ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 10, Issue, 06(I), pp. 33298-33303, June, 2019

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

A STUDY ON VANET AND ITS SECURITY ISSUES

[1]Krishna Verma, [2]Ritika Yaduvanshi, [1]Shashank Shekhar Tiwari , [1]Prince Rajpoot, and [1]Shivendu Mishra

[1]Department of Information Technology, Rajkiya Engineering College Ambedkar Nagar (U.P), India
[2]Department of Computer Science and Engineering, Mahamaya College of Agricultural Engineering and Technology, Akbarpur, Ambedkar Nagar (U.P), India

DOI: http://dx.doi.org/10.24327/ijrsr.2019.1006.3646

ARTICLE INFO

Article History:
Received 6th March, 2019
Received in revised form 15th April, 2019
Accepted 12th May, 2019
Published online 28th June, 2019

Key Words:

RSU (Road Side Unit), V2I (Vehicle to Roadside Infrastructure), V2V (Vehicle to Vehicle), IVC (Inter Vehicle Communication), OBU (On Board Unit), AU (Application Unit)

ABSTRACT

Vehicular ad hoc Network or VANET is a sub form of Mobile ad hoc Network or MANET that provides us communication between vehicles and also between vehicles and road side base stations. Since we know vehicles generally proceed at a high speed, hence the network topology also changes quickly. It's an important and bright application of the Intelligent Transport System or ITS. In order to achieve safety and security in Vehicular Transportation, we can implement VANET as there happens an Inter Vehicular Communication. Also, there are many challenges when it comes about implementing VANET. This Survey Paper's goal is to provide an overview on VANETs, its Measures, Security Issues, Applications and existent VANET routing protocols.

INTRODUCTION

In today's life the large volume of traffic tends to affect the safety and effectivity of the whole traffic surroundings. A huge number of people died in road accidents all around the globe every year. It has always been a challenge to stop and avoid all such accidents and provide people's safety. Safety applications are very important in nature since these are directly associated to the users and their lives. One of the promising ways is providing the traffic situations to the vehicles around so that it can be used to analyze the traffic conditions of the vehicles all around which can be detected by sharing of information between them. With enhancement in the technology of microelectronics, it has now become possible to integrate nodes and network devices into a single unit and wireless interconnections [1]. VANET is one of the important applications of Mobile ad-hoc Networks (MANETs). VANET is that technology which delivers naturalistic vehicle to vehicle (V2V) and vehicle to roadside infrastructure (V2I) communications. VANET is a self-formed system in which vehicle works as node and to form these networks WIFI technologies are used. VANET is used for making an intelligent transportation system (ITS) that makes roads safer, provides traveler welfare and traffic efficiency. Achievement in VANET relies upon the essential elements like statistics routing in between nodes and the entrance to the internet. Vehicular ad hoc Networks (VANETs) lead to the foundation of Intelligent Transportation System (ITS) which is done by making vehicles able to communicate to each other through Inter-Vehicle Communication (IVC) also with safer and more efficacious roads by giving appropriate information to the drivers and interested authorities.

Simulating study area on Vehicular Network can only be done where we can bring the ad hoc system to its entire potency. When this statistical data got exchanged repeatedly on frequent times then it clearly points out towards the role of security. In order to communicate securely it is very important that the statistical data should be transmitted accurately from source to destination for the safety program. Therefore, security is such a vital issue that cannot be ignored in a case. Attackers may generate difficulties by accessing the system fully hence any kind of malicious attack can result in loss of lives and loss of money as well. Therefore, information's and data's protection are very critical in VANET system [2].

Corresponding author:* **Krishna Verma
Department of Information Technology, Rajkiya Engineering College Ambedkar Nagar (U.P), India

Architecture and Infrastructure

VANET's framing is done with the three kinds of fields which are mobile, generic and infrastructure. It is also built up with some elements like application units, on-board units, and road-side units. A brief description is given below.

Generic Domain

The generic domain is made up of three parts as follows:

In-Vehicle Domain

In in-vehicle domain there is one on-board unit (OBU) and one or more application units (AUs). Generally, these are connected with wired medium but sometimes wireless too. Application Units are the in-vehicle entities and several AUs can be incorporated by only one OBU which shares the processing of OBU and also wireless resources. The main work of OBU is to give the vehicle-to-vehicle and vehicle-to-infrastructure communications. The OBU is equipped by one network device. Generally, a network device is used to send, receive and accelerate the messages about safety and non-safety, to the ad-hoc domain.

