


## Article

# An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs

Abdul Malik <sup>1</sup>, Muhammad Zahid Khan <sup>1</sup>, Mohammad Faisal <sup>1</sup>, Faheem Khan <sup>2,\*</sup> and Jung-Taek Seo <sup>2,\*</sup>

<sup>1</sup> Network System & Security Research Group, Department of Computer Science & IT, University of Malakand, Chakdara 18800, Pakistan; qariabdulmalik@uom.edu.pk (A.M.); mzahidkhan@uom.edu.pk (M.Z.K.); mfaisal@uom.edu.pk (M.F.)

<sup>2</sup> Department of Computer Engineering, Gachon University, Seongnam 13120, Korea

\* Correspondence: faheem@gachon.ac.kr (F.K.); seojt@gachon.ac.kr (J.-T.S.)

**Abstract:** Rapid and tremendous advances in wireless technology, miniaturization, and Internet of things (IoT) technology have brought significant development to vehicular ad hoc networks (VANETs). VANETs and IoT together play a vital role in the current intelligent transport system (ITS). However, a VANET is highly vulnerable to various security attacks due to its highly dynamic, decentralized, open-access medium, and protocol-design-related concerns. Regarding security concerns, a black hole attack (BHA) is one such threat in which the control or data packets are dropped by the malicious vehicle, converting a safe path/link into a compromised one. Dropping data packets has a severe impact on a VANET's performance and security and may cause road fatalities, accidents, and traffic jams. In this study, a novel solution called detection and prevention of a BHA (DPBHA) is proposed to secure and improve the overall security and performance of the VANETs by detecting BHA at an early stage of the route discovery process. The proposed solution is based on calculating a dynamic threshold value and generating a forged route request (RREQ) packet. The solution is implemented and evaluated in the NS-2 simulator and its performance and efficacy are compared with the benchmark schemes. The results showed that the proposed DPBHA outperformed the benchmark schemes in terms of increasing the packet delivery ratio (PDR) by 3.0%, increasing throughput by 6.15%, reducing the routing overhead by 3.69%, decreasing the end-to-end delay by 6.13%, and achieving a maximum detection rate of 94.66%.

**Keywords:** AODV; BHA; IoT; network security; VANET



**Citation:** Malik, A.; Khan, M.Z.; Faisal, M.; Khan, F.; Seo, J.-T. An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs. *Sensors* **2022**, *22*, 1897. <https://doi.org/10.3390/s22051897>

Academic Editor: Rebeca P. Díaz Redondo

Received: 19 November 2021

Accepted: 23 February 2022

Published: 28 February 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



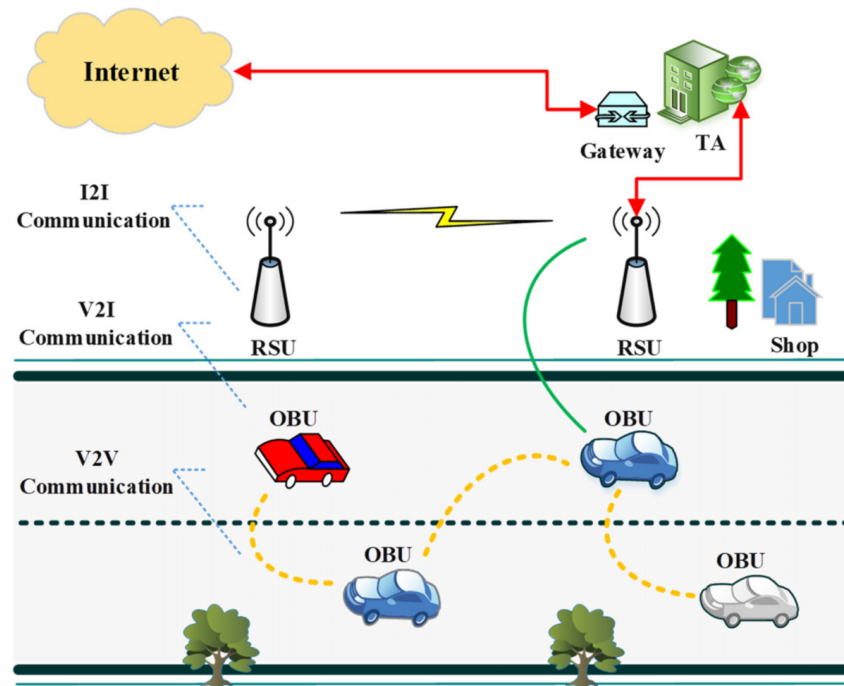
**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

A vehicular ad hoc network (VANET) is a special type of mobile ad hoc network (MANET) in which vehicles and roadside units (RSUs) are linked to create a safer and more efficient driving environment [1]. A typical VANET architecture consists of three primary components, namely, onboard units (OBUs), roadside units (RSUs), and trusted authority (TA) [1–3]. Every vehicle has an OBU that collects, analyses, and transmits information to other vehicles in the vicinity. An RSU is installed along the roadside that is used to communicate with vehicles, infrastructure, and a TA. In essence, a TA is a registration unit that manages the VANET system by registering the OBUs, RSUs, and vehicle users. A VANET is the backbone of the intelligent transportation system (ITS) and it plays a crucial role in supplying real-time and sensitive information to the drivers and traffic authorities [4,5]. Another key component of an ITS is the IoT [6], which transforms conventional VANETs into the Internet of vehicles (IoV), enabling data collection and sharing data about infrastructures, vehicles, humans, and road conditions [7–9].

The primary distinction between a MANET and a VANET is their MAC addressing, as a MANET operates on IEEE 802.11m and a VANET operates on IEEE 802.11p technology [10]. In a MANET, the movement of nodes is random, while in a VANET, some nodes are fixed (RSUs) and others (vehicles) travel at high speed along the roadside. A

VANET's nodes have unlimited energy and processing power, whereas a MANET lacks these features [11]. Within a VANET, communications are divided into three distinct categories: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-infrastructure (I2I) communications [12,13]. V2V communication is purely on an ad hoc basis, which allows for the exchange of information between vehicles over a short range. V2I communication provides information to vehicles and static infrastructures. Meanwhile, I2I communication provides additional traffic information over 3G/4G channels, which is important for driver assistance and vehicle tracking. The generic architecture of a VANET is shown in Figure 1.



**Figure 1.** Generic architecture of a VANET.

The high mobility of vehicles, high dynamic network topology, non-centralized control, large scale network, time-critical communications, and open access to both legitimate and illegitimate users are some of the distinguishing characteristics of VANETs [14–17]. In VANETs, data communication and routing are constantly vulnerable to many security attacks due to these characteristics and constraints. As a result, one of the primary considerations in VANET applications is to secure communications. However, in VANETs, data transmission between two nodes requires the assistance of intermediate nodes to transfer the data because the destination node is not often lying in the transmission range of the source, hence routing protocols are used to establish the best route between nodes. Over time, various routing protocols and security mechanisms have been developed [18]. Out of these, the ad hoc on-demand distance vector (AODV) [19] was found to be one of the most famous and commonly used routing protocols in VANETs [20,21]. AODV is also known as a demand-driven protocol since it discovers a new route only when it is required, rather than in advance. AODV provides a fast, dynamic network connection with little processing overhead and memory requirements, making it an ideal choice for a highly dynamic VANET [22,23]. However, there are several significant security vulnerabilities and challenges with the AODV protocol that must be addressed. For instance, the source node is always unaware of the intended destination. Such features of AODV make VANETs more vulnerable to various security attacks, such as a wormhole attack, black hole attack (BHA), and gray hole attack (GHA) [2,16,24,25].

Secure and efficient communications in VANETs are very essential because the vehicles are moving quickly, and the information is often safety related and time sensitive. Ensuring the security of the messages generated by the vehicles is very crucial, as the nodes in VANETs exchange them in the open wireless medium. Due to the presence of the aforementioned attacks, the applications and services of VANETs are compromised. One such kind of attack is a BHA in which a malicious node completely drops the packets instead of forwarding them onto its final destination. These packets may contain important emergency messages and warning alerts. A BHA drops such packets, which results in degradation of the overall network security, performance, and disruption in the network information-sharing process. Road accidents are a significant cause of deaths and physical disabilities. Hence, dropping all such packets in a highly dynamic VANET could result in road fatalities, accidents, traffic jams, and congestions. Motivated by this, in this study, we proposed a novel and efficient solution for the detection and prevention of a well-known security attack BHA in the AODV routing protocol to improve the overall security and performance of VANETs. The solution was based on calculating a dynamic threshold value from sequence numbers of RREPs and generating a forged RREQ packet. In a nutshell, the proposed solution increased the PDR and network throughput while reducing the routing overhead and end-to-end delay.

The rest of the manuscript is organized as follows: Section 2 provides a brief background of BHAs in VANETs, Section 3 describes the related work, Section 4 explains the proposed work, Section 5 discusses the implementation and evaluation, and Section 6 concludes and gives future direction to the research work.

## 2. Black Hole Attacks (BHAs) in VANETs

The highly dynamic, open-access medium, distributed infrastructure, and protocol designing issues have made VANETs vulnerable to many security attacks, such as a denial of service (DoS) attack, Sybil attack, wormhole attack, flooding attack, impersonation attack, jellyfish attack, GHA, and BHA [2,16,24,25]. Due to the presence of these attacks, the applications and services of VANETs can be compromised.

A BHA is a type of DoS in which a malicious node completely drops packets from the legitimate node. In a BHA, when a malicious node receives an RREQ packet from the source node, it quickly responds with a fake RREP without checking its routing table. This RREP packet contains a higher sequence number and minimum hop count value, which is considered to be the freshest and shortest route in AODV [26,27]. Once the source node receives the fake RREP packet, it deceptively considers it an optimized path and starts transferring data packets toward the black hole node. A BHA drops such packets instead of forwarding them to their final destination, which results in degradation of the overall network security and performance, as well as disruption in the network information-sharing process. These packets may contain critical information messages, such as emergency notifications and warning alerts, which must be delivered quickly and within a specific time frame. Dropping such packets in a highly dynamic VANET could result in road fatalities, accidents, traffic jams, and congestion. Our research focus in this study was to address the BHA issue in VANETs and propose a new, more efficient solution. Because a BHA is one of the most serious attacks in VANETs, it serves as the foundation for DoS attacks in which the network service is unavailable to the intended users.

In the above Figure 2, a BHA in the AODV protocol is explained with the help of an example scenario. For instance, source vehicle  $vs.$  wants to communicate with destination vehicle  $V_D$ .  $vs.$  broadcasts an RREQ packet to all its neighboring vehicles, i.e.,  $V_1$ ,  $V_2$ , and  $V_3$ . Upon receiving the RREQ,  $V_1$  quickly responds with a fake RREP containing a spoof higher destination sequence number (DSN) value (4484). Meanwhile, vehicles  $V_2$  and  $V_3$  increase their hop count values by one in the RREQ packet and broadcast it further to their next-hop vehicles. In the meantime,  $vs.$  receives the first RREP from  $V_1$ . Therefore, source vehicle  $vs.$  selects a route to destination  $V_D$  that goes through  $V_1$  (i.e., black hole attacker) and starts transferring data packets. Upon receiving the packets,  $V_1$  drops all these packets

rather than forwarding them to  $V_D$ . The RREP(s) that arrives later is discarded by the source vehicle  $V_S$ .

