Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.603 – 609

A SURVEY ON VANET ARCHITECTURE, CHALLENGES AND MOBILITY MODELS

Manju
Student, M.Tech. (CSE), Royal Institute of Technology and Management
Mkundu108@gmail.com

Dhirendra Mohan
Asstt. Professor, CSE Dept., Royal Institute of Technology and Management
erdhiru1986@gmail.com

Abstract— VANET is public network with high speed vehicle network. The network is applied in larger geographical area with various architectural constraints. In this paper, a study work is provided to explore various associated aspects. The paper has discussed the network architecture along with associated architecture level, communication level and security challenges. The open issues for future scope are also discussed in this paper. The paper also explored different mobility model to control the network architecture and communication.
Keyword: Security Challenges, Mobility Model, VANET Architecture

I. INTRODUCTION

Vehicular communication is a term that defines communication between the vehicles. Its main purpose of deploying VANET is to reduce the level of accidents. It has a great effect on passenger's safety and for drivers to drive smoothly in the urban area. As vehicles increase day by day the rate of accidents also increases, therefore it is necessary for the vehicles to communicate. For example, suppose a vehicle A is moving in front of vehicle B and suddenly A meets with an accident by a thunderstorm and it applies its brakes, it does not want B to face the problem, then automatically, the brake sensors and rain sensors of A obtain activated and pass the signal to the main unit and then it broadcasts a message (Alert Message) to other vehicles. After obtaining the alert message, B slows down. By this example, we simply know the use of inter-vehicular communication and why it is needed.
According to the World Health Organization (WHO) the Road-Traffic Injuries statistics of all countries show that after 2000, road accident is a major cause of death [1][2][3]. Hence, there must be a better traffic system to solve this problem. VANET is such an advanced network which mainly provides Intelligent Transportation System (ITS) services to the end users for providing fast data exchanges and safety. It uses different standards like DSRC and WAVE for fast data communication.

A) VANET Architecture

VANET architecture mainly consists of vehicles (V), Road Side Unit (RSU) and Infrastructure Domain (I). Communication is conducted mainly by using wireless standards (e.g. IEEE 802.11p). RSU acts like a router and has high range (coverage) than vehicles range. Vehicles are installed with an On Board Unit (OBU) for communication. It is also installed with a Global

Positioning System (GPS) for knowing its own position as well as for tracking other vehicles. Electronic license plate (ELP) is also set in the vehicle for identification. Radio detection and ranging (RADAR)/light amplification by simulated amplification of radiation (LASER) technologies are also used for knowing the position of other vehicles. It is also supplied with high battery power. A Certification Authority (CA) exists in the architecture for providing services (e.g. security and TCP/IP) and applications. Fig. 1 shows the architecture of VANET.

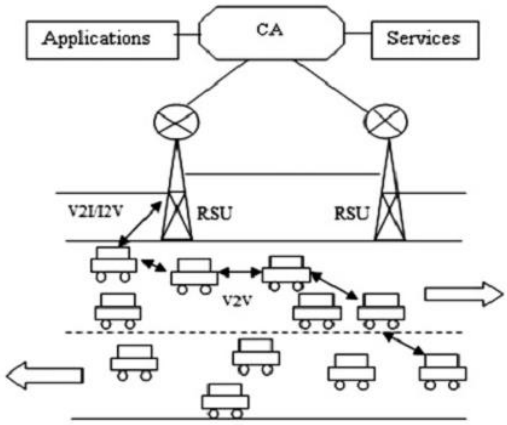

Figure 1: Network Architecture [1]

II. LITERATURE SURVEY

VANET is one the most critical and promising research area for which different researchers provided the research solution. In this section, some of the contribution of earlier researchers is discussed. S. Ahmed and S. S. Kanhere in [1] proposed a co-operative content distribution scheme based on novel network coding called VANETCODE for Content distribution is challenging in Vehicular Ad-Hoc Networks (VANET) is due to the high mobility, rapidly topology changing and iterant connectivity observed in these types of networks. Using VANETCODE, leverages of the wireless medium of the broadcasting nature to accelerate the distribution of encoded blocks over neighbouring one-hop neighbours and is completely self-reliant of routing. X. Lin et. al proposed a riskless data downloading protocol with preserving privy in VANET [2], which endow vehicles to download data from RSUs securely with their privacy protection under single or even under multiple RSUs are compromised .This protocol give the assures for vehicles to swanky access their requested data while eavesdroppers cannot obtain any privy information of the vehicles. K. Sampigethava et. al describes techniques used for privy-preserving and secure protocol based on identity (ID)-based and group signature [3]. This protocol gives the guarantee the requirements of privy and security of the each vehicle. But it can also give the each vehicle desired traceability in the event that the ID of the sender message must be revealed by the authority for any disputes of an event.

