THINK INDIA Journal

ISSN:0971-1260
Vol-22-Issue-16-August-2019

A Review: Architecture, Applications, Security Threats And Routing Protocols In VANET

Rajeev Kumar[1, 2], Dilip Kumar[3]and Dinesh Kumar[4]

[1]Department of Electronics and Communication Engineering, IKG-Punjab Technical University, Kapurthala, India, rajeev.patial@lpu.co.in
[2]School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara, India
[3]Department of Electronics and Communication Engineering, SantLongowal Institute of Engineering and Technology, Longowal, India
[4]Department of Information Technology, DAV Institute of Engineering and Technology, Jalandhar, India

Abstract. According to the previous researches, we are noticing to step up the interest in the vehicular communication. A VANET is composed of the movement of the cars as the nodes with different types of the communication link such as vehicle to vehicle (V2V), Vehicle to infrastructure (V2I), and roadside units (RSUs). VANET is a prominent type of Mobile ad hoc networks in which network terminals are mostly road vehicles. It provides an efficient mechanism to enhance the safety for vehicle passengers, drivers and to the public and enables to improve traffic management techniques. It establishes distant communication between vehicles, roadside infrastructure units and traffic management centers. VANETs provide a great significance in accessing an enormous variety of applications to the vehicle passengers. It has been evolved as operative field of exploration, standardization, and progress with an extreme capability to enhance road, vehicle and passenger safety, traffic efficiency, and ease as well as amenity to drivers, passengers, and public. This paper is dedicated to establish an organized and thorough summary of the previous research advances on various parameters of VANETs.

Keywords:VANET, DSRC, Architecture, Application, Security, Privacy, Protocols.

1. Introduction.

In the last decade, ad- hoc networking is gaining the demand nowadays. It becomes attractive topic among the researchers. Most of the articles, surveys have been published with new algorithms, solutions in theoretically and practically with best of its results. VANETs provide the efficient ways to secure the data of the users as well as infrastructure side using clustering. Apart of its advantage, vehicle ad- hoc network also ply with number of security applications and in addition to protection gives secured communication against the attackers. Data security also plays a crucial role in versatile environment as it leads to the privacy threats to the user.

ISSN:0971-1260
Vol-22-Issue-16-August-2019

According to WHO, road accident is the main reason behind the increase of death rate after year 2000. Therefore, we must be requiring a better traffic management system to reckon with this issue. Advancement in vehicular communication makes it adaptable to the environment which helps to build Intelligent Transportation system [4] service to the users to cater to information exchange, quick update and give secure communication to the client. It uses different standards like Dedicated Short range Communication (DSRC) [1] and Wireless Access In vehicular Environment (WAVE) [2] for efficient information communication. The DSRC is a short to medium range communication service supports communication in very noisy environment. The DSRC service having seven channels from which one of the channel are control channel and the other six channels are called service channels. Currently, DSRC also called IEEE 802.11p [3] has been proposed for the communication standard, specifically for VANETs.

The main motivation to using VANET is for traffic estimation i.e. to estimate the traffic density in dense areas at any given time by using V2I communication. There are number of ways to estimate the traffic estimation but it does not give that much accuracy as per our requirements. Authors exploited group signature and identity based signature technique in order to secure the communication [7]. Product based solution for reduced check time overcomes the computational overheads of RSU [8]. A comprehensive overview of VANET architecture, routing protocol, and security threats are detailed by authors in [12].

The paper is organized as follows: Section II presents the architecture and Applications of the VANET, Section III: Security threats and privacy protocols. Section IV: Routing Protocols in VANETs. Section V: Conclusion and Future scope.

2. Architecture and applications

VANET Network Architecture is the sub part of MANETS with the movement of vehicles. VANET consist of (i) On board units (OBUs) is a transceiver equipped in vehicle for the exchange of information with the OBU of the others vehicles including the computational devices and RSUs. (ii) Roadside units (RSUs) is a device which are fixed along the roadside and expressways or on specific places such as road curves, parking places etc. It consists of antennas, sensors, processors and transceivers. (iii) Trusted Authority (TA) is meant for the registration for the RSUs, vehicle users and the OBUs of the vehicles. It provides authentication and authorization of OBU of the vehicles in order to prevent from entry of malicious vehicles onto the system.

