Survey: Road Side Units Based Various Technique in Vehicular Ad-Hoc Networks

Renuka[1], Er. Chandni Guleria[2]
[1]M.Tech, [2]Assistant Professor
Department of Electronics and Communication Enginering, Sri Sai University Palampur

Abstract - VANETS is the most prevalent network which is called Vehicular Ad Hoc Network. The researchers make a lot of work in this network. From the Works review, VANETs mechanism on the basis of real time system where the vehicles are moving nodes and travel with a very high rapidity on the highways in the urban areas. There are many security issues like authentication, channel attacks, intelligent system approach, impact detection, congestion avoidance, communication system approach etc. A Vehicular Ad hoc Network involves of a set of communicating wireless mobile nodes or devices that do not have any form of secure organization or integrated authority. The security in VANET has become a significant and active topic within the investigation community. This is because of high demand in sharing streaming video and audio in various applications, one VANET could be setup quickly to facilitate communications in a hostile environment such as battlefield or emergency condition likes disaster liberation operation. In spite of the several attacks aimed at specific nodes in VANET that have been discovered, some attacks involving multiple nodes still receive little attention. A reason behind this is because people make use of confidence instruments applicable to wired networks in VANET and overlook the security measures that apply to VANET. Furthermore, it may also have to do with the fact that no survey or taxonomy has been done to explain the features of different multiple node attacks.

Keywords - Vehicular ad hoc network, Security threads, Sybil attack and AODV

I. INTRODUCTION

Vehicular networks permit cars to communicate with each other and with a distinct infrastructure on the road. Infrastructures can be purely ad hoc between cars or facilitated by making use of an infrastructure. The organization typically consists of a set of so called roadside units that are connected to each other or even to the Internet [1]. Otherwise, remaining infrastructure such as cellular networks can be used for this resolve. VANET is normally part Movable Ad-hoc system. Vehicular Ad-hoc System is mixture of Ad-hoc System& sensing System. In Vanet, automobiles act as sensing's which container interchange data between each other deprived of any infra-structure System created. Directional mobility& high dynamic of the Automobiles are significant characteristics. In order to contribute in such a system, a vehicle has been prepared with a superior electric instrument which will give ad hoc system connectivity for the automobiles. VANETs are continuously shaped between[2] affecting Automobiles prepared with wireless interfaces that might have dissimilar& same wireless boundary tools, employing less range to intermediate range message system. The best instance of VANET is Transport System of one travel support or any company which is merged internally. This Transport System of a Automobiles are affecting in any parts of city& dissimilar routes to pick or drop client or workers if they are associated together, which make an Ad hoc System& connected wireless[3].

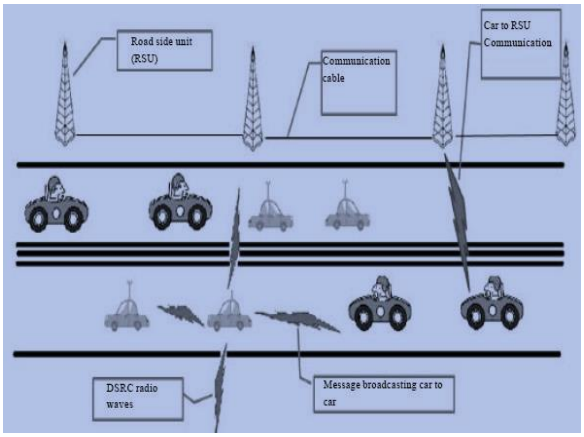

Fig.1 Vehicular ad-hoc network

The main advantages of Vehicular ad hoc network described as:

a) Extremely dynamic topology: The quick of the Automobiles beside the accessibility of choices of different methods characterizes the component topology of VANETs [3].

b) Frequent separated system: The rapid of the Automobiles in one way characterizes the component topology while then again needs the unvarying prerequisites of the roadside unit absence of which results a nonstop separations.

c) Mobility representative& Forecast: The forecast of vehicle position& their developments is tremendously worrying. This highlights of transportability demonstrating& forecast in VANETs is in view [4] of the accessibility of predefined guide's models. The rate of the Automobiles is over an imperative for creative

system summary.

d) Communication Environment: When we are having the [4] movability classical, yet we are not done. As the versatility model may have distinctive highlights relying on street construction moulding, roadways, or city conditions. Informing in these circumstances must be taken deliberation [5].

