ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Performance Evaluation of Routing Protocols in VANETs

Tejpreet Singh[1], Balpreet Kaur[2] , Sandeep Kaur Dhanda[3]

Student, CSE/IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (Punjab), India[1]

Asst. Prof., CSE/IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (Punjab), India [2,3]

Abstract: VANETs is a technology that provides communication between moving vehicles. VANETs are a type of Mobile Ad-Hoc networks in which moving vehicles will act as nodes. VANETs are highly dynamic in nature due to mobility of nodes and this dynamic nature causes topological change in the network, which may affect the communication and security of whole network. There are various attacks which may effect the network but wormhole attack is one the harmful attack which may affect the communication in VANET. This is so because wormhole may lead to attacks like Denial of service attack, data tampering, masquerading etc. In this paper performance of different routing protocols are analysed on the basis of metrics like throughput, end-to-end delay and jitter. Performance of routing protocols are analysed in two cases first is without wormhole attack and second is with wormhole attack and it has been checked how much performance of routing protocols AODV, OLSR and ZRP are degraded with wormhole attack.

Keywords: AODV, MANETs, OLSR, ZRP, RSU, V2I, V2V, VANETs.

I. INTRODUCTION TO VANETS

A Vehicular Ad-Hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network [31]. VANET turns every participating car into a wireless router or node, allowing cars create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created [24].

Vehicular Ad-Hoc Networks (VANET) is a subclass of Mobile Ad-Hoc Networks (MANETs) [31,35]. In VANETs there is two type of communication mechanism one is vehicle to vehicle (V2V) communication in which vehicle communicate with other vehicles in the network second is vehicle to infrastructure (V2I) communication in which vehicle will communicate with access points i.e. Road Side Units to get required information.

It provides safety and comfort to road users. VANET assists vehicle drivers to communicate and to coordinate among themselves in order to avoid any critical situation through vehicle to vehicle (V2V) communication. For example, road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc. Besides safety applications, VANET also provide comfort applications to road users through vehicle to infrastructure communication (V2I). For example, information of petrol pumps, information of nearby hospital, hotel, weather forecasting information, internet access and multimedia applications [23].

II. ROUTING PROTOCOLS

A. AODV (Adhoc on Demand Distance Vector): AODV [8] is a reactive protocol. The reactive routing protocols do not periodically update the routing table like table driven proactive protocols. In AODV, when there is some data to send, they initiate route discovery process through flooding which is their main routing overhead. Reactive routing protocols also suffer from the initial latency that occurs in the process of route discovery, which subsequently makes them unsuitable for safety applications in a network. AODV is a well known distance vector routing protocol [4] and it works as follows. Whenever a node wants to communicate with another node, it looks for an available path to the destination node, in its local routing table. If there is no path exists, then it broadcasts a route request (RREQ) message to its neighbourhood nodes. Any node that receives this message for route discovery looks for a path leading to the respective destination node. If there is no path exist then, it will re-broadcasts the RREQ message and sets up a path leading to RREQ originating node. This helps in establishing the end to end path when the same node receives route reply (RREP) message. Every node follows this mechanism until this RREQ message reaches to a node which has a valid path to the destination node or broadcasted RREQ message reaches to the destination node itself. Either way the RREQ receiving node will send a RREP to the sender of RREQ message. In this way, the RREP message reaches at the source node, which originally issued RREQ message. At the end of this request-reply mechanism a path between source and destination node is created and is available for further

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

communication. In situation where there is no route error (RERR) message is issued for nodes that potentially received its RREP message. This message helps to update the path when an intermediate node leaves a network or loses its next hop neighbour. Every node in AODV maintains a routing table, which contains the information: next hop node, sequence number and hop count. All packets destined to the destination node are sent to the next hop node. The sequence number is a measure of freshness of route and also acts as a form of time-stamping. This helps in using the latest available path for the communication process. The hop count represents the current distance between the source node and the destination node. AODV does not introduce routing overhead, until a RREQ is generated. This is useful as bandwidth is not wasted unnecessarily by the routing protocol. But on the other hand this introduces a latency factor, where a node has to wait for some time to find the path to the destination node to start communication. This can be for time critical and safety related emergency applications.

