ENHANCEMENT IN VANET SECURITY SYSTEM

[1]M.s. Asha. R, [2]Tharun. J, [3]S.B. Rishik, [4]Akilan Ganesan, [5] M.Mageswaran
[1]A.P SRMIST, [2]B.Tech. Student SRMIST, [3]B.Tech. Student SRMIST, [4]B.Tech. Student SRMIST, [5]B.Tech. Student SRMIST
[1]Computer Science,
[1]SRM IST, Chennai, India

Abstract : Recently, Vehicular Ad hoc Networks (VANETs) have achieved widespread applicability in different application domains related to transportation systems such as providing public safety and assistance, driving improvement, toll collection, roadside service finders, traffic monitoring and control, highway Internet access and enhancing safety and efficiency of highway systems. VANETs are also known as Wireless Access in Vehicular Environment (WAVE) that supports Intelligent Transportation Systems (ITS) through Dedicated Short-Range Communication (DSRC). In VANETs, there are two types of communications: vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). Vehicles have On Board Units (OBUs), which consist of Omni directional antennas, processors, GPS unit, and sensors for V2V communications.Vehicles also perform V2I communications with roadside infrastructures, which are placed within a fixed distance of each other depending upon the communication range of the roadside devices, also known as Road Side Units (RSUs). RSUs communicate each other through wireless medium or wired connections.

IndexTerms **- VANET, On board unit, Road side unit.**

I. INTRODUCTION

Recently, Vehicular Ad hoc Networks (VANETs) have achieved widespread applicability in different application domains related to transportation systems such as providing public safety and assistance, driving improvement, toll collection, roadside service finders, traffic monitoring and control, highway Internet access and enhancing safety and efficiency of highway systems. VANETs are also known as Wireless Access in Vehicular Environment (WAVE) that supports Intelligent Transportation Systems (ITS) through Dedicated Short-Range Communication (DSRC).

In VANETs, there are two types of communications: vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). Vehicles have On Board Units (OBUs), which consist of Omni directional antennas, processors, GPS unit, and sensors for V2V communications.Vehicles also perform V2I communications with roadside infrastructures, which are placed within a fixed distance of each other depending upon the communication range of the roadside devices, also known as Road Side Units (RSUs). RSUs communicate each other through wireless medium or wired connections. They can also be mobile. The V2I communications can be further extended to provide applications such as Internet since RSUs can be connected to a network. The V2V communications can be used to send emergency and real-time information such as an accident or road traffic information so that other vehicles can take alternative routes to prevent traffic congestions.

II. RELATED WORKS

Since VANETs support emergency real-time applications and also deal with life critical information they should follow the security requirements such as privacy, confidentiality, integrity, and non-repudiation to provide secured communications against attackers, and malicious nodes. Various security attacks such as Denial of Service (DOS), Sybil attack ,Wormhole attack ,Illusion attack and Purposeful attack not only affect the privacy of the drivers and vehicles but also compromise traffic safety and eventually lead to loss of life. Security is a big challenge everywhere because the accidents are are increasing day by day owing to the unsafe and insecure security systems in vehicles,and VANET systems. Several technologies are available to keep vehicles safe from intruders, but most common VANET systems work on wireless GSM communication. Such systems provide security from natural, incidental, intended, unintended, accidental and human made problems by continuously monitoring the VANET network and making sure the network cannot be breached from the outside and making it foolproof from the inside as well.

III. VANET SECURITY

Since VANETs support emergency real-time applications and also deal with life critical information they should follow the security requirements such as privacy, confidentiality, integrity, and non-repudiation to provide secured communications against attackers, and malicious nodes. Various security attacks such as Denial of Service (DOS), Sybil attack ,Wormhole attack ,Illusion

attack and Purposeful attack not only affect the privacy of the drivers and vehicles but also compromise traffic safety and eventually lead to loss of life. Security is a big challenge everywhere because the accidents are are increasing day by day owing to the unsafe and insecure security systems in vehicles,and VANET systems. Several technologies are available to keep vehicles safe from intruders, but most common VANET systems work on wireless GSM communication. Such systems provide security from natural, incidental, intended, unintended, accidental and human made problems by continuously monitoring the VANET network and making sure the network cannot be breached from the outside and making it foolproof from the inside as well.

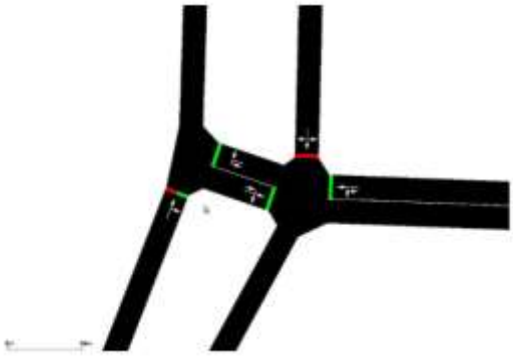


Fig 1. Implementation of VANET on NS3.

