OVERVIEW OF VANET WITH ITS FEATURES AND SECURITY ATTACKS

M.Newlin Rajkumar[1], M.Nithya[2],P.HemaLatha[3]

[1]*Assistant Professor, Department of Computer Science, Anna University Regional Centre Coimbatore*

[2]*P.G Scholar, Department of Computer Science, Anna University Regional Centre, Coimbatore*

[3]*P.G Scholar, Department of Computer Science, Anna University Regional Centre, Coimbatore*

Abstract-*Vehicular Ad-Hoc Network (VANET) is created by using principles of Mobile Ad-Hoc Network (MANET) for impulsive creation of wireless network for enhancing the data to domain of vehicles. Safety is an important aspiration for VANET in view of the facts that improved safety which reduces accidents and consequently improve traffic conditions and yet save lives. The security of VANETs is vital as their existences relate to grave intimidating situations. The security is most decisive issues because their information is broadcast in open access environments. It is obligatory that all transmitted data can be injected or changed by users who have malevolent goals. The problem of VANET is difficult to solve because of the size of network, vehicle speed, their relative geographic positions, and the arbitrariness of the connectivity between them. In this article here going to discuss about VANET along with its securities and their attacks.*

***Keywords** : VANET standards, Securities, Attacks.*

1. Introduction

VANET is a type of network that wires a enormous field of mobile circulated applications which runs in vehicle. Vehicular Ad-hoc Network (VANET) should be an exacting form of the Mobile Ad-hoc Network (MANET) where the vehicle acts as the mobile nodes within the network exposure with stay on connection; the node should communicate with each other through single hop or multi hop. Here the node can be a vehicle, Road Side Unit (RSU). It had better dispensation and storage capability. It is a key component of Intelligent Transportation System (ITS). It also a generic term in Inter Vehicle Communication (IVS). In research area it made more interest for developing more service and security applications. The ultimate goal of VANET is to provide road safety information among the nodes hence the frequent exchange of such type of data on the network clearly signifies the role of the security.

2. Overview

The Intelligent Transportation Systems (ITS) main aspire is to offer solution for accidental protection of passengers and the traffic overcrowding problems. The ITS enhanced wellbeing and driving surroundings with integrating information technology in transport systems. The possible types of communications:

Vehicle To Vehicle (V2V): It provide interaction within vehicles in ad hoc approach. In V2V, a vehicle can accept broadcast and exchange helpful traffic news i.e., traffic conditions and road accidents in particular area or with other vehicles.

Vehicle to Infrastructure (V2I): In this communication type, the information will be broadcast between the nodes (i.e vehicle) and the infrastructure (said as ITS), to discuss about valuable information such as road conditions and safety events which have been taken into account. In this V2I, a vehicle (node) launches a connection between RSU and contact with external networks which is internet.

2.1 Characteristics of VANET

VANET is a infrastructure less network in which the node can said to be a Road Side Unit(RSU) or the moving vehicle. It provides a combination of wireless medium methods and the characteristics ad hoc network which uses a different topology for communication and infrastructure dependent modes. VANET is an application of MANET which had its distinct characteristics can be summarized as:

High Mobility: In VANET, the node moves at high speed that condenses the mesh in the network. So that it is hard to calculate the vehicle position and to provide security for node privacy.

Rapidly changing network topology: The node in VANET is high mobile in nature and the speed of vehicle should also random, so that the node position will change frequently. The topology is dynamic and unpredictable. It facilitates the entire network attacks and make hard to find of misbehavior in the network.

Availability of the transmission medium: VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded. The universal availability of this wireless transmission medium is great advantages in IVC, becomes the origin of some security issues, related to both the nature of transmission in wireless environment and to the security of communications using an open support.

Frequent exchange of information: Normally the VANET is ad hoc nature. It inspire the nodes to collect information form the neighbor vehicles and road side units. So that, the nodes exchange their information periodically.

