DOI: 10.15849/IJASCA.230720.12

Int. J. Advance Soft Compu. Appl, Vol. 15, No. 2, July 2023
Print ISSN: 2710-1274, Online ISSN: 2074-8523
Copyright © Al-Zaytoonah University of Jordan (ZUJ)

Man-In-The Middle Attack Detection Scheme on Data Aggregation in Wireless Sensor Networks

Mohammad Ibrahim Adawy, Muhannad Tahboush, Osama Aloqaily, Waleed Abdulraheem

Faculty of Information Technology Department
The World Islamic Science & Education University
Amman, Jordan

E-mail: mohammad.adawi@wise.edu.jo

Abstract

Wireless Sensor Networks (WSNs) consist of small devices, sensors, which are deployed densely and arbitrarily in monitoring areas to gather information. Typically, the same event might be reported by many sensors, which causes a higher consumption rate of its energy due to sending redundant data. To resolve the energy problem in WSN, data aggregation is recommended in the literature. Nevertheless, aggregated data is subject to malicious interference (i.e., Man in The Middle attack (MITM)). In later vulnerability, the compromised node allows the adversary to change the original data and send it to the Cluster Head (CH), which leads to incorrect results at Base Station (BS). This paper studied the security issue of data aggregation and proposed an enhanced Aggregation Scheme, namely, the Secure Data Aggregation Scheme (SDAS), which detects Man-in-The Middle Attacks on aggregated data and ensures the accuracy and integrity of aggregated data. The primary purpose of proposed scheme is to ensure that the BS will receive accurate aggregated data. OMNeT++ simulator has been used to perform an experimental study and obtain the results. The results show that the proposed scheme effectively helps both Cluster Members CMs and CHs nodes to consume less energy, to detect malicious nodes, to maintain the accuracy of aggregated data by up to 90%, and finally, it is significantly suitable for several monitoring applications.

Keywords: *Wireless sensor network; data aggregation; Man-in-The Middle Attack; Cryptographic; Integrity; Accuracy.*

1 Introduction

Wireless sensor networks (WSNs) consist of small devices, that can communicate together wirelessly and collect data from surrounding coverage areas [1], [2], [3]. WSN has been used in many applications, including monitoring systems such as target monitoring, fence monitoring, environment monitoring, security monitoring, and agricultural monitoring [4], [5]. The sensor node is typically equipped with a small battery, limited processor, small memory, and limited communication capabilities [6], [7]. In this regard, sensor nodes are prone to failure and death due to low battery energy [8], [9]. Furthermore, the sensor nodes might be deployed densely and randomly [10], [11], [12] in unattended and hostile environments [13], [14]. In such an environment, the sensor nodes are vulnerable to deliberate security attacks [15], [16] [17], [18] by attackers, which results in sending false data [19], [20]. Security in WSN is a crucial aspect of a wide range of applications [18], [21], and [22].

Sensor nodes are grouped in clusters. Each cluster has a Cluster Head (CH) and Cluster Members (CMs) [23]. Many CM nodes might simultaneously sense the same event and send redundant data packets to the CH node [24], [25],[26]. Consequently, the CM nodes will spend a lot of energy when they transmit redundant data packets to the CH [27], [28], [29]. One of the essential approaches to removing the redundant data in clustered WSN is data aggregation [30], [31]. In this matter, the CH node performs data aggregation, which reduces the energy of transmitting redundant data [24], [32], [33],[34], [35]. The performance of the data aggregation can be measured by numerous criteria, such as energy consumption, data forwarding delay, end-to-end loss rate, and accuracy [36], [37]. Nevertheless, data aggregation adds more vulnerability by compromised nodes, which may send false data to aggregator nodes [19], [13], [38]. Moreover, two conventional cryptographic algorithms can be applied to secure data aggregation in WSN: end-to-end encrypted data aggregation and hop-by-hop encrypted data aggregation [39], [40]. Also, many researchers proposed using Elliptical Curve Cryptographic (ECC) technique to secure data aggregation and using Symmetric Keys (SK) to reduce the computational overhead related with ECC [22], [41]. On other hand, it is infeasible to implement only traditional cryptographic algorithms in each individual node, due to high consumption of node's energy and increase communication overhead [17], [42], [43]. Hence, it is essential to balance between data aggregation performance and data aggregation security.

In this paper has the following contribution: First, propose a Secure Data Aggregation Scheme (SDAS) that detects Man-in-The Middle attacks and ensures the accuracy and integrity of aggregated packets until they reach the Base Station (BS). Second, formulate the equations that validate the proposed model. Finally, conduct intensive simulations to present the effectiveness of SADS in reducing consumed energy at both CMs and CHs, detect the Man in the middle attack, and ensure the accuracy and integrity of aggregated packets. This reminder of this paper is organized as follows: Section 2, summarized the related works in secure data aggregation. Section 3 formulates the proposed system model. Section 4 presents the proposed SDAS scheme. Section 5, explain the simulation environment, performance analysis, and results of the proposed SDAS. The conclusions of this research are presented in Section 6.

