IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

*International Advanced Research Journal in Science, Engineering and Technology*
*Vol. 3, Issue 6, June 2016*

# Message Authentication and Secure Transmission in Wireless Sensor Networks Using Global Elliptic Curve Cryptography Method

**J. Ghayathri**[1], **M. Jhanani**[2]

Associate Professor, Department of Computer Science (PG), Kongu Arts and Science College (Autonomous), Erode, Tamilnadu, India[1]

M. Phil Research Scholar, Department of Computer Science (PG), Kongu Arts and Science College (Autonomous), Erode, Tamilnadu, India[2]

**Abstract:** Message authentication is used to stop unauthorized and corrupted messages from being in Wireless Sensor Networks (WSNs). Message authentication schemes have two approaches: public-key based and symmetric-key based approaches. To address these issues, this research work proposes a scalable authentication scheme based on Global Elliptic Curve Cryptography (GECC). The proposed scheme allows any number of messages to transmit in intermediate node authentication. In addition, the GECC scheme can also provide message source privacy and multiple base station environments. The proposed GECC scheme enables the intermediate node authentication so that all corrupted message can be detected and dropped.

**Keywords:** Key Management, ECC, GECC, ESAMA.

## I. INTRODUCTION

A Wireless Sensor Networks consists of a large number of resource constrained sensor nodes [1] that are widely distributed in a hostile environment and with the resource rich node called as the Base Station (BS). The task of the sensor nodes is to sense physical phenomena from its neighbour’s process them and transmit the sensed data to the other nodes or Base stations. WSNs are for monitoring, tracking and controlling the sensor nodes. But, a sensor node has constraints in terms of power, computation, storage and communication.
The multi-hop communication is preferred when large numbers of nodes are used for transmitting the messages over WSNs. After the nodes get deployed it cannot be manually maintained and monitored because of the security problems. In that case maintaining and monitoring of sensor node and their network of communication becomes difficult in WSNs.

The critical situation arises while the data can be sent and accessed by any node in the network and providing authentication to access this data for preventing unauthorized users from gaining the information. The WSNs consist of a large number of sensor nodes. Each sensor node in the WSNs knows its correct location in the sensor domain and it can be communicating with its neighbouring nodes directly. The whole network is fully connected via multi-hop communications. Security server (SS) is used for generating, storing and distributing the security parameters in the network. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information stored in the sensor nodes can be detected and accessed by the attackers. Then the attackers can be able to reprogram the information which should be sent. Then the Compromised nodes which are captured by the attackers will not be able to create new public keys by the SS and other nodes.

In Passive attacks, the third parties could secretly listen to the messages which are transmitted in the network and perform traffic analysis. Active attacks can be launched from the compromised sensor nodes. Once the sensor nodes get compromised, the adversaries will obtain the information stored in the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages.

In addition, the scheme can also provide message source privacy. Also multiple base station environments are considered. Here the adversary is not only limited to modify the data packet but it can change the complete packet stream by adding extra packets. So the receiver must confirm whether the data used in any decision-making process comes from the authorized source. Data authenticity should identify the communicating nodes and it is used for recognizing and rejecting the information from illegal nodes. Authentication is required for many administrative tasks.

The remainder of this paper is organized as follows. Section 2 reviews the security issues and related works in wsns. Section 3 we briefly discuss authentication mechanism and then the proposed authentication methodologies are presented in section 4. Section 5 discuss about the results. Section 6 concludes this paper and finally section 7 consists of references.

DOI 10.17148/IARJSET.2016.3650

## II. RELATED WORKS

Authentication in WSNs can be divided into three categories, namely base station to sensor nodes, sensor nodes to other sensor nodes, and outside users to sensor nodes. The problem of authenticated broadcast by the base station has been widely addressed [2], [5], [9], [10], [11]. We focus on the other two categories, i.e., authenticated broadcast/multicast by the sensor nodes and outside user authentication.

A. Authentication broadcast/multicast by the sensor nodes
During multi-hop forwarding the wireless communication allows third parties to compromised the nodes and inject false messages causes sensor nodes to relay false data and deplete their energy. In that case the sensor nodes on the path should be able to authenticate and filter out false messages as early as possible to save energy. Therefore, they are also potential receivers of these messages, arising the need of authenticated multicast by sensor nodes. In battlefield application, all sensor nodes in the network are potential receivers of critical information, arising the need of authenticated broadcast by sensor nodes. To summarize, all these secure mechanism are used to enable all sensor nodes in the network to send an immediate authenticated message to report when there is a critical situation arises, and on the other hand, it enables every receiver to verify this message whether it has been send by the authenticated sender or by the adversaries . For simplicity, both broadcast and multicast are referred as broadcast in the rest of this paper.

