10.48047/jocaaa.2025.30.02.20

Secure Data Aggregation in Wireless Sensor Networks Using Homomorphic Encryption

Dr.G.M.Tamilselvan[1]
Professor,Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, principal@shanmugha.edu.in
Mr.P.Sudarsan[2]
Assistance Professor, Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, sudarsanps@gmail.com
Mrs.C.K.Balasundari[3]
Assistance Professor, Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, balasundari@shanmugha.edu.in
Mr.E.Santhose[4]
Assistance Professor, Department of Electronics and Communication Engineering, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Morur (Post), Sankari (Tk), Salem, santhosh.e@shanmugha.edu.in

Abstract- the aggregating methodology ensures that transmitted data remain visible in clear text in the aggregated units or nodes. Data transmission without encryption is vulnerable to security issues such as data confidentiality, integrity, authentication and attacks by adversaries. On the other hand, encryption at each hop requires extra computation for decrypting, aggregating, and then re-encrypting the data, which results in increased complexity, not only in terms of computation but also due to the required sharing of keys. Sharing the same key across various nodes makes the security more vulnerable. An alternative solution to secure the aggregation process is to provide an end-to-end security protocol, wherein intermediary nodes combine the data without decoding the acquired data. As a consequence, the intermediary aggregating nodes do not have to maintain confidential key values, enabling end-to-end security across sensor devices and base stations.

Keywords – homomorphic encryption, data aggregation, wormhole attack, secure data aggregation, IoT-based WSN.

INTRODUCTION

The IoT-based wireless Sensor network (WSN) is a revolutionary system for smart observation. An IoT-based Wireless Sensor Network (WSN) is defined as a number of spatially dispersed and dedicated sensors for observing and recording the physical conditions, such as temperature, humidity, etc., of the environment [1]. The collected data are forwarded through a wireless network to an internet-based base station. The primary goal of data fusion or aggregation is to extend network life by reducing sensor network resource use, which includes batteries, power, and bandwidth. Data aggregation techniques, on the other hand, could affect key quality of service measures in WSN, such as accuracy, speed, and failure. Furthermore, data aggregation introduces new risks [2]. A hacked sensor node, for instance, might either fraudulently release or broadcast the data it acquires from neighbouring nodes, or return random results as aggregated data. As a

result, an opponent may violate both the secrecy and the integrity of the information over a broad section of the WSN by compromising a significant number of aggregating units near the base station [3]. Rafik et al. offered a secure data accumulation strategy which guarantees data privacy through symmetric-key homomorphic encryption (HE) using homomorphic signatures to validate data integrity. The protocol is prone to wormhole attack. Lacking understanding about the key procedures of cryptography, a wormhole exploits the network communication architecture. Wormhole threats are primarily designed to confuse routing protocols and communication services [4]. As a result, developing an end-to-end secure data aggregation technique, while achieving confidentiality, integrity and attack detection, is a challenging task because an effective security strategy is essential in order to preserve integrity and durability and to retain sensitive data. he key objectives of the proposed protocol are as follows.

- A novel HE technique enabling end-to-end data secrecy/confidentiality is proposed. The proposed EEHE could be used by aggregators to apply arithmetic aggregation functions on cipher texts [5].
- MAC is used to ensure data integrity. Within the proposed methodology, monitoring nodes generate MACs to the collected data so that certain participants in the group may instantly derive and check the MACs to ensure data integrity. As a result, there is no need to provide the non-encrypted data for confirmation [6].
- To identify wormhole attacks as soon as feasible during the data forwarding and aggregating operations, a paradigm focused upon neighbouring tables is proposed, comprising a monitoring, forwarding, and an aggregator's adjacent node [7].

