applied sciences

MDPI

Article

Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs

Shamim Younas [1], Faisal Rehman [1], Tahir Maqsood [1], Saad Mustafa [1], Adnan Akhunzada [2] and Abdullah Gani [3,*]

[1] Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus, Abbottabad 22060, Pakistan
[2] Department of Data & Cybersecurity, College of Computing and IT, University of Doha for Science & Technology, Doha 24449, Qatar
[3] Faculty of Computing & Informatics, University Malaysia Sabah, Kota Kinabalu 88400, Malaysia
* Correspondence: abdullahgani@ums.edu.my

Abstract: Vehicle ad hoc networks (VANETs) are vital towards the success and comfort of self-driving as well as semi-automobile vehicles. Such vehicles rely heavily on data management and the exchange of Cooperative Awareness Messages (CAMs) for external communication with the environment. VANETs are vulnerable to a variety of attacks, including Black Hole, Gray Hole, wormhole, and rush attacks. These attacks are aimed at disrupting traffic between cars and on the roadside. The discovery of Black Hole attack has become an increasingly critical problem due to widespread adoption of autonomous and connected vehicles (ACVs). Due to the critical nature of ACVs, delay or failure of even a single packet can have disastrous effects, leading to accidents. In this work, we present a neural network-based technique for detection and prevention of rushed Black and Gray Hole attacks in vehicular networks. The work also studies novel systematic reactions protecting the vehicle against dangerous behavior. Experimental results show a superior detection rate of the proposed system in comparison with state-of-the-art techniques.

Keywords: vehicle ad hoc networks (VANETs); black hole; Gray Hole; linear regression (LR); linear discriminant analysis (LDA); support vector machine (SVM); naïve Bayes (NB)

Citation: Younas, S.; Rehman, F.; Maqsood, T.; Mustafa, S.; Akhunzada, A.; Gani, A. Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs. *Appl. Sci.* **2022**, *12*, 12448. https://doi.org/10.3390/app122312448

Academic Editor: Wenbo He

Received: 2 August 2022
Accepted: 9 September 2022
Published: 5 December 2022

1. Introduction

Vehicular networks that form on-the-spot VANETs play a crucial role in the development and applications of self-driving and moderately automotive cars [1]. In autonomous as well as semi-autonomous vehicles, both internal communication systems and external communication systems are critical components. As can be seen in Figure 1, VANETs in radio coverage areas represent exchange of messages among cars (V2R) and roadside units (RSUs) or in-vehicle (V2V). External communication in intelligent transport system (ITS) between self-driving cars and highway infrastructure depends largely on the wireless transmission standard IEEE 802.11p [2]. The communication uses Cooperative Awareness Messages (CAMs) or basic safety, which are exchanged between RSUs and automobiles or between vehicles in the region [3]. The major purpose of ITS communication is to ensure the safety of drivers and passengers on the road. Because previous networks lacked a set safety infrastructure, such as cables network, VANETs [4] are movable nodes that enable communication with the RSU and in a certain zone [5]. Many researchers view VANETs as a Mobile ad hoc Network Subclass or Subtype (MANETs) [3]. They immediately influence the ITS by providing drivers and passengers with comfort and safety applications. The main objective of VANETs is to maintain the protection of both road operators and automobiles. As mentioned above, such systems could reach their targets as well as provide assistance and relief reports to drivers as well as passengers, including emergency alarms, warnings or accident alerts, by transmitting warning and control data [5–8].

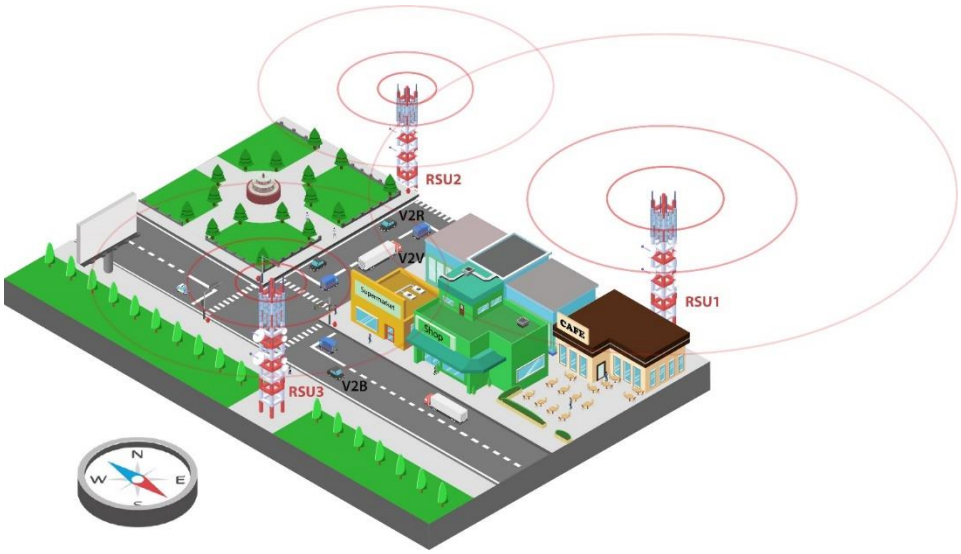

Figure 1. Basic structure of VANETs.

In vehicular ad hoc networks, there are three types of routing techniques used: (1) the pre-emptive, (2) reactive, and (3) the hybrid [7]. The routing protocol employed by demand vectors is an important routing protocol that is frequently used in outside messages for self-driving automobiles. The protocol known as ad hoc On-Demand Distance Vector (AODV) was chosen because of its higher performance and lower latency [7]. The use of sequence numbers empowers AODV to run further, effectively in contrast to other routing protocols. In autonomous and semi-autonomous cars, message and car authentication in supportive vehicle ad hoc systems is essential to provide security, as well as notification messages and threatening notices along with control information. Traditional safety mechanisms such as encryption/decoding methods can prevent external assaults from reaching their objective of stealing vital data and information monitoring among roadside units and autonomous vehicles. These cars, still, are incapable of protecting external communication from internal threats. Moreover, each VANET layer is subject to attacks [8,9], making its protection one of the biggest challenges [9]. The focus of this article is denial of service, Black Hole, Gray Hole, and rush attacks [10]. The Gray Hole and rush occurrences can halt collaboration and cause cars to be disconnected from the roadside [10]. The development of an appropriate security system is essential for network layer routing protocols. Perhaps, malevolent nodes displace or discard packets instead of delivering packets to the right target node. Most packets received are discarded and are not forwarded to their target node for such assaults. Other difficulties may occur with such an assault, such as overhead rise and the packet delivery rate (PDR) for network decrease [10]. Attack detection is challenging since data packets are dropped selectively [11]. A network with a Gray Hole attack transmits packets as a 'true' behavior to the target node during the process discovery phase, and then when the network acts badly, they are discarded [9–13].

Denial of Service (DoS) and Black Hole attacks are the most virulent types of cyber-attacks available. In VANETs, this kind of assault is known as a full packet drop attack. A Black Hole node might enter the network invisibly due to the open medium and dynamic topology of MANETs and remain there indefinitely. During the route discovery phase, the emergence of Black Hole nodes is a common occurrence. It is initially unknown whether the receiver can reach the source node via a feasible route. The path between the source and destination nodes is found when intermediary systems obtain a Route Request (RREQ) message [12–15]. A Gray Hole assault is a sort of distributed service denial assault that is an extension of a Black Hole assault in nature. It is referred to as a partial packet dropping technique because it loses only the data packets that are targeted during transmission. Gray nodes are not harmful nodes at first since they act in the same way as regular nodes

during the process of path discovery. When it comes to MANETs, detecting Gray Hole nodes might be a difficult process, since during the route selection procedure, they do not communicate the right sequence number. They eventually transform into hostile nodes when data packets are delivered from the source over an extended length of time to the target node [16–20].

