International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 3; Issue 2; March 2018; Page No. 1093-1097

Vehicular AD HOC networks

Munisha Devi
Research Scholar, Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India

Abstract
A new kind of ad hoc network is hitting the streets: Vehicular Ad Hoc Networks (VANets). In these networks, vehicles communicate with each other and possibly with a roadside infrastructure to provide a long list of applications varying from transit safety to driver assistance and Internet access. In these networks, knowledge of the real-time position of nodes is an assumption made by most protocols, algorithms, and applications. VANets advance into critical areas and become more dependent on localization systems, GPS is starting to show some undesired problems such as not always being available or not being robust enough for some applications.
For this reason, a number of other localization techniques such as Dead Reckoning, Cellular Localization, and Image/Video Localization has been used in VAN ets to overcome GPS limitations. VANETs are currently deployed on a large scale, research in this area is mostly simulation based. Mobility models or the movement patterns of nodes communicating wirelessly, play a vital role in determining the protocol performance in VANET. To evaluate and support scalability and efficiency of protocols for VANET, simulations with realistic mobility models are needed. A significant characteristic while studying VANETs is the requirement of having a mobility model that gives aspects of real vehicular traffic.In our paper we reviewed demonstration and description of mobility model.

Keywords: network, vehicular Ad Hoc network

Introduction
Research in vehicular communications, specifically Vehicular Ad Hoc Networks (VANETs), is playing a vital role in the future safety and ease of our roads. VANETs will enhance driver safety and reduce traffic deaths and injuries by implementing collision avoidance and warning systems. In addition, VANETs can relieve traffic congestion by providing a driver with live routes that avoid road hazards and bottleneck areas. The vast sensor network that VANETs will create, is inciting countless other applications, and making VANETs a hot topic in adhoc networking today [1].VANETs are one of the most promising application areas of MANETs. VANET communication is normally accomplished through special electronicdevices placed inside each vehicle so that an ad hoc network of the vehicles is formed on the road. A vehicle equipped with a VANET device should be able to receive and relay messages to other VANET device equipped vehicles in its neighborhood. VANET applications can be broadly classified into two categories: safety applications and comfort applications [2]. An example of a safety application is on-board active safety systems to assist drivers with information (like accidents, road surface conditions, intersections, highway entries and etc) about the road ahead. Comfort applications are those applications that can provide noncritical services like weather information, gas station or restaurant locations, mobile e-commerce, Internet access, music downloads andetc.

Fig 1, 2 and 3 depict the possible communication configurations in intelligent transportation systems.

a) Inter-vehiclecommunication

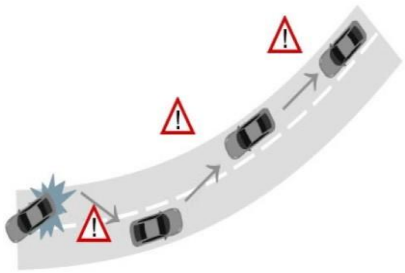

Fig 1: Inter-vehicle communication

There are two types of message forwarding in inter-vehicle communications: *naïve broadcasting* and *intelligent broadcasting*. In *naïve broadcasting*, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. The limitations of the naïve broadcasting method is that large numbers of broadcast messages are generated, therefore, increasing the risk of message collision resulting in lower message delivery rates and increased delivery times.

b) Vehicle-to-Roadside communication

The vehicle-to-roadside communication configuration (Fig. 2) represents a single hop broadcast where the roadsideunit sends a broadcast message to all equipped vehicles in the vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions.

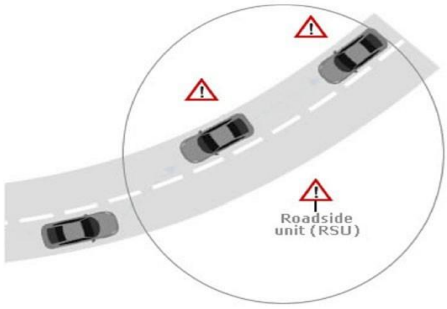

Fig 2: Vehicle-to-roadside communication

c) Routing-based communication

The routing-based communication configuration (Fig. 3) is a multi-hop unicast where a message is propagated in a multi-Routing-based communication hop fashion until the vehicle carrying the desired data is reached. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.

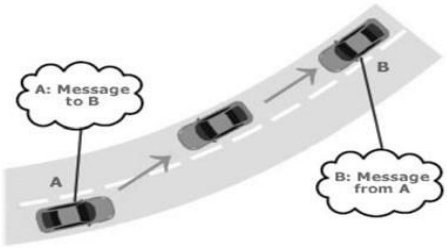

Fig 3: Routing-based communication

VANETs resemble MANETs with respect to the dynamically and rapidly changing network topologies due to fast moving vehicles. However, the mobility of the vehicles is normally constrained by predefined roads and speed limitations. Mobility of the vehicles is also affected due to traffic congestion in the roads and the traffic control mechanisms (like stop signs and traffic lights). Route stability is an important design criterion to be considered in the design of MANET and VANET routing protocols. The routing protocols should be able to dynamically adapt to the rapidly changing network topologies while taking into consideration the layout of theroads.

