International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Security Analysis of Vanet (Vehicular ad-hoc Network)

Sandeep Kumar, Amandeep Kaur, Charanjeet Kaur Raina

Department of Computer Science and Engineering, Adesh Institute of Technology, Chandigarh, Kharar, Punjab, India

ABSTRACT

VANET is a network in which cars or any other vehicles are used as mobile nodes. These mobile are used to form a communication network and these cars can move freely in any direction. VANET is a wireless network which is used for data exchange. As the VANET network name suggests, it is performed in vehicles. VANET consists of vehicle-to-vehicle (V2V) and vehicle - to - infrastructure (V2I) communications supported by wireless access technologies. In VANET, routing protocols have most significant role in terms of performance. The way of sending and receiving the packets is determined by routing protocols. In this paper, we examine and analyze the performance of Ad-hoc On-Demand (AODV), Destination-Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR) routing protocols over Constant Bit Rate (CBR) by using different speeds and number of nodes. VANET wireless communication is used to improve road safety and traffic efficiency. The performance measurements : Packet Delivery Ratio and Average Throughput, Average End to End Delay are examined with respect to speed and number of nodes. The objective of this study is to find the best routing protocol for security purpose so that it can be further used. Based on our validated results, AODV performs the best among from all three protocols.

Keywords : Vanet, Applications, Routing Protocols, Security System Requirements.

I. INTRODUCTION

VANET network supports the spectrum at wide range of mobile distributed applications that performed in vehicles. Traffic accidents are one of the largest societal problems which is faced by all over the world. It provide the drivers safety in driving on the roads which is considered as the important service. A number of people die in traffic accidents as not died by diseases and natural disasters. If the traffic information is provided to people then the occurrence of accidents can lowered in so much amount. Several studies show that 60% of the accidents can be avoided if the warning messages were provided before just few seconds at the moment of crash.It has high mobility speed of number of nodes and their position constraints to the layout of the streets and roads. In VANET, the vehicles (nodes) communicate with each other through Vehicle to Vehicle (V2V communication) and road-side infrastructure (V2I communications). It provides the information about the traffic conditions and other useful information to drivers. All adhoc networks are used in the VANET but it does not have any specific protocol. The main purpose of the adhoc network on reducing the consumption of energy and resources. The VANET architecture are carefully designed to protect against misuse activities. A mobile network whose node are vehicles (i.e., car, trucks, etc.) considered an extension of a MANET (Mobile Ad-hoc Network) because the possibility of working without infrastructure.

II. METHODS AND MATERIAL

APPLICATIONS

VANET support a wide range of applications – from simple dissemination messages to multiple dissemination of messages over large distances e.g cooperative awareness messages (CAMs). VANET can use any type of wireless networking technology from short to large range of technologies, cellular and LTE can be used in VANETs. Vehicular adhoc networks (VANETs) are created by applying the principles of

mobile adhoc networks (MANETs) – the spontaneous creation of a wireless network for data exchange – to the domain of vehicles. In the earlier years, the VANET applications are developed in the research field by applying MANET principles. The term VANET is similar with the generic term inter - vehicle communication (IVC), although the focus remains on the aspect of spontaneous networking. In VANET, the vehicles move in a particular fashion rather than moving randomly. Example Applications of VANETs are:

1. Electronic brake lights, which allow a driver to react to vehicles braking even though they might be obscured (e.g., by other vehicles).
2. Platooning, which allows vehicles to closely (down to a few inches) follow a leading vehicle by wirelessly receiving acceleration and steering information, thus forming electronically coupled "road trains".
3. Traffic information systems, which provides information to drivers through vehicle's satellite navigation system.

SECURITY SYSTEM AND ITS REQUIREMENT

The VANET and also other systems of communications between vehicles look for to guarantee the security and efficiency of transport systems, supplying, for example, acknowledgments of the warnings of the environmental hazards (fog, fire, etc.) and conditions of the road traffic (emergency or places of construction). The main characteristic of VANET without infrastructure of this network, it can access the base station, inside of WIFI, WIMAX, GSM or UMTS. The people communicate with each other through the multiples steps of the intermediate collaboration, who are out of the reach of the radio broadcast, Different routing protocols are used for security, these are Ad-hoc On Demand (AODV), Destination-Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR). The security of the protocol can be specified by hierarchic levels reliable between we or by requirements of security as authenticity and not-repudiation. The levels can be defined by allotting a private key between we and the system distribution of keys. SAR (Security Aware Routing) is the first protocol used for sensor networks that includes the notion of QoS in its routing decisions. This protocol maintains the routes of reactive routing protocols as the AODV and the DSR and becomes insurance the discovery processes. An implementation of SAR protocol based on the AODV protocol. AODV possess the specified level of security they only can be incorporated during the process of route discovery.

