iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46186

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VIII August 2022- Available at www.ijraset.com

A Review Paper of M-AODV Routing Protocol in VANET to Detect and Prevent Black Hole Attack

Ms. Shubhvardhani Jain[1], Mr. Nilesh Kumar Sen [2]
[1, 2]*Department of Computer Science Engineering, BTIRT, Sagar M.P.*

Abstract: ***In the field of contemporary intelligent transportation, vehicular ad hoc networks (VANETs) are a popular and promising technology. They are employed to provide effective life safety, intelligent transportation systems, and traffic information systems (TIS). Due to the nodes' mobility and the connections' brittleness, the VANET is open to a variety of security risks. One type of security risk known as a "black hole attack" involves a node presenting itself to other nodes in such a way that it has the quickest and most direct access to the target. As a result, an effective method for the detection and eradication of the Black hole attack in the Vehicular Ad Hoc Networks (VANET) is given in this research study. One of the most widely used routing protocols for VANET, AODV (Ad hoc On Demand Distance Vector) is used to achieve the suggested method. In the first stages of route discovery, the technique can identify both a single black hole attack and a cooperative black hole attack. The simulation is carried on NS2 and the results of the proposed scheme are compared to [14] and the fundamental AODV routing protocol, this results are examined on various network performance metrics such as packet delivery ratio, throughput and end-to-end delay. The found results show the efficacy of the proposed method as throughput and the delivery ratio of the network does not deteriorate in presence of the back holes.***
Keywords: VANET, Black hole attack, Security, M-AODV

I. INTRODUCTION

Vehicular ad hoc networks (VANET) are now used to create an effective Traffic Information System because to advancements in wireless communication technology and the rising number of traffic incidents (TIS). Vehicle-to-Vehicle (V2V) technology, according to the National Highway Traffic Safety Administration (NHTSA), has a significant potential for saving lives in about 80% of multi-vehicle incidents. [1].

The Mobile Ad-hoc Network (MANET) subtype known as VANET consists of a large number of nodes (vehicles) that are capable of talking with one another without the use of a permanent infrastructure [19]. VANET, in contrast to MANET, has a very dynamic topology because of the significant mobility of vehicles. Nodes often travel in a predetermined sequence. Additionally, VANETs have the potential to be on a vast scale with numerous members and the ability to cover the entire road network [2]. Consequently, attacks & routing protocol: The VANET's lack of centralised management places additional burdens on vehicles. As a result, each vehicle manages and regulates the communication on the network in addition to being a part of it. The links between cars frequently connect and disengage because to the high node mobility, which makes routing difficult. As a result, routing in VANET has been the focus of numerous academics. These suggested routing methods' major goals are to increase throughput and Packet Delivery Ratio (PDR) while lowering control overheads and packet loss ratio. Numerous routing protocols that play a significant part in structuring network security have been proposed in this direction. However, there are three types of ad hoc routing protocols: proactive, reactive, and hybrid [3], Proactive protocols are typically table driven. Examples of this type include the Global State Routing GCR and the Destination Sequence Distance Vector (DSDV). Reactive protocols, on the other hand, do not automatically update the routing data. Like Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing, it only determines the route when necessary (DSR). Reactive and proactive strategies are both used in hybrid protocols. Zone Routing Protocol is an example of this sort of protocol (ZRP). We will focus on the well-known and clever black hole attack in the AODV base VANET in this essay. A malicious node uses an intelligent black hole attack to evade detection and get around security measures by intelligently adapting and varying its behaviour. Although AODV is a reactive routing system, as was already mentioned, nodes will only provide control data when it is absolutely necessary. The node that needs to communicate data creates a packet called a Route Request (RREQ) and broadcasts it. If a malicious node (black hole attack) is present in the network, it will lure all other nodes to route packets through it by sending Route Reply (RREP) after receiving an RREQ message but not actually having a route to the target If more than one node collaborates in the attack, the damage is increased.

However, cooperative and intelligent black hole attacks are less effective than solitary black hole attacks, which is the focus of many research endeavors.