We present a strategy termed dual attack detection for Black and gray node [3] in order to detect and isolate rogue nodes from VANETs. In the beginning, Dual attack Detection for Black and Gray hole attacks (DDBG) used Connected Dominating Set (CDS) technology to create tiny groups of nodes within the network. Second, the DDBG chooses the intrusion detection system (IDS) component set of tiny CDS node groups that have sufficient power and do not belong to the blacklist. The third stage selects an IDS node with maximum energy in the IDS set. The IDS node needs to be a node of trust. The IDS node then regularly transmits status packets to detect the malicious node in the IDS set. If the behavior of any node is suspected of being malicious, the IDS node sends a block message to alert all nodes. All nodes will then terminate contact with the specific malicious node. Unlike previous works, we present a neural network-based intelligent system for the detection and prevention of rushed Black and Gray Hole attacks. The following are the contributions of this study:

- Using the linked dominant set (CDS) approach, we present a detection method for harmful Black Holes and Gray Holes using the nodes for intrusion detection. When used in dense networks, the proposed method is also effective in distinguishing hostile nodes, particularly those that use clever Gray Hole attacks.
- We use neural networks for efficient detection of attacks that results in better throughput as compared to conventional schemes.
- Comprehensive experimental results reveal that the proposed approach is an effective strategy for Black and Gray Hole attack identification compared with the state-of-the-art techniques.

The rest of the article is summarized as follows. Prior research work is discussed in Section 2. System models and methodology used in this work are presented in Section 3. Proposed techniques and algorithms are presented in Section 4. Section 5 outlines the simulation scenario and experimental results. Conclusions and future work are discussed in Section 6.

2. Literature Review

An algorithm developed by researcher [7] in a vehicular network was utilized to locate Black Hole nodes [8]. Each node in the network has a trust routing table (TRT), which comprises a list of all the network's trustworthy nodes. In response to packets received from the destination node, each sender node updates its trust value on a periodic basis [21–24]. To determine which neighbor is the best, the trust value is combined with the progress value. For the purpose of finding a single Black Hole node, the author employs a greedy geographical routing protocol, also termed as position-based routing. Following the receipt of the initial RREQ, the authors of [9] enhanced performance on the original AODV by inserting a timer into the Rimer Expired Table after receiving the initial RREQ to collect requests from other nodes. The collect route replay table also saves the destination number and time, counts the timeout on the basis of the initial RREQ and assesses the validity of the route by checking the threshold values with the destination number and the received time [5].

The watchdog approach was proposed by [10], who offered a mechanism for identifying malicious nodes. In this approach, nearby nodes keep track of the data packets that they overhear being transmitted and received by their surrounding nodes and then store those records. When the number of failures exceeds a specific threshold, it is transmitted to the source node. It is not possible to detect rogue nodes using this method when collisions occur [10].

The researchers in [11] proposed methods for detecting and eliminating Black Hole attacks. The header of the AODV is changed in this manner by the addition of a parent vehicle. The addresses of the packet's previous originator are contained in this parent vehicle field. In order to eliminate route recovery sessions, which are also known as link failure sessions, the route redundancy technique is utilized. Although it decreases E2E latency, routing overhead increases as a result of this. In [25], the use of a hash function to defend against AODV's Black Hole attacks was advocated. Here, the first optimal path is rejected, and the second optimal path is chosen over the first optimal path. Here, the hash function is employed to ensure data integrity, and this function may be used to detect the rogue node in the second optimum path. The message's hash value is calculated at the source node as (SHA-ONE), and the received message's hash value is calculated separately at the destination node as (SHA-ONE) (SHA-TWO). It is possible that the message received will not be altered if both hash values are the same; otherwise, a data packet error (DPE) message will be sent throughout the network. A table will be used to keep the record of information, which is called the routing table.

By combining the ad hoc On Demand Multipath Distance Vector (AOMDV) routing with soft encryption, the researchers in [8] provide a method for combining trust-based multipath AOMDV routing with a soft-encryption technique. This strategy uses XOR operations to encrypt messages, the second approach uses the multiple route node disjoint AOMDV routing protocol with various trust-based values, and the third approach uses XOR procedures to encrypt messages. The final stage is message decryption, which occurs at the destination end of the transmission. According [14], the 'Resource Efficient Accountability (REAct)' method includes an auditing, searching, and identifying procedure. A feedback message is delivered to the source node whenever a packet is lost, and the source node then picks an audit node. The audit node makes use of the bloom filter in order to obtain a proof of behavior. Although the routing overhead is reduced, the identification latency is enhanced with this method. There is a significant drawback to this technique in that it does not utilize cooperative Black Hole identification [14].

In [26] a heuristic technique to detect, in MANETs, Black Hole assaults. The approach was used by MANET, although it is also applicable to VANET. The method is commonly utilized for sending fake packets to discover the AODV path. Since a Black Hole rarely searches the routing table first before the requested node is returned, a Black Hole is caught by responding with its request to the false IP address that has not been found in the system. This method has been used to identify solo and joint Black Hole assaults. The author established an automobile monitoring procedure. Vehicles are placed together in their solution into several clusters lead by the cluster head (CH), which in each cluster is the most dependable automobile. Whenever a new car is added to the cluster, the verifier begins scanning for information about the new vehicle's characteristics and actions. It notifies CH when the verifier observes that the van often drops packages; otherwise, it does nothing. CH therefore decreases the trust value of the car and reports this incidence to its neighbors. When the trust value of a vehicle is below a certain threshold, CH alerts a certificate authority (CA). The automobile is placed on the Black List by the CA. It then alerts all the cars that it stops connecting within the Black Listed node. The testing findings show that the proposed strategy can detect malicious intruders even when they move quickly [27].

The preventive technique introduced in [27], and the verifier selection is refined in [28]. The researchers in [29] further expanded the strategy given in [27], including a methodology used to eliminate and isolate from the entire network a Black Hole. The procedure presented in [28] is identical to the approach proposed in [27]. It is distinguished by the additional parameter used to isolate the attacker and the alerts created by the identification of the malicious node that is spread around the networks. When compared to [24], the suggested method was more effective in preventing and detecting attackers with high mobility. The authors in [26] improved the technique of detection introduced in [27] by increasing the number of checks to run, which is determined by the load, the

distance between checks and the suspicion score. When comparing simulation results to those given in [27], it has been discovered that performance metrics have improved.

Regarding MANETs, a method was developed for recognizing nodes with a Black Hole or Gray Hole, which was published by researchers [30]. The authors used the AODV MAC layer to execute their security measures. The team (Cseq) created two new control packets: the Response sequence (Rseq) and Code Sequence (CodeSeq). To find a route and gain access to a channel, a source must first send Cseq to all of its neighbors, and that neighbor must then send Rseq to all its neighbors. A link to a network layer is formed if both the Cseq and the Rseq of a given neighbor match; otherwise, that neighboring node is rejected by the source node, and others are informed that this is a dangerous node.

