IMPROVED SOURCES ANONYMITY MESSAGE AUTHENTICATION CODE TECHNIQUE USING GLOBAL HOP LEVEL PUBLIC CRYPTO SCHEME IN WSN

Jeyakumar. L
M.Phil Part time Scholar
Department of Computer Science
Erode Arts College and Science, Erode, India
Mob.No:80569-99987

Dr. Senthil Kumar. C
Associate Professor
Department of Computer Science
Erode Arts and Science College, Erode, India
Mob.No 9486273812

Abstract--- Message authentication is one of the most effective ways to stop unauthorized and corrupted messages from being forwarded in Wireless Sensor Networks (WSNs). Message authentication schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. The symmetric-key based approach requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a Message Authentication Code (MAC) for each transmitted message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. For this reason, many message authentication schemes have been developed, based on public-key cryptosystem. However, both symmetric and public-key methods have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks*. This paper proposes a scalable authentication scheme based on Elliptic Curve Cryptography (ECC). While enabling intermediate nodes authentication, the proposed scheme allows any node to transmit an unlimited number of messages with safety. In addition, the Global Hop Level Public Crypto Scheme (GHLPS) scheme can also provide message source privacy in multiple base station environments.

Keywords— ***Source Anonymous Message Authentication Code (SAMC), Key Management (KM), Elliptic Curve Cryptography (ECC), Global Hop Level Public Crypto Scheme (GHLPS), Message Verification (MV).***

I. INTRODUCTION

A Wireless Sensor Networks consists of a large number of resource constrained sensor nodes [1-2] that are spatially distributed in a hostile environment and the resource rich node called as the Base Station (BS) (Fig 1.1). The sensor nodes task is to sense physical phenomena from its immediate surroundings, processes and transmit the sensed data to the other nodes or Base stations. WSNs are used in applications that are sensitive to environmental parameters that require monitoring, tracking and controlling. But, a sensor node has constraints in terms of power, computation, storage and communication. Also, as the number of nodes in the WSN is very large multi- hop communication is preferred in WSN. Since the nodes after the deployment cannot be manually maintained and monitored, security becomes critical. In such a scenario maintaining and monitoring of sensor node and their network of communication becomes a major issue in WSN. The data can be sent and accessed by any node in the network and providing authentication to access this data is critical preventing unauthorized users from gaining the information.

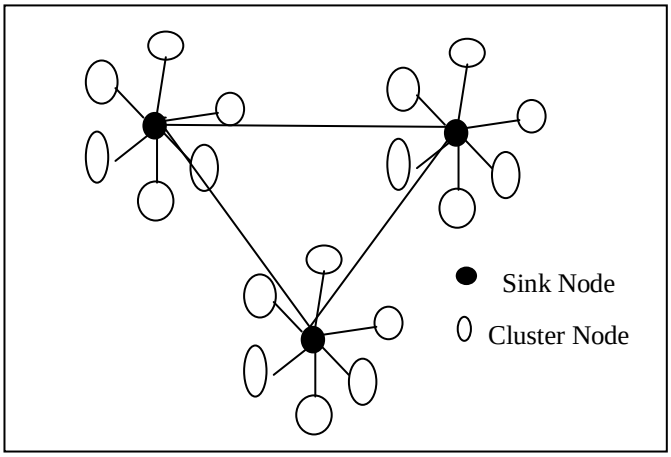


Fig 1.1 Wireless Sensor Work

Each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. Security Server (SS) 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. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the Security Server (SS) and other nodes.

This research paper considers two types of attacks launched by the adversaries: passive and active attack. Passive attacks, the adversaries could eavesdrop on messages transmitted in the network and perform traffic analysis. Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised nodes, including the security parameters of 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.

ISSN: 2278 – 1323

An 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 needs to confirm that the data used in any decision-making process comes from the authorized source. Data authenticity is an assurance of the identities of communicating nodes. Nodes taking part in the communication must be capable of 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 II reviews the Security Issues and related works in WSN. Section III we briefly discuss authentication mechanism and then the proposed authentication technologies in are presented in section IV. Section V concludes this paper explains.