Y. Hao et. al give details of how the problem involved in controlling of unauthorized vehicle tracking based on their broadcast communications media, in order to improve user location privy in VANET [4]. AMOEBA provides location privy by utilizing the location group navigation of vehicles. By using vehicle groups for anonymous access to applications location-based services in VANET, for privy protection of user. The robustness of privacy of the user provided is considered under various attacks. J. Byers et. al describes fully scalable and ideal protocol for the applications such as reliable distribution of bulk data for that we call a digital fountain [5]. In this many number of heterogeneous receivers at times of their choice to procure content with maximum efficiency. Here, no feedback channels are required in order to ensure the reliable delivery, even when the face of high loss rates.

Maumita Bandyopadhyay[6] provided a work on Zone adaptive ACO approach for mobile communication optimization. Author used the clustering to generate effective network path and applied the direction based neighbour analysis. Mobility and zone information is used to generate the optimized path. V.Lakshmi Praba performed a work on Isolating Malicious Vehicles and Avoiding Collision between Vehicles in VANET. In this paper, traffic control is achieved by sustaining the distance between the vehicles and the malicious vehicles are secluded and further communication is blocked with the malicious vehicles [7]. Ayonija Pathre performed a work on A Novel Defence Scheme against DDOS Attack in ANET. In this paper Author proposed the novel traffic congestion detection and removal scheme against DDOS attack. Here the attacker behaviour is broadcast the huge numbers of false information packets in network i.e. the false information about the traffic. Proposed security scheme recovers control information and improves the performance of VANET in the presence of an attacker [8]. Rukaiya Y. Shaikh performed a work on Survey on VSPN: VANET-Based Secure and Privacy-Preserving Navigation. Author has described various existing solutions/protocols that are used in order to satisfy the security and privacy requirement of the vehicular ad hoc network. Author has also described security issues and challenges in VANET. Author has presented various security attributes that may be

considered as criteria to measure security such as availability, confidentiality, integrity, authentication and non-repudiation [9]. Subir Biswas performed a work," DDoS Attack on WAVE-enabled VANET Through Synchronization". In this paper, Author analyzes the prospect of a synchronization based DDoS attacks on vehicular communications and propose mitigation techniques to avoid such an attack[10].

TamilSelvan performed a work on A Holistic Protocol for Secure Data Transmission in VANET, VANET is the emerging area of MANETs in which vehicles act as the mobile nodes within the network. VANETs are deployed in untrusted and unsecured environment. In this paper Author propose a new light weight holistic protocol to secure VANET against insider and outsider attacks [11].

Khushboo Mittal performed a work on A Detail Survey of Various Security Issues in Vehicular Adhoc Network. Safety application provides safety to the passengers such as lane change warning, collision detection etc. It also provides comfort and commercial applications to the road users such as electronic toll collection, audio/video exchanging, electronic payments, route guidance, weather information, mobile E-commerce, internet access etc. It provides great comfort to passengers. But some vehicles with an evil intention (or malicious node) attack other vehicles [12]. Swapnil G. Deshpande performed a work on the Classification of Security attack in Vehicular Adhoc network: A survey. Author discusses some of the main security threats and attacks that can be exploited in VANETs and present the corresponding security solutions that can be implemented to prevent those attacks. In this work, Author has done a survey of existing approaches to solve the problems associated with vehicular networks [13].

