Secure and Efficient Data Transmission in Wireless Sensor Networks

J. Manikandan,
ECE department, JCET,
Trichy india

K. Thilaka,
ECE department, JCET,
Trichy india

***Abstract*- Message authentication plays a key role in thwarting illegal and corrupted messages from being forwarded in networks to save the valuable sensor power. For this cause, many verification schemes have been proposed in literature to provide message authenticity and integrity verification for wireless sensor networks (WSNs). In this paper, we propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. Our 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 enabling intermediate nodes authentication, proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, scheme can also provide message source privacy. Proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, packet delivery ratio, message delay, and memory utilization.**

Keywords:* *Message authentication, Elliptic Curve Cryptography, SAMA, MES, Wireless sensor network

I. INTRODUCTION

A wireless sensor network (WSN) consists of a collection of these nodes that have the facility to sense, process data and communicate with each other via a wireless connection. Wireless sensor networks (WSN's), the improvement in sensor technology has made it possible to have very small, low powered sensing devices equipped with programmable compute, multiple parameter sensing and wireless message capability. Also, the low cost makes it possible to have a network of hundreds or thousands of these sensors, thereby enhancing the consistency and accuracy of data and the area coverage. Wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental situation, such as sound, temperature, and motion. In cryptography, a message authentication code is short piece of information used to authenticate a message and to provide reliability and authenticity guarantee on the message. Integrity declaration detects accidental and intentional message changes, while accuracy assurances affirm the message origin. The symmetric -key based approach require complex key management lacks of scalability and is 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 dispatcher to generate a message authentication code (MAC) for each transmitted communication. On the other hand, for this technique, the genuineness and integrity of message can only be verified by the node with the collective key. A trespasser is able to negotiation the key by capturing a solitary sensor node. In addition, this technique does not toil in multicast networks. en route for work out the scalability crisis, a covert polynomial based message verification method was introduced. For the public-key based draw near, each communication is transmitted along through the digital signature of the communication generated by means of the sender's private key. Each midway forwarder and the concluding receiver are able to validate the communication using the sender's public key. One of the restrictions of the public -key based scheme is the lofty computational transparency. The topical steps forward on elliptic curve cryptography (ECC) shows so as to the public-key schemes be able to more advantageous in conditions of computational difficulty, memory practice, and security pliability, since public -key based approaches contain a easy and fresh key administration.

II. RELATED WORK

In this paper [3] C. Blundo, A. De Santis, S. Kutten, A. Herzberg, U. Vaccaro, and M. Yung proposed "perfectly secure Key distribution for dynamic conference".This technique in attendance information theoretic safety measures with thoughts comparable to a verge undisclosed distribution, anyplace the verge is gritty by the degree of the polynomial. as soon as the amount of messages transmits is below the verge, the method enables the midway node to verify the genuineness of the communication from side to side polynomial valuation.

In [6]H. Wang, s.sheng, q. Li and c. Tan, projected "Comparing symmetric -key and Public-key based security schemes in sensor networks: a case study of user access control". Intended for the community key based draw near, every communication is transmitted next to with the digital signature of the communication generated by means of the sender's private key. Both midway forwarder and the final receiver can authenticate the message using the sender's public key. The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of memory usage, communication complexity, and security resilience, since public -key based approaches have a simple and clean key management.

In [4] G. Wang, N. Subramanian, and W. Zhang projected “Lightweight and compromise resilient message authentication in sensor networks,”
To increase the verge and the complexity for the intruder to recreate the top secret polynomial, a random noise, also call a perturbation factor, was additional to the polynomial, to prevent the adversary from compute the coefficient of the polynomial. However, the added perturbation issue can be entirely removed using error-correcting code techniques.

In [1] H. Lou, S. Lu, F. Ye and L. Zhang, projected “Statistical enroute filtering of injected false data in sensor networks”. In this technique each symmetric verification key is collective by a collection of sensor nodes. An intruder can compromise the key by capture a single sensor node. Then, these schemes are not resilient to node compromise attacks. Another type of Symmetric -key scheme requires organization among nodes. These schemes, together with TESLA and its variants, can also provide communication sender verification. Though, this method requires initial time synchronization, which is not easy to be implementing in big scale WSNs.

