OAIJSE

OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

REVIEW ON BLACK HOLE ATTACK IDENTIFIER USING VANET COMMUNICATION IN VECHICLE

[1]Arvindakshan S R, [2]Sai Praneeth Reddy Gogula, [2]I.M Satya Sainath,[2]B.Sai Girish, [2]Rohit Alex Badana, [2]Y.Jashwanth Raj

[1]Department of Cyber Security and Digital Forensics, Vellore Institute of Technology, Bhopal

[2]Department of Computer science Engineering, GITAM Demmed, to Be university, Visakhapatnam, India -530046

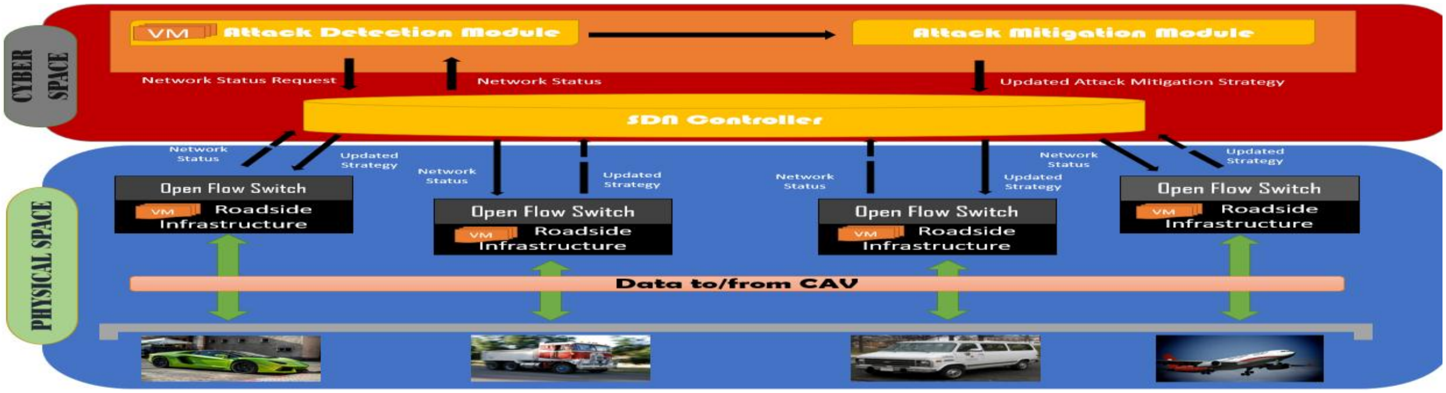
arvind9600akshan@gmail.com

Abstract:- In current generation, the proliferation of autonomy of next generation facilitates the use of independent cars, connected cars and electromobility. It brings new target surfaces that influence the community for high impact cyber threats. To address the cyber-security challenges faced by modern automobiles, a constructive and diversified approach is needed that combines techniques from different fields of ICT. In the next generation mobility ecosystem, emerging innovations such as 5G, LiDAR, new road and roadside sensors and intelligent charging in current automobiles a new problems and potentially protection vulnerabilities. This research proposes a systematic cybersecurity risk management process for vehicles.This includes an appraisal framework and formal measurement approaches to resolve vulnerability improvements, the evaluation, goal and the evidence available during the vehicle life cycle. The level of impact and the level of viability of attack are evaluated in risk assessment and risk analysis. The automotive cyber security risk matrix is then designed to provide a quantitative risk index using a global classification algorithm. The proposed evaluation process aims to derive automotive cyber systematically Improvement AODV in this research by integrated a novel lightweight methodology using detectors and baiting to diagnose and isolate single as well as cooperative black-hole attacks. The MANET node will identify and separate the black-hole nodes in the network during the complex topological change in the suggested technique. Employing NS-2.35 simulations methods for the execution of the proposed methodology. The results of the technique suggested are very similar to the native AODV without black holes in terms of efficiency, End to End Delaying and PDR Analysis studied.

