AN EFFECTIVE DYNAMIC SOLUTION FOR BLACK HOLE ATTACK DETECTION AND PREVENTION IN VANETS

Paramjit[1*], Dr.Saurabh Charya[2]

Abstract
Significant progress in automotive ad hoc networks has been made due to the rapid and considerable advancements in wireless technologies, downsizing, and Internet of Things (IoT) technologies (VANETs). The current intelligent traffic system relies heavily on VANETs and the Internet of Things (ITS). Yet, because of its dynamic nature, decentralised nature, protocol-design-related concerns, and open-access medium, a VANET is extremely susceptible to numerous security assaults. A Black Hole Attack (BHA) is a kind of security hazard in which the malicious vehicle dewdrops controllers or data packets, turning an otherwise secure conduit or link into one that can be exploited. Accidents, deaths, and traffic jams can all result from dropped data packets on a VANET, so avoiding doing that is essential.
Objective:
To safeguard and enhance the general performance and security of the VANETs, a unique technique termed "Detection and Prevention of a BHA (DPBHA) is proposed in this study.
Methodology:
Detection and Prevention of a BHA (DPBHA) is proposed and used.
Findings:
An active threshold value is calculated, and a fake route request (RREQ) packet is generated as part of the proposed solution. The solution is tested in the NS2 simulator and compared to industry standards for performance and effectiveness.
Novelty:
The outcomes presented showed that the planned DPBHA outpaced the benchmark outlines by raising the PDR by 3.0%, increasing the throughput by 6.15%, decreasing the routing overhead by 3.69%, reducing the end-to-end delay by 6.13%, and obtaining a maximum detection accuracy of 94.66%.

Keywords— AODV; BHA; IoT; network security; VANET

[1]*CSE & OSGU, INDIA, paramcse191@osgu.ac.in
[2]CSE & OSGU, INDIA, cser2@osgu.ac.in

***Corressponding Author:** Paramjit
***CSE & OSGU, INDIA, paramcse191@osgu.ac.in

DOI: - 10.48047/ecb/2023.12.si5a.026

Introduction

The term "vehicular ad hoc network" (VANET) refers to a network of motor vehicles that uses an Intelligent Transportation System (ITS) to control traffic and move people and goods. The dispersed nature of VANET means that network security and privacy are paramount concerns, resulting in safer online interactions. With intelligent transportation inside the network, VANET ensures the safety of the roads and reduces traffic congestion. Communication between cars is also made possible. As the vehicles in a VANET are essentially mobile nodes, wireless network security becomes a significant concern for this type of network.

VANET system sets up a network when needed and tears it down when don't. In other words, VANET is a subset of MANET (Mobile Ad-hoc Network). The former, known as MANET, is used in Mobile networks, while the latter, VANET, is used in Vehicle networks. MANET uses Wi-Fi IEEE 802.11m technology, while VANET uses Wi-Fi IEEE 802.11p technology, with the MAC address being the critical distinguishing factor [1]. When comparing data transfer speeds, vehicular networks outperform mobile ones. Mobile networks are disorganised compared to vehicular networks, whose nodes know their network's trajectory. Regarding cryptography and advanced algorithms, the VANET has an advantage over the MANET because of the vehicles' mobility. Yet, VANET avoids the limited battery life that plagues mobile networks.

Because of its decentralised nature, VANET oversees all security criteria in transferring information between the many nodes that comprise the vehicular network. Several attacks can compromise the security of a VANET, including denial-of-service (DoS), spoofed identity (Sybil), jellyfish attacks, and Man-In-The-Middle (MITM). To mitigate the dangers inherent in the VANET and improve the dependability of the ad hoc automotive network, it is essential to detect and prevent malicious attacks.

Vehicles can interact via cellular networks and short- and medium-range VANET interfaces. As a result, routing protocols must determine the optimal path for a data stream coming from a particular program in a vehicle, considering the requirements of the service being communicated. The quality of service provided may be significantly affected by the routing protocol's selection. The notice may come too late for an advertisement broadcast application if the routing selects the cell connection to range a neighbouring vehicle. In that instance, VANET transport would have been the best option for delivery [2].

