ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

A Comprehensive Review on Vehicular Ad hoc Network

Anuradha Singh[1], Mintu Singh[2]

M-Tech Student, Department of CSE, Echelon Institute of Technology Faridabad, India[1]

Assistant Professor, Department of CSE, Echelon Institute of Technology Faridabad, India[2]

Abstract: Vehicular Ad-hoc Network (VANET) is a most critical class of mobile ad-hoc network (MANET) which enables intelligent communication among vehicles and also between vehicle and roadside infrastructures. It is a promising approach for the Intelligent Transport System (ITS). There are many challenges to be addressed when employing VANET. It has a very high dynamic topology and constrained mobility which makes the traditional MANET protocols unsuitable for VANET. The aim of this review paper is to give an overview of the vehicular ad hoc networks, its standards, applications, security issues and the existing VANET routing protocols.

Keywords: VANET, ITS, dynamic topology, mobility, routing protocols.

I. INTRODUCTION

The vision of whole cities covered with dynamic networks of "talking cars" is gradually becoming a reality[1]. The networks so formed are called Vehicular Ad hoc Networks (VANETs). VANET consist of a number of dynamically moving nodes, creating an ad hoc network. It turns every participating vehicle into a wireless router and allow them to connect with each other within 300 meters of range. Vehicles are equipped with Intelligent Transportation System which potentially have extensive on-board storage capacities, longer transmission ranges and rechargeable sources of energy[2].

The mobility of vehicles is constrained by predefined paths, node's speed limit or the congestion level. Advanced wireless technologies enable direct and instant communication among vehicles (Vehicle-to-Vehicle V2V) as well as between vehicles and the road infrastructure (Vehicle-to-Infrastructure V2I)[1].

Finding a route to a certain destination is a common experience for all drivers. In the old days, a driver usually refers to a hardcopy of the atlas. The drawbacks are quite obvious[3]. Routing protocols are used to route the data packets to destination. The main aim of routing protocol is to provide optimum path between two nodes with minimum overhead. Special features of VANETs routing including ever changing network topology, geographical constraints, high dynamics, predicable mobility, high computational capability, high transmission power, partitioning and large scale, and mobility models, make it different to routing in mobile ad-hoc networks (MANETs) [4][5].

To evaluate VANET protocols and applications, outdoor experiments can be used but it can be difficult and expensive to implement because it involves high number of vehicles and real-life scenarios. To overcome these problems, simulation tools are used extensively for VANET simulations [6].

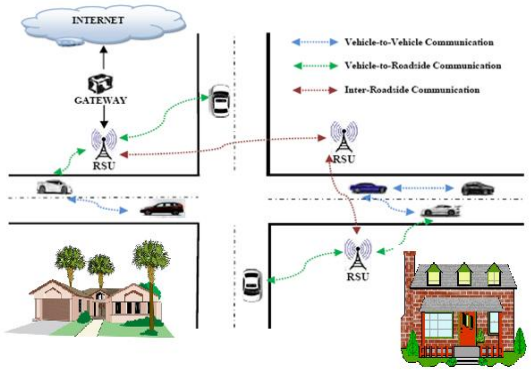

Figure1. Vehicular Ad hoc Network

VANET can be used for a broad range of Safety and Non-Safety applications. It includes sharing of multimedia information and traffic control. When applied to the traffic control, it is helpful in avoiding accidents by distributing information about the road situation, such as traffic accidents and road congestion. Therefore, it can effectively manage city traffic, reduce accidents and improve safety with high efficiency. It can also helps to share some information between vehicles, such as weather forecast, gas station and restaurant addresses. VANET can also provide music or video download services when it is connected to Internet as terminal networks [7]. It also allows many value added services like automated toll payment, traffic management, vehicle safety, location based services like finding closest restaurant, travel lodge, fuel station and infotainment applications like access to internet [8].

II. VANET ARCHITECTURE

In Vehicular network System, vehicles are considered as nodes which can move freely within a network and stay connected, even if they are at high speed. Each vehicle can communicate with other vehicle via DSRC (Dedicated Short Range Communication) [9]. The communication between different units of this system is achieved through a

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

wireless medium known as WAVE (Wireless Access For Vehicular Environment). WAVE provides a wide range of information to the entities (drivers and travelers) of the system and also enables safety application to enhance road safety[10].

