T.C.
ALTINBAS UNIVERSITY
Graduate School of Science and Engineering
Electrical and Computer Engineering

# SECURITY OF VEHICLES PLATOON FROM INSIDE AND OUTSIDE ATTACKS

Mohammed Ismail Al_sheikhly

Master Thesis

Supervisor
Asst. Prof. Dr. Sefer Kurnaz

Istanbul, 2020

# SECURITY OF VEHICLES PLATOON FROM INSIDE AND OUTSIDE ATTACKS

by

**Mohammed Ismail Al_sheikhly**

Electrical and Computer Engineering

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2020

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Asst. Prof. Dr. Sefer KURNAZ

Supervisor

Examining Committee Members

| | | |
|---|---|---|
| Asst. Prof. Dr. Sefer KURNAZ | School of Engineering and Natural Sciences, Altinbas University | _____ |
| Prof. Dr. Osman Nuri UCAN | School of Engineering and Natural Sciences, Altinbas University | _____ |
| Prof. Dr. Mesut RAZBONYALI | Faculty of Engineering and Natural Sciences, Maltepe University | _____ |

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Asst. Prof. Dr. Cagatay AYDIN

Head of Department

Approval Date of Graduate School of Science and Engineering: 14/02/2020

_____

Prof. Dr. Oguz BAYAT

Director

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Mohammed Ismail Al_sheikhly

# ABSTRACT

## SECURITY OF VEHICLES PLATOON FROM INSIDE AND OUTSIDE ATTACKS

Mohammed Ismail Al_sheikhly

M.Sc. Electrical and Computer Engineering Altınbaş University,

Supervisor: Asst. Prof. Dr. Sefer Kurnaz

Date: 02/2020

Pages: 64

Vehicular Ad-hoc Network (VANET) is considered one of the most important networks that improves the efficiency and safety of roads and transportation. Recently, platooning which are subset of VANET become very promising as vehicles can know the intentions of nearby vehicles through V2V communication. Vehicle platoon consist of platoon leader who responsible of all operations inside the platoon and two or more vehicles how follow that leader, these vehicles behaving as a single unit via the coordination of movement. However, VANET face some challenges regarding its security, as there have been many forms of attack against this type of network. In this study, two different approach are discussed which are outside and inside attacks. First approach is outside attack, in which, multiple forms of outside attacks are investigated. These attacks include different scenarios with their classification and organization through smart simulations such as delay, change or prevent message from the Platoon leader to the rest of the platoon members or impersonation of the Platoon itself. This study proposes some appropriate solutions to solve these problems using some of the algorithms used in information security such as (MAC and Hashing) algorithms. The results of the smart simulation show the capability of

these techniques to overcome the attacks and secure the platoon. The investigation also shows that the most serious attack is sybil attack followed by the DOS then comes in the last rank in terms of direct risk is delay attack. In our knowledge this smart simulation never used to investigate vehicles platoon attacks. Regarding the second approach, an advanced terminal attack controller is designed and developed to efficiently detect and recognize the inside attacks that affect vehicles and also specify position of the vehicle which is creating that sort of attack in the platoon. Four type of attacks are implemented i.e. dos attack, botnet attack, ad-hoc attack and drive-by attack for this particular problem of platooning. As a result, the designed system is able to detect and identify the type of the attack as well as the position of the malicious actor in the platoon. After the detection process is finished, the platoon leader will eliminate the threat and re-arranging the platoon members.

**Keywords:** V2V, V2I, Inside attack, Outside attack, DoS, Sybil, Delay, Botnet, Ad-hoc, Drive-by, VANET, Platoon, MAC, Hashing.

# TABLE OF CONTENTS

**Pages**

# LIST OF FIGURES

**Pages**

# LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| VANET | : | Vehicular Ad-hoc network |
| V2V | : | Vehicle to Vehicle Communication |
| V2I | : | Vehicle to Infrastructure Communication |
| VLC | : | Visible Light Communication |
| MMWAVE | : | Millimeter Wave |
| MAC | : | Message Authentication Code |
| NHTSA | : | National Highway Traffic Safety Administration |
| ACC | : | Adaptive Crouse Control |
| CACC | : | Comparative Adaptive Crouse Control |
| LIDER | : | Light Detection and Ranging |
| GPS | : | Global Positioning System |
| MANET | : | Mobile Ad-hoc Network |
| DOS | : | Denial of Service Attack |
| ITS | : | Intelligent Transportation System |
| DDOS | : | Distributed Denial of Service Attack |
| PKI | : | Public key Infrastructure |
| DOA | : | Direction of Arrival |
| AES | : | Advanced Encryption Standard |
| DES | : | Data Encryption Standard |

IRC : Internet Relay Chat

P2P : Peer to Peer

OT : Operational Technology

IT : Information Technology

# LIST OF SYMBOLS

M : Original Message

P : Padding Number

$\oplus$ : XOR Operation

E : Encryption Algorithm

Ks : Symmetric Keys

C : Cipher Code

d : Distance Between Platoon Node

# 1. INTRODUCTION

## 1.1 BACKGROUND

With the exponential growth of wireless and wired networks and the Internet, this growth has developed tremendously and smartly in transport systems, and vehicle networks have become a very important subject in research and occupy researchers [1]. This modern network consists of a platoon with one leader and many followers and sends messages through radio communications. There are two types of communication in the platoon, the first communication is between the platoon members and known as vehicle to vehicle communication (V2V) and the second one between the platoon leader or free vehicle that not belonging to any platoon and the infrastructure known as vehicles and infrastructure (V2I), meaning that there are internal and external communications in the platoon [14].

Vehicular system considered one of the most important research topics in the present time. Autonomous vehicles are rising technology where efficient transportation and safety will be provides among other things. Each year millions of people die due to traffic accident caused by human error, to handle this issue intelligent transportation system (ITS) proposed automated vehicles as a solution to improve safety and maximize the efficiency.

National Highway Traffic Safety Administration (NHTSA) classified the automated vehicles into four levels where the first level is (no-automation) and the last one is (full automation). Autonomous vehicles depend on the communication system (V2V and V2I) to share different information among vehicles through wireless communication. Vehicle-to-everything (V2X) which refer to V2V and V2I has been investigate in the recent years to support vehicular system applications such as (blind spot, Adaptive Cruise Control (ACC) and parking assistance) etc.

The technology that will be used in this system aims to secure the communication between (V2V and V2I) and maintain the stability of the platoon, but most of the technologies now does not meet these demands, for that visible light communication (VLC) will be used to achieve these demands. With the increasing of traffic data, traditional technologies show their weakness for supporting high data rate that will be required for the vehicular applications such as Light Detection and Ranging (LIDARs), cameras, Global Positioning System (GPS) and many other due to limited bandwidth. visible light communication is a valid solution due to the high

security, more bandwidth and much higher data rate that this technology provide [7]. Therefore, autonomous vehicles can immediately determine the optimal driving strategy. Platoon is a sub-network of VANET, where a group of vehicles follow each other and have same speed, destination and inter vehicle distance, the communication between these vehicles happen in wireless manner [1]. Previously Adaptive Cruise Control (ACC) used to have constant speed only, but the new version which known as Cooperative Adaptive Cruise Control (CACC) keep a safe distance between vehicles and allow them to communicate with each other, in addition to the sensors that equipped these days in vehicles to achieved semi-autonomous one. light detection and ranging (LiDAR) are one of the most used sensors in vehicles that able to scans more than 70 m in all directions and provide 3D map of surroundings [2].

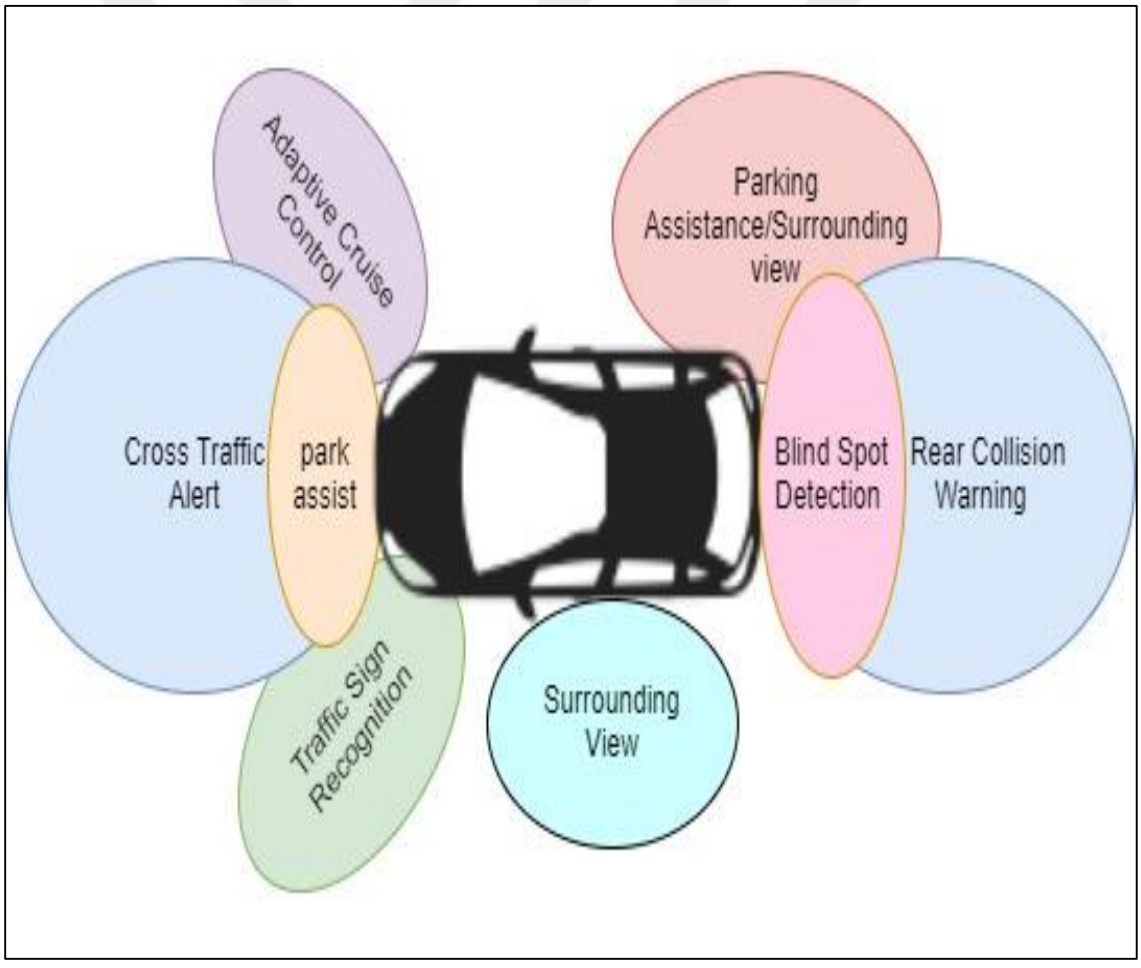


**Figure 1.1:** Automatous Vehicle Sensors.

VANET networks are scalable networks and independent and consist of a large number of nodes and multiple commanding groups. Each platoon is made up of a number of cars that are not specific and have high traffic and automatically follow their leader and communicate with each and with infrastructure via (V2V and V2I).

Networks that dedicated to vehicles utilize to solve many important problems and have many advantages such as solving traffic congestion, locating accidents, locating faults, ease of movement and safety of drivers. But to rely on these networks and make the most of their services, we need to make sure that the network is free of all forms of attacks [3][4]. Figure 1.2 shows a typical VANET scenarios, here the communication between vehicles and also between vehicles and infrastructure happen in wireless manner to share sensitive information that maintain the stability of the platoon.

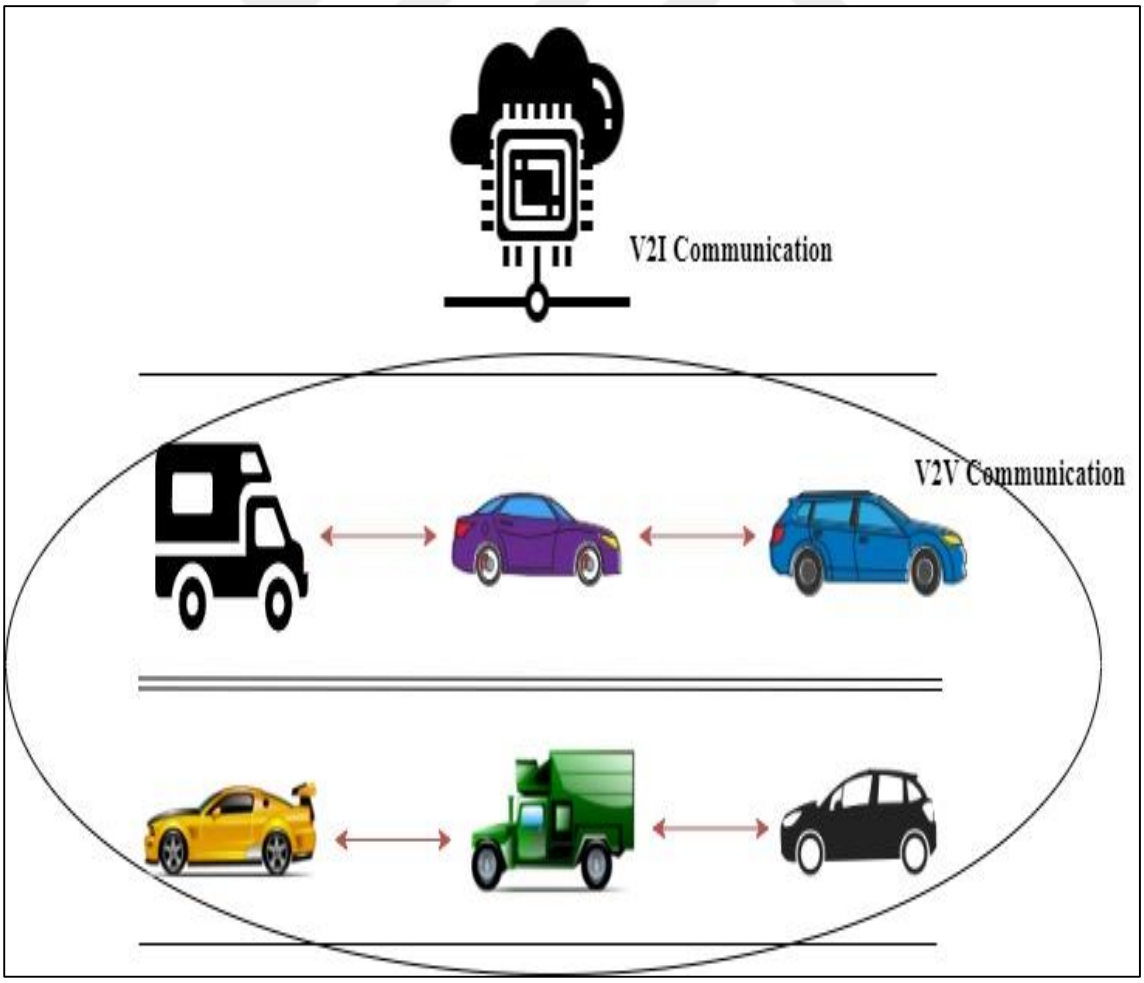


**Figure 1.2:** Different VANET Connections.

Recently, platooning or CACC become very promising as vehicles can know the intentions of nearby vehicle through V2V communication and advanced on-board technology. Vehicle platoon is one of the innovations in the automotive industry with a main goal of securing the platoon communication to preform maneuver operation under various type of security attacks that maintain the stability of the platoon. Platoon will provide many advantages such as improve the safety, efficiency, travel time of vehicles, reduced traffic congestion, reduce pollution and reduce stress form passengers. In vehicular system the platoon leader is the first vehicle in the platoon which are responsible of all the operation of the platoon from (merge, split, leave, join) etc. Vehicles of the platoon share sensitive information such as speed, acceleration and position, etc. and to send these information from one vehicle to another vehicle-to-vehicle communication technology will be used such as VLC, MmWave and IEEE802.11p. VLC transceiver will use LED as a transmitter and CMOS camera or photo diode as a receiver which is commonly used these days in vehicles due to the long service time life [23], for that VLC technology have higher probability for using in vehicle to vehicle communications to share different information such as speed, acceleration, position etc. VLC also provides more bandwidth, higher data rate and more security due to the directionality of it. Vehicle platoon consist of platoon leader and two or more vehicles how follow that leader, the platoon leader responsible of all the operation inside the platoon. The speed of the platoon leader will be constant, and the followers will modify their speed to catch up the leader and keep safe distance between two consecutive vehicles. Security is the most important issue that facing self-driving, these security threats can be from inside or outside the platoon, but the inside attacks consider the most dangerous one where the malicious actor will send an authenticate message with intention of destroying the platoon stability. Figure 1.3 describe the formation of the platoon and the attacker, where the platoon as demonstrate will consist of the leader which is the first vehicle in the platoon, a members vehicles which are vehicles who follow the leader, tail vehicle which is the last vehicle in the platoon, in addition to the attacker\malicious actor.

