ISSN: 2366-1313

VERIFICATION AND PROTECTION: ENSURING MESSAGE INTEGRITY AND SOURCE CONFIDENTIALITY IN WIRELESS SENSOR NETWORKS

#1**Dr.Y. VENKATESHWARLU,** ***Professor,***

Department of Computer Science and Engineering,

#2**KONTHAM SRIDHAR,** ***Associate Professor,***

Department of Computer Science and Engineering

MOTHER THERESA COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TS.

ABSTRACT: Message authentication is a great way to ensure that wireless sensor networks (WSN) do not send unwanted or incorrect data. As a result, a plethora of message authentication mechanisms utilizing both private and public key encryption have emerged. Despite this, the bulk of these systems have significant processing and connection latency, making resource-intensive operations challenging. To obtain access to nodes, simple hacking techniques can also be utilized. A innovative polynomial-based technique was used to solve these problems. The adversary will be able to reconstruct the complete polynomial if more messages are sent than the limit. This study explains how to use elliptic curve cryptography (ECC) to improve authentication security and flexibility. The suggested solution intends to make authentication for intermediary nodes easier. The problem of message termination is overcome by using this mechanism, and each node can now send a limitless number of messages. Furthermore, our solution secures the sender's privacy during communication. The strategy used in this investigation took less computational time and mental work than the polynomial-based method. The information in the message is designed to protect the sender's privacy.

***Keywords*—**Wireless Sensor Networks(WSN),Elliptic curve cryptography(ECC)Source Anonymous MessageAuthentication(SAMA)

1. INTRODUCTION

Message authentication is required to ensure that messages sent via networks have not been tampered with or sent illegally. As a result, several identification methods have been developed to simplify the verification of the validity of data supplied by wireless sensor networks (WSNs). The systems are classified into two types: public key systems and symmetric key systems. Because both the sender and the recipient must have the same secret key, a symmetric-key system is difficult to manage. In addition to scalability difficulties, these technologies can be used to undermine the security of the nodes that use them in a variety of ways. Using the shared key, the sender creates a message authentication code (MAC) for each message delivered. Nonetheless, only the node that has the secret key can verify the transmission. A set of sensor nodes normally shares the confidential key. One hacked sensor location is enough to open all doors. The utilization of several networks exacerbates the performance problem with this technology. To solve the issue of scalability, a cryptographic approach that uses polynomials to verify the authenticity of secret messages was devised. The degree of the polynomial effects the system's threshold determination. This results in a mechanism similar to a threshold secret sharing method. A mechanism exists to ensure that a shared secret key remains private as long as the number of messages exchanged remains below a particular threshold. The intermediary nodes utilize polynomial evaluation to validate the message's authenticity. When the total number of messages transmitted exceeds the limit, the polynomial can be recalculated, resulting in lasting system damage. A new process was devised to make it more difficult for the intruder to identify the polynomial coefficients. This method attempts to make determining the values of an equation more difficult by introducing a random disturbance, often known as random noise. Modern research, on the other hand, has shown that error-correcting code approaches can remove all polynomial noise. Using the public-key technique, each message is digitally signed with the sender's private key. The sender's public key can be used to authenticate the message at any point during the transfer procedure. The idea has a number of flaws, one of which is that it may place an excessive amount of work on computers. New elliptic curve cryptography (ECC) discoveries show that public key approaches are more secure, need less memory, and are more successful at preventing data decryption from outsiders. Because it is efficient and simple to use, the management of encrypted keys in public-key systems is unique. The anonymous message authentication (SAMA) mechanism we used in our research is exceptionally safe and reliable. This system makes use of the best modified El Gamal signature (MES) technique, which was specifically created for elliptic curves. Adaptive chosen-message attacks on the Message Encryption Scheme (MES) are judged insignificant in the random oracle hypothesis. The proposed strategy, which attempts to increase the performance of sensor resources, is based on giving intermediate nodes the ability to validate communications. You may quickly discover and eliminate unneeded contacts using this method. It is recommended that you use a method that maintains source anonymity, is extremely difficult to penetrate, and allows you to choose when to validate the data. In simulations and theoretical evaluations, our suggested system outperformed polynomial-based algorithms that give the same level of security.

