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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

Analysing the effect of Speed on Security Protocol in VANETS

Ramanpreet Kaur[1], Er. Khyati Marwaha[2]

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]

Abstract: VANET (Vehicular Ad-Hoc Network) is a sub class of MANETs (Mobile Ad-Hoc Networks) in these moving vehicles will act as node. VANETs are a technology that provide secure driving environment by wireless communication between vehicles. Due to Ad-Hoc nature of VANETs it's vulnerable to various attacks that breach the security . In this paper, I am going to analyse the effect of varying speed of vehicles on security protocol with on behalf of different routing protocols. Speed of vehicle goes on changing that may affect the performance of network. Speed is the major factor that is to be handled for secure and efficiently implementation of VANETs. Varying speed of vehicle makes the environment more dynamic which may lead to topology change and this topological change affect the routing criteria of routing protocols. In this paper performance of VANETs will be analysed on behalf of metrics like Throughput and End-to-End Delay.

Keywords: VANETs, MANETs, RSU, V2V, V2I

I. Introduction

A Vehicular Ad-Hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network [11]. 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 [18].

Vehicular Ad-Hoc Networks (VANET) is a subclass of Mobile Ad-Hoc Networks (MANETs) [10, 11]. 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 [8].

II. Routing Protocols

A routing protocol specifies how router communicates with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. A routing protocol shares this information first among immediate neighbours, and then throughout the network. This way, routers gain knowledge of the topology of the network. There are two types of routing protocols which are reactive and proactive. In reactive routing protocols the routes are created only when source wants to send data to destination whereas proactive routing protocols are table driven.

A. AODV (Ad-hoc On Demand Distance Vector) protocol:

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 [13] 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 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 [2]. This is useful as bandwidth is not wasted unnecessarily by the routing protocol. But on the other hand this introduces an 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) protocol:
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 [3]. 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 Neighbour Discovery Protocol (NDP) in order to detect the new neighbouring nodes and link failures.

III. IPSEC SECURITY PROTOCOL

IPSEC (Internet Protocol Security) is a protocol suite that secures internet protocol communication by authenticating and encrypting each IP packet of communication session [15]. It provides end-to end security. It operates at internet layer of the internet protocol suite. IPSec works in two modes tunnel mode and transport mode. Transport Mode protects packets coming from transport layer to network layer by encapsulating the payload only but doesn't encapsulate the header. The IPSec header and trailer are added to message coming from transport layer. Transport mode is used when Host-to-Host protection of data is required. In tunnel mode whole packet is protected along with the header. The IP header is added in this mode. Tunnel mode is used when communication occurs between two routers, between a host and a router, or a router and host. There are two protocols in IPSec suite: Authentication header (AH) protocol and Encapsulating Security Payload (ESP) that provide authentication and encryption for packet security. Authentication header protocol authenticates the source host and ensures the payload integrity carried in IP packet. This protocol uses hash function and symmetric key to create the message digest; digest is inserted into authentication header and then AH is placed in appropriate place according to the mode. Authentication Header provides authentication and integrity, but doesn't provide privacy. Then alternative protocol for privacy is designed that is known as Encapsulating Security Payload (ESP). The ESP's authentication header and trailer added at the end which makes the calculation easy [16].

IV. SIMULATION SETUP

Simulation is done using QUALNET 4.5.1 tool with terrain size 1500x1500 for 150 sec. Varying number of nodes (16,24) are placed randomly on canvas that act as vehicles. Two subnets are placed these subnets will act as Road Side Units and moving nodes will act as vehicles. Different routing protocols (AODV, OLSR, ZRP) are used in this simulation. Speed of nodes is varied with IPSec security protocol and their performance is measured on the basis of metrics like throughput, end-to-end delay and jitter.

A. SIMULATION PARAMETER:

Simulator	QUALNET
Terrain Size	1500x1500
No. of nodes	16, 24
Speed of Vehicles	30, 60, 90 mps
Routing Protocol	AODV, OLSR, ZRP
Radio/Physical layer	802.11b
Mobility Model	Random way point
Security Protocol	IPSec
Battery Model	Simple Linear
Antenna Model	Omni Directional
Simulation time	150 sec
Data Size	512 bytes

B. Scenario Design

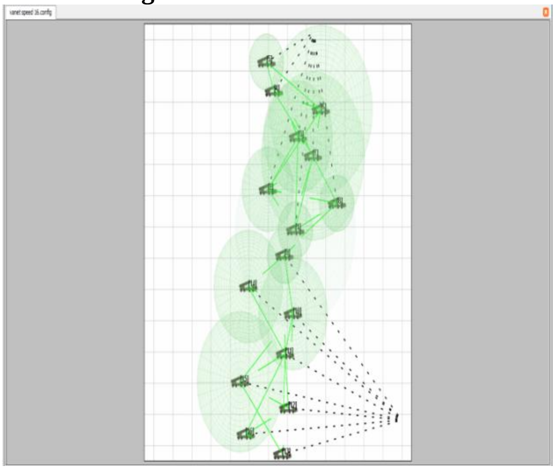

Figure1. 3D Analyser Scenario

V. RESULT AND EVALUATION

We evaluate the performance of security protocol on behalf of routing protocols with varying speed of nodes i.e. vehicles in VANETS on the basis of different parameters like throughput and end-to-end delay.

