Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on QoS and Security in Vehicular Ad hoc Networks

Diyar Khairi M S
DEEI, University of Algarve, Portugal
University of Duhok UoD, Iraq

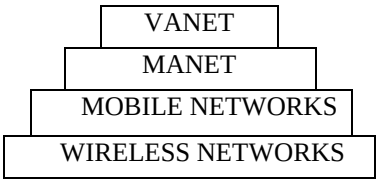
Amine Berqia
DEEI, FCT
University of Algarve, Portugal

Abstract— This paper presents a survey on the state of the art for vehicular ad hoc networks (VANETs). We start by reviewing possible applications of VANETs which could be classified into safety and non-safety applications. We expose theforces and weaknesses of this class of Mobile Ad hoc Networks. We survey two of their most critical issues which consist on the Quality of Service (QoS) and security. QoS becomes a hot topic due to unique features such as high mobility of the vehicles and the mediocre quality of links between them. Security is another challenging issue since vehicular networks are processing in open environments.Then, we review some of the recent solutions proposed in the literature about QoS and security.We review the Network Mobility (NEMO) approach based on MIPv6 which is interesting to keep the connectivity for vehicles moving from one access point to another. Finally we conclude with perspectives for security and QoS issues in VANETs.

Keywords—Vehicular ad hoc networks, Security, Quality of Service, NEMO, Survey.

I. INTRODUCTION

The need for communication when the deployment of any fixed infrastructure is impossible and the advancement of computer and wireless communication technologieshas led to the development of Mobile Ad hoc Networks (MANETs). This category of wireless networks does not rely on any fixed infrastructure, this make their deployment very easy. In addition, nodes in MANET are enhanced with routing functionalities to provide multi-hop communications. These specific features have allowed the expansion of their use in different application domains. During the last years,a great interest was awarded to the deployment of MANETs to improve road safety, then, Vehicular Ad hoc Networks have emerged.



Vehicular Ad hoc Networks (VANETs) are a subclass of MANETs. They are a promising approach for the Intelligent Transportation System (ITS).VANET is a set of vehicles moving on the road, equipped with communication capabilities among one another and with Road Side Units using wireless technologies such as Wi-Fi or WiMAX. The number of possible applications of VANETs is expanding. In addition to safety applications, vehicles are foreseen to support entertainment applications such as peer-to peer applications and Internet connectivity applications. However, these advantages create other challenges in terms of attacks on security [11, 21] since information is distributed in open access environments.

Approaches designed for MANETs are not suitable for VANET because they do not consider the high mobility constraints.Protocols designed for VANETs must take into consideration QoS requirements which are important for VANET safety, emergency and multimedia services. QoS parameters such as throughput, latency, jitter, packet loss are key requirements in VANETs.In this paper we survey some of the recent approaches developed to deal with QoS and security needs in VANETs.

Nowadays, the need of users to access Internet anywhere at any time is increasingly becoming a necessity.Unlike other wireless environments that are mostly stationary or with low mobility, data transmission in VANETs poses more challenges to be resolved. Since the topology is constantly changing, vehicles could move away from their home network and cause connectivity breakage. In order to cope with this problem, a vehicle connected to the wireless network should be able to move using different access points available along the road. These access points could belong to different networks or wireless technologies like Wi-Fi, WiMAX or 3G. Network Mobility (NEMO) is one the proposed solutions to keep connectivity of users in VANETs.

Our contribution in this paper consists to give a survey of QoS and security proposals in VANET. After presenting a general overview of VANET, we expose the QoS parameters needed to satisfy safety and non safety requirements.After that, we address security as another main challenge in VANET. Then, we survey some recent proposals which have been elaborated in the literature to improve QoS and security deficiencies in vehicular environments. We review the use of NEMO BS to manage mobility of terminal in the highly mobile VANETs.

The reminder of this paper is organized as follows. We start in section 2 with describing VANETs architecture, characteristics, applications and their challenging issues. In section 3 and section 4, we focus on QoS and Security requirements for VANETs, respectively, and review some of the recent proposals in order to cope with their derivedshortcomings. In section 5, we expose the NEMO technology and some of the proposed NEMO-based solutions for QoS and security issues in VANETs. Then, we conclude the paper in section 6.

II. VEHICULAR AD HOC NETWORKS

Vehicular communication networks have emerged as a key technology for next-generation wireless networking. The main goal of these wireless networks consists in providing safety and comfort for passengers by preventing vehicles crashes and traffic jam. In [1], the authors described vehicular Ad Hoc Networks: (VANETs) can be defined as a form of ad hoc networks to provide communications among nearby vehicles and between vehicles and nearby fixed equipments. VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. Vehicles which are members of a VANET share information about road conditions via Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) wireless communications.

This category of wireless networks does not rely on any central control unit and enables vehicles to intelligently communicate with each other and with roadside infrastructure. Each vehicle that is part of a VANET is equipped with an On Board Unit(OBU) and a set of sensors to collect and process information about road conditions, vehicle's position, speed, direction, etc, then send it as a message to other vehicles or RSU through the wireless medium using broadcast communication. The main functions of an OBU are: wireless radio access, ad hoc and geographical routing, network congestion control, IP mobility, reliable message transfer and data security [2].VANETs allow vehicles equipped with OBUs to share information through Vehicle to Vehicle communications (V2V) and to perform communications between vehicles and Road Side Units (RSUs) through Vehicle to Infrastructure communications (V2I). The RSUis equipped with one network device for a Dedicated Short Range Communication for Wireless Access Technology for Vehicular Environment(DSRC//WAVE),developed by the IEEE 1609 Group, which utilizes IEEE 802.11p, a modified version of IEEE 802.11 (Wi-Fi) standard.The motivation behind deployment of DSRC is to enable collision prevention applications (fig.1). These applications depend on frequent data exchanges among vehicles, and between vehicles and roadside infrastructure [3].RSU is responsible about extending the communication range of the ad hoc network by re-distributing the information to other OBUs and by sending the information to other RSUs in order to forward it to other OBUs, running safety applications such as a low bridge warning, accident warning or work zone, using Infrastructure to Vehicle communication (I2V) and acting as a source of information and providing Internet connectivity to OBUs [2]. The OBU is connected to other OBUs or RSUs trough a wireless link based on IEEE 802.11p radiofrequency channel. OBU can also communicate with other hosts for non-safety applications, using the communication of cellular radio networks (GSM, GPRS, UMTS, HSDPA, WiMAX and 3G or 4G).