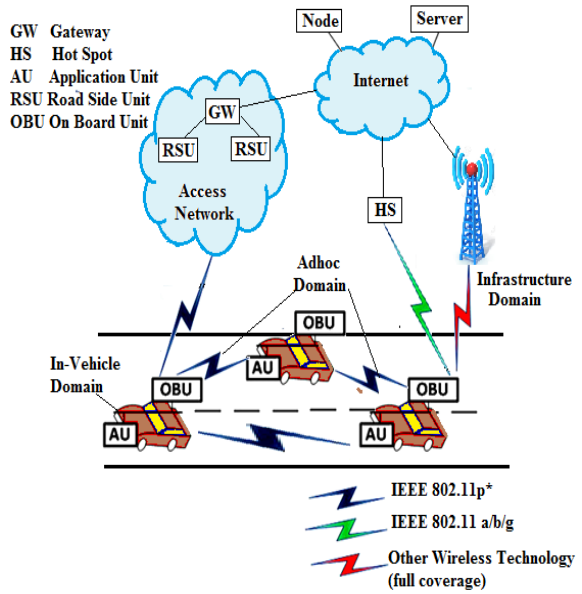

Figure2. VANET Architecture

VANET consists of different domains and many individual components [11]. Three distinct domains:

i. *In-Vehicle Domain*
This consists of one or more Application unit (AU) and On-board Unit (OBU) inside a vehicle. Both AU and OBU can reside in a single physical unit.

ii. Ad hoc Domain
This consists of vehicles equipped with OBU and Road Side unit (RSU), forming VANET. OBU forms a mobile ad hoc network which allows communication between the nodes so there is no need for a centralized coordinator.

iii. Infrastructure domain
In this, the infrastructure consists of RSU and wireless Hot spot (HT), accessed by vehicles for safety and non-safety applications. Internet access from RSU are setup by road administrator and hotspots that are publicly or privately owned, are set up in a less controlled environment.VANET consists of some individual components that are:

A. *On Board Unit (OBU)*
On Board Unit is a wave device which is mounted on-board a vehicle.OBU connects the vehicles with other OBUs and RSUs. It is used to exchange the information between other units via DSRC.DSRC is a short range communication system which is used to provide high data transfer rates and minimum latency in communication link. OBU consists of RCP (Resource Command Processor) and resources with read/write memory used to store and retrieve information, user interface, network device for wireless communication, interface to with other OBUs. It basically deals with ad hoc routing, geographical routing, wireless radio access, reliable message transfer, IP mobility, network congestion control, security of data[10].

B. *RSU (Road Side Unit)*
Road side unit is a wave device which is fixed along the roads or in dedicated locations such as junction and near parking spaces.RSU acts as router between the vehicles on road and other network devices. It helps in extending the communication range of ad hoc network, running safety application and providing Internet connectivity to OBUs[10].Main functions of RSU are:

i. RSU extends the communication range of an ad hoc network by forwarding and distributing the information to other OBU and RSU.
ii. ii. It acts as information source and receiver and provides internet connectivity to OBUs.

C. *AU (Application Unit)*
Application Unit is a device equipped in vehicles which communicates with the network through OBU [8]. AU is an in-vehicle entity and executes a set of applications utilizing the communication capabilities of OBU[10].

III. VANET COMMUNICATION STANDARDS
The requirements of interconnectivity and interoperability can be guaranteed only by the use of standard. Also, the standard can helps to verify the emergence of new products to enable rapid implementation of new technologies. Various standards that relate to wireless access in vehicular environment are[12]:

A .Dedicated Short Range Communication (DSRC):
DSRC (Dedicated Short Range Communication) is a short to medium range communication service that offers communication between Vehicle to Vehicle (V2V) and Vehicle to Road Side Unit (V2R).

