International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 08, August 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

A Secure Routing Protocol with Black Hole Attack Prevention in VANETs

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

[1] CSE, OSGU HISAR, HARYANA. INDIA

paramcse191@osgu.ac.in

[2] CSE, OSGU HISAR, HARYANA. INDIA

deansvs@osgu.ac.in

Abstract

Real-time information sharing between automobiles and fixed infrastructure is a major driving force behind the revolutionary potential of Vehicular hoc networks (VANETs). Because of its potential to improve road safety and traffic management, secure data transfer in VANETs is of the utmost importance. The widespread danger of Black Hole Attacks, in which evil nodes delete data packets, endangers network and traffic security. The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is enhanced in this work with a 32-bit CRC-32 hash function to detect and avoid Black Hole Attacks in VANETs dynamically. The proposed solution improves security without adding unnecessary complexity or breaking backwards compatibility with existing messages. Based on their knowledge of the network's topology, intermediate nodes take a role in detection, forwarding, and response. Source nodes thoroughly inspect all incoming Route Reply (RREP) messages, discarding malicious ones. Extensive simulations using the NS-2 simulator show that our technique outperforms existing methods regarding Packet Delivery Ratio (PDR) and throughput. Our approach is robust and applicable since it can detect and prevent clever adaptive black hole attacks.

Keywords: *AODV routing protocol, Black Hole Attacks, security, CRC-32 hash function, Detection, Prevention, Packet Delivery Ratio (PDR), Throughput, VANETs.*

Introduction

With the development of VANETs, the transportation industry has undergone a revolutionary change in the modern era. VANETs are a subset of MANETs developed explicitly to improve transportation safety and efficiency through two-way vehicle and infrastructure communication [1]. To achieve their goal of real-time data transmission, these networks use vehicles' capabilities to construct a networked mesh. Recent years have seen a surge of interest in VANETs due to their potential to enhance road safety and traffic management and serve as a foundation for new technologies, including autonomous vehicles, emergency response systems and intelligent traffic control. Despite the evident advantages of VANETs, deploying them presents a significant challenge: protecting the confidentiality and integrity of data during transmission across such a fluid and widely dispersed network. Black Hole Attacks are a significant cause for concern regarding VANET security [2]. Attacks of this type occur when a hostile device falsely claims to be the quickest way to a target and then drops data packets instead of forwarding them. Such attacks can potentially have devastating results, including the interruption of traffic management systems and the occurrence of fatal accidents.

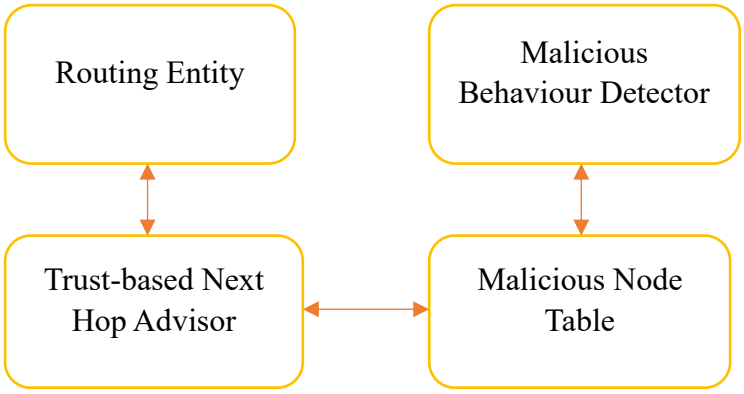

Figure 1 Secure Routing Architecture

There is an urgent need for secure and reliable routing protocols in VANETs. Communication in VANETs relies on safe routing protocols, which ensure that data is reliably, efficiently, and securely transported to its intended destination. Creating and deploying novel ways to protect data transmission is crucial because a vulnerability in these protocols can jeopardise the entire VANET ecosystem.

