International Journal of Computer Engineering & Technology (IJCET)
Volume 9, Issue 1, Jan-Feb 2018, pp. 8–19, Article ID: IJCET_09_01_002
Available online at
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=9&IType=1
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

ATTACKS ON VANET SECURITY

Prof. Ajay N. Upadhyaya
Computer Engineering Department, Doctoral Research Scholar,
Faculty of Technology, RK University, Rajkot, India
Assistant Professor L.J. Institute of Engineering & Technology,
GTU, Ahmedabad, India

Dr. J.S. Shah
Computer Engineering Department, Ex. Principal,
Government Engineering College, Patan, India

ABSTRACT

VANET is an emergent technology with a promising advantages but having high challenges in its security. VANET is a self-organizing network established among vehicles equipped with communication facilities. A lot of works have been done towards VANET but less attention is given to security of VANET. VANET is a Key component of intelligent transportation systems (ITS) and it can be used to improve road safety and allow a wide variety of different value-added services. Many forms of attacks against VANETs have emerged recently which compromise the security of such networks. Secure communication is a prerequisite for adopting VANET communication as a solution for the various applications. Delay or alteration of message in VANET application makes VANET environment non Trustable. In this paper we have done the analysis on different types of attacks on VANET security. We represented VANET Characteristics with security challenges and constraints. VANET attackers are represented into different categories based on their nature and the based on security services requirement.

Key word: Security, Authentication, Availability, Confidentiality, Integrity, Non Repudiation.

Cite this Article: Prof. Ajay N. Upadhyaya, Dr. J.S. Shah, Attacks on VANET Security. *International Journal of Computer Engineering & Technology*, 9(1), 2018, pp. 8–19.
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=9&IType=1

1. INTRODUCTION

Vehicular networking is nowadays very hot topic within the research field of communications. Lot of different approaches exists nowadays, although the standard approach called IEEE 802.11p is gaining the majority of interest. VANET is used for the applications like Life Critical Safety Application, Basic Safety Application, Road Side

Service Finder, Group Communication, Internet Access, Electronic Tall Connection and many more. Fig. 1 is showing graphical representation of different VANET Applications.

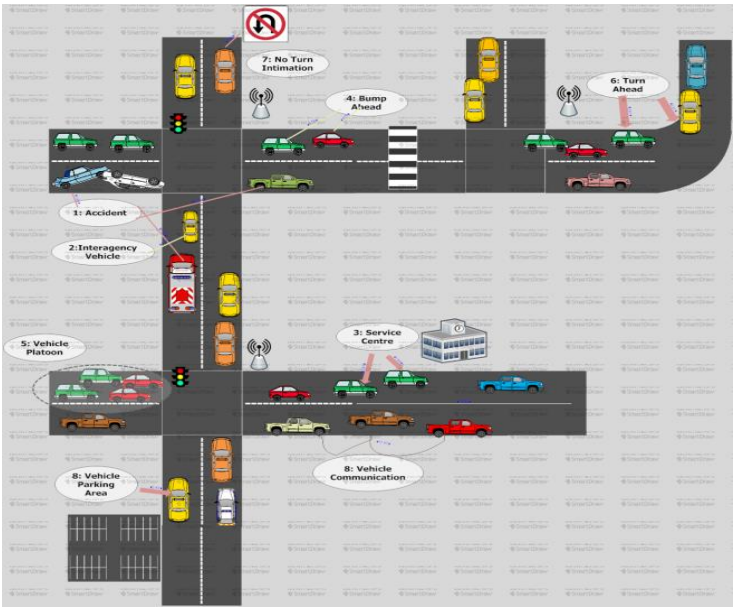

Figure 1 Applications of VANET

These types of applications are only useful when it provide correct and accurate details on time. The main concern is how to provide best security in VANET without any negotiating with performance & reliability. Security is often considered to be the major "roadblock" in commercial application of VANET. Two types of communication can be possible in VANET. One is V2V (Vehicle to Vehicle) and other is V2I (Vehicle to Infrastructure). Each Vehicle contain OBU (On Board Unit) and each cross road enabled with RSU (Road Side Unit). Attackers disturb the communication by getting full or partial access in communication of network. Here we are discussing some of the property of attackers and based on them we categories them into different category.