This generational procedure is rehashed until the point when an end condition has been achieved. Normal ending conditions are:

· An answer is discovered that fulfills least criteria

· Settled number of generations found

· Designated spending plan (calculation time) found

· The most elevated positioning arrangement's wellness is coming to or has achieved a level to such an extent that progressive cycles never again create better outcomes

· Manual investigation

· Blends of the above conditions.

IV. IMPLEMENTATION

4.1Simulation Software

A network simulator is software that predicts the behavior of a computer network. Since communication networks have become too complex for traditional analytical methods to provide an accurate understanding of system behavior, network simulators are used. In simulators, the computer network is modeled with devices, links, applications etc. and the network performance is reported. Simulators come with support for the most popular technologies and networks in use today such as Wireless LANs, mobile ad hoc networks, wireless sensor networks, vehicular ad hoc networks, cognitive radio networks, LTE / LTE- 5G, Internet of Things (IoT) etc..

4.2Simulation

A simulator written in Java, which can generate mobility traces in several formats. There are also other traffic simulators, like TranSim , which makes use of a cellular automaton for simulating the interaction of vehicles. Cellular Automaton Based Vehicular Network (CAVENET) , is a lightweight simulator written in MATLAB and ns-2/ns-3 which can be used to understand the properties of the mobility models of vehicular trafficfic and their impact on the performance of VANETs. The Opportunistic Network Environment (ONE) is a simulation environment that is capable of generating node movement using different movement models, routing messages between nodes with various DTN routing algorithms and sender and receiver types, visualizing both

mobility and message passing in real time in its graphical user interface. ONE can import mobility data from real-world traces or other mobility generators. It can also produce a variety of reports from node movement to message passing and general statistics. Also, SUMO is another trafficfic simulator, intended for trafficfic planning and road design optimization. There is an attempt to interface SUMO with NS2. In this regard, we used SUMO simulator which can be used to understand the properties of the mobility models of vehicular trafficfic and their impact on the performance of VANETs and interface it with NS3 to evaluate the performance of routing protocols

Function for plotting the obstacles. The coordinates of the actual obstacles can be simulated in the program using the vector functions and polygons. The code snippet below describes the mapping of the obstacles.

For our performance comparison study, we choose different routing protocols HWMP, OLSR and DD. We will shortly describe these protocols in following.

4.3HWMP Protocol

Hybrid Wireless Mesh Protocol (HWMP) defined in IEEE 802.11s, is a basic routing protocol for a wireless mesh network. It is based on AODV [19] and tree-based routing. It relies on peer link management protocol by which each mesh point discovers and tracks neighboring nodes. If any of these are connected to a wired backhaul, there is no need for HWMP, which selects paths from those assembled by compiling all mesh point peers into one composite map. HWMP protocol is hybrid, because it supports two kinds of path selection protocols. Although these protocols are very similar to routing protocols in case of IEEE 802.11s they use MAC addresses for “routing”, instead of IP addresses. Therefore,we use the term “path” instead of “route” and thus “path selection” instead of “routing”. HWMP is intended to displace proprietary protocols used by vendors like Meraki for the same purpose, permitting peer participation by open source router firmware.

4.4OLSR Protocol

The OLSR protocol is a pro-active routing protocol, which builds up a route for data transmission by maintaining a routing table inside every node of the network. The routing table is computed upon the knowledge of topology information, which is exchanged by means of Topology Control (TC) packets. OLSR makes use of HELLO messages to find its one hop neighbours and its two hop neighbours through their responses. The sender can then select its Multi Point Relays (MPR) based on the one hop node which offer the best routes to the two hop nodes. By this way, the amount of control traffic can be reduced. Each node has also an MPR selector set which enumerates nodes that have selected it as an MPR node. OLSR uses TC messages along with MPR calculated and used as a parameter to select the next iteration of species forwarding to disseminate neighbour-information throughout the network. Host Network Address (HNA) messages are used by OLSR to disseminate network route advertisements in the same way TC messages advertise host routes.

4.5DD Protocol

The core of the DD protocol is based on the concept of a utility function. A utility function assigns a utility value, Ui, to every packet i, which is based on the metric being optimized. The Ui is defiend as the expected contribution of packet i to this metric. The DD replicates packets first that locally result in the highest increase in utility. For example,assume the metric to optimizes average-delay.The utility function defiend for average delay is Ui = −D(i), basically the negative of the average delay. Hence, the protocol replicates the packet that results in the greatest decrease in delay. The DD, like MaxProp, is flooding-based, and will therefore attempt to replicate all packets if network resources allow.