Security concerns become crucial to VANET due to the unpredictable nature of nodes in-vehicle networks. While there are several threats to vehicular networks, the Blackhole assault is the most problematic in the context of VANET. A black hole is a malicious router that responds to route requests by falsely claiming to be the quickest way to the destination and discarding all packets from the source or any intermediate routers [3]. Multiple black hole nodes are required for a cooperative black hole attack. These nodes coordinate their attack launch to maximise their effectiveness.

For the sake for the driver's convenience and safety and for usage as an intelligent traffic information system, VANET's primary objective is the design of a vehicle-based communication system [4]. Second, the security and privacy of the application are crucial concerns when deploying the VANET network as ITS technology in the real world. VANET, being a wireless network, is susceptible to various threats. A malicious actor may, for instance, provide fictitious traffic data via the network. Misleading traffic reports can force drivers to take alternative routes. If an accident occurs, traffic delays will be significantly more severe [5].

Furthermore, there are issues with energy- or battery-powered wireless ad-hoc networks. It is essential to conserve this power so the network can remain online indefinitely and the batteries last as long as possible. Network nodes have different energy requirements when actively transmitting, receiving data, or sitting idle. As mentioned in the problem statement, testing blackhole and flooding attacks against the energy-efficient routing protocol AODV on the VANET and comparing the results regarding packet loss, end-to-end delay, throughput, and energy is necessary.

Aim

This study aims to improve the safety and dependability of data transmission within VANETs by creating and evaluating a dynamic and effective solution for the detection and prevention of Black Hole Attacks.

Literature Review

Black Hole Attacks in VANETs

Recent years have seen increased awareness and investigation into the potential danger of Black Hole Attacks in VANETs. According to [6], a Black Hole Attack occurs when a hostile vehicle falsely claims to be the quickest path to a destination and fraudulently consumes incoming data packets without forwarding them to their intended recipients. The VANET's communication ability is severely hampered by this hostile activity, threatening road safety, data integrity, and the network's dependability.

ADOV

As a reactive routing protocol, AODV is a part of the family. Control messages are sent in the form of Route Replies (RREP), Route Requests (RREQ), and Route Errors (RERR). It takes care of backward learning and source routing [7]. An RREQ message is broadcast widely by a source node to establish a connection with a target node. After receiving RREQ packets, the destination decides which path has the fewest hops and returns an RREP packet to the sender. The data is transmitted along the determined route once it reaches the source node.

Key Challenges and Previous Solutions

For several reasons, black hole attacks in VANETs are challenging to detect and prevent. The constant change that characterises VANETs is a significant obstacle. [8] The network is constantly expanding and contracting as vehicles join and leave. Traditional security procedures are often insufficient, making it difficult to develop confidence in cars.

The distributed nature of VANETs presents still another difficulty. Decentralised networks are more vulnerable to assaults since no central authority enforces security policies.

Using a safe AODV routing algorithm, [9] presented a method for detecting Black Hole Attacks. Their approach is geared towards making VANET routing more secure.

[10] described a distributed trust mechanism for monitoring VANETs for malicious activity. Their method is able to detect and remove malicious nodes from the network by relying on the vehicles' established credibility.

Black Hole Attacks can be detected and avoided with the help of a dynamic method suggested in [11]. They train to be adaptable and aware of the subtleties of different attacks.

In their research [12], the authors present a proactive and efficient method for detecting and evading Black Hole Attacks. This study is foundational to our research since it emphasises the value of active security approaches for VANETs.

Black Hole Attack detection was published in [13] using a secure AODV routing scheme. Their approach inspired ours since it strengthens the safety of routing and throws light on the importance of protecting VANET data transmission.

[14] developed a distributed trust mechanism to monitor VANETs for malicious activity. Our trust-based method for detecting Black Hole Attacks is based on their research, which emphasises the significance of trust in VANET security.