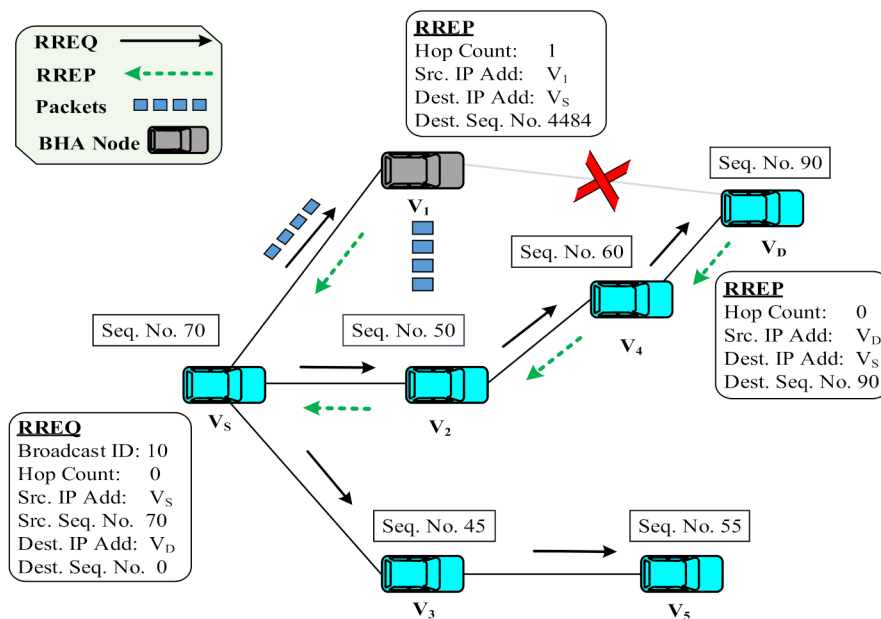


Figure 2. Black hole attack.

Figure 3 shows a visual representation of the impact of BHA on VANET. In this figure, a collision occurs between two vehicles and a warning alert is sent by vehicle  $V_3$  to vehicle  $V_4$  (BHA vehicle).  $V_4$  drops the warning alert instead of forwarding it to the approaching vehicles, i.e.,  $V_5$  and  $V_6$ . As a result, it could lead to more accidents, hazards, and traffic jams.

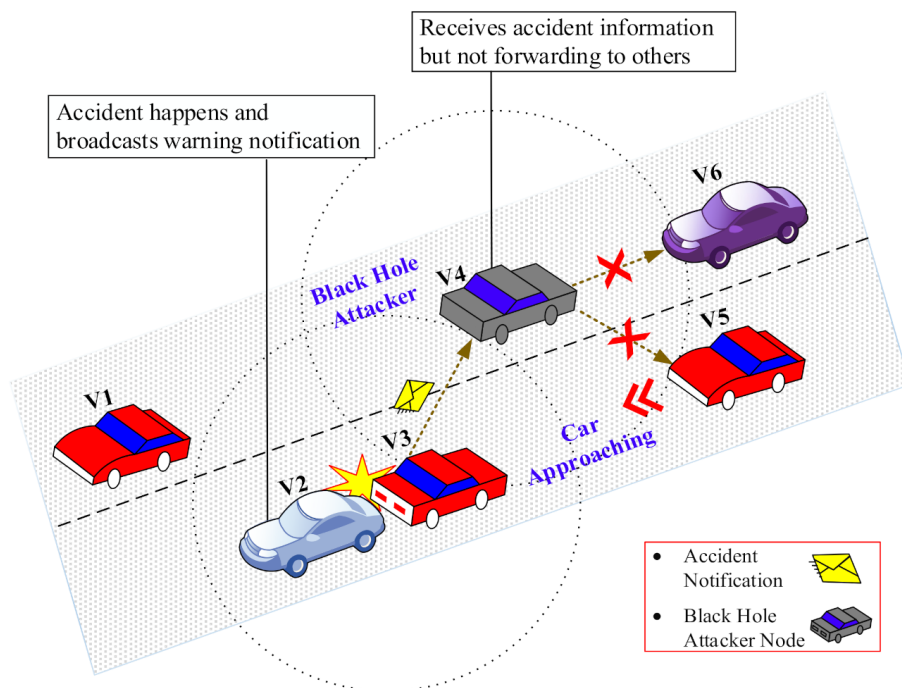


Figure 3. A visual representation of the impact of a BHA on VANET.

### 3. Related Work

Concerning the mitigation of BHA and eradication of malicious nodes in VANETs, over time, many solutions were proposed and reported in the relevant literature. One such notable related work was proposed by Hortelano et al. [28], which was a watchdog-based intrusion detection system (IDS). In this scheme, when a source node A transmits packets to an intermediate node B, then node A checks whether node B further forwarded the packets or not to the next vehicle by continuously listening to node B's transmission. Every node maintains a table of its neighbors' trust levels. If a malicious node drops the packets repeatedly and exceeds the threshold level, then that node is declared malicious. The scheme has proven to be effective in detecting selfish and malicious vehicles. However, due to the periodic listening of nodes' actions and maintaining an extra buffer for recording other nodes' trust levels, the scheme generates an additional routing overhead and end-to-end delay. Similarly, in [29], Daeinabi et al. proposed an algorithm for the detection and isolation of malicious vehicles in VANET called DMV (detecting malicious vehicle). In this algorithm, vehicles are grouped into clusters led by a cluster head (CH). Whenever a new vehicle enters the cluster, the verifier vehicle starts scanning the entered vehicle's actions. If the entered vehicle continuously drops the packets, then the verifier vehicle reports it to the CH. The CH decreases the reported vehicle's trust value. If the trust value of the reported vehicle reaches a pre-defined threshold, then CH reports it to the certification authority (CA). The CA then enters it into the blacklist and informs all other vehicles through alarms. The simulation results show that the proposed approach is capable of detecting most of the available attacks in VANETs. However, the approach takes longer to process and has an impact on other performance metrics, including throughput, end-to-end delay, and jitter [30].

In [30], Kadam et al. proposed the detection and prevention of malicious vehicles (D&PMV) to address BHAs in VANETs. The authors made some improvements to the DMV algorithm proposed in [29] by adding the cache mechanism for path construction during the route discovery phase. This algorithm first scans all the existing paths for the availability of BHA; if the path with a BHA is found, then it ignores the path and reconstructs a new path. As compared to DMV, this algorithm can detect and prevent BHAs with high mobility and reduce the impact of BHAs inside VANETs. However, this algorithm still requires additional time for its processing, which results in high end-to-end delay [20]. In [31], Dhaka et al. proposed a scheme for the identification and removal of BHAs and GHAs. The authors modified the original AODV routing protocol by adding two additional control packets, i.e., the response sequence (Rseq) and the code sequence (Cseq). In this scheme, a source node broadcasts the Cseq packet to all of its neighboring nodes. Upon receiving the Cseq, each node responds with the Rseq packet. A connection is established toward the destination if both packets' IDs match a specific neighbor. Otherwise, the source node discards the Rseq of the node and informs all other nodes about the malicious node. The scheme provides a higher PDR and is applicable in other reactive routing protocols. However, due to the usage of additional control packets, the technique causes substantial routing overhead in the network.

In [32], Jahan and Suman proposed an acknowledgment-based model to detect BHA in VANETs. In this model, each intermediate node informs the source node through an acknowledgment that it has forwarded the packet to the next-hop node. This process is continued until the destination is reached. This model generates excessive network congestion due to the use of extra acknowledgments provided by each intermediary node, causes substantial routing overhead, affects the PDR, and generates delay. In [33], Li et al. proposed an attack-resistant trust (ART) management scheme based on evaluating the trustworthiness of data and nodes to identify and detect malicious nodes. The scheme is split into two phases: data analysis and trust management. First, the traffic data is collected from vehicles and then analyzed using Dempster–Shafer theory. However, it is possible that some malicious nodes forward packets correctly but later start acting maliciously (i.e., dropping data packets).

In [34], Purohit et al. proposed a secure vehicular on-demand routing (SVODR) scheme to mitigate BHAs in VANETs. A new field called an encrypted random number is inserted into the RREQ packet and broadcast to all its neighboring nodes. Upon receiving the RREP, the source node checks its own routing table's destination sequence number (DSN) and the RREP's DSN and encrypted/decrypted random numbers. A node is genuine if its RREP's DSN is greater than the source vehicle's routing table DSN and both functions' random numbers are equal. Otherwise, the vehicle is declared malicious. A downside of this scheme is that it requires extra fields in the control packets for cryptographic algorithms that need extra resources, resulting in a large routing overhead and end-to-end delay. In [35], Tyagi et al. proposed a three-step BHA detection algorithm called enhanced secure AODV (ES-AODV). In step 1, the RSU plays an additional role as the certificate authority (CA), which manages public and private key pairs. In step 2, the source broadcasts the RREQ packet along with the vehicle's certificate, nonce encryption, and the public key of the destination. In step 3, a BHA is detected based on the threshold value obtained from the sequence number of RREP and verification of the nonce value. The technique is built on public-key cryptography, which protects the network against external attacks, but an internal BHA may create disruption. Second, to detect a BHA, the method requires the presence of RSUs, which may not be applicable in all VANET scenarios.

In [36], Zardari et al. proposed a dual-attack detection of BHA and GHA (DDBG) scheme based on a connected dominating set (CDS) and IDS to detect malicious nodes. In this scheme, the IDS node broadcasts a status packet and starts waiting for its response. On receiving all the replies, the IDS node checks which node has not sent a reply properly and why. If any node does not respond or sends a bogus reply, that node is declared as a malicious node. The key problem with this scheme is that it periodically broadcasts a status packet to detect malicious nodes in the network, which results in a huge routing overhead. In [4], Cherkaoui et al. proposed a novel method to detect BHAs in VANETs based on using a variable control chart. The method is implemented in each receiving vehicle to detect the BHA through the supervision of the throughput and end-to-end delay metrics. Each vehicle calculates the parameters of the chart and transforms the received packets into a graphical representation. A node is declared malicious when the metrics curves oscillate outside of the chart limits. However, deploying the monitoring system on each receiving individual node causes unnecessary processing overload. Second, the techniques are often used in industrial fields to monitor the quality of a particular system; therefore, using a variable control chart in the VANET context is impracticable.

In [20], Hassan et al. proposed an intelligent detection BHA (IDBA) scheme in autonomous and connected vehicles (ACVs). The scheme pre-calculates four threshold values from the four key metrics: sequence number, hop count, PDR, and end-to-end delay (i.e., Th1, Th2, Th3, and Th4, respectively). According to this scheme, when a node receives a new RREP packet, it checks whether the RREP's sequence number is greater than Th1 and the hops count is equal to Th2; if so, it adds such a node into the gray-list. Then, the node checks whether the PDR is greater than Th3 and the end-to-end delay is less than Th4; if so, the gray-listed node is assigned to the black-list. An alarm message is flooded into the network to isolate the BHA node. The scheme is completely based on pre-calculated threshold values generated from old data so that the traffic condition, such as congestion, may be changed from time to time. Thus, threshold values generated in advance may consider a malicious node genuine and vice versa. In addition to that, calculating four key thresholds on each node results in high end-to-end delay and processing overhead. In [10], Kumar et al. proposed a secure AODV (SAODV) with improvements made in the RREQ and RREP control packets. To detect a BHA, first, a message is forwarded to the neighboring nodes to know their status. Second, an encrypted packet is forwarded to all its neighboring nodes to calculate their reputation. Third, the forwarded packets are verified for reputation. Fourth, a secret key is forwarded to the known neighbors. Finally, the RREQ and RREP are verified and start forwarding data packets. The source node appends an encrypted value (sequence number) in the RREQ and broadcasts it to all the

neighboring vehicles. On receiving the RREP, the source node declares a node as malicious if the encrypted value of the routing table and the decrypted value of the RREP are not equal. The approach uses extra fields in the control packets for cryptographic functions, which needs extra resources, resulting in a heavy routing overhead. Second, it contains five different phases to identify and detect BHA, which is quite complex and generates extra processing overhead, resulting in high end-to-end delay.

The details, pros, and cons of each of these schemes are given in Table 1. In VANETs, a BHA is a major security threat in which a malicious node drops all the data packets and does not forward them to other nodes in routing, which leads to degradation of the overall security and performance of the VANET. To stop this attack, many solutions are presented in the literature. From the critical analysis of the related literature shown in Table 1 above, it is evident that the existing schemes have many limitations. For example, most of these schemes [8,20,28–32,34,36] employed some extra DPS/IDS nodes and exchanged additional control packets, which increased the routing overhead and end-to-end delay. The PDR decreases whenever the network is denser, and the higher the end-to-end delay in the network leads to lower average throughput. These limitations cause the consumption of valuable network bandwidth and compromise network performance and security. To address these challenges, we present a novel solution for detecting and preventing a BHA with a small routing overhead and end-to-end delay in this study. Furthermore, the proposed solution improves VANET security and performance by increasing the PDR and throughput while eliminating false positive and false negative rates. The proposed solution used a new approach based on calculating a dynamic threshold value from sequence numbers and generating a forged RREQ packet.

