A Survey: Efficient & Lightweight Hop-By-Hop Message Data Authentication and Preserving Source Privacy in Wireless Sensor Networks

Atul M. Patil
Department of Computer Engineering
A. C. Patil College of Engineering, Kharghar
Navi Mumbai, India
atulpatil470@gmail.com

Nitin P. Chawande
Department of Electronics & Telecommunication Engineering,
A. C. Patil College of Engineering, Kharghar
Navi Mumbai, India
npchawande@acpce.ac.in

ABSTRACT-A WSN is network which are consisting distributed independent device are connected to each other. In Wireless sensor network has main feature communicated to node and transferred message. In message transferring most effective ways to unauthorized and corrupted message using authentication. For authentication has used to symmetric key and asymmetric key cryptosystem. In large hop by hop network has transferred message to long route, between route ha multiple node are available. In route receiver node check sender information is valid or not. To large computation network has issue to minimum threshold message are transferred because unique key are not available for message authentication. To avoid theses problem we implement hop by hop message authentication system using ECC algorithm. In ECC has multiple key generation for authentication system. Our proposed system transfer unlimited message without suffering threshold problem. An each node of receiver can check sender is authorized or not. A hop-by-hop message authentication scheme based on the source anonymous message authentication (SAMA). Intermediate node can be authenticated unauthorized and corrupted message dropped to node. To getting scalability and resilience of compromised node does not getting threshold problem. When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification. We compared our proposed scheme with the bivariate polynomial-based scheme through simulations using java.

Keywords— ***Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, wireless sensor networks (WSNs), distributed algorithm, decentralized control***

I. INTRODUCTION

To save the energy of important network sensors it is necessary to reject or discard the unauthorized and corrupt data to be forwarded into the network. To do so many messages authentication methods are put forwarded for message authentication in wireless network sensors. Most of these proposed methods are categorized into two parts first is public key based approach and second is symmetric key based approach.

In symmetric key based approach, sender and receiver has to share a secrete key [1] [2] [3] [4]. This shared key is used by sender to generate a message authentication code for each and every generated message. This approach is not good as this approach involve complex key management, lack of scalability and not reliable for large network. In this method a message reliability and authenticity is only verified by the shred secrete key which is shared by a group on nodes. A burglar can get a key by capturing any single node in network.

To mitigate above mention problems many methods are introduced, one of such a method is secrete polynomial based message authentication method. This method is very similar to threshold secrete sharing method in which the threshold is determine by the degree of polynomial. Though if the count of messages to be sent is greater than the threshold the polynomial is fully recover and system is completely broken. To solve this problem a method is given in [3]. In this method to restrict the intruder from recovering polynomial, coefficient of polynomial is computed. Some noise is also added to this so that coefficient is not easily identified.

In public key based approach, every message is transmitted with a digital signature which is generated using sender's private key. Each intermediate node forwarded the message and last receiver authenticates the message by sending public key. The recent studies shoes that elliptic curve cryptography public key method is more reliable in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management [6].

To resolve the entire problem and to increase the scalability we introduce a method based on optimal modified ElGamal signature (MES) system on elliptic curves. This method is secure against adaptive chosen

message attacks in random oracle model. Our method allows all the intermediate nodes to authenticate all the messages so that the corrupted messages can drop from network and energy can be saved.

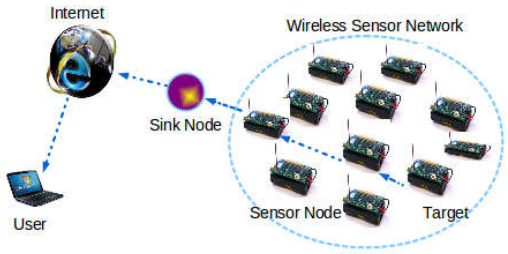

Figure 1.1: General Architecture of WSN [2]

II. RELATED WORK

WSN is newest technology growing rapidly throughout the world. It provides various useful services which have provided immense benefits to the various computer users as well as other clients. It refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location.

Fan Ye, Haiyun Luo and Songwu Lu in [1] introduce a novel approach called statistical en-route filtering i.e. SEF method to detect and reject the false data in network while forwarding the data into network. In large scale sensor network one of the node is being hacked or get interrupted by some hacker and introduce false data into the network which is than stored into final form as original data which may lead to wrong analysis of system or may generate false alarm. To eliminate such error this methods generates a key message authentication code and multiple MACs which are attached to event report. As the report passes node to node each node is verified through this repost and if MAC is not valid than that node is dropped. SEF starts the network scale to exclude false report by means of collective decision making with manifold sensing nodes and collective false detecting by manifold forwarding nodes.

Sencun Zhu, Sanjeev Setia et.al present a technique called interleaved hop-by-hop authentication method. In this method they guarantee that the base station node will detect any false introduction of data packets when certain number of nodes is compromised. They also show that this method rejects the false data injected into the network before they reach to the base node [2].