Ad-hoc Domain

This ad-hoc domain is built up of vehicles in which OBUs and RSUs are fitted. In ad hoc network an OBU works as a mobile node and RSU as a static node. We can connect the RSU to the internet via the gateway through which RSUs can make a communication with them. Main work of RSU is providing the internet connectivity for the OBU. Hence OBU make a mobile ad hoc network which gives permission to the vehicles for communication among them.

Infrastructure Domain

RSU- Road Side Unit is such a device which is placed at few non-moving places of roads and highways and also at few stable locations like hospitals, shopping complexes, restaurants, parking places, organization buildings, schools etc. It is furnished with one network device. RSU's main function is the Internet connectivity with the OBUs.

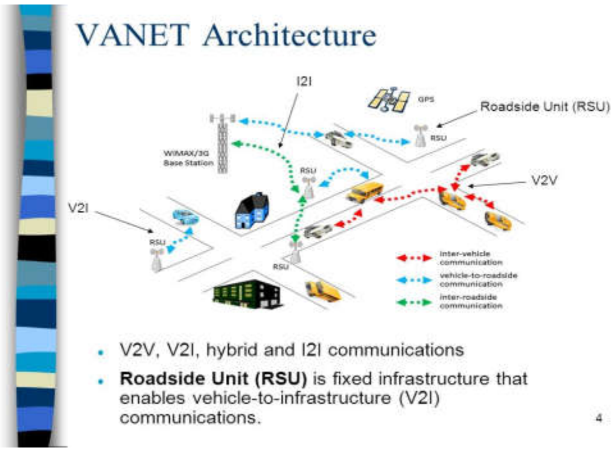
HS- Hotspot is used for the communication purposes.

Application Unit (AU)

The Application Unit (AU) is installed within the vehicle. In one OBU, many AUs can be plugged where OBU's processing and wireless resources can be shared in between. The application unit communicates only through the On-Board Unit that takes care of all the wandering and network usefulness on its behalf. The only difference between AUs and OBUs is of consistency. Here we can physically co-locate the application unit with the on-board unit.

On-Board Unit (OBU)

Main work of on-board unit is to make a communication between vehicles and vehicles and vehicle and roadside infrastructure. It delivers the communication service to application unit and also send on data and related information. The on-board unit is equipped with single network device.



VANET Architecture

I2I
GPS
Roadside Unit (RSU)
RSU
WiMAX/3G Base Station
RSU
V2V
V2I
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

- V2V, V2I, hybrid and I2I communications
- **Roadside Unit (RSU)** is fixed infrastructure that enables vehicle-to-infrastructure (V2I) communications.

4

Figure 1 VANET Architecture [7].

Kinds of vanet Netwok Architecture

We can divide VANET's architecture in three categories namely Cellular or WLAN, Pure ad-hoc and Hybrid [8]. Brief description of each category is given below.

Cellular Network Architecture

In this kind of network architecture WLAN/WiMAX access points are used. For establishing an internet connection, fixed and cellular gateways are used.

Ad hoc Network Architecture

It is very costly to establish a cellular network framing since it uses set gateways and access points. Therefore, for eliminating such kind of problems the vehicles and all roadside units make an ad-hoc network by themselves.

Hybrid Network Architecture

Hybrid network architecture is built up by combining architecture of both, cellular network and ad-hoc network which can also be a possible solution to VANET. It can be explained better with hybrid structure. There occurs an issue of unlined passage of communication in between dissimilar wireless system.

Communication Types

V2V

Vehicle to vehicle communication is the communication between vehicles for exchanging the all the related information while travelling.

V2I

Vehicle to infrastructure is the communication between the vehicles and the roadside infrastructure which happens for collecting the information from the vehicles and providing it to the other vehicles.

Hybrid

Hybrid is the mixture of both the communication systems.

Measures of Wireless Access in Vanet

There are many communication measures that vehicular environment supports and conversate with wireless access. These standards are given below.

Dedicated Short Range Communication (DSRC)

It's range of communication is in between 300 m and 1 km. V2V and V2R communication takes place in this. The spectrum of DSRC is distributed between 7 channels where each is of 10 MHz One channel is used for communicating safely, out of these 7 channels. Two channels are used for the critical safety of human lives or public and the remaining are utilized as the service channels.

