International Journal of Combined Research & Development (IJCRD)
eISSN: 2321-225X;pISSN:2321-2241 Volume: 4; Issue: 8; August -2015

A Distributed Cryptography Algorithm for Source Privacy in Wireless Sensor Networks

Sharanagouda, Ramesh S Jadhav

[1]*P.G.Student, Department of Computer Science & Engineering,*
Appa Institute of Engineering and Technology, Gulbarga, Karnataka, India
[2]*Assosciate Professor, Department of Computer Science & Engineering,*
Appa Institute of Engineering and Technology, Gulbarga, Karnataka, India

***Abstract*— Message authentication is an effective mechanism, used to authenticate the messages in wireless sensor networks (WSNs). Wireless Sensor Network consists of a large number of sensor nodes. Each sensor node knows its location specifically in the sensor domain and is having the capability of communicating with its neighbouring nodes directly using geographic routing. Many message authentication schemes are depend on either cryptosystems like symmetric-key cryptosystems or other cryptosystem present is public-key cryptosystems. An existing system like polynomial based scheme authenticate the message based on threshold value, this is a problem of existing system because only limited number messages are authenticated. Here we are proposing a new authentication system by the name Source Anonymous Message authentication, popularly known as SAMA is a scalable authentication system scheme based on standard elliptic curve cryptography, known as ECC is used to allow or access generally any node to send and perform authenticate large number of network messages, and hence without affecting from the issue like threshold problem and provides successively message source privacy efficiently.**

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

I. INTRODUCTION

In a design of generally considered hop by hop authentic system, i.e. performing message authentication and also help in source privacy in standard wireless sensor network. Various techniques are used. In this technique, the process hop to hop with message authentication scheme means that, messages would be transferred with from sender node to destination node through the various present intermediate nodes in the network. The Standard wireless communication promises or guarantees that the message which we send should be performed authenticated or not. And next in this technique, the message which we have to send, if that message is corrupted, then to provide solution many numbers of techniques are suggested and proposed. In this message authentication technique or mechanism can be able to implement in standard wireless sensor networks. Hence the security goals to be considered her for transmitting in general sensor networks show how these attacks against standard ad-hoc and general peer-to-peer networks can be obtained into very powerful attacks of network against commonly used sensor networks, going to introduce two categories of attacks against general sensor networks. In this, many authentication techniques had implemented i.e. many researchers have worked in the past for giving security, helps in communication authenticity system and integrity in standard wireless sensor networks.

The standard Wireless Sensor Network consists of a many number of general sensor nodes. And hence each sensor node come to know it location or position in the sensor domain or network and is having capability of making communication with its nodes i.e. neighbouring nodes in the direct way by making use of geographic routing system. Here the standard Wireless sensor network is considered as a group of general, specialized transducer units with a system called communications infrastructure system dedicated to monitor and make record conditions at different diverse locations. Next commonly observed or monitored values or parameters are temperature value, humidity parameter, pressure unit, wind direction value and the speed value, considering vibration intensity value, sound intensity value, power-line voltage system, chemical concentrations units, considering pollutant levels and also allowing important body functions. Generally a sensor node in a standard wireless sensor network which is capable of doing some important processing operations such as collecting sensory data and making effort to communicate with other common nodes connected with each other in the network system.

II. LITERATURE SURVEY

Message authentication schemes are used in different applications and security. Key verification concepts in all the applications for that, many authors proposed different kinds of security algorithms like symmetric key algorithm and public key algorithm.

A. Statistical En-route Filtering

Statistical En-route Filtering (SEF) mechanism detects the false message. SEF requires each sensing report must be validated by using multiple keyed message authentication codes (MACs), sender generate a private key after finding the public of that key. The message is hashed. Finally, the receiver node is going to find the possibility of key. That is similar with sender key then only accepting the message to be transmitted. Each generated message by a node that is going to detect the same event. MAC is to be able to detect any attempt by the adversary to modify the transmitted data.SEF limits the amount of security information to each node.MAC length is dropped during the forwarding process by intermediate nodes. The following disadvantages like receiver collisions, limited transmission power, false misbehaviour report.SEF mechanism does not describe the how to detect the compromised node.