The researchers utilized an IDS based on information (datasets) from trace files that were kept in a database by executing the Network Simulator 2 (NS2) code in a VANET environment. Trace files have been broken down into three categories: the basic trace, the trace of internet protocol, and the trace of AODV. In order to estimate the proposed solution, the features obtained from the trace files were then employed to inform future developments. When determining if a vehicle's behavior is malevolent or normal, these characteristics were utilized as the determining factor. For the purpose of feature extraction, a statistical approach known as Proportional Overlapping Scores was employed (POS) [31].

The above studies proposed different security techniques to deal with multiple kinds of attacks in Black and Gray Holes. Moreover, recent works also considered the detection of malicious nodes. Different encryption techniques such as hashing with SHA-256 were also considered to secure the communication. However, recent works neglected the use of neural networks for efficient detection of rushed Black and Gray Hole attacks, which is the main focus of this study. We present the classification of DOS attacks discussed above in Figure 2.

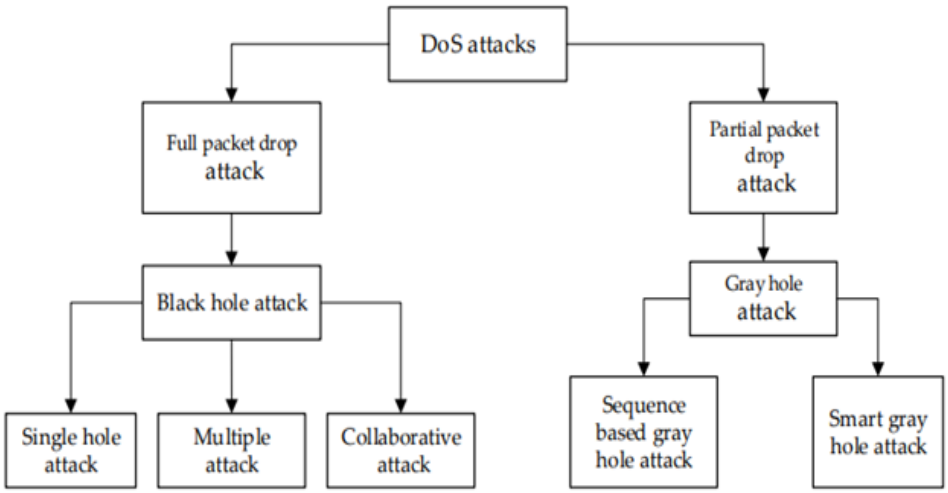

Figure 2. Classification of DDOS attack.

3. Research Methodology

3.1. Technical Overview

The VANETs are closely related to Mobile ad hoc Networks (MANETs), but they vary in that their nodes are mobile and that their topology changes frequently, making them more difficult to discern [32]. Furthermore, VANETs are established on their own initiative and have a rather limited lifespan. VANETs are predominantly used by mobile nodes (i.e., cars), while networks can also support ongoing facilities called Road Side Units (RSUs) [33]. In the event where a node is not immediately in range of another, nodes that desire to interact with that node can accomplish this by forwarding neighboring nodes in the network to reach their target. Many different routing protocols are available, but we concentrate on the ad hoc on demand distance vector routing protocol (AODV), which is among

the most important and commonly utilized protocols in works today. Security breaches affecting the availability of VANETs and other Internet of Things (IoT) devices are a major source of worry, particularly as the dependence on applications that need intravehicular communication grows [34–36]. This document discusses in more detail the Black Hole assault. A node during this assault misrepresents itself as having the quickest path to a target in order to gain attention. Following the selection of this route, packets from the source should be relayed to the next hop on the route by the node. However, these packets are intentionally dropped, blocking communication between the source and destination nodes from taking place. In the event of a single node, we propose a detection mechanism for the assault existing in a network, which is discussed in subsequent text. The single malicious node scenario represents the most basic example regarding this issue. In this work, we present two new ways to improve the capability of our defenses to identify and prevent Black Hole attacks involving many malicious nodes, which are currently ineffective. We are able to show the effectiveness of these new methods and our better preventive measures through simulations of the attack and through the use of our solution in network simulator 2 (NS-2). The results of these simulations indicate that our countermeasure is accurate in its detection of Black Hole assaults and is effective in its prevention of Black Hole attacks. In instances when a Black Hole attack was present, the usage of our approach resulted in a proportional boost in network performance when compared to when it was not used.

3.2. Network Simulator 2 (NS-2)

We have performed our experiments on Network Simulator 2 (NS2). NS2 is used for validating the performance of Wireless Networks, such as WBANs. This simulator is object oriented and programming based. We have added the detail of protocol to initiate a system programming that changes the bytes, packets headers and implements the algorithm that will run on the dataset of human body sensor values. In this system, we checked the cluster head selection and we calculated the energy consumption between nodes. Exponentially Weighted Move-Average was employed (EWMA) [37]:

$$E_{harvest}\left(t, P_{setup}\right) = Z\left(t, P_{setup}\right)\, t\, \lambda_{i\ (0)} d_0$$

where $E_{harvest}$ is the estimated gathered energy of the sensor nodes i for a period of 0, whereas the charge rate of node i at the time 0 is λ_i (0).

3.3. Performance Evaluation

We evaluated our model by calculating the following numbers of nodes.

3.3.1. Dead Nodes Numbers

These nodes have an energy, but they become dead by supplying energy. This tells us the total number of energy consumption in the Wireless Body Area Networks (WBANs).

3.3.2. Alive Nodes Numbers

These nodes have energy, and they are supplying energy. After supplying energy, they have enough energy to survive. Alive node numbers are used to attain energy for the whole WBAN.

3.3.3. Cost Factor Calculation

Based on the given information about loss of the energy, current energy and other parameters, the optimum cluster head was selected. The dissipation of energy arises because of the data transfer. We calculated total energy loss from the Flower Pollination Algorithm [38].

Total Energy Loss = Energy Lost by All Cluster Members + Energy Lost by Sensor Nodes. These following energies and losses are calculated:

Cluster Member's Energy Loss [39]:

$$E_{c-member(i)} \sum_{j=1}^{N} \{Eamp\ x\ n\ x\ K\ x\ D(i,j)\ x\ E(tx) x\ K\}$$

Eamp x n x K x D (*i*, *j*) (*D* is the distance of node from sink) *x E*(*tx*) are the total number of energies and $E_{c-member(i)}$ is the cluster member's total energy loss.

Energy loss for SN [40]:

$$E_{Loss-SN(i)} = \sum_{j=1}^{N} \{(Etx - E(D - aggregation))Eampx\ n\ x\ K\ x\ D(i, sink)\ x\ E(rx) x\ K\}$$

where $(Etx - E(D - aggregation))$ is the energy used in transmission and $E(rx)$ is the energy used in reception

- Sensor node energy

$$\mathrm{E(Total - curr(i))} = \mathrm{ERes(i)} + \mathrm{EHarvest(i)}$$

- Required Transmission power

$$TP = \frac{SNR}{\propto}$$

where *SNR* is signal to noise ratio.

3.3.4. Performance Evaluation Metrics Compared with Other Protocols

Network Lifetime

Total working time of a network in terms of seconds is called the network lifetime. It is also considered the main evaluation parameter in terms of the wireless network systems in which nodes are involved as a mobile sensor or as a battery-operated device. The best network lifetime is the responsibility of the best wireless sensor network [41].

$$T^{n}{}_{n=} min\ T_v \{v \epsilon V\}$$

T is the total network lifetime, and T_v is the point at which the first node dies.

