DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN VANET USING SECURED AODV ROUTING PROTOCOL

Salim Lachdhaf[1], Mohammed Mazouzi[2], Mohamed Abid[3]

[1]Department of Informatics, Faculty of Sciences of Gabes,
University of Gabes, Gabes, Tunisia
[2]Assistant Professor at Higher Institute of Business Administration of Sfax,
Member of CES-Laboratory, University of Sfax, Sfax, Tunisia
[3]Professor at National School of Engineering of Sfax,
Director of CES-Laboratory, University of Sfax, Sfax, Tunisia

ABSTRACT

Vehicular ad hoc networks (VANETs) are becoming popular and promising technologies in the modern intelligent transportation world. They are used to provide an efficient Traffic Information System (TIS), Intelligent Transportation System (ITS), and Life Safety.

The mobility of the nodes and the volatile nature of the connections in the network have made VANET vulnerable to many security threats. Black hole attack is one of the security threat in which node presents itself in such a way to the other nodes that it has the shortest and the freshest path to the destination.

Hence in this research paper an efficient approach for the detection and removal of the Black hole attack in the Vehicular Ad Hoc Networks (VANET) is described. The proposed solution is implemented on AODV (Ad hoc On demand Distance Vector) Routing protocol one of the most popular routing protocol for VANET. The strategy can detect both the single Black hole attack and the Cooperative Black hole attack in the early phase of route discovery.

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, AODV

1. INTRODUCTION

Recently, with the improvement in the wireless communication technologies and the high number of road accidents, vehicular ad hoc network (VANET) are used to provide an efficient Traffic Information System (TIS). According to the National Highway Traffic Safety Administration (NHTSA), vehicle-to-vehicle (V2V) has a high lifesaving potential that address approximately 80 percent of multi-vehicle crashes. [1].

Natarajan Meghanathan et al. (Eds) : NeTCoM, CSEIT, GRAPH-HOC, NCS, SIPR - 2017
pp. 25– 36, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.71503

VANET is a subclass of Mobile Ad-hoc Network (MANET) which consists of number of nodes (vehicles) with the capability of communicating with each other without a fixed infrastructure [19]. However, compared to MANET, VANET has an extremely dynamic topology due to high mobility of vehicles. the nodes tend to move in an organized pattern. Besides, VANETs have a potentially large scale which can comprise many participants and the capacity to extend over the entire road network [2]. Therefore, Routing protocol & Attacks: Lack of centralized management in VANET puts extra responsibilities on vehicles. Hence each vehicle is a part of the network and also manages and controls the communication on that network. Due to the high mobility of nodes the links between vehicles connect and disconnect very often which make routing process challenging. Hence, many researchers have focused on routing in VANET. The main aim of these proposed routing protocols is to maximize Packet Delivery Ratio (PDR) and throughput while minimizing controlling overheads and packet lose ratio. In this direction many routing protocol has been proposed which has important role in organizing the network safety. However, ad hoc routing protocols can be divided into proactive, reactive and hybrid protocols [3], Proactive protocols are typically table driven. Destination Sequence Distance Vector (DSDV), Global State Routing GCR are examples of this type. On the contrary, reactive protocols do not periodically update the routing information. It finds the route only when needed like Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

AODV is the most frequently used reactive routing protocol in VANET [4]. But this protocol is not designed to tackle the security threats. So it's prone to black hole attack, gray hole attack, warm hole attack, Sybil attack, etc. [5].

In this paper, we will concentrate on well-known and Intelligent black hole attack in AODV base VANET. An intelligent black hole attack it's used by a malicious node that intelligently adapt and vary their behavior to avoid the detection and to bypass security solutions. However, as it is mentioned above, AODV is a reactive routing protocol; nodes will only send the control data only when is necessary. The node which has data to send, it generates Route Request (RREQ) packet and broadcasts it. If malicious node (black hole attack) is present in the network, the attacker node, on receiving RREQ message, sends Route Reply (RREP) without even having an actual route to the destination, and will entice all other to route packets through it. The attack becomes more severe if more than one node colludes in attack. Many research works focus on a single black hole attack but are less effective in cooperative and intelligent black hole attacks.