2 Related Work

Several previous works focused on data aggregation performance and security. The study in [16] proposed a scheme that helps to secure data aggregation. A study [19] proposed a secure and energy-efficient data aggregation scheme that can detect malicious nodes and does not allow them to send forged data to BS. The scheme depends on the homomorphic encryption algorithm employed in CM nodes and sends encrypted packets to the CH node. Without decrypting them, the Cluster Head aggregates the encrypted packets, which provides security to the aggregated packets, and sends it to BS. This scheme trades off between computation energy and security. However, the proposed scheme increased the consumed energy of CM nodes because of applying the homomorphic encryption algorithm in individual CM nodes. The study in [40] proposed a secure data aggregation scheme for private data using the LEACH protocol. The authors implemented hop by hop encryption algorithm in clustered WSN. Each CM node encrypts its data by adding an actual number with sensory reading and sends the collected data to the CH node. The received data is decrypted by the CH node. Moreover, the CH node encrypts the aggregated data and sends the encrypted packets to BS. The BS decrypts the results and extracts the correct aggregated data. Consequently, the scheme provides privacy during the data transmission of the node's data to BS. Still, encryption and decryption for each transmitted data packet increase energy consumption and communication overhead.

According to [17], To secure aggregated data Cluster Head runs data aggregation based on Bayesian fusion. A later algorithm measures the probability of the trustworthiness of each CM node, the CH node calculates the trust factor for each CM node in the cluster. Also, the CH node checks if the CM node has a lower trust probability and considers the malicious node. The simulation results show that the scheme effectively detects untrust nodes with minimum energy consumption. Still, the CH node consumes much energy due to implementing data aggregation and calculates trust probability for each CM node in this scheme, quickly prone it to death. The authors of [13] proposed a "Secure Protocol and Energy-Efficient for Data Aggregation in Wireless Sensor Networks (SPEEDA)" scheme. In their work, each Cluster Head collects data about events from Cluster Members in addition to the transmission date, identification number, and Message Authentication Code (MAC), which verifies the authentication and integrity of transmitted data. MAC is calculated from the shared key for a set of CM nodes by CH node. Moreover, the scheme uses a symmetric encryption method based on MAC. The receiver computes the Message Authentication Code using the given key. If the computed key and received key is similar, the CM source node is authenticated, and the data is stored. Otherwise, the CM source is suspended, and the packet is marked as corrupt.

In [22], researchers proposed a new method based on lossless data aggregation in WSN using Argument Chinese Reminder System (ACRS). ACRS provides signature verification and removes data validation from the separated algorithms. The ACRS method provides data encryption to accomplish data integrity and authentication at the same time as well as to data aggregation. The BS node broadcasts a secret key for each node within WSN and sends a copy of these keys for each CH node. The secret keys are used to aggregate and encrypt data received from CM nodes. The CM nodes send their data packets during their time slot in a TDMA cyclic to the CH node. The implementation of the offsetting and scaling process can be applied to the CM or CH nodes. The scale and offset factors are obtainable to BS in the initialization time. The ACRS function aggregates the received packets of each CM node with the corresponding secret key, encrypts packets, and sends the encrypted packet to BS. In comparison to the Merkle Hash Tree aggregation method [22], results confirm that the proposed ACRS method consumes less energy is more quicker. The study in [18] proposed a five phases scheme called "Secure Cluster-based Data Aggregation Protocol (SCDAP)". In the first phase, public and private keys are generated using the Diophantine Power algorithm. In the network clusters phase, the BS selects the CHs based on remaining energy, throughput, and distance among the neighbor's nodes, whereas it implements the N-means algorithm to form clusters. Also, in the secure data aggregation, all Cluster Members send sensory data to their associated Cluster Head. After receiving data from Cluster Heads, Aggregation Cluster Head (ACH) aggregates, encrypts, and sends results to the BS.

3 System Model

In this section, the resources constrain on sensor nodes are considered. Therefore, symmetric cryptography is used to reduce the energy consumption of the nodes. Nodes will encrypt the data with a set of keys whose size is acceptable for the WSN.

3.1. Network Model

WSN is formed by a set of clusters. One CH and many CMs from each cluster. the following assumptions are considered in our system:

1. Sensors are homogenous and randomly deployed in the simulation area.
2. Sensors are stationary and have fixed positions.
3. The sensors are grouped into clusters denoted by C:

$$C= \{C_1, C_2, ..., C_m). \tag{1}$$

4. Each cluster has a set of CMs node and one CH node:

$$CM = \{CM_1, CM_2, ..., CM_n\}. \tag{2}$$

5. Assume that each CM_i node within cluster C_i has the same transmission range and same sensing range.
6. Assume that single-hop communication is used between CM_i and CH in cluster C_i, and The CHs and BS.
7. Assume that the event randomly appears within the cluster in which the data event is composed of environmental parameters such as temperature, humidity, and light density.
8. The BS consider laptop or server without constrains on its resources.
9. The radio channel is symmetric as in [44].
10. Symmetric encryption used in [13] is employed here to encrypt packets.
11. BS has a set of random numbers RN.
12. Each CH node has a set of random keys K.
13. It assumes the data event for node CM_i is D_i.
14. The cluster's random number of CM nodes is used between the CH node and BS to encrypt and decrypt the aggregation data.
15. The CM_i node collects data event D_i and sends data packet P_{Di} periodically to the CH node.
16. Each data packet P_{Di} has sequence number $Sq_{i.}$
17. It assumes that Man-in-the middle attack occur between CM_i and CH node, where each compromised CM_i node sends its data packet to the attacker. The attacker may drop the packet or change its content and then forward it to the CH node.
18. It is assumed that the encryption method with the random number for CM_i denotes EncNRi (D_i).

3.2 Energy Model

The first radio model by Heinzelman, Chandrakasan, and Balakrishnan [45] represents the energy consumption in the components of the sensor node in transmission and receiving operations. E_{elec} is the energy dissipated to run the transmitter or the receiver circuit for one bit, and E_{emp} is the energy dissipated by the transmission amplifier for one bit in the one-meter square (m^2).

$$E_{TX}(k, d) = (E_{elec} {}_* k) + (E_{emp} * k * d^{\alpha}) \tag{3}$$

$$E_{RX}\left(k\right) = \left(E_{elec} * k\right) \quad (4)$$

where

E_{TX} *(k, d)* is the energy dissipated to transmit k bits.
E_{TX} *(k)* is the energy dissipated to receive k bits.
α is exponential loss and it is equal 2 in this research

4 Secure Data Aggregation Scheme

In the proposed SDAS, we have four packets that are transmitted within WSN: Table 1 shows the packet types.