The classic security requirements which we observed are the authentication, the Integrity, the confidentiality, the not – repudiation and the availability. The authentication guarantees that one given entity is really who it says to be, while that not - repudiation hinders that the sender of a message denies its authorship. The confidentiality guarantees the secrecy will be changed of the information and the integrity allows to affirm that the information received had not been modified during the transit to the long one of the net. The availability treats to guarantee that if there will be necessary then resources will be available.

COMPARISON OF ROUTING PROTOCOLS

We compares the these three routing protocols; DSDV and AODV over VANET by using NS2 simulator. The comparison aims to compare these protocols to analyze the packet loss rate and performance of the throughput. They conclude that AODV has the highest throughput and the best performance among these three. Also, they state that the network performs better with existence of Road Side Unit (RSU). The performances of AODV and DSDV was analyzed based on variation of speed and node density values. Based on the analysis, both protocols AODV and DSDV provide a high Packet Delivery Ratio and perform very well whenever the low speed and node density were used. A comparison of DSDV and AODV routing protocols was presented. The Packet Delivery Ratio and Average End to End Delay were measured. The paper concludes that AODV provides a high Packet Delivery Ratio. Moreover, the AODV can be considered as the best routing protocol for carrying the packet over VANET. The effect of different packet size with the implementation of AODV routing protocols in homogeneous and heterogeneous MANET focuses on the transmission of packets throughout the network from one to all nodes in broadcast way using MIMO technology. Its research attracts a lot of attention from researchers working in various fields including networking, electronics,security, automotive, software engineering, transportation, and so on. VANET related some issues include areas such as routing, capacity, Quality Service (QoS), security attacks and threats, the effects of

transmission power on protocol performance. The accuracy of the analytical result is confirmed through extensive simulations.

The Packet Delivery Ratio, Average Throughput and Average End to End Delay for each of DSR, AODV and DSDV routing protocols have been measured. Different speeds in the range from 1m/s to 45 m/s under CBR traffic connections is used to evaluate the performance these three routing protocols. We used the different number of nodes and varying speed as a performance parameter. The speed ranges from 1 m/s to 40 m/s and number of node ranges from 5 to 40 to examine and analyse the performance of the protocols. We received different results based on the node speed and number of nodes for our measured parameters ; Packet Delivery Ratio, and Average Throughput, Average End to End Delay Packet delivered ratio is the ratio of number of data packets transmitted to the total received data packet successfully. Results with CBR data traffics for fixed and mobile nodes are simulated with various numbers of nodes and node mobility speed.

III. CONCLUSION

AODV, DSR and DSDV routing protocols using CBR traffic connections. We considered the speed and the number of nodes as the controlled parameters in our experiments to determine the best routing protocol. As per the simulation, for considering packet delivered ratio AODV is superior then DSDV and AODV proves to be consistent for various speed and different number of nodes. Secondly considering, Average throughput with AODV better throughput is measured with node mobility. We recommend AODV for secured communication in VANET's based on the simulation results .With the Addition of security it can achieve better performance for the mentioned parameters.

IV. REFERENCES

[1]. Vehicular ad hoc network - Wikipedia Retrieved from https://en.wikipedia.org/ wiki /Vehicular_ad_hoc_network

[2]. VANET : The Vehicular Ad-Hoc Network | Emerging Technologies, Retrieved from https://emerging technology.wordpress.com/2007/.../vanet-the-vehicular-ad-hoc-network...

[3]. Ameer Ali; Dr. Latha C.A, Defining the Performance Analysis of Ad-Hoc Routing Protocols for VANET Using NS2 Simulation. Retrieved from https://www.researchgate.net/publication/281116796_Performance_Analysis_of_Ad-Hoc_Routing_Protocols_for_VANET_Using_NS2_Simulation

[4]. Kirti A. Yadav ;P. Vijayakumar ,defining the VANET and its Security Aspects: A Review | Yadav | Indian Journal of ...Retrieved from www.indjst.org/index.php/indjst/article/view/97105

[5]. Mohan Li , defining the security in VANET's. Retrieved from https://www.researchgate.net/.../258248007_Vehicular_ad-Hoc_networks_VANETs-An...

[6]. Saif Al-Sultan ; Moath M. Al-Doori ;Ali H. Al-Bayatti ; Hussien Zedan . Defining the comprehensive survey on vehicular Ad Hoc network.Retrieved from www.sciencedirect.com/science/article/pii/S108480451300074X

[7]. Sabih ur Rehman , M. Arif Khan , Tanveer A. Zia , Lihong Zheng,Defining the Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges, Retrieved from article.sapub.org/10.5923.j.jwnc.20130303.02.html

[8]. VANET/ITS Introduction | VANET/ITS Website (NEO). Retrieved from neo.lcc.uma.es/staff/jamal/vanet/?q=node/1

[9]. VANET - Vehicle Ad hoc Networks - ULisboa. Retrieved from comp.ist.utl.pt/~rmr/WSN/CaseStudies2007-no/WSN_Transportation