The remaining of this paper is organized as follows: In section II we introduced background of AODV protocol and black hole attack. Relevant related work and their limitations are discussed in section III. Section IV describes the proposed methodology and related algorithm. The simulation experimental outcomes along with the analysis of performance are presented in the Section V. Finally, Section VI contains our conclusions and the future work of our research.

2. AODV ROUTING PROTOCOL AND BLACK HOLE ATTACK

The Ad hoc On-demand Distance Vector (AODV) routing protocol [5][3] uses on-demand approach to find routes, thus, a route is established only when it is needed by a source node to send data packets. There are two mechanisms used in AODV, first is route discovery and second is route maintenance. When a node needs to forward a data packet, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the data packets to the destination. If a route is not available or the previously entered route is inactivated, it buffers the packet and broadcasts a Route Request message (RREQ). The source node and the intermediate nodes store the next-hop information corresponding to each flow of

data transmission.

When an intermediate node receives a RREQ, it either forwards it or generates a Route Reply (RREP) and it does not forward the RREQ any further if it has a valid route to the destination. RREP is a unicast message routed back along the reverse path to the source node. Only the destination node itself or an intermediate node that has a valid route to the destination are allowed to send a RREP to the RREQ's source node, hence, RREQ messages may not necessarily reach the destination node during the route discovery process. This enables quicker replies and limits the flooding of RREQs. This process continues until a RREP message from the destination node or an intermediate node that has a fresh route to the destination node is received by the source node.

However, the source node may obtain multiple routes to a destination for a single RREQ. The destination sequence number is used to identify the latest route. The highest destination sequence number means the freshest path to the destination node, which is accepted by the source node for the data transmission. If two or more paths to the destination node have the same highest sequence number, the source node choses the route with the lowest hop count.

In route maintenance, a route established between two nodes is maintained as long as needed by the node which want to transmit data packets. if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes until the source node is reached. The affected source node may then choose to either stop sending data or reinitiate route discovery process sending a new RREQ message.

AODV is exposed to a variety of attacks since it has no security mechanisms [6]. Black hole attack is one such attack and a kind of denial of service (DoS) attacks [7] where a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the freshest and the shortest path to the destination node even if no such route exists since in AODV, any intermediate node could respond to RREQ message if it has a fresh route.

The main goal of black hole attack is rerouting the network traffic through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh route to the intended destination. Malicious nodes respond immediately to the source node without even checking its routing table by claiming that it has the freshest and the shortest route to the destination on the route reply packet sent to the source node. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and accepts the path through the malicious node to route the data packets. The attacker now drops the received data packets instead of forwarding them to the destination as the protocol requires.

For example, in Fig. 1, the source node (S) needs to send a data packet to node (D), so it broadcasts a route request packet RREQ to its neighbors to find a route to that node. It is assumed that node B is a black hole in the network and the intermediate node A has a fresh route to the destination node (D). the nodes (A, B, C, F) receive the RREQ packet from the source node (S), the node B replies directly using a fake RREP and it claims that it has the highest sequence number and lowest hop count to the destination node (D) without checking its routing table. So, the malicious RREP reaches fastest to the node (S) compared to other replies from other nodes in the network. As result, node (S) accepts the freshet and the shortest route through the black hole node (node B) and sends data packets to the node (D) via this node, the other received RREP packets are rejected (in this example, the RREP packet from the node A is rejected). The source node (S) assumes that the data would reach safely to the destination node but, in fact, the black hole node drops all data packets instead of forwarding them to the destination.