B. User Authentication
Sensor nodes data may be confidential and in some situations only the subscribed users, who have paid, are allowed to obtain this data. A user authentication mechanism aims to prevent unauthorized users to access data from sensor nodes. Usually, a mechanism to provide an outside user access to sensor nodes data requires three tasks:

- User Authentication allows only legitimate users of the data to access it.
- Access Control allows a user to access only the data which he is entitled to access.
- Session Key Establishment enables secure exchange of user queries and confidential data between users and sensor nodes.

In centralized user authentication, all users are authenticated through the base station. This mechanism is easy to deploy because the base station is a powerful device which can perform complex cryptographic operations. However, this approach has a few drawbacks. Firstly, it makes the base station a single point of failure. Secondly, it causes sensor nodes near the base station to deplete their energy quickly as for every user request; they relay packets between base station and queried sensor nodes.
Furthermore, it causes a severe DOS attack where an adversary sends fake request messages causing sensor nodes to relay them towards the base station for verification, increasing network traffic and depleting their energy User authentication schemes discussed in [4], [8], all suffer from these problems. To avoid this kind of DOS attack, a user should be locally authenticated by the sensor nodes without the involvement of a third entity, i.e., a distributed approach. This approach reduces traffic congestion and transmission overhead within the network. However, it puts the burden of authentication on sensor nodes. As sensor nodes are resource constrained devices as compared to the base station, a lightweight user authentication mechanism is needed for sensor nodes to verify authenticity of the users.

Data integrity and data origin authentication are the minimum security requirements to prevent modification and insertion of false data into the network, which would otherwise distort the overall results. This can be achieved using Message Authentication Codes (MACs) or cryptographic signatures which are attached to network packets and validated by the receiver. Another approach, using classic Public Key Cryptography (PKC) with Public Key Infrastructure (PKI), involves a huge key distribution problem on a distributed network of wireless sensor nodes, since every node would need access to the senders' public keys.

A. An intrusion detection scheme for routing and service level attack discovery
The mobile ad-hoc networks are infrastructure less environment. The system performs two types of intrusion detection process. The routing based attack detection process uses the EAACK scheme [12]. RSA algorithm and Secure Hash Algorithm (SHA) are used for the security process. The service request based attack detection is integrated with the system. The EAACK scheme is used for the routing level attack detection process. The Bayesian classification algorithm is used for the service request based attack detection process. The cluster based detector assignment model and cluster integrated detector assignment models are used for the detector assignment process. The simulation process is tested with different network conditions and node count levels. The energy consumption, traffic rate and detection latency performance metrics are used to evaluate the system performance. Dynamic interval is assigned for intrusion detection process. The system reduces energy consumption, network traffic and detection latency in all network conditions.

## III. AUTHENTICATION METHODOLOGY

A. Message Authentication Code
MACs provide a way to authenticate messages between parties of communication partners. They enable detection of modification of the message itself, data integrity, but also authentication of data origin, i.e. knowing who send a message. It requires the senders and the receivers to share a common private secret, the Pre-Shared Key (PSK). Only the parties knowing the PSK can produce valid MACs for messages and are able to verify MACs for messages.

DOI 10.17148/IARJSET.2016.3650

### B. Public Key Signatures

PKC is an asymmetric cryptographic concept using different keys for en-/decryption and signing/verification. Some early implementations of this concept are RSA [2], which can use for confidentiality and authentication, and Digital Signature Algorithm (DSA), only for authentication. Each member of the crypto system has its own private and public key. The private key is used to sign messages and proof the ownership of a certain key. Using the public key, receivers can verify signatures of messages.

To identify nodes in a WSN by their public key, the public key needs to be securely bound to the identity of one particular node and this binding must be known at verification time by the verifying entities. Otherwise they can't know who signed a message. One way to do this, and as it is done in the World Wide Web (WWW), is to use certificates. Certificates basically bind a public key with an identity and are signed by a higher entity, a Certificates Authority (CA), which assures this binding. Using this concept all nodes only have to trust the CA. There are also PKC schemes, which are based on Elliptic Curve Cryptography (ECC). For the same level of security, ECC-based schemes, like elliptic curve DSA, require smaller public key sizes due to fact that the underlying mathematical problem of DSA, computing discrete logarithms, is much harder on elliptic curves.