Wireless Access in Vehicular Environments (WAVE)

For the communication over a short range it supplies the ITS applications. For improving the performance of VANET it provides the real time statistics. It improves transport sustainability. It contains IEEE 1609 standard which is the upper layer standard. For the division of signals into various narrow band channels it uses a technique known as Orthogonal Frequency Division Multiplexing.

Cellular Access in Vehicular Environment (2G/2.5G/3G/4G)

The phenomenon of cellular access came into the existence regarding the reuse of available limited frequencies for the services. GSM is the oldest that provides a data rate of 9.6 Kbps and called as 2G cellular service. Then GPRS came into the existence which gives a data rate of 170 Kbps and called as 2.5G cellular service. After that 3g was evolved that gives us a data rate of 2 Mbps. And now 4G is currently active which is the fastest cellular service till the date and gives us maximum data transfer rates.

Security Issues in Vanet

As the wireless medium is quite open in VANET, there are some attacks due to which the VANET can be exposed. Few attacks are given below [5, 7].

Security Challenges in VANET

Real Time Constraint: Time is very critical in VANET so the safety messages must be delivered with a maximum transmission delay of 100ms. And to do so some fast and secure cryptographic algorithms are used in order to achieve message authentication.

Data Consistency Liability: A mechanism is developed to avoid the data inconsistency and accidents since an authenticate node can also act as a malicious node sometimes.

Low Tolerance for Error: Some probabilistic algorithms are used to design the protocols since a small error can cause harm of lives and vehicles.

Key Distribution: In order to transmit the messages securely, messages are encrypted from the sender side and then decrypted at the receiver end either with the same or different keys [16].

Incentive: Most of the vehicle manufacturing companies make vehicles as per the interests and likings of the consumers since they want to attract them hence this becomes a challenge in implementing security in VANET and require incentives.

High Mobility: Since vehicles in VANET are highly mobile hence the reduction in execution time is needed.

Security Requirements in VANET

Authentication: Authentication is highly needed since there is need of verification of sender and receiver to be legitimate.

Availability: Availability shows that the data should only be available to the legitimate user.

Non-Repudiation: Non-repudiation shows that a node cannot deny that it has not sent the message.

Privacy: Privacy is highly required so that any unauthorized node cannot access its data.

Data Verification: Data verification is needed to avoid the false reception of messages.

Attackers in VANET

Insider and Outsider: Insider attackers are the authenticated members from the network while outsider attackers are the intruders from outside the network.

Malicious and Rational: Malicious attackers are those attackers which do not attack the system for their personal benefits while rational attackers have their personal benefits in attacking the system.

Active and Passive: Active attacker generates the signals while passive attacker only senses the network.

Attacks in VANET

Impersonate: In impersonate attacks, the attacker tries to assume the identity and privileges of the authorized node so that it can access the resources of that particular node which it was not able to access under normal conditions.

Session Hijacking: In this kind of attack, the attacker tries to take control of sessions between the nodes.

Identity Revealing: In most cases the driver is the owner of the vehicle hence it puts the privacy at risk.

Location Tracking: Location of the driver can be easily traced by getting the information of location of the vehicle at a given time of the path.

Repudiation: In this kind of attack two or more entities can have similar identity at the same time hence it is difficult to distinguish between the two.

Eavesdropping: The aim of this kind of attack is to get the access of the confidential data/information.

Denial of Services: In VANET, denial of services can be the most dangerous attack. Main goal of DOS is stopping the authorized person from accessing the network services. These are of three kinds as follows [13,15]:

Jamming: Jamming is such an attack that blocks the communication channel so that no any information can be flown. And it is done by a malicious node which becomes able to determine the frequency of the channel.

SYN Flooding: In this kind of attack the attacker tries to send a number of requests at the same time so that it can consume the maximum resources and make the system unresponsive.

Distributed DOS attack: This kind of attack is a dangerous attack since it is distributed and its impact is spread out in the network.

Routing Attacks

Black Hole Attack

There is a dangerous node which exploits overflowing routing and incorrectly publicize that it has an optimal route for reaching destination node. Here the spiteful node sends a reply to the node that is requesting before the actual node's reply which helps in creating a bogus route. In this attack the attacker node forms a black whole as a result of which all the involved routes broke down which leads to the failure of propagating the messages. Thus, the correct information is not sent to the authorized vehicles and the dangerous node stops the information and leave it or forward it to the unknown addresses and hence plunge the traffic of network.

