A SURVEY ON BLACK HOLE & GRAY HOLE ATTACKS DETECTION SCHEME FOR VEHICULAR AD-HOC NETWORK

Arpita Rathod[1], Prof. Shreya Patel[2]

[1]*Student, Dept. Of Computer Engineering, Grow More Faculty of Engineering Himatnagar, Gujarat, India*
[2]*Asst. Professor, Dept. of Computer Engineering, Grow More Faculty of Engineering Himatnagar, Gujarat, India*

Abstract - *Vehicular Ad Hoc Network(VANET) is a technology which accommodate the vehicle to interconnect with each other through a wireless network. So that it can track and locate other vehicles to provide road safety. Security is a major issue in VANET as it can be life threatening. VANET is a subclass of ad hoc network and it is almost same as Mobile Ad Hoc Networks (MANET) but in VANET nodes are vehicles. It is a challenging topic because of frequent link disruptions caused by vehicle mobility. The black hole attack is a form of a denial of service attack that makes a gap for data traffic in a VANET. A Gray hole is a technique in which the spiteful node just drops the packet from some specific node in the network and forwards all other packets to its destination. This paper discusses some of the techniques put forwarded by researchers to detect Black hole and gray hole attack in VANET.*

Key Words: **VANET, Security Attacks, Black hole attack, Grey hole attack, Omnet++.**

1.INTRODUCTION

A wireless ad hoc network (WANET) or MANET is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use[8] .

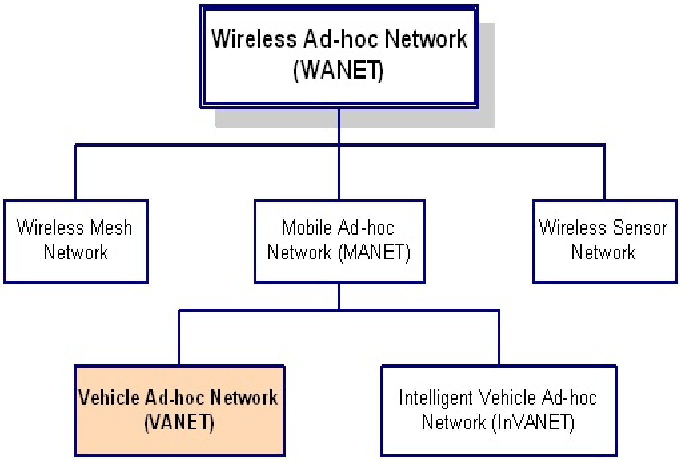
Wireless Ad-hoc Network (WANET)
Wireless Mesh Network
Mobile Ad-hoc Network (MANET)
Wireless Sensor Network
Vehicle Ad-hoc Network (VANET)
Intelligent Vehicle Ad-hoc Network (InVANET)

Fig -1: wireless ad-hoc network[9]

Vehicular Ad Hoc Network(VANET) is a technology which accommodate the vehicle to interconnect with each other through a wireless network. Vehicular ad hoc networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) the spontaneous creation of a wireless network for data exchange to the domain of vehicles. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services[1]. VANETs are a key part of the intelligent transportation systems (ITS) framework.

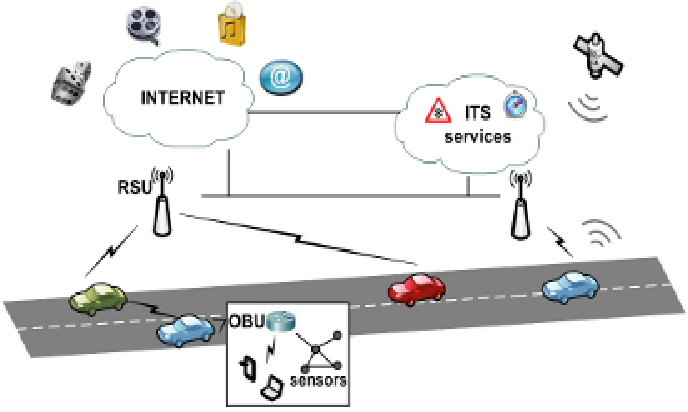

Fig -2: ITS framework[7]

2. Attacks of VANET

There are various types of attacks that can affect the entire system or can mortify the execution of system. These attacks can be marked into subsequent types:

- Impersonation Attack
- Denial of Service Attack
- Routing Attacks

I. Worm Hole Attack
II. Black Hole Attack
III. Gray Hole Attack

2.1. Impersonation Attack :

Each vehicle has a unique identifier in VANET and it is used to verify the message whenever an accident happens by sending wrong messages to other vehicles. Fig 3 explains this scenario in which vehicle A involves in the accident at location Z. When police identify the driver as it is associated with driver's identity, attacker changes his/her identity and simply refuses it.