Table 1: Data Packet Types

Packet	Description
P_{BS}	Contains the random Numbers (RN_i)
P_{CH}	Contains the random key (k_i)
P_{N_i}	a notification packet that contains the RN_i and k_i for CMi node.
P_{RTS}	Is requested to send packet
P_{D_i}	Contains sensory data D_i , Totali and packet sequence (Sq_i) for CMi node.

Where

$$Total_i = RN_i + K_i + Sq_i \quad (5)$$

The SDAS contains three phases:

<u>Phase 1</u>: Random numbers and random keys distribution:

1- The BS sends a packet (P_{BS}) that contains Random Number (RNi) to each sensor node within WSN before forming clusters:

$$RN_i = \left\{RN_1,\ RN_2,\ \ldots,RN_N\right\} \quad (6)$$

RN_i is chosen as a non-repeated random number.

2- The CH node sends a packet (P_{CH}) that contains the Random key (k_i) to each CM node in its cluster after clusters are formed:

$$k_i = \{k_1, k_2, \ldots, k_N\} \tag{7}$$

k_i is chosen as a non-repeating random number.

Phase 2: Transmitted data from CM nodes to CH node without implementing cryptography method:

1- CMi node collects data events and notifies the CH node about having data by sending Notify packet (P_{N_i}).

2- The CH node receives notify packet and sends Request to Send packet (P_{RTS}) to the CMi node.

3- Each CMi node transfers its data packet (P_{D_i}) to the CH node after a receiving request to send the packet (P_{RTS}).

4- The CH node computes the integrity of the data packet using the following equation for each received data packet (P_{D_i}):

$$Integrity\ P_{D_i} = Total_i - \left(RN_i + K_i + Sq_i\right) \tag{8}$$

5- The CH node checks the integrity of each data packet P_{D_i} :

$$\left\{\begin{array}{ll} \mathrm{P_{D_i} is\ correct;} & \mathrm{Integrity}\ \mathrm{P_{D_i}} == \mathrm{zero} \\ \mathrm{P_{D_i} is\ corrupted;} & \mathrm{Else} \end{array}\right\} \tag{9}$$

6- The CH node combines or aggregates correct data events from two or more different data packets such as P_{D_i} and P_{D_j} using one of the aggregation functions, we use the sum as shown in the following equation:

$$D_{i,j} = D_i + D_j \tag{10}$$

Phase 3: Transmitting encrypted aggregated data from CH node to BS:

1- The CH node encrypts the aggregated data $\left(D_{i,j}\right)$ by a symmetric algorithm using $RN_{i,j}$ as a secret key:

$$RN_{i,j} = RN_i + RN_j \tag{11}$$

$$Enc_{RNi,j}\left(D_{i,j}\right) \tag{12}$$

$$Cipher_{i,j} = Er\left(D_{i,j}\right) \tag{13}$$

2- The CH node send encrypted data $Cipher_{i,j}$ to BS which computes $RN_{i,j}$

3- The BS decrypt aggregated data by using $RN_{i,j}$ a secret key:

$$Drc_{RN\ i,j}\left(Cipher_{i,j}\right) \tag{14}$$

Figure.1 shows the SDAS proposed Scheme flowchart.