In [2]S. Zhu, S. Setia, S. Jajodia, and P. Ning projected “An interleaved hop by hop authentication scheme for filtering false data in sensor networks”. Within this paper, in attendance an interleaved hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised. This scheme is efficient with respect to the safety events it provides, and it also allows a exchange between security and recital.

III. DESCRIPTION OF THE SCHEME

In this section, we propose an unconditionally secure and well-organized SAMA. The main idea is that for each one message m, to be released, the message dispatcher, or the sending node, generates a source anonymous message authenticator for the message m. The creation is based on the MES method on elliptic curves. For a ring signature, every ring member is required to compute a forgery signature for all other members in the AS. In addition, our design enables the SAMA to be verified through a single equation without individually verifying the signatures.

A. Message Authentication

The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular cluster. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.

B. Message Integrity

The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In further terms, the adversaries cannot alter the message content without being detected.

C. Hop-by-hop Message Authentication

Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.

D. Node Compromise Resilience

The scheme should be re-salient to node compromise attacks. No substance how many nodes are compromised, the left over nodes be able to still be protected.

E. Efficiency

This scheme should be efficient in terms of both computational and communication overhead.

IV. PROPOSED SYSTEM

A. Source Anonymous Message Authentication on Elliptic Curves

In this section, we propose a completely protected and resourceful SAMA. The foremost thought is that for each message m to be unrestricted, the message sender, or the sending node, generates a resource unidentified message authenticator for the message m. The production is based on top of the MES method on top of elliptic curves.

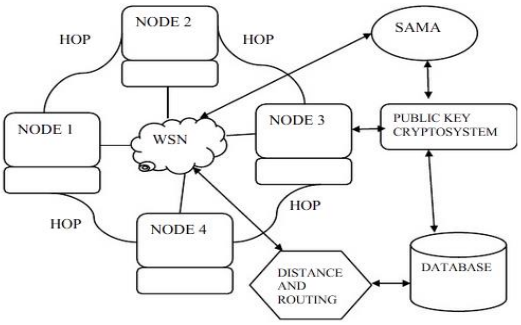


Fig.1. System Architecture

in support of a ring signature, every ring member is necessary to calculate a fake signature for all further members in the AS. In our method, the whole SAMA creation requires just three steps, which tie each and every one non-senders plus the message sender to the SAMA comparable. In accumulation, our plan enables the SAMA to be confirmed throughout a single equation without independently verifying the signatures. This is the enhanced form of SAMA it generates a source unidentified message authenticator for the message. The creation is based on MES method on elliptic curves. SAMA creation requires three steps, which link all non-senders and the message sender to the SAMA. SAMA is established all the way through a solitary equation without independently verifying the signatures.

B. Modified Elgamal Signature Scheme

The modified ElGamal signature scheme consists of the following three algorithms. In Key generation algorithm, Let p be a large prime and g be a generator. Both p and g are made public. For a random private key, the public key y is computed from

$$Y = g^x \bmod p \qquad (1)$$

In Signature algorithm, The MES can also include a lot of variants. For the reason of efficiency, we will explain the variant, called best method. To sign a message m, one chooses a random k, and then computes the exponentiation

$$Y = g^x \bmod p \qquad (2)$$

and solves s from

$$S = rxh(m,r) + k\text{mod } (p-1) \qquad (3)$$

Where h is a in one direction hash function and The signature of message m is defined as the duo

$$M = \text{pair } (r,s) \qquad (4)$$

In Verification algorithm: The verifier checks whether the signature. If the equality holds right, then the verifier accepts the signature, and Rejects if not.

