Research Journal of Computer and Information Technology Sciences ____________________E-ISSN 2320 – 6527
Vol. **4(9),** 9-13, September **(2016)** *Res. J. Computer and IT Sci.*

Review Paper

Efficient and Secure Routing Protocols in VANET: A Simulation Result

Kavita Tandon[1*] and Sneha Kanchan[2]
[1]Department of Computer Science and Engineering, Bhilai Institute of Technology, Durg, Chhattisgarh, India
[2]Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, India
tinkytandon@gmail.com

Available online at: www.isca.in, www.isca.me
Received 24th Feburary 2016, revised 3rd August 2016, accepted 30th August 2016

Abstract

Vehicular Ad Hoc Networks (VANETs), introduced as a trivial subset of Mobile Ad Hoc Networks (MANETs), creates unpremeditated network of vehicles to exchange information between them, providing a prominent approach for communication in transportation media to form an Intelligent Transport System (ITS). Besides being launched as a subset of MANET, both share differences in several important properties such as special mobility pattern, unlimited battery life and hastily changeable topology in VANET. The design of routing protocols in the network is one of the prime issues in supporting smart ITS. The routing protocols of MANET are not equally effective in VANET as later are more sensitive to the safety problems. The intrusion on the support of transmission is easier conducting denial of service attack by jamming the frequency bands used. Attacks against the routing protocol for the network can be designed to change the protocol itself. The need of a reliable and robust network can be fulfilled only if it is having advanced security and privacy features, which ultimately depends upon the routing protocols used. Secure routing is imperative during the routing process to incorporate mutual trust between these nodes. Establishing trust is a challenge while one or more malicious nodes attempt to disrupt route discovery or data transmission in the network. This report represents the simulation results performed using Network Simulator-3 (NS-3) on various routing protocols. The already published results on protocols are also taken into consideration. Finally, we have shown the effect of response time of network using specific protocols after increasing the number of nodes i.e. scalability.

Keywords: VANET, Routing Protocols, Security, Simulation.

Introduction

Vehicular Ad Hoc Network (VANET) is a prominent subclass of Mobile Ad Hoc Networks (MANETs) invented for vehicular communication providing an eminent approach for inter-vehicle communication which leads to Intelligent Transport System (ITS). The nodes (vehicles) can talk to each other as well as to the roadside units (RSU) e.g. traffic lights. These networks were basically designed to comfort drivers and passengers in a safe way. The accident rate or death rate in any road accident is very high all over the globe which is a serious issue to deal with. On top of that, traffic jams in big cities are extreme nuisance. These problems hinder daily routine of the travellers by squandering their most of the time on road only[1]. Hence VANET is innovated as the ad hoc network which will save the traveller's life, assets, money and time in a comforting manner. To support the intelligent transportation, routing techniques must be precise. Hence, designing an efficient routing protocol, which is accurate at the same time, is the necessary overhead of the network analysts. Although VANET is elevated for its unlimited battery and storage capacity, the dynamic topology and definite mobility pattern are the major concern of the network over MANET. In addition, it requires trusted vehicles to vehicles communication which is primarily contingent on their privacy and safety features, and so pivoting the role of routing protocols used. The routing data needs to be transmitted among vehicles, known as V2V communication, and to roadside infrastructure, known as V2I communication.

To make this network efficient, we need to implement a routing protocol which will give quick but accurate routing decision. In other words, it must be fast enough to meet each requirement of the network in any traffic condition. Since, it is always advantageous to consider the pros and avoid the cons of the existing protocols to develop a new protocol, we will first check for the efficiency of the existing ones. Being a new and interesting technology, since beginning only, VANET has taken immense attention from every sector either academy or industry. Many major automobile manufacturer companies have already gathered up with government agencies to develop solutions aimed at helping drivers on the roads, however any pivotal advancement has not been seen yet[2]. To count one of the development in this field is Wireless Access for Vehicular Environment (WAVE) that has been designed for supporting the short range communication in ITS by managing the traffic and its safety. The technique is based on IEEE 802.11p which is an improved version of IEEE 802.11 standard. The objective of this protocol was particularly for Dedicated Short Range

