ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (222-227), Month: January - March 2015, Available at: www.researchpublish.com

Efficient Message Authentication and Source Privacy in Wireless Sensor Networks

A. Arul packiaraj[1], M. Merlin Moses[2]

PG Student, Einstein college of Engineering, Tirunelveli, India
Assistant Professor, Einstein college of Engineering, Tirunelveli, India

Abstract: **Message authentication is used to prevent the unauthorized messages forwarded in the Wireless Sensor Networks (WNS). The main aim of this project is to prevent unauthorized and corrupted message by allowing intermediate efficient node authentication. Many authentication schemes have been proposed to provide message authenticity; these schemes can be either public-key based approaches or symmetric-key based approaches. Scalable authentication scheme based on Elliptic Curve Cryptography (ECC) enables the intermediate node to authenticate the message and provide Hop by Hop message authentication. Route request is encrypted for authentication of messages with source privacy. An efficient key management framework is proposed to ensure isolation of the compromised node. The compromised node will be identified and alert information sends to all nodes.**

Keywords: **Wireless Sensor networks, Message authentication, Source privacy, Symmetric key cryptosystem, compromised node.**

I. INTRODUCTION

A wireless sensor network (WNS) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location. The WSN is built of "nodes" from a few several hundreds or even thousands, where each node is connected to one sensors. Message authentication plays an important role in thwarting unauthorized and corrupted messages from being forwarded in Wireless Sensor Networks. For this reason many authentication schemes introduce to provide message authenticity. The schemes can largely divide into two categories: Public-key based approaches and Private Key based approaches. The symmetric key based approach requires complex key management, lack of scalability, and not resilient to large number of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a Message Authentication code for each transmitted message. An intruder can compromise the key by capturing a single sensor node.

To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial. When the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial. A source anonymous message authentication code (SAMAC) is designed based on elliptic curves that can provide security. This scheme mainly for source privacy it will be defined by the route request is encrypted and send to all nodes. . An authentication scheme is designed to achieve the following goals: message authentication, message integrity, hop by hop message authentication, identity and location privacy, and to increase efficiency.

II. REVIEW OF LITERATURE

Fan Ye, Haiyun Luo, Songwu Lu and Lixia Zhang in paper titled statistical en-route filtering of injected false data in sensor networks[1] proposed a statistical en-route filtering(SEF) mechanism. This method is used to detect the false report and drop the false report during forwarding prosess in WSN. It filter the false report through collective decision-making by multiple detecting nodes. Assuming that the same event can be detected by multiple sensors, in SEF each of

the detecting sensors generates a keyed message authentication code (MAC). SEF exploits the network scale to filter out false reports through collective decision-making by multiple detecting nodes. multiple surrounding sensors collectively generate a legitimate report and endorse it by attaching to it their message authentication codes (MACs); a report with an inadequate number of MACs will be dropped.

Sencun Zhu Sanjeev Setia Sushil Jajodia Peng Ning in paper titled interleaved hop-by-hop authentication against false data injection attacks in sensor networks [2] proposed an interleaved hop by hop authentication method. Standard authentication echanisms cannot prevent if the adversary has ompromised one or a small number of sensor nodes. The base station can detect injected false data immediately when no more than t nodes are compromised, where t is a system design parameter. Schemes enable for an intermediate forwarding node to detect and discard false data packets as early as possible. This provide the authentication by the base ation. The base station in a secure location to control the sensors and collect data reported by the sensors.

Wensheng zhang and Nalin Subramanian guiling wang in paper titled lightweight and compromise-resilient message authentication in sensor networks [3] proposed a novel message authentication approach. This method adopts polynomial based technique and to achieve some goals like resilience to a large number of node compromises, immediate authentication, scalability, and non repudiation. Polynomial schemes for message authentication,which provides higher adaptability than existing authentication techniques based on multiple MACs. The polynomial based message authentication uses bivariate polynomial based method for authenticating message sent from trust worthy base station to ordinary sensor nodes.

A.Perrig, R. Canetti, J. Tygar, and D. Song in paper titled efficient authentication and signing of multicast streams over lossy channels [4] proposed two methods for authenticating data streams efficiently in the lossy environment in wireless sensor networks. TESLA (Timed Efficient Stream Loss-tolerant Authentication) is a first solution uses only symmetric cryptographic primitives such as pseudorandom functions and message authentication code. This scheme has some properties like Low computation overhead, arbitrary packet loss tolerated, and unidirectional dataflow. EMSS(Efficient Multichained Stream Signature) is a second solution and it is based on signing a small number of special packets in a data stream for providing authenticity in wireless sensor networks. It amortizes the cost of a signature operation over multiple packets, typically about one signature operation per 100 to 1000 packets.