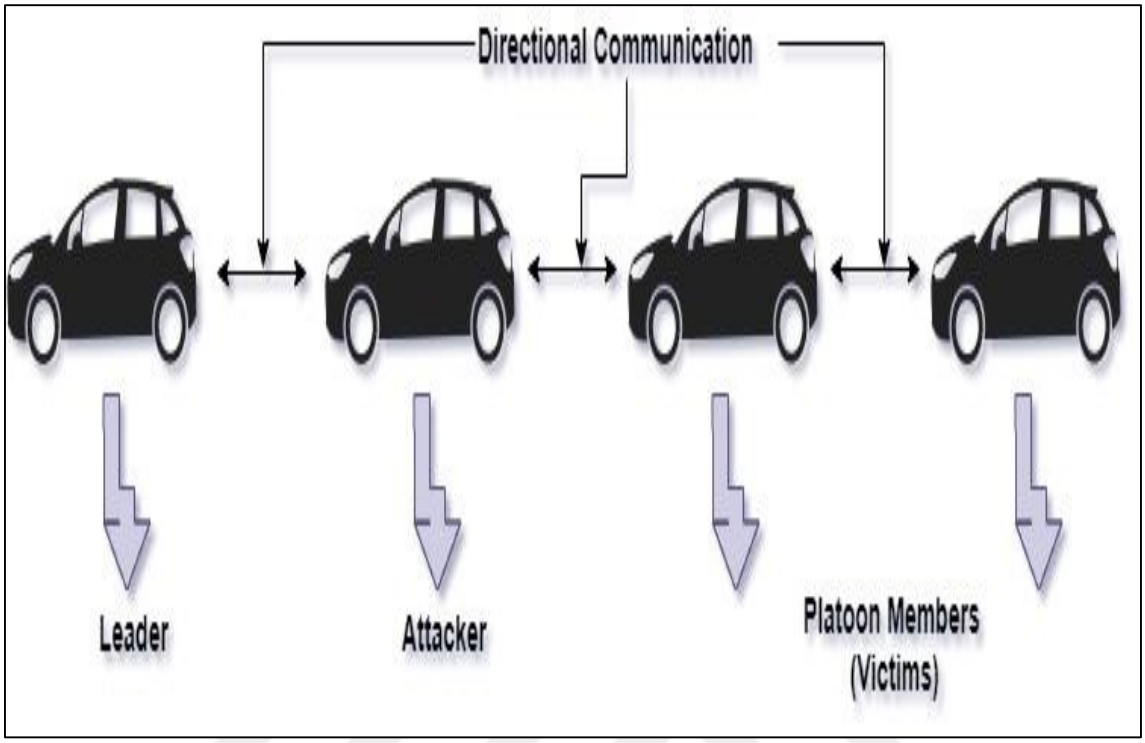


**Figure 1.3:** Vehicles Platoon.

Since there are two types of attacks (outside and inside) attacks. Our study will be divided into two aspect. The first aspect, we will investigate the attacks from outside the platoon and showing its effects using a smart simulation (php). In our knowledge that smart simulator (php) never used before to demonstrate the effects of platoon attacks. The second aspect, focusses on detecting the inside attack that can destroy the concept of vehicular system (autonomous vehicles) and secure the platoon from these attacks by eliminating the threats using C++. The reason behind using C++ language that's it works on very low level and has good interactivity with the simulated files that specify the attacks type.

## 1.2 RELATED WORK

MANET is super class of VANET, which nodes are recognized as vehicles, and it has various characteristics that are distinctive from MANETs, such as scalability, vehicles' movement, and dynamic topologies.

Platoon will bring many advantages to autonomous vehicles, where traffic congestion will be decreased and also pollution will be reduced. To ensure the stability of the platoon V2V are essential part in it, but the existing one such as IEEE 802.11p suffer from many drawbacks like security problem, these security problem have the ability to destroy the self-driving technology for that reason the security of autonomous vehicle is one of the hot research topic right now.

Vehicular protocol was investigated in the previous studies [12]. by considering the communication among vehicles is secured [11][12]. Nevertheless, the security attacks impact on the platoon and the stability of the membership was not taken in these protocols.

The absence of security protocol was investigated in recent studies and how this absence causes instability in the platoon under jamming attacks and message falsification attack [16][17]. Radio RF technology and IEEE802.11p was integrate in the platoon system. IEEE802.11p is the standard for WAVE. Although, the high transmission of IEEE802.11p provides access to many vehicles at the same time. the wide rang make it vulnerable to interrupting or even in worst case block the communication. Security infrastructure and architectures have been investigated [18] [19].

V2V is the core of autonomous vehicles, mainly in platoon configurations. The wide coverage area of the wireless technology for example IEEE 802.11p make it vulnerable to various attacks and for its latency [40].

Standard security protocols are introduced in [20]. One of the most used infrastructures in VANET is public Key Infrastructure (PKI). PKI supports the identification and distribution of general encryption keys that allow vehicles to share sensitive information safety and check other vehicles identity.

Last decade the industrial spend billions of dollars to achieve self-driving. Autonomous vehicle will be applied in smart city where everything will be connected to the internet for more reliability and to prevent human errors that cost millions of lives each year. To overcome these problem VLC will utilized in vehicles for V2V communication due to the security that this technology provides and also for high data rate [8][9].

VLC is a new technology that can overcome these attacks. problem of collaborative driving for vehicles platoon in the existence of message falsification vulnerability and communication weakness on wireless vehicular networks is investigated [10].

To secure the communication between vehicles new technology called VLC was proposed, to carry the digital information in wireless manner it will use modify light radiation in the visible light spectrum. VLC transceiver use LED to send the information and CMOS or diode image for the receiver. Improving safety performance and its long service, LED become common in automotive lighting. Similarly, many vehicles use CMOS for tracking purposes and parking assist. Previous studies have focused on VLC vehicle connections on derivation of channel characteristics [21], requirements [22][23], advanced modification schemes [7][11]. Few studies focus only on VLC security, but for non-vehicle scenarios [20].

Other studies focus on making independent vehicles more reliable and support decision-making by referring to the confidence system while integrating the maneuver scenario into the platoon. Vehicles that want to join the platoon and the relationship between platoon members have been described in the case of priority and speed adjustment but not in the security situation [15].

VANETs purpose of improving the protection of the highways, stopping collisions, supporting the passengers and help cars to interact with other vehicles [24].

In [27] it produces a complete taxonomy of threats in VANET. Several threats are categorized based on various circumstances, e.g. standardize, appearance, influence upon the system etc. Potential countermeasures and remedies suggested for various class of interventions are also considered to evaluate their effectiveness.

In [28] they formed system connection among vehicles and provided securable connection between cars and block several threats.

In MANET there are distinctive kind of network called VANET that allow vehicles to communicate with each other. One of the attacks that facing this network is DoS attack. This study proposed solution for this attack which adds security level to the previous solutions based on rate decreasing algorithm and state transition mechanism [43].

In [25] develop a research paper utilized to identify the DOS (Denial-of-Service) assaults before the confirmation time to reduces the overhead delay and improves the protection in VANET. V2V and V2I security which known as V2X has been describe as a serious problem that can devastating road safety. A possible cyber-attack was investigated in [9] and one of the security threats in vehicular system is denial of service (DOS) [10].

Jamming attack is a kind of Denial of Service attack, which occupy the channel and prevent the nodes from using it. Eavesdropping is any attempt to steal information over the network, it’s also

known as a sniffing or snooping attack. In [13,14]. Jamming attack and eavesdroppers were investigated, the result shows attacks ability to destroy the stability of the platoon but for nondirectional communication.

In [26] A investigate the achievement of a Misconduct Detection System (MDS) for Sybil attacks. This paper recognizes that the review of this recommended design is not very susceptible to the specific dynamics of the vehicle on short scales.

Vehicular system was proposed to enhance transportation safety that caused millions of human lives each year. But, system like that require apt security architecture to protect the system from different attacks. Vehicular system facing many security threats and one of these threats is Sybil attack. Sybil attack produce multiple copies with identity belonging to other vehicles. This study shows that authentication methods are dependable and valuable in term of security requirements that include (privacy, authenticity and integrity). Unlike the position verification methods, which will be used to verify the position after receiving the location information which are transmitted by vehicles for applications regarding position [41].

Detection of Sybil attack was introduced by lightweight security scheme based on signal strength distribution. The proposed scheme in this study aim to hold the attack ability instead of removing or eliminate the attacker, by monitoring the signal strength distribution of the suspicious node over a period of time [42].

To provide different and sensitive information among vehicles, VANET consider critical for intelligent transportations. Man in the middle attack is kind of cyberattack where the malicious actor enters the network and start to change or send sensitive information to others attackers, which reduce the stability and compromises drivers privacy. [45]. In [44] investigates the impact of man in the middle attack which consider as an outsider in the system such as fleet or random strategies. the study Shows that MITM attack enormous impact on VANET in term of packet loss and expose messages.

VANET will reduce relying on costly sensors which make it easier for deployment for autonomous vehicles. In [46] investigate a possible botnet attack on vehicular system which can cause sever congestion by targeting hot spot road segments which increase the arrival time. Explain VANET-based botnet communication which hidden itself in the network by investigating the features of the communication that the attacker used to execute the attack and

implement defense mechanisms to deactivate it. The study showed that it's impossible to detect the attack due to present vulnerabilities in VANET [47].

The most popular ways to infect a group of users\vehicles is by Drive-by attack. Where the malicious actor will take full benefit of the internet functionality. This study shows that no big steps have been made for their successful detection and prevention, also shows that the effects of such an attack different based on the malware that will be send with the message without realizing it from the user\vehicle [48]. In [49] investigate the performance of black- or whitelisting techniques to detect Drive-by attack. This study shows that these techniques suffer from non-up-to-date security information.

This thesis aims to secure the platoon from inside attacks by detecting the attacks, identify its position then eliminate the threat vehicle and investigate multiple forms of outside attacks and propose a appropriate solution to overcome these attacks such as message authentication code and hashing algorithm.

## 1.3 CONTRIBUTIONS AND OBJECTIVES

The contribution of this thesis will focus on detecting and securing the platoon from inside attacks, investigate multiple forms of outside attacks, showing a taxonomic study of the forms and types of attacks that pose a security challenge for this type of wireless network and showing some background about vehicular system.

In this study, two different approach are discussed which are outside and inside attacks. First approach is outside attack, in which, multiple forms of outside attacks are investigated. These attacks include different scenarios with their classification and organization through smart simulations such as delay, change or prevent message from the Platoon leader to the rest of the platoon members or impersonation of the Platoon itself. This study proposes some appropriate solutions to solve these problems using some of the algorithms used in information security such as (MAC and Hashing) algorithms and showing the results through smart simulation that used to test and to promote the proposal. In our knowledge this smart simulation never used to investigate vehicles platoon attacks.

Regarding the second approach, an advanced terminal attack controller is designed and developed to efficiently detect and recognize the inside attacks that affect vehicles and also

specify position of the vehicle which is creating that sort of attack in the platoon. Four type of attacks are implemented i.e. dos attack, botnet attack, ad-hoc attack and drive-by attack for this particular problem of platooning. As a result, the designed system is able to detect and identify the type of the attack as well as the position of the malicious actor in the platoon. After the detection process is finished, the platoon leader will eliminate the threat and re-arranging the platoon members.

## 1.4 THESIS STRUCTURE

Chapter I start with general introduction and background of vehicular system, platooning, security challenges and technologies that will utilized in that system, also present the related work and the aim of this thesis. The following chapters of thesis is prearranged as follows:

- Chapter II start with description of vehicular system communication and security with their classification and importance.
- Chapter III start with description of outside attacks and its types, including our system model in term of the platoon and the attacker. This chapter will also show the effect of each attack and the techniques that used to overcome these attacks in a smart simulation.
- Chapter IV start with definitions of inside attacks, then present our methodology and result that show our detection and how we secured the platoon from these threats.
- Chapter V present the conclusions of this thesis.
- Chapter VI Present our future work

# 2. VEHIVULAR SYSTEM COMMUNICATIONS

## 2.1 COMMUNICATION SYSTEM

Vehicular system relies on the communication technologies that will be utilized to share information such as V2V and V2I communication as shown in Figure 2.1. In the previous work many technologies was proposed as a solution for the communication of the vehicular system such as IEEE802.11P, but these technologies suffer from lack of security that make it vulnerable to the malicious actor unlike visible light communication (VLC) or millimeter wave (MmWave) that provide more security due to the directionality of it, in addition to the high speed data rate that these technologies provide to share these information from different sensors such as LiDAR that provide 3D map in all direction or HD video and many other. For a hybrid communication the VLC will be responsible of the V2V communication and MmWave will be responsible of V2I. By using visible light for V2V communication sensitive information will be shared among vehicles such as (speed, acceleration, position), while V2I will share road condition and traffic congestion etc.

