

Article

Secure Data Aggregation Using Authentication and Authorization for Privacy Preservation in Wireless Sensor Networks

Samuel Kofi Erskine ^{1,2} 

¹ College of Science and Technology, University of Bridgeport, Bridgeport, CT 06604, USA; serskine@my.bridgeport.edu

² Department of Computer Information Science, Florida A & M University, Tallahassee, FL 32310, USA

Abstract: Existing secure data aggregation protocols are weaker to eliminate data redundancy and protect wireless sensor networks (WSNs). Only some existing approaches have solved this singular issue when aggregating data. However, there is a need for a multi-featured protocol to handle the multiple problems of data aggregation, such as energy efficiency, authentication, authorization, and maintaining the security of the network. Looking at the significant demand for multi-featured data aggregation protocol, we propose secure data aggregation using authentication and authorization (SDAAA) protocol to detect malicious attacks, particularly cyberattacks such as sybil and sinkhole, to extend network performance. These attacks are more complex to address through existing cryptographic protocols. The proposed SDAAA protocol comprises a node authorization algorithm that permits legitimate nodes to communicate within the network. This SDAAA protocol's methods help improve the quality of service (QoS) parameters. Furthermore, we introduce a mathematical model to improve accuracy, energy efficiency, data freshness, authorization, and authentication. Finally, our protocol is tested in an intelligent healthcare WSN patient-monitoring application scenario and verified using an OMNET++ simulator. Based upon the results, we confirm that our proposed SDAAA protocol attains a throughput of 444 kbs, representing a 98% of data/network channel capacity rate; an energy consumption of 2.6 joules, representing 99% network energy efficiency; an effected network of 2.45, representing 99.5% achieved overall performance of the network; and time complexity of 0.08 s, representing 98.5% efficiency of the proposed SDAAA approach. By contrast, contending protocols such as SD, EEHA, HAS, IIF, and RHC have throughput ranges between 415–443, representing 85–90% of the data rate/channel capacity of the network; energy consumption in the range of 3.0–3.6 joules, representing 88–95% energy efficiency of the network; effected network range of 2.98, representing 72–89% improved overall performance of the network; and time complexity in the range of 0.20 s, representing 72–89% efficiency of the proposed SDAAA approach. Therefore, our proposed SDAAA protocol outperforms other known approaches, such as SD, EEHA, HAS, IIF, and RHC, designed for secure data aggregation in a similar environment.

Keywords: wireless sensor networks; secure data aggregation; authentication; authorization; time complexity; energy efficiency; privacy



Citation: Erskine, S.K. Secure Data Aggregation Using Authentication and Authorization for Privacy Preservation in Wireless Sensor Networks. *Sensors* **2024**, *24*, 2090. <https://doi.org/10.3390/s24072090>

Academic Editor: José I. Alonso

Received: 5 February 2024

Revised: 19 March 2024

Accepted: 22 March 2024

Published: 25 March 2024



Copyright: © 2024 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Wireless sensor networks (WSNs) can achieve transmission when the network senses data between a node and another set of sensor nodes (SNs). During data transmission in WSNs, sensed data may require significant amounts of energy in terms of power consumption, energy dissipation, etc. [1]. The sensor nodes (SNs) gather the information through event monitoring from their environments and transfer it to the next SN or the base station (BS). However, WSNs obtain data from vulnerable deployment environments through the Internet or sensor actuators. WSNs are usually deployed in several applications such as battlefield surveillance, disaster recovery [2], healthcare applications [3], homeland

security [4], agricultural monitoring [5], environmental monitoring, home automation, oil-refinery monitoring process, industry applications, etc. [6,7]. These WSN applications usually occur in vulnerable conditions. Each SN in a WSN is associated with resource constraints such as restricted battery power and limited resources.

Regarding computational capability [8], the sensor nodes deployed in the event-monitoring area often experience redundant data transmission. As a result, the nodes consume additional energy, and congestion may occur in the network when the redundant data are transmitted to the base station (BS) [9]. In addition, different energy consumption may occur due to redundant data transmission. Consequently, aggregating the data locally and adjusting the data to become redundant-free data packets before advancing the data to the BS is urgently desired. After a SN collects identical data packets and makes a single copy of the data, an aggregator node forms. The aggregator node can omit the redundant data using several methods, such as artificial intelligence or probabilistic or statistical approaches [10,11].

Transmitting redundant data is a concern in secure data aggregation. The transmitted data must hop multiple times before the data reaches the BS. Consequently, it becomes inefficient to transmit redundant data in the network. In addition, it is inefficient to hop redundant data because WSNs have limited computational capability and constrained memory of sensor nodes (SNs). The BS/SN discovers such redundant data and drops it. By performing this action, it improves the lifetime of the network, and thus, the energy consumption is reduced, and any delay introduced in the network is also reduced.

Securely aggregating sensed data via aggregator nodes plays a vital role in conserving energy efficiency in the network. In aggregating the sensed data, BS utilizes a security control mechanism. Secure data aggregation (SDA) uses security control mechanisms like authentication and authorization methods in WSNs. Thus, secure data aggregation ensures confidentiality, integrity, and availability for privacy preservation [12] in a WSN while avoiding communication overhead (CO). Thus, secure data aggregation uses sensed data and avoids communication overhead. Consequently, SDA enhances the energy utilization of the SN during sensed data collection. In addition, SDA protocols play a vital role. They act as a firewall that should authenticate and authorize legitimate SN data for privacy preservation against any vulnerabilities or cyberattacks in the network. Due to this limitation of security control mechanisms such as secure node authorization, the lifetime of the WSN becomes a significant challenge. This challenge is due to the need to approve authenticated and authorized legitimate sensor nodes (SN) for secure data transmission in the network, which would subsequently leads to privacy concerns.

Thus, there is an urgent need for a privacy-preserving secure data aggregation approach to handle data aggregation issues and appropriately address data privacy concerns to maintain QoS provisioning [13] in the network. Secure data aggregation is an indispensable paradigm that removes data redundancy and prevents additional energy consumption [14], which requires further security design investigation. Therefore, researchers have introduced privacy-preserving aggregation of time-series data schemes for WSN and uploaded encrypted values for the data aggregation. A data aggregation process calculates the sum of the participants' SNs. However, it needs access to learn the contents of the data due to limitations in authorization and authentication security control mechanisms in the network, leading to communication overhead (CO).

However, communication overhead (CO) is a significant concern in WSNs because of the constrained features of sensor nodes. Secure data aggregation and privacy preservation of SN that extend network lifetime reduce CO. Reducing CO leads to sensed data in data aggregation, which helps make essential decisions in the WSN application. Nevertheless, the accuracy of final aggregation outcomes is significant. Therefore, researchers proposed an Energy-efficient and high-accuracy (EEHA) approach for secure data aggregation [15]. EEHA aims to achieve accurate data aggregation without sharing private sensor information and reducing communication overhead. The proposed EEHA achieved its objectives of reducing communication overhead. However, the proposed solution only partially applied

to realistic situations from a privacy-preserving secure data aggregation security standpoint. False sub-aggregate values are a security threat for the WSNs created by compromised sensor nodes. In this type of attack, significant errors are generated at the base station. The false sub-aggregate attacks restrict the authentication and authorization process of the nodes, since the EEHA protocol requires authorization of each SN in the network.

As a result of limited authorization, a false sub-aggregate error synopsis diffusion (SD) [16] approach reduced only false errors in WSNs. SD involves the algorithm that enables the base station (BS) to securely calculate the sum in the presence of those vulnerable or compromised attacks. Furthermore, the SD algorithm helped to calculate the actual aggregate to avoid the contributions of conceded sensor nodes in the aggregation hierarchy. However, cyberattacks like sybil node and sinkhole node [17] cyber threats are prominent vulnerabilities or attacks that compromise legitimate nodes' confidentiality, integrity, due to limited authentication and authorization. As a result, the sensor node's transmitted data are not secure.

Accordingly, the authors in [18] proposed a hybrid secure data aggregation (HSA) approach that provides end-to-end secure data communication for WSNs. HSA aims to reduce communication overhead. The approach used a symmetric key-based privacy homomorphism method to guarantee the sensor nodes' data reading to maintain the network's privacy. Furthermore, HSA efficiently dealt with key management issues. However, key management issues lead to energy efficiency concerns when maintaining end-to-end data communication. HSA aggregation methods try to use averaging functions to perform the aggregation. However, method like HSA is highly vulnerable to node compromises and all forms of cyberattacks, due to limited secure authentication and authorization.

Therefore, an iterative filtering method was proposed in WSNs to annul these attacks. Iterative filtering algorithms concurrently aggregate data from multiple sources to safeguard the confidentiality level of these sources. However, the iterative filter could not achieve its aim. Subsequently, an improved iterative filtering (IIF) [19] approach successfully handled sophisticated collusion attacks using an initial approximation algorithm in a WSN. IIF focused purely on a single collision attack. However, IIF has limitations in QoS provision, including authentication and authorization security control mechanisms. Therefore, a WSN approach known as a renewable hash chain (RHC) [20] provides confidentiality, authentication, and integrity in WSNs. However, there were no QoS metrics and no authorization security control mechanism in the WSN.

In this study, we consider secure data aggregation that utilizes both authentication and authorization (SDAAA) to enhance the energy efficiency and privacy preservation of the sensed aggregated data in a WSN. We also identify vulnerabilities and cyberattacks that affect confidentiality, integrity, and availability in SNs, to enhance privacy preservation. Consequently, the proposed SDAAA secure data aggregation protocol in WSN improves QoS performance metrics, such as accuracy in sensed data, that confirms the energy efficiency of the network [21]. Our proposed SDAAA approach maintains the tradeoff between authentication, entity-based authorization, and freshness while maintaining the QoS parameters and energy efficiency. We contribute as follows.

- Our approach provides an entity-based authentication and authorization process that allows only legitimate sensor nodes to communicate and only collects sensed data from those honest sensor nodes in the network. However, unlike WSN privacy-preserving methods such as SD, EEHA, HAS, IIF, and RHC, our approach uses a multi-feature authentication methods.
- In our proposed network architecture, SDAAA utilizes the base station (BS) in the network to authenticate and subsequently authorize the data aggregator node to drop the aggregated packets of those nodes which are not issued a tag to be part of the network. By contrast, SD, EEHA, HAS, IIF, and RHC approaches do not include such security control mechanisms.

- Our proposed SDAAA approach ensures data validity via a novel data freshness mechanism. By contrast, SD, EEHA, HAS, IIF, and RHC do not have any data freshness mechanisms.
- In our proposed SDAAA approach, we determine the sensor nodes' energy efficiency (EF) before sending the data to that node. In addition, we determine residual energy after the 'N' number of communication rounds. In contrast, SD, EEHA, HAS, IIF, and RHC approaches have no EF computation mechanisms.
- Our proposed SDAAA approach detects sybil and sinkhole nodes and other vulnerabilities or cyberattacks when injected into the network. The attacks may be from either malicious outside or inside adversaries. In contrast, SD, EEHA, HAS, IIF, and RHC do not detect all these vulnerabilities or other forms of cyberattacks.
- Our proposed SDAAA approach includes reliability vs. malicious trend of the nodes, throughput performance, and energy efficiency in the presence of malicious nodes. In addition, SDAAA protocol utilizes time complexity, and resilience time of the effected network that provide reliability in the network. In contrast, other protocols like SD, EEHA, HAS, IIF, and RHC do not have such reliability mechanism in their network.