Gray Hole Attack

It is a special kind of black whole attack where behavior of dangerous node is completely uncertain. Firstly, it acts as a genuine node while the process of finding route, then it changes its province to the dangerous node. Due to network congestion and overloading, it's not easy to detect the gray hole attack. A gray hole attack is that attack which disturbs the process of route discovery and decreases the network functioning by some dangerous activities.

Vanet Simulators

It is that software or hardware which tells us about the network behavior without the presence of a real network. Some of them are graphical user interface driven while some necessitate the input scripts and commands. Hunting files is the important output of these simulators.

NS-2

It is a distinct case simulator which is used for networking exploration. Initially NS-2 was made in C++ which provided the model interface by OTcl. The association of C++ and OTcl is very effectual since use of C++ to implement the elaborated protocol where OTcl is kept for controlling the model perspective of users and scheduling the outcomes.

Fearures

1. It takes care of modelling time and leaves all the occurring events in the event queue with bringing up the suitable network constituents.
2. It is competent as NS-2 separates the control path implementation from data implementation.It is competent as NS-2 separates the control path implementation from data implementation.

OPNET

Known as Optimized Network Engineering Tool. It can be defined as a device which models the doings of system with a process of modeling events of system and work on it accordingly as processes defined by users. Its work is studying about network communication, and its applications. It also gives users some tools for programming for defining data format and the protocols.

Fearures

1. Gives many libraries of components having some source codes.
2. Gives different simulation surroundings.
3. Grid computing is supported.

Qualnet

Known as Quality Networking Tool. It is generally used for bigger different networks which is supported by both protocols either its wired or wireless.

Features

Employs models that are based on extremely detailed measures. It connects to many software as well as hardware application.

Routing in Vanet

Routing is a phenomenon in which we transmit the data from source to destination via multi-hop steps with the least rate. Due to unpredictability and dynamicity in VANET's nature the routing becomes harder because of the large network size, high mobility of nodes and intermediate communication between vehicles. Vehicles are not informed about the network structure so they need to evolve the network structure and then make it able to be stored in a data structure known as table of routing further distributing it for finding efficient and feasible route. Routing is the biggest challenge while designing the architecture for vehicular communication since finding an efficient strategy that guarantees the minimum delays, maximum reliability and timely exchange of information. The main goal of routing protocol is finding an optimal route which will consume minimum bandwidth and will have minimum overhead [9, 10].

Proactive Routing Protocol

These protocols acknowledge a network node for maintaining the routing table in which structuring information of all the nodes is stored where every entry of table has next furtherance skip node that is put upon path to the goal without taking care about their current participation in the communication. Table is upgraded sporadically which speculate the changes in the network topology that is broadcasted to the neighbors. After the exploration of the routes the shortest route is chosen by shortest path algorithm to every possible goal given in the table [14].

Advantage

Destination route get stored in the background.

Disadvantage

May not work on VANET because of high consumption of bandwidths and routing tables with huge data.

Reactive Routing Protocol

In this protocol, the routing information does not get continuously exchanged with the surrounding nodes. Alternatively, the route is found out on the request and maintained only for such routes which is to be required in the present communications. The route discovery process got started when a source node finds a route to the destination node where the query packets are transmitted to the network for searching the path. The destination node then agrees for establishing the route and this phase got completed finally when the route is found [13].

Advantages

There is no distribution of routing information.
It is effective in route maintenance and less bandwidth.

Disadvantages

It takes more time in the discovery of route.
Network overcrowding because of exuberant flow of messages.

Vanet Applications

A number of applications has been developed for the communication between the vehicles that gives drivers and passengers a huge amount of information. Due to this the road security and soothe of passengers has been increased. We can divide these applications into two categories as per their intentions [3, 4, 6].

Safety Oriented Applications

The aim of these applications is to highlight upon road safety and to avoid the accidents with the help of wireless communication between the vehicles and between the vehicles and infrastructure.