RELATED WORK

The literature discusses a vast scope of secure data aggregation methodologies centered around homomorphically encrypted algorithms. Hung et al. suggested a solution that guarantees the confidentiality of data, reliability, and resistance to eavesdropping threats. Additionally, it recognizes malicious activity with certain added costs [8]. The scheme's primary issue is that no source authentication is accomplished, making it susceptible to Sybil threats. The above limitation is taken into account in the concealed data aggregation (CDA) method in which data aggregators (DA) perform only gathering and merging operations using encrypted messages. As a result, DAs are not required to hold vulnerable encryption keys [9]. The concept of clustering along with data aggregation was introduced by the authors of the protocol, in which the notion of clustering, as well as data aggregation and algebraic features of polynomials, was included. A further end-to-end data aggregating strategy, which employs homomorphic encryption includes elliptic curve cryptography. Compared with previous complicated techniques, the elliptic curve cryptography technique allows nodes to produce keys with a reduced key size. This technique is remarkable for generating two distinct encrypted messages given two exactly identical messages [10]. This is robust to documented plain text threats, and man-in-the-middle attacks. However, such a solution merely gives secrecy, neither authentication nor integrity. In order to achieve integrity and authentication along with confidentiality, there was a need for more efficient secure data aggregation techniques. Authors suggested a simple and evidently secure encrypting approach relying upon indistinguishable characteristics of a cryptographic basic, Pseudo Random Function (PRF) [11]. The methodology assumes the integrity of aggregated data, but also end-to-end authentication. The fundamental aspect of the next protocol, SEEDA, is that it has minimal network communication overheads. The constraint of such an approach is that it only achieves secrecy and does not ensure integrity or authentication. Another issue, along with the achievement

of confidentiality, integrity and authentication, is that the data aggregation process is vulnerable to various attacks, such as false data injection, node compromised attacks, Sybil and wormhole attacks. Data aggregation incorporating fake information monitoring is enabled by a protocol [12].

NETWORK ARCHITECTURE

In the proposed architecture, a small part of the WSN, consisting of 15 sensor nodes, is considered. Out of these nodes, three nodes are designated as the Monitoring, Neighbouring, and Forwarding nodes (MNF), respectively [13]. These nodes constitute a group known as the MNF group. The function of the monitoring node is to calculate the MAC of the data. The relaying and neighbouring nodes collaborate to verify the data generated by the monitoring node. The monitoring and neighbouring nodes record wormhole attacks as well. The DA gathers the information from every cluster, encodes it, and transmits it to a centralized controller, i.e., a base station. Every group's forwarding node (FN) is also interconnected to the FNs of other groups [14]. For fake information detection, each successive DA shares a symmetric key pair. Nodes W1 and W2 form a wormhole link in order to per- form malicious activities such as packet dropping, data modification, routing misguiding, etc., as shown in Figure 1. The different colors of various nodes signify the nodes' different functions; red is for the Data Aggregator node, purple is for the forwarding node, light blue is for the normal sensor node, dark blue is for the monitoring node, black is for the base station, and green is for the neighbouring node, respectively [15].