C. Hop by hop message authentication And Compromised Node Detection

We assume that all sensor information will be delivered to a sink node, which can be colocated
With the Security Server (SS).Since the SAMA scheme guarantees that the message integrity is untampered, when a bad or meaningless message is received by the drop node, the resource node is viewed because compromised. But the compromised resource node only transmits solitary message, it would be extremely not easy for the node to be identified without additional network traffic information. However, when a compromised node transmits more than solitary message, the drop node be able to slender the possible compromised nodes down to a extremely small set. When the compromised resource node transmits two messages, the drop node will be able to tapered the resource node down to the set .if the drop node keeps tracking the compromised message, at hand is a lofty likelihood that the compromised node can be inaccessible. If the compromised nodes repeatedly employ the similar AS, it makes interchange examination of the compromised nodes possible, when a node has been identified as compromised, the SS be able to take away its public key from its public key catalog. Once the public key of a node has been detached from the public key catalog, and/or broadcasted, any message with the AS containing the compromised node be supposed to be dropped without any procedure in order to save the valuable sensor power.

D. Source Privacy

An AS (Anonymous set) acting a solution function in message resource solitude, since the real message resource node will be hidden in the AS. In this part, we will talk about techniques that can avoid the adversaries as of tracking the message resource through the AS examination in blend with limited interchange examination. Earlier than a message is transmitted, the message resource node selects an AS from the public key catalog in the SS as its preference. This set should include itself, jointly with a number of other nodes. While an adversary receives a message, he can perhaps find the direction of the preceding jump or even the real node of the preceding jump. However, the adversary is unable to distinguish whether the preceding node is the actual resource node or simply a forwarder node if the adversary is unable to monitor the traffic of the preceding hop. Therefore, the selection of the AS should create enough variety so that it is infeasible for the adversary to find the message resource based on the selection of the AS itself.

E. Key Sever Management

Key management is one of the main issues for secret-key based verification methods. This is particularly accurate for big level WSNs. whereas several of these schemes are intended to give node verification; they can only give end-to-end node verification using the secret key shared between the two nodes. This means that no midway node can validate the message in broad. The midway nodes may have to forward a manipulated message for lots of hops before the message can finally be authenticated and dropped by the getting node. This not simply consumes additional sensor power, but too increases the network collision and decreases the message delivery ratio. Therefore, raising a protocol that can supply hop-by-hop midway node verification is an important research mission.

Most of the verification schemes are based on symmetric-key methods, including the polynomial valuation based verge verification method. Our method enables every node to transmit the message to the drop node as a message originator. The recent growth on ECC has verified that the public-key based methods contain more reward in terms of memory practice, message difficulty, and security pliability, since public-key based approaches contain a easy and fresh key management.

V. EXPERIMENTAL RESULTS

We conduct simulations using NS2 on Red Hat Linux system. In this Section, we implement our proposed scheme and the bivariate polynomial based scheme in a real world comparison. The comparison is based on comparable security levels.We will compare the computational overhead, communication overhead, delivery ratio, power utilization, broadcast delay, and memory expenditure of our projected method with the bivariate polynomial-based scheme.

A. Network Formation

In our simulation Wireless sensor network contain 32 nodes.We presume there is a security server (SS) that is accountable for generation, storage and allocation of the security parameters between the networks.

B. Attacker Performance

In WSN, false data injection and packet loss is occurs by means of attacker node present in network due to wireless environment. The attacker present in the network means the throughput level is decreased. The attacker is not present in the network means the throughput level is high. Due to attacker the performance of the network is decreased and the data get lost or modified. We assume there is 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.

