2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)
Amity University

Communication Architecture for Vehicular Ad Hoc Networks, with Blockchain Security

Priya Singh, Pooja Khanna, Sachin Kumar
Amity University, Lucknow Campus
singh.priya7732@gmail.com , pkhanna@lko.amity.edu, skumar3@lko.amity.edu

***Abstract*—Vehicular ad hoc networks (VANETs),is a new concept in the direction of making human life more comfortable and secure. Starting with the invention of wheel the journey of the road communication has reached to a point of driverless vehicles. Road communication is the widely spread and most preferred way of commuting the places. This is the reason to create a safer infrastructure for road transportation. Present work is a study about Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications architecture. On-Board Units (OBUs) enabled vehicle in the market can form a Vehicular Ad Hoc Networks (VANETs) that allow wireless communication in a completely distributed manner while they can communicate with Roadside Units (RSUs) in an infrastructure mode. The work presented here also proposed a hybrid Block chain Communication Architecture that will ensure more security in V2V and V2I communication**

Keywords— VANET, Vehicular, Ad Hoc Networks, Blockchain, Communication architecture.

I. INTRODUCTION

Karl Benz gave rise to automobile industry 1896. It made lives of people easy by efficiently lessening the burden of travelling on the shoulders of commuters. With its evolution, safety people was ensured with the introduction of airbags, seatbelts and other components. Despite being well equipped, driving a car is dangerous nowadays. According to a survey by WHO, approximately 1.35 million people die each year as a result of road traffic crashes, 93%of the world's fatalities on the road occur in low- and middle- income countries. Or that there is a need to upgrade safety of vehicles and the update is VANET.[1-2]

Vehicular Ad Hoc Networks (VANET) comes under a special type of Mobile Ad Hoc Networks (MANETs) formed by vehicles furnished with wireless gadgets which permits the cars to interact with one another as well as with the infrastructure or rod side unit without using any central base station or controller [3]. A VANET urns every car in a router or node, permitting vehicles approximately at a range of 100-300 meters to communicate with one another, in turn , forming a wide network. However, new challenges emerge with the rise of VANET like lack of infrastructure unpredictability of path of cars moving at a high speed. With VANET, a vehicle can interact with one another directly called Vehicle to Vehicle (V2V) communication, or with infrastructure such as Road Side Unit (RSU), known as Vehicle-to-Infrastructure communication.

A. Characteristics of VANET

Security of data is one of the major concerns in VANET as there is a constant exchange of information between the nodes; there are chances that it might get hacked or manipulation of data by the attacker. Privacy and security are the biggest challenges under the requirement of efficiency. Frequent disconnections – due to the movement of vehicles on high speeds there are lot of connections and disconnections. Use of other technologies – most cars today is able to integrate their systems with accessible technologies for example Global Positioning System (GPS). [4]

B. VANET Architecture

Architecture of system of vehicular Ad hoc networks is described. Firstly the main components of VANET's architecture along with the domain view and secondly the communication architecture is explained in VANET. Main Components: According to articles [5-8] VANET system can be divided into three domains: the generic domain, the mobile domain and the infrastructure domain. The mobile domain constitutes of the mobile domain and the vehicle domain. The vehicle domain consists of all types of vehicles like cars, buses and trucks. The mobile domain constitutes of all sorts of portable devices like smart phones and personal navigation devices. The infrastructure domain comprises of two domains. They are the roadside infrastructure domain i.e. Road Side Unit (RSU) and central infrastructure domain. The RSU domain consists of things like traffic lights, etc. The central infrastructure domain consists of infrastructure management centers such as vehicle management centers and traffic management centers (TMCs). [8]Still, the architecture of VANETs varies from area to area. The reference article in Vehicle-to-vehicle communication system which pursues C2C varies from CAR-2-X communication system. The architecture of this system constitutes of three domains: infrastructure, ad hoc and in-vehicle domain. The in-vehicle domain comprises an on-board unit (OBU) and multiple application units (AU). The connection between OBU and AU is usually wired or wireless. Whereas the Ad Hoc domain comprises vehicles furnished with OBU and road side units (RSU). An OBU is a sort of a mobile node whereas a RSU is a static node. OBU can communicate with Internet via RSU or Hotspots. Also in their absence, it can communicate with the help of cellular networks i.e. 4G, UMTs, GSM, etc. RSUs can communicate with each other directly and is connected with the internet via Gateway. Infrastructure domain constitutes of Hotspots and RSUs.

