

Secure Data Communication in a Clustered Network in Wireless Sensor Networks using AES Cipher

Manjunatha A S¹ and Dr. Venkatramana Bhat P²

¹Assistant Professor, Nitte (Deemed to be University), NMAM Institute of Technology (NMAMIT), Department of Computer and Communication Engineering
Email: Manjunatha.as@nitte.edu.in

²Professor, Nitte (Deemed to be University), NMAM Institute of Technology (NMAMIT), Department of Computer Science and Engineering
Email: pv.bhat@nitte.edu.in

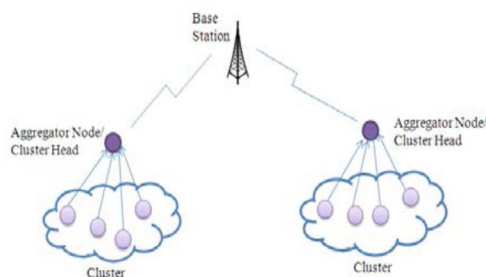
Abstract— Data is collected and forwarded to the cluster head by sensor nodes in the Wireless Sensor Network (WSN). Ensuring the confidentiality and integrity of the data that must be provided to the base station is tough. We recommend using a simple Caesar cipher and Advanced Encryption Standard (AES) technique at the cluster head node level for effective communication from the cluster head to the base station with little power consumption.

Index Terms— WSN, Caesar Cipher, AES, Cluster head, Base Station

I. INTRODUCTION

Wireless sensor networks (WSN) research is one of the main areas in computer science. WSN is used in many modern applications, including those in robotics, agriculture, the military, healthcare, and residential settings, among others. The WSNs can be used to track enemy intrusion, forest fires, and floods, as well as to monitor network traffic flows and environmental pollutants. A wireless sensor network is made up of many sensor nodes that all read environmental data. A sensing device, a microcontroller, an RF module, and a limited quantity of battery power are all included in each sensor node. The sensor nodes are set up to send the base station the data they have gathered.

WSNs resemble ad hoc networks with a large number of sensor nodes. However, because wireless sensor networks lack a stable infrastructure, the sensor nodes can be set up and run in an ad hoc manner. To track real-time data



flow, the cluster head uses a bare minimum of precise software. The cluster head will send the sensed data to the backup data center for further processing and analysis. The fundamental architecture of a typical wireless sensor network is shown in Fig. 1.1, and it includes the cluster head.

Security is one of the WSNs' main drawbacks. WSNs are frequently put in remote locations and run unattended, making the privacy of the data collected at each node and the prevention of attack critical considerations. The classification for the sensed data and the security countermeasure strategies are of interest. The difficulty in this direction is ensuring secure data transmission in wireless sensor networks.

II. LITERATURE REVIEW

In recent years, a number of security issues have been discovered. Two categories [1] of security threats can be made from them:

1. Active attacks

Attacks in which the attacker changes the information in the detected data are referred to as active attacks. Active attacks include, but are not limited to, wormhole attacks, compromised node attacks, and node replication attacks.

2. Passive attacks

Passive attacks occur when a network is being watched by the attacker to ensure that data is being communicated. Eavesdropping is an example of a passive attack, which compromises the privacy of the data.

The nature of wireless sensor networks is dynamic because nodes often join and depart the network [2]. The writers have also covered the many types of attacks that could be launched against sensor networks. The low-level security of mobile sensor networks has been discussed.

The threats against broadcast services in wireless sensor networks have been covered by Seonho Choi et al. [3]. The most devastating effects on power and other resource limits will result from these attacks. The sensor nodes will just waste their energy and memory on broadcasting and buffering those erroneous packets as they propagate through the sensor nodes without being filtered out. For sensor networks, they suggested a brand-new, secure broadcast authentication. Their research suggests that this authentication method can be used to identify erroneous packets and separate links that originate from compromised nodes, increasing resilience to various security assaults, including DoS attacks. Lightweight Neighbor Authentication Protocol (LNAP) and Predictive Hash-Based Broadcast Protocol (PHBBP) are the two parts of their study. LNAP is used to verify whether a packet is actually from a neighbor or not when it is received. Each sensor node can use this protocol to verify whether a packet they receive is coming from a neighbor or not. The PH technique and size selecting the forwarding approach are the foundations of the PHBBP protocol.