The remainder of the paper is as follows: Section 2 discusses related work, challenges, privacy preservation, and design objectives. Section 3 presents the system model and architecture, attacker model, secure data aggregation using authentication and authorization encryption, and data freshness models. Section 4 is the simulation setup and experimental results. Finally, Section 5 concludes the entire work.

2. Related Work and Design Challenges

2.1. Related Work on Privacy Preserving Wireless Sensor Network including Secure Data Aggregation

The authors in [22] proposed preserving data and key privacy (PDKP) data aggregation for wireless sensors that attained data and privacy protection of keys in data aggregation in WSN. Using simple techniques, PDKP uses encrypted data without exposing data content and its key to other SNs. The protocol preserves the key and the data content from an adversary while using less computational overhead. PDKP has no authentication and authorization mechanism in the proposed method.

In [1], the authors proposed an energy-efficient and privacy-preserving data aggregation algorithm (EPDA) for less energy consumption, decreased energy consumption, and prolonged network lifetime. Sensor nodes (SNs) were organized in a tree and connected to the tree's leaf nodes to form chains. The EPDA used only sensed data through the tail SN nodes of the chains, which were sliced to ensure privacy in the network. However, no authentication and authorization mechanisms are in the proposed method.

The authors in [23] proposed secure data aggregation to preserve data and key privacy (SAPDKP) in wireless sensor networks with multiple sinks to protect keys and data in the data aggregation to preserve data and critical privacy in WSNs with multiple sinks. Multiple sinks consume less energy in computation and communication overhead. However, security concerns include data confidentiality [24], data integrity freshness [25], and data authentication. SAPDKP uses a straightforward technique to perform aggregation and encryption, and uses no authorization security measures.

In [12], the authors proposed multi-dimensional privacy-preserving average consensus (MPPAC) in wireless sensor networks as a solution to the privacy-preserving average consensus (PPAC) [26] problem only; this solution focused solely on a one-dimensional state, not a realistic simulation of an actual scenario. MPPAC divides nodes into two types: sink nodes and ordinary nodes. MPPAC was used to introduce a super-increasing sequence and an RSA algorithm into the network. This super-increasing sequence played a key role and dealt with any multi-dimensional measurement in the sensors, while the RSA achieved privacy, preserving average consensus only among sink nodes—however, the proposed method needed authentication and authorization mechanisms.

In [27], to create an efficient privacy- and integrity-preserving data aggregation in WSNs, the authors proposed an aggregation scheme for multiple applications (PIMA) in WSNs, using homomorphic encryption which aggregates hybrid sensor data into real WSN applications. The proposed protocol had to satisfy multi-application environment requirements and make use of sensors deployed in heterogeneous environments. PIMA employed Paillier encryption and homomorphic MAC to protect data privacy and check the integrity of the aggregated data. However, there were no authentication and authorization security mechanisms in place. The authors in [28] proposed a design for a privacy and energy-efficient data aggregator (EPSDA) for WSNs. The EPSDA was proposed to overcome energy-intensive aggregator node decryption that reveals a large amount of privacy-protected information to adversaries of the network, which result in the generation of inaccurate results. The proposed EPSDA protocol overcame these limitations and performed direct aggregation on the data, encrypted using homomorphic encryption. The EPSDA restricted old data transferred in the network. However, authentication and authorization mechanisms were not proposed in the scheme.

The authors in [29] proposed a novel energy-efficient and privacy-preserving data aggregation algorithm for WSNs known as CBDA (chain-based data aggregation). CBDA organized sensor nodes (SNs) into tree topology, where leaf nodes sequentially reconnect with each other and form chain topologies. Tail nodes in the topology ensure data privacy by gathering and slicing sensing data into fragments. The CBDA method did not use any authentication and authorization mechanisms in the proposed scheme.

The privacy-preserving secure data aggregation approach involves two main techniques: the first technique applies cryptography to allow the aggregation process to decrypt the data aggregation or sum with different keys. The second technique uses the differential privacy approach to protect data from being compromised [30]. Consequently, the authors in [31] proposed an energy-preserving approach named secure data aggregation watermarking (SDAW) based in homogeneous WSNs. SDAW used lightweight, fragile watermarking without encryption to guarantee integrity and authentication. Malicious nodes in the network can attempt to inject false data to mislead the nodes and gather important information due to the limitation of authorization in the network. The proposed SDAW did not use any authentication and authorization security mechanism in the proposed scheme.

Therefore, adversarial or malicious nodes in WSNs result in confidentiality concerns and compromise data. The compromised data cause additional energy consumption in the network and subsequently lead to communication overhead. As a solution to compromised data, a practical secure data aggregation (SDA) approach was proposed in [32] to ensure data privacy and prevent excess energy consumption. This SDA approach used additive homomorphic, identity-based signatures and batch verification schemes with a proposed algorithm to filter false data injected by malicious nodes without authorization, leading to communication overhead concerns. However, the proposed SDAAA security mechanism methodology needs an authentication and authorization mechanism.

These design challenges in the privacy-preserving secure data aggregation protocols and well-known approaches such as SD, EEHA, HAS, IIF, and RHC (discussed in Section 1) must be outlined and investigated in WSNs.

2.2. Design Challenges of SD, EEHA, HAS, IIF, and RHC, including Other Privacy-Preserving Secure Data Aggregation Protocols

As noted in the preceding discussion, privacy-preserving wireless sensor networks' secure data aggregation protocols and the contending protocols, such as SD, EEHA, HAS, IIF, and RHC, experience various network design challenges based on the following.

1. SD, EEHA, HAS, IIF, and RHC secure data aggregation protocols incur QoS concerns and communication overhead due to the absence of authentication, encryption, and authorization [33] security control mechanisms. The absence of these security control mechanisms leads to privacy preservation concerns such as data confidentiality and data integrity.

2. SD, EEHA, HAS, IIF, and RHC secure data aggregation protocols and other privacy-preserving wireless sensor network secure data aggregation incur access control security mechanism concerns. The access control security limitation leads to data redundancy because of limited authorization security control mechanism that would authorize only legitimate SN to be part of the network.
3. SD, EEHA, HAS, IIF, and RHC secure data aggregation protocols, and other privacy-preserving wireless sensor network secure data aggregation protocols encounter network throughput issues. The throughput issue is due to vulnerable SNs and all other cyber-attacks. Hence, privacy protections were unavailable in their networks due to limited authentication and authorization security control mechanisms in the networks.
4. SD, EEHA, HAS, IIF, and RHC secure data aggregation protocols and many other privacy-preserving secure data aggregation protocols experience energy efficiency issues, leading to a shorter sensor node lifespan. Therefore, improving a network's residual energy efficiency algorithm using authentication and authorization security control mechanism is essential to ensure the network's availability.
5. SD, EEHA, HAS, IIF, and RHC secure data aggregation protocols and many other privacy-preserving wireless sensor network secure data aggregation protocols have experienced the ability to manage node failure. The node failure is due to limitations in secure authentication and authorization in the sensed data, which lead to privacy, reliability, and integrity of data concerns in the network.
6. SD, EEHA, HAS, IIF, and RHC secure data protocols incur scalability regarding large-scale sensor deployment concerns. Scalability of legitimate sensor nodes to be part of the WSN requires availability of well authenticated and authorization security control mechanism.

Therefore, it is important to solve these security challenges in WSN secure data aggregation and privacy-preserving protocols, including well-known WSN approaches such as SD, EEHA, HAS, IIF, and RHC. We first provide an overview of privacy preservation and design objectives, including secure authentication and authorization. After that, we describe the design of a new system model, specifically a mathematical and analytical secure data aggregation model, using our proposed SDAAA protocol methods to assess new QoS performance metrics in the network.

2.3. Privacy Preservation and Design Objectives

In WSN applications like WBANs (wireless body area networks), privacy, secure authentication, and authorization of patients' information are in high demand. WBANs include emerging widespread wireless sensor network applications, especially in intelligent WSN healthcare applications. Secure authentication and authorization ensure that collected, stored, and transmitted data cannot be accessed and modified by unauthorized agents in networks, such as cyber hackers. Privacy preservation ensures that only authorized agents can access and use data in the network. Consequently, it becomes imperative to address authentication, authorization, and privacy protection concerns for WBANs [34].

Cyber hackers could launch various attacks, specifically cyberattacks, including sinkhole node and sibyl node attacks, that could breach healthcare data privacy. Healthcare data privacy is a significant issue leading to the need for protection in wireless sensor networks. Therefore, we focus on the data privacy protection issue resulting from cyberattacks, including sinkhole node and sibyl node attacks that can occur during healthcare WSN patient information monitoring. Cyber threats, including sinkhole node attacks, are internal attacks that compromise network nodes. As a result, compromised or vulnerable sensor nodes (SNs) attempt to attract all network traffic from the neighboring sensor nodes and generate fake routing metrics. Cyber threats resulting from sinkhole node attacks cause routing information issues such as acknowledgment spoofing and selective forwarding attacks. They can also send simulated data to the base station.

Conversely, cyber threats resulting from sybil node attacks sabotage the reputation of hop-to-hop communication systems, generating many fake identities. Sybil node cyber

threats happen after sinkhole node attacks, so both attacks rely on each other. We assume hackers understand the deployed security mechanism in the wireless sensor networks. Therefore, hackers may be able to compromise a node by applying a radio communication channel at the medium access control (MC) sublayer. After compromising the node, the attacker launches the sinkhole node cyber threats that release privacy data to the cyber enemies, compromising any individual sensor node privacy. The public key cryptographic authentication technique can secure ad hoc networks. Still, it is not compatible with wireless sensor networks due to the highly resource-constrained attributes of the sensor node.

The proposed SDAAA protocol guarantees energy efficiency and reliability, and the scalable, secure data communication process in this research model leads to privacy preservation in the network. Consequently, the design objectives of the proposed SDAAA approach are to obtain energy efficiency and fast data aggregation with maximum throughput while maintaining data privacy as a tradeoff. As presented in this research, the proposed SDAAA approach depends on the authentication process that helps maintain node authorization security and ensures privacy in the WBAN healthcare system. Our proposed paradigm considers accuracy as a standard for gauging authentication performance and energy efficiency.

Therefore, we provide a new system design and mathematical analytical secure data aggregation model to reevaluate new network QoS performance as required.