**Table 1.** Summarized literature review.

Author (s) and Citation	Solutions/Schemes	Strengths	Performance Metrics	Limitations
Hortelano et al. [28]	Watchdog-based IDS	Easy to implement and applicable in any routing protocol; detects selfish and greedy nodes efficiently	False positive and false negative	The technique fails when two malicious nodes work together; a high false detection rate in a short time; generates a huge routing overhead and end-to-end (E2E) delay
Daeinabi et al. [29]	Detecting malicious vehicle (DMV)	Detect any kind of malicious node with high promptness	PDR and packets dropped	High jitter and high E2E delay; low throughput
Kadam et al. [30]	Detection and prevention of malicious vehicles (D&PMV)	Provides lower jitter and higher throughput compared to DMV method	Packets dropped, E2E delay, throughput, and jitter	Requires more time for processing; results in high E2E delay
Dhaka et al. [31]	Based on new control packets: Cseq and Rseq	Provides higher PDR and is applicable in other reactive routing protocols	PDR and E2E delay	Huge routing overhead due to use of additional control packets
Jahan and Suman [32]	Acknowledgment-based model	The model is capable of detecting any kind of malicious node	Packets dropped, throughput, packets received, and PDR	Heavy routing overhead and E2E delay; low throughput and PDR
Li et al. [33]	Attack-resistant trust (ART) management scheme based on evaluating trustworthiness	Accurately evaluates the trustworthiness of data and nodes in VANETs; capable of detecting various DoS attacks	Precision, recall, and communication overhead	High processing overhead when the number of malicious nodes increases; cannot detect a smart BHA
Purohit et al. [34]	Secure vehicular on-demand routing (SVODR)	The modified AODV can mitigate the impact of BHAs in VANETs	PDR, throughput, normalized routing load (NRL), E2E delay, and average path length	It cannot be employed with other protocols; using extra fields for cryptographic functions leads to a heavy routing overhead and E2E delay

Table 1. Cont.

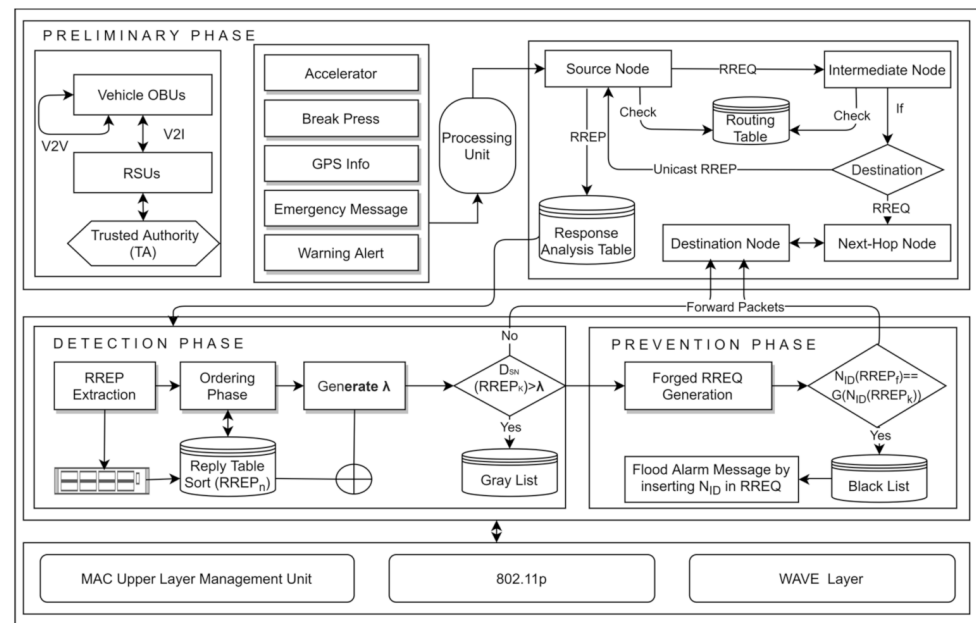
Author (s) and Citation	Solutions/Schemes	Strengths	Performance Metrics	Limitations
Tyagi et al. [35]	Enhanced secure AODV (ES-AODV) based on asymmetric public-key cryptography	The algorithm is simple, fast, and has a lower storage cost	Packets dropped, packet collision, E2E delay, throughput, routing overhead, and PDR	Provides security against external attacks but internal attacks may inflict havoc on the network
Zardari et al. [36]	Dual-attack detection for a BHA and GHA (DDBG)	Provides a fast propagation rate of data and only trustworthy nodes can interact across the network	Detection rate, PDR, throughput, routing overhead, and E2E delay	Generates a huge routing overhead, which affects the throughput and PDR
Cherkaoui et al. [4]	Use of variable control chart to detect BHA	Easy to implement and does not need any modification in the routing protocols	Throughput and E2E delay	High processing overhead and may not apply in the VANET's environment
Hassan et al. [20]	Intelligent detection of a black hole attack (IDBA)	Capable of detecting a BHA and the results revealed better performance compared to benchmark schemes	PDR, throughput E2E delay, packet loss ratio, and routing overhead	Generates four thresholds, which causes a high processing and routing overhead
Kumar et al. [10]	Secure AODV	Capable of detecting malicious nodes in VANETs	PDR, throughput, and E2E delay	High routing overhead and E2E delay, resulting in a decreased throughput and PDR
Proposed DPBHA	Use of dynamic threshold value and forged RREQ packet	Efficiently detects and prevents a BHA in terms of reduced routing overhead and E2E delay, increased throughput, and PDR; eliminates the false positive and false negative rates with 98% accuracy; no additional hardware and IDS/DPS nodes are required	PDR, throughput, E2E delay, packet loss ratio, routing overhead, and detection ratio	The proposed DPBHA addresses BHA only and it is incapable of addressing other DoS attacks, such as cooperative BHA and GHA, which will be addressed in future research work

#### 4. Proposed Work

In this section, we elaborate and discuss the proposed detection and presentation of a black hole attack (DPBHA). The proposed DPBHA exploits the two main malicious properties of a BHA. First, the RREP of the attacker node contains a higher sequence number and minimum hop count value since it pretends to have a fresh route toward the destination. Second, the attacker node always responds first to every RREQ without going to check its routing table. Fair modifications are made in the default operations of the AODV routing protocol to take advantage of these two properties to detect and prevent BHAs in VANETs. The proposed DPBHA operates mainly in three phases, i.e., the connectivity phase, detection phase, and prevention phase, as shown in Figure 4.

In the connectivity phase, the network under consideration is initiated, the topology is established and communication between vehicles (nodes) is assumed to be started. The suspected malicious node that tends to be a black hole (with a 50% likelihood) is found in the second phase. The suspected malicious node is 100% proven to be a black hole node in the third phase, and it should be removed from the network.





**Figure 4.** The framework of DPBHA.

#### 4.1. Connectivity Phase

A highly dynamic VANET in which  $N$  number of nodes (vehicles and RSUs) are randomly deployed across the road segment in an urban traffic area. All vehicles are assumed to be intelligent, i.e., embedded with onboard units (OBUs). Each vehicle's OBU has radio equipment, such as a global positioning system (GPS) for location tracking and IEEE 802.11p for communication purposes. Furthermore, RSUs are deployed along roadsides at equal distances to cover the urban traffic area. In traffic management theory, the free-flow state denotes low traffic density and weak vehicle interaction. We investigated the connectivity of VANETs in the free flow state in this research work. According to empirical studies, the Poisson distribution is an excellent model for the vehicle arrival rate in the free-flow state [37,38]. The speeds of different vehicles in a free-flow state follow a normal distribution [39,40]. We suppose that each vehicle is given a random speed from a normal distribution and maintains that speed while traveling on the highway.

Graph theory is a promising approach for modeling and representing the connectivity analysis of vehicular networks [41,42]. A random geometric graph (RGG) is a particular model of traditional graph theory that accurately characterizes randomly deployed networks, such as wireless sensor networks [43–47] or VANETs [48]. In an RGG, the nodes are independently distributed at random according to some spatial probability distribution, and two nodes can be connected by an edge if and only if the distance between them is less than the transmission range ( $T_R$ ). The topology of a VANET is represented by an RGG, where nodes in such a graph are independently deployed according to a Poisson distribution with a transmission range  $T_R \geq 0$  [49]. Let us assume that a graph  $G = (N, E, C)$ , where  $N$  indicates a set of nodes (vehicles and RSUs),  $E$  represents a set of edges (links), and  $C$  represents a set of connections among nodes. The graphical representation of VANET's topology is given by Equation (1).

$$A = \begin{cases} C_{ij}, & \text{If } (V_i, V_j) \in C \text{ and } 0 < C_{ij} < 1 \\ 1, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

where  $A$  is the affinity matrix and  $(V_i, V_j) \in C$  signifies that  $V_i$  and  $V_j$  are connected. To compute the vehicular network's adjacency matrix, we employed three conditions:

- (1) If vehicles  $V_i$  and  $V_j$  are connected, the value of the link connectivity is added to the  $ij$ th position of the adjacency matrix  $Adj$ .
- (2) If a link  $C_{ij}$  has the same connectivity in both directions ( $i = j$ ), 1 is added to the connectivity. However, a node can be connected to itself through other nodes in a multi-hop manner, for instance,  $V_1 \rightarrow V_3 \rightarrow V_4 \rightarrow V_1$ .
- (3) When the above two conditions fail, the term “otherwise” is evaluated in Equation (1). When two vehicles are not connected, we add zero. The adjacency matrix  $Adj$ , which represents vehicle interconnectivity, is given by Equation (2).

$$Adj = \begin{bmatrix} C_{11} & C_{12} & C_{13} & \dots & C_{1n} \\ C_{21} & C_{22} & C_{23} & \dots & C_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & C_{n3} & \dots & C_{nn} \end{bmatrix} \tag{2}$$

where  $C$  denotes the connection reliability between two vehicles. Suppose a segment of a unidirectional two-lane highway of length  $L$  kilometers is labeled by interval  $M = [0, L]$ . Each node enters the highway at  $X = 0$  with a random speed and exits at  $X = L$ . We assumed that the process of vehicles entering the highway follows a Poisson distribution. As shown in Figure 5,  $X_i$  denotes the location of the  $i$ th vehicle from the origin and the headway is represented as  $Y_i = X_{i+1} - X_i$  and  $Y_0 = X_1$  for  $i = 1, 2, 3, \dots, n - 1$ .

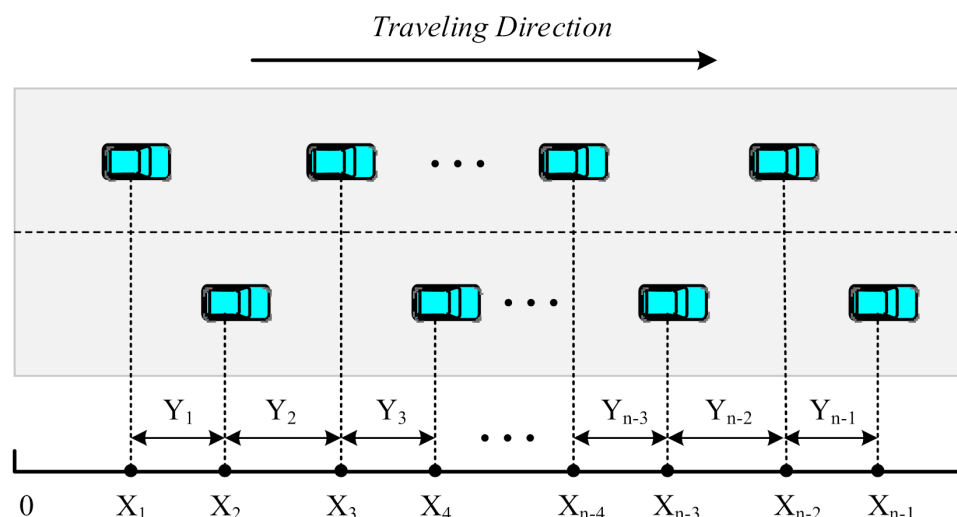


Figure 5. The mobility model of vehicles.