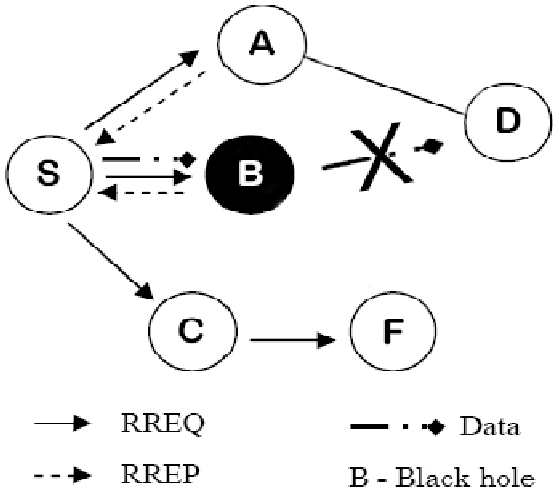

Figure 1. Routing discovery in AODV under black hole attack

This paper provides routing security to the AODV routing protocol by detecting and preventing the threat of Black Hole attacks.

3. LITERATURE REVIEW

Lately, black hole detection has been an active area of research and many solutions have been proposed. However, most of the solutions can detect and prevent only the single black hole attacks and requires high overhead to detect collaborative and intelligent adaptive attacks. Several solutions have been proposed for MANETs can be implemented in VANET. This section discusses some of these works.

In [8], R. Khatoun et al. proposed a reputation system for the detection of the black hole attacks, a watch dog is used to check the modification of information in received packets. In other hand a reputation score is used to identify the nodes that drop packets frequently. This mechanism fails in the presence of cooperative black hole attacks, since, the calculation of the reputation score for a vehicle is based on the reports sent by its neighbors.

Roshan et al. have presented a routing strategy to detect and prevent malicious nodes in [9], the idea of the proposed strategy is based on double acknowledgement packet which means every intermediate node has to inform the source node that it has sent the packet forward. This process ends when the destination is reached. This method adds heavy overhead in the network and extra delay.

In [10], Sathish et al. proposed a novel strategy to reduce the impact of the single and collaborative black hole attacks. In their scheme, a fake RREQ is broadcasted with non-existing destination address. Any node replies to that RREQ is putted in black hole list. In this solution a cooperative black hole is those nodes that have a next hop node listed as black hole. The author proposed a second approach to prevent the black hole impact using digital signature and a trust value. The simulation results show that the proposed scheme creates extra delay.

In [11], Chaker et al. proposed a mechanism for the detection of intelligent malicious and selfish nodes using threshold adaptive control. However, direct and indirect trust are computed based on the number of legal and malicious actions. Direct trust is calculated between a node and its

neighbor. In the other hand, indirect trust is calculated based on the recommendation from one hop neighbors about other vehicles. But this fails if there is a collaborative black hole attack. P.S. Hiremath et al. proposed an adaptive system of fuzzy interference to detect and prevent the black hole attack. In [12], four input used for the Fuzzy Interference System (FIS): trust, data loss, data rate, and energy (characterize the quality of next hop neighborhood). These information are sent periodically by each node to update neighbor information. The system of fuzzy interference is used in the step of selecting of the next hop neighbor. This strategy is compared to an adaptive method [13] and the simulation results shows a better performance for the proposed solution.

In [14], Sagar R Deshmukh et al. proposed an AODV-based secured routing to detect and prevent single and cooperative black hole attacks. The authors idea is to attach a validity value to the RREP and keep the basic mechanism of AODV unchanged. The simulation results show a good performance against the black hole attack with negligible overheads compared to the normal AODV. However, in the presence of an intelligent adaptive black hole in the network, this method falls flat, hence, an intelligent malicious node could easily set the validity in the same way in which it claims that it has the shortest and the freshest route to a target node.

4. PROPOSED MYTHOLOGY

In the basic mechanism of AODV, when a source node has a data packet addressed to a destination node, the source node checks its routing table first which contains the next hop to use to reach the destination node. However, if a valid route is found, the source node sends the data packet to the next hop to forward it to the target node. If no route is found, the source starts route discovery phase and to find new route to the destination. The route discovery phase is initiated by broadcasting a route request message (RREQ). A route reply message (RREP) is sent back if an intermediate node has a valid route to the destination or the RREQ message reach the destination node itself. The solution proposed in this paper makes minor change in basic mechanism of AODV as shown in flow graph of figure 2.