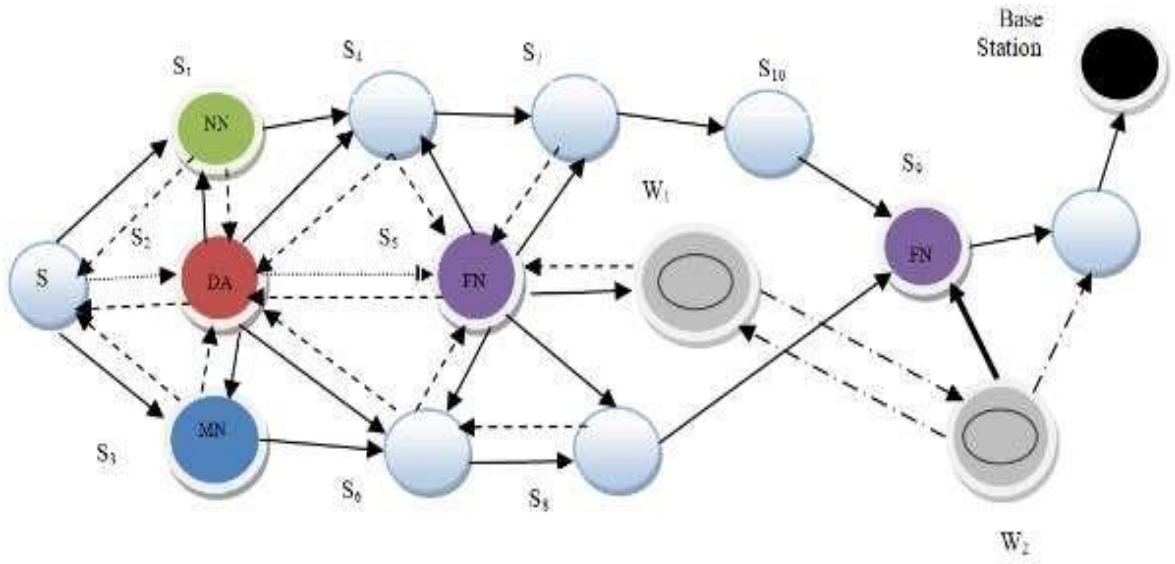

Figure 1- Proposed Architecture[6]

END-TO-END HOMOMORPHIC ENCRYPTION-BASED DATA AGGREGATION PROTOCOL FOR WIRELESS SENSOR NETWORKS

The proposed protocol (as illustrated in Proposed Algorithm 1) is based on the concept of a group of three sensor nodes designated as the monitoring node, neighbouring node and forwarding node. The group is called the MNF group. The flow of the proposed work can be understood from Figure 3 and the timing diagram shown in Figure 2. Detailed steps are as follows [16-18].

- MNF Group Formation and Key Distribution. First of all, an MNF group consisting of three nodes (monitoring node, neighbouring node and forwarding node) is formed. The

base station distributes a Gk to the MNF group and its public key to each node at the time of deployment of the sensor networks [19-20].

- Common Neighbour Table (CNT) Formation. Information about common neighbours between the sender node, i.e., MN node and neighbour nodes is recorded in a table with the help of a CNT algorithm. This table will be helpful in detecting wormhole nodes.
- Wormhole Detection. A wormhole node is detected with the help of common neighbour information between a sender and the neighbour node. There is a separate algorithm for wormhole detection, which will be explained in later sections [21-26].