II. *LITERATURE SURVEY*

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 [4] [9] [10] [11]. The problem of authenticated broadcast by the base station has been widely addressed [4]. The following section 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

There are many critical situations where a sensor node requires sending a quick message. For example:

- In a forest fire alarm application [13], sensor nodes deployed in a forest should immediately inform authorities about the event and the exact location of the event before the fire spreads uncontrollably.
- In a traffic application [3], whenever a sensor node senses an accident on the road it sends an immediate message in all directions to alert other traffic approaching this location.
- In a military application scenario [13], where a troop of soldiers needs to move through a battlefield. Sensor nodes deployed there detect the presence of the enemy and broadcast this information immediately throughout the network. Soldiers, passing near these sensor nodes, use this information to strategically position themselves in the battlefield.

Moreover, in all the above mentioned applications, sensor nodes on the path from the sender node to the receiver(s) relay the messages towards destination. Wireless communication allowing a challenger to inject false messages during multi hop forwarding [12] causes sensor nodes to relay false data and deplete their energy. Hence, sensor nodes on the path should be able to authenticate and filter out false messages as early as possible to save relaying energy [14] [15].

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 scenarios require a secure mechanism which, on one hand, enables all sensor nodes in the network to send an immediate authenticated message to report a critical situation, and on the other hand, enables every receiver to verify this message. 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 efficient.

User authentication schemes discussed in [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.

This paper proposed algorithm and approach to reduce traffic congestion and transmission overhead within the wireless sensor network. However, it puts the trouble 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.

ISSN: 2278 – 1323

III. AUTHENTICATION METHODOLOGY

A. Message Authentication Codes [MAC]

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.

B.Public Key Signatures [PKS]

Public key cryptography is an asymmetric cryptographic concept using different keys for encryption/decryption and signing/verification. Some early implementations of this concept are RSA [16], which can used for confidentiality and authentication, and Digital Signature Algorithm (DSA), only for authentication. Each member of the crypto system has it's 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.

C. Cryptographically Generated Addresses

CGAs, as described by Aura [17], 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 neighbor discovery and router advertisement replies. The public key sends 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 [18].

D. 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 [18]. 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 [19], [20]. Pairing-free IBCs chemes haven't seen much attention with in the research community compared to paring-based approaches and space-efficient IBC, which has considerably worse performance.

IV PROPOSED AUTHENTICATION METHODOLOGY

A. ECC METHODOLOGY

Elliptic Curve Cryptography (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

ISSN: 2278 – 1323

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.
- It is suitable for homogeneous sensor node environment.
- Only single base station or sink node environment is considered.

B. GHLPS METHODOLOGY

Global Hop Level Public Crypto Scheme (GHLPS) algorithm is an unconditionally secure and efficient source anonymous message authentication (ESAMA) 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 con- serve 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 4.1** 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 4.2** transmission media receives and display the message and the message is converted into the packet 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.

To send the packet from source to destination, first the source, destination node and the hop level node are selected. With the selected nodes the message is prepared and sends to the destination by producing a public key using Elliptical Curve Cryptography [ECC] method.