3. System Model and Design Objectives

To maintain network reliability for QoS performance, confidentiality, integrity, and availability [35] and guarantee privacy preservation [36,37], the proposed SDAAA system model utilizes an intelligent WSN healthcare application monitoring [38] scenario. The WSN application scenario includes a WPAN (wireless personal area network) and a WBAN (wireless body area network) as shown in Figure 1. We monitor patient data and protect healthcare applications (HAs) against all cyberattacks, including sinkhole nodes and sybil node cyber attacks [38,39]. Figure 1 assumes a wireless sensor network consists of a clustered-based topology with limited mobile cluster nodes (MCNs), which are mobile sensors, and static cluster nodes (SCN), which are static sensors, deployed with cluster head nodes (CHNs) in the WSN. However, this cluster provision is unavailable in contending WSN privacy models such as SD, EEHA, HAS, IIF, and RHC protocol system models. Thus, these contending WSN models do not possess MCNs or SCNs or the CHN attributes that enhance network reliability and energy efficiency. However, based upon the cluster network deployment in the proposed SDAAA approach, sensor nodes collectively complete monitoring tasks.

Due to cost limitations, the sensor nodes are without tamper-resilient hardware. In addition, stationary resourceful heterogeneous sensor nodes are in locations directly connected to the base station (BS). Our proposed SDAAA aggregation system model applies to each cluster in the WSN application, which utilizes four types of sensor nodes in the wireless sensor network: actor nodes (ANs), mobile sensor nodes (MSNs), data aggregator nodes (DANs), and event-monitoring nodes (EMNs). These four types of node provide reliability in the network. By contrast, as stated previously, contending models like SD, EEHA, HAS, IIF, and RHC protocols do not utilize cluster-based network design in their network. Thus, the contending secure data aggregation models do not have the four types of sensor nodes that provide reliability. In our proposed SDAAA approach, the BS is the target point used to compute the aggregation result. The following assumptions are held.

- 7 Cyberattacks, including sinkhole and sybil node hacks, may occur in healthcare computer systems.
- 8 EMNs are static cluster nodes (SCNs) that link the static sensor nodes or mobile cluster nodes (MCN) that link the mobile nodes; they are deployed together with the CHNs in the network, and they have the capability to be utilized by WPANs to monitor patients' health conditions. SCNs or static sensor nodes are deployed in fixed

- infrastructure equipment. In this research, the EMN communicates with the mobile sensor nodes or MCNs and sensing center to query for patient sensing data.
- 9 DANs can be either static or mobile sensor nodes that serve as CHNs (cluster head nodes). DANs receive data from the neighboring nodes, aggregate the data, and forward the aggregates to the BS or the gateway. DAN plays a major role in the secure aggregating process. DANs possess more computational and processing capabilities and storage capacity than EMNs.
 - 10 MCNs also link mobile sensor nodes attached to patients and any vehicles within the healthcare environment. They extend the capability of the static nodes in the WSN. MCNs also extend the coverage efficiency of patients and vehicles in the network. Moreover, MCNs can forward updated information to DANs.
 - 11 ANs are actor nodes and can also serve as gateway nodes. They are potent power nodes and processing units for decision processing. ANs have additional computational power and resources responsible for collecting the data from DANs. In addition, they support the BS in identifying legitimate DANs.

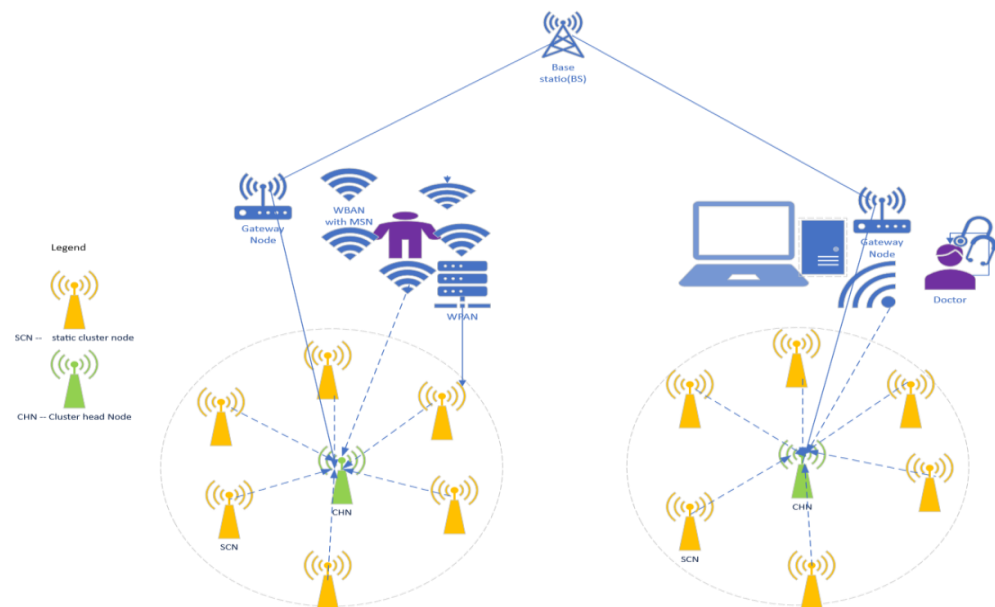


Figure 1. SDAAA healthcare monitoring system architecture model.

Figure 2 initiates a data fragmentation process for secure data aggregation. EMNs are responsible for collecting the data from patient health monitoring events. An EMN forwards the data to the data fragmenting node to fragment data into variable sizes. The data fragmenting node forwards fragmented data to a 1-hop neighborhood, and this fragmenting process keeps moving until it locates a DAN. The DAN collects the data from the data fragmenting node and applies the aggregation processes before sending it to another DAN or the base station.

Furthermore, DANs can communicate with other DANs. A DAN can use typical aggregation functions, including AVERAGE, MIN, MAX, SUM, COUNT, and authentication and authorization features. The additive aggregation functions comprise standard deviation, grouping, and variance that can quickly expand into additive SUM functions [40]. This secure data aggregation supports data fragmentation, as depicted in Figure 1.

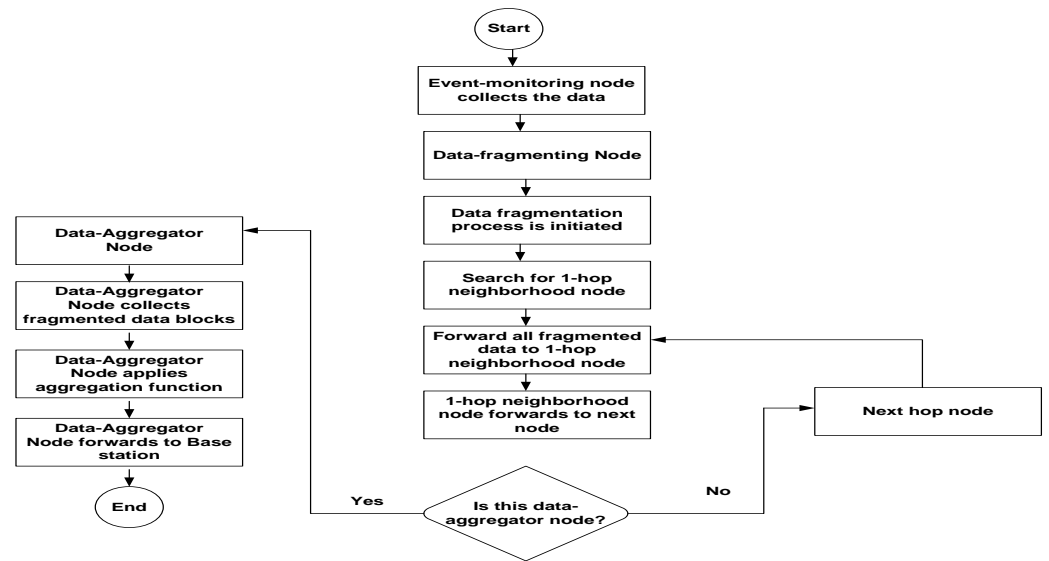


Figure 2. Proposed schematic process for secure data aggregation in WSNs.

3.1. Attacker Model

Due to privacy issues such as packet drop and errors of some control packets, signature mismatch may occur. Signature mismatch may lead to the false detection and isolation of inauthentic nodes by the BS (base station).

Therefore, we use the probability analysis attacker model for detection of any cyberattack such as sinkhole nodes and sybil attacks in the network. Thus, the probability analysis attacker model detects any packet drops or error messages for any malicious node attacks or sensor nodes compromised by cyberattacks. Therefore, the probability analysis attacker model investigates network reliability and reduces any packet drop or errors in the network. This probability analysis attacker model is deployed in our proposed SDAAA protocol. The probability analysis attacker model is not found in any of the contending secure data aggregation protocols. Therefore, we model the packet drop and errors in the network as below.

As proposed in our previous work [41], which is extended by our proposed SDAAA protocol in this research, we optimize the probability of false detection/error by the BS by doubling isolation of any cyberattacks in the network system architecture, which is necessary and is modeled as follows:

Let

P_r = probability of error detection or packet drop in the network

P_{DP} = probability of packet drops regarding any privacy concern in the network application

RP = packet generation rate within the network

t = time interval of the BS detecting attack or error in the network

ASM_i = number of authorized signature mismatches of node N_i among its neighbors

Then, the probability of ASM exceeding the maximum threshold ASM_{th} is as in Equation (1):

$$P_r(ASM > ASM_{th}) = 1 - 2 \sum \binom{RPt}{i} P_D^i (1 - P_{DP})^{Rt-i} \quad (1)$$

where

W = number of warnings received by node N_i when any of its neighbors turns out to be malicious or there are vulnerable nodes in the network.

The probability of W exceeding the maximum threshold W_{th} is given in Equation (2) as:

$$P_r(W(N_j) > W_{th}) = 1 - \sum_{i=1}^{W_{th}} \binom{NH}{i} P_{FD}(N_j)^i (1 - P_{FD}(N_j))^{NH-i} \quad (2)$$

where

NH is the number of neighbors of node N_i

$P_{FD}(N_j)$ is the probability of false detection of node N_j , which is given in Equation (3):

$$P_{FD}(N_j) = 1 - \exp\left(-2 \cdot \frac{(R.t.P_D - ASM_{th})^2}{R.t.}\right) \quad (3)$$

Then, the probability of doubling detection and Isolating any cyberattacks in the network is P_{FI} and is given by Equation (4) as:

$$P_{FI}(N_j) = 1 - \exp\left(-2 \cdot \frac{(NH.P_{FD}(N_j) - W_{th})^2}{NH}\right) \quad (4)$$

3.2. Secure Data Aggregation Using Authorization and Authentication in Wireless Sensor Networks (SDAAA)

Secure data aggregation presents the most significant security challenge for privacy in WSNs. The primary objective of secure data aggregation is to enhance the network lifetime. Another objective is to reduce the energy consumption of the sensor nodes through proper use of battery power and efficient bandwidth. However, the data aggregation process may significantly affect QoS, accuracy, and fault tolerance. A decline in QoS and accuracy leads to weak security control mechanisms, such as the limitation of authorizing legitimate sensor nodes (SNs) through authentication and encryption security. Since data aggregation enhances security by reducing redundant data, it could be affected by a compromised or malicious sensor node. Compromised or malicious sensor nodes may illegally obtain the collected data from the neighbor sensor node and report false values as aggregated data.

