International Journal of Computational Science and Engineering.
ISSN 2249-4251 Volume 8, Number 1 (2018), pp. 17-28

http://www.ripublication.com

A Survey on Security Challenges in Internet of Vehicles

Mamatha T[1], Dr. Aishwarya[2], Soumyashree R B[3]

[1] Department of Computer Science & Engineering, R V College of Engineering, Bangalore, India.

2 Department of Computer Science & Engineering, Atria Institute of Technology, Bangalore, India.

3 Department of Computer Science & Engineering, R V College of Engineering, Bangalore, India.

Abstract

The near future is going to witness object to object communication through Internet of Things. IOT is a bridge between Living and Non-Living Objects. Many application of IOT in line are Smart home, Smart Grid, Wearable's, Smart City, connected car, Connected Health, Smart retail, Smart Transport system. A smart transport system has positive impact on the flow of traffic, efficient fuel consumption and towards safety of the lives. The vehicles are more vulnerable to security threats due to wireless medium. In this paper we survey security and privacy threats involved in internet of vehicles

Keywords: Internet of Things; VANET; Intelligent Transport System; second generation telematic; IoV;.

INTRODUCTION

The internet is experienced everywhere homes, offices, malls, coffee shops, it is difficult to imagine not being connected. In the near future, we the human being will be living in an environment where every entity surrounding will have intelligence built in them. And will have capability to exchange information with us. Whether be it a garment or shoes we wear or plantation or wood surrounding us. This interaction between living and non-living entity is possible by embedding computational capabilities in these entities. Building a smart world like smart car, smart homes to

smart bracelet requires integration of different research communities like IOT, MC, PC and WSN. In fact, one of the most important elements of IOT paradigm is WSN [1]. The fundamental pillars towards building a smarter world are sensors.IOT and WSN would impact positively the qualitative living in the world with safe transportation, monitoring energy consumption of smart building and checking on delays in transportation. In general, a smart world would contribute in large towards reducing global warming. Systems will synergistically interact with each other to build holistic, new, common and unpredictable services.

Internet of Vehicles is one flavor of Smart Transport system.IOV involves vehicles with advance sensing and communication, with road side infrastructure which are capable of communication and computation. It is a platform for exchanging huge volume of data between various connected or networked devices. Where these networked devices or objects can be internal to the vehicle or external to the vehicle. IOV enables information exchange between Vehicle to Vehicle, Vehicle to Internet, and Vehicle to infrastructure. IOV is emerging technology which is the convergence of VANET with internet of things. IOV deals with delivery of real time information with growing number of services around the connectivity in vehicles where people feel safe, secure and connected. IOV is more of your vehicle serving you like your mobile phone with different services and applications running in the vehicle.IOV are dynamic mobile communication system connecting to public network through your vehicle.

Several automobile industries and government have shown interest towards the safety of the passengers and trying to keep the people connected inside the vehicle. In New Delhi, all 55,000 licensed rickshaws have been fitted with GPS devices so that drivers can be held accountable for their questionable route selection. China's Ministry of Transport (MOT) has ordered that GPS systems be installed and connected on all long-haul buses and hazmat vehicles by the end of 2011 to ensure good driving habits and reduce the risk for accidents and traffic jams. The Brazilian government has set a goal for all cars in circulation to be fitted with electronic ID chips from its National Automated Vehicle Identification System (Siniav) [1].

Tech Mahindra’s Connected Vehicle solution supports mobile and personal devices like smart phones, tablets and media players that can be brought in to the car for a completely personalized experience. The integrated app store provides access to apps across navigation, remote control and driving behavior.

There is a possibility of security vulnerability through any communication channels. The vulnerabilities may be between V2V, V2I or Vehicle to heterogeneous objects which are networked with the vehicle. The security challenges in Internet of Vehicles can be identified as object identification, authorization and authentication, data privacy, Denial of Service Attack, False Message Injection, Malware, but not limited to only these challenges.