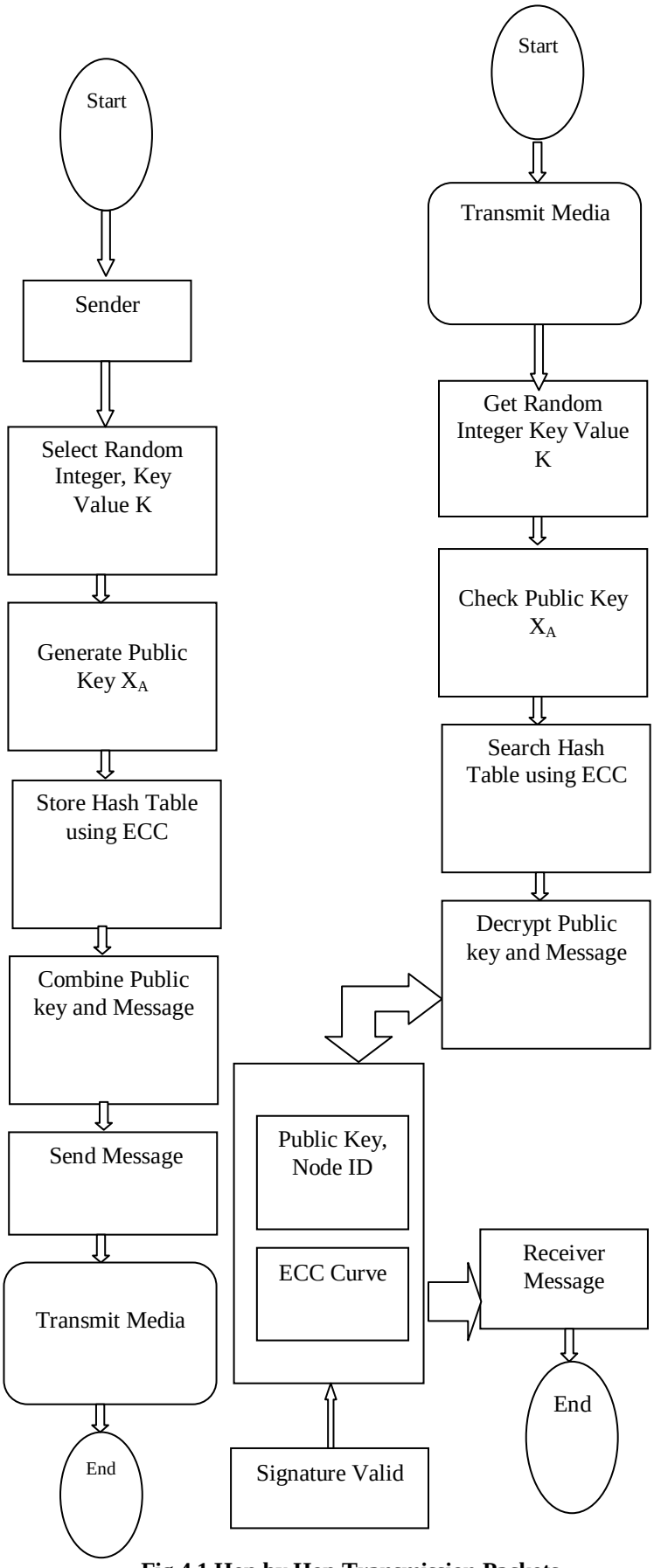


Fig 4.1 Hop by Hop Transmission Packets

ISSN: 2278 – 1323

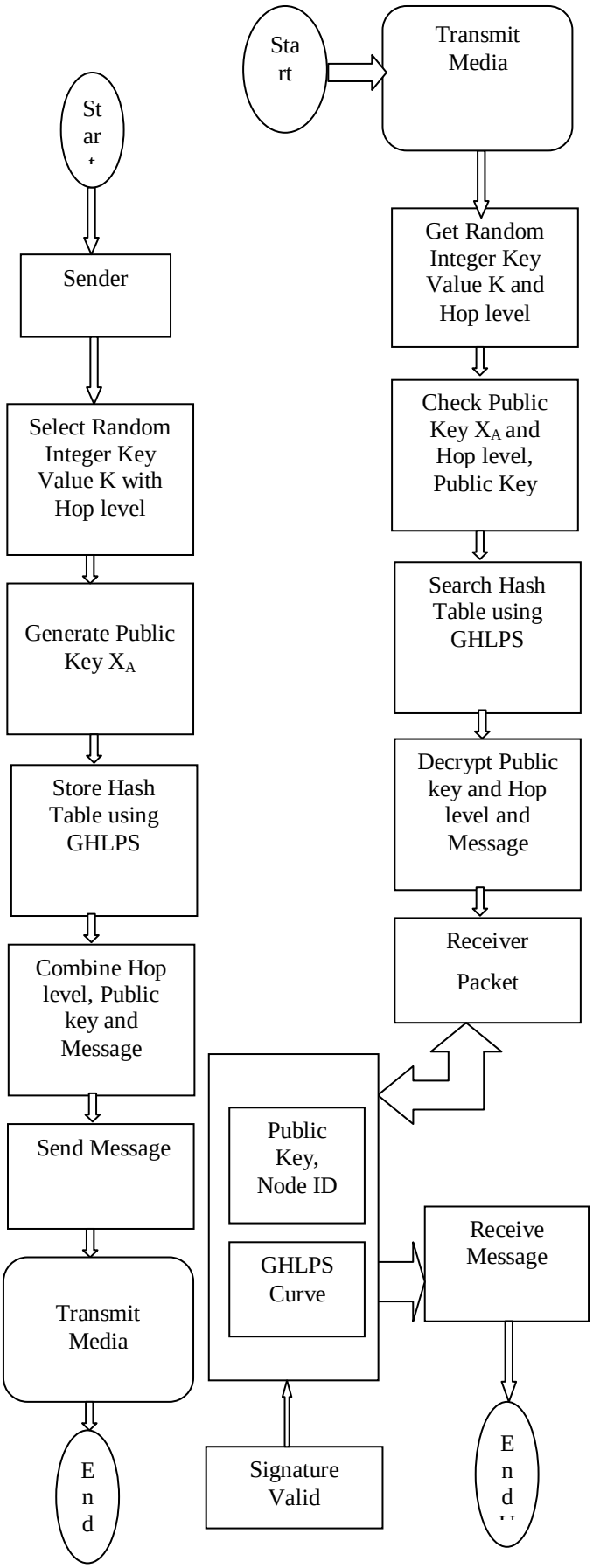


Fig 4.2 Transmission Media Receives Packets

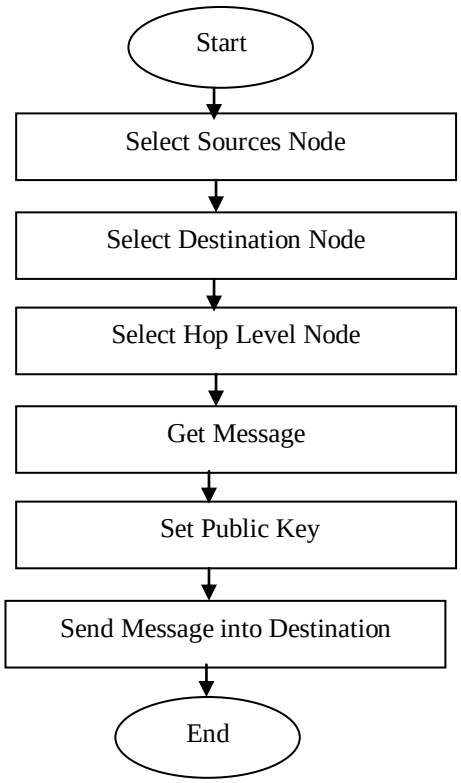


Fig 4.3 Transmission Media Sender Packets

The destination node receives the message only by checking the public key. The public key which is send to the destination is verified and then message is delivered.

