Check if the number of nodes are greater than 3 (or else it breaks operation)

3. Consider random topology

4. Consider number of base station ID (Sink)

5. Construct Message

6. Input Arguments: Number of Nodes, random Top, ID of BS

7. Initialize Elliptical Curve

8. Find the length of message [Reason: For formulating the encryption]

9. Initialize b as 1 and initialize q as n and B as 5.

10. For each value of x from 0-(q-1), compute c and d as output of

$$\begin{bmatrix} X \\ \mathrm{mod}(x^3 + x, n) \end{bmatrix}$$

11. Compute uniformly distributed three random integer between 1 and (q-1). Store as dA and dB and i.

12. Store ith element of c and d in P1 and ith element of c in P3.

13. Compute average of $\frac{1}{2}\sum^{i=1,j=2}(P1(i) + P1(j))$, Store in a.

14. Compute $\sum a + P3/2$ //Elliptic Curve Cryptography

15. Call EllipticCurvePointsModpOrder, pass P1, a, b, n to get Order.

16. Call EllipticCurveFastScalMult, pass P_1, d_A, a, b, n to get Q1.//Modified ElGamal Digital Signature Generation Algorithm

17. Call ElGamal Encrypt, pass P3, a, message, n, and Order and get A and C.

18. Call ElGamalDigitalSig_FM, and pass P3, a, message, n, Order and get P2, r, s. //Modified ElGamal Digital Signature Authenticate - Verification

19. Call ElGamalDigitalSigAuthenticate_FM and pass P2, r, s, A, n, Order

END

V. RESULTS

The proposed framework is simulated considering 50 number of nodes, it is seen than before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice. This set should include itself, together with some other nodes. When an adversary receives a message, he can possibly find the direction of the previous hop, or even the real node of the previous hop. The red markings indicate the active nodes that participate in performing the task of data aggregation i.e. cluster head. The last figure shows all dead nodes.

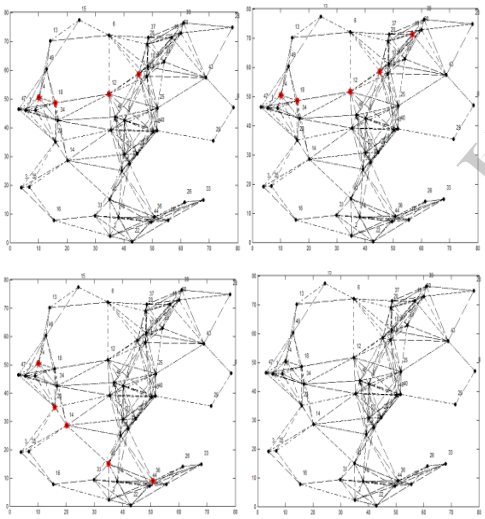

Figure 2: Simulation Results considering 50 Nodes

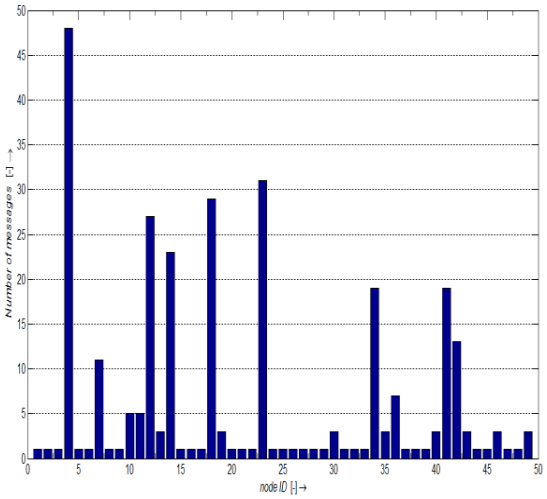

Figure 3: Simulation Results

Figure 3 highlights the simulation results that show that number of message of specified length successfully travels from node 0 to node 50 with less communication overhead and in more secure way.

VI. CONCLUSION

The proposed paper has discussed technique that ensures source anonymous message authentication technique based on elliptic curve cryptography. While ensuring message sender privacy, the proposed technique can be applied to any messages to provide hop-by-hop message content authenticity without the weakness of the built-in threshold of the polynomial-based scheme. Both theoretical and simulation results, conducted using Matlab show that the proposed framework gives better packet delivery ratio and secure hop based authentication of sensor nodes.

REFERENCES

[1] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in Advances in Cryptology - Crypto'92, Lecture Notes in Computer Science Volume 740, pp. 471–486, 1992

[2] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromiseresilient message authentication in sensor networks," in IEEE INFOCOM, (Phoenix, AZ.), April 15-17 2008.

[3] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control," in IEEE ICDCS, (Beijing, China), pp. 11–18, 2008.

[4] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Advances in Cryptology–ASIACRYPT, Lecture Notes in Computer Science, vol 2248/2001, Springer Berlin / Heidelberg, 2001.

[5] http://en.wikipedia.org/wiki/ElGamal_encryption

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