Keywords: Cyber-Security, VANET, MANET, Routing Protocols, Black-Hole attack, Cyber threats, E-Vehicles

---

Graphical Abstract:



1. INTRODUCTION

VANET is represented as an ad-hoc vehicle that works to ensure road safety and manages road transport through its smart transport system [1]. In the network, protection and privacy are a crucial problem for VANET because the dispersed architecture makes the network safer during the conversation [2]. VANET manages road safety and monitors traffic jams by intelligent network transportation [3]. It enables coordination between various vehicles. VANET regards the vehicles as the nodes of mobility and thus safety in the wireless link is an important concern. VANET is a technology to automatically form a network and to disrupt the network if it is not necessary [4]. VANET is a MANET subsection (Mobile Ad-hoc Network). MANET is a mobile network technology, while VANET technology is used on vehicle networks. The only distinction is that MANET works with the IEEE 802.11m and VANET works for Wi-Fi on IEEE 802.11p technology [5]. The pace of vehicle networks is higher than mobile networks while sharing data. Vehicle networks are hierarchical and structured, the nodes know their network's route, but cellular modems are unstructured. In VANET, complex algorithms and encryption techniques can be applied on vehicle networks, although MANET does not apply to these complex algorithms and encryption techniques. Mobility networks have a power challenge, but VANET has no problem battery capacity [6]. The attacker node assumes that it has the shorter path to every chosen node in the Network and therefore, all packets are passing through it. This allows the black hole node to forward or discard packets while passing traffic.Normal nodes are accepts any response to their requests and to the Black-hole node that they thrive from this and want to respond to a request that it has the shortest route to the node it desires. Nodes normally begin exploration to find a route to the destination node [7]. The source node transmits a message to the target node and any node accepting this request verifies whether the node has a new route to the target node. When this message is received by the Black-hole Node, the broadcaster automatically responds that the station has the clear and shortest path to the destination node [8]. This response was supposed by the source node since there is no mechanism for verifications. Source node assumes that the response is provided since the request cannot be checked by any process from a regular node or a black node [9]. The source node starts transferring packets to the black node with the intention of sending them to the destination node and then the black node begins to drop them. Black-hole attacks can be divided into two types: individual black-hole and cooperative attacks in which the classification is depends on the quantity of attacker nodes. An individual black-hole attack only has a specific attacker node and a party of attacker nodes is involved in the co-operative black-hole attack to weaken the stability of the network [10].

In this study the routing protocol of AODV is chosen since it provides superior performance than other reactive routing protocols in several performance measurement methods, according to [5]; it combines the techniques of both DSR and DSDv, and has the benefits. although AODV is better than other reactive routing protocols. The construction of two nodes using AODV requires different sorts of control packets termed route request (RREQ) and route response (RREP).RREQ will be broadcast to nearby nodes to request a route to a desired node, nodes will continue to forward RREQ until the destination node or a node that has a path towards it hits the destination node. RREP is sent from the destination node to the source node, or from a path to the destination node. After an RREP source node is sent, packets will be sent to the destination node [11-15]. In reactive routing protocol performance was investigated under various types of attacks. The efficiency of attacks, in particular of the Packet Delivery Ratio (PDR), decreased during the black-hole attack.

2. Problem Statement

The safety of MANET is important to avoid the damage that various types of attacks may do. The black hole attack is regarded as one of the common attacks that damage the network and attempt to avoid any network link. AODV routing protocol can find the shortest path to communicate in the network between two nodes where the path is necessary. An algorithm to detect and avoid the black-hole attack is not used in AODV protocol. The aim of this paper is to improve the AODV routing protocol with a lightweight technology for detecting and preventing the black-hole attack in the network.

In this section, we have explained the techniques developed in particular to bait the attacks of black hole in reactive routing protocol and the restrictions of each technique as well as black hole attacks circumvent the technique developed. We mean the intruder node knows the strategy and can use all its functionality against the other MANET nodes with regard to an intelligent black hole attack connection.

3. Existing Study

3.1 Strategy of Baiting

The strategy of baiting is based on the node id of yourself. A bait request is sent to all neighbouring nodes for the identification of the black-hole node. The bait request includes a Source Sequence Number (SSN) and a source id; it tests whether the source node receives a response with a higher DSN than its own SSN; this means that the response was sent from a black hole since the network node could have a higher DSN compared to the source node. Since the black-hole node has been detected in a network, a Black-hole warning would be sent to all neighbouring nodes [16].