In order to solve the gray-hole issues that arise in ad hoc mobile networks, [15] employs a reputation-based approach. In this strategy, the AODV routing protocol relies on a system of trusted. During the route-finding process, the confidence in each node is evaluated. To lessen the likelihood of a Blackhole node accessing the path, the AODV routing protocol was designed in [16]. The RREP'2 protocol is the official name for it. The protocol calls for the source node to discard the initial or initial two RREPs. Each RREP packet that arrives is continually chosen. This is because the Blackhole node's RREP is the first or second RREP the source node has ever received. This technique can be quite helpful when the Blackhole node is geographically close to the source node. To counteract Blackhole attacks, a new variant of the AODV routing protocol, PCBHA, is proposed in [16]. In [17], a new method, DPRAODV (Detection, Prevention, and Reactive AODV), was developed to counteract Blackhole assaults in VANET networks and protect MANETs from a cooperative Blackhole attack. Similar to Tamilselvan and Sankaranarayanan's approach. But with this approach, they offered a dynamic mechanism for preventing the Blackhole node from spreading.

These chosen sources have been at the forefront of illuminating the difficulties of Black Hole Attacks in VANETs and proposing novel approaches to overcoming them. Based on these earlier findings, we propose a novel and practical method for ensuring secure routing in VANETs.

Proposed methodology

In order to determine the path to the target node, AODV begins with the source node querying its routing table. If, however, a valid path is found, the sending node will send the packet on to the next one. If the preferred path can't be found, the origin will start the route discovery process. It all starts with a RREQ sent out into the network. The RREQ message will be answered with a RREP by the destination node or by an intermediate node if any of them understands the way to the destination. The method presented in this paper alters the AODV process, as seen in the flowchart in Figure 2. The suggested technique uses a Cyclic Redundancy Check (CRC-32) [18] hash function, which contains 32 bits. As can be seen in Figure 3, the RREQ format is the only part of the AODV messages that has been altered. The RREQ message format is maintained by replacing the destination address with its CRC-32 value, which is the same length (32 bits). As a workaround, the sending node might keep track of the receiving address and substitute the RREQ's CRC-32 value for it before sending it on. When an intermediate node receives an RREQ, it checks the CRC32 of its IP address to the node's destination address set on the RREQ to identify whether or not it is the destination, and then sends back an RREP with the correct destination node address. In all other cases, the intermediate node will relay the RREQ message.

IJARSE
ISSN 2319 - 8354

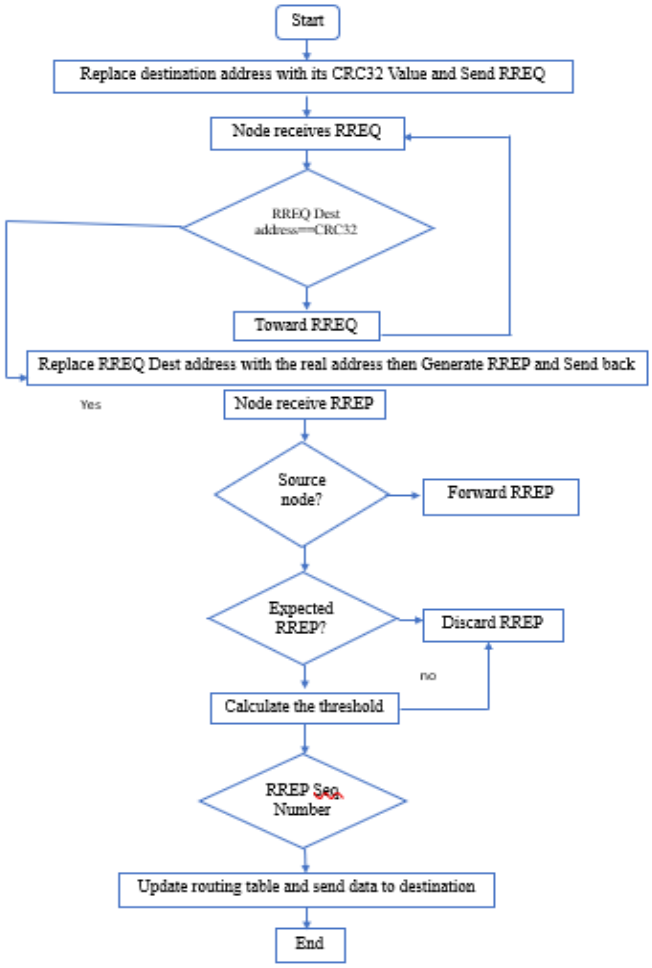

Figure 2 Proposed method chart

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type J R G D U Reserved Hop Count