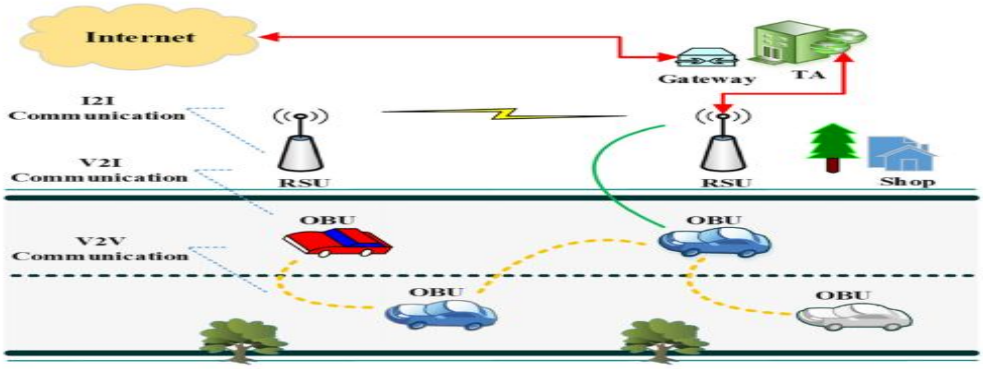


Figure 1 VANET Generic architecture

The rest of this essay is structured as follows: The backdrop of the AODV protocol and the black hole attack were introduced in part II. The limits of pertinent related work are described in section III. The suggested methodology and associated algorithm are described in Section IV. In Section V, the results of the simulation experiments and an analysis of performance are presented. Section VI concludes with a discussion of our findings and our research's future directions.

II. AODV ROUTING PROTOCOL AND BLACK HOLE ATTACK

A route is only established by the Ad hoc On-demand Distance Vector (AODV) routing protocol [5][3] when a source node needs it to transfer data packets since it utilises an on-demand approach to locate routes. In AODV, there are two mechanisms in use: route discovery and route maintenance. A node first checks its routing table when it needs to forward a data packet to see if there is already a route to the destination. If so, it sends the data packets over that route to the desired location. It buffers the packet and emits a Route Request message if a route is not available or the previously entered route has been deactivated (RREQ). Each flow of data transmission's associated next-hop data is stored by the source node and intermediate nodes.

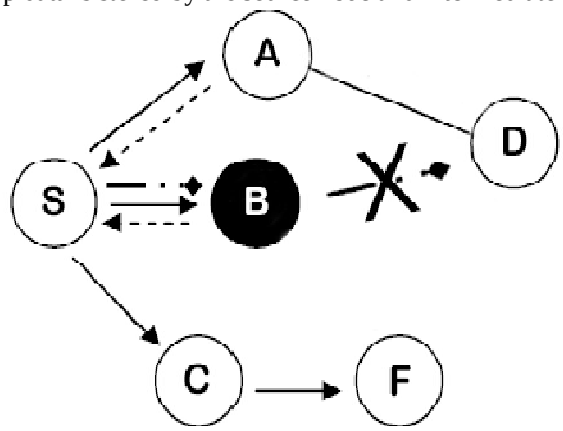


Figure 2 Routing discovery in AODV under black hole attack

III. LITERATURE REVIEW

Black hole detection has become a hot topic of research recently, and numerous techniques have been put forth. The majority of solutions, however, are only able to identify and stop solitary black hole attacks, and they have a high overhead to identify cooperative and intelligent adaptive attacks. Discusses a few of these works that have been presented as remedies.

In [8], R. Khatoun et al a reputation system for detecting black hole attacks has been proposed; a watch dog is employed to monitor the alteration of data in received packets. On the other hand, the nodes that regularly drop packets are identified using a reputation score. The calculation of a vehicle's reputation score is based on the reports sent by its neighbours, hence this method fails in the presence of coordinated black hole attacks.

Roshan et al. have described a routing approach in [9] to identify and block rogue nodes. The concept behind the proposed technique is based on double acknowledgement packets, meaning each intermediate node must notify the source node that it has forwarded the packet. When the goal is attained, the procedure is over. This approach causes significant network overhead and additional delay.

