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

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 promising and popular technologies in the recent intelligent transportation world. They are used to provide an Intelligent Transportation System (ITS), efficient Traffic Information System (TIS), and Life Safety.

The mobility of the vehicles 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 vehicles that it has the freshest and the shortest path to the destination. Hence in this research paper an efficient approach for the detection and prevention of the Black hole attack in the Vehicular Ad Hoc Networks (VANET) is presented.

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 proposed strategy can detect both the single and the Cooperative Black hole attacks in the early phase of route discovery.

The simulation is carried on NS-2 and the results of the proposed scheme are compared to the fundamental DYMO 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 efficiency of the proposed method as the delivery ratio and end to end delay of the network does not deteriorate under a black hole attack.

KEYWORDS

VANET, Black hole attack, Security, AODV

1. INTRODUCTION

Recently, because the high number of road accidents and with the improvement in the wireless communication technologies and, 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].

VANET is a subclass of Mobile Ad-hoc Network (MANET) which consists of number of nodes (vehicles) communicating with each other without a fixed infrastructure [19]. However, compared to MANET, due to high mobility of vehicles, VANET has an extremely dynamic topology. The

DOI:10.5121/acij.2018.9101

nodes tend to move in an organized pattern [21]. Besides, VANETs have a potentially large scale which can comprise many participants and the capacity to extend over the entire road network [2]. Therefore, 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. The links between vehicles connect and disconnect very often which make routing process challenging due to the high mobility of nodes. Hence, many researchers have focused on routing in VANET. aiming to maximize Packet Delivery Ratio (PDR) and throughput while minimizing packet lose ratio and controlling overheads. 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 reactive, proactive and hybrid protocols [3], 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). Proactive protocols are typically table driven. Destination Sequence Distance Vector (DSDV), Global State Routing GCR are examples of this type. On the contrary. Hybrid protocols make use of both proactive and reactive 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 gray hole attack, black hole attack, Sybil attack, warm hole 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 is used by a malicious node that intelligently vary their behavior and adapts to avoid the detection and bypass security solutions. However, AODV is a reactive routing protocol as it is mentioned above; 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 to its neighbors. If malicious node (black hole node) is present in the network, the attacker node receives the RREQ packet and sends immediately a Route Reply (RREP) without even having an actual route to the destination, which will entice all other to route packets through it. The attack becomes more severe if more than one node colludes in the attack. Many research works focus on a single black hole attack but are less effective in collaborative and intelligent black hole attacks.

The remaining of this paper is organized as follows: In section II we introduced background of AODV routing protocol and black hole attack. In section III, relevant related work and their limitations are discussed. 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, so, a route is established only when it is needed by a source node to send data packets. In AODV, two mechanisms are used, 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, for a single RREQ, the source node may receive multiple routes to a destination. The destination sequence number is used to identify the freshest 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. The source node choses the route with the lowest hop count if two or more paths to the destination node have the same highest sequence number.

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 by 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 exploits the vulnerabilities of the route discovery process of the routing protocol to advertise itself as having the shortest and the freshest path to the destination even if no such route exists in its routing table since in AODV, any intermediate node that has a fresh route could respond to RREQ message.

Rerouting the network traffic through a specific node controlled by the attacker is the main goal of black hole attack. 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 back 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 data packets. The data packets will be dropped now by the malicious node instead of forwarding them to the destination as the protocol requires.

For example, in figure 1, the source node (S) needs to send 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 the intermediate node A has a fresh route to the destination node (D) and the node B is a black hole in that network. 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. As result, the route through the black hole node (node B) is accepted by the source node (S) as the freshet and the shortest route and sends data packets to the destination (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 will reach safely to the destination node but, in fact, the black hole node (B) drops all data packets instead of forwarding them to the destination (D).