Mobility models used in VANET research are primarily derived from the broader scope of Mobile Ad-hoc Network (MANET) mobility. The most commonly used elementary models are *(i)* the Random Walk (RW), a movement pattern where direction and speed are set according to the output of a continuous, memory less random process, and *(ii)* the Random Waypoint (RWP), where direction and speed are still random, but they are maintained between two – random or zero – pause times. Movements usually occur on a region represented by a convex domain, without any obstacles to nodemobility.

A family of mobility models that, though originally designed for MANETs, arguably represents a step towards actual VANET behaviors are the so-called Group Mobility models, where nodes, though oblivious of each other, still show some coordination in theirmovements.

In fact Proper design with proper model is required for getting better results. Various approaches can be adopted in modeling the movement ofvehicles

1. Mobility models can be commonly classified into thefollowing Categories

A. Macroscopicmodels: Vehicular traffic is regarded as a continuous flow, and gross quantities of interest, such as the density or the mean velocity of cars, are modeled, often using formulations borrowed from fluid dynamics theory.

B. Mesoscopicmodels: Individual mobile entities are modeled at an aggregate level, exploiting gas kinetic and queuing theory results or macroscopic-scale metrics, such as velocity/density relationships, to determine the motion of vehicles.

C. Microscopicmodels: Microscopic models are able to reproduce fine-grained real world situations, such as front -to-rear car interaction, lane changing, flows merging at ramps, and intersections. Although macroscopic and mesoscopic descriptions are employed to capture the dynamics of large -scale vehicular systems.

D. Stochasticmodels: Vehicle movement is regarded at a microscopic level which is constrained on a graph representing the road topology, mobile entities follow casual paths over the graph, traveling at randomly chosen speed. Stochastic models are the most trivial way to mimic car mobility, and were introduced by pioneering works in the field of vehicularnetworking.

E. Traffic streammodels: Vehicular mobility is observed from a high level and treated as a continuous phenomenon. Traffic stream models determine cars' speeds, leveraging fundamental hydrodynamic physics relationships between the velocity, density, and outflow of a fluid, and thus fall into the macroscopic or mesoscopic categories definedbefore.

F. Car-followingmodels: The behavior of each driver is computed on the basis of the state (position, speed, and acceleration) of the surrounding vehicles.

G. Flows-interactionmodels: Built upon an instance of one of the previous categories, flows interaction characterizes the mutual dynamics that merging vehicular flows induce reciprocally, e.g., at highway ramps or urban intersections.

2. Lanechange

Lane Change is the class that implements the lane changing

model for a Vehicle. Each lane change in this model must satisfy both the safety criterion and the incentive criterion. The safety criterion states that the lane change must not cause the vehicle that is being change in front of to decelerate unsafely. The incentive criteria satisfied if lane changing vehicle advantages is greater than other vehicle disadvantages. Changed in front of (the back vehicle) todecelerate unsafely (faster than a certain threshold).the incentive criteria is usually much easier to satisfy than the safely criteria, both must hold for lane change to occur.

3. Existing Vanet Mobilitymodels

Basically, these models simulate movements in routes. For instance, some models use route intersections, and others just assume continuous movement at these points. Some assume routes to be single lane, some others support multi-lanes routes.

A. **Freeway Mobility Model(FMM):** Freeway is a generated-map -based model, defined. The simulation area, represented by a generated map, includes many freeways, each side of which is composed of many lanes. No urban routes, thus no intersections are considered in this model. At the beginning of the simulation, the nodes are randomly placed in the lanes, and move using history-based speeds. A between two vehicles is less than this required minimal distance, the second one decelerates and let the forward vehicle moves away. The change of lanes is not allowed in this model. The vehicle moves in the lane it is placed in until reaching the simulation area limit, then it is placed again randomly in another position and repeats the process. This scenario is definitely unrealistic

B. **Manhattan MobilityModel(MMM):** This is also a generated-map-based model, introduced to simulate an environment. Initially, the nodes are assumed to be randomly placed in the street intersections. The movement of a node is decided one street at a time. To start with, each node has equal chance (i.e., probability) of choosing any of the streets leading from its initial location. After a node begins to move in the chosen direction and reaches the next street intersection, the subsequent street in which the node will move is chosen probabilistically. If a node can continue to move in the same direction or can also change directions, then the node has 50% chance of continuing in the same direction, 25% chance of turning to the east/north and 25% chance of turning to the west/south, depending on the direction of the previous movement. If a node has only two options (this occurs when the node is in one of the four bounding streets of the network), then the node has an equal (50%) chance of exploring either of the two options. If a node has only one option to move (this occurs when the node reaches any of the four corners of the network), then the node has no other choice except to explore that option.