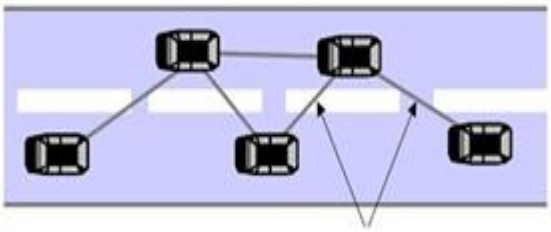


Fig.1. V2V Communication

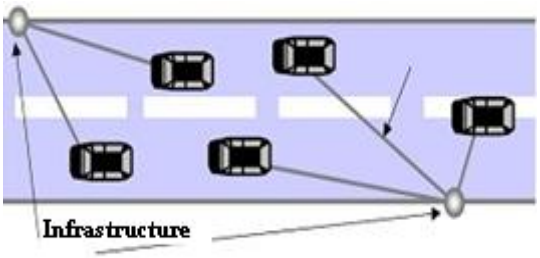


Fig.1.V2I Communication

The three major classes of VANETs applications are safety applications, convenience applications and commercial applications [13, 14, 15]. For example, applications like collision alert, weather conditions, road surrounding warning are classified under safety applications. They use the message broadcast feature of VANETs to inform nearby vehicles about critical alerts. Convenience applications would detect road congestion, help tool booths to collect toll without stopping vehicles. These applications are classified as safety applications which aim to ameliorate traffic conditions and prevent road accidents and save peoples' lives.

Commercial and entertainment applications become an attractive tendency. They include a wide range of future multimedia and data applications, such as audio/video as well as e-maps and roads vehicle related services. Road side businesses such as hotels and restaurants can use content rich video streams to broadcast advertisements to drivers on the

road. Peer-to-peer applications are another category of non-safety VANET applications. Passengers in nearby cars can set up a video conversation by using the inter vehicle streaming technology, exchange music, instant messages, stream music or movies from special servers. Travelers could play games in order to alleviate boredom. Vehicles are envisaged to become a part of internet in the near future, either as mobile endpoints, as mobile backbone routers or as mobile sensors.

VANETs have individual characteristics that are decisive in the design of the communication system. These include: dynamic topology, large scale network, high computational capability, impredictiblemobility, infinite energy supply in order to provide real time message dissemination platform to share data between vehicles and guarantee reliable exchange of information.

Infinite energy supply: vehicles in VANETs are not energy constrained like are nodes in a MANET. The vehicle can provide energy to the OBU continuously via the long life battery.

Rapid changes in the network topology:due to the high speed of vehicles, the topology of the network is very dynamic. VANETs will not have constant connectivity because of the high-speed movement between vehicles. In low-density vehicles, the link is highly likely to be disconnected.

Predictable mobility:unlike MANET where nodes move in a random way, VANET topology is not absolutely random. VANET movement restrictions are defined by road layout, topology, traffic rules, and the reaction to messages sent by other vehicles.

High computational capability: Because the nodes in VANET are vehicles, they can be equipped with a sufficient number of sensors and computational resources; such as processors, a large memory capacity, advanced antenna technology and global position system(GPS).

VANETs inherit from the wireless network shortcomings since they use radio frequency channel to exchange information between the different entities composing the network. These shortcomings consist on signal fading and bandwidth limitations [22].

Signal fading: This phenomenon is mainly frequent in urban regions. Buildings or other vehicles may constitute obstacles for nodes communications. These objects may cause transmitted signal fading or prevent it from reaching its destination.

Bandwidth limitations: as mentioned before, VANETs do not rely on any central administration. Consequently, this brings outproblemsabout the management of nodes communication and contention control. In order to optimize vehicular communications, it is necessary to use the available bandwidth efficiently. The high density of vehicles in urban regions may increase the probability of channel contention. An efficient utilization of the available bandwidth influences the time delay of message dissemination. Channel contention increases data transmission latency. This has very negative impacts, especially for warning messages delivery in safety applications. For entertainment applications, channel contention and the non-optimal use of bandwidth causes degradation of QoS requirement of users.

In addition there are some challenges which are specific for VANETs. Some of these challenges are time constraints, large scale of the network, and high mobility of nodes [20].

Time constraints:Safety messages are critical information which should be delivered with respect to time limitations.Warning messages are very time sensitive, so they must be delivered in a short interval of time beyond which they are useless.A driver must have enough time to react to a received warning message in order to prevent a crash.

Large scale network: the growing number of vehicles on the road will become, in the near future, one on the main constraints facing VANETs. A global authority must be set to manage information about users and others related to security. Since the security and privacy rules differ from a region to another in the world, their standardization will be complicated.

High mobility of nodes:

VANETs are characterized by high topology changes due to the high speed of vehicles. These changes cause frequent link failures. To alleviate this problem it is necessary to elongate link life by increasing the transmission power. But this solution can cause throughput degradation[9]. The vehicles high speed may cause handoff and cause packets loss which can reduce the throughput of the network.Since vehicles frequently change their point of network attachment when they access Internet services, they need mobility management schemes that provide seamless communication. This mobility management meets requirements such as seamless mobility, support IPV6, scalable overheads and low handoff latency. One approach for mobility management recently proposed NEMO Basic Support.VANETs differ from MANETs in the highly mobile nodes, the probability of network partition which is higher and end-to-end connectivity which is not guaranteed.

Privacy and security: VANETs are very constrained in terms of security and privacy. Making a balance between security and privacy to protect, users and data, in the same time, is a key challenge which must be solved. While registration to the network, vehicles provide some credentials because users require trustworthy information. However, this may violate source privacy.

In the following sections, we review two of the Quality of Service and security requirements for VANETS and some examples of the proposed solutions to meet these requirements.

III. QUALITY OF SERVICE IN VANETS

One of the most challenging tasks in VANETs is the quality of service (QoS) parameters. QoS is defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination [18].In wired networks, the QoS parameters are generally described in delay and throughput. The QOS

parameter in vehicular ad hoc networks is difficult to meet because of the network topology changes, scalability, the delay constrained routing and the impact of density and driving environments on the offered QoS services.

The data that is transmitted over the VANET can be classified into real-time (such as safety messages and video/ audio signals) and non real-time traffics (such as e-maps and road/vehicle–traffic/weather information), which impose the diverse quality of service (QoS) requirements for VANET designs. Supporting the delay-bound QoS is challenging when the VANET is under contention-based (e.g., IEEE 802.11 protocol) environments, where the packet delay and data congestion level increase dramatically as the total number of vehicles contending for the common wireless media (and, thus, the collision rate) gets large.

