International Journal of Future Generation Communication and Networking
Vol. 8, No. 6 (2015), pp. 239-246
http://dx.doi.org/10.14257/ijfgcn.2015.8.6.23

Performance Evaluation of Routing Protocols in VANET

Ravneet Kaur[1] and Haramandar Kaur[2]

[1]Student at G.N.D.U
[2]Assistant Professor at G.N.D.U
[1]neetarora58@gmail.com, [2]harmandargndu@gmail.com

Abstract

Vehicular Ad-hoc Networks (VANETs) are rapidly emerging networks that are a particularly challenging subset of Mobile Ad Hoc Networks (MANETs). Open medium is one of the main features of VANET due to which it often suffers from security attacks and changing its topology dynamically, lack of management and central monitoring, and there is no clear defence mechanism. In this paper, we investigated the impact of Black Hole attack, Worm-Hole attack and Sybil attack on network performance towards VANET environment. We have also analysed which routing protocol is more vulnerable to the different attacks mentioned earlier in VANET. We have also determined that AODV is the most vulnerable routing protocol to attacks in VANET compared to OLSR routing protocol.

Keywords: *VANET, Black Hole attack, Wormhole attack, Sybil attack Routing Protocols*

1. Introduction

Vehicular Ad-hoc Networks (VANETs) is a rapidly emerging network, particularly challenging Mobile Ad Hoc Networks (MANETs). One of the main advantages of VANET is that being mobile it communicates with rest of the world. VANET is an open medium with limited bandwidth, memory and processing capabilities and these characteristics consider as major disadvantage. VANET do not rely on a predefined infrastructure, it is a collection of vehicular nodes to keep the network connected. In VANET each vehicle is a node equipped with communications devices which allow sending and receiving messages through wireless communication channels. Therefore trust and cooperation between nodes is the main function of VANET. Vehicles share the responsibility of managing the network and help each other in conveying information about the topology of the network. Each vehicular node acts as a host and does the function of routing and relaying messages for other nodes. VANET is vulnerable to various kinds of attacks due to lack of centralized management security.

2. Architecture of VANET

VANET architecture is designed for communications between Vehicle to infrastructure and Vehicle to vehicle. There are mainly two types of nodes in VANET, mobile nodes and static nodes named as OBUs (On Board Units) and RSUs (Road Side Units) respectively. In VANET's technology, mobile network is created by using moving cars as nodes. VANET turns every vehicle into a wireless router, allowing them approximately 50-250 meters of each other to connect and create a wide range network. As cars fall out of the signal range and not able to catch the network others cars can join in, connecting vehicles to another so that a mobile internet is created. It is estimated that the first systems to fully integrate this technology will be the police and fire vehicles to communicate with each other for safety purposes. VANET is used to alert the driver of other vehicles in case of emergency. These vehicles serving incidents then launch alert signals which are transmitted node (vehicle) to node (vehicle) along the road. In such case of an accident, we can prevent crashing of cars with an early collision warning system.

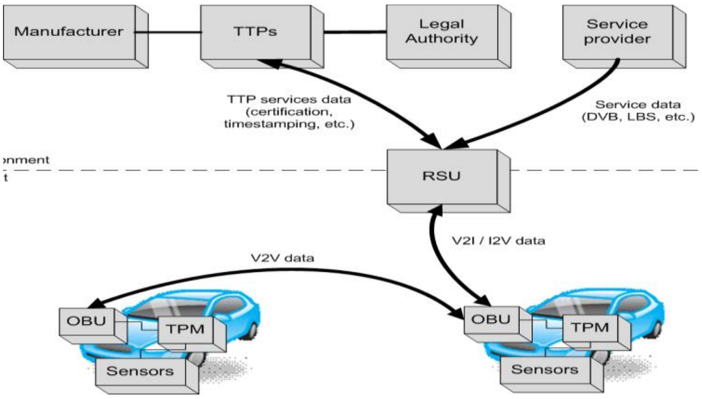

Figure 1. Architecture of Vanet

A. Barriers To Implementation

(i) **Technical barriers:** In VANET high mobility of vehicles introduces frequent topology changes that negatively affect existing solutions. To develop effective localization and data gathering mechanisms, several challenges have to be faced.