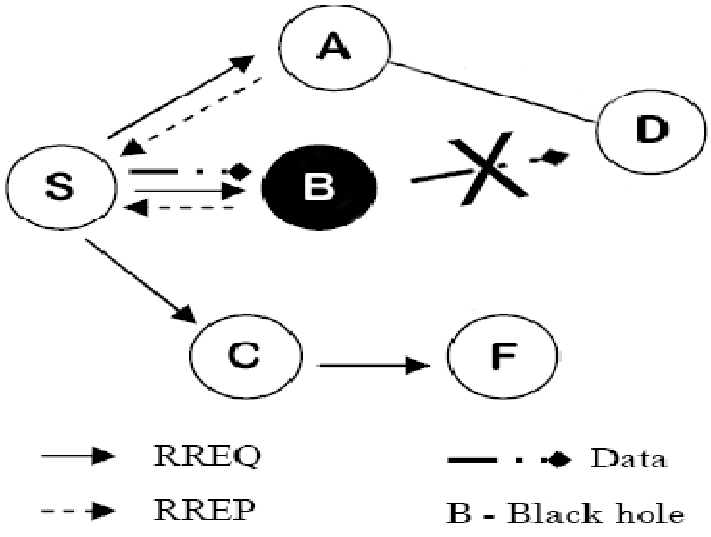

Figure 1. AODV Routing discovery under Black Hole attack

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, the most of solutions can detect and prevent only single Black Hole attacks and requires high overhead to detect cooperative 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], 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 [9], 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 [10], 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 [11], Chaker et al. proposed a mechanism for the detection of selfish and intelligent malicious nodes using threshold adaptive control. However, direct and indirect trust are computed based on the number of malicious and legal actions. Direct trust is calculated between a specific node and its neighbor. In the other hand, indirect trust is calculated based on the recommendation from one hop neighbors about other vehicles. But, in the presence of collaborative Black Hole attack this mechanism fails.

P.S. Hiremath et al. proposed an adaptive system of fuzzy interference to detect and prevent the Black Hole attack. In [12], four inputs used for the Fuzzy Interference System (FIS): data, trust, data rate, data loss, 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]. The new proposed strategy shows a better performance in the simulation results.

Sagar R Deshmukh et al. proposed an AODV-based secured routing to detect and prevent single and cooperative black hole attacks in [14], The idea of the authors is keeping the basic mechanism of AODV unchanged and just attach a validity value to the RREP. The simulation results show a good performance against the Black Hole attack with negligible overheads compared to the fundamental AODV. However, in the presence of an intelligent adaptive Black Hole in the network, this strategy falls flat, hence, an intelligent malicious node could easily set the validity value in the same way in which it claims that it has the freshest and the shortest 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 node starts route discovery process to find new route to the destination. The route discovery phase is initiated by broadcasting a route request packet (RREQ). A route reply (RREP) packet is sent back if an intermediate node has a valid route to the destination or the RREQ packet reached the destination node itself. The proposed solution in this paper makes minor changes in basic mechanism of AODV as shown in flow graph of figure 2.