Different certificate/key distribution models are imaginable for PKC in WSNs. One way is to distribute all certificates on all nodes. This requires large storing capabilities for the nodes and is hard to maintain on change of membership. Once a node is added to the network, its certificate needs to be distributed to all sensor nodes, so they can identify the new node. Another way of handling the key distribution problem is, sending the certificate, which binds the public key used to create a signature to an identity, along with the message and signature. This certificate, signed by a CA, can then be verified using the static public key of the CA and afterwards, the actual signature can be verified using the public key of the certificate. Since a valid, with respect to the public key in the certificate, signature can only be generated using the secret private key corresponding to the public key, the sender has proven ownership of this private key and is thereby securely identified.

### A. Cryptographically Generated Addresses

CGAs, as described by Aura [3], provide a way to proof that a public key belongs to a certain communication partner. This is done by having the network address of the communication partner include a hash of the public key. In IPv6 this are the lower 62 bits of the address. CGAs have been primarily designed for authenticating neighbour discovery and router advertisement replies. The public key sends along can be proven to belong to the sender by verifying it against the senders address which includes a hash of its public key. Since CGAs proof ownership of a public key, a CA is not needed. This facility is deployment in distributed and spontaneous settings. However, the CGAs aren't certificate themselves and anybody can generate a new valid CGA for a subnet, although resulting in a different address. Having part of the address being occupied for the hash of a nodes public key, limits the free choice of an address [9, p. 83].

### C. Identity Based Signatures

IBSs are signatures based on Identity-based Cryptography (IBC), where each party of the system can use any bit string, i.e. an e-mail address or IP-/Ethernet address, as their public key. IBC, first introduced by Shamir, provides asymmetric cryptography, where an arbitrary string can be used as public key and the corresponding private key is generated by a common trusted entity of the participating entities, usually known as TA [5].The private keys are then securely distributed to each authenticated member of the system. For signature verified only the public parameters of the system, sender's public key, message and signature are needed. There are various schemes for realization of IBC, classified as either pairing-based or pairing-free. A pairing-based IBC scheme is used to pairing-based cryptography to implement an identity-based encryption scheme [2]. Pairing-free IBCs schemes haven't seen much attention with in the research community compared to paring-based approaches and space-efficient IBC, which has considerably worse performance [3].

## IV. PROPOSED AUTHENTICATION METHODOLOGIES

### A. ECC Methodology

ECC algorithm develops a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity. It offers an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation. It devises network implementation criteria on source node privacy protection in WSNs. It proposes an efficient key management framework to ensure isolation of the compromised nodes. 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 existing system, the entire (Source Anonymous Message Authentication) SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA. The following problems are very challenge in WSN message authentication system.

- Adaptable only in situations where same initial set of resource availability.
- Suitable for single cloud service provider environment only.
- Data transfer cost is not considered between different cloud data centres.

### B. GECC Methodology

GECC algorithm is an unconditionally secure and efficient source anonymous message authentication (ESAMA)

DOI 10.17148/IARJSET.2016.3650

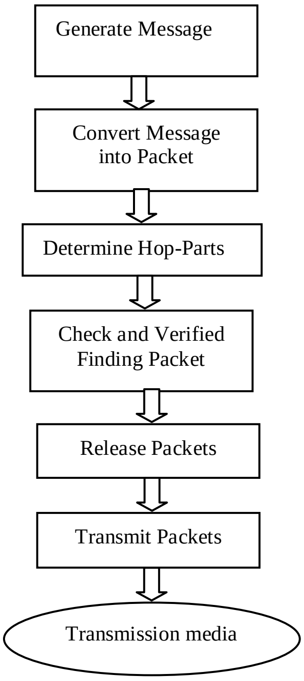
scheme based on the optimal modified ELGAMAL signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. While achieving compromise-resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based algorithms under comparable security levels. The following problems are solving in this paper WSN message authentication system.

- It is suitable for heterogeneous sensor node environment.
- Multiple base station or sink node environment is considered.

C. Architecture

In this paper, for the Fig 1 hop by hop message transaction first a message has been generated. The generated message is converted into the packets, and then by the performance of the hop, the packets are determined to choose the hop parts. The packets are processed into the hop by checking and verifying the public key using elliptical curve cryptography in the node and transmit the packet to the transmission media.