3.3.5. Period of Stability

It is time for stability covering all the time of a network before the death of its first sensor node. The best stability shows the best performance of a protocol because of the best efficiency of power and energy.

$$T^{n}{}_{n=} T_{1v} \{v \epsilon V\}$$

where T_{1v} is the time taken by the first node to die.

3.3.6. Residual Energy

Residual energy is a long-lasting energy at which the death of a sensor network occurs. Residual energy consumption is measured in joules against time in seconds.

$$p = f(psend)\ x\ \lambda\ x\ pn\ x\ \mu$$

where *p* is residual energy and *psend* is the total energy of the transmission by each node.

3.3.7. Throughput

Useful data sent to the sink from sensor nodes in a specific time is called its (network's) throughput. Starting rounds in every protocol are sharp. Later, the processing becomes minimized, as the information is reused again and again.

$$S = \sum_{k=0}^{\infty} S(k) \cdot g(k)$$

S is throughput, where $S(k)$ is the total amount of nodes and $g(k)$ is the total data sent from the nodes.

3.3.8. End to End Delay

The time a node takes for data transfer to the target node is called an end-to-end latency. In the end, a high value of the end-to-end hindrance refers to the optimal cluster heads selection.

Total delay = No. of hops (1st packet total delay) + (Transmission delay + Processing delay + Queuing delay).

4. Model Design and Implementation

4.1. System Model

In this work, we assume that all cars in an urban environment are evenly dispersed throughout a two-dimensional region. There is no difference between the cars when it comes to the transmission radius (r). Vehicle v is a neighboring vehicle of node u only if the distance between them is lower or equal to r vehicles. All the cars go at the same pace. As illustrated in Figure 3, the source and destination are considered within two hops with three lanes. Each car is anticipated to identify the attacker within a two-hop automobile radius, lowering the possibility that a quick attacker will be capable of fleeing before being captured. All of the cars are controlled by a single algorithm that participates in the communication process. Human intervention in driving is minimal, if not non-existent, according to this theory. In addition, we suppose that there are two sorts of vehicles present: Black Holes and cooperative vehicles. During the route discovery phase and data packet forwarding procedure, cooperative vehicles follow the routing protocol's instructions.

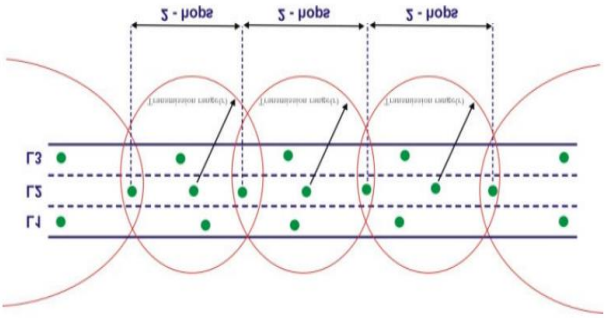

Figure 3. System scenario.

4.1.1. Vehicle Behavior's Stochastic Properties

For a specific value of $W(t)$, for all $a > t$, the value of $W(a)$ is independent of the values of $W(b)$ for all $b > t$, and the random process is called a Markov process [41]. This indicates that the process's future results are not determined by previous values, but rather by current values, where Wn is the current state of a stochastic or random process at time $tn + 1$, and the future state $Wn + 1$ at time $tn + 1$ is dependent only on the present state Wn and not on the previous states $Wn1, Wn2, \ldots, W0$. A Markov chain is a succession of states consisting of the values Wn.

4.1.2. Probabilistic Modeling

If a vehicle V has at least one Black Hole neighbor and n neighbors, it is isolated from the network. If $V(IS)$ represents this, perhaps the vehicle will be in an isolated state; the vehicle probability of being in an isolated state is obtained by assuming that the vehicle has neighbors is stated below [32]:

$$Pr\ V(IS)|D\ (v) = d = Pr(VB \geq 1) = 1 - (1 - PB)$$

4.2. Proposed Technique

In this work, we present an Optimized Enhanced ad hoc On-demand Distance Vector (OEAODV) protocol for the detection of Gray and Black Hole attacks. Two of the parameters in our suggested solution OEAODV are the sequence number and the hop count, which are both included in the four major parameters. These two aspects are used by the Black Hole and Gray Hole to compromise the network's integrity and availability. The remaining three metrics in the table are network performance outputs that have deteriorated as a consequence of the first two (parameters) being attacked. Therefore, we are able to figure out the assault according to Algorithm 1 more efficiently than earlier research by combining these four features and determining the criteria for future Black Hole operations in advance. The architecture of the proposed system and flow diagram of OEAODV are presented in Figures 4 and 5, respectively.

Algorithm 1 Optimized enhanced ad hoc on-demand distance vector protocol

Input: Insecure data communication with Black Hole and Gray Hole attacks
Output: Secure data communication with Black Hole and Gray Hole attacks

```
Start
SN floods RREQ with Fake IP
If (IN reply back to Fake IP) OR (Seq > Th1) (GrayListing)
    SPN Affirmation
    Initialization of normal AODV route discovery
    Data packets Routing
    If (PDR < Th2 and E2E delay > Th3 and overhead(OH) > Th4) or (Blacklisting)
        MN Affirmation
        Blacklisting MN
        Addition of extra field in RREQ to encapsulate ID of MN for alarm
    else
        AODV ();
    end if
else
    start ();
end if
End
```

Keywords: SN, Source Node; IN, Intermediate Node; SPN, Suspicious Node; MN, Malicious Node; Seq, Destination Sequence Number; Th 1, Threshold for Seq; Th 2, Threshold for PDR; Th 3, Threshold for E2E; Th 4, Threshold for OH.

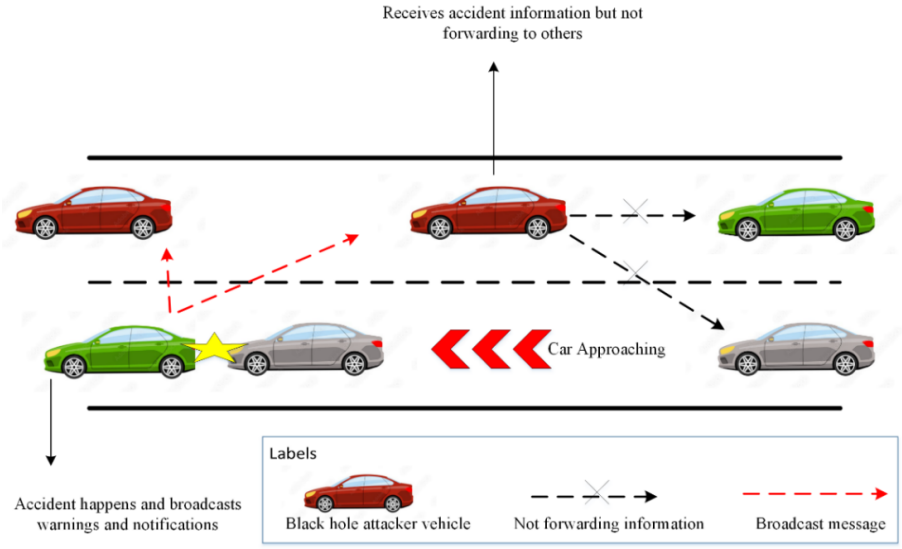

Figure 4. Proposed architecture.