Communication (DSRC) services which include toll collection, commercial transaction via vehicles, and other safety services. WAVE has been successfully implemented in Portuguese city of Porto where it enables the communication between public vehicles and wifi access for its passengers. In similar way, every vehicle should be equipped with the technology that empowers drivers and passengers of other vehicle to be able to send/receive messages to upgrade the driving experience. Another development can be given as TraceNet, developed by Microsoft's MSN TV and KVH, which can provide in-motion access to the internet developing an automotive-vehicle Internet-access system and turning the whole vehicle into an IEEE 802.11-based Wi-Fi hot-spot[3]. Using TraceNet, the vehicles can be traced, detect jams, locate another vehicle as well. In brief, VANET has not implemented much in real life scenario, it is an active area of research as it enhances road safety, magnifies travel efficiency, controls traffic, and ultimately provides convenience, comfort and ease of travelling to the riders[4].

Routing Challenges in VANET

The idea of equipping each vehicle with sensors needs massive improvements in existing routing protocols. VANET poses unique features which differentiate it from MANET and so the need of efficient routing protocols arises. Those can be given as below: i. Dynamic topology, ii. Frequent disconnected network, iii. Mobility modelling, iv. Battery power and storage capacity, v. Communication environment, vi. Interaction with on-board sensors. In other wireless networks, the nodes have constraints on energy, storage and processing capacity[5]. Thankfully in VANET, there is no limitation on all these. The routing protocols are categorized in VANET on the basis of topology, position, clustering, broadcasting and security.

Topology Based Routing Protocols: In VANET, the topology changes very frequently and so makes it difficult for the topology based routing protocols to work as efficient as in fixed sensor network. Since there is an immense need of quicker route discovery and maintenance, the overall load on the network increases. These protocols use link information for sending packets from source to destination. Because of the high mobility factor, network partitions frequently, leading to frequent disconnection of routes resulting in re-computation of the entire topology again. These protocols are further classified as:

Proactive Protocols: Proactive routing protocols create their tables as soon as the network is created and regularly update those tables if there is any change in the network. That means that the routing details are calculated by each node after every change in network regardless of its requirement. This fulfils the request very fast after being made on the cost of several unused calculations and reduced bandwidth. A table is constructed and maintained within a node and also maintains unused data paths, which causes the reduction in the available bandwidth. Since VANET is a real time application, it is very inefficient to update the routing table that frequently.

Reactive Protocols: Reactive routing protocols discover routes only if there is any request. Hence it doesn't need to find routes after any modification which saves several CPU cycles and memory. Whenever there is any request, route request packets are flooded in the network, followed by the route discovery. Although the process takes time in comparison to Proactive ones, it causes lesser overhead resulting in efficient use of given bandwidth.

Hybrid Protocols: Hybrid protocols combines the benefits of both discussed above and diminishes their drawbacks. In particular, it tries to pose lesser routing overhead as well as lesser initial route discovery delay by restricting the use of proactive protocols for a defined local neighbourhood whereas using reactive protocols for global network.

Position Based Routing Protocols: Position based routing is also called geographic routing. In contrast to topological based routing, here no establishment or maintenance is needed. Instead location services like Global Position System (GPS) are used. The nodes in the network decides routes the basis of their geographic position. Since no global routes are formed, it consists of lesser overhead. The protocol has been further divided in two protocols: i. Greedy V2V protocols, ii. Delay Tolerant Protocols.