If a vehicle  $V_i$  is lying within the transmission range ( $T_R$ ) of another vehicle  $V_j$ , i.e., ((distance between  $V_i$  and  $V_j$ )  $\leq T_R$ ), then they are presumed to be connected by a unidirectional link  $l_i \in E$ . Whenever  $V_i$  transmits a packet, it is directly received by  $V_j$  via an edge  $l_i$ . An edge  $E = (V_i, V_j)$  exists between two vehicles if the Euclidean distance [50] between them is less than or equal to their  $T_R$ , as given in Equation (3).

$$E = \{ (V_i, V_j) | (POS_i - POS_j) \leq T_R \} \tag{3}$$

where  $POS_i$  and  $POS_j$  are the coordinates for vehicle  $V_i$ . and vehicle  $V_j$ , denoted by  $(X_i, Y_i)$  and  $(X_j, Y_j)$ , respectively at time  $t_0$ . The equation leads to an undirected graph that may be connected or unconnected based on the Euclidean distance ( $d$ ) between  $V_i$  and  $V_j$ , as calculated using Equation (4).

$$d = \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2} \tag{4}$$

If the distance between two nodes is greater than their transmission range, then the packets are exchanged between them indirectly in a multi-hop fashion. Consider  $(X_s, Y_s)$  and  $(X_{N_N}, Y_{N_N})$  as the coordinates of a source node S and a neighboring node  $N_N$ , respectively, with their corresponding speeds denoted by  $V_s$  and  $V_{N_N}$ , respectively, and  $T_R$  is the transmission range. Therefore, the link (E) lifetime between the S and  $N_N$  nodes are calculated using Equation (5).

$$E_{s,N_N} = \frac{T_R - \sqrt{(X_{N_N} - X_s)^2 + (Y_{N_N} - Y_s)^2}}{V_s - V_{N_N}} \quad (5)$$

Assume that there are N number of nodes, which are randomly distributed in an urban area of  $w \times l$  square meters,  $T_R$  is the transmission range, S is the source, and D is the destination node. The probability (P) of a neighboring node  $N_N$  being within the transmission range of node S is calculated using Equation (6).

$$P = \frac{\pi T_R^2}{w \times l} \quad (6)$$

The two most important metrics for measuring the performance of highly dynamic networks are link reliability [40] and connectivity [38]. The truncated Gaussian probability density function (PDF) of the vehicle's velocity is given by Equation (7).

$$f_v(v) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(v-\mu)^2}{2\sigma^2}} \quad (7)$$

where  $\mu$  is the average speed and  $\sigma$  is the standard deviation of the vehicle speed. On the road segment, two vehicles are said to be connected if and only if they are lying within each other's transmission range ( $T_R$ ). Vehicle connection is determined by the generalized speed factor (GSF) in [38], which indicates the number of vehicles on a certain road segment in units of km/h and the effect of relative velocity with inter-vehicle spacing. The normal distribution of relative speed and the exponential distribution of inter-vehicle spacing are used to define the GSF [38,39]. Therefore, the definition of the GSF is a truncated Gaussian PDF [39], as given by Equation (8).

$$GSF = \int_{v_{\min}}^{v_{\max}} \frac{\hat{f}_v(v)}{v} dv \quad (8)$$

where

$$\hat{f}_v(v) = \frac{f_v(v)}{\int_{v_{\min}}^{v_{\max}} \frac{1}{\mu} e^{-\frac{-s}{\mu}} ds} \quad (9)$$

where  $f_v(v)$  is the Gaussian PDF of the vehicle's velocity defined in Equation (7),  $v_{\min}$  is the minimum speed, and  $v_{\max}$  is the maximum speed of a vehicle. Moreover,  $v$  denotes the speed and  $s$  denotes the inter-vehicle spacing, where they have an indirectly proportional relationship to each other. According to the definition of the GSF, the probability of the connectivity of N number of vehicles at time can be obtained using Equation (10).

$$P_c(N)t = \prod_{i=1}^{N-1} \left(1 - e^{-(p)(GSF)(T_R)}\right) = \left(1 - e^{-(p)(GSF)(T_R)}\right)^{N-1} \quad (10)$$

where  $p$  denotes the density of vehicles and  $T_R$  is the V2V transmission range. Equation (10) indicates that the speed, density, and transmission range of inter-vehicle communication significantly affects the vehicle connectivity process on a free-flow highway. The notations used in this paper and their descriptions are tabulated in Table 2.

**Table 2.** Notations and their descriptions.

Symbol	Description
N	Node: vehicle or RSU
S	Source node
D	Destination node
E	Edge
T	Timer
V	Vehicle
$N_N$	Neighboring node
$N_{HN}$	Next-hop node
$R_T$	Routing table
$V_{N_N}$	Speed of neighboring node
ID	Identity of a node
G	Gray list
B	Black list
RREQ	Route request
RREP	Route reply
$T_R$	Transmission range
$\sigma$	Standard deviation
$F_V(V)$	Probability density function of a vehicle's velocity
$D_{SN}$	Destination <sub>sequence number</sub>
$\mu$	Mean value
P	The density of vehicles
$\Lambda$	Threshold value (sequence numbers)
I and j	Variables <i>i</i> and <i>j</i> range from 1, 2, 3, . . . , n

**Assumptions**—For the development of our proposed DPBHA and its operations to work, some assumptions were necessary in order to provide a consistent scenario within which to work. These assumptions are reasonable and useful to consider in accordance with the design consideration of VANETs. These assumptions are:

- (1) We assumed that the black hole node is a malicious node that always exploits its harmful properties to each requesting node and that all other nodes are genuine nodes that act normally.
- (2) All the network nodes should be uniquely identifiable, and only BHA will exist in the network. Other network attacks, such as a GHA, Sybil attack, or impersonation attack, will not exist.
- (3) The solution assumed that multiple RREPs will arrive at the source node during the route discovery process and they will be stored in an additional response analysis table (RAT).
- (4) All the network nodes have the same features, and it was assumed that if node A is lying in the transmission range of node B, then node B will also lie in the transmission range of node A.
- (5) All the nodes were assumed to be healthy and they must participate in the route discovery process according to assumption (1).

#### 4.2. Detection Phase

In this phase, a dynamic threshold value is generated to identify the malicious node (black hole node) in the network. Upon receiving all possible RREPs within a time  $t$  ( $rrep\_time\_out$ ), the source node stores them in the RAT. To calculate the threshold value ( $\lambda$ ), the source node sorts out all the received RREPs in descending order with respect to destination sequence number ( $D_{SN}$ ). Then, S calculates the average of all the received RREPs'  $D_{SN}$  values with the difference of the last RREP's  $D_{SN}$  from its routing table's  $D_{SN}$ . The calculation procedure of the  $\lambda$  is presented in the following Equation (11).

$$\lambda = \text{Average} \left[ \begin{array}{l} (D_{SN}(RREP_1) - (D_{SN}(RREP_n) - D_{SN}(R_T))) \\ + (D_{SN}(RREP_2) - (D_{SN}(RREP_n) - D_{SN}(R_T))) + \\ (D_{SN}(RREP_3) - (D_{SN}(RREP_n) - D_{SN}(R_T))) + \dots \\ + (D_{SN}(RREP_n) - (D_{SN}(RREP_n) - D_{SN}(R_T))) \end{array} \right] + n(D_{SN}(RREP_n) - D_{SN}(R_T))$$

$$= \frac{\sum_{i=1}^n D_{SN}(RREP_i) - (D_{SN}(RREP_n) - D_{SN}(R_T))}{n} + n(D_{SN}(RREP_n) - D_{SN}(R_T)) \tag{11}$$

The difference between the last RREP’s  $D_{SN}$  and its routing table’s  $D_{SN}$  is calculated using (12).

$$\Delta = D_{SN}(RREP_n) - D_{SN}(R_T) \tag{12}$$

where  $\Delta$  denotes the difference between the sequence number of the last RREP and existing  $R_T$ . To further simplify the above formula for calculating the threshold value ( $\lambda$ ), the equation can be written as Equation (13).

$$\lambda = \left| \mu \left( \sum_{i=1}^n D_{SN}(RREP_i) - \Delta \right) + n\Delta \right| \tag{13}$$

The source node checks each RREP’s  $D_{SN}$  with the calculated threshold value ( $\lambda$ ) shown in Equation (14). The RREP with a higher  $D_{SN}$  than the threshold value ( $\lambda$ ) will be considered as a malicious node.

$$N_{ID}(RREP_k) = \begin{cases} G, & \text{if } (D_{SN}(RREP_k) > \lambda^{th}), \\ N, & \text{otherwise} \end{cases} \tag{14}$$

Figure 6 illustrates an experimental scenario of the detection phase. In this experiment, we assumed that node S is the source node, node D is the destination node, node 1 is the black hole attacker node, and all the remaining nodes are intermediate nodes.

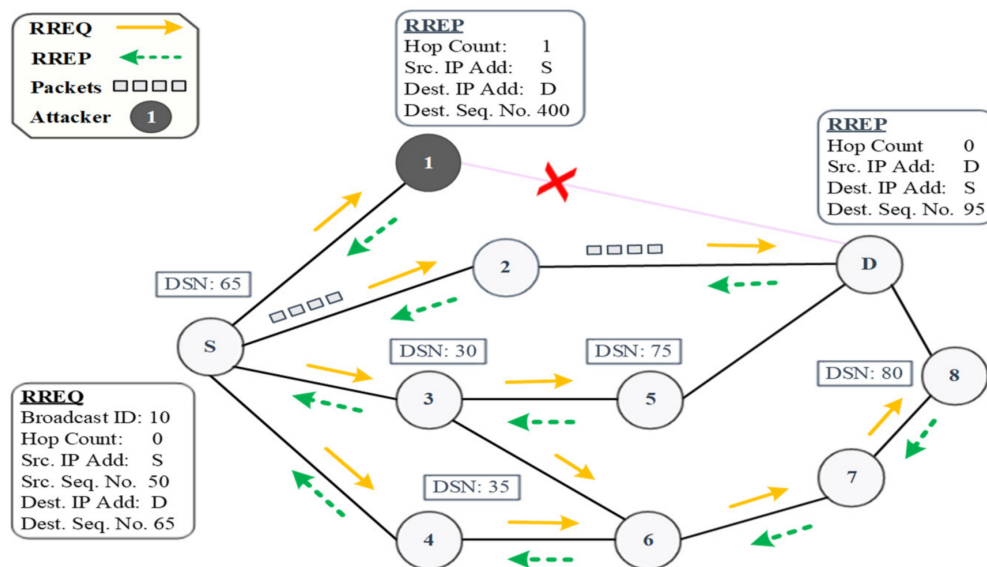


Figure 6. A scenario demonstrating the detection phase.

After broadcasting an RREQ packet, node S receives four RREP packets and sorts them in descending order with respect to  $D_{SN}$  in its RAT, as shown in Table 3. To calculate the threshold value ( $\lambda$ ), first, node S calculates the difference ( $\Delta$ ) between the last RREP’s  $D_{SN}$  and its routing table’s  $D_{SN}$  by putting the values into Equation (12), which gives  $\Delta = 75 - 65 = 10$ . Now, node S calculates the threshold value from all the received RREPs by putting the values into Equation (13), i.e.,  $\lambda = ((390 + 85 + 70 + 65)/4) + 40 = 193$ .

Next, node S compares each received RREP's  $D_{SN}$  value with  $\lambda$ . Node S finds that node 1 has a higher  $D_{SN}$  (400) than the threshold value ( $\lambda = 193$ ). Node S marks it as a suspicious node with a 50% probability and moves it into the gray list.