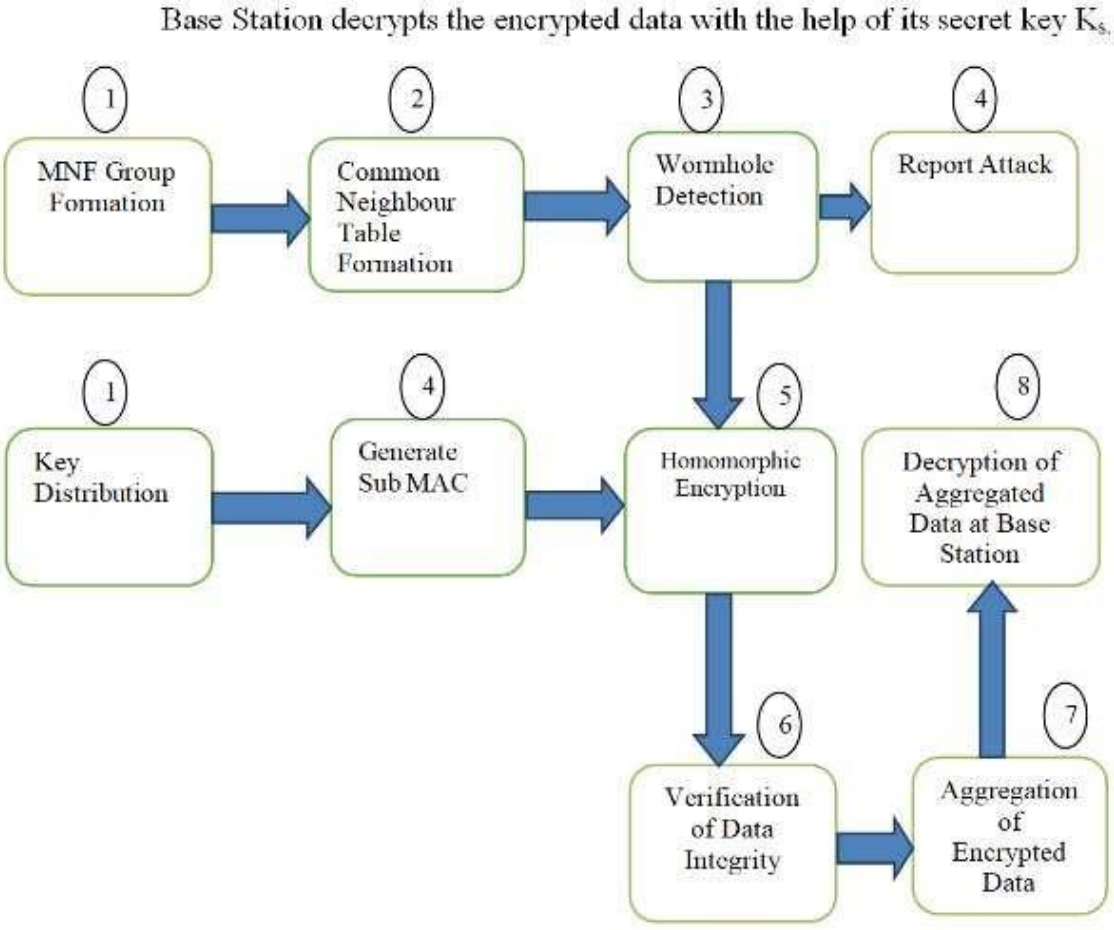

Figure 2- Flow Chart of the Proposed Algorithm[11]

- Report Attack and Generate subMAC. An attack detection report is sent to the base station whenever a wormhole attack is detected. Now, the decision of isolation and removal is taken by the base station, which will be discussed in later sections. In order to verify the integrity of the message, a subMAC is generated by the monitoring node. This message subMAC (MNi) is sent to the DAc. Now, the end-to-end homomorphic value and subMAC EEH (DAc), subMAC (DAc), subMAC (MN) of the message are sent to the Forwarding Node (FN)[19].

- Homomorphic Encryption. Sender calculates the homomorphic value Mi = Mijmod n and sends it to the Neighbouring Node (NN). The Monitoring Node also receives this value and calculates a subMAC (MNi). This subMAC is then sent to the current Dac [20-26].
- Verification of Data Integrity. DAc verifies the integrity of the data by recalculating the subMAC and sends the end-to-end homomorphic value and subMAC [node EEH(DAc), subMAC(DAc)] to a forwarding node (FN)[12].
- Aggregation of Encrypted Data. Now, the current DA computes the aggregated value i .EEHE(p,q)(mi) mod n and sends this value to the base station.
- Decryption of Aggregated Data at Base Station. The Base Station decrypts the encrypted data with the help of its secret key Ks[15].

PROPOSED ALGORITHM

Algorithm 1: Proposed Algorithm.

Input: - Readings of sensor nodes
Output: - Secure aggregated data transmission
Step 1: - MNF group consisting of three nodes (Monitoring node, Neighbouring Node and Forwarding node) is formed. Key distribution is also performed by Base Station.
Step 2: - Common neighbour table of a MNF group is created by calling the CNT algorithm with request message Mreq and reply message Mrep.
Step 3: - Check selected node is secure or not for transmission. Call Algorithm Wormhole Detection.
Step 4: - If wormhole is detected, an error is reported to the Base Station; else, go to step 5. - SubMAC is generated by the monitoring node for data integrity check.
Step 5: - EEHE is performed by the sender node with the help of the public key of Base Station to ensure confidentiality of data.
Step 6: - Data integrity is verified by the neighbouring node by recalculation of MAC.
Step 7: - Aggregation of encrypted data is performed by DA node.
Step 8: - Base station decrypts the aggregated and encrypted data with the help of its secret key.

