International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Hop By Hop Secure Data Routing In Wireless Sensor Network

Shivani Shitole[1], Manisha Jadhav[2], Meghana Dhaware[3], Neha Sheikh[4], Archana Jadhav[5]

[1]*Student, Dept. of Information Technology, AISSMS College of Engineering, Kennedy Road, Pune, India*
[2]*Student, Dept. of Information Technology, AISSMS College of Engineering, Kennedy Road, Pune, India*
[3]*Student, Dept. of Information Technology, AISSMS College of Engineering, Kennedy Road, Pune, India*
[4]*Student, Dept. of Information Technology, AISSMS College of Engineering, Kennedy Road, Pune, India*
[5]*Professor, Dept. of Information Technology, AISSMS College of Engineering, Kennedy Road, Pune, India*

FPAbstract – *In Wireless Sensors Networks (WSNs) avoiding issue of a message being corrupted as well as unauthorized is very essential. This issue is efficiently addressed by message authentication and prevents corrupt and unauthorized message. There are numerous methodologies developed on the basis of symmetric-key cryptosystems or public-key cryptosystems. But number of them fails in case of communication as well as computational overhead and less flexibility and scalability also decreases the ability of compromise the attack. In recent days, a new approach presented to solve this issue by using polynomial-based method. Method have drawback of built-in threshold which is considered on the basis of polynomial degree. If transferred messages are larger than the threshold then attacker is able to regain whole polynomial. In this paper we propose flexible as well as scalable method on the basis elliptic curve cryptography (ECC). Our method permits any nodes to transfer infinite messages without difficulty of threshold issue at the time of authentication of mediatory nodes and also message source privacy is ensured. We examined method on basis of analysis as well as visualization and outcomes are shown that our method more effective as compared with polynomial-based technique in case of communication as well as computational overhead.*

Key Words: Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, wireless sensor networks (WSNs), distributed algorithm, decentralized control.

1. INTRODUCTION

Message authentication is a most important way to avoid the issue of corrupted and unauthorized messages sent over wireless sensor network as well as save the useful sensor energy. Number of methods is provided for message integrity and authenticity for wireless sensor networks. These methods have two categories such as public-key and symmetric-key based techniques.

Symmetric-key based technique includes difficult key-management, limited scalability and not flexible in the case of numerous nodes compromises attacks when exchange of secret key between sender and receiver. Using exchanged key sender create MAC (Message Authentication Code) for each message. Message integrity as well as authenticity is confirmed by the node through distributed secret key between groups of nodes. An intruder has to compromise the secret key through accessing only one sensor node and this method not supports to multicast networks.

In public-key based technique each message contains digital signature of message which is created by using private key of sender. Each of mediatory nodes as well as destination node can authenticate the message using public-key of sender. A drawback of this method is large computational overhead. Recently done process on elliptic curve cryptography resulted that public-key methods are more beneficial in case of computational difficulty, utilization of memory and flexible security. It is possible when management of public-key is easier and elegant.

In this paper we proposed absolute as well as effective source anonymous message authentication (SAMA) method on the basis of optimal modified ElGamalSignature (MES) method for elliptic curves. This method is secure and has ability prevent flexible selected-message attacks in random oracle model. In our method mediatory node have right of authenticate the message to eliminate corrupted message and save energy of sensor. When we try to gain the flexibility, time-companioned authentication as well as security of source identity our method doesn't compromise with the issue of threshold. Analysis and practical examinations are resulted that our proposed method is more effective as compared with polynomial based algorithms as well as in the case of security.

2. RELATED WORK

In this paper [1], author shows an interleaved jump by-bounce confirmation method. Method guarantees that base station may recognize injected wrong data bunch which is almost near to count t nodes that are infected. Moreover,author's method provided an upper bound to the number of jumps which a wrong data bunchwillsend before it recognized and eliminated andagreed that

traded off nodes. They additionally propose another part of methodthat guarantees and works little. Author's execution results are describes that the method provides security as well as allows exchange of data between security and execution.

In this paper [2], author proposes a flexible authentication method on the basis of elliptic curve cryptography (ECC). Authors proposed method allows all mediatory nodes to transferhuge messages without any problem of threshold. Additionally, author's method provides security to source of message.

