IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

*Digital Object Identifier 10.1109/ACCESS.2017.Doi Number*

# Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles

**Zohaib Hassan[1], Amjad Mehmood[1,2], Carsten Maple [2], Muhammad Altaf Khan[1], Abdulaziz Aldegheishem[3]**

[1]Institute of Computing, Kohat University of Science and Technology, Kohat 26000, Pakistan
[2]Secure Cyber Systems Research Group, WMG, University of Warwick, Coventry, UK
[3]Traffic Safety Technologies Chair, Urban Planning Department, College of Architecture and Planning, King Saud University, Riyadh 11574, Saudi Arabia

engr.afridi81@yahoo.com, dramjad.mehmood@ieee.org, cm@warwick.ac.uk, dr.altaf@kust.edu.pk, aldeghei@ksu.edu.sa

Corresponding author: Amjad Mehmood (dramjad.mehmood@ieee.org )

**ABSTRACT** Detection of Black Hole attacks is one of the most challenging and critical routing security issues in vehicular ad hoc networks (VANETs) and autonomous and connected vehicles (ACVs). Malicious vehicles or nodes may exist in the cyber-physical path on which the data and control packets have to be routed converting a secure and reliable route into a compromised one. However, instead of passing packets to a neighbouring node, malicious nodes bypass them and drop any data packets that could contain emergency alarms. We introduce an intelligent black hole attack detection scheme (IDBA) tailored to ACV. We consider four key parameters in the design of the scheme, namely, Hop Count, Destination Sequence Number, Packet Delivery Ratio (PDR), and End-to-End delay (E2E). We tested the performance of our IDBA against AODV with Black Hole (BAODV), Intrusion Detection System (IdsAODV), and EAODV algorithms. Extensive simulation results show that our IDBA outperforms existing approaches in terms of PDR, E2E, Routing Overhead, Packet Loss Rate, and Throughput.

**INDEX TERMS** ACVs, VANETs, MANETs, Detection, Black Hole, AODV, Routing, Secure, Communication.

## I. INTRODUCTION

VANETs were approved by the Federal Communications Commission (FCC) in 2002 [1]. VANETs permit autonomous (self-driving or partial self-driving) vehicles to mutually exchange data packets and sensitive messages (emergency alarms) with other vehicles and roadside units (RSUs) in the form of Cooperative Awareness Messages (CAMs) [2],[3]. Three types of communication that exist in VANETs are vehicle to vehicle (V2V), vehicle to infrastructure (V2I), and infrastructure to infrastructure (I2I) as shown in Figure 1 [4]. VANETs seek to provide security measures and privacy and safety to vehicles and drivers by exchanging alarm messages and CAMs [5],[6]. Due to some properties of VANETs, they are vulnerable to various routing (network layer) attacks like Black Hole, Rushing, Denial of Service (DoS), and Grey hole [7]. VANETs exhibit characteristics like high mobility, dynamic topology, and unbound communication medium. These features make security a challenging issue for autonomous vehicles [8],[9].

Autonomous vehicles are considered to be one of the greatest revolutions in the automobile and research industry [10]. They are equipped with On-Board Units (OBUs) and Application Units (AUs). These parts play a key role in communication between the vehicles and the RSUs to create and mutually exchange CAMs to decrease the number of accidents that could occur as a result of human mistakes [11]-[14].

VANETs are a sub-class of Mobile ad hoc networks (MANETs), inheriting most of their characteristics. The main similarity between them is the absence of a backbone infrastructure in the network for messages exchange. Moreover, the continuously changing topology is another common factor. The communication range between the nodes is also restricted, which means that each mobile node needs the assistance of intermediate nodes to send data towards the destination in a multi-hop fashion [15].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3034327, IEEE Access



Nevertheless, VANETs have several characteristics that vary from MANETs. The movement of nodes in MANETs is random while in VANETs, nodes are supposed to travel along the roads. Also, every vehicle is equipped with On-Board Sensors. These sensors are used for obtaining the vehicles' speed and location. Due to these characteristics, implementing secure routing in VANETs, which leads to secure communication is a challenging issue [16]-[19].

Ad hoc on Demand Distance Vector (AODV) is a renowned and mostly configured routing protocol for ad hoc networks. Two main control messages that AODV uses for route discovery are route request (RREQ) and route reply (RREP). When the source needs to send data to communicate with the destination, and a route is not available, then it floods RREQ messages to its neighbours. The Neighbours reply with RREP if they have the best path to the destination. If they do not have one, then they further flood RREQ to their neighbours and the route discovery process continues until RREQ reaches the destination or the intermediate node which has got the route. The source unicast data packets upon receipt of RREP. Although AODV offers reactive routing and route discovery, however, it lacks security features (AODV-RFC 3561).

There are a variety of attacks that can harm data communication. Some attacks are internal which are initiated by an authorized malicious vehicle and some are external that are launched by a non-authorized malicious vehicle. The attacks can also be categorized as passive such as eavesdropping and active in particular routing attacks that directly disrupts data communication. One of the routing attacks in the field of ad hoc networks is a Black Hole attack, shown in Figure 2. During a black hole attack, fake RREP is sent as responses to legitimate RREQ requests without consulting the routing table. The fake RREP craft parameters to the maximum value of the destination sequence number and the minimum available to the hop count. That makes an adversary to appear as the one preserving the best path to the destination. This is because AODV will interpret this node as the next hop in the path. The source which receives the fake RREP forwards all data packets to the Black Hole. These packets are then dropped instead of being forwarded to the destination [20]-[24].

This attack might have devastating effects in VANETs as each data packet, which may include alarms as well as emergency messages, needs to be delivered to the destination within limited time constraints [25]-[28]. The higher the speed, the more dangerous the attack is, as dropping all or even some data packets in high dynamic scenarios causes failure in the end to end communication that can lead to accidents and fatalities.

A lot of research and experiments have been performed on the isolation and detection of Black Hole Attacks for MANETs through AODV. Due to many similarities that exist between MANETs and VANETs, solutions proposed for MANETs, are extended to VANETs by researchers [29]-[31]. Since we are considering ACVs, which are a sub-class of VANETs and carry all of their features, solutions proposed in the literature can also be considered for ACVs. However, one crucial aspect of ACVs is autonomy, i.e. a reduction in the degree of human intervention in driving. When it comes to driverless cars the attack surface is expanded due to the different levels of control on car safety and operational functions than those controlled by drivers. Regarding this important factor, there is a big research gap in the field of ACVs. Keeping this aspect into consideration, solutions for the detection of Black Hole attacks that have already been proposed for MANETs and VANETs cannot be directly applied to ACVs. Rather, some improvements need to be made.