II LITERATURE REVIEW

RREQ source

The drawbacks of this approach are that an intelligent black-hole node will verify if the recipient RREq is requesting a path to the same RREQ source. The black hole warning can also be used by a smart black node and false black hole warnings may be transmitted to separate selective nodes from the network. a technique that relies on the process of Cooperative Bait Detection Scheme (CBDS) [17]. In CBDS, the black hole identification is divided in Bait, Tracking, and Reactive Defense in three steps. In Bait process, the source node randomly selects one of its adjacent and sends a bait application with its id. A list of the suspect node in reverse traces stage

In Reverse Trace the RREP of the Bait RREQ will have a list of suspicious nodes and then in promiscuous mode will join the neighbour nodes to detect if an intruder node is in the path. A black-hole warning is sent to neighbouring nodes with each black-hole node found on the network. If the PDR is smaller than a certain level in Reactive Defense process source node, the PDR is running again in Bait phase. This strategy is limited by the fact that nodes join a promiscuous mode, which is not suitable to all nodes. Because certain nodes do not want unauthorized users to listen to their own packets, it also facilitates passive attacks in real time. The Blackhole Warning function can be used by a smart black-hole node and false black hole warnings can started differentiating to differentiate network nodes [18].

Black Hole Attacks

The technique is created with the help of timers and baiting message to avoid smart black-hole attacks. The Blackhole attack is known as a Denial-of-Service (DOS) Sequence Number Attack (SNA) since it uses packet drop sequence numbers as shown in table 1 . The series number is a numbering system maintained by the RREQ and RREP messages root node. For root finding, RERR, and HEY messages, the root maintenance, the hop numbering and the serial numbers are then used for the RREQ and the RREP packet in the AODV routing prototype. RREQ will be broadcast to nearby nodes to request a route to a desired node, nodes will continue to forward RREQ until the destination node or a node that has a path towards it hits the destination node. RREP is sent from the destination node to the source node, or from a path to the destination node. After an RREP source node is sent, packets will be sent to the destination node. In reactive routing protocol performance was investigated under various types of attacks [19, 20]. The efficiency of attacks, in particular of the Packet Delivery Ratio (PDR), decreased during the black-hole attack.

Reactive Routing Protocol

The receptive steering is outfitted with another moniker named on-request directing convention. Not like the proactive directing, the responsive steering is just begun when hubs want to communicate information bundles. The strength is that the squandered data transfer capacity instigated from the consistently broadcast can be decreased. In any case, this may likewise be the deadly injury when there are any vindictive hubs in the organization climate. The shortcoming is that detached steering technique prompts some parcel misfortune. Here we momentarily portray two pervasive on-request steering conventions which are imprompt on-request distance vector (AODV) and Dynamic Source Directing (DSD) convention [21].

AODV is constructed based on DSDV routing. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node can't be reached from the source node, the route discovery process will be executed immediately. In the route discovery phase, the source node broadcasts the route request (RREQ) packet first. Then all intermediate nodes receive the RREQ packets, but parts of them send the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. [22] On the other hand, the route maintenance process is started when the network topology has changed or the connection has failed. The source node is informed by a route error (RRER) packet first. Then it utilizes the present routing information to decide a new routing path or restart the route discovery process for updating the information in routing table.

The plan thought of DSR depends on source steering. The source directing implies that every information parcel contains the steering way from source to objective in their headers. Not at all like the AODV which just records the following bounce data in the directing table, the portable hubs in DSR keep up their course reserve from source to objective hub. As far as the above conversation, the directing way can be controlled by source hub on the grounds that the steering data is recorded in the course reserve at every hub. Notwithstanding, the presentation of DSR diminishes with the portability of organization builds, a lower parcel conveyance proportion inside the higher organization versatility [23].

Single Black Hole Attack

A black hole attack means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbours. A single black hole attack is easily happened in the mobile ad hoc networks. As a result, node malicious node is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely [24].