Cluster Based Routing: Clustering is done to divide the network into interconnected sub-structures known as clusters. The nodes themselves calculate their respective clusters and head of their particular cluster. The routing process in these clusters is governed by those heads with the use of gateway nodes (nodes present in two or more clusters; media of communication between clusters). These protocols posses good scalability because a very large network can also be divided into sub-networks communicating via their cluster heads but the delay is often noticeable. Also, forming a new cluster, choosing cluster heads and gateway nodes are very hectic in frequently changing VANET.

Broadcast Routing Protocols: Broadcast based routing protocols are used to share the reports about traffic, weather, road conditions, or any emergency message among vehicles. These can also be beneficial for broadcasting any report, announcements or even advertisements. Multi-hop routing is used to deliver the message to each node in the network on the cost of bandwidth and duplicate issue.

Secure Routing Protocols: The most known secure protocols are: Secure Efficient Ad hoc Distance Vector (SEAD), Secure Remote Password protocol (SRP), Secure Ad hoc On-Demand Distance Vector (SAODV), ARAN and ARIADNE. SAODV uses public key cryptography to encrypt the messages like routing request RREQs, routing reply RREPs, and routing error

RERRs messages. These messages are signed by the nodes using their private keys before sending it out to provide authenticity. Receiving node can verify the message by decrypting it using generator's public key. SEAD, the secure version of DSDV, protects the nodes from Denial of Service, DoS attack in which the resources of network are deliberately made unavailable by the attacker[6]. Authenticated Routing for Ad-hoc Networks (ARAN) is a secure on-demand routing protocol that was specially designed for dealing with authenticity and integrity of messages in ad hoc networks. It observes and takes action against any malicious activity.

It also provides non-repudiation which means message sent to the network cannot be denied by the source. ARIADNE is a secure version of DSR that provides point to point authentication. It prevents flooding of RREQ packets unlike the base protocol, and so preserves the network from cache poisoning attack but it cannot protect against wormhole and rushing attack (typically results in denial of services)[7].

Security Issues in VANET

Since VANET is a wireless and distributed network, it is less protective in nature, and hence more susceptible to security attacks. The attacker can be an insider or outsider depending on their authenticity to access the network. They generally target main area of the road but, even chances are very low, they can also try to attack the restricted area. Their goal of attack is constrained by their budget, time, technical expertise, and tools which ultimately depend upon how secure our protocols are. There are several types of attacks possible e.g. network attack, timing attack, monitoring attack etc. On the whole, these attacks are categorized here in two categories: i. Active attacks. ii. Passive attacks.

Active attacks can track as well as modify the contents of the message sent in the network whereas in Passive ones, the attackers can only listen through the channels but they are unable to modify the contents. Attackers change their attacking strategies from time to time. And hence they are difficult to be tracked. Users require safe and secure journey and for that we must have secure vehicular network and its applications. However, there are several securities issues in VANET which can are be more dangerous than in other wireless networks. Few of them can be categorized as below: i. Bogus Information attack, ii. Unauthorized pre-emption attack, iii. Message Replay attack, iv. Message modification attack, v. Node Impersonation attack, vi. RSU replication attack, vii. Denial of Services attack, viii. Movement tracking.

So, the desired requirements in this network also changes when comparing with other networks[8]. These include: i. Data origin authenticity and origin, ii. Anonymous User Authentication, iii. Vehicle Anonymity (Conflicts with Authentication), iv. RSU ID exposure, v. Prevention of RSU replication, vi. Vehicle ID traceability, vii. Efficiency and Real Time Constraints.

Network Simulation

Network Simulation is a technique of modelling the network behaviour by observing in a test lab. To check the changing behavior in different conditions, the attributes of the environment can be modified as well. There are different types of simulators available to simulate the ad hoc network and NS (Network Simulator) is one of the most popular simulators among those. It is a series of discrete event simulators which specially includes NS-2 and NS-3. Both are targeted for networking research especially for TCP, routing protocols, multicast protocols etc over wired and wireless networks. Among two, NS-2 has been used and widely accepted by a larger community. The components of NS-2 are written in OTcl and C++ both. Like NS-2, NS-3 is also an open source tool but with modular design. All the components are completely written in C++. It provides a set of simulation models implemented as C++ objects emphasising more on emulation. Python can also be used as the programming language in NS-3.