Riaz Ahmed Shaikh, Hassan Jameel, Brian J.Auriol, Heejo Lee,Sungyoung Lee and Young Jae Song in paper titled achieving network level privacy in wireless sensor networks [5] proposed route and location privacy algorithms and data privacy mechanism. Full network level privacy has often been categorized into four sub-categories Identity, Route, Location and Data privacy. To achieve full network level privacy is a critical and challenging problem due to the constraints imposed by the sensor nodes (e.g., energy, memory), sensor networks (e.g., mobility and topology) and Quality of services issues (e.g., packet reach-ability).

III. PROPOSED SYSTEM

The main aim is to prevent unauthorized and corrupted messages being forwarded by allowing intermediate node authentication. Scalable authentication scheme based on elliptic curve cryptography (ECC). This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise resiliency, flexible-time authentication and source identity protection, the proposed scheme does not have the threshold problem.

This authentication scheme is designed to achieve the following goals: message authentication, message integrity, hop by hop message authentication, identity and location privacy, node compromise resilience, and to increase efficiency. The major contributions of this proposed method are the following: Firstly to develop a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. Secondly to offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation. Thirdly to devise network implementation criteria on source node privacy protection in WSNs and to propose an efficient key management framework to ensure isolation of the compromised nodes. The proposed scheme is more efficient in terms of computational and communication overhead under comparable security levels while providing message source privacy. Figure [1] shows that the process of message authentication and privacy.

The WSNs are assumed to 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 neighboring nodes directly using AODV. The whole network is fully connected through multi-hop communications. This scheme provides 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. However, after deployment, the sensor nodes may be captured and compromised by attackers.

Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled 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. The appropriate selection of an Ambiguity Set plays a key role in message source privacy, since the actual message source node will be hidden in the AS. This section discusses techniques that can prevent the adversaries from tracking the message source through the AS analysis in combination with local traffic analysis.

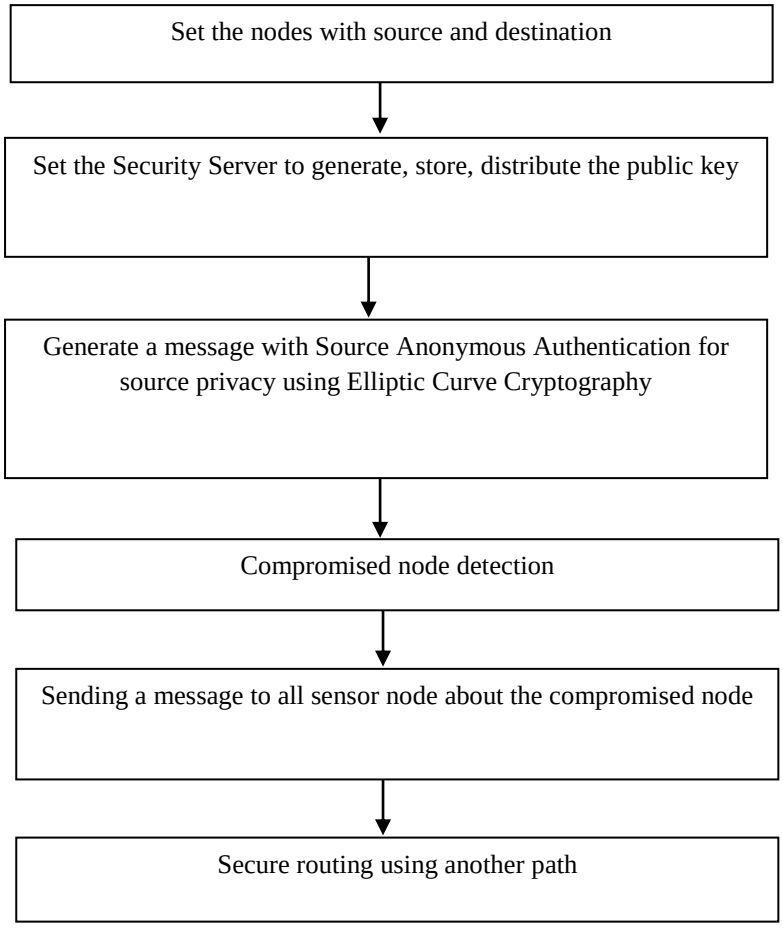

Fig: [1] Process of message authentication and source privacy

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. However, the adversary is unable to distinguish whether the previous node is the actual source node or simply a forwarder node if the adversary is unable to monitor the traffic of the previous hop.

