INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# A REVIEW ON AUTHENTICATION OF MESSAGE THROUGH HOP BY HOP WITH SOURCE PRIVACY IN WIRELESS SENSOR NETWORKS USING OPTIMAL TECHNIQUE

**MS. A. R. KUKADE, PROF. N. M. DHANDE**

Department of Computer Science & Engg, Agnihotri College of Engineering, Wardha, India.

**Accepted Date: 15/03/2016; Published Date: 01/05/2016**

**Abstract:** Authentication of Message in Wireless Sensor Networks (WSNs) is one of the most effective ways to thwart unauthorized and corrupted messages. For this purpose, there are number of different scheme for message authentication based on cryptography which includes either symmetric-key cryptosystems or public-key cryptosystems. Most of them, have the limitations for high computational and communication overhead with the lack of scalability and resilience to node compromise attacks. There are number of solutions for this problem. Here is one scheme which gives one better way. In this paper, we propose a scheme for message authentication which is based on Elliptic Curve Cryptography (ECC). Our scheme can provide message source privacy with authentication for intermediate nodes. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based approach in terms of computational and communication overhead under comparable security levels while providing message source privacy.

**Keywords:** Message authentication, source privacy, wireless sensor networks (WSNs)

**Corresponding Author: MS. A. R. KUKADE**

**Access Online On:**

www.ijpret.com

**How to Cite This Article:**

A. R. Kukade, IJPRET, 2016; Volume 4 (9): 1-7

***PAPER-QR CODE***

## INTRODUCTION

INTERNET- become one of most important thing in these modern days. Almost there is nothing now which is happened without this word. So because of this Internet, today almost all have a brief knowledge about the networking and its structure. As Network is nothing but the collection of things, but here Computer Network is the collection of autonomous computer which are interconnected. And in the Computer Network communication is between Sender & Receiver by sharing Message between them. For that communication, through the Messages it surely needs Authentication for security reasons. Message authentication is one of the most effective ways to protect against unauthorized and corrupted messages from being forwarded in the Network For this reason, there are number of Message Authentication schemes have been developed, based on either symmetric key cryptosystems or public-key cryptosystems. Here is one technique which is better than the previous techniques that is, a scalable authentication scheme based on Elliptic Curve Cryptography (ECC). This enables intermediate hops for authentication, which allows transmission without unauthorized message. Now, **What is Wireless Sensor Network?.** This question might be struggle you. So, Wireless Sensor Network that is WSN are also called as Wireless Sensor Actor Network (WSAN). These are autonomous sensors which are used to monitor conditions like environmental or physical such as temperature, pressure, sound, etc. And pass these respective data to the main location through the network. There are number of applications of this WSN. Some of them are as follows.

### 1. Area Monitoring-

In area monitoring, the WSN is established over a area or region where some phenomenon is to be examined or monitored. The best example is that for Military purpose. Here by using the sensors, it can detect enemy & their movements etc.

### 2. Environmental Sensing-

In this application, the WSN sense the conditions and report it to the respective area to get precautions against the bad environment which causes large amount of lose in terms of money, lives etc.

### 3. Health Care Monitoring-

WSN can be useful in medical terms too. WSN can provide the information about an individual’s health, fitness & energy expenditure. So, these are some of the applications for WSN and similarly there are many more number of useful applications in many fields.

## LITERATURE REVIEW

The following session gives an idea different systems existing in the relevant area.

D. Pointchval & J. Stern, "Security Proofs for Signature Schemes". This paper - exclusively focus on signatures & its security. Here Signature is one of the technique in Cryptography to provide more security between sender & receiver in the network. The sender uses a Signing Algorithm to sign the message. This message & the signature are sent to that receiver. The receiver receives the message & the signature and applies the Verification Algorithm to the combination. If the result is True then the message is Accepted otherwise, it is Rejected. A digital signature needs a public-key system. The signer signs with her private key then verifier verifies the signer's public key. This process is called Digital Signature process [1].