B. *Polynomial Message Authentication*

A polynomial based message authentication technique was implemented to prevent message to accessed from unauthorized user. These techniques are based on some threshold value. Generally only limited numbers of specific messages are authenticated or validated. Specifically the threshold value is going to be calculated generally by the degree of the polynomial operation. According to this scheme, if the number of particular messages transferred is going to be below the threshold value, then the intermediate node is going to validate in general the authenticity of the specified message through the standard operation i.e. polynomial evaluation. On the other hand when the number of messages transferred is larger than the threshold value, the specific polynomial parameter is going to be fully recovered by particular adversary value and the system is going to be specifically broken completely. Therefore messages are to be transmitted directly to destination node over the network.

III.PROPOSED METHODOLOGY

Our proposed authentication scheme aims at achieving the following goals:

1. Message authentication:
Generally the message receiver unit should be able to justify whether a particular received message is sent by the node that is specifically claimed or by a node in a particular group. In other words, the standard adversaries cannot behave like an innocent node and going to put false messages into the specified network without generally being detected.

2. Hop-by-hop message authentication:
Here to consider that every forwarder node specifically on the routing path should be able to check the authenticity and standard integrity of the messages upon reception [1] in the system.

3. Identity and location privacy:
The adversaries or attackers are not going to find out the message sender's particular ID and corresponding location by analyzing generally the message contents or particularly the local traffic [3] over the network.

4. Efficiency:
The scheme considered here should be efficient enough in terms of specifically mutually computational and general communication overhead [15] over the network.

The system which is proposed here going to focuses generally on providing high privacy value to the message authentication technique. Hence in addition to the hop-by-hop standard message authentication key exchange technique has been enabled through standard deffiee helmen key exchange technique the source node is going to encrypt the data or information after receiving the data or information it needs a private key value for performing decrypting the data. So, specifically the receiver is going to request key server generally to produce a private key value. The key server validates the receiver access operation through key authentication mechanism or technique. It is not an easy task for malicious node generally to get a key from key server.

IV. ARCHITECTURE

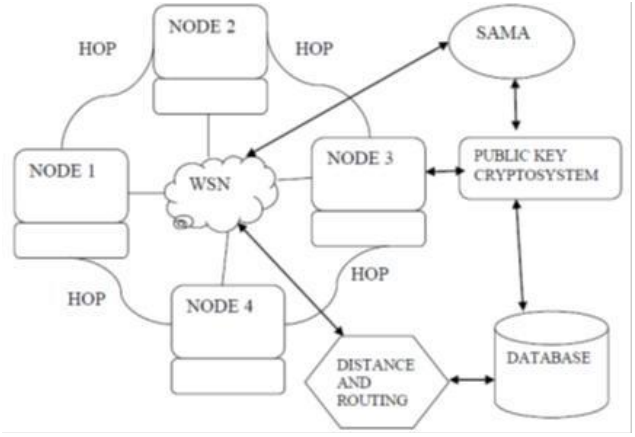

Figure 1 Hop by Hop Message Authentication and Source Privacy in Wireless Sensor Networks.

In standard wireless sensor network is going to provide on high privacy value to the message authentication mechanism. Therefore, while specifically enabling the intermediate nodes standard message authentication technique is going to allow

any specific node to send an unlimited number of messages generally without suffering the threshold problem.
We going to develop a source anonymous authentication code commonly referred as SAMAC an standard elliptical curve that is going to provide specifically unconditional source anonymity through standard hop-by-hop message authentication process.

A. Source Anonymous Message Authentication

(SAMA) on Elliptic curves SAMA techniques does not have the threshold problem. Unlimited numbers of messages are authenticated. SAMA is a secure and efficient mechanism, generates a source anonymous message authenticator for the message m. The message generation is based on the MES scheme on elliptic curves. An elliptic curve E is defined by an equation of the form:
E: $y^2=x^3 +ax + b \bmod p$;
1. Considering a base point elliptic curve.
2. Assuming the private key of sender node.
3. Calculate public key of sender.
4. The message is to be hashed and left bit of hash functions are converting into binary format.
5. Finding the signature of message.