Wensheng Zhang and Nalin Subramanian et.al in [3] mention that there are number of methods introduce now a days to authenticate the message while transmitting it through multiple networks. But such a methods are having some drawbacks such as high computation rate, no flexibility, huge number of nodes get compromised while data transmission, poor scalability etc. to eliminate such problems they introduce a new technique based on perturbed polynomial to achieve the goal of lightweight, quick authentication etc. They used a polynomial based method for authentication rather than MACs based authentication technique. They also used immediate authentication method of this technique.

Adrian Perrig, J. D. Tygar, Ran Canetti and Dawn Song mention that multicast streaming authentication signing is very challenging problem. For such a problems to mitigate this they introduce two methods. First is the TESLA stand for Timed Efficient Stream Loss-tolerant Authentication. In this they used symmetric cryptographic primitives like pseudo random function and message authentication code ie MAC which is based on time release key by sender. The second is the EMSS stand for Efficient Multichained Stream Signature which is based on signing a number of special data packets in data stream which is associated to signed packet via multiple hash chains [4].

Taher Elgamal introduce a new approach called public key cryptosystem and a signature system based on implementation of Diffie-Hellman key distribution technique which is archive by public key cryptographic system. They proposed a new digital signature technique which depends on the difficulty of computing discrete logarithms over finite fields [5].

Haodong Wang, Bo Sheng et.al in [6] mention that symmetric key based method are time efficient but require complicated key management which may lead to requirement of large memory and communication overhead. On the other hand public key based method has clean key management but require more computational time. To eliminate this problem they introduce a method based on elliptic curved cryptography which involve pairwise key sharing among neighbor sensor, local access control and remote access control.

David Pointcheval and Jacques Stern in [7] introduce some problem related to security for signature based technique in random oracle model. They create this technique against adaptively chosen message attacks. This method shows the great improvement against the methods which uses committed values which are hashed together with message.

Michael K. Reiter and Aviel D. Rubin proposed a system to improve the security over World Wide Web named Crowed which is based on approach of “blending into a crowd" which means that hiding ones action into many others. According to this first a user has to join the crowd and then has to send a request to server. This request is not directly given to server it first forwarded to any random user and from that either it is forwarded or send to server. After forwarding then also it is forwarded to other random user or sends to server. By doing

this server will not identify the user from where this request is come [8].

David Pointcheval and Jacques Stern proposed a Arguments for Digital Signatures and Blind Signatures. In this paper they provide security of blind signatures which is very important thing for secrecy on offline electronic cash systems. For this they first introduce a so called "Random Oracle Model" and explain how it is providing validity to cryptographic technique. They also introduce the use of blind signature and its uses in anonymity in electronic cash technique [9].

Ronald L. Rivest1, Adi Shamir2, and Yael Tauman in this paper they validate the idea of ring signature method. They improve the idea of ring signature which creates the possibility to postulate a group of possible signers without enlightening which member generates the signature. Ring signature not having any setup procedure, it has no manager, any user can select any group of signers which includes him, and sign any message with the help of his secrete key and public key without permission and assistance of any other members. They also shows that ring signature gives an efficient way to produce authoritative secrete in a secrete way which allows only authorized recipient to receive the message [10].

Limitations

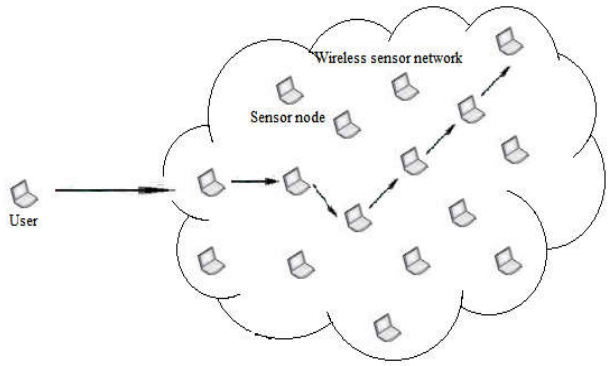

Figure 2.1: Limitations of WSN [10]

Wireless sensor network has combination of multiple networks which has connected to internet. In Internet has transmitted data to one network through another network. The network has connected to multiple node like sensor node which are transfer information to each other. In fig 1 has shown to wireless sensor network approach which has multiple node are available in network. If any user wants any information to network node then it has transfer request to network through internet. The internet has accepted request from protocol and transfer to related application level node, which node has read request and send related acknowledgement to sender. The continuously these process are working. To transfer information from sender to receiver which has some security issue are available.

A. High Computational

In network has multiple node are available, in network has used to MAN network then communication rate are large. Message are visited to multiple node to transfer means its not one to one communication. Every node has check message then possibility to hack data. To control process network are limited like in LAN. The hacker are disease message to add some data to message or change content of message. To provide secure message then try to send message in limited network.

B. Shortest Key Generation

To communication secure way is send information in encrypted format. To cryptography process used to symmetric key and asymmetric key encryption process. If network node are large or communication rate are high then increase to unique key for encryption. To generate new unique key are limited to cryptography algorithm, so we find a new algorithm which are generate high key. In existing system are worked to 8 bit to 128 bit keys combination are available. To large document or converted to secure authentication then used for large key generation. to using large keys are converted multiple data to cipher text format.