1. Throughput (bps) at speed 30 mps

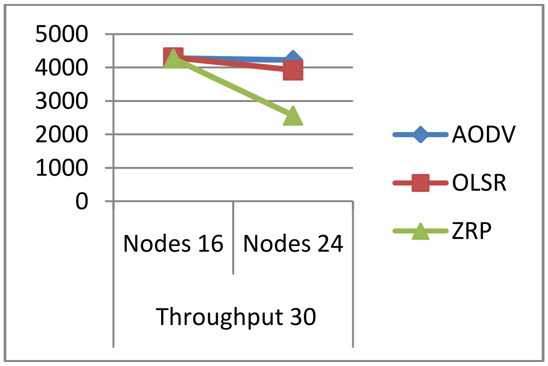

Figure.2 Throughput

The above graph shows the variation in the throughput of different routing protocols with density of nodes at speed 30mps. In this the AODV routing protocol performs well as compared to others. Its throughput decreases with density of nodes. The throughput of AODV is 827bps more than ZRP routing protocol.

2. End-to-end Delay (sec.) at speed 30 mps

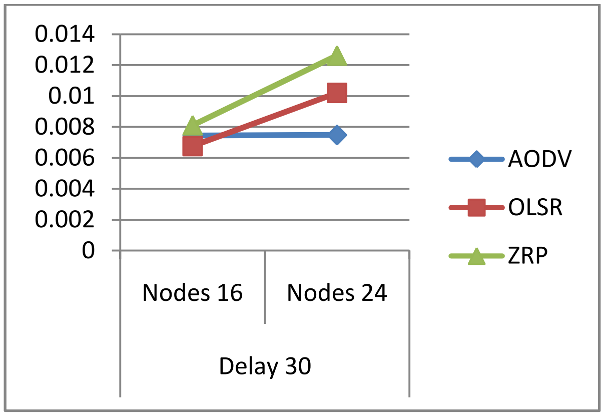

Figure.3 End-to-end delay

In this above graph the end-to-end delay of AODV routing protocol is less as compared to other routing protocols and it increases with increase in number of nodes. The differnce between AODV and ZRP routing protocol is 0.0029085 sec.

3. Throughput (bps) at speed 60 mps

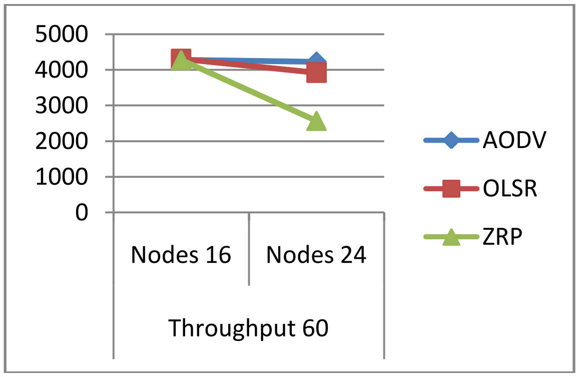

Figure.4 Throughput

In this with increase the in speed the throughput of AODV routing protocol remains same and it is heigher than other routing protocols. Here, the diffrence between AODV and ZRP routing protocol is 827.03 bps which is more than the value at speed 30 mps.

4. End-to-end Delay (sec.) at speed 60 mps

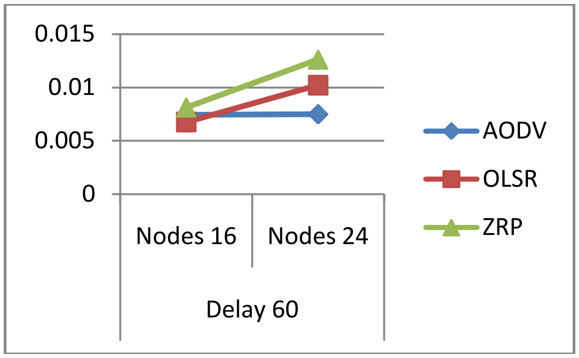

Figure.5 end-to-end delay

In this the delay of AODV is less and remain stable with increase in speed. Here, the difference between the end-to-end delay of AODV and ZRP routing protocol is 0.0029087sec. which is more than value of end-to-end delay at speed 30 mps.

5. Throughput (bps) at speed 90 mps

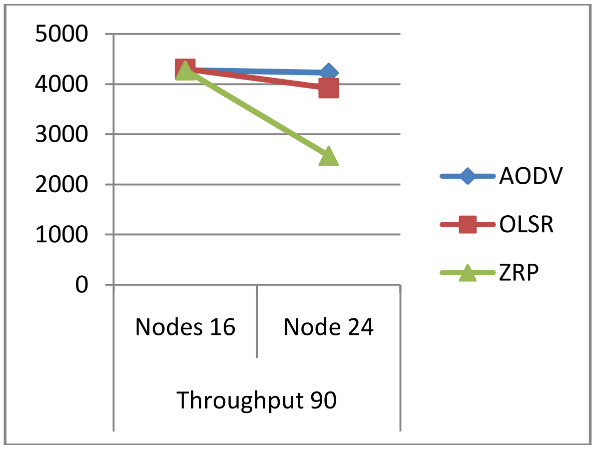

Figure.6 Throughput

In this, the variation in throughput of different routing protocol with speed 90 mps is shown. Here, the diffrence between AODV and ZRP routing protocol is 826.992 bps. The AODV routing protocol performs well at high speed.