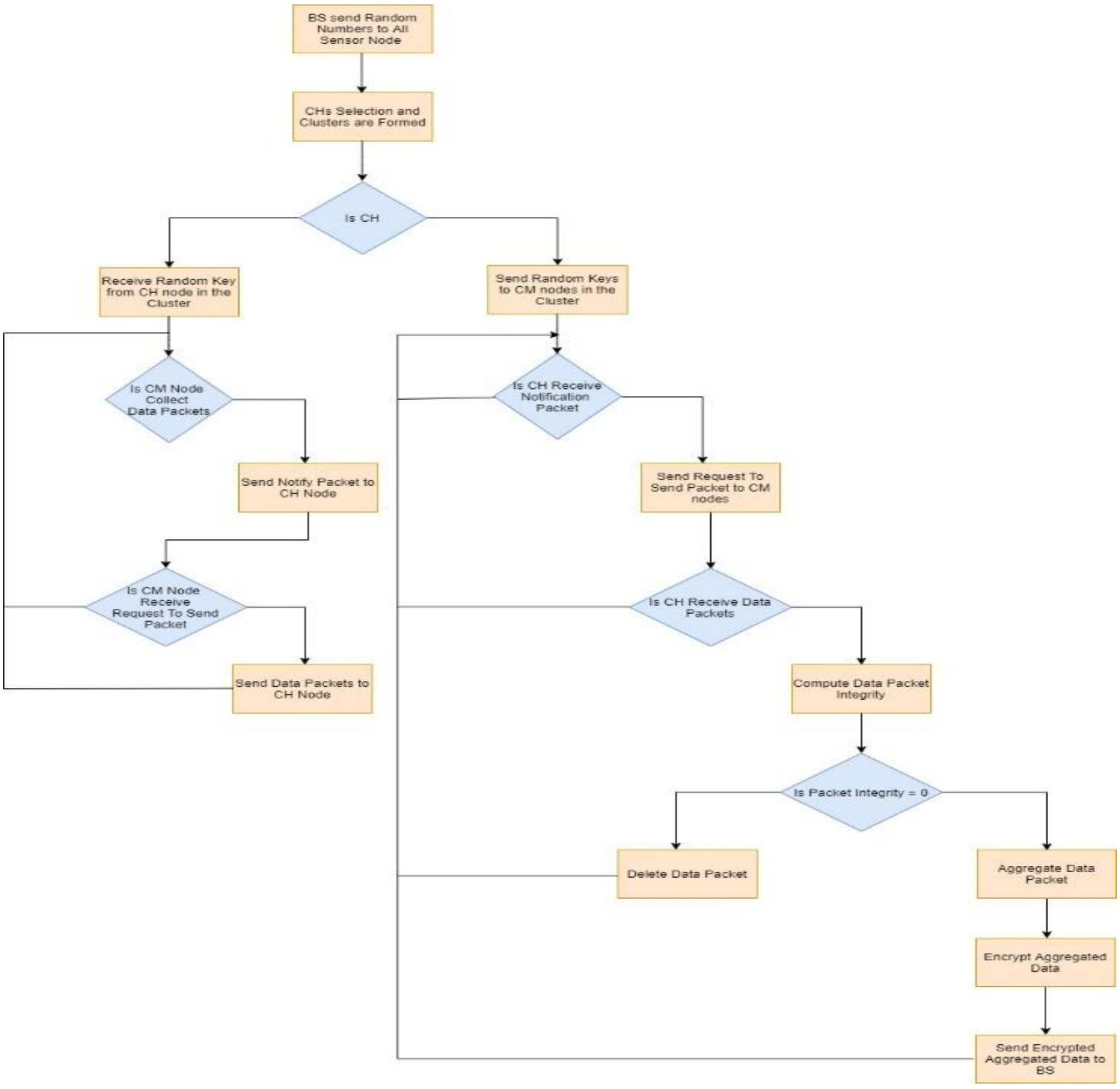
BS send Random Numbers to All Sensor Node
CHs Selection and Clusters are Formed
Is CH
Receive Random Key from CH node in the Cluster
Send Random Keys to CM nodes in the Cluster
Is CM Node Collect Data Packets
Is CH Receive Notification Packet
Send Notify Packet to CH Node
Send Request To Send Packet to CM nodes
Is CM Node Receive Request To Send Packet
Is CH Receive Data Packets
Send Data Packets to CH Node
Compute Data Packet Integrity
Is Packet Integrity = 0
Delete Data Packet
Aggregate Data Packet
Encrypt Aggregated Data
Send Encrypted Aggregated Data to BS

Fig 1: Proposed SDAS Scheme

5 Results analysis, and Discussions

OMNet++ network simulator is used to simulate the proposed SDAS scheme. Table 2 demonstrates the simulation parameters used. it will assume that number of CM nodes in the cluster is 10 nodes, and all of them detect the same event within the cluster. Figure 2 shows the simulation topology using OMNeT++.

Table 2: OMNet++ Simulation Parameters

Parameter	Value
Area of WSN	1100m * 600m
Transmission Range	1200 m
CH Node Initial Energy	50 J
CM Node Initial Energy	50 J
Transmission Energy Consumption for Each byte	0.1 uJ
Number of Nodes	10, 15, 20, 25, 30
Simulation Time	70 Seconds

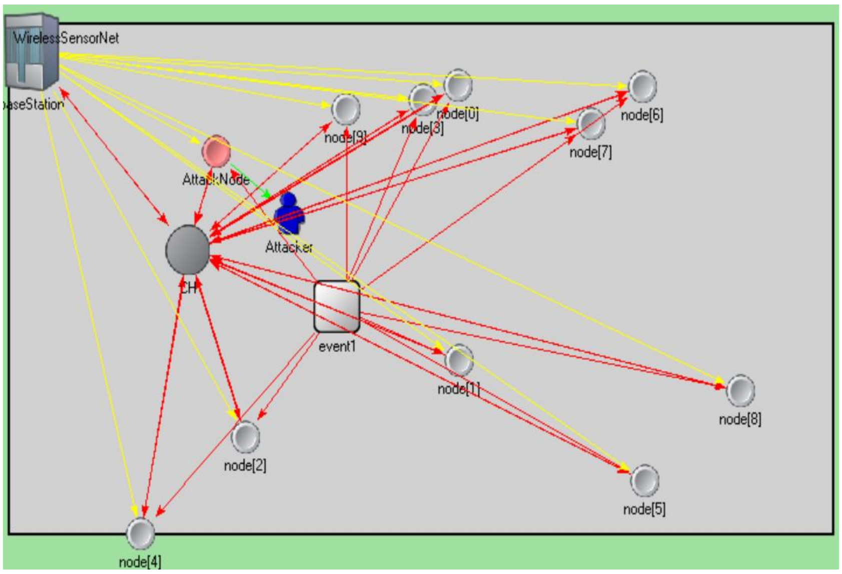

Fig 2: OMNeT ++ Running Proposed Scheme

1) Aggregation Accuracy: The CM node sends its data packet to the CH node. The CH node checks if the data packet is corrupted or not. The CH node deletes the corrupted data packets and aggregates the data event in the correct data packets. We calculate the aggregated data accuracy based on the Packet Delivery Ratio (PDR) which is the number of received data packets by the CH node to the number of the data packet transmitted from CM nodes within the cluster.

2) Integrity: The CH node can distinguish between the correct and corrupted data packets by examination of each data packet's integrity. Also, the CH node encrypts the aggregated data by using random numbers that are given to CMs and sends the cipher of aggregated data to the BS.

3) Energy Consumption: we calculate the energy consumption from CH node due to performing the data aggregation and encryption process. Also, we calculate the total energy consumption from CM nodes within the cluster.

5.1 Simulation Results

In Figure 2, illustrates the simulation topology, which consists of 10 CM nodes, and one attacked node. The malicious node can receive all packets within its transmission range, any data packet transmitted to the CH will be interfered with by the attacker. The attacker alters the content of the packets and forwards them to the CH node. During OMNeT++ simulation, it is important to calculate the consumed energy during the data aggregation and encryption process.

Table 3: OMNet++ Simulation Results for 10 Nodes

Node id	$Total_i$	k_i	RN_i	Sq_i	*Integrity* P_{D_i}
0	190	3	5	1	181
1	44	35	8	1	0
2	69	64	4	1	0
3	99	95	3	1	0
4	77	69	7	1	0
5	100	94	5	1	0
6	6	0	5	1	0
7	51	50	0	1	0
8	38	36	1	1	0
9	40	34	5	1	0

Table 3 reveals the results of proposed SDAS for a cluster of 10 nodes. The malicious node is node 0, with random keys 3, and 5 random numbers therefore the integrity of data packet is not equal to zero. The attacker alters all data packets sent from node 0 to CH. Consequently, upon reception of corrupted packets, the CH identifies that packet is corrupted because of the integrity value. In this case, the CH node ignores the corrupted packet and aggregates other correct packets. After that, the CH encrypt aggregated data based on the received random number from the CM nodes and send the aggregated data to BS. In the BS, a decryption process for the received packet is performed.

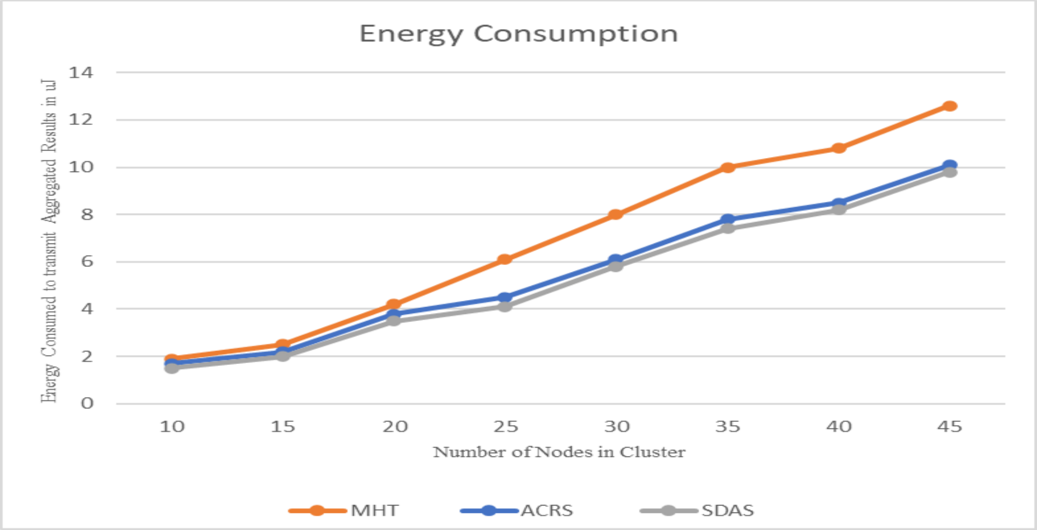

Figure 3: Energy Consumption for MHT, ACRS, and Proposed SDAS Scheme

Figure 3 presents the energy consumption of the transmit aggregation packets sent from the CH node using three schemes: Merkle Hash Tree (MHT), Argument Chinese Reminder System (ACRS), and our proposed SDAS. The results show that the proposed SDAS consumes less energy than the other schemes. Hence, the proposed SDAS is appropriate for data aggregation in clustered WSNs, where energy consumption is the main limitation.

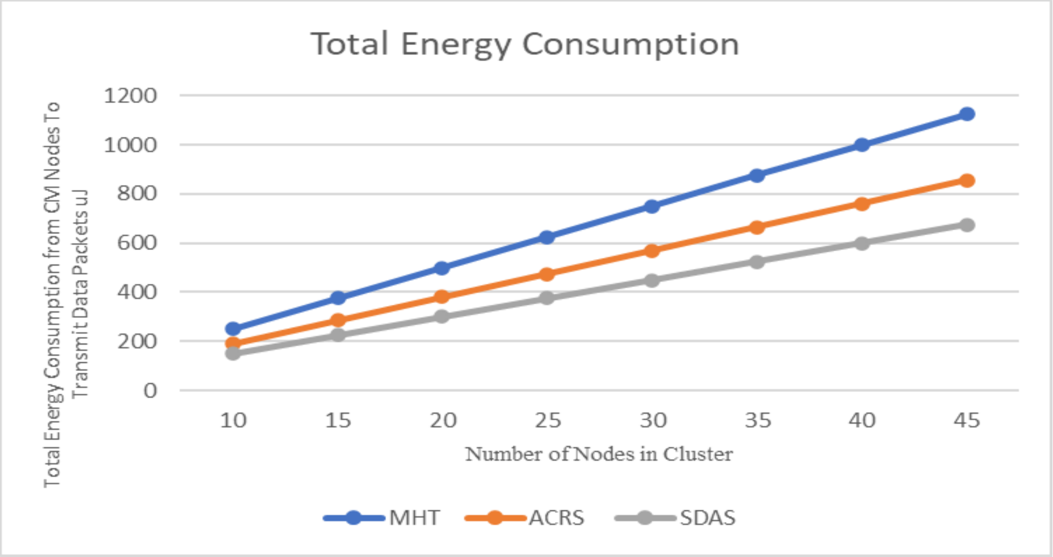

Figure 4: Total Energy Consumption from CM nodes to Transmit Data for MHT, ACRS, and Proposed SDAS Scheme

Figure 4 presents the total energy consumption from CM nodes in MHT, ACRS, and SDAS. The proposed SDAS significantly improves the cluster's total energy consumption of CM nodes. That significant improvement is due to data packets transmitted to the CH node without an encryption process.

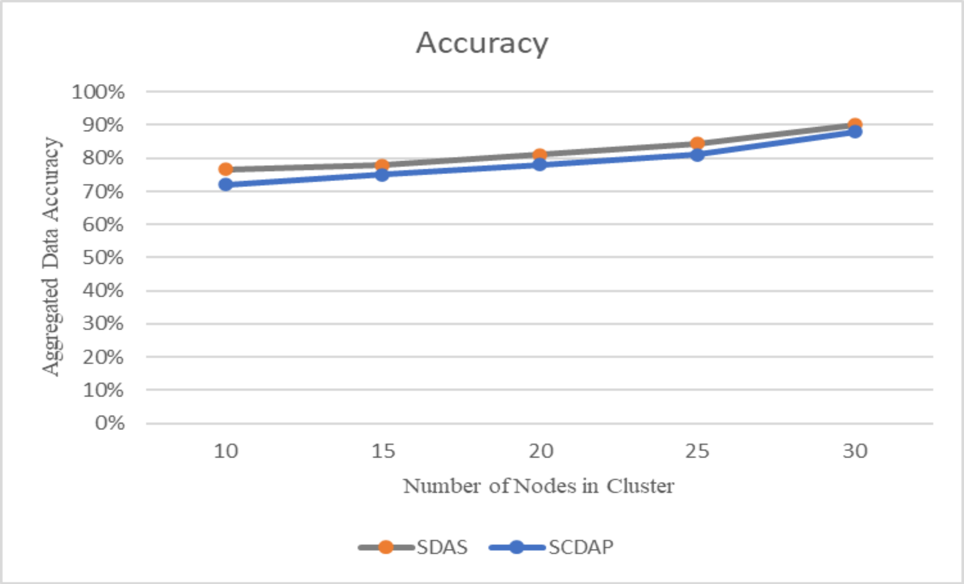

Figure 5: Aggregation Accuracy for SCDAP and SDAS Proposed Schemes

In Figure 5 shows the simulation results of aggregated data accuracy reaching approximately 90% when the number of nodes is 30. In contrast, the accuracy is 85% when the number of nodes equals 25 nodes within the cluster. Consequently, the accuracy increases when the number of nodes is increased due to the number of regular nodes being increased compared with the number of malicious nodes. Also, the figure shows the proposed SDAS achieves aggregated data accuracy more than SCDAP. Thus, the proposed SDAS is significantly suitable for data aggregation in clustered WSNs.

6 Conclusion

In Wireless Sensor Network (WSN), The sensor nodes are randomly deployed in unwanted and hostile environments. Thus, the sensor nodes may closely situate from each other. This led to collecting the same data event and producing redundant data packets. The sensor nodes consume a lot of energy to send redundant data. Thus, data aggregation is a crucial in-network process that decreases energy consumption from sensor nodes. In clustered WSN, data aggregation can be exposed to further vulnerabilities by a compromised node letting the Man-In-The Middle attacker add corrupted data and send it to the Cluster Head (CH). This causes the CH node to produce and send false aggregated results to Base Station (BS). This paper addresses data aggregation with security issues by proposing a new Secure Data Aggregation Scheme (SDAS) that detects Man-in-The Middle Attacks and ensures aggregated results' accuracy and integrity until they reach BS. The results show that the proposed SDAS effectively detects malicious nodes and keeps the integrity of aggregated results. Also, the proposed SDAS exposes the maintenance of aggregated data accuracy when malicious nodes exist and send corrupted data packets to the CH node. Consequently, the proposed scheme considers both the energy consumption of aggregated data and encryption with security requirements such as aggregated integrity.

References

[1] A. Chowdhury and D. De, “Energy-efficient coverage optimization in wireless sensor networks based on Voronoi-Glowworm Swarm Optimization-K-means algorithm,” *Ad Hoc Networks*, vol. 122, no. July, p. 102660, 2021, doi: 10.1016/j.adhoc.2021.102660.

[2] S. Kaur and R. Naaz Mir, “Clustering in Wireless Sensor Networks- A Survey,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 8, no. 6, pp. 38–51, 2016, doi: 10.5815/ijcnis.2016.06.05.

[3] N. M. Zamry, A. Zainal, and M. A. Rassam, “Unsupervised anomaly detection for unlabelled Wireless Sensor Networks Data,” *Int. J. Adv. Soft Comput. its Appl.*, vol. 10, no. 2, pp. 172–191, 2018.

[4] S. Taruna and M. R. Tiwari, “An Event Driven Energy Efficient Data Reporting System for Wireless Sensor,” *Int. J. Eng. Res. Technol.*, vol. 2, no. 2, pp. 1–9, 2013.

[5] A. Khalifeh, K. Rajendiran, K. A. Darabkh, A. M. Khasawneh, O. Almomani, and Z. Zinonos, “On the potential of fuzzy logic for solving the challenges of cooperative multi-robotic wireless sensor networks,” *Electron.*, vol. 8, no. 12, 2019, doi: 10.3390/electronics8121513.

[6] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Comput. Networks*, vol. 52, no. 12, pp. 2292–2330, 2008, doi: 10.1016/j.comnet.2008.04.002.