B. VANET Communication Architecture.

Communication architecture describes the function of communication occurring in VANET system. It can be classified into three categories: (i) Vehicle to Vehicle communication (V2V) refer the communication between the vehicles for exchanging information including warning messages etc. (ii) Vehicle to infrastructure communication (V2I) refer the communication between vehicle roadside units to provide the information related to the current updates of weather and traffic etc. (iii) Vehicle to broad-cloud communication (V2B) refer to the communication between vehicles by making the use of wireless

ISSN:0971-1260
Vol-22-Issue-16-August-2019

broadband communication to provide the real time and an active assistance to the drivers and also responsible for vehicle tracking.

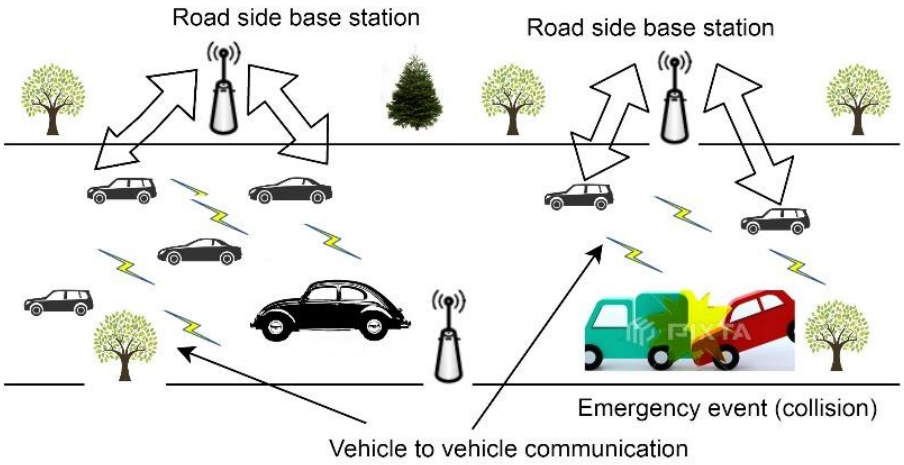

Fig.1: Communication architecture

C. VANET Applications

VANET communication provides mobility services in which, service creator as well as the consumer achieves the better facilities. VANET application [5] can be classified into two main categories: (i) safety based applications; (ii) User/Client based applications

(i) Safety applications: Applications which provide safety and set up the strong relation between producer and consumer are called safety applications.
Collision risk warning: RSUs detects the risk of collision two or more vehicles and broadcast the information to the RSUs to all neighborhood vehicles.
Warning about traffic conditions: If a Vehicle that detects some traffic obstacles, then it broadcast the messages to all RSUs and neighbor vehicles to alternate the path.
Stationary vehicle warning: If any of the vehicles is disabled, due to some obstacle, accident or any other reasons then it broadcast message to RSUs and further to all connected vehicles
Wrong lane driving warning: when a vehicle detects that it is driving in wrong way then signals to the other vehicles and RSUs about this situation.

ISSN:0971-1260
Vol-22-Issue-16-August-2019

Assistance for Lane change: This helps in reducing the blind spots on the road in order to avoid collisions.

(ii) User/Client based application: This application provides information, advertisement and entertainment to the users during their long journeys. Two major client based applications are as follows:
Internet access: Constant internet connectivity has become the first priority of all the users and many of the VANET applications require internet connectivity. So, provide uninterrupted internet access to the user is important.
Peer to Peer application: To lessen boredom, P2P application plays an interesting role in VANETs. Users in the vehicles could play games, movies, music and chat with each other during long journeys.

3. SECURITY THREATS AND THEIR SUPPORTING FEATURES TO VANET.

In the last few years, security becomes the prominent challenge in VANET communication. Any kind of insecure transmission may result into catastrophe. Any successful attack can lead to serious accident, loss of life or economical loss. VANET have to focuses on the improvement of the security communication to secure the users from unbidden threats.