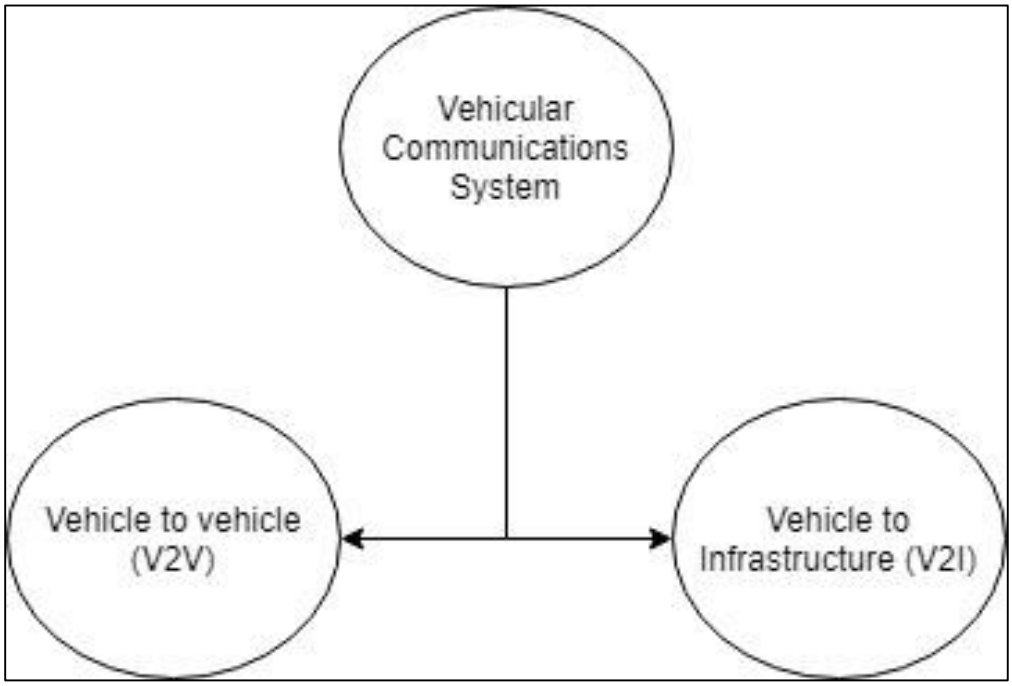


**Figure 2.1:** Vehicular System Communications.

### 2.1.1 Vehicle to Vehicle Communication

Vehicles will start to exchange data such as position, speed and direction of travel when they arrive to a connecting range. Real time of exchange sensory data (LiDAR or HD video) among vehicles will provide through the use of V2V communication that can also cover the blind area and share vision in bad weather. Each platoon consists of the platoon leader and many followers that follow the leader, the platoon leader will be responsible of (speed, acceleration, deceleration and platoon maneuvers) etc. On the other hand, due to the directionality of the VLC and the lack of access to light limits the reception of data in given area, usually within light coverage, making it difficult to intercept data from outside, this will restrict the availability of data to attackers while still allowing the communication among vehicles [4]. So, for secure communication the technology of VLC will be used in vehicles. In the case of VLC transceiver, the transmitter will use LED and for receiver it will use photo diode or CMOS camera, due to the long service life in diode it's become more and more common in vehicles. But on another hand, the malicious actors will still able to destroy the stability of the platoon by overhearing or hacking the channel communication. So, in that case we need to establish a secret key in asymmetric cryptography, sender and receiver agree on a secret key by using a key establishment protocol, for that public key infrastructure will be used to establish the secret key.

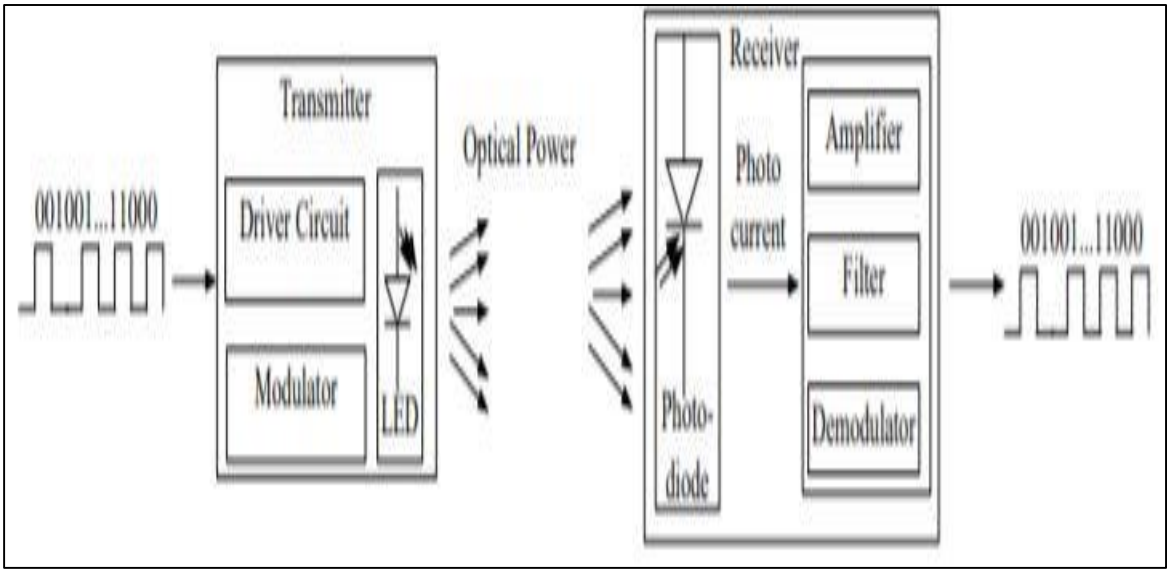


**Figure 2.2:** Visible Light Communication Architecture [2].

#### 2.1.1.1 Public Key Infrastructure (PKI)

PKI is a framework where services integration will be related to cryptography. PKI provide (access control, integrity, confidentiality and authentication). To enable both users and computer to exchange data securely over the network PKI support the distribution of public key. The component of PKI are software, hardware, policies and standards to manage revocation of keys, distribution, administration and digital certification. Four issue addressed before the transmission can occur:

1- Ensuring the confidential of the message.

2-Ensuring that during the transmission the message did not modify.

3- Since the sender and receiver do not know each other the sender have to prove that the document is in fact send by him.

4- Ensuring that the receiver get the message and could not deny it in the future.

### 2.1.2 Vehicle to Infrastructure Communication

When vehicles connect with road infrastructure it will provide the vehicles with sensitive information such as nearby traffic condition and weather condition etc. For instance, When an accident occurs at a distance far from the platoon and there are no possibility for V2V communication the infrastructure will be responsible to inform the platoon that there is an accident and the speed should be reduced to avoid it or to inform the platoon about the best way to reach the destination as well as the safety that this technology provides due to its directionality make it very essential for vehicular system, where beam-forming and smart antenna technologies will be used to concentrate the beam in one direction and have more than one beam simultaneously.

#### 2.1.2.1 Beamforming

Beamforming is a signal processing technique that focus the transmitter energy into a specific direction and reduce the interference. The time delay among different antennas will control the

direct of the beam, so more antenna means narrower beam. By using the antenna array, we can generate multiple link simultaneously and its direction will change fast enough to catch the vehicles speed and the beam forming can be realized in both digital or analog domain [4]. Digital beam forming includes a higher degree of freedom and better transmission performance. Analog beam forming is a simple and effective method that generate high beam forming gain by controlling phase-shift and variable gain amplifier. So, a hybrid structure of analog and digital beam forming will be used in the vehicular system to quickly track high speed vehicles and provide multiple beam if one infrastructure needs to connect multiple vehicle simultaneously.

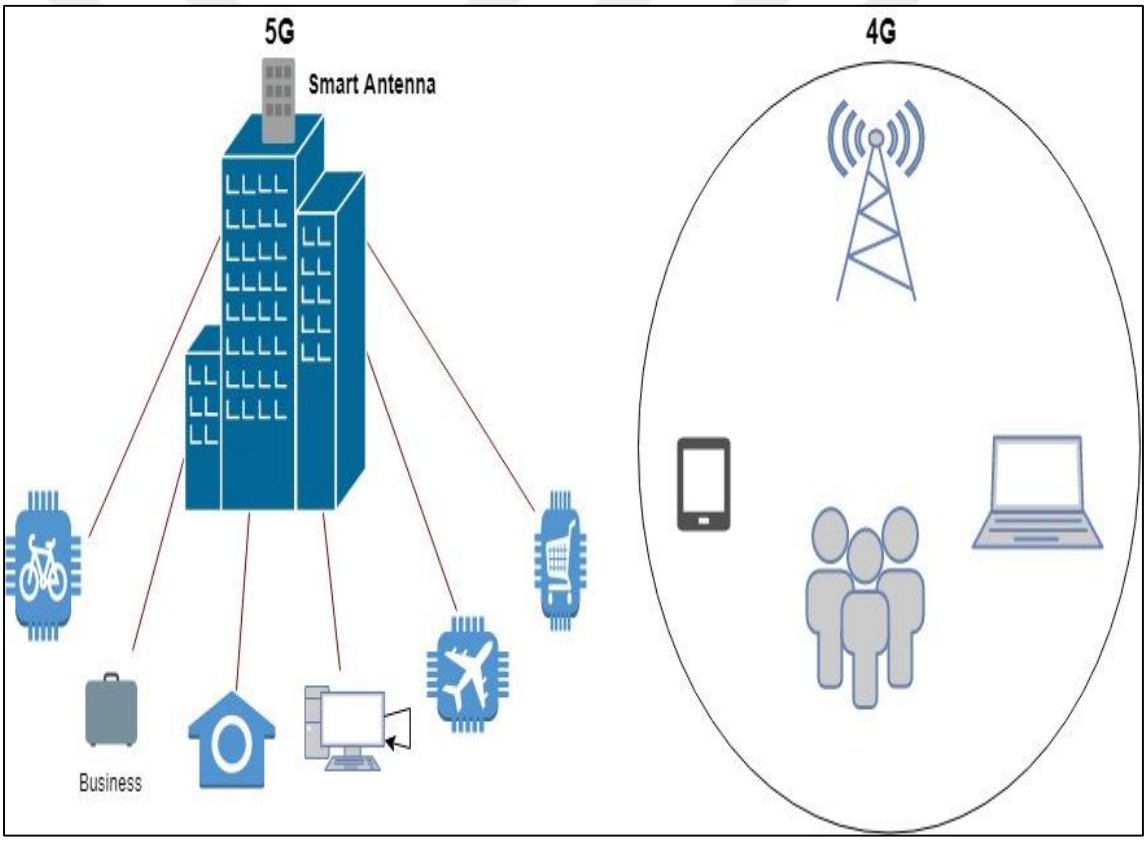


**Figure 2.3:** Beamforming Technology.

### 2.1.2.2 Smart antenna

To increase the efficiency smart antenna will be used in the communication system. Smart antenna takes advantage of transmitter and receiver diversity (source and destination) in wireless

system [4]. Diversity mean multiple radio frequencies of the transmission and reception will used to reduce the communication error and increase the speed of transmission. In most wireless systems this type of technology has already been found to be important, where signal processing algorithms will used with antenna array to identify and track different wireless targets such as mobile. It is also used to calculate the vectors of the beam configuration and the direction of arrival [DOA] of the signal.

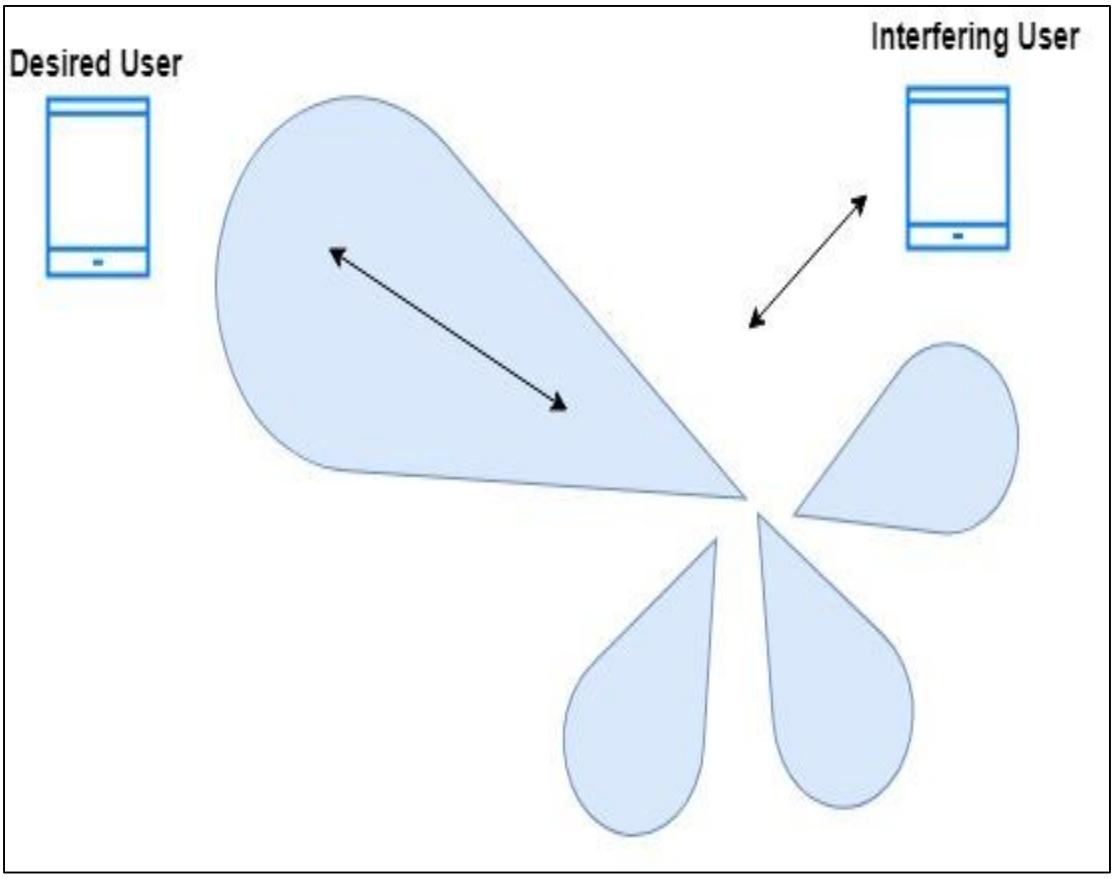


**Figure 2.4:** Smart Antenna Technology.

## 2.3 VANET ATTACKS

Currently, there are many types of attacks that pose a threat to any type of network, especially wireless networks. VANET networks need a lot of security services to protect the messages sent and the data exchanged from the leader to the followers and vis versa [35]. The various security requirements include:

- Availability: One of the most important security points that must be available is the availability of messages continuously from the commander to the rest of the platoon and not cut. Here it is possible for the attacker to penetrate the network and attack on one target from more than one point to prevent the server from temporarily or permanently.
- Confidentiality: One of the important points is to maintain the confidentiality of data and the details of messages sent by the commander to the rest of the platoon.
- Integrity: The most important point at all because its loss causes great damage. Here the recipients should make sure that the messages are correct and from the correct source.