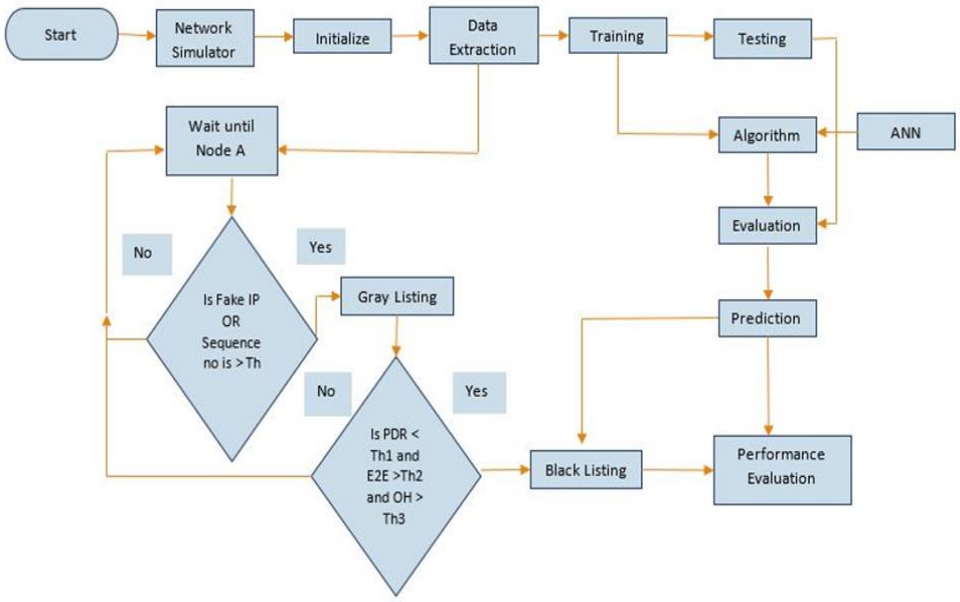

Figure 5. Proposed model.

5. Results and Discussion

Simulations of our suggested approach are carried out with the help of the NS2 (v2.34) running on a system with Ubuntu 20.04 with Intel core i7 having 16 GB of RAM. AODV algorithms such as B-AODV, Ids-AODV, and EAODV were compared to our method. EAODV has been made accessible for MANETs. Furthermore, in [26], the researchers additionally stated that these concepts could be useful to the enormous majority of ad hoc networks, which they believe to be accurate. Their reasoning, as stated in the preceding paragraph, have been taken advantage of, and the findings have been compared to [26]. EAODV would have failed if the attacker had scanned a network, but that was not the case, if OEAODV (our technique) had been evaluated in the same situation.

5.1. Packet Delivery Ratio (PDR)

The PDR is the percentage of actual data packets received to total data packets sent. Figure 6 shows how the PDR changes as the number of nodes increases, with the greatest value occurring when there are 60 nodes. The OEAODV method, however, provides a

higher PDR rate for each node check than EAODV as well as other techniques. Variations in PDR values are the result of changes in the network environment. Pre-defined criteria were employed in our method in order to determine whether or not a path to the destination was free of attack activity for the packets that were to be sent to the destination when compared to other methods.

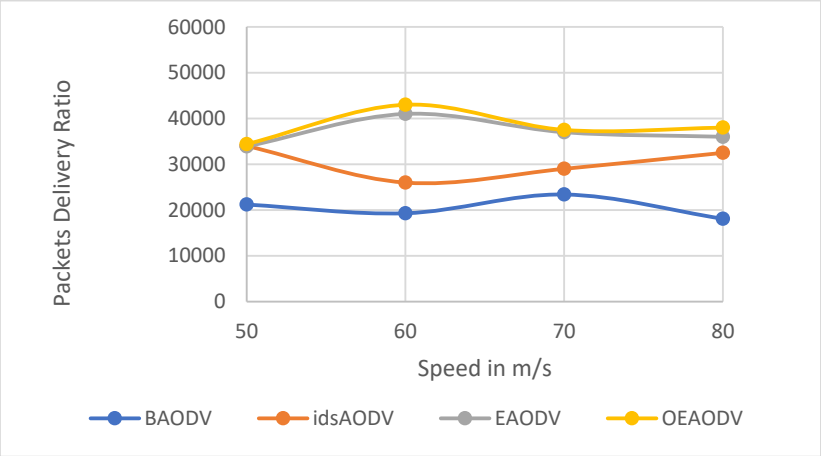

Figure 6. Number of packets sent by nodes from each technique.

5.2. Routing Overhead (ROH)

The number of packets to process and route across a network connection is referred to as the ROH. Figures 7 and 8 demonstrate E2E delay and throughput yield optimal outcomes in situations when PDR was greater in Figure 6, and it is thus particularly assessed in these figures. This means that, when compared to the EAODV technique as well as other techniques, the largest number of packets is delivered to the destination with the least amount of latency. Overhead in the proposed model OEAODV is less than the other, which means that detection of Black Holes and Gray Holes is much better, as mean processing of malicious packets is reduced, and as a result, routing overhead is reduced in our technique as matched to our competitor. We have checked it on various speeds and performances of OEAODV (our technique) as starting on 50 m/s was approximately the ssame as for EAODV, but as we cannot make a decision on a single speed in the vehicular network, especially where nodes are moving, we have verified it on different speeds as we moved from 50 to 60 m/s. On other speeds as well, we can see that our technique is outperforming.

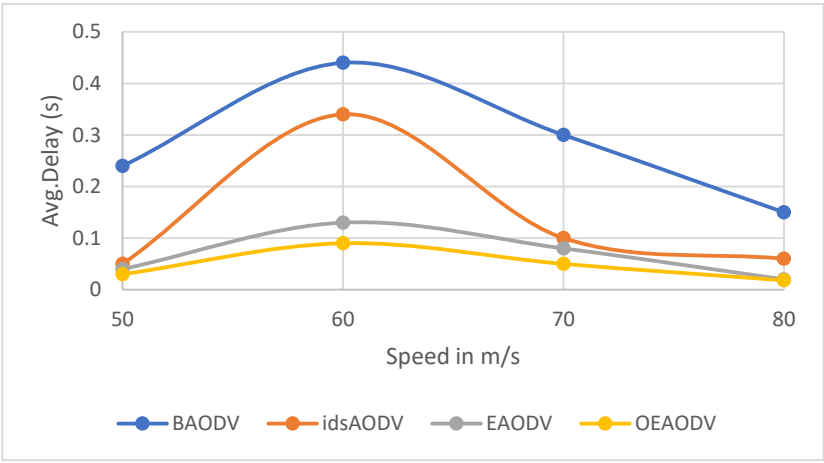

Figure 7. End-to-end delay for packet sending from nodes of each technique.