A solution for the security of concealed data aggregation (CDA) and broad private data aggregation (PDA) has been proposed by the authors in [5], which also discusses the safety framework for protecting privacy in data aggregation in wireless sensor networks. The authors claim that both private-key and public-key based CDA/PDA constructions are covered by the security model. But in order to prevent active attacks, suitable security measures are needed for end-to-end communication.

In [6], a light-weight security protocol (LiSP) is put out that has key renewability and strikes a balance between resource usage and security. In addition, the authors suggested a combined authentication and recovery algorithm for rekeying, in which the key server regularly broadcasts a new key before it is used for encryption or decryption, and a client node authenticates the received key before recovering the previously lost keys. Figure 2 depicts the key hierarchy that was employed in LiSP.

The main issues with wireless sensor networks are wormhole-based attacks [7]. The authors claim that in wormhole assaults, attackers establish a low-latency link between two network nodes. The attacker gathers the data packets, transfers them via the low-latency link, and then replays them at the other end after the link has been established. Wormhole attacks change the way data flows across the network before tricking the base station. The authors reviewed wormhole attacks and provided examples of the most recent advancements in wireless sensor network wormhole attack detection. The authors covered a range of wormhole assaults, including those that use encapsulation, high-quality/out-of-band channels, high power transmission capabilities, and protocol distortion. They also talked about the mechanisms for detecting wormhole attacks, including connectivity - based, distance - bounding/consistency - based, synchronized clock-based, multi-dimensional scaling-visualization, trust-based, localization-based, secure neighbor discovery, and radio fingerprinting approaches.

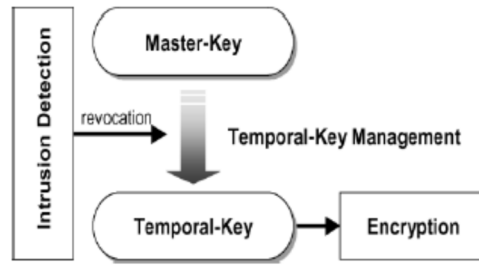


Figure 2. The key hierarchy used LiSP

Riaz Ahmed Shaikh et al. provided an integrated privacy, security, and trust solution for WSNs in [8], which is required to achieve the security solution's fullness. In order to better understand how different components interact with one another, they also provided integration details for the privacy, security, and trust components. They conducted theoretical analyses and assessments of memory usage, communication overhead, and other topics. Their memory usage result is shown in Figure 3.

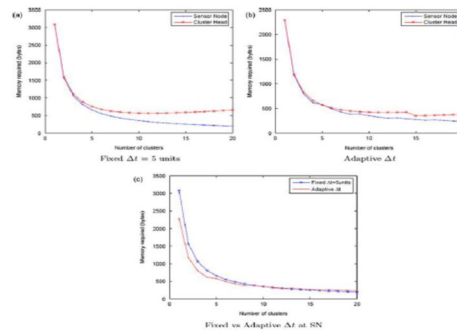


Figure 3. Memory consumption

The outcome in terms of communication overhead when moving data from the cluster head node to the base station is shown in Figure 4.

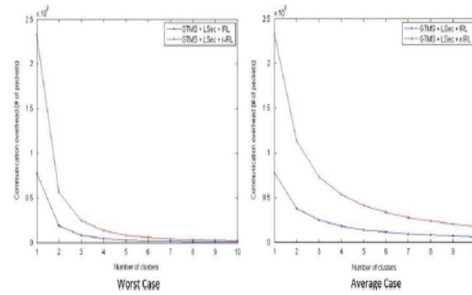


Figure 4. Communication Overhead

The authors' idea uses the AES, DES, and m-RSA algorithms to combine the benefits of symmetric and asymmetric encryption systems [9]. The plain text is separated into three parts for the encryption scheme, with the first portion being encrypted using AES, the second using DES, and the third using m-RSA. Through the use of MATLAB 2017a's parallel Computing Toolbox function, these are applied simultaneously. The three cipher messages are combined to create the ciphertext, which is sent to the recipient.