2. PROBLEM DEFINITION

The cloud can quickly re-sign blocks, saving users time. This saves time for users. Because the gadget can save the secret key for each user, this is possible. Given that many people have little faith in the cloud, storing confidential keys there would be exceedingly hazardous. If a user's access is revoked, other users should be able to verify the accuracy of the data without having to download the complete set. It is challenging to develop a solution that meets the demands of the impacted users while also preventing them from downloading all of the data from the cloud and allowing a third party to verify the accuracy of the shared data.

3. SYSTEM ANALYSIS

The existing approach for exchanging a secret key between a message's sender and recipient has concerns with key management, handling high volumes of messages, and being subject to various hacking tactics. The responder constructs the message using the shared key. Using the public-key technique, each message is digitally signed with the sender's private key. It is feasible to validate the message at each stage of transit using the sender's public key. The method's dependency on a large number of computer resources is a big disadvantage. It was easier to confirm the authenticity of covert communications using polynomial-based approaches. The degree of the polynomial effects the system's threshold determination. This results in a mechanism similar to a threshold secret sharing method. The intermediary nodes utilize polynomial evaluation to validate the message's authenticity. The polynomial function can be used once the total number of messages exceeds the limit.

The second illustration. Despite the fact that the dataflow map has restored to normal, the system is still unworkable due to its current state. This technique has various drawbacks, including restricted scalability, vulnerability to node compromise attacks, high processing requirements, and a threshold issue.

4.SYSTEM DESIGN

The data flow structure is depicted in Figure 2, while the system configuration and operation are depicted in Figure 1. It is possible to use this technology to quickly and securely verify the validity of messages whose origin is unknown. The modified ElGamal signature (MES) approach is used to make it compatible with elliptic curves. Based on this data, we can conclude that adaptive chosen-message attacks are ineffective against the Message Encryption Scheme (MES) used in this case under the random oracle paradigm. The proposed strategy, which attempts to increase the performance of sensor resources, is based on giving intermediate nodes the ability to validate communications. This strategy enables you to quickly discover and eliminate undesirable contacts. We use an approach that eliminates threshold difficulties while preserving source privacy, tamper resistance, and the capacity to adapt to changing conditions. This method has various advantages, including the capacity to address the threshold problem, safeguard the identity of the source, allow for variable time identification, and give a strong protection against deceit.

