USER VALIDATION AND SECURE DATA COMMUNICATION USING ELLIPTICAL CURVE ENCRYPTION THROUGH MULTIPLE HOPS IN THE WIRELESS SENSOR NETWORK

Pooja Gupta[1], Shashi Bhushan[2], Parminder Singh[3]

[1]Research Scholar, Dept of Information Technology, Chandigarh Engineering College, Landran,India
[2]Professor, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, India
[3]Professor, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, India

Abstract*- Wireless sensor networks are the networks which are deployed in any environment where any other network is hard to implement. As the word signifies these networks are free- wired and organised by the collaboration of small and cost effective nodes. These nodes are made up of sensing, computation units and battery source. These networks can be placed in harsh environments; hence, security is the prime concern for such networks. In this paper, security is achieved by using private and public key encryption procedure. Public key will be created at server end whereas private key at the user end. Authentication of sender and receiver node is also accomplished for secure transmission of information through multiple hops in the specified wireless sensor environment. Also, many important factors are analysed for improvisation in the work.*

Keywords- **Wireless sensor networks, Encryption, Security, Authentication, Data Transmission, Cryptography, Multiple Hops.**

1. INTRODUCTION

Wireless sensor networks are the systems which comprise of sensor units which are disseminated in the critical situations. These sensors are used to gather information from their surroundings and then scrutinize the parameters. As a final point the sensor nodes gather the information and pass it to the main station where calculations are done for judgment and decision making. The main benefit of these wireless sensor network [4] is that they can be applied and systematized in irregular and hostile environments. The nodes in the wireless sensor networks are usually very small in mass and self-governing in nature, which makes the wireless sensor networks more appropriate to organize. These nodes have the ability to configure themselves on their own by connecting to their nearby nodes, in this way they form a network where the data is transferred through multiple hops i.e. from one node to another [11]. These networks are budget effective but reserved to some parameters like energy consumption, battery lifetime, computation overhead, throughput [3] etc.

As these networks are deployed in open atmosphere, hence, security can be another important factor to be considered. The pictorial representation of the wireless sensor network is given in figure1.Wireless sensor networks are used for military purposes in the starting but now they are used in various and uneven locations where it is hard to reach. Here we can observe that nodes are dispersed in the area and they all are interconnected with each other and the data is streamed to the main station which is also called base station.

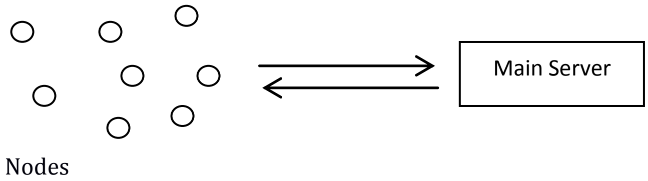

Figure 1. Wireless sensor network

In figure 1, we can observe that wireless sensor network is organized of nodes dispersed in the environment. It generally consists of self-configured nodes which are encompassed of sensing unit, computational unit, and transceiver unit with battery source. These nodes are connected to the main station which analyses the accumulated information by these nodes. These networks are alike to ad-hoc networks, but some differences are as:

- In wireless sensor network, the nodes must sense the surroundings because on the basis of this information decisions can be made.
- Data handling is necessary in the wireless sensor networks.
- As they are deployed in hostile environments hence damage and failure probability can be high.
- These networks are restricted by energy constraints [9].
- They are more prone to several attacks.