Source anonymous message authentication:

Sender anonymity means that a particular message is not linkable to any sender, and no message is linkable to a particular sender. The proposed method uses Source Anonymous Message Authentication consists of the following two algorithms namely signature generation and signature verification algorithm.

Signature generation:

Given a message m and the public keys $Q_1,Q_2, \ldots Q_n$ of the AS (Ambiguity Set) $S=\{A_1,A_2, \ldots,A_n\}$, the actual message sender A_t , $1 \leq t \leq n$, produces an anonymous message S(m) using its own private key d_t.

Signature verification:

Given a message m and an anonymous message S(m), which includes the public keys of all members in the AS, a verifier can determine whether S(m) is generated by a member in the AS.

Ad hoc on-demand distance vector (aodv) routing:

The AODV Routing Protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the Route Request packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single Route Request.

Key distribution:

In key distribution SHA1 is used. SHA1 stands for "Secure Hashing Algorithm". The sensor node may be captured and compromised by the attackers. Once compromised, all information stored in the sensor node will be accessible to the attackers and further assume that the compromised node will not be able to create new public keys that can be accepted by the SS. For efficiency, each public key will have a short identity.SHA1 is currently the most widely used SHA hash function, although it will soon be replaced by the newer and potentially more secure SHA2 family of hashing functions. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP.SHA1 outputs a 160bit digest of any sized file or input. In construction it is similar to the previous MD4 and MD5 hash functions, in fact sharing some of the initial hash values. It uses a512 bit block size and has a maximum message size of 2^{64} -1 bits.

SHA1 Algorithm description:

Padding- Pad the message with a single one followed by zeroes until the final block has 448 bits. Append the size of the original message as an unsigned 64 bit integer.

1. Initialize the 5 hash blocks (h0,h1,h2,h3,h4) to the specific constants defined in the SHA1 standard. Hash (for each 512bit Block).
2. Allocate an 80 word array for the message schedule, Set the first 16 words to be the 512bit block split into 16 words.
3. Loop 80 times doing the following.
4. Calculate SHAfunction() and the constant K (these are based on the current round number.
   - e=d
   - d=c
   - c=b (rotated left 30)
   - b=a
   - a = a (rotated left 5) + SHAfunction() + e + k + word[i],Add a,b,c,d and e to the hash output.
5. Output the concatenation (h0, h1, h2, h3, h4) which is the message digest.

IV. RESULT AND DISCUSSION

Packet loss:

The packet loss of the network is defined as the failure of one or more transmitted data to arrival at the user. When packetloss is low the efficiency of message is high. From the simulation result existing packetloss compare with proposed packetloss. Message authentication is increase when packetloss is low.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (222-227), Month: January - March 2015, Available at: www.researchpublish.com

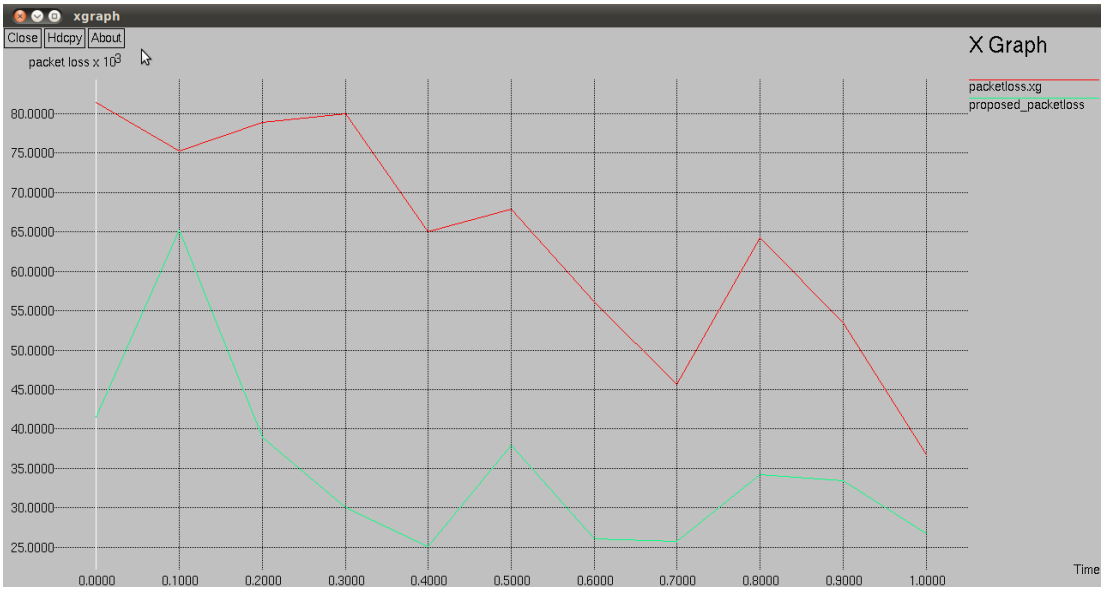

Fig: [2] Packetloss

Throughput:

Throughput of the network is defined as how much data can be transferred from the base station to the user in the given amount of time. From the simulation result indicates throughput level is high when compare with existing methods. When throughput level is high the pcketloss is low and the hop by hop message will receive without packetloss.

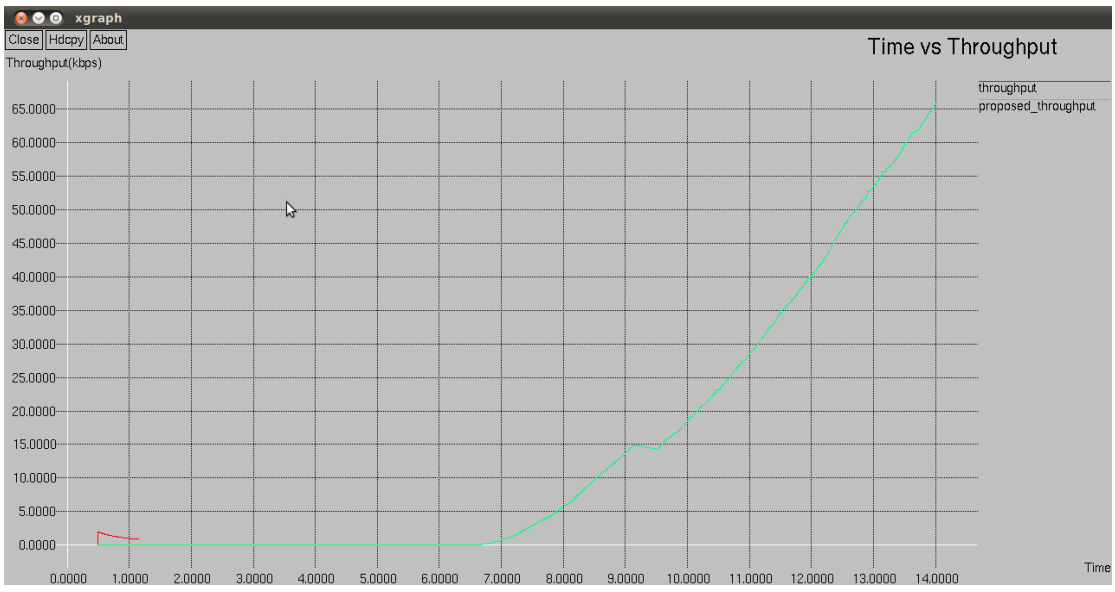

Fig: [3] Throughput

V. CONCLUSION

This scheme first proposes a novel and efficient SAMA based on 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 the weakness of the built in threshold of the polynomial-based scheme, this scheme then proposed a hop-by-hop message authentication scheme based on the SAMA. SHA1 algorithm is used for key distribution. When applied to WSNs with fixed sink nodes, it also discussed possible techniques for compromised node identification. Both theoretical and simulation results shows that in comparable scenarios this proposed scheme is more efficient than the other scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

ACKNOWLEDGEMENT

I sincerely thank my college and my guide Mr. Merlin Moses for his full support and encouragement for preparing this paper.

REFERENCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, Mar. 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," Proc. IEEE Symp. Security and Privacy, 2004.

[3] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

[4] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authenticationand Signing of Multicast Streams over Lossy Channels," Proc.IEEE Symp. Security and Privacy, May 2000.

[5] Riaz Ahmed Shaikh , Hassan Jameel , Brian J. d'Auriol , Heejo Lee , Sungyoung Lee,and Young-Jae Song "Achieving Network Level Privacy in Wireless Sensor Networks" Article about sensors, February 2010.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

[7] 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," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

[8] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. Advances in Cryptology (Crypto '92), pp. 471-486, Apr. 1992.

[9] Xi, Y.; Schwiebert, L.; Shi, W. Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks. In Proceedings of Parallel and Distributed Processing Symposium (IPDPS 2006), Rhodes Island, Greece, 2006.

[10] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology," , Feb. 2008.