ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015
International Journal of Innovative Trends and Emerging Technologies

# PROVIDING SOURCE PRIVACY IN WIRELESS SENSOR NETWORK USING MESSAGE AUTHENTICATION SCHEME BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

SELVARAJAN J[1], ARRVIND M[2], HEMAKUMAR B[3], JAGADEESAN M[4], DR. D JAYASHREE[5] B.UDAYA[6]
[1,2,3,4]UG [Scholar], [5,6]Professor, [1,2]Department of Computer Science and Engineering,
[1,2] Rajalakshmi Institute of Technology, Chennai, Tamil Nadu, India,
[1]selva0328@gmail.com, [2]arrvind.m.2011.cse@ritchennai.edu.in, [3]kumar.suba93@gmail.com
4jagadeesanm6@gmail.com, [5]hod.cse@ritchennai.edu.in, [6]udaya.b@ritchennai.edu.in

***Abstract* – With advancements in sensor network deployment, various applications use sensor nodes to meet the needs of our lives. Wireless Sensor Network (WSN) consists of hundreds to several thousand sensor nodes communicate locally with neighboring sensors and send data over peer-to-peer sensor network. However, sensor networks face challenges to provide security using public key cryptosystem. Sensor networks are also vulnerable to several node attacks by an adversary. For this reason, message authentication schemes are required to thwart such node attacks from an attacker. In this paper, a scalable authentication scheme is proposed based on Elliptic curve cryptography (ECC). The message authentication scheme proposed also provides source privacy.**

***Index Terms – WSN,*** *Source privacy, Message authentication, Public key cryptosystem; Elliptic Curve Cryptography*

## 1 INTRODUCTION

Wireless Sensor Networks (WSN) consist of numerous small nodes that can sense, collect, and spread information for many different types of applications such as energy management, medical monitoring, logistics, inventory management, to interact with the physical world. Usually, sensor networks are deployed in adverse or hostile environment and are used to collect and organize the information. However, sensor nodes are subject to several attacks which can lead to false alarms in these networks. [14, 17]. These attacks range can range from accidental node failures to intentional tampering.

Consider a military application of sensor networks where the force activities are to be monitored (e.g., tank movements, ship arrivals or departures) [19]. To achieve this, a cluster of sensor nodes have to be deployed around the area of interest. A base station has to be deployed in a secure location to control the sensor nodes and obtain data from the sensor nodes [19]. So, sensor nodes on a path from an area of interest to the base station can facilitate data. However, the unattended nature of sensor networks leads to several attacks, such as, physical destruction of sensor nodes, security attacks on routing protocols, resource consumption attacks, node compromise attacks, etc. [19]. Several schemes and mechanisms have been proposed to manage problems faced by wireless sensor networks [2, 3 6, 9, 10, 12, 16 - 19, 21, 23].

There are two types of attacks are considered – passive attacks and active attacks [25]. Passive attacks are the ones in which the adversary eavesdrop on messages transmitted. Active attacks are launched only when a node is compromised by an attacker. The attacker can modify the contents of messages and also inject their own messages into the sensor networks.

The deployment of sensor network makes it vulnerable to false data injection attacks. An adversary may compromise several nodes to inject false data into the network. In this paper, an unconditionally secure and efficient anonymous message authentication scheme based on elliptic curve cryptography is considered. The scheme enables intermediate nodes to authenticate messages.

So, the paper can be summarized as follows:

1. An anonymous message authentication based on elliptic curves is considered.
2. An efficient hop-by-hop authentication mechanism for Wireless Sensor Networks is developed.

The rest of the paper is organized as follows. Section 2 provides the related work for this paper. The proposed scheme is discussed in Section 3. Section 4 Authentication on Elliptic curves. Section 5 The security analysis. Section 6 Conclusion.

## 2 RELATED WORK

Earlier, numerous authentication mechanisms have been proposed for thwarting various attacks in wireless sensor networks [18, 19, and 21]. Ye F et. al. proposed a statistical en-route filtering (SEF) mechanism. While sending injected bogus reports from a compromised node, this mechanism detected and neglected these false reports [18]. In that they assumed that the false reports can be detected by multiple sensors. So, in SEF mechanism, each of the sensor generated a keyed message authentication code (MAC). Each MAC is attached to the event report and is verified by each sensor node. Zhu et. al S. proved that a standard authentication mechanism is not enough to prevent false data injection attacks over sensor networks. So, Zhu et. al S. proposed an interleaved hop-by-hop authentication scheme. When the base station detected any injected false data packets [19].