1.1 FEATURES OF WIRELESS SENSOR NETWORKS

Despite of the diverse uses, sensor networks posture a number of exceptional technical features due to the following reasons:

- *Ad-hoc arrangement*: Most sensor nodes are deployed in regions which have no prescribed structure at all. A distinctive way of arrangement in a forest would be stirring the sensor nodes from an airplane. In such a condition, it is up to the nodes to detect its connectivity and circulation.
- *Self-adjustable procedure:* In most cases, once deployed, sensor networks have no humanoid involvement. Hence the nodes themselves are accountable for re-configuration in case of any fluctuations.
- *Unmetered*: The sensor nodes are not allied to any energy foundation. There is only a predetermined sources a thought-provoking fact is that communication dictates handling in energy consumption. Thus, in order to make optimum usage of energy and communication should be underrated as much as probable.
- *Energetic changes:* It is obligatory that a sensor network system be adjustable to changing connectivity as well as altering ecological provocations. Thus, contrasting customary networks, where the emphasis is on increasing channel output or diminishing node arrangement, the main concern in a sensor network is to outspread the system lifespan as well as the system sturdiness.

1.2. GAINS OF WIRELESS SENSOR NETWORKS

Wireless sensor networks are the demanding networks now days, because they are feasible to implement and do not need complex configuration mechanisms. While using wireless sensor networks [5], we can have many advantages. Some of them are listed below:

- The implementation of wireless sensor network is not complex to organize and manage.
- We can easily accomplish network arrangements without stable structure and pre-defined setting.
- The implementation budget is economical.
- Wireless sensor networks are perfect for the non-reachable spaces such as crossways the marine, elevations, pastoral areas or dense timberlands.

2. RELATED WORK

Wireless sensor networks are on an urge these days as they are very much practicable to implement. Saru Kumari, Muhammad Khurram Khan and Mohammed Atiquzzaman recommend the potential work in the field of security in the wireless sensor network. They show the impediment of different safety features, as wireless sensor networks are deployed in harsh environments where attacks are very much common and hard to handle. They also discuss the functional features that are to be reflected while executing an epitome user certification arrangement for wireless sensor networks. They projected work on various attacks like session attack, parallel session attack, pass by attack, replay attack etc. in the wireless sensor network.

They enlighten the security and authentication factors for the wireless sensor networks [7]. Energy is another constraint for performance output analyzation of these networks. Parth M Dave and Purvang D Dalal illustrate the work on energy efficiency constraint in the wireless sensor network. Routing protocols have a acute part in most of these events because energy is used in deciding the path and transmission of data from one node to another. Global addressing system is not available in the wireless sensor networks therefore routing is another thought-provoking assignment for such networks. More factors include the distance between source and destination covering multiple hops and because of data redundancy, the routing decision is challenging factor [4]. Throughput of network also depends on such parameters.

Yang yu and Viktor K. Prasanna also depicts the work on energy efficiency of the network. They work on energy efficient [11] agenda for package communication over a multi hop transmission pathway by means of modulation scaling. Their objective is to reduce the leading energy dissipation over entire nodes in the network. They compute the deviation in information packet proportions and latency constriction while transmitting of data through the network. They demonstrate the potential work but there is a point i.e. disputation avoidance in the network and performance trade off, which can be explored further [11]. Gopikrishnan and P. Priakanth anticipated the Hybrid Secure Data Aggregation which accelerates security in specific environment and the process is energy competent also. Additional essential factor in the wireless sensor network is the node certification and sanction because these networks are more susceptible to numerous attacks. They recommended the approach that carry out the private key generation and encryption at the end node, in this way the trustworthiness and confidentiality of the data is retained in the network [6]. Arivanantham Thangavelu and Abha Pathak deals with the complications in the wireless sensor networks that are restricted energy, delay in the network etc. They proposed a number of clustering methods [8] which can be used to depreciate the communication overhead in the network as well as it also raises the network lifespan. Security is also taken into consideration while working on other constraints [2].

3. IMPLEMENTATION PROCEDURE FOR PROPOSED WORK

In this work we implemented algorithm for node deployment, unit authentication and secure data transmission. Data is encrypted to achieve protected transmission through multiple hops in the network. Elliptical curve algorithm is used to encrypt the data. This encryption algorithm is very fast and efficient as compared to other encryption algorithms. The flowcharts for node deployment, unit authentication and secure data transmission are given below with their explanations to have clear view for the proposed work.The implementation procedure is depicted for node authentication in the wireless sensor network which should be done with concentration as if the node deployment is not done securely then there is a chance of entrance of black node in the network which may cause harm to network and also allow different attacks in the network.

