International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I3P222

Volume 69 Issue 3, 138-146, March 2021
© 2021 Seventh Sense Research Group®

An Efficient Data Aggregation Technique for Green Communication in WSN

D. Anita Daniel[1], S. Emalda Roslin[2]
[1]*Research Scholar,* [2]*Professor*
Faculty of Electronics, Sathyabama Institute of Science and Technology, Chennai, India.
[1]d.anitaedwin@yahoo.com, [2]roemi_mich@yahoo.co.in

Abstract - *Wireless Sensor Networks (WSNs) progressively participate in many applications. Green communication is the actual application of selecting the energy-efficient method for exchanging the information, networking technologies, and services, minimizing resources used whenever possible in all communications present in WSN. The major issues in WSN are the communication overhead and energy efficiency of each individual sensor node. It should be made to ensure that the valid data is being shared to avoid any remarkable degradation in system function because of faulty or inexact information. It will create confidentiality, a more secured network in which all devices are recognized and no data drawn from an unknown device. To have a protected WSN that is able to withstand malicious trust attacks, contribute an efficient data aggregation technique (EDAT) to enhance the packet delivery ratio in the network while reducing the time to segregate any malicious behavior focusing the trust in the entire network. The detailed evaluation acquired from the theoretical interpretation and the experimental simulations exhibit that the technique can bring down the communication overhead, energy consumption of the network and protect the information from reaching a compromise when compared with the existing schemes.*

Keywords - *Base Station, Cluster Head, Data Aggregation, Security, Wireless Sensor Networks.*

I. INTRODUCTION

In recent times the application of WSN for environmental monitoring based on green communication has constantly increased [1]. Normally collected data about the conditions and the evolution of the green environment can help to discover and warn hazardous events and to assess and process the natural resources in order to maintain an ecological balance. e.g., climate change, environmental sensing, and habitat loss, etc. [2]. The environmental monitoring application is often challenging because the quality of radio communication between sensor nodes (SNs) can be changeable, especially during atmospheric happenings such as heavy rain, snow, fog, etc., and due to the gradual gathering of dirt on SNs [3]. Temperature variations may break before the due time of the SNs, which increases the operating cost for the maintenance of SNs in open nature [4]. Transmission protocol scalability and field deployment may be expanded for the applications that require more SNs for pervasive monitoring. WSN implementation typically relies on existing hardware and software components to maintain a broad range of applications [5]. However, applications with precise requirements, such as low cost, a huge number of SNs, fast field deployment, and reduced maintenance, can provide custom design and implementation of the entire WSN platform [6]. Secured communication may outline as confidence that something is authentic that will not destruct the regular services of real-time applications. To address privacy-related concerns, though many authentic communication methods are extensively used in WSN, the elaborate evaluation of performance has not been done [7]. Hence, we have been prompt to resolve the security issue, which includes features, challenges, and security requirements in the WSN environment [8]. This needs privacy-preserving data aggregation protocols to safeguard the data from mutual concessions. Hence it necessitates the development of an efficient data transmission technique algorithm with high security and its hardware implementation in WSN.

This paper is structured as follows. Section 2 spotlight some of the issues related to security, challenges, and requirements in WSN. Section 3 focuses on the related works. Section 4 explains the system model of the proposed work in WSN. Section 5 exhibits the simulation results and hardware implementation. Section 6 concludes the paper by emphasizing the future scope of our work.

II. WSN Security Issues

A. *Features in WSN*

Location Awareness: Based on the location, the data collections had been made. Hence, every individual SN in the network should be aware of their place where they have positioned with neighbor SN by knowing their actual location [9].
Reliability: In WSN, effective transmission of data through the nodes will take place by giving a request to a proper node. That request, efficiently processed by the proper node and will give the reply on time [10].
Fault tolerance: In WSN, the failure of any one of the SNs will not affect the operation of the entire network since the other adjacent SNs collecting similar data, and only it reduces the accuracy of the collected data [11].

B. Challenges in WSN

Challenges in WSN arise while implementing it in some specific applications like a nuclear power plant and militant area [12]. There are so many factors that have to consider for the implementation of WSN, such as

Energy conservation: In WSN, each SN is equipped with sensors, and the working condition of the SN mainly depends mainly on the power supplied by the connected battery [13]. In order to have improved performance, the network should operate for a longer period, but the battery capacity and the available energy is not as much, and also fills again, or replacement of the battery is not possible in some applications [14]. To overcome this issue, a more energy-efficient protocol is to be designed so that the SN operates efficiently by improving both throughput and network lifespan.

Security: A node compromised attack is the most common attack that can be launched against a Sensor node. In WSN, security is a critical issue because the communication channel is public so that any device can access the exchanged information [15].

Communication quality: The quality of Sensor network communication depends upon the surroundings where it is operated. In the troublesome scenario, the quality of communication will be very low.

Availability: In WSN, the required resources are not available, it is hard to give the desired QoS [16].

Data Aggregation (DA): Aggregating data through more numbers of SNs may carry unwanted data, and DA desired in the processing of data so that irrelevant data will not be transmitted more number of times and in turn, it will reduce the energy usage for transmission[17].

Scalability: WSN consists of a large number of SNs, and in the design stage, more number of nodes can be added.

Node failure handling: WSN should have the capacity to handle node failures [18].

