JACET Journal of Advances in Computer Engineering and Technology, 2(3) 2016

Vehicular Networks: A Survey on Architecture, Communication Technologies and Applications

Mohammadreza Pourkiani[1], Sam Jabbehdari[2], Ahmad Khademzadeh[3]

Received (2016-04-22)
Accepted (2016-08-08)

***Abstract* - Intelligent traffic systems (ITS), sometimes called intelligent transportation systems, apply communications and information technology to manage traffic flow, encourage drivers to use alternate forms of transport, and enable people to find the services and information which they need to drive safely, avoid traffic jams, and perform their daily routine with fewer hassles and with more peace of mind. Vehicular Ad-hoc Network which is an application of Mobile Ad-hoc Networks provides wireless Ad-hoc communication between vehicles. VANET is a mobile wireless technology which is designed to improve safety of transportation with exchanging real time data between vehicles and providing different services to the users. It has special characteristics like high mobility and provides a broad range of services to the users and it has been emerged as one of the research interests in the field of computer and telecommunication networks. In this paper we present different aspects of ITS and VANET to help the researchers to understand the architecture, communication technologies and applications of these networks.**

***Index Terms* - ITS, VANET, Ad-hoc Networks, Mobile communication**

1- Department of Information Technology, Science and Research Branch, Islamic Azad University, Tehran, Iran. (m.pourkiani.ir@ieee.org)
2- Department of Computer Engineering, Tehran North Branch, Islamic Azad University, Tehran, Iran.
3- Department of Education and International Cooperation, Iran Telecommunication Research Center, Tehran, Iran.

I. INTRODUCTION

1. Intelligent Transportation Systems

INTELLIGENT Transportation System (ITS) is a system which is based on the increasing demands of the transportation development and is able to exchange different kinds of information of its moving objects. It converges remote sensing and communication technologies to improve safety of transportation and it also makes journey more enjoyable. As the objects are moving, wireless communication technology plays an important role in this system. ITS integrates information, communications, computers and other technologies and applies them in the field of transportation to build an integrated system of people, roads and vehicles by utilizing advanced data communication technologies [1]. It includes a broad variety of means of transportation and a broad variety of usage scenarios and user preferences and interests [2].

The typical ITS scenario is land traffic on roads and the most common examples of ITS applications are the exchange of traffic information to provide roadside assistance, warning in case of emergencies and traffic jam, these services deal with data as, e.g. road condition, traffic light status and position of the single vehicle [2].

There are four typical ways of transportation, on the land by car or train, in the air or water. The most common traffic coming into our mind in combination with Intelligent Transportation Systems is traffic on land.

2. Vehicular Ad-hoc Networks

Among the means of transportation, the most prominent are cars, at the present time cars and other private vehicles are used daily by many

people. The biggest problem regarding the increased use of private transport is the increasing number of fatalities that occur due to accidents on the roads. In recent years traffic congestion and accidents, as well as environmental pollution caused by road traffic and fuel consumption have become important global issues [3].

Vehicular networks are proposed to provide information exchange via Vehicle-to-Vehicle (V2V) and vehicle to infrastructure (V2I) communications. A Vehicular Ad-Hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network, it turns every participating vehicle into a wireless router or node [4]. VANET is capable of enhancing driving safety by exchanging real-time transportation information and it should upon implementation, collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it [5].

VANET has its own characteristics when compared with other types of MANETs, Authors in [6] describe the unique characteristic of VANET as follows:

- Predictable mobility
- Providing safe driving
- No power constraints
- Variable network density
- Rapid changes in network topology
- Large scale networks
- High computational ability

The key role that VANETs can play in the realization of ITS has attracted the attention of major car manufactures and they continue to incorporate more and more technological features into their vehicles [4]. It is reported that over 50% of interviewed consumers are highly interested in the idea of connected cars, 22% of whom are willing to pay $30-65 per month for value-added connectivity services while on the road [7]. However, there are lots of challenges in this field. Authors in [6] listed the issues as follows:

- Signal fading
- Bandwidth Limitation
- Connectivity
- Small effective diameter
- Security and privacy
- Routing

Because of the challenges, limitations and new requirements in VANETs, the idea of Heterogeneous Vehicular Networking has emerged recently.

3. Heterogeneous Vehicular Networks

Authors in [3] define the term Heterogeneous Vehicular Networks (HVN) as follows:

HVN integrates cellular networks with Ad-Hoc networks which is a potential solution for meeting the communication requirements of the ITS. Although there are a plethora of reported studies on either DSRC or Cellular Networks, joint research of these two areas is still at its infancy. Emerging Heterogeneous Networks not only have the ability of providing wide-area coverage to all vehicles in large-scale networks, but also supports real-time safety messages distribution in local areas in order to reduce traffic accidents. Therefore, Heterogeneous Vehicular Networks may well support the communication requirements of the Intelligent Transportation System. A car that takes part in such a network is equipped with a WLAN and cellular communication device [3].

The rest of the paper is organized as follows: In section II we present some proposed architecture for vehicular networks while in section III different communication technologies in VANETs are described. In section IV security issues and challenges in vehicular communications are described and in section V applications of vehicular networks are given before the conclusion in section VI.

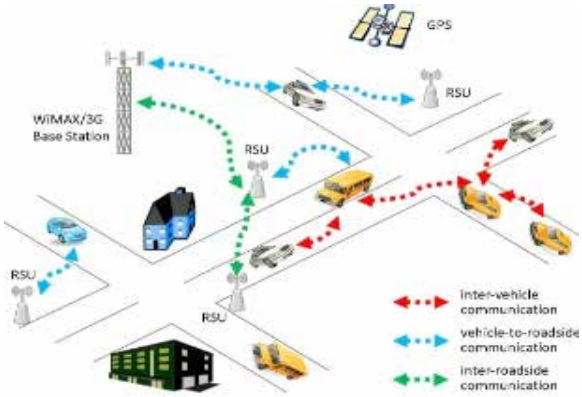

Fig. 1. VANET Architecture [8].

II. ARCHITECTURE

The main architecture of ITS includes mobile nodes (vehicles), base stations and core network. Fig. 1 shows the main parts of ITS architecture. Authors in [6] describe the main system components as follows: Application Unit (AU), On Board Unit (OBU) and Road Side Unit (RSU).

An OBU is a wave device usually mounted on-board a vehicle used for exchanging information with RSUs or other OBUs. The OBU connects to the RSU or to other OBUs through a wireless link based on the IEEE 802.11 p radio frequency channel, and is responsible for the communication with other OBUs or with RSUs.

The AU is the device equipped within the vehicle that uses the application provided by the provider using the communication capabilities of the OBU.

The RSU is a wave device usually fixed along the road side or in dedicated locations such as at junctions or near parking spaces. The RSU is equipped with one network device for a dedicated short range communication based on IEEE 802.11 p radio technology, and can also be equipped with other network devices so as to be used for the purpose of communication within the infrastructural network (Fig. 2-4). Typically the RSU hosts an application that provides services and the OBU is a peer device that uses the services provided. The application may reside in the RSU or in the OBU; the device that hosts the application is called the provider and the device using the application is described as the user.

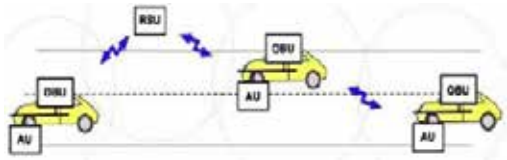

Fig. 2. RSU extends the range of the ad hoc network [6].

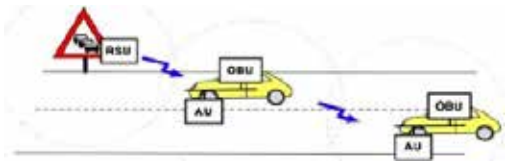

Fig. 3. RSU works as information source [6].

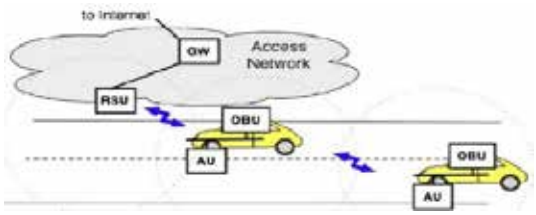

Fig. 4. RSU provides internet connectivity to the OBUs [6].

Fig. 4. RSU provides internet connectivity to the OBUs [6].

Each vehicle is equipped with an OBU and a set of sensors to collect and process the information then send it on as a message to other vehicles or RSUs through the wireless medium [6]. The main functions and procedures associated with RSUs are:

- Extending the communication range of the Ad-Hoc network by re-distributing the information to other OBUs and by sending the information to other RSU in order to forward it to other OBUs.
- Running safety Applications
- Providing Internet Connectivity to OBUs

However, this architecture could not support all requirements and applications, therefore to remedy the drawbacks of existing vehicular networks, new ITS network architecture is needed in order to support various services under dense vehicular environments. Authors in [3] described the framework of Heterogeneous Vehicular Networks (HVN) as follows:

As illustrated in Fig. 5, a HVN is composed of three main components, namely a Roadside Access Network (RAN), a Core Network (CN), and a Service Centre (SC). Service providers can often supply a variety of services to vehicular users through the SC. The CN is a key component of the HVN because it provide many important functions, such as aggregation, authentication, switching and so on.

Authors in [4] present an overview of integration of VANET and WiMAX. Architecture of VANET based on WiMAX consists of several logical network entities including subscriber station (SS) or mobile station (MS), access service network (ASN) and connectivity service network (CSN) as shown in Fig. 6, [9], [10]. The SS is for fixed device terminal and it is not required to support handover capability. The MS providing handover function is installed or embedded in car for VANET and it should support handover. ASN is a set of network functions to provide wireless connection and WiMAX system profile. These functions are including media access control for MS, transfer of authentication, authorization and accounting (AAA) messages by RADIUS, network discovery and selection, radio resource management and IP connectivity.

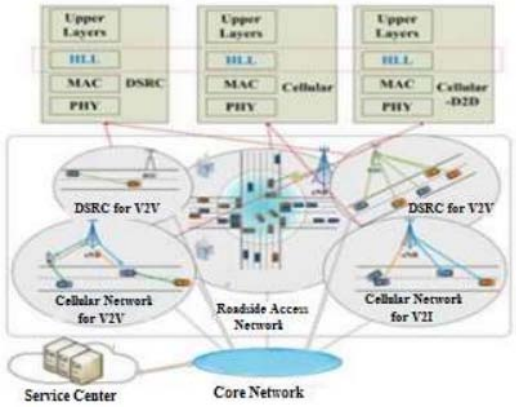

Fig. 5. Illustration of the unified HetVNET framework [3].

ASN is composed of BS and ASN gateway which connects several BSs based on cell planning. Local server is required for VANET application. The local server processes collected information from the MSs in vehicles and sends warning messages to MSs [4]. The messages type depend on features, dangers of collisions, accident information and so on. CSN is a set of network functions that provide IP Connectivity service to MS. CSN comprise network elements such as router, gateway for internetworking and various kind of servers. These servers are including DHCP for IP address allocation, AAA proxy/server, user database, home agent for mobility management, central server for VANET application and so on [11]. Authors in [12] proposed an integrated VANET-WiMAX network and they also simulated their proposed idea to verify the efficiency of 802.11 p and WiMAX integrated network. The main components of the WiMAX network are Base Station (BS), Access Service Network Gateway (ASN-GW) and Connectivity Service Network (CSN). In the integrated network, the Vehicle to Vehicle communication takes place through IEEE 802.11 p protocol and Vehicle to Infrastructure communication takes place through 802.16e protocol.

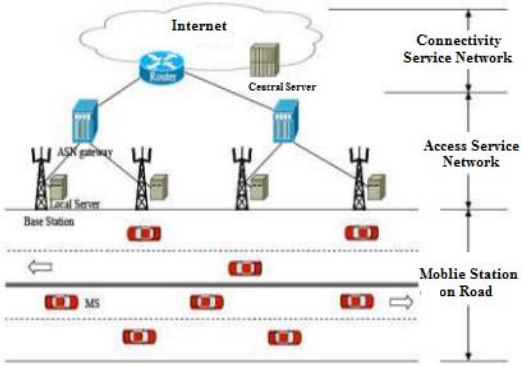

Fig. 6. VANET architecture with mobile WiMAX [4].

In order to evaluate the performance of both technologies, they carried out several simulations in NCTUNs network simulator and emulator and they concluded that integration of WiMAX and IEEE 802.11p offers better performances in terms of throughput, coverage range and packet loss.

III. COMMUNICATION TECHNOLOGIES

In previous sections we investigated the main components of the ITS and Vehicular Networks. These components need to be connected to each other in order to communicate together to send and receive data. As we mentioned, wireless technologies play an important role in these networks. We can use Wi-Fi (for short range communication), DSRC, WiMAX (for wide broadband communications), GSM, LTE, etc.

1. Types of Communications in VANET

A vehicle can communicate with other vehicles directly forming vehicle to vehicle communication (V2V) or communicate with fixed equipment next to the road, referred to as road side unit (V2R) which is also able to process special applications forming vehicle to infrastructure communication (V2I).

Vehicle to Vehicle communications gained attention from researchers, academics and industry leaders, especially in US, EU and Japan. According to its ability to improve road traffic safety, driving efficiency and to extend on board device horizons [13], vehicles communicate with other vehicles through OBUs forming a MANET, which allows communication between vehicles in a fully distributed manner with decentralized coordination. Vehicle communicates with another vehicle directly if there is a direct wireless connection available between them, forming a single hop vehicle to vehicle communication (V2V); when there is no direct communication

between them a dedicated routing protocol is used to forward data from one vehicle to another until it reaches the destination point, forming a multi-hop vehicle to vehicle communication [6].

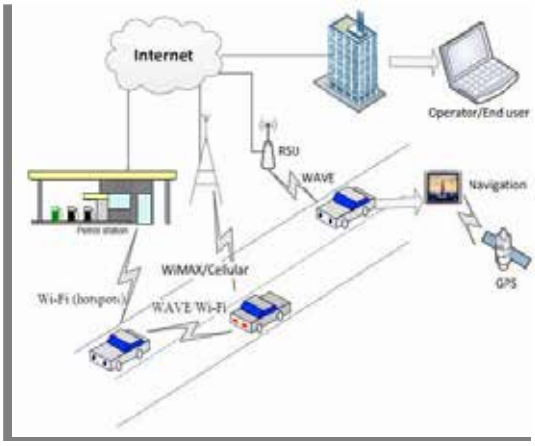

Fig. 7. Communications in VANET

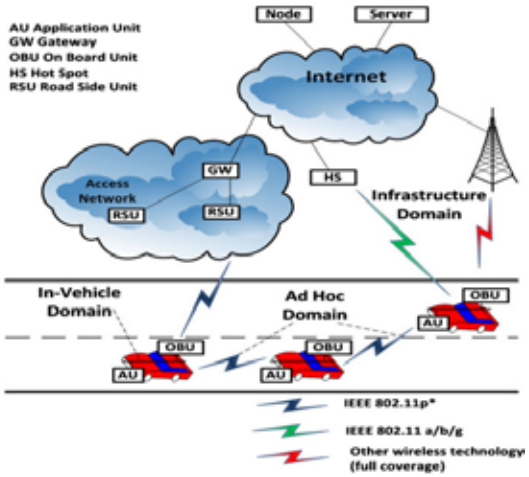

Fig. 8. Communication domains in VANET [14]

Vehicles communicates with an RSU in order to increase the range of communication by sending, receiving and forwarding data from one node to another or to benefit from the ability of the RSU to process special applications forming Vehicle to Infrastructure communication (V2I) [6].

2. Wireless Technologies in Vehicular Networks

Base on services, wireless network for VANET should support point to multipoint and point to point transmission mode. Information can be transmitted either event-driven or periodical. If information is periodically generated, interval time should be defined. Wireless communication technology should be satisfied with maximum duration of time to transmit as well as maximum distance between source and destination [4]. These technologies should support high data rate, Quality of Service and security.

Wireless technologies that are able to cover the requirements of these kind of networks are described as follows:

- DSRC: In 1999, Federal Communications Commission (FCC) allocated 75 MHz (from 5.850 GHz to 5.925 GHz) bandwidth for Dedicated Short Range Communication (DSRC) in vehicular environments [3]. DSRC is also called as Wireless Access in Vehicular Environments (WAVE) and it is based on IEEE 802.11 p which originated from IEEE 802.11a and was amended for low overhead operation in the DSRC spectrum. Primary purpose of DSRC is to enhance public safety applications, to save lives and to improve traffic flow by vehicle to vehicle and infrastructure to vehicle communications [4]. The U.S Department of Transportation (DOT) estimated that V2V communications based on DSRC can reduce up to 82% of all road crashes in U.S, potentially saving thousands of lives and billions of dollars [15]. DSRC can provide efficient real-time information exchange among vehicles without the need of pervasive roadside communication infrastructure [3]. DSRC provides 6-27 Mbps Data rate and 100-1000 meter radio coverage, it also provides very low latency (200 Micro Seconds) and supports point to point and broadcast communications [16]. The MAC layer in IEEE 802.11p has several significant drawbacks. For example, in vehicular scenarios, WAVE drops over 53% of packets sent according to simulation results [17]. Furthermore results in [18] show that throughput decreases to almost zero with 20 concurrent transmissions. Additionally, IEEE 802.11p does not support Quality of Service (QoS).
- Wi-Fi/WLAN: Wireless Local Area Network (WLAN) or wireless fidelity (Wi-Fi) can provide wireless access to enable V2V or V2I communications. Wi-Fi is a short range wireless local area network technology based on the IEEE 802.11 network standard [19] operating on radio frequency of 2.4 GHz offering high data rates of up to 600 Mbps (IEEE 802.11n). IEEE 802.11 standards can be applied to provide wireless connectivity; IEEE 802.11a works at 5 GHz and provides a data rate of 54 Mbps with a communication range of at least 38 m indoor and

a 140 m range for outdoor use [6]. IEEE 802.11g also provides the same data rate and covers the same range as IEEE 802.11a but works at 2.4 GHz [14]. IEEE 802.11b works at 2.4 GHz and provides a data rate of up to 11Mbps [20]. IEEE 802.11n operates on radio frequency of 2.4 and 5 GHz and provides a data rate of up to 600 Mbps with a communication range of at least 70 m indoor and a 600 m range for outdoor use. In addition, WLAN technologies might not be able to cover dense urban areas and the range of coverage will be really short compared to cellular technologies and WiMAX.

- WiMAX: Worldwide Interoperability for Microwave Access (WIMAX) is a long range wireless metropolitan area network technology based on the IEEE 802.16 for fixed and 802.16e for mobile access. WiMAX works at 10-66 and 2-11 GHz and provides up to 70 Mbps data rate and covers maximum range of 50 Km. WiMAX supports point to multipoint (PMP) as well as mesh mode. In the PMP mode, multiple subscriber stations (SSs) are connected to one base station (BS) where the access channel from the BS to the SS is called the downlink channel and the one from the SS to BS is called the uplink [12]. The purpose of WiMAX is deployment of broadband wireless access networks by using a global standards. WiMAX is also capable of supporting fast moving users in a mesh network structure. IEEE 802.16e is an amendment to the original WiMAX and provides a high data rate and covers a wide transmission range with reliable communications and high quality of service, which makes it suitable for those applications requiring these features such as multimedia, video and voice over internet protocol applications [6]. WiMAX achieves a high data rate of up to 35 Mbps using MIMO, with an orthogonal frequency division multiplexing (OFDM) and covers a transmission range of 15 Km [21]. Mobile WiMAX aims at maintaining mobile clients connected to a MAN while moving around [12]. Mobile WiMAX is a suitable wireless technology for networked vehicular applications because of its mobility support at vehicular speeds and its inherent wide coverage, which minimizes rate of handover and thus data loss due to disrupted communication [4].
- Cellular Communications: The concept of the cellular system is to reuse the limited frequency available for service [22]. Mobile cellular data are able to support vehicular services because they can provide wide geographical coverage and high data rate services to vehicular users. Cellular networks offer two transmission modes, namely unicast and multicast/broadcast, which can be utilized for V2I communications. Unicast can be used for both uplink and downlink message distribution, which is point to point communication between a vehicle and the base station, On the other hand broadcast is exclusively used for the distribution of downlink messages, which is point to multipoint transmission [3]. However, using cellular networks has its own drawbacks. The requirements of services that require stringent real time safety cannot always be guaranteed by cellular networks [3].

The main cellular technologies are GSM, GPRS, EDGE, UMTS, 3G and LTE. Global System for Mobile (GSM) communication considered to be one of the cellular system standards that provides a data rate of a maximum of 9.6 Kbps and is characterized as a second generation network (2G) [14]. Two frequency band are available for GSM 890-915 MHz for uplink and 935-960 MHz for downlink [6]. These frequency bands are divided into channels and the capacity of each channel is 200 KHz [22]. General Packet radio service (GPRS) also known as 2.5 G [23] is an evolved version of GSM, it provides a data rate of up to 170 Kbps [24] and it operates on 1710-1785 MHz for uplink and 890-915 MHz for downlinking and uplinking respectively [6]. Enhanced Data rates for GSM Evolution (EDGE); also known as 2.75 G are evolution of GPRS which provide a peak data rate of 384 Kbps [20]. The Universal Mobile Telecommunication System (UMTS) provides a data rate of up to 2 Mbps. 3G is an ITU specification for the third generation of mobile communications technology. 3G promises increased bandwidth, up to 384 Kbps when a device is stationary or moving at pedestrian speed, 128 Kbps in a car, and 2 Mbps in fixed applications [ITUT]. Long Term Evolution (LTE) is the next step forward in cellular 3G services. LTE is a way for cellular communications to operate at that high data rate and it is based on a 3GPP standard that provides for a downlink speed of up to 150 Mbps and an uplink speed of up to 50 Mbps [25]. The bandwidth of LTE is 20 MHz and supports a maximum mobile speed of 350 Km per hour. LTE is envisioned to well support V2I communications. Especially, in the initial deployment stage of vehicular networks, LTE

is expected to play a crucial role in supporting vehicular services. For instance, LTE can support up to 1200 vehicles per cell in rural environments with an uplink delay under 55 milliseconds [26].

3. Handover between VANETs and Cellular Networks

As there are currently several ways of wireless access to support vehicular communications, it is necessary to make a seamless handover decision to guarantee QoS of communications for a vehicle moving in the regions covered by more than one access networks. How to make handover decision is a challenging problem. It requires that demands of vehicles should be satisfied while the overall network performance is optimized. Several internetworking mechanism for combining WLANs and cellular networks into integrated wireless environments have been proposed [35]. Authors in [36] proposed vertical handoff decision (VHD) method that simply estimates the service quality for available networks and selects the network with the best quality but as it is shown in [36] the known vertical handoff algorithms are not adequate in coordinating the QoS of many individual mobile vehicles, so, authors in [37] proposed the VHD controllers (VHDCs) to tackle this problem and in [35] a controller is provided to operate an algorithm which guarantees the performance of optimized handover decision. The controller collects real time traffic information, then it informs the vehicle of an appropriate access point. The optimization is a well-defined objective function which include consideration of a data rate overall networks and load balancing across access points. Each vehicle's demand should be satisfied to ensure their fairness to a certain extent. The considered framework for the study of handover is shown in Fig. 9, authors considered a section of an expressway in Shanghai, China. They introduce the following three core components of the framework to highlight the characteristics for internet access: Infrastructure, Vehicle and Controller.

The controller is connected to BSs, RSUs and Internet backbone. It allocates the network radio resources and services demands requested to vehicles based on the real time road traffic information. Based on the above framework, a vehicular heterogeneous wireless network which includes VANET and cellular network is formed. Vehicles that move in the highway may be covered by more than one access network. Due to vehicular mobility and characteristics of networks, vehicles may experience weak or degrade received signal strength (RSS) from their current access point (RSU or BS).

If any vehicle wants to get service or maintain an underway service, an appropriate access point (RSU or BS) needs to be chosen. This introduces a problem about handover. With a proper handover, the continuous service and QoS experience of vehicle can be significantly enhanced. Authors in [35] considered following two cases of network selection:

1) While in service at an RSU, the RSS for vehicle has dropped below a specified threshold (e.g., car A in Fig. 9).

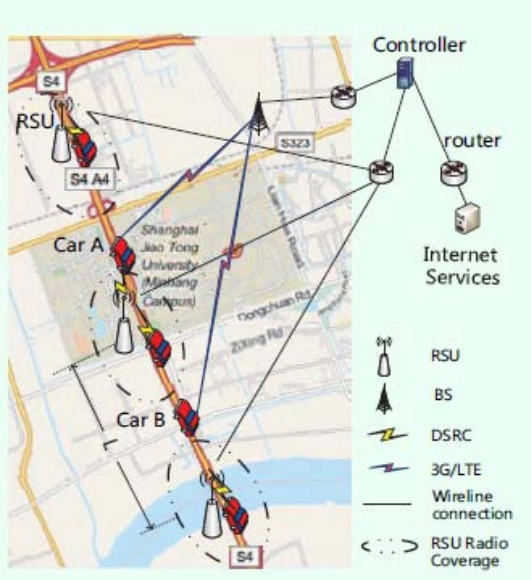

Fig. 9. The considered framework for the study of handover

2) While in service at a BS, the RSS from the next RSU has just exceeded a specified threshold (e.g., car B in Fig. 9).

Then, how can the controller find appropriate access points for vehicles. After the collection of real time road traffic information, the controller optimizes the well-defined joint objective function. Then, proper access points are found and the performance of internet access is improved with the heterogeneous network [35].

However, with an ever increasing number of vehicles, LTE networks are easily overloaded [3] and several problems need to be solved before LTE systems can be widely used for V2I communications [7]. Authors in [27] show that DSRC in conjunction to IEEE 802.11p exhibits poor performance in the event of a large number

of vehicles, WiMAX and Wi-Fi also have their own drawbacks and benefits, and to remedy the drawbacks of existing vehicular networks, new ITS network architecture is needed in order to support various services under dense vehicular environment [3].

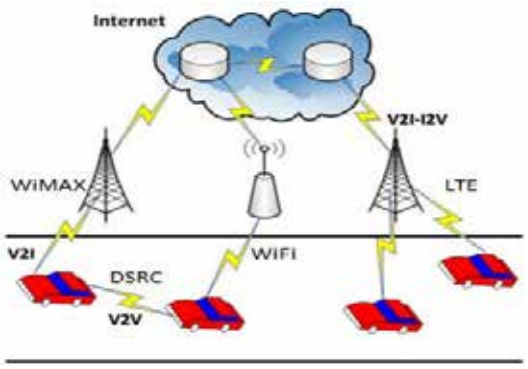

Fig. 10. Combined DSRC, Cellular, Wi-Fi and WIMAX [7].

IV. SECURITY ISSUES IN VANETS

Safety in VANETs is crucial because it affects the life of people. It is essential like that the vital information cannot be modified or deleted by an attacker. Securing VANETs systems must be able also to determine the responsibility of drivers while maintaining their privacy. Communications passing through a vehicular network as well as information about the vehicles and their drivers must be secured and protected to ensure the smooth functioning of intelligent transportation systems.

1. Attacks

VANETs suffer from various attacks and in this paper we are concentrating on attacks perpetrated against the message itself rather than the vehicle, as physical security is not in the scope of this paper.

1.1. Denial of Service attack

This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application's information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles [38], [39], [40], and [41].

Authors in [38] discussed a solution for DoS problem and saying that the existing solutions such as hopping do not completely solve the problem, the use of multiple radio transceivers, operating in disjoint frequency bands, can be a feasible approach but even this solution will require adding new and more equipment to the vehicles, and this will need more funds and more space in the vehicle. Authors in [42], proposed a solution by switching between different channels or even communication technologies (e.g., DSRC, UTRA-TDD, or even Bluetooth for very short ranges), if they are available, when one of them (typically DSRC) is brought down.

1.2. Message Suppression Attack

An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time[39].

The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points [43]. For instance, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive the warning and forced to wait in the traffic.

1.3. Fabrication Attack

An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else. This attack includes fabricate messages, warnings, certificates and identities [39], [41], [43].

1.4. Alteration Attack

This attack happens when attacker alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted [39]. For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested [43].

1.5. Sybil Attack

This attack happens when an attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route [39],[44]. Sybil attack depends on how cheaply identities

can be generated, the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the system treats all entities identically. For instance an attacker can pretend and act like a hundred vehicle to convince the other vehicles in the road that there is congestion, go to another rout, so the road will be clear.

2. Attackers

2.1. Selfish Driver

The general idea for trust in Vehicular Network is that all vehicles must be trusted initially, these vehicles are trusted to follow the protocols specified by the application, some drivers try to maximize their profit from the network, regardless the cost for the system by taking advantage of the network resources illegally [39]. A selfish driver can tell other vehicles that there is congestion in the road, so they must choose an alternate route, so the road will be clear for it.

2.2. Malicious Attacker

This kind of attacker tries to cause damage via the applications available on the vehicular network. In many cases, these attackers will have specific targets, and they will have access to the resources of the network [38], [39].

2.3. Pranksters

Include bored people probing for vulnerabilities and hackers seeking to reach fame via their damage [39]. For instance, a prankster can convince one vehicle to slow down, and tell the vehicle behind it to increase the speed.

V. VEHICULAR NETWORKS APPLICATIONS

Applications of Vehicular networks are divided into 2 categories; safety services and non-safety related services, Vehicular Networks are nowadays widely identified enablers for improving traffic safety and efficiency.

The applications regarding safety are strictly tied to the main purpose of vehicles; moving from a point till to destination [28]. Car collisions are currently one of the most frequent dead causes, so safety applications convey safety critical information based on sensor data from other vehicles or RSUs to report and avoid emergencies [14, 29]. Examples include a sudden brake warning sent from a remote preceding car, information about road conditions and maintenance, accident annunciations, emergency brake light, collision warning, etc.

Non-safety applications include entertainment and online connectivity and they typically obtain data on-demand such that a node requests information of interest [14, 30]. Examples of non-safety applications are electronic payments, toll services, file sharing, audio or video streaming, parking space locator, map updates, Internet surfing, online gaming, etc. A key aspect of these applications is the availability of high bandwidth and scalable Internet connectivity [31].

Intelligent Transportation systems, are also considered to be a green technology. In order to reduce the amount of CO2 vehicles may corporate with each other and road infrastructures. The information exchange will make drivers aware of possible stops ahead, such as stops during a red light period [32]. Recent research [33] has shown that vehicular communications can be used to advise drivers in order to optimize their driving and avoid unnecessary stops to reduce fuel consumption and CO2 emissions [32].

Moreover, in [34] authors briefly present how mobility players and enablers (driver, vehicle and road network) influence energy consumption and pollutant emissions and they propose a number of recommendations and future research directions in the area of Green ITS.

VI. CONCLUSION

Vehicular communications is one of the research areas in the field of computer networks and telecommunication engineering. It has emerged by improvement and convergence in computer science and telecommunication. There are challenges and problems according to this field of research like, security issues, clustering, QoS provisioning, routing, message dissemination, MAC layer issues etc. In this paper we provided a survey on vehicular networks and presented an overview of architecture, applications and communication technologies as the main aspects of VANETs which helps the researchers to understand the main and basic concepts of these networks.

REFERNCE

[1] An. S. H, Lee. B. H, Shin. D. R, 2011. A survey of Intelligent Transportation System. Third International Conference on Computational Intelligence, Communication Systems and Networks,

[2] Kastell. K. A, 2013. Network planning for Intelligent Transportation Systems Based on Existing Wireless Networks. 5th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshop, Almaty, Kazakhstan.

[3] Zheng. K, Zheng. Q, Xiang. W and Zhou. Y, June 2015. Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions. Communications Surveys & Tutorials, IEEE, vol. 17, no. 4 pp.2377 – 2396

[4] Gandhi. A, Jadhav. B. T, 2012. Role of Wireless Technology for Vehicular Network. International Journal of Computer Science and Information Technologies, vol.3, no.4, pp. 4823-4828, 2012.

[5] Shrivistava. P, Ashai. S, Jaroli. A, Gohil. S, Aug. 2012. Vehicle to Road-Side-Unit Communication Using Wimax. International Journal of Engineering Research and Applications, vol.2, no.4, pp. 1653-1655.

[6] Al-Sultan. S, Al-Doori. M, Al-Bayatti. A. H and Zedan. H, Jan. 2014. A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications, vol. 37, pp. 380-392.

[7] Araniti. G, Campolo. C, Condolusi. M, Iera. A, Molinaro. A, May. 2013. LTE for Vehicular Networking: a survey. IEEE Commun. Mag., vol. 51, no. 5, pp. 148-157.

[8] Sahasrabudhe. M. S, Chawla. M, 2014. Survey of Applications based on Vehicular Ad-Hoc Network (VANET) Framework. International Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 3937-3942.

[9] WiMAX Forum, Feb. 2009. Network Architecture Stage 2: Architecture Tenets, Reference Model and Reference Points, Part 1- Release 1.0 Version 4.

[10] Etemad. K, Oct. 2008, Overview of Mobile WiMAX Technology and Evolution. IEEE Comm. Magazine, vol. 46, no. 10, pp. 31-40, October.

[11] Kim. S, Kim. H, Jin. J, Lee. S, "A new approach for vehicle accident prevention on the highway using Mobile WiMAX", Wireless Technology Department, Central R&D laboratory, KT 17 Woomyeon-Dong, Seocho-Gu, Seoul, 137-792.

[12] Devarajan. V, Gunasundari. R, Karthik. T, Rajasekaran. V, Feb. 2013, Integration of VANET-WiMAX Network. Journal of Information and Communication Technologies, vol. 3, no. 2, pp. 695-700.

[13] Luo. J, Hubaux. J, 2004. "A survey of inter vehicle communication," School of computer and communication sciences, Laussane, Switzerland.

[14] Olariu. S, Weigle. S, 2009. Vehicular Networks: from theory to practice, 1st ed, Chapman & Hall.

[15] Kenney. J, 2011. Dedicated Short Range Communication (DSRC) standards in the united states. Proceedings of the IEEE, vol. 99, no. 7, pp. 1162-1182.

[16] Guo. J, 2006. "Vehicle Safety Communications in DSRC," 6th U.S Army winter workshop.

[17] Bilstrup. K, Uhleman. E, Storm. E, Bilstrup. U, 2008. Evaluation of the IEEE 802.11p MAC Method for Vehicle to Vehicle Communication. Vehicular Technology conference, (pp. 1-5)

[18] Stibor. L, Zang. Y, Reumerman. H, 2007. Evaluation of communication distance of broadcast messages in vanet using IEEE 802.11p. proceedings of the IEEE Wireless Communications and Networking Conference, (pp. 254-257).

[19] IEEE standard for information technology telecommunications and information exchange between systems Local and metropolitan area network specific requirements. 2007. part 11: Wireless Lan Medium Access Control (MAC) and Physical Layer Specifications.

[20] Moustafa. H, Zhang. Y, 2009. Vehicular networks: techniques, standards, and applications. CRC Press

[21] Vaughan-Nichols. S, 2008. Mobile Wimax: The Next Wireless Battle Ground. Computer, vol. 41, no. 6, pp. 16-18, June 2008.

[22] Rahnema. M, 1993. Overview of GSM system and protocol architecture. IEEE Communications Magazine, vol. 31, no.4, pp. 92-100.

[23] Jakubiac. J, Koucheryavy. Y, 2008. State of the art and research challenges for vanet. IEEE 5th Consumer Communication and networking conference, Las Vegas, Nevada, U.S.A, 2008.

[24] G. Brasche, B. Walke, "Concepts, services and protocols of the new GSM phase 2+ general packet radio service," IEEE communication magazine, vol. 35, no.8, pp. 94-104, 1997.

[25] Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description, 3GPP TR 36.201.

[26] "Intelligent transport systems (ITS); framework for public mobile networks in cooperative ITS (C-ITS)," ETSI Technical Committee Intelligent Transport System, Tech. Rep. 102962, 2012.

[27] Han. C, Dianati. M, R. Tafazolli, Kernchen. R, Chen. X, 2012. Analytical study of the IEEE 802.11p MAC sublayer in vehicular networks. IEEE Trans. Intell. Transp .Sys., vol.13, no.2, pp. 873-886.

[28] Vegni. A, Biagi. M, Cusani. R, 2013. Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks. Vehicular Technologies-Deployment and Applications, L. Gelordano, Ed. InTech.

[29] H. Hartenstein, H. Fuler, M. Mauve, W. Franz, "Simulation Results and Proof-ofoConcept Implementation of the FleetNet Position-Based Router," Personal Wireless Communications, PWC (2003), Venice, Italy, Sep. 2003, pp. 192197.

[30] IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks specific requirements, Part 11: Wireless LAN Medium Access Control and Physical Layer (PHY) Specifications, 2007. [Online].Available: https://standards.ieee.org/develop/project/802.11.html, [Accessed: Dec. 8. 2015]

[31] Mojela. L. S, Booysen. M. J, 2013. On the use of WIMAX and Wi-Fi to provide in-vehicle connectivity and media distribution. IEEE International Conference on Industrial Technology, Cape Town, South Africa, 25-28 (pp. 1353-1358).

[32] Suthaputchakun. C, Zhili. S, Dianati. M, 2012. "Applications of Vehicular Communications for reducing Fuel Consumption and Co2 Emission: The State of the Art and Reseach Challenges," IEEE Communications Magazine, Vol. 50, no. 12, pp. 108-115.

[33] Katsaros. K, Kernchen. R, Dianati. M, Rieck. D, Zinoviou. C, 2011. Application of vehicular communications for improving the efficiency of traffic in urban areas. Wireless Communications and Mobile Computing, vol. 11, no. 12, pp. 1657-1667.

[34] P. M. d'Orey, M. Ferreira, 2014. "ITS for Sustainable Mobility: A Survey on Applications and Impact Assessment Tools," IEEE Transactions on Intelligent Transportation Systems, vol. 15, no. 2, pp.477-493.

[35] Bi. S, Chen. C, Du. R, Guan. X, 2014. Proper Handover between VANET and Cellular Networks. IEEE 80th Vehicular Technology Conference (pp. 1-5).

[36] Nasser. N, Hasswa. A and Hassanein. H, 2006, Handoffs in fourth-generation multi-network environment," IEEE Commun. Mag., vol.44, no.10, pp. 96-103.

[37] Lee. S, Seriram. K, Kim. K, Kim. Y, and Golmie. N, 2009, Vertical Handoff decision algorithms for providing optimized performance in heterogeneous wireless networks IEEE Trans. Vehicular Technology, Vol. 58, No. 2, pp. 865-881.

[38] Raya. M, Papadimitratos. P, Hubaux. J, Oct. 2006, Securing Vehicular Communications. IEEE Wireless Communications, vol. 13.

[39] Parno. B and Perrig. A, 2005, Challenges in securing Vehicular Networks. Proc. Of Hotnets-IV.

[40] Aad. I, Hubaux. J, Knightly. E, Aug. 2008, Impact of Denial of Service Attacks on Ad-Hoc Networks. Networking IEEE/ACM Transactions on Volume 16.

[41] Raya. M, Hubaux. J, 2005. The Security of VANETs. Proceeding of the 2nd ACM International Workshop on Vehicular Ad-hoc Networks.

[42] Raya. M, Hubaux. J, 2005. The Security of Vehicular Ad-hoc Networks. Proc. Of the 3rd ACM workshop on security of ad-hoc and sensor networks.

[43] Rahman. S, Falaki. H, Security and Privacy for DSRC-based Automotive Collision Reporting.

[44] Douceur. J, 2003. The Sybil Attack. First International Workshop on peer-to-peer Systems. Springer, First Ed. USA.