2. RELETED WORK

Different researchers have analyzed VANET security issues, needs and priorities with the different perspective. In recent research work [1], [2], [3] & [5], author discussed about different types of attack and security mechanism for avoiding such network attacks. In [4], the author shown detail survey of emerging and established wireless ad-hoc technologies and also highlight their security features, privacy features and deficiencies. In [6] author represented the communication architecture of VANETs and the give outlines of privacy and security challenges that need to be overcome to make networks safety usable in practice. In [7], author discussed the security features, challenges, and attacks of VANETs and they classify the security attacks of VANETs based on different network layers. In [8], author addresses the security of VANET with a detail threat analysis and appropriate security architecture. In [9], [10] & [14], author represented different security proposal proposed by various researches. In [11], author represented survey of existing trust models in VANETs and point out their key issues. Based on these studies, author suggests desired properties towards effective trust Management in VANETs. In [12], author proposed Sybil attack detection approach in VANET. In [13] author presented the existing security protocols and mainly concentrates on different ways to improve the intelligence of the decision system for enhance the security in VANET. In [15], author discussed about hierarchical structure of

VANET with the different types of threats. In [16], author discussed Emerging attacks on VANET security based on GPS Time Spoofing.

3. VANET CHARACTERISTICS, SECURITY CHALLENGES AND CONSTRAINTS

3.1. VANET Characteristics

Here we will discuss some of the VANET characteristics like Scalable network, High mobility, Sufficient energy, Sufficient storage source and Time Sensitive Exchange of Information.

VANET is a *scalable* and unbounded network which is completely independent from the number of nodes. It can be implemented for one or several cities even for whole country. *High mobility* is responsible for dynamic changes in network topology. Nodes in VANET are moving with very high mobility which make harder to predict their position and the network topology. OBU attached in vehicle having *continuous unlimited power source* and also having *high storage capacity*. Vehicle nodes are having their own power in the form of batteries and high computing powers to run complex cryptographic calculations for maintaining security. V2V and V2I communication are exchanging *time sensitive information* in which Fraction of second's delay may create unwanted harmful result.

3.2. Security Challenges

VANET communication must be secure and having guarantee that transmitted message is not inserted or modified by any attackers. We will discuss some of them at here: Trustworthiness of the data, Key distribution, Secure optimizes route selection.

In VANET, communication is done between V2V and V2I. In both type of communications nodes are gathering information from other nodes or from RSU which must be *trustworthy*. Before accepting any information need to verify the authenticity of sender who forwarded the data. *Key distribution* handling is difficult to manage because high mobility of vehicle. Each message is encrypt and need to decrypt at receiver side with same or different key. Different manufacturers may use different solutions for it which is very challenging task to handle. Dynamically changes are occurring in vehicle topology due to their fast movement. Data must be communicated through optimized path. Here there is need to select an *authenticated optimized path* for secure communication.

3.3. Constraints

Here we will discuss constraints of V2V and V2I communication like Bandwidth, security, Privacy of vehicles and participation of vehicles.

Due to limited *bandwidth*, there is a need to find smart usage of available bandwidth. For better utilization of bandwidth one basic solution is filtering of data. Send as less as possible data in network by different data processing and filtering. Second constraint is *security* which is mandatory for real-world systems. There is need to detect malicious node, before they harm the system. Several methods are available for secure communication. As a part of security we have to register vehicle node and need to authenticate before transmitting any kind of data. Another constraint is maintaining *privacy* of vehicle by hiding the vehicle id to other user. It is depends on user to declare his identity or vehicle id to others or not. Here the question of privacy is generated from others and also we have to keep some vehicles id hide like VIP persons from other user for security reasons. *Participation* of vehicle is also one of the major constraints. All vehicles must be equipped with transceiver, which can transmit and receive

VANET data. It is depends on node that, node want to participate in network or not. For the limited amount of data it is ok, but if amount of data to send is high then there question will arise *why should I transfer?* So here need to do equal distribution of data lode on node.