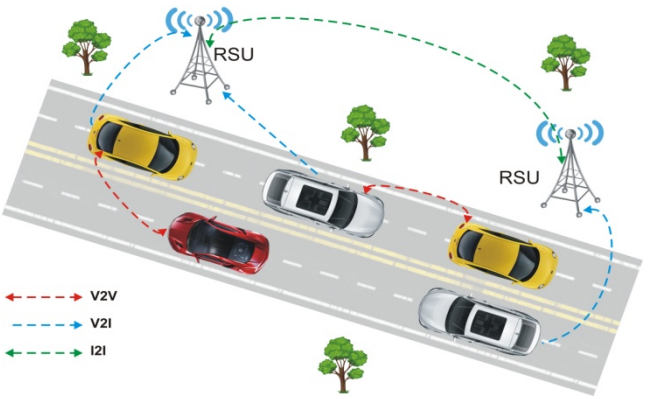


**FIGURE 1.** Basic VANET architecture

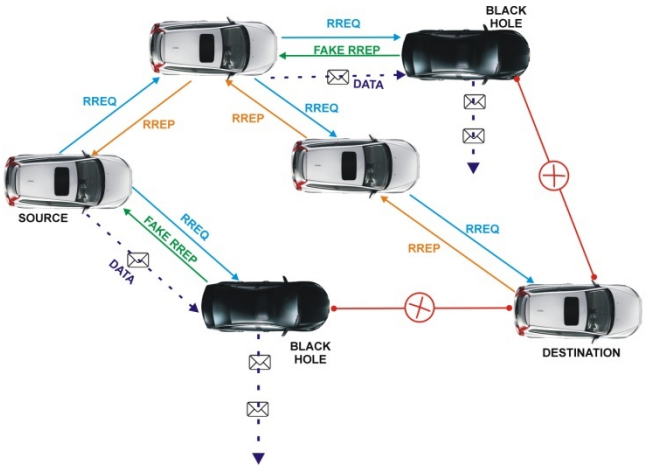


**FIGURE 2.** The Black Hole Attack

In this paper, we propose a detection algorithm IDBA. All Parameters that Black Hole exploits are precalculated in this technique. To make the detection intelligent, 802.11p is used at the mac layer. Since 802.11p is employed for Intelligent Transport Systems (ITS), that is why any technique utilising 802.11p would be named as intelligent by definition.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3034327, IEEE Access



Additionally, four main parameters that have never been combined for Black Hole detection are collectively configured in our security algorithm. These are Hop Count, Destination Sequence Number, Packet Delivery Ratio, and End-to-End delay.

The rest of the paper is structured as follows: Section II gives existing works published in public literature. Section III gives mathematical modeling of the Black Hole attack. Section IV is based on the overall proposed methodology. In Section V, simulation results are given. Section VI presents the conclusions and future directions for research.

## II. BACKGROUND AND RELATED WORK

Security is considered a main area of research in the domain of MANETs and VANETs. In the past years, various researchers took keen interest and gave several solutions for the improvement of security mechanisms in routing for Ad hoc Networks. Table 1 provides a brief overview of the comparison among the different state of the art Black Hole detection techniques.

In [32], Hortelano *et al*. elaborated on the watchdog mechanism for VANETs. In their mechanism, if source node A transmits some packets to intermediate node B, then A can verify if B forwarded the packets or not by continuously listening to node B's transmission. Every vehicle utilises a trust neighbour level for each neighbour vehicle. This can be calculated by the ratio of the packets sent to a neighbour to packets that are forwarded by the neighbour. Hence if a malicious vehicle continuously drops packets and it reaches the calculated level, then it is declared as a Black Hole.

In [33], Delkesh *et al*. proposed a heuristic approach to detecting Black Hole attacks in MANETs. The technique was used for MANET but equally applies to VANET as this is a heuristic approach and offers a generalised scheme based on fake IP address crafting techniques. The technique is often used to send forged packets in the AODV route discovery. Since a Black Hole never consults its routing table before sending back a reply to the requesting node, as a result, a Black Hole is trapped by replying to the requested fake destination IP address which never existed in the network. In this way detection of both single and cooperative Black Hole attacks occurred.

In [34], Daeinabi *et al*. developed an algorithm that was based on car monitoring. In their solution, vehicles are grouped into different clusters led by a cluster head (CH) which is the most reliable car in each cluster. Whenever any vehicle joins the cluster, the verifier begins their scanning about the behaviors of the joined vehicle. If the verifier notices that the vehicle is continuously dropping packets, then it reports to CH. Subsequently, CH decreases the trust value of the vehicle and also informs the neighbours of the vehicle. If somehow that trust value becomes lesser than a pre-defined threshold, CH directly reports to a certificate authority (CA), and the CA adds the vehicle to the Black List. It then informs all the vehicles to stop communicating with that Black Listed node. The experimental result shows that the proposed solution can detect malicious attackers at very high movements. In [35] the prevention mechanism is added to [34], and the selection of the verifier is improved in [36].

In [35], Kadam et al. made improvements to the algorithm proposed in [34] by adding the prevention and isolation mechanism of a Black Hole from the network. Almost the entire algorithm proposed in [35] is the same as in [34]. The difference lies in the additional parameter used for the isolation of an attacker and the alarm used, which is contained in the identity of the malicious node broadcasted across the network. The proposed technique could prevent and detect attackers at high mobility compared to [34].

In [36], Uzma *et al*. enhanced the detection mechanism proposed in [34] by improving the selection of the verifiers based on Load, Distrust Value, and Distance. Simulation results have shown improvements in performance metrics as compared to those shown in [34].

In [37], Yao *et al*. derived a solution for the detection of selfish nodes for Quality of Service and Optimized Link State Routing (QOS-OLSR). Each car utilises three parameters of trust. Every vehicle estimates its direct trust value to its neighbour's vehicle. Then a recommendation value is calculated based on a previously calculated trust value. Thirdly the comprehensive trust value is made by combining the direct trust value and recommendation value. If a vehicle's comprehensive calculated trust value is less than the threshold, then the neighbour vehicle is declared as an attacker.

In [38], Wahab *et al*. used the concept of watchdog technique to detect selfish behaviors with a Black Hole. The technique proposed has got five phases. The first phase is known as the *reputation phase* for calculation. In this phase, initial reputation values are given to the vehicles. Multipoint Relay (MPR) vehicles are chosen by the cluster heads to forward data to different clusters. Next, is the watchdog phase for monitoring in which cluster members analyse the work of MPR nodes. The third phase is known as the *voting phase based on aggregation,* CH uses a voting technique and collects analysed data from the cluster members to check the trustworthiness of MPR. The fourth phase is the *Tit for Tat* phase for cooperation and regulation in which the reliability of MPR is checked by comparing it with a precalculated threshold value. The fifth phase is the *information propagation phase*, CH shares information about MPR to the cluster members and other CHs. Based on this, a member vehicle marks those vehicles as a Black Hole which were determined as malicious.

In [39], Baiad *et al*. gave a solution by utilising a watchdog scheme in an efficient way in which monitoring has been deployed to both network and data link layers for the detection of a Black Hole that targets the Multipoint Relays (MPRs). Authors in [39] used the mechanism in [40] where the monitoring is deployed on the network layer to avoid a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3034327, IEEE Access



wrong accusation of innocent nodes i.e. loss of packets, because of normal collisions. So to minimise the level of the false-positive ratio, the information about the detection of the attacks is further scanned with the help of data link monitoring. If the RTS sent are different from the CTS received, then packet losses have occurred due to the normal collisions. False positives escalated because of an increase in packet loss caused by the normal collision of legitimate nodes. In [41], the authors expanded their cross-layer detection scheme by merging the physical layer monitoring process side by side with the MAC and network layer monitoring.