The Fig 2 transmission media receives and display the packet and the packet is converted into the message by checking and verifying the key with the help of geometrically elliptical curve cryptography method. Finally the released packet is received with the corresponding packet



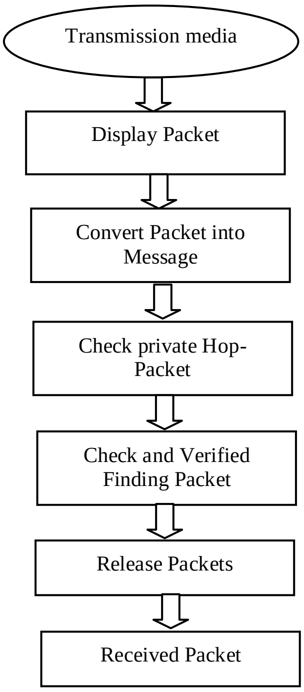


Fig. 1. ECC Methodology Fig. 2. GECC Methodology

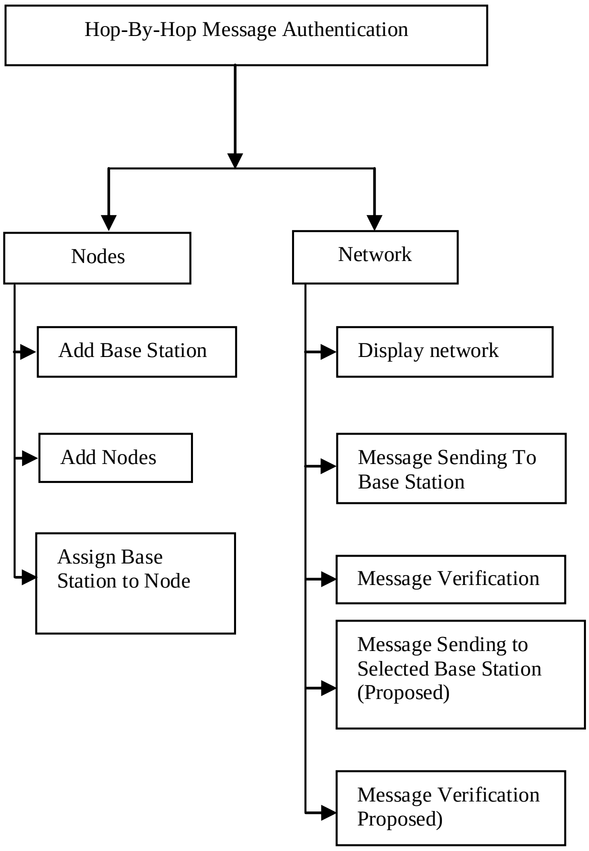

Hop-By-Hop Message Authentication
Nodes
Network
Add Base Station
Add Nodes
Assign Base Station to Node
Display network
Message Sending To Base Station
Message Verification
Message Sending to Selected Base Station (Proposed)
Message Verification Proposed)

Fig. 3 Hop-By-Hop Authentication Process

D. Algorithm

1) Authentication Generation Algorithm:

Suppose m is a message to be transmitted along with base station node id. The private key of the message sender User1 is dt; 1 <= dt <= n. To generate an efficient scheme for message m, User1 performs the following steps:

//For User1 to sign a message m

1. Select a random hop level integer $H_A$, $1 \leq H_A \leq N \leq 1$.
2. Calculate total hop level with total terminal client node N1
3. Select a random integer $k_A$, $1 \leq kA \leq N \leq 1$.
4. Calculate $r = x_A \bmod N$ & $H_A$ Mod $N_1$, where $x_A$; $y_A = k_A G$. If $r = 0$, go back to step 1.
5. Calculate $h_A \leftarrow h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and ← l denotes the l leftmost bits of the hash.
6. Calculate $h_A \leftarrow G(m, r)$, where h is a cryptographic hash function, such as SHA-1, and ← l denotes the l leftmost bits of the hash.
7. Calculate $s = rd_A h_A + kA \bmod N$.If $s = 0$, go back to step2
8. The signature is the pair (r1, s1).

2) Verification algorithm:

For User2 to verify the scheme $(m, S, r1, y1 \dots r_n, y_n, s)$, User2 must have a copy of the public keys Q1... Qn.

The proposed GECC algorithm checks the hop level whether the node is persist on the global elliptic curve to enable the intermediate nodes to authenticate the message.