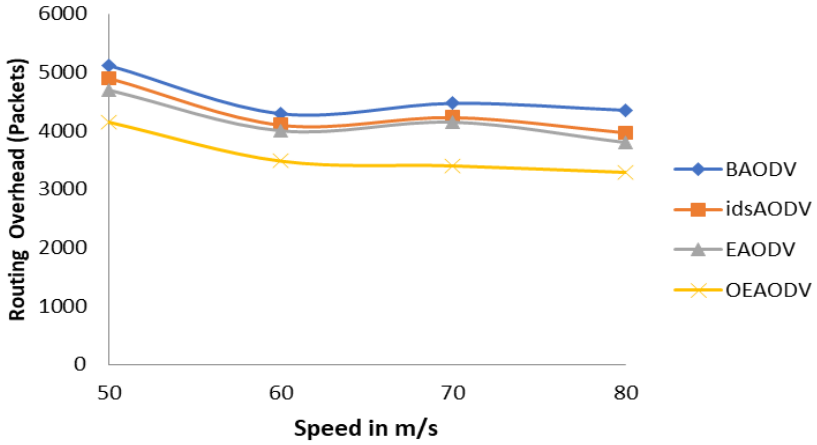

Figure 8. Routing overhead in the kilobit stream from nodes of each technique.

5.3. Throughput

For the amount of data packets transmitted from one source to another, assessing speed throughput is one of the most important parameters utilized, and it is considered one of the most significant factors in determining network performance. Here, we can see that the amount of data packets transmitted in our technique (OEAODV) is very fast. Overall performance of OEAODV at different speeds is outperforming as compared with previous techniques, which is compared at random speeds from 50 to 80 m/s, and the results of different speeds show that OEAODV is outperforming. Figure 9 shows that the higher the throughput, the lower the rate of packets lost.

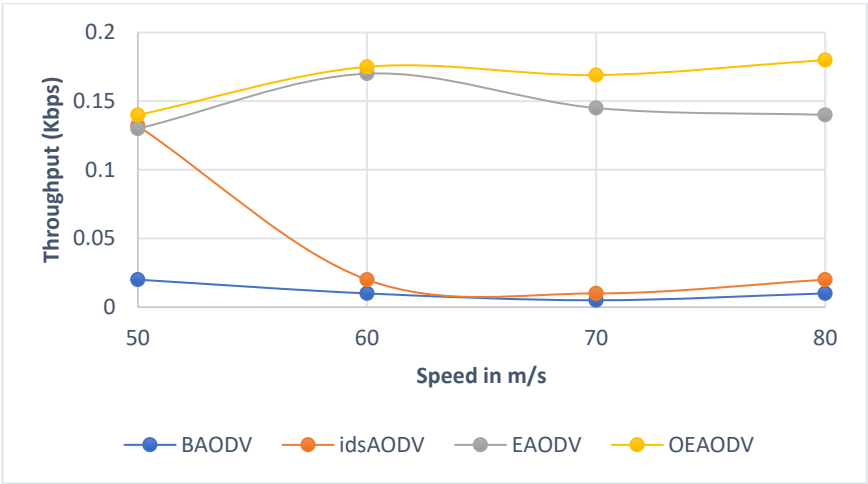

Figure 9. Throughput of nodes from each technique.

5.4. Packet Loss Rate (PLR)

The difference between data packets that are broadcast and received is used to calculate PLR. The number of packets lost is seen in Figure 10. Because there were four rogue nodes in BAODV that did not have a detection mechanism, the number of lost packets reached 89 percent. When under assault, OEAODV (our technique) had a lower packet loss rate than BAODV as well as the two intrusion detection methods, idsAODV and EAODV, and this was in comparison to the industry standard BAODV. This may also be determined by looking at Figure 8, which shows that the higher the PDR, the lower the rate of packets lost. When compared to other methods, Figure 10 shows that OEAODV requires a smaller number of packets that must be routed in order for network communication to take place, and as a result, it has a lower processing overhead.

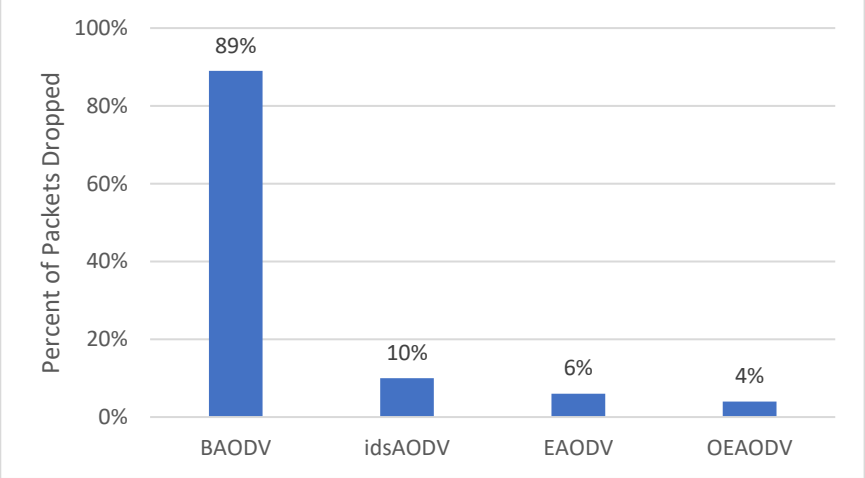

Figure 10. Packet loss ratio in each technique.

5.5. Packets Generated

For each scenario with varying numbers of nodes, a variety of packets are generated over the span of the simulations. The number of packets created is directly proportional to the number of mobile nodes, as can be demonstrated in Figure 11.

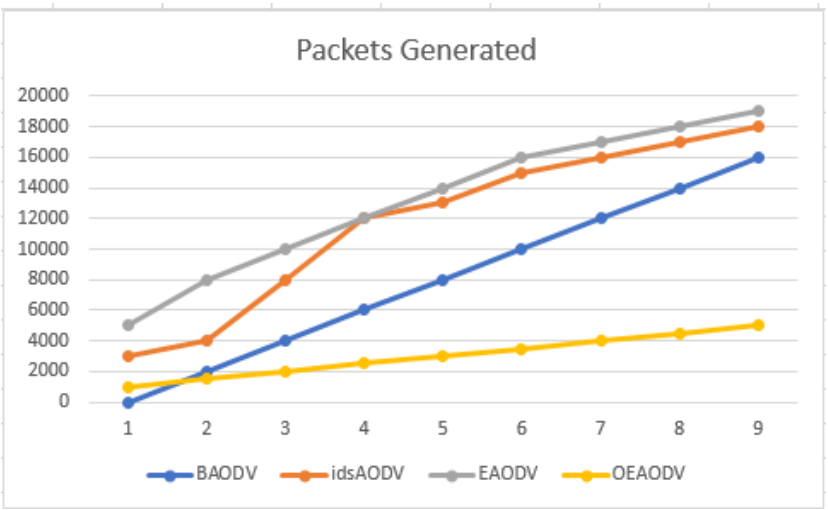

Figure 11. Generated packets.

5.6. Packets Dropped

Packets dropped is the overall number of packets that have been dropped because of factors such as time limitation, collisions, and queue congestion. When a Black Hole node is present in the network, the packet drop is quite high because the Black and Gray Hole nodes swallow the packets. Figure 12 shows the total number of packets dropped. However, as Black Hole and Gray Hole detection is getting better with OEAODV (our approach), the packet drop rate in our proposed technique is much less as compared to previous techniques, as shown in Figure 11.