B. OLSR (Optimized Link State Routing): OLSR [10] is a proactive routing protocol or table driven protocol. Proactive routing protocols continuously update the routing table, thus generating sustained routing overhead. Basically OLSR is an optimization of the classical link state algorithm used in wireless ad hoc networks. In OLSR, three levels of optimization are achieved. First, some nodes are selected that will act as Multipoint Relays (MPRs) to broadcast the messages during the flooding process. This is in contrast to what is done in classical flooding process, where each and every node broadcasts the messages and generates too much overhead traffic. OLSR achieved RFC status in year 2003. Second level of optimization is achieved by using only MPRs to generate information regarding link state. This will results in minimizing the "number" of control messages flooded in the whole network and hence overheads are also reduced. In final level of optimization, an MPR can chose to report only that links that links between itself and those nodes which have selected it as their MPR. This results in the distribution of partial link state information in the network. OLSR also periodically exchanges topology information with other nodes at regular intervals. MPRs play a major role in the functionality of the protocol. Every node selects a subset of its one hop neighbour nodes as MPR. MPRs periodically announce in the network that it has reach ability to the nodes which have selected it as an MPR. Nodes which are not selected as MPR by any node, will not broadcast information received from it. The functionality of OLSR lies in the process of exchange of HELLO and TC messages. The periodic dissemination of HELLO packets in the process also enables a node to know whether a node or a set of nodes have selected it as MPR. This information is called as 'Multipoint Relay Selector Set', and is critical to determine whether to broadcast forward the information received from a node(s) or not. In a dynamic and rapidly changing environment, the set of nodes can change over the time. HELLO messages are also used for link sensing and neighbourhood detection. TC messages are used to provide every node enough information regarding link-state for the calculation of routes. Basically, a TC message is sent by a node to broadcast a set of links, which includes the links to all nodes of its MPR selector set. TC message is only broadcast forwarded by MRPs and offers controlled flooding of the topology information into the whole network. OLSR is designed to support large and dense wireless networks.

C. ZRP (Zone Routing Protocol): ZRP is combination of two protocol a proactive routing protocol that's also known as intra zone routing protocol (IARP) and its used inside routing zones and other protocol is reactive routing protocol that is known as Inter-zone Routing Protocol (IERP), is used between routing zones. When the route between different zones is to be required than IERP (Inter zone routing protocol) a reactive protocol is used for discovering the route between the source and the destination. This process eradicates the necessity for maintaining the entire picture of the network at every single node. BRP (Border cast resolution protocol) is a technique which controls the traffic between the zones and hence reducing the number furthering in route discovery of IERP. The change of the zone radius will further allow the protocol to acclimatize to different WSN environments. Larger radius of the zone will errand proactive routing protocol, which is optimal for slow-moving nodes or large amount of traffic whereas a smaller zone radius will errand the reactive routing protocol, which is best for fast-moving nodes or smaller amount of traffic. ZRP relies on Neighbor Discovery Protocol (NDP) in order to detect the new neighboring nodes and link failures.

III. WORMHOLE ATTACK

Wormhole attack is one of the Denial-of-Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. [12] The wormhole attack may be launched by a single or a pair of collaborating nodes. In this the attacker destroy the routing table like one send the packet to the neighbor node then authentication is check that packet is send to the right node or not . This procedure is done under routing table. In routing table one node has all the information of the neighbor node when there is attack then all the information is change. Wormhole attack tunnels the packet to the network to other node. Then Wormhole attack does not require MAC protocol information as well as it is immune to cryptographic techniques. [29] This makes it very difficult to detect. A number of approaches have been

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

proposed for handling wormhole attack. Some approaches only detect the presence of wormhole in the network.

IV. IMPLEMENTATION

Scenario of VANET is designed using QUALNET 4.5.1 simulation tool. Scenario is designed using terrain size of 1500*1500. 18 mobile nodes are placed on canvas which will act as vehicle. Clouds placed on canvas will act as RSU (road Side unit). Simulation is done for 150 sec with different routing protocols. Protocols are evaluated with and without wormhole on behalf of metrics throughput, delay and jitter.

A. Simulation Scenario

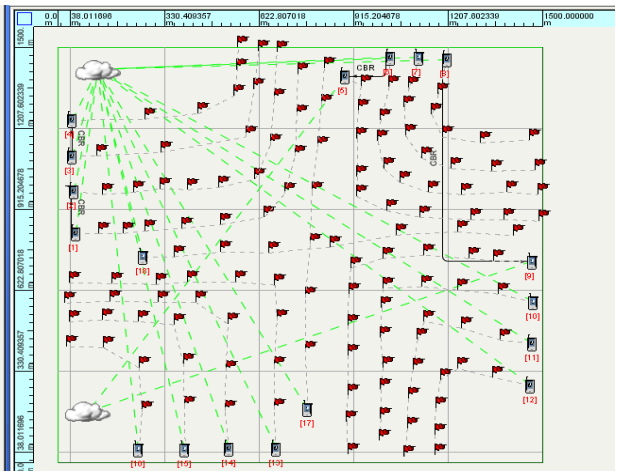

Figure 1. Scenario Design

B. Simulation parameters

Simulator	QUALNET
Terrain Size	1500*1500
Mobility Model	Random Way Point
Radio/Physical Layer	802.11b
Battery Model	Simple Linear
Antenna Model	Omni Directional
Routing Protocols	AODV, ZRP, OLSR
No. of Nodes	18
Simulation time	150 Sec

V. RESULT AND EVALUATION

We evaluate the performance of different routing protocols in VANETS under wormhole attack the effect of the wormhole attack on routing protocols is analysed on the basis of parameter like throughput, end-to-end delay and jitter.

A. Throughput:

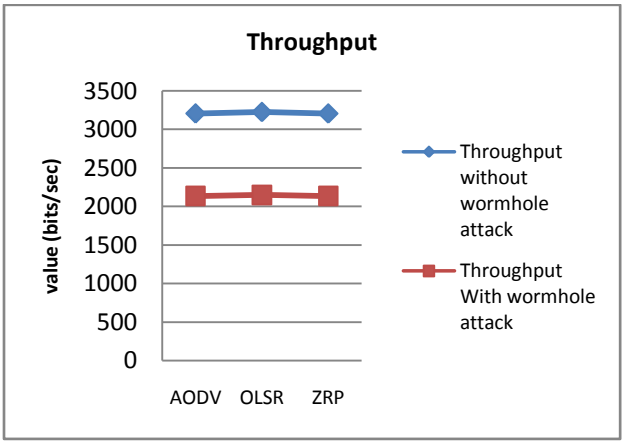

Figure 2. Throughput

The above graph shows the variation in the throughput of different routing protocols under wormhole attack. In this, the OLSR routing protocol performs well both with wormhole attack and without wormhole attack on VANETs. The throughput of OLSR is more than other routing protocols in both cases.

B. End-to-end Delay

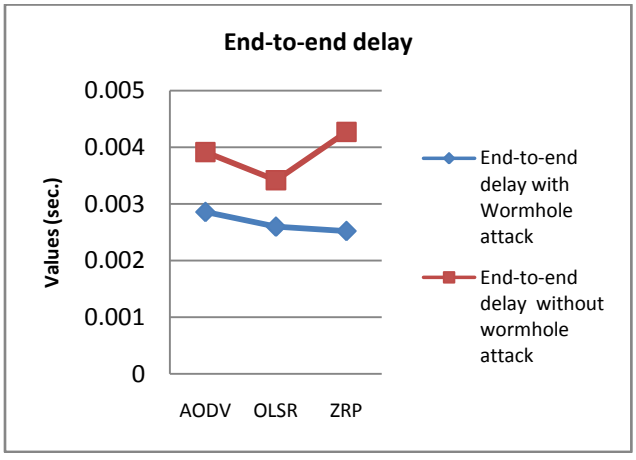

Figure3. End-to-end Delay

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

The above graph shows the variation in the end-to-end delay of different routing protocols under wormhole attack. In this, the end-to-end delay of OLSR routing protocol in case of no wormhole attack on network is less as compared to other routing protocols but in case of wormhole attack on network then the end-to-end delay of ZRP routing protocol is less than others. There is slight difference between the end-to-end delay of OLSR and ZRP routing protocol when attack is there on network

B. Jitter

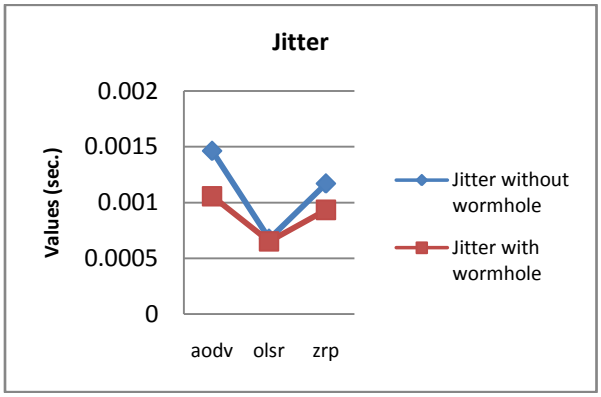

Figure4. Jitter

The above graph shows the variation in the jitter of different routing protocols. In this, the jitter of OLSR routing protocol is less as compared to other routing protocols.