In [10], A innovative approach was put out by Sathish et al. to lessen the effects of both individual and group black hole attacks. Their plan involves broadcasting a phoney RREQ with an imaginary target address. Any node that responds to the RREQ is added to the list of black holes. A cooperative black hole in this solution is any node that has a next hop node listed as a black hole. The author suggested utilising a digital signature and a trust value as a second method to stop the black hole impact. The outcomes of the simulation demonstrate that the suggested approach adds additional latency.

In [11], Chaker et al. proposed using threshold adaptive control a method for the detection of selfish and malevolent intelligent nodes. However, the amount of lawful and malevolent behaviours is used to calculate both direct and indirect trust. A node and its are assessed to have a direct level of trust. Neighbor On the other hand, indirect trust is determined by one hop neighbours' recommendations for other automobiles. However, this falls short in the event of a coordinated black hole attack.

P.S. Hiremath et al. presented a fuzzy interference adaptive system to find and stop the black hole attack. Four inputs were utilised in [12] for the Fuzzy Interference System (FIS): energy, data rate, data loss, and trust (characterize the quality of next hop neighborhood). Each node sends this information on a regular basis to update neighbour information. The procedure of choosing the next hop neighbour employs the fuzzy interference technique. This approach is contrasted with an adaptive method [13], and the simulation results indicate that the suggested solution performs better.

In [14], Sagar R Deshmukh et al. suggested an AODV-based secured routing to recognise and stop individual and group black hole assaults. The authors' plan is to maintain the RREP's fundamental AODV mechanism while giving it a validity value. In comparison to the standard AODV, the simulation results demonstrate effective defence against black hole attacks with very low overheads. An intelligent malicious node might simply set the validity in the same way that it claims to have the shortest and freshest route to a target node since the intelligent adaptive black hole in the network renders this method useless.

IV. BLACK HOLE ATTACKS (BHAS) IN VANETS

VANETs are susceptible to a variety of security attacks, including denial of service (DoS) attacks, Sybil attacks, wormhole attacks, flooding attacks, impersonation attacks, jellyfish attacks, GHA attacks, and BHA attacks, due to the highly dynamic, open-access medium, distributed infrastructure, and protocol design issues. [15,16,17,18]. The applications and services offered by VANETs may be jeopardised as a result of the existence of these assaults.

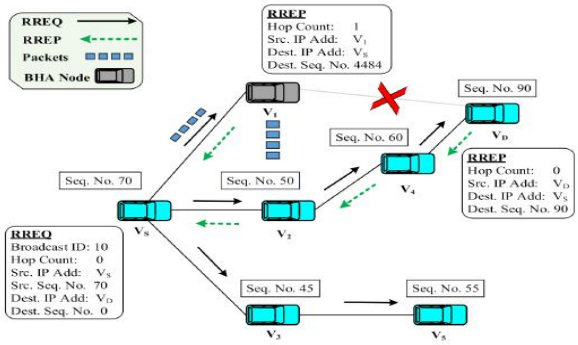


Figure 3 Black hole attack.

When a malicious node totally discards packets from a legal node, it is known as a BHA. A rogue node in a BHA will instantly send a bogus RREP in response to an RREQ packet it gets from the source node without first consulting its routing table. This RREP packet, which is thought to be the shortest and most recent route in AODV [20,21], has a higher sequence number and minimum hop count value.

The bogus RREP packet is received by the source node, which mistakenly views it as an efficient path and begins sending data packets to the black hole node. Such packets are dropped by a BHA rather of being sent to their intended destination, which compromises the overall security and performance of the network and disrupts the information-sharing process. These packets could include urgent information messages that need to be given right away and within a certain window of time, such warnings and emergency notifications. Dropping such packets could lead to traffic fatalities, accidents, backups, and congestion in a very dynamic VANET. In this study, our main goal was to identify the BHA problem in VANETs and suggest a fresh, more effective approach. A BHA, one of the most harmful attacks in VANETs, forms the basis for DoS attacks that prevent the network service from functioning to the intended users. A BHA in the AODV protocol is described with the aid of an example situation in Figure 3 above. For instance, the destination vehicle VD wishes to communicate with the source vehicle versus. An RREQ packet is broadcast by vs to all of its nearby cars, namely V1, V2, and V3. V1 instantly replies with a false RREP that has a higher spoof destination sequence number (DSN) value after getting the RREQ (4484). Vehicles V2 and V3 simultaneously broadcast the RREQ packet to their next-hop vehicles while increasing their hop count values in the packet by one. In the interim, V1 sends Vs. the first RREP. So, source vehicle vs. chooses a path to destination VD that passes via V1 (i.e., black hole attacker), and then it begins sending data packets along that route. As soon as it receives the packets, V1 decides not to send any of them on to VD. The source vehicle VS discards any RREPs that arrive later.