Massive data gets flooded in the network between vehicles and heterogonous objects, Vehicle to Vehicle or Vehicle to Infrastructure. One such scenario of flooding of data is broadcasting of message for driving safety, which contain information like location,

velocity and time of the vehicle. If the real identities of vehicles are used in broadcasting the messages, eavesdropping is possible. There is a need to emphasis on security and privacy of the data, authentication of the objects involved in the communication. In this paper issues and challenges for security and privacy in Internet of vehicles is surveyed.

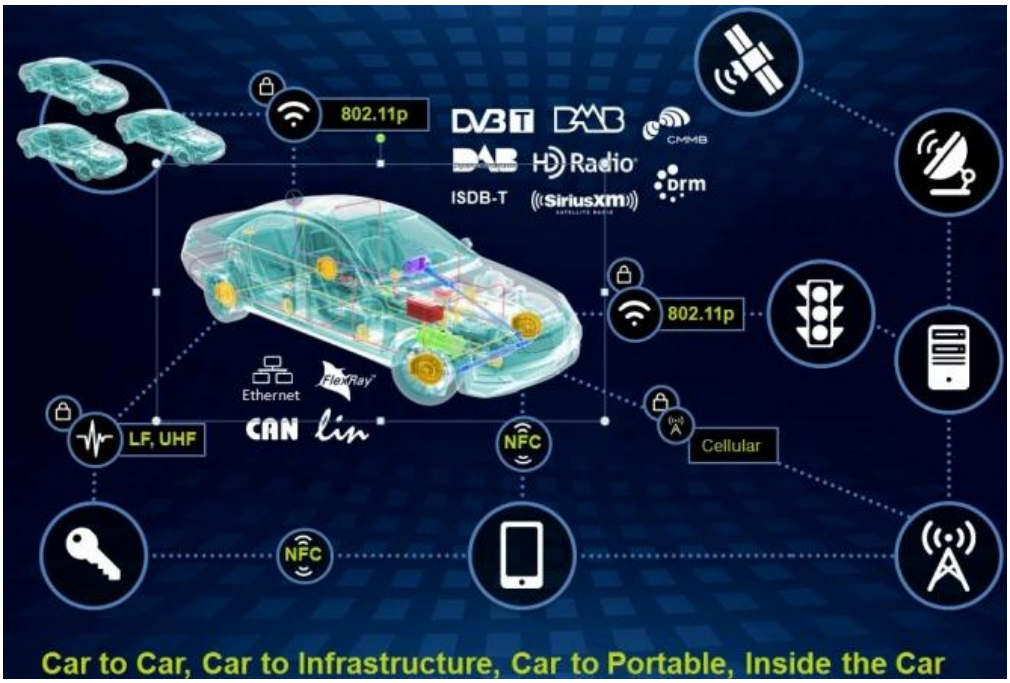

Figure 1. Vehicular Communication in IoV

CHALLENGES OF CONNECTED CARS

A connected car is a car with internet access which connects to devices inside and outside the car. It provides additional benefits to user by notifying about the crashes, traffic jams, and weather reports, optimal routes to destination, speeding and safety alerts, parking and gas stations. Some automakers like GM, Audi, Google, Honda, Hyundai have come up with open automotive alliance to bring android platform into the car.

A. IBM Connected Cars

Focus on the security aspects since the automobile can be easily hacked and can be fatal. The Hackers can hack into the software of the car using their laptops. They can control the car remotely by displaying false telemetry, by suddenly applying brakes when the vehicle is on high speed, switching on or switching off the engine.

The added challenge can be security and privacy threat to passengers and drivers data. The hacker can get their hands on information about the location of the vehicle, hack into emails, phone details and other personal information.

The whole concept and technology of connected vehicle is new and still evolving for the automotive industry. Hence the security risk to manufactures and consumers are high. Challenge for automobile industry is multifaceted [2]. Security in connected vehicles should aim at providing security at different levels. Design secure vehicle, design secure infrastructure, drive with confidence. Every software and hardware component should be designed with security. The integration of these can cause security breach hence a consolidated security plan is required.

