International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 2 – FEBRUARY 2016.

ENHANCED DYNAMIC ROUTING WITH SECURE TRANSMISSION USING ELGAMAL SIGNATURE BASED MESSAGE AUTHENTICATION

Mrs.T. SathyaPriya, M.Sc, M.Phil[1] , Miss. S. Selvamani [2]

[1] *Assistant Professor, Department of Computer Science, Theivanai Ammal College for Women (Autonomous), Villupuram-645 401, India. Email Id:* ***sathyakumar141@gmail.com***

[2]*M.Phil Scholar, Department of Computer Science, Theivanai Ammal College for Women (Autonomous), Villupuram-645 401, India. Email Id:* ***selvasuresh8215@gmail.com***

Abstract- **This paper upgrades the current dynamic routing framework for information integrity with message verification model. Message confirmation is a standout amongst the best approaches to obstruct unapproved and debased messages from being sent in Wireless Sensor Systems (WSNs). Thus, numerous message validation plans have been created, in light of either symmetric-key cryptosystems or public key cryptosystems. The greater parts of them, be that as it may, have the restrictions of high computational and correspondence overhead apart from the absence of adaptability and strength to hub trade off assaults. To address these issues, a polynomial-based plan was as of late presented. Be that as it may, this plan and its augmentations all have the shortcoming of an inherent threshold controlled by the level of the polynomial. When the quantity of messages transmitted is bigger than this limit, the adversaries can completely recuperate the polynomial. In this paper, we proposed the Source Anonymous Message Authentication plan (SAMA) for secure message sending. The proposed plan permits any hub to transmit a boundless number of messages without agony from threshold issue. We are utilizing ElGamal signature for message confirmation. In this plan, we empowers the hubs to verify the message with the goal that all polluted message can be identified and dropped. We build up the SAMA code on elliptic bends that can give unlimited source obscurity. We propose a productive key administration structure to guarantee the detachment of the traded off hubs. Likewise, our plan can likewise give message source protection. Both hypothetical and simulation results exhibit that our proposed plan is more proficient than the polynomial-based methodology as far as computational and correspondence overhead under practically identical security levels while giving message source protection.**

Keywords: Dynamic Routing, Polynomial based plan, Source Anonymous Message Authentication (SAMA), ElGamal signature and Elliptical bends.

I. INTRODUCTION

In hop by hop message verification with source protection in the wireless sensor system, were privacy is successful approach to shield from unapproved clients affected the messages by sending through wireless sensor systems. Numerous message confirmation schemes have been utilized to secure the messages; however these verification plans have the impediments of high overhead, absence of capacity, to hub assaults and threshold issue. Message confirmation has a principle part in upsetting unapproved and affected messages from being sent in systems to spare the vitality. Numerous authentication forms have been actualized to give the message validness and authentication for remote sensor systems. The symmetric key based methodology has entangled a key administration and absences of ways. It is not taken to vast quantities of hubs trade off the assaults subsequent to the message sender and the recipient need to share their secret key. The sender utilizes shared key to produce a message confirmation code for each transmitted message. The credibility and honesty of message can confirm just by the hub utilizing the shared secret key, which is for the most part shared by gathering of sensor hubs. So, it does not work in multicast networks.

To take care of the issue, a secret based for the message validation plan was presented. The technique is like an edge secret sharing, where it is controlled by the level of the value. This offers data security of the mutual secret key when the number of messages transmitted is not exactly the limit. The center hubs check the originality of the message. On the off chance that the transmitted messages are bigger than the edge, can be completely recouped. For public key based strategy, each message is transmitted with the digital signature message delivered utilizing the sender's private key. Each intermediate forwarder and the final beneficiary can verify the message utilizing the sender's public key. One of the limitations of public key strategy is the high computational overhead.

The major contributions in this paper are listed as follows:

- We develop a Source Anonymous Message Authentication (SAMA) code on ElGamal scheme that can provide unconditional source anonymity.
- We offer an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation.
- We devise network implementation criteria on source node privacy protection in WSNs.
- We propose an efficient key management framework to ensure isolation of the compromised nodes.

II. RELATED WORK

The symmetric key based methodology has complex key administration, absences of versatility and also not flexible to expansive quantities of hub compromise assaults, due to the need of sharing secret key between message [1] sender and collector. Here the sender utilizes the common secret key to produce the Message Verification Code (MAC) for each transmitting messages. The legitimacy and integration of messages can verify by the hub utilizing the common secret key, which is for the most part shared by a gathering of sensor hubs. As a result of this, an aggressor [2] can without much of a stretch compromise the key by catching a solitary sensor hub, so this technique doesn't work in the multi cast systems. To address this issue, a mystery polynomial based message validation plan has been presented; however this plan and its augmentations (Perturbation factor), all have the shortcoming of inherent threshold issue dictated by the level of the polynomial [3].