In order to incorporate the attributes mentioned earlier, the model proposed is further layered in client layer, communication layer, fog layer and cloud layer. The cloud

978-1-7281-0666-3/20/$31.00©2020IEEE

layer comprises Permanent VANET cloud and Temporary VANET cloud. The Permanent cloud layer consists of traditional cloud computing infrastructure and also integrates the Temporary VANET cloud and thus garners the benefits of both in the cloud layer. VANET cloud layers are as follows: Client Layer –it comprises of the users and the ones which use VANET on "pay-as-you-go" subscription. It can be either a general customer or a VANET node that needs the service. By the help of usage of devices like laptop, mobile phones, GPS or with the help of a wired or wireless connection, a contact with the other layers can be established by the SAP (Service Access Point). Also from this only the sender receives the service response. Communication Layer –the point of this layer is to initiate a contact between the client layer and the cloud layer. The contact can be established between them by the internet, tactile internet, RSUs, GPS, private networks and wireless networks like 5G, etc. At this layer, all connection technologies are described with regard to the communication device used. Also one more factor that affects the communication is the type of client and the data center. Fog Layer – It is very much similar to Mobile Cloud Computing wherein MCC enhances the capabilities of cell phones. Edge computing does the exact same thing, it reduces requirements for data transmission, thus saving network bandwidth costs and avoiding proliferation of data storage. An instance of how to improve performance and effectiveness by storing information is a CDN (Content Distribution Network) closer to its users. Fog computing bridges the space between cloud and client layer by enabling networking, data management, storage and computing in the range of devices. The decision making, networking, storage does not take place in cloud but also in the client-to-cloud path therefore making fog computing necessary. Cloud Layer – the cloud data centers which provide the VANET services are makes the cloud layer. Now the cloud layer consists of two sub-models. They are Permanent cloud layer and Temporary cloud layer. The permanent cloud layer makes use of static clouds or traditional stationary cloud and also the temporary cloud layer.

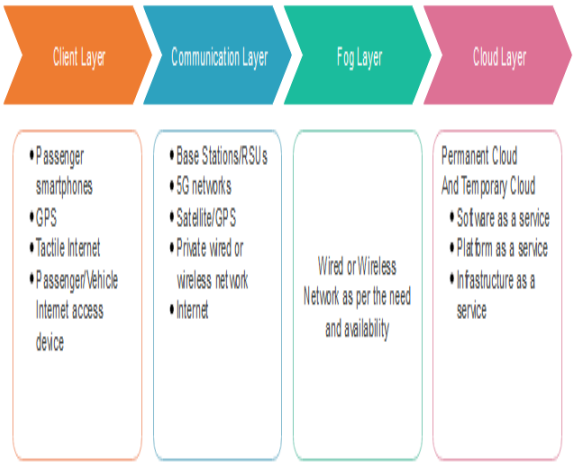

Fig.1. Existing four layer architecture of VANET.

C. *Security and Privacy Issues in VANET*

Security should be considered as an important issue in VANET. Nowadays many intelligent applications store personal data which can disclose an individual's whereabouts. As highly sensitive and confidential data is being transferred as information in VANET therefore it needs to be protected from malevolent people for exploitation. The revelation of critical fact about a person can lead to manipulation of data. Also loss of revenue needs to be taken care of. Network on Wheels (NOW) [21] and Secure Vehicular Communication (SEVECOM) are consortiums that are running with a primary view of security related issues associated with VANET. As per basic cyber security, cyber-attacks on a computer can be justified into three major categories- Availability threat, Authenticity threat and lastly, Confidentiality threat. Confidentiality threat is of our more concern as far as VANET is concerned. An attacker might be able to get the information about the person and also the details of exact location of a person. With broadcast authentication scheme, the receivers are able to authenticate that the received information was really sent by that person. Few approaches for security in VANET are mentioned in [22, 23]. The approaches mentioned are that the vehicle should be loaded with more public keys rather that one default key and the other one is in which user can switch between different identities. However, the disadvantage associated with both of them is put undue constraints or pressure on the network that is already being exceeded due to the lack of bandwidth. A better approach to security in VANET is to provide authentication of each node. Secure authentication of the sender should be done.

In VANET security, the attacks can be classified in these categories-

- Bogus Information- sending bogus information in VANET can lead to disastrous situations
- ID Disclosure- exact position of the vehicle can be detected by the attacker.
- Denial Of Service – attacker might be able to overflow the network with information so that the service no longer functions.