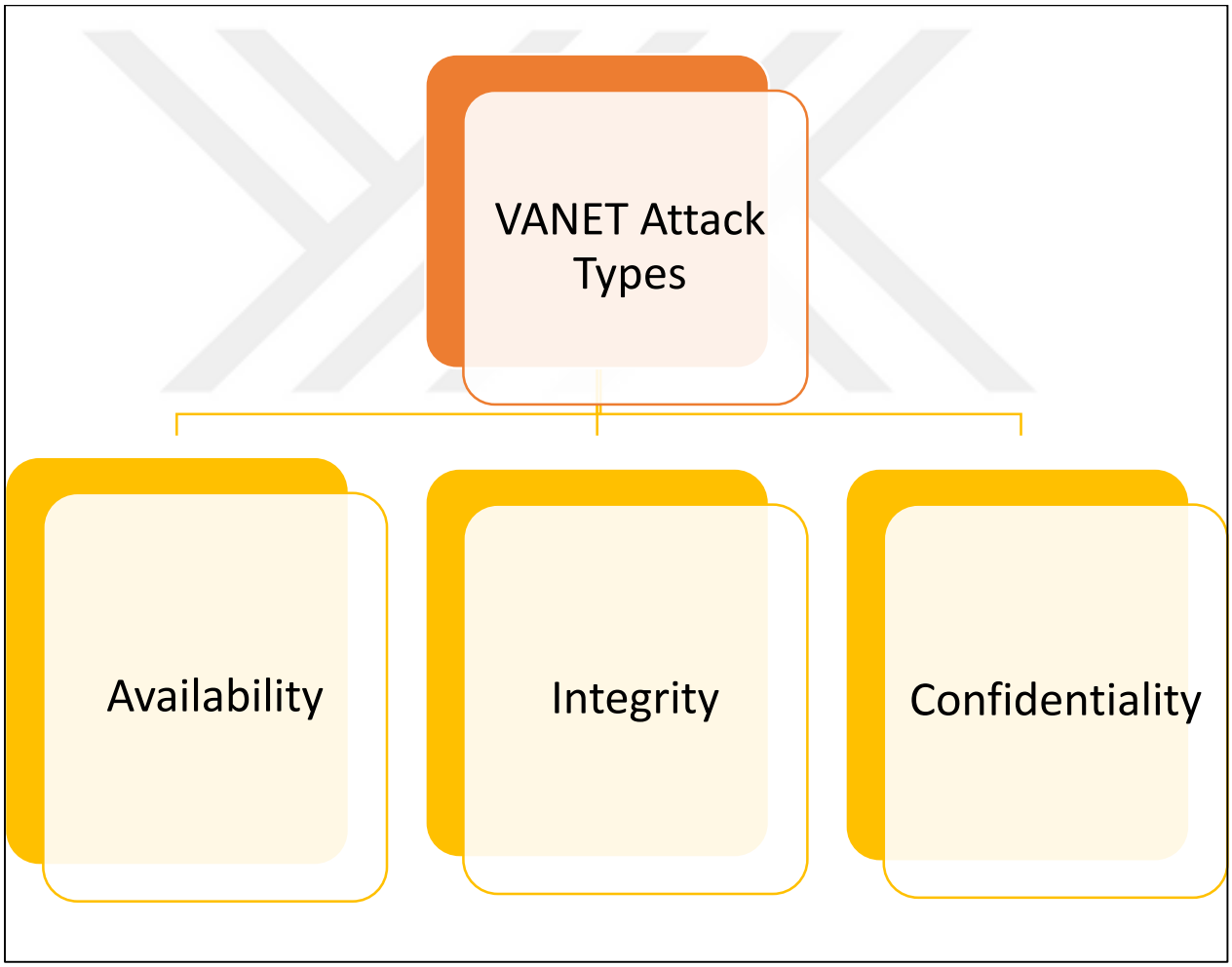


**Figure 2.5:** Types of Attacks in VANET.

In order to achieve the goal, a secure network must first identify the types of attackers and their ability and the nature of what they do attacks to disrupt the network and penetration [35]. Attackers are therefore classified into two main categories:

- First, we can classify attackers in terms of activity (an active attacker or a passive attacker) so that an active attacker can destroy the network or block messages, that is to say, it does damage and damage. A passive attacker can play a role in intercepting others or stealing data without destroying it, ie, it does not cause inconvenience or harm, but only stands for observation.
- Second, we can classify the attackers in terms of attack direction (inside or outside the attacking squad) so that the internal striker is considered more dangerous than the outside because he is considered one of the squad and knows more details being inside the squad and his discovery is more difficult than the striker who comes from abroad.

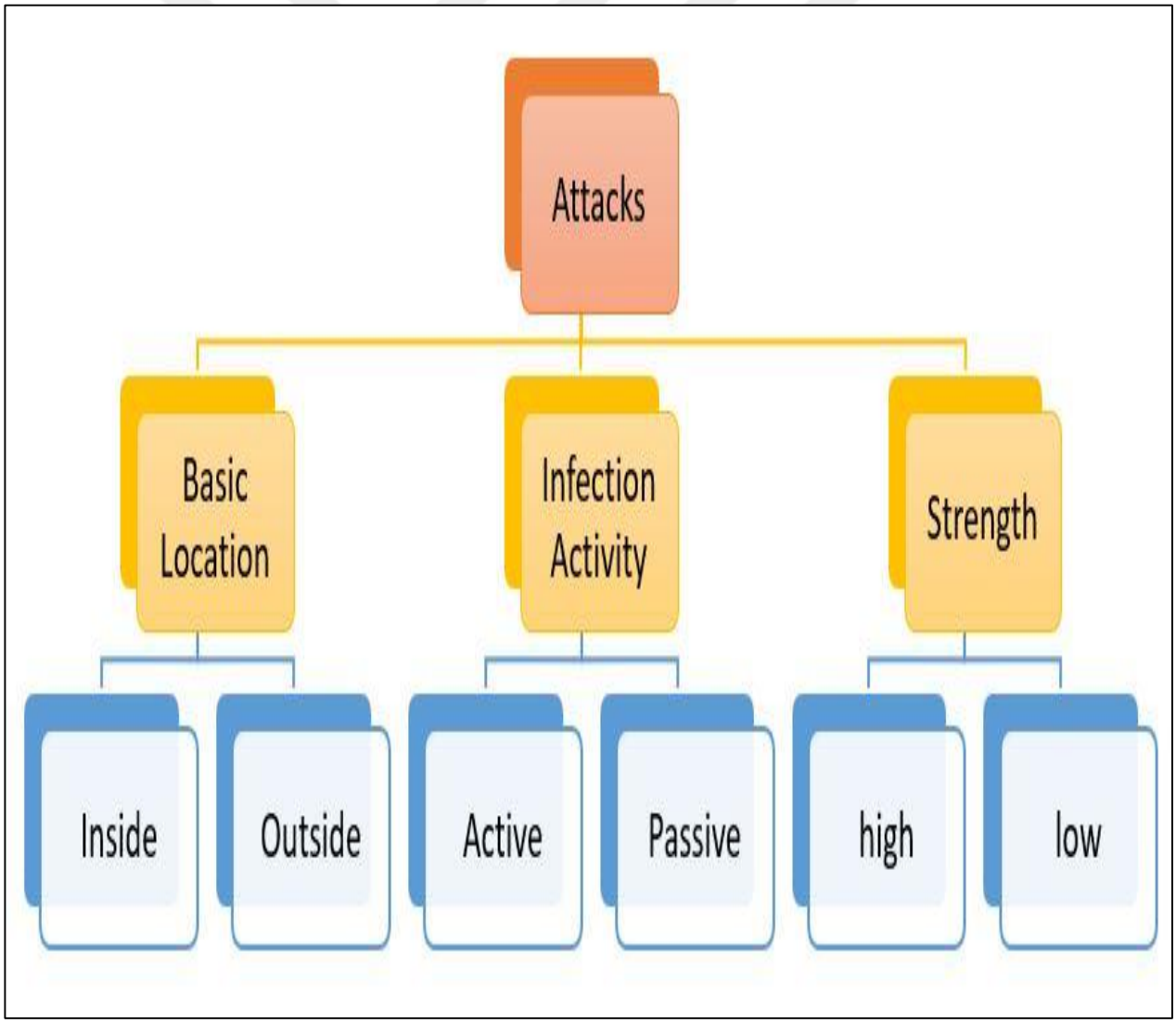


**Figure 2.6:** Categories of Attacks in VANET.

# 3. OUTSIDE ATTACK

## 3.1 FOCUS OF THIS CHAPTER

In this chapter we will talk about attacks from outside the platoon, where the malicious actor will not consider a part of the platoon members but as a vehicle near the platoon. We will also investigate the attacks effects and how these encryption techniques will be able to overcome these attacks. in this approach there will be no detection only investigating the effects and show the experimental result of how these techniques will overcome these attacks.

## 3.2 TYPES OF OUTSIDE ATTACK

The following list will describe different types of outside attacks that can affect the vehicular system.

### 3.2.1 Sybil Attack

Vehicular system was proposed to enhance transportation safety that caused millions of human lives each year. But, system like that require apt security architecture to protect the system from different attacks. Vehicular system facing many security threats and one of these threats is Sybil attack. Sybil attack produce multiple copies with identity belonging to other vehicles

In this type of attack, the attacking entity launches false messages disguised as the Platoon or sink of the team and its purpose is to collect the greatest number of faction or group nodes. This type of attack is considered very harmful because it sends a fake message and directly affects the network in favor of the attacker. The main motive is to force other vehicles on the road to leave the road in favor of the attacker. The scenario in Figure 3.1 explains the Sybil attack where multiple duplicate copies will be creates by attacker [30].

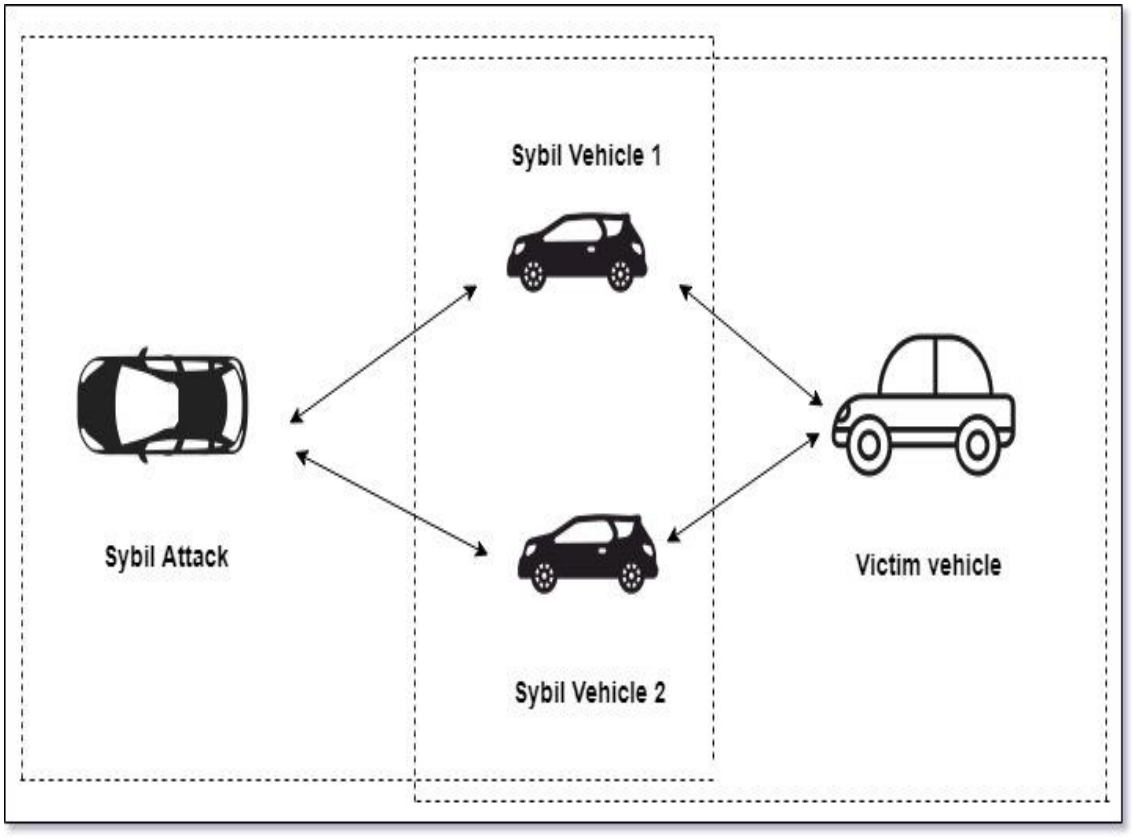


**Figure 3.1:** Sybil Attack.

### 3.2.2 Delay or Timing Attack

This type of attack is one of the famous types that can cause serious damage to this type of networks because of the high speeds and total dependence on timing and accuracy. In this type of attack depends on the attacker to add additional time slot for each message sent and delayed the delivery time for the confusion inside the network. Attackers do not disturb or fabricate the content of message, but they only create delay in the message time slot [3].

### 3.2.3 DoS attack

Denial of Service or "DoS" represent the primary goal of a class of cyberattacks designed to make the service inaccessible. prominent websites are the most DoS attack heard by people, where they are repeatedly announced by the media. However, including industrial control systems any attack support critical processes, can lead to denial of service. When a website

suffers from a DoS attack, the effect depends on your point of view. For the average user, the site seems to have simply stopped showing content. For companies, this may mean that the Internet systems on which they depend have stopped responding. The effect of a DoS attack against industrial control systems may involve the inability to recover sensor data or control critical processes. One of the DoS called DDoS attack where more than on site can be attacked and also can extend in the duration. So, when it's come not from one source but from different sources is the most generic form of DDoS. As the example of a shopping site indicates, the reason for denial of service can be entirely legitimate user. For instance, Black Friday sales, when Hundreds, even thousands of users seek a deal, often cause a denial of service. But it can also be harmful. In this case, an attacker intentionally tries to exhaust the resources of the site, preventing legitimate users from accessing. In other words, this type of attack is the most famous of the rest of the attacks because of the severe damage it causes as it intercepts the messages and prevents their arrival. This type depends on the attacker to block messages by cutting or jamming the transmitter and then separates the vehicle from the rest of the platoon as represented in Figure 3.2. This type of attack is classified as damaging sources and causing network failure and cannot be remedied by detecting the source of the attack through the authentication techniques [31].

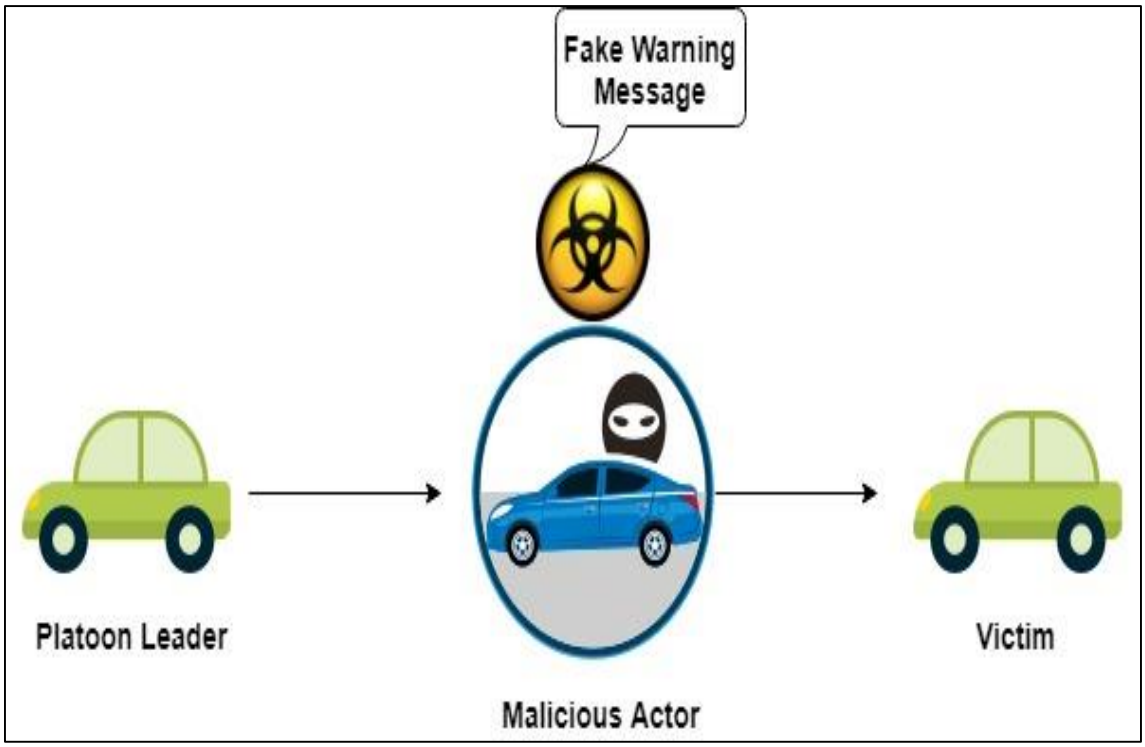


**Figure 3.2:** DoS Attack

### 3.3 SYSTEM MODEL

This part will present the steps of implementing a measurement system to measure the vulnerability of this type of network using different types of attacks. In this section we will present the scenario of the deal between the platoon and other cars in same faction, how the attacker intervened and influence the faction. Here are some basic steps:

- First, we will determine the number of vehicles that make up the work of the platoon, each of which has a number that distinguishes it and Platoon one as its leader sends her messages and follow him. The working environment should be 100 meters vertically and 100 meters horizontally.

- Secondly, we will need a technique to determine the nearest vehicle of the platoon within 20 meters to send the messages and therefore we will use the following equation, which aims to find the shortest distance between two points.

$$d_i = \sqrt{(x - x_i)^2 + (y - y_i)^2} \tag{3.1}$$

where d is distance between platoon node within the transmission range (R) of the car.