6. End-to-end Delay (sec.) at speed 90 mps

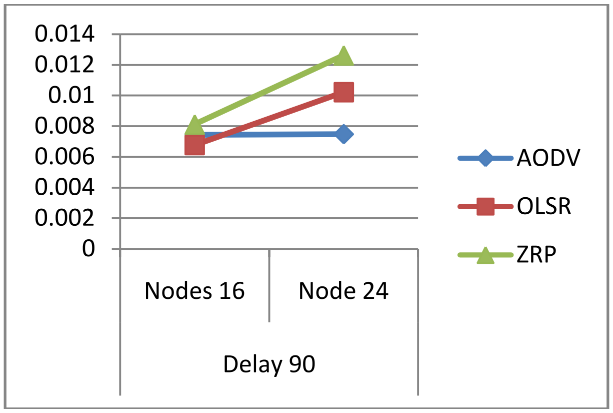

Figure.7 End-to-end delay

In this above graph, with increase in speed the delay of ZRP routing protocol increases rapidly but of AODV there is little variation. The difference between AODV and ZRP routing protocol is 0.0029089 sec. Which is more than the value of end-to-end delay at previous speed.

VI. Conclusion

In this paper, we analysed different routing protocols with varying speed of nodes on behalf of security protocol. The performance of routing protocol with IPSec security protocol is analyses on the basis of metric like throughput and end to end delay. The routing protocol used is of different type. AODV is reactive routing protocol which works on ad-hoc mode basis, OLSR is proactive routing protocol which is table driven and ZRP is hybrid routing protocol which is combination of both reactive and proactive routing protocol. Experimental results shown that on increasing speed the performance of protocol get effected in such way that there throughput decreases and delay increases. If density is increased then also throughput decreases and delay increased. The reason behind this change is the ad-hoc nature of routing protocols. These are the topological routing protocols as speed varies the topology get changed very rapidly and hence which may affect the routing schedule of the routing protocols. From all of three protocols the performance of AODV proactive protocol with IPSec security protocol is best as compare to other two protocols i.e. OLSR and ZRP. The degradation in throughput is quite less as compare OLSR and ZRP.

References

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

[2] Prof. Bhagat Sunilkumar 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.

[3] B. Ramakrishnan, Dr. R. S. Rajesh, R. S. Shaji in “ Analysis of Routing Protocols for Highway Model without Using Roadside Unit and Cluster” ,2012.

[4] Kun Zhu, Dusit Niyato, Ping Wang, Ekram Hossain*;* and Dong Kim“Mobility and Handoff Management in Vehicular Networks: A survey” in IEEE Electronics, Communication and Photonics Conference, 2012.

[5] Irshad Ahmed Sumra, Iftikhar ahmad, Halabi Hasbullah “Classes of Attacks in VANET” in IEEE Electronics, Communication and Photonics Conference, 2011.

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

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

[8] Kamini, Rakesh K “VANET Parameters and Applications: A Review” in Global Journal of Computer Science and Technology, September 2010.

[9] Asim Rasheed, Dr. Amir Qayyum in “Security Architecture Parameter in VANET” in IEEE Transactions on Vehicular Technology, 2010.

[10] 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.

[11] Bersen, J. Manivannam, “Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service” In the fourth international conference on Wireless and Mobile Communications, 2008.

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

[13] T.Taleb, E.Sakhaee, A. Jamalipour, K.Hashimoto, N. Kato, and Y. Nemato, “A stable routing protocol to support its services in vanet networks” IEEE Transactions on Vehicular Technology, November 2007.

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

[15]M. Raya and J.P. Hubax, “Security aspect of inter-vehicle communications” in Swiss Transport Research Conference, 2005.

[16] Maxima Raya, Jean-Pierre Hubax “The security of vehicular ad hoc networks” Proc. Of the ACM Workshop on Security of Ad hoc and Sensor Networks (SASN), 2005.

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

[18] M.E. Zakri, S. Mehrotra, G.Tsudik, and N.Venkatasubramanian, “Security issues in a future vehicular network,” In European Wireless Conference, 2002.

BIBLIOGRAPHY

Ramanpreet kaur is currently pursuing M.Tech in CSE (E-security) in BBSBEC, Fatehgarh sahib, Punjab, India. Her research area is VANETs.

Er. Khyati Marwaha is currently serving as Assitant Professor in CSE/IT Department at BBSBEC, Fatehgarh Sahib, Punjab, India. Her reseach area is Mesh Networks and Adhoc networks.