III. VANET SECURITY

Security in VANET [16 –18] is a challenging problem for researchers in the era of cyber threats. The message passing from one vehicle to another vehicle may be trapped or hacked by an intruder or imposter who creates vulnerability in the systems performance. In VANET, many types of attack occur on the system like Position Cheating [19, 20], GPS Information Hacking, ID Cheating, Message Modification, and Spoofing and so on. Malicious drivers can create problems in the traffic which leads to accident and traffic jam. Hence, the vehicles should use security mechanisms to resist these threats. In this section, we present the threats to the VANET system and the security mechanisms to check the attacks.

A) Threats to Security Goals

There are three types of security goals: first is Confidentiality, second is Integrity and third is Availability. However, these goals are strongly affected by malicious drivers. The attacks [3, 16 –18] performed by malicious drivers are discussed as follows:

Snooping: In this attack, an attacker accesses the information without any authorisation. When a vehicle in the network sends information to another vehicle then the attacker intercepts and accesses the contents of the information and uses it for its own work. Snooping is a passive attack in which the attacker only monitors or accesses the information without modifying the data.

Traffic analysis: In this attack, an attacker analyses the traffic (collection of information/ transactions). The attacker collects all the information by monitoring the vehicular network constantly. By collecting the information like email addresses, requests and responses of all the vehicles communicating, the attacker can attack by a guessing strategy. It is also a passive attack in which no data modification is performed by the attacker.

Data modification: In this attack, an attacker intercepts and modifies the data. When a vehicle in the network sends an important information say warning message (Thunderstorm Ahead) to another vehicle, then the attacker may modify the data, delete the data or delay the data. By doing this, the second vehicle suffers from thunderstorm problem and accident occurs. This is a very dangerous attack in which the attacker for its own benefit weakens the system. It is an active attack in which the data is modified.

Replay attack: In this attack, an attacker intercepts and saves a copy of the message and later uses it for replaying. In the VANET systems, when a vehicle sends a warning message to another vehicle, the attacker keeps a copy of the message and later uses it to create delay in the system by unnecessarily stopping a vehicle by warning. It is also an active attack.

Masquerading: In this attack, an attacker impersonates some other vehicle by providing false ID and advertises as a legal node. When two vehicles communicate in the system then the attacker acts as a man in the middle and spoofs as a second vehicle and gains information from the first vehicle. This is also an active attack where the data can be modified.

Repudiation: In this attack, an attacker denies that he/she sends a message. In the VANET systems, a sender vehicle or a receiver vehicle can create this attack by denying that it sends a message or it receives a message, respectively.

B) Challenges in VANET Security

The main challenges while implementing security systems in VANET are discussed as follows:

Authentication : There should be an authentication of all the messages transmitted from one vehicle to another. Each vehicle in the network is to be authenticated by the central authority.

High mobility: As the vehicle moves faster, there is a link disruption problem and handshaking is lost. By this, the vehicles are unable to interact and establish secure communication between them.

Location-based services: By beaconing, we know the location of other vehicles. However, by implementing GPS, sensors, LASER, RADAR and so on we know the correct position of the vehicles.

Real-time system: To develop a real-time system is a challenging task because in a high mobile area it is difficult to send a warning message in correct time before the deadline.

A key challenge of securing VANETs is to provide sender authentication in broadcast communication scenarios. This so-called broadcast authentication is challenging because vehicles might not have met before, and link-layer losses might affect different broadcast receivers with differing severity.

C) Open Issues

This section presents some future research directions for HetVNETs, especially those closely related to heterogeneity. Addressing these open issues is vital to alleviating the restrictions imposed by heterogeneity.
Inter-system handover issues: Since a HetVNET consists of various wireless networks, e.g., WCDMA, LTE and DSRC, vehicular users may frequently switch among different networks due to their fast movement. It is desired that a vehicle always keeps connected with the most suitable network. Handover is imperative to achieve continuous seamless transmission in HetVNETs. Traditional handover mechanisms for cellular networks are mostly centralized, which are not well suited for the hybrid-distributed vehicular architecture. Also, the handover decision usually depends on a single threshold, affected by a number of factors such as the network load, receiving signal strength, channel conditions, and so on. However, it lacks an appropriate model for mapping a number of these parameters to the threshold. Furthermore, the handover of vehicular users is more frequent than cellular users, resulting in an excessive signalling overhead. Therefore, the main challenge in designing an effective handover strategy in HetVNETs is to strike an elegant trade-off among QoS requirements, implementation complexity and signalling overhead.
Big Data issues: All participants in an ITS act as data generators, yielding huge volumes of data, e.g., beacon messages, warning messages, and so on. For instance, most commuters may like to socialize with other commuters or watch popular movies in the car or bus during the long and boring commuting time, which would generate huge volumes of data and requests. With millions of miles of roads, millions of vehicles as well as drivers collecting data over the years, the sheer number of data points is extraordinary. Thus, how to exploit this big data in HetVNETs has drawn much attention. However, the methods, models and algorithms for big data that are used today may not work well for HetVNETs. In general, big data are physically and logically decentralized, but virtually centralized [89]. In order to achieve an effective balance between information processing and data transmission, advanced data processing and mining techniques are required to find, collect, aggregate, process, and analyze information in HetVNETs. There is much more work to be done.