In proposed strategy, Cyclic Redundancy Check 32 bits(CRC-32) [15] is used as hash function. However, as shown in figure 3, the only change made on the AODV message formats is the RREQ message format. In fact, the destination address field is replaced by its CRC-32 value which have the same length (32 bits) [6] that keeps the RREQ message format unchanged and it will not result any extra overhead.

In Accordance to the proposed method, before sending the RREQ, the source node stores the intended destination address and replace it by its CRC-32 value in the RREQ and broadcast it. If an intermediate node receives the RREQ, it sends back a RREP after setting the real address of the destination node only if it's the destination by comparing the CRC32 of its IP address with the destination node address set on the RREQ or, it has a valid route to the destination by comparing the CRC32 value of each route present on its routing table with the destination node address set on the RREQ. Otherwise, the intermediate node sends the RREQ message forward.

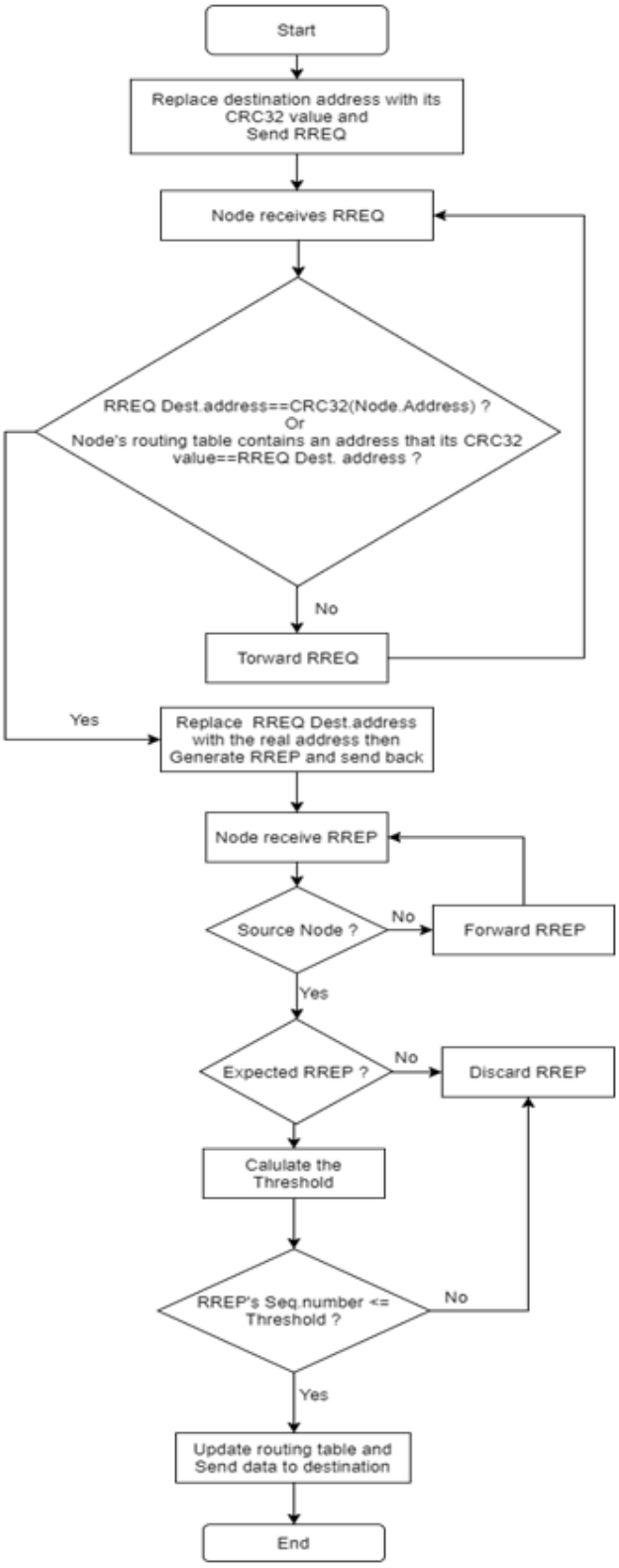

Figure 2. Flow graph of proposed method

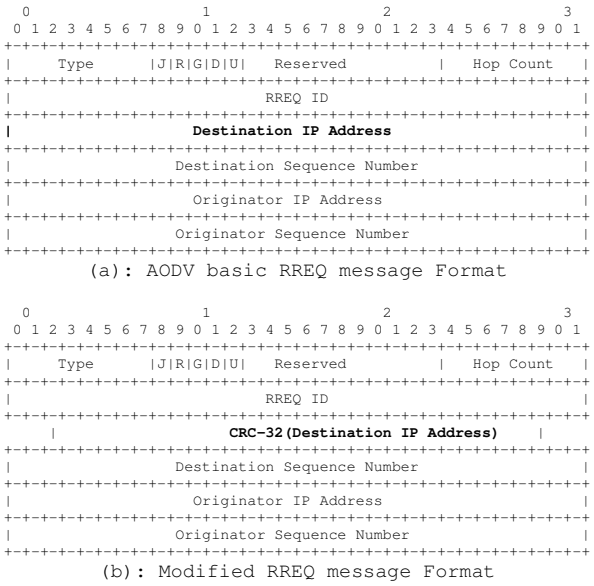

Figure 3. RREQ message format modification

However, for each RREP received, the source node applies two phases of checking:

1- If RREP's source address is not expected (not matching any destination address stored by the RREQ's source node), it will be rejected. Since, only malicious nodes reply for no existing target address.