In [42], Arwind *et al*. designed an algorithm for Gray and Black Hole nodes detection in MANETs. They implemented their security on the AODV MAC layer. They introduced two control packets, Response sequence (Rseq) and Code Sequence (Cseq). When any source wants to discover a route and access a channel, it first sends Cseq to all its neighbours, and in turn, the neighbour replies with Rseq. If both Cseq and Rseq match a particular neighbour then the connection to the network layer is established; otherwise, a source node discards that neighbour node and also informs others about that neighbour as a malicious node.

In [43], Li *et al*. gave a Trust Management Scheme in which the reliability of data in VANETs is evaluated by detecting the attacker nodes. In this algorithm, data was collected from various vehicles to make a prediction for data to be trusted. The solution is divided into two steps: analysis of data and management of the trust. In the analysis of data, data is collected from various vehicles and utilising Dempster-Shafer theory.

In [44], Alheeti *et al*. gave an intrusion detection system (IDS) for the detection of DoS and Black Hole attacks in VANETs. This work was proposed for the security of communication in autonomous cars. The algorithm is based on Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) for the prediction of the attack, which is based on the observation of the vehicle's behaviour. The results were generated by carrying out data fuzzification, which indicated the behaviour of different vehicles as normal or malicious. After the detection process, different mobility scenarios were generated.

In [45], Alheeti *et al*. developed an Intrusion Detection System (IDS) which was dependent on a dataset gathered from the trace files that were extracted by running the NS2 coding in the VANET environment. Trace files were divided into *"basic trace", "internet protocol trace" and "AODV trace"*. The characteristics extracted from the trace files were utilised to evaluate the proposed solution. These features were used as the criteria to decide whether the behaviour of vehicles is malicious or normal. A statistical method was used for feature extraction named Proportional Overlapping Scores (POS).

In [47], Cai *et al*. proposed a path based solution for Gray and Black Hole attack detection. In the proposed work, every node keeps a FwdPktBuffer. The algorithm executes over three stages. In the first stage, forwarded packets are added into the packet buffer, and the source node starts listening. In the second stage, when a neighbour forwards packets and is listened by the source node, the stored packets from the buffer of the source node will be released. In the third stage, the source node compares the overheard rate with the precalculated threshold value to declare the neighbour as a legitimate node or an attacker, who continuously drops the data packets.

In [48], Tyagi *et al*. introduced a three-phase algorithm for the detection of Black Hole. Under the first phase, RSU plays the role of a certificate authority (CA) which maintains and generates a public and private key as well as certificates for the vehicles. Before the start of any communication, vehicles have to be verified from the RSU. In the second phase, the source broadcasts RREQ along with the correct certificate, nonce encryption, and destination's public key. The destination sends RREP back with the source's public key. In the third phase, Black Hole vehicles are detected based on the threshold of the destination sequence numbers, extracted from the RREPs, which are stored in the data structure used in the algorithm called Heaps.

## III. MATHEMATICAL PROOF OF VEHICLE'S ISOLATION FROM COMMUNICATION UNDER BLACK HOLE ATTACK

In this section, we present the mathematical modeling of the Black Hole attack with emphasis placed upon vehicle isolation and presence attributes during the attack.

### A. SYSTEM SCENARIO ASSUMPTIONS AND SUPPOSITIONS

In our work, we assume that all vehicles are equally distributed in an urban scenario over a 2-dimensional area. The radius of transmission r is the same for all vehicles. Vehicle v is considered as a neighbour node of vehicle u, if and only if, a distance of transmission between them is $\leq$ r. All vehicles have a constant speed. Source and destination within 2 hops having three lanes are considered, as shown in Figure 3. By taking 2-hops, each vehicle is supposed to detect the attacker within 2-hop cars surrounding, which eliminates the probability for a high-speed attacker to escape the range before detection. All vehicles run a single algorithm that participates in communication. It is assumed that there is little or even no intervention of humans in driving. We further assume two types of vehicles named Black Hole and Cooperative. Cooperative vehicles are those that follow the instructions of routing protocol in the route discovery process and data packets forwarding. In contrast,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3034327, IEEE Access



Black Hole vehicles violate the instructions of the routing protocol, hence drop data packets. T(V) is used to denote a network, where

$$V = V_C \cup V_B \quad (1)$$

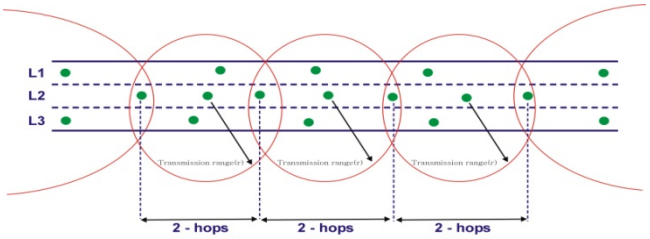


**FIGURE 3.** System Scenario

**TABLE 1.** Comparison among Various Black Hole Detection Techniques

| Author, Publisher, and year | Detection Techniques | Scenario/Citations | Simulators Used | Performance Metrics | Limitations |
|---|---|---|---|---|---|
| **Hortelano et al. IEEE (2010) [32]** | Watchdog based IDS | VANET/85 | CASTADIVA | False positive and false negative | High false detection rate |
| **Delkesh et al. Springer (2019) [33]** | Heuristic approach using Fake Destination IP Address | MANET/12 | NS-2.34 | PDR, E2E, overhead, packet loss rate, and throughput | Algorithm fails if network is being scanned by the attacker using a network analyser. Also, hop count is not mentioned |
| **Daeinabi et al. Springer (2013) [34]** | DMV | VANET/61 | Not mentioned | PDR and packet duplication | High jitter and high E2E |
| **Kadam et al. Springer (2014) [35]** | D&PMV | VANET/7 | NS-2 | Average throughput, packets dropped, E2E and jitter | Consumes more time for processing |
| **Uzma et al. Springer (2015) [36]** | DMN | VANET/71 | NS-2 | Average throughput, PDR, and E2E | The technique may be enhanced for isolation process |
| **Yao et al. Elsevier (2017) [37]** | Entity-Centric Trust Model | VANET/54 | VanetMobiSim | PDR, average path length, and E2E | Data trust model can be improved in utility and default parameters |
| **Wahab et al. Springer (2014) [38]** | Dempster-Shafer Based Tit-for-Tat | VANET/25 | Matlab-9.0,VanetMobiSim | False negative and detection rates | Extra processing is required |
| **Baiad et al. IEEE (2014) [39]** | Novel cross-layer intrusion detection | VANET/17 | Matlab-8.0 | False positive and detection rates | Detection rates can be increased by adding physical and transport layer monitoring |
| **Arwind et al. Elsevier (2015) [42]** | MAC layer monitoring using Control packets | MANET/34 | NS-2 | PDR and E2E | High routing overhead |
| **Li et al. IEEE (2016) [43]** | ART | VANET/209 | GloMoSim-2.03 | Precision and Recall | High processing overhead when no.of malicious nodes increases |
| **Alheeti et al. Elsevier (2017) [44]** | Linear Quadratic Discriminant Analysis with data Fuzzification | VANET (Autonomous Vehicles)/17 | NS-2, SUMO, MOVE | PDR, E2E, average throughput, false positive, false negative, true positive, and true negative rates | Error rates can be reduced by enhancing RSU's with intelligent IDS and cars using AI techniques |
| **Alheeti et al. IEEE (2015) [45]** | Proportional Overlapping Scores (POS) | VANET (Autonomous Vehicles)/44 | NS-2, SUMO, MOVE | False positive rate, false negative rate, true positive rate, and true negative rate | System needs extra memory resources |
| **Kumar et al. Elsevier (2015) [46]** | Sequence Number threshold-based | MANET/51 | NS-2.34 | Packet delivery ratio and throughput | Can be improved by adding the threshold for Hop Count with the Sequence Number |
| **Cai et al. IEEE (2010) [47]** | Path-based detection algorithm | Wireless Ad Hoc Networks/127 | NS-2 | Packet delivery rate, collision rate, detection rate, and false positive rate | Less rate of competitive detection |
| **Tyagi et al. Springer (2018) [48]** | ES-AODV | VANET/5 | NCTUns | PDR, E2E, routing overhead, average throughput, packets dropped, and packet collision | Security for RSU's may be deployed to avoid compromisation of certificates and key pairs of the vehicles |