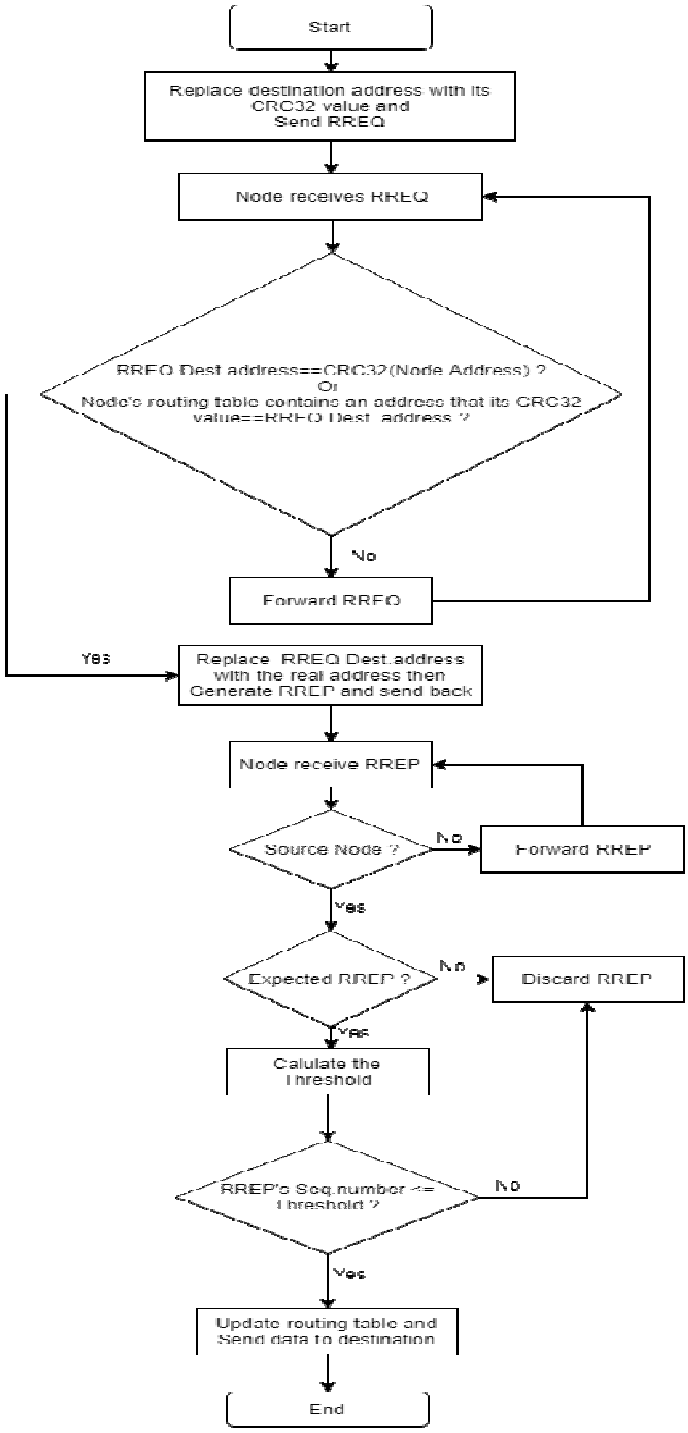

Figure 2. Flow graph of proposed method

In the 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 the same and it will not result any extra overhead.

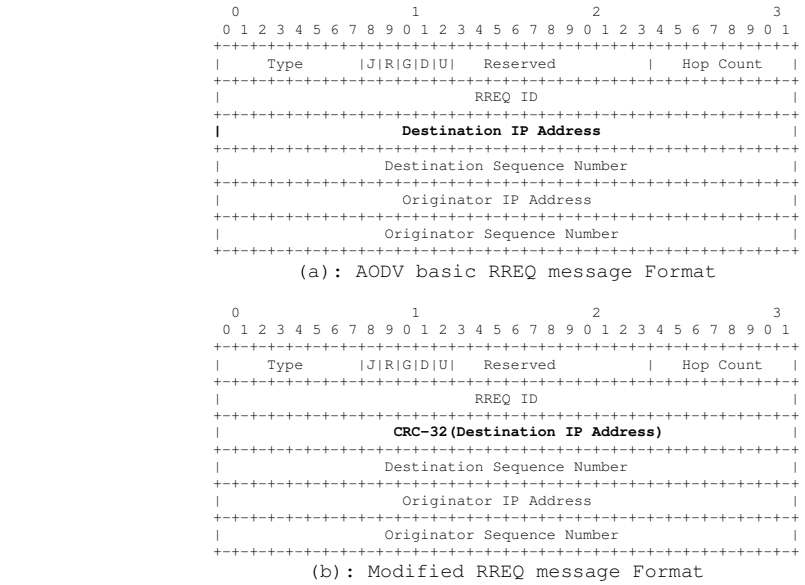

Figure 3. RREQ message format modification

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 packet and broadcast it. If an intermediate node receives the RREQ, it sends back a RREP after setting the real address (clear 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 packet 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 packet. Otherwise, the intermediate node forwards the RREQ packet.

However, for each RREP received by the source node, two phases of checking are applied:

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 non-existing target address.

2- If the RREP is valid 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 valid 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 the detection and prevention single and 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

In order to test and confirm the performance of proposed strategy, we have implemented the proposed solution in a simulation environment which generates the same behavior in the real vehicular ad-hoc networks.