RREQ ID

DESTINATION IP ADDRESS

DESTINATION SEQUENCE NUMBER

ORIGINAL IP ADDRESSS

ORIGINATOR SEQUENCE NUMBER

Figure 3 AODV Message format basic request

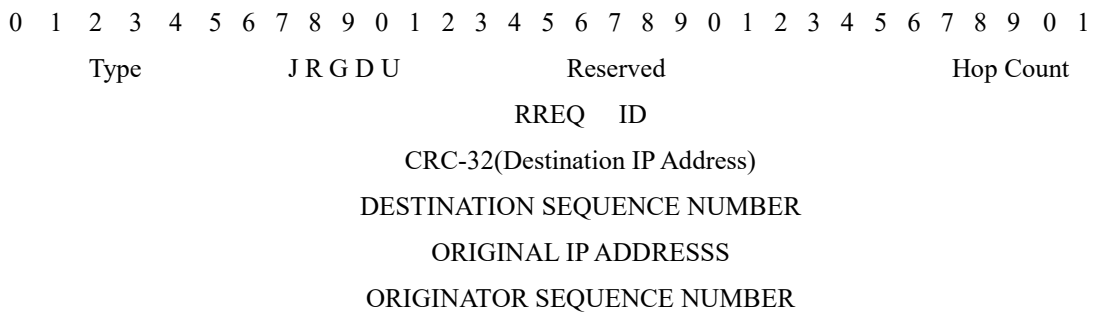

Figure 4 Modified Message format

However, each RREP that is received at the source node is verified in two different ways. If the source address of the RREP and the destination address of the RREQ are different, the RREQ will not be acknowledged from the source node. Only malicious nodes will reply to invalid addresses, so only those should be avoided. Second, the source node compares the RREP's sequence number to the threshold it has set; if the number of sequences is below or equivalent to the threshold, the RREP has been accepted, and the routing table of the source node is changed. In that case, we cannot accept the RREP. The threshold in this case is the average plus the minimum of all RREP sequence numbers received (i.e., all RREPs). The proposed scheme will protect against a typical black hole attack in the first phase, but in the second phase, an intelligent adaptive black hole can behave like a real node by checking its routing table and reacting with a high sequence if it has a route to the destination. The proposed approach can be used to detect and block attacks from both singular black holes and groups of black holes that collaborate, due to the fact that the CRC32 remains reversible.

Results and discussion

The NS-2 simulator was used to test the effectiveness of the suggested method, with the simulation parameters specified in Table 1. Figure 5 displays the results of our research and analysis using Network Animator (NAM). To simulate car travel, we used OpenStreetMap's Manhattan map as a basis for generating mobility traces with SUM

Table 1 Parameters Values of NS2 stimulation

Parameters	**Values**
Simulator	NS2 (Version 2.34)
Simulation area (km x km)	2.5 x 2.5
Simulation time	300 s
Network interface type	Wireless Phy Ext
MAC Layer	802.11
Movement Model	Manhattan Grid/Random Way Point
Permissible lane speed (km/h)	[0,80]
Transmission range (m)	250
Packet size (byte)	512
Packet Generation Rate	5 Packets per Second

IJARSE
ISSN 2319 - 8354

Number of vehicles	[100, 200]
Traffic type	CBR
Malicious Node	1
Routing protocols	AODV, Proposed,