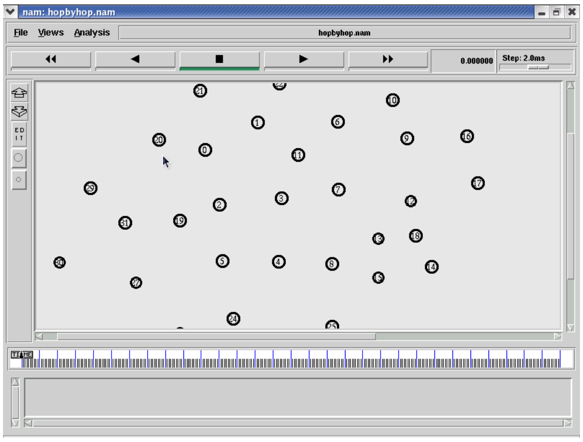


Fig.2. network formation

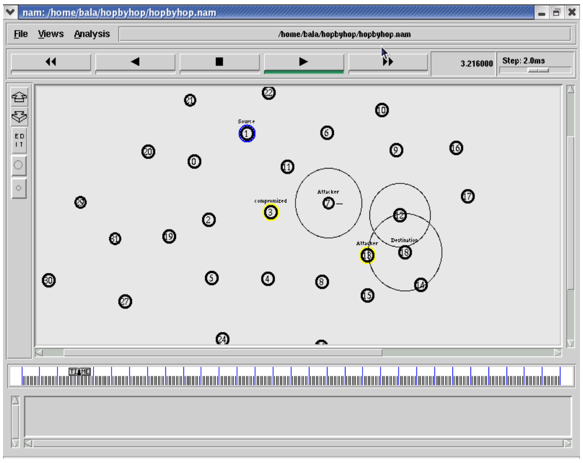
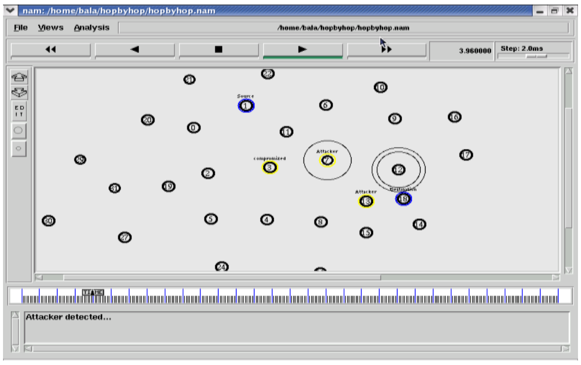


Fig.3. Attacker performance

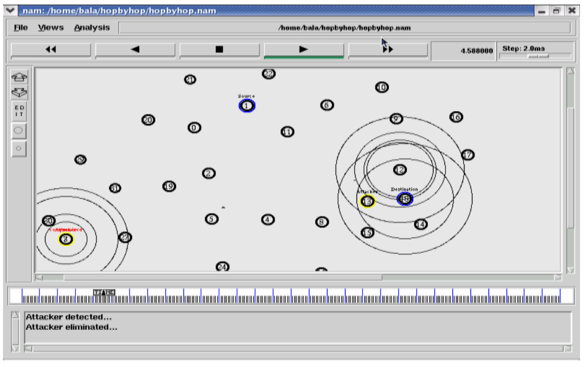
C. Detect and Eliminate Attacker

The attacker node is determined and eliminate by our proposed scheme. Compromised node detection is important purpose of our proposed system.



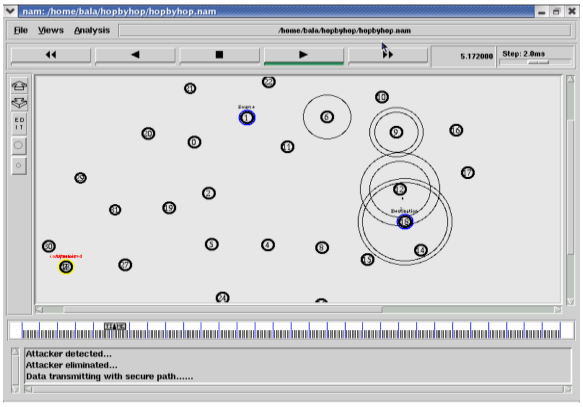
```
Attacker detected...
```

Fig.4. Detection of Attacker


nam: /home/bala/hopbyhop/hopbyhop.nam
File
Views
Analysis
/home/bala/hopbyhop/hopbyhop.nam
4.588000
Step: 2.0ms
Source
Attacker
Destination

```
Attacker detected...
Attacker eliminated...
```

Fig.5. Elimination of Attacker



Attacker detected...
Attacker eliminated...
Data transmitting with secure path......

Fig.6. Data Transmission In Secure Path

After elimination of attacker data transmitted through secure path. So overall network efficiency is increased.

D. Energy Consumption

In large scale WSNs the existing bivariate polynomial based scheme consumes extra sensor power, when compare to our proposed scheme that can improve energy consumption by enabling intermediate node authentication.