Sending and receiving correct data in a fixed duration of time is critical in this type of networks. Safety warning applications require minimum End-To-End delay because if a warning message is received with high delay, that message could be useless for preventing an accident. Rescue vehicles could instantly receive exact coordinates of the location of an accident to reach the scene of the emergency faster. Furthermore, information about traffic and road hazards could be acquired and fed into vehicle navigation systems in real-time to provide alternate driving routes [19].

Diverse solutions were developed to improve QoS in MANETs. These solutions perform either in network layer, MAC layer or physical layer. However, their utilization in VANETs presents some shortcomings. Among these solutions, we site proactive and reactive routing protocols. Their suitability for vehicular networks was studied in different articles[5].Due to the instability of the paths in VANEs, proactive routing protocols such DSDV[7] and OLSR [8] may fail. These protocols are based on the exchange of routing tables between neighbor nodes. This becomes worse in case of large scale networks.

Reactive protocols do not use routing tables but use a flooding method for route discovery that initiates more routing over head and also suffer from the initial route discovery process. Thus, they become unsuitable for security applications in VANET.

AODV [6] is an example of reactive protocols.AODVfloods the network with route request packets which leads to high overhead. The frequent topology changes in VANETs cause an important traffic which consists on control messages. In addition, the main drawback is that AODV needs end-to-end paths for data forwarding, which is difficult to handle because in VANETs end-to-end paths break often due to high speeds of vehicles. Therefore, it is recommended to develop the existing routing protocols to take into consideration the short life of the paths while respecting end-to-end delay, data losses and optimal use of bandwidth.

Furthermore, clustering is an efficient technique to reduce data congestion and support QoS over wireless networks. Lately, extensive research efforts have been dedicated to the design of clustering algorithms to organize nodes in Vehicular Ad Hoc Networks (VANETs) into sets of clusters. However, due to the dynamic topology of VANET, nodes frequently joining or leaving clusters compromise the stability of the network. The impact of these perturbations becomes worse on network performance if these nodes are cluster heads. Therefore, cluster stability is the key to maintain a predictable performance and has to consider reducing the clustering overhead, the routing overhead and the packet losses.

The non contention-based method TDMA (Time Division Multiple Access)was proposed as anefficient solution in the physical layer for mobile and sensor networks. This method consists toallocate a time slot for each node to send its packets. This method is efficient because it provides high reliable communications, resolve the problem of hidden nodes. However, in VANET, this method suffers from the merging collisions problem [4]t hat is due to the changing network topology.

A. QoS issues for VANETs

In [23], MPLS which can be compatible with any layer 2 technology is proposed as a forwarding method in order to improve QoS in terms of end-to-end delay, packet loss and throughput in urban areas. MPLS may result in improvement of E2E delay due to the fast processing of layer 2 headers, but it has its overhead for the wireless nodes, that move with fast speed. The idea of using MPLS in VANET, specifically in the roadside backbone network to gain better QoS is introduced. Due to the unreliability of V2V communications, we propose a method for vehicles in urban areas to send data to the nearest base station and after that data is sent via wired RBN which is MPLS domain, and have higher reliability in terms of E2E delay, packet loss and throughput. For data routing, AODV is used as a wireless routing protocol. AODV is a reactive routing protocol which reduces network load. It requires less space to store routing information and also consumes less bandwidth to communicate among neighbors.

In [28], AODV- ABE establishes forwarding paths that satisfy the bandwidth required by the applications. AODV is improved by introducing ABE (available bandwidth estimator) in its operations to estimate the available bandwidth on the wireless link. Nodes periodically update their available bandwidth using the ABE mechanism. ABE combines channel monitoring to estimate each node's occupancy including distant emissions probabilistic combination of these values to account for synchronization between nodes, estimation of the collision probability between each couple of nodes, and variable overhead's impact estimation. The available bandwidth estimation of a wireless link in ABE uses the idle time periods of the emitter and the receiver of the link. However, for a communication to take place, emitter and receiver must be both idle. As there is no reason that emitters and receivers are always idle at the same time, ABE includes, in its estimation, the probability that two end nodes of a link be both idle at the same time. When a new source wants to send a packet to a destination, AODV-ABE floods a route request message (RREQ) to that destination by including the required bandwidth in the RREQ. Each intermediate node that receives the RREQ checks if there is enough bandwidth on the link from which it receives the RREQ. If this is the case, the RREQ is forwarded; conversely, the required bandwidth cannot be satisfied and the RREQ is simple discarded. This allows the establishment of a forwarding

path that satisfies the required bandwidth, when such a path exists. As expected, AODV-ABE only accepts a new flow if the medium has enough capacity to offer the required throughput. AODV-ABE shows more stable throughputs and establishes forwarding paths that are able to guarantee the required bandwidth, so it is suitable for bandwidth demanding services such as video-streaming.

In [29], MQOG (MutichannelQoS Cognitive MAC) which is a new MAC protocol dedicated for VANET environments is developed. MQOG incorporates efficient channel negotiation on the dedicated control channel whereas data is transmitted on the other channel without contention. MQOG assesses the quality of channel prior to transmission employing a dynamic channel allocation and negotiation algorithm to achieve significant increase in channel reliability and throughput. It uses a unique dedicated control channel and multiple service channels for data transfer. MQOG is capable of prioritizing traffic to ensure QoS mitigating interference in high multipath environments and maximize system throughput by introducing a unique multichannel cognitive operation.This protocol separates the control traffic from the actual data transmission.A CNST (Channel Neighbor State Table) table is used to track communications between neighboring vehicles. The changes of the topology are reported by the neighboring nodes and stored in the CNST table.The underlying communication and intelligence lies on the control channel to dedicate a service channel for data transfer. Each vehicle is assumed to have two transceivers. The first one is dedicated for control traffic while the cognitive radio is used for data transmission and reception. A dynamic channel allocation algorithm is used where the cognitive radio assesses the available DSRC channel.Then, the noise and interference level is estimated in order to check the best available channel. If all the messages to be sent are safety messages and there is no channel with acceptable quality, a vehicle waits until the first good path detected becomes free. The safety messages are prioritized to non safety messages. A handoff mechanism is considered when a high priority frame must be sent. This frame queries the channel used by low priority frames.

In [30], a new QoS aware routing approach was proposed. In this approach, vehicles within the same transmission range and moving toward the same direction form clusters. Each vehicle can either be a cluster head, a gateway and ordinary member (OM). The node in this scheme is however in three modes: transmitting mode, receiving mode, and CH mode. Ultimately, the CH utilizes a long range transmission power when it wants to exchange information with its neighboring CHs. Whenever a CH wants communicating with its cluster member; it chooses a short range transmission power to gather/transmit safety messages over data channel using upstream-TDMA/downstream-broadcast method adopted. Much more, the CH allocates the accessible data channels towards the cluster-member nodes for the non-real-time traffics. Therefore, each CH determines the TDMA frame structure based on the number of OMs within the cluster. Subsequently, to broadcast the safety related messages within the cluster, the CH uses its available mini slots to broadcast the message on CCH from the TDMA frame.