The overall protocol is composed of four steps:

1)Initialization: Meta-data is exchanged to help estimate packet utilities.

2)Direct Delivery:Packets destined for immediate neighbour are transmitted.

3)Replication: Packets are replicated based on marginal utility (the change is utility over the size of the packet).

4) Termination: The protocol ends when contacts break or all packets have been replicated.

V. SIMULATION SYSTEM DESIGN AND DESCRIPTIONS

Simulation System Structure The simulation system structure. The behavioural analyzer block (SUMO), generates the movement pattern of the vehicles that is used by the communication protocol analyzer (NS3 simulator). The detailed simulation model is based on NS-3 (version 3.14.1). The NS3 simulator is developed and distributed completely in the C++ programming language, because it better facilitated the inclusion of C-based implementation code. The NS3 architecture is similar to Linux computers, with internal interface and application interfaces such as network interfaces, device drivers and sockets. The goals of NS3 are set very high: to create a new network simulator aligned with modern research needs and develop it in an open source community. Users of NS3 are free to write their simulation scripts as either C++ main() programs or Python programs. The NS3 low-level API is oriented towards the power-user but more accessible "helper" APIs are overlaid on top of the low-level API.In order to achieve scalability of a very large number of simulated network elements, the NS3 simulation tools also support distributed simulation. The NS3 support standardized output formats for trace data, such as the pcap format used by network packet analysing. tools such as tcpdump, and a standardized input format such as importing mobility trace files from NS2. The NS3 simulator has models for all network elements that comprise a computer network. For example, network devices represent the physical device that connects a node to the communication channel. This might be a simple Ethernet network interface card, or a more complex wireless IEEE 802.11 device.

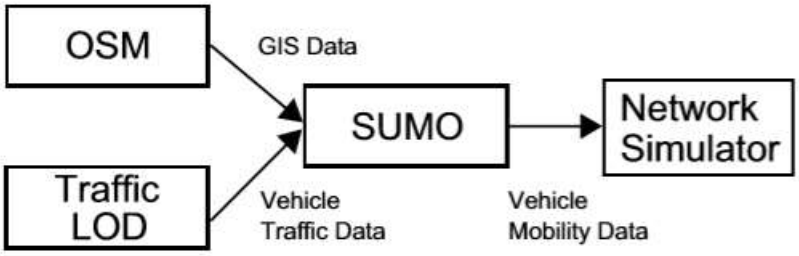
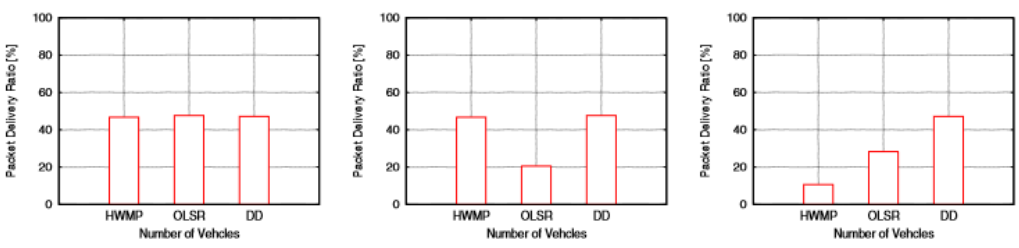


Fig 2. Simulation system structure

VI. RESULTS

We present here some simulation results for HWMP, OLSR and DD protocols done by means of SUMO and NS3. For performance evaluation, we use three metrics: the average PDR, throughput and delay. In Fig. 3 are shown the simulation results of PDR for three protocols. We can see that the performance of DD protocol is better than HWMP and OLSR protocols.The simulation results of throughput. Forms all number of vehicles,three protocols perform almost the same. However, when the number of vehicles is 220, the DD protocol has a better performance than HWMP and OLSR protocols. The simulation results for delay. For small number of vehicles, the HWMP protocol has low delay. However, for big number of vehicles, the DD protocol has low delay.



(a) Number of Vehicles: 20 (b) Number of Vehicles: 110 (c) Number of Vehicles: 220

Fig 3. Implementation of VANET in Different protocols

VII. FUTURE SCOPE

Additionally, mobility of vehicles and dynamic nature of the network impose a great challenge to eliminate malicious vehicles and design secured data transmission protocols. Though extensive researches are being conducted to provide security and privacy in VANETs most of these approaches consider reducing computational and communication overhead, and processing delay for authentication between the source and destination vehicles. Beside, most existing security schemes of VANETs do not support the security checks while handing over a vehicle from one Road Side Unit (RSU) to another RSU. The protocols for high priority applications are still in exploratory level in terms of security measures. In addition, the following aspects should be considered as future research possibilities in this area.