Connected vehicles are intended to be designed and built with security as a foundational requirement [2].Designing a secure infrastructure is required since the passenger interacts within the cabin and outside world. Communication between vehicle and users is mediated by automakers who are the service providers. The communication should be encrypted and the network should be monitored for any suspicious activity.

To resolve these threats, the users of the system and control access to the vehicle should be authenticated. For correct functioning of the traffic system, parking system, toll system every infrastructure component has to be secure.

The technologies involved in Vehicle network is CAN, automobile Ethernet. A Controller Area Network (CAN) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer[4].The purpose of using CAN bus for in vehicle communication between different electronic units is that the data exchange is reliable during noisy and electromagnetic conditions.

The common type of attack is the physical attack via CAN. The attacker can get access to the elements like engine, brake, power steering, camera, radio, driver information console and airbags. The communication protocols in IOV are not encrypted; the unencrypted information can be intercepted thereby allowing malicious attacks such has packet forging, DOS attacks, Man –in-the-middle attacks, spoofing.

Both wireless and physical communication protocol (CAN) are not encrypted and are at risk of attacks. The Road Side Unit (RSU) which are the base station are the next element which is vulnerable to the attacks. The RSU are at locations easily accessible to the attacker. These RSU are prone to attacks like Denial of Service (DOS) attacks, which cause the infrastructure in that area to be disabled.

The other challenges of IOV are high mobility of nodes (vehicles), due which the network topology is very dynamic and channel conditions change frequently. The security breach lies in the high mobility, dynamic topology, wireless medium and the communication of the vehicle with numerous other devices and apps. The size of the network is not bound and can vary in rural areas to nights in urban areas. A complete security solution to such system is practically difficult to deploy.

RELATED WORK

The several possible security attacks in IOV are discussed in this section.

According to recent predictions1, 25 billion "things" will be connected to the Internet by 2020, of which vehicles will constitute a significant portion. With increasing numbers of vehicles being connected to the Internet of Things (IoT), the conventional Vehicle Ad- hoc Networks (VANETs) are changing into the Internet of Vehicle (IoV) [3].The author discusses about evolving IOV from VANET and brings out the difference between VANET and IOV.IOV is vehicle networking and intelligence where vehicle networking is VANET and IOV is intelligent integration of humans, vehicles, things and environment.IOV is vehicle telelmatics involves vehicle with more complex communication technologies. VANET and vehicle telematics does not have capacity to process global information as compared with IOV

The paper [3] proposes the Network model comprising of swarm model and individual model for IOV. The network model is the integration of *humans, vehicles, environment, and things.* Here humans are not limited to driver or passengers, but includes people around the vehicle such as pedestrians, cyclist etc. Vehicles in IOV are those who provide or consume services. Things are those around the vehicles which does not include humans or other vehicles. The combination of humans, vehicles and things form the environment. An individual model focuses in a single vehicle. IOV focuses on integration of multiple users, multiple vehicles, multiple things and the environment into global network. Security in such environment involving multiple networks, multiple things, and various communication protocols is at high risk.

In [2] the author discuss about the entities involved in VANET security such as driver who is the interactive component with the driving assistant system, OBU is the next element, in the network there is possibility of existence of normal vehicles and malicious vehicles. Same with RSU possibility of malicious RSU nodes with normal nodes. The attacker is another entity which can be group of cooperative vehicles, internal or external, active or passive. In this paper [2] the authors classify the VANET threats and attacks as availability attack, attack on authenticity and identification, Confidentiality attack, Integrity and data trust, availability attack. The authors further group different attacks under these classifications for instant DOS, Jamming, malware under availability attacks, Sybil attack, replay attack under authenticity and identification attack. Here the authors also discuss about various cryptographic solutions to these attacks.