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.

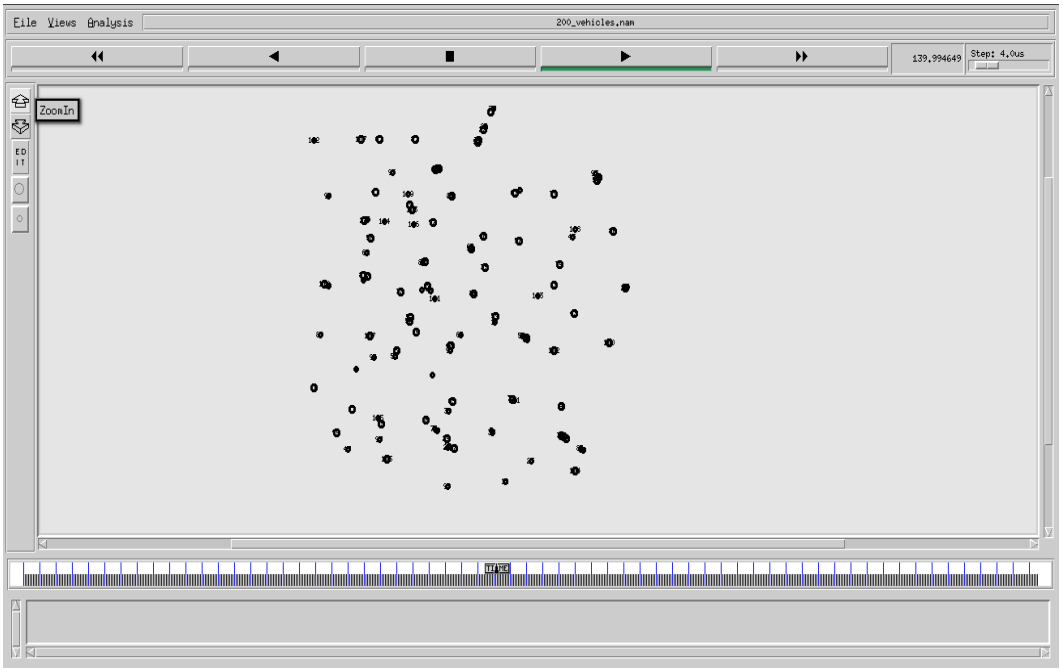

Figure 4: NAM output for the excerpt of the generated NS-2 trace

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.