2- If the RREP is legitimate then compare its sequence number to calculated threshold: if RREP's sequence number **<=** threshold then the source node accepts the RREP and update its routing table, else, the RREP will be rejected. Where the threshold is calculated as following:

   Threshold=*AVERAGE* (all received RREPs' sequence number) + *MIN* (all received RREPs' sequence number).

In the proposed scheme a well-known black hole attack will be prevented from the first phase, but an intelligent adaptive black hole can behave just like a genuine node by checking it routing table and send back a RREP with a high sequence only if it has a route to the destination to be accepted as the freshest route to the destination which will be detected in the second phase.

This method can be used for single black hole detection and prevention as well cooperative black hole attacks, since, if a group of black hole are in collaboration, none of them can get the real address to the destination because the CRC32 is not reversible, hence, according to the proposed solution the unexpected RREP will be rejected.

5. SIMULATION RESULTS AND DISCUSSION

To evaluate the proposed solution, we relied on the NS-2 simulator [16] with the simulation parameters chosen as mentioned in the Table 1. To make further study, and simulation process and analysis we used Network Animator (NAM) [20] as shown in figure 4.

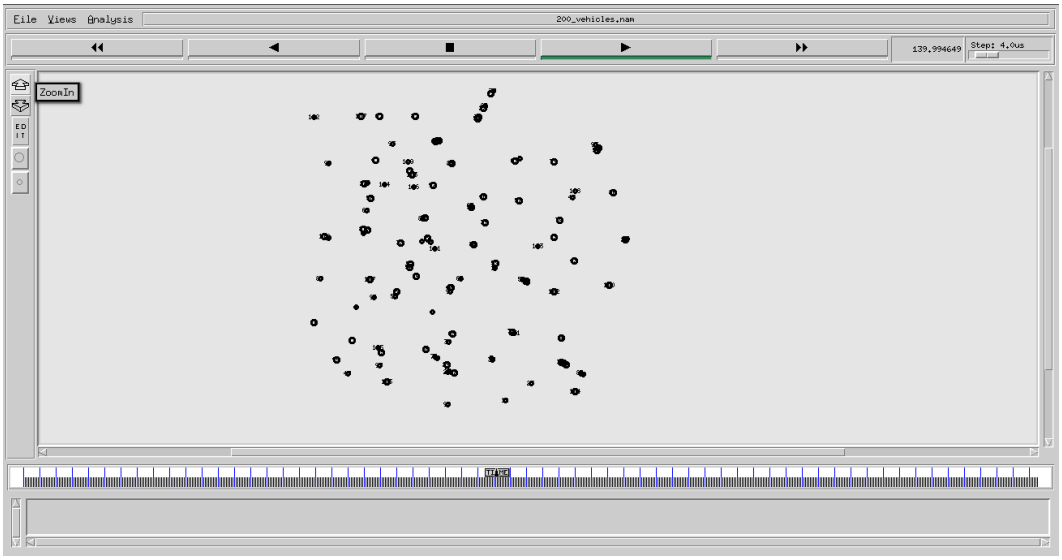

Figure 4: NAM output for the excerpt of the generated NS-2 trace

To generate vehicular traffic, we used SUMO [17] to create mobility traces based on real map (in our case Manhattan map) extracted from OpenStreetMap [18] as shown in figure 5.