- Thirdly, the target goal is minimizing time and localization error. The objective function is formulated as:

$$f(x,y) = \min\left(\sum_{i=1}^{M}\left(\sqrt{(x - x_i)^2 + (y - y_i)^2}\right)^2\right) \tag{3.2}$$

where M is the cars node within the transmission range (R) of the platoon node.

- Fourthly, we will need a wireless connection to transmit messages between cars and use visual light technology with GSR routing protocol.

- Fifthly, we need a way to detect attacks through the following scenario. Then we need ways to treat whether the attacks have been detected.

## 3.4 RESULT OF OUTSIDE ATTACKS

In this section we will review many of the scenarios used in the practical application of smart simulation. There are two types of scenarios for each type of attack. The first type is a platoon that follows one leader and is predefined. The second type we will focuses on is that the platoon composed of many cars in different numbers with their commander and the attacker are randomly and automatically distributed to measure the accuracy of simulation in each position separately. The statistics of the attack are shown in red (effect of the attack, number of vehicle and the time its take). As well as statistical for the platoon and his followers in green and the number of cars belonging to him on the horizontal axis and timing on the vertical axis.

### 3.4.1 Sybil Attack

In this type of attack (Sybil Attack), as shown in the next Figure 3.3, the platoon consists of five vehicles in a random way with 20m range and 1 second for sending packet. Where the platoon sends a message to the nearest vehicle belonging to him and then move messages from one vehicle to another. In this experiment, the attacker came directly behind the platoon and thus completely prevent his arrival to the rest of the platoon members. The attackers attacked the first vehicle (below), which was 20 meters below, sent a message to the platoon and then proceeded with the rest of the squad vehicles. The result show that the attacker will take control over the platoon after 9 seconds and the platoon leader will not be responsible of any vehicle.

### 3.4.2 Delay Attack

In this type of attack (Delay Attack), as shown in Figure 3.4, the platoon consists of five vehicles in a random way with 20m range and 1 second for sending packet. Where the platoon sends a

message to the nearest vehicle belonging to him and then move messages to the rest of the platoon members. It was found in this experiment that the attack affected 3 vehicles, but the platoon leader still followed by these vehicles. The statistics of the attack are shown in red as well as statistical for the platoon and his followers in green and the number of vehicles belonging to him. The result shows that the first vehicle will receive the message after 2 second instead of one and the last vehicle in the platoon will received it after 5 seconds.

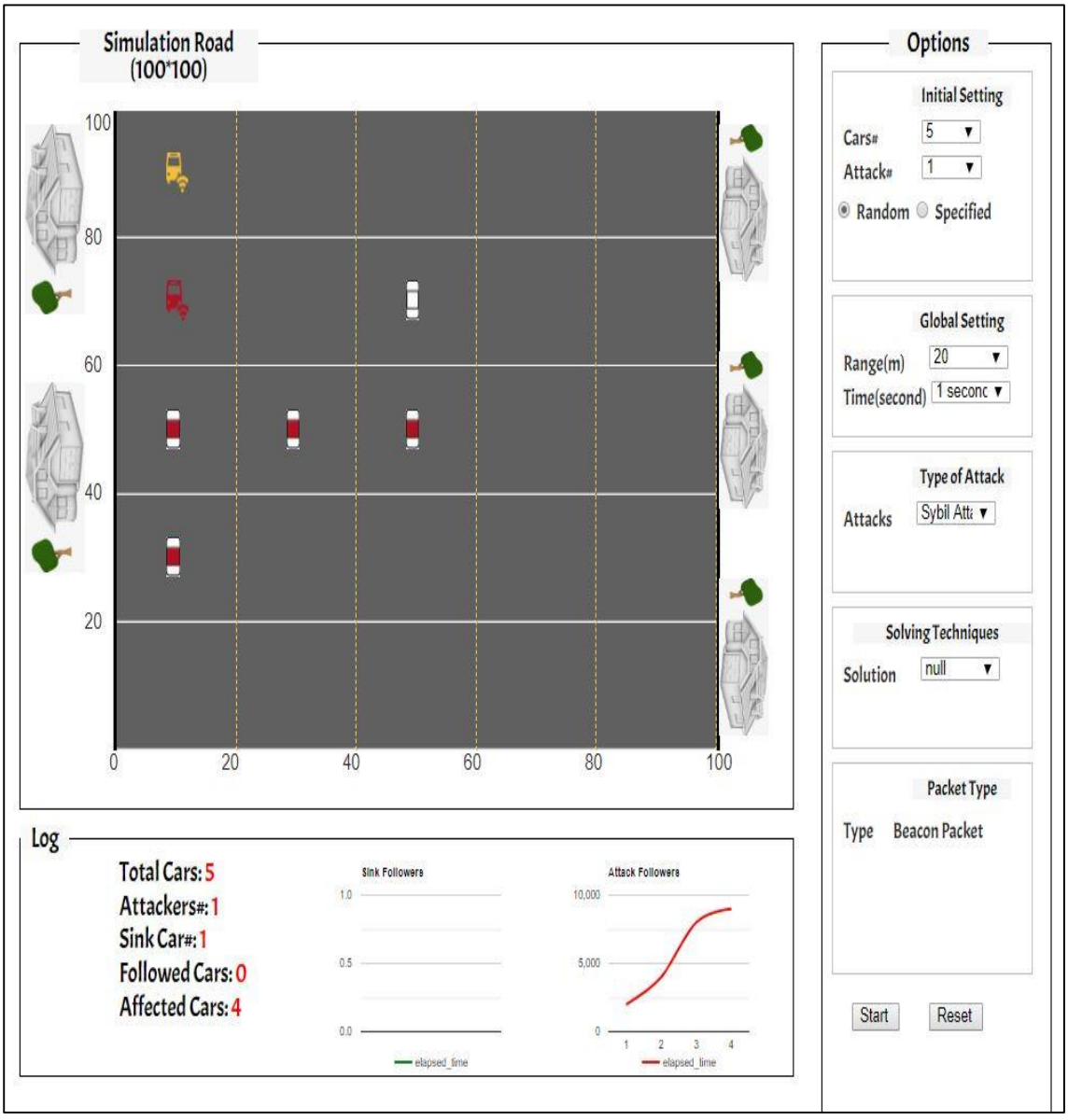


**Figure 3.3:** Random Scenario of Sybil Attack Using Five Cars.

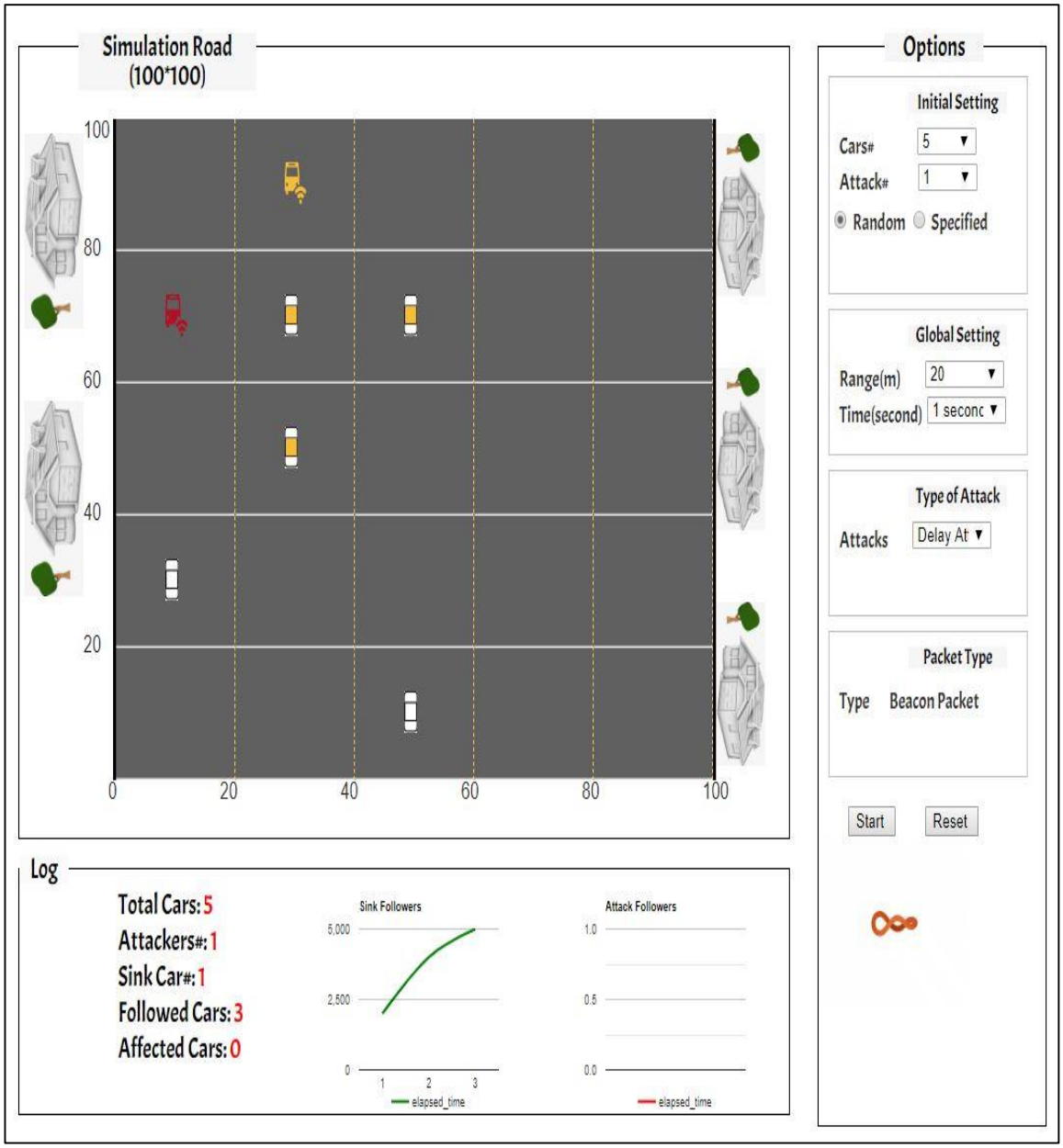


**Figure 3.4:** Random Scenario of Delay Attack Using Five Cars.

### 3.4.3 Dos Attack

In this experiment, we discuss a serious type of attacks (DoS). The purpose is not to impersonate the leader nor to disrupt the message but to prevent it completely from reaching. Often the target in this type of attack is the closest vehicle to the attacker and not just all vehicles.

In this type of attack (DOS), as shown in Figure 3.5, the platoon consists of five vehicles in random way with 20m range and 1 second for sending packet. Where the platoon sends a message to the nearest vehicle belonging to it and then move the message until its reach the last vehicle in the platoon. It was found in this experiment that the attack affected only one vehicle which is the second one in the platoon. So, by blocking the second vehicle the platoon leader will have no control over the entire members.

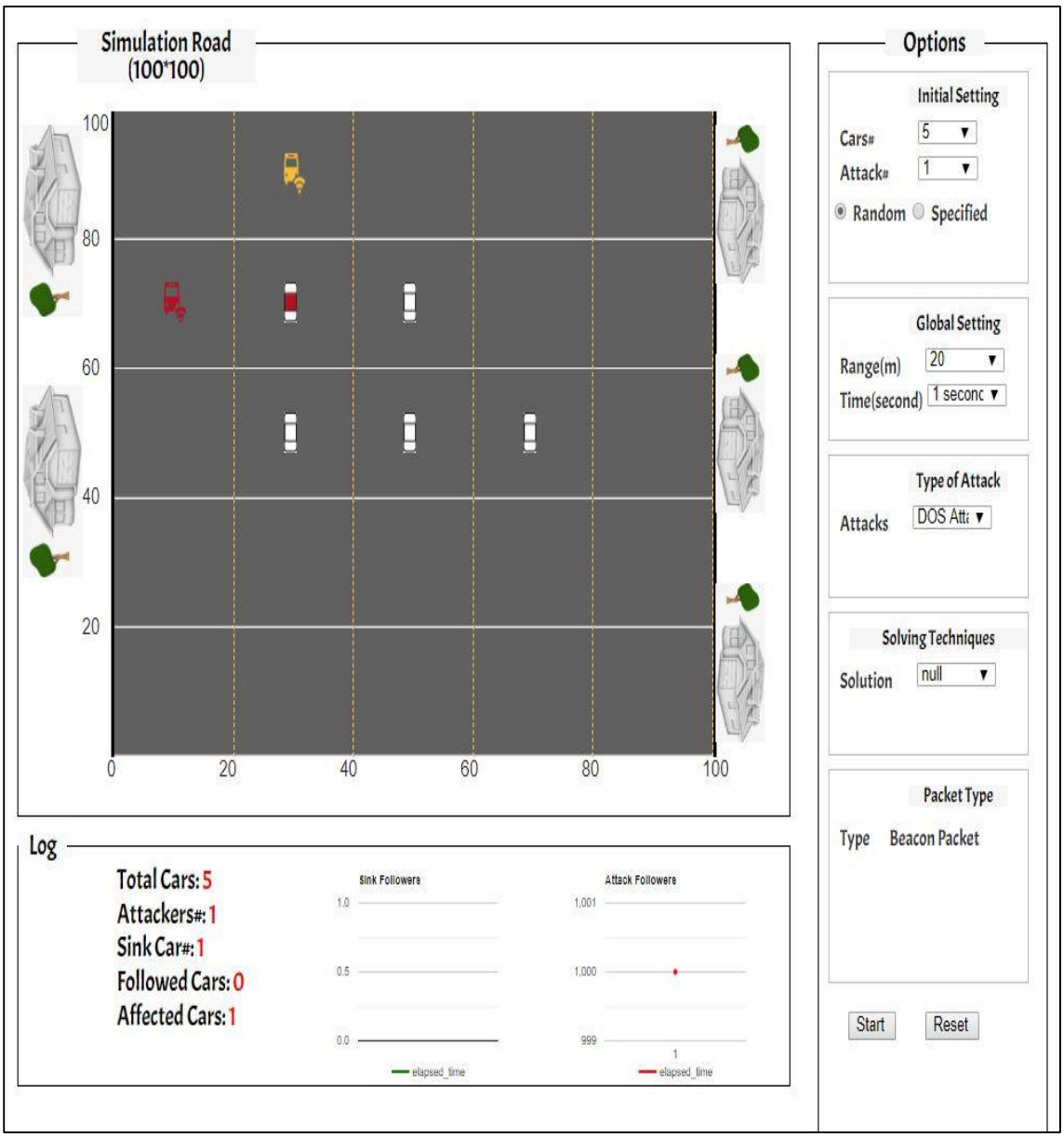


**Figure 3.5:** Random Scenario of DOS Attack Using Five Cars.

## 3.5 OUTSIDE ATTACKS SECURITY TECHNIQUES

the security techniques of outside attacks presented in following sections.

### 3.5.1 Message Authentication Technique

MAC is one of the most popular ways to discover that a message is not from a trusted source. MAC method can show that the message sent is fake or not. This method consists of several processes, which are like and represented in the Figure 3.6:

- First, it is necessary to calculate the authentication code at the sender first by inserting the message on a complex mathematical process to extract the code to prove the character of the sender.

- Second, the sender of the network commander to add the code in the previous step to the message sent without encryption and then sent to platoon members.

- Thirdly, in any car of the platoon, both the message and the code are separated. And then insert the message received on the same complex process used by the sender and the extraction of special code for the car.