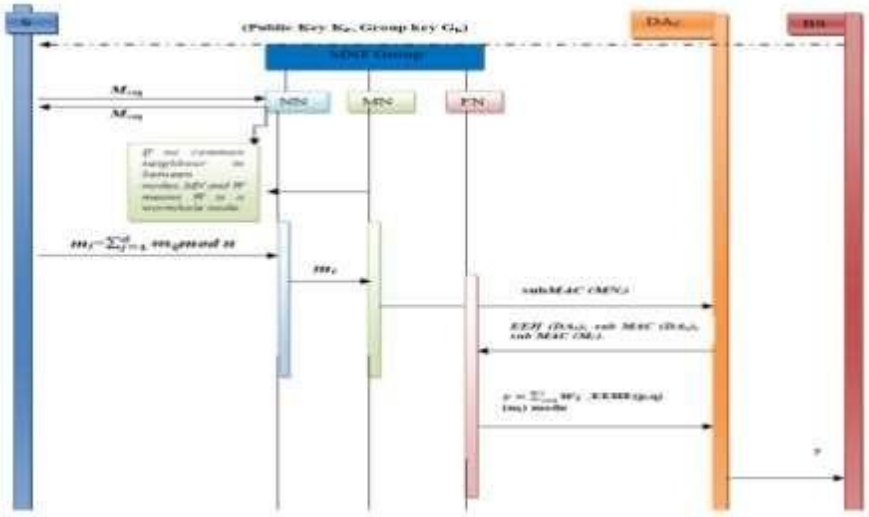

Figure 3- Timing diagram of the proposed work[14]

CONCLUSION

In this paper, a technique is described that ensures confidentiality in data fusion between a transmitter and receiver and also identifies wormhole threats on a specific node utilizing the shared neighbours table. In the proposed protocol, a common neighbor table is created in order to perform an integrity check and detect a wormhole. Due to the overhearing property of wireless communication, common neighbours between a sender and a receiver decide whether the receiver is a wormhole or not. Thus, there are fewer chances of false positive results. The identification and removal of all wormhole nodes in the network are also discussed in the proposed protocol. An EEHE technique is used for achieving end-to-end confidentiality of the aggregated data. The proposed scheme requires less energy compared with the protocol, and there are fewer chances of false positives. The key features of the SDT technique are that it does not require any guard nodes or special hardware, and there is no data loss owing to wormhole events.

REFERENCES

[1]. Singh, S.; Verma, H.K. Security for Wireless Sensor Network. Int. J. Comput. Sci. Eng. 2022, 3, 2393–2396. [CrossRef]

[2]. Fasolo, E.; Rossi, M.; Widmer, J.; Zorzi, M. In-Network Aggregation Techniques for Wireless Sensor Networks: A Survey. IEEE Wirel. Commun. 2023, 14, 70–87. [CrossRef]

[3]. Znaidi, W.; Minier, M.; Babau, J.P. Detecting wormhole attacks in wireless networks using local neighborhood information. In Proceedings of the IEEE Personal, Indoor and Mobile Radio Communications (PIMRC), Cannes, France, 15–18 September 2022; pp. 1–5.

[4]. Othman, S.B.; Bahatta, A.A.; Trad, A.; Habib, Y. Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption. Wirel. Pers. Commun. 2023, 80, 867–889. [CrossRef]

[5]. Jaydip, S. Homomorphic Encryption: Theory & Application. In Theory and Practice of Cryptography and Network Security Protocols and Technologies; Sen, J., Ed.; Intech Publishers: Rijeka, Croatia, 2022; pp. 1–21.

[6]. Sun, H.; Lin, Y.; Hsiao, Y.; Chen, C. An efficient and verifiable concealed data aggregation scheme in wireless sensor networks. In Proceedings of the ICESS08, Chengdu, China, 29–31 July 2023; pp. 19–26.

[7]. Westhoff, D.; Girao, J.; Acharya, M. Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption key distribution and routing adaptation. IEEE Trans. Mob. Comput. 2022, 5, 1417–1431. [CrossRef]

[8]. Perrig, A.; Szewczyk, R.; Tygar, D.; Wen, V.; Culler, D. SPINS: Security protocols for sensor networks. Wirel. Netw. J. 2023, 2, 521–534. [CrossRef]

[9]. Jangra, A. Wireless Sensor Network (WSN) architectural design issues and challenges (IJCSE). Int. J. Comput. Sci. Eng. 2022, 2,3089–3094.