//For User2 to authenticate User1's signature

1. Check that $H_A$. ≠ O otherwise invalid
2. Check that Global Curve Point $G_P$
3. Checks that $Q_A$ ≠ O, otherwise invalid
4. Checks that $Q_A$ lies on the curve
5. Checks that nQA ≠ O

After that, Bob follows these steps to verify the signature:

1. Verify that r and s are integers in $[G_p, N \leq 1]$. If not, the signature is invalid.
2. Calculate $h_A \leftarrow h\ (m, r1)$, where h is the same function used in the signature generation.
3. Calculate $(x1, x2) = sG \leftarrow r\ h_A\ Q_A \bmod N_1$.
4. The signature is valid if $r = x_1 \bmod N_1$, otherwise invalid.

## V. RESULTS AND DISCUSSION

The experimental result for secure transmission node analysis of existing system contains number of time slot interval in minutes and by using that given time interval, the average ratio of secure transmission node's percentage will be detected.

TABLE I ECC SECURE TRANSMISSION

| S. No | Node Details | Time Slot | Ratio of Secure Transmission Node (%) |
|---|---|---|---|
| 1 | Node1, Node2, Node3 | 10 | 0.43 |
| 2 | Node4, Node5, Node6 | 20 | 0.52 |
| 3 | Node7, Node8, Node9 | 40 | 0.61 |
| 4 | Node10, Node11, Node12 | 60 | 0.69 |
| 5 | Node13, Node14, Node15 | 80 | 0.74 |
| 6 | Node16, Node17, Node18 | 100 | 0.80 |
| 7 | Node19, Node20, Node21 | 120 | 0.86 |
| 8 | Node22, Node23, Node24 | 140 | 0.90 |
| 9 | Node25, Node26, Node27 | 150 | 0.93 |
| 10 | Node28, Node29, Node30 | 160 | 0.97 |

The experimental result based on Table I for secure transmission node analysis of existing system is described in the Fig 4.

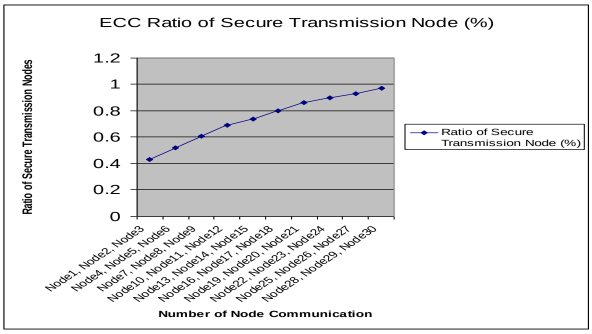


Fig. 4. ECC Secure Transmission

This chart shows the time slot interval and ratio of secure transmission of the respective node in percentage.

The experimental result for secure transmission node analysis of proposed GECC method contains number of time slot interval in minutes and by using that time interval, the average ratio of secure transmission node's percentage will be detected (Table II)

TABLE II GECC SECURE TRANSMISSION

| S. No | Node Details | Time Slot | Ratio of Secure Transmission Node (%) |
|---|---|---|---|
| 1 | Node1, Node2, Node3 | 10 | 0.48 |
| 2 | Node4, Node5, Node6 | 20 | 0.57 |
| 3 | Node7, Node8, Node9 | 40 | 0.66 |
| 4 | Node10, Node11, Node12 | 60 | 0.72 |
| 5 | Node13, Node14, Node15 | 80 | 0.77 |
| 6 | Node16, Node17, Node18 | 100 | 0.83 |
| 7 | Node19, Node20, Node21 | 120 | 0.89 |
| 8 | Node22, Node23, Node24 | 140 | 0.92 |
| 9 | Node25, Node26, Node27 | 150 | 0.95 |
| 10 | Node28, Node29, Node30 | 160 | 0.98 |

The experimental result based on Table II for secure transmission node analysis of existing system is described in the Fig 5 This chart shows the time slot interval and ratio of secure transmission of the respective node in percentage.

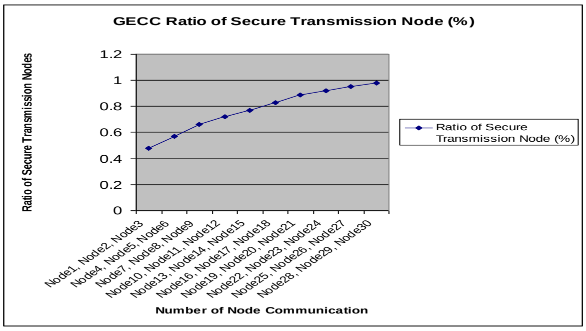


Fig. 5. GECC Secure Transmission

The experimental result shows the comparison of secure transmission node analysis of the existing system (ECC) and proposed system (GECC). The Table III shows the increased average ratio of secure transmission node's percentage (GECC).

