Middle-East Journal of Scientific Research 24 (12): 3798-3804, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.3798.3804

Vehicular Networks: Issues and Challenges

[1]M. Siva Sangari and [2]K. Baskaran

[1]Research Scholar, Anna University, Chennai, India
[2]Associate Professor, Department of EEE, GCT, CBE, India

Abstract: Vehicular Ad-Hoc Network or VANET is an emerging technology in the modern world.Here moving vehicles act as nodes in a network to create a dynamic network. Vehicular Ad-hoc Networks can be viewed as main component of the Intelligent Transportation Systems (ITS). Vehicular networks provide two types of communications: Vehicle –to-Vehicle, Vehicle-to-Roadside. Vehicular Ad-hoc Networks communicate based on Dedicated Short Range Communications (DSRC) which is a type of WiFi, Cellular, Satellite and WiMAX. The Communication is based on the Wireless Access for Vehicular Environment (WAVE) dedicated to vehicle-to-vehicle and vehicle-to-roadside communications. This paper also focuses the various issues and challenges associated with the real time implementation of the vehicular aspects.

Key words: Vehicular Networks · GPRS · DSRC · Mobility Management · Handover

INTRODUCTION

In recent years, the technical advancement of the car manufacturers such as Ford, GM and BMW had made them introduce their new vehicles equipped with GPS receivers and navigation systems to include significant computing power inside their cars. This technology allows the vehicle to communicate with other vehicles in addition to the road base station. Road base station are sited in vital section of the road like a traffic lights, intersections or stop signs, to create safety for drivers and improve the driver experience. The communication device is also known as On Board Units (OBU). Vehicle communicates with each other and also communicates with base station. VANET allow communicating with vehicle and base station. The base stations are connected to backbone network so that the other application and services can be provided to the vehicles.

The Federal Communication Commission (FCC) allocated a bandwidth of 75MHz around the5.9GHz band for vehicle to vehicles and vehicles to roadside infrastructure communications through the Dedicated Short Range Communications (DSRC) services. The emergence of vehicular networks enable several useful Intelligent Transport Service (ITS) applications, both safety and non-safety applications such as automatic road traffic alerts dissemination, dynamic route planning, service queries (e.g., parking availability), audio/video flesharing during mobility and context-aware advertisement.

Communications in Vehicular Networks: A Vehicular network can be formed based on the type of communication support provided by the network. Normally the vehicular network provides the user to utilize one of the three types of communication namely: using cellular network, roadside infrastructure or vehicle-to-vehicle communications.

i) Using Cellular Networks : This method connects moving vehicles to the Internet via cellular data networks using technologies like3G, EV-DO, GPRS, etc. This service is already made commercially available by the car manufacturers by making the vehicle to be transformed into an IEEE 802.11 (WIFI) hotspot and the Internet connection shared by gadgets in the car. The amount of data transfer by this communication is found to be 1GB or 5GB maximum per month. Though the possession of Internet connectivity in each vehicle is found to be the advantage of this type of communication, the dependence on the cellular operator is found to be the major drawback.

ii) Vehicle to Roadside Infrastructure Communications: This method of communication is based on the roadside infrastructure. Here, vehicles connect to other vehicles or to the Internet via roadside access points positioned

Corresponding Author: Dr. K. Baskaran, Associate Professor, Department of EEE, GCT, CBE, India.

along the roads. The access points can be either installed specifically for providing Internet access to vehicles or may be a open 802.11 (WiFi) access points along city streets. This method helps the vehicles to connect to the Internet using high data rates of 11Mbps than through the cellular network. Access points installation cost along the roads to obtain reasonable coverage is found to be the major drawbacks.

iii) Vehicle-to-Vehicle Communications: Using Internet-based communications to and from vehicles will be based on the method of choice used for communications. However, the Wi-Fi-ready vehicles open the way for ad hoc networks of moving vehicles. The advantage is the availability of distinct, high bandwidth network to the existing infrastructure network and the drawback is need for new set of protocols that are able to satisfy the throughput and delay requirements of applications.

Handover: The problem of seamless connectivity becomes even more challenging as vehicles move across overlapping heterogeneous wireless environment. In such cases, frequent switching from serving network to a target network may occur, which degrade the network performance. When Mobility Management (MM) is classified by layer concept, mobility can be divided into two parts:

- ***Horizontal mobility*:** Mobility on the same layer. Generally referred as the mobility within the same access technologies.
- ***Vertical mobility*:** Mobility between different layers. Generally referred as the mobility between different accesses technologies.