Cellular networks are more appropriate for a connection-based interactions with a server on the internet than infrastructure networks for accessing VANET gateways. The best answer has to consider both the application's requirements and the network's current status. The GwDiscE2E protocol was developed to aid the routing protocol in its decision-making. Using a VANET system, the gangway is permanently linked to all vehicles with access to the system. They show, via extensive simulations, how routing methods can take use of this trait when they're given direct access to the backbone network. Due to the unreliability of the VANET's end-to-end link to the gateways, this allows for the diversion of time-critical traffic across less reliable channels [3].

The fast-moving vehicles and the potentially life-or-death nature of the transmitted information make safe and effective communications in VANETs crucial. Since the Sensor 2022, 22, 1897, three out of every twenty-six nodes in VANETs transmit these messages through an unsecured public wireless means. The apps and services provided by VANETs are vulnerable to the attacks above. A BHA is an attack in which a malicious node fails to transfer packets to their intended destination. Important emergency texts and warning alarms could be contained in these packets. Such packages are dropped by a BHA, which compromises network security, slows data transmission, and disrupts information flow throughout the network [4]. Deadly and disabling road accidents occur all too frequently. So, in a dynamic VANET, discarding all such packets could lead to road deaths, traffic jams, accidents, and congestion. To address this issue and enhance the reliability and efficiency of VANETs, we suggested an innovative and effective method for detecting and preventing the notorious safety attack BHA inside the AODV routing protocol in this work. “The problem was solved by forging an RREQ packet based on the sequence numbers of previously received RREPs and a configurable threshold value. As a recap, the proposed technique improved PDR and network performance while decreasing routing overhead.”

Limitations in the existing system are

1) The method could be more effective when two malicious nodes collaborate; it has a high false detection accuracy in a short time; it causes a significant increase in routing overhead and end-to-end (E2E) delay; it is time-consuming to implement.

2) More processing time is needed, leading to significant end-to-end (E2E) latency.
3) While this helps keep outsiders out, it leaves the network vulnerable to damage from insiders.

Black Hole Attacks in VANETs

A malicious node in a BHA causes a Denial of Service by intentionally dropping packets from a friendly node. When it receives a Route Request (RREQ) packet from the source address, a malicious BHA node will send back a false RREP lacking first checking its routing database. This Route Reply (RREP) packet contains the newest and quickest path, according to AODV [5,6]. Data packets will be sent to the black hole nodes because the transmitting node will believe the fake RREP packet is an optimal path. When a Router drops packets rather than forwards them, it affects performance, network security, and data flow. Some of the data in these packets may be time-sensitive. Congestion, accidents, and even deaths could result from reducing such packages on a live VANET. The study's primary objective was to develop a workable answer to the BHA issue in VANETs. Denial-of-service (DoS) attacks on VANETs employ BHAs to keep users off the network. DoS, Sybil, flooding, wormhole, jellyfish, GHA, impersonation, and BHA are just some of the attacks that can be launched against VANETs [7]. As a result of these assaults, VANET services and programmes are at risk.

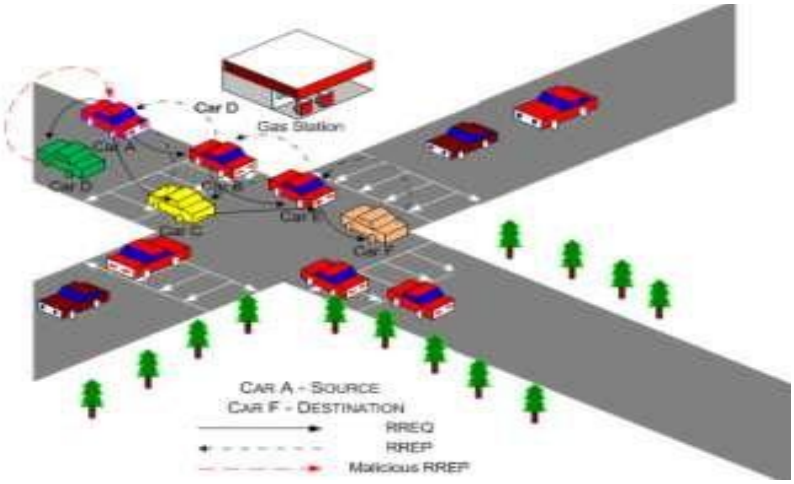

Figure 1Blackhole Attack in VANET

The solutions for lowering BHA and removing rogue nodes in VANETs which have been proposed and discussed in the appropriate works are Kumar et al. projected an acknowledgement-based method for VANET BHA detection [8]. The packet is acknowledged back to its sending node by each intermediate node. The PDR is impacted, routing costs are increased, and operation time is lengthened due to the additional acknowledgements generated by each intermediate node. The Attack-Resistant Trust (ART) helps effectively based on data, and node reliability was designed by Li et al. [9] to detect and remove misbehaving nodes from the network. The technique is based on analysing data and managing trust. The traffic data collected by vehicles is analysed in Dempster-theory. Shafer's Although many nodes forward data, some of them are malicious.