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3034327, IEEE Access



### B. VEHICLE BEHAVIOR'S STOCHASTIC PROPERTIES

A random process is defined to be a Markov process if for a given value of W(t), the value of W(a) for a > t does not depend on the values of W(b) for b < t [49]. This means future results of the process do not depend on past values but present values. If a stochastic or random process at time $t_n$ is state $W_n$, the future state $W_{n+1}$ at time $t_{n+1}$ depends only on the present state $W_n$ and not on the past states $W_{n-1}$, $W_{n-2}$,....., $W_0$. The sequence of states $\{W_n\}$ is called a Markov chain. Any vehicle can be modeled according to the proposed model as in the connected state (CS) and isolated state (IS). A vehicle can be either in any one of these states in the presence of Black Hole. A two-state Markov model is given in Figure 4. Variables x and y for the vehicle K at time instant i are formally defined as:

$$x = P[K_i = IS | K_{i-1} = CS] \quad (2)$$

$$y = P[K_i = CS | K_{i-1} = IS]$$

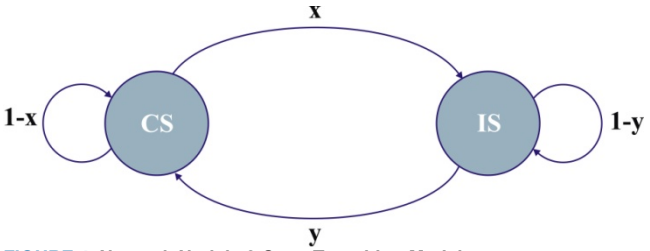


**FIGURE 4. Network Node's 2-State Transition Model.**

So the state of K as any instant i is given by

$$K_i = \begin{cases} CS, & \text{if } y = V_C \geq 1 \text{ and } x = V_B = 0 \\ IS, & \text{otherwise} \end{cases} \quad (3)$$

where $V_C$ and $V_B$ represent the number of Cooperative and Blackhole vehicles.

Let's suppose that the probability of the two-state model be $P_S = [P_{CS}, P_{IS}]$. By solving a set of linear equations (2) and (3), this vector can be obtained.

$$D.P_S = P_S \quad (4)$$

Here probability transition matrix is represented by D.

$$P_{CS} + P_{IS} = 1 \quad (5)$$

**TABLE 2. 2-State Markov Chain's Probability Transition Matrix.**

| State | Connected | Isolated |
|---|---|---|
| Connected | 1 – x | x |
| Isolated | y | 1 – y |

By comparing and solving equations (4) and (5) we get

$$P_{CS} = \frac{y}{x+y} \quad \text{and} \quad P_{IS} = \frac{x}{x+y} \quad (6)$$

From (6) we can say that $P_{CS} = \frac{V_C}{V_C+V_B} = P_C$ and $P_{IS} = \frac{V_B}{V_C+V_B} = P_B$.

### C. VEHICLE'S ISOLATION UNDER BLACK HOLE ATTACK (PROBABILISTIC MODELING)

#### 1. LEMMA

A vehicle V is isolated from the network if at least it has one Black Hole neighbour, provided it has n neighbours [49].

According to Lemma, let $V_{(IS)}$ denotes that the vehicle is in an isolated state, then, the vehicle probability being in the isolated state provided that the vehicle has neighbours is given by:

$$\Pr(V_{(IS)} \mid D(v) = d) = \Pr(V_B \geq 1) = 1 - (1 - P_B)^d \quad (7)$$

### D. VEHICLE'S CONNECTIVITY PROBABILISTIC MODEL WITH THE NETWORK

A vehicle is in the connected state with the network if it has q-cooperative neighbours where $1 \leq q \leq d$. Given vehicle v with degree $D_{(v)} = d$, v is said to be in a q-connected state to the network if $D_{(c,v)} = q$ which is only true if v has q cooperative neighbours and no Black Hole neighbours where $D_{(c,v)}$ denotes the degree of cooperation of vehicle v. Hence the probability of vehicle v being q connected provided D(v) = d is given by:

$$\Pr(D_{(c,v)} = q | D_{(v)} = d) = \Pr(V_C = q, V_B = 0 | D = d) \quad (8)$$

According to Binomial Distribution

$$\Pr(D_{(c,v)} = q | D_{(v)} = d) = \binom{d}{q} P_C^q \quad (9)$$

Where the probability of cooperative neighbours is represented by $P_C = 1 - P_B$ which can also be written as

$$\Pr(V_{(CS)} | D_{(v)} = d) = \binom{d}{q} P_C^q \quad (10)$$

Suppose that N number of vehicles exist in a network M, then the condition which is necessary to be fulfilled for a network to remain in the q-connected state is that every vehicle must have at least q cooperative neighbours. Hence the probability for a vehicle to have at minimum q cooperative neighbours is given by:

$$\Pr(D_{(c,v)} \geq q) = \{1 - \Pr(D_{(c,v)} < q)\}^N \quad (11)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3034327, IEEE Access



### 1. POISSON'S MODEL TO PROVE MAXIMUM NETWORK CONNECTIVITY WHEN $P_B$=0

To calculate neighbour vehicle's distribution Pr(D(u)=d), we split a network of area A into N smaller blocks where each block size is equal to the vehicle's physical size and N represents the number of vehicles in area A. The distribution of Poisson can be used to model a vehicle's distribution as given:

$$\Pr\left(\mathrm{D}_{(\mathrm{v})}=\mathrm{d}\right)=\frac{\mu^{\mathrm{d}}}{\mathrm{d}}\mathrm{e}^{-\mu} \tag{12}$$

Where an average number of vehicles is denoted by $\mu$ within the area and vehicle's transmission range. Value of $\mu = \rho\pi r^2$ and $\rho = \frac{N}{A}$ which denotes the vehicle's density in the network of area A.

Applying the Total Probability Law on (9) and (12), we get

$$\Pr\left(\mathrm{D}_{(\mathrm{c,v})}=\mathrm{q}\middle|\mathrm{D}_{(\mathrm{v})}=\mathrm{d}\right)=\sum_{\mathrm{d=q}}^{\mathrm{N-1}}\binom{\mathrm{d}}{\mathrm{q}}(1-\mathrm{P_B})^{\mathrm{q}}\,\frac{\mu^{\mathrm{d}}}{\mathrm{d}}\mathrm{e}^{-\mu} \tag{13}$$

$\Pr(\mathrm{D}_{(\mathrm{c,v})}<\mathrm{q})$ can be derived using (13) as follows:

$$\Pr\left(\mathrm{D}_{(\mathrm{c,v})}<q\middle|\mathrm{D}_{(\mathrm{v})}=\mathrm{d}\right)\approx\sum_{\mathrm{m=0}}^{\mathrm{q-1}}\sum_{\mathrm{d=q}}^{\mathrm{N-1}}\binom{\mathrm{d}}{\mathrm{m}}(1-\mathrm{P_B})^{\mathrm{m}}\,\frac{\mu^{\mathrm{d}}}{\mathrm{d}}\mathrm{e}^{-\mu} \tag{14}$$

$$\approx\frac{\boldsymbol{\Gamma(\mathrm{q},\mu(1-\mathrm{P_B}))}}{\boldsymbol{\Gamma(\mathrm{q})}} \tag{15}$$

To obtain the probability of a vehicle to have at least q cooperative degree vehicles, substituting (15) in (11) as follows:

$$\Pr\left(\mathrm{D}_{(\mathrm{c,v})}\geq\mathrm{q}\right)=\left\{1-\frac{\boldsymbol{\Gamma(\mathrm{q},\mu(1-\mathrm{P_B}))}}{\boldsymbol{\Gamma(\mathrm{q})}}\right\}^{\mathrm{N}} \tag{16}$$

Where

$$\Gamma(\alpha,\beta)=(\alpha-1)!\,e^{-\beta}\sum_{i=0}^{\alpha-1}\binom{\beta^i}{i!}$$

$\alpha \epsilon N$ gives the incomplete gamma function and $\Gamma(q) = (q-1)!$ gives the complete gamma function. Nevertheless, the network can have maximum connectivity if and only if $\mathrm{P_B} = 0$ provided that A, N, and q have fixed values.

## IV. PROPOSED TECHNIQUE

Our proposed solution IDBA uses four main parameters in which two of them are sequence number and hop count. The Black Hole exploits these two to damage the availability and integrity of the network. The other two parameters are outputs of the network performance that are degraded as a result of the attack on the first two parameters. So by combining these four parameters and precalculating the thresholds regarding the future actions of the Black Hole, we achieved to detect the attack according to Algorithm 1 more efficiently as compared to others' work. IDBA process is shown in Figure 5.

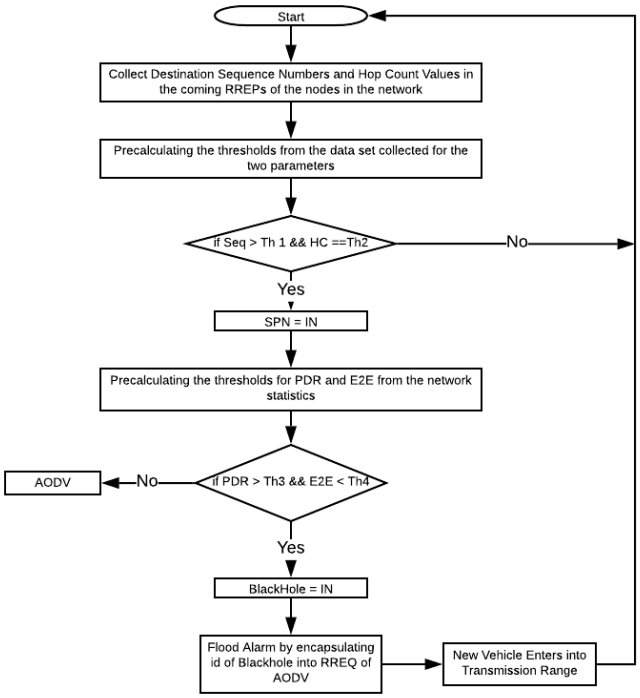


**FIGURE 5. IDBA detection process**

### A. IDBA DETECTION PARAMETERS

#### 1) SEQUENCE NUMBER

The sequence number is one of the main metrics of AODV based on which a node decides which route it has to mark fresh to transmit its data. Black Hole compromises this metric by setting the destination sequence number to a maximum possible value to elude the source to believe that a different node than the legitimate should be the next hop. Algorithm 2 has been used to find the threshold for the destination sequence number and make the distinction between an attack or not manifested in the network. Any Precalculations of the destination sequence numbers generated both by the normal nodes and the malicious nodes are done according to Algorithm 2.

#### 2) HOP COUNT

The second main metric considered in our work is the hop count value. Lower count leads to a fresher route. A Black Hole advertises this metric as low as 2 side by side with the destination sequence number to the source to mark itself as next-hop [50].

### 3) PACKET DELIVERY RATIO AND END TO END DELAY

The threshold values for these two parameters are calculated according to the procedure adopted in [33]. Advantage has been taken of the claim made by the authors that their solution can also be considered for a majority of ad hoc networks under the hierarchy of which ACVs also fall [51]-[54].

**Algorithm 1:** Black Hole Detection

1. **Input**: n, $\alpha_{th}$, $\beta_{th}$, $\gamma_{th}$, $H_c$, ID_RREP$_z$_B
2. **begin**
   **for**(i=1; i<=n; i++)
   **if** {(DS_RREP$_z$ > $\alpha_{th}$) && ($H_c$ == 2)} **then**
3. G ← RREP$_z$
   goto step 5
   **else**
4. goto start
   **end**
5. **if** {(PDR < $\beta_{th}$) && (E2E > $\gamma_{th}$)} **then**
6. B ← G
7. RREQ ← ID_RREP$_z$_B
8. Alarm ← RREQ
9. Flood Alarm
   **else**
10. AODV();
   **end**
   **end**
   **end**

**Algorithm 2:** Sequence Number Threshold Precalculation

1. **Input**: Sum, z, DS_RREP$_z$ , DS_RREQ, n
2. **start**
3. Sum ← 0
   **for** each reply [z] do
   **if** (DS_RREP$_z$ > DS_RREQ) **then**
4. D ← DS_RREP$_z$ – DS_RREQ
5. Sum ← Sum+D
   D ← 0
   **else**
6. AODV();
   **end**
   **end**
7. $\alpha_{th} \leftarrow \frac{Sum}{n}$
   **end**

## V. SIMULATION ENVIRONMENT, PARAMETERS, AND RESULTS

Simulations are performed for our proposed technique using NS2 (v2.34) network simulator 2. We compared our approach with B-AODV, Ids-AODV, and EAODV algorithms. EAODV was offered for MANETs. However, authors of [33] additionally claimed that the technique could be applied to a vast majority of ad hoc networks. Advantage has been taken of their argument as discussed in the previous paragraph, and results are compared to [33]. Also, if the attacker had scanned a network, EAODV would have failed, would not be the case when IDBA was considered in the same scenario.

**TABLE 3.** *Notations and Descriptions.*

| Notations | D E S C R I P T I O N S |
|---|---|
| $V_B$ | Black Hole vehicles |
| $V_C$ | Cooperative vehicles |
| V | Total number of Black Hole and Cooperative vehicles |
| $P_{CS}$ | Probability of a vehicle in a connected state |
| $P_{IS}$ | Probability of a vehicle in an isolated state |
| $P_S$ | Total probability of a vehicle either in a connected or isolated state |
| $P_C$ | Probability of Cooperative vehicles |
| $P_B$ | Probability of Black Hole vehicles |
| $V_{IS}$ | Vehicle in an isolated state |
| $V_{CS}$ | Vehicle in a connected state |
| $D_{(V)}$ | Degree of a vehicle connected with the network |
| $D_{(C, V)}$ | Degree of a vehicle connected with the cooperative vehicles of the network |
| $\mu$ | The average number of vehicles |
| $\rho$ | Vehicle density |

**TABLE 4.** *Notations and Descriptions.*

| Notations | D E S C R I P T I O N S |
|---|---|
| RREQ | Route Request |
| RREP | Route Reply |
| RREP$_z$ | Route Reply generated by a node who received RREQ |
| D | The difference of sequence number generated by a neighbour and source |
| DS_RREQ$_z$ | The sequence number of destination generated by a neighbour |
| DS_RREQ | Sequence number of destination generated by a source |
| ID_RREP$_z$_B | The ID of the attacker in the fake route reply sent by the Black Hole |
| $H_c$ | Hop count |
| $\alpha_{th}$ , Th1 | The threshold value for the Sequence number |
| $\beta_{th}$ , Th3 | The threshold value for PDR |
| $\gamma_{th}$ , Th4 | Threshold value for E2E |
| G | Variable to mark node in Gray List |
| B | Variable to mark Gray Listed node in Black List |
| n | Total number of vehicles/nodes |
| $P_S$ | Total number of packets sent |
| $P_R$ | Total number of packets received |
| $T_A$ | Arrive Time |
| $T_S$ | Sent Time |
| C | Total number of connections |
| Th2 | The threshold value for Hop count |
| IN | Intermediate Node |
| SPN | Suspicious Node |

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3034327, IEEE Access



### A. Packet Delivery Ratio (PDR)

PDR is the ratio of the total number of data packets received to the total number of data packets sent as given in Eq. 17.

$$PDR = \frac{\sum P_R}{\sum P_S} \quad (17)$$

### B. End-to-End Delay (E2E)

E2E is the average time required for the data packets to be delivered from the source to the destination, as shown in Eq. 18.

$$E2E = \frac{\sum (T_A - T_S)}{\sum C} \quad (18)$$

### C. Routing overhead (ROH)

ROH is defined as the number of packets that need to be processed and routed during network communication.

### D. Throughput

It is the average number of data packets delivered to the destination by the source.

### E. Packet loss rate (PLR)

PLR is defined as the difference between the data packets sent to the data packets received.

$$PLR = \sum P_S - \sum P_R \quad (19)$$

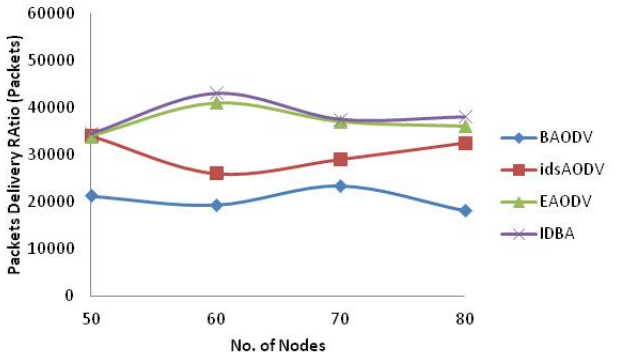


**FIGURE 6.** Packet delivery ratio in BAODV, idsAODV, EAODV and IDBA

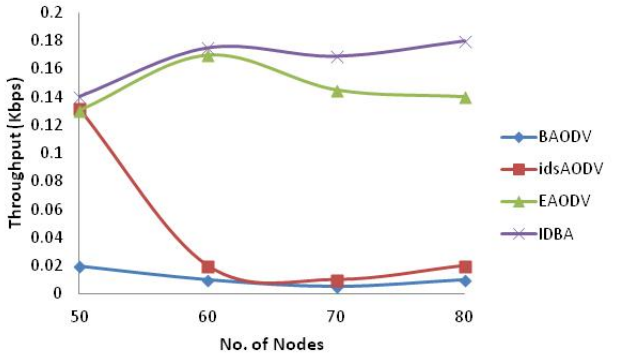


**FIGURE 7.** Throughput in BAODV, idsAODV, EAODV and IDBA

**TABLE 5.** *Simulation parameters*

| Parameters | Values |
|---|---|
| Standard Protocol | 802.11p |
| Simulation environment | 1000m x 1000m |
| Number of vehicles | 50 , 60, 70, 80 |
| Black Hole Attackers | Max. 4 |
| Simulation time | 500s |
| Vehicle's speed | Max. 30 m/s |
| Packets size | 512b/s |
| Routing Agent | UDP/CBR |
| Range of Transmission | 250 m |
| Base Routing Protocol | AODV |
| The threshold used for the packet delivery ratio | 35,000 packets |
| The threshold used for end to end delay | 0.01 s |

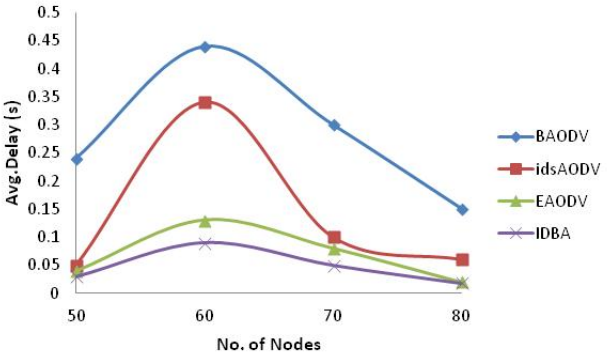


**FIGURE 8.** End-to-End delay in BAODV, idsAODV, EAODV and IDBA

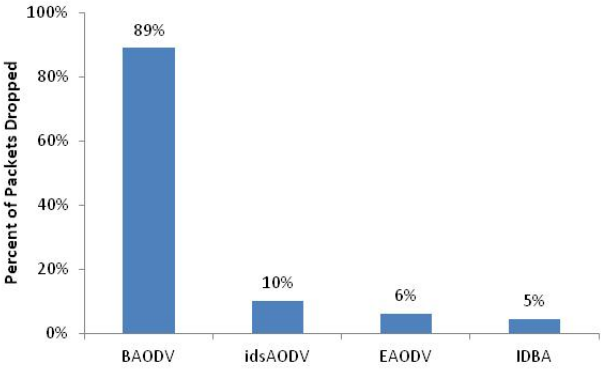


**FIGURE 9.** The packets loss rate in BAODV, idsAODV, EAODV and IDBA

Fig. 6 shows the variations in the PDR according to the number of nodes and gives a maximum value when nodes are 60. Nevertheless, for every node check, IDBA gives a high PDR rate than EAODV and other algorithms. Variations in the values of PDR are due to the network conditions. There were pre-defined thresholds used in our technique to check whether the path is clear from the attack, for the packets which are to be routed to the destination. Simulation results in Fig. 6 show that PDR with IDBA gives better results as compared to other algorithms.