In paper [4] the authors discuss about vehicular cloud and autonomous vehicle (AUV). Driverless car or a robotic car is an autonomous car that has self driving capabilities by sensing its environment. Objective of autonomous vehicle is making driving safer and less stressful. But this comes at the cost of security.AUV are dependent on the infrastructure such as RTUs, WIFI access and LTEs. Infrastructure failure, due to natural disaster or attacks on these infrastructure components, will require human drivers to take over the functioning of the vehicle to avoid a second disaster. Providing

secure communication access and securing infrastructure components should be at higher priority in autonomous vehicles, since the life of humans can be at stake.

In DoS attack aims to exhaust the availability of network and communication resource to the victim node in the network layer by Jamming the Channel. The resources that are affected are processor power, memory and bandwidth. In [5] the author proposes various cryptographic algorithms to defend DoS. The ECDSA (Elliptic Curve Digital signature algorithm) is an asymmetric key cryptography which uses public and private keys to provide strong authentication and non-repudiation but it suffers from computation based DoS. To overcome the computation DoS a symmetric key algorithm, TESLA (Timed Efficient Stream Loss-tolerant Authentication) is proposed to authenticate the message with MAC (Message Authentication Code) .The delayed key disclosure in TESLA lead to memory based attack. TESLA++ (Timed Efficient Stream Loss-tolerant Authentication) is similar to TESLA but stores very less information in the memory at the receiver side. For multi-hop communication ECDSA and TESLA++ are combined as VAST (VANET Authentication using Signature and TESLA++) to prevent packet loss and to provide increased scalability and non-repudiation. To suppress DoS in dynamic environment PBA (Prediction Based Authentication) symmetric cryptographic algorithm is used which combines both ECDSA signatures and TESLA algorithms to predict vehicle's position based on the network topology and vehicle speed by using Merkle hash tree. The PBA uses TESLA signatures piggyback to minimize the computational overhead when the packet loss rate is high.

Flooding can be prevented by Fast Authentication (FastAuth) which constructs chained Huffman hash trees to predict the single-hop messages. To limit the scope of multi-hop flooding Selective Authentication (SelAuth) is used which implements the forwarder identification mechanism to isolate the malicious node from the network. IP address can be used to defend the DoS. IP-CHOCK uses a Bloom Filter data structure which stores the IP address of the vehicle to reduce memory space, time required for detection and bandwidth utilization by isolating the malicious vehicles from the network. Cellular Automata provides fast authentication efficient mechanism to prevent DoS using complex random pattern and XOR operations. To prevent the Black Hole Attack an Ant-Colony Optimization(ACO) algorithm is proposed in [6] which decreases the packet dropping rate. To identify the path containing malicious node low trust and pheromone values are used with average energy consumption and end to end delay.Another solution to prevent DoS attack is switch between different technology, frequency or DSRC channel. When the malicious node launches the attack in one technology the authentic vehicle can use another available technology such as WiFi, WiMax, 3G/4G cellular network, UMTS, Zig-Bee. Similarly, vehicle can change the channel and frequency-Authentication Technique is used to authenticate the vehicle prior to defend DoS. It reduces the time to verify the vehicle identity but can't be applied to outsiders.

In [7], A Novel Defence Scheme against Distributed DOS Attack is presented. The attacker broadcast the multiple packets containing false traffic information to the entire network thus denying the use of commutation resources. In this approach RSU (Road Side Unit) identify the attacker node by monitoring the network traffic. If a node continuously sends the false information RSU broadcast the information about misbehaving node and all legitimate vehicles stop receiving the packet from the attacker node. After the attacker is identified the performance of the network is not affected even though attacker increases the message broadcasting there by eliminating DDOS.

The attacker tries to act as the identity of many vehicles rather than one and create an illusion that there are hundreds of vehicles in the network. The authentic vehicles are forced to take alternate route as they experience traffic congestion. Traditional solutions to the Sybil attack are radio resource testing, registration and position verification.