User authentication is also another important factor for security of the network because user should be genuine and validated so that no extra malicious data can be transmitted in the network which in return affect the performance of the network.Approach is the logical, methodical and speculative exploration of the methods applied in the projected work. It gives the clear idea of the steps taken to compute and perform the tasks in the proposed work. The steps taken in the methodology are:

- Secure deployment of node in the network.
- Authentication process for user by registering it.
- Data selection by source to transmit it to the destination node.
- Secure data transmission from source to destination through multiple hops.
- Analyze various parameters for improved work.

With these steps we will achieve the authenticated node deployment and secure data transmission in the wireless sensor networks and accumulate the results to analyse various parameters for enhancing performance of proposed work.

In the proposed work we implemented the node deployment process. In this when any node wants to join the network it will send its preloaded key to the key server for validation of the node. The preloaded key is transferred in the form of message digest which is generated with the help of MD5. Then the key server receives the message digest and deciphers it to original form, then check the information in its database. If the credentials match the database credentials then the node is allowed to join the network. Then if the node is allowed, a certificate is issued by the key server to node and finally the authentication of node is completed. The certificate issued by the server is the proof that the node is authenticated and validated as the credentials of the node is matched with the data provided in the database. This guarantees that the joined node is not black node and cannot harm the specified network while transmitting the data through multiple hops in the sensor network. It also ensures the integrity of the data because during transmission no alteration by black node is done. The secure node deployment is very important factor for network reliability and better performance. The node can be authenticated using the above technique in the wireless sensor network.

In this way, we restrict the entry of any black node in the network. And also the network is composed of only authenticated nodes.

Authentication process is done in order to authorize the unit to transmit the data through the network. The unit need to create account for this process. After successful account creation the unit will receive one key which is used for its authorization process. When the unit will login in the system, its credentials will encrypt with above key and send it to key server for validation. And then the key server will decrypt the credentials and check it in database. If the credentials match the information in the server's database, then the unit is validated and allowed to login in the network. If they are not matched, then the login is unsuccessful and the unit cannot send the data through the network. This is how unit authentication is achieved in the wireless sensor networks. Unit or user authentication is very concerning factor while arranging the network as well as transmitting the data. Because if the user is not authenticated it may cause many attacks in the network like packet flooding attack, which may degrade the performance of the sensor network and make it untrustworthy to implement. With this we may get unexpected outputs. The network should be trustworthy and consistent and to achieve this security is taken into concern while assembling wireless sensor networks.

After successful login, the unit will transmit the data to destination through multiple hops in the wireless sensor network. In this the unit selects the data and then the key server will send public key and the formula to generate private key to the unit and receiver. The private key will compute first and then pass the generated key to encrypt the data and sends it to the destination. If the key at the receiver end matches the above created key then the encrypted data is deciphered else it is discarded. Then the receiver will decrypt the data and allowed to download the data. The data which is to be transmitted in the network through multiple hops can be encrypted and decrypted using the above mentioned process. In this way a secure transmission of data is achieved in the specified wireless sensor network. Reliability and integrity of the data is maintained through the authentication process used in the proposed work.