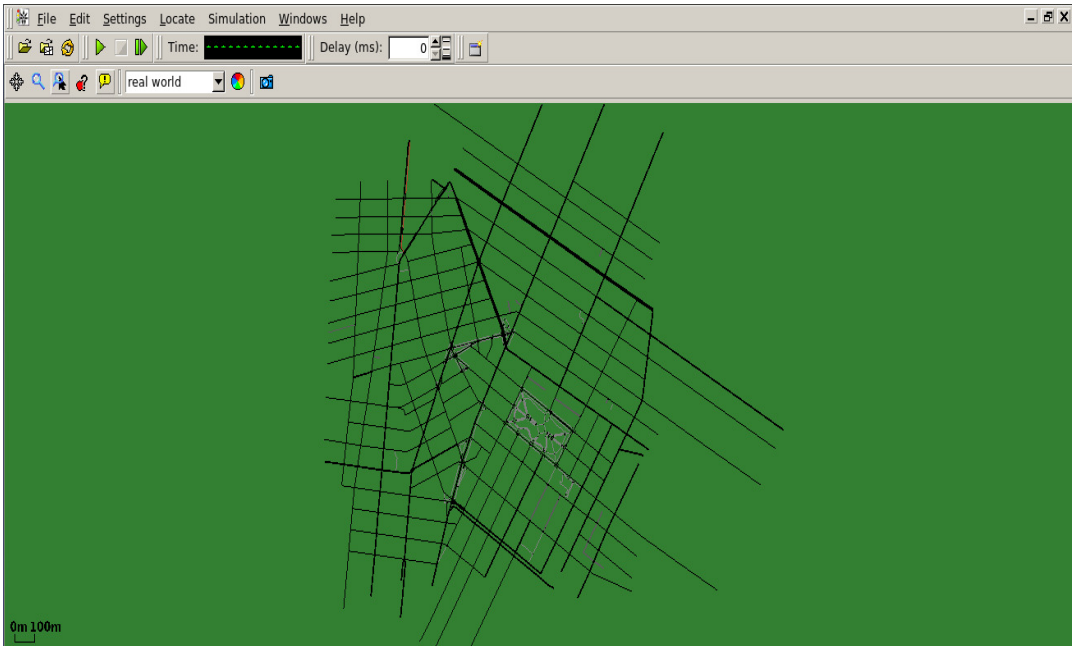

Figure 5: Extracted map from OpenStreetMap for the simulated scenario

In this scenario, a group of cars from 100 to 200 vehicles are moving randomly on the road of the extracted map (2.5km x 2.5km). the speed of vehicles depends on the used road and road lights (highway, urban, stopping lights, …) which is between 0 to 80 km/h. in addition, each vehicle has a maximal transmission range set to 250m and it is able to broadcast messages where the packet size is set to 512 bytes. The traffic generation rate is set to 5 packets per second.

Table 1: 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

However, an intelligent adaptive Black Hole attack was used in this scenario to prove the efficiency of the proposed scheme and to prove that [14] is vulnerable to a such attack. In this scenario the malicious node exploits both AODV routing protocol (which is vulnerable even against a well-known Black Hole attack) and [7]' secured AODV by setting the validity field in the same way as claiming that it has the shortest and freshest route to the destination.

In the other hand, trying to bypass the proposed scheme, the malicious node used to check its routing table before sending a RREP in the same way as a legitimate vehicle trying to find the real address. If the address is found it sets a high sequence number and sets the clear destination address and send back the RREP, otherwise, it behaves as a well-known black hole node.

To evaluate 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.
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.

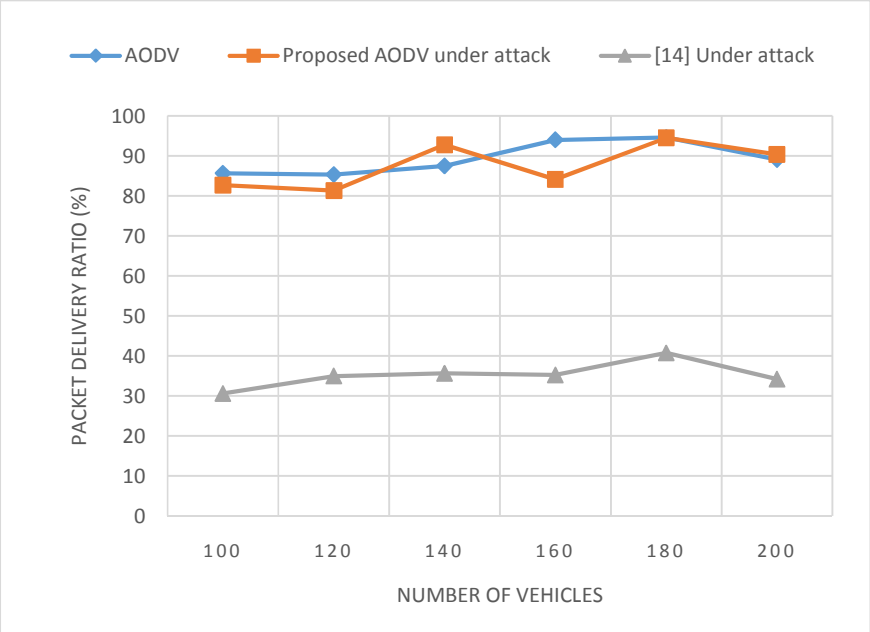

Figure 6: PDR for varying number of vehicles under an intelligent Black Hole attack

The figure 7 shows that based on our scheme, the end to end delay is comparable to AODV when there is no attack.

