Scalability Impact on VANET Routing Protocols Performance

Zolidah Kasiran
Faculty of Computer & Mathematical Sciences
Universiti Teknologi MARA
Shah Alam, MALAYSIA
zolidah@tmsk.uitm.edu.my

Siti Noryazidah Hassan
Faculty of Computer & Mathematical Sciences
Universiti Teknologi MARA
Shah Alam, MALAYSIA
yazidah.hassn@gmail.com

***Abstract*— Vehicular Ad-hoc Networks (VANETs) represent a rapidly emerging, particularly challenging class of Mobile Ad Hoc Networks (MANETs). VANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. In this research, we investigated the impact of Black Hole attack on network performance towards VANET environment in terms of throughput, packet loss ratio, packet delivery ratio and normalized routing load. Besides that, we also analyzed which routing protocol is more vulnerable to the Black Hole attack in VANET. We simulated Black Hole. The results shows that Black Hole attack gave negative impact towards network performance in VANET. We also determined that AODV is the most vulnerable routing protocol to Black Hole attack in VANET compared to OLSR routing protocol.**

Keywords-VANET, Blackhole attack, Routing Protocols

I. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) represent a rapidly emerging, particularly challenging class of Mobile Ad Hoc Networks (MANETs).The main advantage of this is communicating with rest of the world while being mobile. The disadvantage is their limited bandwidth, memory, processing capabilities and open medium. VANET is a collection of vehicular nodes that do not rely on a predefined infrastructure to keep the network connected. Each vehicle equipped with communications devices will be a node in the VANETs and allow to receive and send other messages through wireless communication channels. So the functioning of VANET is dependent on the trust and co-operation between nodes [1]. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each vehicular node does the function of routing and relaying messages for other vehicular nodes [2]. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, VANET is vulnerable to various kinds of attacks.

.

II. RELATED WORK

A. VANETs Routing Protocol

Routing is a process of finding path from source to destination and as for the ad hoc routing protocols it has several ways to check the available path to send the packet. Ullah et al. [4] stated that routing protocols in VANETs can be classified into four different categories according to their functionality which are Reactive protocols, Proactive protocols, Hybrid protocols and Geographic routing protocol.

B. Reactive Protocol

Reactive protocols also known as on-demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded. When a node wants to communicate with another node in the network, and the source node don't have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. Normally reactive protocols don't find route until demanded. When it tries to find the destination "on demand", it uses flooding technique to propagate the query. Besides that, it does not consume bandwidth for sending information but it consumes bandwidth only, when the node start transmitting the data to the destination node.

C. Ad Hoc on -Demand Distance Vector (AODV)

Mobile nodes in the ad hoc network are dynamic and they use multi-hop routing by using Ad-Hoc On-Demand Distance Vector algorithm. AODV will not maintain the routes unless there is a request for route. Mobile nodes respond to the any change in network topology and link failures in necessary times. In case of the link failures the respective defective nodes are notified with the message, and then the affected nodes will revoke the routes using the lost link. This will help AODV to avoid the Bellman-Ford "counting to infinity" problem and then its operation is known as loop-free[5].

AODV uses Destination Sequence Numbers (DSN) for every route entry. DSN is created by the destination this DSN and the respective route information have to be included by the nodes while finding the routes to destination nodes[6]. Routes with the greatest DSN are preferred in selecting the route to destination.

AODV uses the message types Route Request (RREQ), Route Replies (RREP) and Route Error (RRER) in finding the route from source to destination by using UDP (user datagram protocol) packets. A typical AODV protocol follows the following procedure while routing:

i. A source node intending to communicate to a destination it generally uses the RREQ constituting the source address and the broadcast ID address to its neighboring nodes to find the route to destination,

ii. This broadcast ID is incremented for every new RREQ. Once a neighbor notice a destination route it will respond with RREP to the source 16, iii. If the destination route is not found then it will rebroadcast the RREQ to its corresponding neighboring nodes by incrementing hop count.

iv. In this process a node participating in communication may receive the numerous copies of the broadcast packets in the pool of transmissions from all the corresponding nodes

v. Then the node cross check the broadcast ID of the request if the broadcast ID is new and have not received so far by the particular node then it will process the request if not the node drops down the superfluous RREQ and avoids the rebroadcast.