In this situation, a malicious node could harm the privacy, confidentiality, and integrity of the confidential data in WSNs. The malicious node could impersonate neighboring or further aggregator nodes. In addition, the attacker may prefer to install a hostile node near the base station to compromise it. As a result, QoS parameters such as energy efficiency, reliability, and accuracy are affected. The fragile design features of WSNs may easily invite destructive cyber attacks, mainly when deployed in unpromising environments.

WSNs comprise resource-restricted sensor nodes with insufficient storage, limited power resources, and lower computational capability. Hence, it is crucial to examine traditional security algorithms in secure data aggregation in WSNs such as SD, EEHA, HAS, IIF, and RHC protocols, as these frailer algorithms cannot meet desired security requirements. Researchers have examined the traditional security balance tradeoffs between security metrics and performance-improving parameters. Secure data aggregation should be reliable, accurate, scalable, and flexible. The reliability, accuracy, and flexibility of the proposed SDAAA approach model enhance fast data aggregation algorithms based on authentication and authorization by the BS (base station). This should be considered when designing secure data aggregation for WSNs.

Designing protocols meeting single characteristics based on secure data aggregation might be susceptible and exposed to malicious attackers, but multi-featured algorithms can curtail the security risk. Most existing data aggregation methodologies such as SD, EEHA, HAS, IIF, and RHC protocols do not meet these security requirements. Our proposed SDAAA approach utilizes the BS and addresses the node authentication, authorization, freshness, and energy efficiency processes to discourage cyber attacks in a WSN. Furthermore, we focus on improving the QoS provisioning, energy efficiency, and accuracy.

3.3. Authorization Process

Prevailing contending proposed secure data approaches such as SD, EEHA, HAS, IIF, and RHC protocols focus only on authentication and ignore the authorization process in wireless sensor networks [42]. Since a newly deployed node could be malicious, a WSN protocol must be cautious when a new node deployment occurs in the network. Newly installed malicious nodes may be difficult to distinguish from legitimate ones due to current wireless sensor network design limitations. A secure data aggregation protocol must prevent hackers from directly deploying malicious nodes. Therefore, it is not enough to protect the wireless sensor networks only from the perspective of node identity; cyberattacks such as sinkhole node and sybil node attacks occur. These attacks introduce malicious nodes that hackers could operate and compromise in the existing legitimate sensor nodes.

The old deployed genuine nodes possess authenticated and authorized certificates, and the newly created malicious nodes have the same legitimate identities. Therefore, there is a need to distinguish between the old, deployed, and new nodes to defend the network from possible cyber hackers or attacks. The proposed SDAAA protocol utilizes a timestamp technique in both the authentication and authorization processes. It maintains freshness to avoid the potential threats and hacking of the data; this feature is unavailable in approaches such as the SD, EEHA, HAS, IIF, and RHC protocols. Thus, our secure authentication process guarantees authentication, authorization, and freshness. In our proposed SDAAA approach, Algorithm 1 describes the authorization procedure as follows:

Algorithm 1. Authorization process for legitimate and non-legitimate sensor nodes

1. Initialization: (K_{auth} : authorized Sensor node; $Auth$: authorization; k : sensor node; k_{leg} : legitimate sensor node; Me : Message; BS_n : Base station; C_{auth} : Certificate for authorization; E_{BS} : expected action performed by base station; W_{sn} : Wireless Sensor Network; k_{id} : Sensor node's identity)
 2. Input: ($Me, C_t, k_{id}, PU_K, C_e$)
 3. Output: $\{(Auth), C_{auth}\}$
 4. Set $k = W_{sn}$
 5. If W_{sn} allows entry to the 'sensor node, then.
 6. BS_n Starts E_{BS} for k
 7. BS_n releases C_{auth} for k_{leg} : $C_{auth}C_{auth} = h\{k_{id}, C_e \parallel PU_K\}$ // released certificate for legitimate node.
 8. Set $Authfork$ // $Auth = \{Me, t_c, Sig(BS_n)\{(k_{id}||t_c||Me)\}, C_{k_{id}}\}$ // Authorization process.
 9. end if
 10. BS_n broadcasts $Auth$ (Me) for the k node in W_{sn}
 11. If $k \in K_{auth}$, then
 12. K_{auth} reads $Auth$ (Me)
 13. Set $Auth = k$ node $\in K_{auth}$
 14. else if $Auth \neq k$
 15. BS_n declines access the Knode
 16. end if
 17. end if else
-

Algorithm 1 shows the authorization process. In lines 1–3, we describe the parameter-initialization, input, and output processes, respectively. In line 4, the sensor node forms part of the network to participate in the data-monitoring/data-gathering process. In lines 5–7, if the WSN permits the sensor node to join the network, it performs a particular action as a guaranteed authorization certificate. As a result of the authorization certificate issued by the BS, the BS authorizes the legitimate sensor nodes to send and receive data in the network in line 9. In lines 10–13, the base station (BS) only broadcasts the message to authorized nodes to continue communication with them. Thus, only nodes authorized by the BS can read the messages in the network. In lines 14–15, the node is checked; if the

node does not have authorization, then data communication with that node is stopped. Table 1 shows the variables used in the broadcasting message and certificate.

Table 1. Used variables and description.

Notations	Description
Me	Message
C_t	The current time of sent message
$Sig(BS_n)$	Signature of Base station
h	Hash function
k_{id}	Sensor node's identity
PU_K	Public key
$C_{k_{id}}$	A certificate was issued to identify the sensor node
C_e	Certificate expiration time

3.4. Authentication Formation

Here, we show the performance of the entity-based authentication features of the proposed SDAAA model that helps the base station discover any falsely aggregated data. This is unlike the contending WSN approaches such as SD, EEHA, HAS, IIF, and RHC protocols, which do not utilize entity-based authentication in their network. Let us assume that sensor node 'k' is a compromised node and launches false sub-aggregate data by inserting a few wrong data bits into the collected aggregated data. To prevent this, the base station broadcasts the data aggregation query message that uses the random value ' R_{val} '. In response, sensor node 'k' sends its message authentication code (MAC) to the base station to authenticate the sensed value ' S_v '. The node 'k' uses ' R_{val} ' and its own identity ' N_{id} ' to compute the MAC as follows:

$$N_{MAC} = \sum k(R_{val}) + N_{id} \quad (5)$$

Based on the computed MAC address, the base station generates the random value and can also determine the falsely inserted portions of the aggregated data:

$$BS_n = G + \sum (R_{val})^\beta \times k_n \quad (6)$$

where G is the random generator, β is the number of generated values based on the number of sensor nodes, and k_n is the total number of sensor nodes in the network.

Then, the base station ' BS_n ' generates the random value that determines the inserted false data bits in aggregated data given by:

$$B_f = \sum (BS_n) \times N_{MAC} \simeq D_a \quad (7)$$

where D_a : aggregated data, N_{MAC} : number of MAC addresses, and B_f : false data bits that are available in aggregated data.

Lemma 1: *The hacker cannot generate an MAC associated with the false data aggregation data bits ' B_f ' that the base station cannot discover as false.*

Proof: Let us assume if sensor node 'k' contributes the data bits $B = \{b_1, b_2, b_3, \dots, b_n\}$ in its local summation ' $\gamma \nabla$ ', then it generates the MAC for authentication purpose ' k_{MAC} ' written as $k_{MAC}(A_k, K_l)$.

Where A_k : secret key generated by sensor node 'k' and ' K_l ': key length.

The sensor node ' k ' shares this key with base station ' BS_n ' with length ' K_l '. Thus, the characteristics of the key ' K_c ' can be written as:

$$K_c = [K_e(B + R_v)] \rightarrow BS_n \quad (8)$$

where K_e : the encrypted key, which encrypts the data bits before sending them to the base station.

Each legitimate node ' L_n ' in the network appends the key length ' K_l ' with $(K_l + K_l^*)$ which is the same as:

$$(K_l + K_l^*) = [K_e(B + R_v)]$$

Thus, the key can be simplified as follows:

$$(K_l + K_l^*) = K_c$$

$$K_{Ex} = (K_l + K_l^*)$$

$$K_c = K_{Ex} \quad (9)$$

where K_{Ex} : extended key length. \square

Let us assume the sensor node's MAC address ' k_{MAC} ' is compromised and the extended key ' K_{Ex} ' reaches the base station ' BS_n '. Another sensor node cannot inject the key of node ' k ' without detection. We observe that ' K_{Ex} ' cannot include false data bits of aggregated data. This feature helps maintain the authentication process in the SDAAA approach.

3.4.1. Authentication and Encryption

Secure data packet transmission in our proposed SDAAA approach can increase authentication and authorization utilizing encryption. Furthermore, it maintains the freshness of the message, which limits hackers' access to data. Contending approaches, such as SD, EEHA, HAS, IIF, and RHC protocols, only use authentication without any authorization or encryption process. Let us assume that the sensor node ' km ' forwards the data to the cluster head ' CH '. The encrypted packet, data sent to the cluster head, and data payload are as shown below:

$$[P_E = \{k_{id}, C_{Hid}, R_v, M_k(k, CH).P_{data} \times (\Delta d)\}] \quad (10)$$

In Equation (10), the packet encrypted procedure includes sensor node ' k ' and its identity ' k_{id} ', cluster head ' CH ' and its identity ' C ', randomly chosen value for encrypting the data R_v MAC's key ' M_k '. In addition, data payload ' P_{data} ' and the amount of data sent ' Δd ' occur. The base station and other sensor nodes can identify the packet's source based on the inserted information.

$$\Delta d = k_{id} || C_{Hid} || R_v || P_{data} \quad (11)$$

Equation (11) shows the amount of data sent in different forms from different sources (e.g., node's identity, cluster head's identity, randomly generated value, and data payload).

$$P_{data} = M_k(k, CH)k_r \quad (12)$$

Equation (12) shows the data payload format, and it involves the MAC key ' M_k ' generated for the sensor and cluster head node and the sensor node's reading ' k_r ' obtained through an event-monitoring process.

The data sent using the MAC key ' M_k ' complies with the message authentication code of the data. The cluster head node ' CH ' receives the aggregated encrypted packet ' A_{EP} ' from node ' k ' and forwards it to the next hop node ' N_{CH} ', which could be either another

sensor node ' k_a ', cluster head node ' CH ' or base station ' BS_n '. Thus, Equation (13) shows the aggregated encrypted packet as:

$$A_{EP} = [k_a || C_{H_{id}} || BS_n(id) \{ P_{data} \} \times R_v] \quad (13)$$

where $BS_n(id)$: base station' identity.

Equation (13) shows secure data sent via encryption $e(\Delta d')$ after applying the aggregation process ' D_{ag} '.

$$e(\Delta d')(D_{ag}) = (GK_{ran} \{ (CH || BS_n). \Delta d1 \} + k_a || CH(\Delta d2)) \quad (14)$$

where $\Delta d1$ denotes data shared between the cluster head node and the base station; $\Delta d2$ denotes data transmitted between the next-hop sensor node and the cluster head node.