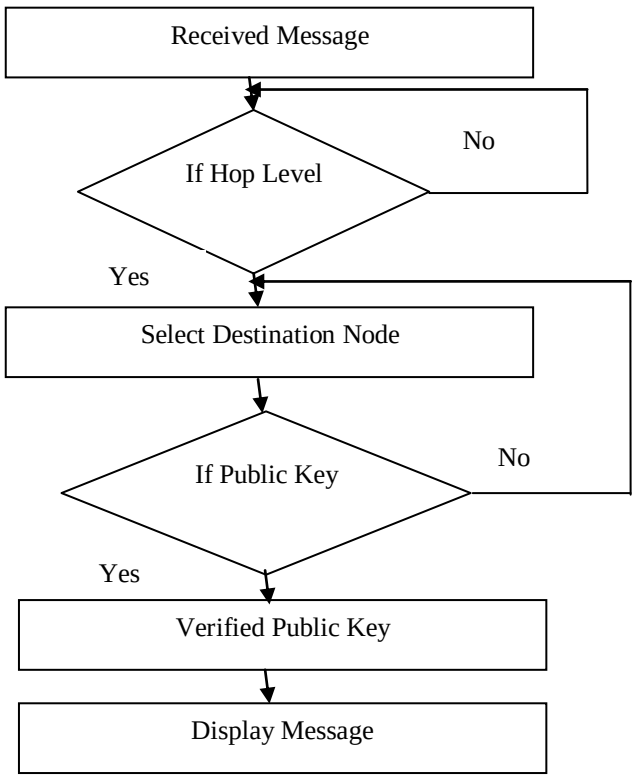


Fig 4.4 Receiver Packet Process

ISSN: 2278 – 1323

ALGORITHMS

/* Signature generation algorithm */

For Alice to sign a message **m**

// Select Number of Node and Range

Step 1: Select a random integer k_A, $1 \leq k_A \leq N \leq 1$.

Step 2: Calculate $r = x_A \bmod N$, where x_A; $y_A = k_A G$. If $r = 0$, go back to step 1.