4. TYPES OF ATTACKERS & SECURITY REQUIREMENT (SERVICES)

4.1. Types of Attackers

For secure VANET communication first we have to discover who are the attackers, their capacity and nature to spoil the network communication. Based on their nature we divided attackers into following five categories:

Active and Passive Attacker: Based on the participation nature of attackers we can categories attackers into two categories: Active and Passive Attacker. Active Attacker takes active part in communication by replying the message, by changing the content of message or dining the available services to legitimate users. Passive Attacker does not disturb the communication, but only observes the communication and monitors the traffic and position details of other vehicles.

Insider and Outsider attacker: Based on the Network knowledge we can categories the attacker in two categories: Insider and Outsider Attacker. Insider attacker is having all the communication details running inside the network and outside attackers haven't such details or having very less details. Insider attackers are the authenticated type of attacker, whom has details knowledge of network. These types of attacker learn about the design and structure of network and launches attack based on gain knowledge to disturb communication. Outsider attackers are also authenticated user of system but have a less knowledge of internal system. These types of attacker have limited scope compare to insider attacker.

Area Attacker: Such attackers are targeting some specific area before spreading such attacks in network. Total reflected area is depends on type of attack. It can be reflect communication of V2V or V2I in specific area. It can affect single or multiple OBU/RSU communication which is area specific.

Communication Attacker: This type of attacker attacks on specific communication like RSU to RSU communication, RSU to OBU Communication, and OBU to OBU Communication. Attackers want to deny user or the group of users by not allowing specific type of communication like denying of specific type of services.

Malicious and Rational Attacker: Malicious attackers are not having any personal benefits by disturbing the network. Such attackers only want to disturb the running network. Rational attackers are having any personal reason or profit for doing such malicious activities inside the network.

Timing Attacker: In this type of attack, attackers involve unnecessary delay in transmitted messages. Legitimate user will get the important message after required time. Due to such type of delay message becomes useless and some time it becomes very harmful in safety related messages.

4.2. Security Requirement (Services)

The security services increase the security of processing and data exchange in VANET. The security requirement includes:

Authentication: It ensures that message is generated through legitimate user. Receiver will only trust on data which are coming from the authenticated source.

Availability: Different attackers make target on availability of node or service provided by node. Attacker will try to block services for legitimate users or deny the user for the specific limited period of time or permanently.

Confidentiality: It involves the set of rules or a promise that limits access restrictions on certain resources**.** Attackers directly or indirectly will attack on confidential details of users.

Integrity: Data which is received by receiver it is in the same form in which sender send it. In this attacker try to exchange the data transmitted by sender. Digital signature is used for data integrity.

Non Repudiation: Sender or receiver can't deny after sending or receiving of transmitted messages.

Privacy and anonymity: It hides the identity of the user against unauthorized user nodes using temporary and anonymous keys.

Traceability: Although a vehicle real identity should be hidden from other vehicles, still it must be traceable. There should be a minimum one component with the ability to obtain vehicles' real identities if it's required.

5. VANET ATTACKS

Here we have will discuss different thirteen types of VANET attacks. Different types of attack and its effect is shown in Table I, which will be followed by detailing of different VANET attacks.