This approach aims to improve channel utilization, data transfer rate and diminish the number of packet drop. The proposed TDMA-based QoS routing and conventional AODV are show lower performance at lower speed mobility. However our scheme is gradually increase to outperform existing protocol at higher speeds. Therefore the Overall throughput is significantly high with UDP connection as in comparison to TCP. TDMA based QoS routing is suitable for the rapid topology changes as a result of high mobility speed. Based on the several issues arising in guaranteeing bandwidth in vehicular ad hoc network, enhancement scheme is proposed by utilizing clustering approach using TDMA scheme. LORA-CBF is a reactive routing protocol with cluster-based flooding for inter-vehicle communications. Firstly, this protocol improves the traditional routing algorithms, based on non-positional algorithms, by making use of location information provided by GPS. Secondly, it minimizes flooding of its Location Request (LREQ) packets. Member nodes are converted into gateways when they receive messages from more than one cluster head. All the members in the cluster read and process the packet, but do not retransmit the broadcast message. This technique significantly reduces the number of retransmissions in a flooding or broadcast procedure in dense networks. Therefore, only gateway nodes retransmit packets between clusters (hierarchical organization). Moreover, gateways only retransmit a packet from one gateway to another in order to minimize unnecessary retransmissions, and only if the gateway belongs to a different cluster head. The protocol does not generate extra control traffic in response to link failures and additions. Thus, it is suitable for networks with high rates of geographical changes. As the protocol keeps only the location information of the [source, destination] pairs in the network, the protocol is particularly suitable for large and dense networks with very high mobility.

In [31] VANET QoS-OLSR is proposed in order to maintain the vehicular network stability while achieving the QoS requirements. VANET QoS-OLSR comprises three components: the QoS-based clustering, the cheating prevention and the MPR (Multi Point Relay) recovery. Optimized link State Routing (OLSR) groups the vehicles into clusters controlled by a cluster head that is elected. First, the cluster-head election algorithm elects a set of optimal cluster-heads which have the maximum QoS value. To compute QoS value for nodes different metrics are considered. These metrics are bandwidth, connectivity, mobility that includes residual distance and velocity. Next, the elected cluster-heads select a set of optimal MPR (Multi Point Relay) nodes responsible for transmitting the packets and connecting the clusters. This operation is done using an Ant Colony Optimization (ACO) algorithm that aims to reduce the end-to-end delay and increase the packet delivery ratio through a path guaranteeing the Quality of Service and mobility constraints. However, some nodes having high mobility and low QoS value may send false QoS value to be elected as MPRs. To guarantee the truth-telling and prevent the cheating during the selection procedure, a cheating prevention mechanism was introduced and that consists of encrypting the QoS values during the selection. After being selected, some MPR nodes may cause link failures and break the stability of the network. Therefore, an MPR recovery algorithm was introduced that is able to select alternative MPR nodes with acceptable Quality of Service and mobility metrics able to keep the network connected

and reduce the re-elections. This mechanism provides the stability of the network during the clusters formation, during the routing process, and in case of link failures while preserving the Quality of Service requirements.

In [27], a TDMA-based MAC protocol for VANET is developed. In order to reduce the probability of occurrence of merging collision during topology changes, the number of time slots in a frame is increased. In case of traffic density, the TDMA slot is increased. When the number of time slots is important, there is weak probability that two vehicles choose the same time slot. Therefore, the probability of merging collisions is reduced.As in MAC ADHOC, the size of the TDMA frame in adjusted according to vehicles density on the road, in this approach; the size TDMA slot is increased. The authors of the effect of raising the size of a TDMA frame by N times on reducing the likelihood of the occurrences of merging collisions. However, increasing S by N times reduces the bandwidth usage of each vehicle to 1/N times. The simulation conducted show that N=2 can carry satisfactory performance improvement without compromising too much bandwidth loss. So, to keep a fair usage of the bandwidth, the size of a TDMA frame is increased to two times as largewhen traffic density is high.

IV. SECURITY IN VANETS

Vehicular ad hoc networks (VANETs) are being increasingly important as they are foreseen to deeply influence and improve road safety and driving conditions. Before implementing VANET applications, different security issues such as authenticity, integrity, must be solved because any malicious behavior of users, such as modification and replay attacks with respect to disseminated traffic-related messages, could be fatal to other users.

A. Security challenges in VANETs

Security is not a separate issue but linked to the control and management of QoS network and services. Security is an important issue in any communication system. Due to the fact that VANETs are composed of number of communicating autonomous entities moving at high speed, the randomness of the connectivity between the vehicles and their relative geographic positions raises concerns about users and data security. Most desired security attributes as criteria to measure security for all VANET applications are authenticity, privacy, availability confidentiality and non-repudiation. Attacks in VANETs hinder vehicles communications by deteriorating or interrupting their functions. To meet aforementioned security requirements, several approaches were proposed by researchers which aim to prevent or diminish the consequences of attacks.

A key challenge of securing VANETs is to provide sender authentication in broadcast communication scenarios. To authenticate users or messages in VANETs, we have recourse to the identification. A vehicle is identified by being registered to the VANET; a vehicle must provide a registration number to certified authority or trusted authority. This authority is responsible of providing an authenticated recognition to each vehicle in the network. Vehicle credentials provided to Certified Authorities allow the localization of vehicles by geographic localization services like GPS. This information may be used by adversaries to track the vehicle or get personal information about drivers. In order to preserve privacy, it is necessary to use cryptography and digital signature. Therefore, the cryptographic techniques and digital signature used in VANETs must have low traffic and processing overheads while generating and exchanging public keys.

A malicious entity within the VANET may broadcast false information. This attack is known as Sybil attacks. In a Sybil attack, a vehicle sends multiple copies of messages to other vehicles and each message contains a different fabricated identity. The problem arises when malicious vehicle is able to pretend as multiple vehicles and reinforce false data. A Sybil node may create an illusion of traffic congestion. There are several technique proposed to encounter Sybil attack in VANETs such asstatistical and probability, signal strength and session keys [16]. Another category of attacks on the data integrity is spoofing which consists on node impersonation. Spoofing is an attempt by a node to send modified version of message and claims that the message comes from originator for the unknown purpose.