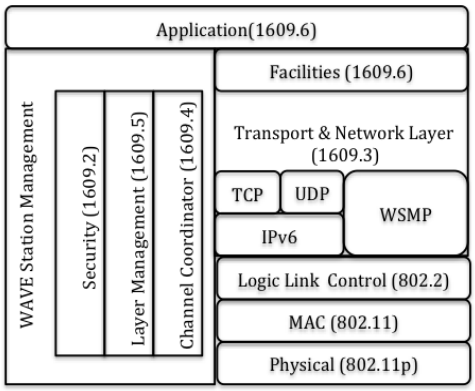

Figure3. Dedicated Short Range Communication

It provides high data transfers and low latency in small communication zones. The Federal Communication Commission (FCC) allocated 75 MHz of spectrum at 5.9 MHz to be used by DSRC. The DSRC spectrum is divided into seven channels, each 10 MHz wide. One channel is restricted for safety communication, two other channels are for special purposes and remaining channels are

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

service channels for either safety or non-safety applications.

B. IEEE 1609 – Standards for Wireless Access in Vehicular Environments (WAVE) (IEEE 802.11p)

Due to special challenges of VANET, the technology 802.11 used in Mobile Ad Hoc Network (MANET) results in low performance in VANET.

To overcome this problem, ASTM migrated to IEEE 802.11 standard group which renamed DSRC to IEEE 802.11p Wireless Access in Vehicular Environment(WAVE).

The complexity and operational functions of DSRC are carried out by upper layers of IEEE 1609 standards which define how application that utilize will function in WAVE environment .

IV. VANET ROUTING

Routing is a process of finding a path from source to destination. The main aim is to send the data packets among randomly distributed nodes in a network [13].

High mobility of nodes and rapid changes of topology are the main factors that influence the need of generating an efficient routing protocol which can deliver a packet in minimum period of time.

A well designed routing protocol can increase the reliability and scalability of the system and can reduce interference to a great extent.

Types of Routing Protocol:

1) Pro-active Routing Protocol
2) Reactive Routing Protocol

A. *Pro-active Routing Protocol*

In this, a table called Routing Table that stores information about all the routes, is maintained whether route is necessary or not. So, it is also called as Table-Driven Protocol.

The table is updated with change in network topology and is broadcasted periodically. Shortest Path Algorithm is used to find out entire path. DSDV (Destination Sequenced Distance Vector), OLSR (Optimized Link State Routing) are Table Driven protocols [6].

Advantages:

- Route is always available.
- No route discovery is required.
- Low latency for real time applications.

Disadvantages:

- It becomes difficult to maintain routing table as the network size increases.
- It leads to overhead in high mobility network.
- Not for larger networks [14].
- Consumption of more bandwidth [14].

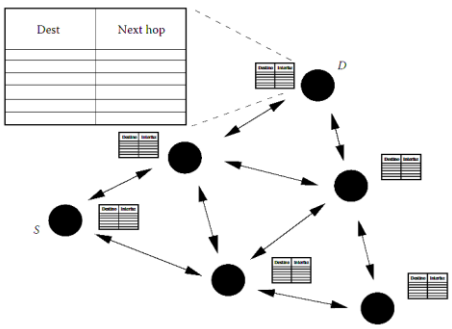

Figure5. Proactive Routing Scheme

B. Reactive Routing Protocol

In this protocol, route between source and destination is determined on a demand or need basis. So, it is also called as On-Demand Routing Protocol. It establishes a route only when a node requests for it by initiating a route discovery process [15]. Reactive routing protocol do not store or continuously update their routing tables with new route topology. If a node wants to send a packet to another node then it searches for the best possible route and establishes the connection to transmit and receive the packet. The route discovery is established by flooding the route request packets throughout the network [14]. AODV (Ad hoc On Demand Distance Vector), DSR (Dynamic Source Routing) are On-Demand Routing Protocols[6].

Advantages:

- Reduced burden on network.
- Easy to maintain routing information.
- Suitable for application scenarios.

Disadvantages:

- Limited number of routes.
- Finding routes lead to high latency.
- Failed to discover a complete path due to frequent network partition.

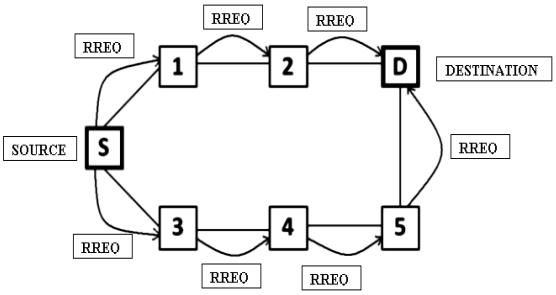

Figure 6. Route Request Reactive Routing

V. VANET SIMULATION

Evaluation of different application and protocols could be made via real outdoor experiment but they are time costly and claim a large number of resources. Instead, Simulation can be used to evaluate different simple or complicated or innovative solutions before implementation [16].