We observed that for data $e(\Delta d')(D_{ag})$, the attacker or hacker could not modify data $e(\Delta d')(D_{ag})$ because they were fully encrypted using the group's secret random keys ' GK_{ran} '.

Where GK_{ran} : group of secret random keys shared by either two cluster head nodes or cluster head nodes and base station.

Equation (14) shows fully encrypted shared data $\Delta d1'$ between cluster head node ' CH ' and base ' BS_n ' station as:

$$\Delta d1' = e \{ BS_n(id) + C_{H_{id}} \} + R_v \times P_{data} \quad (15)$$

where $\Delta d2$ denotes data transmitted between the next hop sensor node and cluster head.

In Equation (16), the secure data transmitted between the next-hop sensor node and cluster head $\Delta d2'$ is given by:

$$\Delta d2' = \left\{ e \left(k_{a(id)} || C_{H_{id}} \right) . \Delta d2 + (R_v \times P_{data}) \right\} \quad (16)$$

$k_{a(id)}$: next hop sensor node's ID; e: identity encryption process

By combining the features of equations from above, we obtain the secure data aggregation and authentication processes, which leads to QoS ' Q_{pr} ' in the WSN as follows:

$$Q_{pr} = A_{EP} + \Delta d1' + \Delta d2' + e(\Delta d')(D_{ag}) \quad (17)$$

3.4.2. Secure Data Freshness Process

We observed the sensor reading ' k_r ' obtained by the sensor node ' k ', and resultant aggregation listening capability ' ϵ ' of the cluster head node ' CH ' in the premises of any number of events E'_n . This is important for securing the freshness of the data. Thus, every valid sensor node ' k ' belongs to its respective ' CH ' and has a total number of sensor nodes ' k_n ', which can forward the valid ' V_u ' and invalid ' I_u ' updated information to the cluster head CH . Hence, the current detection time ' D_t ' for the right communicating cluster head node ' V_{CH} ', conforms to the proposed SDAAA approach; however, it is absent in the other contending approaches like SD, EEHA, HAS, IIF, and RHC protocols. The proposed SDAAA approach secure data freshness is as shown below:

$$D_t = \frac{(k_r * E_n) \times k_n}{\epsilon} \quad (18)$$

Nevertheless, it is a tricky process to identify a valid cluster head node. We assume the right cluster head node ' V_{CH} ' and non-valid cluster head node ' NV_{CH} ' are available in the network. However, finding the valid cluster head node increases the necessity of secure

freshness to avoid compromising the aggregated data. Thus, the right cluster head node ' V_{CH} ' can be obtained by:

$$V_{CH} = \begin{cases} V_{CH} + 1, D_t > \frac{V_{CH}-1}{V_{CH}} \\ V_{CH}, otherwise \end{cases} \quad (19)$$

Once the valid cluster head node is determined, it is also appropriate to isolate the non-valid cluster head node ' NV_{CH} ' from the network; otherwise, it could damage the data integrity, which is vulnerable when securing data freshness. Thus, non-valid cluster head node ' NV_{CH} ' is obtained by:

$$NV_{CH} = \begin{cases} NV_{CH} + \tau(\Delta d_r), D_t > \frac{V_{CH}-1}{V_{CH}} \\ NV_{CH}, otherwise \end{cases} \quad (20)$$

where τ : data-affecting process; Δd_r : resultant aggregated data of cluster head node.

Henceforth, the same process also correctly determines the valid (legitimate) and non-valid (malicious) sensor nodes when forwarding the data in the network.

3.4.3. Energy Efficiency

Communication overhead (CO) leads to additional energy consumption. Therefore, we attempted to reduce communication overhead that occurs in the contending WSN approaches, such as SD, EEHA, HAS, IIF, and RHC protocols as compared to the proposed SDAAA approach, which resolves CO as follows:

In the proposed SDAAA protocol, let us assume the sensor network ' N_s ' consists of the sensor nodes ' k_n ', which exchange the messages ' M_1 ' and ' M_2 '. Determining the message exchange process between intermediate nodes is of paramount significance for determining the consumed energy of the nodes. Thus, we determine the communication overhead ' C_{o1} ' of the source node as:

$$C_{o1} = (1 - M_1) * k_n * M_2 \quad (21)$$

When forwarding data to either the next hop or the destination hops, data dependency ' D_d ' may occur at each hop, increasing communication overhead. Thus, the communication overhead for the next hop nodes or destination node, except the source node, is given by:

$$C_{o2} = (1 - M_1) * k_n \times \sum k * (D_d - 1) \quad (22)$$

Equations (21) and (22) show the communication overhead of the messages exchanged between source and destination nodes. Therefore, the total communication overhead ' C_{to} ' of the message exchange can be determined as follows:

$$C_{to} = (1 - M_1) * k_n + (1 - M_1) * k_n \times \sum k * (D_d - 1) \quad (23)$$

Equation (23) shows that when the overhead ratio ' R_o ' of our proposed SDAAA approach is compared with other known approaches, our proposed SDAAA approach communication overhead is much lower, as determined by Equation (24):

$$R_o = \frac{((1 - M_1) * k_n + (1 - M_1) * k_n) + \sum k * (D_d - 1)}{M_1 * M_2} \quad (24)$$

Thus, the communication overhead of our proposed SDAAA approach is less than that of the other contending approaches, which helps preserve energy consumption.

$$R_o = \frac{((1 - M_1) * k_n + (1 - M_1) * k_n) + \sum k * (D_d - 1)}{M_1 * M_2} < 1 \quad (25)$$

To determine the energy consumption, the sensing energy ' E_s ' of the sensor node ' k ' can be computed as:

$$E_s = \hat{\eta} \times R_s \quad (26)$$

where $\hat{\eta}$: a constant representing the energy to sense a bit of data and R_s : sensing rate in bit/s.

For communication purposes, we calculate the energy dissipated ' E_d ' by sensor node ' k ' to transmit the data packet of size ' P_s ' to destination sensor node ' k_d 's as:

$$E_d = (k, k_d, r, P_s) = ((\tau_1 + \tau_2 \times r(k, k_d)^{nh}) \times (R_s \times P_s) + R_o) \quad (27)$$

After the energy dissipation for transmitting the packet is obtained, the energy for receiving the packets ' E_r ' can be obtained as:

$$E_r = (k, k_d, P_s) = ((\tau_4 * R_s \times P_s) + R_o) \quad (28)$$

Finally, we determine the total energy consumption ' E_t ' for the entire communication process as follows:

$$E_t = \left((\hat{\eta} \times R_s) + ((\tau_4 * R_s \times P_s) + R_o) + ((\tau_1 + \tau_2 \times r(k, k_d)^{nh}) \times (R_s \times P_s) + R_o) \right) \quad (29)$$

By substituting the values, we obtain:

$$E_t = (E_s + E_d + E_r) \quad (30)$$

where r : 1hop distance between two sensor nodes set to 1, τ_2, τ_3, τ_4 : constant parameters, nh : Number of hops between source and destination nodes.

4. Simulation Setup and Experimental Results

This research was implemented and secure data aggregation simulated using an authentication and authorization approach for wireless sensor networks. Secure data aggregation involves challenges regarding security, QoS, energy efficiency, throughput, performance, and large-scale network deployment. We generated eight simulation scenarios close to realistic scenarios covering an entire intelligent healthcare WSN application scenario. We tested the generated scenarios and validated them using our proposed SDAAA approach. Our approach was programmed using C++ and was run on an OMNET++ simulator to achieve these goals. We tested each scenario several times to determine the strengths and limitations of our proposed SDAAA approach. We also compared our proposed SDAAA approach with contending approaches such as SD, EEHA, HAS, IIF, and RHC protocols. Finally, we collected the results based on ten simulation runs for each scenario as below.

- Scenario 1: Monitoring the internal data regarding the patient's condition using a WSN monitoring application to check for inside malicious involvement in the network using static nodes.
- Scenario 2: Monitoring entities outside of the intelligent WSN (e.g., vehicles, deployed persons, etc.) using static and mobile sensor nodes.
- Scenario 3: Monitoring internal and external activities using static sensor nodes.
- Scenario 4: Monitoring internal and external activities using static and mobile sensor nodes.
- Scenario 5: Generating 2% malicious sensor nodes in Scenario 1.
- Scenario 6: Generating 2%, 5%, and 10% malicious nodes in Scenario 2.
- Scenario 7: Generating 5% and 10% malicious nodes in Scenario 3.
- Scenario 8: Generating 5% and 10% malicious nodes in Scenario 4.

The simulation aims to validate the performance of the proposed SDAAA approach in the presence of malicious nodes (internal and external) and detect the impact using QoS

metrics. Furthermore, we compared our proposed SDAAA approach with the contending approaches: SD, EEHA, HAS, IIF, and RHC. We used similar parameters for all the methods in the simulation. For simulation purposes, we used a 1300×1300 network topology and involved 540 sensor nodes with a transmission range of 40 m. We set the initial energy of the nodes to 5 joules. The node bandwidth was 50 kb/s, and the maximum energy consumption of the sensor nodes for receiving and transmitting the data was set to 13.5 mW and 15.0 mW, respectively. Sensing and idle modes were set to 10.4 mW and 0.45 mW, respectively. The total simulation time/round was 36 min, and the pause time was 15 s, set for phase initialization before starting the simulation. We show the simulation parameters in Table 2.

Table 2. Simulation parameters for the proposed SDAAA protocol.

Used Parameters	Detail of Parameters
Network topology	$1300 \times 1300 \text{ m}^2$
Total sensors	540
Node's transmission range	40 m
Node's sensing range	30 m
The initial energy of a node	5 joules
Bandwidth of node	50 kb/s
Simulation time/rounds	36 min
Data packet size	256 bytes
Initial pause time	15 s
Total hops	22
Proposed and contending aggregation methods	SDAAA, SD, EEHA, HAS, IIF, and RHC
Buffering capacity	50-packet buffering capacity at each node
Mobility (speed of the nodes)	0 m/s to 15 m/s
Base station location	(0, 820)
Power intensity	−14 dBm to 13 dBm.
Rx energy	13.5 mW
Tx energy	15 mW
Routing protocol	Hop-by-hop
Medium access control protocol	IEEE 802.15.4 cluster-based MAC

Based on the simulation, we obtained the following results:

- Average throughput
- Average energy consumption
- effected network vs. resilience time.
- Complexity

4.1. Throughput

Throughput is a significant metric generally expressed as the data transmitted over the sensor network. We consider that the source nodes generate a random number of data packets in ranges that can lead to delay/latency and can affect the throughput of the network. We developed several simulation scenarios to measure our proposed SDAAA approach's maximum throughput and compared it with contending approaches such as SD, EEHA, HAS, IIF, and RHC. Based on the simulation results, we observed that when time increases, the throughput performance of all approaches remains variable; see graphs in Figure 3.