- Fourth, compare the code accompanying the message with the new code generated by the vehicle. If the same code is equal, this message is sent by the correct sender. But if they are not equal this message is false.

$$MAC\ (M) = E(Ks, (M \oplus P)) \tag{3.3}$$

M = original message (variable size)

P = padding numbers (random)

$\oplus$ = XOR operation

E = Encryption Algorithm (DES)

Ks = (Symmetric keys)

MAC(M) = message authentication code of message (variable size)

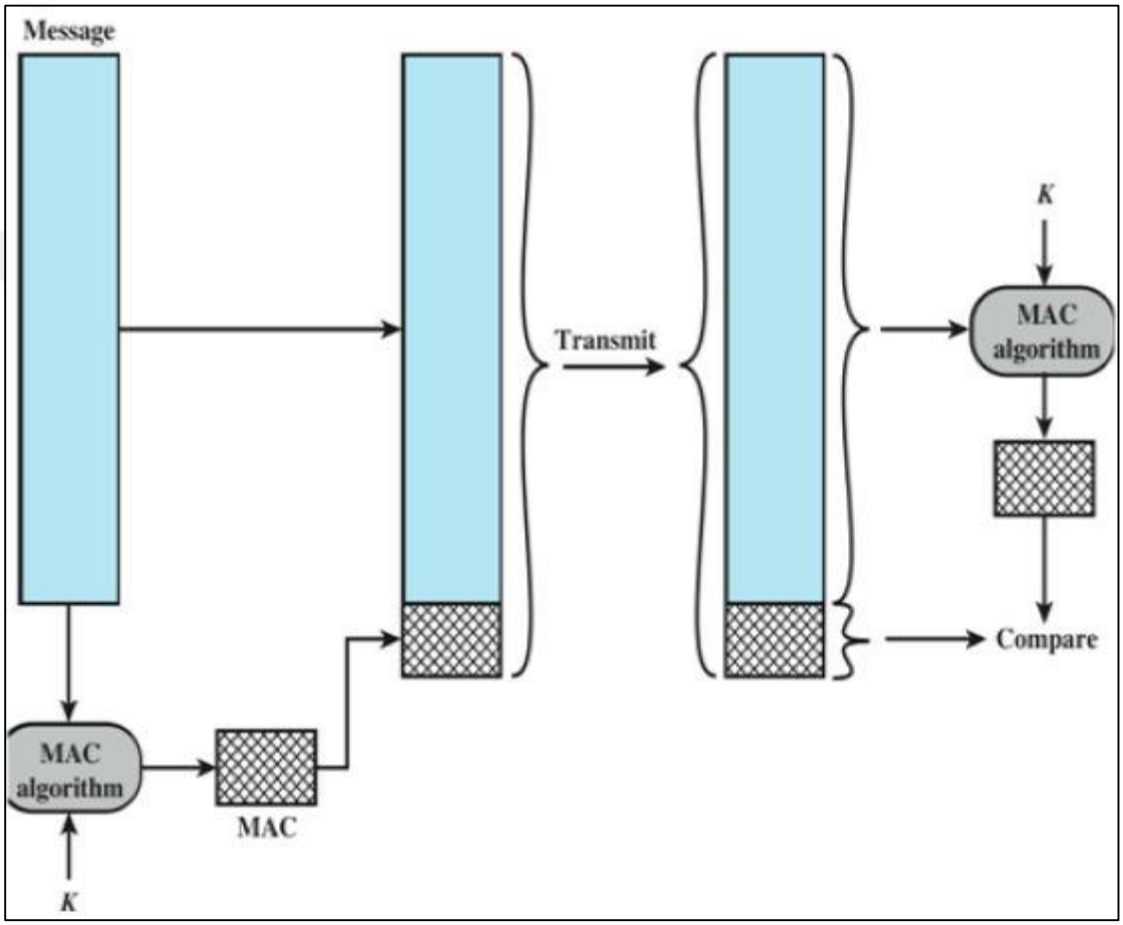


**Figure 3.6:** MAC Technique.

### 3.5.2 Encryption Techniques

In this part we will talk about another important way to prevent attacks. But use this method and become effective in case of passive attack. In passive attacks, the main purpose of the attack is to intercept and not to cause damage.

In this section we will talk about encryption methods. Encryption has many types and algorithms starting from the Middle Ages to the present. But vary among themselves in the difficulty and complexity of the code and the difficulty of decoding. The cryptographic algorithms are divided

into two parts, the first is the old one, which deals with texts only. The other part is the most important and the most difficult and the latest is the binary and here it can deal with all elements such as pictures, video, text messages and digital. The following Figure 3.7 represents the classification of cryptography techniques. But currently rely entirely on the binary algorithms. Under this part of the coding methods are the two most recent algorithms, namely AES (Advanced Encryption Standard) and DES (Data Encryption Standard).

While Figure 3.8, we will review the steps of AES. AES is one of the most popular encryption methods that require 12 or more consecutive times and every time a dedicated key is used.

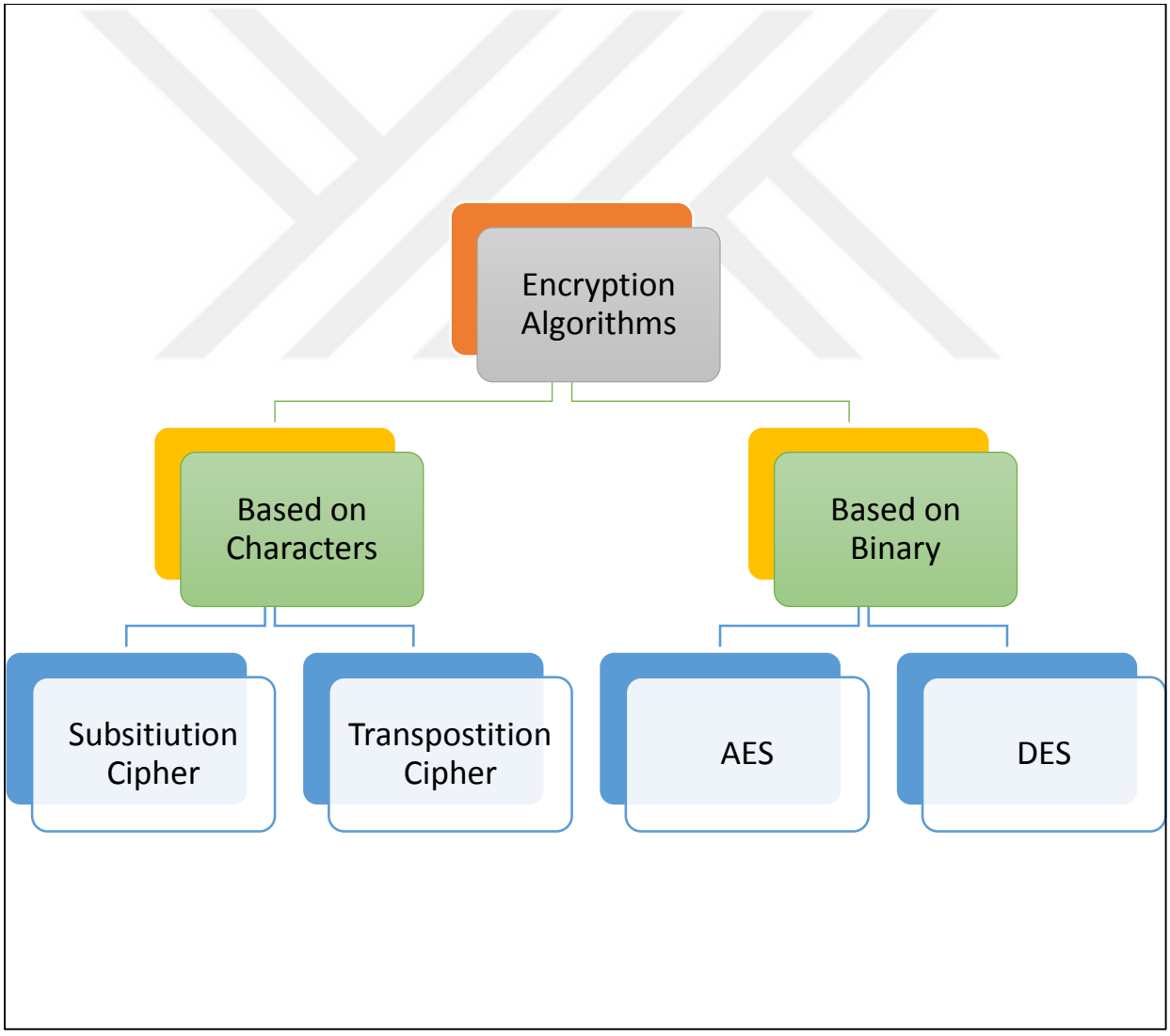


**Figure 3.7:** Classification of Encryption Techniques.

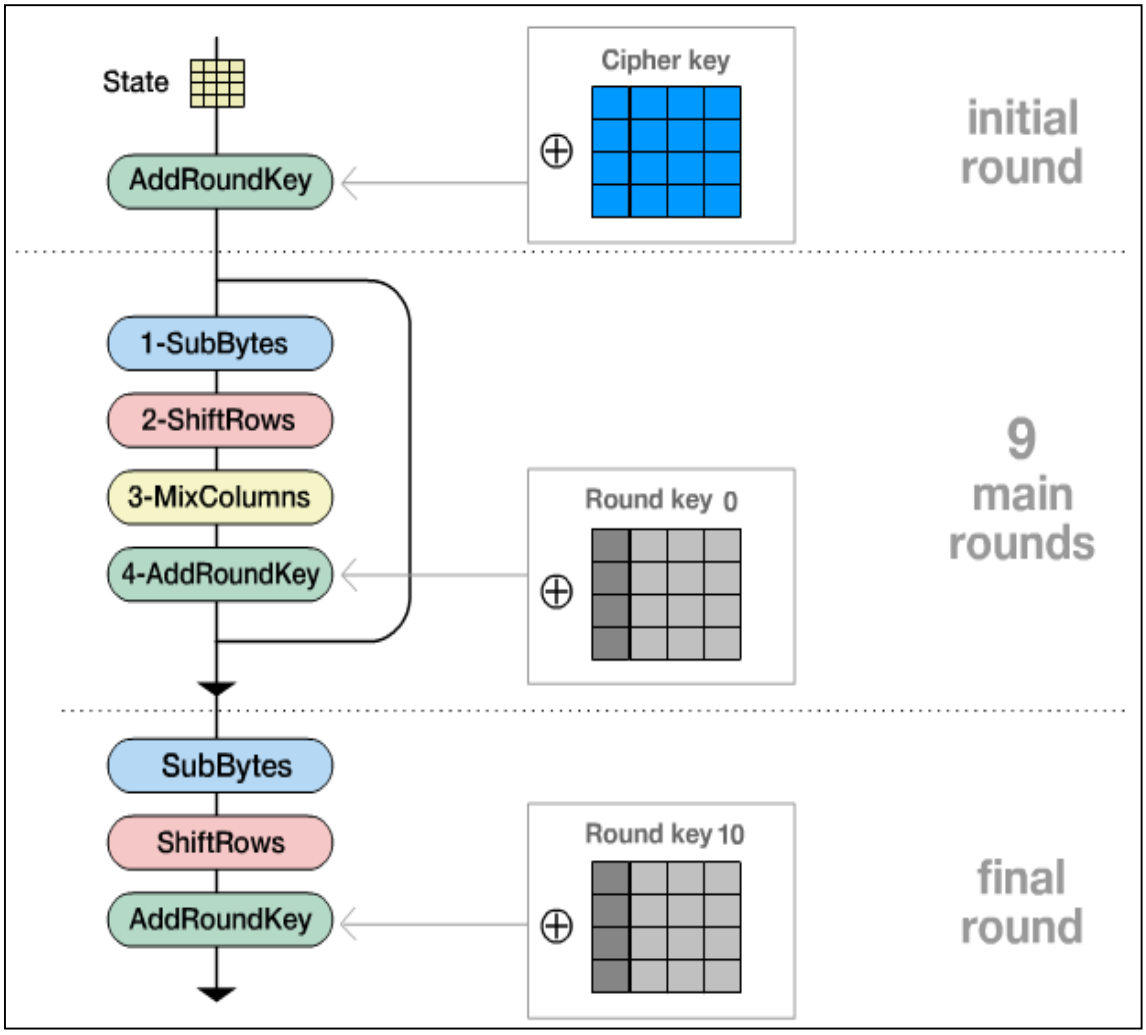


**Figure 3.8:** Steps of AES Technique.

### 3.5.3 Hashing Techniques

In this section we will review one of the most important methods used in reprisals attacks and maintain the availability and validation. In this section we will discuss the third method, the process of hashing. This process can be performed in one of the following ways as shown in Figure 3.9 below.

- Method 1: By symmetric encoding of the hashing code. In this method, the sender sends the message to the Hashing algorithm and then encrypts the output using a symmetric key between the sender and the addressee. Then the message is sent along with the encrypted

code. When the sender receives the message and the encrypted code. It encrypts the message using the same key and if the resulting code is the same as the sender code if the message is true and if not, it is fake.

- Method 2: By the asymmetric encoder of the Hashing code. Here we use the same steps but using an asymmetric encryption key. Asymmetric mean that the secret key known only by the owner unlike the symmetric where the shared key will used among two or more vehicles.

- Method 3: By using the secret word, the message is surrounded by all parties. That word consists of the original message content. If the message is changed, it does not produce the same password and therefore it is recognized that the message is fake and not from the correct source.

$$H(M) = Md5(M \oplus P) \quad (3.4)$$

$$C = E(Ks, H(M))$$

M = original message (variable size)

P = padding numbers (random)

$\oplus$ = XOR operation

Md5 = Hashing Algorithm produce fixed digest

E = Encryption Algorithm (DES)

Ks = (Symmetric keys)

C = Cipher code

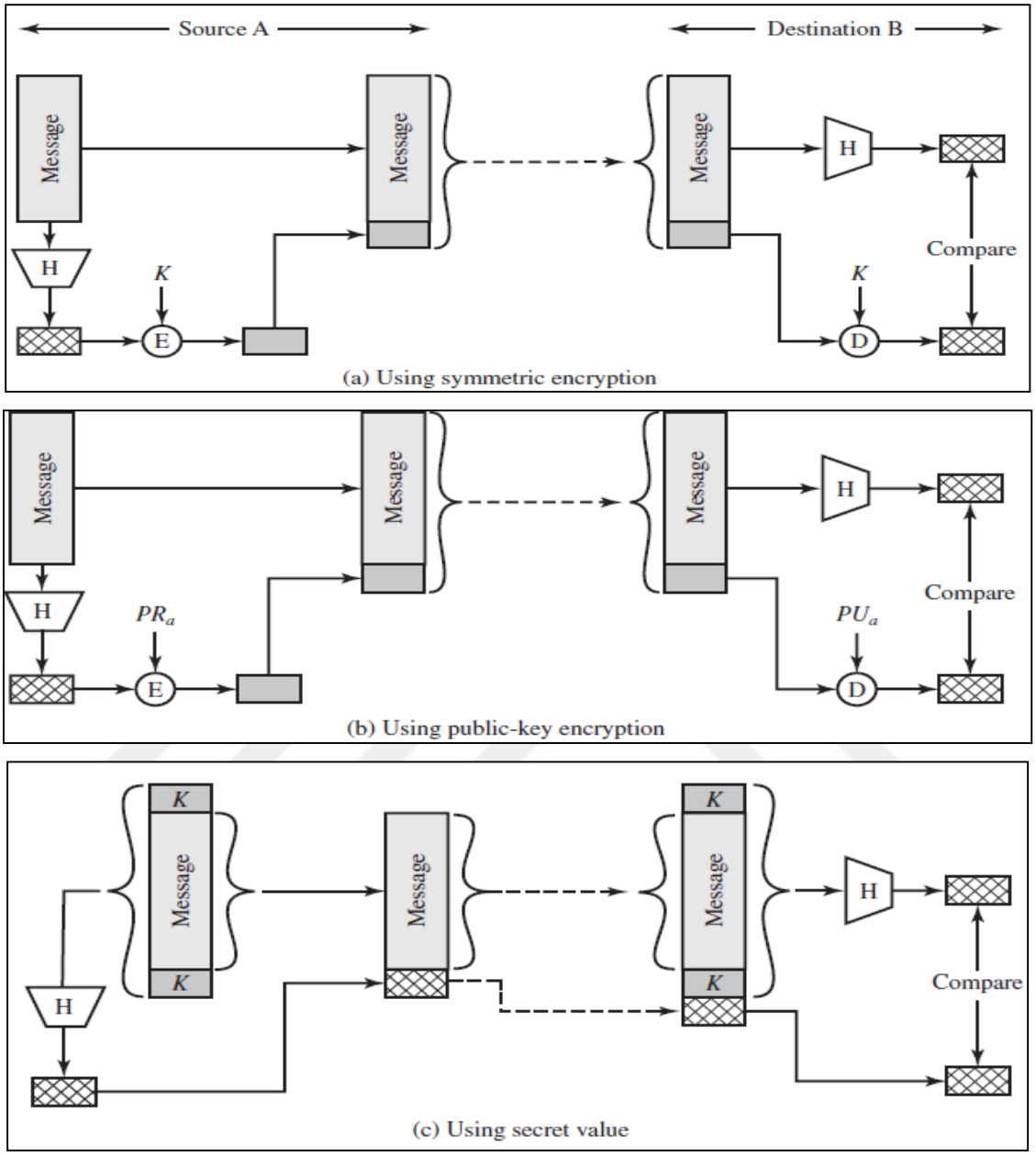


**Figure 3.9:** Hashing Ways.

## 3.6 SOLUTION OF OUTSIDE ATTACKS

In this section, security techniques such as (MAC and Hashing) will utilized to overcome the sybil attacks, DoS attack and delay attack which consider an outside attack using Message Authentication Technique and Hashing Techniques through a smart simulation, as we have already mentioned before.