II. COMMUNICATION ARCHITECTURE

Communication architecture consists of In-vehicle communication, Vehicle-to-vehicle (V2V) communication, Vehicle-to-road infrastructure (V2I) communication and Vehicle-to-broadband cloud (V2B) communication, as presented Fig 2.Communication architecture consists of In-vehicle communication, Vehicle-to-vehicle (V2V) communication, Vehicle-to-road infrastructure (V2I) communication and Vehicle-to-broadband cloud (V2B) communication. In-vehicle communication is very much important in VANET's research. It is critical for determining a vehicle's performance, drivers' condition and

also for safety of the public. It basically refers to in-vehicle domain.

Vehicle-to-vehicle (V2V) communication provides a platform for data exchange for the vehicles for the information and warning messages to be shared so as to ensure driver assistance and safety of driver. Vehicle-to-road infrastructure (V2I) communication enables exchange of information like of weather and traffic updates for

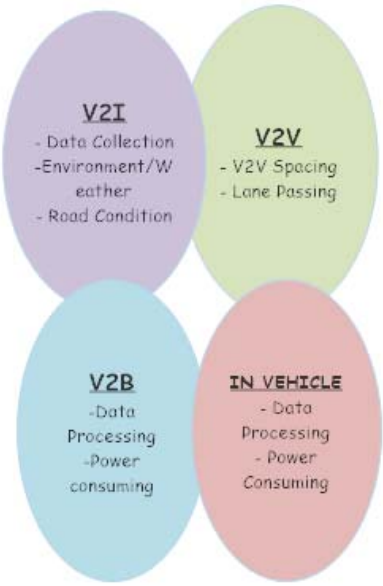

Fig.2. Existing communication architecture of VANET

vehicles and does environmental monitoring and sensing. Vehicle-to-broadband cloud (V2B) communication refers to communication of vehicles over wireless broadband like 3G/4G. It is a better form of V2I as it provides traffic information as well as infotainment and is useful for vehicle tracking and assistance.

III. Hybrid Communication Architecture for Vehicular Ad-Hoc Networks

Communication in VANET can be categorized in three layers – Vehicle level, inter-vehicle level and Cloud level. As visible from Fig 3, the lowermost layer is of vehicles. Vehicles in standalone VANET has actuators, radar, sensors and GPS. Amongst them communication will take place at the vehicle level that will lead to the generation of alert messages from the car level.

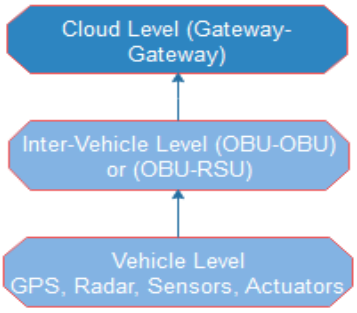

Fig.3. Existing three layer architecture of VANET

The second level is Inter-vehicle layer. Here the Vehicles interact on-board unit (OBU) level with each other. The topmost layer permits cars to interact at cloud level where RSU and cars will serve the purpose of gateways. The selection of gateways depends upon the VANET framework. We propose a secure vehicles communication using blockchain technology. The proposed architecture is a hybrid mechanism communication network enabled connected device/vehicles with blockchain technology.

A. Block Chain Technology

Block chain technology is a decentralized system composed of linked structures known as blocks in which information is stores using the security of crypt-algorithms. The concept of block chain was first commercialized with bit coin crypto currency in 2008 [24-26]. Block chain has applications in various domains like business(B2B, P2P), health, inventory management and finance. Features of block chain technology include a secure environment both for public and private networks. A public network is one where random nodes can be added to the network in ad-hoc way, while a private network requires a secure way to allow nodes to access the network resources. Block chain architecture allow both permissioned and permission less architecture for a secure network setup. Depending on the type of network security and privacy requirement different architectures are available; the difference between the architecture is the way component of the block chain interacts. Various components of block chain includes; Smart Contract: that defines the relationship between the various stake holders of the network, all nodes in a network may play different roles and responsibility and smart contracts are the way to organize the relationship structure amongst the nodes in a block chain network. Another important component is ledger, it can be understood as the file to store all the transaction information of a network, it is one of the important asset of the network and if the distribution of this asset amongst the nodes is controlled its comprises a permissioned architecture and in an open architecture mining of the ledger is open to all random nodes joining the network. The entire network of block chain architecture follows governance rules as specified by consensus algorithms.