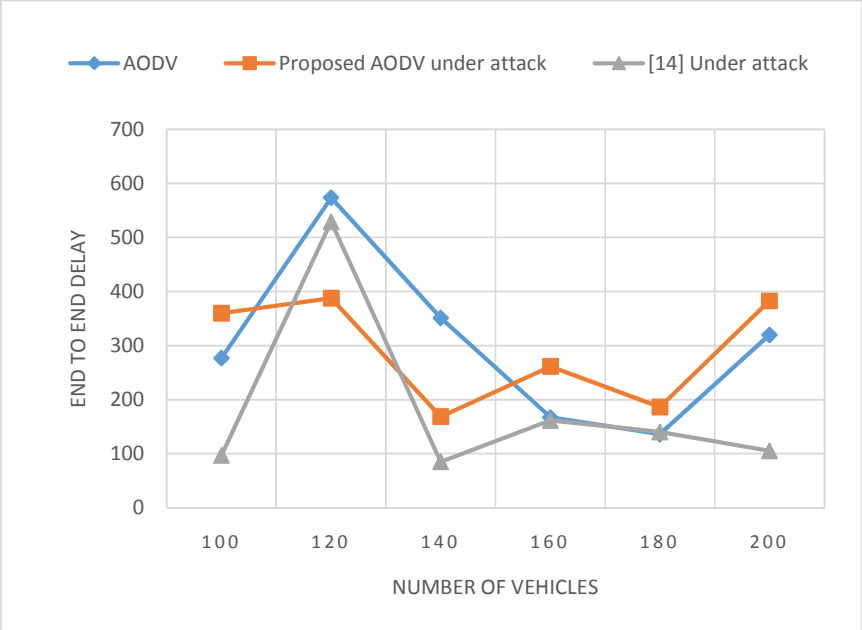

Figure 7: Average delay for varying vehicles density under an intelligent Black Hole attack

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] under an intelligent adaptive black hole attack are those when the source node and the destination are too close or neighbours otherwise these packet will be deleted by the black hole node.

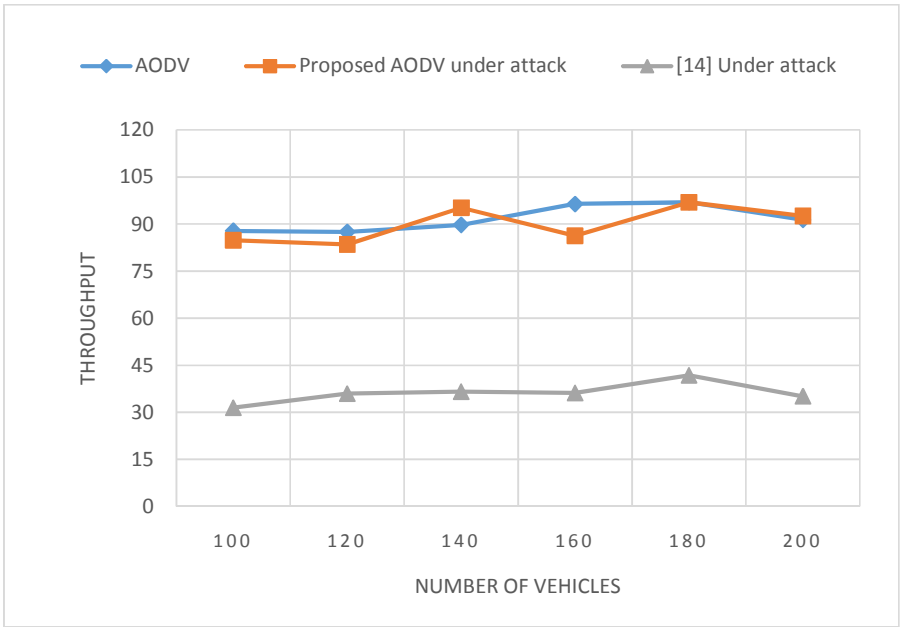

Figure 8: Throughput for varying number of vehicles under an intelligent Black Hole attack

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

The figure 9 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.