One of the major requirements for MM in the NGN networks is to support the mobility across the heterogeneous access networks. The next generation a network is composed with the characteristics of heterogeneous access networks which makes a big distinction between horizontal handover and vertical handover;

- ***Horizontal handover*:** Handover within same access networks which is generally referred to as the Intra-AN handover.
- ***Vertical handover*:** Handover across heterogeneous access networks which is generally referred to as the Inter-AN handover.

Horizontal Handover: The main concern of horizontal handover is to maintain the on-going services, although there may be a change of IP address due to the movement of a mobile node. Maintaining on-going service is done by thrashing the change of IP address (e.g., Mobile IP) or updating the changed IP address dynamically (e.g., mSCTP).

To hide the change of IP address during the movement of a mobile node, Mobile IP maintains two types of IP address; one permanent IP address (Home address) might be used above transport layer and one changeable IP address (Care-of address) might be used under transport layer. The majority of handover mechanism include in horizontal handover because they focus on maintaining the on-going services without any interruption even though the IP address is changed.

Vertical Handover: Vertical handover happens when a mobile node moves across heterogeneous access networks. It differs from the horizontal handover both in the access technology as well as the IP address usage, because the mobile nodes moves across different access network using different access technology. The main concern of vertical handover is to maintain on-going services by concerning the change of IP addresses, the change of network interfaces, QoS characteristics etc.

The main features of vertical handover as compared to horizontal handover are as follows

- Usage of different access technologies
- Usage of multiple network interfaces
- Usage of multiple IP addresses
- Usage of multiple (changeable) QoS parameters
- Usage of multiple network connections (multi-homing features)

a)Vertical Handover Mechanism: Wireless networks adopt a heterogeneous broadband technology model to guarantee seamless connectivity in mobile communications. A vertical handover (VHO) is a process preserving users' connectivity on-the-move and following changes of network. VHO schemes can be classified on the basis of the criteria and parameters adopted for initiating a handover from the serving network to the target network.

b)Vertical Handover Parameters: The decision for vertical handoff may depend on various parameters like Bandwidth, Received Signal Strength (RSS), Signal to

Inference Ratio (SIR), cost, latency, security, velocity, battery power, user preferences, service capacities and Quality of service (QoS). During handover, different parameters have to be monitored and decided.Different researchers have given different views and techniques to achieve vertical handoff.

c)Received Signal Strength (RSS): RSS is the most widely used criterion because it is easy to measure and is directly related to the service quality. Majority of existing horizontal handover algorithms use RSS as the main decision criterion, but it is not enough for a complete decision. RSS represents the strength of the signal received; the Vertical Handoff is feasible i.e. the handoff takes place if and only if RSS of the BS or Access Point (AP) is above the threshold.

d)Available Bandwidth: Bandwidth is a measure of the width of a range of frequencies. It refers to the data rate supported by a network connection or interface. It measures the amount of data transferred over a specific connection in a given amount of time. In order to provide seamless handoff, there is a need to manage bandwidth of mobile node during movement. Higher offered bandwidth ensures lower call dropping and call blocking probabilities, thus providing higher throughput.

e)Network Throughput: Network throughput refers to the average data rate of successful data or message delivery over a specific communication links. Network throughput is measured in bits per second (bps). Maximum network throughput equals the TCP window size divided by the round-trip time of communication data packets. As network throughput is considered in dynamic metrics for making decision of VHO, it is one the important requirement to be considered for the VHO.

f)Network Load: Network load is to be considered during effective handoff. It is important to balance the network load to avoid drop in quality of services. Variation in the traffic load among cells will reduce the traffic carrying capacity. To provide a high quality communication service for mobile nodes and to enhance the high traffic attention has to be paid to the network load when there is a variation in traffic.

g)User Preferences: The user preferences could be preferred networks, user application requirements (real time, non-real time), service types, QoS etc. User Preferences can also be considered for VHO in next generation wireless networks.

h)Cost: A multi criteria algorithm for handoff should also consider the network cost factor. The cost is to be minimized during VHO in wireless networks. The call arrival rates and handoff call arrival rates is analyzed using cost function. Next generation heterogeneous networks combine the advantage on coverage and data rates, which offer a high QoS to mobile users. In such scenario, multi-interface terminals should seamlessly switch from one network to another, to obtain improved performance or to maintain a continuous wireless connection.

