Avoiding Node Compromise Attacks in Wireless Sensor Network

S. Divya
M.E. Computer Science And Engineering
Surya Group of Institutions
Vikiravandi,Villupuram

B. Lakshmi Devi
Assistant Professor
Surya Group of Institutions
Vikiravandi, Villupuram

ABSTRACT
Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to falsedata injection attacks. In a large-scale sensor network individual sensors are subject to security compromises. Numerous authentication schemes have been proposed in the past for protecting communication authenticity and integrity in wireless sensor networks. Most of them however have following limitations: high computation or communication overhead, no resilience to a large number of node compromises, delayed authentication, lack of scalability, etc. To address these issues, we propose message authentication approach which adopts a scalable authentication scheme based on elliptic curvecryptography (ECC). While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, our scheme can also provide message source privacy.Theotrical and simulation results are compared.

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

1. INTRODUCTION
Message authentication is used to prevent the unauthorized and corrupted message .To provide message authenticity and integrity verification for wireless sensor networks many authentication schemes have been proposed [1],[2],[3]. The scheme is divided into two categories: public-key based approaches and symmetric-key based approaches.

The symmetric-key based approach has some scalability problem since a secret key is shared by message sender and the receiver. To generate a message authentication code (MAC) for each transmitted message a sender uses the shared key. To solve the scalability problem the secret polynomial based scheme is introduced, it is similar to threshold sharing and it is determined by degree of polynomial. The authenticity of the message is verified through polynomial evaluation.

In this paper, we propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme, based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted packets can be dropped to conserve sensor power.

The major contributions of this paper include: (i) we develop a source anonymous message authentication (SAMA) 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 ns-2 on multiple security levels.

2. TERMINOLOGY AND PRELIMINARY

2.1 Models and Assumptions
The wireless sensor network consists of large number of sensor nodes. The whole network is connected through multi-hop communications. This server will never be compromised. Once compromised, all information stored in the sensor nodes can be accessed by the attackers.

Based on the above assumptions, this paper considers both passive attacks and active attacks.

2.2 Design Goals
Our proposed authentication scheme aims at achieving hop-by-hop message authentication, compromised node resilience, efficiency, message authentication, message integrity.

3. PROPOSED ALGORITHM
SAMA consists of the following two algorithms:

3.1 Signature generation
1. Generate message (m,Q1,Q2, · · · ,Qn). For Sender Node to sign a message m, it follows steps 2 to 6
2. Select a random integer $r=k_A$, 1 <=kA <= N − 1.
3. Given a message *m* and the public keys $Q_1,Q_2, \cdots ,Q_n$ of the AS (ambiguity set) S ={$A_1,A_2, \cdots ,A_n$}
4. Considers Message sender A_t,1 ,<=t<=n produces an anonymous message S(m) using its own private key d_t.
5. Calculate *s*=hA =h(m, r), where h is a cryptographic hash function, such as SHA-1 or MD5, and l − denotes the leftmost bits of the hash.
6. The generated signature is the pair (r, s).

3.2 Signature verification algorithm
1. Given a message *m* and an anonymous message S(m), which includes the public keys of all members in the AS.
2. To verify S(m), Receiver Node to authenticate sender's signature, it must have a copy of her public key QA, then follow the steps.
3. Checks that QA lies on the curve.
4. Verify that s is an integers in [1,N − 1]. If not, the signature is invalid
5. Check X1=hA =h(m, r), where h is the same function generated during signature generation.
6. The signature is valid if r = x1, invalid otherwise.

7. A verifier can determine whether S(m) is generated by a member in the AS.

4. IMPLEMENTATION

4.1 Node deployment

The wireless sensor networks consist of a large number of sensor nodes. Each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighbouring nodes by geographic routing. The whole network is fully connected through multi-hop communications. We consider a wireless sensor network with N nodes. Let N denote the set of all nodes in the network. The communication among all n nodes is based on tree topology with the sink as the root. The tree is formed in the initial phase as follows. The sink first broadcast a message with a hop counter. The nodes receiving the message will set the message sender as the parent node, increase the hop counter by one, and broadcast it to their neighbours. Data are transferred along the edges in this communication tree.