The symmetric encryption and decryption mechanism in wireless sensor networks was mentioned by WeiZhou et al. [10]. They also mentioned wireless sensor networks for data transmission. The authors claim that by utilizing the symmetric key technique, the security of data transmission in wireless sensor networks can be significantly improved. In order to increase the overall transmission performance of the wireless sensor networks, the transmission performance of the wireless sensor networks is further examined in light of this.

Tanveer Zia et al. highlighted the many security problems that could impair the data flow in wireless sensor networks in [12], along with workable solutions to these problems. They also identify a number of wireless sensor network restrictions, including node, network, and physical restrictions.

There are two primary management strategies: distributed and centralized strategies [13]. A reliable third-party key distribution center (KDC) is used by the centralized method to distribute and manage keys. In contrast, the generation and updating of keys are entirely carried out in a distributed way under the distributed approach.

Using homomorphic encryption, Soufiene Ben Othman et al. [14] examine the confidentiality and integrity of data aggregation in WSN. The system uses homomorphic encryption with symmetric keys to safeguard the privacy of the data and combines it with homomorphic signature to verify the accuracy of the aggregated data. They demonstrated that their system had lower overheads for processing and communication compared to currently used techniques.

A security architecture against the selfishness problem for cluster based WSN was proposed by Zeba Ishaq et al. [15]. They demonstrated how, particularly when a cluster head node becomes selfish, the selfishness attack (also known as a passive attack or insider attack) in cluster based WSNs can result in major performance disaster. They bring forth a security architecture that uses a novel clustering technique in addition to a reputation system at nodes to curb selfishness and encourage cooperation and integrity.

Puneet Azad et al. talked about choosing cluster heads in [16]. They chose to choose the cluster heads using a fuzzy multiple attribute decision-making approach. They took into account factors including residual energy, the quantity of neighbors, and the separation between the base station and the nodes while choosing the cluster leaders. Since symmetric encryption methods require little energy, they are frequently used to achieve the fundamental security of data transfer. Nodes could go dark if energy intake and consumption are out of balance. A plan was put up by Jong Min Kim et al. [17] in which, based on an energy threshold, switching between symmetric-key and public-key encryption allows the level of security to be balanced against the necessity of energy-saving.

To counter malicious node attacks on WSNs, Turki Ali Alghamdi et al. introduced a convolutional approach in [18] that creates security bits using convolutional codes. Different security codes were generated at various hops, with the findings demonstrating a reduction in computational cost when compared to current methods.

For WSN, Cheng-Kang Chu et al. [19] suggested using practical-ID based encryption. It divides the encryption procedure into an offline step and an online step. All of the complex calculations are carried out in the offline portion without knowing who the receiver is. In the online stage, the recipient's identity and the plaintext message are all that are needed, together with simple computations like modular operation and symmetric-key encryption. In the WSN, symmetric encryption and the blockchain process are discussed by Alma E. Guerrero-Sanchezin et al. [20]. Based on the security benefits offered by blockchain technology and the usage of cryptographic tools, they proposed an approach that aids in protecting data availability and integrity. Their findings demonstrated that their approach is less vulnerable to several of the key attacks.

III. METHODOLOGY

A. Data Aggregation

The data from the numerous sensor nodes are gathered through experimental study. Utilizing MATLAB and changing numbers of sensor nodes, the LEACH algorithm is developed. The cluster head is where the present work collects and obtains sensor readings. The graph displays the energy used by the sensor nodes. The cluster head is located, and the amount of energy used there is measured. For the purpose of data aggregation, the LEACH algorithm is taken into consideration.

B. Encryption

The fundamental encryption algorithm should be used to encrypt the sensed data acquired at the cluster head, and the cluster head's energy consumption is noted. The effective method is now being further implemented after this initial work has been completed. In the cluster head node, the AES algorithm is used. A graph is created showing the energy used by each node.

IV. RESULTS AND DISCUSSIONS

A. Data Aggregation

A wireless sensor network is built using MATLAB. Six sensor nodes, two cluster heads, and one base station are shown in a wireless sensor network model in Figure 5.