However, the throughput performance of our proposed approach was better than that of the contending approaches. Based on the graphs in Figures 4–6, our proposed SDAAA approach's throughput performance is much better than other competing approaches like SD, EEHA, HAS, IIF, and RHC. In Figure 3, the approximate throughput performance of our proposed SDAAA approach is 422 kb/s, while other competing approaches have 361–406 kb/s.

In Figure 4, the average throughput performance of our proposed SDAAA approach was 444 kb/s. In contrast, the performance of competing approaches like SD, EEHA, HAS,

IIF, and RHC protocols was 415–443 kb/s with several increased sensor nodes. As depicted in the graph in Figure 5, we generated 5% malicious nodes to confirm the effectiveness of our approach and other competing approaches. The results show that our proposed SDAAA approach had a 426.5 kb/s throughput performance, which indicates less latency, compared with the competing approaches like SD, EEHA, HAS, IIF, and RHC, which have 405–418 kb/s, indicating high latency. We generated 10% malicious data, as shown in Figure 6. The number of malicious nodes increased, affecting the throughput performance of competing approaches. However, our proposed SDAAA approach is promising. Our proposed SDAAA approach reached 424.5, while other contending approaches like SD, EEHA, HAS, IIF, and RHC reached 402–409 kb/s. The reason for better throughput in our method is the lightweight authentication and authorization process that handles the malicious node's activities effectively.

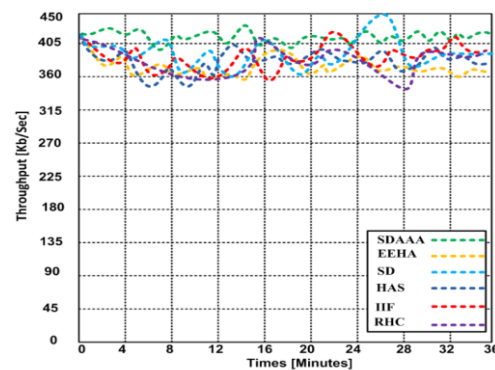


Figure 3. Average throughput of our proposed SDAAA and other contending approaches: EEHA, SD, HAS, IIF, and RHC over entire simulation time.

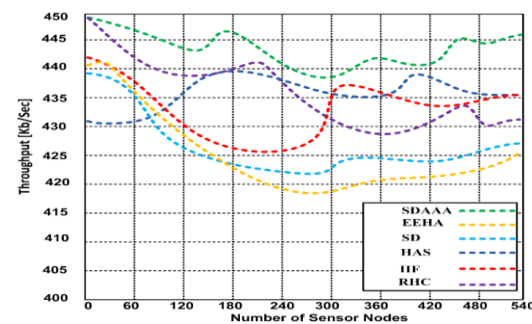


Figure 4. Average throughput of our proposed SDA and other contending approaches: EEHA, SD, HAS, IIF, and RHC in the presence of malicious nodes.

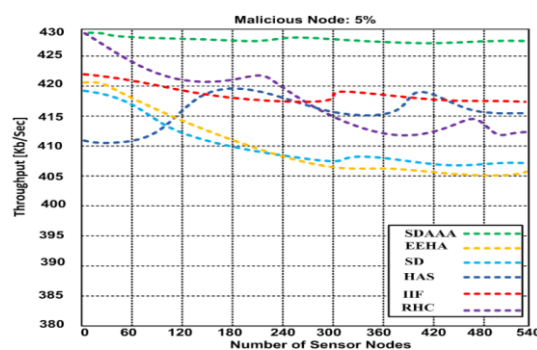


Figure 5. Average throughput of our proposed SDA and other contending approaches: EEHA, SD, HAS, IIF, and RHC in the presence of malicious nodes.

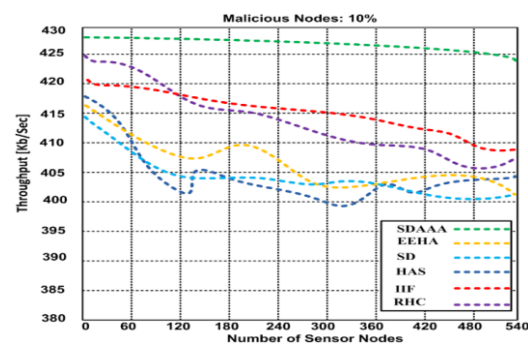


Figure 6. Showing average throughput of our proposed SDA and other contending approaches: EEHA, SD, HAS, IIF, and RHC in the presence of malicious nodes.

4.2. Average Energy Consumption

Secure data aggregation should focus on improving QoS, so for the network to consume minimum energy for enhanced data communication is paramount. After completing the experiments on the network, we determined the energy salvation process by monitoring and data-forwarding packets to the data aggregation and sink nodes. We generated three scenarios involving malicious and non-malicious nodes. Based on the simulation results, we perceived that the energy consumption upsurges when event-monitoring rounds increase. Figure 7 depicts the result for the non-malicious scenario; 2.6 joules of energy are consumed during the 36 event-monitoring rounds using our proposed SDAAA approach, whereas other contending approaches such as SD, EEHA, HAS, IIF, and RHC consumed 3–3.62 joules.

We generated 2% malicious nodes in Figure 8. We observed that nodes consume more energy in adversarial node scenarios. Our proposed SDAAA approach consumes 2.91 joules over 36 event-monitoring rounds compared to other competing approaches like SD, EEHA, HAS, IIF, and RHC, which consumed 3.5–3.94 joules in a similar scenario. In Figure 9, the generated scenario comprises 5% malicious nodes, and the results show that as the number of malicious nodes increases, additional energy is consumed. The increased number of malicious nodes significantly affects QoS and reduces the network lifetime. Our proposed SDAAA approach required 3.32 joules, while other contending approaches like SD, EEHA, HAS, IIF, and RHC consumed 4.39–4.52% over 36 event-monitoring rounds. Our proposed SDAAA approach consumed less energy overall. The reason behind the minimal energy consumption in our proposed SDAAA approach is the incorporation of an energy-efficient model that helps cause less energy consumption in the network.

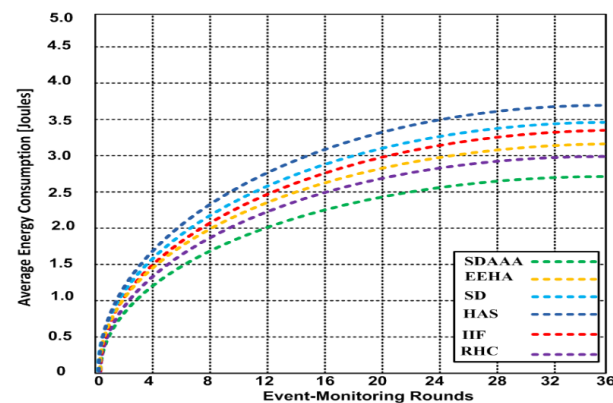


Figure 7. Energy consumption of proposed SDAAA and other contending approaches: EEHA, SD, HAS, IIF, and RHC during different event-monitoring nodes.

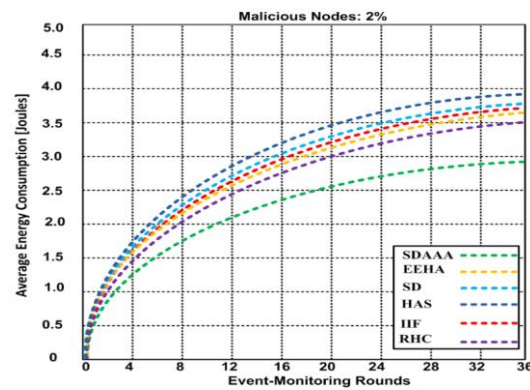


Figure 8. Energy consumption of proposed SDA and other contending approaches (EEHA, SD, HAS, IIF, and RHC) by different event-monitoring nodes in the presence of malicious node.

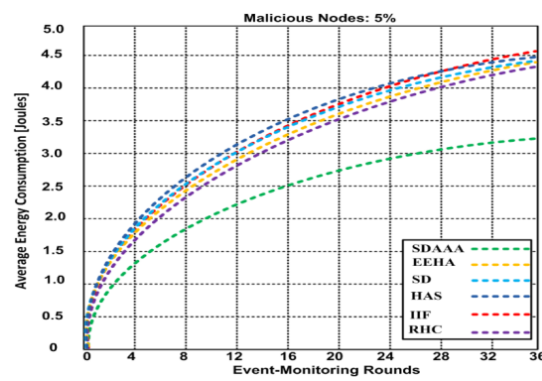


Figure 9. Energy consumption of proposed SDA and other contending approaches (EEHA, SD, HAS, IIF, and RHC) by different event-monitoring nodes in the presence of malicious node.

4.3. Affected Network vs. Resilience Time

Regarding resilience time, we determined the performance of our proposed SDAAA approach and other contending approaches such as SD, EEHA, HAS, IIF, and RHC. We generated three malicious scenarios and diagnosed the affected network. We noticed in the results, as depicted in Figure 10, that when a network is affected by malicious nodes, then the resilience time also increases. However, our proposed SDAAA approach obtains minimum resilience time compared to the other contending secure data aggregation approaches like SD, EEHA, HAS, IIF, and RHC. Our proposed SDAAA approach yielded a 2.45% effected network with 0.9 maximum resilience time, whereas competing approaches like SD, EEHA, HAS, IIF, and RHC produced a 2.98–3.62% affected network with 0.9 full resilience time.

Figure 11 depicts a malicious scenario involving 5% malicious nodes. Based on the results, our proposed SDAAA approach has an affected network of 2.62%, with 0.9% resilience time, whereas other competing approaches like SD, EEHA, HAS, IIF, and RHC have effected network of 3.68–4.38%, with 0.9% resilience time. In Figure 12, the ratio of malicious nodes' is increased up to 10%. This increment highly affects other contending approaches such as SD, EEHA, HAS, IIF, and RHC, which lead to a high network effect of 4.47–4.99%, while our proposed approach SDAAA is not significantly effected has only 2.67%. We surmise that the better performance of our proposed SDAAA protocol is due to the use of authentication, authorization, and a data-freshness paradigm, which helps the data aggregation nodes to identify false aggregated data accurately. Our SDAAA approach was unaffected, while the other contending secure data aggregation approaches did not provide authorization, authentication, or energy efficiency.

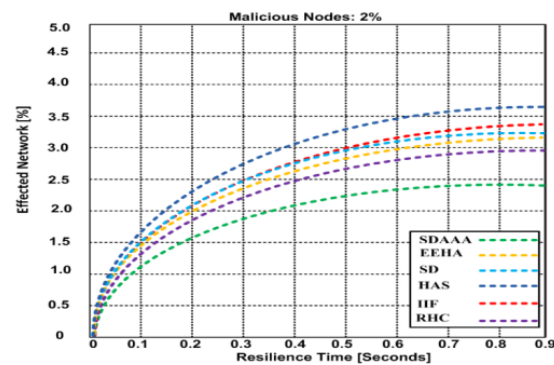


Figure 10. Effected network vs. resilience time of the proposed SDA and other contending approaches (EEHA, SD, HAS, IIF, and RHC) in the presence of malicious nodes.