Neighbourhood-based and Routing Recovery Scheme

Bo Sun and Alem *et al.* use AODV as their routing example, and claim that the on-demand routing protocols such as DSR are also suitably applied after a slightly modified. The detection scheme uses on a neighbourhood-based method to recognize the black hole attack, and a routing recovery protocol to build the correct path. The neighbourhood-based method is employed to identify the unconfirmed nodes, and the source node sends a *Modify_Route_Entry* control packet to destination node to renew routing path in the recovery protocol [25].

In this scheme, not only a lower detection time and higher throughput are acquired, but the accurate detection probability is also achieved. To deserve to be mentioned, the routing control overhead does not increase in Bo Sun *et al.*'s proposal. However, this scheme is useless when the attackers cooperate to forge the fake reply packets.

Redundant Route Method and Unique Sequence Number Scheme

Himral *et al.* propose two solutions to avoid the black hole attacks in MANET. The first solution is to find more than one route from the source node to the destination node. In other words, there exist some redundant routes within the routing path, and authors assume there are three routes at least in the scenario. The working flow of redundant route mechanism is described briefly as below. First, the source node sends a ping packet, a RREQ packet, to the destination. The receiver who has a route to the destination will reply this request, and a acknowledge examination is executed at source node. Then the sender will buffer the RREP packet until there are more than two received RREP packets, and transmit the buffered packets after identifying a safe route. It represents that there are at lowest two routing paths coexisting at the same time. After that, the source node recognizes the safe route from the number of hops or nodes, and prevents the black hole attacks [26].

In the simulation results, these two solutions have less RREQ and RREP numbers than AODV. Furthermore, solution two is better than solution one due to the sequence number included in every packet in the original routing protocol. The communication overhead can be eliminated by this solution because of the inbound cryptography method. Nevertheless, the cooperative black hole attacks can't be detected in both proposed solutions. The redundant route and unique sequence number can be easily broke by two collaborative black hole nodes.

Collaborative Black Hole Attack

There are various mechanisms have been proposed for solving single black hole attack in recent years. However, many detection schemes are failed in discussing the cooperative black hole problems. Some malicious nodes collaborate together in order to beguile the normal into their fabricated routing information, moreover, hide from the existing detection scheme. As a result, several cooperative detection schemes are proposed preventing the collaborative black hole attacks [27]

DRI Table and Cross Checking Scheme

Shahabi *et al.* exploit data routing information (DRI) table and cross checking method to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology [].

The procedure of proposed solution is simply described as below. The source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the IN's honesty. After that, SN sends the further request to IN's NHN for asking its routing information, including the current NHN, the NHN's DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path [28].

Bait DSR (BDSR) based on Hybrid Routing Scheme

Khin EE et al. And Po-Chun Tsou et al. designed a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing. This solution is briefly introduced as below.

In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and non-existent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. All of the response sent by the adversaries should be drop. After the initial phase, authors employ the original DSR route discovery procedure. If the data delivery rate is lower than the pre-defined threshold value, the bait procedure will be triggered again to examine the uncertainly suspicious nodes [29,30].

Compare with the primitive DSR scheme and watch dog method, the simulation results show that BDSR provides an excellent packet delivery rate. The packet delivery ratio of BDSR is 90% which is more superior to DSR and WD approach. Moreover, the communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

A technique based on the Cooperative Bait Detection System has been developed. In CBDS, the detection of a black hole in bait and reverse trace and reactive defence is split into three stages. At the Bait source node, one of the neighbours is selected by chance and the ID is used for sending a bait request as shown in fig.1 . A list of suspect nodes is built in the reverse trace step in the RREP of the bait RREQ, and the next nodes enter promiscuous mode to detect whether an intruder node is on the track. A black-hole warning is transmitted on neighbouring nodes on each black-hole node found in the network [31].

If the PDR is less than a defined threshold in reactive defence source node tests, Bait process is re-executed. This strategy is limited by the fact that nodes join a promiscuous mode which is not suitable for all nodes. Since some nodes do not allow unauthorized users to listen to their own packets, it also makes passive attacks possible in promiscuous mode. The black-hole warning can be used by an intelligent black node and false black-hole warnings start being transmitted to isolate network nodes.