Then, 50 nodes are added to the wireless sensor network. Initial energy is taken into account when building a wireless sensor network as 10 units, measured in Joules. It is assumed that 50×10^{-9} units of Joules per bit are needed to power the circuitry for the transmitter and receiver. The necessary number of sensor nodes are setup in the WSN. As shown in Figure 6, we have chosen a node count of 50 for the demonstration. The zone division is completed after the necessary number of sensor nodes has been determined. We have set the zone size for the

present implementation at 400x400. Anywhere in the zone is suitable for the sink node. The sink node's position needs to be specified. In this approach, the sink node is located at coordinates 210x210. The LEACH method is used, and the outcomes are displayed below. Additionally, the direct approach is used, and the sensed data is relayed straight to the base station. The graph in Figure 7 compares and plots the output of these two algorithms.

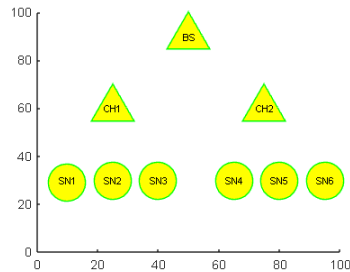


Figure 5. Basic Configuration of WSN with two cluster head and six sensor nodes with Base Station

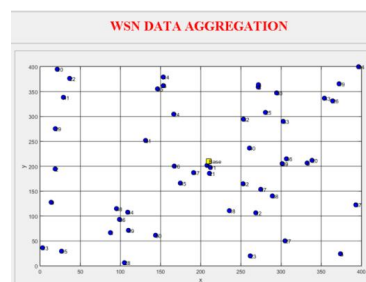


Figure 6. WSN with 50 nodes with Base Station

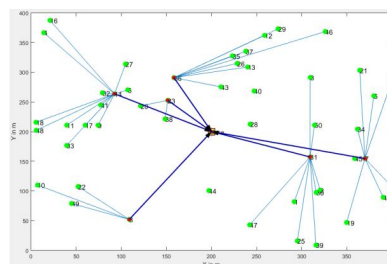


Figure 7. Simulation Results

According to the findings, the LEACH algorithm uses less energy when compared to sending sensed data directly. The outcome is displayed in Figure 8.

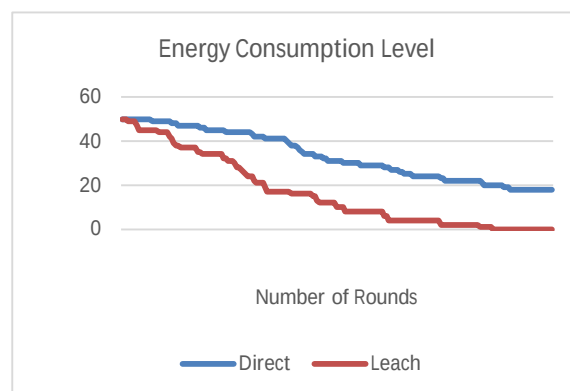


Figure 8. Average Energy Consumption

The average amount of energy used by the algorithm is calculated in a similar way, and the findings indicate that LEACH has better energy usage. The graph in Figure 9 displays the comparison of outcomes.

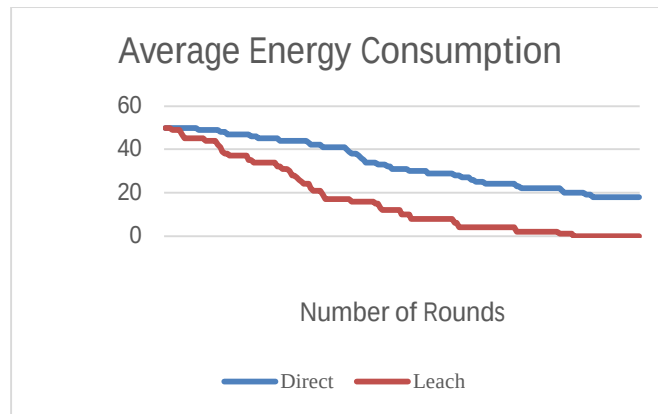


Figure 9. Average Energy Consumption

The average energy consumption is shown in Figure 9 above. The results show that energy is reduced as the round goes on.