C. Security Requirements

The major security requirements are listed below.

Data confidentiality: The secrecy of the sensed data cannot be revealed to the unauthorized SN by means of confidentiality of the transmitted data. This means that the data transmitted by each SN is readable only by those nodes to which that data is addressed. Confidentiality can be achieved through cryptographic methods, which can be classified mainly into two categories: Symmetric-key cryptography and Public-key cryptography [19], [20].

Authenticity: SNs use a shared wireless medium to communicate so that the mechanisms for authenticity are needed to detect maliciously injected or spoofed packets in order to ensure that the transmitted data is actually provided by the expected SN. The lack of authenticated communication between the SNs could lead to several attacks, namely node impersonation, denial of service, Sybil attack, and so on [21].

Data Integrity: This ensures that the trustworthiness of a content of a transmitted message has not been changed, either maliciously or accidentally. Data integrity can be achieved by a mechanism called a MAC (Message Authentication Code) to provide both authentication and integrity [22],[23].

Data freshness: In order to protect WSN against replay attacks, the sensed value with the same information content should consider in a distinct way every time when they are transmitted so that the attacker cannot utilize the confidentiality, the authenticity, or the integrity of transmitted information [24].

III. Related Works

Ajay et al. [25] developed a clustering mechanism, namely as PODC mechanism. It mainly depends on two activities such as cluster formation and steady-state activity. In the cluster formation scheme, five tasks are assigned with time durations in TDMA timeslots, such as data gathering task T1, Cluster head (CH) competition task T2, SN redundancy check and activation task T3, and cluster formation task T4. Consumption of Energy in SN can be minimized by keeping the SN in sleep mode, which is not taking part in transmission, and thus the other SNs can have time slots and get preferences. The result of the proposed PODC depicts the improved lifetime in the network and energy depletion among SNs when compared with SA-EADC and EADC.

Farah Kandah et al. [26] proposed a CH Trust Propagation mechanism, and it consists of four main phases such as CH voting, cluster trust propagation, DA, and network trust propagation. This method is minimizing trust erasing network attacks and trust pollution network attacks present in the network by maintaining energy efficiency. CH Trust Propagation method accomplishes malicious node isolation in a short term duration than the existing trust managers scheme.

Gulzar et al. [27] proposed a research work to increase the reliability in remote patient monitoring. In order to create trust values, a design has developed, and then, depending on the trust estimated value, a system named CCS with a cryptographic-based solution is developed. This method tries to boost the accurate reliability assistance to healthcare users. Additionally, the planned CCS scheme boosts the trust level and accuracy with the least energy consumption, and the mean communication delay is also minimized. A fuzzy logic-based ranking system is finally used to indicate that the proposed scheme exceeds the possible strategies.

Syed Gul Shah et al. [28] developed a method to reduce the number of communications between the CH and BS. This method introduces a node called supernode, which is responsible for the selection of CH, communications, and all activities inside the network. Finally, this method's simulation result is compared with the existing methods LEACH and C-LEACH, and it gives less energy consumption and delay.

IV. Proposed Model and Contributions

In this section, an overview of WSN and the problem identified for the proposed work, along with the proposed model, is given.

A. Overview

In WSN, different secure DA protocols support different aggregation functions such as MINIMUM, MAXIMUM, and AVERAGE, etc. The security preserving capacities also vary, and the adversaries can release different types of attacks. In the tree-based aggregation approach, there are two types of nodes, leaf nodes (SN) and intermediate nodes (CH). SN only measure physical environmental information such as temperature, radiation level, light, etc., while intermediate nodes not only measure physical environmental information but also gathering their cluster node's data. The physical length between two SNs in the network is about 10m, and SNs can only exchange information with their child nodes or parent nodes. Each SN has a unique ID to protect from some specific attacks. CH nodes can accomplish encryption for security purposes. BS has unconstrained energy and computing capacity, and it is in charge of collecting physical information from the nodes and forwarding control data from the users. Therefore BS can distribute query messages to the complete network making use of the authenticated method. In this paper, more secured communication between CH and the BS is proposed. Figure 1 shows the architecture of WSN. This architecture shows the Cluster formation, and Cluster head election using Q-LEACH protocol and DA takes place in the CH and also shows the communication between the CH and BS.

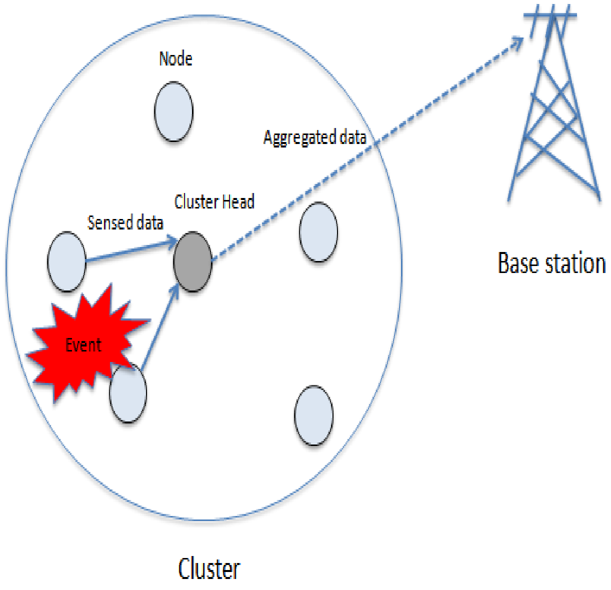


Figure 1. The architecture of Wireless Sensor Networks.