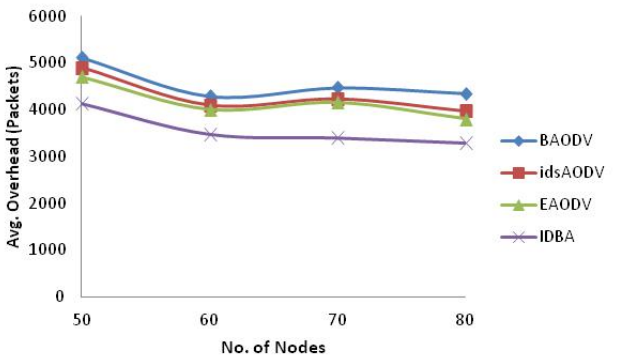


**FIGURE 10. Routing overhead in BAODV, idsAODV, EAODV and IDBA**

High PDR gives low E2E and optimal throughput. It is thus specifically evaluated in Fig, 7, and Fig. 8 that E2E and throughput give optimised results where PDR was higher in Fig. 6. This means that maximum packets are transmitted to the destination with less latency as compared to EAODV and other algorithms.

Fig. 9 shows the number of packets dropped. Since in BAODV, there were 4 malicious nodes without a detection algorithm, so the dropped packets reached 89%. IDBA, when under attack, gave a lower packet dropped rate as compared to BAODV and two detection algorithms i.e. idsAODV and EAODV. This can also be analysed from Fig.6 as the greater the PDR, the lower will be the rate of packets dropped.

Fig. 10 indicates that IDBA requires less number of packets that needs to be routed for network communication and hence reduces processing overhead as compared to other algorithms.

## VI. CONCLUSION AND FUTURE DIRECTIONS

Detection of the Black Hole attacks is becoming an indispensable issue with the exponential increase in car automation. Black Hole directly impacts communication, which is unacceptable when it comes to ACVs, where delay even in a single data packet can cause accidents. Thus, the deterring of these attacks is imperative.

To ensure secure autonomous vehicular applications, i.e. comfort, safety, and transport of the vehicles and passengers, we proposed and tested our solution which gave more satisfactory results in terms of PDR, E2E, PLR, ROH, and Throughput against existing solutions. For this reason, our technique could be deployed for real-world scenarios that would minimise the number of accidents.

The proposed technique can be enhanced by combining smart clustering techniques to deter Black Hole Attacks.

**ACKNOWLEDGMENTS:** This research was funded by EPSRC through the grants EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research - University of Warwick), EP/N510129/1 (The Alan Turing Institute), EP/R029563/1 (Autotrust), and EP/S035362/1 (PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity).

## REFERENCES

[1] A. Kumar and M. Sinha, ""Design and development of new framework for detection and mitigation of wormhole and black hole attacks in VANET"", *Journal of Statistics and Management Systems*, vol. 22, no. 4, pp. 753-761, 2019.

[2] Tyagi and D. Dembla, ""A secured routing algorithm against black hole attck for better intelligent transportation system in vehicular ad hoc network"", *International Journal of Information Technology*, vol. 11, no. 4 pp. 743-749, 2019.

[3] K. Ali Alheeti and K. McDonald-Maier, ""Intelligent intrusion detection in external communication systems for autonomous vehicles"", *Systems Science & Control Engineering*, vol. 6, no. 1, pp. 48-56, 2018.

[4] P. Gautham and R. Shanmughasundaram, ""Detection and isolation of Black Hole in VANET"", *International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, India, 2017, pp. 1534-1539.

[5] W. Ben Jaballah, M. Conti, M. Mosbah and C. Palazzi, ""The impact of malicious nodes positioning on vehicular alert messaging system"", *Ad Hoc Networks*, vol. 52, pp. 3-16, 2016.

[6] D. Tian, J. Zhou, Y. Wang, G. Zhang and H. Xia, ""An adaptive vehicular epidemic routing method based on attractor selection model"", *Ad Hoc Networks*, vol. 36, pp. 465-481, 2016.

[7] G. Lee, G. Epiphaniou, H. Al-Khateeb and C. Maple, ""Security and Privacy of Things: Regulatory Challenges and Gaps for the Secure Integration of Cyber-Physical Systems"", *Advances in Intelligent Systems and Computing*, Springer, Singapore, 2018, pp. 1-12.

[8] F. Hagenauer, T. Higuchi, O. Altintas and F. Dressler, ""Efficient data handling in vehicular micro clouds"", *Ad Hoc Networks*, vol. 91, p. 101871, 2019.

[9] V. Gayathri and P. Supraja, ""Optimised RBIDS: detection and avoidance of black hole attack through NTN communication in mobile ad hoc networks"", International Journal of Computer Aided Engineering and Technology, vol. 13, no. 12, p. 4, 2020.

[10] N. Panda and B. Kumar Pattanayak, ""Energy aware detection and prevention of black hole attack in MANET"", International Journal of Engineering & Technology, vol. 7, no. 26, p. 135, 2018.

[11] M. Trivedi and S. Malhotra, ""Identification and Prevention of Joint Gray Hole and Black Hole Attacks"", *International Journal of Ambient Computing and Intelligence*, vol. 10, no. 2, pp. 80-90, 2019.

[12] O. Wahab, H. Otrok and A. Mourad, ""VANET QoS-OLSR: QoS-based clustering protocol for Vehicular Ad hoc Networks"", *Computer Communications*, vol. 36, no. 13, pp. 1422-1435, 2013.

[13] M. Singh and P. Singh, ""Black Hole Attack Detection in MANET Using Mobile Trust Points with Clustering"", *International conference on smart trends for information technology and computer communications*, Springer, Singapore, 2016, pp. 565-572.

[14] A. Mehmood, A. Khanan, A. Mohamed, S. Mahfooz, H. Song and S. Abdullah, ""ANTSC: An Intelligent Naïve Bayesian Probabilistic Estimation Practice for Traffic Flow to Form Stable Clustering in VANET"", *IEEE Access*, vol. 6, pp. 4452-4461, 2018.

[15] K. Ghafoor, K. Abu Bakar, J. Lloret, R. Khokhar and K. Lee, ""Intelligent beaconless geographical forwarding for urban vehicular environments"", *Wireless Networks*, vol. 19, no. 3, pp. 345-362, 2013.

[16] S. Al-Sultan, M. Al-Doori, A. Al-Bayatti and H. Zedan, ""A comprehensive survey on vehicular Ad Hoc network"", *Journal of Network and Computer Applications*, vol. 37, pp. 380-392, 2014.

[17] K. Ghafoor, M. Mohammed, J. Lloret, K. Bakar and Z. Zainuddin, ""Routing Protocols in Vehicular Ad hoc Networks: Survey and Research Challenges"", *Network Protocols and Algorithms*, vol. 5, no. 4, pp. 39-83, 2013.