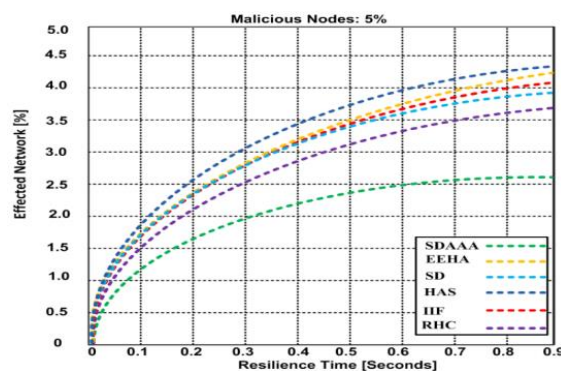


Figure 11. Effected network vs. resilience time of proposed SDA and other contending approaches (EEHA, SD, HAS, IIF, and RHC) in the presence of malicious nodes.

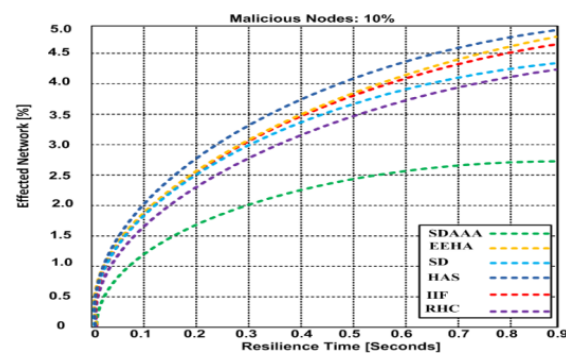


Figure 12. Effected network vs. resilience time of proposed SDA and other contending approaches (EEHA, SD, HAS, IIF, and RHC) in the presence of malicious nodes.

4.4. Time Complexity

The time-related performance of any protocol depends on the task's complexity. Time complexity refers to the time required to run a task, signifying effectiveness in the input. We measure the time complexity by calculating the number of basic operations accomplished by the algorithm. Based upon this, an essential operation takes a constant amount of time to execute. In Figure 13, we draw the trend of the time complexity for our proposed SDAAA approach and compared its time complexity with other contending approaches such as SD, EEHA, HAS, IIF, and RHC. The results confirm that the proposed SDAAA approach had $O(\log n)$ time complexity and required 0.08 s to complete 0.9 aggregated data. Time complexity was determined using 2% malicious nodes in the network.

Our proposed SDAAA approach had the lowest time complexity because it uses secure authentication, authorization, and energy efficiency that help lessen the time complexity.

We establish our proposed SDAAA approach and contending approaches on a recursive basis. Therefore, time complexity can be determined using recursive features given by the following formula, and the details are in Table 3.

$$T(n) = \begin{cases} O(1) & \text{If } n = 1 \\ at(\frac{n}{b}) + O(n) & \text{If } n > 1 \end{cases} \tag{31}$$

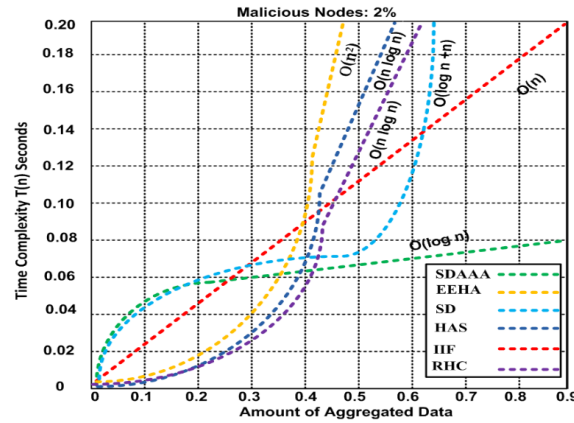


Figure 13. Time complexity of SDAAA, SD, EEHA, HAS, IIF, and RHC.

Table 3. Time complexity for SDAAA and contending SD, EEHA, HAS, IIF, and RHC protocols.

Time Complexity of Proposed Approach	Time Complexity
EEHA	$T(n) = T(n - 1) + T(0) + O(n)$ $= T(n - 1) + O(n)$ $= O(n^2)$
SDAAA	$T(n) = at(\frac{n}{b}) + O(n)$ The problem consists of a finite set of inputs, but computation complexity remains constant ('n') $T(n) = t(\frac{n}{2}) + O(n)$ $T(n) = t(\frac{n}{2}) + n$ $(n) = t(\frac{n}{n}) + n$ $T(n) = t(1) + n$ $T(n) = t + n$ Where t is ignored; therefore, we obtain $T(n) = n$ $n = k \ \& \ k = \log n$ By substitution, we obtain thus, the complexity is $O(\log n)$
IIF	$T(n) = at(\frac{n}{b}) + O(n)$ The problem consists of a finite set of inputs, but its computation time increases linearly. Thus, $T(n) = t(\frac{n}{2}) + O(n)$ $T(n) = t(\frac{n}{n}) + O(n)$ $T(n) = t + O(n)$ Where t is ignored; therefore $T(n) = O(n)$

Table 3. Cont.

Time Complexity of Proposed Approach	Time Complexity
HAS	$T(n) = at\left(\frac{n}{b}\right) + O(n)$ Here, we divide the problem into two portions of the same size. However, the algorithm is infinite. Thus: $T(n) = 2t\left(\frac{n}{2}\right) + O(n)$ $T(n) = 2t\left(\frac{n}{2}\right) + O(n)$ $(n) = 4t\left(\frac{n}{4}\right) + n + n$ $T(n) = 4t\left(\frac{n}{n}\right) + 2n$ $T(n) = 4t + 2n$ $T(n) = O(kn)$ $T(n) = O(\log nn)$ Where $k = \log n$ $T(n) = O(n \log n)$
SD	$T(n) = at\left(\frac{n}{b}\right) + O(n)$ The problem consists of a finite set of inputs, but computation complexity remains constant ('n'). $T(n) = t\left(\frac{n}{2}\right) + O(n)$ $T(n) = t\left(\frac{n}{2}\right) + n + n$ $(n) = t\left(\frac{n}{n}\right) + n + n$ $T(n) = t(1) + n + n$ $T(n) = t + n + n$ Where t is ignored; therefore, we obtain $T(n) = n + n$ $n = k \ \& \ k = \log n$ we get $O(\log n + n)$
RHC	$T(n) = at\left(\frac{n}{b}\right) + O(n)$ We divided the problem into two parts with different sizes according to the needs of the proposed algorithm. $T(n) = t\left(\frac{n}{3}\right) + t\left(\frac{2n}{3}\right) + O(n)$ $T(n) = t\left(\frac{n}{3}\right) + t\left(\frac{2n}{3}\right) + O(n)$ $T(n) = t\left(\frac{n}{3}\right) + t\left(\frac{2n}{3}\right) + n + n$ $T(n) = t\left(\frac{n}{n}\right) + t\left(\frac{2n}{n}\right) + n + n$ $T(n) = 2t + 2n$ $T(n) = \log nn$ $T(n) = O(n \log(n))$

Based on the time complexity results, we evaluated our proposed SDAAA and the other contending approaches like SD, EEHA, HAS, IIF, and RHC; details are given in Table 4.

Table 4. Time complexity $T(n)$ and other characteristics of SDAAA, SD, EEHA, HAS, IIF, and RHC.

Name of Approach	Time Complexity	Impact of $T(n)$	Probabilistic Attack Detection	Robust to Communication Loss
SDAAA	$O(\log n)$	Excellent	Yes	Yes
SD	$O(\log n + n)$	Fair	No	Yes
EEHA	$O(n^2)$	Worst	No	No
HAS	$O(n \log n)$	Bad	No	No
IIF	$O(n)$	Good	Yes	No
RHC	$O(n \log n)$	Bad	No	No

The simulation results confirm that our proposed SDAAA approach performs better than the known secure data aggregation approaches like SD, EEHA, HAS, IIF, and RHC. We show the detailed outcomes of metrics used in our proposed SADAA approach, compared with the other secure data approaches like SD, EEHA, HAS, IIF, and RHC in Table 5 as follows:

Table 5. Showing performance of SDA AA protocol comparison with the different contending approaches like SD, EEHA, HAS, IIF, and RHC protocols.

Approaches	Throughput			Average Energy Consumption			Effectuated Network		
	0% Malicious Node	5% Malicious Node	10% Malicious Node	0% Malicious Node	2% Malicious Node	5% Malicious Node	2% Malicious Node	5% Malicious Node	10% Malicious Node
EEHA	415 kb/s	405 kb/s	402 kb/s	3.24 Joule	3.7 Joule	4.41 joules	3.25%	4.27%	4.48%
SD	427 kb/s	407 kb/s	402 kb/s	3.4 Joule	3.82 Joule	4.42 joules	3.28%	4.89%	4.48%
HAS	436 kb/s	415 kb/s	404.4 kb/s	3.62 Joule	3.92 Joule	4.49 joules	2.98%	4.38%	4.99%
IIF	435.5 kb/s	418 kb/s	409 kb/s	3.35 Joule	3.71 Joule	3.32 joules	3.34%	4.08%	4.66%
RHC	431 kb/s	412.2 kb/s	407 kb/s	3.0 Joule	3.5 Joule	4.39 joules	3.62%	3.68%	4.47%
SDAAA	444 kb/s	426.5 kb/s	424.5 kb/s	2.6 Joule	2.91 Joule	3.32 joules	2.45%	2.62%	2.67%

5. Conclusions

This paper proposes a method of secure data aggregation using the authentication and authorization (SDAAA) protocol for detecting cyberattacks, including sybil node and sinkhole node attacks or hackers in wireless sensor networks. The proposed paradigm aims to monitor and protect intelligent healthcare application systems and personnel from internal and external cyber security threats that can disrupt the functional process of smart healthcare application monitoring. The paradigm uses a node authorization algorithm. The algorithm prevents the entry of prohibited or malicious nodes known as sybil node and sinkhole attacks in the network. Furthermore, the paradigm focuses mainly on authentication, authorization, and freshness, which combat malicious node effects in the network and improve the energy consumption of the WSN. These security mechanisms sustain the tradeoff between energy efficiency, accuracy, and QoS provision in the WSN.