Keeping a reasonable balance between the security and privacy is one of the main challenges in VANET. On the one hand, the receivers want to make sure that they can trust the source of information. On the other hand, the availability of such trust may contradict the privacy requirements of the sender. While registration, information provided by the vehicle may be used by a malicious entity in order to localize the vehicle and track it. The privacy issues are concerned with protecting and disclosing driver's personal information such as name, location, etc.

Messages should reach the destination within the relevant time period. As VANETs consist on vehicles moving at high speed, the development of secure routing protocols is necessary. The efficacy of VANET communication depends on providing critical data within the relevant time to give users enough time to take into consideration the critical data. As vehicles use the scarce resource radio channel to communicate, VANETs are prone to attacks on network availability. Two possible threats to availability are for example DoS and jamming attacks. Another availability problem might be caused by selfish nodes that do not provide their services for the benefit of other nodes in order to save their own resources like battery power [17].

The DSRC/WAVE standard, as specified in a range of standards including those generated by the IEEE P1609 working group, enables V2V and V2Iwireless communications. This connectivity makes possible a range of applications that rely on communicationsbetween road users, including vehicle safety, public safety, and other application .the increasing number of applications using VANETs, risks are being more, and the safety-critical nature of many WAVEapplications makes it vital that services be specified that can be used to protect messages from attacks suchas eavesdropping, spoofing, alteration, and replay. Additionally, the fact that the wireless technology will bedeployed in personal vehicles, whose owners have a right to privacy, means that in as much as possible thesecurity services should

respect that right and not leak personal, identifying, or linkable information tounauthorized parties.With this in mind, at the time that IEEE P1609 was established to develop the standards for the DSRCwireless network stack, the IEEE also established later renumbered as IEEE 1609.2 todevelop standards for the security techniques that will be used to protect the services that use this networkstack. These applications face unique constraints. Many of them, particularly safety applications, are timecritical:the processing and bandwidth overhead due to security must be kept to a minimum, to improveresponsiveness and decrease the possibility of packet loss.

B. Security proposals for VANET

In [10], authors developed a secure MAC protocol taking account of the DSRC channel structure. This protocol takes into consideration different security parameters and ensures the freshness of the message using a time-stamp, digital signature and trusted certificate. Considered security parameters are message authentication and integrity, message non-repudiation and privacy and anonymity of the senders. The protocol uses a part of IEEE 1609.2 security infrastructure including PKI (Public Key Infrastructure) and ECC (Elliptic Curve Cryptography). Four queues per OBU are reserved to different priority message classes. Each OBU is associated a scheduler which allows higher priority message before lower priority messages. A preemptive policy is adopted to schedule high priority messages to get the channel immediately before the transmission of low priority message is completed. In this approach, each OBU is supposed to have a secure database which contains cryptographic keys used for digital signature. These keys change periodically and are certified by the CA which uses these certificates in case of accident or law investigation to prevent non-repudiation. PKI is used for certificates delivered by the CA for Each vehicle. For safety messages, the confidentiality is not required, so they are sent in plaintext. Safety messages are signed with the private key and include the CA's certificate. A time stamp signed with the private key is added to indicate the freshness of the message. The messages are small sized and do not create an overhead in the network. The other vehicles extract the public key of the sender to decrypt the signature and verify the integrity of the message and the time-stamp.

In [25], a Symmetric-Masquerade Security Scheme (SMSS) was proposed. This new approach achieves security requirements of V2V communications while keeping a low system overhead. In a firs t step, an entering vehicle in the coverage of a certain BS, it broadcasts a message containing a public key to apply for a pseudonym and another one as a pre-shared key which is updated periodically. The message includes a time stamp to avoid replay attacks. After that, he BS assigns a local pseudonym to the vehicle. To protect the privacy of each vehicle, only the base station knows their real names and their corresponding pre-shared key. So when vehicles within the coverage of a BS want to communicate, the BS assists the symmetric key exchange between them to verify the integrity of the nodes. After the symmetric keys are exchanged between the communicating vehicles, a link is established for a short time to allow secure end-to-end communications without the assistance of the BS. When a vehicle leaves the range of a base station, it returns the pseudonym that will be assigned to a future entering vehicle. BSs maintain a table which records the uni-mapping between the pseudonyms and the real identifications of current users. This mechanism allows the BS to identify imposture immediately. This security scheme does not create overhead in the network such as asymmetric schemes where private and public keys are exchange between communicating entities.

In [35], a secure position-based routing protocol is developed. Authors applied a security mechanism to the protocol GPSR (Greedy Perimeter Stateless Routing). In this security scheme, every node in the VANET estimate the behavior of other nodes to know if a node has ever tampered or dropped packets previously. The scheme can detect malicious nodes and keep the validation of the routes by detecting the malicious nodes. The security solution comprises two mechanisms: routing message protection mechanism and node evaluation mechanism. For the protection of routing data, a signature verified scheme is employed to achieve end-to-end authentication and integrity. A signature field is added to the routing packet. For node evaluation, every node is turned in a hybrid mode to check all the messages sent by its neighbors. The reliability of a node is estimated according to its forwarding ratio. The evaluation mechanism used comprises forward evaluation and backward evaluation. Forward evaluation algorithm aims to find out the drop malicious nodes. In the forward evaluation, a sender assesses the receiver to know if it has relayed the packet. The backward evaluation algorithm is used to find out the tamper malicious node. When a node sends a packet to a neighbor node, the later one assesses the source of the received packet. In backward evaluation, the integrity of the packet is verified using the digital signature. an evaluation value is calculated using forward and backward evaluation values. Then, the calculated value is compared to the threshold one in order to decide if the corresponding node can be selected as a next hope.

In [36], the security solution relies on location information and corresponding time. A mobility pattern which allows the detection of misbehaving nodes was proposed in order to enhance security and privacy. Vehicles periodically sign and broadcast their current locations. In each time slot, nodes construct their public key and their anonymous pseudonyms address and broadcast them to their neighbors. Location and time id exchanged between nodes in small intervals of time.The location is used to reveal the existence of the vehicle while keeping its privacy protected because there is no link between the physical vehicle location and the identity of the vehicle. The communication paradigm among vehicles and the periodic location information is used to detect misbehavior. A vehicle is represented by series of locations in its trajectory. If random locations are received, this behavior is considered abnormal. In order to protect vehicles privacy, nodes communicate using their dynamic locations since vehicles are assumed to be equipped with positioning systems (GPS). When a vehicle gets its location coordination via GPS, it generates two pairs of keys based on group signature, then, the location and time are signed using the private key. A Location Anonymous Message (LAM) is used by the vehicle to broadcast the signed information to its neighbor nodes. When the later receive the message, they store the location in a Location/Time Table (LTT) with the corresponding time. The main contribution of this work is the

mobility pattern formation and misbehaving node detection based on it. The mobility pattern helps predicting some possible attacks. LA messages stored in the LTT serve to build the mobility pattern. The location information gathered by the vehicle is compared to the road map to detect malicious nodes which consist on locations that are not within the road perimeter. The mobility pattern helps nodes to evaluate the integrity of the received messages. For example, if a node claims its presence in different locations in a short period of time, this information could be used to detect possible attacks such as Sybil attack. Therefore, the suspect node is removed from the VANET.