**Table 3.** RAT with the normal and malicious nodes' RREPs.

$N_{ID} (RREP_i)$	$D_{SN}$	Hop Count
1	400	1
D	95	1
8	80	4
5	75	2

Furthermore, to confirm whether the suspected node that claims a higher  $D_{SN}$  is really malicious or it is a genuine node, the source node pledges to the next phase.

#### 4.3. Prevention Phase

In this phase, the source node modifies the format of the RREQ packet by replacing a non-existing IP address over the destination node IP address field. The new forged RREQ packet format is shown in Table 4. The source node broadcasts the forged RREQ packet in the network. Only a malicious node can give a response, as it does not search the routing table for the route toward the destination and produces an RREP packet. If the same node that is marked as a 50% suspected in the previous phase responds to a forged RREQ, then that particular suspicious node will be confirmed and marked as a 100% black hole node, shown in Equation (15). The source node immediately enlists it to the black list and broadcasts the alarm message into the network by inserting the identity of the black hole node in the RREQ.

$$f(N_{ID}, (RREP_k)) = \begin{cases} G \leftarrow [N_{ID}], & \text{if } D_{SN}(RREP_k) > \lambda^{\text{th}} \\ S \rightarrow RREQ_{\text{forged}} \\ B \leftarrow G, & \text{if } (N_{ID}(RREP_f) = G(N_{ID}(RREP_k))) \\ S \rightarrow \text{Alarm}_{\text{message}} \text{ to } N_N \\ N \leftarrow G, & \text{Otherwise;} \\ S \rightarrow \text{Packets to D} \end{cases} \quad (15)$$

**Table 4.** The format of a forged RREQ packet.

Packet Type	Flags	Reserved	Hop Count
RREQ (Broadcast) ID			
(Non-existing Destination IP Address)			
Destination Sequence Number			
Originator IP Address			

The next RREP's route with the highest  $D_{SN}$  below or equal to the threshold value and minimum hop count will be selected for routing data packets. Figure 7 depicts an experimental scenario of the prevention phase with the generation of a forged RREQ packet. In Figure 7, the source node broadcasts the forged RREQ with a destination IP address K in the network. Here, a genuine node will not reply as the forged RREQ has an IP address that does not exist in the network. Only a malicious node can give a response, as it does not search the routing table for the route toward the destination; therefore, node 1 unicasts the RREP. Upon receiving the RREP, the source node confirms and marks it as a black hole node. Figure 8 illustrates a complete flowchart for the proposed DPBHA, along with the internal data flow processes of the three core phases. Algorithm 1 illustrates the complete step-by-step process of the proposed DPBHA solution.

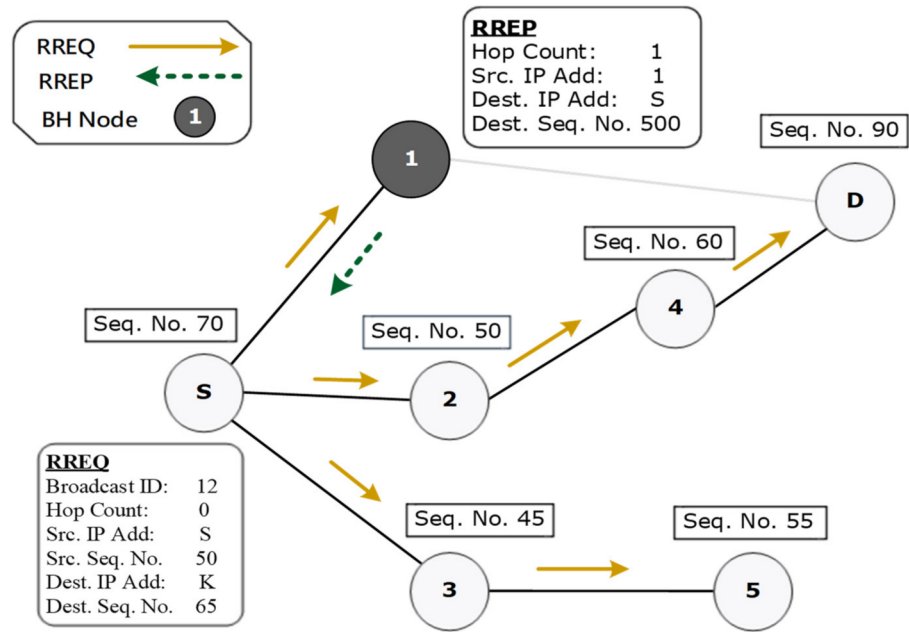


Figure 7. A scenario demonstrating the prevention phase.

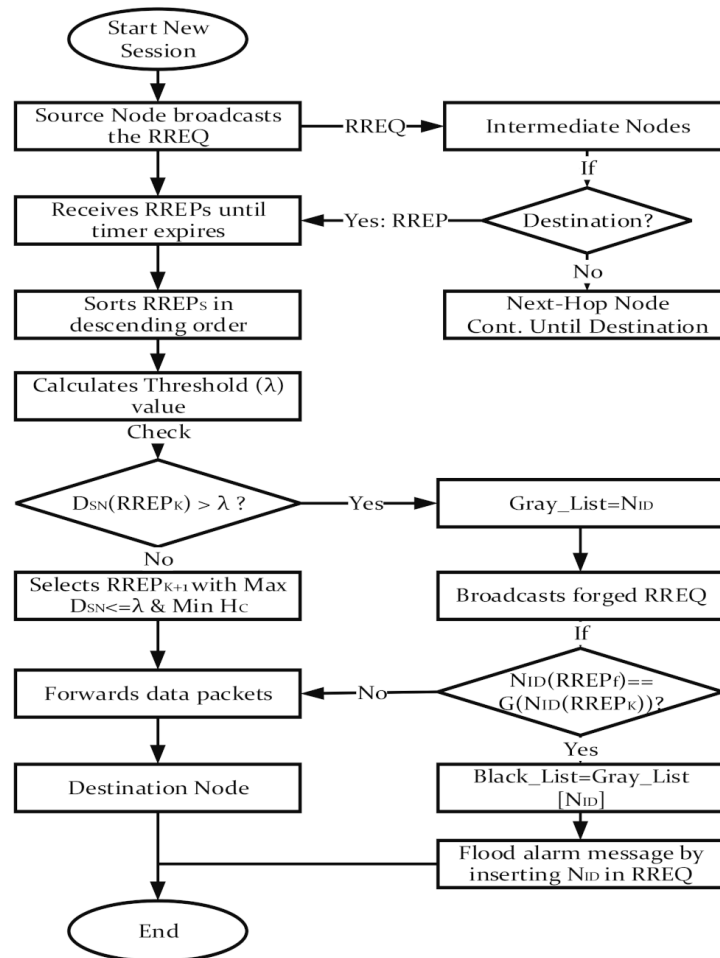


Figure 8. Flowchart of the proposed DPBHA.

**Algorithm 1:** Black Hole Attack Detection and Prevention

---

**Input:** RREQ, RREP, G, B, Forged-RREQ  
**Output:** BHA Detection and Prevention, Best and Secure Path Selection

1. **Initialization:**  $i = 0, 1, 2, 3, \dots, n$
2.  $S \rightarrow$  RREQ to  $N_N$  and sets  $t$
3. **if** route to D in  $R_T$
4.     **goto** step 11
5. **else**
6.     **do**
7.          $N_N \rightarrow$  RREQ to  $N_{HN}$
8.         **while**( $N_N = D$ )
9.     **end**
10. **end**
11.  $D \vee N_N \rightarrow$  RREP to S
12.  $S [RAT] \leftarrow$  RREP <sub>$i$</sub>  till  $t$
13. Quicksort( $S [RAT(D_{SN}(RREP_i))]$ ), start, end, pivot)
14.  $\Delta = D_{SN}(RREP_n) - D_{SN}(R_T)$
15.  $\lambda = \left| \mu \left( \sum_{i=1}^n D_{SN}(RREP_i) - \Delta \right) + n\Delta \right|$
16.  $\forall$  each RREP <sub>$i-n$</sub>   $\in [RAT]$
17. **if** ( $D_{SN}(RREP_k) > \lambda^{th}$ )
18.      $G \leftarrow N_{ID}(RREP_k)$
19. **else**
20.     Selects RREP <sub>$k+1$</sub>  (Max  $D_{SN} \leq \lambda^{th}$  and Min HC)
21.     **goto** step 30
22. **end**
23.  $S \rightarrow$  RREQ<sub>forged</sub> to  $N_N$
24.  $S \leftarrow$  RREP <sub>$f$</sub>
25. **if** ( $N_{ID}(RREP_i) = G(N_{ID}(RREP_k))$ )
26.      $B \leftarrow G [N_{ID}]$
27.      $S \rightarrow$  Alarm<sub>message</sub> to  $N_N$
28.     **goto** step 20
29. **else**
30.      $S \rightarrow$  Packets to D
31. **end**

---

**5. Implementation and Result Evaluation**

The proposed DPBHA was implemented and evaluated in a simulation-based environment (NS-2 Simulator v2.35) and its performance and efficacy were compared to the benchmark schemes. NS-2 allows for a wide range of simulation settings, making simulation more practical and realistic. The results were compared with the most relevant schemes that exist in the literature, namely, AODV [19], SAODV [10], and IDBA [20]. The parameters used in the simulation experiments are tabulated in Table 5.

For the performance evaluation, a general urban traffic scenario was selected with a variable traffic density of 25 to 150 nodes (vehicles, RSUs, and black hole nodes). Each simulation experiment contained 8% malicious nodes (black hole nodes).

Figure 9 demonstrates one of the initial states of the first experiment performed with 25 nodes comprising 21 normal vehicles (with black circles), 2 black hole nodes (with red circles), and 2 RSUs (with blue circles). Before performing the statistical analysis, each simulation experiment was run 10 times in the simulator and the average values were obtained after aggregating the results. The following performance metrics were used to evaluate the proposed solution:

- Routing overhead;
- Packet delivery ratio (PDR);
- End-to-end delay;



- Throughput;
- Packet loss ratio;
- Confusion metrics.

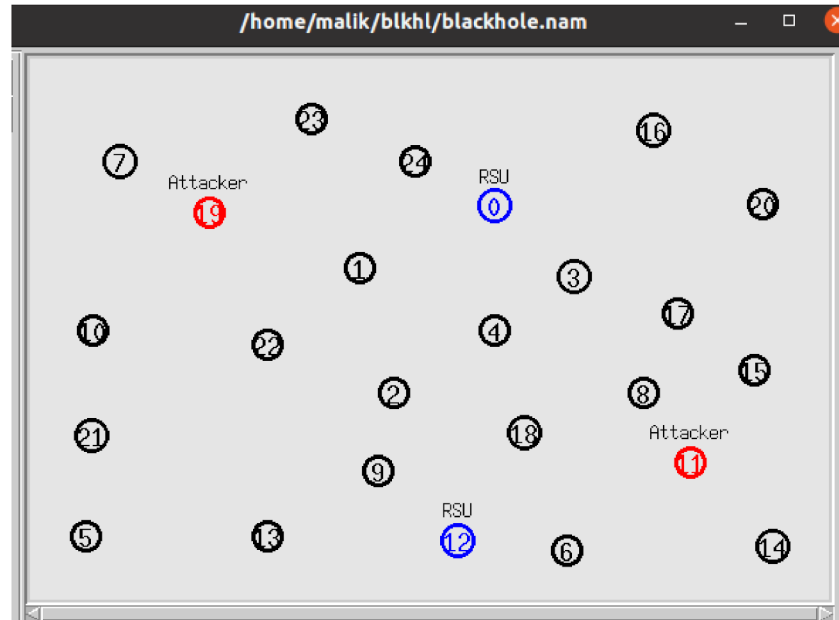


Figure 9. Initial state of the first experiment.

Table 5. Simulation parameters.