[10]. Ozdemir, S.; Xiao, Y. Secure data aggregation in wireless sensor networks: A comprehensive overview. Comput. Netw. 2009, 53, 2023. [CrossRef]

[11]. Bharathi L et. al “Burst rate based optimized IO queue management for improved performance in Optical Burst Switching Networks” IEEE International Conference on Advanced Computing & Communication Systems (ICACCS), 2019

[12]. Ozdemir, S.; Çam, H. Integration of False data detection with data aggregation and confidential transmission in WSN. IEEE/ACM Trans. Netw. 2022, 18, 736–749.

[13]. Ozdemir, S.; Yang, X. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. Comput. Netw.2023, 55, 1735–1746.

[14]. [14]. Li, H.; Lin, K.; Li, K. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks. Comput. Commun.2022, 34, 591–597.
[15]. L.Bharathi, R. Sasikala and A.Srinivasan, "Adaptive Burst Assembly Algorithm for Reducing Burst Loss and Delay in OBS Network", Asian Journal of Information Technology, ISSN 1682 3915 Volume 13, pp. 2123 – 2132, 2016
[16]. Zhou, Q.; Yang, G.; He, L. A secure-enhanced data aggregation based on ECC in wireless sensor networks. Sensors 2023, 14,6701–6721. [CrossRef]
[17]. Li, X.; Chen, D.; Li, C.; Wang, L. Secure Data Aggregation with Fully Homo-morphic Encryption in Large-Scale Wireless SensorNetworks. Sensors 2022, 15, 15952–15973. [CrossRef] [PubMed]
[18]. Sanjay Kumar Suman, Dhananjay Kumar and L. Bhagyalakshmi, "Non Cooperative Power Control Game with New Pricing for Wireless Ad hoc Networks", International Review on Computers and Software, vol. 9, no. 1, pp. 18-28, 2014. ISSN: 1828-6003,
[19]. S. Porselvi, Sanjay Kumar Suman and L. Bhagyalakshmi, "Harvesting RF energy for mobile charging", Australian Journal of Basic and Applied Science, vol. 9, no. 20, pp. 454-465, June 2015.
[20]. K. Swapna, P. Rajalakshmi and Sanjay Kumar Suman, "Security Enhancement in MANET using Game Theory", Middle East Journal of Scientific Research, vol. 23, pp. 190-195, 2015.
[21]. Sujeetha Devi, Bhagyalakshmi L and Sanjay Kumar Suman, "Cluster based energy efficient joint routing algorithm for delay minimization in wireless sensor networks", International Journal of Pure and Applied Mathematics, vol. 119, no. 15, 307-313, 2018
[22]. Sujeetha Devi, Bhagyalakshmi L and Sanjay Kumar Suman, "Enhancing the Performance of Wireless Sensor Networks through Clustering and Joint Routing with Mobile Sink", International Journal of Engineering and Advanced Technology, vol. 8, issue 6, pp. 323-327, 2019. https://doi.org/10.35940/ijeat.E7664.088619
[23]. L. Bhagyalakshmi, Sanjay Kumar Suman, S. Mohanalakshmi, and Satyanand Singh, "Improving Spectral Efficiency and Coverage Capacity of 5G Networks: A Review", Advances in mathematics: scientific journal, vol.9, no. 6, pp. 3387-3397, 2020. https://doi.org/10.37418/amsj.9.6.19
[24]. L.Bharathi, R. Sasikala and A.Srinivasan, "Hybrid Method for a Reliable Buffer less OBS Network with Reduced End-To-End Latency and Burst Drop", International Journal of Operational Research, 2020 Vol.37 No.2, pp.220 – 244.
[25]. Tan H.; Ostry, D.; Zic, J.; Jha, S. A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor networks. In Proceedings of the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16–19 March 2023;pp. 245–252.
[26]. Bharathi .L et.al "Attribute Table based Energy-Efficient and QoS-of Multipath Routing Protocol Using in Loss-Free Optical Burst Switching Networks", Jour. of Adv Research in Dynamical & Control Systems, Vol. 11, 06-Special Issue, 2019.