We programmed in C++ and implemented on the OMNET++ simulator to confirm the legitimacy and strength of our proposed SDAAA protocol. Based on the extensive experimental results, we have validated that our proposed SDAAA protocol has an accuracy of 444 kb/s representing 98% of data rate/channel capacity of the network, an energy consumption of 2.6 joules representing 99% energy efficiency of the network, an affected network of 2.45 representing 99.5% achieved overall performance of the network, and a time complexity of 0.08 s representing 98.5% efficiency of the proposed SDAAA approach. By contrast, contending protocols such as SD, EEHA, HAS, IIF, and RHC have a throughput range of 415–443 representing 85–90% of the data rate/channel capacity of the network, energy consumption in the range of 3.0–3.6 joules representing 88–95% energy efficiency of the network, effectuated network range of 2.98 representing 72–89% achieved improved overall performance of the network and time complexity in the range of 0.20 s representing 72–89% efficiency of the proposed SDAAA approach. Thus, our proposed SDAAA protocol outperformed the other similar types of protocols such as SD, EEHA, HAS, IIF, and RHC, from the perspective of average throughput, average energy consumption, affected network, resilience time, and time complexity in the presence of malicious nodes. In the future, we aim to extend our proposed SDAAA protocol to include a mobility model to investigate further state-of-art QoS metrics, with different data markings applicable to that situation.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Available upon request.

Acknowledgments: The author would like to thank Florida Agricultural and Mechanical University for supporting this research. This research is part of a dissertation sponsored by the University of Bridgeport. The authors are grateful for all the constructive comments by the reviewers.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Zhou, L.; Ge, C.; Hu, S.; Su, C. Energy-Efficient and Privacy-Preserving Data Aggregation Algorithm for Wireless Sensor Networks. *IEEE Internet Things J.* **2020**, *7*, 3948–3957. [\[CrossRef\]](#)
2. Ramonet, A.G.; Noguchi, T. Node Replacement Method for Disaster Resilient Wireless Sensor Networks. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 789–795. [\[CrossRef\]](#)
3. Srivastava, S.; Singh, J. Wireless Communication Security Breaches in Smart Healthcare Applications. In Proceedings of the 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 17–18 December 2021; pp. 1240–1244. [\[CrossRef\]](#)
4. Binh, H.T.T.; Binh, N.T.M.; Hoang, N.H.; Tu, P.A. Heuristic algorithm for finding maximal breach path in a wireless sensor network with omnidirectional sensors. In Proceedings of the 2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Agra, India, 21–23 December 2016; pp. 1–6. [\[CrossRef\]](#)
5. Mulik, V.; Patil, V. Wireless Visual Sensor Network Application in Monitoring and Detection of Agricultural Crop Diseases: Review. In Proceedings of the 2023 7th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 18–19 August 2023; pp. 1–6. [\[CrossRef\]](#)
6. Nourildean, S.W.; Hassib, M.D.; Mohammed, Y.A. AD-Hoc Routing Protocols in WSN-WiFi based IoT in Smart Home. In Proceedings of the 2023 15th International Conference on Developments in eSystems Engineering (DeSE), Baghdad & Anbar, Iraq, 9–12 January 2023; pp. 82–87. [\[CrossRef\]](#)
7. Liu, J.; Zhao, Z.; Ji, J.; Hu, M. Research and application of wireless sensor network technology in power transmission and distribution system. *Intell. Converg. Netw.* **2020**, *1*, 199–220. [\[CrossRef\]](#)
8. Rahayu, T.M.; Lee, S.-G.; Lee, H.-J. A secure routing protocol for wireless sensor networks considering secure data aggregation. *Sensors* **2015**, *15*, 15127–15158. [\[CrossRef\]](#)
9. Swamy, T.J.; B, P.; Amaraveni, V.; Sireesha, Y.; Siddarth, S. Secure Data Dissemination in Wireless Sensor Networks with The Help of Module Based Blockchain Technology. In Proceedings of the 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 23–25 June 2023; pp. 1–6. [\[CrossRef\]](#)
10. Dhasian, H.R.; Balasubramanian, P. Survey of data aggregation techniques using soft computing in wireless sensor networks. *IET Inf. Secur.* **2013**, *7*, 336–342. [\[CrossRef\]](#)
11. Zhang, W.; Liu, Y.; Das, S.K.; De, P. Secure data aggregation in wireless sensor networks: A watermark-based authentication supportive approach. *Pervasive Mob. Comput.* **2008**, *4*, 658–680. [\[CrossRef\]](#)
12. Yu, L.; Yu, W.; Lv, Y. Multi-Dimensional Privacy-Preserving Average Consensus in Wireless Sensor Networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2022**, *69*, 1104–1108. [\[CrossRef\]](#)
13. Liu, C.; Liu, Y.; Zhang, Z.; Cheng, Z. High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks. *Int. J. Commun. Syst.* **2013**, *26*, 380–394. [\[CrossRef\]](#)
14. Frej, M.B.H.; Elleithy, K. Secure Data Aggregation Model (SDAM) in Wireless Sensor Networks. In Proceedings of the 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 9–11 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 330–334.
15. Li, H.; Lin, K.; Li, K. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks. *Comput. Commun.* **2011**, *34*, 591–597. [\[CrossRef\]](#)
16. Roy, S.; Conti, M.; Setia, S.; Jajodia, S. Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 681–694. [\[CrossRef\]](#)
17. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil attacks and their defenses on the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 372–383. [\[CrossRef\]](#)
18. Parmar, K.; Jinwala, D.C. Hybrid Secure Data Aggregation in Wireless Sensor Networks. In *International Workshop on Design, Modeling, and Evaluation of Cyber Physical Systems*; Springer International Publishing: Cham, Switzerland, 2015; pp. 116–131.

19. Choudhari, E.; Bodhe, K.D.; Mundada, S.M. Secure data aggregation in WSN using iterative filtering algorithm. In Proceedings of the 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, 21–23 February 2017; pp. 1–5. [[CrossRef](#)]
20. Dai, T.; Huang, H.; Wang, R.; Pan, X. Novel self-renewal Hash chain based on Ito-Saito-Nishizeki secret sharing scheme. *J. China Univ. Posts Telecommun.* **2012**, *19* (Suppl. S2), 122–127. [[CrossRef](#)]
21. Babu, T.; Jayalakshmi, V. The Challenges for Context-Oriented Data Accumulation with Privacy Preserving in Wireless Sensor Networks. In Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 11–13 March 2020; pp. 866–871. [[CrossRef](#)]
22. Akila, V.; Sheela, T. Preserving data and key privacy in Data Aggregation for Wireless Sensor Networks. In Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICT), Chennai, India, 13 May 2017; pp. 282–287. [[CrossRef](#)]
23. Akila, V.; Sheela, T. Secure Data Aggregation to Preserve Data and Key Privacy in Wireless Sensor Networks with Multiple Sinks. In Proceedings of the 2019 3rd International Conference on Computing and Communications Technologies (ICT), Chennai, India, 21–22 February 2019; pp. 86–93. [[CrossRef](#)]
24. C, V.; Premi, G.; Solainayagi, P.; Srinivasan, C.; Kuppusamy, P. Data Privacy and Confidentiality in Healthcare Applications of IoT-Enabled Wireless Sensor Networks. In Proceedings of the 2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon), Singapore, Singapore, 18–19 August 2023; pp. 610–614. [[CrossRef](#)]
25. Elmahdi, E.; Yoo, S.-M.; Sharshembiev, K.; Kim, Y.-K.; Jeong, G.-H. Protecting Data Integrity for Multi-Application Environment in Wireless Sensor Networks. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 90–95. [[CrossRef](#)]
26. Ruan, M.; Gao, H.; Wang, Y. Secure and Privacy-Preserving Consensus. *IEEE Trans. Autom. Control* **2019**, *64*, 4035–4049. [[CrossRef](#)]
27. Zhou, Q.; Qin, X.; Liu, G.; Cheng, H.; Zhao, H. An Efficient Privacy and Integrity Preserving Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks. In Proceedings of the 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, 9–11 August 2019; pp. 291–297. [[CrossRef](#)]
28. Phakade, S.V.; Singla, C.R.; Rajankar, O. Design of Privacy and Energy-Efficient DATA Aggregators for Wireless Sensor Networks. In Proceedings of the 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, 26–28 August 2022; pp. 1–5. [[CrossRef](#)]
29. Hu, S.; Liu, L.; Fang, L.; Zhou, F.; Ye, R. A Novel Energy-Efficient and Privacy-Preserving Data Aggregation for WSNs. *IEEE Access* **2020**, *8*, 802–813. [[CrossRef](#)]
30. Shi, E.; Chan, H.T.H.; Rieffel, E.; Chow, R.; Song, D. Privacy-preserving aggregation of time-series data. In *Annual Network & Distributed System Security Symposium (NDSS)*; Internet Society: Reston, VA, USA, 2011.
31. Boubiche, D.E.; Boubiche, S.; Toral-Cruz, H.; Pathan, A.-S.K.; Bilami, A.; Athmani, S. SDAW: Secure data aggregation watermarking-based scheme in homogeneous WSNs. *Telecommun. Syst.* **2016**, *62*, 277–288. [[CrossRef](#)]
32. Shim, K.-A.; Park, C.-M. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 2128–2139. [[CrossRef](#)]
33. Shin, S.; Kwon, T. A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things. *IEEE Access* **2020**, *8*, 67555–67571. [[CrossRef](#)]
34. Zhang, J.; Dong, C. Secure and Lightweight Data Aggregation Scheme for Anonymous Multi-Receivers in WBAN. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 81–91. [[CrossRef](#)]
35. Shi, L.; Zheng, W.X.; Liu, Q.; Liu, Y.; Shao, J. Privacy-Preserving Distributed Iterative Localization for Wireless Sensor Networks. *IEEE Trans. Ind. Electron.* **2023**, *70*, 11628–11638. [[CrossRef](#)]
36. Sheena, B.G.; Snehalatha, N. An Energy Efficient Network Slicing with Data Aggregation Technique for Wireless Sensor Networks. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021.
37. Madan, S.; Kumar, E.D.; Agnihotri, E.A. Privacy-Preserving Data Aggregation in Wireless Sensor. In Proceedings of the 2018 International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 23–24 November 2018; pp. 165–167. [[CrossRef](#)]
38. Rizvi, S.; Gualdoni, J.; Razaque, A. Securing Wireless Networks from Sinkhole and Sybil Attacks Using Secure Data Aggregation Protocol. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 721–726. [[CrossRef](#)]
39. Zhang, B. A Lightweight Data Aggregation Protocol with Privacy-Preserving for Healthcare Wireless Sensor Networks. *IEEE Syst. J.* **2021**, *15*, 1705–1716. [[CrossRef](#)]
40. Razaque, A.; Rizvi, S.S. Secure data aggregation using access control and authentication for wireless sensor networks. *Comput. Secur.* **2017**, *70*, 532–545. [[CrossRef](#)]

41. Erskine, S.K.; Chi, H.; Elleithy, A. SDAA: Secure Data Aggregation and Authentication Using Multiple Sinks in Cluster-Based Underwater Vehicular Wireless Sensor Network. *Sensors* **2023**, *23*, 5270. [[CrossRef](#)] [[PubMed](#)]
42. Sudheer, B.N.; Sujatha, K. A Brief Survey on Data Aggregation and Data Compression Models using Blockchain Model in Wireless Sensor Network. In Proceedings of the 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 14–15 March 2023; pp. 406–413. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.