F. Ye, H. Lou, S. Lu & L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks". This paper- shows the hop by hop authentication scheme that guarantees that base station will detect the false data packets. That means if corrupted data packets are to be found then that packet will recognized and then able to discard or reject. The given technique will work on this method to provide more security to the message which is sent between sender and receiver in the wireless network. Also this paper provides the scheme for authentication to the intermediate hops in the wireless network as the complications in the wireless network are more difficult to manage or to operate that is, there are more complexity in the Wireless network. So to give more scalability and security to the network, this paper gives a way which is more efficient to work on wireless communication [2].

S. Zhu, S. Setia, S. Jajodia & P. Ning, "An Interleaves Hop-By-Hop Authentication Scheme for Filtering False Data in sensor Networks" - provides the technique which gives the Filtration to the network. This filter provides the wanted and uncorrupted data or data packets. It will filter the unwanted and corrupted data which is transmitted in the wireless network and which is responsible for the energy and time wastage. It will recognized the route between the sender and the receiver.

And then it will detect that type data that is unwanted by its technique which is used and then filter it[3].

H. Wang, S. Shemg, C. Tan & Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks- describes the comparison between the Symmetric key & public key cryptography. The cryptography is the process in the network to provide the security between sender & receiver. This cryptography includes Encryption and Decryption of the message which is transmitted in the network. This technique is mostly based on Symmetric Key & Public Key cryptography. Symmetric Key is based on the Similar Keys method which are present at both the sender and the receiver. Whereas the Public Key is based on the Different Keys mechanism that is Public Key & Private Key. Both are different and are occupied by either sender or receiver. As compare to the symmetric-key mechanism, this public-key method is more secure as this method uses different keys for cryptosystem and it is very difficult to attack by any type of network attacker to corrupt data or information in the network. And it is more stable and reliable to the different attacks occurred on the network specially in Wireless Network. Whereas in symmetric-key system, it only uses same keys at the both side of sender and the receiver. The network. Thus, as a result the Public-Key method is more secure and stable as compared to the Symmetric-Key method [4].

## PROPOSED SYSTEM

Proposed system will work out in following ways to overcome all the drawbacks of previous methods:

- We propose an unconditionally secure and efficient SAMA that is Secure Anonymous Message Authentication. 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.
- This is based on Elliptic curves cryptography for more security purpose, high scalability against attacks with very less memory usage as compare to previous work.
- This scheme enables the intermediate hops to authenticate the message so that all corrupted message can be detected and dropped.
- In our scheme, the entire SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA alike. In addition, our design enables the

SAMA to be verified through a single equation without individually verifying the signatures.

- This approach is mainly based on Elliptic Curve Cryptography which is extreme secure than previous methods like Symmtric-Key and Public-Key systems. Also it allows high security in small memory with more reliability & stability against to network attacks.