Implementing a network on computer is done through network simulators that allow researchers to test scenarios which are difficult and expensive to simulate in real world [17]. Network Simulators helps to study how network

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

would behave under a given set of conditions, as per user's requirement .Network simulators are relatively fast and inexpensive as compared to the cost and time involved in setting up an entire test bed containing multiple networked computers, data links and routers[18]. Various network simulators are:

A . NS-2:

NS-2(Network Simulator Version 2) is a discrete event simulator developed under VINT (Virtual Inter Network Test bed) at the University of California in 1995[18].NS-2 need Cygwin software to install it in window.

Features:

- Support TCP, routing and multicast protocol.
- Open Source
- Modularity
- Complex scenarios can be easily tested.

Limitations:

- Unreliable bugs.
- Too complex to model real system i.e. complicated structure.

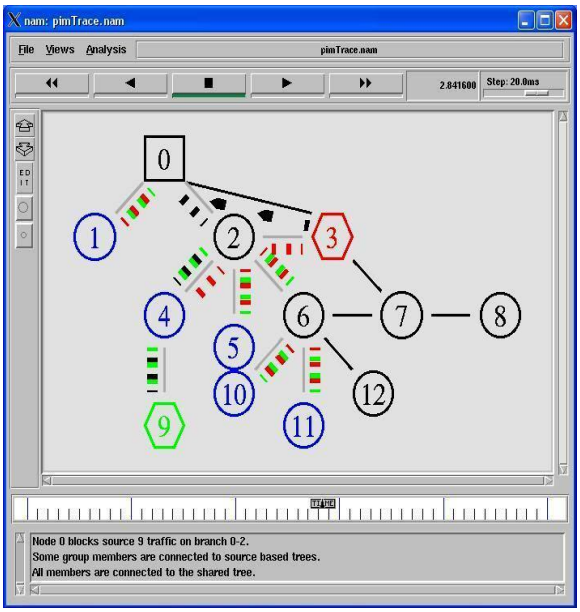

Figure7. Network Simulator (Version 2)

B. QualNet

QualNet is the commercial network simulator from Scalable Network Technologies. It can simulate large, heterogeneous networks and distributed application that executes on such network [17].

Features [20]:

- Optimized for scalability and speed on one processor.
- Executes simulation multiple times faster as compared to processor.
- Simulate models with as many as 60,000 mobile nodes.

C. *OPNET:*

Optimized Network Engineering Tools (OPNET) was acquired by Riverbed Technologies in 2012. It provides a wide variety of possibilities to simulate entire heterogeneous network with various protocol [17].

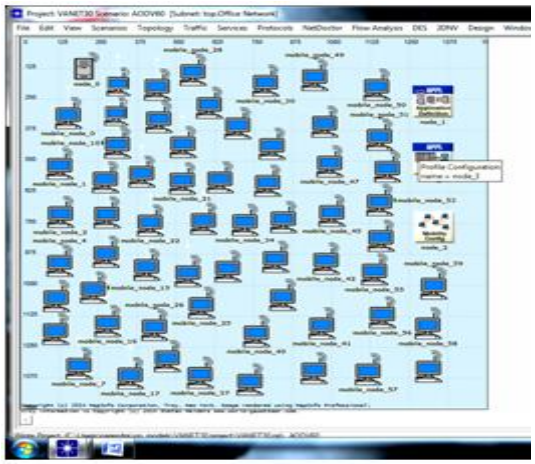

Figure 8. OPNET GUI Window

Features:

- Scalable wireless simulation support.
- Integrated, GUI based debugging and analysis
- Object oriented modeling
- Open interface for integrating external component libraries.
- Supports hybrid simulation.