A large portion of the prior chips away at energy efficient routing in remote sensor system utilizes the Minimum Total Energy (MTE) [5] routing for information transmission approach to minimize the vitality utilization to achieve the destination by sending the movement to same way, yet in the event that all the activity takes after the same way then every one of the hubs of that way will drained their vitality rapidly [3]. Rather than attempting to minimize the devoured vitality, the principle target is to amplify the lifetime of the framework [4]. As in [4] the greatest lifetime issue is a straight programming issue and resolvable in polynomial time. In this works, Chang and Tassiulas proposed vitality effective routing estimations. Stream redirection is the redirection based calculation where some measure of stream is diverted from least longest length way to biggest longest length way. Where biggest longest length way is the way in which has biggest limit regarding battery control and have less vitality utilization per bit transmission. MREP calculation increases the stream on the way whose base vitality after the stream increase will be longest.

Dispersed energy balanced routing is proposed as in [12]. This routing calculation utilizes the vitality equalization way for information transmission. It firstly ascertains the aggregate vitality expense of the considerable number of ways from source hub to base station and after that select vitality proficient way for information transmission. Anyhow, the disseminated vitality adjusted the routing calculation of a system situation where couple of hubs can represent with base station. For vast system DEBR calculation is not works appropriately, a more exact directing calculation and issue definition is required for this class of situation.

For the public key based methodology, the sender transmits every message alongside the signature of the message created by utilizing the sender's private key. The sender's public key [14] is utilized by each intermediate node and the last recipient to confirm and check the transmitted message, yet the constraint of the public key based plan is the high computational overhead. So to beat this constraint, the advancement on the Elliptic Curve Cryptography (ECC) [15] demonstrates that public key plans can have more advantages as far as security strength, computational multifaceted level, and memory employments. According to this, we can discover that, public key based methodologies have a simple and efficient key administration than the symmetric key based methodologies. The major drawbacks exist listed as follows:

- In this scheme, each symmetric verification key is shared by a gathering of sensor hubs. An interloper can trade off the key by catching a single sensor hub. Consequently, these plans are not strong enough to the hubs to trade off the assaults.

- Another kind of symmetric key plan requires synchronization among hubs. These plans, including tesla and its variations, can likewise give message sender validation. Be that as it may, this plan requires beginning time synchronization, which is difficult to be actualized in extensive scale WSNs. Moreover, they additionally present delay in message validation, and the deferral increments as the system scales up.
- In polynomial plan, only predetermined number of messages can be transmitted.

III. ENHANCED SOURCE ANONYMOUS MESSAGE AUTHENTICATION (SAMA)

An unrestricted secure and productive Source Anonymization Message Authentication (SAMA) plan in view of the ideal altered ElGamal signature (MES) plan on elliptic curve. This plan empowers the intermediate hubs to verify the message, so all polluted message can be distinguished and dropped to save the sensor power. While accomplishing the trade off flexibility, an adaptable time verification and source identity protection is established. It needs a build up Source Anonymous Message Verification Code (SAMAC) on elliptic curves that can give unlimited source secrecy. At that point, it offers an effective hop by hop message verification system for WSNs without the edge threshold. At that point, we propose an effective key administration structure to guarantee the seclusion of the compromised nodes.

The wireless sensor systems are accepted to comprise of a huge number of sensor hubs. Accept that every sensor hub knows its relative area in the sensor space and is equipped for denoting with its neighboring hubs utilizing geographic routing. The entire system is completely associated through multi-hop correspondences. In this venture, there is a Security Server (SS) that is accountable for era, storage and circulation of the security parameters among the system. This server will never be traded off. Anyhow, the sensor hubs might be caught and traded off by aggressors. Once traded off, all data put away in the sensor hubs can be obtained by the assailants. The bargained hubs can be reinvented and completely controlled by the assailants. Nonetheless, the traded off hubs won't be ready to make new public keys that can be acknowledged by the SS and different hubs.

In view of the above suspicions, this paper considers two sorts of assaults dispatched by the adversaries:

1) Passive assaults: Through passive assaults, the foes could listen eavesdrop on messages transmitted in the system and perform traffic investigation.

2) Active assaults: Active assaults must be dispatched from the traded off sensor hubs. Once the sensor hubs are traded off, the foes will acquire all the data put away in the traded off hubs, counting the security parameters of the traded off hubs. The adversaries can adjust the content of the messages, and infuse their own messages.