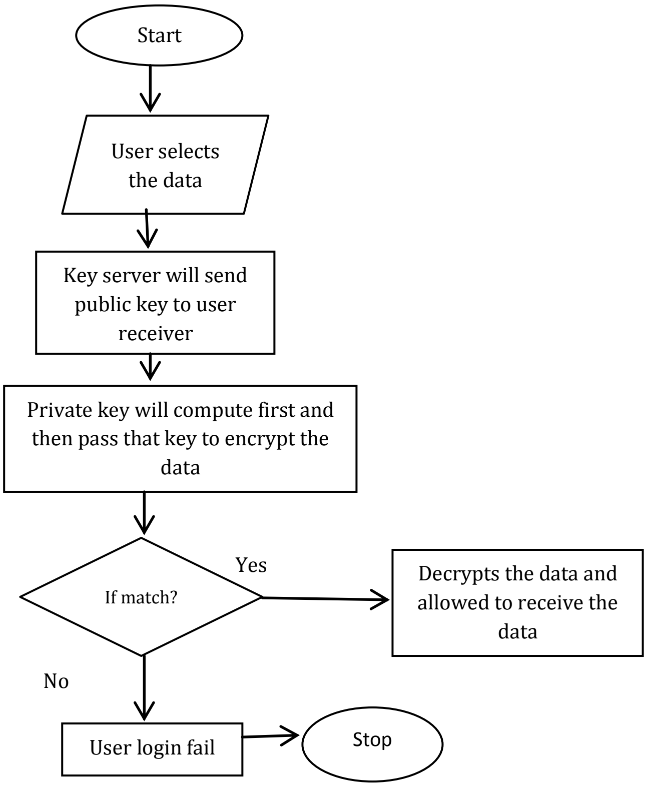
Start
User selects the data
Key server will send public key to user receiver
Private key will compute first and then pass that key to encrypt the data
If match?
Yes
Decrypts the data and allowed to receive the data
No
User login fail
Stop

Figure 2. Flowchart for data encryption and decryptionprocess.

Figure 2 shows the flowchart for the process of data encryption and decryption process. With the help of these steps we can understand the process of data encryption at the sender end and the decryption at the receiver end.

4. RESULTS

In this section results are analysed for the performance of the proposed technique for the specified network.

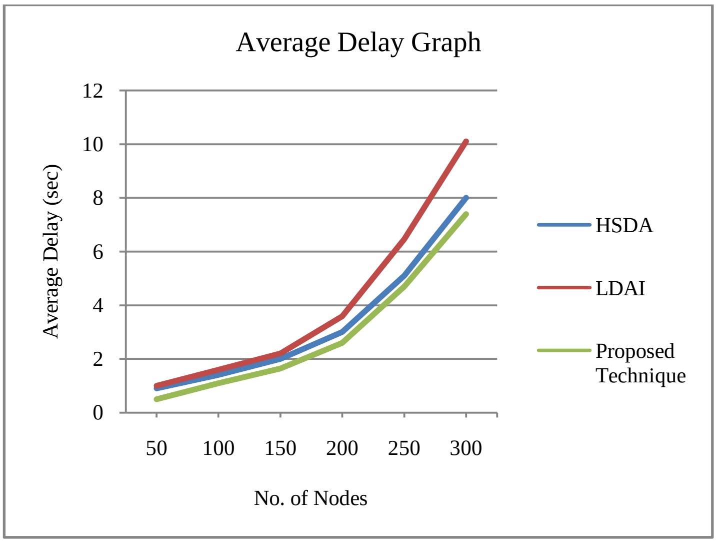

Figure 3. Graph between Average Delay vs. Number of Nodes

Figure 3 shows the line comparison graph between average delay and number of nodes. We compared proposed technique with existing work. Delay should be less for output performance of the network. It also shows the reliability of the network while transmitting the data through nodes in the network.