Table1. Comparison of Network Simulators [19]

	NS-2	**QualNet**	**OPNet**
VANET			
IEEE 802.11	Only for ns-2.33	No	Yes
Software			
Portability	Yes	Yes	Yes
Open Source	Yes	No	No
GUI	Yes	Yes	Yes
Continuous Development	NS-3	Yes	Yes
Parallel Processing	No	Yes	Yes
Ease of use	Hard	Moderate	Moderate
Ease of setup	Easy	Moderate	Moderate
Examples	Yes	Yes	Yes
Scalability	Poor	High	High
Programming Language	C++ & OTcl	C/C++	C

VI. VANET SECURITY ISSUES

With dynamic nature and high mobility, use of wireless media makes VANET vulnerable to attacks which can exploit broadcast and open nature of wireless communication. Unique characteristics of VANET leads to unique security challenges [21]. Some serious attacks of VANET are:

A. *Sybil Attack*

Sybil Attack allows a malicious sender to create a number of fake identities called Sybil nodes and behaves as a

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

normal node. It depends on how cheaply fake identities can be generated, the degree to which a system accepts input from those identities that do not posses a chain of trust linking them to a trusted authority, and whether the system identically treats all entities [10].

B. Warm Hole Attack

Using an extra communication channel called tunnel, attacker connects two distinct parts of ad hoc network. As a result, two distant nodes send data using this tunnel, assuming that they are neighbours. Wormhole Attack is occurred between two malicious nodes/worms connected through a high speed wired or wireless link called Worm hole link or tunnel [22]. It is hard to detect as the path used to transmit the data packets is not a part of actual network.

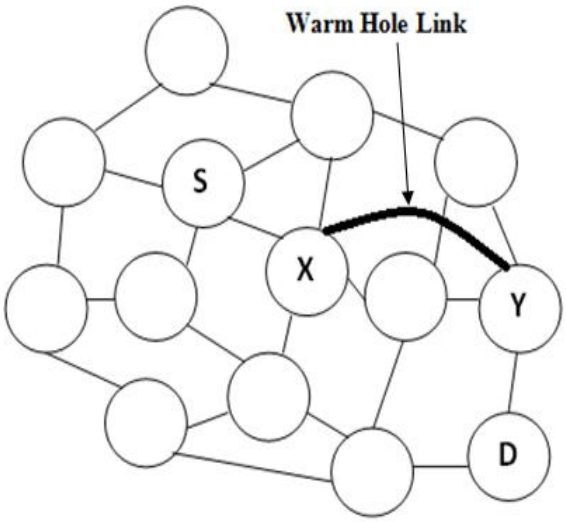

Figure 9. Warm Hole Attack

C. Sink Hole Attack

Sink Hole Attack prevents the Road Side unit/Base station from obtaining correct and complete sensing information. Intruder attracts surrounding nodes with unfaithful routing information and then selectively forwards or alters the data packets passing through the network.

It severely affects wireless sensor networks given the vulnerability of wireless links.

D. Jamming Attack

Jamming Attack is a special case of DoS attack. DoS attack aimed at disrupting the complete routing information. Attacker/Jammer transmit a signal along with security threat and prevents reception of legitimate data packets [23].

E. Black Hole Attack

The malicious node advertises the shortest path to reach the destination node during route discovery process in AODV. The malicious node tries to drop all data packets or to hinder the entire route discovery process.

So, Black hole node receive the data packets if it is the destination else drop the packets[24].

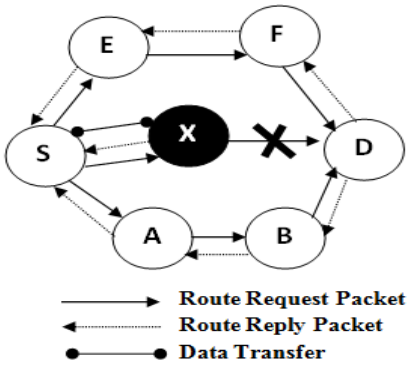

Figure10. Black Hole Attack

VII. VANET APPLICATIONS

Communication between the vehicles has led to the development of a number of applications and provides a wide range of information to drivers and travelers. This has increased the road safety and comfort of the passengers. Applications can be classified into two, on the basis of their purpose.

A. Comfort Application

It is also called Entertaining application. These are non-safety applications, aiming at improving the comfort level of drivers and travelers.

B. Safety Application

These applications focus on improving road safety and in avoiding accidents by using the wireless communication between the vehicles or between vehicles and infrastructure.

1) Vulnerable Individual Protection
2) It includes services like audio message for blind person.
3) On Coming Traffic Warning It helps the driver about overtaking maneuvers, by provide information about in-coming traffic.
4) Traffic Signal Violation RSU broadcast messages to warn vehicles about violation in traffic signal.
5) Public Safety Public safety applications are required if an accident has been physically reported. It alerts the vehicles so that they can give a way to the emergency vehicle.