In [37], a protocol for Authentication with Multiple Levels of Anonymity (AMLA) is proposed. In this approach, each vehicle is assumed to be connected to a Security Service Provider (SSP). This server is responsible for providing privates keys to vehicles. When a vehicle enters decide to be a part of a VANET, it requires from the SSP, a number of pseudonyms and the desired life time of each pseudonym. Each vehicle is supposed to be equipped with a tamper proof device which stores its secret keys. These keys are accessed only by the SSP to keep the privacy of the vehicle. To ensure authenticity of messages, AMLA uses the identity based Encryption (IBE) and signature mechanism. A vehicle transmits messages signed with its private key corresponding to one of its pseudonyms, so its identity remains hidden. The private key of a vehicle is a function of its pseudonym. When the neighboring nodes receive the message, they use the public key of the sender and the public key of the SSP. AMLA provides different levels of anonymity to vehicles which is determined by the number of pseudonyms and the lifetime of each pseudonym.AMLA implements short term credentials without the use of any public key certificate; this keeps the overhead in the network low compared to certificate based approaches.

In [12], a new identity based secure algorithm for VANET is proposed. The primary objective of this solution include the management of identities using signam, pair of public-private key and hash function, the security of communications and the integration of privacy enhancing technologies. In this scheme, a unique identifier is introduced. Ea vehicle is assumed to be equipped with an OBU which is tamper proof device that stores the secret information and the event data recorder. A vehicle sends its identifier to the vehicular authority (VA) which issues an USN for a unique identification which does not reveal the true identity of the vehicle. The vehicle sends its USN to the RSU which relies with a signam.RSU only provides the authentication signature and restrictions for the vehicle to signam generation. Vehicles true identity and private information are not known by the RSU. This mechanism allow secure communications while keeping the privacy of the vehicles protected.

V. NETWORK MOBILITY (NEMO)

IP protocol is increasingly presented as a solution for the problems encountered by mobile users to access Internet.Using IP (IPv4 or IPv6) protocol, mobile nodes would not be reachable because their point of attachment and their IP address have changed. This results in the connectivity breakage and then, increase of packet loss.In order to cope with these problems, a protocol which allows nodes to remain reachable while moving around in the IPnetworks was developed. This protocol is known as Mobile IP.

To allow nodes to remain reachable, even ifit changes its point of attachment to Internet, Mobile IP uses a Mobile Router (MR). The MR allows local fixed and mobile nodes and even visiting nodes to still connecting to Internet. The MR reduces transmission power. Nodes communicate with a MR rather than an access router on the Internet. Furthermore, the MR reduces handoffs because it handles link layer handoffs. MR reduces the bandwidth consumption and location update delays. When a network changes its point of attachment to Internet,all mobile and fixed nodes inundate their Home Agent (HA) with registration messages, but with the use of a MR, one registration message is sent to HA to register the whole network.The HA is a router which delivers packets to a mobile node when it is away from its home network and maintains current location information for the mobile node.When away from its home network, a mobile node is associated a Care-of Address (CoA)that reflects its current point of attachment. This allows nodes to keep their home IP addressand to receive packets sent to it by a Correspondent Node. The mechanisms of MIP make the movement of nodes being transparent to transport and higher layer protocols and applications.

Mobile IPmay be used in IPv4, but the restricted scale of addresses makes communication management of mobile terminals being complicated. IPv6 is preferable due to its great number of available addresses which allow attribution of temporary addresses to the moving stations. In [34], MIPv6 was defined as a protocol allowing mobile nodes to move from a link to another while keeping their home address unchangeable.The use of IPv6 routing header by MIPv6 results in a reduced overhead, then improves the use of the resources of the communication medium.

However, MIPv6 is unable to support network mobility. Not all devices in amobile network such as the sensors on an aircraftmay be sophisticated enough to run these complexmobility support protocols. In addition, once a device has attached tothe MR on a mobile network, it may not see anylink-level handoffs even as the network moves.Thus the host mobility protocols such as MIP andMIPv6 do not get triggers indicating link-levelhandoffs and as a result will not initiate handover. This paved the way to the development of a Mobility management mechanism which consists on Network mobility basic support.Till now, only nodes mobility is considered. However, different scenarios of entire moving networks exist (WLANs on trains, planes, ships etc.). In order to support Network Mobility (NEMO), an extension of MIPv6 was realized.

NEMO Basic Support (NEMO BS) [33] is developed to cope with the aforementioned insufficiencies of MIPv6. NEMO BS is an extension of MIPv6 protocol. It allows terminals within a mobile network to globally and continuously be connected to the Internet. The NEMO BS is designed so that network mobility is transparent to the node inside the mobile network, only MR and HA are aware of the network changes, since Mobile Network Nodes (MNNs) continue to be connected with MR using the same address configured using the Mobile Network Prefix (MNP).

A. Deployability of NEMO in VANETs

If the mobility of each node is managed independently, this results in an important amount of control messages which overload the wireless link. Since all the devices on a vehicle are moving in the same trajectory and with the same speed, managing the mobility of these nodes jointly affects deeply the amount of generated traffic in the wireless link and optimizes the use of available bandwidth. Therefore, NEMO BS is suitable to manage devices mobility in vehicular networks due to their highly mobile nature. The main goals of the mobility management protocol are providing continuous communications without service disruption owing to mobility events; and allowing reachability to nodes onboard regardless of their location.

The connectivity to Internet offers the possibility of remote assistance of vehicles and providing communication services to onboard users. So, it is necessary to secure data communication services and network mobility management exchanges from attacks which can cause the breakage of ongoing communication. A disconnection due to security attacks can isolate the mobile network and result in the interruption of remote assistance of vehicles by the provided ITS services.

In NEMO, the MR needs to allow subscribers from different domains to get Internet connectivity through it. In such settings where static trust relationships are lacking, a variety of security threats arises. Security and performance are critical aspects of NEMO. Mobile networks travel on foreign, and possibly untrusted, networks when away from home. Because MNNs are unaware of mobility, it is important that NEMO provides security while a network is away. Also, performance is important in accomplishing the goal of NEMO to provide seamless mobility to unaware IP device. In the NEMO BS protocol the use of IPsec to protect signaling messages is advocated. Security mechanisms for network mobility are at a preliminary stage and much work needs to be done in order for mobile networks to be deployed in a secure setting.