Table 1 Vanet Attacks and its Impact on Network

Attack Name	Active / Passive	Security Requirement	Impact on Network
(DOS) Attack	Active	Availability	High
(DDOS) Attack	Active	Availability	High
Sybil Attack	Active	Authentication	Medium
Node Impersonation Attack	Active	Integrity	Medium
Eavesdropping	Passive	Confidentiality	Medium
Masquerading	Active	Authentication	High
Global Positioning System (GPS) Spoofing	Active	Authentication, Traceability	Medium
Brute force Attack	Active	Confidentiality, Privacy and anonymity	High
Pranksters	Active	Integrity	High
Application Attack on safety and Non Safety messages	Active	Availability, Integrity	High
Black Hole attack	Active	Availability	High
Worm Hole attack	Active	Availability	High
Gray Hole attack	Active	Availability	High

5.1. Denial of service (DOS) Attack

In DOS attack attacker attack on services provided by service provider. Legitimate user will not access the service in the network though free recourses are available. Attacker jams the main communication medium. This type of attack is limited to range of service provider. Attackers may achieve this goal in two different ways: In basic level attackers overwhelm the resource by sending large sets of requests. So resource will remain continuous busy by giving response to such fake requests and will not be able to attend other legitimate user requests. Such attacks can be extended by sending a very large set of requests and jam the

communication. So RSU cannot handle any request sent by OBU. Fig. 2 is representing DOS attack in which Car C is attacker car and is denying the other user Car B, D, E, F, G and H for accessing the services from RSU.

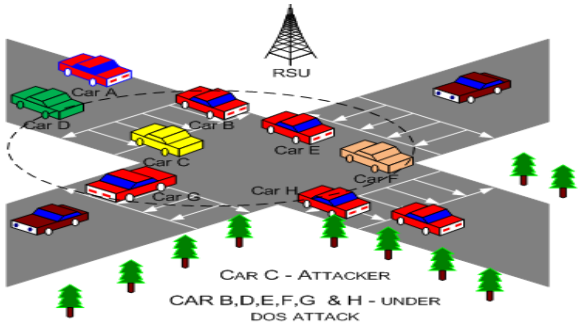

Figure 2 DOS Attack in VANET

5.2. Distributed Denial of service (DDOS) Attack

DDOS attack is generated by managing DOS attack in distributed manner. In DDOS attack multiple attacker targets the single or multiple service provider from multiple location to create inconvenience in use of service provided by service provider. In this attack more number of malicious OBU nodes involved which block the other legitimate users to access the services form one or more RSU. Attackers increase unnecessary transmission latency of network by sending spam messages in the network. Spreading of such attack is very dangerous for VANET. Fig. 3 is representing DDOS attack in which Car C & Car I is attacking on the services provided by RSU. Car B, D E & G denied by attacker Car C and Car F, H & J denied to access services of RSU by Attacker Car I.

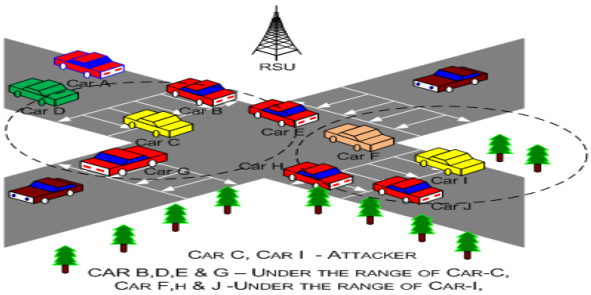

Figure 3 DDOS Attack in VANET

5.3. Sybil Attack

In Sybil attack attacker creates multiple identities of nodes which spread the wrong information in the network. In this type of attack data are broadcasted with fabricated identity. This type of attack implemented by the attacker OBU on the other legitimate OBU for getting the different benefits. In this attack attacker vehicle create the multiple identities and send the messages to legitimate user like there is a *more traffic on selected trip road so change the route*. One illusion will create by attacker and similar type of message will send to the same vehicle. Now legitimate user will receive the same kind of messages and due to the illusion it will fill that messages are send by different sender and by believing it vehicle will change the route. This decision is beneficial to attacker and now attacker vehicle will get clear route on selected trip. This type of attack will also use to redirect user on wrong place. Fig. 4 is representing Sybil attack in which Attacker Car C is creating multiple identities and send messages to other user that road is having high traffic. So by getting such messages Car B and Car D will choose other alternate path and now car C will receive free road.