B. Hybrid Block Chain VANET Communiation Architecture

This section proposes a Hybrid blockchain for VANET communication architecture. The proposed architecture combines the features of permissioned blockchains to

address the authentication, of smart vehicles in a VANET and permission less block chain structure for maintaining the inter vehicular communication. A smart vehicle ones enters a VANET needs to register with the VANET block chain platform according to the set smart contract. A smart contract act as the governance rules and structure and this is maintained to ensure the security in vehicular network. A vehicular network has a structure where devices are on move and frequently exchange the information with infrastructure and other devices. Authentication is required whenever a smart vehicle enters a network and to provide a secure way for information management. The registration of a smart vehicle includes the information of registration certificate (RC), Insurance information. In proposed architecture a hybrid block chain layer is introduced between VANET infrastructure and client layer that includes the OBD, Smart phones and other smart devices and whole communication architecture is set up at two levels.

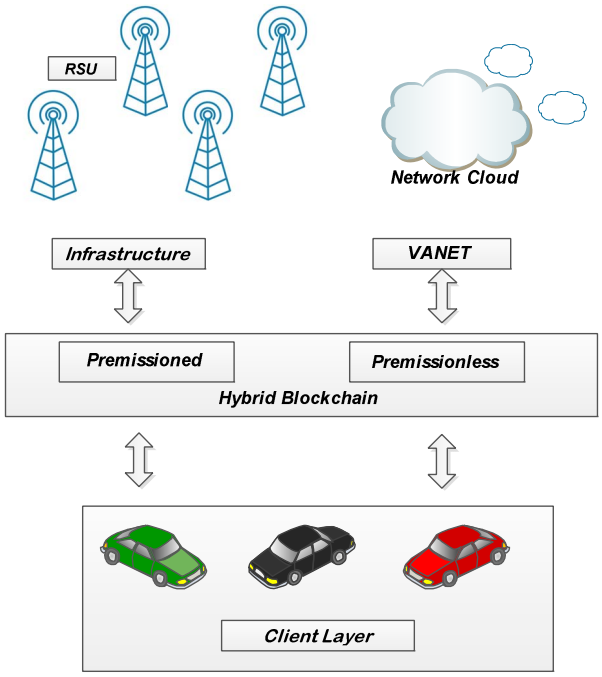

Fig. 4. Hybrid Block Chain VANET communications Architecture

Level 1: Communication between Infrastructures to hybrid Block Chain:

This is the first step for a smart vehicle to get attached to the communication structure of VANET. A client layer sends a validation request for new arriving devise, for permissioned blockchain endorser. Endorsers as per the governance rules already specified among them to ensure that device is safe for network add it to the current network. For a smart device it is necessary to get validated by the endorsing node for utilizing the communication Architecture network of VANET. A permissioned architecture ensures the security in VANET as this architecture ensure secured information management, of the devices this is one time process as a device enters the range of VANET infrastructure, and as soon the device is out of the coverage area it is the job of endorsing node to de register the device.

Level 2: Communication between hybrid Block Chain and Client layer:

The next step is setting a communication link between the nodes in client layer of the VANET architecture. Once, a node is registered with the block chain platform it is provided with an identity, using this identity it can establish further communication with other client layer devices. The communication in level two is governed by permission less block chain architecture and this allow frequent and easy communication among the fast devices as inter vehicular requires a scalable network. Communication medium proposed to use for inter vehicular communication are short range links and depending on the distance on the road these devices can establish or re-establish links between fast moving devices.

The hybrid block chain architecture will provide a way to deal with various securities related issues as discussed in earlier sections using secure two layer structure. In proposed architecture a permissioned structure ensure the validity of new arriving node. At this level the critical information are checked stored with the infrastructure. Once the new node is registered with system it is provided with a secure identity. At the next level using the secured ID a node can established a connection using permission less architecture with other nodes of the architecture. This architecture will ensure better management of information.

IV. Conclusion

Work here is a detailed study of the VANET architecture and the issues encountered in present VANET architecture. Work discussed the applications of VANET, its architecture, different routing protocols, security and privacy and challenges associated with VANET. It has become the most successful field of research nowadays. The number of vehicles is increasing day by day and so is the need for an efficient VANET system. So a proper modeling technique is required for effective communication between vehicles and between vehicles and road side unit. The hybrid block chain architecture proposed in the work will provide a way to deal with various securities related issues as discussed in the work using secure two layer structure. It is proposed in the work that a disruptive technology like block chain platform can handle the issues like fake information, sending bogus information in VANET can lead to disastrous situations, ID Disclosure or extracting exact position of the vehicle.