[7] G. M. Abdulsahib and O. I. Khalaf, “An Improved Cross-Layer Proactive Congestion in Wireless Networks,” *Int. J. Adv. Soft Comput. its Appl.*, vol. 13, no. 1, pp. 178–192, 2021.

[8] D. C. Mocanu, M. T. Vega, and A. Liotta, “Redundancy Reduction in Wireless Sensor Networks via Centrality Metrics,” in *Proceedings - 15th IEEE International Conference on Data Mining Workshop, ICDMW 2015*, 2016, no. November 2015, pp. 501–507, doi: 10.1109/ICDMW.2015.53.

[9] S. Randhawa and S. Jain, “Data Aggregation in Wireless Sensor Networks: Previous Research, Current Status and Future Directions,” *Wireless Personal Communications*, vol. 97, no. 3. pp. 3355–3425, 2017, doi: 10.1007/s11277-017-4674-5.

[10] M. N. Khan *et al.*, “Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks,” *IEEE Access*, vol. 8, pp. 176495–176520, 2020, doi: 10.1109/ACCESS.2020.3026939.

[11] R. Rajagopalan and P. K. Varshney, “Data-aggregation techniques in sensor networks: A survey,” *IEEE Commun. Surv. Tutorials*, vol. 8, no. 4, pp. 48–63, 2006, doi: 10.1109/COMST.2006.283821.

[12] P. Padmaja and G. V. Marutheswar, “Energy efficient data aggregation in wireless sensor networks,” *Mater. Today Proc.*, vol. 5, no. 1, pp. 388–396, 2019, doi: 10.1016/j.matpr.2017.11.096.

[13] S. Wayzani and C. Diallo, “SPEEDA: A Secure Protocol and Energy Efficient for Data Aggregation in Wireless Sensor Networks,” *Int. J. Eng. Technol.*, vol. 7, no. 4.20, p. 598, 2018, doi: 10.14419/ijet.v7i4.20.27422.

[14] M. Gupta, O. Almomani, A. M. Khasawneh, K. A. Darabkh, and others, “Smart remote sensing network for early warning of disaster risks,” in *Nanotechnology-Based Smart Remote Sensing Networks for Disaster Prevention*, Elsevier, 2022, pp. 303–324.

[15] M. Adil, M. A. Almaiah, A. O. Alsayed, and O. Almomani, “An anonymous channel

categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors (Switzerland)*, vol. 20, no. 8, pp. 1–19, 2020, doi: 10.3390/s20082311.

[16] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," *SenSys'03 Proc. First Int. Conf. Embed. Networked Sens. Syst.*, pp. 255–265, 2003.

[17] S. Ranjani and Radhakrishnan, "Data Aggregation in Cluster based Wireless Sensor Networks," in *International Conference on Science, Engineering and Management Research*, New Delhi: Springer India, 2014, pp. 391–400.

[18] G. Lavanya, B. L. Velammal, and K. Kulothungan, "SCDAP –secured cluster based data aggregation protocol for energy efficient communication in wireless sensor networks," *J. Intell. Fuzzy Syst.*, pp. 1–10, 2022, doi: 10.3233/jifs-223256.

[19] S. Ben Othman, A. Trad, H. Alzaid, and H. Youssef, "Secure and energy-efficient data aggregation for wireless sensor networks," *Int. J. Mob. Netw. Des. Innov.*, vol. 5, no. 1, pp. 28–42, 2013, doi: 10.1504/IJMNDI.2013.057146.

[20] K. Hemapriya, "SDA-seech : Secure data aggregation using seech algorithm in wireless sensor networks," vol. 6, no. April, pp. 12170–12183, 2022.

[21] G. G. Gebremariam, J. Panda, and S. Indu, "Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using Artificial Neural Network," *Wirel. Commun. Mob. Comput.*, vol. 2023, 2023, doi: 10.1155/2023/2744706.

[22] S. Thomas and T. Mathew, "Secure Data Aggregation in Wireless Sensor Network using Chinese Remainder Theorem," *Int. J. Electron. Telecommun.*, vol. 68, no. 2, pp. 329–336, 2022, doi: 10.24425-ijet.2022.139886/983.

[23] M. Raju and K. P. Lochanambal, "An Insight on Clustering Protocols in Wireless Sensor Networks," *Cybern. Inf. Technol.*, vol. 22, no. 2, pp. 66–85, 2022, doi: 10.2478/cait-2022-0017.

[24] B. Sepehr, "Adaptive Clustering and Data Aggregation in Wireless Sensor Networks (ACDA)," University of Guelph, 2013.

[25] J. Shih, H., Chu, Sh., Roddick, J., Ho, J., Liao, B. & Pa., *A Reduce Identical Event Transmission Algorithm for Wireless Sensor Network*, vol. 179, no. 1. Verlag Berlin: Springer-Verlag Berlin Heidelberg 2013, 2011.

[26] J. H. Ho, H. C. Shih, B. Y. Liao, and J. S. Pan, "A Reduce Identical Composite Event Transmission Algorithm for Wireless Sensor Networks," *Appl. Math. Inf. Sci.*, vol. 6, no. 2S, pp. 713–719, 2012, [Online]. Available: http://www.naturalspublishing.com/Article.asp?ArtcID=518.

[27] M. I. Adawy, S. A. Nor, and M. Mahmuddin, "Data redundancy reduction in wireless sensor network," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, no. 1–11, pp. 1–6, 2018, [Online]. Available: journal.utem.edu.my/index.php/jtec/article/download/3841/2739.