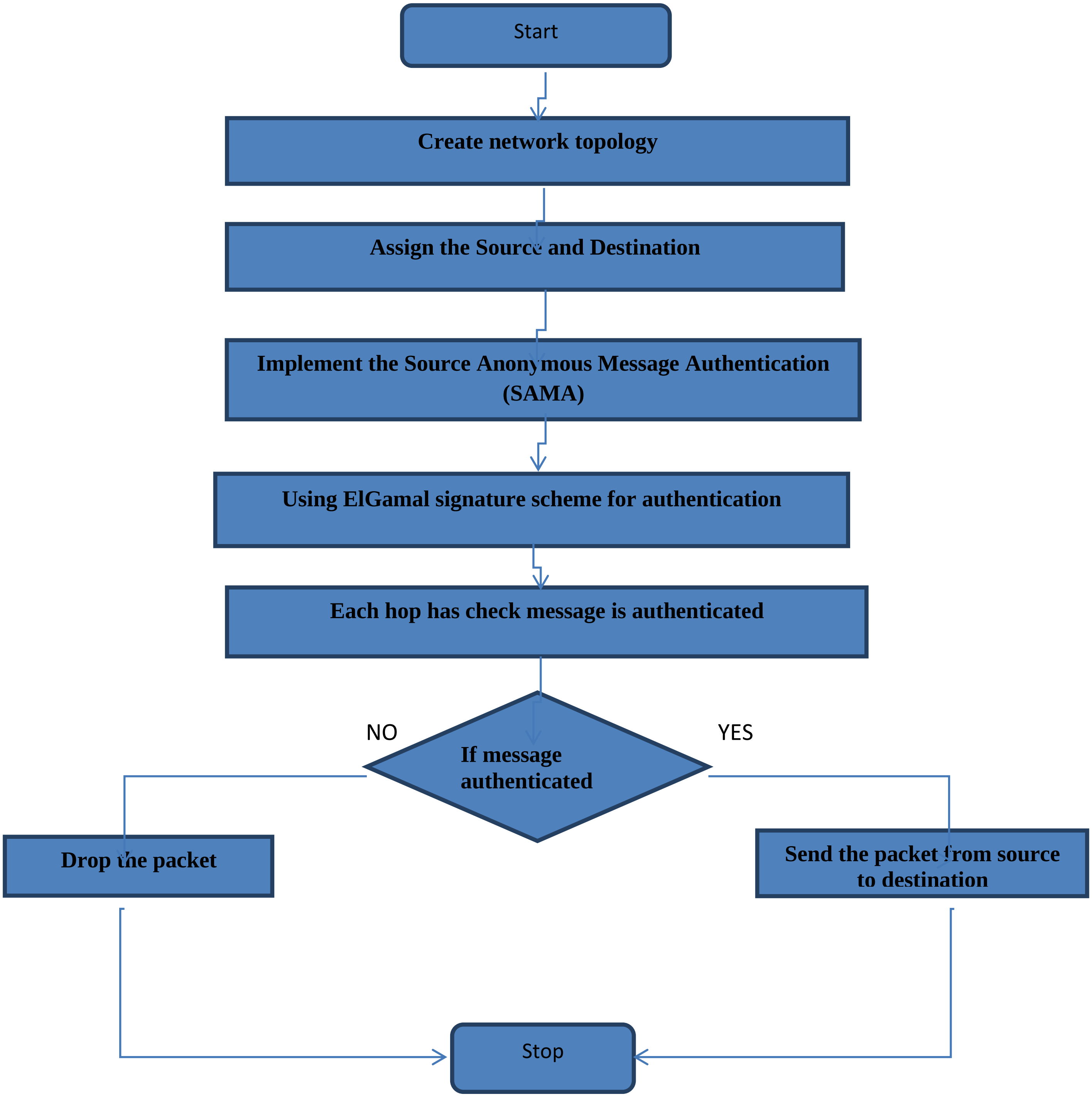
## SYSTEM ARCHITECTURE

This system architecture gives the brief idea about the given proposed system with the following diagram for architecture**.** This paper states that in the wireless communication every intermediate nodes give an authentication for the corrupted or unauthorized packet so, whenever found they can able to discard that one to save energy of each node.

Here the following figure shows that, first it will start then, it will create the topology- topology is the graphical representation of the network or it is the physical layout of the network. Next it will assign the respected source and its destination for the data transmission or communication. Then next, the actual working of this paper will begin that is, it will implement the algorithm to create SAMA- Source Anonymous Message Authenticator which the authenticate each data packets.

After that then again EIGamal signature scheme will get implemented to verify the sent message or the data packet to save the energy of each intermediate node between source and its respective destination.

Then once authentication is done, it will found that there is any corrupted data packet is present or not. If YES then that time it will discard, otherwise it will forwarded to the next hop to complete the communication.


Start
Create network topology
Assign the Source and Destination
Implement the Source Anonymous Message Authentication (SAMA)
Using ElGamal signature scheme for authentication
Each hop has check message is authenticated
NO
If message authenticated
YES
Drop the packet
Send the packet from source to destination
Stop

@IJMTER-2015, Reserved 321 Send them to

Fig: System Architecture

## ADVANTAGES OF PROPOSED SYSTEM

1. A novel and efficient SAMA based on ECC. While ensuring message sender privacy, SAMA can be applied to any message to provide message content authenticity.

2. To provide hop-by-hop message authentication without the weakness of the built- in threshold of the polynomial-based scheme, we then proposed a hop-by-hop message authentication scheme based on the SAMA.

3. When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification.

## REFERENCES

1. D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology EUROCRYPT), pp. 387-398, 2000.
2. 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.
3. 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.
4. 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.
5. D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.
6. D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J Cryptology, vol. 1, no. 1, pp. 65-75, 1988.
7. A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Managementa Proposal for Terminology," http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.