S. No.	Parameters	Values
1.	Simulation tool	NS-2.35
2.	Simulation area	1000 m × 1000 m
3.	Number of nodes	25, 50, 75, 100, 125, 150
4.	Simulation time	900 s
5.	Vehicle mobility	1 km/h–100 km/h
6.	Routing protocols	AODV
7.	Standard protocol	802.11p
8.	Black hole nodes	2, 4, 6, 8, 10, 12
9.	Transport protocol	UDP
10.	Packet size (bytes)	512 b/s
11.	Type of traffic	CBR (1 Mbps)
12.	Antenna	Omni-directional

### 5.1. Routing Overhead

The routing overhead (ROH) represents the ratio of the total number of control packets transmitted to the total number of data packets, as given in Equation (16).

$$\text{ROH} = \frac{\sum \text{control packets transmitted}}{\sum \text{data packetstransmitted}} \quad (16)$$

Figure 10 shows the simulation results, indicating the number of nodes on the  $x$ -axis and the routing overhead (in the number of packets) on the  $y$ -axis. The routing overhead increased with respect to an increase in the number of nodes. As the network became more congested, path breakages and packet drop rates became more common. The presence of more malicious nodes caused more RREPs to be sent to the desired route, resulting in increased routing overhead. The routing overhead behavior for the proposed DPBHA was plotted in comparison to benchmark schemes, namely, classic AODV, SAODV, and IDBA.

By detecting the malicious nodes instantaneously from the network, the routing overhead was reduced in the proposed DPBHA as compared to the benchmark schemes. In the case of classic AODV, more replies were generated in the network due to the presence of malicious nodes, resulting in a huge routing overhead of 28.57%. Similarly, in the case of SAODV, more control packets were generated in its five-step detection mechanism such that its routing overhead was 26.59%, which was also very high. In the case of IDBA, the average routing overhead was 23.52% which was close to the proposed DPBHA. Figure 10 indicates that in most of the points in DPBHA, the average routing overhead was 21.30%, which was the minimum among all the schemes. Therefore, the proposed DPBHA decreased the average routing overhead by 3.69%.

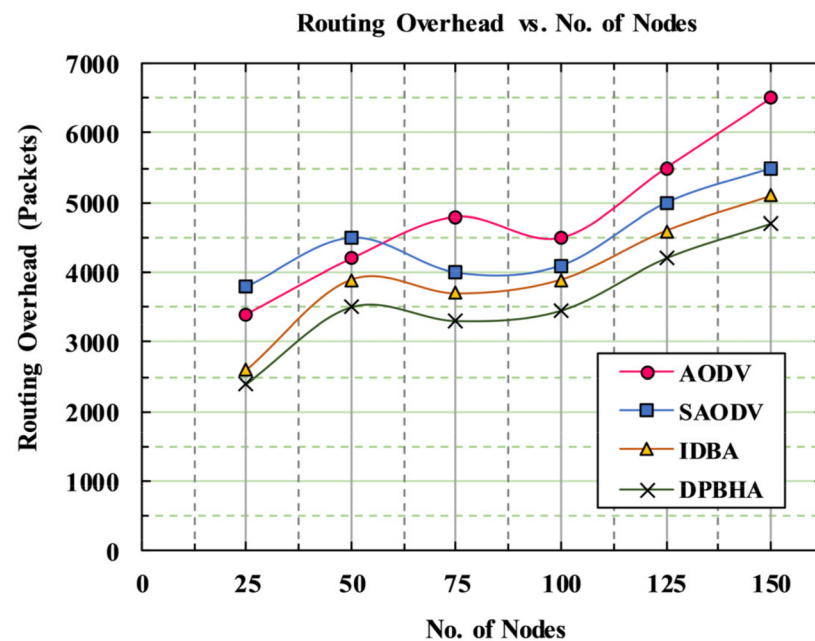


Figure 10. Graphical representation of routing overhead.

### 5.2. Packet Delivery Ratio

The packet delivery ratio (PDR) represents the ratio of the total number of packets received at a destination node to the total number of packets originated at the source node, as shown in Equation (17).

$$\text{PDR} = \frac{\sum \text{Number of packets received}}{\sum \text{Number of packets sent}} \quad (17)$$

Figure 11 shows the simulation results, indicating the PDR in terms of percentage on the  $y$ -axis and the number of nodes on the  $x$ -axis. It can be observed that as the number of nodes increased, the PDR decreased due to the presence of more malicious nodes and packet collision occurrences in the network. When a malicious node performs a packet-dropping attack, it badly affects the PDR. The proposed DPBHA first identifies the malicious node with the help of a dynamic threshold value and then confirms it as malicious by broadcasting a forged RREQ.

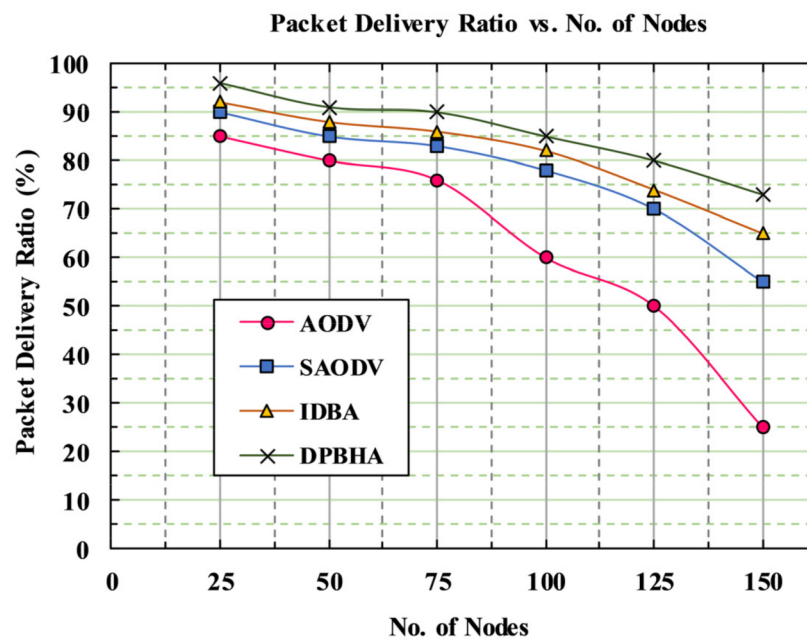


Figure 11. Graphical representation of packet delivery ratio.

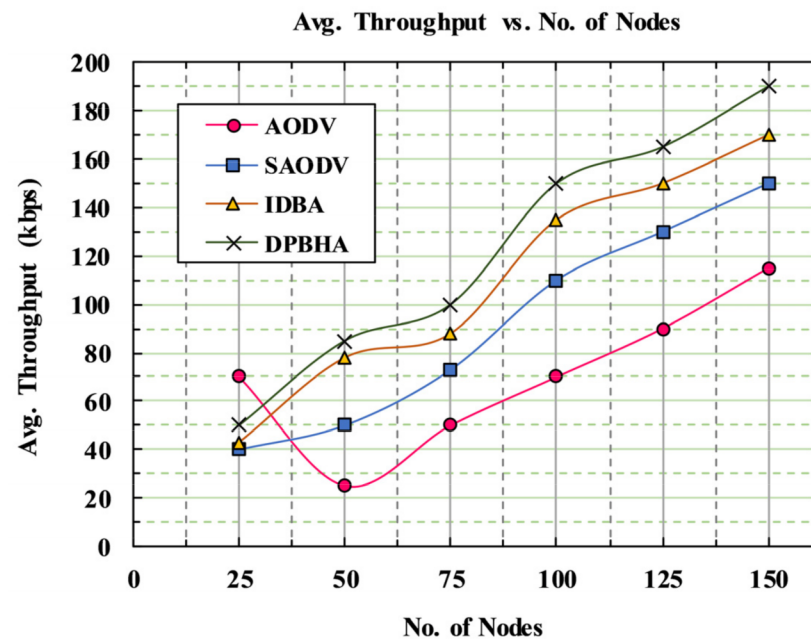
In Figure 11, it can be observed that the proposed DPBHA had the best performance results in PDR compared to the rest of the schemes. The PDR decreased significantly in the case of the classic AODV, with an average of 20.44%, while the PDR of other schemes showed less of a decrease due to the presence of some security mechanisms. The average PDRs for the SAODV and IDBA schemes were recorded as 25.06% and 26.48%, respectively. The classic AODV severely suffered from the presence of a BHA: as the number of malicious nodes in the network grew, its PDR dropped drastically. The average PDR of our proposed DPBHA was 28%, which was a 3.0% improvement above the total average PDR.

### 5.3. Throughput

Throughput represents the average rate of successful data packet delivery to the final destination by the source node, as given in Equation (18). Throughput can be measured in packets per second (pps), bits per second (bps), or packets per time slot.

$$\text{Throughput} = \frac{\sum(\text{Received Packets} * \text{Packet Size})}{\text{Simulation Time}} \quad (18)$$

Figure 12 shows the performance of the throughput metric (in kbps) for the proposed DPBHA and benchmark schemes. The throughput of the classic AODV had the lowest significant values on each point because of the presence of BHAs and the destination node received extremely few packets. Another reason for the throughput degradation was the high speed of the vehicles, causing frequent link breakages, which led to a decrease in throughput. The average throughput of the classic AODV was recorded as 17.68%, which drastically suffered from the increase in the number of malicious nodes in the network. The average throughputs of the SADOV and IDBA schemes were recorded as 23.36% and 27.78%, respectively. These schemes achieved a certain level of better performance in throughput because both of them employed some security mechanisms that detect a BHA instantly. In terms of throughput, the proposed DPBHA outperformed the existing schemes. The average throughput of the proposed DPBHA was recorded as 31.15%, which was the highest among all the schemes. Therefore, the proposed DPBHA improved the overall average throughput by 6.15%.



**Figure 12.** Graphical representation of average throughput.

#### 5.4. End-To-End Delay

The end-to-end delay describes the time between when the packet is generated at the source node to when the packet is received by the destination node. It is the average time needed for the data packets to be transmitted from the source node to the destination node, as given in Equation (19).

$$\text{E2E Delay} = \frac{\sum_{i=1}^n (\text{Received Packet Timer} - \text{Sent Packet Timer}) * 1000(\text{ms})}{\text{Total Number of Packets Delivered Successfully}} \quad (19)$$

Figure 13 plots the performance metric of E2E delay (in seconds) for the DPBHA and benchmark schemes. Here, the E2E delay was high when the density of nodes was high. It can be observed that the average E2E delay of the proposed DPBHA was lower than the other schemes. A high PDR leads to a lower E2E delay and optimal throughput due to a large number of packets being delivered to the destination node with less amount of time. The classic AODV shows a significant hike in E2E delay when the number of nodes increased from 25 to 150. The average E2E delay of the conventional AODV was 30.93%; this was because of the presence of more malicious nodes and packet collision events in the network. When the target destination was not reached, a new route discovery process needed to be initiated. Using a combination of the dynamic threshold value and a forged RREQ mechanism, the speed of data transmission increased and the delay decreases in the proposed DPBHA, as shown in Figure 13. This was because the DPBHA quickly detected the malicious nodes from the network and selected the best and most secure route for data transmission. The average E2E delay of the proposed DPBHA was recorded as 18.86%, which is the lowest among all the schemes. Similarly, the average E2E delays of the SADOV and IDBA were recorded as 27.04% and 23.15%, respectively. Hence, the proposed DPBHA reduced the overall average E2E delay by 6.13%.