[28] Z. Qu and B. Li, "An Energy-Efficient Clustering Method for Target Tracking Based on Tracking Anchors in Wireless Sensor Networks," *Sensors*, vol. 22, no. 15, 2022, doi: 10.3390/s22155675.

[29] S. V. Selvin and S. M. Kumar, "Tree Based Energy Efficient and High Accuracy Data Aggregation for Wireless Sensor Networks," *Procedia Eng.*, vol. 38, pp. 3833–3839, 2012, doi: 10.1016/j.proeng.2012.06.439.

[30] S. Siddiqui, A. A. Khan, and S. Ghani, "A Survey on Data Aggregation Mechanisms

in Wireless Sensor Networks," *Inf. Commun. Technol. (ICICT), 2015 Int. Conf.*, pp. 1–7, 2015, doi: 10.1109/ICICT.2015.7469596.

[31] K. Maraiya and K. Kant, "Architectural Based Data Aggregation Techniques in Wireless Sensor Network : A Comparative Study," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 3, pp. 1131–1138, 2015.

[32] D. Suresh and K. Selvakumar, "Double Cluster Head Based Reliable Data Aggregation for Wsn," *World Eng. Appl. Sci. J.*, vol. 6, no. 3, pp. 136–146, 2015, doi: 10.5829/idosi.weasj.2015.6.3.22229.

[33] M. Noori and M. Ardakani, "Lifetime Analysis of Random Event-Driven Clustered Wireless Sensor Networks," *IEEE Trans. Mob. Comput.*, vol. 10, no. 10, pp. 1448–1458, 2011, doi: 10.1109/TMC.2010.254.

[34] Nurhayati, "Re-cluster Node on Unequal Clustering Routing Protocol Wireless Sensor Networks for Improving Energy Efficient," *Int. J. Comput. Commun.*, vol. 6, no. 3, pp. 157–166, 2012, [Online]. Available: http://www.naun.org/cms.action?id=3058.

[35] A. Al-Baz and A. El-Sayed, "A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 31, no. 1, pp. 1–13, 2018, doi: 10.1002/dac.3407.

[36] J. Feng, "Performance of Data Aggregation for Wireless Sensor Networks," University of Saskatchewan Saskatoon, 2010.

[37] S. Sirsikar and S. Anavatti, "Issues of Data Aggregation Methods in Wireless Sensor Network: A survey," *Procedia Comput. Sci.*, vol. 49, no. 1, pp. 194–201, 2015, doi: 10.1016/j.procs.2015.04.244.

[38] M. Tahboush, M. Agoyi, and A. Esaid, "Multistage security detection in mobile ad-hoc network (MANET)," *Int. J. Eng. Trends Technol.*, vol. 68, no. 11, pp. 97–104, 2020, doi: 10.14445/22315381/IJETT-V68I11P213.

[39] M. A. Almaiah, A. Al-Zahrani, O. Almomani, and A. K. Alhwaitat, "Classification of cyber security threats on mobile devices and applications," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, Springer, 2021, pp. 107–123.

[40] A. Jangra, "Cb-SDA : Cluster-based Secure Data Aggregation for Private Data in WSN," *Wirel. Mob. Technol.*, vol. 1, no. 1, pp. 37–41, 2013, doi: 10.12691/wmt-1-1-7.

[41] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, Ahmad Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6461–6471, 2020, doi: 10.11591/IJECE.V10I6.PP6461-6471.

[42] A. Taghavirashidizadeh, A. B. Zarei, and A. Farsi, "Analysis of the attack and its solution in wireless sensor networks," *13th Int. Conf. Eng. Technol.*, pp. 1–8, 2019.

[43] Z. Xia, Z. Wei, and H. Zhang, "Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks," *Comput. Intell. Neurosci.*, vol. 2022, 2022, doi: 10.1155/2022/3449428.

[44] S. Lindsey and C. Raghavendra, "PEGASIS: Power efficient Gathering in sensor information systems," *Proceeding IEEE Aerosp. Conf.*, vol. 3, pp. 1125–1130, 2002, doi: 10.1109/AERO.2002.1035242.

[45] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2, no. c, pp. 1–10, 2000, doi: 10.1109/HICSS.2000.926982.

Mohammad Adawy received the Ph.D. degree in Computer networks and networks security. He is currently Dr at the Department of Information System and Networks, The World Islamic Sciences and Education University, Amman, Jordan. His research interests include Computer Networks, Wireless Networks, Wireless Sensor Networks and Networks Security**.**

Muhannad Tahboush received the Ph.D. degree in Cybersecurity from Cyprus International University. He is currently Dr at the Department of Information System and Networks, The World Islamic Sciences and Education University, Amman, Jordan. His research interests include network security, cryptography, and information security.

Osama I. Aloqaily received his B.S. degree in electrical and computer engineering from Yarmouk University, Jordan, in 2004, he received his M.A.Sc in Electrical and Computer Engineering form University of Ottawa, Canada, in 2016, where he is currently an assistant professor at the department of Networking Security in World Islamic Sciences and Education University. His current research interests include wireless sensor networks, AI, IoT and Smart Grid, and Network and Information Security.

Dr. Waleed Abdulraheem has received his B.S degree in computer and network from AOU Jordan, in 2012, M.S degree in computer and information security from MEU Jordan, in 2014, and Ph.D. in Cybersecurity from UPM Malaysia in 2019. His mater thesis was concentrating about cloud computing security and cryptography. While his Ph.D dissertation was related to lightweight cryptography. He is currently an Assistant Professor at the Information and network security and privacy department, with WISE University, Jordan. His research interests are cryptography, IoT security, Blockchain, network security, Human-Computer Interaction (HCI) and cloud computing security.