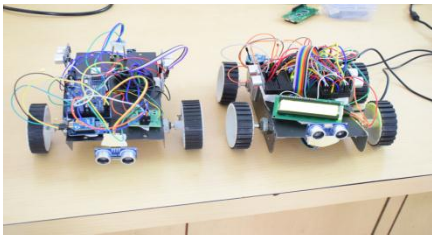
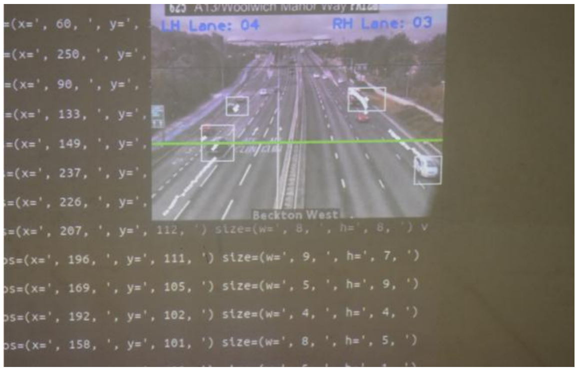


Fig. 1: Prototype for Vehicular ad hoc networks(VANET)

The methodology suggested is designed with timers and messages to avoid intelligent black attacks. Blackhole attack is known as the Denial-of-Service (DOS) sequence number assault (SNA) since it uses packet dropping sequence numbers. The number for the sequence is a count scheme maintained by the RREQ and RREP source Node. For the root exploration, RERR and HEY messages, RREQ and RREP packets are therefore used in root management, hop numbers, and serial numbers in the AODV routing protocol [32]. As shown in table 2.

This protocol assigns the target sequence number for each root entry from the routing table. The Routing Protocol of the AODV routing protocol contains separate fields of RREQ and RREP communications. The malicious node uses this field knowledge to develop from the RREQ packet from its neighbouring node. This increases the sequence number for the destination and sends a receipt packet to the RREQ source node. Misleading node raises the target sequence number and transfers the packet back to the source node. It transcends the smaller target series and addresses the neighbour and redirects the entire network traffic into a malicious node. The attack on Blackhole drops all VANET data packets to reduce VANET's total performance stimulation as shown in fig. 2 . A solution in the form of the modern Secure AODV route protocol, an updated version of the original AODV routing protocol, is created to identify the black hole attack in the AODV routing protocol. The RREQ packet and packet protocol RREP modifications are performed [33].

Before sending the packet the node will be verified.The methodology proposed ensures that every black-hole node that permits connection between MANET nodes is detected self-isolated. The methodology suggested does not use the black hole alarm, to avoid the use of this function by false alarms by a smart black-hole node. In order to prevent congesting the system with bait requests and responses, we have set the TTL of the bait message. Randomness in fake id as well as in bait-timer would not enable the black-hole node to recognise a trend to oppose it. No overhead packages and special packages make it lightweight [34].



```
=(x=', 60, ', y=',
=(x=', 250, ', y=',
=(x=', 90, ', y=',
=(x=', 133, ', y=',
=(x=', 149, ', y=',
=(x=', 237, ', y=',
=(x=', 226, ', y=',
=(x=', 207, ', y=', 112, ') size=(w=', 8, ', h=', 8, ') v
s=(x=', 196, ', y=', 111, ') size=(w=', 9, ', h=', 7, ')
s=(x=', 169, ', y=', 105, ') size=(w=', 5, ', h=', 9, ')
s=(x=', 192, ', y=', 102, ') size=(w=', 4, ', h=', 4, ')
s=(x=', 158, ', y=', 101, ') size=(w=', 8, ', h=', 5, ')
```

Fig. 3 : Vehicular Tracking Networks

III CONCLUSION

The suggested approach is much superior in contrast. The deletion ratio of the END-2-END for a variety of malicious nodes. The average delay from end to end for the work proposed is 0.03375 while the current protocol for AODV routing is 0.0812

