electronics

MDPI

Article

SDA-RDOS: A New Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to DOS Attacks

Murat Dener

Information Security Engineering, Graduate School of Natural and Applied Sciences, Gazi University, 06560 Ankara, Turkey; muratdener@gazi.edu.tr

Abstract: In a typical Wireless Sensor Network (WSN), thousands of sensor nodes can be distributed in the environment. Then, each sensor node transmits its detected data to the base station with the help of cooperation. In this type of network, data aggregation protocols are used to increase the network's lifetime and reduce each sensor node's communication load and energy consumption. With Data Clustering, the density of data circulating in the network is reduced, thus increasing the network's life. Energy, delay, and efficiency are essential criteria in Data Clustering; however, security is another crucial aspect to be considered. A comprehensive solution for secure data clustering has yet to be seen when the literature is examined. In the solutions developed, data availability, which means that the WSN is resistant to Denial of Service (DOS) attacks, has been neglected too much, even though confidentiality, integrity, and authentication are met with different algorithms. This study developed a comprehensive, secure clustering protocol by considering all security requirements, especially data availability. The developed protocol uses the blowfish encryption algorithm, EAX mode, and RSA algorithm. The proposed protocol was theoretically analyzed, empirically evaluated, and simulated from many perspectives. Comparisons were made with LSDAR, SUCID, and OOP-MDCRP protocols. As a result of the study, a comprehensive security solution is provided and more successful results were obtained according to Energy Efficiency, Network Lifetime, Average Delay, and Packet delivery ratio criteria.

Keywords: WSN; secure data aggregation; IoT; DOS attacks

Citation: Dener, M. SDA-RDOS: A New Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to DOS Attacks. *Electronics* **2022**, *11*, 4194. https://doi.org/10.3390/electronics11244194

Academic Editor: Dimitris Kanellopoulos

Received: 12 November 2022
Accepted: 14 December 2022
Published: 15 December 2022

1. Introduction

The Wireless Sensor Network (WSN) is a wireless network in which sensor nodes cooperate to measure and monitor physical and environmental conditions. After performing the measurement task, the sensor nodes in the environment send the detection values to the base station with the help of cooperation [1]. The data coming to the base station are also transferred to the internet environment, allowing users to follow the appropriate environment from where they are. An example of a WSN is given in Figure 1.

The sensor nodes that make up the WSN consist of a sensing unit, a processing unit, a power unit, and a radio unit. Sensor nodes have three capabilities: computation, sensing, and communication. Sensor nodes consume the most energy during communication. An application's number of sensor nodes may be hundreds or even thousands. Therefore, a sensor node should cost as little as possible. For the sensor nodes to be cost-effective, hardware is preferred accordingly, and therefore the sensor nodes' processor, memory, energy, etc., is limited. There are three types of topologies in a WSN: star, tree, and mesh. Most topologies are mesh when considering real applications.

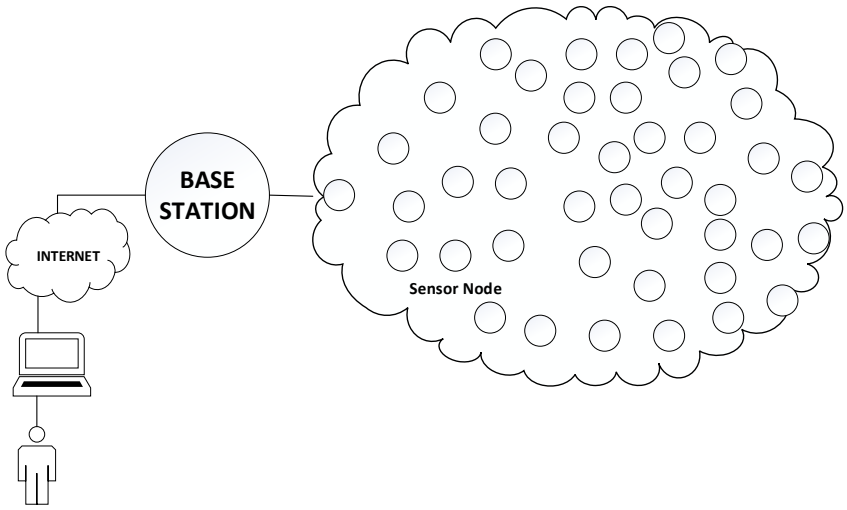

Figure 1. The general architecture of a WSN.

Moreover, the WSN types are Terrestrial WSN, Underground WSN, Underwater WSN, Multimedia WSN, and Mobile WSN. The requirements for each type are different. There are five layers in a WSN: Physical, Data Link, Network, Transport, and Application. On the other hand, Data Clustering is included in the Network layer because it is related to routing operations. Before developing a new protocol with a WSN, it is necessary to have a good grasp of the characteristics, challenges, and advantages of the WSN. Because a comprehensive security protocol that consumes much energy may be meaningless for a WSN, an energy-efficient but delay-insensitive routing protocol may be inefficient for a WSN. This information is given in the following section [2].

The WSN characteristics: Large scale, Limited resource, Redundancy, Security sensitivity, Data-centric processing, High unpredictability, Real-time constraints.

Challenges of a WSN: Limited Functional Capabilities, Limited Energy, Network Lifespan, Scalability, Redundancy, Lack of global identification, Storage, Search, and Retrieval Production Costs, in- network Processing, Latency, and Fault tolerance.

Advantages of a WSN: Robustness to Withstand Rough Environmental Conditions, Ease of Deployment, Fault Tolerance, Ability to Cover Wide and Dangerous Areas, Self-Configurable, Mobility of Nodes, Unattended Operation, Improved Lifetime, and Improved Accuracy [3].

A WSN has a wide range of applications, such as Home applications, Environmental applications, Industrial applications, Health applications, Military applications, and Commercial applications. While a WSN is one of the subsets of the Internet of Things (IoT), it is the most used technology in IoT systems.

The basis of smart systems in IoT is the WSN, that is, sensor nodes. Therefore, the WSN forms an essential part of IoT. A smart world can become possible with a WSN. There are three parts to developing an intelligent system. First, we can send any value measured from a sensor. In the second place, we can use any protocol to communicate this information. Finally, we have external systems to show these data. The raw material of all smart systems is the sensor nodes in a WSN. Smart Cities, Smart Environments, Smart Water, Smart Metering, Smart Agriculture, and Smart Animal Farming systems can be smart with a WSN. With it, a person can do whatever he/she needs with a WSN. In a WSN, data transmission of sensor nodes is a necessary process, which is very important today and will continue to develop within the IoT in the future.

Under normal conditions, the data detected by the sensor nodes are transmitted to the base station in the form of the hop by hop. However, data aggregation approaches are preferred in transmission to reduce the amount of data circulating in the network and for energy efficiency. For example, in Data Clustering, the detected data are transmitted to the collector node, and only the calculated value (sum, average, min, max, and count) is

transmitted to the base station. This way, the amount of data circulating in the network is reduced, reducing the overall energy consumption.

Providing security and the ability to use energy effectively [4] are essential for critical WSN applications. There are optimization problems, such as meeting the speed requirements of the users by minimizing the total transmission power [5], increasing the service quality, and increasing the transmission power and speed of the system [6,7]. It can be seen as an optimization problem to use the limited energy efficiency while keeping the security high for critical WSN applications.

The DOS attacks are one of the most powerful cyber weapons [8] against individuals and institutions. Therefore, many systems, including the Bayesian game theory-based mechanism [8], and DNS rule-based mechanism [9], have been proposed to reduce the impact of these attacks. At the same time, attack detections were made using techniques such as Machine Learning [10], Adaptive Quantum Artificial Immunity System [11], and Parallel Quantum Genetic Algorithm [12] using datasets.

It is a practical issue to perform a secure data clustering that addresses confidentiality, integrity, and verification, as well as detecting and defending DOS attacks in an energy and cost-effective manner.

In this study, a comprehensive new secure data clustering protocol was developed. The following are the significant contributions of this paper:

- Attributes of a suitable data aggregation protocol and security needs are mentioned.
- A detailed literature review on secure data clustering is presented.
- A new cluster selection process was carried out.
- A cluster head assistant's setup was created. In this way, a more remarkable survival of the cluster leaders is ensured.
- Blowfish + EAX part of the SDA-RDOS was developed based on a new integrated data confidentiality, integrity, and authentication approach.
- The RSA, preferred as Partially Homomorphic Encryption for this study, was used to ensure privacy and reduce the number of transactions during data clustering.
- Neglected DOS attacks were taken into account in secure data clustering. A new DOS unit consisting of a detection and defense unit was developed.
- Comprehensive security iwas provided for data clustering.
- Energy Efficiency, Network Lifetime, Average Delay, Packet delivery ratio (PDR), and Security were the performance metrics used. Comparisons were made with LSDAR, SUCID, and OOP-MDCRP protocols, and more successful results were obtained.
- A secure protocol was developed for critical WSN applications with high-security needs and consisting of many sensor nodes.

The features and security needs of a suitable data clustering protocol are explained in the second part of the study. The related studies are given in Section 3, and the proposed protocol is introduced in Section 4. Section 5 includes the comparative experimental results of the developed protocol. While the discussion section is in Section 6, the general results of the study are presented in Section 7.

2. Attributes of a Good Data Aggregation Protocol and Security Need

There are three elements in Data Clustering: sensor node, aggregator node, and base station. The gray ones are the aggregator nodes, and the white ones are the sensor nodes (Figure 2). In a large network, nodes can be displayed in a randomly distributed manner, as in Figure 1. In WSN applications, nodes are typically distributed in this way. In a WSN with data clustering, communication takes place as follows. In a WSN, cluster head nodes are selected based on specific criteria. Each sensor node sends the value it detects to the cluster head node it is connected. The cluster head node collects the data it detects from the nodes connected to it with the selected transaction function and transmits it to the base station. If the cluster head node is located far from the base station, it transmits the collected data to the base station over other cluster head nodes.

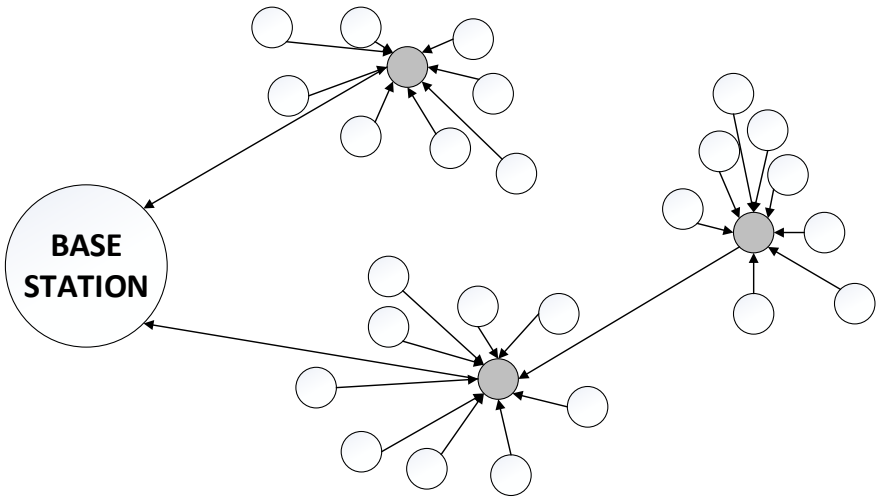

Figure 2. The general architecture of a Clustered WSN.

Below are the points to consider regarding a suitable data clustering protocol [13]. Energy: The most critical constraint in WSNs is energy because the WSN disappears when the energy of the nodes is depleted. Therefore, all work processes developed for the protocol must be energy efficient. In a WSN, Network Lifetime is directly proportional to the energy.

Latency: An essential criterion is latency for critical applications in WSNs. The work operations for the protocol must be delay sensitive.

Scalability: Depending on the application, the number of sensor nodes can be hundreds or even thousands. The designed protocol is expected to be effective in a WSN consisting of few or many nodes.

Packet Transmission Range: Packet transmission rates are expected to be high in WSNs. It can be said that a WSN works well when this ratio is high, otherwise, if this ratio is low, there is a problem with the WSN.

Communication Overhead: If communication overhead increases in a WSN, energy and bandwidth efficiency may decrease, therefore, additional control information should be used proportionately.

Data Accuracy: Evaluation of the ratio of the total number of readings received at the base station to the total number of readings generated.

Security: One of the most critical criteria in a WSN is security. As WSNs can be installed in uncontrolled environments, they may face a security problem anytime. Complete security is expected from some critical WSN applications such as military and health because an attacker who infiltrates the network can create security vulnerabilities that will put the country or people in trouble, steal critical information and use them maliciously. The following criteria are expected to be met for security in a WSN [14].

Data confidentiality: The fact that the data are not sent openly means that the data are hidden. Therefore, the attacker who gets the data gets the secret data, not the open data; these data also mean nothing to him.

Data integrity: It ensures that data are not changed on the way from source to destination. For data integrity, message authentication codes can be used.

Data freshness: The freshness of the data is important. An attacker, copying old network data, may want to send it to the network at different times to mislead the WSN and deceive it. Therefore, it should be questioned whether the data are up to date.

Source Authentication: It is determined that the node communicating with authentication is from the same WSN. This way, nodes trying to join the network with a fake identity will not get any results.

Data availability: It means that a WSN is also efficient during DOS attacks. Although there is no process of seizing the environment due to DOS attacks, the efficiency of the

network is considerably reduced. Therefore, the effect of DOS attacks should be reduced by developing detection-defense units. Examples of these attacks are the following [15–17]. Here, DOS attacks that occur at the network layer are considered.

Sybil Attack: An attempt to control the network by creating multiple fake identities in the WSN. The malicious node identifies itself with multiple identities. As a result, the malicious node can constantly send false information to the network, leading to wrong decisions. Figure 3 shows the illustration of a Sybil Attack.

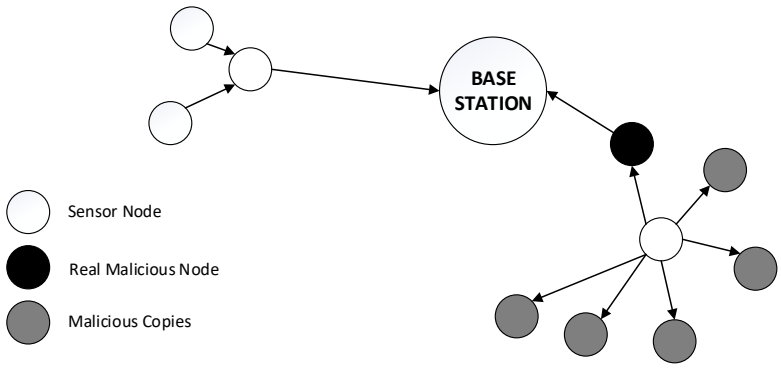

Figure 3. Demonstration of a Sybil Attack.

Sinkhole Attack: The malicious node requests almost all the traffic from a given area through a node, creating a metaphorical pit between it and the base station. The illustration of a Sinkhole Attack is given in Figure 4.

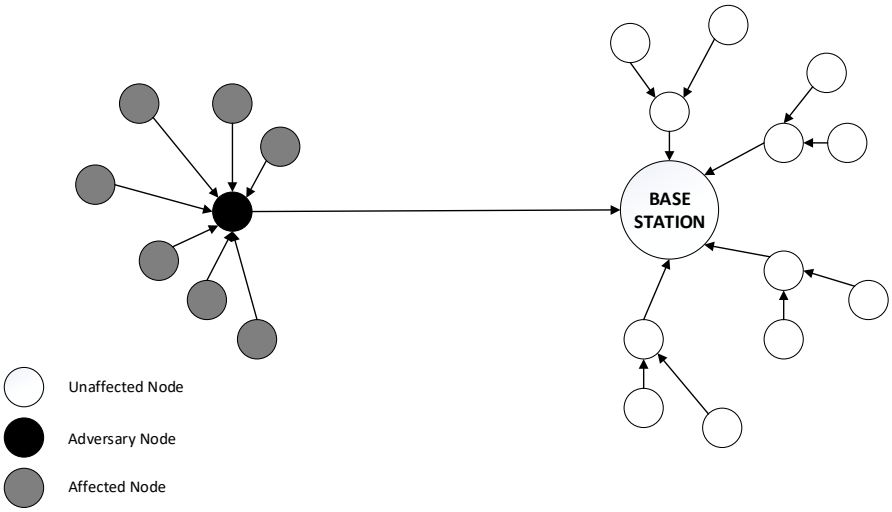

Figure 4. Demonstration of a Sinkhole Attack.

Blackhole Attack: In this attack, the malicious node identifies itself as the closest node to the base station and collects data from neighboring sensor nodes to be transmitted to the base station. The purpose of the malicious node is that the collected data does not reach the base station. Figure 5 shows the illustration of a Blackhole Attack.

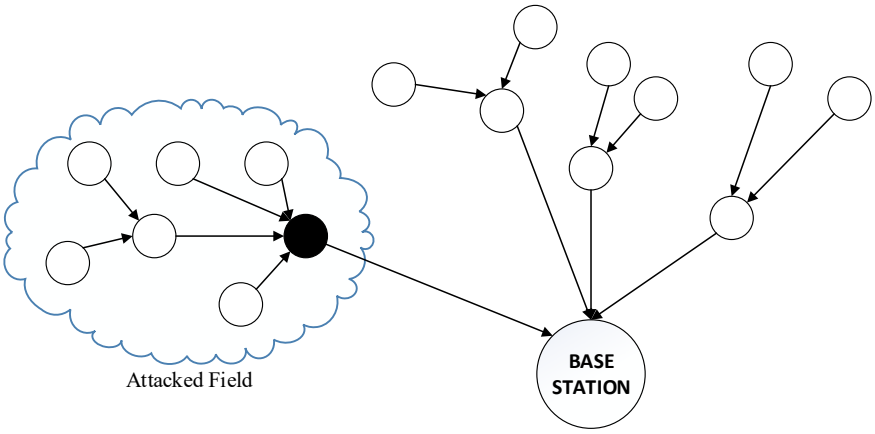

Figure 5. Demonstration of a Blackhole Attack.

Wormhole Attack: In this attack, two malicious nodes establish a high-quality communication channel between each other. They then advertise this channel for routing, collecting data from neighboring sensor nodes. However, these nodes do not transmit the data either to the base station or transmit the data by changing it. The illustration of a Wormhole Attack is given in Figure 6.

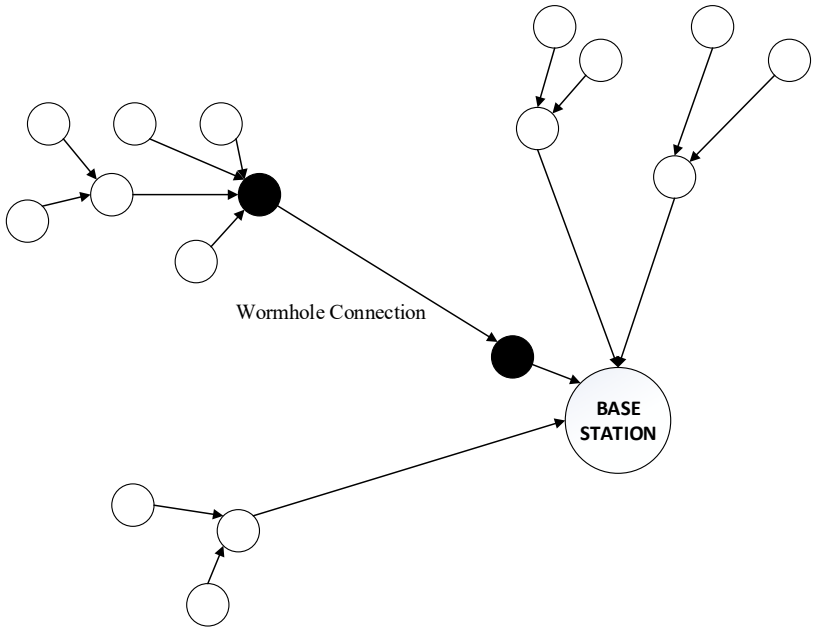

Figure 6. Demonstration of a Wormhole Attack.

Selective Forwarding Attack: In this attack, the malicious node can accept and forward some of the incoming packets and reject other packets and drop the packet. The malicious node may/may not accept packets based on specific criteria. For example, it can forward all packets from a particular node and reject them from another node. The illustration of a Selective Forwarding Attack is given in Figure 7.

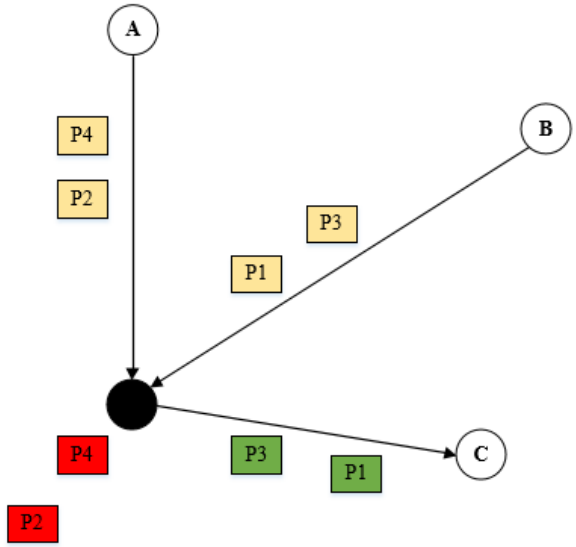

Figure 7. Demonstration of a Selective Forwarding Attack.

Hello Flooding Attack: The malicious node sends a HELLO packet to the nodes in the WSN, thus keeping the neighboring nodes busy. Figure 8 shows the illustration of a Hello Flooding Attack.

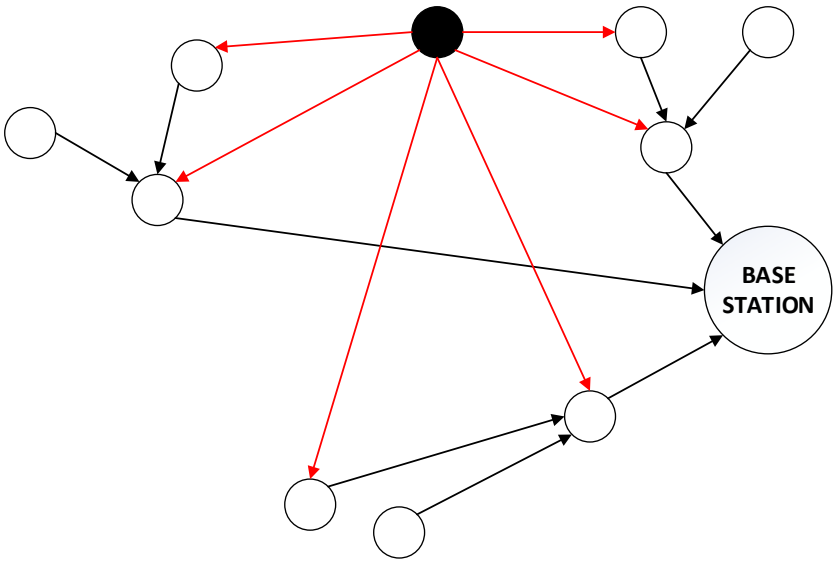

Figure 8. Demonstration of a Hello Flooding Attack.

With all this, new approaches are required for security in data clustering because data privacy can be achieved by using a symmetric algorithm in a normal non-clustering WSN. Nodes in the network perform the detection, encrypt the data, and transmit it to the base station. In base station, it decodes the data and does what is necessary. Considering a clustered WSN, the sensor nodes detect, encrypt the data, and transmit it per cluster. The cluster head decrypts the data and collects it according to the transaction function, then encrypts it and transmits it to the base station. In the base station, it decodes the data and does what is necessary. As can be seen, the WSN, which includes data clustering, had to be encrypted-decrypted twice. As a result, data privacy was violated, and the need for additional time has arisen.

3. Related Works

This section presents current studies on secure data clustering in a WSN. In the study [18], a privacy-protected data clustering protocol was developed for WSNs. In the developed protocol, the names PASKOS and PASKIS were given, considering whether or not the base station was involved in the process. It was stated that protocols reduce data loss and energy consumption and increase life expectancy. The study's main purpose was to guarantee the confidentiality of the nodes participating in the clustering process. It was emphasized that the proposed solutions are vulnerable to DOS attacks. The main idea of the protocol was to obtain key values using the hash function and use them in the clustering process. The protocol was compared with the basic data clustering protocol TAG and gave successful results.

In the study [19], a secure data clustering model supported by Fog was proposed for use in health systems. Encrypted data were communicated between the collector and the Fog server. Compression methods were also used to reduce the amount of data. Simulations were carried out in the Ns2 environment. Obtained results were better than TMT, GCEDA, and SPPDA according to Storage, Communication, Transmission Rate, Energy Consumption, and Endurance criteria.

The study [20] proposed a secure clustering protocol for large-scale WSNs. It was stated that the cluster heads close to the base station performed more data-receiving, collecting, and transmitting operations. Therefore, in large-scale networks, it was stated that the cluster heads close to the base station consumed more energy than the cluster heads far from the base station. It was emphasized that the lifetime of the WSN will be reduced due to the load imbalance to which the cluster heads are exposed. In the study, a secure clustering protocol called HCR was proposed, taking into account load balancing and scalability. The proposed protocol divided the WSN into virtual circular layers. The Ant lion optimizer technique was also used in cluster head selection. The proposed protocol was compared with PSO-ECHS, PSO-C, and BERA in the MATLAB environment in terms of Network lifetime, energy efficiency, balanced clustering, efficiency, and better results were obtained.

The study [21] recommended a safe clustering technique that prevents selective forwarding attacks. In the study, nodes were divided into three categories as Control Node, Head of Cluster, and Member Node. It was assumed that the control node knows all the job operations performed by the cluster heads. Therefore, it was desired to be protected with the control node in the clustering process as the cluster heads were the riskiest nodes. If the cluster head was attacked, all cluster elements lost their connection with the base station. In the proposed technique, there were two stages: detection and correction. The effect of selective forwarding attacks decreased with the proposed technique. The control node tries to detect the attack node using parameters such as data loss, delay time, and response time. The study was tested in an Ns2 environment considering criteria such as Packet loss rate, false detection rate, and energy consumption.

The study [22] proposed a new model for efficient data processing and secure data clustering in a large-scale WSN. Homomorphic encryption was used in the study, and it consisted of three stages. The WSN was divided into clusters in the first step, and cluster heads were selected according to the fuzzy if-then rule. In the second stage, data confidentiality was ensured by homomorphic encryption. In the third stage, message authentication codes were used for data integrity. In current techniques, cluster heads receive the data, decrypt it, apply the defined function, and re-encrypt it to transmit the result. Therefore, more transactions are made, and more delays may occur. Therefore, homomorphic encryption, which does not need data decryption without causing communication delay, was preferred in this study. The study was tested in an Ns2 environment with good results.

In the study [23], for the data clustering stages an algorithm that performs jamming detection for WSNs was proposed. The number of retransmissions of the nodes, the energy consumption per node, the time required for the network to return to a steady state, and the changes in the routing tables at the nodes were tracked for this. The study was implemented

on the simulation platform with PEGASIS, TEEN, LEACH, and HPAR and on Zigbee and LoRa as the real environment. According to the test results, the node with abnormal behavior in the proposed algorithm can be detected with low power consumption.

The study [24] proposed a heuristic approach for secure data clustering in a WSN. In real-time applications, it was stated that the sensor nodes were distributed in the environment. Moreover, it was stated that all nodes' distances and transmission ranges were different because the nodes were randomly placed. In the study, an approach required by randomly distributed sensor nodes in different geographical regions in different distributed structures was carried out. In the developed approach, the WSN environment was divided into multiple virtual rings; each ring was divided into clusters. It was tested in the MATLAB environment and had good results.

The study [25] proposed a data clustering technique that provides confidentiality and integrity using peer monitoring. The proposed technique considered privacy, flexibility, scalability, and efficiency criteria. Homomorphic encryption and lightweight key distribution technique were used in the study.

The study [26] proposed a multidimensional secure clustering model for a WSN. In addition, the study proposed a trust management scheme using the binomial distribution and a secure transmission scheme considering the environment-distance-energy-security domains. The study was tested in the MATLAB environment, compared with LEACH, I-LEACH, and LEACH-TLC, with better results.

The study [27] proposed a secure data clustering approach using the Fuzzy C-Means and ECC-ElGamal encryption algorithm. Fuzzy C-Means was used for cluster formation and cluster head selection, while the homomorphic encryption-based ECC-ElGamal encryption algorithm was used for data encryption. The proposed approach was shown to provide better security than existing ECC and RSA algorithms.

The study [28] proposed a secure clustering model that ensures confidentiality and integrity using homomorphic encryption. The proposed approach consisted of four steps that were set up, encrypt-sign, collection, and verification. The proposed approach was developed on the TinyOS 2.0 simulator (TOSSIM) and PowerTOSSIM.

The study [29] proposed a secure clustering approach in a hybrid structure. The study was based on the composition of star and tree structures. The network was geographically divided into four equal parts, with a star structure indicated in each section. Each node was assigned a parent node to transmit its data, then, the data were transmitted to the base station using the tree structure. Symmetric encryption was used in the study. The proposed method was compared with TMS, FSAMR, and EATSRA protocols in the Ns2 environment and tested according to energy consumption and data distribution latency criteria, and better results were obtained.

In the study [30], a secure clustering approach was proposed for faster detection of security threats, considering many factors in a WSN. In the proposed approach, it was stated that the energy efficiency was increased, and the delay and calculation time was reduced.

The study [31] proposed a secure clustering protocol based on QoS. Energy, network lifetime, and security were considered QoS parameters. In the proposed protocol, in the first place, temporary cluster heads were determined using an adaptive neuro fuzzy based clustering technique according to the criteria of residual energy, distance from the base station, and distance to neighbors. Then, among the temporary cluster heads, the most suitable ones were selected as cluster heads with the deer hunting optimization (DHO) algorithm. Finally, an intrusion detection system was developed, which uses a deep belief network to detect malicious nodes in the network. The proposed protocol was tested in MATLAB and compared with the IPSO algorithm, KHA, F5NUCP, and FUCHAR. It gave better results in terms of energy efficiency, network lifetime, packet delivery rate, average latency, and attack detection rate.

The study [32] suggested a safe clustering technique with cluster head selection. Particle Swam Optimization and Water Wave Optimization were integrated and used in

the proposed technique. To measure the performance of the technique, the number of live nodes, the coverage area, the energy balancing index, and the average remaining energy according to the number of laps were considered. It was compared with DICMLA and P-SMO and gave better results.

The study [33] proposed a hybrid secure data clustering approach for WSNs. In the study, an optimal slice selection process was carried out to increase the network's performance and ensure confidentiality. Fuzzy logic was used in this process. The study gave better results than PECDA and SMART as it was tested in a MATLAB environment, considering low communication load, energy efficiency, and safety criteria.

The study [34] proposed a secure data clustering protocol that can detect malicious nodes in a WSN. The tree topology was taken as a reference in the study. In the proposed protocol, the threshold value was determined for each node; it was calculated based on the number of data packets transmitted and the number of successfully received data packets. According to the threshold value, the node was either in the normal or blocked list. In this protocol, it was checked whether each node was reliable. The study was tested in an Ns2 environment.

The study [35] recommended a privacy-protected clustering protocol using the elliptic curve cryptosystem in a WSN. The study was tested in the MATLAB environment and compared with RIX-ECDLP, ESR, and LEACH-MAC according to processing time, packet delivery rate, energy consumption, average latency, network processing load, and network lifetime, and better results were obtained.

The study [36] proposed a secure clustering approach using the Integration of Distributed Autonomous Fashion with Fuzzy If-then Rules algorithm. The cluster head can be selected by considering the energy, efficiency, and quality of the node. Packet delivery rate dropped packet rate, residual energy level, network life, and energy consumption criteria were tested, and successful results were obtained.

The study [37] proposed a load-balanced and authentication-based clustering approach. In the study, researchers stated that the cluster heads in the active area can be overloaded compared to the cluster heads in the less active areas. This problem has not been fully taken into account in the current studies. In the study, load balancing and secure authentication were combined. The nodes' real-time load and energy values were considered for load balancing. The study gave better results than S-LEACH, MS-LEACH, and SS-LEACH in terms of packet transmission rate, network lifetime, and compute load criteria.

In the study [38], redundant data were eliminated with the k-means clustering algorithm for efficient data clustering in a WSN. In the study, it was stated that a network will perform more efficient data clustering by eliminating redundant data. The study proved that meaningless data can be eliminated, and data can be put together intelligently. The study was compared with the EK-means algorithm according to speed and energy criteria and gave good results.

The study [39] proposed a secure data clustering approach using the autoregressive integrated moving average model, a time series technique. It was stated that data integrity protection was not taken into account in the study that ensures data confidentiality. The study was tested considering accuracy, computational cost, and communication cost criteria. The ESDA, TAG, CPDA, and RPDA were compared and gave better results.

The study [40] proposed a secure data clustering model that provides query-based privacy protection in a WSN. As a result, computational complexity was reduced, and data confidentiality was ensured with homomorphic encryption by combining multiple queries in a single package. The work was tested in the MATLAB environment and proven to reduce energy consumption and protect data privacy.

The study [41] proposed a secure data clustering approach that detects selective forwarding based on the Noise-Based Density Peaks Clustering (NB-DPC) algorithm. The study was tested in the MATLAB environment and it was observed that nodes exhibiting abnormal behavior were detected.

In the study [42], an energy-efficient and privacy-protected secure data clustering algorithm was proposed for the WSN that consisted of three stages. The tree topology was created in the first stage, and the leaf nodes were organized. In the second step, the data collected by the leaf nodes were sliced, and the data pieces were sent to the neighboring nodes. In the last stage, data collection was carried out. The study was tested in the MATLAB environment and compared with SMART and PECDA considering communication load, energy consumption, privacy protection, and accuracy criteria, and it gave better results. It was emphasized that future work related to reducing redundant and useless data in data clustering is needed.

In the study [43], an integrated trust-based energy-efficient data clustering approach was proposed for a WSN. Neighbors with less communication overhead were defined for each node. The route path was determined according to the confidence value gained. The Greedy Congestion Sensitive Data Collection model was used to increase the packet delivery rate. The study was tested in an Ns2 environment and compared with HRM and BTEM considering communication overhead, energy consumption, and packet delivery rate criteria, and better results were obtained.

In the study [44], a new confidence function-based approach was proposed for cluster head selection in a WSN. The Threshold value was calculated for cluster head selection. The remaining energy of the node and the distance from the base station was used when calculating the threshold value. In this way, random cluster head selection was presented in the study. The study was tested in the MATLAB environment and compared with the Stable Election Protocol, considering the criteria of network lifetime, stability time, and node survival rates, and gave better results.

The study [45] proposed a secure clustering approach using Integer Matrix Keys in a WSN. It was to ensure data confidentiality and data integrity by placing the digital signature on the collected data and using integer matrices as keys.

The study [46] proposed an efficient clustering approach that ensured data integrity, wherein a new key management scheme was proposed, and data integrity was ensured and verified by neighboring nodes in the environment without needing a base station. The study was tested in the TinyOS environment, compared with CMT, SAWN, SecureDAV, SDAP, and SHAN, and gave better results, considering the criteria of energy consumption and mean time to fake data detection.

The study [47] proposed a secure clustering protocol using the A-star heuristics algorithm and one-time pad (OTP) encryption scheme. The study was tested in the NS2 environment and showed success in energy consumption, network lifetime, end-to-end latency, and packet drop rate criteria.

As can be seen from these related studies, a comprehensive, secure data clustering protocol focusing on data availability has not yet been developed. In fact, in a recent review [48], this situation was mentioned, and it was stated that availability from the Confidentiality, Integrity, and Availability (CIA) was an inevitable research topic. In the study [48], current research was illustrated in Figure 16 [48], and it was said that availability was neglected quite a lot.

In this study, a new secure data clustering protocol focused on data availability was developed.

4. Proposed Protocol

In this section, the network model, communication model, and proposed protocol are introduced.

4.1. Network Model

A WSN having an area a $\times$ a square units and N number of Sensor Nodes are deployed randomly. The base station is located at the head of the WSN and has unrestricted computational ability, storage, and battery power. Further, all the Sensor Nodes have similar storage, transceiver, and battery power. It is assumed that base station knows

the location of all Sensor Nodes, which can be obtained from localization techniques or received signal strength indicator value. Communication is done using the CSMA\CA technique to avoid any packet collisions. There are four types of nodes: the base station with unlimited energy, cluster head node, cluster head assistant nodes, and end nodes. End nodes are responsible for continuously sensing data and transmitting results to cluster nodes. Cluster nodes, in turn, are responsible for aggregating data and forwarding data to the base station. On the other hand, Cluster Head Assistant can be used to be the head of the cluster when necessary and to provide coordination between the base station and the cluster when necessary. Thanks to the cluster head assistant, the nodes' energy levels and load balances are protected.

It is known that a typical network in a WSN consists of a random distribution of sensor nodes. Even though a WSN is now used in most areas, one of the original aims of the WSN was to be able to establish networks in places that could not be networked, for example, on borders, near valleys, in impenetrable woodlands, etc. The WSNs were formed by scattering thousands of pre-programmed sensor nodes, such as via a helicopter, from a high place. Consequently, in some areas, the sensor nodes were dense, while in others, they could be sparsely distributed. Furthermore, in real nature applications, the base station's location is outside, not in the middle of the area where the sensor nodes are located. The study was carried out considering these criteria.

The base station manages the operation of the network, which is important for security. Otherwise, a compromised cluster head can threaten more networks than a compromised node. It should be considered that when control nodes are created within the WSN, they can also be captured. Therefore, the control must be done by the base station. Routing tables are created for each node by the base station in the network, clusters are created and followed. Tables are updated at specified time intervals. The base station provides the coordination of the network together with cluster heads and cluster head assistants. When necessary, the base station can also communicate directly with the end nodes.

4.2. Cluster Selection Process/Setup Process

In this study, first, the nodes were randomly distributed to the environment, then, clusters were formed by dividing the available area into n equal parts. The first view of the network is given in Figure 9.

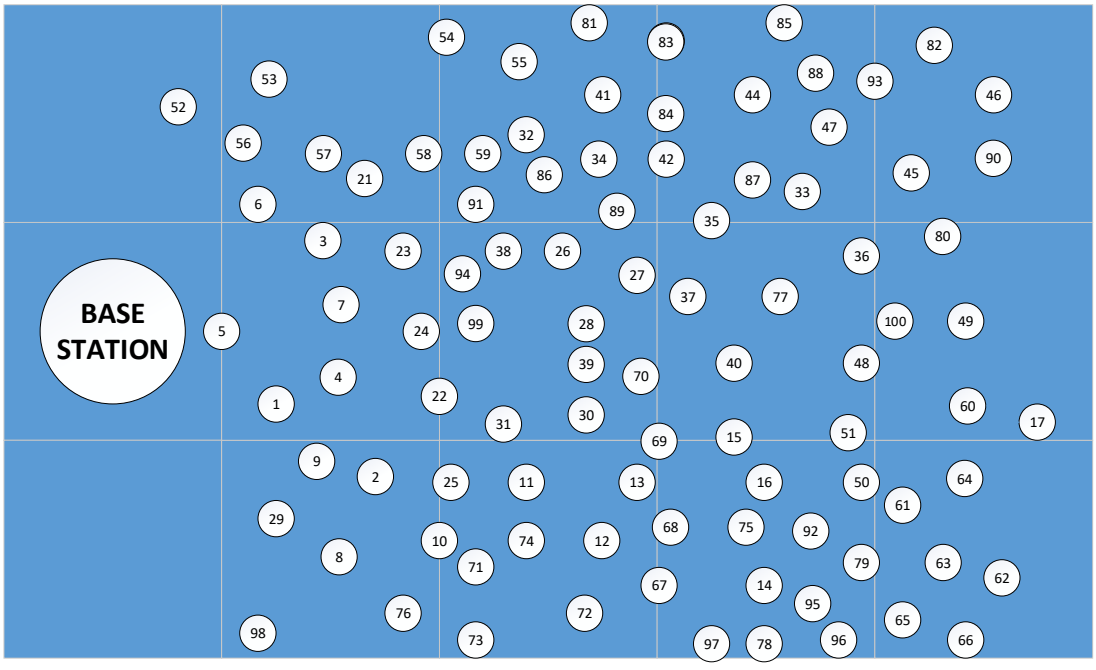

Figure 9. First view of the network.

For example, there are 15 split areas in Figure 10. As can be seen, the number of nodes in each area differs from that in real environments. For example, there is one node in the 1st area, there are eight nodes in the 2nd area, 14 in the 3rd area, 11 in the 4th area, and six in the 5th area. Table 1 gives each cluster's nodes, number, and common cluster nodes. When determining the cluster nodes in each area, first, it starts with the nodes close to the center point, then it continues outward. It is known that when writing the cluster nodes from the inside to the outside, the ones written first are the cluster head candidates, and the remaining nodes are out of the field. If the node carries over to both domains, it is numerically added to the number of clusters in each domain and is also shown in the common nodes section.

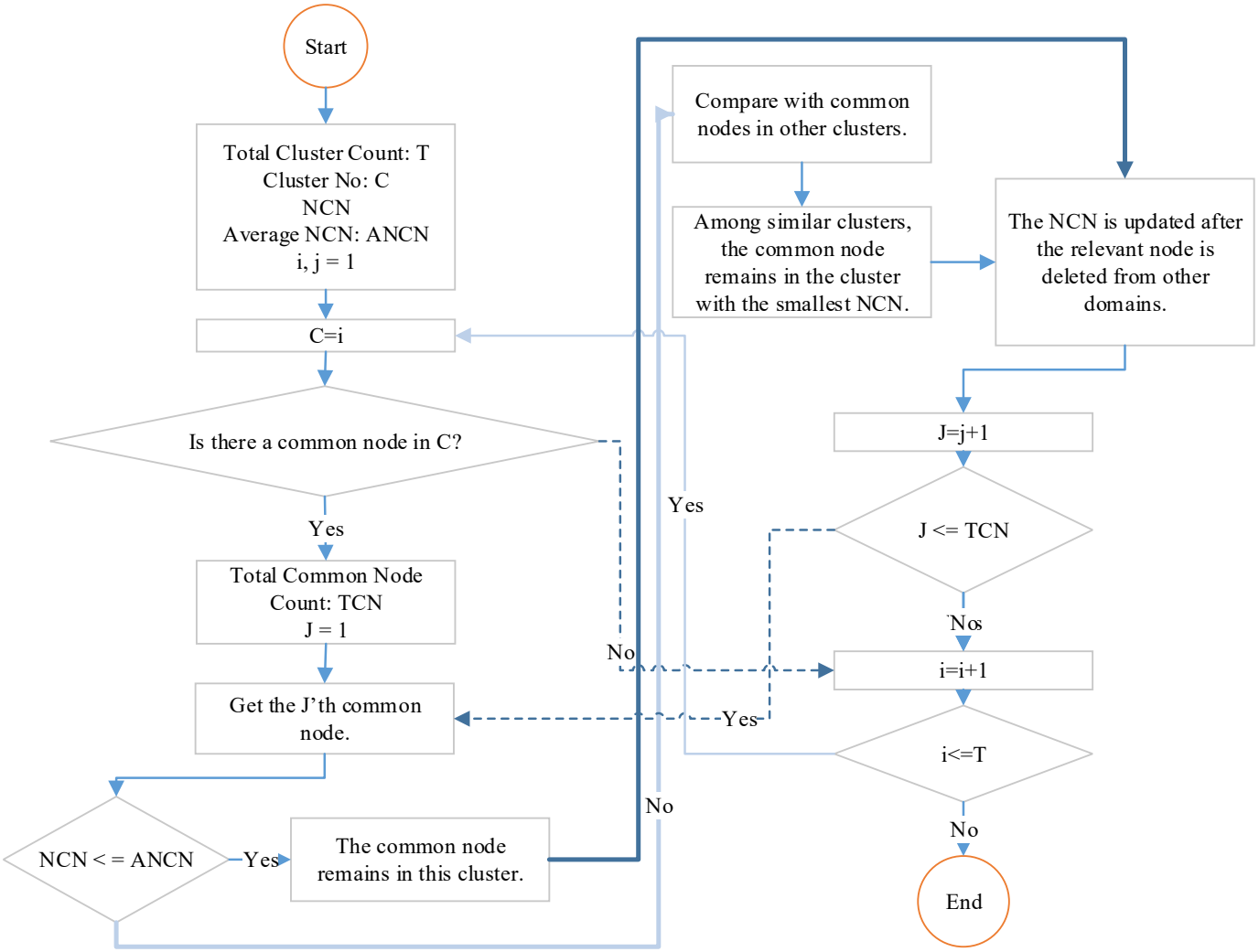

Figure 10. Flowchart determining actual clusters of common nodes.

Table 1. The initial state of the nodes.

Cluster No	Cluster Nodes	Common Nodes	NCN *
1	52		1
2	57, 21, 53, 56, 6, 58, 54, 3	6, 58, 54, 3	8
3	32, 86, 34, 41, 55, 59, 81, 91, 89, 54, 83, 84, 42, 58	91, 89, 54, 83, 84, 42, 58	14
4	44, 88, 47, 87, 33, 85, 83, 84, 42, 35, 93	83, 84, 42, 35, 93	11
5	46, 90, 45, 82, 93, 80	93, 80	6
6	Base Station	-	-
7	7, 4, 1, 23, 5, 3, 24, 22, 6	3, 24, 22, 6	9
8	28, 39, 26, 99, 38, 30, 94, 27, 70, 31, 22, 69, 89, 91, 24	70, 31, 22, 69, 89, 91, 24	15
9	77, 40, 37, 36, 48, 51, 35, 15, 69, 70	36, 48, 51, 35, 15, 69, 70	10
10	49, 60, 100, 17, 80, 36, 48	17, 80, 36, 48	7
11			-
12	8, 2, 29, 76, 9, 98, 10, 25	10, 25	8
13	74, 12, 71, 11, 72, 13, 73, 25, 67, 10, 69, 68, 31	25, 67, 10, 69, 68, 31	13
14	75, 92, 14, 95, 16, 97, 78, 96, 79, 50, 68, 67, 69, 15, 51	79, 50, 68, 67, 69, 15, 51	15
15	62, 63, 64, 61, 65, 66, 50, 79, 17	50, 79, 17	9

* NCN: Number of Cluster Nodes.

The number of clusters that should be in each cluster in the network is calculated with the help of Equation (1).

$$\text{Number of clusters required} = \text{Total Number of Cluster Nodes}/\text{Total Area} \quad (1)$$

When the total number of Cluster Nodes is divided by 126 and the total area by 13, the result is 9.6. That is, the number of cluster nodes for each domain should be approximately nine. The area with the base station (6) and the area with no nodes (11) are not taken into account in the Total Area part. In a network where random nodes are distributed, the network may not work efficiently if there is an obvious imbalance between clusters, for example, having 15 nodes in one cluster and one node in another makes the network unstable.

As the next operation, the actual clusters of common nodes must be determined so that the Cluster Node Number can be nine. The actual clusters of common nodes are determined according to the flow given in Figure 10. The flow is as follows: Starting from the first cluster (i), the common node list (j) is looked at sequentially. The first common node is taken, in turn, compared to all the common nodes in other fields. Next, the partner node is added to the field; whichever cluster it is in has the lower NCN number and is deleted from the other clusters. If the NCN is less than or equal to the mean, the common node is left in this field and deleted from the others. The NCN count is updated after the relevant node is deleted from other domains. The NCN count is reduced by one from the cluster whose partner node is deleted. The flow continues until the actual clusters of all common nodes are determined. After the operations, the few remaining nodes in the cluster are included in the nearest cluster.

After the operations, the final state of the network is given in Figure 11 and the final state of the nodes is given in Table 2.

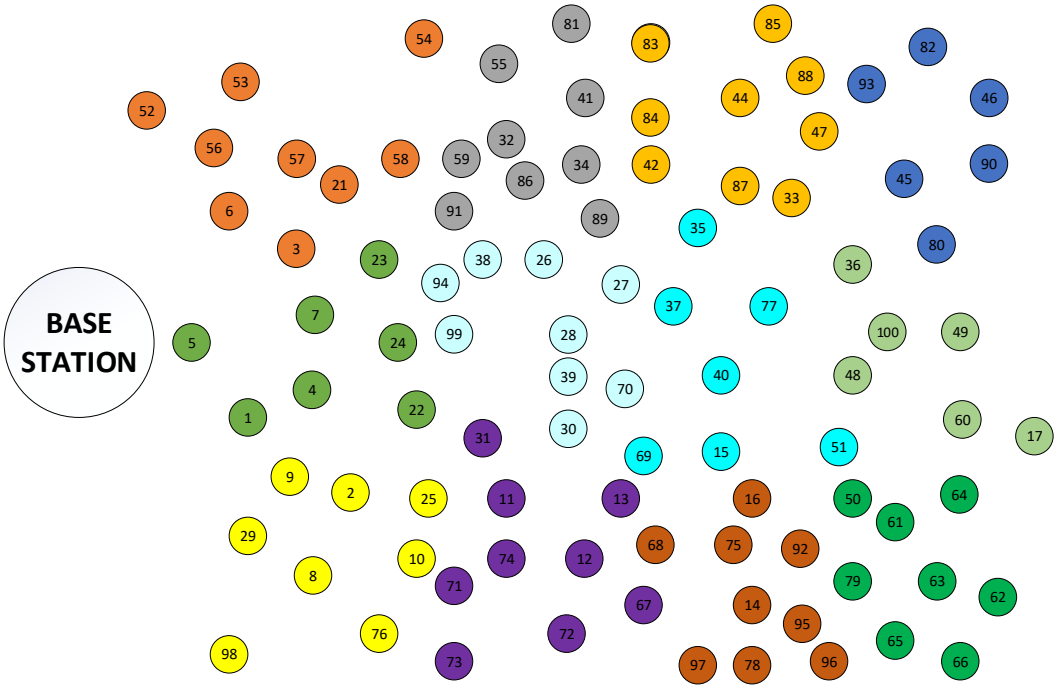

Figure 11. The final state of the network.

Table 2. The latest status of the nodes.

Cluster No	Cluster Nodes	Common Nodes	NCN *
2	57, 21, 53, 56, 6, 58, 54, 3, 52		9
3	32, 86, 34, 41, 55, 59, 81, 91, 89		9
4	44, 88, 47, 87, 33, 85, 83, 84, 42		9
5	46, 90, 45, 82, 93, 80		6
6	Base Station		-
7	7, 4, 1, 23, 5, 24, 22		7
8	28, 39, 26, 99, 38, 30, 94, 27, 70		9
9	77, 40, 37, 51, 35, 15, 69		7
10	49, 60, 100, 17, 36, 48		6
11			-
12	8, 2, 29, 76, 9, 98, 10, 25		8
13	74, 12, 71, 11, 72, 13, 73, 67, 31		9
14	75, 92, 14, 95, 16, 97, 78, 96, 68		9
15	62, 63, 64, 61, 65, 66, 50, 79		8

* NCN: Number of Cluster Nodes.

In this way, clusters are determined in the network. As a result, energy and load balancing in the network are positively affected since the number of nodes of all clusters is brought close to each other.

4.3. EAX

The authors who developed OCB analyzed CCM in five different categories, namely efficiency, parameterization, complexity, variable-tag-length subtleties, and some wrong security claims, and revealed many disadvantages [49]. As a result, the authors have

developed a new mode of operation called EAX, which preserves the main features of CCM and eliminates the disadvantages they have stated. The EAX mode [50] was submitted on 3 October 2003, to the attention of NIST in order to replace CCM as the standard AEAD mode of operation as the CCM mode lacks some desirable attributes of EAX and is more complex. The representation of EAX is given in Figure 12.

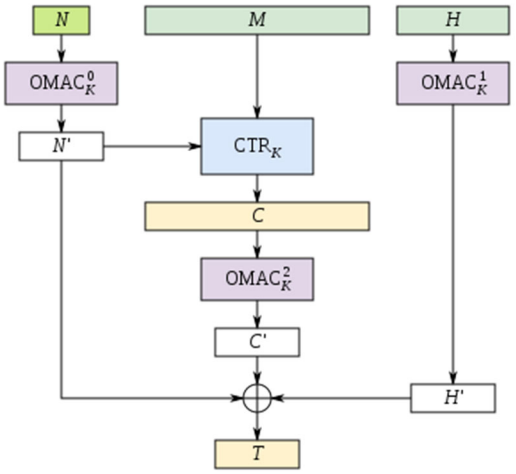

Figure 12. The general architecture of EAX (M—message, K—key, H—authenticated header, N—nonce, C—encrypted message, T—authentication tag).

The EAX mode (encrypt-then-authenticate-then-translate) is a mode of operation for cryptographic block ciphers. It is an Authenticated Encryption with Associated Data (AEAD) algorithm designed to simultaneously provide authentication and privacy of the message (authenticated encryption) with a two-pass scheme, one pass for achieving privacy and one for authenticity for each block. In the studies, different transaction modes were compared, and it was seen that the EAX mode could be a good choice for WSNs [51–53], therefore, it was chosen in this study.

4.4. Blowfish

Blowfish [54] is an encryption technique designed by Bruce Schneier in 1993 as an alternative to the DES Encryption Technique. It is significantly faster than DES and provides a reasonable encryption rate with no effective cryptanalysis technique found to date. The Blowfish algorithm is executed in three steps, generation of subkeys, initialization substitution boxes, and encryption.

Step 1: 18 subkeys {P [0] . . . P [17]} are needed in both encryption as well as decryption process, and the same subkeys are used for both processes. These 18 subkeys are stored in a P-array, with each array element being a 32-bit entry.

Step 2: 4 Substitution boxes (S-boxes) are needed {S [0] . . . S [4]} in both encryption as well as decryption process, with each S-box having 256 entries {S[i][0] . . . S[i][255], 0&lei&le4} where each entry is 32-bit.

Step 3: The encryption function consists of two parts: Rounds: The encryption consists of 16 rounds with each round (Ri) taking inputs from the plainText (P.T.) from the previous round and the corresponding subkey (Pi). Post-processing: The output after the 16 rounds is processed as follows: Every round r consists of four actions: Action 1—XOR the left half (L) of the data with the r th P-array entry. Action 2—Use the XORed data as input for Blowfish's F-function. Action 3—XOR the F-function's output with the right half (R) of the data. Action 4—Swap L and R. In the studies, different encryption algorithms were compared, and it was seen that the Blowfish algorithm could be a good choice for WSNs [55–57], therefore, it was chosen in this study.

The Blowfish + EAX part of the SDA-RDOS was developed based on a new integrated approach. It mainly utilizes the idea that the Blowfish encryption algorithm is restructured using EAX. The Blowfish + EAX portion of the schema of SDA-RDOS is depicted in Figure 13.

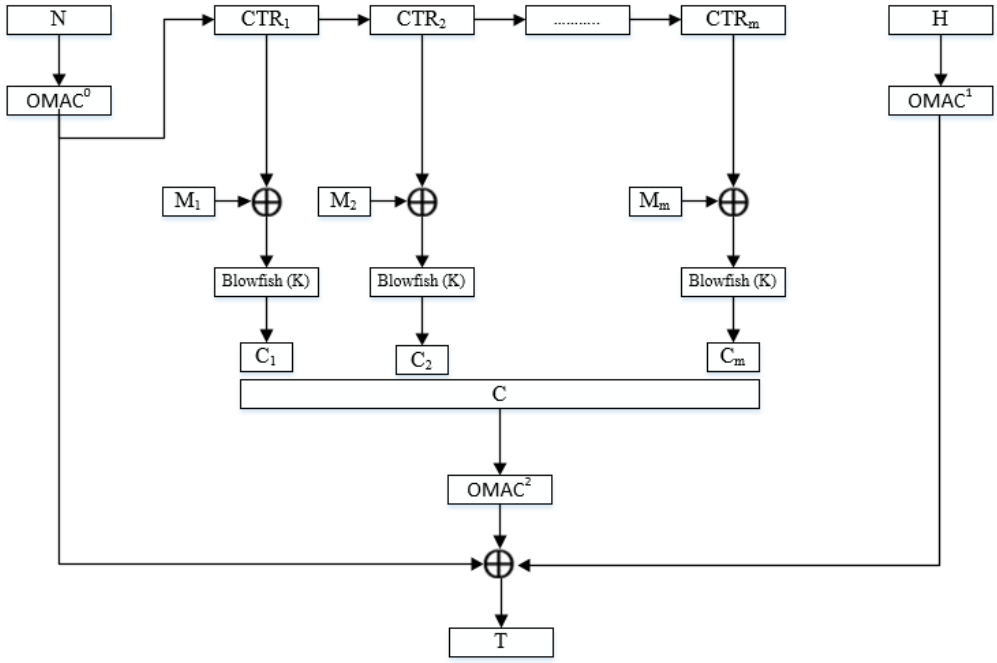

Figure 13. Blowfish + EAX part of SDA-RDOS Protocol.

The Blowfish + EAX part of SDA-RDOS consists of eight steps. These are listed below:

First Step: The Entered message is divided into blocks of 64 bits (M [1], M [2], ... M [m]). If the last message block is not 64-bit, then the remaining bits are filled with 0's.

Second Step: NONCE value is a random value. An OMAC algorithm encrypts the generated NONCE value. (N')

Third Step: N' value is encrypted with CTR. This result is processed the same as the first message block. This process continues sequentially until each message is blocked. Then, the message block is xored with the result obtained from CTR operations as many as the number of blocks.

Fourth Step: The result obtained is encrypted with the Blowfish algorithm. The encrypted message block is obtained.

Fifth Step: The encrypted message is encrypted with the OMAC algorithm. (C')

Sixth Step: The H value is encrypted with OMAC. (H')

Seventh Step: N' value, H' value, and C' values are Xored. The selected t bit is used as the Tag. The generated tag value is then used for data authentication.

The last step consists of the encryption of all the values and the production of the encrypted script with the tag value.

4.5. RSA—Partial Homomorphic Encryption

Data clustering is a structure that enables the sensors in the network to save energy by reducing the amount of data. To avoid security problems, the party sending the data should encrypt it and send it to the base station. However, the sensors on the path of the data must make the data clear text and perform the data set operation. Security and data clustering work in opposition to each other [58]. The party sending the data to the base station sends the data with symmetric key encryption. The sensors on the network decrypt the data, cluster the data, and then send the data by performing the encryption process again. Data loses its confidentiality during these processes [58]. Homomorphic

Encryption structure can be used both to ensure data confidentiality and to perform data clustering. Thanks to the Homomorphic Encryption structure, the party sending the data to the base station encrypts the data. The sensors on the network perform the data aggregation process and send the data without performing the decryption process. As the encrypted data are not opened along the way, data confidentiality is ensured, and data clustering is performed [58].

Homomorphic Encryption [59,60] is a structure that allows performing different types of transactions in countless numbers without being limited to a single operation type on encrypted data. The Homomorphic Cipher structure can basically be thought of as a ring homomorphism. For example, let A be plaintext space, B ciphertext space, Enc() encryption algorithm, and Dec() decryption algorithm. Accordingly, the encryption process can be considered a function defined from the A ring to the B ring [61].

Enc():$A \rightarrow C$

$m1, m2 \in A$;

$$\text{Enc}(m1) \oplus \text{B Enc}(m2) = \text{Enc}(m1 \oplus \text{A } m2) = \text{Dec}(\text{Enc}(m1 \oplus \text{A } m2)) = m1 + m2 \quad (2)$$

$$\text{Enc}(m1) \otimes \text{B Enc}(m2) = \text{Enc}(m1 \otimes \text{A } m2) = \text{Dec}(\text{Enc}(m1 \otimes \text{A } m2)) = m1 \times m2 \quad (3)$$

It can be shown as a Homomorphic Encryption structure.

Full-Homomorphic Encryption supports addition and multiplication operations simultaneously and an unlimited number of times. If we add or multiply the contents of two or more ciphertexts, when we decrypt the result, the plaintext we get should be the same as if we had performed operations on the unencrypted information. The partially Homomorphic Encryption method was preferred in this study as the communication costs required by fully homomorphic encryption methods are very high compared to the WSN. Furthermore, partial HEs are preferred because they are faster than Fully HEs and their ciphertext size is smaller. Partial homomorphic encryption is the most important type of homomorphic technique; it performs the computation on some of the mathematical operations and has high efficiency for practical applications. Most PHE schemes support one type of operation.

The homomorphic property of RSA [62–66], which was preferred as Partial HE for this study, was introduced later by Rivest, Adleman, and Dertouzous using the term "privacy homomorphism" [67], which was an early example of PHE. The RSA scheme involves four algorithms as follows:

Keygen Algorithm: The public key is two integers (n, e), where n = pq and p, q are large primes and e chosen such that gcd (e, φ(n)) = 1, where φ(n) = (p − 1)(q − 1) and namely e is invertible (mod φ(n)). The secret key is (d, n), where d is determined such that d is the inverse of e (i.e., ed = 1 (mod φ(n))).

Encryption Algorithm: First, the message is converted into a plaintext m E Zn, then computes the ciphertext c as follows:

$$\text{E(m)} = \text{me (mod n)} = \text{c}, \quad (4)$$

where the ciphertext c ∈ Zn.

Decryption Algorithm: Takes the secret key (d, n) with ciphertext c to decrypt

$$\text{D(c)} = \text{cd (mod n)} = \text{m}, \quad (5)$$

because d is the multiplicative inverse of e in Zn, then ed = 1 (mod φ(n)).

Homomorphic Property: For m1, m2 ∈ Zn,

$$E(m1) \times E(m2) = (m1e \pmod n) \times (m2e \pmod n), \quad (6)$$

$$= (m1 \times m2)e \pmod n, \quad (7)$$

$$= E(m1 \times m2). \quad (8)$$

As we can see, the homomorphic multiplication property of RSA can evaluate E(m1 × m2) directly from E(m1) and E(m2) without decrypting them. RSA was chosen because it is more efficient than other PHEs [68–70].

4.6. DOS Mode

The DOS unit consists of two parts, the detection and defense unit. Figure 14 shows the representation of the DOS unit.

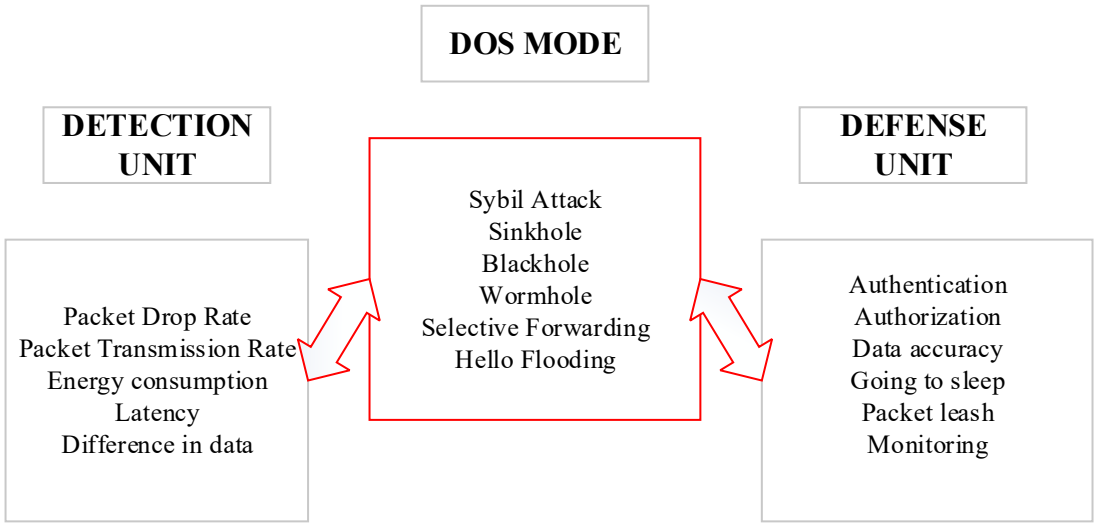

Figure 14. Dos Mode part of SDA-RDOS Protocol.

Detection Unit: If something is wrong with the network, it is the unit that works to reveal it. If a DOS attack occurs during the operation of the network, the following situations may occur. These; Packet Drop Rate increases, Packet Transmission Rate decreases, Energy Consumption increases, and Latency increases.

As explained earlier, this information for each cluster is monitored by the base station. If a result above the threshold values occurs, an attack is detected. At the same time, clusters and nodes are monitored by the base station. If there is a difference between the values from the nodes or cluster heads and the base station, this is a problem. Central management is based on the base station because the base station energy is considered unlimited. Average values from all cluster heads in the environment are checked. If there is a cluster head with a difference in mean values, data are requested from all nodes in this cluster for proof testing. It is checked whether there is an attack by processing the incoming data.

Defense Unit: For defense, Packet Leash, Authorization, Authentication, Monitoring, Data accuracy, and Sleeping methods [71–73] are used.

Packet Leash: It is determined by how many steps each node will send the packet. The base station initially determines it. If it exceeds this number of stages, the packet is dropped. In this way, a limit is placed on the circulation of the packet in the network.

Authorization: In the base station, all clusters and cluster heads, cluster head assistants, and cluster nodes are all registered. All nodes are centrally managed, authorized, and authorized by the base station. It can warn clusters based on base station calculations. Each

of the nodes in the network has an id and is authenticated by the cluster leaders and their neighbors, namely the cluster head helpers. No packets are received from any node whose id does not match the network. Threshold values for packet transmission/drop rate, energy consumption, and delay parameters are determined, and nodes above the threshold values are removed from the communication for a certain period.

Authentication: During the network setup, there are embedded codes in each node that cannot be seen even by those who take over the node. The verification unit uses these codes. If there is compatibility in the codes obtained after a process with the sent code, there is no problem with the nodes. The authentication mechanism between the base station and the nodes is as follows: The base station requests a message from the node it wants to authenticate. Node A encrypts the message (ID etc.) with its private key followed by the symmetric key and sends it to the base station. Base station decrypts the incoming message with its private key and authenticates A, then decrypts the remainder with A's public key. If successful, node A is validated. These transactions can also occur between two nodes or the cluster head and cluster member nodes. The identity of each node in the cluster with the problem is authenticated. The problematic node is removed from the routing lists, and new notifications are re-transmitted to the nodes.

Monitoring: In the cluster with the problem, first of al, cluster head replacement is made, considering that the cluster head is exposed to the attack. Member nodes transmit their data per new cluster. The new cluster head also transmits it to the base station. The previous cluster head may have been attacked if there is no problem with the threshold values or if it is not used for a certain time. If the problem persists, data are received sequentially and sent to the base station, with only one member node left out. According to the incoming values, the node which has a problem is removed from the routing lists or not used for a certain period.

Data accuracy: The nodes in the cluster transmit the data they detect to the cluster heads. Cluster heads also transmit these data to the base station by summing/averaging. At the specified time intervals, the base station requests data separately from the relevant cluster head and the related cluster member nodes to prove the data accuracy. It guarantees data accuracy by comparing incoming data. In this way, wrong decisions are avoided in the network.

Going to sleep: In some DOS attacks, continuous messages are sent only to keep the node busy instead of hijacking data and sending false information to the network. The aim is that the node cannot transmit the data it needs to send and reduces the energy of the node. Considering the enemy node has limited energy, our node can be put to sleep as a defense mechanism.

4.7. Communication

In clustered networks, the attack or hijacking of the cluster head affects all cluster nodes. Therefore, the importance of cluster heads further increases. In this study, cluster head assistants were created to prevent this situation, balance the energy-efficiency status of the cluster heads, and obtain information about the cluster. In the list created regarding Table 2, the first nodes are assigned as cluster heads, the following two nodes as cluster head assistants, and the remaining nodes as cluster member nodes. Information about the 2nd, 7th, and 10th clusters is given in Table 3.

Table 3. Information on the 2nd, 7th, and 10th Clusters.

Cluster Number	Cluster Head	Cluster Head Assistants	Cluster Member Nodes
2	57	21, 53	56, 6, 58, 54, 3, 52
7	7	4, 1	23, 5, 24, 22
10	8	2, 29	76, 9, 98, 10, 25

After the network is established, the base station creates the routing table for each node, then, this information is transmitted to the relevant nodes. In this way, the nodes in the network transmit the data they detect only to the specified target nodes. For example, the routing table of cluster 2 is given in Table 4.

Table 4. The routing table of cluster 2.

Source Node	Destination Node	Hop Count
52	57	1
3	57	1
54	57	1
58	57	1
6	57	1
56	57	1
53	57	1
21	57	1
57	Base Station	2 (7)

When the base station receives data from all cluster heads, it simultaneously checks them. The number of packets from each cluster records the values temporally. It monitors the energy levels of the nodes, taking into account the number of incoming packets and the communication density. The base station requests data from the cluster nodes at specified intervals. The routing information can only be changed by the base station.

As seen in Figure 15, the communication of base station with cluster heads or cluster head helpers is again with Blowfish + EAX. The blowfish + EAX model was applied here in a new way to ensure data confidentiality-integrity in the setup-initial communication between the base station and the nodes. Confidentiality and security must also be ensured in the process of determining the subsequent behavior of the network. It is an essential process for the network. The RSA Homomorphic method was used in data clustering, being preferred as there is no need for decrypt-encrypt operations again during the clustering phase. During the data collection phase, member nodes perform detection operations. The detected values are averaged over the cluster head nodes and transmitted to the base station. Thanks to the central control carried out by the base station, the security and coordination of the network were increased to the highest level.

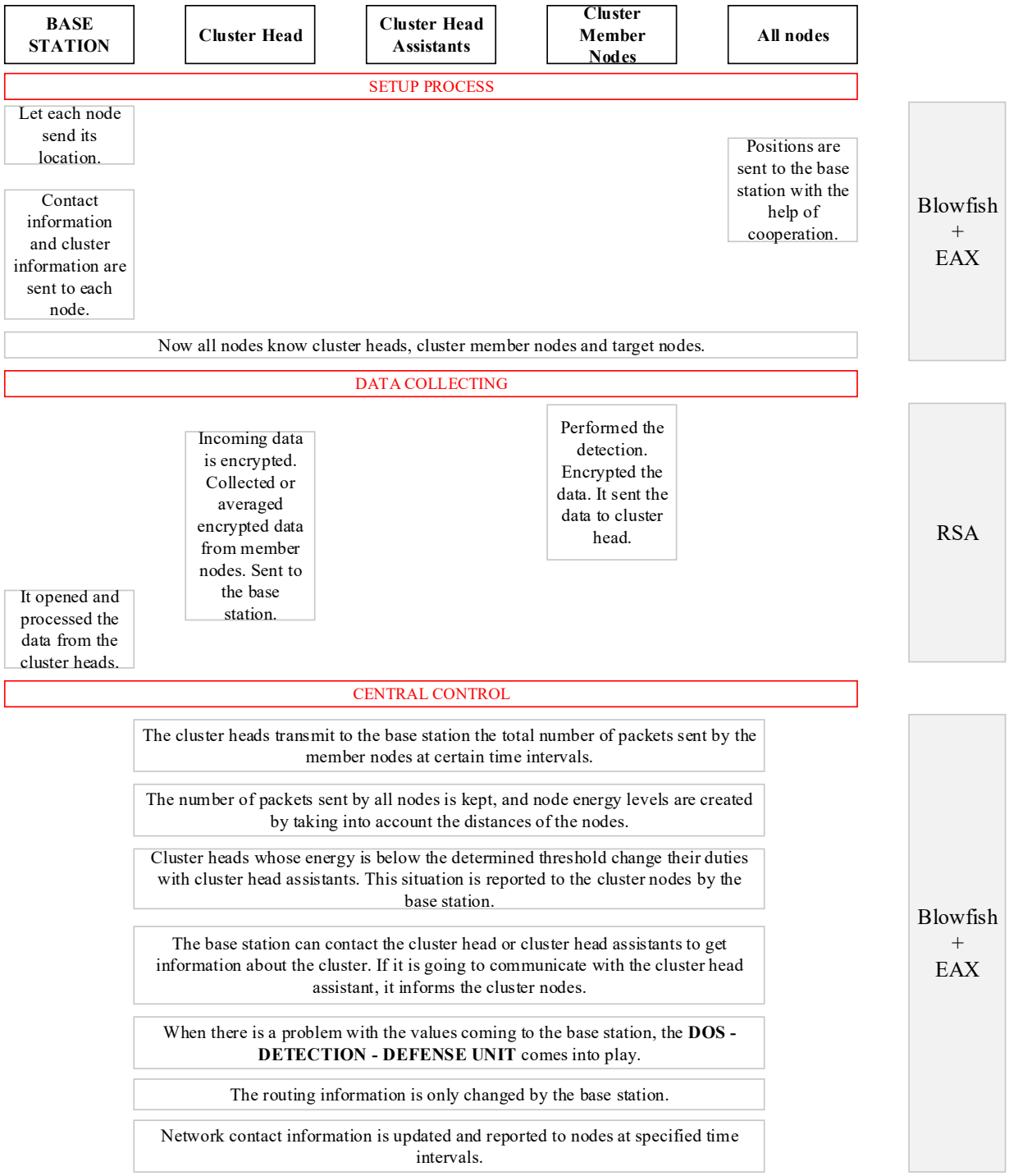

Figure 15. General Representation of SDA-RDOS Protocol.

5. Simulation Results

In this section, the performance of the proposed SDA-RDOS protocol is evaluated and compared with popular clustering protocols, namely LSDAR [47] (Light-weight structure-based data aggregation routing protocol), SUCID [31] (Secure Unequal Clustering Protocol with Intrusion Detection System), and OP-MDCRP [35] (Optimal Privacy-Multihop Dynamic Clustering Routing Protocol). These protocols are up to date and have given good results compared to many protocols. LSDAR > ECH-DUAL, ZBRP/SUCID > IPSO, KHA, F5NUCP, FUCHAR/OP-MDCRP > ESR, LEACHMAC.

5.1. Simulation Environment

Energy Efficiency, Network Lifetime, Average Delay, Packet delivery ratio (PDR), and security are the performance metrics used in this paper to validate the simulation results. The SDA-RDOS protocol was implemented using MATLAB R2021a and a core i5 processor with Windows 7. The parameters used in MATLAB are defined in Table 5.

Table 5. Simulation Parameters.

Parameters	Values
Area of deployment (x,y)	100 m × 100 m
Number of nodes	1000
Coordinate of the base station	50 × 10
The initial energy of each sensor	1 J
Eelec	50 nJ/bit
Efs	10 pJ/bit/m2
Emp	0.0013 pJ/bit/m4
Eda	5 nJ/bit
Number of rounds	1000
Control packet size	200 bits
Data packet size	4000 bits
Network Interface Type	Wireless IEEE 802.11

5.2. Experimental Results

Energy Efficiency Analysis: Initially, the energy of all nodes in the network was equal. Nodes consume energy in the Reception and Transmission processes.

$$\text{Total Energy: Etransmission + Ereception} \quad (9)$$

The energy consumed in transmission and reception is directly proportional to the number of bits sent and the distance. The Energy Efficiency Analysis of the study is given in Figure 16.

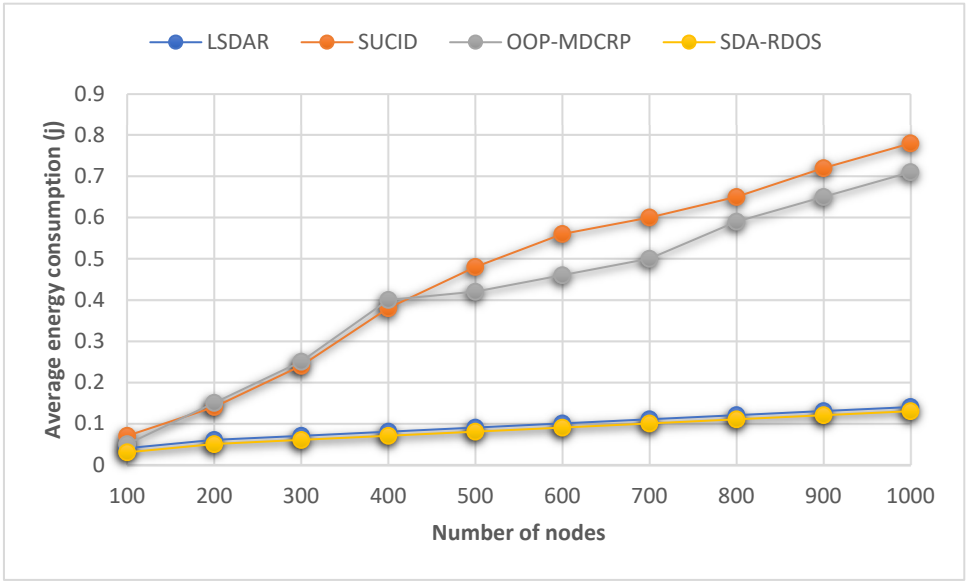

Figure 16. Energy Efficiency Analysis of LSDAR, SUCID, OOP-MDCRP, and SDA-RDOS protocols.

The initial energy of all nodes is equal. The data transmission of each node after detection is recorded. Member nodes in the cluster can reach the cluster with a single hop, and as their distances from the cluster heads are essentially the same, the energy consumption of these nodes is determined by the number of packets they send. The hop numbers and distances are different for the cluster heads to deliver the data to the base station. For this reason, the number of hops and the distance is included as a multiplier, together with the number of packets sent by the cluster heads regarding energy consumption. The RSA, Blowfish, and EAX models were preferred in the study because they are energy efficient. At the same time, the fair distribution of common nodes in cluster selection increases network collaboration and load balancing and reduces energy consumption. In the study, energy efficiency occurs because the target nodes to which the nodes will send their data are determined. When Figure 16 is examined, the protocol with the closest values to the SDA-RDOS protocol is the LSDAR protocol. Other protocols gave higher results.

Network Lifetime Analysis: Nodes that run out of energy in the network die. The network is terminated when the energy of all nodes in the network is exhausted. The time from the start to the end of the network gives the network's lifetime. The Network Lifetime Analysis of the study is given in Figure 17.

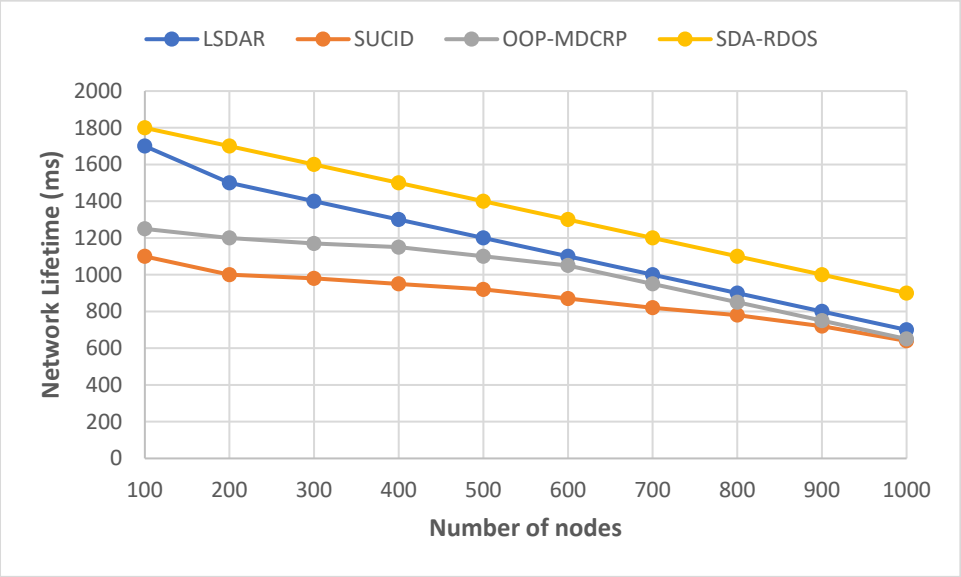

Figure 17. Network Lifetime Analysis of LSDAR, SUCID, OOP-MDCRP, and SDA-RDOS protocols.

Thanks to the central management of the base station, the cooperation of the nodes is high. Thanks to the cluster head assistants, the cluster heads are prevented from consuming their energy prematurely. Cluster head helpers are sometimes used to direct the data of other cluster heads to the base station, and sometimes they are used for energy conservation of the cluster head. The problem of consuming more energy for cluster heads close to the base station than for cluster heads far away from the base station is also eliminated with cluster head assistants. At the same time, if the cluster heads are captured, the network may be compromised, while this threat is eliminated thanks to the cluster head assistants. Figure 17 shows that the protocol with the closest values to the SDA-RDOS protocol is again the LSDAR protocol. Other protocols gave lower results.

Average Delay Analysis: It is defined as the time elapsed between the time the packets are sent from the source node and the time the destination node receives the packet. The average Delay Analysis of the study is given in Figure 18.

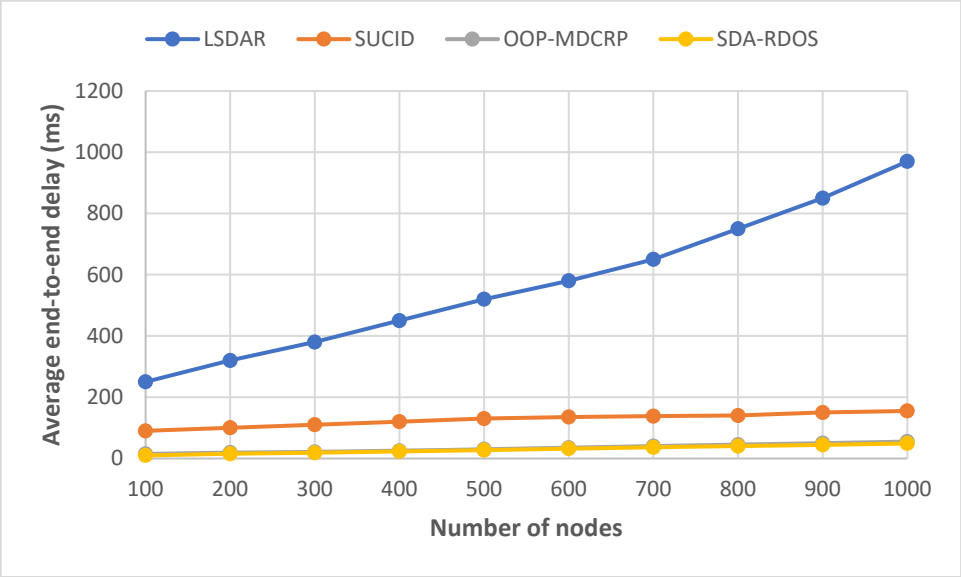

Figure 18. Average Delay Analysis of LSDAR, SUCID, OOP-MDCRP, and SDA-RDOS protocols.

The cluster head receives the encrypted data from the member nodes in data clustering operations. The cluster head decrypts encrypted data. After data are collected/centered, they are encrypted again to be sent to the base station. Data privacy is violated in these transactions, and network delay occurs due to encryption/decryption processes. In the study carried out, because the RSA Homomorphic method is used, the data sent by the cluster member nodes are collected/averaged by the cluster head and transmitted to the base station without decrypting them. Figure 18 shows that the protocol with the closest values to the SDA-RDOS protocol is the OOP-MDCRP protocol. Other protocols gave higher results.

Packet delivery ratio (PDR) Analysis: The ratio of the number of packets produced by the source to the number of packets received by the destination gives the packet delivery rate. Every package produced may not always reach the target in case of environmental conditions, package conflict, or attack. The packet delivery ratio (PDR) analysis of the study is given in Figure 19.

Thanks to the privacy and protection techniques used in the study, malicious threats cannot harm the network. Furthermore, as the route of all member nodes and cluster heads is clear, the effect of malicious nodes is minimized. Figure 19 shows that the protocol with the closest values to the SDA-RDOS protocol is the SUCID protocol. Other protocols gave lower results.

Security Analysis: All security requirements, including data availability, were met in the study. Data confidentiality, integrity, freshness, and Source authentication are provided with Blowfish + EAX + RSA. A detection and defense unit was developed for DOS attacks on data availability. As the packet drop rates in the network exceed the threshold value, the defense unit is activated. As stated in the literature, Authentication, packet leash, Authorization, Data Accuracy, Monitoring, and Sleeping methods were used as defense mechanisms for Sybil Attacks, Sinkhole, Blackhole, Wormhole, Selective Forwarding, and Hello Flooding attacks. All attacks were run simultaneously and the status of the protocols at the time of the attack was monitored for security analysis. Packet Transmission/Drop Rates were used for analysis. As is known, the Packet Forward/Drop Rate is the number obtained by dividing the number of packets sent by the source node by the number of packets received by the destination node. When this rate decreases, it turns out that the generated packets cannot be transmitted to the destination, and the packets are dropped. The Security Analysis of the study is given in Table 6, and the packet drop ratio values at the time of the attack are given in Figure 20.

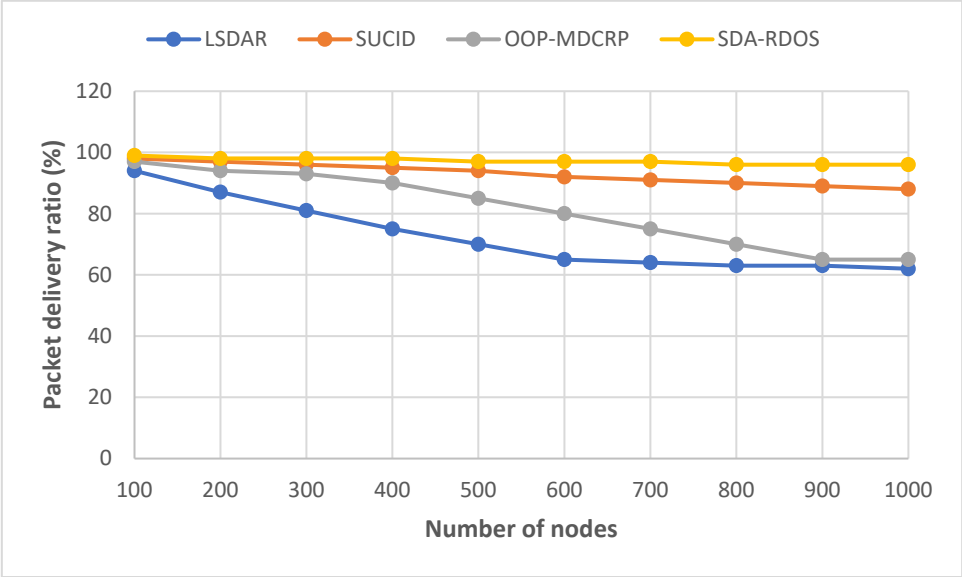

Figure 19. Packet delivery ratio (PDR) Analysis of LSDAR, SUCID, OOP-MDCRP, and SDA-RDOS protocols.

Table 6. Security Analysis of LSDAR, SUCID, OOP-MDCRP, and SDA-RDOS protocols.

Security Requirements/Protocols	LSDAR	SUCID	OP-MDCRP	SDA-RDOS
Data confidentiality	+	-	+	+
Data integrity	-	-	+	+
Data freshness	-	-	-	+
Source Authentication	-	-	+	+
Data availability	-	+	-	+

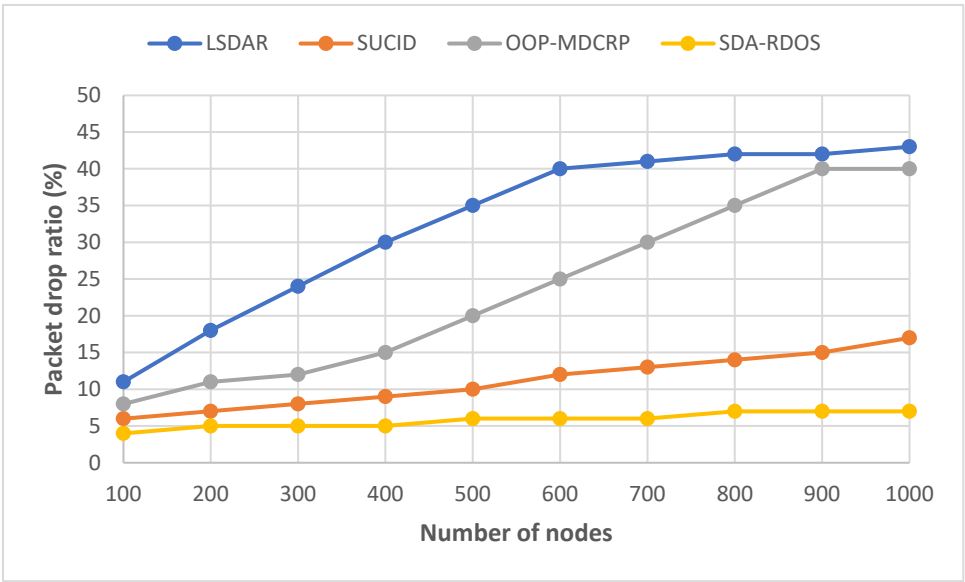

Figure 20. Security Analysis of LSDAR, SUCID, OOP-MDCRP, and SDA-RDOS protocols.

In LSDAR, which is one of the leading protocols in the literature and gives good results to many protocols, each node maintains its own neighbor table. The TDMA is used in cluster operations and a star heuristic algorithm is used in cluster head selections. It also

has a data security algorithm. The SUCID performs cluster selection according to fuzzy methods and DHO algorithm. It also has an intrusion detection unit. The OP-MDCRP provides security with 160-bit ECC. It meets many security requirements. In SDA-RDOS, all requirements are met.

As SDA-RDOS includes a direct detection and defense unit against DOS attacks, its success can be clearly seen. Figure 20 shows that the protocol with the closest values to the SDA-RDOS protocol is the SUCID protocol. Other protocols gave higher results.

6. Discussion

In this study, a secure data aggregation protocol was developed. This protocol satisfies the often-neglected data availability security requirement. In addition, cost-effective algorithms were selected for all transactions, and they were used with a new approach. Double encryption/decryption operations that occur during data clustering were also prevented by homomorphic encryption.

When developing a new protocol in a WSN, one needs to use some metrics to show that this protocol is better. These are energy efficiency, latency, packet delivery rate, packet drop rate, and network lifetime. According to these metrics, simulations were made with 1000 nodes and initial energies of 1 J, and better results were obtained.

Some assumptions were made in this study as discussed in Section 4.1. However, the protocol can be implemented on real nodes and the simulation environment, therefore, practices and evaluations on real nodes are more valuable.

The followings can be done as future works. First, efficiency comparison can be made by choosing different algorithms instead of the algorithms used in the study. In this way, the most effective solutions can be revealed. Second, homomorphic methods that can operate on encrypted data can be enriched so that there is no encryption/decryption twice in a data clustering network. Third, new and more cost-effective solutions can be produced against DOS attacks. Finally, the studies can be implemented on real nodes.

7. Conclusions

We can now easily see WSNs around us. As smart systems become widespread, the importance of WSNs in the smart system increases. Security is an essential issue in data clustering methods used to reduce data density in the network and the network's total energy consumption. Highly critical information in the network can fall into the hands of enemies without secure communication in critical network applications. In this study, a secure data clustering protocol was developed. The DOS attacks, which have been neglected until now, are also included in the study with the developed protocol. Effective cluster selection process, cluster head assistants, centralized management by the base station, and effective use of Blowfish-EAX-RSA have strengthened the protocol. The success of the simulation results on energy, network lifetime, delay, packet delivery rates, and security shows the importance of SDA-RDOS. The developed secure protocol can be used in military applications such as border security, monitoring of enemy lines, and in WSNs consisting of many sensor nodes used in critical infrastructures of a country, such as energy, water, and communication sectors.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

WSN	Wireless Sensor Network
DOS	Denial of Service
LSDAR	Light-weight Structure Based Data Aggregation Routing Protocol
SUCID	Secure Unequal Clustering Protocol with Intrusion Detection System
OOP-MDCRP	Optimal Privacy-Multihop Dynamic Clustering Routing Protocol
IoT	Internet of Things
EAX	Encrypt-then-authenticate-then-translate
ECC	Elliptic-curve Cryptography
RSA	Rivest–Shamir–Adleman
PDR	Packet Delivery Ratio
WSNs	Wireless Sensor Networks
QoS	Quality of Service
CIA	Confidentiality, Integrity, and Availability
NCN	Number of Cluster Nodes
OCB	Offset Codebook Mode
CCM	Cipher Block Chaining-Message Authentication Code
AEAD	Authenticated Encryption with Associated Data
OMAC	One-key MAC
CTR	Counter
PHE	Partially Homomorphic Encryption

References

1. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. *Comput. Netw.* **2002**, *38*, 393–422. [CrossRef]
2. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Comput. Netw.* **2008**, *52*, 2292–2330. [CrossRef]
3. Gupta, S.K.; Sinha, P. Overview of Wireless Sensor Network: A Survey. *Int. J. Adv. Res. Comput. Commun. Eng.* **2014**, *3*, 5201–5207.
4. Lin, Z.; An, K.; Niu, H.; Hu, Y.; Chatzinotas, S.; Zheng, G.; Wang, J. SLNR-based secure energy efficient beamforming in multibeam satellite systems. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, 1–4. [CrossRef]
5. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. Refracting RIS aided hybrid satellite- terrestrial relay networks: Joint beamforming designand optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724. [CrossRef]
6. Lin, Z.; Lin, M.; Wang, J.; Cola, T.; Wang, J. Joint beamforming and power allocation for satellite-terrestrial integrated networks with non-orthogonal multiple access. *IEEE J. Sel. Top. Signal Processing* **2019**, *13*, 657–670. [CrossRef]
7. Lin, Z.; Lin, M.; Cola, T.; Wang, J.; Zhu, W.; Cheng, J. Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks. *IEEE Internet Things J.* **2021**, *8*, 11123–11134. [CrossRef]
8. Dahiya, A.; Gupta, B. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. *Future Gener. Comput. Syst.* **2020**, *117*, 193–204. [CrossRef]
9. Alieyan, K.; Almomani, A.; Anbar, M.; Alauthman, M.; Abdullah, R.; Gupta, B.B. DNS rule-based schema to botnet detection. *Enterp. Inf. Syst.* **2019**, *15*, 545–564. [CrossRef]
10. Mishra, A.; Gupta, B.B.; Perakovic, D.; Penalvo, F.J.G.; Hsu, C. Classification based machine learning for detection of ddos attack in cloud computing. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 10–12 January 2021. [CrossRef]
11. Ling, Z.; Hao, Z.J. An Intrusion Detection System Based on Normalized Mutual Information Antibodies Feature Selection and Adaptive Quantum Artificial Immune System. *Int. J. Semant. Web Inf. Syst.* **2022**, *18*, 25. [CrossRef]
12. Ling, Z.; Hao, Z.J. Intrusion Detection Using Normalized Mutual Information Feature Selection and Parallel Quantum Genetic Algorithm. *Int. J. Semant. Web Inf. Syst.* **2022**, *18*, 24. [CrossRef]
13. Dener, M. A New Energy Efficient Hierarchical Routing Protocol for Wireless Sensor Networks. *Wirel. Pers. Commun.* **2018**, *101*, 269–286. [CrossRef]
14. Dener, M.; Bay, O.F. TeenySec: A new data link layer security protocol for WSNs. *Secur. Commun. Netw.* **2016**, *9*, 5882–5891. [CrossRef]
15. Dener, M. Security Analysis in Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 303501. [CrossRef]
16. Mahalakshmi, G.; Subathra, P. A survey on prevention approaches for denial of sleep attacks in wireless networks. *J. Emerg. Technol. Web Intell.* **2014**, *6*, 106–110. [CrossRef]
17. Kour, P.; Panwar, L.C. A review on security challenges and attacks in wireless sensor networks. *Int. J. Sci. Res.* **2014**, *3*, 1360–1364.
18. Zhang, L.; Zhang, H.; Conti, M.; Di Pietro, R.; Jajodia, S.; Vincenzo Mancini, L. Preserving privacy against external and internal threats in WSN data aggregation. *Telecommun. Syst.* **2013**, *52*, 2163–2176. [CrossRef]

19. Ullah, A.; Said, G.; Sher, M.; Ning, H. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. *Peer–Peer Netw. Appl.* **2020**, *13*, 163–174. [CrossRef]
20. Singh, H.; Singh, D. Hierarchical clustering and routing protocol to ensure scalability and reliability in large-scale wireless sensor networks. *J. Supercomput.* **2021**, *77*, 10165–10183. [CrossRef]
21. Singh, S.; Singh Saini, H. Learning-Based Security Technique for Selective Forwarding Attack in Clustered WSN. *Wirel. Pers. Commun.* **2021**, *118*, 789–814. [CrossRef]
22. Shobana, M.; Sabitha, R.; Karthik, S. An enhanced soft computing-based formulation for secure data aggregation and efficient data processing in large-scale wireless sensor network. *Soft Comput.* **2020**, *24*, 12541–12552. [CrossRef]
23. Del-Valle-Soto, C.; Mex-Perera, C.; Nolazco-Flores, J.A.; Rodríguez, A.; Rosas-Caro, J.C.; Martínez-Herrera, A. A Low-Cost Jamming Detection Approach Using Performance Metrics in Cluster-Based Wireless Sensor Networks. *Sensors* **2021**, *21*, 1179. [CrossRef] [PubMed]
24. Krishnasamy, L.; Kumar Dhanaraj, R.; Gopal, D.G.; Gadekallu, T.R.; Aboudaif, M.K.; Nasr, E.A. A Heuristic Angular Clustering Framework for Secured Statistical Data Aggregation in Sensor Networks. *Sensors* **2020**, *20*, 4937. [CrossRef] [PubMed]
25. Di Pietro, R.; Michiardi, P.; Molva, R. Confidentiality and integrity for data aggregation in WSN using peer monitoring. *Secur. Commun. Netw.* **2009**, *2*, 181–194. [CrossRef]
26. Fang, W.; Zhang, W.; Chen, W.; Liu, J.; Yepeng, N.; Yang, Y. MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2021**, *14*, 1–20. [CrossRef]
27. Reegan, A.S.; Kabila, V. Highly Secured Cluster Based WSN Using Novel FCM and Enhanced ECC-ElGamal Encryption in IoT. *Wirel. Pers. Commun.* **2021**, *118*, 1313–1329. [CrossRef]
28. Othman, S.B.; Bahattab, A.A.; Trad, A.; Youssef, H. Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption. *Wirel. Pers. Commun.* **2015**, *80*, 867–889. [CrossRef]
29. Naghibi, M.; Barati, H. SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 10769–10788. [CrossRef]
30. Mathapati, M.; Kumaran, T.S.; Prasad, K.H.S.; Patil, K. Framework with temporal attribute for secure data aggregation in sensor network. *SN Appl. Sci.* **2020**, *2*, 1975. [CrossRef]
31. Maheswari, M.; Karthika, R.A. A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**, *118*, 1535–1557. [CrossRef]
32. Khot, P.S.; Naik, U. Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection. *Wirel. Pers. Commun.* **2021**, *119*, 2405–2429. [CrossRef]
33. Hajian, R.; Erfani, S.H. CHESDA: Continuous hybrid and energy-efficient secure data aggregation for WSN. *J. Supercomput.* **2021**, *77*, 5045–5075. [CrossRef]
34. Gomathi, S.; Krishnan, C.G. Malicious Node Detection in Wireless Sensor Networks Using an Efficient Secure Data Aggregation Protocol. *Wirel. Pers. Commun.* **2020**, *113*, 1775–1790. [CrossRef]
35. Loretta, G.I.; Kavitha, V. Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment. *Peer–Peer Netw. Appl.* **2021**, *14*, 821–836.
36. Babu, M.V.; Alzubi, J.A.; Sekaran, R.; Patan, R.; Ramachandran, M.; Gupta, D. An Improved IDAF-FIT Clustering Based ASLPP-RR Routing with Secure Data Aggregation in Wireless Sensor Network. *Mob. Netw. Appl.* **2020**, *26*, 1059–1067. [CrossRef]
37. Zhou, J.; Lin, Z. Lightweight load-balanced and authentication scheme for a cluster-based wireless sensor network. *Int. J. Distrib. Sens. Netw.* **2021**, *17*, 1550147720980326. [CrossRef]
38. Pattamaset, S.; Choi, J.S. Irrelevant data elimination based on a k-means clustering algorithm for efficient data aggregation and human activity classification in smart home sensor networks. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720929828. [CrossRef]
39. Song, H.; Sui, S.; Han, Q.; Zhang, H.; Yang, Z. Autoregressive integrated moving average model–based secure data aggregation for wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720912958. [CrossRef]
40. Liu, X.; Zhang, X.; Yu, J.; Fu, C. Query Privacy Preserving for Data Aggregation in Wireless Sensor Networks. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 9754973. [CrossRef]
41. Ding, J.; Zhang, H.; Guo, Z.; Wu, Y. The DPC-Based Scheme for Detecting Selective Forwarding in Clustered Wireless Sensor Networks. *IEEE Access* **2021**, *9*, 20954–20967. [CrossRef]
42. 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]
43. Uvarajan, K.P.; Gowri Shankar, C. An Integrated Trust Assisted Energy Efficient Greedy Data Aggregation for Wireless Sensor Networks. *Wirel. Pers. Commun.* **2020**, *114*, 813–833. [CrossRef]
44. Narayan, V.; Daniel, A.K. A Novel Approach for Cluster Head Selection Using Trust Function in Wsn. *Scalable Comput. Pract. Exp.* **2021**, *22*, 1–13. [CrossRef]
45. Chethana, G.; Padmaja, K.V. Integer Matrix Keys for Secure Data Aggregation in Clustered Wireless Sensor Networks. *INTL J. Electron. Telecommun.* **2020**, *66*, 637–645.
46. Bagaa, M.; Challal, Y.; Ouadjaout, A.; Lasla, N.; Badachea, N. Efficient data aggregation with in-network integrity control for WSN. *J. Parallel Distrib. Comput.* **2012**, *72*, 1157–1170. [CrossRef]
47. Haseeba, K.; Islama, N.; Sabab, T.; Rehmanb, A.; Mehmoodc, Z. LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. *Sustain. Cities Soc.* **2020**, *54*, 101995. [CrossRef]

48. Liu, X.; Yu, J.; Li, F.; Lv, W.; Wang, Y.; Cheng, X. Data Aggregation in Wireless Sensor Networks: From the Perspective of Security. *IEEE Internet Things J.* **2020**, *7*, 6495–6513. [CrossRef]
49. Rogaway, P.; Wagner, D. *A Critique of CCM*; University of California: Davis, CA, USA, 2013; pp. 1–9.
50. Bellare, M.; Rogaway, P.; Wagner, D. *The EAX Mode of Operation. Fast Software Encryption '04, Lecture Notes in Computer Science*; Bimal, R., Meier, W., Eds.; Springer: Berlin/Heidelberg, Germany, 2004.
51. Svenda, P. Basic comparison of Modes for Authenticated-Encryption (IAPM, XCBC, OCB, CCM, EAX, CWC, GCM, PCFB, CS). 2021. Available online: https://www.fi.muni.cz/~{}xsvenda/docs/AE_comparison_ipics04.pdf (accessed on 1 October 2022).
52. Simplicio, M.A., Jr.; de Oliveira, B.T.; Barreto, P.S.L.; Margi, C.B.; Carvalho, T.C.M.; Naslund, M. Comparison of Authenticated-Encryption Schemes in Wireless Sensor Network. In Proceedings of the IEEE 36th Conference on Local Computer Networks, LCN 2011, Bonn, Germany, 4–7 October 2011.
53. Pereira, G.C.C.F.; Alves, R.C.A.; da Silva, F.L.; Azevedo, R.M.; Albertini, B.C.; Margi, C.B. Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems. *Secur. Commun. Netw.* **2017**, *2017*, 2046735. [CrossRef]
54. Schneier, B. The Blowfish Encryption Algorithm. In *Fast Software Encryption, Cambridge Security Workshop Proceedings*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 191–204.
55. Chaurasiya, U.; Vardhan, M. A Comparative Survey on Different Symmetric Key Cryptography Algorithms. *Int. J. Creat. Res. Thoughts* **2018**, *6*, 374–377.
56. Nandisha, V.R.; Reshma, M. A Reliable and Efficient Technique for Balanced Energy Consumption in Wireless Sensor Networks. *Int. J. Innov. Res. Sci. Technol.* **2016**, *2*, 244–250.
57. Singh, A.K.; Alshehri, M.; Bhushan, S.; Kumar, M.; Alfarraj, O.; Pardarshani, K.R. Secure and Energy Efficient Data Transmission Model for WSN. *Intell. Autom. Soft Comput.* **2021**, *27*, 761–769. [CrossRef]
58. Ozdemir, S. Secure Data Aggregation in Wireless Sensor Networks via Homomorphic Encryption. *J. Fac. Eng. Arch. Gazi Univ.* **2008**, *23*, 365–373.
59. Peralta, G.; Cid-Fuentes, R.G.; Bilbao, J.; Crespo, P.M. Homomorphic Encryption and Network Coding in IoT Architectures: Advantages and Future Challenges. *Electronics* **2019**, *8*, 827. [CrossRef]
60. Ogburna, M.; Turner, C.; Dahal, P. Homomorphic Encryption. *Procedia Comput. Sci.* **2013**, *20*, 502–509. [CrossRef]
61. Yi, X.; Paulet, R.; Bertino, E. *Homomorphic Encryption and Applications*; Springer: Berlin/Heidelberg, Germany, 2014.
62. Milanov, E. The RSA Algorithm. 2021. Available online: https://sites.math.washington.edu/~{}morrow/336_09/papers/Yevgeny.pdf (accessed on 1 October 2022).
63. Wainakh, A. Homomorphic Encryption for Data Security in Cloud Computing. Master's Thesis, Middle East University, Ankara, Turkey, 2018.
64. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22–26*, 644–654. [CrossRef]
65. Rivest, R.L.; Adleman, L.; Dertouzos, M.L. On data banks and privacy homomorphisms. *Found. Secur. Comput.* **1978**, *4*, 169–180.
66. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21–22*, 120–126. [CrossRef]
67. Acar, A.; Aksu, H.; Uluagac, A.S.; Conti, M. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *ACM Comput. Surv. (Csur)* **2017**, *51*, 1–35. [CrossRef]
68. Al-Shibib, R.A. Performance Analysis for Fully and Partially Homomorphic Encryption Techniques. Master's Thesis, Middle East University, Ankara, Turkey, 2016.
69. Chandravathi, D.; Lakshmi, P.V. Performance Analysis of Homomorphic Encryption algorithms for Cloud Data Security. *Int. J. Res. Appl. Sci. Eng. Technol.* **2018**, *6*, 1589–1592.
70. Fotohi, R.; Firoozi Bari, S.; Yusefi, M. Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. *Int. J. Commun. Syst.* **2019**, *33*, e4234. [CrossRef]
71. Singla, D.; Diwaker, C. Analysis of security attacks in wireless sensor networks. *Int. J. Softw. Web Sci.* **2014**, *14*, 26–30.
72. Ali, H.; Mamun, A.A.; Anwar, S. All possible security concern and solutions of WSN: A comprehensive study. *Int. J. Comput. Sci. Technol.* **2015**, *6*, 64–74.
73. Ghildiyal, S.; Mishra, A.K.; Gupta, A.; Garg, N. Analysis of Denial of Service (DOS) Attacks in wireless sensor networks. *Int. J. Res. Eng. Technol.* **2014**, *3*, 140–143.