In this paper [3], author introduced a Statistical En-course Filtering (SEF) methodology to find and eliminate the corrupt messages. SEF have need of every message is authenticated on the basis of message authentication codes (MACs) as well as each created by a node identifies the similar event. A message is authenticated by each nodeas well as observed the accuracy and drops corrupt messages by MACs. Further, sink node eliminates paths which contains corrupt message. SEF utilizes all performance of system to find out the integrity of every message by total selection creating by various recognizing nodes and collect false-message-location by various sending nodes. Author's examination shows with an overhead for every message SEF is capable to eliminate injected corrupt messages by exchange node within sending bounces and decrease energy utilization.

Authors exhibit [4] that the heuristic security conflicts given for these adjusted schemes try not to hold, besides, that they can be completely broken once Author allows even a Slight increase of the parameters past those achieved by the concealed information theoretic schemes. Authors attack applies to the key pre-distribution scheme of Zhang et al. (MobiHoc 2007), the entrance controls arrangements of Subramanian et al. (PerCom 2007) and the affirmation schemes of Zhang et al. (INFOCOM 2008).

In this paper [5], author presented crucial concept to keep the recipient and sender or perhaps their relationship hidden, analyzed some as possible executions and important dynamic increases, furthermore, propose some suitable execution and reliability updates.

3. IMPLEMENTATION DETAILS

3.1 System Overview

The aim of proposed system is to send data securely using Hop-by-Hop authentication system. In this system first anonymous source and destination is selected which is not detected by other nodes. Then select the path and send the data in encrypted format in hop-by-hop way. For encryption ECC algorithm is used. While sending data the AS region is generated and select the random nodes and send data. Due to this the attackers not detect the actual source node. The source node send data with destination ID, the node which have mach identity and key can decrypt the data. In this way system provide the source privacy.

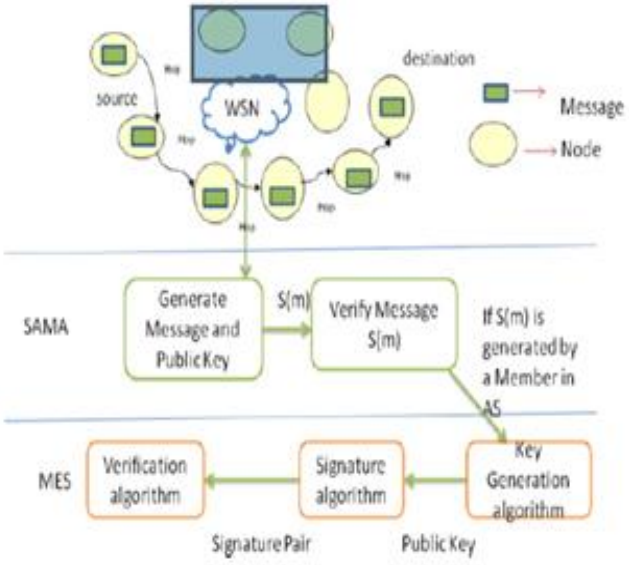

Fig -1: System Architecture

3.2 Algorithm

Algorithm 1: MES (Modified ElGamal signature)

The modified ElGamal signature scheme consists of the following three algorithms
1. Key generation algorithm
2. Signature algorithm.
3. Verification algorithm

Algorithm 2: Key generation algorithm

- Let p be a large prime and g be a generator of
- Both p and g are made public.
- For a random private key x ε Zp, the public key y is computed from $y = g^x \bmod p$

Algorithm 3: Signature algorithm

- The MES can also have many variants
- For the purpose of efficiency, we will describe the variant, called optimal scheme.
- To sign a message m, one chooses a random k ϵ Z*p-1,
- Then computes the exponentiation $r = g^k \bmod p$ and solves s from:

$$s = rxh(m , r) + k \bmod (p-1)$$

Where h is a one-way hash function. The signature of message m is defined as the pair(r , s)

Verification algorithm

- The verifier checks whether the signature equation

$$g^s = ry^{rh(m,r)} \bmod p$$

- If the equality holds true,
- Then the verifier accepts the signature, and Rejects otherwise.