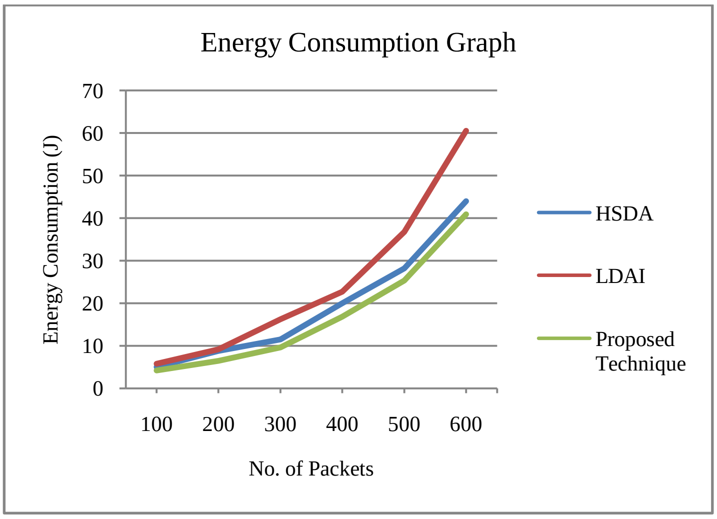

Figure 4. Graph between Energy Consumption vs. Number of Packets

Figure 4 shows the line comparison graph between energy consumption and number of nodes. We compared our technique with the existing models to show the enactment of the network. The energy consumption by the network must be low because as wireless sensor networks are strictly bound to energy constraints hence this parameter should be small as possible. Communication overhead and computation overhead are also computed in terms of energy consumption. The results and discussions for computation and communication overhead is given below. For wireless sensor network it should be less for long lifetime of the network.

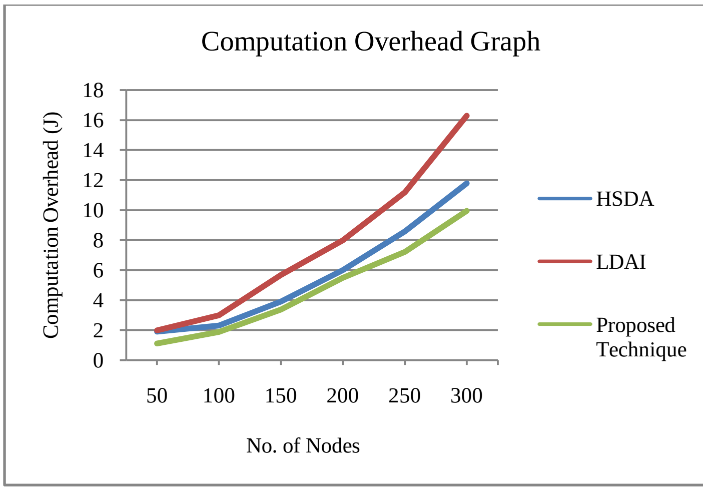

Figure 5. Graph between Computation Overhead vs. Number of Nodes

Figure 5 shows the line comparison graph between computation overhead and number of nodes. The energy consumption in transmission of data includes the computational overhead in terms of energy while encrypting and decrypting data. Hence, the computational overhead should be less for better performance. The graph shows that the proposed technique evaluates less computation overhead as compared to existing models.

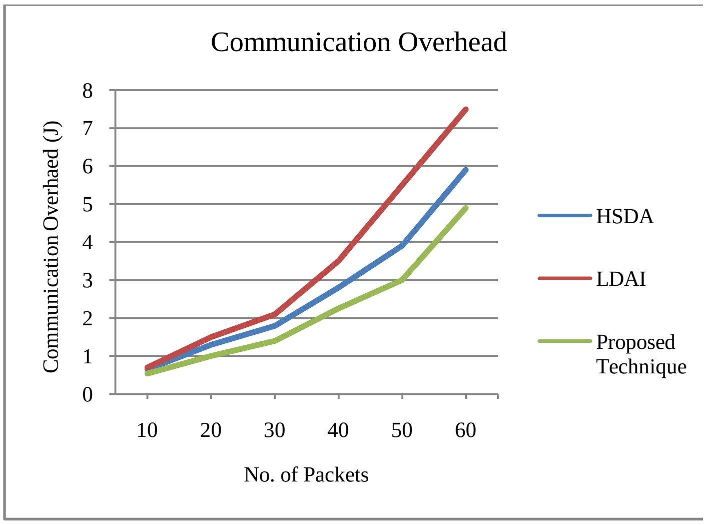

Figure 6. Graph between Communication Overhead vs. Number of Packets.

Figure 6 shows the line comparison graph between communication overhead and number of nodes. Communication overhead is measured in terms of energy which computes the collision problems in the network. As we basically concentrate on the security of the network therefore it does not disturb the communication competence of the network. The graph shows that the communication overhead of the proposed technique computes less communication overhead compared to other models.