Cooperation issues: Due to vehicle mobility, wireless links for vehicular communications are unreliable and of limited capacity. Thus, minimizing end-to-end latency and maximizing throughput are key issues in HetVNETs. Spatial diversity has been shown to be effective in enhancing energy efficiency and improving spectral efficiency in vehicular networks. However, the multiple antennas technique is not employed in DSRC, and equipping vehicle nodes with multiple antennas may not always be practical. As an alternative solution, cooperative communications can reap the benefits of spatial diversity gains so as to increase link capacity. For example, due to the unstable features of the wireless channel, the data download volume of an individual vehicle per drive through is quite limited. In order to solve this problem, a cooperative Drive-through Internet scheme, dubbed Chain Cluster, is proposed to select appropriate vehicles to form a linear cluster on the highway. The cluster members then cooperatively download and share the same content of information, increasing the probability of successful content download. Current studies have shown that: i) cognitive radio technology provides more opportunities for cooperative communications; ii) the performance of link scheduling with an appropriately selected transmission mode is better than purely relying on one single transmission mode; and iii) cooperative Multiple Input Multiple Output (MIMO) techniques provide attractive benefits for vehicular networks. Schemes such as link adaptation, relay selection and radio resource management in cooperative communications are important for improving system performance. The optimization problem in cooperation is usually NP-hard and computationally intractable. The main issue is how to balance between performance and complexity.

Cross-layer design issues: HetVNETs are expected to support a wide variety of safety and non-safety related services such as web browsing, file transfers and video streaming. As opposed to the traditional wireless and wired environments, the highly dynamic vehicular environment causes some serious concerns. For example, the communications channel is more prone to unpredictability, and connectivity of counterparts is easy to break. Hence, stringent and diversified QoS requirements of ITS services are hard to be met by traditional layered designs. Correspondingly, there has been increased attention to exploiting significant interaction among various layers of the protocol stack for performance enhancement. The main challenge is how to design the upper layer functions based on the feedback from lower layers. At the same time, the implementation complexity of the system needs be taken into account.

Vehicular Cloud Networking (VCN) issues: As computing and communication technologies have been rapidly developed, the vehicles with powerful computing abilities are advocated to be regarded as service providers rather than being only service consumers. As a result, the concept of Vehicular Cloud Computing (VCC) has been proposed, that jointly makes use of computation, communication and storage resources in vehicle equipments, e.g., on-board computer/communication devices or mobile user equipments arrived by passengers. In general, services in the VCC system can be divided into four types according to the function of the resources, i.e., "Network-as-a-Service (NaaS)", "Storage-as-a-Services (StaaS)", "Sensing-as-a-Service (SaaS)", and "Computation-as-a-Service (CaaS)" . Differently from the traditional cloud computing system, the VCC system has its unique features. For example, one of them is the variability of the available computation resources in Vehicular Clouds (VCs). Due to the uncertainty of the vehicle behaviour, i.e., vehicles may randomly join or leave VCs, the resources in VCs are time varying. Another obvious feature is the heterogeneity of VCs resources. Vehicles are produced by different vendors and thus have inherently different computation resources. Therefore, there are lots of problems in vehicular cloud networking needed to be solved.

