International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 7 (July '2016)

A SURVEY ON SECURITY ISSUES AND CHALLENGES IN VANET

Dr.T.Ramaprabha,
Professor,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Sciences for Women,
Tiruchengode,Tamilnadu,India.

V.Premalatha,
M.Phil Scholar,
Department of Computer Science,
Vivekanandha College of Arts and Sciences for Women,
Tiruchengode,Tamilnadu,India.

Abstract: The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range.VANET is emergent technologies that they deserve, recently, the attention of the industry and the academic institutions. The vehicular communications (VC) meet in the centre of numerous initiatives of the research that enhance the security and the efficiency of transportation systems, supplying, for example, acknowledgments of the ambient conditions (snow, fire, etc.), traffic in the road conditions (emergency, construction sites, or congestion). In this paper, we survey on security issues and challenges in VANET.

keywords: VANET, IEEE 802.11 , Security, TDMA, SDMA, and CSMA.

I. INTRODUCTION ON VANET

Now days, the sheer volume of road traffic affects the safety and efficiency of traffic environment. Approx 1.2 million people are killed each year on the road accidents. Road traffic safety has been the challenging issue in traffic management. One possible way is to provide the traffic information to the vehicles so that they can use them to analyse the traffic environment. It can be achieved by exchanging the information of traffic environment among vehicles[2]. All the vehicles are mobile in nature, hence a mobile network is needed which can be self organised and capable of operating without infrastructure support. With the progress of microelectronics, it becomes possible to integrate node and network device into single unit and wireless interconnection, i.e. ad hoc network. Further this network is evolved as mobile ad hoc network. VANET is an application of mobile ad hoc network. More precisely a VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers. Two types of communication are provided in the VANET.

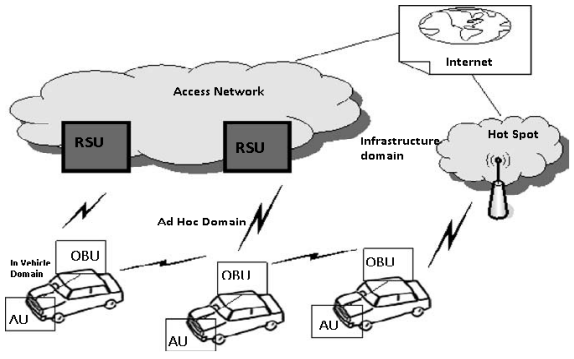

Figure 1: C2C-CC Architecture of VANET

First a pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure. Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle. Each node in VANET is equipped with two types of unit i.e. On Board Unit and Application Unit (AU). OBU has the communicational capability whereas AU executes the program making OBU's communicational capabilities. An RSU can be attached to the infrastructure network which is connected to the Internet. Figure 1 describes C2C-CC architecture of VANET.

These signals can co-operate the driver for an uninterrupted and safe driving.

VANET APPLICATIONS AND CHARACTERISTICS

To deploy VANETs, there must be some commercial applications that benefit from them. The applications where VANET can play major role can be categorised into two broad categories.

A. SAFETY RELATED APPLICATION

These applications are used to increase the safety on the roads. These applications can be further categorised in following way.

- **Collision Avoidance**: According to some studies, 60% accidents can be avoided if drivers were provided a warning half a second before collision. If a driver get a warning message on time collision can be avoided.
- **Traffic optimization:** Traffic can optimized by the use of sending signals like jam, accidents etc. to the vehicles so that they can choose their alternate path and can save time.
- **Cooperative Driving:** Drivers can get signals for traffic related warnings like curve speed warning, Lane change warning etc.

B. USER BASED APPLICATION

These applications provide the user infotainment. A VANET can be utilized to provide following services for the user apart from safety:

- **Peer to peer application**: These application are useful to provide services like sharing music, movies etc. among the vehicles in the network.
- **Internet Connectivity**: People always want to connect with the Internet all the time. Hence VANET provides the constant connectivity of the Internet to the users.
- **Other services**: VANET can be utilised in other user based application such as payment service to collect the tall taxes, to locate the fuel station, restaurant etc.

II. CHARACTERISTICS OF VANET

VANET is an application of MANET but it has its own distinct characteristics[1] which can be summarized as:

- **High Mobility:** The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy.
- **Rapidly changing network topology:** Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.
- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.
- **Frequent exchange of information:** The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.
- **Wireless Communication:** VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication.
- **Time Critical:** The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.
- **Sufficient Energy:** The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.
- **Better Physical Protection:** The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack.

III. CHALLENGING ISSUE IN VANET

Although the characteristics of VANET distinguishes it a different network but some characteristics imposes some challenges to deploy the VANET[4]. These challenges can be categorized into following categories:

A. TECHNICAL CHALLENGES

The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET. Some challenges are given below:

- **Network Management:** Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained as rapidly as the topology changed.
- **Congestion and collision Control**: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.
- **Environmental Impact:** VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.
- **MAC Design:** VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.
- **Security:** As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied.

B. SOCIAL AND ECONOMIC CHALLENGES

Apart from the technical challenges to deploy the VANET, social and economical challenges should be considered. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring. Conversely, consumer appreciates the warning message of police trap. So to motivate the manufacturer to deploy VANET will get little incentive.

IV. SECURITY ISSUES AND CHALLENGES IN VANET

Among all the challenges of the VANET, security got less attention so far. VANET packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security.

SECURITY CHALLENGES IN VANET

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges:

- **Real time Constraint**: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.
- **Data Consistency Liability**: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data

from different node on particular information may avoid this type of inconsistency.

- **Low tolerance for error**: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.
- **Key Distribution:** All the security mechanisms implemented in VANET dependent on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become major issue. Therefore distribution of keys among vehicles is a major challenge in designing a security protocols.
- **Incentives:** Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET.
- **High Mobility:** The computational capability and energy supply in VANET is same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces. Hence the design of security protocols must use the approaches to reduce the execution time.

Two approaches can be implementing to meet this requirement.

A**. Low complexity security algorithms:** Current security protocols such as SSL/TLS, DTLS, WTLS, generally uses RSA based public key cryptography. RSA algorithm uses the integer factorisation on large prime no. which is NP-Hard. Hence decryption of the message that used RSA algorithm becomes very complex and time consuming. Hence there is need to implement alternate cryptographic algorithm like Elliptic curve cryptosystems and lattice based cryptosystems. For bulk data encryption AES can be used.

B. **Transport protocol choice:** To secure transaction over IP, DTLS should be preferred over TLS as DTLS operates over connectionless transport layer. IPSec which secures IP traffic should be avoided as it requires too many messages to set up. However IPSec and TLS can be used when vehicles are not in motion.

V. SECURITY REQUIREMENTS IN VANET

VANET must satisfy some security requirements before they are deployed. A security system in VANET should satisfy the following requirements:

- **Authentication**: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied.
- **Availability**: Availability requires that the information must be available to the legitimate users. DOS Attacks can bring down the network and hence information cannot be shared.
- **Non-Repudiation**: Non-repudiation means a node cannot deny that he/she does not transmit the message. It may be crucial to determine the correct sequence in crash reconstruction.
- **Privacy**: The privacy of a node against the unauthorised node should be guaranteed. This is required to eliminate the massage delay attacks.
- **Data Verification**: A regular verification of data is required to eliminate the false messaging.

VI. ATTACKERS ON VEHICULAR NETWORK

To secure the VANET, first we have to discover who are the attacker, their nature, and capacity to damage the system. On the basis of capacity these attackers may be three types.

• **Insider and Outsider**: Insiders are the authenticated members of network whereas
Outsiders are the intruders and hence limited capacity to attack.
• **Malicious and Rational**: Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Rational attackers have the personal profit hence they are predictable.
• **Active and Passive**: Active attackers generate signals or packet whereas passive attackers only sense the network.

VII. ATTACKS IN THE VANET

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below:

• **Impersonate:** In impersonate attack attacker assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network. This type of attack is performed by active attackers. They may be insider or outsiders. This attack is multilayer attack means attacker can exploit either network layer, application layer or transport layer vulnerability. This attack can be performed in two ways:

A. False attribute possession: In this scheme an attacker steals some property of legitimate user and later with the use of attribute claims that it is who (legitimate user) that sent this message. By using this type attack a normal vehicle can claim that he/she is a police or fire protector to free the traffic.

B. Sybil: In this type of attack, an attacker use different identities at the same time.

• **Session hijacking:** Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.
• **Identity revealing**: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.

• **Location Tracking**: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.
• **Repudiation:** The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.
• **Eavesdropping** is a most common attack on confidentiality. This attack is belongs to network layer attack and passive in nature. The main goal of this attack is to get access of confidential data.
• **Denial of Service:** DOS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DOS attacks can be carried out in many ways.

a)Jamming: In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.

b) SYN Flooding: In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

c) Distributed DoS attack: This is another form Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

• **Routing attack:** Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET:
a) Black Hole attack: In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.
b) Worm Hole attack: In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries.
c) Gray Hole attack: This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two type:

1. A malicious node can drop the packet of UDP whereas the TCP packet will be forwarded.
2. The malicious node can drop the packet on the basis of probabilistic distribution.

VIII. CONCLUSION

In this paper we have done the absolute survey and discussed on VANET. The aim of this paper is to give an overview of the vehicular ad hoc networks. Through this study we have represented about the open issues and challenges involved in VANET.

IX. REFERENCES

[1] Mahmoud Hashem Eiza, Qiang Ni, Thomas Owens and Geyong Min "Investigation of routing reliability of vehicular ad hoc networks" EURASIP Journal on Wireless Communications and Networking 2013, pp.179 , 1 July 2013.

[2] MarwaAltayeb and ImadMahgoub "A Survey of Vehicular Ad hoc Networks Routing Protocols" International Journal of Innovation and Applied Studies, Vol. 3 No. 3, pp. 829-846, July 2013.

[3] SheraliZeadally, Ray Hunt, Yuh-Shyan Chen Angela Irwin, Aamir Hassan "Vehicular ad hoc networks (VANETS): status, results,and challenges"Telecommunation System, EURASIP Journal on Wireless Communications and Networking.

[4] Rakesh Kumar and Mayank Dave "A Review of Various VANET Data Dissemination Protocols" International Journal of u- and e- Service, Science and Technology, Vol. 5, No. 3, September, 2012.

[5] Yanmin Zhu1, Chao Chen1 and Min Gao "An evaluation of vehicular networks with real vehicular GPS traces"EURASIP Journal onWireless Communications and Networking 2013,pp.190, 13 July 2013.

[6] Avdhesh Kumar Sharma "Ad-Hoc Network" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 7, July – 2013.

[7] Yun-Wei Lin, Yuh-Shyan Chen And Sing-Ling Lee "Routing Protocols in Vehicular Ad Hoc Networks:A Survey and Future Perspectives" Journal of Information Science and Engineering 26,pp 913-932 (2010).

[8] Bijan Paul, Md. Ibrahim, Md. Abu NaserBikas"VANET Routing Protocols: Pros and Cons"International Journal of Computer Applications ,Volume 20– No.3, April 2011.

[9] V. Namboodiri and L. Gao, "Prediction-based routing for vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 56, no. 4, pp. 2332– 2345, Jul. 2007.

[10] T. Taleb, M. Ochi, A. Jamalipour, N. Kato, and Y. Nemoto, "An efficient vehicle-heading based routing protocol for VANET networks," in Proc.IEEE Wireless Commun. Netw. Conf., 2006, pp. 2199–2204.