Malicious vehicle identification and avoidance for VANET BHAs was developed by Ouazine et al. [10]. The authors enhanced the DMV method by caching so during route searching [11]. The first step of this method is to consider all possible futures for BHA. If one is located, it is discarded, and a new one is made. This technique outperforms DMV in detecting and mitigating extremely mobile BHAs in VANETs. End-to-end latency is a result of processing time. Hassan et al. [12] suggested looking for BHAs and GHAs and removing them. The standard AODV routing protocol was enhanced by totaling two new control packages: the Response sequences (Rseq) and the Coded sequence (Cseq). The Cseq pack is broadcast from a base node to its neighbours. Connecting nodes then send Rseq after Cseq. If the IDs of the two packets are compatible, they will communicate with one another. Instead of using Rseq, the initiating node will alert all other nodes to the presence of the malicious node. PDR is improved, and compatibility with different protocols for reactive routing is ensured. However, the additional routing overhead caused by control packets must be considered.

Research Method

This section expands on and discusses the presented and proposed Detection of a Black Hole Attack (DPBHA). The suggested DPBHA takes advantage of the two most dangerous characteristics of a BHA. As attacking node imagines taking a new route to its endpoint, it includes higher sequence numbers and minimal hop count values in its RREP. Second, the malicious node always answers RREQs first without consulting its routing table. Modifications to the AODV routing protocol's default operations take full benefit from these dual traits, making it easier to spot and stop BHAs in VANETs. Figure 2 depicts the general flow of operations for the proposed DPBHA, which consists of three stages: "connectivity," "detection," and "prevention."

In the connectivity task, the target network is launched, the topology is defined, then it is expected that communication has begun between vehicles (nodes). The second phase reveals Sensor 2022, 22, 1897 9 out 26 as the location of the malicious node, which is most likely a black hole (50% certainty). In the tertiary stage, the malicious node is confirmed as a black hole node and must be eliminated from the network.

Manipulating the threshold value and creating a false RREQ packet reduces routing overhead and end-to-end delay, boosts throughput and packet delivery ratio, and requires no extra hardware or Intrusion Detection System (IDS)/Personal Firewall (PFR) nodes to detect and prevent a BHA.

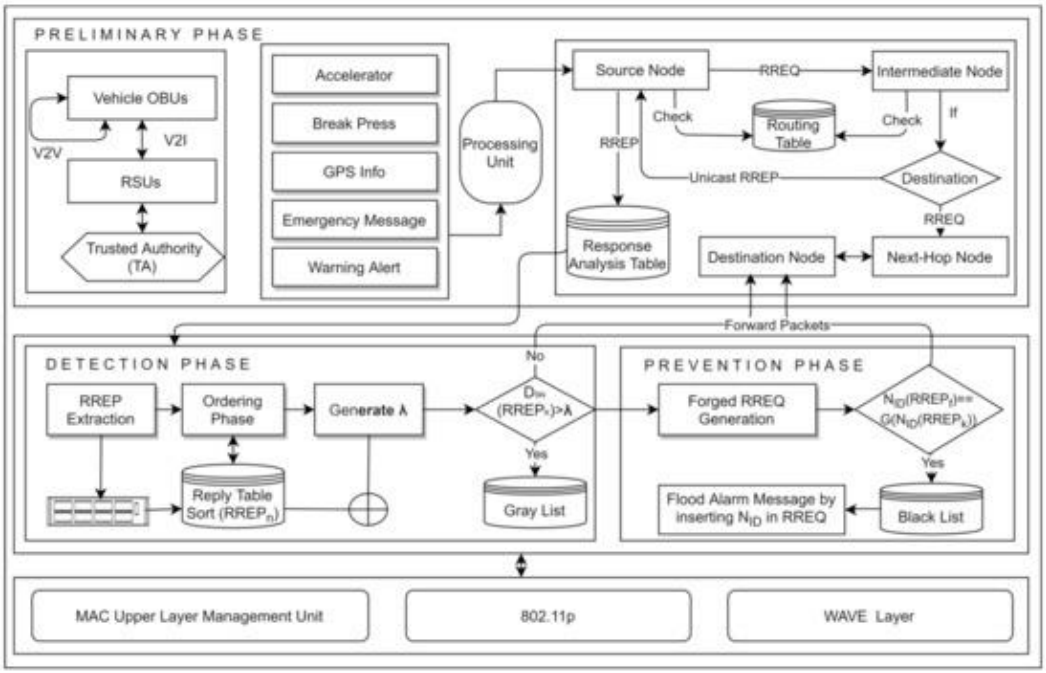

Figure 2 The framework of DPBHA

Result and discussion

The proposed DPBHA was tested in a simulated setting (using NS2 Simulator v2.35) to gauge its performance and effectiveness related to industry standards. NS2 enables flexible simulation parameters, improving the simulation's usefulness and realism. To validate the findings, they were compared to three of the most popular schemes in the works: SAODV, AODV, and IDBA [12].

We chose a generic urban traffic scenario with densities ranging from 25 to 150 nodes to conduct our performance analysis (black hole nodes, RSUs, and vehicles). Every simulation run had 8 per cent malicious nodes (black hole nodes). Twenty-one regular cars, two black hole nodes (shown as red circles), and two RSUs make up the 25 nodes used in the first experiment (with blue circles). Each simulation was carried out in the simulant ten times, in addition then the middling values were calculated in preparation for the statistical analysis.

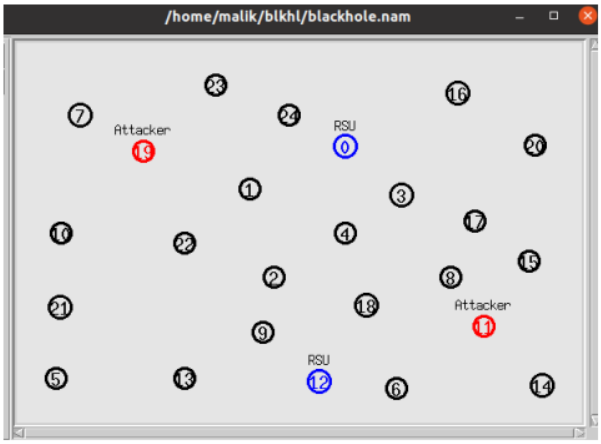

Figure 3 Initial state of the first experiment

To gauge how well the proposed solution performs, we looked at the following indicators: Metrics for routing overhead, PDR, throughput, end-to-end latency PLR, PLO, and confusion.

Routing Overhead

The routing overhead (ROH) is the sum of all control packets and overall data packets sent.

Classic SAODV, AODV, and IDBA were used as benchmarks against which to map the overhead routing behaviour of the proposed DPBHA. The ROH in the projected DPBHA was lesser than in the benchmark systems because rogue nodes could instantly be identified in the network. Due to the increased number of answers generated by the network's malicious nodes, classic AODV experienced a massive 28.57% increase in routing overhead. Similarly, SAODV's five-step detection process increases the number of control packets, resulting in a very high ROH of 26.59%. IDBA's average route overhead was 23.52%, which was quite near to the suggested DPBHA. DPBHA has the lowest average ROH of all the schemes at just 21.30% over most nodes. As a result, the moderate view that includes was reduced by 3.69% to the proposed DPBHA.

Packet Delivery Ratio

The Packet Delivery Ratio (PDR) is the proportion of sent packets successfully received at their final destination.

The proposed DPBHA employs a changing threshold value to identify the malicious node and prove its malignancy by having it broadcast a fake RREQ. The suggested DPBHA outpaced the other systems in terms of PDR performance. Classic AODV's PDR declined by an average of 20.44 per cent, whereas other schemes' PDR decreased by less because of the presence of security systems. Average PDRs were 25.06% for the SAODV scheme and 26.48% for the IDBA scheme. The existence of a BHA substantially hindered the classic AODV; its PDR declined precipitously as the quantity of malicious network nodes increased. Our suggested DPBHA had a PDR of 28%, which was 3.0% higher than the industry standard.

Throughput

The average rate at which data packets delivered from a source node reach their destination. Quantifying throughput in terms of containers per minute (pps) bits each second (bps) of packet per time slot is possible.

By way of the numeral of malicious nodes improved, the average throughput of the traditional AODV protocol dropped to 17.68%. SADOV and IDBA were measured to have average throughputs of 23.36% and 27.78%, respectively. Both schemes' instantaneous BHA detection techniques contributed to their superior throughput performance. The proposed DPBHA achieved higher throughput than the state-of-the-art methods. The proposed DPBHA achieved the most significant average throughput (31.15%) of the tested schemes. As a result, the average throughput was increased by 6.15 per cent after implementing the proposed DPBHA.

End-To-End Delay

The period it takes by a packet to go beginning the node that created it to the node that received it is known as the end-to-end latency. It's typical time for data packets to travel from one node to another. In this case, the E2E delay increased as the number of nodes increased. The proposed DPBHA has a significantly lower average E2E delay than the other schemes. The planned DPBHA has the shortest end-to-end (E2E) hold of the schemes studied. Similarly, the SADOV & IDBA had delays of 27.04% and 23.15% on average from start to finish. The projected DPBHA cut the mean E2E delay by 6.13 per cent.

Packet Loss Rate

The packet loss rate (PLR) is calculated by subtracting the number of data packets that benefit from implementation by the destination node from the entire quantity of data packets supplied by the source node. The most common causes of packet loss are malicious nodes and increased network congestion.

In the existence of a BHA, the traditional AODV suffered greatly, with an average loss of 37.33% of the packet because of the absence of security safeguards. While comparing SAODV and IDBA, it was found that their average PLRs were 24.77% and 20.14%, respectively. These two methods performed well regarding PLR because they both use real-time safety mechanisms that can identify a BHA. Like the planned DPBHA, this method initially uses a dynamic threshold level to pinpoint the malicious node and then uses forged RREQ broadcasts to verify the node as BHA. Although BHAs could be immediately removed, the suggested DPBHA had a PLR of 15.15 per cent. The projected DPBHA resulted in a 9.84% decrease in PLR on average.

Confusion Matrix

The following confusion matrix measurements are typically used to evaluate Intrusion Detection Systems (IDSs), as indicated in Table. Cases that fit the expected category are shown in the table columns. Similarly, each row in the Table stands in for an actual class instance.

Table 1 Confusion matrix

	Actual Reality class		
	class	**Normal**	**Attack**
Test result	**Attack**	**False positive (FP)**	**True positive (TP)**
	Normal	**True negative (TN)**	**False negative (FN)**

Detection Rate

The detection ratio is essential for evaluating a model's efficacy in pinpointing and eliminating rogue network nodes. The simulation outcomes for the suggested DPBHA's detection ratio are compared to benchmark systems in Figure 4.

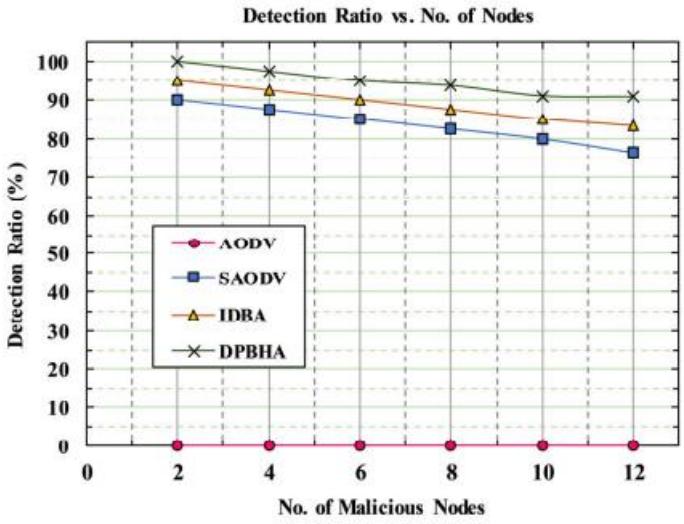

Figure 4 Graphical representation of detection rate

With a reported average detection ratio of 94.66%, the suggested DPBHA outperformed all other schemes in this study. The suggested DPBHA examines the sequence number of each RREP against the computed dynamic threshold value, which is the fundamental cause for the most significant detection rate. A suspect node is identified with a 50% chance if the sequence

number of the received RREP is greater than the threshold value. In addition, if the malicious node responds to the falsified RREQ, it is proved to remain a black hole node in the subsequent stage. This indicates that the suggested DPBHA can perform the two-stage technique in real time and accurately identify and avoid malicious nodes. When both good and bad nodes began to increase in the network, congestion and packet collisions made it more challenging to locate the latter. The suggested DPBHA, on the other hand, has the potential to identify and remove the BHA faster and

more accurately than current standards. As shown in Figure 4, the detection rate for the traditional AODV was a whopping 0% because it lacked any security feature in its design. SAODV had an average detection rate of 83.6%, whereas IDBA had an average detection rate of 88.88%. As shown in Figure 4, the suggested DPBHA had a high detection ratio overall, averaging 94.66%.