4.2 One Hop Neighbour discovery

A sensor network with a graph G(k)= (V(k),e(k)), whose node set V(k) represents the sensor nodes active at time k and the edge set e(k) consists of pairs of nodes (u,v) such that nodes u and v can directly exchange messages between each other at time k. By an active node we mean a node that has not failed permanently. All graphs considered are undirected, i.e., (i, j) =(j,i). The neighbours of a node i is the set Ni of nodes connected to i, i.e., Ni. The number of neighbours of i, is called its degree, which is denoted by di(k). A path from i to j is a sequence of edges connecting i and j. A graph is called connected if there is a path between every pair of nodes. From source node to destination node, neighbours of a source node are taken and all possible paths are created.

4.3 Ambiguity Set (AS)

Choosing of AS provides source privacy. It also prevents adversaries from tracking the message source before message is transmitted. The source node selects an AS from public key list. When another node receives this, he can find the previous hop, but cannot guess whether it is the actual source node. Steps to select an AS:

- AS should include node from opposite direction.
- Based on geographic routing ,some nodes cannot be included in AS
- Active routing path nodes are selected in AS.

This concept can be explained by taking an example of 25 nodes and finding a path from a given node to a destination node as shown in **Figure 1**.

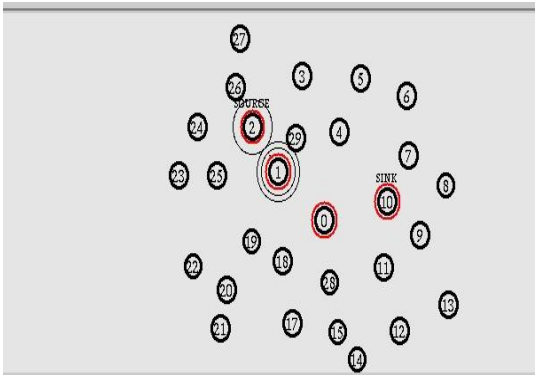

Fig: 1Source Privacy

4.4 Signature generation

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. Signature generation is done using two methods, first one is random ID generation, in which random ID is generated and assigned to all initialized nodes. The second one is SHA-1 ID generation, in which an unique ID is generated through SHA-1 algorithm and assigned to nodes.

4.5 Source Anonymous Message Authentication (SAMA) scheme

Message authentication is done when the source node transmits packet via relay nodes to destination. Under SAMA scheme, relay node check the random ID of the message forwarder, if the ID is correct, then the message is authenticated.

4.6 ModifiedElGamal Signature (MES) Scheme

Message authentication is done when the source node transmits packet via relay nodes to destination. Random ID is generated and assigned to all nodes. Similarly, a cryptographic hash function, such as SHA-1 is used to create another unique ID ‘h’ and assigned to all nodes. Under MES scheme, relay node check the random ID and SHA-1 generated ID of the message forwarder, if the ID is correct, then the message is authenticated.

5. SIMULATION

A simulation of SAMA and MES has been done on ns2, considering a random network of 25 nodes. A routing path has been calculated and is provided source privacy while transferring message with hop by hop network of 25 nodes .A graph has been plotted considering different ranges and corresponding distances has been plotted.

5.1 Delay

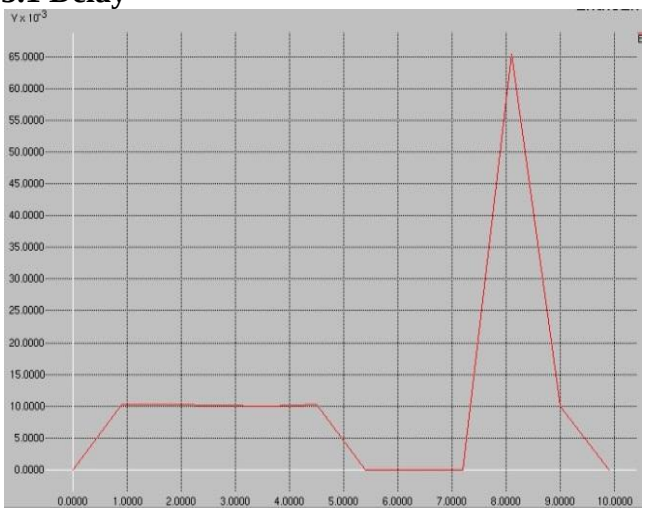

Fig 2 End to End Delay

The above graph figure 2 defines the delay in the simulation phase. The experiment was running 10 seconds of time. End to End Delay refers to the time taken for a packet to be transmitted across a network from source to destination during the simulation time