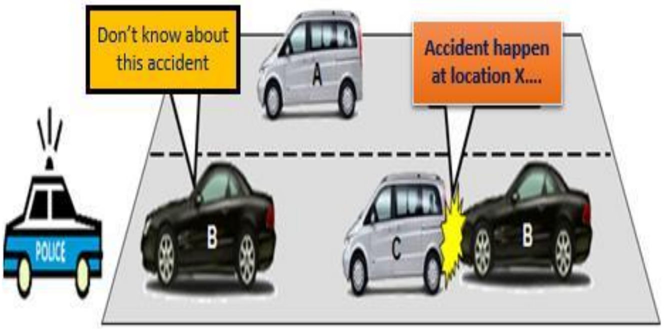
Don't know about this accident
A
Accident happen at location X....
POLICE
B
C
B

Fig -3: Impersonation Attack

2.2 Denial of Service Attack :

Dos attacks are most famous attacks in this list. in this attack attacker check the authorised user to use the service from the suffered node . In this, attackers may transfer dummy messages to jam the channel and thus, diminish the effectiveness and completion of the network. In this figure a malicious black car forges a great number of fake identities and transfer the dummy messages "lane close ahead" to a authorised car behind it and even to an RSU to generate a illusion in the network.

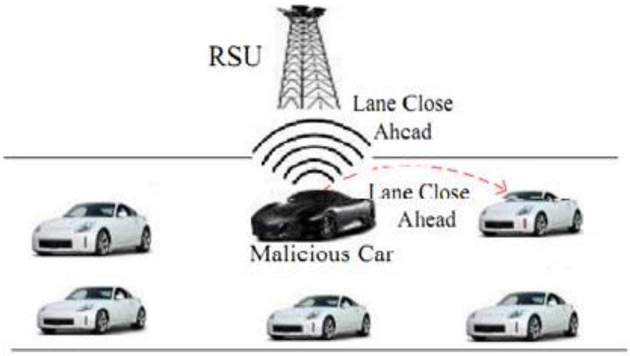

Fig -4: Denial Of Service Attack

2.3 Routing attack:

Routing attacks are those attacks which utilize the risk of network layer routing protocols. In this type of attack the attacker either releases the packet or disorders the routing process of the network.

Following are the most common routing attacks in the VANET:

2.3.1 Worm Hole attack:

It is provocation to observe and stop this attack .in this attack, an competitor receives packets at one point and tunnels them to another point in the network ,and then repeat them into the network from that point. This tunnel between two competitors are called wormhole . It can be created through a single long-range wireless link[2].

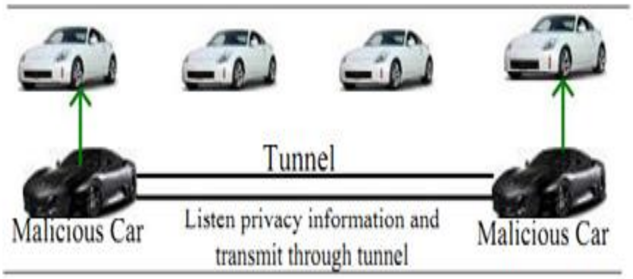

Fig -5: Worm Hole Attack

2.3.2 Black Hole Attack :

In this type of attack, the attacker firstly engage the nodes to transfer the packet through itself. When some malicious user enter into the network and stop onward messages to next nodes by releases messages are called as black node[3]. When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node.

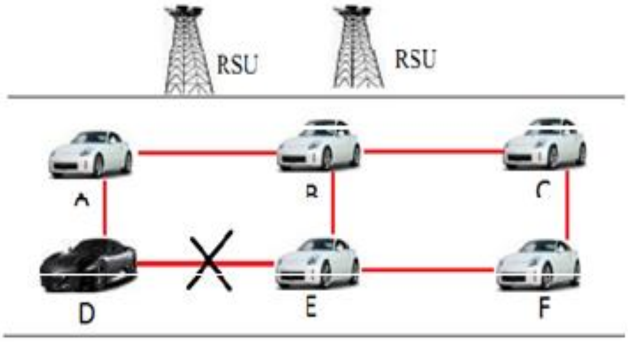

Fig -6: Black Hole Attack

2.3.3 Gray Hole attack:

This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message. In this way wrong information is broadcast.A Gray hole is a technique in which the spiteful node just drops the packet from some specific node in the network and forwards all other packets to its destination. This is the addition of black hole attack[3]. In this type of attack the malicious node behaves like a black node but it releases the packets selectively .

Fig -7: Gray Hole Attack

3. OVERVIEW OF ATTACKERS IN VANET[6] :

1. Passive Attackers
2. Active Attackers
3. Insider Attackers
4. Outsider Attackers
5. Malicious Attackers
6. Rational Attackers
7. Local Attackers

1. Passive Attackers: As the name suggests these attackers do not participate in the communication process but only surveillance the wireless channel to bring out information and pass them on to other attackers that is they have an indirect involvement in the attack.