4. Vchicular ad Hocnetworking

5. Security

The security of VANETs is crucial as their very existence relates to critical life threatening situations. It is imperative that vital information cannot be inserted or modified by a malicious person. The system must be able to determine the liability of drivers while still maintaining their privacy. These problems are difficult to solve because of the network

size, the speed of the vehicles, their relative geographic position,and the randomness of the connectivity between them. An advantage of vehicular networks over the more commonad hoc networks is that they provide ample computational and power resources. For instance, a typical vehicle in such a network could host several tens or even hundreds of microprocessors.

5.1 Threats to availability, authenticity,and Confidentiality

Attacks can be broadly categorized into three main groups: those that pose a threat to availability, those that pose a threat to authenticity and those that pose a threat to driver confidentiality. The following sections present threats posed to each of the areas of availability, authenticity, andconfidentiality.

i) threats to availability the following threatsto

The availability of vehicle-to-vehicle and vehicle-to-roadside communication (including routing functionality) have been identified:

- **Denial of Service Attack**: DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network's nodes, onboard units and roadside units cannot sufficiently process the surplusdata.
- **Broadcast Tampering**: An inside attacker may inject false safety messages into the network to cause damage,

such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosenroute

- **Malware**: The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network whenthe onboard units and roadside units receive software andfirmware updates.
- **Spamming**: The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralisedadministration.
- **Black Hole Attack**: A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagatemessages.

ii) Threats to authenticity

Providing authenticity in aalter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network. These include:

- **Masquerading**: Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join thenetwork is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.
- **Replay Attack**: In a replay attack the attacker re-injects previously received packets back into the network, poisoning a node's location table by replayingbeacons..
- **Tunneling**: An attacker exploits the momentary loss of positioning information when a vehicle enters a tunnel and before it receives the authentic positioning information the attacker injects false data into the onboard unit.
- **Position Faking**: Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.
- **Message Tampering**: A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to- vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forgeresponses.
- **Message Suppression/Fabrication/Alteration**: In thiscase an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from applicationbeacons.

iii) Threats to confidentiality

Confidentiality of messages exchanged between the nodes of a vehicular network are particularly vulnerable with techniques such as the illegitimate collection of messages through eavesdropping and the gathering of location information available through the transmission of broadcast messages. In the case of eavesdropping, insider and/or outsider attackers can collect information about road users without their knowledge and use the information at a time when the user is unaware of the collection. Location privacy and anonymity are important issues for vehicle users. Location privacy involves protecting users by obscuring the user's exact location in space and time. By concealing a user's request so that it is indistinguishable from other users' requests, a degree of anonymity can be achieved.

5.2 Authentication with Digitalsignatures

Authentication with digital signature is a good choice for VANETs because safety messages are normally standalone. Moreover, because of the large number of network members and variable connectivity to authentication servers, a Public Key Infrastructure (PKI) is an excellent method by which to implement authentication where each vehicle would be provided with a public/private key pair. Before sending a safety message, it signs it with its private key and includes the Certification Authority (CA) certificate. By using private keys, a tamper-proof device is needed in each vehicle where secret information will be stored and the outgoing messages will be signed. The large computational burdenof verifying a digital signature for every received packet has led to an exploration for alternatives. A Timed Efficient Stream Loss-tolerant Authentication (TESLA) where the sender signs messages using a symmetric signature algorithm and then broadcasts this message with the signature (but most importantly, not the key). A short time later, he sender broadcasts the key and instructs all that this disclosed key is not to be used in the future. Receivers cache the original message until the key is received and then verify the signature

Related Work

Kun-chan Lan [9] introduced a tool MOVE that allows users to rapidly generate realistic mobility models for VANET simulations. MOVE is built on top of an open source micro-traffic simulator SUMO. They evaluated the effects of details of mobility models in three case studies of VANET simulations (specifically, the existence of traffic lights, driver route choice and car overtaking behavior) and show that selecting sufficient level of details in the simulation is critical for VANET protocol design. Yoann Pigne [10] introduced a novel vehicular macro- mobility model, using both survey-based and traffic-based models features. Relying on SUMO for microscopic traffic simulation, it provides a tool that generates vehicular mobility traces based on real traffic counting data. A parametrized destination model based on real data from OpenStreetMap allows to tune the model. A set of traffic counting data is used to compare the generated traffic and offers a framework for optimizing the parameters of the model. G.Hosein Mohimani [f11] proposed a new analytical mobility model for VANETs based on product form queueing