5.2. Through put

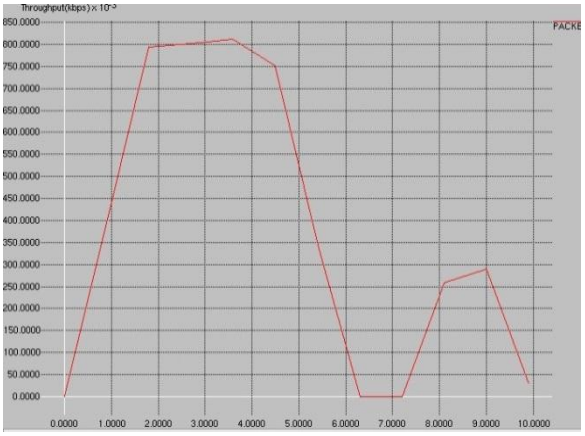

Fig: 3 Through put

The above graph figure 3 defines the throughput for the proposed protocol. The experiment was running 10 seconds of time. Throughput is the rate at which a network sends receives data. It is a good channel capacity of net connections and rated in terms bits per second (bit/s).

5.3 Packet loss

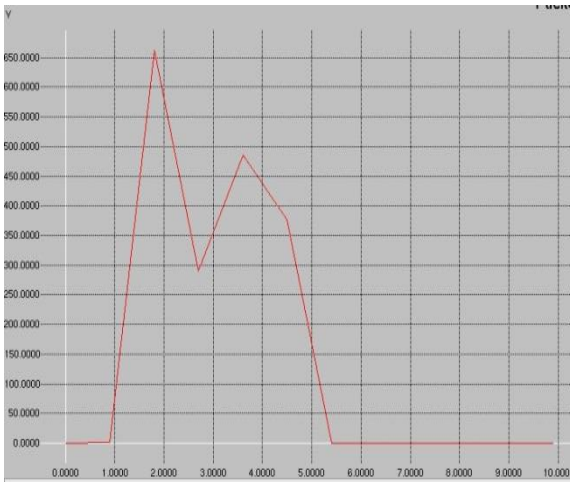

Fig: 4 Packet Loss

The above graphfigure 4 defines packet drop in the simulation time. The experiment was running 10 seconds of time. Packet Loss is where network traffic fails to reach its destination in a timely manner. Most commonly packets get dropped before the destination can be reached.

6. CONCLUSION

In this approach an efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC). While ensuring message sender privacy, SAMA can be applied to any message to provide message content authenticity. To provide hop-by-hop message authentication without thresholdwe then propose a hop-by-hop message authentication scheme based on the SAMA. When applied to WSNs with fixed sink nodes, also discussed possible techniques for compromised node identification. In future,the low energy capacity assigned to each node and provided efficient routing to maximize the lifetime of sensor nodes. Also, more comparisons study can be done with other protocols

7. REFERENCES

[1] 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.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in IEEE Symposium on Security and Privacy, 2004.

[3] 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, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

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

[5] 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.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking crypto graphic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org/.

[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications. of the Assoc. of Comp. Mach., vol. 21, no. 2, pp. 120–126, 1978.

[8] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory,vol. 31, no. 4, pp. 469–472, 1985.

[9] 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, 2008, pp. 11–18.

[10] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 1070, 1996, pp. 387–398.

[11] D. Chaum, "Untraceable Electronic Mail, Return Addresses, andDigital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb.1981. [12] D. Chaum, "The Dinning Cryptographer Problem: UnconditionalSender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1,pp. 65-75, 1988.