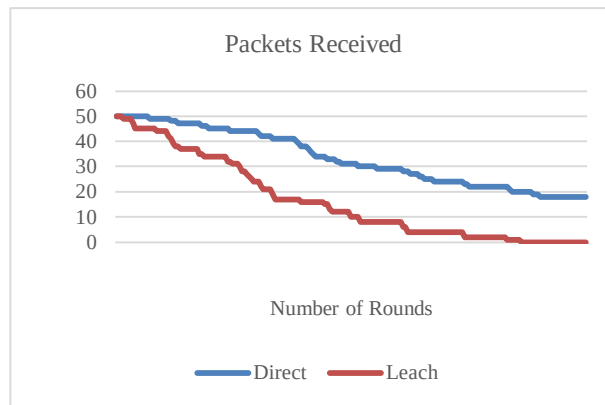


Figure 10. Packets received at the base station using the direct method and the LEACH algorithm.

As the round progresses due to energy limits, the overall number of nodes will decrease. This is depicted in Figure 11, which we can see in the round.

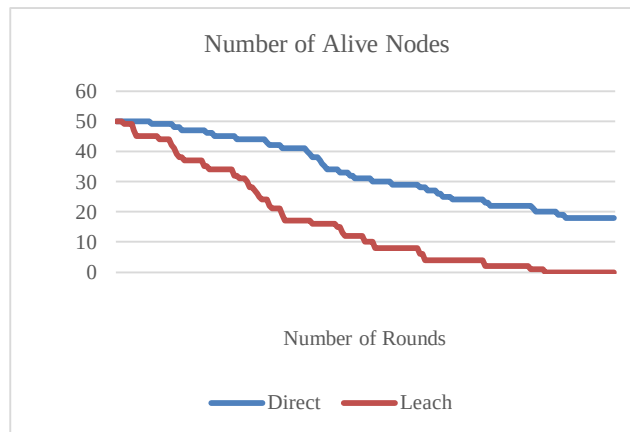


Figure 11. The total number of alive after simulating into 200 rounds.

Most of the nodes in the direct method are not participating in any transmissions because they are outside of the service area. As a result, they are still alive 200 rounds later. We obtained the results as LEACH created the improved transmission rate because there were more nodes involved in the data transfer.

After using the LEACH method to encrypt the data before transmitting it to the base station, the AES technique is used at the cluster node level. We used the fundamental encryption algorithm (Caesar Cipher) at the cluster head

in order to compare the outcomes. When using the AES method, energy consumption is higher, whereas when using the Caesar cipher, energy consumption is lower because the Caesar cipher requires less computation. The comparison findings are displayed in Figure 12.

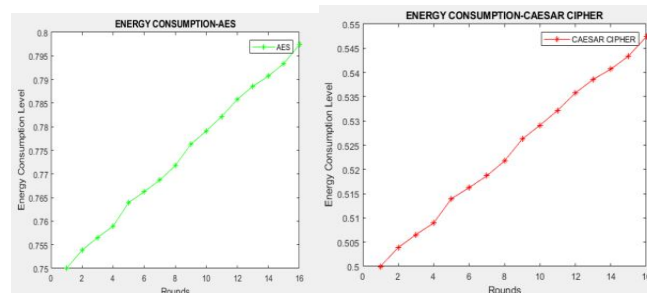


Figure 12. Comparison of AES and Caesar cipher

V. CONCLUSION

Implementing the AES algorithm has produced results and the same have been acquired and plotted. The analysis reveals that the Caesar cipher uses less energy than the AES method. In comparison to the conventional Caesar cipher approach, we have shown that the AES algorithm performs better.