In [8], To detect Sybil attack the author assumed that speed of the vehicle are fixed, mobile nodes should have immediate node information and RSU has all information about the vehicle and its neighbours. RSU is responsible to verify the identity of the vehicle, store its neighbour information and specify the vehicle speed as threshold value. When the vehicle identity is changed the RSU will verify neighbour nodes information. If the vehicle information is not same as compared to other vehicle the speed of the vehicle is compared with threshold value. If the speed of the vehicle exceeds the threshold value, then the vehicle is identified as malicious and is detected as Sybil attack.

To reduce the impact of Sybil attack, the author proposed a Time Stamp Series Algorithm [9]. The RSU uses asymmetric key algorithm to generate private key and digitally signed timestamp for each node in the network. The vehicle need timestamp to send message to other vehicles and can get any number of certified timestamp from the RSU. The Sybil attack is identified when the node has same certificate given by two RSU. To give priority to the emergency vehicle in case of Sybil attack a priority based batch verification algorithm is presented in [10]. To slow down the speed and to mislead the legitimate node from the right path the Sybil node sends the message by obtaining multiple timestamp from RSU. To defend Sybil attack Prevention algorithm is implemented in RSU to restrict the vehicle from getting continuous timestamps in a short period. A predefined timer is set, if the vehicle sends multiple requests within that timer expires the vehicle is marked as attacker and its information is tracked. To process the request on priority the RSU uses Priority Batch Verification Algorithm (PBVA) which detects the high priority vehicles such as police, fire and ambulance based on their unique vehicle identifier and provide the services in real time

The attacker modifies the packet content transmitted by the source node to increase the delay in transmission or to send false information.

In [11], Hash chain is used to mitigate data manipulation attack. In this method, the source node sends the packet with the hash value as hashing is computationally less complex. When the packet is received at the destination node the destination node computes the hash value based on the received message. If discrepancy is found in hash value the destination node identify that the packet has been modified, stop the re-transmission of the packet and wait for the retransmission of packet from the source. Contention window adaption is used to increase the throughput of the network and to reduce the re-transmission delay.

In IoV vehicles form a dynamic topology for communication as they are mobile nodes. The vehicles must be able to differentiate between legitimate and malicious vehicles. To verify the trustworthiness the vehicles, communicate with RSU (a fixed infrastructure). The delay involved in this communication can exploit vehicle evacuation attack. In this attack if the attacker travel from right to left it sends false information related to the traffic to the vehicles which are travelling from left to right so that the vehicles exit from the highway and take an alternate route this is possible only when there is a delayed involved in communication between the legitimate vehicle and RSU to verify the trusts of the vehicle and the content of the message. The only know solution to this problem is to have RSU to provide internet access to vehicles in real time [12].

For fast and secure vehicle to vehicle communication cluster head is dynamically selected from the group of nodes in the network which has more energy and capacity. Attacker node can drain the power, energy and bandwidth of the cluster head, the attack is called as vampire attack. Vampire attack makes the malicious node as the main node and further exploits other types of attack. To defend against vampire attack LEACH (Low Energy Adaptive Hierarchy) protocol is proposed which changes the cluster node when the node not able to send the message to the destination with a timeframe. LEACH protocol detects the attack by considering the delay experienced by the attacked cluster head. When the delay and energy required by the head node is more the protocol detect the attack and select another node in network as cluster head to provide secure communication [13].

One of the dangerous attack to break the security of vehicle is wormhole attack, here the attacker node get the packet in one location and transmit the packet to another attacker node in a tunnel to broadcast it. The attack is menacing as it can perform DOS (Denial of Service) attack, break the security of message transmission and can gain unauthorized access. To prevent wormhole attack Packet leash technique is adopted. A leash is extra information added to the packet to restrict the maximum transmission distance. A leash can be location information or time to detect the wormhole attack. The receiver will reject the packet if the packet travelled more than the distance or the time specified in leash. Message authentication code can be further added to make it more secure as the attacker can able to change the time or location of the leash. To avoid multiple authentication code in the network a cryptographic technique, RSA algorithm is proposed to encrypt the packet with location, time and identifier. This

method is infeasible when they are large number of vehicles in the network as it requires more computation and power [14].