5. CONCLUSION

Wireless sensor networks are more prone to several attacks like entrance of black node to affect the reliability of the network. Therefore, to maintain the security of the network, authenticated node deployment is done which ensures that any black node cannot enter in the network. Log table is also maintained at the server which keeps the record of each node arranged in the network. The main concern is on the security of the network so that the reliability and integrity is maintained. Only authenticated unit is allowed to send data to another unit, if the unit is not authenticated then the data is not forwarded. The evaluation of parameters like less key generation time, end to end delay [1], average delay, energy consumption, cipher text size, encryption time and increased throughput [3] of network is achieved to show improved results. In this way we can accomplish secure data transmission through multiple hops in the particular environment and authenticated node deployment in the specified environment.

6. REFERENCES

[1] Akanksha Dubey and Anand Rajavat, "Analyze the Performance difference between Delay Sensitive and Delay Insensitive Routing Algorithms in Underwater Sensor Networks", International Journal of Computer Applications, Vol. 130, pp. 10-15 2015.

[2] Arivanantham Thangavelu and Abha Pathak, "Clustering Techniques to Analyze Communication Overhead in Wireless Sensor Network", International Journal of Computational Engineering Research, Vol 4,pp 75-78,2014.

[3] Husna Jabeen, Suresh Chimkode, Anil Kulkarni, "Operative Data revelation protocol to enable multihop sensing on demand for wireless sensor network", International Journal of Engineering and Technical Research",Vol. 3,pp. 103-107, 2015.

[4] Parth M Dave and Purvang D Dalal, "Simulation & Performance Evaluation of Routing Protocols in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, pp 1405- 1412, 2013.

[5] Rudranath Mitra, Tauseef Khan, "Secure and Reliable Data Transmission in Wireless Sensor Network: A

Survey", International Journal of Computational Engineering Research, Vol. 2, pp. 748-754, May- June 2012.

[6] S.Gopikrishnan, P. Priakanth, "HSDA: hybrid communication for secure data aggregation in wireless sensor network", Springer Science, Business Media New York, Vol. 22, pp. 1061-1078, 2015.

[7] Saru Kumari, Muhammad Khurram Khan and Mohammed Atiquzzaman, "User Authentication Schemes for Wireless Sensor Networks: A Review", Ad Hoc Networks,Vol. 27, pp. 159-194 , 2015.

[8] Shiv Prasad Kori and Dr. R. K. Baghel, "Performance Comparison in Terms of Communication Overhead for Wireless Sensor Network Based on Clustering Technique", International Journal of Electronics Communication and Computer Engineering, Vol. 4, pp 743- 746, 2014.

[9] Shweta Bhatele and Lalita Bargadiya, "Evaluation of Communication Overhead and Energy Consumption in Wireless Sensor Network using Different Clustering Techniques", International Journal of Software and Hardware Research Engineering, Vol. 2, pp 81- 87, 2014.

[10] Srikanta Kumar Sahoo and Manmanth Narayan Sahoo,"An Elliptic-Curve-Based Hierarchical Cluster Key Management in Wireless Sensor Network", Advances in Intelligent Systems and Computing Springer,Vol. 243,pp. 397-408, 2014.

[11] Yang Yu and Viktor K. Prasanna, "Energy-Efficient Multi Hop Packet Transmission using Modulation Scaling in Wireless Sensor Networks", Global Telecommunications Conference, IEEE Vol. 1, 2003.

AUTHOR'S BIOGRAPHIES

Pooja Gupta, pursuing Masters in Information Technology at Chandigarh Engineering College, Landran, Mohali. She has done Bachelors in Information Technology from Seth Jai Prakash Mukand Lal Institute of Engineering and Technology, Radaur, Yamunanagar.

Dr. Shashi Bhushan, Professor, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali.

Dr. Parminder Singh,Professor, Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali.