future internet

MDPI

Article

Optimizing Multi-Tier Scheduling and Secure Routing in Edge-Assisted Software-Defined Wireless Sensor Network Environment Using Moving Target Defense and AI Techniques

As'ad Mahmoud As'ad Alnaser [1,*], Said S. Saloum [2], Ahmed A. M. Sharadqh [3] and Hazem (Moh'd Said) Hatamleh [1]

[1] Applied Science Department, Al-Balqa Applied University, Ajloun 26824, Jordan; hazim-hh@bau.edu.jo
[2] Computer Engineering and Networks Department, Jouf University, Sakaka 42421, Saudi Arabia; sssaloum@ju.edu.sa
[3] Electrical Engineering Department, Al-Balqa Applied University, Amman 11134, Jordan; dr.ahmed.sharadqah@bau.edu.jo
* Correspondence: asad1-99@bau.edu.jo

Abstract: Software Defined Wireless Sensor Networks (SDWSN) enable flexibility in Wireless Sensor Network (WSN) environments by defining the controllable functions to WSN nodes by the Software Defined Network (SDN) controller. Due to the rapid evolution of SDWSNs, adverse effects also have occurred in terms of interference, energy consumption, and security issues. Several state-of-the-art works lend their utmost best to the SDWSN environment. However, the complete picture (i.e., relatability and security in SDWSN) poses severe challenges. The state-of-the-art issues is addressed in this research by proposing interference-aware Multi-Tier Scheduling for the SDWSN environment (MTS-SDWSN). First, we perform network construction in which the proposed network is constructed in a 2D hexagonal grid structure to resolve the connectivity issue. Upon constructing the network, the SDWSN nodes are clustered and managed to reduce the energy consumption using the Divide Well To Merge Better (DWTMB) algorithm in which the optimal Cluster Leader (CL) is selected based on adequate constraint. The data from the clustered nodes are sent to the Local Base Station (LBS) via CL in which they are scheduled in multi-tier format to diminish the complexity and interference issues. The first tier involved in scheduling among Cluster Members (CMs) and CL using adequate metrics, whereas the successive tiers (i.e., second and third) involved in scheduling among CLs to LBSs and LBSs to Sink Node (SN) are done using the Non-Cooperative Fuzzy Theory (NCFT) method. Last, the scheduled nodes are routed to appropriate destinations using Secure and Optimal Routing Protocol (SORP). The proposed SORP includes the Alibaba and Forty Thieves (AFT) and Multi Criteria Decision Making (MCDM) algorithms for selecting and ranking the optimal routes. Further, the security of the routes is enabled by adopting trust and Moving Target Defense (MTD) mechanisms. The MTD includes route switching among the SDWSN devices and active switch handling using Cycle Generative Adversarial Networks (CGAN) among the switches. The proposed work is implemented using a NS-3.26 simulation tool, and performance of the proposed model and existing works shows that the proposed work outperforms the existing works.

Keywords: Software Defined Wireless Sensor Networks (SDWSN); scheduling; secure routing; Moving Target Defense (MTD); network construction; clustering

Citation: Alnaser, A.M.A.; Saloum, S.S.; Sharadqh, A.A.M.; Hatamleh, H. Optimizing Multi-Tier Scheduling and Secure Routing in Edge-Assisted Software-Defined Wireless Sensor Network Environment Using Moving Target Defense and AI Techniques. *Future Internet* **2024**, *16*, 386. https://doi.org/10.3390/fi16110386

Academic Editor: Paolo Bellavista

Received: 13 September 2024
Revised: 14 October 2024
Accepted: 15 October 2024
Published: 23 October 2024

1. Introduction

Wireless Sensor Networks (WSNs) have attracted widespread curiosity regarding various applications such as industrial monitoring, environmental monitoring, etc. With the massive proliferation of WSNs, the operational, deployment cost, and sensor lifetime management of the WSN nodes in a dynamic and critical infrastructure is a stringent task [1–3]. In consideration of the aforementioned issues, the Software Defined Network (SDN) to assist the WSN was designed using Software Defined Wireless Sensor Networks

(SDWSN) [4,5], which is composed of three planes: the sensor plane, the forwarding plane, and the control plane. The sensor plane is composed of wireless sensor nodes, the forwarding plane is composed of OpenFlow SDN switches that forward the data from the sensor plane, and the control plane is composed of single/multiple SDN controllers for the global management of the SDWSN environment. The adoption of the SDWSN provides flexibility to manage, deploy, secure, and monitor the whole network [6,7].

As the SDWSN is still in the early stages of research, energy consumption, standardization, monitoring, security, temperature, electromagnetic noise, and radiation are of major concern. Normally, wireless sensor nodes are highly prone to these issues [8–12]. Prior research has focused on the clustering of such nodes. However, the prior clustering methods were highly prone to sparsity and mobility issues [13]. Other issues associated with these nodes are secure routing and scheduling, which are highly prone to link failure and security issues [14]. For that, much research adopts sleep scheduling and trust-based routing in the SDWSN environment [15]. On the other hand, the routing among SDN switches also faces severe security issues by imposing attacks on weak links and compromising switches [16]. These attacks were held in the existing environment due to the static nature of detection and prevention techniques. Furthermore, the SDWSN environments were highly prone to several types of routing attacks such as selective forwarding attacks, which refuse to forward messages from selected nodes, reducing traffic and increasing data loss. On the aspect of scheduling, the existing works relied on scheduling in one tier (i.e., schedules the overall nodes in one tier), which also creates interference and complexity when the nodes possess mobility [17].

Generally, the SDWSN environment needs full-fledged research on security, energy consumption, and interference issues. The proposed work overcomes the aforementioned by performing a complexity-aware and dynamic secure model using intellectual techniques.

1.1. Motivation and Objectives

The SDWSN environment suffers from various issues such as energy efficiency, security, and connectivity, respectively. The existing works fail to provide combined solutions for the routing—scheduling issues in the SDWSN environment and security. Some of the major problems of the SDWSN environment regarding routing and scheduling are provided below:

- Fewer Energy Efficiency and Connectivity Issues—All the existing works tend to increase their energy efficiency and connectivity at the node level, leveraging the communication management among the sink nodes and wireless sensor nodes (i.e., random placement of sink nodes in the SDWSN environment), which affects the connectivity and energy efficiency of the SDWSN environment.
- Improper Scheduling—The scheduling undergone by the existing works is merely based on the control messages and faults. However, with these metrics, the scheduling was not done in an effective manner. Furthermore, the existing works are limited to single-tier routing (i.e., schedules all the nodes in the SDWSN environment on a single round), which leads to increased interference issues.
- Poor Routing Security Measures—The existing works only consider trust-based routing as a security practice. However, they lack providing security to the routing data, which leads to spoofing attacks. In addition, the routing path and detection surface are kept static, which also leads to reconnaissance attacks.

The main aim and scope of this research are to ensure energy efficiency, connectivity, and security to the SDWSN environment using intellectual techniques. In addition, this work also addresses and resolves the important existing issues in the SDWSN environment. The foremost objective of this research is to model an energy-efficient and secure SDWSN environment for enabling secure routing and interference-aware scheduling. In addition, this research also coins an effective problem statement by leveraging the issues in the prior works. Some of the supplementary objectives of this work are provided below:

- To reduce the connectivity issues in the proposed environment by performing connectivity-based network construction, which also improves the energy efficiency.
- To resolve the issue of energy consumption by performing clustering of the underlying wireless sensor nodes-based density, which also manages the nodes' mobility in the SDWSN environment.
- To reduce the interference in the SDWSN environment by performing scheduling of the wireless sensor nodes into three tiers that also improve the sensor node lifetime in the network.
- To mitigate the cyber vulnerabilities in the SDWSN environment by performing secure routing in two ways, which also reduces the link failure issues.

1.2. Research Contribution

Some of the headmost contributions of this work are enumerated below:

- For resolving the connectivity issues in the SDWSN environment, we have performed connectivity-aware network placement, which also overcomes the issue of less energy efficiency.
- For reducing the energy consumption of the SDWSN nodes, we have performed density-based clustering using the DWTMB algorithm based on several metrics. In addition, the resilient cluster leader also was selected based on high residual energy, less mobility, less distance, and high trust score.
- For reducing the unwanted interference and complexity issues, we have performed multi-tier scheduling based on a NCFT approach in which the scheduling is performed in three tiers such as CMs to CL, CLs to LBSs, and LBSs to sink nodes.
- For reducing the cybersecurity threats and link failures during routing, we have performed two-way routing in the SDWSN environment using a MTD approach. Furthermore, security during routing is utilized by the CEA algorithm.

1.3. Paper Organization

The rest of the paper is organized as follows: Section 2 provides the literature survey of the state-of-the-art works with the problems listed; Section 3 explains the specific existing issues along with the proposed research solutions; Section 4 details the system model in the proposed research along with the overall architecture; Section 5 specifies the proposed model with appropriate theoretical, mathematical, and diagrammatic explanations; Section 6 provides the experimental results with simulation setup, comparative analysis, and summary of the research; and, finally, Section 7 supplies a better conclusion for the proposed work.

2. Literature Survey

This section itemizes the existing literature on SDN, WSN, and SDWSN environments in a brief manner. Furthermore, we have also highlighted the corresponding literature issues in the existing works.

In this paper, the author proposed a secure and energy-efficient routing mechanism in the WSN environment [18]. Initially, this work mainly focuses on enhancing network security, thereby minimizing network energy consumption. The nodes trust evaluation scheme was performed using the ant colony optimization algorithm. The proposed model learns the energy consumption in the WSN, and then based on that, the basic ant colony enhances its efficiency to improve the secure routing. Finally, the multiobjective ant colony algorithm was proposed to ensure secure routing. Here, the ant colony optimization algorithm is utilized for performing secure and optimal routing in the WSN environment. However, adoption of ant colony optimization algorithm has poor convergence speed. In [19], a novel architecture for minimizing the load distribution and elongating lifetime in the SDN network was proposed. Initially, a new scheme was introduced for routing of load balancing by SDN and virtualization-based topology, BS, virtual routing, link and controller discovery. Then the Open Flow protocol was adapted for evaluating the

load balancing routing for individual flow based on the network functioning status and gathering information of load link through direct monitoring. Furthermore, the flows in several resource applications pass to the BS through various routes. Finally, the virtual routing intends to forward the optimal nodes for every IoT application. Here, the load balanced routing was performed in an effective manner in the SDWSN environment; however, without considering the security of the SDWSN environment during routing leads to cybersecurity threats.

In this paper, the author offers a model-based intelligent traffic control mechanism entrenched on deep graph reinforcement learning (DGRL) in the SDWSN environment [20]. Initially, the proposed algorithm learns and optimizes the data forwarding policy for improving intelligent traffic control. Then, the intelligent control policies are generated by the SDWSN controller for network topologies and dynamic traffic patterns. Finally, the designed actor-critic which combines both graph convolution network and deterministic policy gradient was employed for determining the policies accomplished at sensor nodes for optimizing the process of data forwarding. This work performs intelligent and optimal routing by using deep reinforcement algorithm. However, the lack of managing the entities in the physical layer leads to increased connectivity issues. The author of this work proposed a trust-based and energy-aware routing protocol in the WSN environment [21]. This protocol was proposed by utilizing adaptive genetic algorithm TAGA, which aims to resist general routing attacks and specific trust attacks, thereby reducing energy consumption computed by data transmission. Initially, the TAGA builds the nodes' trust values entrenched on their direct trust values contemplating volatilization and adaptive penalty factors. Then, the filtering approaches were exploited for constructing the indirect trust values. Furthermore, the cluster head was optimally selected using threshold function based on nodes' dynamic changes, residual energy, and trust values. Finally, the secure and optimal routing path was identified using a genetic algorithm. Here, the secure routing was achieved by adopting the trust values of the wireless sensor nodes. However, the trust values were not enough for performing secure routing in the WSN environment.