Most of the authentication schemes proposed had limitations, such as, high communication overhead, lack of scalability, resilience, etc. In order to overcome these limitations, Zhang S et.al [] proposed a message authentication scheme which includes a perturbed polynomial-based technique [21]. The polynomial had a

built-in threshold determined by the degree of the polynomial. This author, Perrig A et. al. presented two efficient authentication schemes: TESLA and EMSS [12]. TESLA, abbreviated for Timed Efficient Stream Loss-tolerant Authentication and EMSS, abbreviated for Efficient Multi-chained Stream signature provides a strong sender and slightly delayed authentication [12]. Blundo C et. al. analyzed a secure key distribution scheme for a group of users called 'conferences' [6]. Using this scheme, Blundo C et. al. presented a model with its adaptation to network topologies and to communication models (e.g., client-server) [6]. Another efficient key management scheme was proposed by Eschenauer L et. al. [16]. This scheme constituted selective distribution and revocation of keys to sensor nodes efficiently [16]. Chan H et. al. presented a framework for pre-distribution of key for sensor networks [17].

The implementation of security mechanisms in sensor networks is quite difficult due to the constrained nature of sensor nodes [23]. Albrecht M et. al. examined an approach based on perturbation polynomials and showed attacks on cryptographic schemes in sensor networks [23]. The approach is applied on to a key pre-distribution scheme, an access control scheme and an authentication scheme [23]. Rivest R.L. et. al. proposed an encryption method that implemented the public-key cryptosystem and preserved the properties of electronic mail system [1]. Further, D. Chaum et. al. presented a technique that allowed electronic mail to cover up the person communicating with the content [2]. Rivest R.L. et. al. also introduced a technique of ring signatures that verified the sign of electronic mail by the intended recipient [15]. ElGamal T presented a digital signature scheme along with key distribution scheme that achieved the public key cryptosystem [3]. The scheme proposed depends on the computing discrete logarithms [3]. Security proofs were introduced for digital signature schemes by Pointcheval D et. al. [10]. For signature schemes, a message recovery scheme based on discrete logarithms is proposed by Nyberg K et. al. [9]. Wang H et. al. compared symmetric-key and public-key schemes and built a user access control on sensor networks [22].Wang H et. al. also provided insights on the integration of public-key mechanisms for sensor networks [22]. To address the problem of confidentiality, Chaum D et. al. introduced a secure cryptographic scheme based on one-time-use keys or on public keys [26]. Pfitzmann .A et. al. summarized basic concepts of observability of sender and recipient and proposed suitable enhancements [4]. Reiter M.K. et. al. presented a system called 'Crowds' that hide user's anonymity over the Internet [11]. This system addressed the issue of anonymity for web transactions [11]. For untraceability of sender and recipient, Waidner M et. al. described a protocol that sent and received message anonymously through a communication network [5].

# 3 PROPOSED SCHEME

## 3.1 Network Model

Consider a sensor network composed of a large number of small senor nodes along with a sender, a receiver and an attacker as in Figure.3.1.

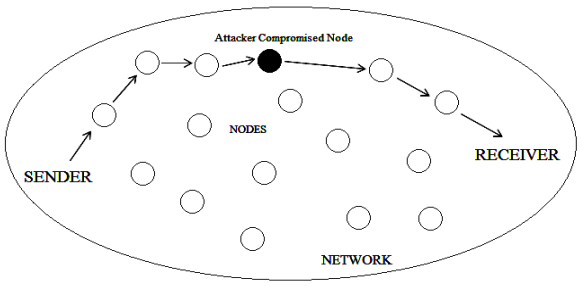


Figure. 3.1: A basic sensor network composed of sensor nodes.

The sensor nodes are assumed to be deployed in high density, so that the receiver can be detected by multiple sensors. The network supports the following communication patterns as in Figure. 1: (i). Sender broadcasts/ multicasts messages to all or certain nodes; (ii). Sensor node broadcasts/ multicasts messages from sender to another node/ receiver; (iii). Attacker might compromise a sensor node and broadcasts/ multicasts his/her own message to another node/ receiver via the compromised node.

A scenario as in Figure. 3.2 is considered, as multiple senders along with multiple receivers are present. Each sender might send messages to multiple receivers. Similarly, each receiver receives message from multiple senders. Communication of messages from sender to receiver takes place via a communication network which consists of large number of sensor nodes. There is a possibility that the network can be injected with bogus reports from an attacker by node compromise attack.