Delay and packet losses constitute another issue for mobility management in VANETs. When a MR does a handover and changes its pointof attachment it needs to activate MIPv6 and theNEMO handover procedures. Upon detection of amovement the MR obtains a care-of address from the foreign network and then indicates to it's HA that it is playing the role of a MR. This handover process results in increased latency due to the multiple levels of indirection involved. The chances of packet loss are also more significant as a result of increase in latency. Research is required to adapt mechanisms such as fast handover to support mobile networks.

In the next subsection, we survey some solutions developed to improve security and QoS requirements of network mobility in vehicular environment.

B. Issues for QoS and security in NEMO-basedVANET

In [38], authors propose a location privacy solution which consists on the fake point to protect privacy of the vehicles in NEMO-based VANETs. The fake point mechanism allows a high level privacy for MNNs. The main idea of this protocol consists on choosing a location inside the hotspot that is called later Fake Point (FP). This FP is considered by the MNNs while calculating their transmission power. If an attacker's device is located inside the FP, it measures the RSS value as being the same for all the MNNs. This makesa deviation in the attacker's estimation of the MNNs distance. Hence, the privacy of the location of the mobile nodes is kept. To exchange authentication information with the MNNs, the AP, represented in this protocol by the OBU/MR, broadcasts periodically frame beacons containing its location, the MNP and the AP certificate. This information allows the MNNs to calculate their distance to the AP according to the RSS, join the NEMO hotspot and check the authenticity of the AP in the hotspot. After that, the AP sends the grid-point's list containing the locations inside the hotspot to the MNNs. Then, the MNN selects a point in the list and calculate its transmission power to this point as it will send its data to the AP via this node. Instead of sending data to this selected FP in grid-point list, a MNN sends it to its AP to confuse attacker devices which may be located in this fake point.

In [39], a handover mechanism based on Care-of Prefix Pool (CoPP) is proposed. The vehicle adopting this handover mechanism can acquire unique Care-of Prefix (CoP) from the new Base Station (BS) with CoPP. The proposed solution leaves out the Duplication Address Detection (DAD) phase, and then significantly reduces the handover delay. In order to cope with the interruption of the communication when a vehicle moves from an access point to another, a CoPP is deployed on the nAR (new Access Router). When a MR moves, it acquires a unique CoP carried by the CoPP, so the MR CoA DAD phase is omitted. The CoPP provides a unique CoP and generates the candidate CoA.The maintaining algorithm of the CoPP to guarantee the uniqueness of CoP and generate the candidate CoA, which is unique acquired by the vehicle's MR. So the DAD process, can be omitted directly.

The authors in [40] have proposed a link-layer authentication and key agreement scheme. This protocol uses the Certificate-less and key agreement (CL-AKA) scheme to secure public hotspots in NEMO-based VANET. When an MNN decides toconnect to the OBU/MR's public hotspot, it first verifies theOBU/MR's public key using an online certificateverification web-site. Putting a threshold time, T, for thecertificate verification's response, the MNN authenticates theMR if it receives the response within T. The MNN sends an authentication request to the OBU/MR that contains three parts of information which consist on its identity encrypted by OBU/MR's public key, one MNP that the MNN chooses from the MNPs found in the periodically broadcasted messages and the MNN's credentials such as payment data. The security of the proposed protocol is based on the hardness of the encryption algorithm used in this mechanism is the Elliptic Curve algorithm which necessitate exponential time to be resolved. Using CL-AKA scheme only authorized users that send valid authentication requests can gain Internet access from OBU/MR. Containing valid credentials such as payment data, the authentication request message is accepted by the OBU/MR that stores the MNN's

identity along with its credentials. Therefore, malicious MNNs that send invalid credentials cannot access the hotspot.CL-AKA achieves lower computation and communication over-heads, higher security levels, and lower energy consumption.

VI. CONCLUSION

The quality of service and security are main challenges in VANETs applications since they are directly related to the safety of people.In this paper, we surveyed the most important requirements of VANETs applications which consist on the Quality of Services, security and privacy aspects. As QoS and security are deeply influenced by the wireless environment such as dynamic topology changes due to the high speed of vehicles, several work were conducted in the literature. After reviewing the architecture, the applications, characteristics and challenges, we presented some of the short comings of QoS and security in vehicular environments. As VANETs are foreseen to provide ubiquitous services for users by keeping them connected to Internet for safety and entertainment needs, NEMO was proposed as a promising solution to cope with users disconnections due to the high speed of vehicles. Thus, we exposed the main idea of NEMO which is still evolving. Then, we presented some recent solutions proposed to improve the different parameters in order to provide efficient and secure communications in vehicular environments.

REFERENCES

[1] Sasha Dekleva, J.P. Shim,UpkarVarshney, and Geoffrey Knoerzer "Evolution and emerging issues in mobile wireless networks", ACM Communications Vol. 50, No. 6, June 2007.

[2] C.C. Communication Consortium; IEEE trial-use standard for wireless access in vehicular environments; Olariu and Weigle, 2009.

[3] John B. Kenney, Dedicated Short-Range Communications (DSRC) Standards in the United States, Proceedings of the IEEE | Vol. 99, No. 7, July 2011.

[4] Jeng-Ji Huang and Yu-Shiang Chiu,A Scheme to Reduce Merging Collisions in TDMA-Based VANETs, Wireless and Pervasive Computing (ISWPC), IEEE 2013.

[5] BaraaT.Sharef, Raed A.AlsaqourMahamodIsmail, Vehicular communication adhoc routing protocols: Asurvey, Journal ofNetworkandComputerApplications40(2014)363–396.

[6] Charles E. Perkins, Elizabeth M. Royer, Ad-hoc On-Demand Distance Vector Routing, In: Proceedings of the 2nd IEEE workshop on mobile computing systems and applications, WMCSA'99; 1999.p.90–100.

[7] Perkins CE,BhagwatP. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, ACM SIGCOMM Computer Communication Review 1994;24:234–44.

[8] Clausen T, Hansen G, Christensen L, Behrmann G, The optimized link state routing protocol, evaluation through experiments and simulation. In: Proceedings of the symposium on wireless personal mobile communications; IEEE 2001.

[9] Saif Al-Sultan, MoathM.Al-Doori, Ali H. Al-Bayatti, HussienZedan, A comprehensive survey on vehicular Ad Hoc network, Journal of Network and Computer Applications 37 (2014) 380–392.