In this work, the author proposed a secure routing approach based on an enhanced optimization algorithm in the WSN [22,23]. Initially, the optimal nodes or paths were selected for secure transmission based on optimal link-state multipath routing. Then, the crossover mutated marriage in honeybee (CM-MH) algorithm was constructed for optimal path selection among source and destination. The Improved Blowfish algorithm (IBFA) was exploited for authentication, and encryption was performed to ensure secure transmission. Finally, the updates were monitored and the supremacy was evaluated for the proposed approach. The author in this work proposed an SDN entrenched load balanced opportunistic routing in duty-cycled WSN [24]. Initially, the candidates were generated and managed in the control plane. Based on the three average probability distributions such as the expected number of hops distribution, residual energy, and transmission distance distribution, depending on the priority, so the traffic is guided by the nodes with higher priority. Finally, the proposed work enhances the network lifetime, energy consumption, routing efficiency, duplicate packets, and sender waiting time.

In this work, the author proposed a secure and trust-aware routing protocol scheme in the WSN [25]. Initially, this work's main intention was to counter the selfish nodes entrenched on the hybrid trust model. The TASRP scheme was adapted for a multi-factor routing mechanism that considers the residual energy, nodes trust scores, and path length to accommodate reliable routing paths. By performing this among the trusted nodes, the energy consumption was minimized. Finally, the multi-factor technique aids in choosing the trusted nodes for forwarding data and reduces energy. In this work, the author proposed a hierarchical trust management technique in the SDWSN environment [26]. Initially, the trust scores were generated and recorded at the individual level of architecture as node, controller levels, and cluster heads. Here, the separate data trust scores and control schemes were accomplished for enhancing trust management. Finally, the proposed technique of a reputation-based scheme was fabricated and applied to detect the malicious behavior of the

sensor nodes such as black-hole attack, DoS attack, and selective forwarding attack. Here, the trust management was performed in the SDWSN environment based on trust scores. However, the detection surface of the SDWSN environment static leads to reconnaissance attacks.

The authors in [27] utilized fuzzy methodology for designing a scheduler for a software-defined wireless sensor network environment. The layers involved in this work are the application layer, control layer, virtualization layer, and physical layer. Initially, the packets are received and analyzed for types (i.e., Geocast, broadcast, multicast, and unicast) based on the information obtained from the packet header. For the multicast packets, the multicast scheduler is galvanized in which ranking for the packets is performed based on delay and fragility index, respectively. Here, the packets are scheduled and ranker based on the priority, whereas the security was not considered to lead to cyber threats. The authors in [28] designed a control protocol for communication for a software-defined wireless sensor network communication environment. The network was composed of entities such as wireless sensor nodes, sink nodes, and SDN controller with infrastructure, control layer, and application layer. The communication control protocol is enabled among infrastructure and control layers, respectively. Based on the information forwarded from the sensor nodes, the controller performs several operations. More clearly, the controller was composed of an intelligent threshold compotator for managing the input packet messages; the flow table manager manages the flow rules, the topology manager manages the network information of all the nodes, and the device manger assigns an identity for every node and logs their sensing details in the personal database.

In [29], the authors tend to provide security to the software-defined wireless network environment against a stumpy rate denial of service attacks. From the network, the traffic information is extracted and provided to the Hilbert-Haung transform for feature compression. The compressed features were then provided to the deep learning algorithm named convolutional neural networks for layer-wise feature extraction and classification, respectively. The convolutional neural network is utilized for feature extraction; however, the adoption of convolutional neural network limits with overfitting issues. In [30], the trusted clustering protocol was designed for a wireless environment by the authors. The network model in this work was composed of a cluster member, cluster leader, and base station. The clustering is performed by adopting a k-means algorithm in which the possible outliers are detected by assessing the trust-based metrics such as recommendation and fuzzy trust method. Finally, they tend to analyze outliers for classifying the cyberattacks into delaying, dropping, and tampering of packets, respectively. The utilization of the k-means algorithm for clustering limits with poor clustering issues as the sensors nodes in the environment possess a heterogeneous nature.

3. Problem Statement

The specific problems employed in the existing works are briefed in this section. Furthermore, this section lists the problems faced by each work and also provides the corresponding solution.

The authors in this work perform packet processing and validation mechanisms for ensuring security to the software-defined network environment [31]. The route update messages were filtered out as they contained malicious and redundant updates based on two conditions such as frequent announcement and withdrawal, respectively. In a similar manner, the authors in [32] enable secure multipath routing for a SDN environment. The entities involved in this work were software-defined nodes, open flow switches, and controller. The network flow information was collected by the controller for packet processing based on validating the flow rules and forwarding them to the other neighbor node. The problems encountered in these works are listed below:

- Here, the security during routing was ensured by validating the route update messages of the neighbor nodes. However, only validating the route updating message and leveraging the neighbor node legitimacy leads to route misdirection attacks.

- Even though this work adopts a routing security problem in the SDN environment, this work lacks with considering interference and link failures during routing, which easily welcomes attackers to impose several malicious attacks.
- Furthermore, the routing path in this work was of a static nature, which was easy prey for the cyber crooks to impose reconnaissance attacks, thereby manipulating the routing path.
- In addition to the static routing path, this work also kept the detection layer as static, which caused the software-defined network switches to be compromised and perform black-hole and wormhole attacks, respectively.

The authors in this work adopt optimization algorithms for enabling energy-efficient secure routing in a wireless sensor network environment [33]. Taylor-based cat swarm optimization algorithm was used. The main entities involved in this work were wireless sensor nodes and base station. The problems that were faced this work are listed below:

- Here, the wireless sensor nodes and base stations were placed in a random manner without awareness of the network dynamics. Such random placement of entities leads to connectivity issues among the nodes and the base station.
- The low-energy adaptive clustering hierarchy protocol was utilized for cluster head selection. However, the adoption of the low-energy adaptive clustering hierarchy protocol limits with sparse distribution of cluster heads, thereby affecting the energy efficiency.

The authors in this work performed an adaptive scheduling method for wireless sensor network environments in a dynamic manner [34]. The entities involved in this work are wireless sensor nodes and base station. This work adopts a duty cycling method for achieving the adaptive and dynamic scheduling in the wireless sensor network environment. The major problems employed in this work are:

- This work only provides scheduling rules for the sensor nodes. As the network is composed of multiple sensor nodes, the mentioned scheduling rules (i.e., four states) did not provide proper management, leading to a high chance of interference.
- Improper management of sensor nodes and base station also affects the scalability and connectivity issues, thereby leading to high delay and energy consumption. In addition, security threats also happened due to improper node management.

Research Solution

The problems procured in the aforesaid specific existing issues are fixed by designing a secure and interference-aware routing protocol for a SDWSN environment. First, we constructed the SDWSN network in the form of 2D hexagonal grids based on the local gateway coverage to reduce the connectivity and coverage whole issues. Followed by network construction, the clustering is performed by the proposed works for WSN nodes using the DWTMB algorithm to reduce the energy consumption and increase the node lifetime. Once clustered, the WSN nodes are scheduled in a multi-tier hierarchical form (i.e., within clusters, among CLs, and among local gateways) using the NCFT algorithm for reducing the interference and collision problems. Upon scheduling the entities, we performed two-way routing (i.e., among WSN nodes and SDN switches) in a secure manner SORP protocol in which the AFT and MCDM algorithms are encapsulated. The AFT is utilized for multiple route selection, whereas the MCDM is utilized for ranking the multiple routes. In the proposed routing, the intermediate attacks are overcome by the CEA algorithm, whereas the passive attacks are overcome by adopting MTD methodology (i.e., route switching in infrastructure layer and switch handling). The switch handling in the switch layer is performed using the CGAN algorithm.

4. System Model

This research aims to improve energy efficiency and secure the SDWSN environment by performing resilient scheduling and routing techniques, respectively. This work

also adopts edge computing technology to overcome the issue of latency in the SDWSN environment.

The main entities involved in this work are WSN nodes, local gateway (LG), sink node, reconnaissance monitoring agent, edge-assisted SDN switches, and SDN controller. There are three layers involved in this work: the infrastructure layer, the edge-assisted switch layer, and the control layer. To ensure the network intelligence and accuracy, this work also utilizes Artificial Intelligence (AI) technology. Figure 1 represents the overall proposed system model.

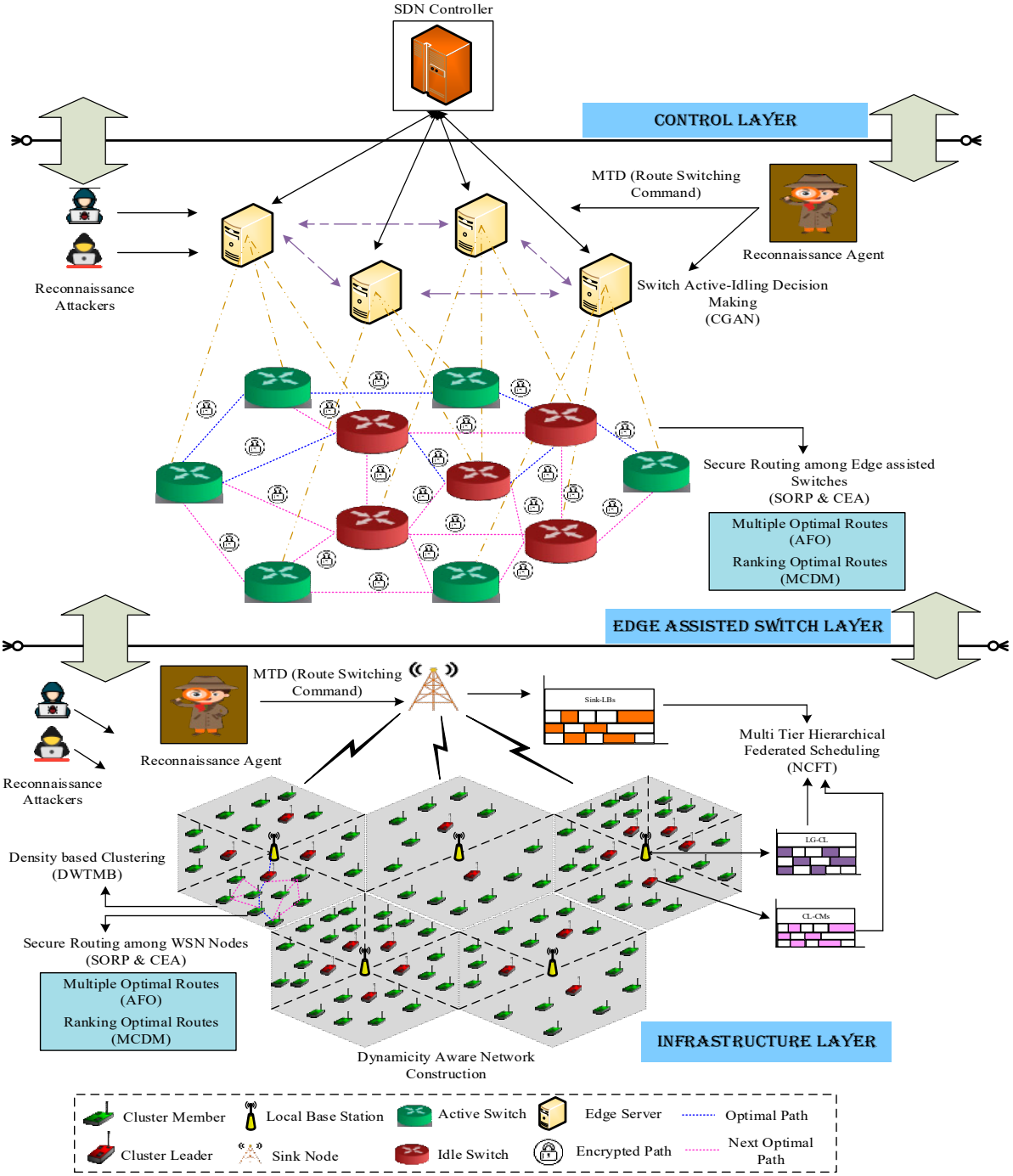

Figure 1. Overall architecture of the proposed model.