Security threats

Authentication: Authentication gives an assurance to the user that the information generated by it is unfeigned. If one vehicle wants to communicate with other vehicle, it provides verification for secure communication.
Confidentiality: sensitive data must be handled by an authorized user, A particular type of key (PKI) to the user that unauthorized user not easily access.
Integrity: An attacker can interpolate the false information to the network by announcing the false accident report to cause a traffic jam. So, data handling at the servers should be handled in secure way that an unauthorized user can't interpret with it.
Delay handling: Traffic information must be time sensitive, so latency should be avoided and handled.
Reliability: The information received in communication must be correct, real and updated. Periodic updating can eliminate the factual incorrect information.
Non- repudiation: It refers to a sender which cannot be deny that he has transmitted the message.
Spoofing of GPS: An intruder transmits interrupted signals which are more powerful then GPS signal to create the jamming condition into the network.

Features defending VANET security

ISSN:0971-1260
Vol-22-Issue-16-August-2019

Some of features defending the VANET security [9] to made strong establishment in the network.
Real time information: Time and information updated continuously in network, by which every vehicle knows the correct position of all other neighbor vehicles.
Central Authority: Many of the authorized centers are established to control the message transmission, identity authorization, vehicle location and other safety based application.
High power status: All vehicles are equipped with high battery backups, by which it performs uncountable complex calculations.
Electronic Number plate: Every vehicle equipped with registered identification plate known as ELP. This ID is unique ELP which provides safety from attackers and thieves.
Government rules: Attacker caught for intruding in the network should be sentenced under those rules.

4. ROUTING PROTOCOLS IN VANETs.

Many number of security protocols have been implemented to secure the VANET communication by using the concept of Authentication, PKI, Digital signature, etc. VANET is classified with different types of routing such as ad hoc, position based, Geo-cast, broadcastand cluster based routing.
Ad hoc routing protocol: It is also called topology based routing protocol from MANETs is also helpful in VANETs. These routing protocol provide link stability to the nodes by deploying along the highways. Many types of protocols are there to improving stability, real time information, reducing overheads and minimizing bandwidth etc. Mainly three types of ad-hoc routing protocol such as proactive, reactive and hybrid routing protocols. (i) In proactive routing more functionality tables are available with all nodes in order to store complete topology of the network. It updates the table regularly in order to maintain quick updates and broadcast it. (ii) Reactive routing activates the route discovery procedure until destination is achieved. This type of routing protocol is created if required. Therefore it is also known as on demand protocol. (iii) Hybrid is combination of reactive and proactive protocol which makes routing scalable and efficient.

TABLE I: AD HOC ROUTING PROTOCOL

Protocol	**Path metric**	**Network type**	**Objective**
DSDV[10]	Shortest path	V2V	Reduce bandwidth
AODV[11]	Long distance	V2V	Increases stability, decrease overheads
VHRP[13]	Most stable path	V2V, V2I	Reduce throughput
DSR[14]	Long distance	V2V	Conserve battery power, minimize Bandwidth
MOPR[15]	Most stable path	V2V	Reduce data loss by finding stable

ISSN:0971-1260
Vol-22-Issue-16-August-2019

			links
PBR[16]	Most stable path	V2V, V2I	Reduce throughput

Broadcast based routing protocol: It is the frequent broadcasting technique to spread the message among the vehicles and between V2I. But large connectivity network creates many obstacles to reduce its performance.

TABLE II: BROADCAST ROUTING PROTOCOL.

Protocol	**Network type**	**Network deployed**	**Objective**
TRRS[17]	V2V	Expressways	Reduce packet loss
Probabilistic[18]	V2V, V2I	Expressways	Minimize propagation delay
AMB[19]	V2V	Prohibited highways	Minimize propagation delay, packet loss
MHVB[20]	V2V	Prohibited urban areas	Minimize propagation delay, packet loss
UMB[21]	V2V, V2I	Urban areas	Minimize packet loss and hidden terminal problem

Geo-cast routing protocol: In this routing protocol, flooding technique is used to broadcast the message throughout the areas and uses multicasting service which reduces collision.