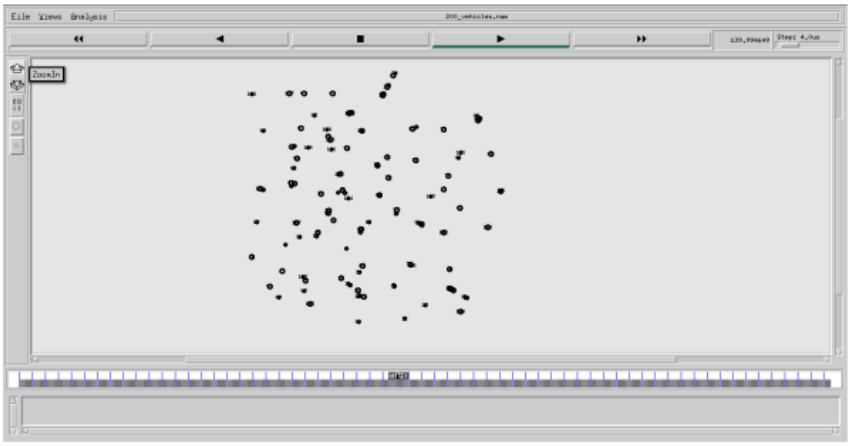

Figure 5 Output of NAM

Packet Delivery Ratio (PDR), Routing Overhead, Throughput, and End-to-End Delay (ETE) are the four performance measures used to evaluate the effectiveness of the suggested approach. Our simulation tests the proposed scheme and [19] in the face of an intelligent black hole attack and compares the resulting network topology to that of the baseline AODV routing protocol.

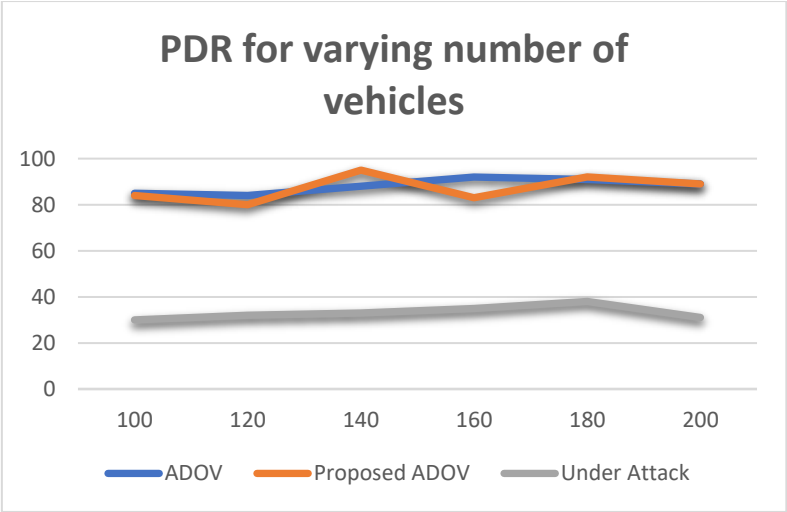

Figure 6 PDR for no of vehicles

Figure 6 shows that our suggested approach has a much higher PDR than the proposed solution and a PDR approximately on par with the basic AODV in the absence of an assault.