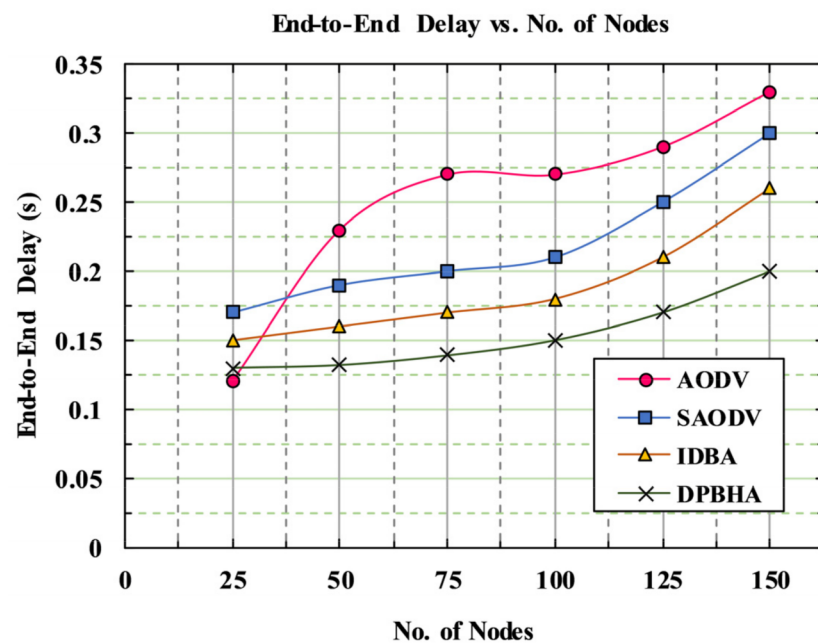


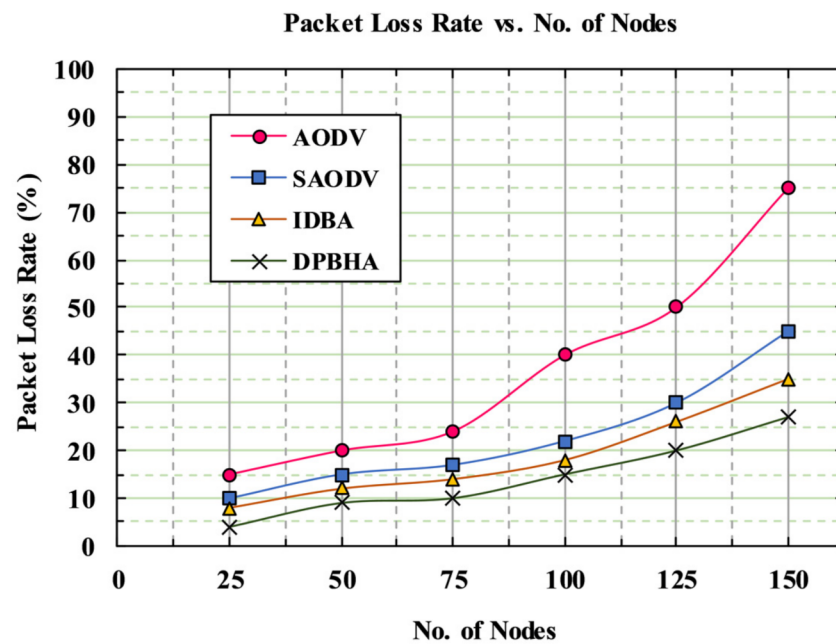
Figure 13. Graphical representation of end-to-end delay.

#### 5.5. Packet Loss Rate (PLR)

The packet loss rate (PLR) is the difference between the total number of data packets sent by the source node and the total number of data packets successfully received by the destination node, as given in Equation (20). Usually, packets are lost by malicious nodes or due to increased congestion in the network.

$$PLR = \sum \text{Number of packets sent} - \sum \text{Number of packets received} \quad (20)$$

Figure 14 illustrates the simulation results, indicating the PLR in terms of percentage on the  $y$ -axis and the number of nodes on the  $x$ -axis. It can be observed that as the number of nodes increased, the PLR increased due to the presence of more malicious nodes and packet collision occurrences in the network. When a malicious node performs a packet-dropping attack, it badly affects the PLR. The classic AODV severely suffered from the presence of a BHA, where an average of 37.33% of packets were lost due to a lack of security mechanisms. It was further observed that the average PLRs for SAODV and IDBA were recorded as 24.77% and 20.14%, respectively. These schemes achieved a good level of performance regarding the PLR because both of them employed some security mechanisms that detect a BHA instantly. Similarly, the proposed DPBHA first identifies the malicious node with the help of a dynamic threshold value and then makes confirms it as BHA by broadcasting a forged RREQ. The PLR for the proposed DPBHA was recorded as 15.15% due to the instant elimination of BHAs. Thus, the proposed DPBHA reduced the overall average PLR by 9.84%.



**Figure 14.** Graphical representation of packet loss rate.

### 5.6. Confusion Matrix

Intrusion detection systems (IDSs) are usually evaluated based on the following measures of confusion matrix shown in Table 6. The columns of the table represent instances in the predicted class. Similarly, the rows of the table represent instances in the actual class.

**Table 6.** Confusion matrix.

		Actual Reality Class		
		Class	Attack	Normal
Test Result Class	Attack		True positive (TP)	False positive (FP)
	Normal		False negative (FN)	True negative (TN)

#### 5.6.1. True Positive Rate (TPR)

When the model correctly identifies and detects an attacker in a network, it is said to be true positive. The sensitivity or detection ratio is another name for the TPR (DR). It is calculated as the ratio between the predicted attacks and the total number of attacks. Mathematically, the TPR can be calculated using Equation (21).

$$TPR = \frac{TP}{TP + FN} \quad (21)$$

#### 5.6.2. False Positive Rate (FPR)

When the model misidentifies a legitimate node as an attacker, it is said to be a false positive. FPR is calculated as the ratio of the total number of normal instances that are wrongly classified as an attacker to the overall number of normal instances. Mathematically, the FPR can be expressed using Equation (22).

$$FPR = \frac{FP}{FP + TN} \quad (22)$$

### 5.6.3. False Negative Rate (FNR)

A false negative occurs when there are attacker nodes that are incorrectly classified as legitimate or normal nodes. It means that an anomaly is not being detected by the model and is labeled as normal. Mathematically, the FNR can be calculated using Equation (23).

$$\text{FNR} = \frac{\text{FN}}{\text{FN} + \text{TP}} \quad (23)$$

### 5.6.4. True Negative Rate (TNR)

A true negative occurs when there is no attacker node and the model identifies it as a normal node. It means that the scheme successfully labels legitimate nodes as normal nodes. Mathematically, the TNR can be expressed using Equation (24).

$$\text{TNR} = \frac{\text{TN}}{\text{TN} + \text{FP}} \quad (24)$$

### 5.6.5. Detection Rate

The detection ratio is an important metric to examine the accuracy of a model when identifying and detecting the malicious nodes in a network. Table 7 illustrates the statistical analysis of the detection ratio of the proposed DPBHA and its comparison to the benchmark schemes with the various number of normal and malicious nodes.

**Table 7.** Detection ratio evaluation values.

No. of Nodes	Malicious Nodes	TPR of AODV	TPR of SAODV	TPR of IDBA	TPR of DPBHA
25	2	00.0%	90.0%	95.0%	100%
50	4	00.0%	87.5%	92.5%	97.5%
75	6	00.0%	85.0%	90.0%	95.0%
100	8	00.0%	82.5%	87.5%	93.7%
125	10	00.0%	80.0%	85.0%	91.0%
150	12	00.0%	76.6%	83.3%	90.8%

Figure 15 depicts the simulation results of the detection ratio of the proposed DPBHA and its comparison to the benchmark schemes. The results showed that the average detection ratio of the proposed DPBHA was reported as 94.66%, which was the highest detection rate across all schemes. The main reason for the highest detection rate was the fact that the proposed DPBHA first checks each RREP's sequence number with the calculated dynamic threshold value. If the received RREP's sequence number is higher than the threshold value, then that node is detected as a suspicious node with a 50% probability. Further, in the next phase, the suspected malicious node is 100% confirmed that it is a black hole node if it replies to the forged RREQ. This means that the proposed DPBHA can detect and prevent the malicious node instantly and accurately by performing the two-stage approach. As soon as the number of legitimate and malicious nodes increased in the network, the chances of malicious node detection decreased due to an increase in congestion and packet collision occurrences. However, the proposed DPBHA could detect and prevent the BHA more accurately and rapidly than other benchmark schemes. The classic AODV was designed with no security mechanism; therefore, its detection rate was recorded as 0.0%, as shown in Figure 15. The average detection rates for SAODV and IDBA were recorded as 83.6% and 88.88%, respectively. Figure 15 reveals that the proposed DPBHA's detection ratio was high for a majority of points, with an average of 94.66%.

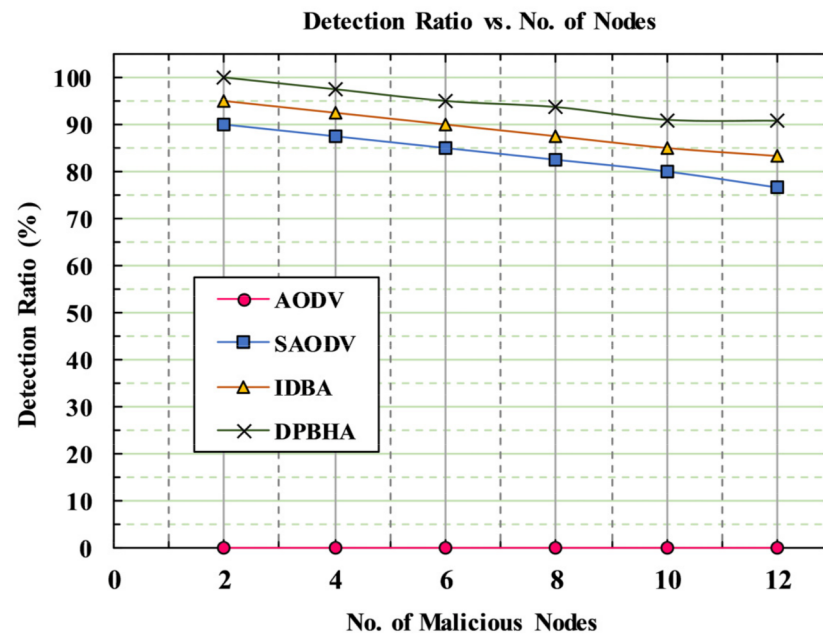


Figure 15. Graphical representation of detection rate.

#### 5.6.6. Accuracy Rate

The accuracy metric measures how accurate the model is in detecting malicious or normal node behavior. It is defined as the percentage of all those correctly predicted instances to the overall instances calculated using Equation (25). In order to maximize the performance of a model, FPR and FNR must be minimized, while TPR and TNR must be maximized.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (25)$$

Table 8 demonstrates one of the experiments of the proposed DPBHA performed with a total number of 75 nodes comprising 69 normal and 6 malicious nodes. After performing the simulation, the model successfully detected five out of six targeted malicious nodes, giving an 83.3% sensitivity. In Table 8, the positive predictive value (PPV) means the probability that the model successfully detected the true attacker nodes and is calculated using  $\text{PPV} = \text{TP} / (\text{TP} + \text{FP}) \times 100 = 5 / (5 + 0) \times 100 = 100\%$ . Similarly, the negative predictive value (NPV) means the probability that the model correctly identifies a negative test as a non-attacker node. Mathematically, the NPV is represented by  $\text{NPV} = \text{TN} / (\text{TN} + \text{FN}) \times 100 = 69 / (69 + 1) \times 100 = 98.5\%$ . Finally, the accuracy rate for the proposed DPBHA was calculated as 98.6%, which is a high accuracy rate for any given model.

Table 8. Example of an accuracy rate calculation.

Total No. of Nodes = 75	Real Class		Predictive Value
	Attacker = 06	Normal = 69	
Attacker = 5	True Positive = 5	False Positive = 0	Positive Predictive Value (5/5) = 100%
Normal = 70	False Negative = 5	True Negative = 69	Negative Predictive Value (69/70) = 98.5%
Results	Sensitivity (5/6) = 83.3%	Specificity (69/69) = 100%	Accuracy = $\frac{5+69}{5+69+0+1} \times 100$ = 98.6%



## 6. Conclusions and Future Work

Safety and security are the major concerns in VANET applications. Many road applications, such as traffic reports and accident notifications, can strongly support safety requirements. However, VANETs are vulnerable to a variety of security threats and attacks because of their highly dynamic, decentralized nature and protocol design concerns. As a result, VANET applications and services are jeopardized. There is the possibility that VANET applications will have certain security requirements. However, life and safety-critical messages must be sent from V2V in a secure and timely way. Because vehicles exchange messages at fast speeds over an open wireless medium, ensuring the security of these messages is critical. The security aspect of VANETs was the focus of this research work. To protect and improve the overall performance of VANETs, an innovative and effective solution was proposed called DPBHA, which could detect and prevent black hole security attacks in the AODV routing protocol. The solution was based on calculating a dynamic threshold value and generating a forged RREQ packet. The proposed DPBHA was implemented and evaluated in the NS-2 simulator, and its performance and efficacy were compared to the benchmark schemes. In conclusion, we showed that the proposed DPBHA outperformed the benchmark schemes in terms of improved PDR by 3.0%, increased throughput by 6.15%, reduced routing overhead by 3.69%, decreased E2E delay by 6.13%, reduced PLR by 9.84%, and achieved a maximum detection rate of 94.66%.