D. Proactive Protocols

Proactive routing protocols works the other way around as compared to reactive routing protocols. Proactive routing protocol also known as table-driven routing protocol. These protocols maintain constantly updated topology of the network[7]. Every node in the network knows about the other node in advance keeping it simple, the whole network is known to all the nodes making that network. All the routing information is usually kept in number of different tables. Whenever there is a change in the network topology, these tables are update according to the changes. The nodes exchange topology information with each other; they can have route information any time when they needed.

E. Optimized Link State Routing (OLSR) protocol

OSLR protocol is a proactive protocol used in ad-hoc networks. It is often called table-driven protocol as it maintains and updates its routing table frequently. OLSR exchanges the topology information always with other nodes[8]. Few nodes are selected as MPRs (Multi point relays). MPRs are responsible for transmission of broadcast messages during flooding and generating link state information. MPRs technique used in OLSR protocol will reduce the message overhead and even minimize the number of control messages flooded in the network. Nodes maintain the information of neighbors and MPR's, by sending and receiving HELLO messages from its neighbors. Figure 1 shows OLSR symmetric link formation.

Node N1 transmits the HELLO message to node N2 and then the message received by node N2 from node N1 can be called asymmetric link. If this HELLO message is retransmitted by the node N2 to node N1 then the resulting link even called as asymmetric link. Finally the resulted bidirectional link is known as a symmetric link. Symmetric link formation will help the nodes to choose MPRs. MPRs will send the topology control (TC) messages containing the information about link status and MRP node information [8].

F. Black Hole Attack

Like any type of communication network, VANET is susceptible to attack. According to [9], in Black Hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. While in [10], they described in Black Hole attack, all network traffics are redirected to a specific node which does not exist at all.

III. METHODOLOGY

A. Research Design

This research focuses on measuring the performance of Ad hoc On-Demand Distance Vector (AODV) and Optimized Link State Routing Protocol (OLSR) for the identified scenario in the VANETs with varying network nodes based on the simulation implemented.

All scenarios are simulated involving 20, 40 and 80 vehicular nodes to measure the scalability impact.

Total of 18 scenarios had been developed, all of them with mobility of 10 m/s. Number of nodes were varied and simulation time was taken 100 seconds. Simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential and packet size (bits) is exponential (1024).

The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.005 watts. The freeway mobility model is selected with constant speed of 10 meter/seconds and with no pause time. In this research, we only focused on one constant average mobility speed. 10 meter/seconds had been chosen by referring to [11] and [12]. This parameter was chosen based on the suitability of freeway mobility model which focused on slow lane. Average mobility speed is used since in a high mobility the data transmission energy may be negligible compared to the energy used for the mobility [12].

Freeway mobility model was chosen because of it is the most suitable mobility model to implement in VANET environment. According to [13], this model is a generated map based model, which it is a depiction of highway traffic between cities but is unrealistic due to its restriction on lane changing and overtaking. However, this model considers the car following model, which is an important characteristic to implement in VANET environment.

B. Scability on VANET Routing Protocols

In term of scalability impact, the performance of the protocols is measured in terms of throughput parameter. The total amount of the data received by the receiver from the sender until the end of last packet transmission is known as throughput.

To observe the effect of scalability over VANET routing protocols, thirty six simulation scenarios were developed. Each scenario has 20, 40, 60, 80, 100 and 120 nodes respectively using AODV and OLSR routing protocols in the campus area of 1000 meters x 1000 meters. These simulation scenarios were in normal and Black Hole

scenario. Figure 2 shows the throughput for AODV routing protocol with 20, 40, 60, 80, 100 and 120 nodes in normal scenario while Figure 4.2 shows the throughput of AODV routing protocol for 20, 40, 60, 80, 100 and 120 nodes in Black Hole scenario.