//Calculated Node Distances and Applied Cryptography Function

Step 3: Calculate $h_A \leftarrow h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and $\leftarrow l$ denotes the l leftmost bits of the hash.

// Calculate Total Number of Key in ECC Curves

Step 4: Calculate $s = rd_A h_A + kA \bmod N$. If $s = 0$, go back to step 2.

//Signature generated

Step 5: The signature is the pair (r, s).

V. EXPERIMENTAL RESULTS

The packet drop count of existing hop base fixed and sliding window protocol is compared with the proposed GHLPS for Multi-Hop Wireless Networks. The packet drop count of existing protocol is drop count threshold 88 (ex: single hop). The packet drop count for the proposed protocol is 31(ex: multi hop) [Table 5.1].

The comparison of packet drop count in ECC and GHLPS.

Table 5.1 Comparison of Packet Drop Count of ECC and GHPLS

PACKETS [n]	ECC PACKET DROP COUNT [n]	GHLPS PACKET DROP COUNT [n]
25	12	8
50	21	17
75	32	28
100	40	33

Fig 5.1 shows the packet drop count of existing hop base ECC protocol is compared with the proposed model for Multi-Hop Wireless Networks.

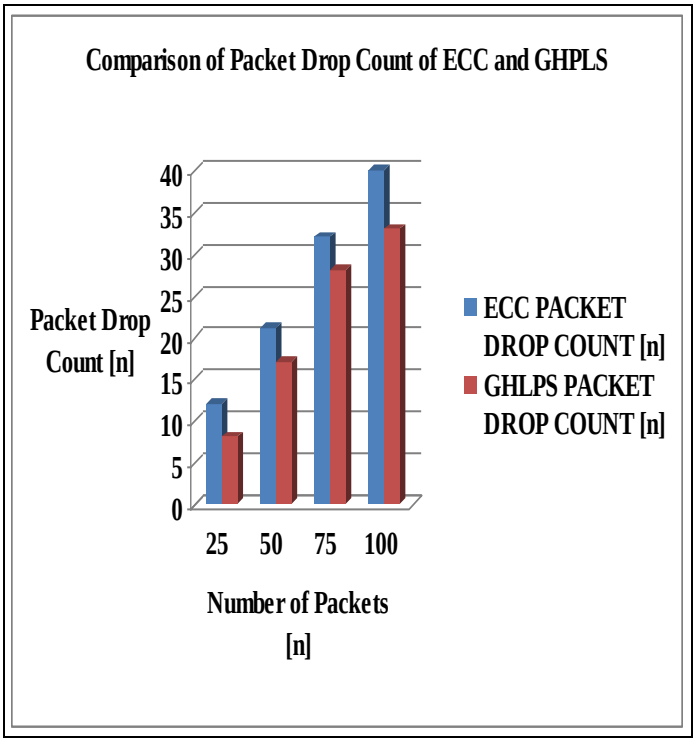


Fig 5.1 Comparison between ECC and GHPLS Packet Drop Count

First design a simplified mechanism to determine the number of neighboring nodes for any given node. Within time Tv, the given node crosses through an area and meets a number of neighbors N. Since wireless sensor nodes are assumed uniformly distributed in the network, approximate N by,

r= radious, T= time slot, V= velocity, ρ = hop level

Where r denotes the transmission range of nodes, *v* is the velocity, and *p* is the density of nodes in the network. Based on the obtained number of neighboring nodes N, we can on firm the value of threshold K.

Table 5.2 Experimental Result for Number of Node and Average of Attacker Node Finding in ECC System

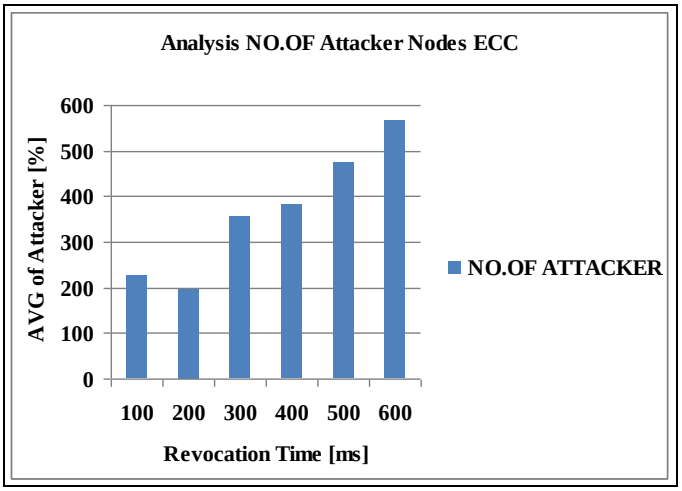
S.NO	REVOCATION TIME (ms)	NO.OF ATTACKER NODES	NO.OF ATTACKER NODES
1	100	226	234
2	200	195	213
3	300	356	383
4	400	384	405
5	500	475	487
6	600	566	625