B. Problem Identification

The major task of an SN is to transmit the sensed or aggregated observations to different kinds of nodes. But there are some more tasks owing to security requirements preventing it from malicious attacks, as they are passed in a wireless transmission will undergo security attacks, such as eavesdropping and jamming, and they require mainly a low computational process and focusing on the scarce energy resource savings effectively for the existence of the entire network. The most threatening attack against DA in WSN is node compromising, which is released by the attacker. An attacker node can obtain the keys of the SNs and send fake messages to disturb the outcome of aggregation. Such attacks can make BS receive the false aggregation outcome without being noticed. Hence it necessitates a scheme to be developed based on the properties introduced in Section 2.

C. Proposed Model

In the proposed Efficient Data Aggregation Technique (EDAT) algorithm, the overall network is divided into subgroups called Clusters, and each Cluster has CH based on their energy in the node, and the election of CH is done by using Q-LEACH protocol. For more secured communication between CH and BS, it uses MAC-based symmetric key encryption. Finally, a prototype of a WSN is developed based on the EDAT algorithm for the implementation of CH and BS.

Pseudocode for the proposed EDAT algorithm

```
Input: {$E_1$,…., $E_N$}
For each round r
  Set $E_{avg}$ = average the total remaining energy in the network;
  For each cluster C in {1,2,….,C}
    If $E_{CH}$ ‹ $A_{vg}$
      Select the random node in cluster C with energy › $A_{vg}$ ;
    End if
  End for
  For each SN N in {1,2,…….,N}
    SN sense-data of event E;
    Set transmission schedule for each SN;
  End for
  For each cluster C in {1,2,…,C}
    DA done in each CH generates message m;
    BS shares public key $Q_B$ with each CH;
    Generate ($k_{ENC}$, $k_{MAC}$);
    Encrypt Ct=ENC(m, $k_{ENC}$);
    Generate tag=HMAC(Ct, $k_{MAC}$);
    CH sends Ct with a tag to BS;
  End for
End for
```

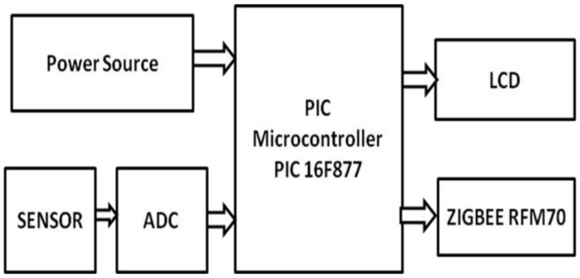


Figure 2. Block diagram of CH

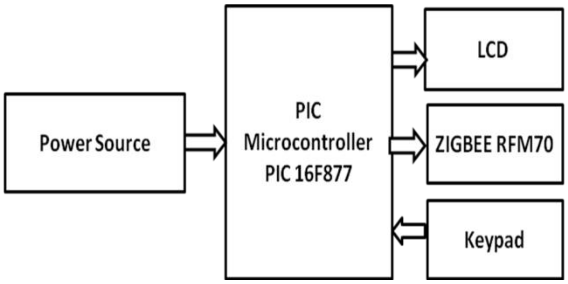


Figure 3. Block diagram of BS

Figure 2 and Figure 3 show the block diagram for the operation in CH and BS. Hardware used for the implementation of the Sensor nodes is PIC Microcontroller 16F877, ZIGBEE, LCD, Arduino, Bridge rectifier, Crystal oscillator, and Silicon controlled rectifier. Software used for the implementation of the Sensor nodes is CCS Compiler, Embedded C, and Proteus version 8.0 pro. Figure 4 and Figure 5 show the flow diagram for the transmitter and receiver section.

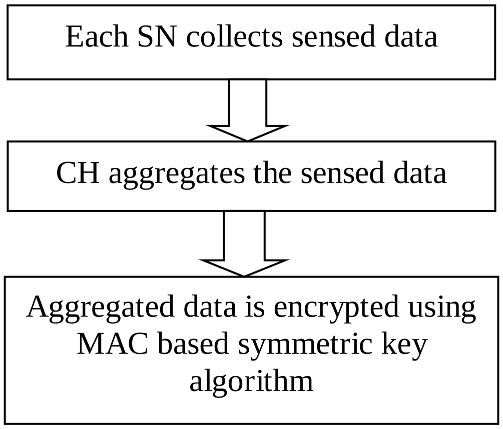

Each SN collects sensed data
CH aggregates the sensed data
Aggregated data is encrypted using MAC based symmetric key algorithm

Figure 4. Flow diagram for Transmitter section in CH

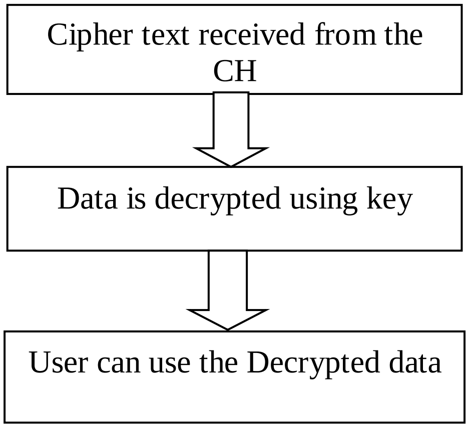

Cipher text received from the CH
Data is decrypted using key
User can use the Decrypted data