To do the simulation, we need to know on which criteria, we want to do our simulation. Since, it is for deciding routing technique, our simulation will mainly concentrate on length of routing packet, delay, goodput, and PHY/MAC overhead. Goodput is throughput of a particular transmission at application level. It generally gives the number of useful data bits (excluding retransmission and other protocol overhead data bits) transmitted to the destination per unit of time. The difference between goodput and throughput is that throughput also includes protocol overhead and retransmission bits, doesn't matter if it is useful or not, whereas goodput occupies useful data only. Throughput measurements, such as those reported by router interface statistics, cannot distinguish the nature of the data owing through the interface merely that bits have gone past. Throughput is not the same as good-put because throughput can include undesirable data such as data retransmissions, or overhead data such as protocol wrappers. In the case of TCP/IP, retransmissions occur because TCP data did not make it to the recipient in a timely fashion. Receivers signal to senders with an ACK that data was received. If a sender does not receive an expected ACK for a block of data, it will retransmit that data. Retransmissions are a waste of bandwidth; the same data traversing a link twice is definitely not part of good put.

MAC/PHY overhead means the extra bits added in the packet along with the actual message at MAC layer and Physical layer to make the message comfortably understandable at receiver side. The length of those extra bits depends upon the protocol used. Sometimes, this length is even greater than the actual message size. In an analysis given in, it is observed that during the time spent on protocol overhead and other delays, 802.11g is able to send another 400 bytes of data at 54 Mbps[9]. This clearly shows how much time and bandwidth are wasted just because of these overheads. So, these overhead must be minimized in order to make the network more efficient.

In VANET, traffic information mainly consists of Routing data and Broadcasting of Basic Safety Message (BSM). BSM is a data packet that is broadcasted from every vehicle at a nominal rate of 10 Hz. It generally consists of core data like size of the vehicle, its position, speed, brake status etc. Few BSM are sent if there is any emergency situation e.g. accident. Obviously, second type of BSM messages is not that frequent but those needs to be handled at high priority. Packet Delivery Ratio (PDR) is the percent of expected packets within range (index) that are actually received.

Simulation Setup: For Our Simulation we are using NS3 as the simulator mainly because NS-3 provides greater scalability and better performance in comparison to NS-2. Number of nodes is varied from 20 to 100 in this work. Mobility model used is Random waypoint Mobility Model (RWP). Mobility model for VANET behave very different in nature than MANET[10]. So, we need to implement our protocol on specific VANET models, but to start with basics, in this paper we are just comparing the effect of RWP on existing VANET routing protocols. Readings are taken from 0 second to 10 seconds. Goodput, MAC/PHY overhead and delay are recorded for concluding the efficient routing protocol. 10 sink nodes are taken in case of 20 nodes, 20 sink nodes are taken in case of 50 and 100 nodes.

Simulation Result

Goodput: The graph has been plotted between number of nodes and acquired Goodput, varying the load on the network in terms of nodes. Only few popular protocols among topology based protocols are considered for this simulation. As explained in graphs, blue bar represents AODV, red ones are for DSDV, green is OLSR and purple is for DSR. In Figure-1, number of total nodes is 20 and number of sink nodes is 10. The highest bar of AODV can be clearly seen in most of the cases. Even if the bar of AODV is not highest, it is very consistent and at least equal to the rest of the protocols. DSR is having the second highest bar. The second and third diagrams i.e. Figure-2 and Figure-3 respectively shows the consistent behaviour of AODV but DSR is performing really well in both the charts even better than AODV in some cases. In third case, DSDV seems to be the better choice than AODV. The Goodput of OLSR is not consistent and giving poor performance in most of the cases.