Table I. Various attacks of IoV (Internet of Vehicles)

Sr. No.	***Attack***	***Working***	***Defenses***
1	Denial of Service (DoS) attack	Attacker sends the unnecessary packets, wrong request to exhaust the resource available and to prevent communication service.	Cryptographic algorithms, Fast Authentication (FastAuth), Selective Authentication (SelAuth), IP-CHOCK, Cellular Automata, Ant-Colony Optimization(ACO) algorithm, Pre-Authentication Technique, Deploy RSU to monitor the network traffic, Switching between different techniques and channel
2	Sybil Attack	Sybil attacker spoofs the identities of other nodes to create an illusion that they are large number of vehicles in the network which results in traffic congestion.	Radio resource testing, Registration, Position verification, Deploy RSU to get neighbor vehicle information, Time Stamp Series Algorithm and Priority based batch verification algorithm
3	Data manipulation/Falsification attacks/Alteration attack	Attacker modifies the content of the massage sent by the legitimate user. Falsified data is transmitted in the network to break the security.	Hash chain
4	Vehicle Evacuation Attacks	Malicious message sent by the attacker misleads the vehicle in other lane to exit the route.	Providing good internet access by having enough RSUs
5	Vampire attack	Attacker become the main node by draining the battery power of cluster head and sends the modified packet to mislead the working node.	LEACH (Low Energy Adaptive Hierarchy) protocol
6	Wormhole Attack	One or more attacker node creates a tunnel to exchange the confidential information to gain the knowledge of neighboring nodes to exploit further attacks.	Packet leash, RSA Algorithm

CONCLUSION

Advancement of technology leads to connecting all things. The Vehicular Ad Hoc Network (VANET) is transferring into Internet of Vehicles (IoV) with added intelligence. In this paper challenge of connected cars is presented with security attacks in vehicular communication. This communication involves critical information about the driver and traffic which are vulnerable. The malicious vehicle can exploit various attacks such as DoS (Denial of Service), Sybil, Data manipulation, vehicle evacuation, vampire and wormhole attack. The future work is to provide a reliable security solution to overcome from these attacks.

REFERENCES

[1] http://www1.huawei.com/enapp/28/hw-110836.htm

[2] http://www-935.ibm.com/industries/automotive/connected_car.htmlJ.

[3] https://www.ixiacom.com/sites/default/files/resources/whitepaper/securing_the_connected_car.pdf

[4] Intssssernet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds .Mario Gerla∗, Eun-Kyu Lee∗, Giovanni Pau∗‡, and Uichin Lee† ∗University of California, Los Angeles, Los Angeles, CA 90095, USA. {gerla, eklee, gpau}@cs.ucla.edu †Korea Advanced Institute of Science and Technology, Daejeon, Korea. uclee@kaist.ac.kr ‡ Universit`e Pierre et Marie Curie (UPMC) - LIP6, Sorbonne Universites - Paris, France.

[5] K. Deepa Thilak, A. Amuthan, "DoS attack on VANET routing and possible defending solutions - A survey", 2016 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1

[6] Kishan N. Patel , Rutvij H. Jhaveri "Isolating Packet Dropping Misbehavior in VANET using Ant Colony Optimization", International Journal of Computer Applications (0975 – 8887) Volume 120 – No.24,June 2015.

