International Journal For Technological Research In Engineering
Volume 2, Issue 7, March-2015 *ISSN (Online): 2347 - 4718*

A SURVEY ON SECURITY IN VANET

Praveen G Salagar[1], Shrikant S Tangade[2]
Reva Institute of Technology and Management
Bangalore, India

Abstract: Vehicular Ad-Hoc Networks (VANET) is an application of MANETs that allows for communication between road transports vehicles and promotes safety on roads. This paper provides a summary of the recent state of the art of VANETs; it presents the communication architecture of VANETs and outlines the privacy and security challenges that need to be overcome to make such networks safety usable in practice.
Key Terms: VANET, Security, Attacks

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have grown out of the need to support the growing number of wireless products that can now be used in vehicles [1]. VANETs can be utilized for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge [2] and infotainment applications such as providing access to the Internet. Over the last few years, we have witnessed many research efforts that have investigated various issues related to V2I, V2V, and VRC areas because of the crucial role they are expected to play in Intelligent Transportation Systems (ITSs). In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router [3] to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. For communication to occur between vehicles and Road Side Units (RSUs), vehicles must be equipped with some sort of radio interface or Onboard Unit (OBU) that enables short-range wireless ad hoc networks to be formed [4].Onboard unit are radio device installed in vehicles that move, while the RSU are placed along the road and constitute the network infrastructure. RSU work as a router between the vehicles. Using the DSRC radios, OBU its link the vehicle to RSU. The goal of the VANETs is to allow the communication between vehicles. In order to be an integral component of a VANET and communicate efficiently, nodes need certain features that will help them to gather information and inform to their neighbors' and make decision by considering the collected information. The architecture in a VANET is split into 3 domains; In-Vehicle domain, Ad-Hoc Domain and Infrastructure Domain. As shown in the above figure the In-Vehicle Domain consists of OBU and many AU's (Application Units). The AU's are user device for example mobile phones and PDAs that performs certain functions when interacting with the OBU. The Ad-Hoc Domain consists of OBU's in vehicles and RSU's which are along the roadside. When the OBS's and RSU's are in range, they communicate wirelessly with each other. This forms an Ad-Hoc Domain because the vehicles connect to RSU's in an Ad-Hoc manner. The Infrastructure Domain consists of the RSU's and the CA (Certificate authority). Multi-hop communication is used between OBU"s and RSU"s when packets are forwarded from one OBU to another to reach the RSU [5].

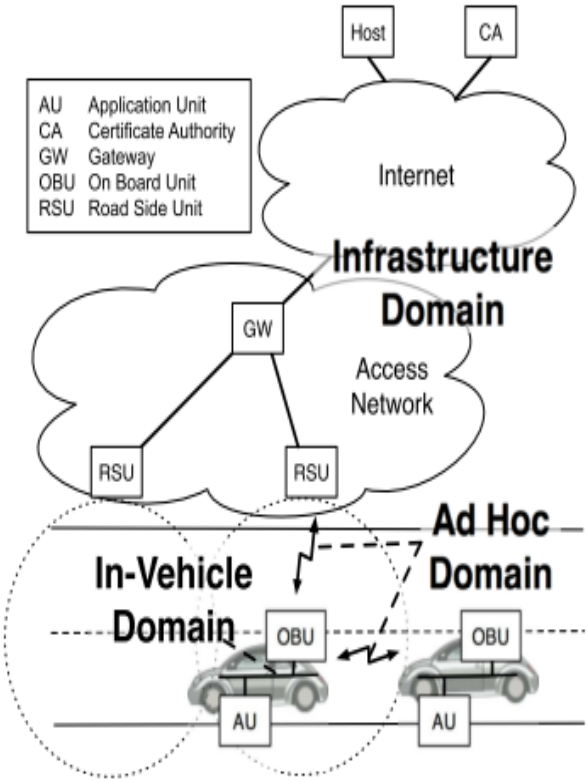

Figure1. VANET System Architecture

II. VANETs APPLICATIONS

VANETs represent an opportunity to develop application that improves the transportation sector and the traffic condition through collaborative systems. According to the functionality, the application are classified in three primary categories which are safety application, efficiency application n and infotainment application

Safety Application: - The main goal is to increase public safety and protect the loss of life. The main characteristic of this application is that safety data should be delivered to the intended receivers within the bounded time [6].

Efficiency and Infotainment Application: - These both applications are non- critical safety application. In this intended to focus only on non-critical safety application

Table 1: Vehicular Application Classification

Category	Sub-Classification	Vehicular Application
Safety application	Collision Avoidance	• Cooperative collision warning. • Safe distance notification. • Hazardous intersection message
	Road sign Notification	• Curve speed warning • Cooperative violation warning.
	Incident Management	• Emergency vehicle notification • Post-crash notification
Efficiency application	Traffic Management	• Intelligent traffic flow • Roadways planning • Congested road notification
	Traffic Monitoring	• Road condition sensing • Vehicles and fleet trafficking
Infotainment application	Contextual Information	• Commercial service announcement • Parking assistance
	Entertainment	• Media content download • Distributed games

III. CHARACTERISTICS AND CHALLENGES OF VANET

VANET is an application of MANET but it has its own distinct characteristics, the characteristics of VANETs are basically a mixture of wireless medium characteristics. The characteristics are:

1. High Mobility: - This is important features of the VANET as nodes move in a high speed all the time with different direction [7]. As per [8, 9], the high mobility of nodes reduces the mesh in the network (fewer routes between nodes). Compared to MANET, VANET mobility is relatively high.

2. Rapid Changing Network Topology: - As nodes move in very high speed so the position of node changes frequently so therefore network topology in VANETs tends to change frequently. The connection times are short especially between nodes moving in opposite direction.

3. No Power criteria: - The VANET node is equipped with a battery that is used as an infinite power supply for the communication and computation task

4. Time Management: - Safety message are the main goal of VANET. Message in VANET must be delivered to the nodes within the time limit so that a decision can be made by the node and perform action according.

5. Wireless Communication: - Data transmission is generally done by nodes. Nodes are connected and exchange their information via wireless communication

6. Bandwidth :- The Wireless Access in Vehicular Environment (WAVE) IEEE 1609.2 standard also known as DSRC 802.11p which support multi-hop communication for vehicles out of range and the range may be around 1000m[10]. The standardized DSRC band (5.850-5.925 GHz) for VANET can be considered as limited. The width of the entire band is only 75MHz, but in some countries it's not allowed. The maximum theoretical throughput is 27Mbps

The main challenges of the VANETs can be summarized as follows:

- Due to high mobility neighborhood location changes frequently-network Management.
- The unbounded network size.(channel load)Congestion and collision Control:
- Due to mobility signal power changes continuously.
- Environmental impact VANETs uses the electromagnetic waves for communication.
- Security as VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied.

IV. SECURITY CHALLENGES IN VANETS

The challenges of security must be considered during the design of VANET architectures, security protocols, cryptographic, algorithms etc. The following are the some security challenges in VANET [7].

- 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.
- Data consistency liability: VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence correlation among the received data from different node on particular information may avoid this type of inconsistency.
- Low tolerance for error: Some of the protocols are designed on the basis of probability. VANET uses life critical information on which action is

performed in very short time and small error in probabilistic algorithm may cause harm.

- Key Distribution: All the VANET security mechanisms which are implemented its dependent on keys. The messages have to be encrypted and 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. Thus the distribution of keys among vehicles is a major challenge in designing a security protocols.
- Incentives: Manufactures they have to build applications that consumer likes most. Very few of the 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.

V. SECURITY REQUIREMENTS IN VANET

In this section, we present security requirements for VANETs. There are several important requirements to achieve security in VANETs, which are discusses as follows [19]

- Authentication: Vehicles should respond only to the message transmitted by legitimate member of network, authentication ensures that the message is generated by the legitimate user. Thus, it is very important to authenticate the sender of a message.
- Data Verification: A regular verification of data is required to check whether the message contains the correct or corrupted data.
- Privacy: The profile or a driver's personal details must be maintained against unauthorized access.
- Non-Repudiation: A sender must not deny that he/she does not transmit the message whenever an investigation or identity of a vehicle is required. For eg. After sending the message, the vehicle should not deny having sent the message this is called sender non-repudiation. Also after receiving a message, the vehicle should not deny having received the message this is called receiver non-repudiation.
- Availability: The network should be available even if it under an attack without affecting its performance. For eg. The services provided by the RSU should be available to the vehicles whenever it is required.
- Data Integrity: It ensures that data or messages received are exactly the same sent by the authorized node without any modification, deletion or replay. This concept in VANETs often combines with the concept "authentication" to guarantee that a should be able to verify that a message is indeed sent and signed by another node without begin modified by attacker.

VI. DIFFERENT TYPES OF ATTACKS IN VANETS

Attackers play an important role in the VANET by launching the different types of attacks, which may create a problem for the user as well as the network.

Attackers can be classified based on scope, behavior of the attack as follow [11]. [12]:

- Active attackers: The attackers can generate message containing wrong information or do not forward the received message.
- Passive attackers: Passive attacker does not generate the message and they do not participate in the communication process of the network. Attackers eavesdrop only on the wireless channel.
- Insider Attackers: The insider attacker is a member node who can communicate with the other member of the network and have details knowledge of network. When they have all the information about the configuration than it is easy to launch attack and create more problem.
- Outsider Attackers: These attackers who is not authenticate to directly communicate with the other member of the network and create a very fewer problems as compare to insider attackers.
- Malicious Attackers: This attacker uses a various method to damage member of the network and these attackers are not personally benefits from attack.
- Rational Attackers: The rational attackers seek for their own benefits from the attack.
- Local Attackers: These attackers send off an attack with a limited scope for a particular area
- Extended Attackers: attacker broadens its scope by controlling several entities that are scattered across the network.

There are five different classes of attacks [13] and every class is expected to provide a better perspective for the VANETs security

A. Monitoring Attacks: In this attack tracking of the vehicles come in this class. The attacker just monitors the whole network, listen to the communication between V2V and V2I. If they find any related information then pass this information to the concern person (ex:- if the polices are planning to perform some operation against the criminal and they communicate each other's and guide about the exits location of the operation. Attackers will listen to all the communication and inform to the criminal about the operation). Every vehicle has its own unique ID and attacker disclose the identity of the other vehicles in the network by using this unique ID the attacker can track the location of required vehicles.

B Social Attack: All unmoral message (social attack) are lies on this class, it is a kind of emotional and social attack. Purpose of these kinds of messages is to indirectly create a problem in the network, any user show angry behavior when they receive such kind of messages

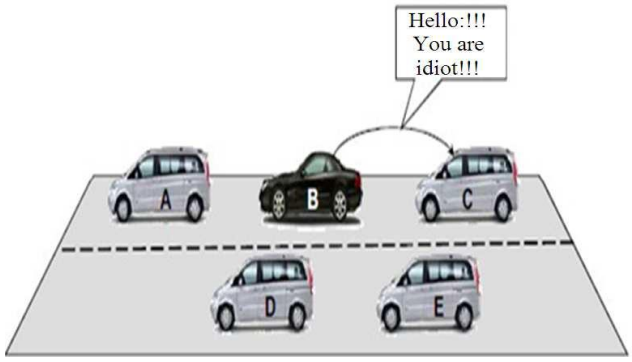

Figure2. Social Attack

In the above figure the attacker B passes a message "hello You are idiot" to nearby vehicle C. When user receives such kind of messages is directly disturb the other user in the network.

C Timing Attack: In this the main object is to add some time slot in original message and create delay in original message. Attackers do not disturb the others content of messages, only create delay in the message and these messages are received after it requires time.

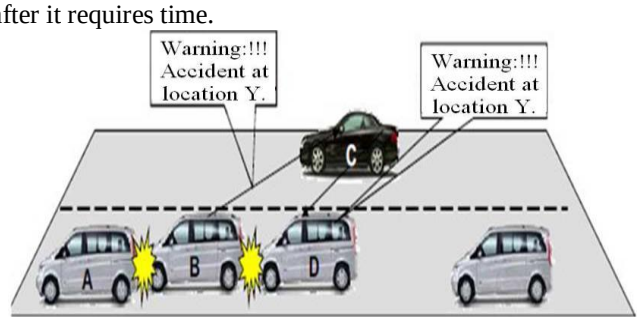

Figure3. Timing Attack

D Application Attacks: Safety and Non-Safety are two types of potential vehicular application. The main purpose of the attacker is to change the content of the message and send wrong or fake message to other vehicles which causes accident. Warning message is important message that are use in safety application. It is very serious condition on the road if the attacker changes the warning message; many accidents are occurred on roads as shown in the figure.

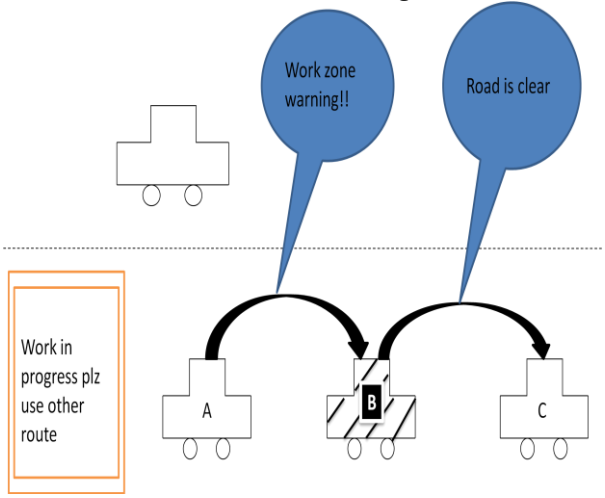

Figure4. Safety Application Attack

The important " warning messages" used in V2V or V2I communication are blind spot, post crash, breakdown, work zone, curve speed, lane change, stop sign violation, emergency vehicle approaching. The non-safety application it is related to the users comfort during their journey. Car parking is one of the major non-safety applications; RSU provides information about availability of parking in the shopping mall and sport complex. There are some services that are considered into non-safety application like Entertainment, toll collection, gas station, shopping mall finding, parking availability. The below figure shows the attack, were user 'A' receive information "parking slot available" from a road side unit(RSU) near the shopping mall, so user A send to user B. The user B actually a attacker for his own benefits he alter the message "no empty parking slot" and pass the message to user C.

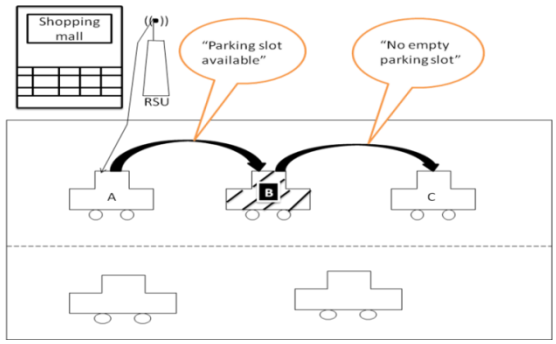

Figure5. Non-Safety Application Attack

E Network Attack: In this attacker can directly affect other vehicle and infrastructure. These attacks are of high priority because these affect the whole network.

There are many attacks that can disturb the security of the VANET and the privacy of its nodes (vehicles). Each type of attacks affects some of the security services in the system. The following are the most common devastating forms of attacks that a VANET can suffer [14]:

Bogus Information: Attacker can send the wrong information or bogus information. It can be sent from outsider or insider. The wrong information can affect the behavior of other drivers. This attack is related to authentications security requirements.

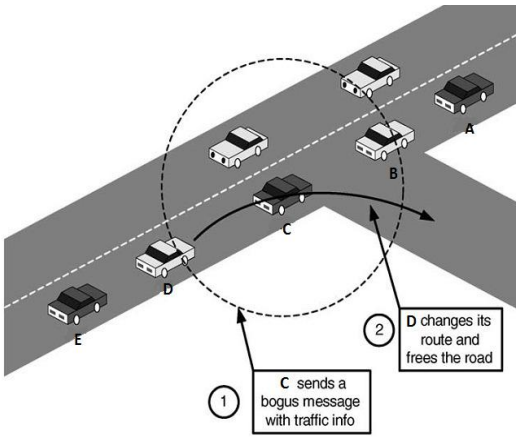

Figure6. Bogus Information

Denial of Service (DoS): [16][17]Here, the main aim is to prevent the authentic user access the network service. Attacker wants to bring down the network by sending unnecessary message to jam the channel and reduce the efficiency and performance of the network. The below figure indicates that a malicious black car transmit a dummy message "Lane close Ahead" to legitimate car behind it and even to the RSU to create a jam in the network.

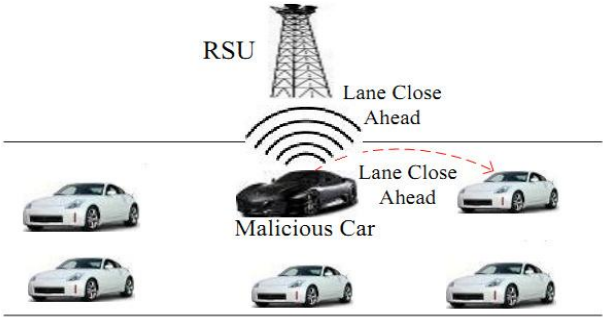

Figure7. Denial of Service ((DoS) Attack

Distributed Dos (DDoS): This attack is more severe than the DoS where number of malicious cars attack on a legitimate car in distributed manner from different location and different timeslots. Below figure 8 demonstrates a number of malicious black car attack on A from different location and timeslot so that A cannot communicate with other vehicles.

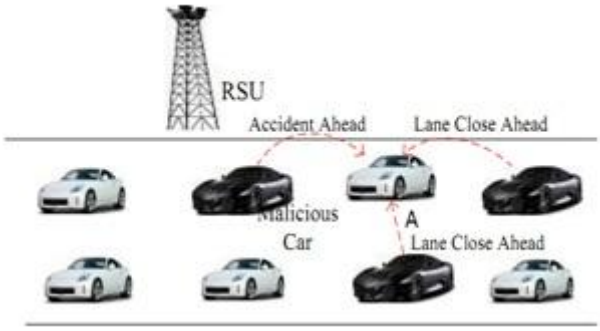

Figure8. Distributed DoS (DDoS) Attack

Sybil Attack figure9: Attacker generates multiple identities to simulate multiple nodes [18]. These identities can be used to play any type of attack in the system. Multiple messages are transmitted by attacker from different IDs to the other vehicles and creating an illusion that message are coming from different vehicles.

Figure9. Sybil Attack

1. *Black Hole Attack*: The node refuses to participate in the network or when an established node drops out to form a black hole. Therefore all the traffic of the network gets redirected towards a specific node which actually does not exist which results in data lost. Figure 10 indicates a black hole attack where the black hole is formed by a number of malicious nodes, which refuses to send the messages received from legitimate cars C and D to the cars E and F.

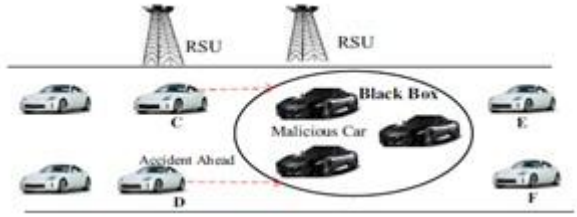

Figure10. Black Hole Attack

VII. SUMMARY

A review of the various approaches to achieve privacy in VANETs has been made in the recent years. A totally acceptable method which overcomes all the drawbacks is yet to be achieved and research in this direction has been done at present. The security aspects have to be achieved as it of paramount importance else implementation of VANETs will not be a success. VANETs represent a challenge in the field of communications security, as well as a revolution for vehicular safety, comfort and efficiency in road transport. We have addressed several important security issues with a special focus on efficiency and self-organization in our proposal. The main goals of any design for VANETs should be: wide applicability, node privacy, efficient group management, strong authentication, and data verification. In order to reach them, any solution has to combine well-known building blocks according to a modular design that includes several components specifically devoted to authentication, encryption, group management, data aggregation, simulation, safety-related/value-added applications, etc. We also discuss on some of the characteristics of VANETs with possible types of attacks based on intrusion detection.

REFERENCES

[1] Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

[2] Gerlach, M. (2006). Full paper: assessing and improving privacy in VANETs. www.network-on-wheels.de/downloads/escar2006gerlach.pdf (accessed: May 29, 2010).

[3] Jinyuan, S., Chi, Z., & Yuguang, F. (2007). An ID-based framework achieving privacy and non-repudiation. In Proceedings of IEEE vehicular ad hoc networks, military communications conference (MILCOM 2007) (pp. 1–7), October 2007.

[4] Stampoulis, A., & Chai, Z. (2007). A survey of security in vehicularnetworks.http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf (accessed: May 29, 2010).

[5] Panagiotis Papadimitratos et al., "Secure Vehicular Communication Systems: Design and Architecture," IEEE Communications Magazine: Topics in

Automotive Networking, pp. 100 - 114, November 2008.
[6] Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21
[7] Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).
[8] A. Dhamgaye, N. Chavhan, Survey on security challenges in VANET, Int. J. Comput. Sci. 2 (2013) 88–96, ISSN 2277-5420.
[9] 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.
[10] DSRC, Dsrc, http://grouper.ieee.org/groups/scc32/dsrc/.
[11] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, 15(1), pp. 39–68, 2007.
[12] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M.Gerlach, R. Kroh, and T. Leinmuller, "Attacks on inter-vehicle communication systems—an analysis". In Proceedings of the 3rd international Workshop on Intelligent Transportation (WIT), 2006
[13] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, "Classes of attacks in VANET", in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1 - 5, 2013.
[14] AJAY RAWAT1, SANTOSH SHARMA, RAMA SUSHIL, "VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS", Journal of Information and Operations Management, Volume 3, Issue 1, pp. 301-304, 2012.
[15] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, "Classes of attacks in VANET", in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1- 5, 2013.
[16] Al-kahtani, Salman bin Abdulaziz, Al Kharj, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)", in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), pp 1- 9, 2012.
[17] Bin Xiao, Bo Yu, Chuanshan Gao, ―Detection And Localization Of Sybil Nodes In VANETs‖, Diwans'06, September 26, 2006.
[18] Maxim Raya and jean-Pierre Hubaux, "The security of vehicular ad hoc network", In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks(SASN '05), 2005.