### 3.6.1 Solution of Sybil Attack Using MAC

MAC represent the solution to this type of attack. By following the steps of the solution that we mentioned earlier, the result as shown in Figure 3.10, represents the random form of car representation, there is no vehicle followed the attacker, although the attacker is close to them due to the use of MAC algorithm that will send coded message it will become more difficult for the attacker to imitate or send false messages because they do not carry these codes and any message that does not carry that code is ignored.

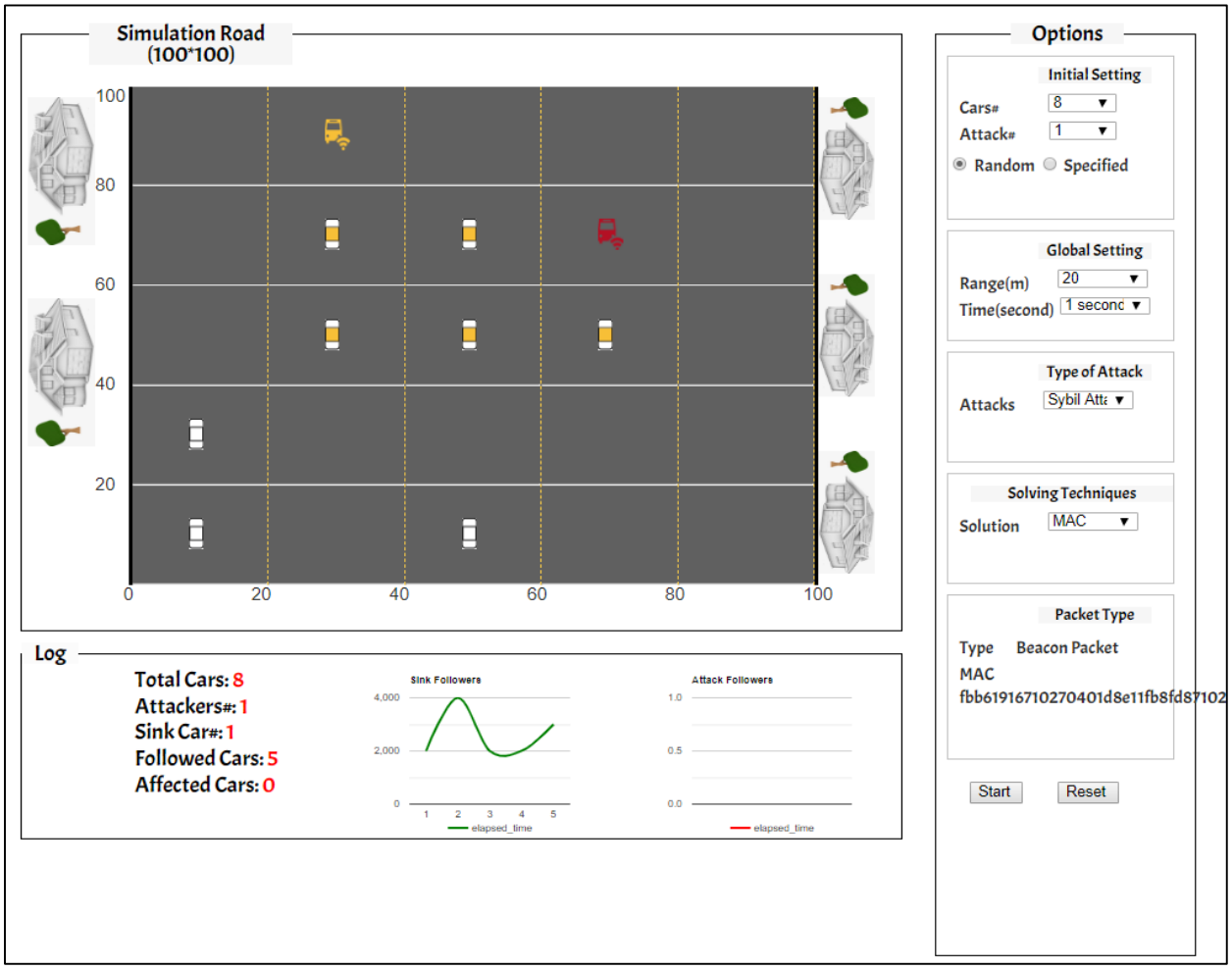


**Figure 3.10:** Solution of Sybil Attack (Random Scenario) Using MAC Technique.

### 3.6.2 Solution of DOS Attack Using MAC

As mentioned in the third chapter, the MAC method is also used to solve the problem of DOS. As we mentioned in the previous section that following the steps of the MAC, it's was found in

Figure 3.11 that the attacker was also overcome and that all the vehicles belonging to the platoon leader became safe and cannot be controlled by the attacker. We also found that the time elapsed is less than before and the network works normally and securely.

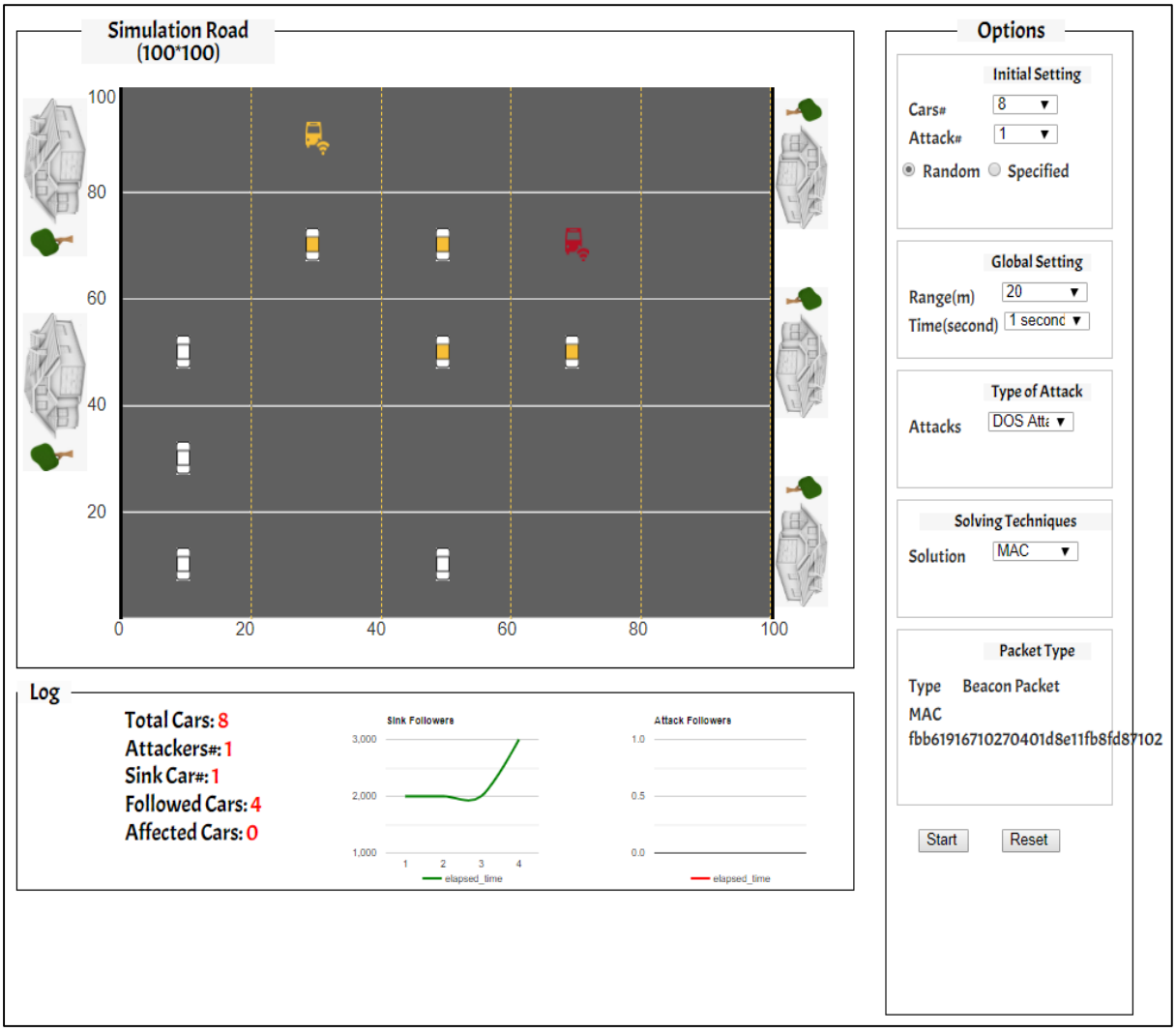


**Figure 3.11:** Solution of DOS Attack (Random Scenario) Using MAC Technique.

### 3.6.3 Solution of Delay Attack Using Hashing Code

As mentioned in the third chapter, the Hashing method is used to solve the problem of delay attack. As we mentioned in the previous chapter, that following the steps of the hashing using symmetric encryption, it's was found in Figure 3.12, that the attack was overcome and that all the vehicles belonging to the platoon leader and the platoon became safe and cannot be

controlled by the attacker. The result also found that the time elapsed is less than before and the network works normally and securely.

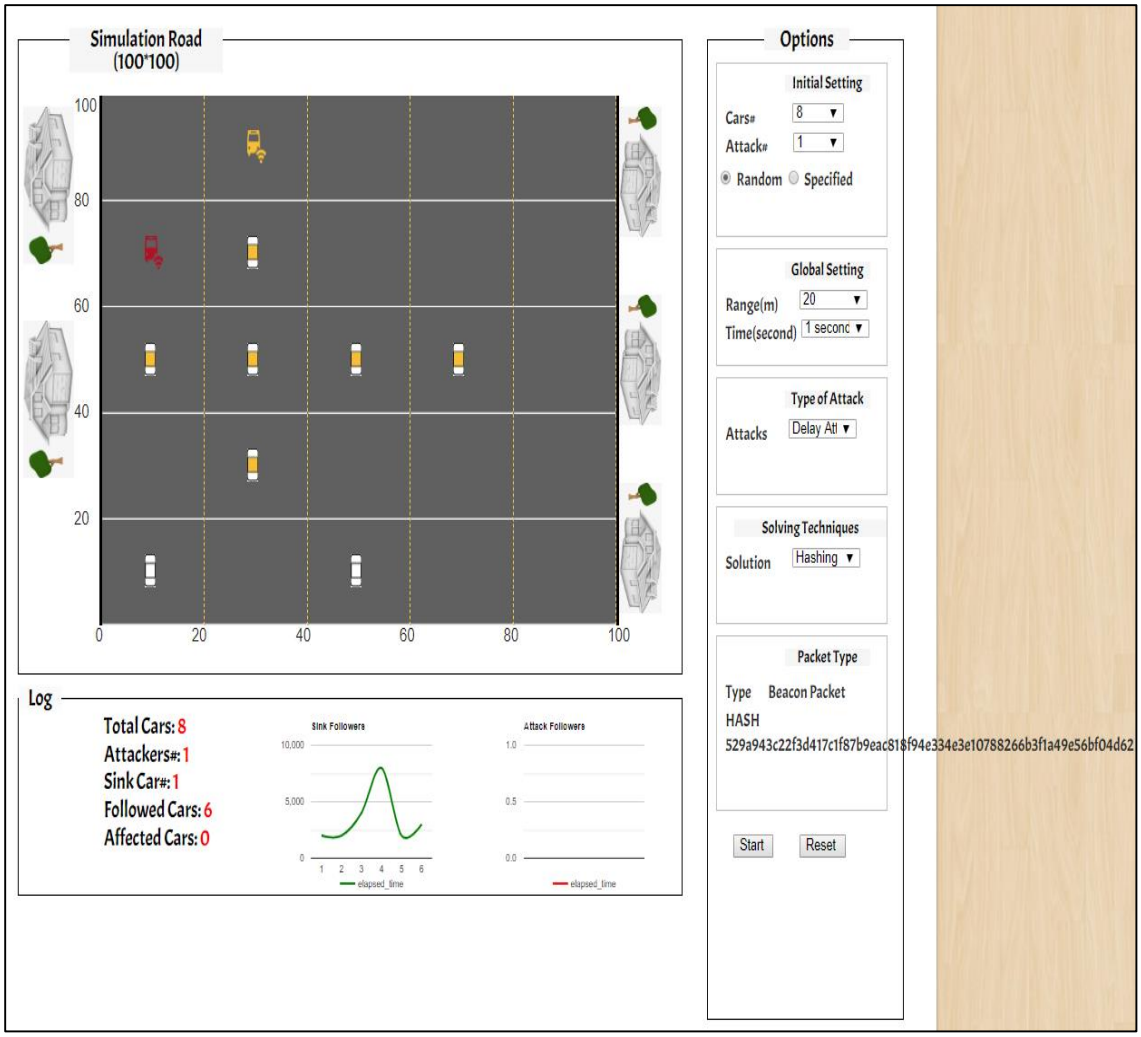


**Figure 3.12:** Solution of Delay Attack (Random Scenario) Using Hashing Technique.

The results above shows the ability of these algorithm to overcome these attacks which is (Sybil, DoS, Delay) attacks and secure the platoon from these attacks. But, all this in case the attacker does not break the algorithm or know the key used in encryption algorithm.

# 4. INSIDE ATTACKS

## 4.1 TYPES OF INSIDE ATTACKS

This chapter will focus on the inside attacks that effect the vehicular system. The following sections will present the types of inside attacks.