Figure 5. Flow diagram for Receiver section in BS

V. Simulation results and hardware implementation

Impact on the number of active SNs and the distance between the inter-nodes will have a vital effect on the output in WSN. Since SNs are randomly placed in real-time simulation, it is necessary to generate randomness as most of the systems are random in nature. The packet lengths, inter-event times, distance between two SNs, and the delays could be the random quantities in a network. Performance evaluations based on several estimating standards will estimate the proposed Efficient Data Aggregation Technique (EDAT) design compared with the existing algorithm CH Trust Propagation scheme (CHTPS) and Prediction Oriented Distributed Clustering SN Distribution (PODCND) method. The metrics used are the energy consumption and packet delivery ratio (PDR). Network Simulator 2 (NS2) tool implemented in Ubuntu operating system is used to implement the work, where the SNs of 200 numbers are deployed randomly over an area of 1000×1000 square meters. Simulations carried over with 50, 100, 150, and 200 SNs. The initial energy of EDAT is taken as 10.1 J, and in the proposed EDAT, the communication range has been chosen between 2-10m. For the planned setup, the IEEE 802.11x MAC protocol technical standard is utilized, and data forwarding is based on a star topology, as shown in Figure 1. All sensors in EDAT are considered as a group of clusters, and the simulation time for the proposed EDAT scheme is 50 seconds. Table 1 Simulation Parameters reveal the parameters that are used for efficient communication in EDAT.

Table 1: Simulation of EDAT parameters

Densities	50,100,150 , 200
Area	1000 X 1000 sq. m
MAC Protocol	802.11
Execution time	25 sec
Propagation Model	Two Ray Ground Model
Type of Antenna	Omni Directional Antenna
Initial Energy	10.1J
Transmission Power	0.3W
Receiving Power	0.3W
Data packet size	5000 bits
Control packet size	500 bits
Sleep power	15 μW

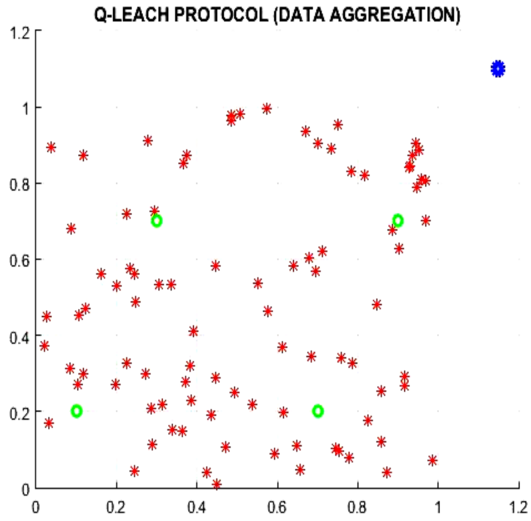


Figure 6. Data Aggregation in Q-LEACH protocol

Figure 6 shows the simulation result for DA in Q-LEACH. Figure 7 shows data packets are sent in each round from SN to BS, dead node increases when data packets are sent, and the sum of residual energy will decrease in each round with respect to data packets sent for the proposed EDAT model.

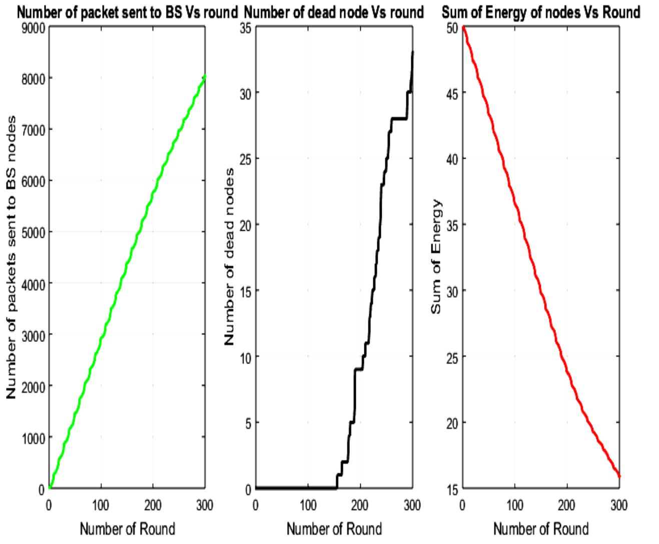


Figure7. Number of Packets sent, Number of Dead nodes, and Sum of Energy of nodes measured w.r.t. the varying node number of rounds for the proposed model