V. PROPOSED WORK

Identifying the problem

The VANET faces significant technological challenges in terms of dependability and secure routes because despite its intrinsic power, it is vulnerable to both internal and external adversaries. Instead of using road construction, the attacker's driving style is a costly and risky way to reduce network traffic and increase the possibility of a careless path.

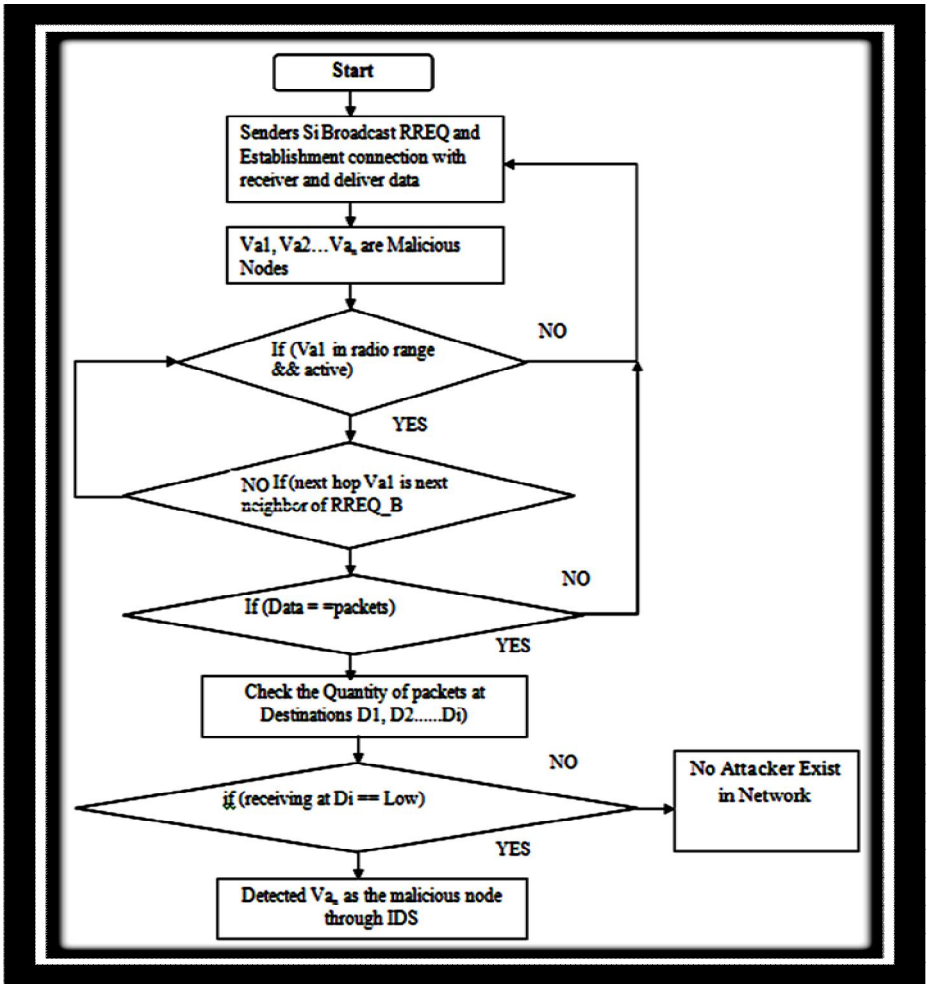


Figure 4 Flow chart of attacker detection

The violent behaviour on the network is brought on by the presence of a Blackhole attacker. Along with providing assurances of safety, some devious or malicious vehicles also cause harm to the system by providing inferior services or placing the vehicles of customers in danger. Therefore, finding those vehicles that are destructive or immoral is an essential part of VANET defence. Automobile users who are harsh may behave viciously in one way and not in another. The attacker can manufacture phoney information on the network and simultaneously throw all of the network traffic packets upon it. Offensive vehicles produce overhead as a result of the packets' considerable loss to the network. Despite the fact that packet redistribution decreases network latency, the presence of blackholes prevents it from managing traffic conditions and removing congestion. Planned SDSR For the secure transmission of multi-hop data packets, dangerous vehicles must be detected and stopped.