Anonymity of the support: By using a wireless medium the data transmission will be generally mysterious. The limit and control of using network can leaved, everyone outfitted with a transmitter, which is operate in the same frequency band that can be transmit and holed that band.

Limited bandwidth: In VANET, the standard DSRC band should be measured as limited, the width of the DSRC band was 27 MHZ. The throughput was 27 Mbps which is a theoretical value.

Attenuations: According to digital transmission, DSRCband has transmission problems with those frequencies, which is reflection, diffraction, and dispersion, different types of fading, and Doppler Effect, losses. The propagation delays occur because of multipath reflections.

Time critical: Within the time period, the information in VANET should send to the accurate node. so that the node will make a decision and execute action correspondingly.

Energy storage and computing: The VANET nodes have no issue of energy, computing capacity or storage failure. This allows VANET usage of demanding technique such as RSA, ECDSA implementation and also provides unlimited transmission power.

Better Physical Protection: In VANET the vehicle should be well protected in physically. So that physically compromising the VANET node will be difficult and it is very difficult to reduce the outcome of infrastructure attack.

Limited transmission power: In the WAVE the transmission power should provide up to the data reached. The data reachability distance can be said to be 1000m. For crisis and any public safety such as accident problem or any traffic congestion problem, it is allowed to transmit with a high power.

3. Applications of VANET

In commercial applications uses a VANET, they benefit by using this. The application used in the VANET can have a vital role, which would be classified into three wide categories.

3.1 Safety related Application

The road safety will be increased by using this application. This type of application is further classified as:

Collision Avoidance: By providing a alert in half a second before crash occurs, leads to avoid the 60% of accidents. Once the warning message send to the driver, the crash can be avoided.

Cooperative Driving: Drivers will obtain signals for traffic associated warnings like Lane change warning, curve speed warning etc. The signal is able to co-operate and make the driver for a non-interruptible safe driving.

Traffic Optimization: Traffic can optimized by make use of sending signals like accidents, jam etc. to the vehicles. So that they can decide their alternate pathway and they can rescue time.

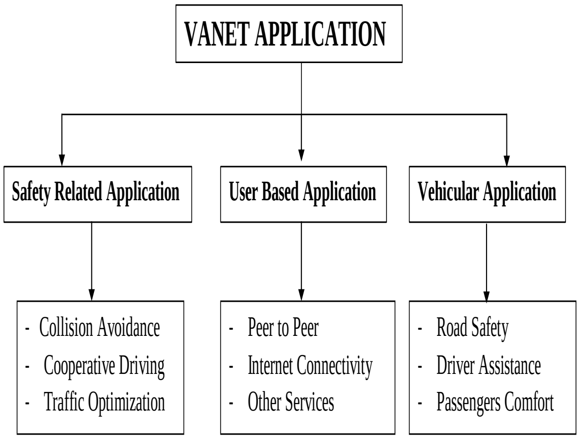
3.2 User Based Application

These applications present the information about user (i.e. user infotainment). A VANET can exploit to offer several services for the user:

Peer to peer application: For sharing music, movies, videos, etc this type of application is very useful among the network used by the vehicle.

Internet Connectivity: At any time, people want to connect with the internet. So for user VANET provides the constant connectivity of the internet.

Other Services: The other user based application will make use of VANET by accessing the location of fuel station, restaurant, and payment service to collect the taxes.



3.3 Vehicular Application

Based on vehicular networks, it has the responsibility of passenger comfort, road safety, and driver assistance.

Application for road safety: To reduce road accidents and to improve travel safety, VANET offer some road work and collision avoidance, fixed obstacles, dissemination of weather information and detection of mobile.

Applications for driver assistance: It's main aim to make easy for driving and also help the driver in specific situations such as prevention of channels output, overtaking vehicles, detection and warning of traffic congestion, warning of potential traffic jams, etc.

Applications of passengers comfort: These applications make comfort to the passengers and also the driver, it provides the following services: messaging, discussion between vehicles, mobile internet access, collaborative network games etc.

4. Standards of VANET

In communication and IT(Information Technology), the standards and normalization helps to make sure the interoperability and the fast achievement of new technologies. Virtually the different layers in OSI (Open System Interconnection) should be affected by the standards used.

DSRC (Dedicated Short Range Communication), WAVE (Wireless Access in Vehicular Environments) and IEEE 802.11p are the standards used to select the entire protocol stack to trade with VANETs.

4.1 DSRC (Dedicated Short Range Communication)

The DSRC band is also regulated by ETSI (European Telecommunications Standard Institute) using only the channels 180 of CCH and 172, 174, 176, 178 of SCH.

The FCC (Frequency Communication Commission) characterizes the highest interoperability and the intention of standardization 0f frequencies in which the VANET works. The FCC attributed the band 5850 to 5925 GHZ. This band will be said as Dedicated Short Range Communication (DSRC).

The band of 10MHZ is separated into seven channels which is 178, 172,1 74, 176,180,182,184. The channel 178 is called as Control Channel(CCH).The other channel said to be Service Channels(SCH).For High Availability and Low latency (HALL) and high power and public safety, the service channels 172 and 184 are allocated.

4.2 WAVE (Wireless Access in Vehicular Environment)

To operate in a VANET situation and to set up a Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, the WAVE station defines the architecture; services, interfaces and a set of standard protocols. It describe the security about exchangeable messages. In the transportation field, the deployment of a huge variety of application are all provided by this WAVE architecture which comprise improved navigation, automatic tolls, road and vehicle safety, traffic management and also many applications.

The WAVE IEEE 1609 standards is organized as,

IEEE P1609.0: In WAVE architecture, it guides for necessary services to the multichannel DSRC machines for communicating in high mobile environment.

IEEE P1609.1 (Resource Manager): Defines command messages and storage data formats, data flows and resources. It specifies the device types which an On Board Unit has supported.

IEEE Std 1609.2 (Security Services for Applications and Management Messages): The secure message formats and the processing method used in WAVE and DSRC system are all defined by this standard. It specifies the method for secure the management messages, application messages, function necessary to hold message security and privacy of vehicle.

IEEE Std 1609.3 (Networking Services): Describes service for the transport and network layers, it includes routing and addressing with the support of secure WAVE data exchange.

IEEE Std 1609.4 (Multi channel operations): It defines the priority access parameters, interval timers, and service channel and control channels process. It describes the channel routing, management services and switching parameter.

IEEE Std 1609.11 (Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS)): It describes secure messages and service needed by the usage of secure electronic payment formats

IEEE Std 1609.12 (Provider Service Identifier allocations (PSID)): Through the WAVE system, it provides the identifier values.

4.3 IEEE 802.11p

To hold vehicular networks IEEE has enlarge it version from IEEE 802.11 protocols to IEEE 802.11p in agreement with DSRC band which describes the medium access and physical layers of VANETs.

5. Security of VANET

Securing VANET system must be able to decide the task of drivers while uphold their privacy. Communications transient through the network such as information about vehicles and their drivers must be protected to ensure the even functioning of intelligent transportation systems. The extremely dynamic situation set apart by regularly immediate arrival of short period connection durations, vehicles and departure, the deployment of a complete security solution has been serious to façade restraint and specific configurations. VANET safety should be an unique concern in traditional networks. The major security concerns comprise availability; integrity and confidentiality are first and foremost involvement with life safety. Essential information cannot be neither deleted nor modified by an attacker. The security point out the message should exchange securely about the vehicles and their corresponding drivers.

5.1 Entities involved in VANET securities

The entities involved in the security of VANETs are:

The driver: He is mainly significant part in VANET safety chain, because he has to make vital decisions. In VANET , for driving aid system has interactive component as driver.

The vehicle (OBU): The VANET network provides two types of vehicle they are, the malicious vehicles and the normal automated vehicle which is exist among network nodes.

Road Side Unit (RSU): RSU station operates in a normal way and in sometimes the malicious node will act as a RSU terminal.

Third parties: There should be an trusted or semi-trusted third parties and also a direct way communication for all digital equivalents of stake holders. The third parties should be referred as the vehicle manufacture, regulator of transport, traffic police and judges.

The Attacker: The attacker violates the vehicle by using various techniques to attain their goal. Attacker may be internal or external, and may be rational or irrational.

The **Rational attacker** follows a rational approach in which attack cost may not exceed than expected benefit.

The **Irrational attacker** may be suicide bomber of its kind.

The attacker may be either active, made his attack with an exposed manner or passive, his action cannot be detected.

5.3 Security requirements in VANET

Before the VANET deployed, it should satisfy a few requirements. A VANET security system satisfies the following requirements:

Authentication: It makes sure that the genuine user created the message. In VANET, a vehicle respond according to the information received from the other vehicles, which satisfy the authentication.

Availability: It confirms that information should be available to the genuine user. The attacks should shut down the network, so that the information cannot be shared.

Non-Repudiation: It explains a vehicle cannot reject that user does not broadcast the message. It might be an critical to conclude the exact sequence of crash reconstruction.

Privacy: There should be an guarantee of privacy node against unauthorized node. The message delay attack should be eliminated.

Data verification: To eliminate the false messaging, a regular verification of data is needed. The message also encompasses their consistency with similar ones because the sender can be legitimate while the message contains the false data.

Real time constraints: The highest speeds are typical in VANET; there should be a strict time restriction which respects security mechanisms.

Electronic License Plates (ELP): ELP should used as same as the traditional license plates, which have the unique verifiable numbers. To checkup the vehicles, it will make the automated paper-based document. Government transportation authorities provide the license plates. The authorities must also have an cross-certification agreements, which makes them to verify the issued ELP with other authorities.

Event Data Recording (EDR): In situations of accidents, the EDR would make to register these type of situation in vehicles.

Tamper proof hardware: To reduce the prospect of information leakage, the VANET stores ELP, tamper-proof hardware which makes them safe from attackers.

Data Correlation: The vehicle will make a result in the level of consistency, creditability and significance of the information received by using data correlation scheme which collect data received from various sources and also bogus information attack will not easily discovered.

Secure positioning: There should be an real requirement to secure position verification. Thus a Vehicle or base-station should have to confirm the position of another vehicles or base-station.

6. Attacks in VANET

VANET has been exhibit to numerous attacks. In normal ad-hoc networks, the computational ability attacks are computationally rigorous and are not feasible in nature. It is important to categorize the attacks in VANET, because the exclusive nature of VANET, which brings unique vulnerabilities and different kinds of attacks, may want significant computing. The VANET may be classified as:

6.1 Attacks on availability

It is a most vital role in VANET which assure the network has been an functional one and also offer needed information during functioning time. This significant security requirement makes VANET to provide the user lives, which is the most important target of the user.

6.2 Attacks on authentication and identification

It has been a major contest for VANET security. In the network, all existing stations should authenticate before contact the available services. The attack engages the process of identification which represents the whole network to serious consequences. In a Vehicular network the authentication ensure to protect the authenticated nodes from the outside or inside attackers clever the network using a false identify. Whenever a vehicle want to join the network or any service, the authentication process will takes place.

6.3 Attacks on confidentiality

Confidentiality will be an key security mechanism in VANET communications, which make sure the data should accessed by authorized user. In the absence of mechanism, the VANET should ensure the exchanged message confidentiality, when it is particularly vulnerable to attacks, which can be said as improper collection of clear information. The attacker can collect the information at particular location of vehicle and it route on user's privacy etc.

6.4 Attacks on integrity and data trust

The integrity of transmitted data in a vehicle has to make sure that exchanged data should not been altered during transmission. These mechanisms assist to protect information against deletion, modification or additional attack.

6.5 Attacks on non-repudiation

In computer security non-repudiation means, the ability to confirm that the sender and the receiver are the entities who can send and receive the messages. The non-repudiation of data origin establish the data has been send to respective sender and the non-repudiation of arrival have to make sure that data has been received only authenticated receiver.

7. Conclusion

Vehicular Ad-hoc Network (VANET) is prevalent in Intelligent Transportation Systems, they obtain to provide services for passenger comfort and provide road safety which related to safety of human lives. VANET make an impact on attackers and symbolize the target for various attacks which cost vary from negligible to server. Securities providing for VANET are most challengeable. Our future work is to over the weakness of existing schemes in security and adapts the intrinsic features of vehicular communication, which involve the new design and development of effective security schemes to support the protection of critical services based on VANETs.

REFERENCES

[1] Mostofa Kamal Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali,*Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network*,International journal of scientific & technology research volume 2, issue 4, april 2013 issn 2277-8616.

[2] Ram Shringar Raw, Manish Kumar, Nanhay Singh,*Security challenges, issues and their solutions for vanet*, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[3] Sherali Zeadally,Ray Hunt, Yuh-Shyan Chen Angela Irwin,Aamir Hassan, *Vehicular ad hoc networks (VANETS): status, results, and challenges*, Springer Science+Business Media, LLC 2010.

[4] A. Dhamgaye, N. Chavhan, *Survey on security challenges in VANET*, Int. J. Comput. Sci. 2 (2013) 88–96, ISSN 2277-5420.

[5] M. Raya, P. Papadimitratos, J.-P. Hubaux, *Securing vehicular communications*, IEEE Wirel. Commun. 13 (5) (2006) 8–15.

[6] B. Mishra, P. Nayak, S. Behera, D. Jena, *Security in vehicular adhoc networks: a survey*, in: Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM, 2011, pp. 590–595.

[7] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, *Vehicular ad hoc networks (VANETs): status, results, and challenges*, Telecommun. Syst. 50 (4) (2012) 217–241.

[8] I.A. Sumra, I. Ahmad, H. Hasbullah, J.-L. bin, Ab Manan, *Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET)*, in: 3rd International Congress on Ultra Modern Telecommunications and Control Sys- tems and Workshops (ICUMT), 2011, IEEE, 2011, pp. 1–8.

[9] M.E. Mathew, A.R.K. P, *Threat analysis and defence mechanisms in VANET*, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 3 (1) (2013) 47–53, ISSN 2277-128X.

[10] A. Rawat, S. Sharma, R. Sushil, *VANET: security attacks and its possible solutions*, J. Inform. Oper. Manag. 3 (1) (2012) 301–304.

[11] J.M. d. Fuentes, A.I. González-Tablas, A. Ribagorda, *Overview of security issues in vehicular ad-hoc networks*, in: Maria Manuela Cruz-Cunha, Fernando Mor- eira (Eds.), Handbook of Research on Mobility and Computing, IGI Global, 2010.

[12] M.S. Al-kahtani, *Survey on security attacks in vehicular ad hoc networks (VANETs)*, in: 6th International Conference on Signal Processing and Communication Systems (ICSPCS), 2012, IEEE, 2012, pp. 1–9.

[13] MohamedNidhalMejri , Jalel Ben-Othman , MohamedHamdi "*Survey on VANET security challenges and possible cryptographic solutions*",www.elsevier.com/locate/vehcom.

[14] ITS, ITS standards fact sheets of IEEE, http://www.standards.its.dot.gov/factsheets/factsheet/80, seen, April 19, 2014.

[15] G. Samara, et al., "*Security issues and challenges of Vehicular Ad Hoc Networks (VANET)*," in 4th International Conference on New Trends in Information Science and Service Science (NISS), 2010, pp. 393-398.