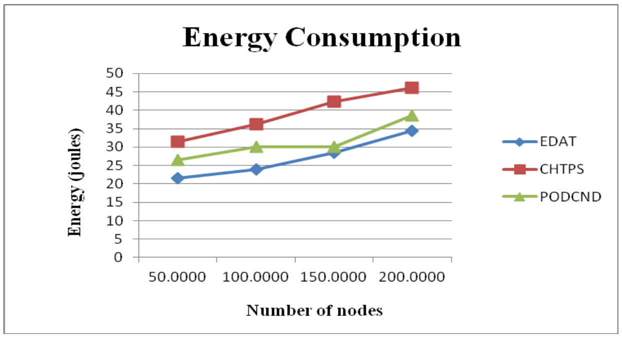


Figure 8. Residual energy vs. No. of nodes

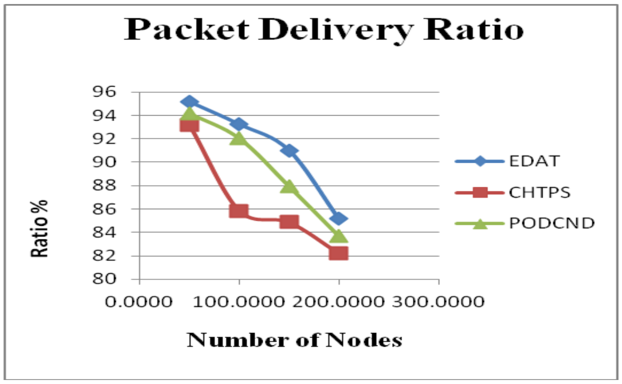


Figure 9. PDR vs. No. of nodes

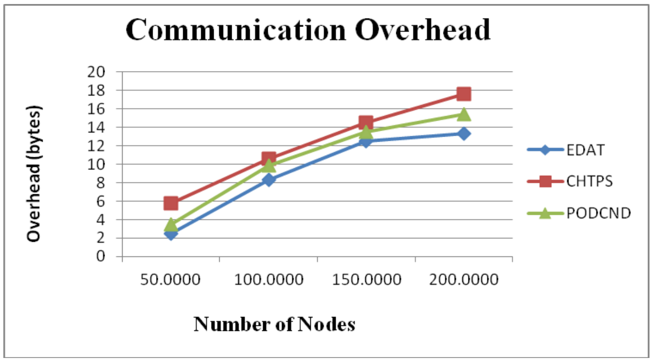
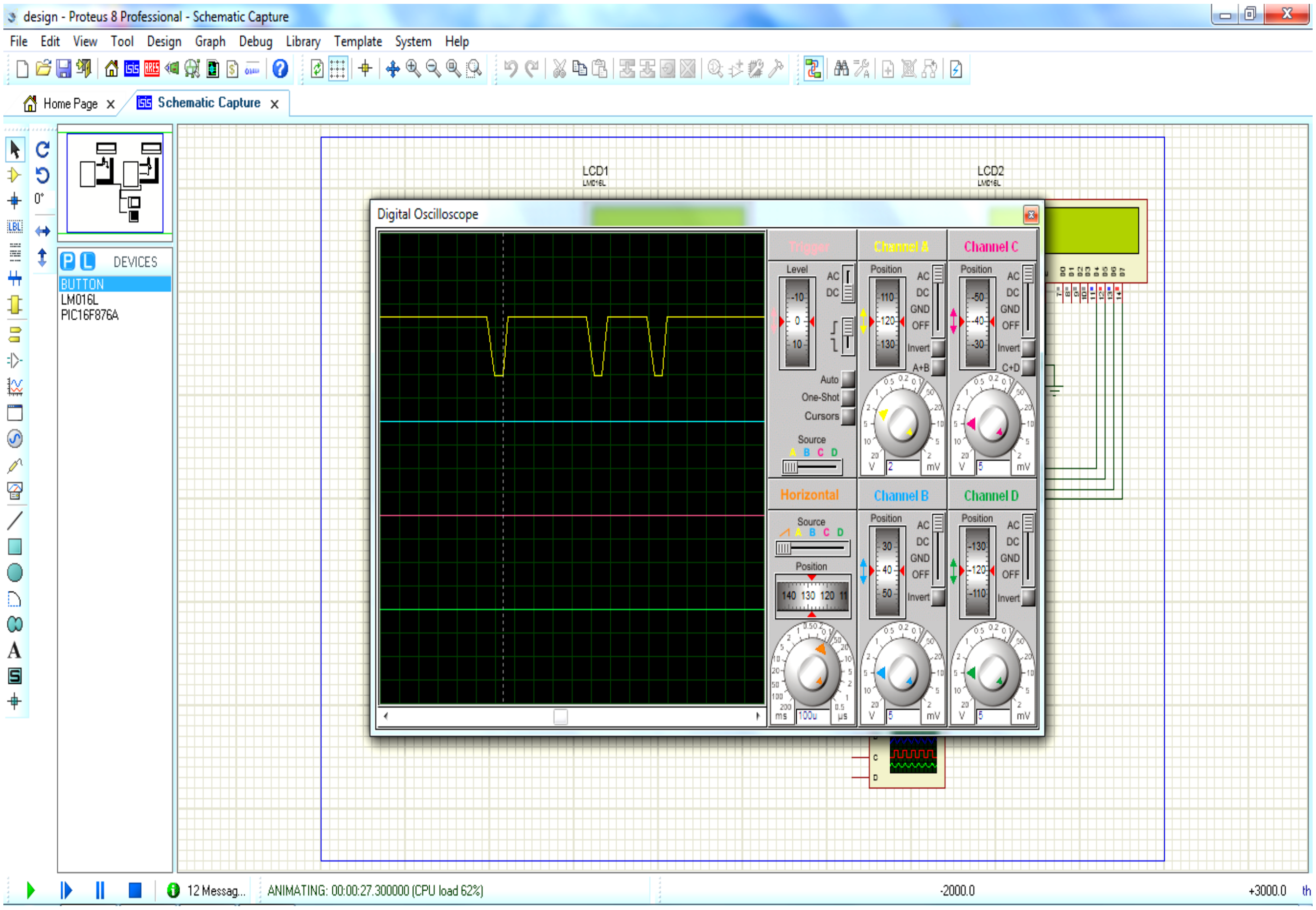