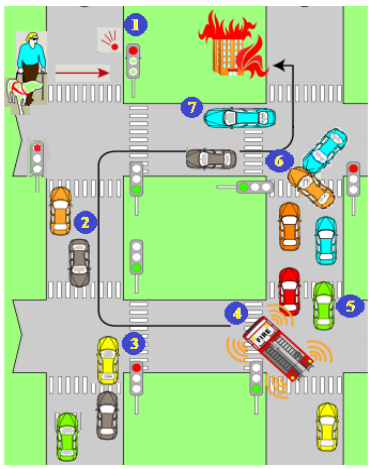

Figure12. VANET Application

DOI 10.17148/IJARCCE.2015.44106

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

1) Electronic Brake Warning
2) It informs the driver that sudden braking is performed by a preceding vehicle.
3) Post Crash Notification
4) Vehicle involved in accident alerts other approaching vehicles by broadcasting warning messages.
5) Intersection Violation Warning

This Intersection violation warning application warn drivers when they are going to pass over a red light.

VII. VANET LITERATURE REVIEW

Author	Year	Work
Sommer et al. [26]	2008	Described bidirectionally coupled simulation framework using the road traffic simulator SUMO and network simulator OMNET++.
J. Zhao et al; [26]	2008	Described a Vehicle-Assisted Data Delivery (VADD) protocol for sparsely connected VANETs. It adopts the idea of "carry-and-forward" in which nodes "carry" packets when there are no routes to the destination under sparse conditions.
Chen, Jiang et al; [28]	2009	Simulate, using ns-2, the effect of IEEE 1609.4 multichannel operations. They show that with channel switching enabled, the performance for safety related communications becomes "unacceptably poor" and recommend an update/revision to the standard.
Y.H. Choi [29]	2009	Proposed an Adaptive Location Division Multiple Access (A-LDMA) scheme to handle safety messages that are sent in one-hop broadcast mode (beacon) along with event-triggered multi-hop relayed (flood) messages.
Wagan, A. A., et al.[30]	2011	Presented a hardware-based security framework that uses both standard asymmetric PKI and symmetric cryptography for faster and secure safety message exchange.
Biswas et al; [30]	2013	Designed an ID-based anonymous user authentication scheme and a cross-layer verification approach to WAVE-enabled VANET's safety messages.
Pradweap et al; [31]	2013	Proposed a novel Road Side Unit (RSU)-aided design which uses one word Certificate Less Sign Cryption (CLSC), without pairing, to provide anonymous authentication. It works efficiently even in the absence of RSU.
Prado et al.[32]	2013	Proposed a new private and reliable geo casting protocol which uses adaptive traffic restriction and dynamic probabilistic forwarding for reliability
Divya Gupta et al; [33]	2014	Improved Genetic Based Routing Protocol for VANETs, using spanning tree and routing tree. The main aim of this paper is to minimize the delay from source node to destination by using genetic algorithm.

CONCLUSION AND FUTURE SCOPE

VANET is a promising technology and with the substantial advancement in wireless technology, vehicles are becoming a vital part of global network. VANET will not only provide life saving applications but will also become a powerful communication tool for users. Here, focus is paid on basic architecture of VANET, routing , simulation, attack and application.

Fulfilling the requirements and facing challenges will result in an efficient communication tool which can also provide life saving tools to the users [6]. If improved it can give better results than other mobile ad hoc network. Vehicles can be designed in a way that they possess learning abilities so as to have perception of potential dangers and to modify vehicle's behaviour consequently. It can help vehicle to take decisions from it's past experience.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

REFERENCES

[1]. Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a , vol., no., pp.1,6, 25-28 June 2012

[2]. Jie Li, Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" , IEEE Transactions on Parallel and Distributed Systems, 2012

[3]. Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," Computers, IEEE Transactions on , vol.63, no.2, pp.510,524, Feb. 2014

[4]. Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on , vol., no., pp.611,615, 8-10 Aug. 2012

[5]. Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survay and taxonomy," Communications Surveys & Tutorials, IEEE , vol.11, no.4, pp.19,41, Fourth Quarter 2009

[6]. Sun Xi; Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," Wireless communication, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on , vol., no., pp.1,4, 12-14 Oct. 2008.