VI. CONCLUSION

In this paper we have analysed, that OLSR routing protocol is better as compare to AODV and ZRP routing protocols 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 Adhoc basis criteria and that's why is get affected with wormhole more than OLSR routing protocol. ZRP routing protocol is hybrid protocol i.e. combination of proactive and reactive routing protocol. ZRP protocol works on inter zone and intra zone concept that increase the routing overhead and hence its performance get degraded with wormhole attack. Due to this reason throughput of OLSR routing protocol is more as compare to AODV and ZRP routing protocol in both the cases i.e. evaluation of routing protocol with or without wormhole attack.

REFERENCES

[1] Agrawal Ankita, Garg Aditi, Chaudhiri Niharika, Gupta Shivanshu, Pandey Devesh and Roy Tumpa , "Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper" in *International Journal of Emerging Technology and Advanced Engineering , January 2013.*

[2] Al-Rabayah Mohammad and Malaney Robert "A New Scalable Hybrid Routing Protocol for VANETs" in *IEEE transactions on vehicular technology, July 2012.*

[3] Bersen, Manivannam J., "Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service" In *The fourth international conference on Wireless and Mobile Communications, 2008.*

[4] Bharadwaj Saishree P., Rashmi S. and Shylaja B.S, "Performance Evaluation of MANET Based Routing Protocols for VANETs in Urban Scenarios", in *International Conference on Network and Electronics Engineering, 2011.*

[5] Gerla Mario and Klein rock Leonard, "Vehicular networks and the future of the mobile internet", in *Conference on Computer Network, Elsevier, 2011.*

[6] Goswami Akshay, Goel Roopali, "Security and Privacy in VANETs", in *International Journal of Engineering and Advanced Technology (IJEAT), August 2012.*

[7] Hafeez Khalid Abdel, Zhao Lian, Liao Zaiyi, Ma Bobby Ngok-Wah "Impact of Mobility on VANETs' Safety Applications" in *IEEE Globecom proceedings, 2010.*

[8] Ho Ivan Wang-Hei, Polak John W. "Stochastic Model and Connectivity Dynamics for VANETs in Signalized Road Systems" in *IEEE/ACM transactions on networking, February 2011.*

[9] Hubaux J.P., Capkun S., And Luo J., "The security and privacy of smart vehicles" in *IEEE Security & Privacy, 2004.*

[10] Kamat P., Baliga A., and Trappe W., "An identity based security framework for VANETs" in *Conference of Computer Communication in Barcelona, 2006.*

[11] Kamini, Kumar Rakesh "VANET Parameters and Applications: A Review" in *Global Journal of Computer Science and Technology, September 2010.*

[12] Kaur Harbir, Batish Sanjay & Kakaria Arvind "An Approach To Detect The Wormhole Attack in Vehicular Adhoc Networks" International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), 2012.

[13] Khairnar Vaishali D. and Pradhan Dr. S.N. , "Mobility Models for Vehicular Ad-hoc Network Simulation" , in *International Journal of Computer Applications, December 2010.*

[14] Lin Yun-wei, Chen Yuh-shyan and lee Sing-ling, "Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives", in *Journal of Information Science and engineering, 2010.*

[15] Manvi S.S. , Kakkasageri M.S. , Mahapurush C.V., "Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols in Vehicular Adhoc Network Environment" In *International conference on future Computer and Communication, April 2009.*

[16] Mateus Bruno G., De Oliveira Carina T., Callado Arthur , Fernandez Stenio and Andrade Rossana M. C., " Impact of Density, Load, and Mobility on the Performance of Routing Protocols in Vehicular Networks" *in IEEE 2012.*

[17] Molisch Andreas F., Tufvesson Fredrik, Karedal Johan and Mecklenbrauker Christoph, "Propagation aspects of vehicle-to-vehicle communications - an overview" *in IEEE, 2009.*

[18] Nagaraj Uma, Kharat Dr. M. U. and Dhamal Poonam, "Study of Various Routing Protocols in VANET" *in International Journal of Computer Science & Technology , December 2011.*

[19] Papadimitratos P., Buttyan L., Holczer T., Schoch E., Freudiger J., Raya M., Ma Z., Kargl F., Kung A., Hubaux J.P. "Secure vehicular communication system: design and architecture" *in IEEE Wireless Communication Magazine, Nov 2008.*

[20] Prof. Kumar Bhagat Sunil Madhusudan, Prof (Dr.) Wadhai V.M "Study of effect of velocity on end to end delay for V2V communication in ITS " in *IEEE/ACM transactions on networking, 2012.*

[21] Ramakrishnan B., Dr. R.S. Rajesh and Shaji R.S., "Analysis of Routing Protocols for Highway Model without Using Roadside Unit and Cluster" in *International Journal of Scientific & Engineering Research January-2011.*

[22] Rasheed Asim, Dr. Qayyum Amir in "Security Architecture Parameter in VANET" in *IEEE Transactions on Vehicular Technology, 2010.*

[23] Raya M. and Hubax J.P., "Security aspect of inter-vehicle communications" in *Swiss Transport Research Conference, 2005.*

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

[24] Raya Maxima, Hubax Jean-Pierre, "The security of vehicular ad hoc networks" in *Proc. of the ACM Workshop on Security of Ad hoc and Sensor Networks (SASN), 2005.*
[25] Sharma Manish and Singh Gurpadam, "Evaluation of Proactive, Reactive and Hybrid Ad hoc Routing Protocol for various Battery models in VANET using Qualnet" in *International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), 2011.*
[26] Sharma Manish and Singh Gurpadam, "Performance evaluation of AODV, DYMO, OLSR and ZRP Adhoc routing protocol for IEEE802.11 MAC and 802.11 DCF in VANET Using Qualnet" in *International Journal on Adhoc Networking Systems, January 2012.*
[27] Shrivastava Priyanka, Ashai Sayir, Jarol Aditya and Gohil Sagar " Improving Connectivity Between Vehicle and Road-Side-Unit" in *International Journal of Scientific & Engineering Research, August-2012.*
[28] Shrivastava Priyanka, Ashai Sayir, Jaroli Aditya and Gohil Sagar, " Vehicle-to-Road-Side-Unit Communication Using Wimax technology ", in *International Journal of Engineering Research and Applications (IJERA), July-August 2012.*
[29] Singh Jagjit, Sharma Neha Sharma "An Advanced IDS Approach to Detect Wormhole Attack in VANET" International Refereed Journal of Engineering and Science (IRJES), 2012.
[30] Sumra Irshad Ahmed, Ahmad Iftikhar, Hasbullah Halabi "Classes of Attacks in VANET" in *IEEE Electronics, Communication and Photonics Conference, 2011.*
[31] Taleb T., Sakhaee E., Jamalipour A., Hashimoto K., Kato N., and Nemato Y., "A stable routing protocol to support its services in vanet networks" in *IEEE Transactions on Vehicular Technology, November 2007.*
[32] Waleed Alasmary, Weihua Zhuang, "Mobility impact in IEEE 802.11p infrastructure less vehicular networks" in *Conference on Adhoc Networks, Elsevier, 2010.*
[33] Wex Philipp, Breuer Jochen, Held Albert, Leinmuller Tim and Delgrossi Luca, "Trust Issues for Vehicular Ad Hoc Networks" , in *Conference on Network Security IEEE , 2008.*
[34] Zakri M.E. , Mehrotra S., Tsudik G., and Venkatasubramanian N., "Security issues in a future vehicular network," In *European Wireless Conference, 2002.*
[35] Zhu Kun, Niyato Dusit, Wang Ping, Hossain Ekram, and Kim Dong Ln, "Mobility and Handoff Management in Vehicular Networks: A Survey" in *Wireless Communication and Mobile Computing, 2009*

BIOGRAPHIES

Tejpreet Singh is presently pursuing M.TECH in CSE(ESecurity) from BBSBEC,Fatehgarh Sahib, Punjab, India. His research includes VANETs.

Er. Balpreet Kaur is currently serving as Assistant Professor in Computer Science and Engineering. Her research includes digital image processing.

Er. Sandeep Kaur Dhanda is currently serving as Assistant Professor in Computer Science and Engineering. Her research includes parallel computing.