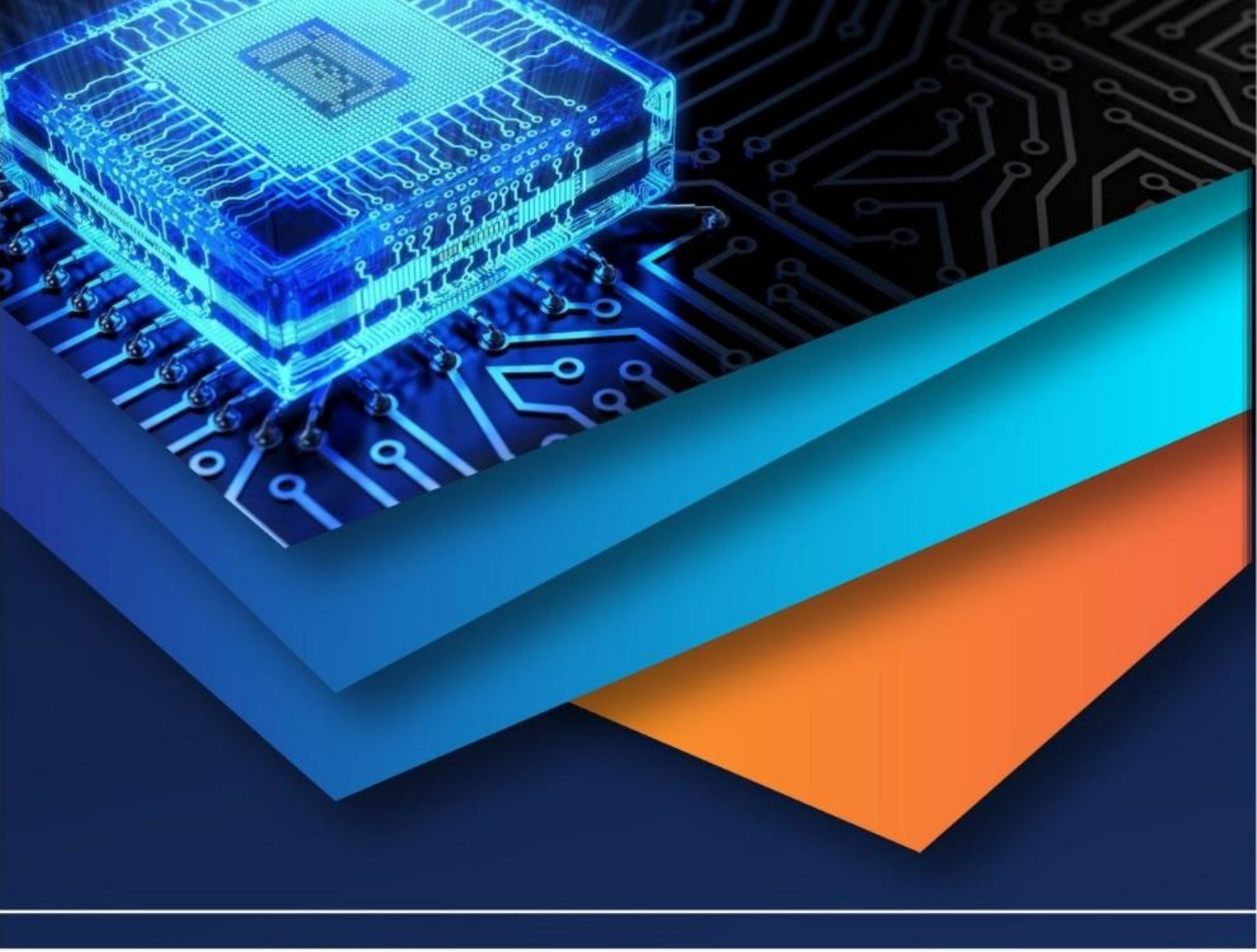
VI. CONCLUSIONS

Newer security measures have prompted the rise of numerous new threats. This paper discusses intelligent black hole attacks and suggests a method to thwart them. The simulation results demonstrated the effectiveness of the suggested approach because it can guarantee high packet delivery ration and throughput with almost the same end to end delay and routing overhead as the basic AODV. The idea also provides a high detection ratio in both low and high vehicle densities.

The suggested strategy is also compatible with other reactive routing protocols, so in future work, we intend to implement it and assess how well it performs for these other reactive protocols, including the Dynamic MANET on Demand (DYMO) routing Protocol, as well as how well it performs against comparable attacks, like the Grey Hole Attack.

REFERENCES

[1] Vehicule to vehicule communication. Available online: https://www.nhtsa.gov/technology- innovation/vehicle-vehicle-communications (accessed on April 2017).
[2] Elias C. Eze, Sijing Zhang and Enjie Liu," Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward", Proceedings of the 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, 2014.
[3] Surmukh, S.; Kumari, P.; Agrawal, S. Comparative Analysis of Various Routing Protocols in VANET. In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22February 2015.
[4] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications, 2013, pp. 29-38.
[5] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, February 1999, pp. 90-100.
[6] C. Perkins, E. Belding-Royer and S. Das, "Ad Hoc On-Demand Distance Vector (AODV)Routing", Network Working Group, Request for Comments, 2003.
[7] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan," Denial of Service (DOS) Attack and Its Possible Solutions in VANET", International Scholarly and Scientific Research & Innovation 4(5) 2010, World Academy of Science, Engineering and Technology, Vol:4 2010-05-25.