Conclusion

In this study, we looked specifically at how VANETs fare regarding security. DPBHA is a novel, and effective solution offered to safeguard and enhance the overall speed of VANETs by detecting and preventing black hole security breaches in the AODV protocol for routing. An adaptive threshold value was calculated, and forged RREQ packets were generated as a solution. The intended DPBHA was tested in the NS2 simulator and compared to industry standard schemes for performance and efficiency. Therefore, we demonstrated that the suggested DPBHA achieved a max detection accuracy of 94.66%, increased PDR by 3.0%, improved throughput by 6.15%, dropped E2E delay through 6.13%, condensed PLR by 9.84%, then reduced overhead employing 3.69% compared to the benchmark methods.

References

1. Sathya Narayanan PS. A sensor enabled secure vehicular communication for emergency message dissemination using cloud services. Digital Signal Processing. 2019 Feb 1;85:10-6. https://doi.org/10.1109/ACCESS.2020.2966747
2. Ahmed Z, Naz S, Ahmed J. Minimizing transmission delays in vehicular ad hoc networks by optimized placement of road-side unit. Wireless Networks. 2020 May; 26:2905-14. https://link.springer.com/article/10.1007/s11276-019-02198-x
3. Arif M, Wang G, Bhuiyan MZ, Wang T, Chen J. A survey on security attacks in VANETs: Communication, applications and challenges. Vehicular Communications. 2019 Oct 1; 19:100179. https://doi.org/10.1016/j.vehcom.2019.100179
4. Cherkaoui B, Beni-hssane A, Erritali M. Variable control chart for detecting black hole attack in vehicular ad-hoc networks. Journal of Ambient Intelligence and Humanized Computing. 2020 Nov; 11:5129-38. http://dx.doi.org/10.1016/j.procs.2017.08.337
5. Malik A, Khan MZ, Faisal M, Khan F, Seo JT. An efficient dynamic solution for the detection and prevention of black hole attack in vanets. Sensors. 2022 Feb 28;22(5):1897. https://doi.org/10.3390/s22051897
6. Abbas S, Talib MA, Ahmed A, Khan F, Ahmad S, Kim DH. Blockchain-based authentication in internet of vehicles: A survey. Sensors. 2021 Nov 27;21(23):7927. https://pubmed.ncbi.nlm.nih.gov/34883933/
7. Al-Heety OS, Zakaria Z, Ismail M, Shakir MM, Alani S, Alsariera H. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet.IEEE Access. 2020 May 6; 8:91028-47. http://dx.doi.org/10.1109/ACCESS.2020.2992580
8. Kumar A, Varadarajan V, Kumar A, Dadheech P, Choudhary SS, Kumar VA, Panigrahi BK, Veluvolu KC. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems. 2021 Feb 1; 80:103352. https://doi.org/10.1016/j.micpro.2020.103352
9. Lee M, Atkison T. Vanet applications: Past, present, and future. Vehicular Communications. 2021 Apr 1; 28:100310. https://doi.org/10.1016/j.vehcom.2020.100310
10. Ouazine K, Slimani H, Nacer H, Bermad N, Zemmoudj S. Reducing saturation and congestion in VANET networks: Alliance-based approach and comparisons. International Journal of Communication Systems. 2020 Mar;33(4): e4245. https://doi.org/ 10.1002/dac.4245
11. Zhang J, Zheng K, Zhang D, Yan B. AATMS: An anti-attack trust management scheme in VANET. IEEE Access. 2020 Jan 15;8:21077-90. https://doi.org/10.1109/ACCESS.2020.2966747

12. Hassan Z, Mehmood A, Maple C, Khan MA, Aldegheishem A. Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles. IEEE Access. 2020 Oct 28;8:199618-28. https://doi.org/10.1109/ACCESS.2020.3034327