IV. MOBILITY MODELS

In order to validate new protocols and applications for adhoc networks, it is important to use a mobility model that will emulate a real life scenario. During the course of time, modelling mobility have grown to be a subject of its own where researchers study and propose new mobility models which is able to imitate real life mobility. Apart from using a synthetic mobility model, researchers have also collected and used mobility traces to validate new opportunistic routing protocols. However, collecting traces is a tedious task, since deploying devices on a large scale is very much limited and costly. Although mobile phones and PDAs have been commonly used in collecting connectivity traces and are a good choice in terms of memory and battery power, they are expensive to deploy on a larger scale. It has been observed most of the times that traces are limited to a university campus or a small conference area. Moreover, there is a large time overhead (6 months-1 year), since traces should be collected over a long time period so as to avoid any biased data from appearing in the data set. For the above limitations synthetic mobility models have gained importance among the researchers. Such models can be applied to an arbitrary number of nodes and over a large scale. Table 1 shows the pros and cons of synthetic mobility models and real-life mobility traces.

Table 1 Comparison: SYNTHETIC MOBILITY MODELS AND MOBILITY TRACES

Characteristics	Synthetic Mobility Models	Mobility Traces
Scalable	Yes	No
Similarity with real life movement pattern	Low	High
Time Overhead	Small	Large
Complexity	*High*	*Low*
Deployment cost	Low	High
Computation Method	Large	Low

Taxonomy of Mobility Models Several synthetic mobility models have been proposed till date and so as to provide a methodical study of these models, we provide a hierarchical classification of these mobility models. Synthetic models are those which are formed out of concrete mathematical models (and formulas) along with physical laws of motion. We divide the entire class of synthetic mobility models into four subclasses viz., the entity mobility models, the correlated or group based mobility models, the human or sociality based mobility models and, the vehicular mobility models. In

simple terms, entity mobility models are those in which the mobility of the nodes is independent of each other. Correlated or group based mobility models are those where movement of a node is dependent on mobility of other nodes. However, it is actually a combination of both of these types that we get to observe in real life. For example, an individual sometimes move as single entities like pedestrians and sometimes move in groups with correlated motion patterns. Vehicular movement can also be cited as an example of correlated mobility model (although we prefer to mention it as a separate class of mobility model) since the movement of a vehicle is highly governed by the motion of other vehicles; for example, the speed of a vehicle moving in queue (such a highway) generally cannot exceed the speed of vehicles ahead of it. Human or sociality based mobility models are those which are governed by human nature and their tendency to socialize. Mobility of an individual may be governed by other human when they socialize and tend to move in groups; for example, group of rescue workers or soldiers. And lastly, vehicular mobility models are those which are governed by nature of vehicular movement on road or highway observed in daily life. Vehicular movement is affected by several factors such as traffic signals, movement of vehicles ahead, lane speed limit, accidents, and so on. Apart from synthetic mobility models, we have the class of real life mobility observed in humans, vehicles, and animals. Some authors prefer to classify the real-life mobility into the following types; pedestrians, vehicles, aerial, dynamic medium, robot and outer space motion.

Entity Mobility Models

1) Random Mobility Models: In random mobility model nodes move freely and without restriction. All the mobility attributes like speed, direction, and waypoints (destination) are selected randomly and independent of previous selection. Hence, these mobility models are generally termed memory less, since speed (or direction) at time instant t is independent of speed (or direction) at previous time instant $t - \Delta t$.

2) Models with Temporal Dependency: When node movement has temporal dependency, it means that mobility is governed by physical laws of motion and its current movement is dependent on its movement history. For example, a node's current velocity may depend upon the previous velocity. Again, in most cases nodes move along a given path; for example vehicles move along roads and movements of pedestrians are may be blocked by buildings.

3) ***Models with Spatial Dependency:*** Movements of nodes are not always random or have temporal dependency. It has been observed on many occasions that the destination of a node may be dependent on its current location. Such node movements are said to have spatial dependency as the location of a node at next time instant is probabilistically related to its location at the present time instant.

4) Models with Geographic Restriction: Sometimes node movement may be restricted to a bounded area; for example movement in a conference area or in an academic institution and campus. Such mobility models are said to have geographic restriction. For example, movement of an individual may be guided by pathways and obstructed by buildings. It may also depend on the specific role of an individual.