MAC/PHY Overhead: MAC/PHY is directly related to bandwidth utilisation. If overhead is lesser, less number of bits is required for information other than the actual data, which clearly means more data bits can be sent in a packet. Figure-4 represents the MAC/PHY overhead involved in the protocols which we are considering for this research. Blue bar represents the overhead when the network was loaded with 20 nodes. Similarly, red and green represent network load of 50 and 100 nodes, respectively. DSR is not considered here because it is having huge overhead when comparing to other three. In comparable protocols, AODV is having highest overhead which significantly becomes to more than half with the increase in number of nodes from 20 to 100. DSDV is having lesser than AODV but greater than OLSR but it also shows noticeable growth in overhead with the network load. OLSR consists of least overhead among all four protocols in all scenarios. The overhead of OLSR does not increase much even when the network load increases. This outcome makes this protocol much efficient than others in terms of overhead and bandwidth utilisation.

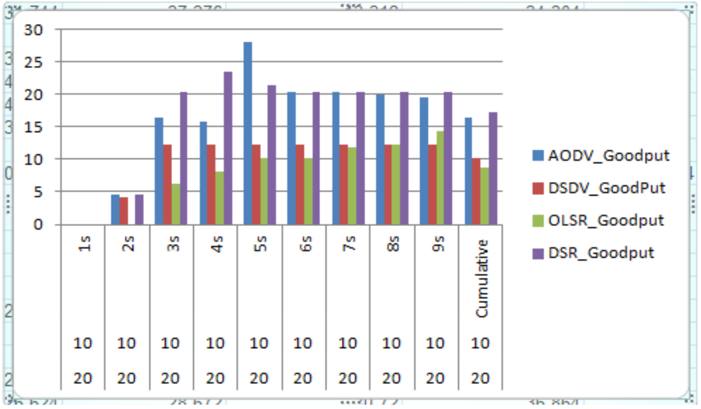

Figure-1
Sinkhole Goodput when node = 20

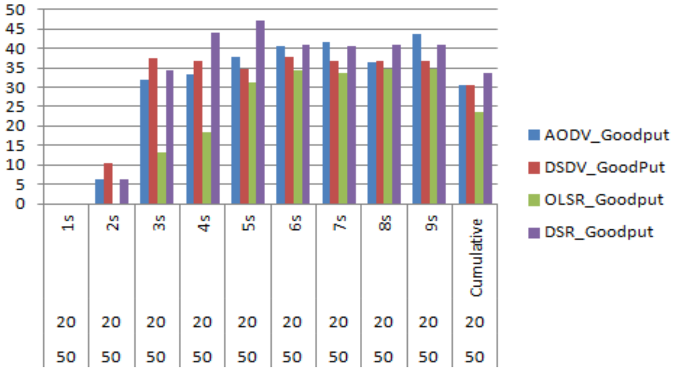

Figure-2
Sinkhole Goodput when node = 50

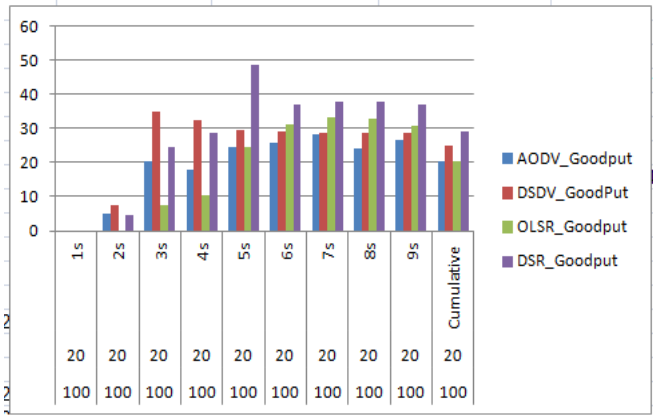

Figure-3
Sinkhole Goodput when node = 100

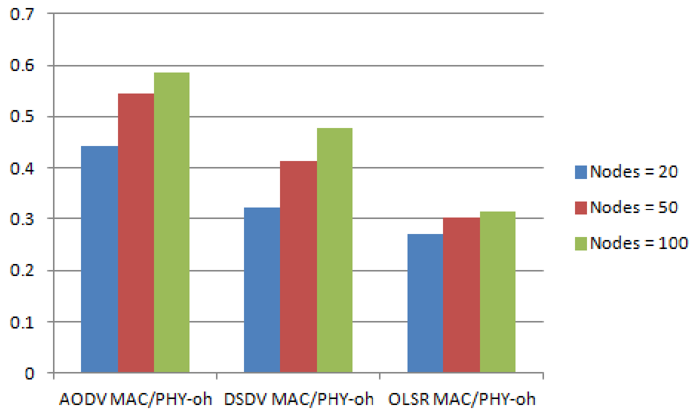

Figure-4
MAC/PHY Overhead

Conclusion

In this report, we have given the brief introduction of routing protocols and Network simulators which can be used for VANETs. We have also discussed simulation setup and their result on routing protocols. According to our results, AODV is the best among topology based protocols in terms of average Goodput but consists of high percentage of MAC/PHY overhead. DSR is also good for Goodput, but the MAC/PHY is incomparably large. Regarding other two protocols, both show average performance in all scenarios. AODV is showing much good performance at the cost of little overhead. So, if we want to increase the overall throughput, AODV is good option. For implementing security, we can use secure