Future research includes detecting and preventing gray hole security attacks, which are considered to be some of the severe attacks on VANETs. Similarly, more efforts will be made in the future to explore state-of-the-art advancements in the field and address various security issues associated with vehicular networks.

**Author Contributions:** A.M. collected data from different resources and performed the formal analysis, investigation, methodology, original draft preparation, and simulation. A.M., F.K. and J.-T.S. contributed in terms of resources, review and editing, and visualization. M.Z.K. and M.F. contributed to supervision and co-supervision, respectively; project administration; and conceptualization. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A2C101218712) (50%) and was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KoFONS) using the financial re- source granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea. (No. 2101058) (50%).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The simulation files/data used to support the findings of this study are available from the corresponding author upon request.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Ahmed, Z.; Naz, S.; Ahmed, J. Minimizing transmission delays in vehicular ad hoc networks by optimized placement of road-side unit. *Wirel. Netw.* **2020**, *26*, 2905–2914. [[CrossRef](#)]
2. Arif, M.; Wang, G.; Bhuiyan, M.Z.A.; Wang, T.; Chen, J. A survey on security attacks in VANETs: Communication, applications and challenges. *Veh. Commun.* **2019**, *19*, 100179. [[CrossRef](#)]
3. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [[CrossRef](#)]
4. Cherkaoui, B.; Beni-hssane, A.; Erritali, M. Variable control chart for detecting black hole attack in vehicular ad-hoc networks. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 5129–5138. [[CrossRef](#)]
5. Fan, N.; Wu, C.Q. On trust models for communication security in vehicular ad-hoc networks. *Ad Hoc Netw.* **2019**, *90*, 101740. [[CrossRef](#)]
6. Khan, M.N.; Rahman, H.U.; Faisal, M.; Khan, F.; Ahmad, S. An IoT-Enabled Information System for Smart Navigation in Museums. *Sensors* **2022**, *22*, 312.

7. Abbas, S.; Talib, M.A.; Ahmed, A.; Khan, F.; Ahmad, S.; Kim, D.H. Blockchain-based authentication in internet of vehicles: A survey. *Sensors* **2021**, *21*, 7927. [[CrossRef](#)] [[PubMed](#)]
8. Al-Heety, O.S.; Zakaria, Z.; Ismail, M.; Shakir, M.M.; Alani, S.; Alsariera, H. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. *IEEE Access* **2020**, *8*, 91028–91047. [[CrossRef](#)]
9. Hatim, S.M.; Elias, S.J.; Awang, N.; Darus, M.Y. VANETS and Internet of Things (IoT): A discussion. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *12*, 218–224. [[CrossRef](#)]
10. Kumar, A.; Varadarajan, V.; Kumar, A.; Dadheech, P.; Choudhary, S.S.; Kumar, V.A.; Panigrahi, B.; Veluvolu, K.C. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocess. Microsyst.* **2021**, *80*, 103352. [[CrossRef](#)]
11. Lee, M.; Atkison, T. Vanet applications: Past, present, and future. *Veh. Commun.* **2021**, *28*, 100310. [[CrossRef](#)]
12. Huang, L.; Jiang, H.; Zhang, Z.; Yan, Z.; Guo, H. Efficient data traffic forwarding for infrastructure-to-infrastructure communications in VANETs. *IEEE Trans. Intell. Transp. Syst.* **2017**, *19*, 839–853. [[CrossRef](#)]
13. Ouazine, K.; Slimani, H.; Nacer, H.; Bermad, N.; Zemmodj, S. Reducing saturation and congestion in VANET networks: Alliance-based approach and comparisons. *Int. J. Commun. Syst.* **2020**, *33*, e4245. [[CrossRef](#)]
14. Zekri, A.; Jia, W. Heterogeneous vehicular communications: A comprehensive study. *Ad Hoc Netw.* **2018**, *75*, 52–79. [[CrossRef](#)]
15. Zhang, J.; Zheng, K.; Zhang, D.; Yan, B. AATMS: An Anti-Attack Trust Management Scheme in VANET. *IEEE Access* **2020**, *8*, 21077–21090. [[CrossRef](#)]
16. Sheikh, M.S.; Liang, J. A comprehensive survey on VANET security services in traffic management system. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 2423915. [[CrossRef](#)]
17. Khan, S.; Sharma, I.; Aslam, M.; Khan, M.Z.; Khan, S. Security Challenges of Location Privacy in VANETs and State-of-The Art Solutions: A Survey. *Future Internet* **2021**, *13*, 96. [[CrossRef](#)]
18. Nazib, R.A.; Moh, S. Routing Protocols for Unmanned Aerial Vehicle-Aided Vehicular Ad Hoc Networks: A Survey. *IEEE Access* **2020**, *8*, 77535–77560. [[CrossRef](#)]
19. Perkins, C.E.; Royer, E.M. Ad-hoc on-demand distance vector routing. In Proceedings of the WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, 25–26 February 1999; pp. 90–100.
20. Hassan, Z.; Mehmood, A.; Maple, C.; Khan, M.A.; Aldegheishem, A. Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles. *IEEE Access* **2020**, *8*, 199618–199628. [[CrossRef](#)]
21. Gautham, P.S.; Shanmughasundaram, R. Detection and isolation of Black Hole in VANET. In Proceedings of the 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT), Kerala, India, 6–7 July 2017; pp. 1534–1539.
22. Su, M.-Y. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Comput. Commun.* **2011**, *34*, 107–117. [[CrossRef](#)]
23. Kudva, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. A scalable blockchain based trust management in VANET routing protocol. *J. Parallel Distrib. Comput.* **2021**, *152*, 144–156. [[CrossRef](#)]
24. Malhi, A.K.; Batra, S.; Pannu, H.S. Security of vehicular ad-hoc networks: A comprehensive survey. *Comput. Secur.* **2020**, *89*, 101664. [[CrossRef](#)]
25. Sleem, L.; Noura, H.N.; Couturier, R. Towards a secure ITS: Overview, challenges and solutions. *J. Inf. Secur. Appl.* **2020**, *55*, 102637. [[CrossRef](#)]
26. Gurung, S.; Chauhan, S. Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. *Wirel. Netw.* **2019**, *25*, 975–988. [[CrossRef](#)]
27. Panos, C.; Ntantogian, C.; Malliaros, S.; Xenakis, C. Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. *Comput. Netw.* **2017**, *113*, 94–110. [[CrossRef](#)]
28. Hortelano, J.; Ruiz, J.C.; Manzoni, P. Evaluating the usefulness of watchdogs for intrusion detection in VANETs. In Proceedings of the 2010 IEEE International Conference on Communications Workshops, Cape Town, South Africa, 23–27 May 2010; pp. 1–5.
29. Daeinabi, A.; Rahbar, A.G. Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks. *Multimed. Tools Appl.* **2013**, *66*, 325–338. [[CrossRef](#)]
30. Kadam, M.; Limkar, S. Performance Investigation of DMV (Detecting Malicious Vehicle) and D & PMV (Detection and Prevention of Misbehave/Malicious Vehicles): Future Road Map. In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013, Odissa, India, 22–23 December 2013; pp. 379–387.
31. Dhaka, A.; Nandal, A.; Dhaka, R.S. Gray and black hole attack identification using control packets in MANETs. *Procedia Comput. Sci.* **2015**, *54*, 83–91. [[CrossRef](#)]
32. Jahan, R.; Suman, P. Detection of malicious node and development of routing strategy in VANET. In Proceedings of the 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 11–12 February 2016; pp. 472–476.
33. Li, W.; Song, H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 960–969. [[CrossRef](#)]
34. Purohit, K.C.; Dimri, S.C.; Jasola, S. Mitigation and performance analysis of routing protocols under black-hole attack in vehicular ad-hoc network (VANET). *Wirel. Pers. Commun.* **2017**, *97*, 5099–5114. [[CrossRef](#)]
35. Tyagi, P.; Dembla, D. Advanced secured routing algorithm of vehicular ad-hoc network. *Wirel. Pers. Commun.* **2018**, *102*, 41–60. [[CrossRef](#)]

36. 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](#)]
37. Roess, R.P.; Prassas, E.S.; McShane, W.R. *Traffic Engineering*; Pearson/Prentice Hall: London, UK, 2004.
38. Khan, Z.; Fan, P.; Fang, S. On the connectivity of vehicular ad hoc network under various mobility scenarios. *IEEE Access* **2017**, *5*, 22559–22565. [[CrossRef](#)]
39. Yousefi, S.; Altman, E.; El-Azouzi, R.; Fathy, M. Analytical model for connectivity in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2008**, *57*, 3341–3356. [[CrossRef](#)]
40. Khan, Z.; Fan, P.; Fang, S.; Abbas, F. An unsupervised cluster-based VANET-oriented evolving graph (CVoEG) model and associated reliable routing scheme. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 3844–3859. [[CrossRef](#)]
41. Eiza, M.H.; Ni, Q. An evolving graph-based reliable routing scheme for VANETs. *IEEE Trans. Veh. Technol.* **2013**, *62*, 1493–1504. [[CrossRef](#)]
42. Elaraby, S.; Abuelenin, S.M. Connectivity analysis of directed highway vehicular ad hoc networks using graph theory. *Int. J. Commun. Syst.* **2021**, *34*, e4745. [[CrossRef](#)]
43. Khan, F.; Khan, W.; Shah, K.; Qasim, I.; Habib, A. An algorithmic approach for core election in mobile ad-hoc network. *J. Internet Technol.* **2019**, *20*, 1099–1111.
44. Rashid, A.; Khan, F.; Gul, T.; Khan, S.; Khan, F. Improving energy conservation in wireless sensor networks using energy harvesting system. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 354–363. [[CrossRef](#)]
45. Khan, F.; Khan, W.; Khan, S.; Qasim, I.; Habib, A. A secure core-assisted multicast routing protocol in mobile ad-hoc network. *J. Internet Technol.* **2020**, *21*, 375–383.
46. Hussain, S.M.; Abdul, W.; Munam, A.S.; Akhuzada, A.; Khan, F.; Amin, N.A.; Arshad, S.; Ali, I. Seven pillars to achieve energy efficiency in high-performance computing data centers. In *Recent Trends and Advances in Wireless and IoT-enabled Networks*; Jan, M., Khan, F., Alam, M., Eds.; Springer: Cham, Switzerland, 2019; pp. 93–105.
47. Khan, F.; Ahmad, S.; Gürüler, H.; Cetin, G.; Whangbo, T.; Kim, C. An Efficient and Reliable Algorithm for Wireless Sensor Network. *Sensors* **2021**, *21*, 8355. [[CrossRef](#)]
48. Kenniche, H.; Ravelomanana, V. Random geometric graphs as model of wireless sensor networks. In Proceedings of the 2010 The 2nd international conference on computer and automation engineering (ICCAE), Singapore, 26–28 February 2010; pp. 103–107.
49. Zhang, Y.; Zhang, H.; Sun, W.; Pan, C. Connectivity analysis for vehicular ad hoc network based on the exponential random geometric graphs. In Proceedings of the 2014 IEEE Intelligent Vehicles Symposium Proceedings, Ypsilanti, MI, USA, 8–11 June 2014; pp. 993–998.
50. Gutiérrez-Reina, D.; Sharma, V.; You, I.; Toral, S. Dissimilarity metric based on local neighboring information and genetic programming for data dissemination in vehicular ad hoc networks (VANETs). *Sensors* **2018**, *18*, 2320. [[CrossRef](#)] [[PubMed](#)]