[7]. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen,Angela Irwin, Aamir Hassan," Vehicular Ad hoc Networks(VANET):Status, Results, Challenges". Springer Science, Business Media.2010

[8]. Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.

[9]. Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.550,555, 22-23 Feb. 2013

[10]. Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.

[11]. Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," Vehicular Technology Conference, 2011 IEEE 73rd , vol., no., pp.1,5, 15-18 May 2011

[12]. Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," Communications and Signal Processing (ICCSP), 2013 International Conference on , vol., no., pp.1170,1174, 3-5 April 2013

[13]. Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on , vol., no., pp.1,5, 26-28 July 2013

[14]. Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[15]. Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," Communications Letters, IEEE , vol.18, no.1, pp.110,113, January 2014

[16]. Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," Communications and Information Technologies (ISCIT), 2014 14th International Symposium on , vol., no., pp.26,27, 24-26 Sept. 2014

[17]. Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.550,555, 22-23 Feb. 2013

[18]. Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on , vol.3, no., pp.261,265, 25-27 May 2012

[19]. Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on , vol., no., pp.152,157, 10-12 Feb. 2014

[20]. Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," ELEKTRO, 2014 , vol., no., pp.424,429, 19-20 May 2014

[21]. Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian , vol., no., pp.135,140, 26-28 Nov. 2014

[22]. Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," Computing for Sustainable Global Development (INDIACom), 2014 International Conference on , vol., no., pp.792,797, 5-7 March 2014

[23]. Mehta, K.; Malik, L.G.; Bajaj, P., "VANET: Challenges, Issues and Solutions," Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on , vol., no., pp.78,79, 16-18 Dec. 2013

[24]. Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian , vol., no., pp.1,6, 7-9 Nov. 2012

[25]. Shuai Yang; Rongxi He; Ying Wang; Sen Li; Bin Lin, "OPNET-based modeling and simulations on routing protocols in VANETs with IEEE 802.11p," Systems and Informatics (ICSAI), 2014 2nd International Conference on , vol., no., pp.536,541, 15-17 Nov. 2014

[26]. Sadeghi, M.; Yahya, S., "Analysis of Wormhole attack on MANETs using different MANET routing protocols," Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on , vol., no., pp.301,305, 4-6 July 2012

[27]. Jhaveri, Rutvij H.; Patel, Ashish D.; Dangarwala, Kruti J., "Comprehensive Study of various DoS attacks and defense approaches in MANETs," Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on , vol., no., pp.25,31, 13-14 Dec. 2012

[28]. C. Sommer, Z. Yao, R. German, and F. Dressler, "On the need for bidirectional coupling of road traffic micro simulation and network simulation," in Mobility Models '08: Proceeding of the 1st ACM SIGMOBILE workshop on Mobility models. New York, NY, USA: ACM, 2008, pp. 41–48

[29]. Zhao and G. Cao, "Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks," Vehicular Technology, IEEE Transactions on, vol. 57, no. 3, pp. 1910 –1922, may 2008.

[30]. Q. Chen, D. Jiang, and L. Delgrossi, "Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications," in Vehicular Networking Conference (VNC), 2009 IEEE, oct. 2009, pp. 1 –8.

[31]. Y. H. Choi, R. Rajkumar, P. Mudalige, and F. Bai, "Adaptive location division multiple access for reliable safety message dissemination in vanets," in Wireless Communication Systems, 2009. ISWCS 2009. 6th International Symposium on, sept. 2009, pp. 565 –569.

[32]. Biswas, S., & Misic, J to Privacy-preser. (2013). "A Cross-layer Approach ving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192

[33]. Pradweap, R. V., & Hansdah, R. C. (2013). A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET. In Information Systems Security (pp. 314-328). Springer Berlin Heidelberg.

[34]. Prado, A., Ruj, S., & Nayak, A. (2013, June). "Enhanced privacy and reliability for secure geocasting in VANET." In Communications (ICC), 2013 IEEE International Conference on (pp. 1599-1603). IEEE.

[35]. Gupta, D.; Kumar, R., "An improved genetic based Routing Protocol for VANETs," Confluence The Next Generation Information Technology Summit, 2014 5th International Conference -, vol., no., pp.347, 353, 25-26 Sept. 2014