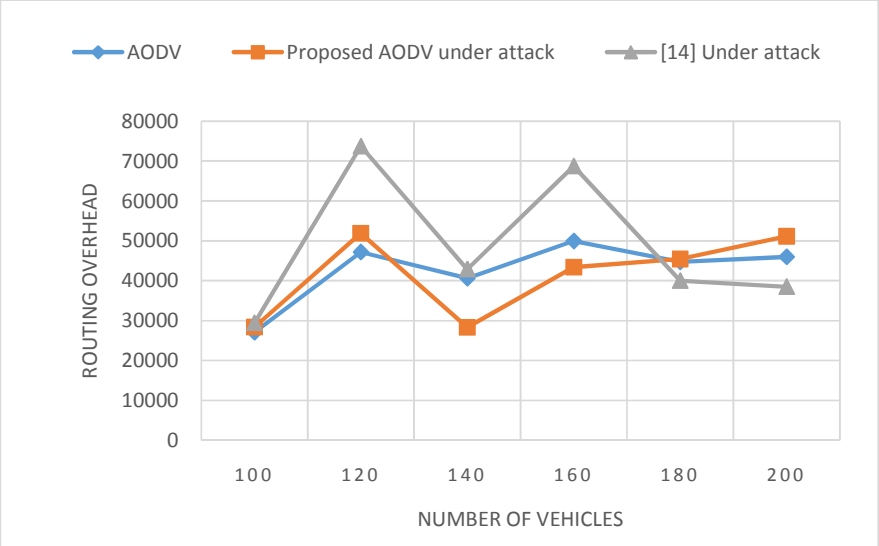

Figure 9: Routing overhead for varying number of vehicles under an intelligent Black Hole attack

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%.

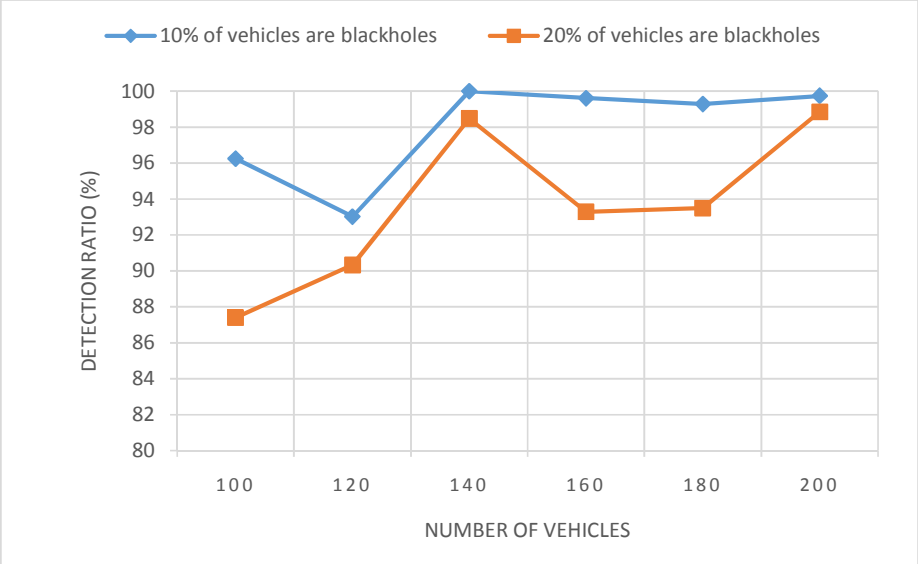

Figure 10: Proposed strategy detection ratio

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 efficiency of the proposed solution since it has the ability to ensure high packet delivery ratio and throughput with nearly the same routing overhead and end-to-end delay 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 the 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, 21–22 February 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] 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.

[9] 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.

[10] 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.

[11] Chaker Abdelaziz Kerrache, Abderrahmane Lakasy, and Nasreddine Lagraa. "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control". In: 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 in MANETs", 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 International Conference 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] Salim Lachdhaf, Mohamed Mazouzi, and Mohamed Abid, "Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol", International Conference on Networks & Communications (NetCom 2017), Dubai, pp. 25-36, November 2017.

[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.

[21] 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.