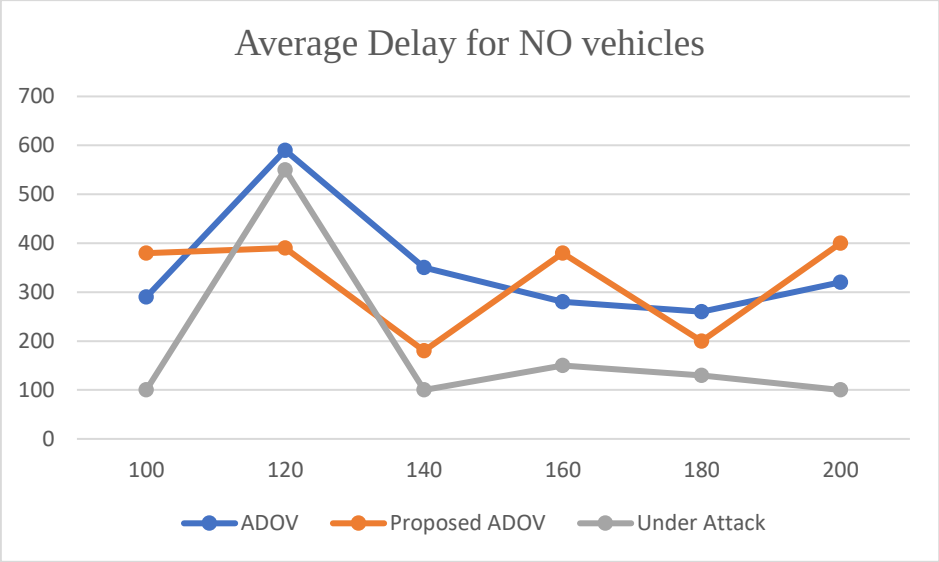

Figure 7 NO of vehicles Average delay

Figure 7 demonstrates that in the absence of an attack, our system achieves ETE delays comparable to AODV's. Since only received data packets are counted towards the end-to-end delay, the solution proposed shows the most negligible ETE. This is because, under an intelligent adaptive black hole attack, the only data packets ever received are those whose source and destination nodes are neighbours.

Figure 8 demonstrates that compared to the AODV, our approach achieves higher throughputs.