Vanet works in two forms first is routing based and second one road side unit. We implemented the Road side unit architecture in vehicular ad hoc network [6].

Road Side Units

The roadside sensor nodes measure the road condition at several positions on the surface, collective the measured standards [7] & communicate their amassed value to an approaching vehicle. The vehicle generates a cautionary message & dispenses it[8] to all automobiles in a certain geographical region, potentially using wireless multi-hop statement. For post-accident examination, sensor nodes continuously measure the road condition and supply this info within the WSN itself [9].

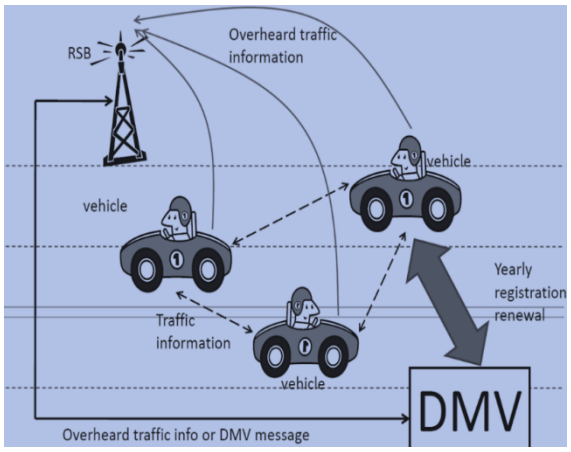

Fig.2: Information transmission using road side units

When a coincidence occurs, road condition data stored over a sufficiently long period can be used for criminal modernization of road accidents. In contrast to the accident prevention service, such a accountability service requirements to be constrained to a well specified group of end-users, e.g. insurance companies or the road patrol. Information stored within the WSN can also be utilized to judge a driver's driving style according to the road condition at the moment of an accident [10].

II. RELATED WORK

Wenjia Li et al., 2015 [11] proposed an attacker trusted management method is proposed for vehicular ad hoc network i.e., Able to detect and manage with attackers and also calculate the trustworthiness of both data to moveable nodes in VANETs. Normally, data trust us calculated based on the data detected and collected from several vehicles node belief is accessible in binary forms i.e. Method trust and rec-commendation trust, which define how likely a vehicle node could full-fill its functionality and how trustworthy the re-commendations from a node for other nodes would be respectively. **Mohammad Javad Faghihniya et al., 2016 [12]** described that the Security in VANET plays vital role. An AODV routing protocol is a sensitive or on-demand routing protocol which resources if there is data to be sent then the path will create. AODV is the most normally used topology based routing procedure for VANET. Using of broadcast packets in the AODV route discovery phase caused it is tremendously susceptible against DOS and DDOS flooding attacks. Flooding attack is a type of a DDoS attack that sources loss of network bandwidth and imposes high overhead to the network. The method proposed in this project called Balanced AODV because it expects all network nodes behave normally. If network nodes are out of the standard behavior (too much route request) then they recognized as malicious node. **Khaoula Jeffane et al., 2016[13]** described that the Vehicular Ad-hoc Networks (VANET) is a particular type of the Mobile Ad-hoc Networks (MANET) and was developed to provide communications in a group of vehicles in range of each other and between vehicles and fixed equipment's within a communication range, usually called equipment of the road. This network was very sensible to safety problem. In this work, a new mechanism was proposed to study the safety problem in VANET networks. This mechanism focuses on denial of service (DDoS) attacks on the corporeal and MAC layers in IEEE standard 802.11p. **Maxim Kalinin, Peter Zegzhda et al., 2016 [14]** defined that it was one of the most intensively growing technologies which shape new social and engineering opportunities such as smart traffic control, effective road safety, optimal rescue maintenance, enhanced customer services. However, common VANET as a large-scale wireless environment with extremely dynamic topology lacks in information security. The specific nature of VANET prevents traditional solutions to be applied 'as is' for security purposes. The paper studied software defined security (SDS) suggested to be employed to provide the programmable and flexible access control to VANET. **Yeka Joseph Abueh et al., 2016[15]** explained that the safety messages such as pre-collision warnings, blind-spot detection, ordinary and object awareness significantly advance the safety for drivers, passengers, and pedestrians. As a consequence, vehicles would be able to travel carefully yet safely together, forming a platoon, thus subsequent in a reduction of traffic congestion and fuel ingesting. Driverless cars also have non-safety-related requests: which are used to simplify traffic management and infotainment dissemination for drivers and passengers. Vehicular Ad hoc Network (VANET), the wireless communication technology enabling driverless cars, features not only active topology but also high mobility. **Georgie Knight et al., 2016 [16]** defined that vehicular communications, Basic Safety Messages (BSMs) can be bundled composed and relayed as to increase the actual