TABLE III: GEOCAST ROUTING PROTOCOL.

Protocol	**Path metric**	**Network type**	**Objective**
GSR[22]	Shortest distance	V2V	Better delivery rate and response time
VADD[23]	Least delay	V2V, V2I	Reduce end-to-end delay
GPSRJ+[24]	Greedy directional	V2V	Improve delivery rate of GPCR
GPCR[25]	Greedy directional	V2V	Better delivery rate of GSR
PROMPT[26]	Least delay	V2V, V2I	Reduce end-to-end delay
SADV[27]	Least delay	V2V, V2I	Reduce end-to-end delay

Position based routing protocol: Position/geography based routing forwards the message using geographical location to the next node. No routes or routing table are required to maintain. GPS, street

ISSN:0971-1260
Vol-22-Issue-16-August-2019

maps, OBU applications are enough for data transmission. The topology changes frequently from next-to-next hop. So, topology based routing is not used.

TABLE IV: POSITION BASED ROUTING PROTOCOL.

Protocol	**Metric**	**Network type**	**Objective**
CLWPR[28]	Urban areas	V2V	Increase packet delivery ratio
DUPE[29]	Urban areas	ITS,V2V	Solve packet loss issue if path failure
PPMR[30]	Dedicated range	V2V	Minimize the route discovery latency
PBRP[31]	Dedicated range	V2V	High packet delivery ratio
DAPB[32]	Long distance	V2V	Increase the longevity of the route

Cluster based routing protocol: This protocol is mainly used for large networks by which vehicles are participated itself to make a cluster. Many of clusters connects to a particular cluster head who gathers all types of information like speed, velocity, relative speed and Re-affiliation rate from the RSUs and broadcast it to all connected vehicles.

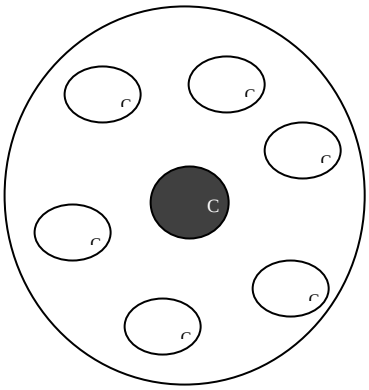

Fig.2: Ideal cluster with cluster head around the cluster nodes

TABLE V: CLUSTER BASED ROUTING PROTOCOL.

Protocol	**Path metric**	**Network type**	**Objective**

ISSN:0971-1260
Vol-22-Issue-16-August-2019

AODV-R[33]	Shortest path	V2V	Better data aggregation, route
TCRP[34]	City	V2V	Stability and interconnectivity of cluster
CMAC[35]	Highways	V2I, V2V	Low delivery rate, high throughput and reliability.
STCM[36]	Highways	V2V	High throughput, real time msg. delivery
MOZO[37]	Urban areas	V2V	High message delivery rate.
COMIP[38]	Highways	V2V, V2I	Minimizing handoffs

5. CONCLUSION AND FUTURE SCOPE.

In this paper, we mainly focused on the fundamental of vehicular network with its architecture, applications, security threats and privacy protocols. Vehicular technology is increasing momentum as the vehicles increasing abruptly. Advancement in VANET lights up new ideas and scopes to the researchers. According to recent researches, VANET gives a new path to the upcoming modern wireless applications and establishes strong network for producers as well as consumers. In the last decade survey papers, security becomes the main issue to degrade the performance of VANETs. We reviewed with number of security protocols who makes network secure, scalable and efficient.