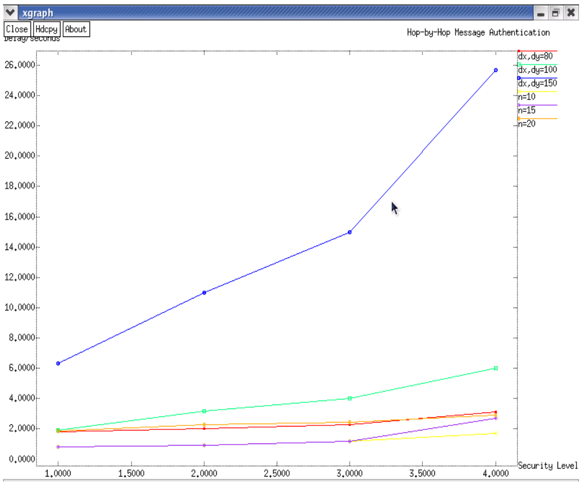


Fig.8. Message Transmission Delay

E. Message Transmission Delay

The communication overhead is determined by the message length. The large communication overhead of the polynomial based scheme will increase the message delay. Our proposed scheme has much lower message delay.

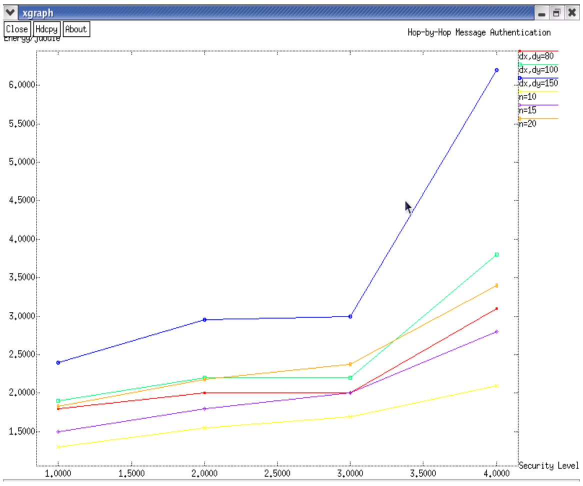


Fig.7. Energy Consumption

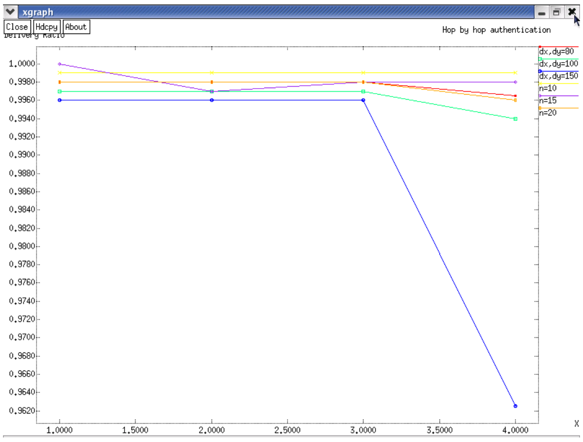


Fig.9. Delivery Ratio

F. Delivery Ratio

The outcome shows that the projected method is slightly better than the bivariate polynomial based method in delivery ratio.

VI. CONCLUSION

Message authentication is an important concern in any network: without this unauthorized users could easily introduce invalid data into the organization. This service is usually provided through the deployment of a secure message authentication code (MAC). In this paper, we first proposed a novel and efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC). While ensuring message sender confidentiality, 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, we then propose a hop - by-hop message authentication scheme based on the SAMA. By providing Message authentication, Message reliability and hop by hop message authentication then source should be in high privacy and network should be efficient.

REFERNCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, “Statistical en -route filtering of injected false data in sensor networks,” in IEEE INFOCOM, March 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,” in IEEE Symposium on 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,” in Advances in Cryptology Crypto’92, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[4] W. Zhang, N. Subramanian, and G. Wang, “Lightweight and compromise resilient message authentication in sensor networks,” in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[5] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, “Attacking cryptographic schemes based on

[6] perturbation polynomials”,” Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org.

[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,” in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[8] D. Pointcheval and J. Stern, “Security proofs for signature schemes,” in Advances in Cryptology EUROCRYPT,ser. Lecture Notes in Computer Science Volume 1070, 1996, pp. 387–398.

[9] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Communications of the ACM, vol. 24, no. 2, pp. 84–88, February 1981.