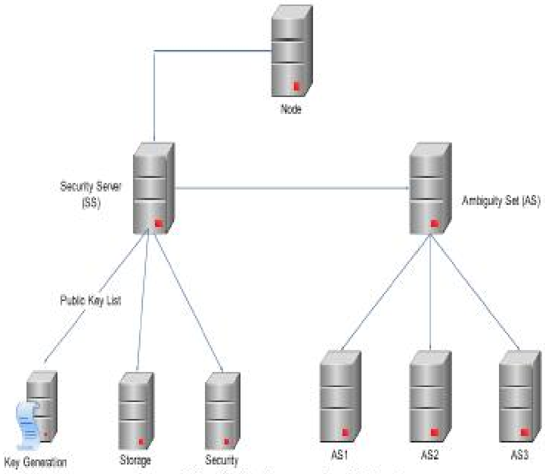


Fig .1. Software Archietecture

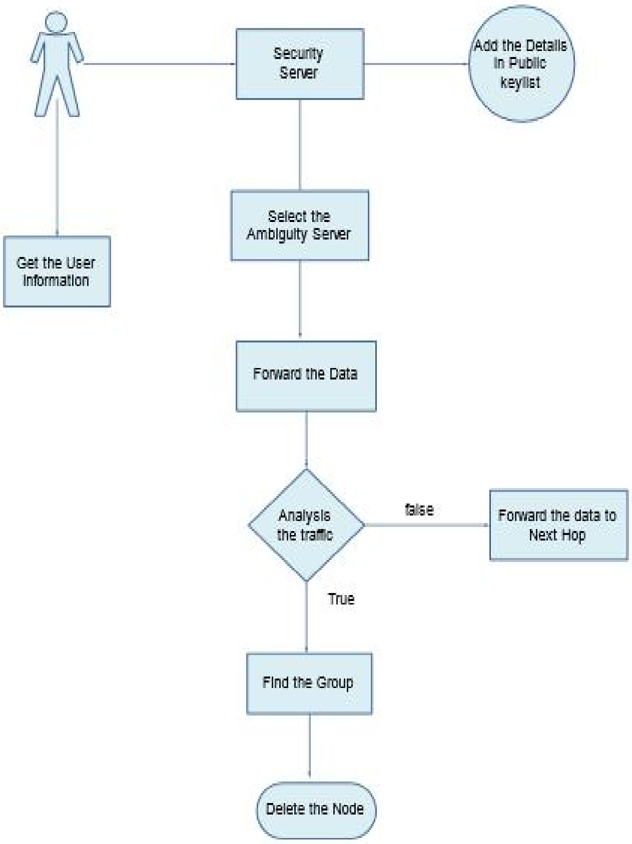


Fig. 2. Dataflow diagram

5. PROPOSED MODEL

This system's components are listed below: How the network is set up. On a security server, this inquiry discusses how to send encrypted packets and verify contact authenticity. A detailed examination of how to discover hacked network endpoints.

Node Creation

Figure 3 demonstrates the steps involved in creating a node. The user's links and node IDs are used to build the node. The IP address and port number of each node are also determined. The user signals that this node can be used as the destination for outbound connections.

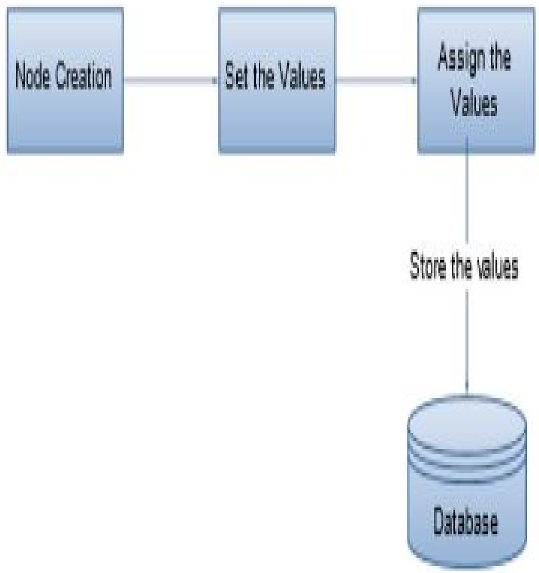


Fig .3. The steps required to construct a node.

Security Server Process

The inner workings of the security server are depicted in Figure 4. There is agreement that each sensor node knows its precise location and can link directly to other nodes in the vicinity using geographic routing protocols. Messages delivered over a network must travel through several nodes before arriving at their destination. Most people assume that the SS is in charge of developing, enforcing, and disseminating network-wide security regulations. Because of its great level of durability, this computer is incredibly difficult to destroy or harm.

Fig .1. The high-level planning and organizing of software systems is known as software design. It entails making an informed framework selection.