Correlated/Group based Mobility Models

Group based mobility models are those in which nodes tend to move in groups and behave in a co-operative manner. The waypoint of a node is largely affected by the other members that belong to the group. They tend to form clusters and rarely deviate from a reference point within the group. The group based mobility model includes six models viz., a) Reference Point Group mobility model, b) Column mobility model, c) Pursue mobility model, d) Nomadic Community mobility model, e) Exponential Correlated Random mobility model, and f) Heterogeneous Random Walk.

Human or Sociality based Mobility Models

Human or sociality based mobility models finds its application in Pocket Switched Networks (PSN). Humans are social animals; hence their movement is largely governed by the type of community to which they belong. Moreover, people tend to remain confined to their own social group and rarely move outside it. Hence, numerous mobility models have been developed, especially with respect to human movement, inspired by the idea of social network. For example, people spend their day in office, evening in pub/bars and return home at night.

Vehicular Mobility Models

Vehicular Communication has become an integral part of intelligent transport system (ITS) and is the key factor in maintaining the road safety. Vehicular communication consists of two basic components viz., vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). V2V and V2I communication has been used in information dissemination, travel time prediction and congestion management. Categorized under VANET, a number of application and routing protocols has been developed for V2V

and V2I communication, whose evaluation strictly depends on modelling vehicular mobility. Vehicular mobility model emulate vehicle movement along road/highway, changes in speed, movement in queues and stops at traffic signals.

V. Conclusion

In this paper, an exploration to various VANET constraints is presented. The paper has identified the architecture level challenges, security challenges and the open up issues of this network. The paper also discussed different mobility models to improve the communication architecture.

References

[1] S.Ahmed and S.S Kanhere, "VANET CODE:Network Coding to enhance cooperative downloading in vehicular ad hoc networks," in Proc. IW CMC,2006.

[2] X.Lin , X.Sun , P-H.Ho,and X.Shen , "GSIS: A secure &Privy Preserving protocol for vehicular communuication," IEEE Trans,Veh.Technol.,Vol.56,no.6,pp.3442-3456,2007.

[3] K.Sampigethava, M.Li,L.Huang , and R.Poovendran, "AMOEBA:Robust location privy scheme for vanet ," IEEE J. Sel . Areas Commun. ,vol. 25 , no.8 , pp.1569-1589, 2007.

[4] Y. Hao , J . Tang , Y. Cheng , and C.Zhou , "Secure data downloading with privy preservation in vehicular adhoc networks,"In Proc. IEEEICC , May 2010.

[5] J . Byers , M . Luby , M . Mitzenmacher ,and A. Rege, " A digital fountain approach to reliable distribution of bulk data ," in Proc.ACM SIGCOMM , 1998, pp.56-678.

[6] Maumita Bandyopadhyay , "Zona Based Ant Colony Routing in Mobile Ad-hoc Network," 978-1-4244-5489-1/10 2010 IEEE.

[7] V . Lakshmi Praba , "Isolating Malicious Vehicles &Avoiding Collision between Vehicles in VANET" , International conferrence on communication & Signal Processing 2013,978-1-4673-4866-9/13 2013 IEEE.

[8] Ayonija Pathre, "A Novel Defense Scheme against DDoS Attack in VANET ," 978-1-4673-5999-3/13 2013 IEEE.

[9] Rukaiya Y.Shaikh, " Survey on VSPN : VANET- Based Secure & Privacy Preserving Navigation," Journal of Engineering Research and Application 2014.ISSN:2248-9622.

[10] Subir Biswas , "DDoS Attack on Wave-enabled VANET through Synchronization".

[11] Tamil Selvan , "A Holistic Protocol for Secure Data Transmission In VANET" , International Journal of Advanced Reasearch in Computer & communication Engineering December 2013,ISSN (Print):2319-5940 ISSN (online): 2278-1021.

[12] Khushboo Mittal , " A Detail Survey of various Security Issues In Vehicular Adhoc N/W" , International Journal of Emerging Technology & Advanced Engineering 2014, ISSN 2250-2459, ISO 9001:2008.

[13] Swapnil G . Deshpande, " Classification of Security attack in Vehicular Adhoc network : A survey" ,IJETICS 2013, ISSN 2278-6856.