Blackhole Attack is one of the VANET safety challenges. The objective of this study is to alleviate the Blackhole attack by means of the AODV Safe Protocol. Blackhole Attack in VANET is a critical activity for detecting and identifying the network. The malicious node drops the packets, and it also disrupts the path and renders it. The suggested AODV routing algorithm detects and aids in elimination of the malicious node from the network successfully. The results reveal that, comparing with the AODV routing protocol, the amount of missing packets is much smaller with the proposed AODV. Performance rate is quantified and evaluated

The efficiency of packet distribution is quantified and analysed. The average performance of the solution is 73.27 for different malicious nodes, compared with 27.31 for the AODV current routing protocol. The suggested solution has an average PDR of 77.64; An average PDR for the current AOD V-routing protocol is 31.56. In order to improve black-hole detection capabilities while maintaining the throughput, final-to-extension and package delivery ratios, TBBT suggested combines both timers and baiting strategies.The simulation outcomes of the methodology proposed showed that the delay, performance and Packet Delivery Ratio are closely related to the AODV. The proposed model is improved in order to also increase the delivery ratio of the throughput and package to decrease the delay. Simulation findings show that the Network PDR is lowered by the Black Hole attack. PDR improves after the infected node has been detected successfully and removed. The proposed approach offers robust results compared to current approaches. Although it is difficult to identify the Black Hole attack due to VANET limitations.

REFERENCE:

[1] Kumar, A., Dadheech, P., Goyal, D., Patidar, P.K., Dogiwal, S.R. and 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), pp.263-274.

[2] Kudva, S., Badsha, S., Sengupta, S., La, H., Khalil, I. and Atiquzzaman, M., 2021. A scalable blockchain based trust management in VANET routing protocol. Journal of Parallel and Distributed Computing.

[3] Selvi, M. and Ramakrishnan, B., 2021. Secured Message Broadcasting in VANET using Blowfish Algorithm with Oppositional Deer Hunting Optimization.

[4] Waseem, R.M., Khan, F.Z., Ahmad, M., Naseem, A., Jhanjhi, N.Z. and Ghosh, U., 2021. Performance Evaluation of AOMDV on Realistic and Efficient VANet Simulations. Wireless Personal Communications, pp.1-20.

[5] Chander, B., 2021. Challenges, Benefits and Issues: Future Emerging VANETs and Cloud Approaches. Cloud and IoT Based Vehicular Ad-Hoc Networks, p.233.

[6] Shaik, S., 2021. A SCENARIO-BASED TRUST MANAGEMENT APPROACH WITH 3R MESSAGE CATEGORIZATION IN VANETS.

[7] Grimaldo, J. and Martí, R., 2018, February. Performance comparison of routing protocols in VANETs under black hole attack in Panama City. In 2018 International Conference on Electronics, Communications and Computers (CONIELECOMP) (pp. 126-132). IEEE.

[8] Tyagi, P. and Dembla, D., 2017. Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). Egyptian informatics journal, 18(2), pp.133-139.

[9] Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S.S., Kumar, V.A., Panigrahi, B.K. and Veluvolu, K.C., 2021. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems, 80, p.103352.

[10] Hamdi, M.M., Audah, L., Abood, M.S., Rashid, S.A., Mustafa, A.S., Mahdi, H. and Al-Hiti, A.S., 2021. A review on various security attacks in vehicular ad hoc networks. Bulletin of Electrical Engineering and Informatics, 10(5), pp.2627-2635.

[11] Sathyaraj, P. and Kannan, K., 2021. Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs.

[12] Kannan, K., Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs.

[13] Datta, D. and Kapoor, C., Security Constraints, Solutions and IDS In Vehicular Network: A Review.

[14] Mustafa, A.S., Hamdi, M.M., Mahdi, H.F. and Abood, M.S., 2020, November. VANET: Towards Security Issues Review. In 2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT) (pp. 151-156). IEEE.

[15] K. Khajavi and N. Hajhassan, "A Mechanism for Detecting and Identifying DoS attack in VANET," International Journal of Information, Security and Systems Management, vol. 7, pp. 737-744, 2018.