B. Modified ElGamal Signature Scheme
Authentication generation algorithm:

Sender node is sending the message to be transmitted to receiver node. (SAMA):
A SAMA consists of the following these steps:
1. Receiver node receiving the hashed message.
2. Left most bit of the hash is taken in decimal format.
3. If it receives same key means allow to transform and access that message.

V. IMPLEMENTATION

The proposed system contains the following modules:

- Network creation and routing
- Implementation of Symmetric Key Approach
- Implementation of SAMA
- Result Analysis

- **Network creation and routing**

In this module, a sample network is n to be created or formed. Consider a network with 'n' number of nodes over the network is to be created. All the nodes are going to be deployed in a random manner across the standard network. All the nodes over the network perform the operation like communicate with each other. The wireless properties or attributes are given to the specified network. Since our network is standard Sensor Network, a DATA SINK should be going to be created. Hence to configure the specified data sink a patch file to the **ns** package is going to be added. The normal basic sensor nodes are configured in the specified network.

- **Implementation of Symmetric Key Approach**

In this module, we are considering the message sender node and the receiver node and they have to share a special secret key. This special shared key is going to be used by the sender node to generate a general message authentication code commonly known as MAC for each transmitted message over the network. However, by considering this technique, the authenticity operation and integrity of the particular message can only be validated or verified by the corresponding node with the special shared secret key value, which is generally going to be shared by a group of specific sensor nodes over the network.

- **Implementation of SAMA**

In this module, for each selected message, the message sender i.e. sender node, or the sending node, going to generate a source anonymous message authenticator commonly referred as AMS for the particular message. This kind of generation part is based on the standard MES scheme on commonly used elliptic curves. At the receiver end, i.e. at the receiver node the assigned AMS value going to be verified or validated by the nodes with public keys.

- **Result Analysis**

In this module, the performance of considered network is going to be analysed. X-graphs are plotted going to be plotted based on considering the results collected from analyse phase. Throughput parameter, delay value, energy consumption parameter are the basic parameters considered here in this phase and X-graphs are going to be plotted for these parameter values.
Finally, the results collected or obtained from this module is going to be compared with third module results values and comparison X-graphs which are standard in simulation projects are going to be plotted. Therefore from the comparison result, the final RESULT is going to be concluded.

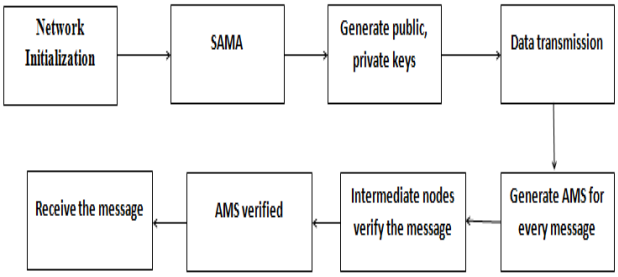

Figure 2 Block Diagram for Proposed System

VI. RESULT ANALYSIS

We use NS2 as our simulating tool. We assigned a network consisting of 41 nodes from node 0 to node 40. After finding its one hop and two hop neighborhoods, a node start transmitting its packet .The source node sends constant bit rate traffic to destination node. The traffic sources are carried by transport layer protocols User Datagram protocol (UDP) or Transmission control protocol (TCP). At the end of simulation, the trace file is created and the NAM is running (since it is invoked from within the procedure finish{}).Trace file gives the details of packet flow during the simulation.NAM trace is records simulation detail in a text file, and uses the text file the play back the simulation using animation.

Here we are assigning 25 nodes from node 0 to node 24 and they are apart from each other.