I)Speed: It is the speed at which the Mobile Terminal (MT) is moving. In vertical handoff algorithms, the speed factor has a large and decisions binding effect than the traditional horizontal handoff decision algorithms. When a user travel at high speed within a network coverage area it is not advised to initiate the vertical handoff process because after a short period of time, the user will have to go back to the initial network because it will get out from under cover network host.

j)Power Consumption: The wireless devices running on battery need to limit the power consumption. If the battery level decreases, switching from a network to another network with low power consumption can provide a longer usage time. The power requirement becomes a critical issue especially if the hand held battery is low. In such situations, it is preferable to transfer to an attachment point to extend the battery life. The attachment to the closest AP or BS is known to consume the least power at a given instant. So if battery level is low, the MT must handoff to the closest AP or BS provided RSS is above the threshold level. The number of users also increases the congestion and in turn even the nearest AP or BS consumes more power.

4. Protocol in VANET: The protocols of VANET are being classified based on the type of communication provided by the network structure. Though there are two types of communications available in VANET namely V2V and V2I, the protocols differ for each type which is represented in the figure 1.3.

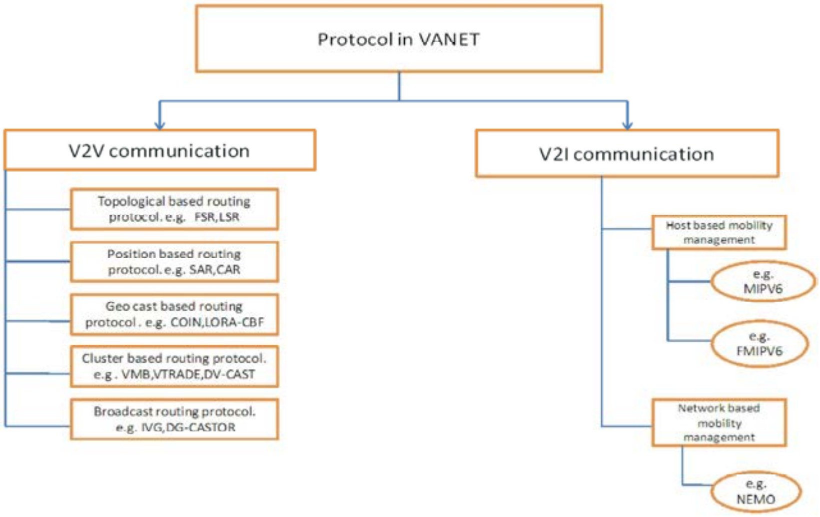
Protocol in VANET
V2V communication
V2I communication
Topological based routing protocol. e.g. FSR,LSR
Position based routing protocol. e.g. SAR,CAR
Geo cast based routing protocol . e.g. COIN,LORA-CBF
Cluster based routing protocol. e.g . VMB,VTRADE,DV-CAST
Broadcast routing protocol. e.g. IVG,DG-CASTOR
Host based mobility management
e.g. MIPV6
e.g. FMIPV6
Network based mobility management
e.g. NEMO

Fig. 1.1: VANET Protocols

4.1 Vehicle to Vehicle Communication Protocols: Cooperation among inter-vehicular networks and sensor networks placed within the vehicles or along the road need to be further analyzed. The different types of routing protocols are used for sending and receiving the message in this ad hoc network. They are classified into five categories: -

a) Topology based Routing Protocol
b) Position based Routing Protocol
c) Cluster based Routing Protocol
d) Broadcast Routing Protocol
e) Geo cast based Routing Protocol

4.2 Vehicle to Infrastructure Communication Protocols: Vehicles gather information and application with the help of road side infrastructure. Mobility Management scheme aim to reduce the control overhead and improve bandwidth utilization during Internet-to-VANET multicasting communication. There are different types of mobility management schemes used in this communication. The following classifications are

i) Host-based mobility management
ii) Network-based mobility management
iii) Host-based mobility management

In such Mobility Management Scheme, the Mobile host/Mobile Node (MH/MN) which move from one network to another involves signaling process which requires protocol stack modification and IP address change on the MN for to maintain the session continuity during handover. This signaling process includes movement detection, Router Solicitation request (RtSolReq), Duplicate Address Detection (DAD) and Binding Updates (Bus) etc. Host Based Mobility Schemes have been used for different applications including real time services and the associated protocols are Mobile Ipv6 and Fast Handovers for MIPv6 (FMIPv6).