[10] Yi Qian, Kejie Lu, and Nader Moayeri, A secure VANET MAC protocol for DSRC applications, "GLOBECOM" proceedings, IEEE 2008.

[11] Ghassan Samara, Wafaa A. H. Al-Salihy, R. Sures, "Security Analysis of Vehicular Ad Hoc Networks (VANET)", Second International Conference on Network Applications,Protocols and Services 2010.

[12] Arpita Chaudhuri, Suparna Dasgupta, Soumyabrata Saha, "Identity based algorithm for VANETs", Procedia Engeneering 38 (2012) 165-171.

[13] Kamini, Rakesh Kumar, "VANET parameters and applications: A review", Global Journal of Computer Science and Technology, vol. 10 issue 7 p 72-77, September 2010.

[14] B. Mishra, P. Nayak, S. Behera, D. Jena, "Security in Vehicular Ad hoc Networks: A survey", ICCCS, February 2011, ACM, Pages 590-595.

[15] C.-T. Li, M.-S.Hwang, and Y.-P. Chu, "A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks". Computer Communications, Volume 31, Issue12, 30 July 2008, Pages 2803-2814.

[16] Bin Xiao, Bo Yu, ChuanshanGao, "Detection and Localization of Sybil Nodes in VANETs", DIWANS, ACM, September 2006.

[17] Pino Caballero-Gil, "Security Issues in Vehicular Ad Hoc Networks", Mobile Ad-Hoc Networks: Applications, Prof. Xin Wang (Ed.), ISBN: 978-953-307-416-0, InTech, 2011.

[18] Sasan Adibi, Shervin Erfani, "mobile Ad-hoc Networks with QoS and RSVP provisioning", CCECE 2005, May 1-4 Saskatoon, Canada.

[19] Shouzhi Xu, Pengfei Guo, Bo Xu, Huan Zhou, "QoS evaluation of VANET routing protocols", Journal of Networks (JNW), Vol 8, NO. 1, pages 132-139, January 2013.

[20] T. Leinmuller, R.K. Schmidt, E. Schoch, A. Held, G. Schafer, Modeling roadside attacker behavior in VANETs, in: GLOBECOM Workshops, IEEE, New Orleans, LO, 2008, pp. 1–10.

[21] R.G. Engoulou et al., VANET security surveys, Comput. Commun. (2014), http://dx.doi.org/10.1016/j.comcom.2014.02.020

[22] Hartenstein H, Laberteaux K P. A tutorial survey on vehicular ad hoc networks. Communications Magazine, IEEE 2008; 46(6): 164–71.

[23] Mahmood Fathy, Saeed Gholamalitabar Firouzjaee, Kaamran Raahemifar "Improving QoS in VANET Using MPLS" , The 7th International Symposium on Intelligent Systems Techniques for Ad hoc and Wireless Sensor Networks (IST-AWSN), Elsevier 2012.

[24] L. Liu ,A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning, 1st Annual Int'l. Conf. Mobile and Ubiquitous Systems: Networking and Services, MOBIQUITOUS, 2004.

[25] Lingyun Zhu, Chen Chen, Xin Wang, Azman Osman Lim, SMSS: Symmetric-Masquerade Security Scheme for VANETs, 2011 Tenth International Symposium on Autonomous Decentralized Systems, 978-0-7695-4349-9/11, IEEE 2011

[26] Subir Biswas, Jelena Mišic, A Cross-Layer Approach to Privacy-PreservingAuthentication in WAVE-Enabled VANETs, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 5, JUNE 2013.

[27] J eng-Ji Huang and Yu-Shiang Chiu, A Scheme to Reduce Merging Collisions in TDMA-Based VANETs,International Symposium Wireless and Pervasive Computing (ISWPC), IEEE 2013.

[28] Tripp Barba, Ahmad Mohamad Mezher, Monica Aguilar Igartua, Isabelle Guérin-Lassousand CheikhSarr, Available Bandwidth-aware Routing in Urban Vehicular Ad-hoc Networks,Carolina, 2012 IEEE.

[29] Hikmat El Ajaltouni, Richard W. Pazzi, and AzzedineBoukerche, An Efficient QoS MAC for IEEE 802.11p Over Cognitive Multichannel Vehicular Networks, Ad-hoc and Sensor Networking Symposium, IEEE ICC 2012.

[30] Abubakar Aminu Mu'azu1, Low Tang Jung, Ibrahim A. Lawal, Peer Azmat Shah, A QoS Approach for Cluster-Based Routing in VANETS Using TDMA Scheme,978-1-4799-0698-7/13, ICTC, IEEE 2013.

[31] Omar Abdel Wahab, HadiOtrok, AzzamMourad,VANET QoS-OLSR: QoS-based clustering protocol for Vehicular Ad hoc Networks, Computer Communications 36 (2013) 1422–1435.

[32] Carlos Gañán, Jose L. Muñoz, Oscar Esparza, Jorge Mata-Díaz, ,Juanjo Alins, EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.002

[33] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert.(2005, Jan).Network mobility basic support protocol.RFC Standard 3963. Available: http://www.ietf.org/rfc/rfc3963.txt

[34] D. Johnson, J. Arkko. (June 2004). Mobility Support in IPv6.RFC standard 3775. Available: http://www.ietf.org/rfc/rfc3775.txt

[35] JieHou, Lei Han, Jia Zhao, Jiqiang Liu, Secure and Efficient Protocol for Position-based Routing in VANETs, IEEE 2012

[36] Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin, Security and Privacy Enhancement in VANETs using Mobility Pattern, 978-1-4673-5990-0/13,ICUFN, IEEE 2013.

[37] BharadiyaBhavesh N, Soumyadev Maity and R. C. Hansdah, A Protocol for Authentication with Multiple Levels of Anonymity (AMLA) in VANETs, 27th International Conference on Advanced Information Networking and Applications Workshops, 978-0-7695-4952-1/13, IEEE 2013.

[38] Sanaa Taha, and Xuemin (Sherman) Shen, Fake Point Location Privacy Scheme for Mobile Public Hotspots in NEMO based VANET, Communication and Information Systems Security Symposium978-1-4673-3122-7/13, IEEE 2012.

[39] Bin Zheng, Yuliang Yang, Handover Mechanism based on Care-of Prefix Poolbin VANET with NEMO, International Conference on Computer Science and Service System, 978-0-7695-4719-0/12, IEEE 2012.

[40] Sanaa Taha, and Xuemin (Sherman) Shen, A Link-layer Authentication and Key Agreement Scheme for Mobile Public Hotspots in NEMO based VANET, Globcom Communication and Information System Security Symposium, 978-1-4763-0921-9/12, IEEE 2012.