3.3 Experimental Setup

This system is developed on Java framework (version jdk 8) and Netbeans (version 8.1)is used as a development tool on Windows platform. The Java Universal Network is a product library that gives a typical and extendible dialect for the displaying, investigation, and representation of information. The system doesn't require any specific hardware to run, any standard machine is capable of running the application.

4. RESULTS

Proposed system algorithm is implemented on JUNG simulator with the help of Java language. This system provides better security as compared with existing system. This system provides source as well as destination anonymity. The construction of shortest path consumes less energy to send the data and improve network lifetime.

4.1 Time Graph

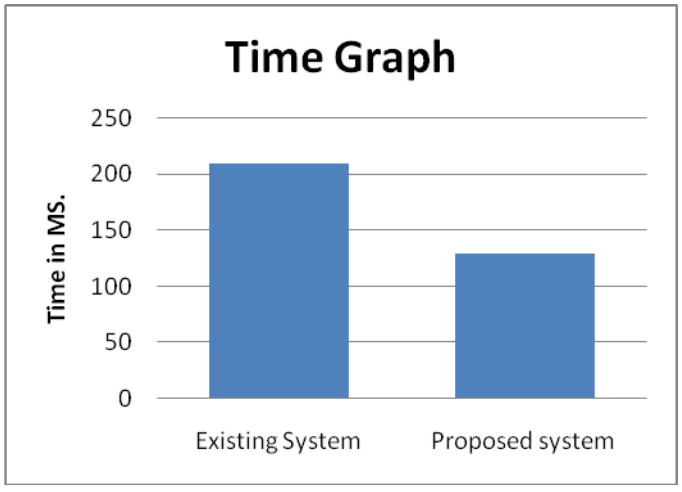

Fig -2: Time Graph

The fig. 2 shows the time comparison between propose system and existing system. The propose system take less time than existing system.

4.2 Network Lifetime Graph

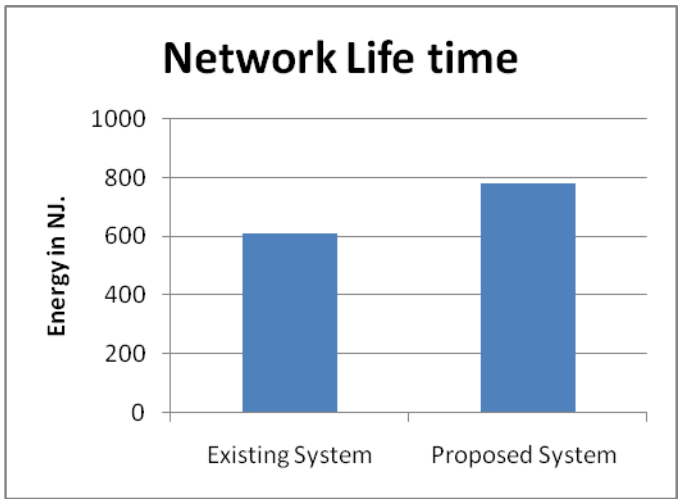

Fig -3: Network Life Time Graph

The fig. 3 shows the network lifetime comparison between propose system and existing system. The propose system consume less energy than existing system and increase the network lifetime.

5. CONCLUSION AND FEATURE WORK

We proposed a new and efficient SAMA on the basis of ECC. This method ensures security of message source. SAMA is able to connect with allmessages to provide message content authenticity and Hop-by-Hop message authentication used without disadvantage limitation of the polynomial-based plan.We proposed a Hop-by-Hop message authenticationon the basis of SAMA and in the case of connected to WSNs with added sink nodes, possible methods for compromisednodefinding. We proposed method with the polynomial-based method by reproductions using ns-2 and TELUS. Reproduction outcomes shows that, in practically identical scenarios, our proposed plan is more successful than the polynomial-based method in case of computational overhead, energy consumption, delivery ratio, message delay and memory consumption. A novel and efficient SAMA based on ECC is proposed which can provide source anonymity.In future we can work on path anonymity with increasing security.

ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule University of Pune. We are also thankful to the reviewer for their valuable

suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

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. TABLE 3 Memory (KB) for the Two Schemes (TelosB) (F Stands for Flash Memory).

[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.z

[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 / literature /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.