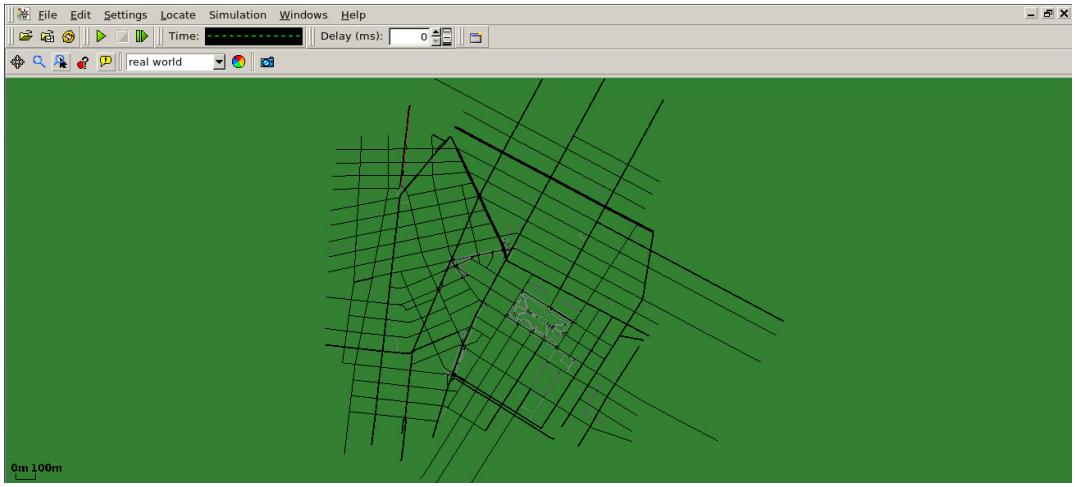

Figure 5: Extracted map from OpenStreetMap for the simulated scenario

Table1: Simulation Parameters

Parameters	**Values**
Simulator	NS2 (Version 2.34)
Simulation area (km x km)	2.5 x 2.5
Simulation time	300 s
Network interface type	WirelessPhyExt
MAC Layer	802.11
Movement Model	Manhattan Grid/Random way Point
Transmission range (m)	250
Permissible lane speed (km/h)	[0,80]
Number of vehicles	[100, 200]

Packet size (byte)	512
Traffic type	CBR
Packet Generation Rate	5 Packets per Second
Routing protocols	AODV, Proposed, [14]
Malicious Node	1

The efficiency of the proposed method is analyzed on the basis of four performance metrics, namely, throughput, packet delivery ratio (PDR), end-to-end delay (ETE) and routing overhead. In our simulation, the proposed scheme and [14] are simulated under an intelligent black hole attack and the results are compared with the fundamental AODV routing protocol.

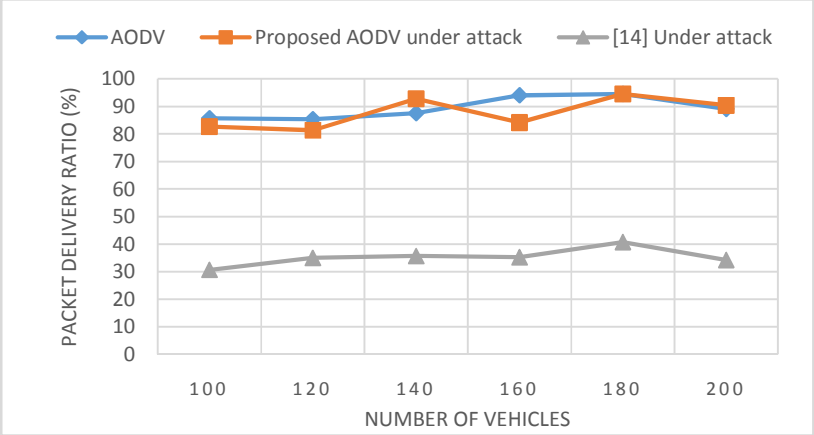

Figure6: PDR for varying number of vehicles under an intelligent black hole attack