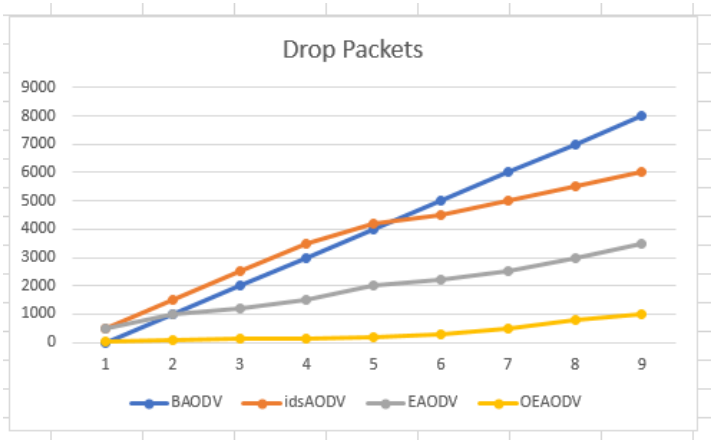

Figure 12. Packet loss.

5.7. Energy Consumption

Energy Consumption is the total amount of energy consumed by a network node. It reduces with a Black Hole and Gray Hole attack because packets sent between the source and destination are discarded, leading to reduced transmission between nodes. Figure 12 compares the energy consumed by the BAODV, idsAODV, EAODV and OEAODV schemes as node speed increases. The goal of this experiment is to compare the overhead imposed in the OEAODV system owing to processing and communication costs to the EAODV and other schemes, which ultimately consume more energy. Packet transmitting and receiving utilize the majority of the node's energy. Our OEAODV system does not increase the quantity of messages exchanged; instead, it makes use of existing routing packets (which are currently required by routing protocol requirements) to share data such as queue and path status. The only additional energy needed by our OEAODV system is for the computation of unique information, such as MAC layer details, queue data, and link shift rates, which are minimal [21]. As could be observed in the diagrammatic representation, the energy expended in both the EAODV and BAODV and other schemes is high, implying that our solution considerably increases network security while consuming very little energy. Figure 13 shows the total energy consumption.

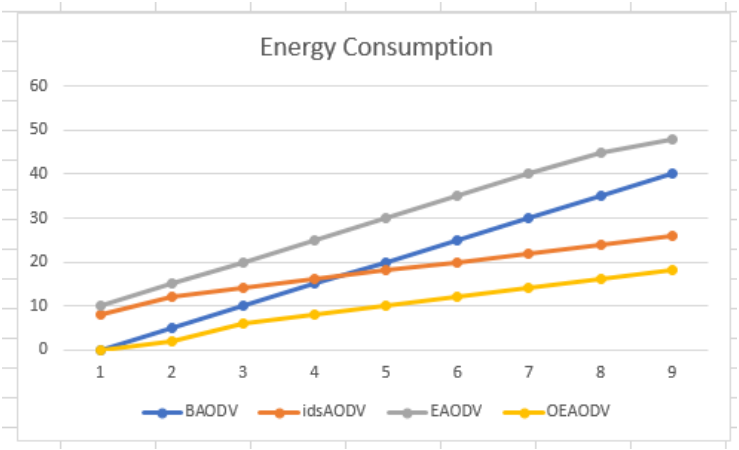

Figure 13. Energy consumption.

6. Conclusions and Future Work

The discovery of Black Hole and Gray Hole assaults has become an increasingly critical problem, as the level of automobile automation continues to develop at an exponential rate. Whenever it concerns ACVs, where such a single packet data latency might lead to an

accident, Black Holes and Gray Holes have a direct impact on communication, which is undesirable in order to ensure safety. As a result, it is critical to discourage future assaults of this nature. As part of our efforts to ensure secure autonomous vehicular applications, which include vehicle and passenger comfort, safety, and transportation, we designed and simulated our approach, which outperformed previous solutions in terms of PDR, PLR, ROH, E2E, as well as throughput. As a result, this strategy could be applied in real-world settings to reduce the number of accidents that occur. Smart clustering techniques can be used in conjunction with the suggested methodology to help prevent Black Hole and Gray Hole attacks from occurring. Many prior interactions show that threat detection mechanisms such as encryption and identity verification, which are commonly regarded as the first line of protection, are insufficient on their own. As systems become more complex, so do their flaws. As a result, intrusion detection is the second line of protection. When an intrusion is discovered, prompt action can reduce or even prevent infrastructure failure. We devised a mechanism for identifying and handling collective Black Hole and Gray Hole assaults in this research. The suggested method can detect malicious nodes and remove them with very little cost or overhead. We attempted to provide a unique way for mitigating Black Hole and Gray Hole attacks in ad hoc networks with our algorithm. The proposed solution has a low end-to-end delay, according to simulation findings and due to the algorithm's quick route identification. Furthermore, because the suggested approach is adaptive, the overhead is minimized by adding an alarm field when it learns that the network is free of any Black Hole and Gray Hole attacks. As a result, the AODV protocol will continue to serve its primary purpose in the network. Because of its ease of implementation and low overhead, the bulk of ad hoc networks employ this technique. The suggested technique was able to outperform the previous method by 4%. Because of the proposed method's capabilities and the fact that it does not require any specific criteria to be used, it can be improved by making a few changes. In this work, we did not consider the real-time environmental factors, such as node mobility. Similarly, different ANN models can be explored to improve the performance of proposed techniques along with various augmentation techniques. Moreover, the findings of this work can be implemented in other sensor and ad hoc networks such as Mobile ad hoc Wireless Networks (MANETs) and other application areas of IoT.

Author Contributions: Conceptualization, F.R. and A.A.; methodology, S.Y., T.M. and S.M.; software, S.Y.; validation, S.M. and A.G.; formal analysis, A.A.; investigation, S.Y.; resources, A.G.; data curation, S.Y.; writing—original draft preparation, S.Y.; writing—review and editing, F.R., T.M. and A.G.; visualization, S.Y.; supervision, F.R.; project administration, T.M. and A.G.; funding acquisition, A.A. and A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: There is no specific dataset used in this work that needs to be published.

Acknowledgments: The paper is financially supported by University Malaysia Sabah.

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. Dhyani, I.; Goel, N.; Sharma, G.; Mallick, B. A reliable tactic for detecting black hole attack in vehicular ad hoc networks. In *Advances in Computer and Computational Sciences*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 333–343.
2. MacCartney, G.R.; Rappaport, T.S.; Samimi, M.K.; Sun, S. Millimeter-wave omnidirectional path loss data for small cell 5G channel modeling. *IEEE Access* **2015**, *3*, 1573–1580. [CrossRef]
3. Ali Zardari, Z.; He, J.; Zhu, N.; Mohammadani, K.H.; Pathan, M.S.; Hussain, M.I.; Memon, M.Q. A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. *Future Internet* **2019**, *11*, 61. [CrossRef]
4. Ali Alheeti, K.M.; Gruebler, A.; McDonald-Maier, K. Intelligent intrusion detection of gray hole and rushing attacks in self-driving vehicular networks. *Computers* **2016**, *5*, 16. [CrossRef]
5. Irwin, R. *Violence against Health Workers in Complex Security Environments*; SIPRI: Stockholm, Sweden, 2014.