The brief working of entities is provided below:

- WSN Nodes—The responsibility of WSN nodes is to sense the environment in its vicinity. More clearly, the nodes are involved in cluster member ($WSN^{cm} = cm^n \in \{cm^1, cm^2, \ldots, cm^n\}$) and cluster leader (CL) $\left(WSN^{CL} = CL^n \in \left\{CL^1, CL^2, \ldots, CL^n\right\}\right)$ nodes in which the cluster member continuously senses and provides the sensing results to the CLs.
- Local Base Station (LBS)—The LBS $\left(LBS^n \in \left\{LBS^1, LBS^2, \ldots, LBS^n\right\}\right)$ is responsible for managing the one hexagonal grid with multiple WSN nodes. The sensing results from the CLs are provided to the LBS. Here, to ensure low latency and reliable transmission, a physical one-hop connection is needed.
- Sink Node (SN)—The SN is responsible for managing the complete 2D hexagonal grids. The aggregated sensing results from the LBS of every grid are provided to the SN for forwarding to the further layers.
- SDN Switches (SDN-SW)—The SDN-SW maintains the routing tables in which the sensed results follow the routing tables based on secure routing protocol. Further, the SDN-SWs can be active and idled for security purposes.
- Edge Server (ES)—The ES is responsible for handling the switches (i.e., active/idle). Further, it also triggers MTD to the SDN-SW.
- Reconnaissance Agent (RA)—The RA is responsible for monitoring the reconnaissance attacks in the proposed SDWSN environment. More clearly, the RA is placed in the infrastructure and edge-assisted switch layers for providing MTD commands.
- Controller—The controller acts as the heart of the SDWSN environment by providing the control messages to the underlying edge-assisted SDN switches. In our work, we utilize a centralized SDN controller.

4.1. Energy Ingesting Model

The energy ingesting model is formulated for the WSN nodes packets transmission and received during multi-tier scheduling, respectively. In this work, the distance among the WSN nodes to LBS, and LBS to SN, is determined in both multipath fading and free space channels, respectively. In our proposed work, the compensation of path loss is achieved by performing clustering, network construction, and switch handling mechanisms, respectively. The formulation of transmission by the WSN nodes to the LBS can be provided as:

$$En^{TX}(z, dis) = En^{TX-con}(z) + En^{TX-Amp}(z, dis) = \begin{cases} z.En^{con} + z.\varepsilon\ fs dis^2, & dis < dis^* \\ z.En^{con} + z.\varepsilon\ Mpf dis^4, & dis \geq dis^* \end{cases} \quad (1)$$

In a similar manner, the reception energy consumption that can be formulated for z-bits is provided below:

$$En^{RX}(z) = En^{RX-con}(z) = z.En^{con} \quad (2)$$

In Equations (1) and (2), En^{con} and En^{Amp} represent the amount of energy consumed for transmission and reception and energy amplifier model, respectively. The ε fs and ε Mpf denote the free space and multipath fading channels, respectively; dis^* is the threshold of the transmission distance among entities. The formulation of dis^* is provided as $dis^* = \sqrt{\varepsilon\ fs / \varepsilon\ Mpf}$.

4.2. Threat Model

The proposed SDWSN environment faced several challenges in terms of cybersecurity issues. Some of the major points in the threat model are provided below:

- This work highlights the security of the WSN nodes and edge-assisted switches against MITM, eavesdropping, Denial of Service (DoS), Flow Table Attacks (FTA), and Packet Mistreating Attacks (PMA). Those attacks are held in both the infrastructure and edge-assisted switch layers to mislead the routing information.

- The reconnaissance attacks are in the edge-assisted switch layer and the SN for manipulating the SDN switches and SNs. The malicious SDN switch can redirect the flow to the malicious destination. Further, the malicious SN causes the WSN nodes to quickly drain out and also causes collision during scheduling.

4.3. Network Assumptions

Some of the network assumptions to be followed before entering into the proposed model are:

- It is assumed that the centralized controller in the proposed environment is considered to be secure and the malicious attackers are not able to manipulate it.
- The proposed encryption algorithm is secure and cannot be bypassed by the attackers.
- The utilized WSN nodes in the environment are of a mobile and heterogenous nature that cannot pose any severe challenges to the network. Furthermore, managing mobility was conducted by organizing the nodes into clusters that allow the leaders to optimize routing updates and isolate any changes resulting from mobility within a specific cluster.
- The channel among the controllers and other entities (i.e., control messages provided by the controller) are secure in the proposed environment.
- Finally, the proposed routing links have enough bandwidth to impose routing in a reliable manner.

5. Proposed Model

In this section, the detailed working of the proposed work is explained with suitable theoretical, mathematical, and pictorial representations. The processes involved in this work are detailed below.

5.1. Connectivity-Aware Network Construction

Initially, the entities in the infrastructure layers are properly constructed to overcome the connectivity issues of huge communication traffic in sparsely connected networks. The entities in the infrastructure layer are composed of WSN nodes, local gateway, and sink nodes. The proposed work constructs the network based on the local gateway coverage in the form of 2D hexagonal grids. Within every local gateway coverage, there are several WSN nodes placed randomly. Note that, the proposed WSN nodes are mobile in nature. The sink nodes are placed at the edge of the infrastructure layer to resiliently communicate with the edge-assisted SDN switches for updating the flow rules. On the whole, the network construction overcomes the connectivity and coverage whole issues, respectively, in the SDWSN environment.

The network construction is initiated by the SN, which tends to place the LBS at the center of every 2D hexagonal grid. The distance between the SN and LBS is denoted as dis, which can be formulated as:

$$D = \sum_{j=1}^{m} dis_j \tag{3}$$

In Equation (3), j = 1, 2, . . ., m, where $m \geq 1$. The WSN sensor nodes are placed among the SN and LBS at a certain distance. The angle between the WSN nodes and LBS can be formulated as:

$$\theta_j = \tan - 1 \frac{(xj + 1 - xj)}{(yj + 1 - yj)} \tag{4}$$

After that, the WSN nodes weights can be computed as follows:

$$wf = \beta Nei^{cnt} Res^{ene} \tag{5}$$

where β denotes the relative constant, Nei^{cnt} denotes the count of neighbor, and Res^{ene} denotes the lingering energy. The WSN node that has amplified wf is selected as a best intermediate node and is placed in close proximity to the LBS. In a similar manner to other WSNs, once the capacity of the hexagonal grid gets overloaded, the hexagonal grid

start constructing continuously until the WSN and LBS are effectively placed with better connectivity.

5.2. Density-Based Clustering

As the WSN nodes in the local gateway coverage are sparsely distributed and possess mobility within the coverage, the lifetime of the WSN nodes gets quickly drained out, thereby affecting the sensing rate in the SDWSN environment. To overcome those issues, the proposed research performs density-based clustering of WSN nodes. The nodes are clustered based on the density and mobility in the specific area within the coverage using the Divide Well To Merge Better (DWTMB) algorithm. The proposed algorithm was composed of three division stages and one merging stage.

5.2.1. Division Stage

At the first subdivision stage, the WSN nodes are split up into several clusters using a k-means algorithm with dissimilar k-values. For instance, consider WSN nodes with r-observations $\{WSN_1, WSN_2, \ldots, WSN_r\}$ in which every observation had g-dimensions of $WSN_j = \left\{WSN_j^1, WSN_j^2, \ldots, WSN_j^g\right\}$. The split dimension data can be further split using the k-means algorithm, which can be formulated as:

$$WSN^{i^{k-means}} = \left\{clu_1^i, clu_2^i, \ldots, clu_k^i\right\}; k = 1, 2, \ldots, t \tag{6}$$

For every k-cluster and $t \geq 1$, the cluster variance can be computed by summing the split clusters, which can be formulated as:

$$\mathbb{V}_{clu^i}(k) = \sum_{j=1}^{k} var\left(clu_j^i\right); k = 1, 2, .., t \tag{7}$$

In Equation (7), the normalized variance can be computed for $\mathbb{V}_{clu^i} = \{\mathbb{V}_{clu^i}(1), \mathbb{V}_{clu^i}(2), \ldots, \mathbb{V}_{clu^i}(t)\}$ and can be formulated as:

$$\mathcal{D}_{clu^i}(k) = \left\{ \frac{\left|\mathbb{V}_{clu^i}(k+1) - \mathbb{V}_{clu^i}(k)\right|}{\mathbb{V}_{clu^i}(k)} : k = 1, 2, .., t-1 \right\} \tag{8}$$

The finest clusters are obtained from the $\mathcal{D}_{clu^i}$ for every dimension that can be formulated as:

$$fin^i = \underset{i}{argmax}\left\{k : \mathcal{D}_{clu^i}(k) \geq Th^1\right\} \tag{9}$$

In Equation (9), the piercing threshold value can be denoted as Th^1. If the $\mathcal{D}_{clu^i}$ is equal or greater than the Th^{ini}, the corresponding dimension is taken as fin^i. After that, the fin^i are further subdivided into several sub-clusters using the k-means algorithm.

Followed by the first subdivision stage, the second subdivision stage is initiated. In that stage, the sub-clusters obtained from the first subdivision stage are divided based on the steps followed in the first subdivision stage. To be clearer, the subdivisions are obtained in the finest sub-clusters of the first stage based on another piercing threshold value Th^2 that can be formulated as:

$$fin^i = \underset{i}{argmax}\left\{k : \mathcal{D}_{clu^i}(k) \geq Th^2\right\} \tag{10}$$

After the second subdivision stage, the third and final subdivision stage is initiated. Similar to the second stage, the finest sub-clusters are further split, and from that, another finest set of sub-clusters is computed based on Th^3. In this stage, there is a high chance of forming trivial sub-clusters within the sub-clusters with many elements.

5.2.2. Merging Stage

At the merging stage, the trivial sub-clusters within the major sub-clusters must be removed to obtain better merging. For that, the threshold range Th^{u} is set for the two finest sub-clusters obtained at the third subdivision stage. The WSNs are merged only when the WSNs have similar density and mobility. On the other hand, the WSN nodes with weaker density and dissimilar mobility are preserved as distinct clusters. Overall, the clusters can be merged by the assimilation threshold Th^{assi} of the distribution of two sub-clusters, which can be formulated as:

$$\text{Merge} = \begin{cases} 1, & \int_{start}^{end} fclu_1(y) fclu_2(y) dy \geq Th^{assi} \\ 0, & \text{otherwise} \end{cases} \quad (11)$$

In Equation (11), the assimilation threshold for merging can be denoted as Th^{assi}. It is noted that if the cluster distribution (i.e., density and mobility) is greater than Th^{assi}, then the value '1' denotes merging; otherwise, the value '0' is treated as separate clusters.

5.2.3. Cluster Maintenance

Furthermore, to reduce the complexity and sudden mobility constraints, this work also performs clustering management strategy (i.e., cluster merging and cluster splitting based on the density and mobility of the WSN nodes). If the forming clusters reach their capacity or are underloaded with fewer WSNs, the cluster maintenance strategy is initiated. Algorithm 1 provides cluster maintenance strategy.

Algorithm 1: Cluster maintenance strategy

If $Clu^{WSN1}, Clu^{WSN2} \geq clu^{capacity}$
  Split the cluster:
  $Clu^{WSN1} \rightarrow \left\{ Clu^{WSN1}{}_{(i)} : Clu^{WSN1}{}_{(ii)} \right\}$
  $Clu^{WSN2} \rightarrow \left\{ Clu^{WSN2}{}_{(i)} : Clu^{WSN2}{}_{(ii)} \right\}$
Else
  Merge the cluster:
  $Clu^{WSN1,2} \rightarrow \left\{ Clu^{WSN1} + Clu^{WSN2} \right\}$
End If

5.2.4. Cluster Leader Selection

From the clustered WSN nodes, the optimal cluster leader (CL) is selected based on metrics such as high residual energy (res^{ene}), less mobility (mob), less distance (dis) from the local gateway, and high trust score (tru) (i.e., provided by the neighbor nodes and local gateway based on its behavior). Overall, the clustering of WSN nodes overcomes the issues of unwanted energy consumption and complexities in the SDWSN environment. Algorithm 2 provides CL selection method.

Algorithm 2: CL selection method

If $WSN > (res^{ene} \&\& tru)$ **then**
  If $WSN < (mob \&\& dis)$ **then**
    $WSN \rightarrow WSN^{CL}$
  Else
    $WSN \rightarrow WSN^{cm}$
  End If
End If

5.3. Multi-Tier Federated Scheduling

After performing clustering and CL selection, the WSN nodes are scheduled to reduce the unwanted interference and data collision in the network. Leveraging the issues faced by the conventional scheduling techniques, this research performs a multi-tier hierarchical scheduling technique into three states such as transmission, reception, and sleep in which the first tier involves scheduling of WSN nodes within the clusters by the CL based on their priority and energy level. To be clearer, the first-tier scheduling is performed among WSN^{CL} and WSN^{CL}s in which every WSN^{CL} in the environment updates the scheduling cycle for completing the transactions. The WSN^{CL} took resilient decision to its WSN^{cm}s based on the priority (pri_{WSN}) and energy level (ene_{WSN}). In such a case, the WSN^{CL} that resides closer to the LBS might lose more energy when compared to the WSN^{CL} with a longer distance from the LBS. Thus, the closer resided WSN^{CL} tends to update its scheduling cycle in a shorter period of time. Therefore, the update of the scheduling cycle by the WSN^{CL} for the first tier can be formulated as:

$$1\text{st tier}\left(SC^{j}\right) = \left(pri_{WSN}{}^{j}, ene_{WSN}{}^{j}\right) \tag{12}$$

Equation (12) is suitable for both transmission and reception, respectively, along with sleep time period. When the first cycle expires, another scheduling cycle is initiated by

$$1\text{st tier}\left(SC^{j+1}\right) = \left(pri_{WSN}{}^{j+1}, ene_{WSN}{}^{j+1}, SC^{j}\right) \rightarrow \begin{cases} \text{Txion} \\ \text{Rxion} \\ \text{Sleep} \end{cases} \tag{13}$$

In Equations (12) and (13), $pri_{WSN}{}^{j}$ and $pri_{WSN}{}^{j+1}$ denotes the WSN node priority for j-th and j+1-th cycles, respectively; $ene_{WSN}{}^{j}$ and $ene_{WSN}{}^{j+1}$ denotes the WSN energy level in j-th and j+1-th cycles, respectively. Figure 2 represents the first-tier scheduling model among the WSN^{CL} and WSN^{CL}s.

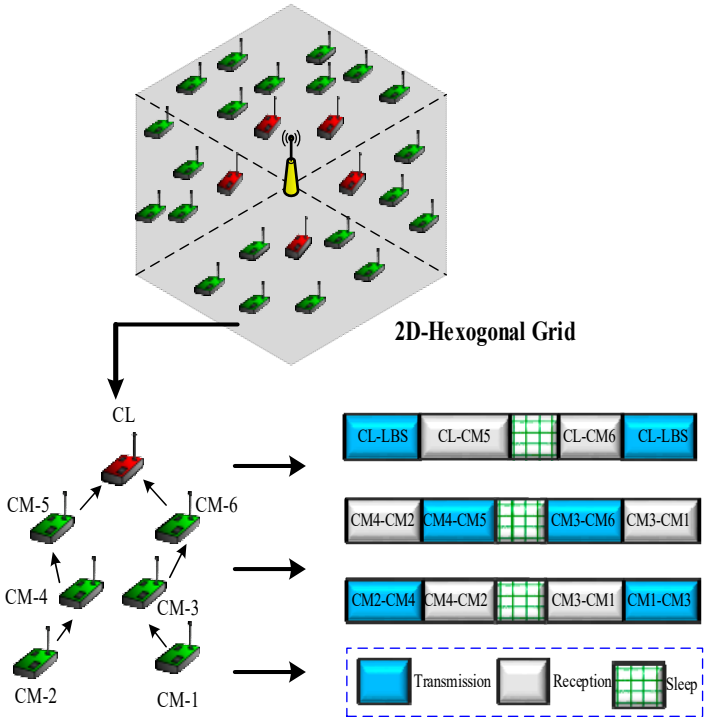

Figure 2. First-tier scheduling model.

The second tier involves federated scheduling of CLs based on their results in first-tier scheduling by the local gateways using the Non-Cooperative Fuzzy Theory (NCFT) ap-

proach. The second-tier scheduling determines which CL performs transmission, reception, and sleep based on the weighted average of priority $\left(\text{Wei}^{\text{pri}}\right)$, energy constraints $(\text{ene}^{\text{cons}})$, transmission time interval (TTI), and deadline (dl). The formulation of second-tier scheduling is provided below:

$$\text{2nd tier} = \text{CL}_{n=1,2,\ldots,n}{}^{(\text{Wei}^{\text{pri}},\text{ene}^{\text{cons}},\text{TTI,dl})} \rightarrow \begin{cases} \text{Txion} \\ \text{Rxion} \\ \text{Sleep} \end{cases} \tag{14}$$

where Txion, Rxion, and Sleep denotes the transmission, reception, and sleep, respectively. The LBS in the hexagonal grid schedules the CLs based on the metrics as mentioned in Equation (14).

Finally, the third tier involves federated scheduling of local gateways by the sink nodes using the NCFT based on the results in the second level and other metrics such as priority (pri), energy constraints $(\text{ene}^{\text{cons}})$, transmission time interval (TTI), channel quality information (CQI), and deadline (dl). The third-tier scheduling determines which local gateways perform transmission, reception, and sleep, respectively. The third-tier scheduling can be formulated as:

$$\text{3rd tier} = \text{LBS}_{n=1,2,..,n}{}^{(\text{pri},\text{ene}^{\text{cons}},\text{TTI,CQI,dl})} \rightarrow \begin{cases} \text{Txion} \\ \text{Rxion} \\ \text{Sleep} \end{cases} \tag{15}$$

On the whole, the proposed multi-tier hierarchical scheduling reduced the interference and data collision problems in the SDWSN environment. For the second- and third-tier scheduling, the NCFT method is utilized. The detailed explanation of the NCFT method for scheduling for second and third tiers is provided below. Figure 3 represents the second- and third-tier scheduling.

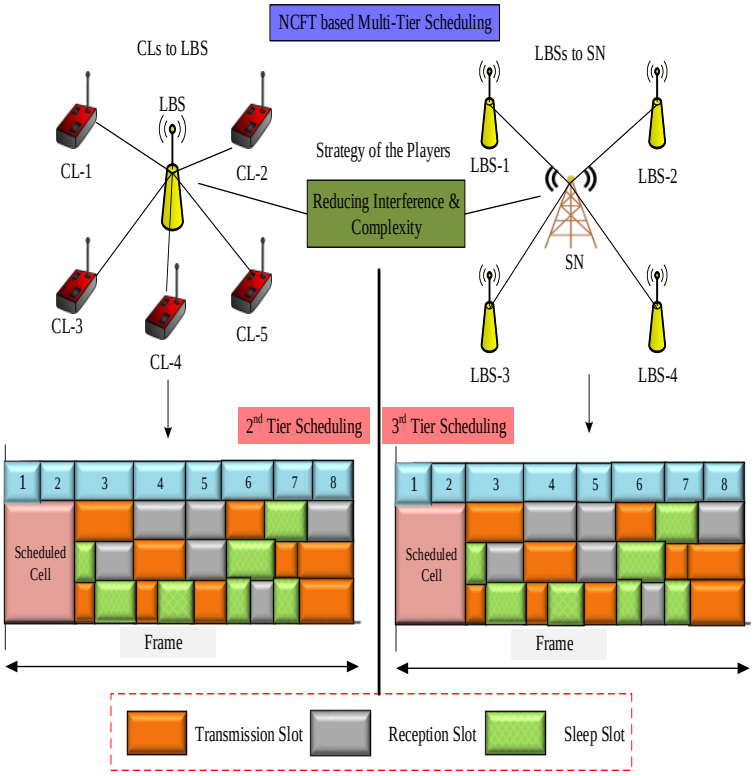

Figure 3. NCFT based Multi-Tier Scheduling.

NCFT-Based Scheduling (Second and Third Tiers)

The proposed work frames the multi-tier scheduling as a non-cooperative game problem in which the players involved in the non-cooperative game theory act selfishly based on their strategies. The entities involved in the proposed NCFT game model are:

$$\begin{gathered} \text{Players} : M = \langle pl_1, pl_2 \rangle \\ \text{Player Strategy} : \ St_{pl_1} = \{\aleph_j\}, St_{pl_2} = \{\aleph_j\}; \ \aleph_j \in \{coll\} \\ \text{Profile of Strategy} : St = St_{pl_1} \times St_{pl_2} \\ \text{Remuneration Function} : R(St) = r_j \end{gathered} \tag{16}$$

where $\langle pl_1, pl_2 \rangle$ denotes the first and second players, respectively, in which pl_1 implies the entity to be scheduled, and pl_2 implies the entity to perform scheduling. The strategy profile of every player can be denoted as $St_{pl_1} \times St_{pl_2}$ in which $\aleph_j \in \{coll\}$ is the strategy of every player to minimize the collision possibility, and $R(St)$ denotes the remuneration function. To be clearer, in NCFT every player tends to maximize their remuneration function based on the $\aleph_j$. The player response can be determined by framing the linear equation based on Nash equilibrium, which can be formulated as:

$$r_1\left(\aleph_1, \aleph_2^*\right) = \frac{k}{2}\left(\frac{\aleph_1 + \aleph_2^*}{2} + c\aleph_1\aleph_2^*\right) - \aleph_1^2 \tag{17}$$

$$r_2\left(\aleph_1^*, \aleph_2\right) = \frac{k}{2}\left(\frac{\aleph_1^* + \aleph_2}{2} + c\aleph_1^*\aleph_2\right) - \aleph_2^2 \tag{18}$$

The linear equations can be differentiated based on the $\aleph_j$ and can be provided as:

$$\frac{\partial r_1}{\partial \aleph_1} = \frac{k}{4} + \frac{kc}{2}\aleph_2^* - 2\aleph_1^* = 0 \tag{19}$$

$$\frac{\partial r_2}{\partial \aleph_2} = \frac{k}{4} + \frac{kc}{2}\aleph_1^* - 2\aleph_2^* = 0 \tag{20}$$

Equations (19) and (20) can be rewritten to obtain the new linear equations that can be provided as:

$$\begin{gathered} \frac{k}{4} + \frac{kc}{2}\aleph_2^* = 2\aleph_1^* \\ \frac{k}{4} + \frac{kc}{2}\aleph_1^* = 2\aleph_2^* \end{gathered} \tag{21}$$

By solving Equation (21), the Nash equilibrium point can be obtained. Since we adopt a non-cooperative game model, the remuneration of the players is reduced; hence, they must obtain lesser r_j with minimized $\aleph_j$. Algorithm 3 provides pseudocode for the proposed NCFT-based multi-tier scheduling.

Algorithm 3: Pseudocode for the proposed NCFT-based multi-tier scheduling (for second and third tiers)

Initialize: M, St, and r_j
Determine the response of every player (16)
Compute the scheduling metrics:
// Second-tier Scheduling by LBS//
For every CL **do**
Compute Wei^{pri}, ene^{cons}, TTI, dl
Solve the linear Equations (17) and (18)
Obtain minimized r_j from solving (21)
Perform second-tier scheduling (14)
End For
End
// Third-tier Scheduling by SN//
For every LBS **do**
Compute ri, ene^{cons}, TTI, CQI, dl
Solve the linear Equations (17) and (18)
Obtain minimized r_j from solving (21)
Perform third-tier scheduling (15)
End For
End
End

5.4. MTD-Based Secure Two-Way Routing

After performing scheduling, the proposed work performs secure two-way routing to overcome the malicious routing attacks such as black-hole and wormhole attacks, respectively. For that, we have selected the optimal and secure routing paths using the proposed Secure and Optimal Routing Protocol (SORP), which involves metaheuristics algorithms named Alibaba and Forty Thieves (AFT) and Multi Criteria Decision Making (MCDM) algorithm. The AFT is responsible for selecting the multiple optimal routes based on metrics such as link stability, direction, trust, and energy, whereas the MCDM is responsible for ranking the selected multiple routes based on high link stability, high trust, and less cost.

AFT-Based Multiple Optimal Route Selection

At first, the possible route positions (ro) are initialized in the dim dimensional search space, which can be formulated as

$$ro = \begin{bmatrix} ro_1^1 & ro_2^1 & \cdots & ro_{dim}^1 \\ ro_1^2 & ro_2^2 & \cdots & ro_{dim}^2 \\ \vdots & \vdots & \vdots & \vdots \\ ro_1^n & ro_1^n & \cdots & ro_{dim}^n \end{bmatrix} \quad (22)$$

From Equation (22), the position of possible routes in the SDWSN environment is denoted as ro_{dim}^n position of n-th route in dim. The formulation of route position population can be formulated as:

$$ro^j = lb_i + RA \times \left(up_i - lb_i\right) \quad (23)$$

From Equation (23), ro^j denotes the j-th route position, RA denotes the random number [0, 1], and $up_i$and lb_i denote the upper and lower bound functions, respectively. Among all the routes in the proposed SDWSN environment, the best routes with respect to the all the ro can be formulated as:

$$b^{ro} = \begin{bmatrix} b^{ro1}_{1} & b^{ro1}_{2} & \cdots & b^{ro1}_{dim} \\ b^{ro2}_{1} & b^{ro2}_{2} & \cdots & b^{ro2}_{dim} \\ \vdots & \vdots & \vdots & \vdots \\ b^{ron}_{1} & b^{ron}_{2} & \cdots & b^{ron}_{dim} \end{bmatrix} \quad (24)$$

From Equation (24), b^{ron}_{dim} denotes the n-th best route among the routes of dimension dim. The fitness value of the route position can be assessed by:

$$fi = \begin{bmatrix} fi^{1}\left(ro^{1}_{1}, ro^{1}_{2}, \ldots, ro^{1}_{dim}\right) \\ fi^{2}\left(ro^{2}_{1}, ro^{2}_{2}, \ldots, ro^{2}_{dim}\right) \\ \vdots \\ fi^{n}\left(ro^{n}_{1}, ro^{n}_{2}, \ldots, ro^{n}_{dim}\right) \end{bmatrix} \quad (25)$$

The array is used to store the fitness value of route positions in which the fitness value of the n-th route of dim is denoted as ro^{n}_{dim}. There are three cases in which the optimal route can be obtained. In the first case, the best route can be obtained based on link stability and direction. In that case, the route positions are updated by:

$$ro^{j}_{t+1} = glo^{best} + \left[tdis^{t}\left(best^{j}_{t} - b^{roj}_{t}\right)RA^{1} + tdis^{t}\left(b^{roj}_{t} - b^{rob(j)}_{t}\right)RA^{2}\right]sgn(RA - 0.5) \quad (26)$$

From Equation (26), ro^{j}_{t+1} denotes the j-th route position at t+1 iteration, b^{roj}_{t} denotes the best route position among all the routes, the global best route based on link stability and direction can be denoted as glo^{best}, $b^{rob(j)}_{t}$ denotes the super best method to determine the optimal route, and the distance of tracking from the optimal route can be denoted as $tdis^{t}$. Furthermore, the fitness score $fi(.)$ can be computed by updating the $b^{rob(j)}_{t}$, which can be formulated as:

$$b^{rob(j)}_{t} = \begin{cases} ro^{j}_{t} & iffi\left(ro^{j}_{t+1}\right) \geq fi\left(b^{rob(j)}_{t}\right) \\ b^{rob(j)}_{t} & iffi\left(ro^{j}_{t+1}\right) < fi\left(b^{rob(j)}_{t}\right) \end{cases} \quad (27)$$

In the second case, the optimal routes can be determined based on energy value, link stability, and direction of the routes. At that case, the route position can be updated by:

$$ro^{j}_{t+1} = tdis^{t}[(up_{i} - lb_{i})RA + lb_{i}] \quad (28)$$

In this case, there is better knowledge on selecting the optimal routes in the SDWSN environment. To further improve the global and local search rate, the optimal routes can be obtained by computing the energy value, link stability, direction, and trust value. Algorithm 4 provides the detailed pseudocode for AFT-based optimal route selection. In that case, the optimal route position can be updated by:

$$ro^{j}_{t+1} = glo^{best} - \left[tdis^{t}\left(best^{j}_{t} - b^{roj}_{t}\right)RA^{1} + tdis^{t}\left(b^{roj}_{t} - b^{rob(j)}_{t}\right)RA^{2}\right]sgn(RA - 0.5) \quad (29)$$

Algorithm 4: Pseudocode for AFT-based Optimal Route Selection

Begin
  Initialize: lb_i, up_i, ro, glo^{best}, $best_t^j$,
  Initialize: Best route position of all routes b^{ro}
  Compute fi(ro) to all the routes
  Set t←1
  While $(t < T)$ **do**
    Set the tracking distance $tdis^t$
    Set the potential of routes ro(p)
    For $j = 1, 2, \ldots, n$ **do**
      If $(RA \geq 0.5)$ **then**
        If $(RA \geq ro(p))$ **then**
          Use case 1 to perform route determination (26)
        Else
          Use case 2 to perform route determination (28)
        End If
      Else
        Use case 3 to perform router determination (29)
      End If
    End For
    For $j = 1, 2, \ldots, n$ **do**
      Search for optimal routes feasibility
      Update glo^{best}, $best_t^j$ of ro
      Update $b^{ro}{}_t^{b(j)}$ based on (27)
    End For
    $t = t + 1$
  End While
End

Once the set of multiple optimal routes is determined, the optimal routes are ranked using the MCDM algorithm based on metrics such as link stability (ls), direction (dir), trust (tru), and energy (ene). The proposed MCDM utilized the Topsis method for ranking the optimal routes. At first, the assessment matrix is created with e-alternatives and q-criteria, which can be denoted as $(\forall_{ji})_{e\times q}$. The matrix $(\forall_{ji})_{e\times q}$ gets normalized using formulation

$$Nor_{ji} = \frac{\forall_{ji}}{\sqrt{\sum_{k=1}^{n} \forall_{ki}^2}},\ j \in [1, n], i \in [1, m] \tag{30}$$

From Equation (30), the normalized route matrix can be denoted as $\mathbb{N} = (Nor_{ji})_{e\times q}$. Once normalized, the weights are provided for every route based on their criteria $We_i \in [0, n]$ in which the n determines the n-number of selected optimal routes. Upon providing the weights for the route criteria, the normalization performed for the weighted matrix can be formulated as:

$$Nwei_{ji} = \forall_{ji} \frac{We_i}{\sqrt{\sum_{k=1}^{n} We_k}} \tag{31}$$

where $Nwei_{ji}$ denotes the normalized weight matrix. After that, we tend to obtain the best and worst route criteria from the weighted matrix that can be denoted as $Nwei_{besti}$ and $Nwei_{worsti}$, respectively. Based on that, we have determined the L2 norm distance among the $Nwei_{ji}$ as well as $Nwei_{besti}$ and $Nwei_{worsti}$. The formulation of L2 norm distance can be provided as:

$$L2_{jbest} = \sqrt{\sum_{i=1}^{m} (Nwei_{ji} - Nwei_{besti})^2},\ j \in [1, n] \tag{32}$$

$$L2_{jworst} = \sqrt{\sum_{i=1}^{m} (Nwei_{ji} - Nwei_{worsti})^2},\ j \in [1, n] \tag{33}$$

After that, the worst condition similarity is determined based on the formula provided below:

$$\text{sim}_{\text{worsti}} = \frac{\text{L2}_{\text{jworst}}}{\text{L2}_{\text{jworst}} + \text{L2}_{\text{jbest}}},\ \text{sim}_{\text{worsti}} \in [0,1],\ \text{j} \in [1,\text{n}] \tag{34}$$

where $\text{sim}_{\text{worsti}}$ is the worst alternative similarity in which routes are categorized based on results from Equation (34) as:

$$\text{sim}_{\text{worsti}} = \begin{cases} 0, \text{ WorstRoute} \\ 1, \text{ BestRoute} \end{cases} \tag{35}$$

Based on that, the optimal determined routes are ranked using the MCDM method. The table illustrates the optimal route ranking using the MCDM method.

From the Table 1 provided below, the green shaded region denotes the best route, whereas the orange shaded region denotes the worst route based on the computation of proposed four route criteria.

Table 1. MCDM-based optimal routes ranking.

Routes	Alternatives	Route Criteria→(q_2,q_2,q_3,q_4)				$\text{sim}_{\text{worsti}}$	Rank
		ls	dir	tru	ene		
ro (1)	e_1	30%	Outwards	0.1	10 J	0.215	6
ro (2)	e_2	80%	Outwards	0.75	20 J	0.842	3
ro (3)	e_3	97%	Towards	0.9	50 J	0.971	1
ro (4)	e_4	60%	Outwards	0.5	15 J	0.787	4
ro (5)	e_5	88%	Towards	0.8	30 J	0.912	2
ro (6)	e_6	50%	Towards	0.3	12 J	0.456	5

The two-way routing is enabled by the local gateway to the underlying WSN nodes and edge-assisted switches. However, the security of the proposed routing is achieved by a trust metric, which is not enough to cover the complete routing security to the SDWSN environment. For that, the proposed work adopts MTD, which alters the attack and detection surface in a random manner to confuse the attackers, thereby improving the attackers' cost.

The first way of routing is performed in the infrastructure layer among the WSN nodes. In that, the intermediated attacks (i.e., MITM and eavesdropping attacks) are overcome by performing the encryption and decryption of routing packets using the Camellia Encryption Algorithm (CEA). The operations of CEA are the same as the work in [35]. Furthermore, the routing paths are randomly switched as the MTD countermeasure from the set of optimal ranked routing paths. By performing random route switching, the reconnaissance attacks in the infrastructure layer are mitigated. Figure 4 represents the CGAN-based MTD in the edge-assisted switch layer.

The second way routing is performed is in the edge-assisted SDN switch layer among the SDN switches. Similar to the infrastructure layer, the routing information was encrypted and the routing path was switched randomly. In addition to that, to overcome the threats faced by the high potential reconnaissance attackers the proposed work utilizes a reconnaissance agent in the switch plane to monitor suspicious activities. The attackers tried to target the weak points of the switches and impose attacks. The suspicious activities include frequent visits to the network, unbounded network traffic, etc. From the suspicious activity, the current active edge-assisted SDN switches are idled and another set of switches are active to increase the attacker cost. The condition of active and idling SDN switches is decided by a deep learning algorithm named Cycle General Adversarial Networks (CGAN) based on the suspicious activity severity. The proposed CGAN is composed of discrimina-

tor (DC_x) and generator $(GN_{y\to x})$, which are trained iteratively to perform MTD operation (i.e., active switch handling). The loss due to adversary in the CGAN can be formulated as:

$$\mathbb{L}(GN_{y\to x}, DC_x) = \min_{\varnothing_{GN}}\max_{\varnothing_{DC}}\{\mathfrak{E}_y[\log DC_x(y)] + \mathfrak{E}_y[\log(1 - DC_x(GN_{y\to x}(x))]\} \quad (36)$$

From Equation (36), $\varnothing_{DC}$ and $\varnothing_{GN}$ denote the discriminator and generator parameters. The unpaired data for the target source can be denoted as $y \in Y$ and $x \in X$, respectively. Since we adopt CGAN, the consistency in backward and forward dependency in training data is defined. Henceforth, the cycle loss can be formulated as:

$$\mathbb{L}(GN_{y\to x}, GN_{x\to y}, DC_x, DC_y) = \mathbb{L}(GN_{y\to x}, DC_x) + \mathbb{L}(GN_{x\to y}, DC_x) + \propto \mathbb{L}_c(GN_{y\to x}, GN_{x\to y}) \quad (37)$$

From which the $\mathbb{L}_c$ is equated as,

$$\mathbb{L}_c(GN_{y\to x}, GN_{x\to y}) = \|GN_{x\to y}(GN_{y\to x}(y)) - y\|_1 + \|GN_{y\to x}(GN_{x\to y}(x)) - x\|_1 \quad (38)$$

Equation (38) shows the cycle consistency loss of the proposed CGAN. On the whole, the MTD-based secure two-way routing resists against malicious routing attacks and also enables optimal routing in the SDWSN environment.

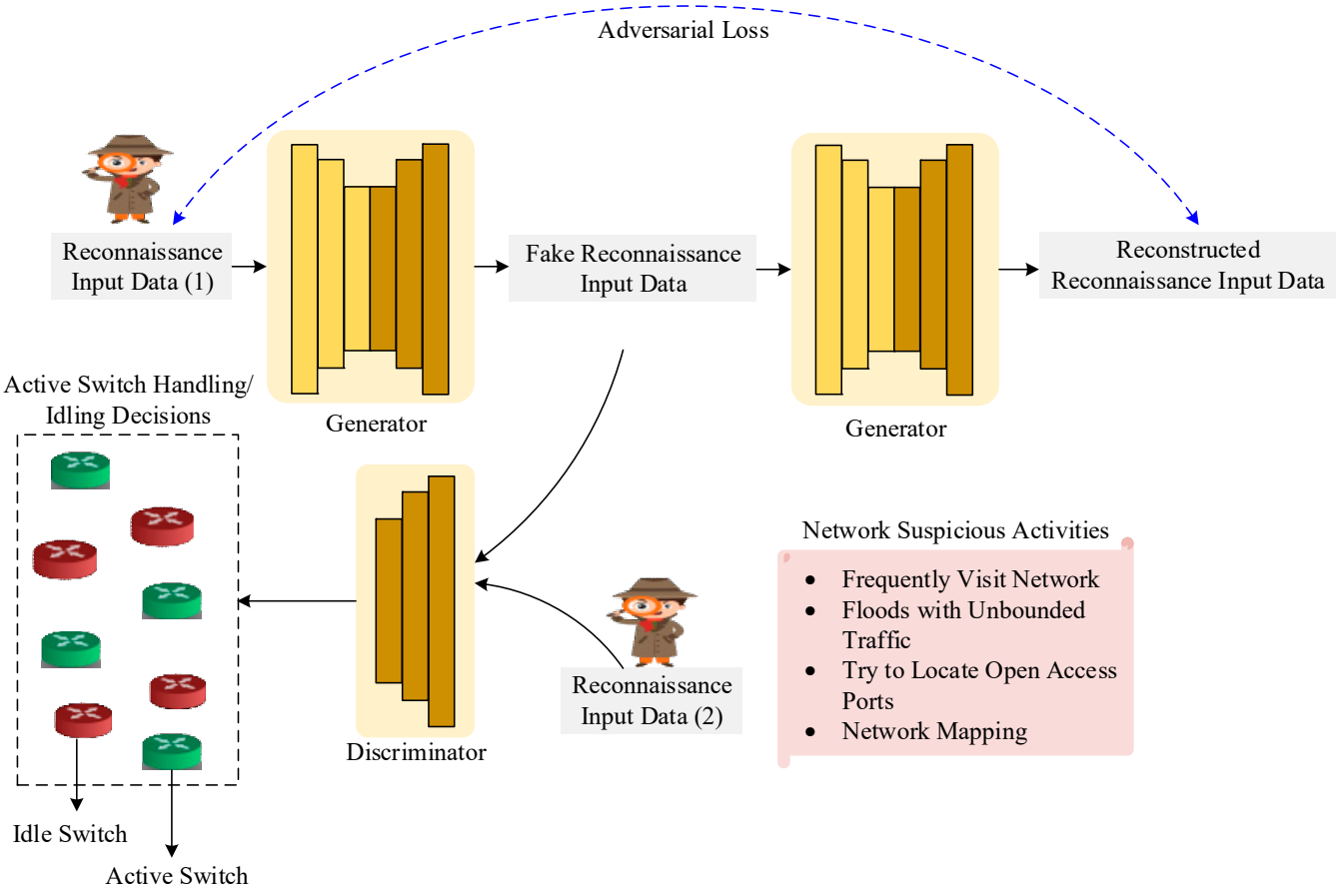

Figure 4. CGAN-based MTD (i.e., Active Switch Handling/Idling).

6. Experimental Results

This section provides the experimental results of the proposed MTS-SDWSN model by comparing it with two major existing models. In this section, the following sub-sections are illustrated: simulation setup, comparative analysis, and research summary. The detailed explanations are provided as follows.

6.1. Simulation Setup

The proposed MTS-SDWSN model is implemented using the Network Simulator-3.26 tool (NS-3.26). The utilization of the NS-3.26 simulator offers a reliable network environment that is perfectly suited for the proposed work. To realize a better simulation environment, the system and simulation configuration must be tuned. The system and simulation settings of the proposed work are shown in Tables 2 and 3. Furthermore, the representation of the simulation environment is also shown in Figure 5.

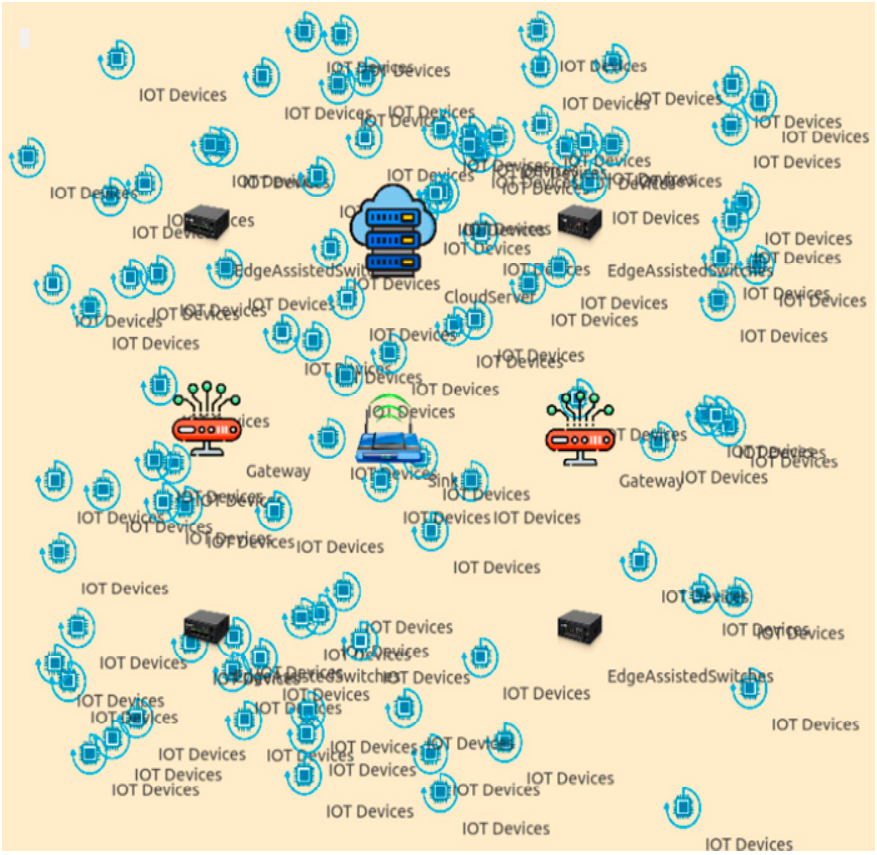

Figure 5. Proposed MTS-SDWSN simulation environment.

Table 2. System settings.

Hardware Settings			Software Settings	
Random Access Memory (RAM)	**Processor Used**	**Hard Disk Capacity**	**Simulation Tool Utilized**	**OS**
8 GB	Intel(R) Core (TM) i5-4590S CPU @ 3.00 GHz 3.00 GHz (Santa Clara, CA, USA)	500 GB	NS-3.26	Ubuntu LTS 14.04

Table 3. Simulation settings.

Simulation Parameter	Description
No. of sensor nodes	100
No. of gateway	2
No. of sink node	1
No. of edge assisted switches	4

Table 3. *Cont.*

Simulation Parameter	Description
No. of cloud server	1
Packet size	2^8 bytes
Transmission rate of packets	2 packets/sec
MAC protocol	IEEE 802.11p
Data transmission rate	3 Mbps
Area for simulation	1000×1000
Simulation time	300 s
Routing protocol for SDN	Open flow
Transmission range of nodes	25 m to 50 m
Size of payload	2^8 bytes

6.2. Comparative Analysis

In this supplementary section, the proposed MTS-SDWSN model is compared with two major existing models: Secure and Energy-aware Multi-hop Routing Protocol for WSN (SEMRP-WSN) [32] and Energy-Efficient Dynamic and Adaptive State Scheduling (EDASS) [33]. Those works are compared in terms of performance metrics such as energy consumption (J), packet delivery ratio (%), end-to-end delay (s), and attack mitigation/prevention rate (%).

6.2.1. Analysis of Energy Consumption

The energy consumption in the SDWSN is defined as the amount of energy spent by the WSN nodes for performing sensing in the environment. Mathematically, the difference among the initial and consumed energy reveals the energy consumption of the WSN node. The formulation is provided below:

$$\text{Ene} = \text{Tot}^{\text{ene}} - \text{Con}^{\text{ene}} \tag{39}$$

where Tot^{ene} is the total energy and Con^{ene} is the consumed energy by the WSN nodes.

Figure 6 represents the comparison of the energy consumption rate for the SDWSN nodes among the proposed MTS-SDWSN and existing works SEMRP-WSN and EDASS, respectively. The graphical inference reveals that the energy consumption gradually increases with an increase in SDWSN nodes. Intuitively, the proposed work gains lesser energy consumption than the existing works. The reason for such lesser energy consumption is the utilized clustering and cluster management methods, respectively. More especially, the clustering is performed using the DWTMB algorithm, which ensures precise and robust clusters, whereas in the worst case, we also perform cluster management by performing cluster splitting and merging based on the density and mobility of the SDWSN nodes. In disparity, the existing works SEMRP-WSN and EDASS lack in performing cluster the WSN nodes, which results in higher energy consumption as all the sensor nodes perform transmission and reception to a longer range. On the whole, the inference results reveal that the proposed work gains lesser energy consumption than the existing models.

The quantitative analysis from the graph shows that the proposed MTS-SDWSN gains energy consumption of 23 J when the number of SDWSN nodes reaches 100, whereas for the same SDWSN nodes the energy consumption rate of SEMRP-WSN and EDASS gains with 40 J and 47 J, respectively, which is 17 J–24 J higher than our proposed model.

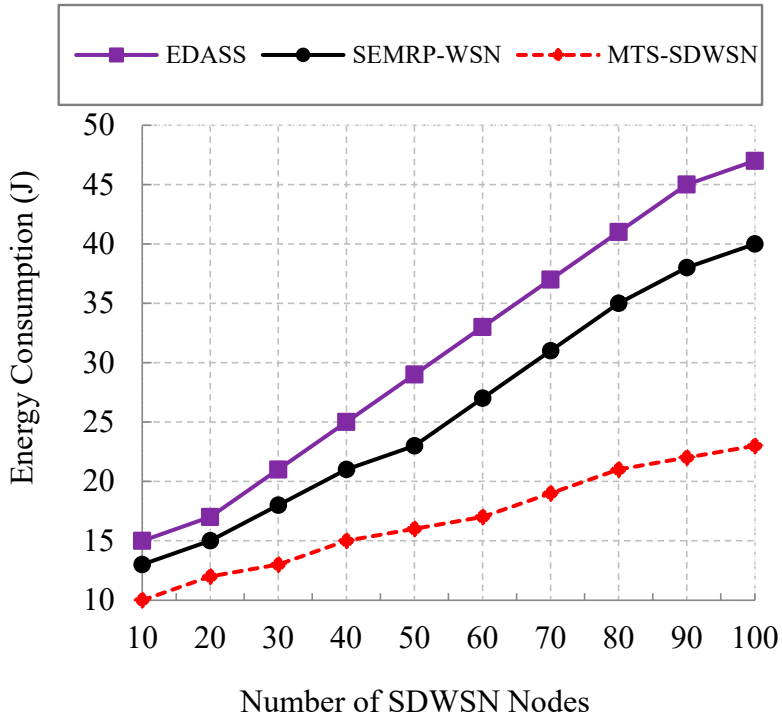

Figure 6. Number of SDWSN nodes vs. energy consumption.

6.2.2. Analysis of Packet Delivery Ratio

The Packet Delivery Ratio (PDR) is defined as the number of packets sent in total to the destination from the source without loss. The formulation of PDR is defined as follows:

$$\text{PDR} = \frac{\text{rec}^{\text{pkts}}}{\text{Tot}^{\text{tx}-\text{pkts}}} \times 100 \tag{40}$$

where rec^{pkts} is the received packets at the destination, and $\text{Tot}^{\text{tx}-\text{pkts}}$ is the total number of packets transmitted from the source.

The PDR comparison of proposed MTS-SDWSN and existing works SEMRP-WSN and EDASS are shown with respect to node speed in Figure 7. When the speed of nodes gets increased, the PDR gets decreased due to channel interference and packet loss. Our proposed MTS-SDWSN model gains better PDR than the existing works. The reason for such better PDR is that we perform multi-tier scheduling and MTD-based secure two-way routing. The multi-tier scheduling is performed among WSN-CLs, CLs-LBSs, and LBSs-SN using the NCFT algorithm. The utilized multi-tier scheduling model overcomes the complexity issue. The MTD-based two-way routing is performed in both infrastructure and switch layers in which the best optimal routes are selected using the SORP method that amalgamates AFT and MCDM. The utilized SORP lessens the PDR to the outer level, whereas the existing models SEMRP-WSN and EDASS lack utilizing such better routing protocol and also lack scheduling, which leads to higher packet and thereby less packet delivery ratio than the proposed work.

The quantitative analysis from the graph shows that the proposed MTS-SDWSN gains higher PDR of 50% when the speed of SDWSN nodes reaches 10 m/h, whereas for the same speed of nodes the PDR rate of SEMRP-WSN and EDASS gains with 28% and 15%, respectively, which is 22–35% less than our proposed model.

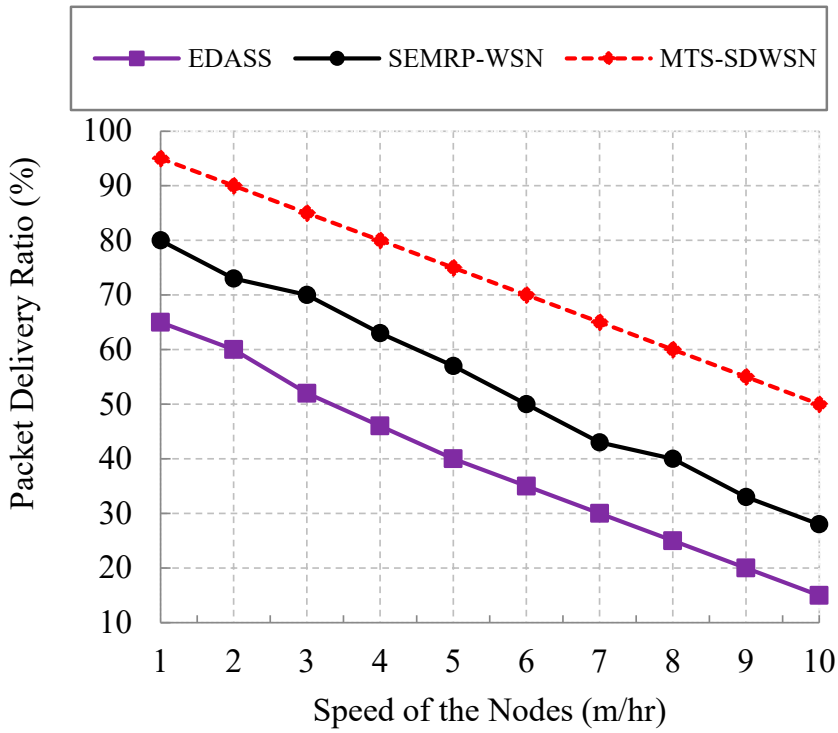

Figure 7. Speed of nodes vs. Packet Delivery Ratio.

6.2.3. Analysis of End-to-End Delay

The end-to-end delay is defined as the amount of time taken by the packets released from the WSN nodes to the destination. The mathematical formulation of end-to-end delay is defined as:

$$\mathrm{E2E} = \mathrm{Ov}^{\mathrm{del}} - \mathrm{Tx}^{\mathrm{del}} + \mathrm{Rx}^{\mathrm{del}} + \mathrm{Pro}^{\mathrm{del}} \quad (41)$$

where $\mathrm{Ov}^{\mathrm{del}}$, $\mathrm{Tx}^{\mathrm{del}}$, $\mathrm{Rx}^{\mathrm{del}}$, and $\mathrm{Pro}^{\mathrm{del}}$ denote the overall, transmission, reception, and processing delay, respectively.

Figure 8 represents the comparison of E2E with respect to SDWSN nodes for the proposed MTS-SDWSN and existing works SEMRP-WSN and EDASS works, respectively. From the figure, it is shown that the E2E of both the proposed and existing models increases with an increase in the number of SDWSN nodes. From the inference, it is shown that the proposed model gains less E2E than any of the existing works. The main reason for such lesser E2E is that we effectively construct the network with 2D hexagonal grids with the aid of ensuring robust and resilient connectivity, so that the packets sent are easily transmitted, received, and processed in less time, thereby achieving less E2E. In contrast, the existing works SEMRP-WSN and EDASS lacks with network construction; rather, they place their WSN nodes in a random manner, which leads to more time for transmission, reception, and processing results in higher E2E than the proposed work.

The quantitative analysis from the graph shows that the proposed MTS-SDWSN gains less E2E of 17 s when the SDWSN nodes reach 100, whereas for the same SDWSN nodes the E2E rate of SEMRP-WSN and EDASS gains with 23 s and 29 s, respectively, which is 6 s–12 s more than our proposed model.

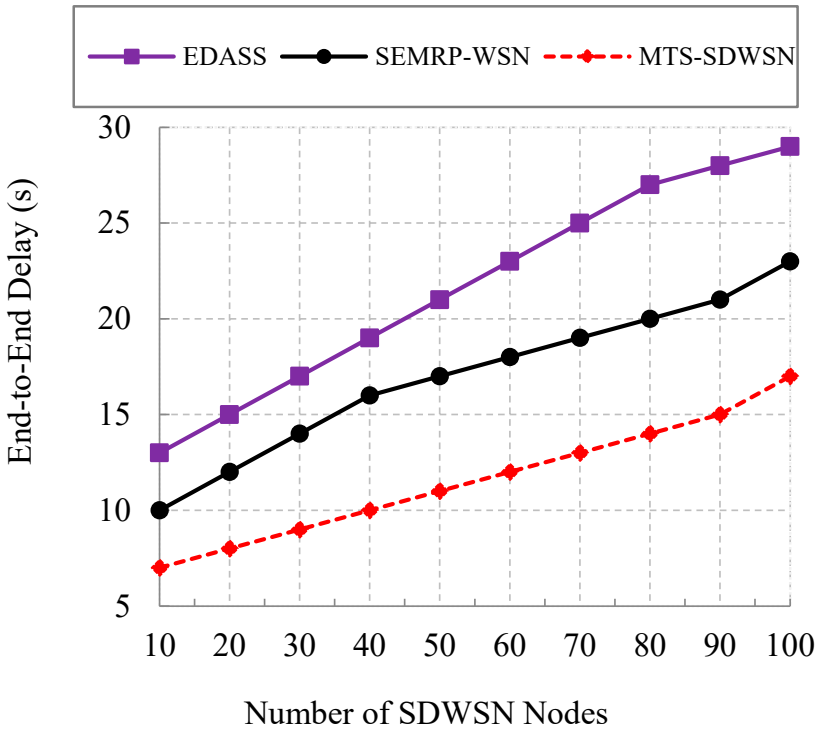

Figure 8. Number of SDWSN nodes vs. end-to-end delay.

6.2.4. Analysis of Attack Mitigation/Prevention Rate

The attack mitigation/prevention rate is defined as the amount of attack mitigated/prevented by the model with the number of security threats. Mathematically, the attack mitigation/prevention rate can be defined as:

$$\mathrm{Att}^{\mathrm{pre/mit}} = \frac{\mathrm{Tot}^{\mathrm{Att}^{\mathrm{pre/mit}}}}{\sum \text{cyber threats}} \times 100 \tag{42}$$

where $\mathrm{Tot}^{\mathrm{Att}^{\mathrm{pre/mit}}}$ is the amount of attack detected/mitigated and $\sum$cyber threats is the summation of cyber threats.

Figure 9 represents the comparison of attack mitigation/prevention rate with respect to the number of SDWSN nodes among the proposed MTS-SDWSN and existing SEMRP-WSN and EDASS works, respectively. From the graphical inference, it is revealed that the proposed work has a higher attack mitigation/prevention rate than the existing works. The reason for such a higher mitigation/prevention rate by the proposed work is that we perform MTD operation in our work. More clearly, the MTD operations by the reconnaissance agents in both the infrastructure and edge-assisted switch layer, respectively, in terms of route switching and active switch handling. The adopting of MTD operations in the proposed environment is more precisely to resist the reconnaissance attacks in the SDWSN environment. On the other hand, the existing SEMRP-WSN and EDASS works did not consider the security measures in their network leads to higher possibility of network entities to be vulnerable to cyberattacks, thereby decreasing the attack mitigation/prevention rate.

The quantitative analysis from the graph shows that the proposed MTS-SDWSN has a higher attack mitigation and prevention rate of 97% when the SDWSN nodes reach 100, whereas for the same SDWSN nodes the attack mitigation and prevention rate of SEMRP-WSN and EDASS gains with 82% and 79%, respectively, which is 15–18% less than our proposed model.

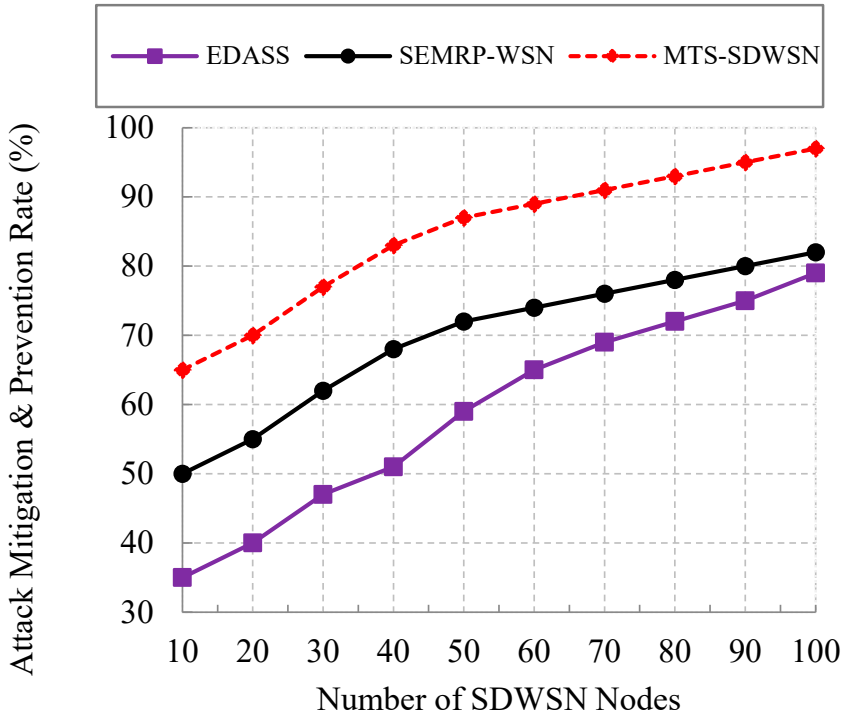

Figure 9. Number of SDWSN nodes vs. attack mitigation/prevention rate.

6.3. Research Summary

This section provides a brief summary of the implementation results. The proposed MTS-SDWSN work is implemented using a NS-3.26 simulation tool with proper system and simulation settings in Tables 2 and 3. The performance of the proposed work toward the implementation is extracted by validating the proposed model with the existing works in terms of four performance metrics. The qualitative and quantitative comparative analyses of the proposed and exiting models are shown in Figures 6–9. The results from both qualitative and quantitative show that the proposed model outperforms the existing works. The average quantitative results of the performance metrics are shown in Table 4.

Table 4. Average results of proposed vs. existing works.

Metrics		MTS-SDWSN	SEMRP-WSN	EDASS	Difference
No. of SDWSN Nodes	Energy Consumption (J)	≅ 16.8	≅ 26.1	≅ 31	≅ (9.3 – 14.2)
	E2 E Delay (s)	≅ 11.6	≅ 17	≅ 21.7	≅ (4.7 – 5.4)
	Attack Mitigation/Prevention Rate (%)	≅ 84.7	≅ 69.7	≅ 59.2	≅ (15 – 25.5)
Speed of the Nodes	PDR (%)	≅ 72.5	≅ 53.5	≅ 38.8	≅ (19 – 33.7)

7. Conclusions and Future Work

Amplified energy consumption, poor connectivity, scheduling, and security are some of the major problems addressed in this work. There are three layers designed in this work: the infrastructure layer, edge-assisted switch layer, and control layer with layer-specific entities.

The processes resided in our work are connectivity network construction, density-based clustering, multi-tier federated scheduling, and MTD-based secure two-way routing.

In the connectivity-aware network construction stage, the entities involved in the infrastructure layer are properly placed in 2D hexagonal grids to overcome the connectivity and coverage hole issues. In the density-based clustering stage, the SDWSN nodes are clustered using the DWTMB algorithm based on density and mobility. From the clustered nodes, the optimal CL is selected using high residual energy, less mobility, less distance from the local gateway, and high trust score. In addition, we have also maintained the cluster-by-cluster merging and splitting methods, respectively. In the multi-tier federated scheduling stage, the CMs-CLs, CLs-LBSs, and LBSs-SN are scheduled in three tiers using the NCFT algorithm with specific scheduling metrics. By performing multi-tier scheduling, the problem of complexity and collisions gets reduced. In MTD-based secure two-way routing, the SORP is proposed to select and rank the best routes using the AFT and MCDM algorithms, respectively. Furthermore, the trust evaluation and MTD methods are introduced in the proposed routing protocol for reduce cyber threats.

The NS-3.26 is a simulation tool used by the proposed work to implement the proposed model in which the performance is analyzed with four major performance metrics such as energy consumption (J), PDR (%), E2E(s), and attack mitigation/prevention rate (%) among the proposed and existing works. The simulation results reveal that the existing model underperforms the proposed work.

In the future, more works and investigations will be conducted on multitier scheduling in the SDWSN environment using different performance metrics such as temperature, electromagnetic noise, radiation, and weather conditions.

Author Contributions: Conceptualization, A.M.A.A. and (H.H.); data curation, A.A.M.S. and S.S.S.; formal analysis, (H.H.), S.S.S. and A.A.M.S.; investigation, A.M.A.A., (H.H.) and S.S.S.; methodology, A.M.A.A. and S.S.S.; resources, A.A.M.S.; software, (H.H.); supervision, A.M.A.A.; validation, A.M.A.A. and S.S.S.; visualization, A.A.M.S.; writing—original draft, A.M.A.A., (H.H.), S.S.S. and A.A.M.S.; writing—review and editing, (H.H.), A.M.A.A., S.S.S. and A.A.M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data will be made available upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lanzolla, A.; Spadavecchia, M. Wireless Sensor Networks for Environmental Monitoring. *Sensors* **2021**, *21*, 1172. [CrossRef]
2. Khalaf, O.I.; Romero, C.A.; Hassan, S.; Iqbal, M.T. Mitigating Hotspot Issues in Heterogeneous Wireless Sensor Networks. *J. Sens.* **2022**, *2022*, 7909472. [CrossRef]
3. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, C. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. *Sensors* **2022**, *22*, 2087. [CrossRef]
4. Sundarraj, S.; Konganathan, G. Energy Efficient Mobile Harvesting Scheme for Clustered SDWSN with Beamforming Technique. *Intell. Autom. Soft Comput.* **2022**, *34*, 1197–1213. [CrossRef]
5. Sixu, L.; Muqing, W.; Min, Z. Particle swarm optimization and artificial bee colony algorithm for clustering and mobile based software-defined wireless sensor networks. *Wirel. Netw.* **2022**, *28*, 1671–1688. [CrossRef]
6. Jurado-Lasso, F.F.; Marchegiani, L.; Jurado, J.F.; Abu-Mahfouz, A.M.; Fafoutis, X. A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current Status and Major Challenges. *IEEE Access* **2022**, *10*, 23560–23592. [CrossRef]
7. Jurado Lasso, F.F.; Marchegiani, L.; Jurado, J.F.; Mahfouz, A.A.; Fafoutis, X. A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current status and major challenges. *IEEE Access* **2016**, *10*, 23560–23592. [CrossRef]
8. Rahimifar, A.; Kavian, Y.S.; Kaabi, H.; Soroosh, M. A Smart Duty Cycle for Lifetime Enhancement and Control Overhead in SDWSN. *Iran. J. Sci. Technol. Trans. Electr. Eng.* **2023**, *47*, 1207–1223. [CrossRef]
9. Sundarraj, S.; Konganathan, G. A Novel Energy Efficient Harvesting Technique for SDWSN using RF Transmitters with MISO Beamforming. *Int. Arab J. Inf. Technol.* **2023**, *20*, 125–133. [CrossRef]
10. Rahimifar, A.; Seifi Kavian, Y.; Kaabi, H.; Soroosh, M. An efficient Markov energy predictor for software defined wireless sensor networks. *Wirel. Netw.* **2022**, *28*, 3391–3409. [CrossRef]
11. Martin, K.; Jozef, K. Distributed Mechanism for Detecting Average Consensus with Maximum-Degree Weights in Bipartite Regular Graphs. *Mathematics* **2021**, *9*, 3020. [CrossRef]

12. Dionisis, K.; Eleftherios, A. Advanced Wireless Sensor Networks: Applications, Challenges and Research Trends. *Electronics* **2024**, *13*, 2268. [CrossRef]
13. Merabtine, N.; Djenouri, D.; Zegour, D.E. Towards Energy Efficient Clustering in Wireless Sensor Networks: A Comprehensive Review. *IEEE Access* **2021**, *9*, 92688–92705. [CrossRef]
14. Orozco-Santos, F.; Sempere-Payá, V.; Silvestre-Blanes, J.; Albero-Albero, T. Multicast Scheduling in SDN WISE to Support Mobile Nodes in Industrial Wireless Sensor Networks. *IEEE Access* **2021**, *9*, 141651–141666. [CrossRef]
15. Bukar, U.A.; Othman, M. Architectural Design, Improvement, and Challenges of Distributed Software-Defined Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**, *122*, 2395–2439. [CrossRef]
16. Amin, R.; Rojas, E.; Aqdus, A.; Ramzan, S.; Casillas-Pérez, D.; Arco, J.M. A Survey on Machine Learning Techniques for Routing Optimization in SDN. *IEEE Access* **2021**, *9*, 104582–104611. [CrossRef]
17. AbdelKhalek, M.; Hyder, B.; Manimaran, G.; Rieger, C.G. Moving Target Defense Routing for SDN-enabled Smart Grid. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 27–29 July 2022. [CrossRef]
18. Wang, X. Low-Energy Secure Routing Protocol for WSNs Based on Multiobjective Ant Colony Optimization Algorithm. *J. Sens.* **2021**, *2021*, 7633054. [CrossRef]
19. Hajian, E.; Khayyambashi, M.R.; Movahhedinia, N. A Mechanism for Load Balancing Routing and Virtualization Based on SDWSN for IoT Applications. *IEEE Access* **2022**, *10*, 37457–37476. [CrossRef]
20. Huang, R.; Guan, W.; Zhai, G.; He, J.; Chu, X. Deep Graph Reinforcement Learning Based Intelligent Traffic Routing Control for Software-Defined Wireless Sensor Networks. *Appl. Sci.* **2022**, *12*, 1951. [CrossRef]
21. Han, Y.; Hu, H.; Guo, Y. Energy-aware and Trust-based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm. *IEEE Access* **2022**, *10*, 11538–11550. [CrossRef]
22. AlOtaibi, M. Improved Blowfish Algorithm based Secure Routing Technique in IoT based WSN. *IEEE Access* **2021**, *9*, 159187–159197. [CrossRef]
23. Sharadqh, A.A.M.; Hatamleh, H.A.M.; Alnaser, A.M.A.; Saloum, S.S.; Alawneh, T.A. Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment. *IEEE Access* **2023**, *11*, 27433–27449. [CrossRef]
24. Farooq, M.U.; Wang, X.; Hawbani, A.; Zhao, L.; Al-Dubai, A.Y.; Busaileh, O. SDORP: SDN based Opportunistic Routing for Asynchronous Wireless Sensor Networks. *IEEE Trans. Mob. Comput.* **2022**, *22*, 4912–4929. [CrossRef]
25. Singh, K.; Khan, T.A. TASRP: A trust aware secure routing protocol for wireless sensor networks. *Int. J. Innov. Comput. Appl.* **2021**, *12*, 108–122. [CrossRef]
26. Bin-Yahya, M.; Shen, X. HTM: Hierarchical Trust Management for Software-Defined WSNs. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019. [CrossRef]
27. Banerjee, A. Design of A Fuzzy-controlled Energy–Efficient Multicast Scheduler (FEMS) For SDWSN. *J. Inf. Technol. Manag.* **2021**, *13*, 111–132.
28. Suja Golden Shiny, S.; Murugan, K. TSDN-WISE: Automatic Threshold-Based Low Control-Flow Communication Protocol for SDWSN. *IEEE Sens. J.* **2021**, *21*, 19560–19569. [CrossRef]
29. Liu, Y.; Sun, D.; Zhang, R.; Li, W. A Method for Detecting LDoS Attacks in SDWSN Based on Compressed Hilbert–Huang Transform and Convolutional Neural Networks. *Sensors* **2023**, *23*, 4745. [CrossRef]
30. Yang, L.; Lu, Y.; Yang, S.X.; Zhong, Y.; Guo, T.; Liang, Z. An Evolutionary Game-Based Secure Clustering Protocol with Fuzzy Trust Evaluation and Outlier Detection for Wireless Sensor Networks. *IEEE Sens. J.* **2021**, *21*, 13935–13947. [CrossRef]
31. Zhu, H.; Qiu, H.; Zhu, J.; Chen, D. SMSEI-SDN: A Suppression Method of Security Incident Impact for the Inter-Domain Routing System Based on Software-Defined Networking. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5539790. [CrossRef]
32. Ren, Q.; Hu, T.; Wu, J.; Hu, Y.; He, L.; Lan, J. Multipath resilient routing for endogenous secure software defined networks. *Comput. Netw.* **2021**, *194*, 108134. [CrossRef]
33. Vinitha, A.; Rukmini, M.S.; Dhirajsunehra. Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. *J. King Saud Univ. Comput. Inf. Sci.* **2019**, *34*, 1857–1868. [CrossRef]
34. Khan, M.N.; Rahman, H.U.; Khan, M.Z.; Mehmood, G.; Sulaiman, A.; Shaikh, A.; Alqhatani, A. Energy-Efficient Dynamic and Adaptive State-Based Scheduling (EDASS) Scheme for Wireless Sensor Networks. *IEEE Sens. J.* **2022**, *22*, 12386–12403. [CrossRef]
35. Wei Ci, C.; Zarina Md Naziri, S.; Che Ismail, R.; Hussin, R.; Nazrin Md Isa, M.; Sufyan Safwan Mohamad Basir, M. Crypto-Core Design using Camellia Cipher. *J. Phys. Conf. Ser.* **2021**, *1755*, 012019. [CrossRef]