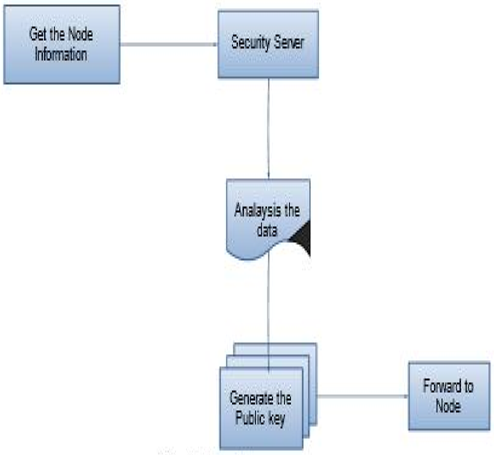
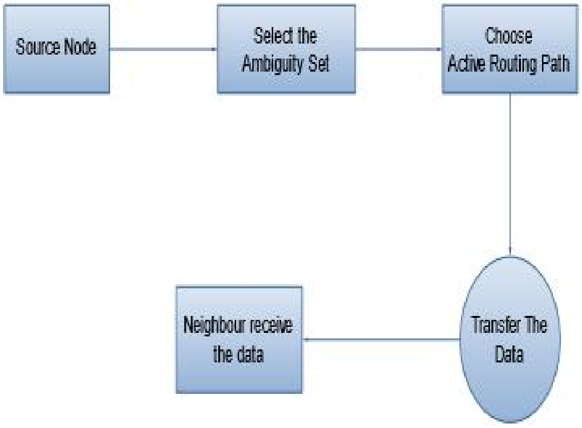


Fig .4. Security server process

Secure Packet Forwarding

Figure 5 shows how critical it is for each relay along the path to validate messages as soon as they arrive.



Compromised Node Detection

Figure 7 shows an example of identifying a susceptible node. When a hacked node is found, the system supervisor (SS) can remove its public key from the public key catalog. The node's abbreviated identifier can also be sent to other nodes in the sensor network. Sensor nodes that use an existing public key to select an Autonomous System (AS) can now get updated keys. It is best to stop talking with the authentication server (AS) that supports the compromised node as soon as its public key is made public or deleted from the list of public keys.

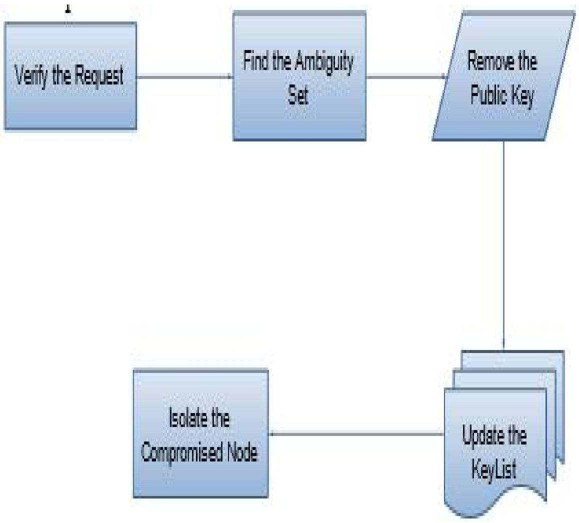


Fig. 7. The stability of the system has been jeopardized. The nodes' identification

6. CONCLUSION

The discussed technology is SAMA (Source Anonymous Message Authentication). The identity of the sender is hidden using elliptic curve encryption. SAMA can be used to validate a message before it is delivered. We then show how SAMA can be used in a hop-by-hop message security scheme. By using a hop-by-hop message validation mechanism, the problems associated with the polynomial-based method can be avoided. Using fixed sink nodes, this study investigates further ways for locating hacked nodes in Wireless Sensor Networks (WSN).

REFERENCES

1. 1.F. Ye, H. Lou, S. Lu, and L. Zhang, Statistical en-route filtering of injected false data in sensor networks, in IEEE INFOCOM, March 2004.
2. S. Zhu, S. Setia, S. Jajodia, and P. Ning, An interleaved hop-by- hop authentication scheme for filtering false data in sensor networks, in IEEESymposium on Security and Privacy, 2004.
3. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and
4. M. Yung, Perfectly-secure key distribution for dynamic conferences, in Advances in Cryptology - Crypto'92, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.
5. W. Zhang, N. Subramanian, and G. Wang, Lightweight and compromiseresilient message authentication in sensor networks, in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.
6. A. Perrig, R. Canetti, J. Tygar, and D. Song, Efficient authentication and signing of multicast streams over lossy channels, in IEEE Symposium on Security and Privacy, May 2000.
7. M. Albrecht, C. Gentry, S. Halevi, and J. Katz, Attacking cryptographic schemes based on perturbation polynomials, Cryptology ePrint Archive, Report 2009/098, 2009,