ISSN: 2278 – 1323

The Table 5.2 represents experimental result for ECC system. The finding malicious node and revocation node process within millisecond details as followed.

The Fig 5.2 represents experimental result for ECC system. The finding malicious node and revocation node process within milliseconds details as followed.

The Fig 5.3 represents experimental result for GHLPS system. The finding malicious node and revocation node process within Milliseconds details as followed.



5.2 Existing ECC Number of Attacker

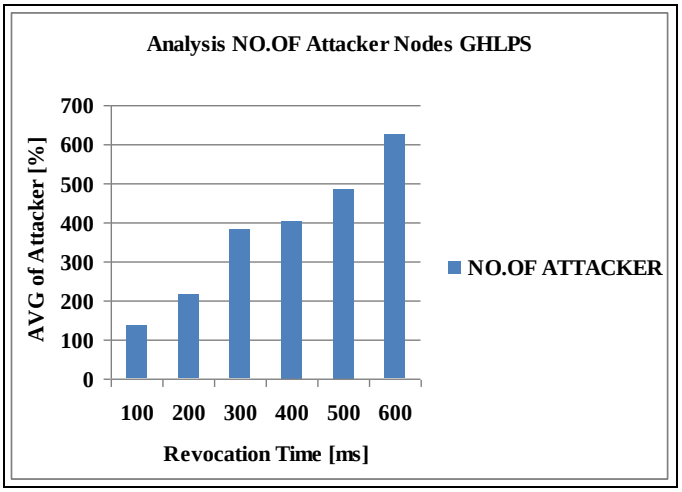


Fig 5.3 Proposed GHLPS - Number of Attacker

VI. CONCLUSION

In this paper, we proposed to use message sending, a physical property associated with each wireless sensor device that is hard to falsify and not reliant on cryptography as the basis for detecting multiple attackers in wireless sensor networks. It provided theoretical analysis of using the hop by hop based inherited from wireless sensor 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 sensor node message sending and compromise detection scheme is proposed using the Global Hop Level Public Crypto Scheme (GHLPS). 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] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, pp. 393–422, 2002.
[2] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," in Proc. EU-ROCRYPT '04. Springer-Verlag, 2004, pp. 268–286.
[3] J. Bohli, A. Hessler, O. Ugus, and D. Westhoff, "A secure and resilient WSN roadside architecture for intelligent transport systems," in Proc. WiSec '08. NY, USA: ACM, 2008, pp. 161–171.
[4] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," Computer Communications, vol. 31, no. 4, pp. 659 – 667, 2008.
[5] W. Chen and Y. Chen, "A bootstrapping scheme for inter-sensor authentication within sensor networks," Communications Letters, IEEE, vol. 9, no. 10, pp. 945–947, Oct. 2005.
[6] C. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and challenges," Proceedings of the IEEE, vol. 91, no. 8, pp 1247–1256, Aug. 2003.
[7] Crossbow, "MICA2." [Online]. Available: www.xbow.com
[8] M. Das, "Two-factor user authentication in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 8, no. 3, pp. 1086–1090, March 2009.
[9] J. Drissi and Q. Gu, "Localized broadcast authentication in large sensor networks," in Proc. ICNS '06. IEEE, p. 25
[10] D. Liu and P. Ning, "Multilevel mTESLA: Broadcast authentication for distributed sensor networks," ACM Trans. Embed. Comput.Syst., vol. 3, no. 4, pp. 800–836, 2004.
[11] D. Liu, P. Ning, S. Zhu, and S. Jajodia, "Practical broadcast authentication in sensor networks," in Proc. MobiQuitous '05: Networking and Services. IEEE Computer Society, pp. 118–132.
[12] M. Luk, A. Perrig, and B. Whillock, "Seven cardinal properties of sensor network broadcast authentication," in Proc. SASN '06.ACM, pp. 147–156.
[13] I. Stojmenovi, Ed., Handbook of Sensor Networks – Algorithms and Architectures. WileyBlackwell, November 2005. [Online]. Available: http://books.google.co.uk