The comparison based on experimental results of existing system (ECC) and proposed system (GECC) secure transmission communication node analysis is described in the Fig 6.

TABLE IIII COMPARISON FOR ECC AND GECC SECURE TRANSMISSION

| S. No | Node Details | Time Slot | Ratio of Secure Transmission Node (%) | |
|---|---|---|---|---|
| | | | ECC | GECC |
| 1 | Node1, Node2, Node3 | 10 | 0.43 | 0.48 |
| 2 | Node4, Node5, Node6 | 20 | 0.52 | 0.57 |
| 3 | Node7, Node8, Node9 | 40 | 0.61 | 0.66 |
| 4 | Node10, Node11, Node12 | 60 | 0.69 | 0.72 |
| 5 | Node13, Node14, Node15 | 80 | 0.74 | 0.77 |
| 6 | Node16, Node17, Node18 | 100 | 0.80 | 0.83 |
| 7 | Node19, Node20, Node21 | 120 | 0.86 | 0.89 |
| 8 | Node22, Node23, Node24 | 140 | 0.90 | 0.92 |
| 9 | Node25, Node26, Node27 | 150 | 0.93 | 0.95 |
| 10 | Node28, Node29, Node30 | 160 | 0.97 | 0.98 |

This chart shows the increase of secure percentage in GECC method than the existing ECC.

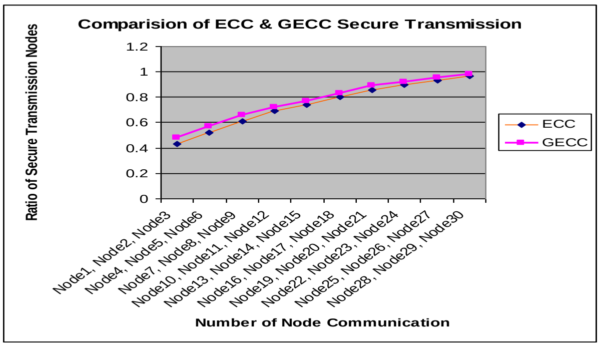


Fig. 6. Comparison for ECC and GECC Secure Transmission

1) Findings:

- For ECC Scheme, the energy cost is high and ratio of secure communication is low. While for the proposed GECC Scheme the energy cost is reduced and the ratio of secure communication is increased. The results will be 25 % to 40% of cost is reduced for the secure communication.
- The proposed GECC Scheme is providing better result to compare the ECC scheme in the authentication mechanism and in the proposed scheme, the verifying time is about half of the authentication generation time, and the generation time is shorter than the verification time.
- Memory utilization of the GECC Scheme is very low comparing to the existing ECC Scheme. The GECC Scheme consumes up to 30 % of memory.
- GECC Scheme provides the efficient energy cost. It provides 25% of cost will be reduced than the existing ECC scheme.
- This GECC scheme doesn't have the threshold problem, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken.

## VI. CONCLUSION

In this paper, we proposed to use message sending, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting multiple attackers in wireless networks. It provided theoretical analysis of using the hop by hop based inherited from wireless nodes for attack detection. The approach can both detects the presence of attacks as well as determine the number of adversaries we can localize any number of attackers and eliminate them. In addition, a Multi hop-based node message sending and compromise detection scheme is proposed using the Global Elliptic Curve Cryptography (GECC). Furthermore, several possible attacks are described against the proposed scheme and proposed multi hop based measures against these attacks. The scheme is evaluated in simulation under various scenarios. The experimental results show that the scheme quickly detects untrustworthy multi hop with a small number of trust reports. In future, the scheme may evaluate against various types of attacker models. It is believed that a game theoretic model is suited for this evaluation. A variety of strategies may be studied that may be taken by detector and adversary.

## REFERENCES

[1] 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.

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

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

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

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

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

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

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

[10] 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.

[11] 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.

[12] J. Ghayathri and L. Parthasarathi, "An integrated intrusion detection scheme for routing and service level attack discovery", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015.

DOI 10.17148/IARJSET.2016.3650