# Abstract: (plagiarism found 8%)

In the advanced and modern world, technologies are used to increase the power of the world. Internet plays an important and vital role in our lives.VANET comes from MANET in which different mobile networks connected through an Ad-hoc network .VANET is recent as one of the most appealing topics for researchers due to their mega possibilities to improve traffic safety. VANET is not rely on sate communication therefore it is a difficult task for the researchers and scientist to slove this. But there are many qualities like the wireless connection between vehicles , active connection and many more. Many Researchers has recently found an issue of security thus to provide the secure network for individuals.VANET provide safe and non-safe applications in a wireless medium which makes it unprotected to several attacks. In this paper, we will describe about the deep study of VANET attacks and how we prevent with these attacks.

# Keywords:

VANET, Security, Attacks, Possible Solutions

# Possible Classes of Attacks:

In VANET. The attackers wish to make a mess and bad impact on the network. The mission of the attackers is to create a maximum number of problems for all other nodes in the network launching differing kinds of attacks.

In 2013, Irshad Ahmed Sumra proposed five different classes of attacks and every class is expected to provide better perspectives for the VANETs security [paper1].

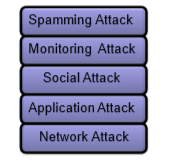


Fig.[classication] Possible Classes of Attacks

# First Class: Network Attack: (plagiarism free 0.0)

In this category, the attackers will directly target the nodes (vehicles) and as well as a roadside unit (RSU). The attack on this class is very high as a result of it affects the whole communication network and creates problems for vehicles.

# Second Class: Application Attack:

In this category, the goal of the attackers are applications that provide added service in VANET [paper1].The attacker wishes to change the contents used in the application and misuse it for their own interest.

# Third Class: Social Attack: (plagiarism free 0.0)

In this category. All the bad, wrongful, unethical messages are used in this class. The Attacker objective is to sending this kind of message in a network to create mess and problems for the other user in the network. Real user of the network would become angry when he gets these kinds of messages. This is what the attacker wants a change from a good behavior of the users to convert it into a negative or bad behavior and the goal of the attacker is achieved. For example, attacker sending you such kind of messages “I love you” or “You are a dog” to other real or authentic user.

# Fourth Class: Monitoring Attack: (plagiarism free 0.0)

In this category. The goal of the attacker is monitoring and tracking of vehicles in the network. In the Monitoring attack. The attacker just monitors the whole network, listening to the communication between V2V (vehicle to vehicle) and V2R (vehicle to road-side units) [classification]. For example, CIA and police have plans to do the operation against the terrorist group in somewhere. So once they communicate with each other using a network the attackers know everything about them so they provide that information to a terrorist group which creates a problem for the region as well as the country.

Fifth Class: Timing Attack: (plagiarism found 20%)

In this category. The goal of the attacker is to add some time slot in the original message. For example, to create delays in order to block this message comes to the receiver before the expiration of its lifetime [paper1]

# Miscellaneous threats:

## Man in the middle attack: (plagiarism free 0.0)

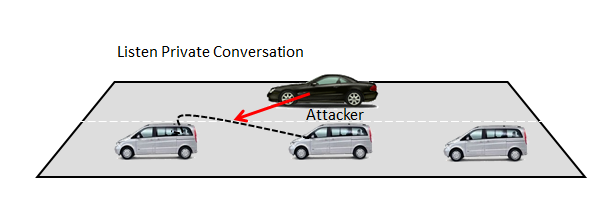
In this attack, the attacker sits in the middle of the communication between sender and receiver and start this attack. In this kind of attack, the attacker controls all the communication between sender and recipient. But the real user of the network feels that they are directly communicating with each other. But on the other hand, attacker listen to all the communication and modify all the sender and recipient messages and then again send those message on the network.

## Social attack: (plagiarism free 0.0)

In this category. All the bad, wrongful, unethical messages are used in this class. The Attacker goal by sending the message in a network to generate mess and problem for the other authenic user in the network. Real user of the network would become angry when he gets these kinds of messages. This is what the attacker wants a change from a good behavior of the users to convert it into a negative or bad behavior and the goal of the attacker is achieved. For example, attacker sending you such kind of messages “I love you” or “You are a dog” to other real or authentic user.

# Man in the middle attack soultion:

The best solution to prevent with this attack is confidential communication by using strong encryption and a secure authentication by hash functions to avoid he message fabrication and modification.

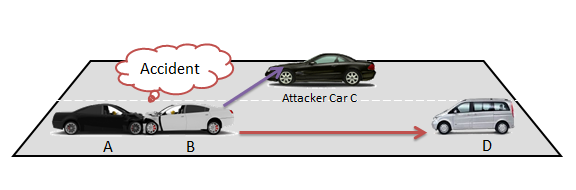


# In timing attacks:

In the time attack when the attacker receive a message from the other vehicles. The attacker don’t forward that message to the other vehicle .The attacker insert some time patches in the genuine message to create delay. Hence the nearby vehicle of the attacker gather the message after some time when that message is useless for that vehicle.

For example

Suppose there was an accident between 2 vehicles A and B. The Attacker car C was notify about this event but that attacker car C add some time patch to original message to create delay. D car should receive this message soon that to change line but because of delay. It only received the message about accident when it has already reached accident position.



The best solution to prevent with time attack is data verification and this verification is involved the elimination of timeslots from packets. TPM (Trusted Platform Module) has two main advantages.

1. TPM is using encrypted methods to provide security and authentication of message.
2. By using TPM we can protect hardware with cipher abilities and secure our data in secure location