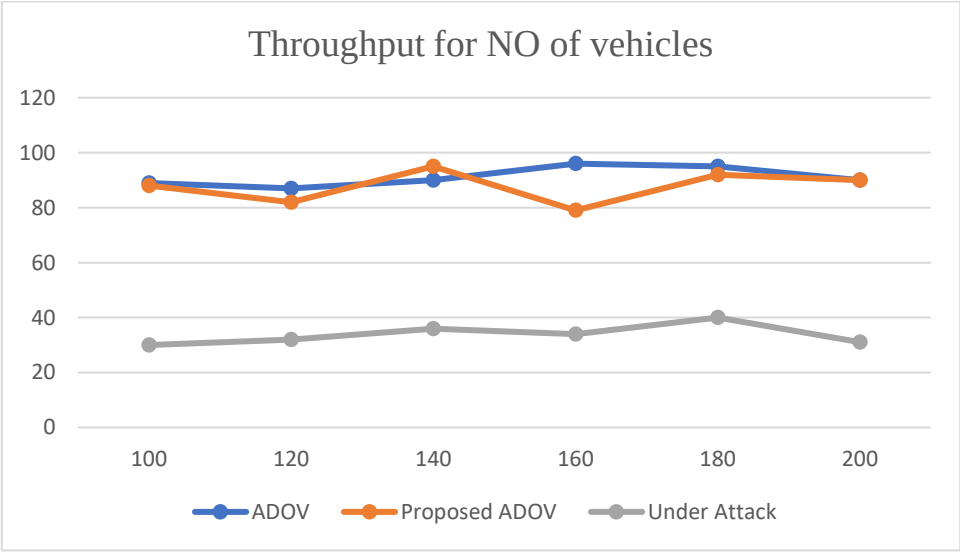

Figure 8 NO of Vehicles Throughput

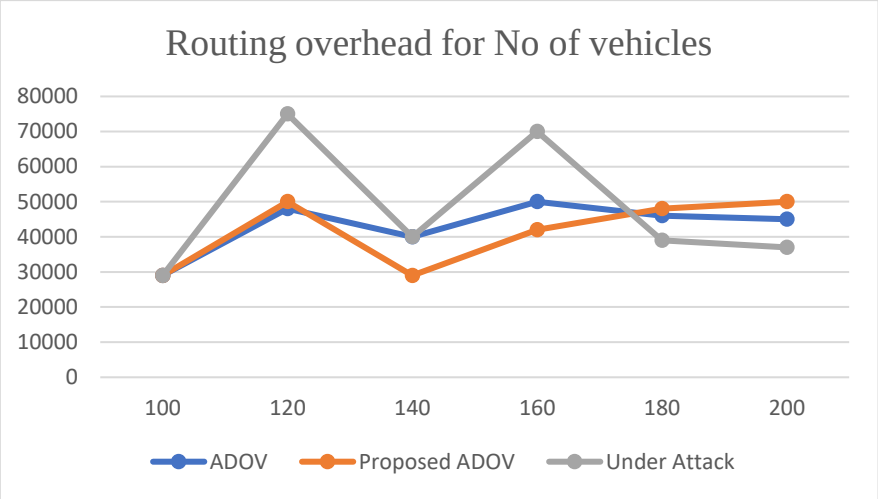

Figure 9 No of Routing overhead

Figure 9 demonstrates that under normal conditions (no attacks), our proposed method has a similar routing overhead to AODV. This is different for most node densities.

The ability of our suggested approach to detect intelligent black hole attacks is depicted in Figure 10 below. The data reveals that our concept can guarantee a more than 85% detection ratio even while facing many sophisticated adaptive black hole attacks. So, as we can see in the preceding Figures and from the encouraging simulation results, Intelligent adaptive black hole attacks in-vehicle networks are a known challenge. Still, our solution is effective in mitigating these threats.

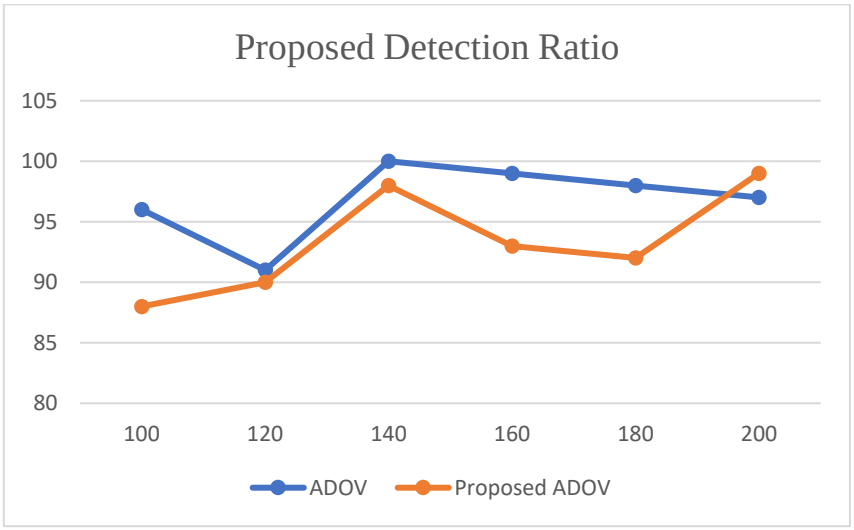

Figure 10 Detection Ratio of proposed method

Conclusion

Data transmission security in VANETs is crucial because of dangers such as Black Hole Attacks. Our research presents a novel and powerful method to identify and stop Black Hole Attacks in VANETs. The structure is intact while improving security by adding a 32-bit CRC-32 hash function to the AODV routing protocol. Results from simulations show that the proposed strategy has potential. Improved PDR and throughput compared to

preexisting alternatives determine the protocol's efficacy. In addition, our method deftly handles the severe security issue of intelligent adaptive black hole assaults. The detection ratio of over 85% achieved in the presence of such attacks shows the solution's practical value and durability. Overall, this study helps pave the way for better road safety, more effective traffic management, and the easy incorporation of new technology by contributing to developing secure communication in VANETs.

Reference

1) Malik, A., Khan, M. Z., Faisal, M., Khan, F., & Seo, J. T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in vanets. *Sensors*, *22*(5), 1897.
2) Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., ... & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems*, *80*, 103352.
3) Fiade, A., Triadi, A. Y., Sulhi, A., Masruroh, S. U., Handayani, V., & Suseno, H. B. (2020, October). Performance analysis of black hole attack and flooding attack AODV routing protocol on VANET (vehicular ad-hoc network). In *2020 8th International conference on cyber and IT service management (CITSM)* (pp. 1-5). IEEE.
4) Kumar, A., Dadheech, P., Goyal, D., Patidar, P. K., Dogiwal, S. R., & Janu, N. (2021). A novel scheme for prevention and detection of black hole & gray hole attack in VANET network. *Recent patents on engineering*, *15*(2), 263-274.
5) Lyu, J., Chen, C., & Tian, H. (2020, August). Secure Routing Based on Geographic Location for Resisting Blackhole Attack in Three-dimensional VANETs. In *2020 IEEE/CIC International Conference on Communications in China (ICCC)* (pp. 1168-1173). IEEE.
6) Ahmed, M. T., Rubi, A. A., Rahman, M. S., & Rahman, M. (2021). Red-AODV: A Prevention Model of Black Hole Attack for VANET Protocols and Identification of Malicious Nodes in VANET. *International Journal of Computer Networks and Applications*, *8*(5), 524-537.
7) Ahmed, A. K., Abdulwahed, M. N., & Farzaneh, B. (2020). A distributed trust mechanism for malicious behaviors in VANETs. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(3), 1147-1155.
8) El Houssaini, S., El Houssaini, M. A., & El Kafi, J. (2022). Novel approach of detecting the black hole attack for vehicular ad-hoc networks based on capability indicators. *International Journal of Pervasive Computing and Communications*.
9) Younas, S., Rehman, F., Maqsood, T., Mustafa, S., Akhunzada, A., & Gani, A. (2022). Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs. *Applied Sciences*, *12*(23), 12448.
10) Pokar, T., Patel, S., & Shah, R. (2019). An Efficient Approach of DSR Protocol to Detect and Prevent Black Hole Attack For VANET. *International Journal of Research and Analytical Reviws (IJRAR)*.
11) Shah, P., & Kasbe, T. (2021, May). Detecting sybil attack, black hole attack and DoS attack in VANET using RSA algorithm. In *2021 Emerging Trends in Industry 4.0 (ETI 4.0)* (pp. 1-7). IEEE.

12) Yadav, D., & Chaubey, N. K. (2022, November). Performance Analyses of Black Hole Attack in AODV Routing Protocol in Vanet Using NS3. In *International Conference on Advancements in Smart Computing and Information Security* (pp. 118-127). Cham: Springer Nature Switzerland.
13) Luong, N. T., & Hoang, D. (2023). BAPRP: a machine learning approach to blackhole attacks prevention routing protocol in vehicular Ad Hoc networks. *International Journal of Information Security*, 1-20.
14) Soni, G., & Chandravanshi, K. (2022). A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack. In *Sustainable Communication Networks and Application: Proceedings of ICSCN 2021* (pp. 649-663). Singapore: Springer Nature Singapore.
15) Alee, R., Nigussie, E., & Hakala, A. (2019). Analysis of Black hole Attack in Ad hoc On-Demand Distance Vector (AODV) Routing Protocol: Vehicular Ad-hoc Networks (VANET) Context.
16) Dhanaraj, R. K., Islam, S. H., & Rajasekar, V. (2022). A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments. *Wireless Networks*, *28*(7), 3127-3142.
17) Oberoi, V. (2020, December). Enhancement of QoS in Security Algorithm for Blackhole Attack in VANET. In *2020 IEEE Pune Section International Conference (PuneCon)* (pp. 33-37). IEEE.
18) Patil, A. N., & Mallapur, S. V. (2022, December). A Review on Security-Based Routing Protocols for Vehicular Ad Hoc Networks. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 399-405). IEEE.
19) Sagar R Deshmukh, P N Chatur, Nikhil B Bhople," AODV-Based Secure Routing Against Blackhole Attack in MANET", IEEE International Conference On Recent Trends in Electronics Information Communication Technology, India, pp. 1960-1964, 2016.