version of AODV i.e. SAODV. Since, DSDV is also giving steady performance, for proactive networks, we can also use SEAD, which is designed to secure the vehicular network using one way hash function instead of expensive cryptographic operations used in SAODV. In future, we will simulate the two secure protocols SEAD and SAODV to check how these protocols work under different load conditions. The simulation of ARAN and ARIADNE can also be included in further research.

References

1. Sumra I.A., Hasbullah H. and Manan J.l.A. (2011). Vanet security research and development ecosystem. National Postgraduate Conference (NPC) 2011, IEEE, 1-4.

2. Lin X., Sun X., Ho P.H. and Shen X. (2007). Gsis: a secure and privacy-preserving protocol for vehicular communications. IEEE Transactions on Vehicular Technology, 56(6), 3442-3456.

3. Ku I., Lu Y., Gerla M., Ongaro F., Gomes R.L. and Cerqueira E. (2014). Towards software defined vanet: Architecture and services. MED-HOC-NET, 2014 13th Annual Mediterranean, IEEE, 103-110.

4. Samara G., Al-Salihy W.A. and Sures R. (2010). Security issues and challenges of vehicular adhoc networks (VANET). NISS, 4th International Conference on, IEEE, 393-398.

5. Rukaiya D.D. and Shaikh Y. (2014). Survey on Vspn: Vanet-based secure and privacy-preserving navigation. *International Journal Of Engineering Research and Applications*, 4(10), 1-5.

6. Ram Shringar Raw, Manish Kumar and Nanhay Singh (2013). Security Challenges, Issues And Their Solutions For Vanet. *International Journal of Network Security & Its Applications (IJNSA)*, 5(5).

7. Mokhtar, Bassem and Mohamed Azab (2015). Survey on Security Issues in Vehicular Ad Hoc Networks. *Alexandria Engineering Journal*, 54(4), 1115-1126.

8. Abdalla G.M., Abu-Rghe M.A. and Senouci S.M. (2007). Current trends in vehicular ad hoc networks. Proceedings of UBIROADS workshop.

9. Dunn Brian P. (2010). Overhead in communication systems as the cost of constraints. Diss. University of Notre Dame, Indiana.

10. Harri J., Filali F. and Bonnet C. (2009). Mobility models for vehicular ad hoc networks: a survey and taxonomy. *IEEE Communications Surveys & Tutorials*, IEEE, 11(4), 19-41.