[18] K. Premkumar and R. Baskaran, ""The Data Dissemination Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks"", *International Journal of Computer Sciences and Engineering*, vol. 7, no. 7, pp. 7-13, 2019.

[19] N. Fan and C. Wu, ""On trust models for communication security in vehicular ad-hoc networks"", *Ad Hoc Networks*, vol. 90, p. 101740, 2019.

[20] V. Jindal and P. Bedi, ""Vehicular Ad-Hoc Networks: Introduction, Standards, Routing Protocols and Challenges"", *International Journal of Computer Science Issues*, vol. 13, no. 2, pp. 44-55, 2016.

[21] T. Darwish and K. Abu Bakar, ""Traffic density estimation in vehicular ad hoc networks: A review"", *Ad Hoc Networks*, vol. 24, pp. 337-351, 2015.

[22] B. Mokhtar and M. Azab, ""Survey on Security Issues in Vehicular Ad Hoc Networks"", *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115-1126, 2015.

[23] T. Qiu, N. Chen, K. Li, D. Qiao and Z. Fu, ""Heterogeneous ad hoc networks: Architectures, advances and challenges"", *Ad Hoc Networks*, vol. 55, pp. 143-152, 2017.

[24] S. Shahabi, M. Ghazvini and M. Bakhtiarian, ""A modified algorithm to improve security and performance of AODV protocol against black hole attack"", *Wireless Networks*, vol. 22, no. 5, pp. 1505-1511, 2015.

[25] W. Liang, Z. Li, H. Zhang, S. Wang and R. Bie, ""Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends"", *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, 2015.

[26] F. Sakiz and S. Sen, ""A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV"", *Ad Hoc Networks*, vol. 61, pp. 33-50, 2017.

[27] S. Singh, A. Mishra and U. Singh, ""Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm"", *Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore,India, 2016.

[28] E. Fazeldehkordi, I. Amiri, O. Akanbi and M. Neely, *A study of black hole attack solutions*. Waltham, MA: Elsevier, 2016.

[29] J. Cui, L. Liew, G. Sabaliauskaite and F. Zhou, ""A review on safety failures, security attacks, and available countermeasures for autonomous vehicles"", *Ad Hoc Networks*, vol. 90, p. 101823, 2019.

[30] Á. Guerrero-Higueras, N. DeCastro-García and V. Matellán, ""Detection of Cyber-attacks to indoor real time slocalisation systems for autonomous robots"", *Robotics and Autonomous Systems*, vol. 99, pp. 75-83, 2018.

[31] A. Dorri, S. Vaseghi and O. Gharib, ""DEBH: detecting and eliminating black holes in mobile ad hoc network"", *Wireless Networks*, vol. 24, no. 8, pp. 2943-2955, 2018.

[32] J. Hortelano, J. Ruiz and P. Manzoni, ""Evaluating the usefulness of watchdogs for intrusion detection in VANETs"", *IEEE International Conference on Communications Workshops,* Capetown, South Africa, 2010, pp. 1-5.

[33] T. Delkesh and M. Jabraeil Jamali, ""EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs"", *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, pp. 1-18, 2019.

[34] A. Daeinabi and A. Rahbar, ""Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks"", *Multimedia Tools and Applications*, vol. 66, no. 2, pp. 325-338, 2013.

[35] M. Kadam and S. Limkar, ""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*, 2014, pp. 379-387.

[36] U. Khan, S. Agrawal and S. Silakari, ""Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks"", *Procedia Computer Science*, vol. 46, pp. 965-972, 2015.

[37] X. Yao, X. Zhang, H. Ning and P. Li, ""Using trust model to ensure reliable data acquisition in VANETs"", *Ad Hoc Networks*, vol. 55, pp. 107-118, 2017.

[38] O. Wahab, H. Otrok and A. Mourad, ""A Dempster–Shafer Based Tit-for-Tat Strategy to Regulate the Cooperation in VANET Using QoS-OLSR Protocol"", *Wireless Personal Communications*, vol. 75, no. 3, pp. 1635-1667, 2014.

[39] R. Baiad, H. Otrok, A. Mourad and J. Bentahar, ""Cooperative cross layer detection for blackhole attack in VANET-OLSR"", in *Wireless Communications and Mobile Computing Conference (IWCMC)*, Nicosia, Cyprus, 2014, pp. 863-868.

[40] H. Sanadiki, H. Otrok, A. Mourad and J. Robert, ""Detecting attacks in QoS-OLSR protocol"", *9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Sardinia, Italy, 2013, pp. 1126-1131.

[41] R. Baiad, O. Alhussein, H. Otrok and S. Muhaidat, ""Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET"", *Vehicular Communications*, vol. 5, pp. 9-17, 2016.

[42] A. Dhaka, A. Nandal and R. Dhaka, ""Gray and Black Hole Attack Identification Using Control Packets in MANETs"", *Procedia Computer Science*, vol. 54, pp. 83-91, 2015.

[43] W. Li and H. Song, ""ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks"", *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960-969, 2016.

[44] K. Alheeti, A. Gruebler and K. McDonald-Maier, ""Using discriminant analysis to detect intrusions in external communication for self-driving vehicles"", *Digital Communications and Networks*, vol. 3, no. 3, pp. 180-187, 2017.

[45] K. Alheeti, A. Gruebler and K. Maier, ""An intrusion detection system against black hole attacks on the communication network of self-driving cars"", in *IEEE*, Braunschweig, Germany, 2015, pp. 86-91.

[46] V. Kumar and R. Kumar, ""An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network"", *Procedia Computer Science*, vol. 48, pp. 472-479, 2015.

[47] J. Cai, P. Yi, J. Chen, Z. Wang and N. Liu, ""An adaptive approach to detecting black and gray hole attacks in ad hoc network"", *24th IEEE International Conference on Advanced Information Networking and Applications*, Perth, WA, Australia, 2010, pp. 775-780.

[48] P. Tyagi and D. Dembla, ""Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network"", *Wireless Personal Communications*, vol. 102, no. 1, pp. 41-60, 2018.

[49] M. Mohanapriya, "Detection and elimination of black hole attacks in mobile ad hoc networks," Ph.D. dissertation, Dept. Infor. and Comm Eng., Anna Univ., Chennai, April. 2014.

[50] M. Yassein, Y. Khamayseh and M. AbuJazoh, ""Feature Selection for Black Hole Attacks"", *Journal of Universal Computer Science*, vol. 22, no. 4, pp. 521-536, 2016.

[51] A. Rana, A. Aldegheishem, M. F. Majeed, A. Mehmood, H. Maryam, N. Alrajeh, M. Carsten, and M. Jawad. ""An Effective Mechanism to Mitigate Real-time DDoS Attack Using Dataset"." *IEEE Access*, vol.8, pp. 126215-126227, 2020.

[52] X. Liu et al., ""Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks"", *Journal of Parallel and Distributed Computing*, vol. 135, pp. 140-155, 2020.

[53] Y. Liu, X. Liu, A. Liu, N. Xiong and F. Liu, ""A Trust Computing-based Security Routing Scheme for Cyber Physical Systems"", *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 6, pp. 1-27, 2019.

[54] Y. Liu, M. Dong, K. Ota and A. Liu, ""ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks"", *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013-2027, 2016.