networks. In this model, author map the topology of the streets and the behavior of vehicles at both intersections and different parts of the streets onto different parameters of a BCMP1 open queueing network comprising M/G/∞ nodes. This model represented a sparse situation for VANETs, effect of dense situation on the mobility model, modify the queueing network as a new one comprising nodes with state-dependent service rates, able to find the spatial traffic distribution for vehicles at both sparse and dense situations. Nayana. P. Vaity [12] mobility modeling approach is discussed to the extent that it can help to understand models formulation and integration strategies with network simulators. This approach is called as flow mobility modeling. It is put into the discussionandelaboratedinsuchwayitclarifiesbasics of flow modeling and its impact. It also finds a different ways of modeling and implementation into existing traffic simulators viz. SUMO, VISSIM etc. Harald Meyer [13] describe how feedback loops can be introduced in arbitrary mobility models and in particular in elementary mobility models. They exemplify the approach by introducing two types of feedback loops for the Manhattan Mobility model, the Random Trip model, and th Constrained Random Trip model. One feedback loop represents points of interest attracting vehicles, such as free parking spaces attracting vehicles searching for parking. The other feedback loop focuses on repelling vehicles, such as a traffic jam etc. Kapil Bhagchandani [14] describe the mobility models like: random way point mobility model and group mobility model is used for cluster based routing approach for VANET, compare their performances with existing routing protocols and increasing the overall network throughput and minimize end to end delay. K. Prasanth [15] proposed Revival Mobility Model (RMM) and evaluate its effect on packet delivery in VANETs. They study and analyze various mobility models and their effect on VANET protocols.

Conclusion

This paper presents performance metrics and various vehicular mobility models that are categories that are deterministic and effective in VANET. And also presents an overview of the performance metrics of models used to determine the effectiveness in VANET.

References

1. Christine Shea, Behnam Hassanabadi, Shahrokh Valaee.3 Mobility-based Clustering in VANETs using Affinity Propagation, 2010.
2. Taleb T, Ochi M, Jamalipour A, Nei K, Nemoto Y. An Efficient Vehicle-Heading Based Routing Protocol for VANET Networks, Proceedings of the IEEE International Wireless Communications and Networking Conference, 2006, 2199-2204.
3. Hong X, Gerla M, Pei G, Chiang C. A Group Mobility Model for Ad Hoc Wireless Networks in ACM Int. Workshop on Modeling and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
4. Luo J, Hubaux JP.3 A survey of inter-vehicle communication, School of computer and Communication Sciences, EPEL, Tech. Rep. IC/2004/24, 2004.
5. Mahajan A, Potnis N, Gopalan K, Wang AIA. Urban mobility models for vanets in Proceedings of the 2nd IEEE International Workshop on Next Generation Wireless Networks, 2006.
6. Bai F, Sadagopan N, Helmy A. The IMPORTANT Framework for Analyzing the Impact of Mobility on Performance of Routing for Ad Hoc Networks, Ad Hoc Networks Journal - Elsevier Science. 2003; 1(4):383-403.
7. Bai F, Sadagopan N, Helmy A. The IMPORTANT Framework for Analyzing the Impact of Mobility on Performance of Routing for Ad Hoc Networks, Ad Hoc Networks Journal - Elsevier Science. 2003; 1(4):383-403.
8. Davies V, Evaluating mobility models within an ad hocnetwork Colorado School of Mines, Colorado, USA, Tech. Rep. Master's thesis, 2000.
9. Kun-chan Lanand, Chien-Ming Chou. Realistic Mobility Models for Vehicular Ad hoc Network (VANET) Simulations, IEEEXplore, 2010.
10. Yoann Pigne, Gregoire Danoy, Pascal Bouvry. A Vehicular Mobility Model based on Real Traffic Counting Data.
11. Hosein Mohimani G, Farid Ashtiani. Mobility Modeling, Spatial Traffic Distribution, And Probability Of Connectivity For Sparse And Densevehicular Ad Hoc Networks, IEEE Transactions On Vehicular Technology, 2009, 58(4).
12. Nayana P, Vaity, Dnyaneshwar V Thombre. A Survey On Vehicular Mobility Modeling: Flow Modeling International Journal Of Communication Network Security. 2012; 1(4):2231-1882.
13. Harald Meyer, Claudio E Casetti. VANET Mobility Modeling Challenged by FeedbackLoops, IEEE, 2011.
14. Kapil Bhagchandani, Yatendra Mohan Sharma, Exploration of VANET Mobility Models with New Cluster Based Routing Protocol, International Journal of Soft Computing and Engineering (IJSCE), 2013, 6(2). ISSN: 2231-2307.
15. Prasanth K, Dr. K Duraiswamy, Jayasudha K, Dr. C Chandrasekar. Packet Transmission Analysis in Vehicular Ad Hoc Networks using Revival Mobility Model, Int. J Advanced Networking and Applications. 2010; (01):252-257.