C. Shortest Path

To large network multiple node are available so if sender send information to destination then must important to find best ways to send information. If best shortest path not available then its delay to transmits information or chance to hack. Any communication system has worked on two parameter i.e. security and time. if you want less time then used for best ways for communication to each node. If node D has connected route are 10 node and 2 node. then obviously data are passing through 2 node ways because you have save time any authentication mode. In second ways has hacking chance are limited because only two node are available. In large network communication best ways for shortest path.

D. Ambiguity

Network data are sending to multiple nodes through sender to receiver. At a time multiple node are communication to each other. The node is sending each request to source to dependable destination. In existing process both node request are available for sender then its ambiguity problem for which request are provided or not. To remove problem we try to check each message to every node to original or not. If data are not original then destroy the data from network route.

III. PROPOSED SYSTEM

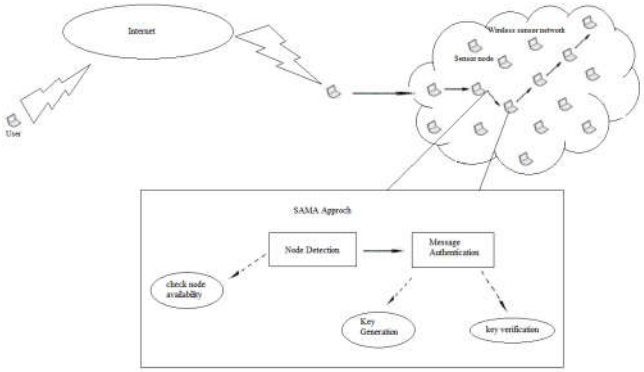

Figure 3.1: Proposed System Architecture.

The above fig. 1 shows our proposed system architecture which consist of a large network which includes number of machines called as node in which one is sender node and others are the receiver nodes. And message is send from sender node to destination node through these intermediate nodes. Each node in the network is enabled with our proposed SAMA approach which includes node detection by checking node availability, message authentication through unique key generation and key verification at each intermediate node of network.

In this project we have proposed a unique, secure and efficient way to transfer message from source to destination called Secure Anonymous Message Authentication system i.e. SAMA based on MES Elliptical curve system. The main approach of this method is that an each message m is to be sending into the network, the message sender or sending node creates a unique and secure message authentication code for message m. The generation of this unique, secure anonymous authentication code is done by MES technique based on elliptical cure method. The whole SAMA process is depends on three steps which connect all non-sending nodes and sending node to SAMA identical.

For the compromised node detection by our proposed system as SAMA gives message integrity untendered, whenever a bad or unauthorized message is received by the hacked node than that node is considered as compromised node. If the hacked node send one message at a time than it is very difficult to identify the compromised node. If it sends mode than one message than the destination node can narrow the hacked node to very small set. When the compromised node generates two messages, the destination node will be able to narrow the source node down to the set with both vertical lines and horizontal lines. When the compromised source node transmits three messages, the source node will be further narrowed down the area. Therefore, if the destination node keeps tracking the compromised message, there is a high possibility that the hacked node can be remove from network.

A. Node Detection

To large network multiple sensor node are available for transmission data to source node to destination node. To transfer data both node must connected to network. If any node are not connected then we can communication to network node. To check node availability module for check Boolean result for true or false. In SAMA approach are working for every node. To check node and send message from network. If any network are large or high computational then compromise node to send data. In compromise remove extra node in route which are available in network. Its support for only route node which are help for communication in network.

B. Message Authentication

Authentication is converted message into unreadable format. To converted plain text into cipher text using cryptography method. Cipher text message are specific unreadable or opposite to plain text data, these data are converted using symmetric key or asymmetric key cryptography system. In existing system has used to Advance encryption standard, DES,RSA algorithm are used. But these techniques limited to key generation. In hop by hop network message authentication to every node for detect corrupt message. If any message are corrupted then destroy to system in current approach.

C. Key generation

Key generations are techniques which are help for message authentication. In system 8, 16, 32, 64, 128 bit key are available for cryptosystem algorithm. To daily hop by hop communication required for unique key are available for encrypted data. Cryptosystem are required same key for encrypted and decrypted file, if keys are different then cannot generate plain text data from cipher text data. To generate multiple unique key to proposed algorithm we have implemented ECC algorithm. Which are implemented multiple unique for cryptosystem?

IV. CONCLUSION

For above survey on various papers we observe that the some systems work on threshold level or some on related to this concept which having a drawback of system crash and complete recovery of polynomial if any one node in multiple node network is get compromised. Some systems developed on the basis of symmetric key which suffers from poor reliability, complex key generation which is hard to maintain. To overcome problem we implement a new and efficient way for hop by hop communication based on ECC. To provide hop by hop message authentication to overcome the problem of

threshold level, we also proposed a hop by hop message authentication based on SAMA. For the WSN we give the technique to identify the compromised node in network.

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-ByHop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[3] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

[4] 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.

[5] 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.

[6] 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.

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

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

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

[10] R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Advances in Cryptology (ASIACRYPT), 2001.

[11] "Cryptographic Key Length Recommendation," http://www. keylength.com/en/3/, 2013.