REFERENCES

- [1] Chun-Ta Li, Department of Information Management, Tainan University of Technology, Taiwan, "Security of Wireless Sensor Networks: Current Status and Key Issues", DOI: 10.5772/13158
- [2] Kashif Kifayat, Madjid Merabti, Qi Shi, David Llewellyn-Jones, "Security in Mobile Wireless Sensor Networks", <https://www.researchgate.net/publication/225933532>.
- [3] Seonho Choi, Hyeonsang Eom, and Edward Jung, "Securing Wireless Sensor Networks Against Broadcast Service Attacks", International Journal of Computers and Applications, ISSN: 1206-212X (Print) 1925-7074 (Online).
- [4] Devender Kumar, Harsh Kumar Singh & Chhahat Ahlawat, "A secure three-factor authentication scheme for wireless sensor networks using ECC", Journal of Discrete Mathematical Sciences and Cryptography, SSN: 0972-0529 (Print) 2169-0065 (Online).
- [5] Aldar C-F. Chan, Claude Castelluccia, "A Security Framework for Privacy-Preserving Data Aggregation in Wireless Sensor Networks", Acn Transactions on Sensor Networks, Vol. 7, No. 4, Article 29, Publication Date: February 2011.
- [6] Taejoon Park and Kang G. Shin, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks", ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, August 2004, Pages 634–660.
- [7] Majid Meghdadi, Suat Ozdemir & Inan Güler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, ISSN: 0256-4602 (Print) 0974-5971 (Online)
- [8] Riaz Ahmed Shaikh, Sungyoung Lee & Aiiad Albeshri, "Security Completeness Problem in Wireless Sensor Networks", ISSN: 1079-8587 (Print) 2326-005X (Online)
- [9] Pooja & R. K. Chauhan, "Triple phase hybrid cryptography technique in a wireless sensor network", ISSN: 1206-212X (Print) 1925-7074 (Online)
- [10] WeiZhou, PingLi, QinJuWang, Narjes Nabipour, "Research on data transmission of wireless sensor networks based on symmetric key algorithm", <https://doi.org/10.1016/j.measurement.2019.107454> 40263-2241/_ 2019 Elsevier Ltd.
- [11] Shadi Nashwan, "AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment", <https://doi.org/10.1016/j.eij.2020.02.005> 1110-8665/_ 2020 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.
- [12] Tanveer Zia, Albert Zomaya, "Security Issues in Wireless Sensor Networks", DOI: 10.1109/ICSNC.2006.66
- [13] Weiping Wang1, Shigeng Zhang, Guihua Duan, and Hong Song, "Security in Wireless Sensor Networks", Higher Education Press, Beijing and Springer-Verlag Berlin Heidelberg 2013.
- [14] Soufiene Ben Othman, Abdullah Ali Bahattab, Abdelbasset Trad & Habib Youssef, "Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption", Wireless Personal Communications, ISSN 0929-6212, DOI 10.1007/s11277-014-2061-z
- [15] Zeba Ishaq, Seongjin Park, and Younghwan Yoo, "A Security Framework for Cluster-Based Wireless Sensor Networks against the Selfishness Problem", 10 Jul 2018, <https://doi.org/10.1155/2018/8961239>
- [16] Puneet Azad and Vidushi Sharma, "Cluster Head Selection in Wireless Sensor Networks under Fuzzy Environment", 24 Feb 2013, <https://doi.org/10.1155/2013/909086>
- [17] Jong Min Kim, Hong Sub Lee, Junmin Yi, and Minho Park "Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks", 16 Mar 2016, <https://doi.org/10.1155/2016/2678269>

- [18] Turki Ali Alghamd, “Convolutional technique for enhancing security in wireless sensor networks against malicious nodes”, 22 October 2019, Human-centric Computing and Information Sciences volume 9,Article number: 38 (2019)
- [19] Cheng-Kang Chu, Joseph K. Liu, Jianying Zhou, Feng Bao, Robert H. Deng, “Practical ID-based Encryption for Wireless Sensor Network”, 4 Jan 2010, International Association for Cryptologic Research
- [20] Alma E. Guerrero-Sanchez, Edgar A. Rivas-Araiza, Jose Luis Gonzalez-Cordoba, Manuel Toledano-Ayala, and Andras Takacs, Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network, Sensors (Basel). 2020 May; 20(10): 2798, doi: 10.3390/s20102798