[8] R. Khatoun, P. Guy, R. Doulami, L. Khoukhi and A. Serhrouchni, "A Reputation System for Detection of Black Hole Attack in Vehicular Networking," International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC), 2015.
[9] Roshan Jahan, Preetam Suman, "Detection of malicious node and development of routing strategy in VANET," 3rd International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp. 472-476, 2016.
[10] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Single and Collaborative Black Hole Attack in MANET," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, pp.2040-2044, 2016.
[11] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control," 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), IEEE, 2016.
[12] P.S Hiremath and Anuradha T, "Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs", International Conference on Information Science (ICIS), pp.245-251, 2016.
[13] P.S Hiremath and Anuradha T, "Adaptive Method for Detection and Prevention of Cooperative Black Hole Attack inMANETs", International Journal of Electrical and Electronics and Data Communication, Volume-3, Issue-4, pp.1-7, 2015.
[14] 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.
[15] Arif, M.;Wang, G.; Bhuiyan, M.Z.A.;Wang, T.; Chen, J. A survey on security attacks in VANETs: Communication, applications and challenges. Veh. Commun. 2019, 19, 100179.
[16] Sheikh, M.S.; Liang, J. A comprehensive survey on VANET security services in traffic management system. Wirel. Commun. Mob. Comput. 2019, 2019, 2423915.
[17] Malhi, A.K.; Batra, S.; Pannu, H.S. Security of vehicular ad-hoc networks: A comprehensive survey. Comput. Secur. 2020, 89, 101664.
[18] Sleem, L.; Noura, H.N.; Couturier, R. Towards a secure ITS: Overview, challenges and solutions. J. Inf. Secur. Appl. 2020, 55, 102637.
[19] Gurung, S.; Chauhan, S. Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. Wirel. Netw. 2019, 25, 975–988.
[20] Panos, C.; Ntantogian, C.; Malliaros, S.; Xenakis, C. Analyzing, quantifying, and detecting the blackhole attack in infrastructureless networks. Comput. Netw. 2017, 113, 94–110.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY