Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Shifting VANET to Cloud - Survey

Ms. Ashwini Abhale*, Mr. Sumit Khandelwal, Prof. Uma Nagaraj

Assistant Professor

Department of Computer Engineering,

MIT Academy of Engineering, Alandi (D), Pune, India

Abstract - Vehicular networking has become a significant research area due to its specific features and applications such as standardization, efficient traffic management, road safety and infotainment. Vehicles are expected to carry relatively more communication systems, on board computing facilities, storage and increased sensing power. Hence, several technologies have been deployed to maintain and promote Intelligent Transportation Systems (ITS). Recently, a number of solutions were proposed to address the challenges and issues of vehicular networks. Vehicular Cloud Computing (VCC) is one of the solutions. VCC is a new hybrid technology that has a remarkable impact on traffic management and road safety by instantly using vehicular resources, such as computing, storage and internet for decision making. This paper we focusing on the various attack in vehicular ad-hoc network. Also, we focus Challenges in designing vehicular cloud.

Keywords— Vehicular Cloud Computing (VCC), Security, Privacy, Attacks.

I. INTRODUCTION

1. Vehicular Ad-hoc Network

Vehicular ad hoc networks have recently received considerable attention. A vehicular ad hoc network (VANET) is used to provide convenient wireless network services. The wide deployment and evolution of wireless communication systems have changed human lives by offering easiness and flexibility in using Internet services and various applications. Researchers have abstracted the idea of Vehicular Ad hoc Networks (VANETs), in which vehicles, equipped with wireless communication devices, positioning systems, and digital maps, act as intelligent machines that communicate for safety and comfort purposes.[1]

A typical car or truck today is likely to contain at least some of the following devices: an on-board computer, a GPS device, a radio transceiver, a short-range rear collision radar device, and a camera, supplemented, in high-end models, by a variety of sophisticated sensing devices. VANETs allow vehicles to connect to roadside units (RSUs), which are fixed infrastructure that are equipped with powerful computing devices and installed at different locations in a city.[2]

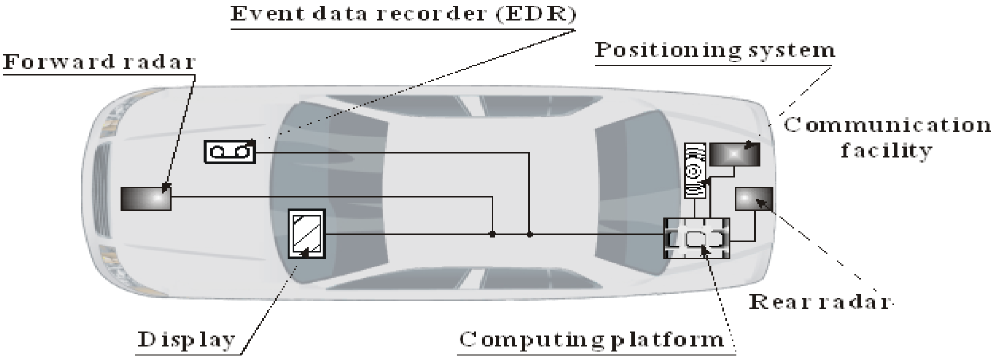

Figure 1.1: Modern Vehicle

In addition, when VANET is installed in vehicles, they can exchange traffic information [3][4]. VANET is used primarily to ensure traffic safety and improve traffic efficiency [1][2] by transmitting messages concerning traffic information and road conditions. Hence, accidents or traffic jams can be avoided. IN a *Vehicular Ad hoc Network* (VANET), vehicles communicate with each other through *Dedicated Short Range Communication* (DSRC) wireless devices. Major goal is to improve road safety and transportation efficiency by exchanging data between vehicles.

The VANETs provides both roadside-to-vehicle (RVC) or Vehicle-to-Infrastructure (V-I) communication (RVC) and inter-vehicle communication (IVC) or Vehicle-to-Vehicle (V-V) Communication capability. V-V works like a multi-hop mobile ad hoc network (MANET) with its own unique characteristics. In traditional VANET architectures, nodes are all treated equally and may participate in packet forwarding. However, vehicles are different in reality. Some vehicles are not willing to forward packets for others, and their wireless devices might be shut down by the driver at any time.

Another unique feature of urban VANETs is that traffic lights have great influence on the vehicle movement, so vehicles are moving like clusters. These features should be considered in the VANET architecture design. RSUs are Routers in VANET. And RSUs are also able to link to a network backbone to provide many diversified services. Different approaches have been considered for RSUs designing such as RSUs may be standalone, some others wired to each other to form a backbone; others are only wired to few neighboring RSUs; while some are hybrid RSUs. [1][2]. All RSUs are considered to be connected over fixed communication links, and distance between them is 2 to 5 km.

2. Cloud Computing and Mobile Cloud Computing

Mobile Cloud Computing is a recent emerging paradigm in the information technology arena. A formal definition of CC: "1) Cloud Computing is an Internet-based computing whereby Information, IT resources, Software applications, are provided to computers and mobile devices on-demand 2) The Storing and Accessing of applications and computer data often through a web browser rather than running installed software on your personal computer or office server" The Mobile Cloud Computing Forum defines MCC as follows [18] "Mobile Cloud computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers". Mobile cloud computing is based on the fact that, without financing in infrastructure, businesses can function by renting the infrastructure and the necessary software for their organization. Several features in Mobile Cloud Computing related to providing hardware and software provisions are low cost High-speed Internet, virtualization and advances in parallel and distributed computing and distributed databases, It gives the ability to pay for use of computing resources on a short-term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by releasing resources (e.g. machines and storage) when they are no longer useful.

The Architecture of Mobile Cloud Computing is shown in Fig 2. It basically consists of three layers Application layer (SaaS), Platform Layer (PaaS), and the Infrastructure Layer (IaaS).

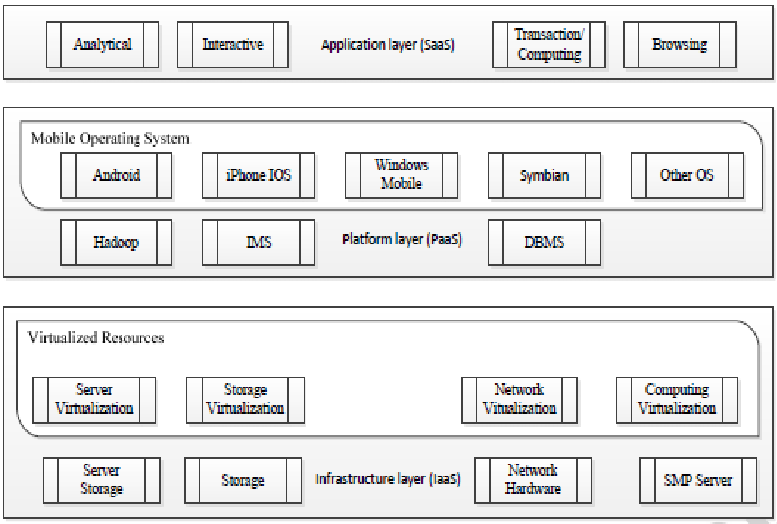

Fig 2. Architecture of Mobile Cloud Computing

Infrastructure as a Service (IaaS): Several types of virtualization occur in this layer. Among the other resources, computing, network, hardware and storage are also included. In the bottom layer of the framework, infrastructure devices and hardware are virtualized and Provided as a service to users to install the operating system (OS) and operate software applications. Therefore, this layer is named Infrastructure as a Service (IaaS). Amazon Web Services (AWS) is a very good example of this category where Amazon provides its customers computing resources through its Elastic Compute Cloud (EC2) service and storage service through both Simple Storage Service (S3) and Elastic Book Store (EBS).

Platform as a Service (PaaS): In PaaS, mobile operating systems such as Android, iPhone, Symbian and other OS, as well as database management and IMS are included in this section. This layer contains the environment for distributing storage, parallel programming design, the management system for organizing distributed file systems and other system management tools for cloud computing. Program developers are the primary clients of this platform layer. Google AppEngine and Microsoft Azure are good example of that category.

Software as a Service (SaaS): Analytical, interactive, transaction and browsing facilities are included in the Application layer. SaaS delivers several simple software programs and applications as well as customer interfaces for the end users. Thus, in the application layer, this type of services is called Software as a Service (SaaS). By using the client software or browser, the user can connect services from providers via the internet and pay fees according to their consumed services, such as in a pay as you go model. IBM is a good example of this category.

3. Vehicular Cloud Computing

The vast number of vehicles on streets, roadways and parking lots will be treated as plentiful and underutilized computational resources, which can be used for providing public services. Every day, many vehicles, spend hours in a parking garage, driveway or parking lot. The parked vehicles are a vast unexploited resource, which is currently simply wasted. These features make vehicles the perfect candidates for nodes in a cloud computing network. Some vehicle owners may agree to rent out excess on board resources, similar to the holders of huge computing and storage facilities who rent out their excess capacity and benefit economically. Using self-organized autonomous resources, vehicles will serve on demand in real time to resolve large, serious problems of unexpected occurrences. The new vehicular clouds will help resolve technical challenges and contribute to complex transportation systems with their evolving behavior.

Thus, there are two key distinguishing characteristics that set the VC2 apart from that the conventional cloud: mobility, agility and autonomy.

II. HOW VANET WORKS

Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today [4], these vehicles will require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for range can reach 1 KM, this communication is an Ad Hoc communication that means each connected node can move freely, no wires required, the routers used called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets, all the information about the vehicle like keys, drivers identity, trip details,
speed, rout etc.

So many Routing algorithms are available for VANET such as AODV, DSR etc. basically each protocol works in two phase. In phase I, it will identify neighbors then creation of infrastructure and broadcast of infrastructure. In phase II, actual data is transferred. In AODV, phase I & II executed parallel while in DSR, Phase I executed first and then Phase II. Because of these AODV is dynamic and more suitable for VANET.

So many simulations are available for VANET.

A VANET simulator has two main components: a network component, capable of simulating the behavior of a wireless network, and a vehicular traffic component, able to provide an accurate mobility model for the nodes of a VANET. Depending on the simulation type, the simulator can contain other components as well. Fig 3. Shows the connection between Traffic simulator and Network simulator.

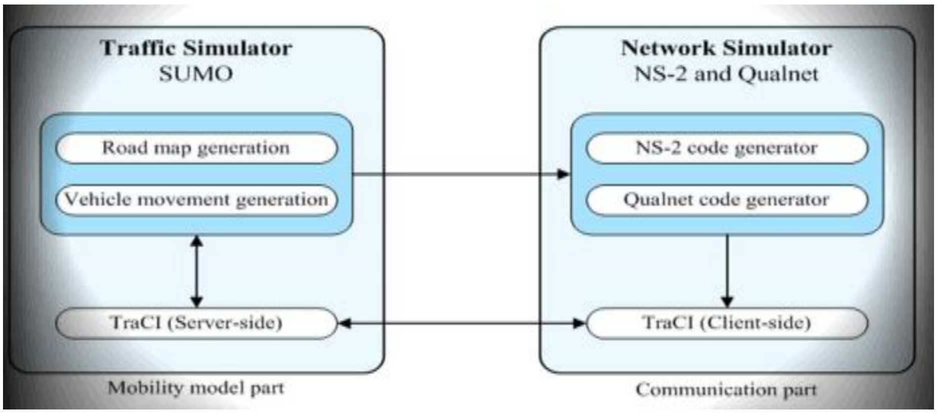

Fig. 3 Connection between Traffic Simulator and Network Simulator

III. SECURITY And PRIVACY

Security and privacy are two major concerns when some resources are shared between more than two users. For sharing resources two constraints should be preserved. First, Security and Privacy of Vehicle's Owner means producer should be maintained. And Second, Security and Privacy of consumer who rent resources should be maintain [2]. In VANET different attacks are possible such as, Denial of Service attack, Fabrication Attack, Alteration Attack, Replay Attack, Message Suppression Attack, Replay Attack, Sybil Attack. Again, different attackers in VANET are such as, Selfish Driver, Malicious Attacker [18] To overcome that some security requirements are should be considered such as Authentication, Availability, Non-repudiation, Privacy, Real-time constraints, Integrity, Confidentiality [5].

Some solution to secure VCC:

The main motivation of VANETs is safety applications thus safety-related messages are major information in the network. Based on emergency level there are three types on safety messages. 1) Public Traffic Condition Information for e.g. traffic jams condition which indirectly prevents some accidents. 2) Cooperative safety applications. Vehicles exchange messages in cooperative accident avoidance applications. This is real time communication. 3) Liability messages. These messages are generated after an accident happens. [7][8].

Safety messages includes the time-stamp, geographic position, speed, percentage of speed change since last message, direction, acceleration, and percentage of acceleration change since last message. The safety message will append information such as public traffic condition and accidents etc.

IV. LIMITATIONS/ CHALLENGES

The challenges in Vehicular Networks are as follows *Mobility:* The basic idea of Ad Hoc networks is that each node is in the network is mobile. In VANET the speed of each node is high. Connection is created for short time and terminated also. These vehicles never met again. So, Mobility Security is hard challenge.

Volatility: Vehicular networks lacks the relatively long life context, so personal contact of user's device to a hot spot will require long life password and this will be impractical for securing VC.

Privacy VS Authentication: TO avoid Sybil attack we have to give identity to each vehicle, but this solution will not be appropriate for the most of the drivers who wish to keep their information protected and private

Privacy VS Liability: Liability will give a good opportunity for legal investigation and this data can't be denied (in case of accidents), in other hand the privacy mustn't be violated and each driver must have the ability to keep his personal information from others (Identity, Driving Path, and Account Number for toll Collector etc.).

Network Scalability: The scale of this network in the world approximately exceeding the 750 million nodes [4], and this number is growing, another problem arise when we must know that there is no a global authority govern the standards for this network, for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles is deferent from the BMW one.

Bootstrap: At this moment only few number of cars will be have the equipment required for the DSRC radios, so if we make a communication we have to assume that there is a limited number of cars that will receive the communication, in the future we must concentrate on getting the number higher, to get a financial benefit that will courage the commercial firms to invest in this technology.

Challenges in Vehicular Cloud Formation:

Flexible mobile architecture: One of the main characteristics of VC is the mobility of the nodes which directly effects on the available computational capabilities and storage resources, for example, the number of parked vehicles in the parking is not constant.

Robust architecture: The fundamental building blocks and structures that compose VC should be engineered and designed to face the structural stress of the unstable working situation.

Service-based network architecture: The existing layered network architecture, for example TCP-IP stack, is not adequate to support ongoing evolving technologies and applications. Hence, It needs to use the service-oriented and component-based network architecture with sufficient learning opportunities and monitoring facilities in order to cope with reusable and extensible applications and resources, which require to be largely deployed as common services available in VC environments.

Scopes of Services: New emerging services can be possible of wise and technically controlled uses of VCC.

V. APPLICATIONS

VANET applications can be divided into two major categories. Applications that increase vehicle safety on the roads are called safety applications. Applications that provide value added services, for example, entertainment, are called user applications. In this article we concentrate only on applications with an important wireless networking component [1][2].

Safety applications

Safety applications can decrease significantly the number of road accidents. According to some studies [6], 60 percent of accidents could be avoided if a driver were provided with a warning half a second before the moment of collision. There are three major scenarios in which safety applications could be very useful.

• *Accidents:* Vehicles travel at a high speed on major roads. This gives drivers very little time to react to the vehicle in front of them. If an accident occurs, the approaching vehicles often crash before they can come to a stop. Safety applications could be used to warn cars of an accident that occurred further along the road, thus preventing a pile-up from occurring. A safety application also could be used to provide drivers with early warnings and prevent an accident from happening in the first place.

• *Intersections:* Driving near and through intersections is one of the most complex challenges that drivers face because two or more traffic flows intersect, and the possibility of collision is high. In 2003, according to the U.S. Department of Transportation (DoT), intersection crashes accounted for more than 45 percent of all reported
crashes and 21 percent of fatalities, that is, 9213 fatalities

occurred at intersections in the United States [8]. The number of accidents would decrease if a safety application warned the driver of an impending collision. The driver then could take action to prevent it.

• *Road Congestion:* Safety applications also could be used to provide drivers with the best routes to their destinations [9]. This would decrease congestion on the road and maintain a smooth flow of traffic, thus increasing the capacity of the roads and preventing traffic jams. It also could have the indirect effect of reducing traffic accidents [10] because drivers would be less frustrated and more inclined to follow traffic regulations.

User Applications

User applications can provide road users with information, advertisements, and entertainment during their journey. Two basic user-related applications are described below.

• *Internet Connectivity:* Constant Internet access has become a daily requirement for many of us and because many user applications also require Internet connectivity, providing this facility to vehicle occupants and other VANET applications is important. Moreover, this means that the usual business framework will be present seamlessly in vehicles, without a requirement for specific redevelopment.

• *Peer-to-Peer Applications:* To alleviate boredom, peer-to-peer applications also are an interesting idea for VANETs. Passengers in the vehicles could share music, movies, and so on and chat with each other and play games. They also could stream music or movies from special servers during long journeys.