ISSN: 2278 – 1323

[14] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise-resilient message authentication in sensor networks," in Proc. IEEE INFOCOM '08. IEEE, 2008, pp. 1418–1426.
[15] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hop-by- hop authentication against false data injection attacks in sensor networks," ACM Trans. Sensor Networks, vol. 3, no. 3, p. 14, 2007.
[16] R. L. Rivest,A. Shamir, and L.Adleman, "AMethod forObtainingDigital Signatures and Public-key Cryptosystems", Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[17] T. Aura, "Cryptographically Generated Addresses (CGA)", IETF, RFC 3972, Mar. 2005.
[18] J.Arkko, T.Aura, J.Kempf,V.-M.Mäntylä, P.Nikander, andM.Roe, "Securing IPv6 Neighbor and Router Discovery", in Proceedings of the 1st ACMWorkshop onWireless Security, ser.WiSE '02, Atlanta, GA, USA: ACM, 2002, pp. 77–86.
[19] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", in Ad-vances in Cryptology, ser. Lecture Notes in Computer Science, G. R. Blakley and D. Chaum, Eds., vol. 196, Springer Berlin Heidelberg, 1985, pp. 47–53.
[20] D. Boneh andM. Franklin, "Identity-Based Encryption fromtheWeil Pairing", in Advances in Cryptology—CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed., vol. 2139, Springer Berlin Heidelberg, 2001, pp. 213–229.
[21] D. Boneh, B. Lynn, andH. Shacham, "Short Signatures fromtheWeil Pairing", Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.
[22] A. Fiat and A. Shamir. How to Prove Yourself: practical solutions of identification and signature problems. In A. M. Odlyzko, editor, Advances in Cryptology { Proceedings of CRYPTO '86, volume 263.
[23] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In G. Brassard, editor, Advances in Cryptology.
[24] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.
[25] D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.
[26] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Trans-action," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.
[27] D. Pointcheval and J. Stern, "Security Arguments for Digital Sig-natures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.
[28] W. Diffie and M. E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, IT{22(6):644{654, November 1976.
[29] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, 21(2):120{126, February 1978.
[30] M. R. Garey and D. S. Johnson. Computers and Intractability, A Guide to the Theory of NP-Completeness. Freeman, San Francisco, CA, 1979.
[31] S. Goldwasser, S. Micali, and R. Rivest. A \Paradoxical" Solution to the Signature Problem. In Proc. of the 25th FOCS, pages 441{448. IEEE, New York, 1984.
[32] S. Goldwasser, S. Micali, and R. Rivest. A Digital Signature Scheme Secure Against Adaptative Chosen-Message Attacks. SIAM Journal of Computing, 17(2):281{308, April 1988.
[33] M. Bellare and P. Rogaway. Random Oracles Are Practical: a Paradigm for Designing Efficient Protocols. In Proc. of the 1st CCCS, pages 62{73. ACM Press, New York, 1993.
[34] National Bureau of Standard U.S. Data Encryption Standard, 1977.
[35] T. El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, IT{31(4):469{472, July 1985.

ISSN: 2278 – 1323

Mr.L.Jeyakumar was born on December 14th 1985. I doing MPhil Part Time research scholar in Department of Computer Science in Erode Arts & Science College (Autonomous), Erode, Tamilnadu, India. I had obtained his Master degree in Computer Applications in Erode Arts & Science College (Autonomous), Erode, Tamilnadu, India.

Dr.C.Senthilkumar was born on January 10th 1963. He is working as Associate Professor, Department of Computer Science in Erode Arts & Science College (Autonomous), Erode, Tamilnadu, India He has obtained his Master degree in Computer Science and M.Phil degree In (Autonomous), Erode, Tamilnadu, India.He has obtained his Master degree in computer science and M.Phil degree in Computer Science from Alagappa University, Karaikudi. He is a research supervisor for M.Phil programmes.His interest area includes Image Processing, Data Mining and Neural Networks. He has presented 12 Papers in National and 12 International Level. He received his Ph.D., from Bharathiar University, Coimbatore.

ISSN: 2278 – 1323