(ii) **Financial issues:** The development costs for the system are very high, but their implementation costs will be very low. The intelligence needed in the cars for processing the information also not a major cost factor. However, the first tens of thousands of cars equipped with the system in the system until there is a sufficient number of cars in the network with which to exchange information, and car owners will therefore be reluctant to spend any additional money on extras which have no use for them for years to come.

A VANET requires fully decentralised network control since no central entity could or should organise the network. Also VANETs hold an complexity due to some conditions such as timing and reliability requirements. Because of the many vehicles that could be incorporated into networks, VANET may become the largest ad hoc network in history. Scalability, undoubtedly, will be a critical factor. Protocol designers should also consider the various consequences the protocol may have on the physical world. Protocols should be adaptable to real-time environmental changes, including traffic flow, vehicle density, vehicle movement, and road topology changes.

B. VANET Characteristic's

As it is cleared from above discussion VANETs possess such network characteristics that make it unique from other of ad hoc networks and influence research in this area. Few characteristics of VANETs are as following:

(i) Rapidly changing network topology
(ii) High Mobility
(iii) Wireless Communication
(iv) Unbounded network size
(v) Frequent exchange of information
(vi) Sufficient Energy
(vii) Time Critical
(viii) Better Physical Protection

3. Related Work

A. Vanets Routing Protocol

The routing protocols in VANET are classified into five categories:

(i) Topology based routing protocol
(ii) Position based routing protocol,
(iii) Cluster based routing protocol
(iv) Geo cast routing protocol
(v) Broadcast routing protocol.

Such protocols are characterized on the basis of area / application where they are most suitable. Figure shows the different routing protocols in VANET.

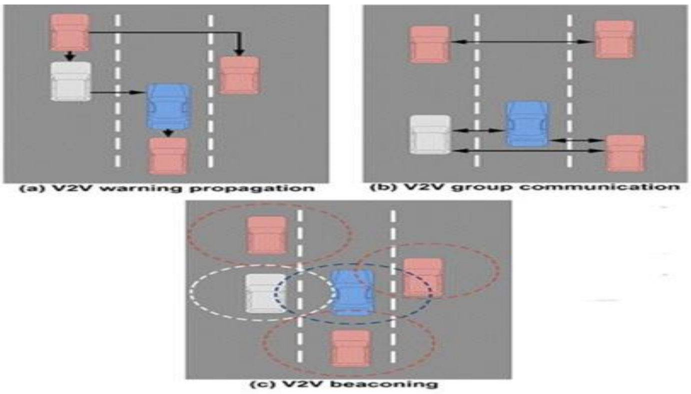

Figure 2. Wireless Communication Pattern

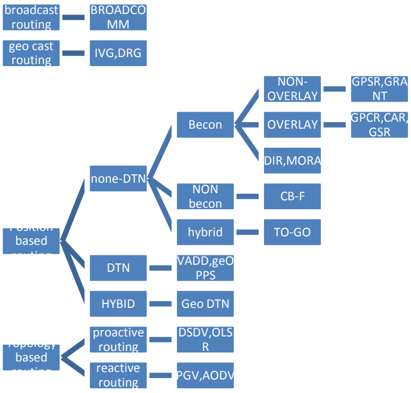

Figure 3. Routing Protocols

In this paper we are going to discuss those protocols which have been used in analysis. The discussion of these protocols is given below.

- **Reactive Protocol:** Reactive protocols can also be called as on-demand driven reactive protocols. These protocols initiate route discovery only when a source node request to find a route, which is why they are known as reactive protocols. Reactive routing protocols will establish a route for the source node to destination node only when it requests to communicate with another node, and the source node don’t have a route to the destination node. Normally reactive protocols find route only when demanded. When any node tries to find the destination “on demand”, flooding technique is used to propagate the query. Besides that, this technique does not consume bandwidth for sending information. It consumes bandwidth only, when the source node start transmitting the data to the destination node.

Ad Hoc on Demand Distance Vector (AODV)**:** Mobile nodes are dynamic in the ad hoc network and use multi-hop routing by using Ad-Hoc On-Demand Distance Vector algorithm. It will not maintain the routes until and unless there is a request for route. Mobile nodes only respond in necessary times whenever there is any change in network topology and link failures. Whenever there is link failures the respective defective nodes gets notification with the message, and then using the lost link the affected nodes will revoke the routes. This helps AODV to find loop free operation to avoid the Bellman-Ford counting to infinity problem. For every route entry AODV uses Destination Sequence Numbers (DSN). When the source nodes have to find the routes to destination nodes they have to include this DSN and the respective route information. Selection of the routes is done on the basis of greatest DSN. AODV uses UDP (user datagram protocol) packets such as Route Request (RREQ), Route Replies (RREP) and Route Error (RRER) in finding route. To find a typical route AODV protocol follows the following procedure:

i. A source node generally uses the RREQ constituting the source address and the broadcast ID address in order to communicate with destination node.

ii. For every new RREQ, broadcast ID is incremented. Once a neighbour node notices a destination route it will respond with RREP to the source.

iii. The hop count is incremented, when the destination route is not found and then it rebroadcast the RREQ to its corresponding neighbouring nodes.

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

v. Then each node cross check the broadcast ID and if the broadcast ID is latest then it will process the request otherwise it drops down the RREQ and avoids the rebroadcast.

❖ **Proactive Protocols:** Proactive routing protocols works in different way as compare to reactive routing protocols. Proactive routing protocol can also called as table-driven routing protocol. Such protocols maintain constantly updated topology of the network. In the whole network each node knows about every other node in advance. All the routing information is usually maintained in different tables. These tables are updated accordingly whenever there is a change in the network topology. Whenever the nodes need the routing information they exchange topology information with each other.

Optimized Link State Routing (OLSR) protocol: OLSR protocol is a proactive protocol used in ad-hoc networks. It is also called table-driven protocol as it maintains and updates its routing table time to time. OLSR always exchanges the topology information with other nodes. Some nodes are selected as MPRs (Multi point relays). During flooding MPRs are responsible for transmission of broadcast messages and generating link state information. This technique is used in OLSR protocol to reduce the message overhead and even to minimize the number of control messages flooded in the network. By sending and receiving HELLO messages from its neighbour's OLSR symmetric link formation, nodes maintain the information of neighbour's and MPR's. Node A transmits the HELLO message to node B and then the message received by node B from node A can be called asymmetric link. If this HELLO message is retransmitted by the node B to node A then the resulting link even called as asymmetric link. Therefore the resulted bidirectional link is known as a symmetric link. This symmetric link formation will help the nodes to choose MPRs. The topology control (TC) message which contains the information about MRP node information and link status are sent by MPR's.

Black Hole Attack: Like any type of communication network, VANET is also non-resistive to attacks. In Black Hole attack, a vicious node uses its routing protocol in order to advertise itself for having the shortest path calculated by the algorithm to the destination node or to the packet it wants to intercept. Irrespective of checking its routing table this hostile node advertises its availability of fresh routes. In this attack, all network traffics are redirected to such a node which does not exist at all.

Worm Hole Attack: This attack is one of the Denial-of-Service attacks. This is effective on the network layer, that can affect data aggregation, network routing and location based wireless security. The wormhole attack can be launched by a single or a pair of cooperating nodes. In this the attacker destroy the whole routing table, one send the packet to the neighbour node then authentication check that whether packet is send to the right node or not. Routing table followed this procedure. In routing table one node has all the information of its entire neighbouring nodes when there is Worm Hole attack then all the information is change. Wormhole attack tunnels the packets to other node in the network. Wormhole attack is immune to cryptographic techniques and does not require MAC protocol information. This makes it very difficult to detect. Various approaches have been proposed for handling this attack. Some approaches can only detect the presence of wormhole attack in the network but cannot solve it.

Sybil Attack: VANET is a real time which supports the services associated with drivers' safety such as the information transmission between vehicles, the warning about dangerous situations and the rear-end collision between vehicles. In Figure (2.3) & (2.4) the attacker sends wrong messages such as the information transmission between vehicles, the rear-end collision between vehicles, and the warning about dangerous situations. It throws other vehicles confusion. That is, as the objective of a Sybil attack is to make other vehicles change the route on the road or leave the road for the attacker, a Sybil attack can be a serious threat because it causes great damage to a VANET's function.

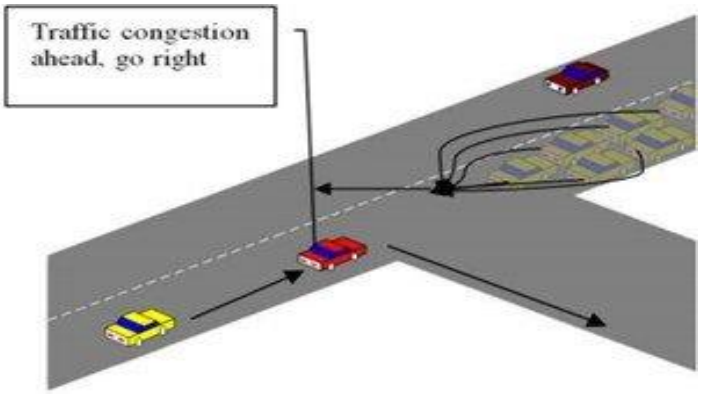

Figure 4. Sybil Attack

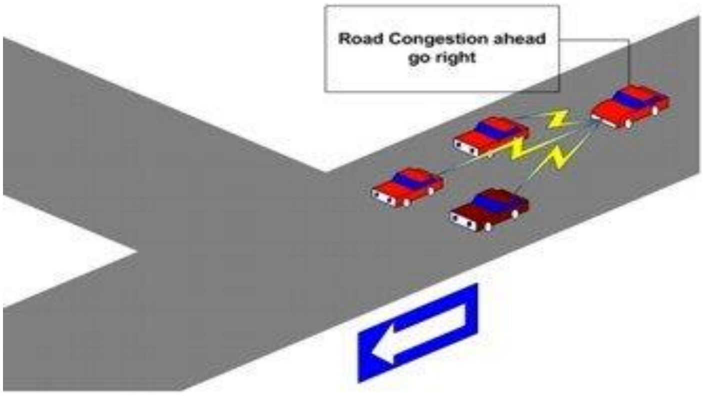

Figure 5: Selfish Driver

4. 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. Scenarios with different attacks involving 80 vehicular nodes to measure the scalability impact. Number of nodes remains same in different attacks.

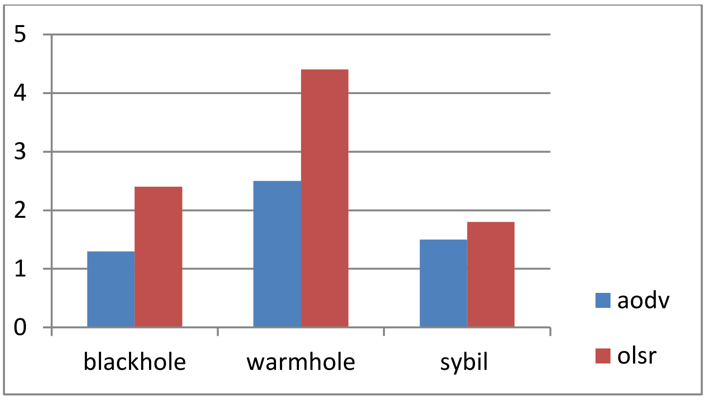

Figure 6. Analysis of Different Protocols during Attacks

5. Conclusion

In this paper we have analysed, that OLSR routing protocol is better as compare to AODV routing protocol in VANETs. OLSR routing protocol is proactive routing protocol i.e. its table driven routing protocol and AODV routing protocol is reactive protocol it work on Ad hoc basis criteria and that’s why is get affected with worm hole and black hole attacks more than OLSR routing protocol. AODV protocol is more vulnerable to attacks than OLSR protocol as shown in figure. In every attack OLSR protocol performs better.

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,.vol.8, Issue 5, no 1, **(2011)**.

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

[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] P. Rani, N. Sharma and K.S. Pariniyojit, “Performance Comparison of VANET Routing Protocols”, Proceedings of 7th International Conference on Wireless Communication, Networking and Mobile Computing, **(2011)**.

[6] L. Shrivastava, G.S Tomar and 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] B.K. Chaurasia, S.T. Ranjeet, “Scability of MANET Routing Protocols for Vehicular ad Hoc Network”, Proceedings of International Conference on Communication Systems and Network Technologies”, **(2012)**.

[8] K.B. Punnet, S. Shipra and D. Vandana, “ 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] K.V. Megha, "Security Analysis in VANETs: A Survey", International Journal of Engineering Research & Technology, vol. 1, no. 8.

[10] S.A.K. Mohammed, "Survey on Security attacks in Vehicular Ad-hoc Networks", Proceeding of 6th International Conference on Signal Processing and Communication Systems, **(2012)**.

[11] A. Tamizhselvi and R.S.D. Wahidabanu, "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)**.

Authors

Ravneet kaur, Student at Guru Nanak Dev University

Harmandar kaur, assistant professor at Guru Nanak Dev University.