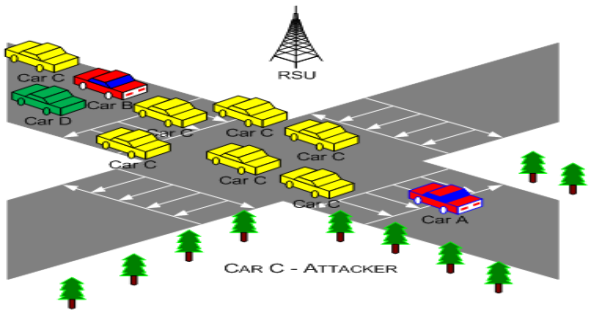

Figure 4 Sybil Attack in VANET

5.4. Node Impersonation Attack

In Node Impersonation Attack Attacker update the message and claims that message comes from original authenticated source. As in Fig. 5, vehicle D is sending messages regarding the accident at location x for getting the help but attacker node C will update the messages and forward it to the ambulance that accident is occur at location Y. In this attack attacker intentionally sending false information in the network. Purpose of this type of message is sending to create confusion in the communication or to send for selfish behavior of node to get some facility. It is also known as a Message Tempering attack. Such type of updates in life critical messages will become very costly in the VANET.

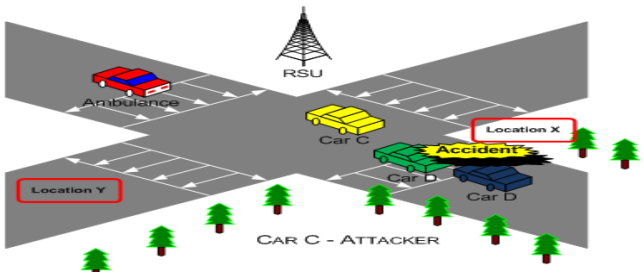

Figure 5 Node Impersonation Attack in VANET

5.5. Eavesdropping Attack

This is a passive attack in which attack is done on confidentiality of network. Attackers gather the confidential data of network. Attackers silently observe the traffic of network or the current position and activities of particular vehicle node. Detection of such attacker is very difficult because they are not giving any reaction in current network. As in Fig. 6, Car C continuously observing the details of ATM Van and leaking such information to burglar. ID Disclosure attack is a one sub category of eavesdropping in which attacker reveal the identity details of node and use it to track targeted node.

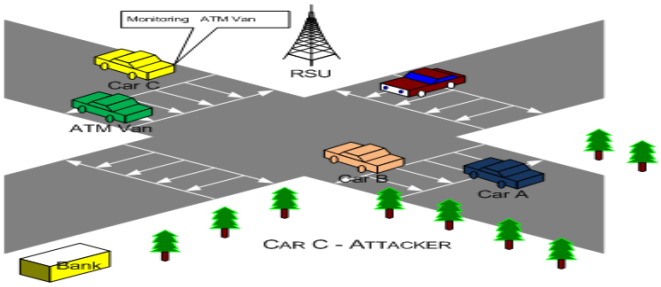

Figure 6 Eavesdropping Attack in VANET

5.6. Masquerading Attack

In this type of attack attacker pretends to be another vehicle by using other vehicle's identity. As in Fig. 7, attackers Car C act as a Police vehicle and through that try to do fraud with other vehicle to slow down their speed or stop the vehicle. By facing such type of attack user will lost their trust from VANET.

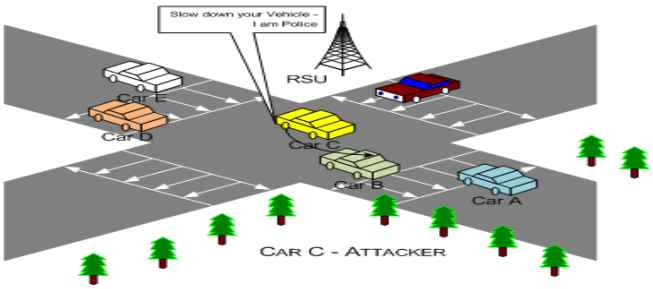

Figure 7 Masquerading Attack in VANET

5.7. Global Positioning System (GPS) Spoofing

This attack is also known as Position Faking attack. In this type of attack attacker tries to change current geographic location identity and produce false information from GPS system by using such technique user is hiding his current position from the network and show the wrong position to others. This attack can be done by single vehicle or group of vehicles. As shown in Fig. 8, five vehicles are moving on Road ID -6 but they are hiding their current position and sending wrong information in the network. By getting such details RSU may pretend that currently there is no any vehicle on Road Id-6.

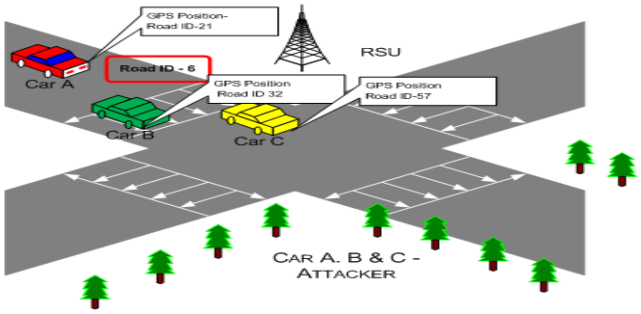

Figure 8 Global Positioning System (GPS) Spoofing in VANET

5.8. Brute Force Attack

Sender vehicle have to send their data to destination vehicle by taking the help from other vehicle, if destination node is away from his range. For maintain the secrecy sender vehicle may encrypt their data and send it to the destination via any mediator vehicles**.** This is a one type of cryptography attack in which mediator vehicle will act as an attacker and try to decrypt the encrypted information by continuously trying different alternate possible solutions. Fig. 9 shows that Car A want to send the message to Car F but it is not in its range. So Car A send the encrypted message to Car F via Car C which is malicious node and by enforcing brute force attack try to decrypt the encrypted data by imposing various possible solution.

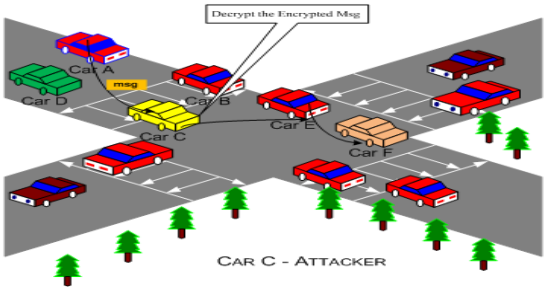

Figure 9 Brute Force Attack in VANET

5.9. Prank Attack

In this type of attack attacker playing pranks with other vehicles. As shown in Fig. 10, malicious node Car C is sending messages to Car A that to "Slow down your speed" and second vehicle Car B which is behind of Car-A that"Increase your speed". Due to this type of attacks user lost trust from the system.

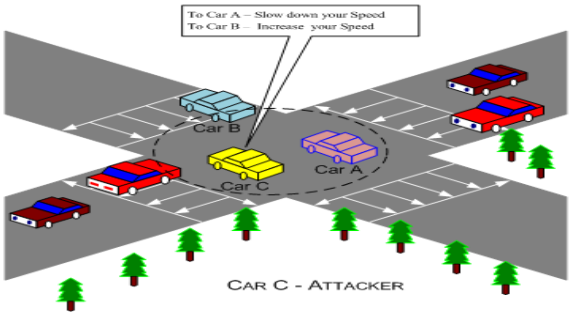

Figure 10 Prank Attack in VANET

5.10. Application Attack on safety and Non Safety messages

Safety messages are one of the main applications of VANET. In VANET user will get messages like Bump Ahead, Traffic Congestion details, Blind Turn ahead, Accident and Slow down Speed for safety. Attacker will updates the content of message and forward wrong information to the legitimate user. Attackers can also do the updates in Non Safety application messages like nearer available Service Station, Petrol Pump or Hotels etc. As in Fig. 11,Gas Station is very nearer to Car A but attacker Car C will updates the contents and send the updated message that petrol pump is 5 km ahead in right direction. This type of attack is a direct attack on the usability on VANET systems.

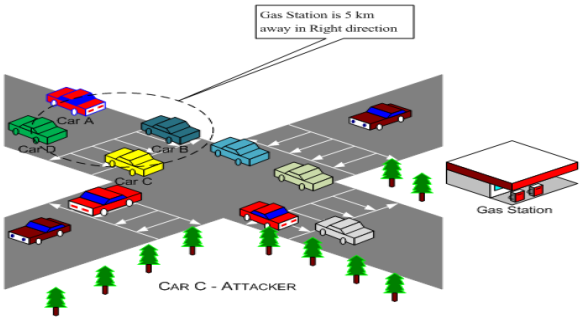

Figure 11 Application Attack on Safety and Non Safety messages in VANET

5.11. Black Hole attack

It is a one types of routing attack in which attacker attract the other node of network to transmit packet through it by showing shortest path to the interested transmitter node. After getting packet it drop the packets. Fig. 12 illustrates an example where Car-A wants to send data packets to Car E AND Car G but it doesn't having any route details for both. Therefore, Car A initiates the route discovery process and RREQ is forwarded to Car B and Car H. As a malicious node, Car H will claim that it is having shortest route to reach at Car E and Car G. Based on available reply, Car A will send all messages to Car H and becomes the victim of blackhole attack.

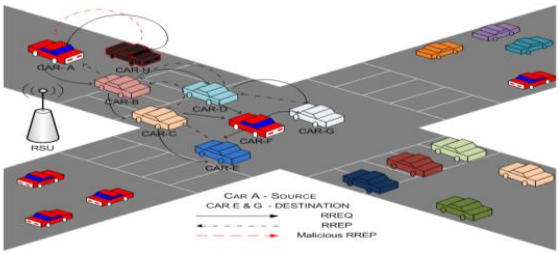

Figure 12 Black Hole attack in VANET

5.12. Wormhole attack

It is also the one type of routing attack in which attacker malicious node receive data packet from the legitimate user at any point in the network and tunnel them and forward it to the other point network. Tunnel created between two malicious nodes are called wormhole attack. Fig. 13 is showing wormhole attack in VANET.

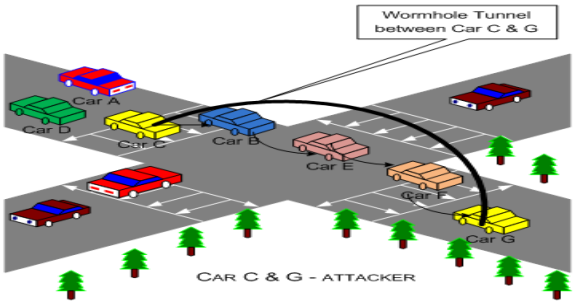

Figure 13 Wormhole attack in VANET

5.13. Gray Hole attack

It is another type of routing attack and also known as an extension of Black hole attack in which instead of dropping all packets it only drops selected packets. It is very difficult to detect such attack because it is not continuous in nature. It is only created for specific time and for specific type of packets only.

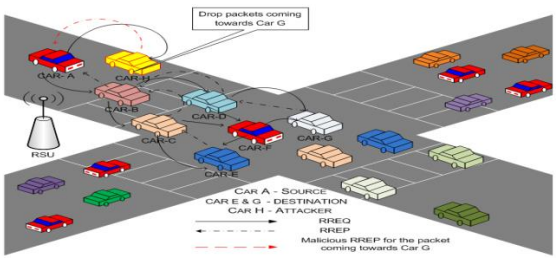

Figure 14 Gray Hole attack in VANET

Fig. 14 illustrates an example where Car A wants to send data packets to Car E & Car G but it doesn't having any route details for both. Therefore, Car A initiates the route discovery process and RREQ is forwarded to Car B and Car H. As a malicious node, Car H in only interested to drop packets coming towards Car G and so it will claim that it is having shortest route to reach at Car G. Based on available reply, Car A will send all messages for Car G via Car H and becomes the victim of Gray hole attack.

6. CONCLUSIONS

VANET communication must be secure from different types of attackers. If an attacker changes the contents of data, create unnecessary delay, changing self identity or misbehave in the network it becomes crucial for VANET network. In this paper we present different types of attacks on VANET with their classification. Proposed classification will helpful to researchers to understand the different attacks. We shown the classification of VANET attacks based on its nature which will be helpful to understand demands of security in VANET.In future, we plan to implement different types of VANET attack and will analyze adverse impact of it on VANET network. We will also work on preventive measurement and attacker detection methods for different types of attack.

REFERENCES

[1] Mohan V. Pawar, J. Anuradha, Network Security and Types of Attacks in Network, Procedia Computer Science, Volume 48, 2015, Pages 503-506, ISSN 1877-0509.

[2] Amandeep Singh, Sandeep Kad, A Review on the Various Security Techniques for VANETs, Procedia Computer Science, Volume 78, 2016, Pages 284-290, ISSN 1877-0509.

[3] S. Sarika, A. Pravin, A. Vijayakumar, K. Selvamani, Security Issues in Mobile Ad Hoc Networks, Procedia Computer Science, Volume 92, 2016, Pages 329-335, ISSN 1877-0509.

[4] R. Di Pietro, S. Guarino, N.V. Verde, J. Domingo-Ferrer, Security in wireless ad-hoc networks – A survey, Computer Communications, Volume 51, 15 September 2014, Pages 1-20, ISSN 0140-3664.

[5] Navjot Kaur, Sandeep Kad, A Review on Security Related Aspects in Vehicular Adhoc Networks, Procedia Computer Science, Volume 78, 2016, Pages 387-394, ISSN 1877-0509

[6] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Vehicular Communications, Volume 1, Issue 2, April 2014, Pages 53-66, ISSN 2214-2096.

[7] Bassem Mokhtar, Mohamed Azab, Survey on Security Issues in Vehicular Ad Hoc Networks, In Alexandria Engineering Journal, Volume 54, Issue 4, 2015, Pages 1115-1126, ISSN 1110-0168

[8] Maxim Raya and Jean-Pierre Hubaux. 2005. The security of VANETs. In Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET '05). ACM, New York, NY, USA, 93-94.

[9] Bharati Mishra, Priyadarshini Nayak, Subhashree Behera, and Debasish Jena. 2011. Security in vehicular adhoc networks: a survey. In Proceedings of the 2011 International Conference on Communication, Computing & Security (ICCCS '11). ACM, New York, NY, USA, 590-595.

[10] J. T. Isaac, S. Zeadally and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," in IET Communications, vol. 4, no. 7, pp. 894-903, April 30 2010.

[11] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-6.

[12] D. Gantsou, "On the use of security analytics for attack detection in vehicular ad hoc networks," 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, 2015, pp. 1-6.

[13] V. Paruchuri, "Inter-vehicular communications: Security and reliability issues," ICTC 2011, Seoul, 2011, pp. 737-741.

[14] G. Samara, W. A. H. Al-Salihy and R. Sures, "Security issues and challenges of Vehicular Ad Hoc Networks (VANET)," 4th International Conference on New Trends in Information Science and Service Science, Gyeongju, 2010,pp. 393-398.

[15] Qingzi Liu, Qiwu Wu and Li Yong, "A hierarchical security architecture of VANET," International Conference on Cyberspace Technology (CCT 2013), Beijing, China, 2013, pp. 6-10.

[16] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer and B. Eissfeller, "Emerging attacks on VANET security based on GPS Time Spoofing," 2015 IEEE Conference on Communications and Network Security (CNS), Florence, 2015, pp. 344-352.