The design goals for authentication were the:

- ***Message authentication***: The message collector ought to have the capacity to check whether a received message is sent by the hub that is guaranteed or by a hub in a specific group. As it were, the foes can't put on a show to be an honest hub and infuse the fake messages into the system without being distinguished.
- ***Message integrity:*** The message collector ought to be ready to confirm whether the message has been adjusted in transit by the foes. At the end of the day, the adversaries can't adjust the message content without being distinguished.
- ***Hop by hop message confirmation:*** Every forwarder on the routing path ought to have the capacity to check the authenticity and integrity of the messages upon receiving.
- ***Identity and location protection:*** The foes can't decide the message sender's ID and location by breaking down the message content or the neighborhood traffic.
- ***Efficiency:*** The plan ought to be effective in both computational and correspondences overhead.

SAMA procedures do not have the threshold issue. A boundless number of messages are confirmed. SAMA is a safe and effective system. Creates a source unknown message authenticator for the message m. The message era depends on the Elliptic bends. The elliptic curve is given by:

$$E : y^2 = x^3 + ax + b \bmod p$$

- Considering a base point in the elliptic bend.
- Presuming the private key of sender hub.

- Figure out public key of sender.
- The message is to be hashed and left bit of hash capacities are changing into binary configuration.
- Estimating the signature of message.

Then the modified ElGamal signature scheme is explained. Authentication era estimation: Sender hub is sending the message to be transmitted to beneficiary hub. A SAMA comprises of the accompanying these strides:

- Beneficiary hub getting the hashed message.
- Left most bit of the hash is taken in the decimal configuration.
- In the event that it gets same key means permit to change and access that message.

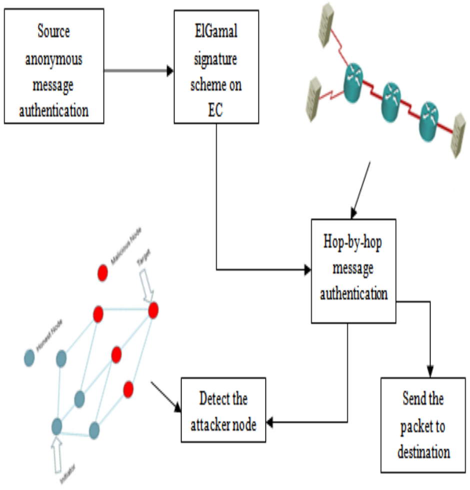
Source anonymous message authentication
ElGamal signature scheme on EC
Hop-by-hop message authentication
Detect the attacker node
Send the packet to destination
Malicious Node
Target
Honest Node
Initiator

Fig.1. Working flow of proposed architecture

IV. EXPERIMENTAL RESULTS

In this area, we can assess the execution of this system. We utilize some assessment measurements:

i) ***Packet Delivery Proportion:*** It is the proportion of the quantity of received packet at destination and number of packet sent by the source. The ratio of data packets delivered to the destination and the data packets generated by the CBR sources are taken packet delivery ratio in our study.

ii) ***End-to-End delay:*** The normal time taken for a packet to be transmitted from source to destination. At few nodes, queuing and channel access delays do not contribute much to the overall delay. The average end to end delay is lower when total number of nodes in simulation scenario is 10 for both routing algorithms but it increases with increasing number of nodes.

iii) ***Energy level:*** The number of vitality expended when the information ought to be transmitted. Due to energy is scares resource in the wireless sensor nodes. it's very important that energy should be used efficiently.

V. CONCLUSION

The vitality supplies of hubs in remote sensor system are not supplanted and in this way the hubs just take part in the system as the length of time that they have energy and conserving battery consumption is the most vital asset. Along these lines, it's not a practical arrangement and rather than this arrangement advances the traffic such that energy consumption is balanced among the nodes. While guaranteeing message sender protection, SAMA can be connected to any message to give message content authenticity. To give hop by hop message validate without the shortcoming of the threshold of the polynomial-based plan, we then proposed a hop by hop message verification plan in light of the SAMA. At the point, when connected to WSNs with altered sink hubs, we too talked about conceivable strategies for the identification of compromised node. Both hypothetical and simulation results demonstrate that, in any situations, our proposed plan is more proficient than the polynomial-based plan as far as computational overhead, vitality utilization, packet delivery proportion, message delay, and memory utilization.

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/ 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.

[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] Jiao Zhang, Member, IEEE, Fengyuan Ren, Member, IEEE, Shan Gao, Hongkun Yang, and Chuang Lin, Senior Member, IEEE, "Dynamic Routing for Data Integrity and Delay Differentiated Services in Wireless Sensor Networks", IEEE Transactions On Mobile Computing, Vol. 14, No. 2, February 2015.