[7] Ayonija Pathre,Chetan Agrawal,Anurag Jain, "A Novel Defense Scheme against DDOS Attack in VANET", 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN) , pp.1 – 5

[8] Mandeep Kaur Saggi, Ranjeet Kaur, "Isolation of Sybil attack in VANET using neighboring information",2015 IEEE International Advance Computing Conference (IACC),pp. 46 - 51

[9] Shikha Sharma, Shivani Sharma, "A defensive timestamp approach to detect and mitigate the Sybil attack in vanet" 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I),pp. 386 - 389

[10] P.VinothKumar, M.Maheshwari, "Prevention of Sybil attack and priority batch verification in VANETs", International Conference on Information Communication and Embedded Systems (ICICES2014).pp. 1 - 5

[11] Danda B. Rawat,Moses Garuba, Lei Chen, Qing Yang "On the security of information dissemination inthe Internet-of-Vehicles",Tsinghua Science and Technology 2017 , Vol.22, Isue: 4, pp. 437 - 445

[12] Mingkui Wei, Zhuo Lu, Wenye Wang, "On modeling and understanding vehicle evacuation attacks in VANETs",2017 IEEE International Conference on Communications (ICC) 2017,pp. 1 - 7

[13] Gayatri A. Jagnade, Saleha I. Saudagar,Sonika A. Chorey, "Secure VANET from vampire attack using LEACH protocol" 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES),pp. 2001 – 2005

[14] Shahjahan Ali,Parma Nand, Shailesh Tiwari,"Secure Message Broadcasting in VANET over Wormhole Attack by using Cryptographic Technique"2017 International Conference on Computing, Communication and Automation (ICCCA),pp. 520 - 523

[15] https://en.wikipedia.org/wiki/CAN_bus

[16] S. Wan, J. Tang, and R.S. Wolff. Reliable Routing for Roadside to Vehicle Communications in Rural Areas. Proceedings of International Conference on Communications, pp. 3017 - 3021, Beijing, May 19-23, 2008.

[17] An Overview of Internet of Vehicles,vYANG Fangchun, WANG Shangguang, LI Jinglin, LIU Zhihan, SUN Qibo .

[18] Y. Ding, C. Wang and L. Xiao. A Static-Node Assisted Adaptive Routing Protocol in Vehicular Networks. IEEE Transactions on Vehicular Technology - IEEE TRANS VEH TECHNOL (Volume: 59, Issue: 5), 2010, pp. 2445 - 2455.

[19] A. Benslimane, S. Barghi and C. Assi. An efficient routing protocol for connecting vehicular networks to the Internet. Pervasive and Mobile Computing, pp. 98-113,February, 2011.

[20] R. K. Shrestha, S. Moh, I. Chung and D. Choi. Vertex-Based Multihop Vehicle-to-Infrastructure Routing for Vehicular Ad Hoc Networks. 43rd Hawaii International Conference on Systems Science, Koloa, Kauai, HI, USA, pp. 1-7, 5-8 January 2010.

[21] Y .Sun, R. Lu, X. Lin, J. Su and X. Shen. Wolff. Roadside Units Deployment for Efficient Short-time Certificate Updating in VANETs. Proceedings of International Conference on Communications, pp. 1-5, Cape Town, May 23-27, 2010.

[22] M. Gerla, "Vehicular Cloud Computing," in IEEE Med-Hoc-Net, June 2012.

[23] N. Fernando, S. Loke, and W. Rahayu, "Mobile Cloud Computing: A Survey," Elsevier Future Generation Computer Systems, vol. 29(1), pp. 84 – 106, July 2013.

[24] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," IEEE Communications Magazine, vol. 50(7), pp. 26 – 36, July 2012.

[25] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content," in ACM CoNEXT, Dec. 2009.

[26] L. Wang, R. Wakikawa, R. Kuntz, R. Vuyyuru, and L. Zhang, "Data naming in Vehicle-to-Vehicle communications," in IEEE NOMEN, Mar. 2012.

[27] Y.-T. Yu, T. Punihaole, M. Gerla, and M. Sanadidi, "Content Routing in the Vehicle Cloud," in IEEE MILCOM, Oct. 2012.

[28] G. Grassi, D. Pesavento, L. Wang, G. Pau, R. Vuyyuru, R. Wakikawa, and L. Zhang, "Vehicular Inter-Networking via Named Data," in ACM HotMobile (poster), Feb. 2013.