communication range of communicating vehicles. This process forms a vehicular ad hoc network (VANET) for the distribution of safety information. The number of "shortest multichip paths" (or geodesics) connecting two network nodes is a significant statistic which can be used to enhance output, validate threat events, defend against collusion attacks, infer location info, and also limit redundant programs thus reducing interference. To this end, it is systematically calculates for the first time the mean and variance of the number of geodesics in 1D VANETs. **Ubaidullah Rajput et al., 2016 [17]** defined that the idea of primary pseudonyms with relatively longer time periods that are used to interconnect with semi-trusted authorities and secondary pen names with a smaller life time that are used to communicate with other vehicles. Most of the current pseudonym based approaches are based on the Certificate Revocation List that causes significant communication and storage above or group-based methods that are computationally expensive and suffer from group-management issues. These schemes also smart from trust issues connected to certification authority. The protocol only expects an honest-but-curious behaviour from otherwise fully trusted authorities. The proposed protocol protects a user's privacy until the user honestly follows the procedure. In case of a malicious activity, the true identity of the user is exposed to the appropriate authorities.

III. SYBIL ATTACK

Vehicular system is a precise kind of mobile ad hoc network anywhere the moveable swellings are substituted with automobiles prepared with on boarding unit communication devices. VANETs have particular diverse features in decision with MANETs counting quick alteration in topology, no power limitation, great scale, adjustable network compactness and high expectable agility. VANET construction is calculated for vehicle to automobile and automobile to organization communications with two statement devices so-called the Curb Unit that is situated on the roadside and OBU installed in automobiles. It also requirements to some sensors connected on the vehicles for meeting conservational and road info. The middle used for transportations amid vehicles is 5.9 GHz Ardent Short Range Announcement identified as IEEE 802.11p. Unpaid to wireless organizations, VANETs are liable to many of the safety attacks. One of the injurious attacks is Sybil attack familiarized by Douceur. In this attack, one invader creates multiple features either by counterfeiting new individualities or stealing eccentricities from adjacent vehicles. Identities can transpire by overhearing characteristics in message circulation, as vehicles within the declaration range of sender can eavesdrop its exchanged messages.

IV. SCOPE OF VANET

Major target is more useful safe roader and efficient will construct through vehicle network by defining to normal security and drivers in time in the planned. Another target is to explore the advancement of vehicular network technology. The propose is to secure and to make possible official requests through range of message networks and system which goes small to medium. The support major concern for critical time secure information and fulfil the quality of services requires of other multi-media software. Next aim to generate high presentation, extremely measure and safety technology of vehicular network. VANET has particular exceptional geographies which make it different from MANET as well as motivating for conniving VANET applications.

- Great active topology the topology of VANET disparities for the cause that of the commission of vehicles at high speed. Presume two vehicles are poignant at the speed of 20m/sec and the radio range midst them is 160 m. Then the link amongst the two vehicles will last 160/20 = 8 sec.
- Normal severed network from the exceedingly dynamic topology results we observe that frequent stoppage occur between two vehicles when they are swapping in-construction. This cessation will occur most in sparse network.
- Movement exhibiting [18] the mobility pattern of vehicles be contingent on traffic situation, roads structure, the speed of automobiles, drivers driving behaviour and so on.
- Battery power and storage bulk in modern vehicles mobile control and stowage is unconstrained. Thus it has appropriate computing power which is unreachable in MANET. It is supportive for effective message & making overpowering results.
- Communiqué atmosphere the statement environment between automobiles is disparate in meagre network & thick network. In dense web building, trees & other objects make as hindrances and in scarce network like road this things are absent. So the routing attitude of light & compressed network will be unlike [19].