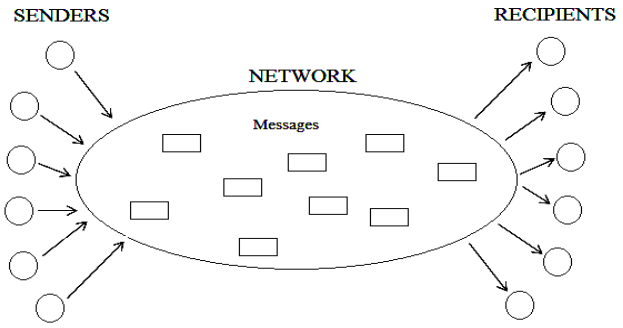


Figure. 3.2: Multiple Senders and Receivers in a sensor network

Let us consider, the attacker attacks the file of the sender by compromising the node. After the attack, the sender sends out all data to the attacker. Now, the attacker launches an attack throughout the entire sensor network. The attacker sends an attacked file to an intermediate node via the sender. However, with the proposed message authentication scheme, the intermediate node verifies the message broadcasted to it. If the message sent is verified and correct, then the intermediate node forwards the message to the receiver. If

the message is not verified, then the intermediate node rejects the message and recognizes it as an injected bogus report. All the sender and receiver data are stored in a database using the public-key cryptosystem or elliptic-curve cryptosystem. The entire framework is explained in Figure.3.3.

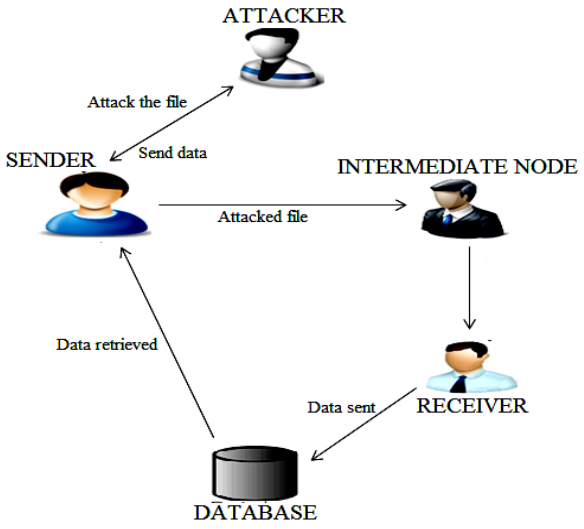


Figure 3.3: Framework of the message authentication scheme

### 3.2 Proposed Model

The main idea is that for each message $m$ that is to be transmitted from one node to another node, the message sender generates a message authenticator for the message. The generation is based on elliptic curves. First, a random integer is selected. Then, a cryptographic hash function is selected which is calculated as $h_A$ $h(m,r)$, where $h_A$ is the generated message authenticator and $r$ is the integer chosen. The generated message authenticator is verified by the receiver of the message authenticator using a verification algorithm. So, the message authentication is defined as $S(m)$ $(m,S,r,h_A)$. This is transmitted to the receiver of the message. Now, receiver verifies this message. If an attacker, compromises a specific node or several nodes, then the attacker is unknown about the value of $r$ and $h_A$ computed from the message authentication. So, if an attacker tries to eavesdrop or tamper messages, then the next node will have knowledge about the attacker and immediately drop the corrupted message. The node, then, acknowledges the corresponding nodes in the network and sends an alert to the administrator of the network regarding the attacker. This will ensure that the attacker is removed from the network and the sensor nodes are not compromised or disrupted. This also ensures hop-by-hop authentication as each message is passed through the nodes in the network.

## 4 AUTHENTICATION ON ELLIPTIC CURVES

In this section, an unconditionally secure and efficient SAMA has been proposed. SAMA is Source Anonymous Message Authentication on elliptic curves The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m. The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS. In our scheme, the entire SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA alike. In addition, our design enables the SAMA to be verified through a single equation without individually verifying the signatures.

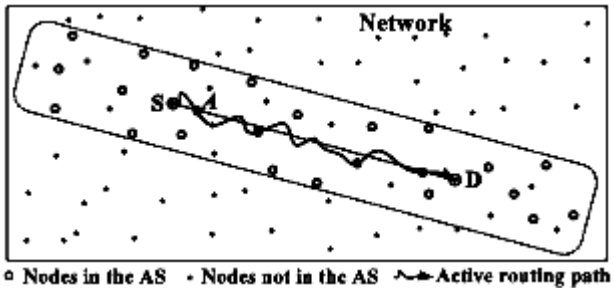


Figure 4.1 Anonymous set selection in active routing

## 5 SECURITY ANALYSIS

In this section, SAMA scheme can provide unconditional source anonymity and provable unforgeability against adaptive chosen-message attacks.