As shown in figure 6, the packet delivery ratio of the proposed scheme is highly better then proposed solution in [14], moreover our proposed scheme has a PDR nearly equal to the fundamental AODV without attack.

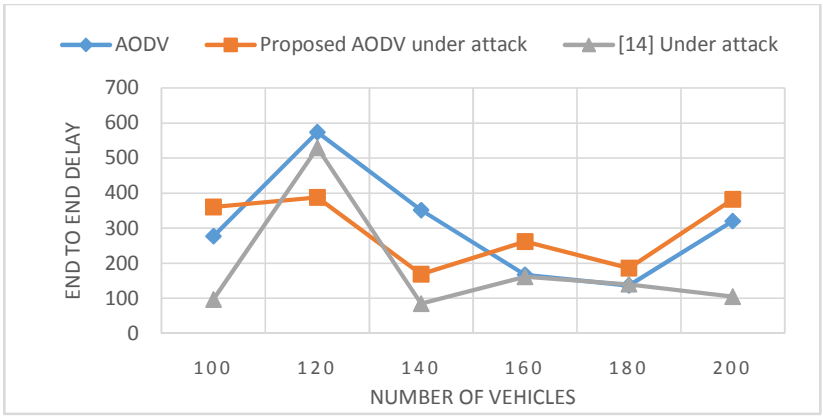

Figure 7: Average delay for varying vehicles density under an intelligent black hole attack

The figure 7 shows that based on our scheme, the end to end delay is comparable to AODV when there is no attack. The proposed solution in [14] shows the lowest end to end delay since the end to end delay is computed only for the received data packets, while the only received data packed in [14] underan intelligent adaptive black hole attack are those when the source node and the destination are too close or neighbors otherwise these packet will be deleted by the black hole node.

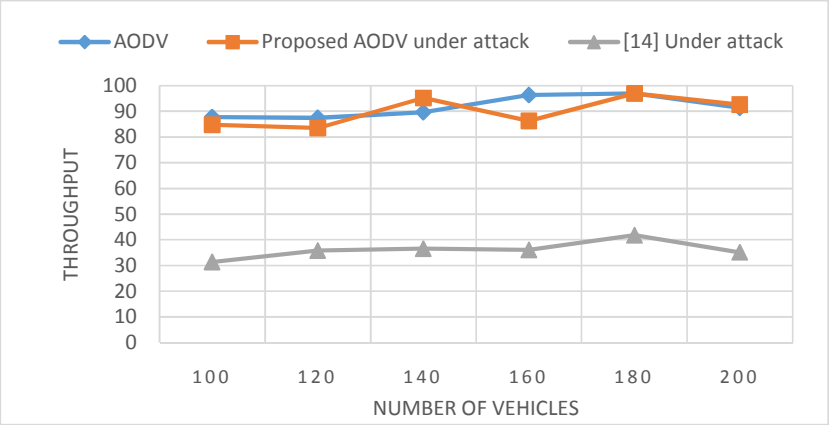

Figure 8: Throughput for varying number of vehicles under an intelligent black hole attack

The throughput of our scheme is nearly equal to the AODV and better then [14] as shown in figure 8.

The figure9 shows that the routing overhead of our proposed scheme is comparable to AODV under normal condition (without attack) which is not the case with [14] in the majority of node density.