REFERENCES

[1] Yin, J., Elbatt, T. &Habermas, S., "Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks", in Proceedings of *VANET'04,* Philadelphia, PA, USA, October, 2004.
[2] Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., Hassan, A.: 'Vehicular ad hoc networks (VANETS): status, results, and challenge', Telecommun. Syst., 2010, 50, (4), pp. 217–241.
[3] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans.Veh.Technol.*, vol. 56, no. 6, , pp. 3442–3456. Nov. 2007.
[4] S. Horng*et al.*, "b-specs+: Batch verification for secure pseudonymous authentication in vanet," *IEEE Tran. Inf. Forensics Security,* vol. 8, no. 11, pp. 1860–1875, Nov. 2013.
[5] Charles E.Perkins et Pravin Bhagwat.(1994). Highly dynamic destination sequenced Distance-Vector Routing (DSDV) for Mobile Computers Proceedings of the Conf. on Communication architectures, Protocols and Applications (SIGCOMM'94), volume 24. October 1994. Pp 234–244.
[6] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications",in*Proc. IEEE INFOCOM*, Phoenix, AZ, USA, pp. 1903–1911 Apr. 13–18, 2008.
[7] T. Taleb, M. Ochi, and Y. Nemoto, "An efficient vehicle-heading based routing protocol for VANET networks", *IEEE Wireless Communications and Networking Conference*, vol. 4. IEEE WCNC '06, 2006.

ISSN:0971-1260
Vol-22-Issue-16-August-2019

[8] V. Rajeshkumar, P. Sivakumar, Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2 », IJARCCE ,Vol. 2, Issue 12, December 2013
[9] M. Menouar, M. Lenardi, F. Filali, H. Eur, and S. Antipolis, "Improving Proactive Routing in VANETs with the MOPR Movement Prediction Framework," in *Proc. 7th International Conference on ITS 2007(ITST'07)*. ITST '07, 2007, pp. 1–6.
[10] V. Namboodiri and L. Gao, "Prediction-based routing for vehicular ad hoc networks," *IEEE Trans. Veh. technol.*, vol. 56, no. 4, pp. 2332– 2345, 2007.
[11] T. Kim, W. Hong, and H. Kim, "An effective multi-hop broadcast in vehicular ad-hoc network," *Lecture Notes in Computer Science*, vol. 4415, pp. 112–125, 2007.
[12] N. Wisitpongphan and O. K. Tong¨uz and J. S. and Parikh and P. Mudalige and F. Bai and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Commun.,* vol. 14, no. 6, pp. 84–94, December 2007.
[13] G. Korkmaz, E. Ekici and F. O¨ zguner, "Black-burst-based multihop broadcast protocols for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 3159–3167, September 2007.
[14] T. Osafune, L. Lin, and M. Lenardi, "Multi-Hop Vehicular Broadcast (MHVB)," in *Proc. 6th International Conference on ITS Telecommunications(ITST 2006)*. ITST 2006, June 2006, pp. 757–760.
[15] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in *Proc. IEEE Intelligent Vehicles Symposium*. IEEE, 2005, pp. 69–72.
[16] J. Zhao and G. Cao, "VADD: vehicle-assisted data delivery in vehicular ad hoc networks," *IEEE Trans. Veh. Technol. (TVT 2008)*, vol. 57, no. 3, pp. 1910–1922, 2008.
[17] K. Lee, J. Haerri, "Enhanced perimeter routing for geographic forwarding protocols in urban vehicular scenarios," in *Proc. IEEE GLOBECOM Workshop*. IEEE GLOBECOM, 2007, pp. 1–10.
[18] M. Mauve, H. Fussler, H. Hartenstein, and C. Lochert, "Geographic routing in city scenarios," *ACM SIGMOBILE Mobile Computing andCommunications Review*, vol. 9, no. 1, pp. 69–72, 2005.
[19] B. Jarupan and E. Ekici, "PROMPT: A cross layer position-based communication protocol for delay-aware vehicular access networks," *AdHoc Neworks (Elsevier) Journal Special Issue on Vehicular Networks*, vol. 8, no. 5, pp. 489–505, July 2010.
[20] Y. Ding, C. Wang, and L. Xiao, "A static-node assisted adaptive routing protocol in vehicular networks," in *4th ACM international workshopon Vehicular ad hoc networks*. ACM, 2007, pp. 59–68.