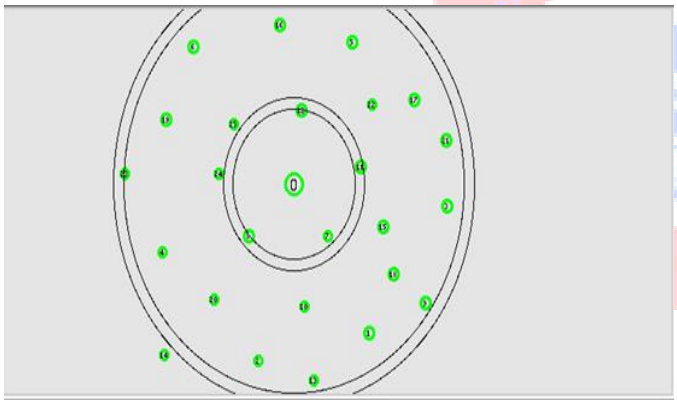

Figure3 Node initialization

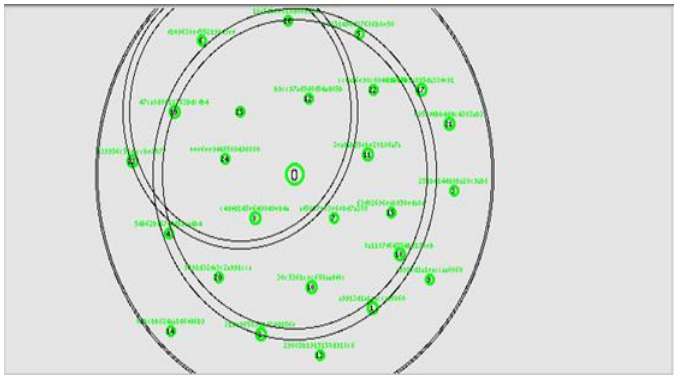

Figure 4 Neighborhood Identification & Node Configuration

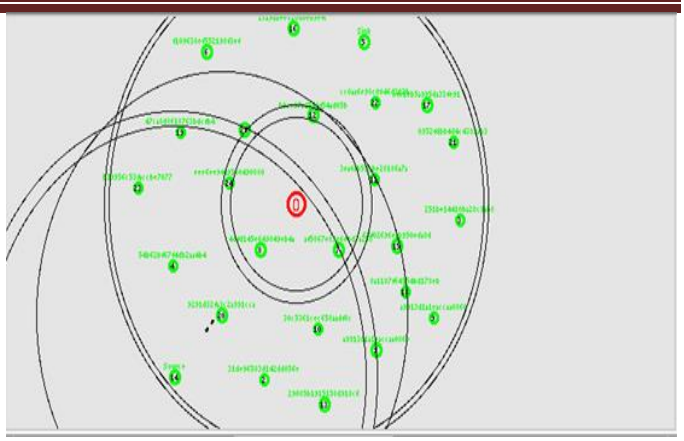

Figure5 Node 14 transmitting the data to the node 0

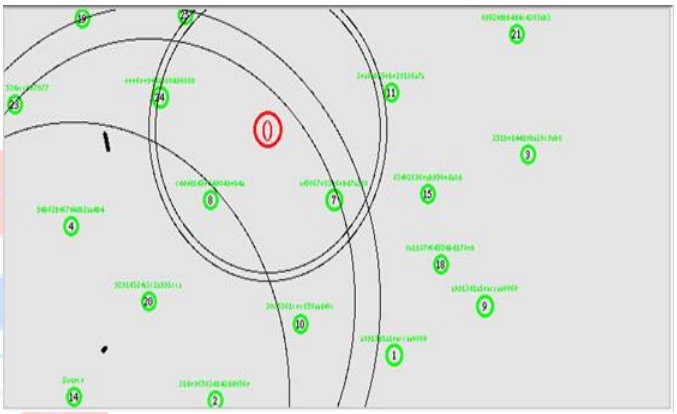

Figure 6 validating the signature

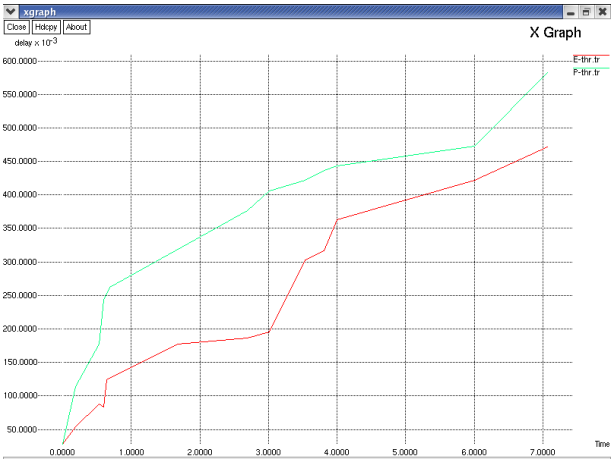

Figure 7 Xgraph for Throughput

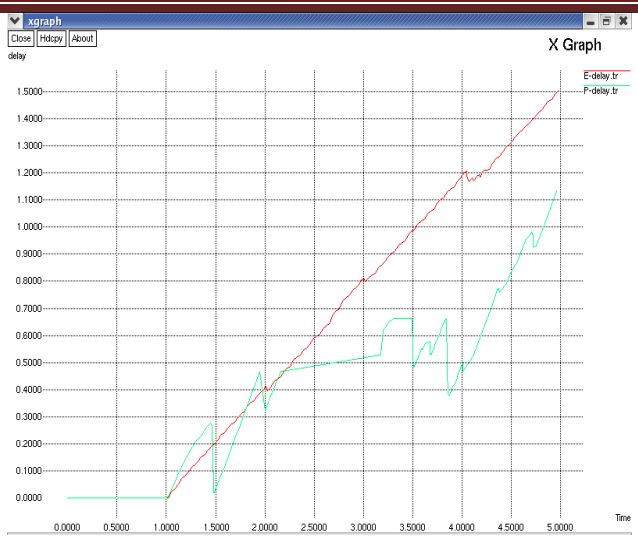

Figure 8 Xgraph for energy consumption

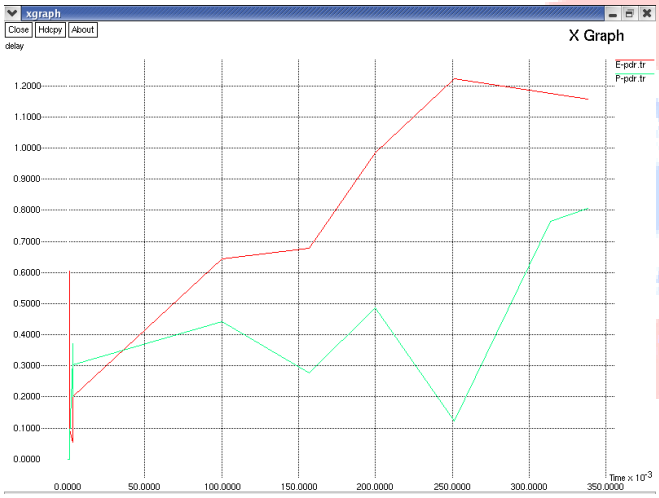

Figure 9 Xgraph for Packet Drop Ratio

VII. CONCLUSION

Message authentication schemes are used to improving the security in wireless sensor Networks. Here specified technique which is an efficient, we call it as Source anonymous message authentication technique, which is based on ECC method 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] 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] 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.
[4] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.
[5] 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.
[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] 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.
[8] 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.
[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," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.
[10] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387-398, 1996.
[11] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.
[12]D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.
[13]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.
[14]A. Pfitzmann and M. Waidner, "Networks without User Observability— Design Options.," Proc. Advances in Cryptology (EUROCRYPT), vol. 219, pp. 245-253, 1985.
[15]M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transaction," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.
[16]M. Waidner, "Unconditional Sender and Recipient Untraceability in Spite of Active Attacks," Proc. Advances in Cryptology (EUROCRYPT), pp. 302-319, 1989.
[17]D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361- 396, 2000.
[18]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.
[19]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.
[20] R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Advances in Cryptology (ASIACRYPT), 2001.

[21] 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.
[22] "Cryptographic Key Length Recommendation," http://www.keylength.com/en/3/, 2013.