Table 1 Safety Focusing Applications

Name	Description
Electronic brake warning	A vehicle which has applied sudden brakes will inform other nearby vehicles
Lane change warning	Drivers can safely change the road lanes
Road hazard	If a vehicle detects some kind of problem then it will inform other vehicles around
Intersection violation warning	Vehicles interchange messages for making a safe crossing
Post-crash notification	If a vehicle got some accident then it will inform the nearby approaching vehicles so that they can take right decision at right time
Traffic vigilance	If someone breaks the rules of road safety then proper action can be taken as cameras installed in RSUs records every activity
Blind crossing condition	Somehow if there are no traffic lights then vehicles will cooperate each other

Non-Safety Oriented Applications

These are some commercial applications that gives entertainment services to the drivers and handles the traffic management system so that traffic efficiency can be increased [14].

Table 2 Non-Safety Focusing Applications

Name	Description
Congested road notification	It detects and notifies about the road conditions, whether there is rush or not, so that passengers can plan their road trips
Value added advertisement	Gives the information about the upcoming petrol pumps, highway food outlets to tempt the driver and passengers about their outlets if lies in the range
Electronic toll collection	Toll payments can be performed electronically at toll points without getting stopped
Parking availability	Assists drivers in finding the usable places of parking in any geographic location
Internet access	Internet access facility can be taken by the vehicles and passengers by establishing connections with RSUs
Media or map download	Maps of highways and city areas can be downloaded for avoiding the traffic jam

CONCLUSION

VANET is an advance technology where significant advancement in wireless technology has brought some technology enhancement in vehicles that have become an important component of the global network. It cannot only give some lifesaving applications but can also turn as a powerful communication tool for the drivers and passengers. We have mainly focused on the VANET architecture, simulation, routing, attacks and its applications. By accomplishing all requirements and by tackling the challenges we can get an effective communication tool that will provide the lifesaving tools to the users. If some more improvements are possible then it will give much better results as compared to other ad hoc networks. Vehicles should be manufactured in such means where they have some abilities of learning by which they can have the abilities of identifying the potential dangers and thus it can modify the vehicle's behavior accordingly. It will also help vehicles to take decisions from its past experiences.

Refrences

1. S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad Hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004
2. Moustafa H., Zhang Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).
3. Yaseer Toor *et al.*, "Vehicle Ad Hoc Networks: Applications and Related Technical issues", IEEE Communications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3, pp. 74-88.
4. Y.- C. Hu and K. Laberteaux, "Strong Security on a Budget," Wksp. Embedded Security for Cars, Nov. 2006; http://www.crhc.uiuc.edu/~yihchun/
5. Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005,
6. Alexandria, Verginia, USA, pp. 11-21
7. Hannes Hartenstein *et al.*, "A tutorial survey on vehicular Ad Hoc Networks", IEEE Communication Magazine, June 2008, pp. 164-171
8. Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, 2010.
9. Murthy, C. S. R., Manoj, B. S.: Ad Hoc Wireless Networks: Architectures and Protocols. PEARSON, ISBN 81-317-0688-5, (2011).
10. Dahill, B. N. Levine, E. Royer and Clay Shields, "A Secure Routing Protocol for Ad Hoc Networks", Proceeding of IEEE ICNP 2002, pp 78-87, Nov 2002.
11. Y. C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", Elsevier B. V., pp 175-192, 2003
12. P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad Hoc Network", ACM Workshop on Wireless Security, San Diego, CA, September 2003.
13. Fasbender, D. Kesdogan and O. Kubitz, "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE VTS, 46th Vehicular Technology Conference, USA, 1996.

14. Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", MobiCom'02, pp. 23-26,2002
15. Fonseca and A. Festag, "A survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS", NEC Network Laboratories, 2006.
16. Xiaodong Lin *et al*., "Security in Vehicular Ad Hoc Network", IEEE communications magazine, April 2008, pp. 88-95
17. Menezes, S. Vanstone, and D. Hankerson, "Guide to elliptic curve cryptography", Springer Professional Computing (Springer, New York 2004).
18. J. Hof fstein, J. Pipher, J. H. Silverman, "NTRU: A ring-based public key cryptosystem", Lecture Notes in Computer Science, Vol. 1423, 1998, pp 267-288.

How to cite this article:

Krishna Verma *et al*., 2019, A Study on Vanet and its Security Issues. *Int J Recent Sci Res.* 10(06), pp. 33298-33303.
DOI: http://dx.doi.org/10.24327/ijrsr.2019.1006.3646

****