2. Active Attackers: Active attackers have a direct involvement in the attack. These kinds of attackers either generate a wrong set of information or do not forward the correct information received that is the message is misinformed.

3. Insider Attackers: Such attackers are the legitimate users having complete knowledge of the configuration and usage of the network which provides them an easier access to creating problems as compared to other attack.

4. Outsider Attackers: As compared to the insider attackers these create fewer problems. Such intruders are the legitimate users and create problems by misusing the protocols of the network and thus attackers in such cases are limited.

5. Malicious Attackers: The objective of such attackers is to disturb the effective working of the network without drawing any personal benefits from it, but harming the network members and its function. Such attackers cause a severe damage to the network and are thus considered as the most hazardous.

6. Rational Attackers: Being more predictable, such attackers seek to draw out personal benefits from the attack.

7. Local Attackers: Attackers are limited to a specified area and thus attack with a limited scope. But this may involve the main area of the road thus causing a severe damage in the network.

4. COMPARISON BETWEEN BLACK HOLE ATTACK AND GRAY HOLE ATTACK :

Now we present the results of the analysis in which we exclusively compare the impact of Black Hole attack with Gray Hole attack on AODV with different network size.

As shown in the following Fig. 8 the packet delivery ratios of nodes in the presence of these two attacks are greatly affected. But if we compare the impact of Black Hole attack with Gray Hole attack, then the packet delivery fraction decreases more than that of Gray Hole attacks[5].

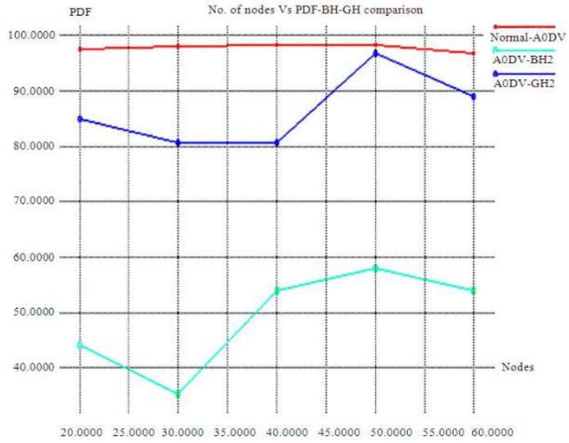

Fig. 8. Comparision graph

So, obviously Black Holes and Gray Holes effects network and leads to poor packet delivery in the network.

Gray Holes attacks in AODV caused too much packet drops. But if we compare the impact of Black Hole attack with Gray Hole attack, then the black Hole caused much packet drops than the Gray Hole attack.

5. CONCLUSIONS

Users require safety on road in future vehicular network and it could be possible by implementing VANET applications. Vehicular applications must be secured; if attackers change the content of safety applications then users are directly affected. Attackers change their attacking behavior and they launch different attacks at different time. It is difficult to control attackers but in future work we will develop such system to identify attacks in network with respect to some specific class of attack. Implementation could be easy of this future human life saving network if we control attackers and their attacks.

REFERENCES

[1] Hanin Almutairi, Samia Chelloug, Hanan Alqarni, Raghda Aljaber, Alyah Alshehri, Dima Alotaish, "A New Black Hole Detection Scheme for Vanets", ACM, 2014.

[2] Rashmi Mishra ,Akhilesh Singh, Rakesh Kumar , VANET Security: Issues, Challenges and Solutions ,IEEE,2016.

[3] Yogita Avinash Chaudhari, "A Probabilistic Black hole & gray hole attacks Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks-Review," International Journal of Innovative Research in Computer and Communication Engineering., 2017.

[4] Swati Verma,Bhawna Mallick, Poonam Verma , Impact of Gray Hole Attack in V ANET ,IEEE, 2015.

[5] Usha and Bose , Comparing The Impact Of Black Hole And Gray Hole Attacks In Mobile Adhoc Networks , Journal of Computer Science 2012, 8 (11), 1788-1802 ISSN 1549-3636 © 2012 Science Publications .

[6] Dilendra Shukla ,AkashVaibhav, Sanjoy Das, Prashant Johri, Security and attack analysis for Vehicular Ad hoc Network- A Survey ,International Conference on Computing, Communication and Automation,2016

[7] Manjyot Saini,Harjit Singh,"VANET, its Characteristics, Attacks and Routing Techniques: A Survey", International Journal of Science and Research (IJSR),2015.

[8] https://en.wikipedia.org/wiki/Wireless_ad_hoc_network

https://www.google.co.in/search?q=difference+between+wanet+and+vanet&dcr=0&source=lnms&tbm=isch&sa=X&ved=0ahUKEwimmqnfuc3XAhVFL48KHRTKCiUQ_AUICigB&biw=1252&bih=604#imgrc=bxsiTol1I8Hm4M