Figure 10. Communication overhead vs. No. of nodes

Figure 8 exhibits the performance of the CHTPS, PODCND, and EDAT with regards to the energy consumption, which is stimulated by a varying number of nodes. The energy consumption is estimated by the energy consumed by transmission, reception, and interference is subtracted from the total initial energy.

This will be observed from Figure 8 that EDAT is 29% and 13.8% lesser and outperforms the present system CHTPS and PODCND with regards to energy consumption. PDR is the proportion of data packets received and the data packets transmitted in the technique. To achieve efficiency in transmission, the PDR should be high. Figure 9 shows that the values calculated for PDR of the existing CHTPS and PODCND exhibit somewhat less performance inefficiency than that of the proposed EDAT. Figure 10 shows that the communication overhead of EDAT is 26% and 16% lesser than that of CHTPS and PODCND.

For the proposed work EDAT, Proteus Version 8.0 Professional simulation software is used for the implementation of the secured communication between the CH and the BS since no hardware is required and it is convenient to use as a training tool. The simulation results are shown in figure 11, and the complete execution of the proposed work is shown in figure 12.



ANIMATING: 00:00:27.300000 (CPU load 62%)

Figure 11. Simulation result using Proteus Version 8.0 Professional Software.

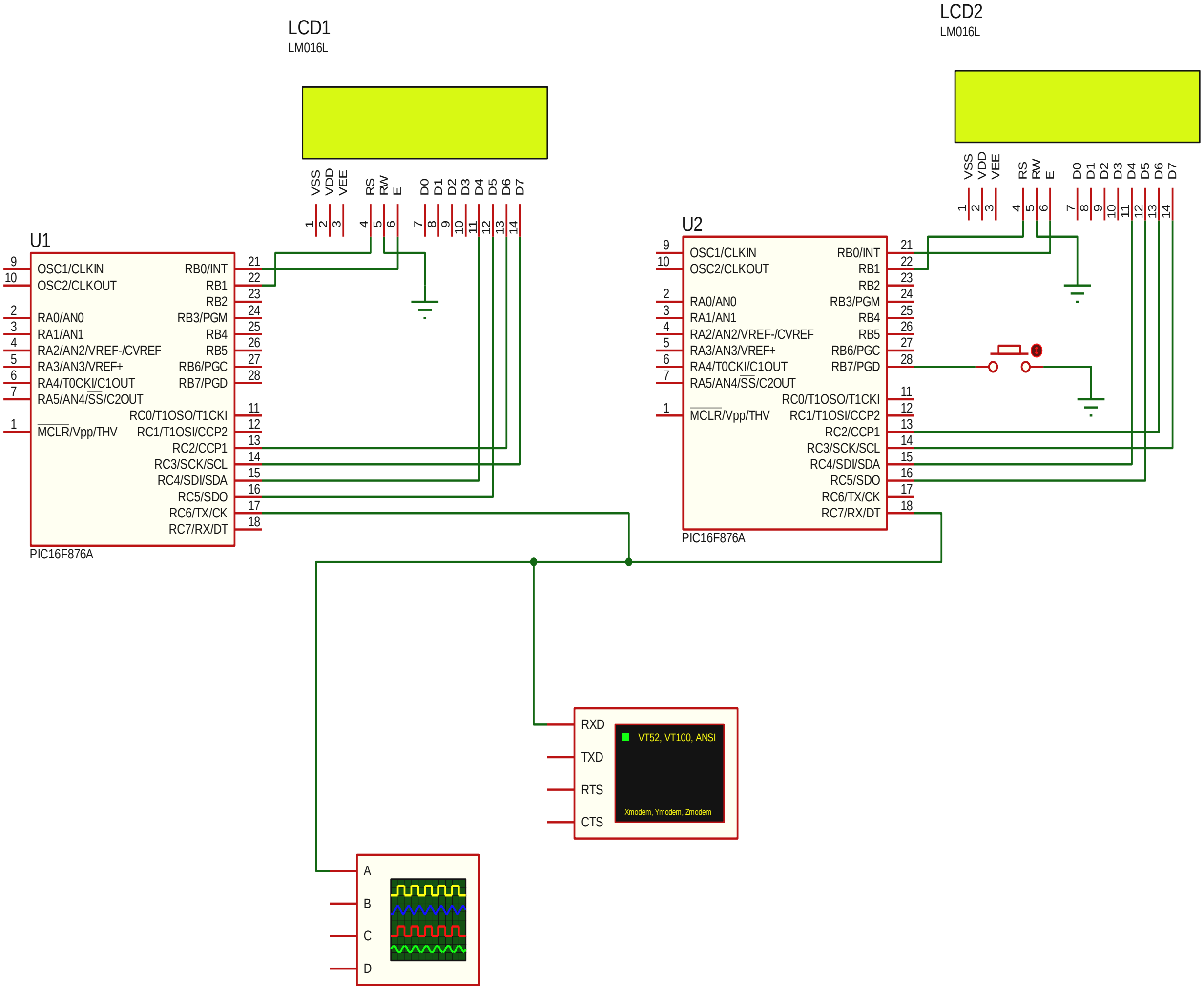


Figure 12. Overall design implemented for the proposed work.