References

[1] https://www.automotivelectronics.com/everything-about-vanet-vehicular-ad-hoc-network/

[2] https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[3] M. Sivasakthi and S. Suresh, "Research on vehicular ad hoc networks (VANETs): an overview," Journal of Applied Sciences and Engineering Research, vol 2, no. 1, pp. 23-27, 2013.

[4] H. Hartenstein and K. Laberteaux, VANET Vehicular applications and inter-networking technologies, 2009.

[5] M. W. Maier, D. Emery and R.Hilliard," Software architecture: introducing IEEE standard 1471," Computer , vol. 34, no. 4,pp-107-109, 2001.

[6] M. W. Maier, D. Emery, and R. Hiliard," ANSI/IEEE 1471 and systems engineering ," Systems engineering, vol. 7, no.3, pp. 257-270, 2004.

[7] D. Emery and R. Hiliard," Every architecture description needs a framework: expressing architecture frameworks using ISO/IEC 42010," in Proceedings of the joint working IEEE/IFIP Conference on software Architecture, pp 31-40, Cambridge, UK, September 2009.

[8] T. Kosch, C. Schroth, M. Strassberger, and M. Bechler, Automotive Internetworking, Wiey, New York, NY, USA, 2012.

[9] C. E. Perkins and E.M. Royer,"Ad-hoc On-demand Distance Vector Routing," in second IEEE Workshp on Mobile Computing Systems and Applications, 1999, pp 90-100.

[10] D.B. Johnson and D. A. Maltz ," Dynamic Source Routing in Ad Hoc Wireless Networks,' in Mobile computing, 1996, ch.5.

[11] M. Zhang and R.S. Wolff,"A border node based routing protocol for partially connected vehicular ad hoc networks," Journal of Communications, vol.5, n.2, pp 130-143, 2010.

[12] NUNDLOLL, G S BLAIR AND P. GRACE," A COMPONENT BASED DESIGN, PP 1-6,2009.

[13] M. Al-Rabayah and R. Malaney," A new scalable hybrid routing protocol for vanets," Vehicular Technoloy , IEEE Transactions on, vol 61, no. 6, pp 2625-2635, 2012.

[14] Y. B. ko and N. H. Vaidya," Location-aided routing (LAR) in mobile ad hoc networks," ACM journal of Wireless Networks, vol.6, pp 307-321, 2000.

[15] D. Akhtar Husain, Brajesh Kumar," A study of location aided routing (LAR) protocol for vehicular ad hoc networks in highway scenario," International Journal of Information Technology and Web Engineering vol. 2, no. 2, pp 118-124, 2010.

[16] Lin and M. Gerla, "Adaptive clustering for mobile wireless networks," IEEE Journal on Selected Areas in Communications," pp 1265-1275, 1997.

[17] R. A. Santos, R. M. Edwards, and L. N. Seed," A location based routing algorithm for vehicle to vehicle communication," vol 00,no. C, pp 221-226,2004.

[18] Y. Luo, W.Zhang and Y. Hu," A new cluster based routing protocol for VANET," in Networks Security Wireless Communication and Trusted Computing(NSWCTC0, 2010 vol 1 , 2010, pp 176-180.

[19] Z. Rawashdeh and S. Mahmud," A novel algorithm to form stable clusters in vehicular ad hoc networks on highways" EURASIP journal on Wireless Communications and Networking, vol 2012, pp 1-13, 2012.

[20] M. Durresi, A. Durrsi and L. Baroli," Emergency Broadcast protocol for inter-vehicle communications," 11th international conference on Parallel and Distributed systems vol2,pp 402-406, 2005.

[21] NOW – Network on Wheels, http://www.network-on-wheels.de/ 2008.

[22] G. Calandriello, P. Papadimitatos, J. P. Hubaux and A. Lioy, "Efficient and robust pseudonyms authentication in VANET" proceedings of 4th ACM international workshop on VANET, 2007.

[23] D. Echkoff, C. Sommer, T. Gansen, R. Germanand F. Dressler, 'Strong and affordable location privacy in VANETs; IEEE Vehicular Networking Conference pp 174-181, 2010.

[24] H. Hartenstein and K. Laberteaux, VANET Vehicular Applications and Inter-networking technologies, intelligent transport systems. Wiley, 2009.

[25] B. Karp and H. T. Kung" GPSR Greedy Perimeter Stateless Routing for wireless networks," in proceedings of ACM/IEEE International Conference on Mobile Computing and Networking(MobiCom),2000.

[26] Naumov, R. Baumann and T. Goss," an evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," proceedings of 7TH ACM international symposium on MANET p 108, 2006.