6. Acquisti, A.; Carrara, E.; Stutzman, F.; Callas, J.; Schimmer, K.; Nadjm, M.; Gorge, M.; Ellison, N.; King, P.; Gross, R. *Security Issues and Recommendations for Online Social Networks*; ENISA Position Paper No. 1; ENISA—European Network and Information Security Agency: Heraklion, Greece, 2007; Volume 43.
7. Huang, K.; Zhou, C.; Tian, Y.-C.; Tu, W.; Peng, Y. Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; IEEE: New York, NY, USA, 2017.
8. Kannan, R.; Ray, L.; Durresi, A.; Iyengar, S. Security-performance tradeoffs of inheritance based key predistribution for wireless sensor networks. *arXiv* **2004**. [CrossRef]
9. Elsaeidy, A.; Elgendi, I.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. A smart city cyber security platform for narrowband networks. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; IEEE: New York, NY, USA, 2017.
10. Reddy, G. A Delay Sensitive Multi-Path Selection to Prevent the Rushing Attack in VANET. In Proceedings of the 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23 October 2021; IEEE: New York, NY, USA, 2021.
11. Sayan, C.; Hariri, S.; Ball, G. Cyber security assistant: Design overview. In Proceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W), Tucson, AZ, USA, 18–22 September 2017; IEEE: New York, NY, USA, 2017.
12. Nair, R.; Ragab, M.; Mujallid, O.A.; Mohammad, K.A.; Mansour, R.F.; Viju, G.K. Impact of wireless sensor data mining with hybrid deep learning for human activity recognition. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9457536. [CrossRef]
13. Tagarev, T. Digilience—A Platform for Digital Transformation, Cyber Security and Resilience. *Inf. Secur.* **2019**, *43*, 7–10. [CrossRef]
14. Hamdi, M.M.; Audah, L.; Abood, M.S.; Rashid, S.A.; Mustafa, A.S.; Mahdi, H.; Al-Hiti, A.S. A review on various security attacks in vehicular ad hoc networks. *Bull. Electr. Eng. Inform.* **2021**, *10*, 2627–2635. [CrossRef]
15. Singhal, P.; Raul, N. Malware detection module using machine learning algorithms to assist in centralized security in enterprise networks. *arXiv* **2012**, arXiv:1205.3062. [CrossRef]
16. Ali, S.; Islam, N.; Rauf, A.; Din, I.U.; Guizani, M.; Rodrigues, J.J.P.C. Privacy and security issues in online social networks. *Future Internet* **2018**, *10*, 114. [CrossRef]
17. Ślezak, D.; Chadzyńska-Krasowska, A.; Holland, J.; Synak, P.; Glick, R.; Perkowski, M. Scalable cyber-security analytics with a new summary-based approximate query engine. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; IEEE: New York, NY, USA, 2017.
18. Andrade, R.O.; Yoo, S.G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *J. Inf. Secur. Appl.* **2019**, *48*, 102352. [CrossRef]
19. Moustafa, A.A.; Bello, A.; Maurushat, A. The role of user behaviour in improving cyber security management. *Front. Psychol.* **2021**, 1969. [CrossRef]
20. Stacey, T.R.; Helsley, R.E.; Baston, J.V. Identifying information security threats. *Inf. Syst. Secur.* **1996**, *5*, 50–59.
21. Nieles, M.; Dempsey, K.; Pillitteri, V. *NIST Special Publication 800-12 Revision 1: An Introduction to Information Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.
22. Zafar, F.; Khattak, H.A.; Aloqaily, M.; Hussain, R. Carpooling in Connected and Autonomous Vehicles: Current Solutions and Future Directions. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 218. [CrossRef]
23. Safaa, O.; Firas, S. On the Designing of two grains levels network intrusion detection system. *Karbala Int. J. Mod. Sci.* **2015**, *1*, 15–25.
24. Singh, R.; Kumar, H.; Singla, R. An intrusion detection system using network traffic profiling and online sequential extreme learning machine. *Expert Syst. Appl.* **2015**, *42*, 86. [CrossRef]
25. Rajasekharaiah, K.; Dule, C.S.; Sudarshan, E. Cyber Security Challenges and its Emerging Trends on Latest Technologies. In Proceedings of the International Conference on Recent Advancements in Engineering and Management (ICRAEM-2020), Warangal, India, 9–10 October 2020.
26. Papamartzivanos, D.; Mármol, F.G.; Kambourakis, G. Dendron: Genetic trees driven rule induction for network intrusion detection systems. *Future Gener. Comput. Syst.* **2018**, *79*, 558–574. [CrossRef]
27. Sornsuwit, P.; Jaiyen, S. A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting. *Appl. Artif. Intell.* **2019**, *33*, 462–482. [CrossRef]
28. Louvieris, P.; Clewley, N.; Liu, X. Effects-based feature identification for network intrusion detection. *Neurocomputing* **2013**, *121*, 265–273. [CrossRef]
29. Harb, H.M.; Desuky, A.S. Adaboost ensemble with genetic algorithm post optimization for intrusion detection. *Int. J. Comput. Sci. Issues IJCSI* **2011**, *8*, 28.
30. Kabir, E.; Hu, J.; Wang, H.; Zhuo, G. A novel statistical technique for intrusion detection systems. *Future Gener. Comput. Syst.* **2018**, *79*, 303–318. [CrossRef]
31. Salih, A.A.; Adnan Mohsin, A. Evaluation of classification algorithms for intrusion detection system: A review. *J. Soft Comput. Data Min.* **2021**, *2*, 31–40. [CrossRef]
32. Liu, X. An optimal-distance-based transmission strategy for lifetime maximization of wireless sensor networks. *IEEE Sens. J.* **2014**, *15*, 3484–3491. [CrossRef]

33. Chou, D.; Jiang, M. A survey on data-driven network intrusion detection. *ACM Comput. Surv. CSUR* **2021**, *54*, 182. [CrossRef]
34. Sajjad, S.M.; Mufti, M.R.; Yousaf, M.; Aslam, W.; Alshahrani, R.; Nemri, N.; Afzal, H.; Khan, M.A.; Chen, C.M. Detection and Blockchain-Based Collaborative Mitigation of Internet of Things Botnets. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1194899. [CrossRef]
35. Abdullah, A.M.; Ullah, I.; Khan, M.A.; Alsharif, M.H.; Mostafa, S.M.; Wu, J.M.T. An Efficient Multidocument Blind Signcryption Scheme for Smart Grid-Enabled Industrial Internet of Things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 7779152. [CrossRef]
36. Adeel, A.; Ali, M.; Khan, A.N.; Khalid, T.; Rehman, F.; Jararweh, Y.; Shuja, J. A multi-attack resilient lightweight IoT authentication scheme. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3676. [CrossRef]
37. Khurshid, A.; Khan, A.N.; Khan, F.G.; Ali, M.; Shuja, J.; Khan, A.U.R. Secure-CamFlow: A device-oriented security model to assist information flow control systems in cloud environments for IoTs. *Concurr. Comput. Pract. Exp.* **2019**, *31*, e4729. [CrossRef]
38. Palma, A.; Pereira, P.R.; Pereira, P.R.; Casaca, A. Multicast routing protocol for Vehicular Delay-Tolerant Networks. In Proceedings of the 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 8–10 October 2012; pp. 753–760. [CrossRef]
39. Trivedi, I.N.; Jangir, P.; Parmar, S.A.; Jangir, N. Optimal power flow with voltage stability improvement and loss reduction in power system using Moth-Flame Optimizer. *Neural Comput. Appl.* **2018**, *30*, 1889–1904. [CrossRef]
40. Aadil, F.; Raza, A.; Khan, M.F.; Maqsood, M.; Mehmood, I.; Rho, S. Energy aware cluster-based routing in flying ad-hoc networks. *Sensors* **2018**, *18*, 1413. [CrossRef]
41. Panda, D.K.; Ranjan Kumar, D. Reliability evaluation and analysis of mobile ad hoc networks. *Int. J. Electr. Comput. Eng.* **2017**, *7*, 479. [CrossRef]