Figure 13 shows the hardware implementation of Cluster Head, and figure 14 shows the hardware implementation of Base Station in WSN.

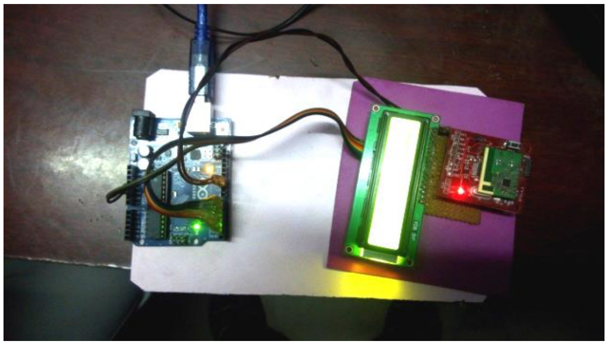


Figure 13. Hardware implementation of Cluster Head in WSN.

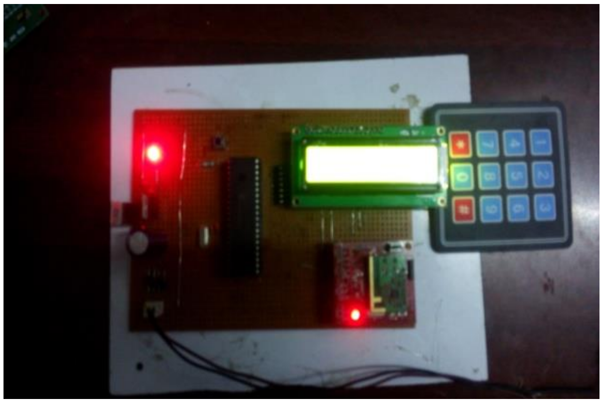


Figure 14. Hardware implementation of Base Station in WSN.

Hardware implementations show that the proposed design can bring off ultimate secrecy when transferring the data in WSN.

VI. CONCLUSION

The security of data plays a vital role in sensor networks. Since they had constraints as they are tiny sensor devices, the routing service will have disastrous effects over the attacks mounted on them in WSN. However, due to their high resource demands, few standard techniques that are used to safeguard from these typical routing attacks are not advisable in sensor networks. Hence, the proposed work influenced a new aspect to develop an efficient security system by making use of the available resources in WSNs. In the proposed EDAT algorithm, the overall network is divided into subgroups called Clusters, and each Cluster has CH based on their energy in the node, and the election of CH is done by using Q-LEACH protocol. For more secured communication between CH and BS uses MAC-based symmetric key encryption. Finally, a prototype of a WSN is developed based on the EDAT algorithm for the implementation of secured communication between CH and BS. Hence in this proposed work, EDAT, an efficient DA technique with high security for green communication in WSN, is designed and compared with the existing methods, and also it is tested using hardware. Further, this technique can be enlarged by including various characteristics considering more indicators like energy harvesting methods.

REFERENCES

[1] S.Kumar, V.Kumar, O.Kaiwartya, U.Dohare, N.Kumar, and J.Lloret., Towards green communication in wireless sensor network: GA enabled distributed zone approach, Ad Hoc Networks, 93 (2019) 101903.

[2] Reza Soosahabi, Dmitri Perkins., Optimal Probabilistic Encryption for Secure Detection in Wireless Sensor Networks, IEEE Transactions on Information Forensics and Security, 9(3) (2014).

[3] Anita Daniel. D, Emalda Roslin. S., A Review on Existing Security Frameworks with Efficient Energy Preservation Techniques in Wireless Sensor Networks, IEEE International Conference on Communication and Signal Processing (ICCSP'15), https://doi.org/10.1109/iccsp.2015.7322571 (2015) 661-665,

[4] Huang Lu, Jie Li, Mohsen Guizani., Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 25(3) (2014).

[5] Kortas, M., Habachi, O., Bouallegue, A., Meghdadi, V., Ezzedine, T., & Cancel, J.-P., Energy-Efficient Data Gathering Schema for Wireless Sensor Network: A Matrix Completion Based Approach, International Conference on Software, Telecommunications and Computer Networks, (2019) .https://doi.org/10.23919/SOFTCOM.2019.8903635

[6] Masanari Iwata, Suhua Tang, and Sadao Obana., Energy-Efficient Data Collection Method for Sensor Networks by Integrating Asymmetric Communication and Wake-Up Radio, Sensors,18(1121) (2018). https://doi.org/10.3390/s18041121

[7] Tristan Daladier Engouang, Yun Liu, and Zhenjiang Zhang., GABs: A Game-based Secure and Energy-Efficient Data Aggregation for Wireless Sensor Networks, International Journal of Distributed Sensor Networks, Article ID 658543, (2015).