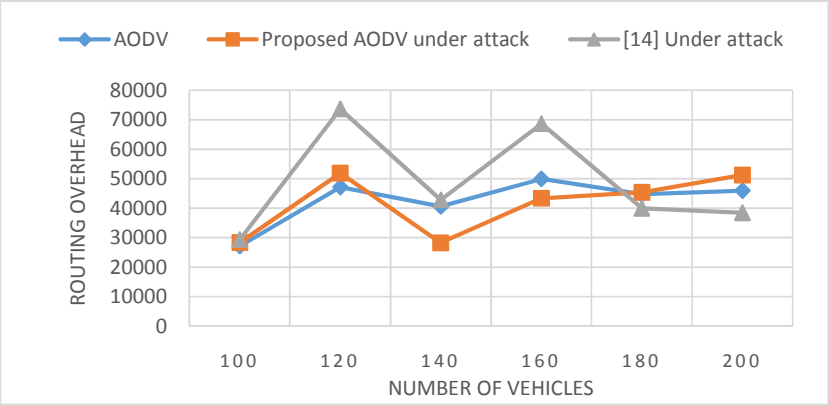

Figure 9: Routing overhead for varying number of vehicles under an intelligent black hole attack

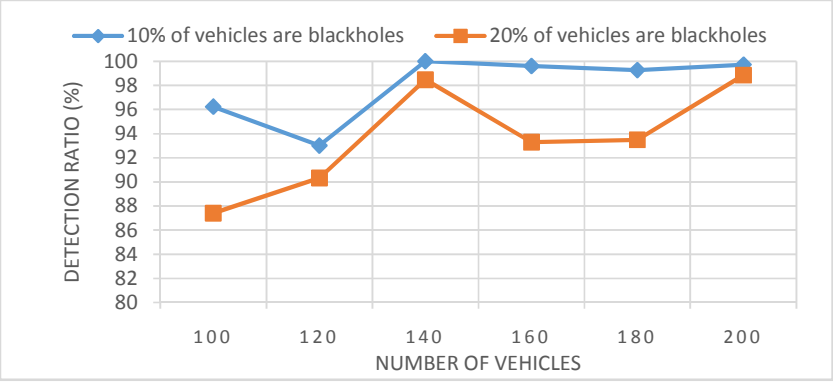

Figure 10: Proposed strategy detection ratio

The figure 10 represent intelligent black hole attacks detection abilities by our proposed scheme. Resulted curves shows that even in the presence of a high number of intelligent adaptive black hole attacks our proposal can ensure a high detection ratio exceeding the 85%.

So, from previous Figures and according to the positive simulation results it can be observed that, in the case of an intelligent adaptive black hole attack our scheme works well against the intelligent adaptive black hole attacks in vehicular networking.

3. CONCLUSIONS

With the emergence of newer security solutions, different kind of threats emerge as well. In this paper, Intelligent Black hole attack is discussed and prevented via our proposed strategy. The simulation results proved the efficacy of the proposed solution since it has the ability to ensure high packet delivery ration and throughput with nearly the same end to end delay and routing overhead compared to the fundamental AODV. Moreover, a high detection ratio is offered by the proposal in low and high vehicles density.

Furthermore, the proposed strategy is compatible with other reactive routing protocols, so, for future work we plan to implement and evaluate the performance of our scheme for other reactive protocols such as Dynamic MANET on demand (DYMO) routing Protocol and evaluate its performance under similar attacks such as 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] Cyclic Redundancy Check (CRC) RFC. Available online : https://tools.ietf.org/html/rfc3385 (accessed on Mars 2016).

[16] Network Simulator- NS-2. Available online: https://www.isi.edu/nsnam/ns/ (accessed on 5 May 2017).

[17] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo–simulation of urban mobility", in The Third InternationalConference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain, 2011.

[18] Open street map. Available online: https://www.openstreetmap.org/ (accessed on Mars 2017).

[19] Heithem Nacer and Mohamed Mazouzi, "A Scheduling Algorithm for Beacon Message in Vehicular Ad Hoc Networks",International Conference on Hybrid Intelligent Systems (HIS 2016),Marrakech, Morocco, pp. 489-497, 2016.

[20] Sirwan A.Mohammed and Sattar B.Sadkhan, "Design Of Wireless Network Based On Ns2", Journal of Global Research in Computer Science (jgrcs), Volume 3, No. 12, December 2012.