5.1 Anonymity

In order to prove that the SAMA can ensure unconditional source anonymity, we have to prove that:

1) For anybody other than the members of S, the probability to successfully identify the real sender is 1=n, and

2) Anybody from S can generate SAMA.

The SAMA can provide unconditional message sender anonymity.

The identity of the message sender is unconditionally protected with the SAMA scheme. This is because, regardless of the sender's identity, there are exactly (N-1) (N-2)…(N-n) different options to generate the SAMA. All of them can be chosen by any members in the AS during the SAMA generation procedure with equal probability without depending on any complexity-theoretic assumptions. The second part, that anybody from S can generate the SAMA, is straightforward.

5.2 Unforgeability

The design of the proposed SAMA relies on the ElGamal signature scheme. Signature schemes can achieve different

levels of security. Security against existential forgery under adaptive-chosen message attacks is the maximum level of security.

In this section, SAMA is secure against existential forgery under adaptive- chosen message attacks in the random oracle model

The security of our result is based on ECC, which assumes that the computation of discrete logarithms on elliptic curves is computationally infeasible. In other words, no efficient algorithms are known for non-quantum computers.

## 6 CONCULSION

In this paper, a message authentication is proposed. This approach is based on elliptic curve cryptography (ECC). Also, this approach enables the intermediate nodes to authenticate messages so that all corrupted messages can be detected and dropped in the Wireless Sensor Networks (WSNs). Using the message authentication scheme, an efficient hop-by-hop has been proposed. Every sensor node on the routing path verifies the authenticity and integrity of the messages upon receiving the messages. In future, we plan to study comparative analysis based on computational overhead, sensor energy consumption, sensor memory consumption, etc.

## REFERENCES

[1] R. Rivest, A. Shamir, and L. Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"* Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[2] D. Chaum, *"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,"* Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981

[3] T.A. ElGamal, *"A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,"* IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[4] A. Pfitzmann and M. Waidner, *"Networks without User Observability— Design Options.,"* Proc. Advances in Cryptology (EUROCRYPT), vol. 219, pp. 245-253, 1985.

[5] M. Waidner, *"Unconditional Sender and Recipient Untraceability in Spite of Active Attacks,"* Proc. Advances in Cryptology (EUROCRYPT), pp. 302-319, 1989.

[6] 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.

[7] M. Bellare and P. Rogaway, *"Random Oracles are Practical: A Paradigm for Designing Efficient Protocols,"* Proc. ACM First Conf. Computer and Comm. Security (CCS '93), pp. 62-73, 1993.

[8] L. Harn and Y. Xu, *"Design of Generalized ElGamal Type Digital Signature Schemes Based on Discrete Logarithm,"* Electronics Letters, vol. 30, no. 24, pp. 2025-2026, 1994.

[9] K. Nyberg and R.A. Rueppel, *"Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem,"* Proc. Advances in Cryptology (EUROCRYPT), vol. 950, pp. 182-193, 1995.

[10] D. Pointcheval and J. Stern, *"Security Proofs for Signature Schemes,"* Proc. Advances in Cryptology (EUROCRYPT), pp. 387- 398, 1996.

[11] M. Reiter and A. Rubin, *"Crowds: Anonymity for Web Transaction,"* ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

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

[13] D. Pointcheval and J. Stern, *"Security Arguments for Digital Signatures and Blind Signatures,"* J. Cryptology, vol. 13, no. 3, pp. 361- 396, 2000.

[14] V. Wen, A. Perrig, and R. Szewczyk, *"SPINS: Security suite for sensor networks,"* in Proc. ACM MobiCom, 2001, pp. 189–199.

[15] R. Rivest, A. Shamir, and Y. Tauman, *"How to Leak a Secret,"* Proc. Advances in Cryptology (ASIACRYPT), 2001.

[16] L. Eschenauer and V. D. Gligor, *"A key-management scheme for distributed sensor networks,"* in Proc. ACM CCS, 2002, pp. 41–47.

[17] H. Chan, A. Perrig, and D. Song, *"Random key predistribution schemes for sensor networks,"* in Proc. IEEE Symp. Security. Privacy,May 2003, pp. 197–213.

[18] 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.

[19] 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.

[20] A. Pfitzmann and M. Hansen, *"Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology,"* http://dud.inf.tu-dresden.de/ literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.

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

[22] 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.

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

[24] *"Cryptographic Key Length Recommendation,"* http://www. keylength.com/en/3/, 2013.

[25] J. Li, Y. Li, J. Ren and J.Wu, *"Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks"*, IEEE Transactions on Parallel and Distributed Systems, VOL. 25, No. 5, May 2014.

[26] D. Chaum, *"The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability,"* J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.