[8] M. Roseline Juliana, S.Srinivasan., SELADG: Secure Energy Efficient Location-Aware Data Gathering Approach For Wireless Sensor Networks, International journal on smart sensing and intelligent systems, 8(3) (2015).

[9] Jong-Min Kim, Hong Sub Lee, Junmin Yee, and Minho Park., Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks, Journal of Sensors, Article ID 2678269, (2016).

[10] Anita Daniel. D, Emalda Roslin. S., Data validation and integrity verification for trust-based data aggregation protocol in WSN, Microprocessors, and Microsystems, 103354, (80) (2021). https://doi.org/10.1016/j.micpro.2020.103354

[11] Khorasani, F., & Naji, H. R., Energy-efficient data aggregation in wireless sensor networks using neural networks, International Journal of Sensor Networks, 24(1) (2017).

[12] https://doi.org/10.1504/IJSNET.2017.084207

[13] Liu, X., Yu, J., Zhang, X., Energy-efficient privacy-preserving data aggregation protocols based on slicing, EURASIP Journal on Wireless Communications and Networking Article, 19 (2020). https://doi.org/10.1186/s13638-020-1643-6

[14] Ali, I., Khan, E., & Sabir, S., Privacy-preserving data aggregation in resource-constrained sensor nodes in the Internet of Things: A review, Future Computing and Informatics Journal, 3(1) (2018) 41–50.

[15] https://doi.org/10.1016/j.fcij.2017.11.004

[16] Joyce Jose, Josna Jose, M. Prince, "A Survey on Privacy-Preserving Data Aggregation Protocols for Wireless Sensor Networks," Journal of Computer and Information Technology, Vol. 22, No.1 (2014) https://doi.org/10.2498/cit.1002318

[17] Anish Soni and Rajneesh Randhawa., OSDAP- Optimized and Secure Data Aggregation Protocol for Wireless Sensor Networks, International Journal of Applied Engineering Research ISSN 0973-4562, 13(5) (2018) 3027-3033.

[18] Keyur Parmar and Devesh C. Jinwala., Symmetric-Key Based Homomorphic Primitives for End-to-End Secure Data Aggregation in Wireless Sensor Networks, Journal of Information Security, 6 (2015) 38-50.

[19] Prathima, Shiv Prakash T, Venugopal K, R.S. S. Iyengar, and L. M. Patnaik., ADA: Authenticated Data Aggregation in Wireless Sensor Networks, International Journal of Computer Applications (0975 – 8887), 167(7) (2017).

[20] Abdul Razak and Syed S. Rizvi., Secure Data Aggregation Using Access Control and Authentication for Wireless Sensor Networks, Elsevier, Computers & Security, http://dx.doi.org/doi: 10.1016/j.cose.2017.07.001, (2017).

[21] Jong Min Kim, Hong Sub Lee, Junmin Yee, and Minho Park., Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks, Journal of Sensors, Article ID 2678269, (2016).

[22] T.V.Suresh Kumar, Dr.Prabhu G Benakop., A Secure Routing Protocol for MANET using Neighbor Node Discovery and Multi Detection Routing Protocol, International Journal of Engineering Trends and Technology, 68(7) (2020) 50-55.

[23] Wei Min,Chen Ruixiang and He Shunbin., A Secure Data Aggregation Approach in Hierarchical Wireless Sensor Networks, ACM, IMCOM '16, January, Danang, VietNam, (2016) 4-6.

[24] Jitendra Kurmi, Ram Singar Verma and Sarita Soni., An Approach for Data Aggregation Strategy in Wireless Sensor Network using MAC Authentication, Advances in Computational Sciences and Technology, ISSN 0973-6107, 10(5) (2017)1037-1047.

[25] Anita Daniel D., Emalda Roslin S., An Efficient Trust-Based Secure Data Aggregation Technique In WSN, Indian Journal Of Computer Science and Engineering, 12(1) (2021) 78-286. https://doi.org/10.21817/indjcse/2021/v12i1/211201227

[26] Dr. Mohammed Ali Hussain, Dr. Balaganesh Duraisamy., Review on Packet drop prevention in MANET by counter-based digester ACK, International Journal of Engineering Trends and Technology 68(8) (2020) 102-107.

[27] Ajay Sikandar, R. Agrawal, M. K. Tyagi, A. L. N. Rao, M. Prasad, and M. Binsawad., Toward green computing in wireless sensor networks: prediction-oriented distributed clustering for non-uniform node distribution, EURASIP Journal on Wireless Communications and Networking, (2020). https://doi.org/10.1186/s13638-020-01788-0

[28] Farah Kandah, Jesse Whitehead, and Peyton Ball., Towards trusted and energy-efficient data collection in unattended wireless sensor

networks, Wireless Networks, (2020). https://doi.org/10.1007/s11276-020-02394-0)

[29] Gulzar Mehmood, Muhammad Zahid Khan, Abdul Waheed, Mahdi Zareei and E.M. Mohamed., A Trust-Based Energy-Efficient and Reliable Communication Scheme for Remote Patient Monitoring in Wireless Body Area Networks IEEE Access, 8 (2020).

[30] Syed Gul Shah, Atiq Ahmed, Ihsan Ullah, and Waheed Noor., A Novel Data Aggregation Scheme for Wireless Sensor Networks, International Journal of Advanced Computer Science and Applications, 10(2) (2019).