A. Advantages of Vanet

- Expand the network
- Faster transaction procedure
- Better communication
- Easy to share the information

B. Disadvantages of VANET

- Costly
- Installation
- Double regions sword of VAN use.

V. CONCLUSION AND FUTURE SCOPE

This paper provides a survey dealing with all the various techniques in RSU, attacks and issues facing VANET, in particular, VANET architectures components, VANET communication domains, wireless access technologies, VANET characteristics, challenges and requirements, VANET applications and simulation tools. This

investigation enables researchers to focus on the issues surrounding VANET and its applications, showing great deal of understanding of how to tackle all issues related to VANET i.e. What architecture component to focus on? What access technology to use? What kind of applications is the new paradigm? And what simulation tool should be the appropriate model to evaluate and implement available approaches. No ultimate answer or platform could be provided from this study, because of the uniqueness each individual case holds. Each scenario holds its own features, criteria and requirements; as an answer, this paper aims to provide the key concepts to undertake all question and concerns ITS researchers are facing. From this survey it has been realized that standard protocols must exist that enables effective communication for various applications all together in a multidimensional way and overcome issues related to those applications. VANET would provide better platform and effective communication between vehicles with further advancement and evolution of new approaches.

VI. REFERENCES

[1]. Boukerche, Azzedine, et al. "Vehicular ad hoc networks: A new challenge for localization-based systems." Computer communications 31.12 (2008): 2838-2849.

[2]. Rawat, Priyanka, et al. "Wireless sensor networks: a survey on recent developments and potential synergies." The Journal of supercomputing 68.1 (2014): 1-48

[3]. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on. IEEE, 2010.

[4]. Samara, Ghassan, and Wafaa AH Ali Alsalihy. "Message Broadcasting Protocols in VANET." *Information Technology Journal* 11.9 (2012): 1235.

[5]. X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[6]. Suriyapaibonwattana, Kanitsom, and Chotipat Pomavalai. "An effective safety alert broadcast algorithm for VANET." Communications and Information Technologies, 2008. ISCIT 2008. International Symposium on. IEEE, 2008.

[7]. Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.

[8]. Xi, Sun, and Xia-Miao Li. "Study of the Feasibility of VANET and its Routing Protocols." Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on. IEEE, 2008.

[9]. Schmidt RK, Leinmuller T, Schoch E, Held A, Schafer G (2008) Vehicle behavior analysis to enhance security in vanets. In:Workshop on vehicle to vehicle communications.

[10]. NEEDHAM, ATTRIBUTED BY ROGER, and Butler Lampson. "Network Attack and Defense." *white paper* (2008).

[11]. Li, Wenjia, and H Song.(2016) "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks." *IEEE Transactions on Intelligent Transportation Systems* 17, no. 4 : 960-969.

[12]. Faghihniya, M Javad, S Mojtaba H, and Maryam T.(2012) "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network." *Wireless Networks*: 1-12.

[13]. Jeffane, K, and Khalil I.(2016) "Detection and identification of attacks in Vehicular Ad-Hoc NETwork." In *Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on*, pp. 58-62. IEEE.

[14]. Kalinin, M, Peter Z, Dmitry Z, Yuri Vasiliev, and Viacheslav Belenko.(2016) "Software defined security for vehicular ad hoc networks." In *Information and Communication Technology Convergence (ICTC), 2016 International Conference on*, pp. 533-537. IEEE.

[15]. Abueh, Yeka Joseph, and Hong Liu.(2016) "Message authentication in driverless cars." In *Technologies for Homeland Security (HST), 2016 IEEE Symposium on*, pp. 1-6. IEEE.

[16]. Knight, G, Alexander P. Kartun-Giles, Orestis Georgiou, and Carl P. Dettmann. (2016) , "Counting Geodesic Paths in 1D VANETs." *arXiv preprint arXiv:1610.01630*.

[17]. Rajput, U, Fizza Abbas, and Heekuck Oh.(2016) "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET." *IEEE Access* 4 (2016): 7770-7784.

[18]. Luo, Yuyi, Wei Zhang, and Yangqing Hu. "A new cluster based routing protocol for VANET." Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Transaction on. Vol. 1. IEEE, 2010.

[19]. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on. IEEE, 2010.