- Distributing certificates securely, validating them very fast and computationally efficient way should be given more attention while designing secured routing protocols for VANETs.

- Determining the mobility pattern of vehicles and linking the mobility pattern with malicious vehicles could be considered as a potential research in providing security and privacy in VANETs.

- Determining and assigning trust values to vehicles and establishing trust among vehicles are significantly important to provide the integrity and reliability of applications in VANETs.

- The change of MAC addresses along with the pseudonyms has not received sufficient attention. If the IP address changes with the pseudonym the MAC address should also change. Otherwise, adversaries can easily track the target vehicle by its MAC address.

VANETs can provide Internet services on highways. Users normally use Internet on highways for emergency communications (e.g., checking emails, and instant messaging) and social network applications (e.g., facebook, twitter). Thus, designing secured communication protocols for VANET's to protect user profiles and private data from malicious vehicles should be given the highest priority in this area of research.

VIII. FUTURE SCOPE

Vehicular Ad hoc Networks (VANETs) are becoming popular in transportation systems since they provide road safety, traffic management, and Internet access on highway and distribute safety information to drivers and passengers. However, it poses a great challenge to implement VANETs in value-added services due to the intruder vehicles and several security attacks. Thus, providing security and privacy in VANETs are considered as the most important research issue in this area. We also evaluated the performance of HWMP, OLSR and DD routing protocols for different number of vehicles in a VANET crossroad scenario considering PDR, throughput and delay as evaluation metrics. We used SUMO to generate the movement of the vehicles and NS3 for the performance of routing protocols. For simulations, we considered IEEE 802.11p standard and TwoRayGround Propagation Loss Model and sent multiple CBR flows over UDP. From simulations, we found the following results. Considering PDR, the performance of DD protocol is better than HWMP and OLSR protocols.For small number of vehicles, three protocols perform almost the same. However, when the number of vehicles is 220, the DD protocol has a better performance than HWMP and OLSR protocols.For small number of vehicles, the HWMP protocol has low delay. However, for big number of vehicles, the DD protocol has low delay.

REFERENCES

[1] J. Harri, F. Filali and C. Bonnet, "Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy", IEEE Communications Surveys & Tutorials, Vol. 11, No. 4, pp. 19-41, 2009.

[2] F. Bai, N. Sadagopan, and A. Helmy, "IMPORTANT: A Framework to Systematically Analyze the Impact of Mobility on Performance of Routing Protocols for Ad-hoc Networks", In Proc. of IEEE INFOCOM-2003, pp. 825-835, MarchApril 2003

[3] N. Sadagopan, F. Bai, B. Krishnamachari, and A. Helmy, "PATHS: Analysis of Path Duration Statistics and Their Impact on Reactive MANET Routing Protocols", In Proc. of the 4-th ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc-2003), pp. 245256, 2003.

[4] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation for VANETs",Proc. of the 40-th Annual Simulation Symposium (ANSS-2007), pp. 301-309, 2007.

[5] L. Smith, R. Beckan, R. Anson, K. Nagel, and M. Williams, "TRANSIMS: Transportation Analysis and Simulation System", In Proc. of the 5-th National Transportation Planning Methods Applications Conference, LA-UR 95-1664, April 1995.

[6] G. De Marco, M. Tadauchi and L. Barolli, "Description and Analysis of a Toolbox for Vehicular Networks Simulation", In Proc. of IEEE ICPADS/PMAC-2WN-2007, Vol. 2, pp. 1-6, 2007.

[7] K. Nagel and M. Schreckenberg, "A Cellular Automaton Model for Freeway Traffic", Journal of Physics I France, Vol. 2, pp. 2221-2229, 1992.

[8] A. Keranen, J. Ott, and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation", In Proc. of the 2-nd International Conference on Simulation Tools and Techniques (SIMUTools-2009), 2009, http://www.netlab.tkk.fi/tutkimus/ dtn/theone/pub/the one simutools.pdf.

[9] M. Piorkowski, M. Raya, A. L. Lugo, M. Grossglauser, and J. P. Hubaux, "Joint Traffic and Network Simulator for VANETs", In Proc. of Mobile and Information Communication Systems Conference (MICS-2006), October 2006

[10] E. Spaho, Gj. Mino, L. Barolli and F. Xhafa, "Goodput and PDR Analysis of AODV, OLSR and DYMO Protocols for Vehicular Networks using CAVENET", International Journal of Grid and Utility Computing (IJGUC), Vol. 2, No. 2, pp. 130-138, 2011.

[11] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc OnDemand Distance Vector (AODV) Routing", IETF RFC 3561 (Experimental), 2003.