[16] M. Y. Su, “Prevention of selective blackhole attacks on mobile ad hoc networks through intrusion detection systems,” Comput. Commun., vol. 34, no. 1, pp. 107–117, 2011.

[17] N. K. Chaubey, “Security analysis of vehicular Ad hoc networks (VANETs): A comprehensive study,” Int. J. Secur. its Appl., vol. 10, no. 5, pp. 261–274, 2016

[18] Y.-C. HU, A. PERRIG, and D. B. JOHNSON, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. - Int. Conf. Netw. Protoc. ICNP, pp. 78–87, 2005.

[19] P. A. N. Upadhyaya, “Blackhole Attack Prevention in VANET,” Int. J. Futur. Revolut. Comput. Sci. Commun. Eng., vol. 3, no. October, pp. 222–229, 2017.

[20] A. Muhtadi, D. Perdana, and R. Munadi, “Performance evaluation of aodv, dsdv, and zrp using vehicular traffic load balancing scheme on vanets,” International Journal of Simulation System, Science and Technology (IJSSST), pp. 13.1– 13.7, 2015.

[21] K. S. Nisha and S. K. Arora, “Analysis of black hole effect and prevention through ids in manet,” American Journal of Engineering Research (AJER), vol. 2, no. 10, pp. 214–220, 2013

[22] Sunkara, S.C., Balaji, R. and Babu, M., 2020. A critical investigation on ultrasound cyber-attack and using fourier transform for defence application against inaudible-attacks. Materials Today: Proceedings.

[23] Samuel, C.E., Kathiresh, K. and Ramachandran, B., 2021. Matlab Algorithm For Driving Pattern Detection And Analysis Using Smartphone Sensors. Information Technology In Industry, 9(1), pp.1457-1470.

[24] Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J. and Nygard, K.E., 2003, June. Prevention of cooperative black hole attack in wireless ad hoc networks. In International conference on wireless networks (Vol. 2003, pp. 570-575).

[25] Alem, Y.F. and Xuan, Z.C., 2010, May. Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. In 2010 2nd International Conference on Future Computer and Communication (Vol. 3, pp. V3-672). IEEE.

[26] Himral, L., Vig, V. and Chand, N., 2011. Preventing aodv routing protocol from black hole attack. International Journal of Engineering Science and Technology (IJEST), 3(5), pp.3927-3932.

[27] Patcha, A. and Mishra, A., 2003, August. Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In Radio and Wireless Conference, 2003. RAWCON'03. Proceedings (pp. 75-78). IEEE.

[28] Shahabi, S., Ghazvini, M. and Bakhtiarian, M., 2016. A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Networks, 22(5), pp.1505-1511.

[29] Khin, E.E. and Phyu, T., 2014. Impact of black hole attack on AODV routing protocol. International Journal of Information Technology, Modeling and Computing (IJITMC), 2(2), pp.9-17.

[30] Thachil, F. and Shet, K.C., 2012, September. A trust based approach for AODV protocol to mitigate black hole attack in MANET. In 2012 International Conference on Computing Sciences (pp. 281-285). IEEE.

[31] Choudhury, D.R., Ragha, L. and Marathe, N., 2015. Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack. Procedia Computer Science, 45, pp.564-570.

[32] Das, R., Purkayastha, B.S. and Das, P., 2012. Security measures for black hole attack in manet: An approach. arXiv preprint arXiv:1206.3764.

[33] Sharma, S. and Gupta, R., 2009. Simulation study of blackhole attack in the mobile ad hoc networks. Journal of Engineering Science and Technology, 4(2), pp.243-250.

[34] Singh, S., Mishra, A. and Singh, U., 2016, March. Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm. In 2016 Symposium on Colossal Data Analysis and Networking (CDAN) (pp. 1-6). IEEE.

[35] Wazid, M., Katal, A., Sachan, R.S., Goudar, R.H. and Singh, D.P., 2013, April. Detection and prevention mechanism for blackhole attack in wireless sensor network. In 2013 International Conference on Communication and Signal Processing (pp. 576-581). IEEE.