From Figure 2, in normal scenario, it shows that the throughput increase when the number of nodes increase. The maximum value of throughput it can reach is about 30 million bits per seconds when the scenario consists of 120 nodes. As for 100 nodes, the maximum value of

throughput is about 33 million bits per seconds. We can conclude that as the time increase, the value of throughput will also increase.

Figure.3 shows the value of throughput for different number of nodes by using AODV routing protocol in Black Hole scenario. When there is a Black Hole attack, it shows the value of throughput decrease. It can be proven by referring Figure . The maximum value of throughput that it can reach is about 25 million bits per seconds. We can see from the graph where for 80 nodes the value of throughput is higher compared to 100 and 120 nodes. It can be assumed that for 80 nodes scenario, the packets sent to the intended destination directly or with little error. As for 100 and 120 nodes, the packets passed through the Black Hole node where the malicious node directly discard all the packets sent to it or forward the packets to the nonexisting nodes.

Figure 4 shows the throughput for OLSR routing protocol with different number of nodes: 20, 40, 60, 80, 100 and 120 nodes in normal scenario. The throughput for OLSR routing protocol with varying numbers of node in Black Hole scenario is shown in Figure 5.

Based on Figure 4, it shows that the throughput for OLSR routing protocol increase when the number of nodes increases. The maximum value of throughput for 120 nodes is 30 million bits per second. From the graph, we can see that after 20 seconds of simulation time, the value of throughput for 120 nodes remain constant until the end of the simulation. It is same goes to all scenarios with different number of nodes.

Figure 5 shows the value of throughput for OLSR routing protocol in Black Hole scenario. We can see that the value of throughput decrease in Black Hole scenario. The maximum value of throughput for 120 nodes is about 26 million bits per second. The value of throughput decrease about 4 million bits per second when the Black Hole attack exist for 120 nodes. After 20 seconds of simulation time, the value of throughput remains constant for all varying number of nodes.

The comparison of throughput value for two different routing protocols in normal and Black Hole scenario for 120 nodes has been made. The pattern of the graph is almost the same for 20, 40, 60, 80 and 100 nodes. Overall, we can conclude that as the number of nodes increase, the value of throughput also increases. However, the value of throughput is different for all routing protocols. OLSR routing protocol has the highest value of throughput compared to AODV routing protocol. All routing protocol have different pattern for the value of throughput. The OLSR protocol had increase at the beginning but , after 20 seconds of simulation time, the value of throughput remains constant until the end of simulation. As for AODV protocol, the value of throughput increase as the simulation time increase.

The performance of the both protocols were effected in the black hole scenario and it can be concluded, the value of throughput decrease when there is a Black Hole attack. It is because Black Hole node will drop all the packets forward to it or forward it to the node that does not exist at all.

REFERENCES

[1] M.Y. Darus and K.A.Bakar, "A Review of Congestion Control Algorithm for Event-Driven Safety Messages in Vehicular Networks." In *International Journal of Computer Science Issues,* 2011.Vol.8, Issue 5, No 1.

[2] Sharma S, Gupta R, "Simulation study of blackhole attack in the mobile ad hoc networks," *Journal of Engineering Science and Technology*, vol. 4, no. 2, pp. 243–250, 2009.

[3] B. Sun, Y. Guan, J. Chen, and U. W. Pooch, "Detecting black-hole attack in mobile ad hoc networks," in *Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492)*, 2003, pp. 490–495.

[4] I. Ullah and S. U. Rehman, "Analysis of Black Hole attack on MANETs Using different MANET routing protocols," *Program Electrical Engineering with emphasis on Telecommunication, Type of thesis-Master Thesis, Electrical Engineering, Thesis no: MEE-2010-2698*, 2010.

[5] Pooja Rani, Sharma N, Pariniyojit K.S, "Performance Comparison of VANET Routing Protocols", *Proceedings of 7th International Conference on Wireless Communication, Networking and Mobile Computing, 2011*

[6] Laxmi Shrivastava, G.S Tomar, S.S. Bhadoria " Performance Evaluation of Reactive Routing in Mobile grid Environment", International Journal of Grid and high Performance Computing IJHPC, IGI Global, Vol 3 No 3, 2011

[7] Brijesh Kumar Chaurasia, Ranjeet S.T, "Scability of MANET Routing Protocols for Vehicular ad Hoc Network", *Proceedings of International Conference on Communication Systems and Network Technologies" 2012*

[8] Punnet K.B, Shipra S, Vandana D, " Comparative Analysis of Reactive and Proactive Protocol of Mobile ad Hoc Network", *International Journal on Computer Sciences and Engineering, Vol 4, No 7, 2012*

[9] Megha K.V, "Security Analysis in VANETs: A Survey", *International Journal of Engineering Research & Technology, vol 1, no 8,*

[10] Mohammed Saeed Al-khatani, "Survey on Security attacks in Vehicular Ad-hoc Networks", *Proceeding of 6th International Conference on Signal Processing and Communication Systems, 2012*

[11] Tamizhselvi, A., Wahidabanu, R.S.D, "Perfomance Evaluation of Geographical Routing Protocol under Different Traffic Scenario." *International Journal of Computer Science and Telecommunications*, Vol. 3, no 3, 2012.

[12] X. Zhao, "An adaptive approach for optimized opportunistic routing over Delay Tolerant Mobile Ad hoc Networks," Rhodes University, 2008.

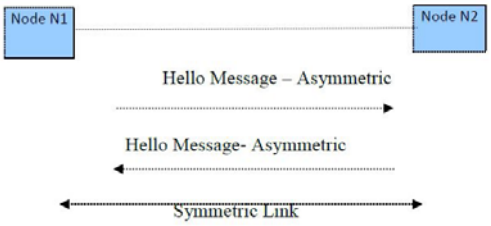

Figure 1: OLSR symmetric link formation

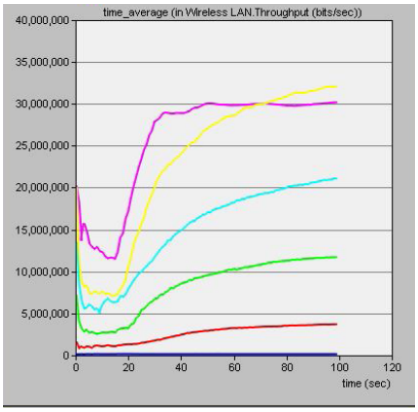

Figure 2: Throughput of AODV in Normal Scenario

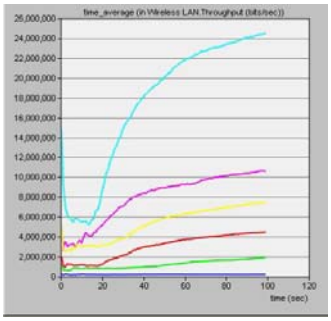

Figure 3: Throughput of AODV in Black Hole Scenario

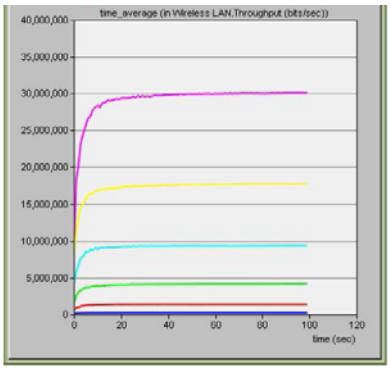

Figure 3: Throughput of OLSR in Normal Scenario

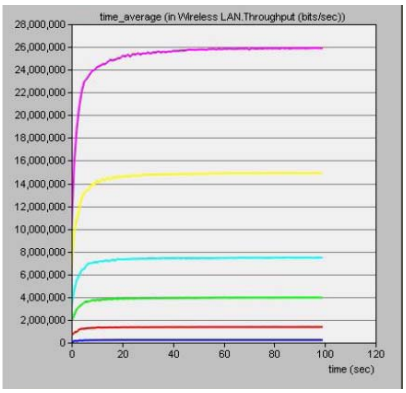

Figure 4: Throughput of OLSR in Black Hole Scenario