1)Mobile Ipv6: Mobile Ipv6 is a global mobility management protocol. MIPv6 has been proposed to support the network layer mobility. In NEMO, the mobile router is defined to extend the MN of MIPv6 by adding ability routing between its PoA and subnet which moves with the MR. MIPv6 are designed to handle the terminal mobility and that is not suitable for handling the NEMO. This protocol allows MN to maintain the connectivity to the Internet while moving from one network to another network. Each MN is identified using its Home Address. When connecting through a foreign network, the MN receives RA message. To obtain the information, Router Solicitation (RS) and Router Advertisement (RS) messages are exchanged between MR and AR. Then, the MR creates NcoA and Duplicate Address Detection (DAD). If the CoA is usable, then the MN sends its location information to it's HA to perform Binding Update (BU), which intercepts packets for the MN and tunnels them to the MN's current location.

2)FMIPv6: MIPv6 is improved as Fast Mobile Ipv6 (FMIPV6) to support the Handover. One of the problems of NEMO BS in the context of ITS is that the packet loss and handover latency during the handover session which is inherited from MIPv6. This problem is more decisive in NEMO as MNNs in a network move at the same time. FMIPv6 reduces the packet loss by employing buffering and tunneling. But the tunneling approach may sustain packet loss during the handover. FMIPv6 is designed for a single MN, a tunnel between the PAR and NAR is established during the handover which is used for single MN.

Ii)network-Based Mobility Management: NEMO (Network Mobility) was introduced in 2005 for network mobility problems. As base station is not directly accessed by all users, as mobile host can only be accessed by using mobile routers (MR). Mobile routers have their own home address. When the MR moves to a foreign access router it requires Care of Address (CoA) from the visited network. When it receives its CoA it sends the updated message to it's HA (Home Address). HA of the MR forward this message to all data packets. The network mobility solutions like NEMO leads to reduced handoff, scalability, reduced complexity.

5. Vehicular Challenges: Vehicular challenges are broadly classified into broad categories namely Technical challenges, Security Challenges, Socio-Economic challenges.

5.1Technical Challenges: The characteristics of VANETs also provide a vital role in forwarding the packets. The forwarding challenges that were identified during the packet transmission are next hop selection, queuing disciplines and paths durations. DSR/GPSR protocols maintain lists of neighbors, to determine the nexthop. If the lists are not accurate, the best next hop could be missed or even worse, a vehicle node which is already out of the transmission range could be chosen. Maintaining updated lists requires frequent "hello" packet broadcasting between the nodes of the network. But too much of broadcasting also leads to overhead. Thus, to use accurate node positions in the selection of the next hop without incurring too much overhead acts as a main challenge in vehicular networks.

The occurrence of high mobility in a network changes the network topology and channel condition quickly thus, does not support tree structure. The traffic load is found to be low in rural areas and high in urban resulting in unbounded network size, these are the challenges related to communication. During the rush hour, the traffic load is high, which leads to frequent network partitions.

The security issues also make a big impact for the researcher to take it for consideration.

5.2 Security Challenges: Among all the challenges of the VANET, security has got less attention so far. VANET packets may contain life critical information hence it is necessary to make sure that these packets are not attacked by the intruder; likewise the liability of drivers is established by informing them the traffic environment correctly at specified time. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other security problems encountered in a general communication network. The following presents some security challenges to be considered.

a) ***Real time Constraint:*** In Vehicular Networks, the time factor is a critical one, as, the message should be delivered with the maximum of 100ms.So in order to achieve this constraint in real scenario, the fast cryptographic algorithm should be used and at the same time, the message and entity authentication also should be carried out in time.

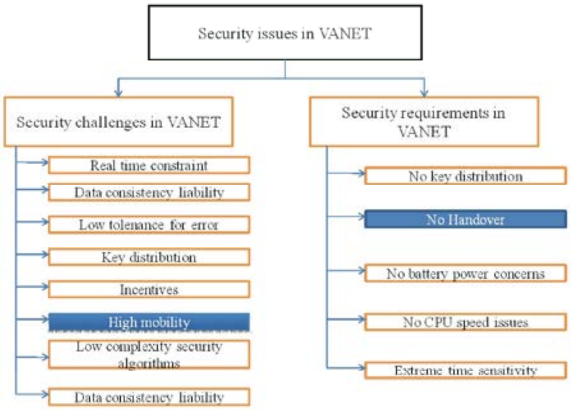

Fig. 1.2: Security issues in VANET

b) ***Data Consistency Liability:*** In VANET, even authenticate node can perform malicious activities in certain situations which may lead to accidents or may disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

c) ***Low Tolerance for Error:*** Some protocols are designed on the basis of probability. The message transfer has to be done in short duration and so a small error in probabilistic algorithm may cause malfunction in the network.

d) ***Key Distribution:*** All the security mechanisms implemented in VANET are dependent on keys generated. Each message is encrypted and needed to be decrypted at receiver end, either with the same key or different key. Also in a public key infrastructure trust on CA become a major issue.