VI. CONCLUSION

In this paper, we addressed the security and challenges of a novel perspective of VANETs, i.e. Shifting VANETs to clouds. Vehicular Ad-hoc Networks (VANETs) will start becoming deployed within the next decade. Among other benefits, it is expected that VANETs will support applications and services targeting the increase of safety on the road, and assist in improving the efficiency of the road transportation network. However, several serious challenges remain to be solved before efficient and secure VANET technology becomes available, one of them been efficient authentication of messages in a VANET. There is a significant body of research work addressing this issue, however, while progress has been made, the challenge is still far from having been resolved and reliable and secure systems ready for deployment becoming available. Form the above limitations discussed; there is a scope for further research to address various issues in the design and implementation of privacy system and its application for the VANET with Cloud, in general, and more specifically to the efficient and multi-level privacy-preserving communication protocol scheme for VANET with Cloud..

REFERENCES

[1] Khaleel Mershad, and Hassan Artail, "Finding a STAR in a Vehicular Network", *IEEE Intelligent transportation systems magazine*, pp. 55-68, 2013.

[2] S.Olariu, I. Khalil, and M. Abuelela, "Taking VANET to the clouds," *Int. J. Pervasive Comput. Commun*., vol. 7, no. 1, pp. 7-21, 2011.

[3] Fleming B. Smarter and Safer Vehicles. Vehicular Technology Magazine, *IEEE* 2012;7:4-9.

[4] Gabauer DJ, Gabler HC.Comparison of roadside crash injury metrics using event data recorders. Accident Analysis & Prevention. 2008, 548-58.

[5] Mousannif H, Khalil I, Al Moatassime H. Cooperation as a Service in VANETs. *Journal of Universal Computer Science* 2011;17:1202-18.

[6] Olariu S, Hristov T, Yan G. The next paradigm shift: From vehicular networks to vehicular clouds. In: S. SINTRONES. 2009.

[7] Olariu S, Khalil I, Abuelela M. Taking VANET to the clouds, *International Journal of Pervasive Computing and Communications.* 2011 ; 7:7-21.

[8] Aijaz A, Bochow B, Dotzer F, Festag A, Gerlach M, Kroh R, et al. Attacks on inter vehicle communication systems-an analysis. 2006.

[9] Lochert C, Scheuermann B, Caliskan M, Mauve M, The feasibility of information dissemination in vehicular adhoc networks. IEEE; 2007. p. 92-9.

[10] Liu Y, Bi J, Yang J. Research on vehicular ad hoc networks. Control and Decision Conference, 2009 CCDC'09 Chinese: IEEE; 2009. p. 4430-5.

[11] Bilal SM, Bernardos CJ, Guerrero C. Position-based routing in vehicular networks: A survey, Journal of Network and Computer Applications. 2013;36:685-97.

[12] Zarifneshat M, Khadivi P. Using mobile node speed changes for movement direction change prediction in a realistic category of mobility models, Journal of Network and Computer Applications. 2013.

[13] Anda J, LeBrun J, Ghosal D, Chuah CN, Zhang M. VGrid: vehicular adhoc networking and computing grid for intelligent traffic control. IEEE; 2005. p. 2905-9.

[14] Czajkowski K, Fitzgerald S, Foster I, Kesselman C. Grid information services for distributed resource sharing. IEEE; 2001. p. 181-94.

[15] Festag A, Baldessari R, Zhang W, Le L, Sarma A, Fukukawa M. Car-2-car communication for safety and infotainment in Europe, NEC Technical Journal. 2008;3:21-6.

[16] Nakanishi T, Yendo T, Fujii T, Tanimoto M., Right Turn Assistance System at Intersections by Vehicle-Infrastructure Cooperation. IEEE; 2006. p. 100-5.

[17] Karagiannis G, Altintas O, Ekici E, Heijenk G, Jarupan B, Lin K, et al. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. Communications Surveys & Tutorials, IEEE. 2011;13:584-616.

[18] Levente Butty´an, Tam´as Holczer, and Istv´an Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs" F. Stajano et al. (Eds.): ESAS 2007, LNCS 4572, pp. 129–141, 2007. c_Springer-Verlag Berlin Heidelberg 2007.

[19] Dandan Ren and Suguo Du, Haojin Zhu, "A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs", IEEE ICC 2011 proceedings, 978-1-61284-231-8/11/$26.00 ©2011 IEEE.