e) ***High Mobility:*** The computational capability and energy supply in VANET is same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that the wired network produces. Hence the design of security protocols must use certain approaches that reduce the execution time.

f) **Low Complexity Security Algorithms:** Current security protocols such as SSL/TLS, DTLS, WTLS, generally uses RSA based public key cryptography. RSA algorithm uses the integer factorization on large prime number which is NP-Hard. So the decryption of the message that uses RSA algorithm becomes very complex and time consuming. Hence there is a need to implement alternate cryptographic algorithm like Elliptic Curve Cryptosystems and for bulk data encryption, AES can be used.

g) ***Transport Protocol Choice:*** To secure transaction over IP, DTLS should be preferred over TLS as DTLS operates over connectionless transport layer. The IPSec which secures IP traffic should be avoided as it requires too many messages to set up. However IPSec and TLS are used when vehicles are not in motion.

h) ***Incentives:*** Only 20% of the customers prefer their vehicles with automatic reporting facility. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET is considered as one of the Socio-Economic related challenge.

The following security requirements have to be satisfied before they are deployed.

- No confidentiality
- No key distribution
- No battery power concerns
- No CPU speed
- Extreme Time Sensitivity

5.3. Social and Economic Challenges: Apart from the technical challenges to deploy the VANET, there exist social and economical challenges. It is difficult to build a system that conveys the traffic signal violation which may increase the production cost which cannot be addressed by the manufacturer

REFERENCES

1. Ahmed Mosa, A., A. Hassan Abdalla Hashim, R.A. Saeed and O.O. Khalifa, 2011. Investigation of route optimization for mobile ad hoc NEMO (MANEMO) based proposals, Australian Journal of Basic and Applied Sciences, 5(6): 814-838.
2. Céspedes, S., X. Shen and C. Lazo, 2011. IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions, IEEE Communications Magazine, 49: 187-194.
3. Chen, Yuh-Shyan, Chih-Shun Hsu and Ching-Hsueh Cheng 2014, ‘Network mobility protocol for vehicular ad hoc networks’, International Journal of Communication Systems, vol. 27, no. 11.
4. Fatimah Abdulnabi Salman and Emad Hassan Al-Hemairy, 2013 ‘Minimizing Handoff Latency and Packet Loss in NEMO’, IJCSI International Journal of Computer Science Issues, vol. 10, issue. 4, no. 2.
5. McCarthy, B., M. Jakeman, C. Edwards and P. Thubert, 2008., ‘Protocols to efficiently support nested NEMO (NEMO+)’, Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture ACM, pp: 43-48.
6. Nagaraj, Uma and Deotale, MDG 2011, ‘Study of Communication using IPv6 in VANET’ International Journal of Computer Science and Communication Networks, vol. 1, no. 3.
7. Naumov, V. and T.R. Gross, 2007. ‘Connectivity-aware routing (CAR) in vehicular ad-hoc networks’. IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications, pp: 1919-1927.
8. Pollini, G.P., 1996. ‘Trends in handoff design’, IEEE Communication Magazine, 34(3): 82-90.

9. Taleb, T., E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato and Y. Nemoto, 2007. 'A Stable Routing Protocol to Support ITS Services in VANET Networks', IEEE Transactions on Vehicular Technology, 56: 3337-3347.
10. TamilSelvan, M.D., V. Vasudevan, P.R. Parasuraman and A.V. Aadhimoolam, 2014, 'Mobility Prediction and Node Prediction Based Light-Weight Reliable Broadcast Message Delivery for Vehicular Ad-Hoc Networks', International Journal of Advanced Research in Computer and Communication Engineering, 3: 5321-5325.
11. Vaishnavi, C., S. Sindhuja, B. Subathra, K. Selvi Priya, C. Bala Subramanian and M. Angelin Nithya Devi, 2014. Improving the Message Delay Overhead Using Nested Nemo Based Vanet, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, vol. 3.
12. Vegni, A.M., G. Tamea, T. Inzerilli and R. Cusani, 2009. A Combined Vertical Handover Decision Metric for QoS Enhancement in Next Generation Networks, Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp: 233-238.
13. Wasnik, M.A. and S.S. Dorle, 2013. Analysis of handover scheme for VANETS' International Journal of Science and Research, 2(2): 73-76.
14. Zao, J., J. Gahm, G. Troxel, M. Condell, P. Helinek, N. Yuan, I. Castineyra and S. Kent, 1999. A Public-Key Based Secure Mobile IP. Wireless Networks, 5: 373-390.