### 4.1.1 Botnet Attack

any group of computers that attached in a symmetric style for malicious purposes called botnet. bot is a computer in a botnet, these bots compose a network of expose computers, a third party will be the controller and used to transmit malware or spam, or to launch attacks. botnet also known as zombie army [37]. botnet primarily established as a tool for the benefit of Internet relay chat (IRC) channels. ultimately, bots where developed by hackers to execute malicious activities such as keystroke logging and password theft. computers with low level of security often attacked by botnet. computers can get controlled by a botnet manipulator in different ways, but the most common through viruses. botnet considerable attack since both organized crime and hackers use to execute illegal activities. for instance, botnets will be sued in organized crime as a way of spam or even by sending phishing attack that is then used for identifying theft, while hackers will use it to start denial of service attacks. systematic network of software robots called botnet, that run automatedly on zombie machines that's spoiled by malware [38]. DDoS attacks are initiated by botnets and also distributed computing, initiated cyberwarfare and hijack personal information as shown in Figure 4.1. botnet is a powerful threat that facing users and internet system. all infected computers are controlled by bot-master and these infected computers will be directed to initiate malicious activities. more devastating botnet will decentralize the system by construct the network in peer to peer (P2P) manner and in that case the communication will only happen with a small number of infected computers. all what mentioned before making it much difficult to detect botnet. like all cyber-attack botnet aim on targeting IT system. but several cases recently show the use of botnet to attack the OT system. the implementation of internet was designed with an aim goal of security often as an afterthought. In this scenario a bot-master is one of the platoon members. Since, each vehicle in the platoon able

to send message to the successor and preceding vehicle, botnet master vehicle will infect one of the members with a virus and then give the order to initiate the attack.

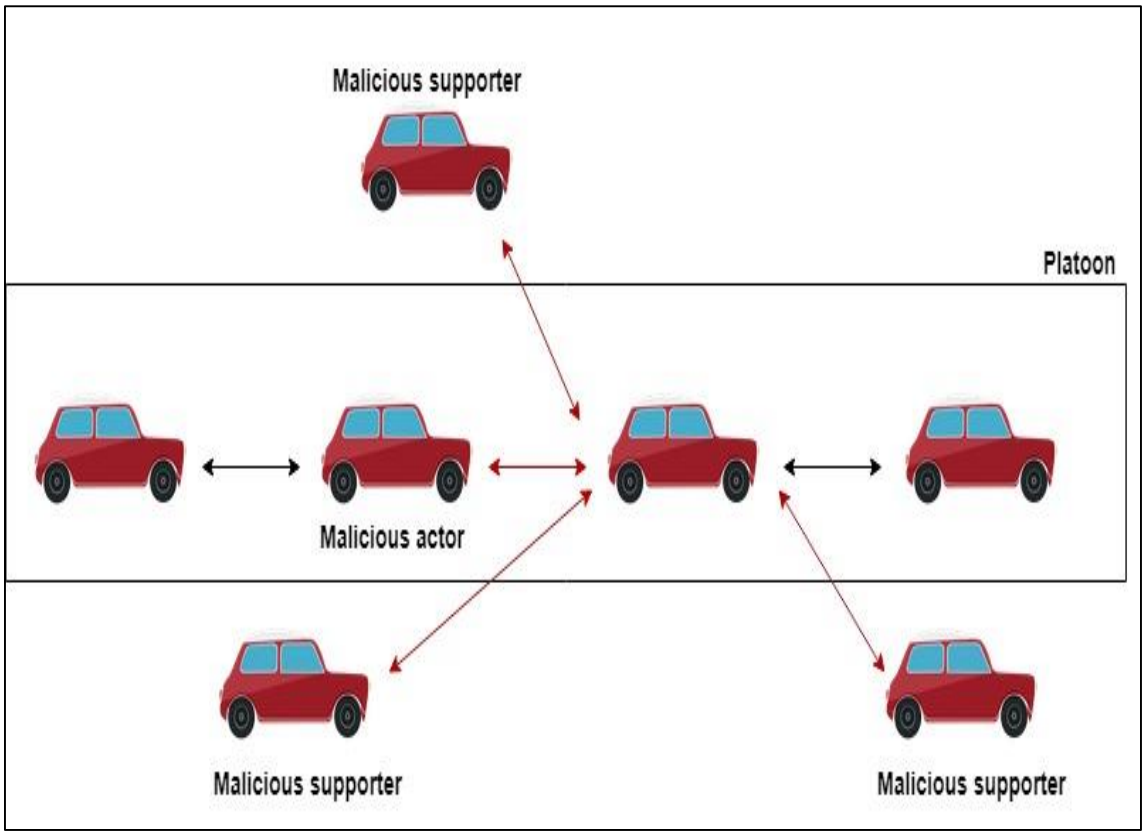


**Figure 4.1:** Botnet Attack.

### 4.1.2 Drive-By Attack

Drive-by Attacks become one of the most common type of attack. Drive-by Attacks used by threat actors in order to force the client into processing an action without the permission of the user. What separate the Drive-by attacks from other attacks of this nature, is that the Drive-by Attacks do not need any user connection or interaction with the content of malicious for the attack to be achieved successfully, such a feature will makes this attack to be incredibly hard for users to not only identify, but also avoiding this type of attack. in recent years Drive by attack become more common attack where web browsers are wrecked by malicious content transmit by web servers [36].

In order to perform the Drive-by attacks, first, the threat actor will look for a vulnerable vehicle and will inject their own code that are going to be loaded by the users as shown in Figure 4.2. The design of the code will enable it to run as the client connects to the vehicle, this depend on the will of the threat actor. There multiple of example that describe how the code perform, for example, the code may tell the client machine to download malware content or redirect the user to the threat actors own malicious content. Drive-by Attacks have variety of use cases and is not limited for one area, the threat actors can implement this type of attack via pop-ups and adverts, email, relying on the exploitation of unpatched security error and defects that present in applications, extensions and operating systems.

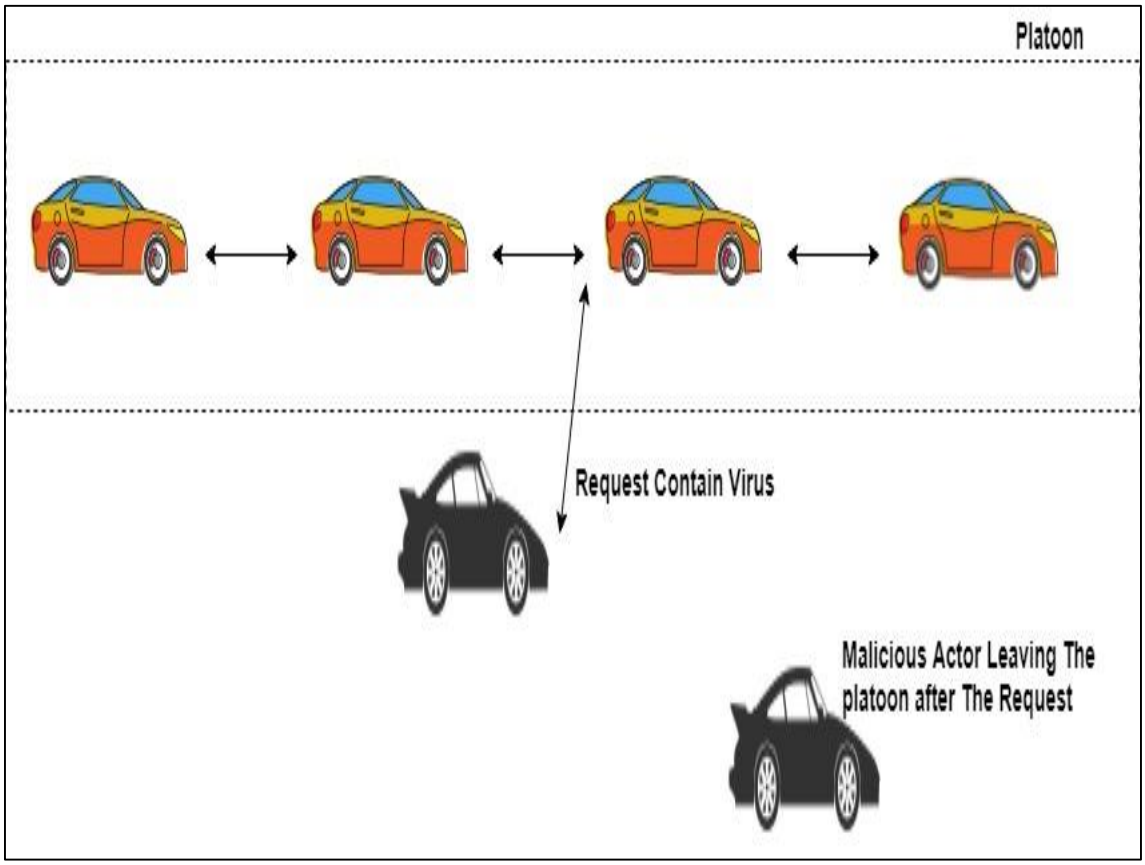


**Figure 4.2:** Drive-by Attack.

### 4.1.3 Ad-Hoc Attack

Ad-Hoc attacks are considered to be very serious and danger type of attacks, in which the attacker (malicious user) use a 3rd party legitimate user as a man-in-the-middle, that is going to

be between attacker's device and other legitimate devices which in that case a vehicle inside the platoon [39].

Such attack required to be working on "device-in-the middle", that can be setup on both Linux or windows device, and it allows to initialize ad-hoc (peer-to-peer) wireless connection between client devices. This connection doesn't need any extra network infrastructure. In other words, a virtual software AP is created and the other device that is associating with the SSID you have created.

The following example will describe a situation of an ad-hoc attack. For an example, let's imagine that the attacker may be any vehicle in the platoon, whether it was 2, 3 or 4. The attacked vehicle (man-in-the-middle) would be vehicle 5.

The Attacker vehicle may connect to the WLAN broadcasted by vehicle 5 and then, use it to route all the traffic to the rest of the platoon via victim vehicle (vehicle 5). Hence, it would look like it is vehicle 5 originating the traffic. The wireless links from the vehicle 5 to the attacker do not have to be a Wi-Fi connection, it can be a Bluetooth or other type of wireless connection technology, that is supported by all the parties that attempt to communicate with each other as shown in Figure 4.3.

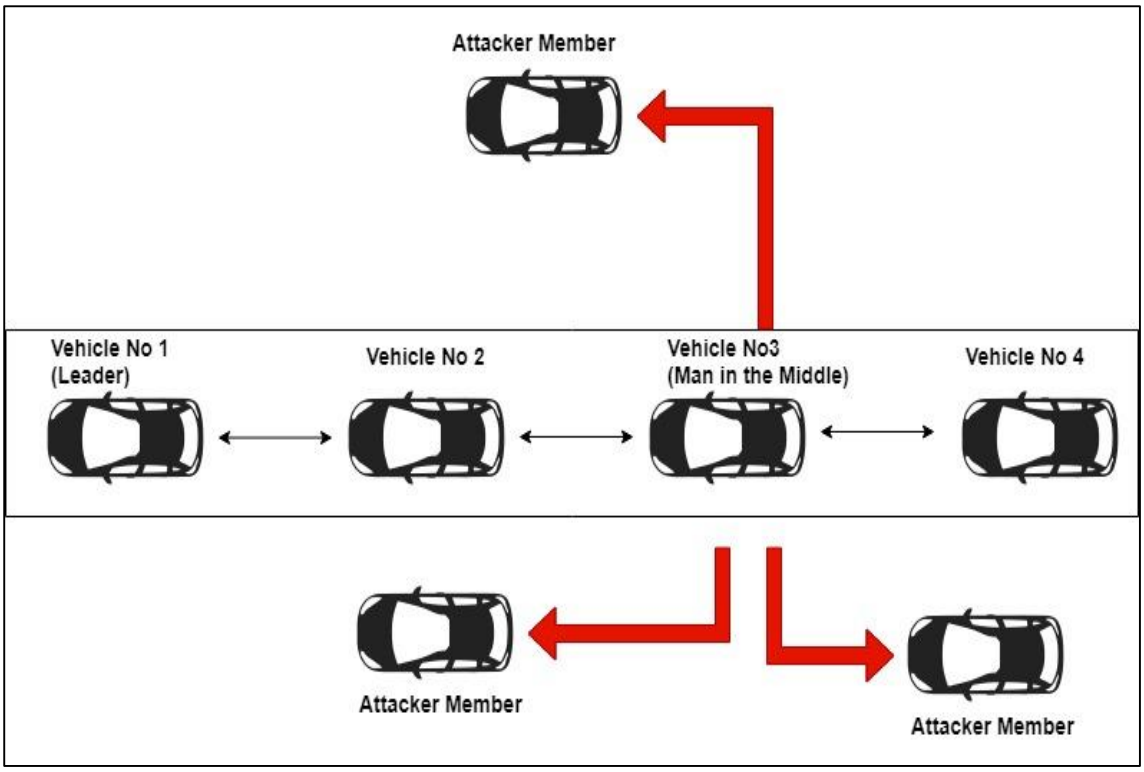


**Figure 4.3:** Ad-hoc Attack.

### 4.1.4 Dos Attack

Denial of service attack “DoS” consider the most famous and dangerous attack since this attack will be able to block a vehicle in the platoon from receiving and transmitting any message by separate the vehicle from the platoon. This attack in particular was covered in the previous chapter where malicious actor can implement this attack as inside and also outside attack. Briefly, this type of attack is the most famous of the rest of the attacks because of the severe damage it causes as it intercepts the messages and prevents their arrival. This type depends on the attacker to block messages by cutting or jamming the transmitter and then separates the vehicle from the rest of the platoon.

## 4.2 METHODOLOGY

For this particular issue of assault on platoon we utilized the linked list to interface various vehicles in the unit. The linked list has two pointers in its structure information type as appeared in its pragmatic work. The next pointer focuses to the following vehicle in the detachment while the previous pointer focuses to the past vehicle. There is no sufficient technique today for checking physical courses of action of vehicles inside a detachment development. In particular, the problem was addressed the issue of a detachment assault where an aggressor identifies nearness inside a platoon to pick up affirmation and in this way execute vindictive attack. To address such concerns, we present linked list, a novel self-sufficient unit confirmation conspires which ties the vehicles' advanced declarations to their physical setting. Linked list misuses the discoveries that vehicles voyaging together experience comparative setting to demonstrate to one another after some time that they are co-present. Work methodology depends on the capacity for vehicles to catch this unique circumstance, produce validation to set up shared keys, and later tie these symmetric keys to their open keys. We structure and actualize the linked list convention and assess it with reenactment on C++. The usage shows that vehicles recognized by their unique situation and this can be used to defeat detachment assaults (i.e. DoS, Ad-hoc, Drive-by and Botnet) and comparable their misconduct.

Among the advances in vehicles platooning is a developing one that is accomplishing extensive footing. Vehicle platooning is an arrangement of composed, where taking an interest vehicle

drive in a solitary record or detachment; every vehicle carefully pursues the previous vehicle, with the preeminent vehicle in the development as the company head.

Four types of simulated attacks have been implemented given by:

- DoS Attack (Header File: Dos.h) [Connected to Platoon.cpp]
- Botnet Attack (Header File: Botnet.h) [Connected to Platoon.cpp]
- Drive-By Attack (Header File: Driveby.h) [Connected to Platoon.cpp]
- Adhoc Attack (Header File: Adhoc.h) [Connected to Platoon.cpp]

Each file has an implementation of warning the type of attack, the warning is generated by each header file and that warning is sent to the main file (i.e. Platoon.cpp), when the warning is generated by the header file it than point the pointer of linked list to the type of warning being generated by the Header file to the Main file. Based on this technique of flagging/warning the type of attack to the main file distinguishes the type of attack among different types of attacks (i.e. DoS, Ad-hoc, Drive-by and Botnet). After identifying the type of attack the vehicle is identified which generates the attack, now it's simple to identify the vehicle because whenever the warning is generated internally/inside by the header files, that vehicle is marked as the intruding or attacking vehicle. The reference of vehicle is than being passed to the delete function, the delete function remove the vehicle from the linked list and updates all the pointers. Linked list is the only most efficient way to rearrange the queue/line of vehicles after an attacking vehicle is removed from the platoon. Scan function de-refer all the pointer to the linked list and issue a flag to scan the type of attack being generated as a flag from the header files as demonstrate in Figure 4.4.

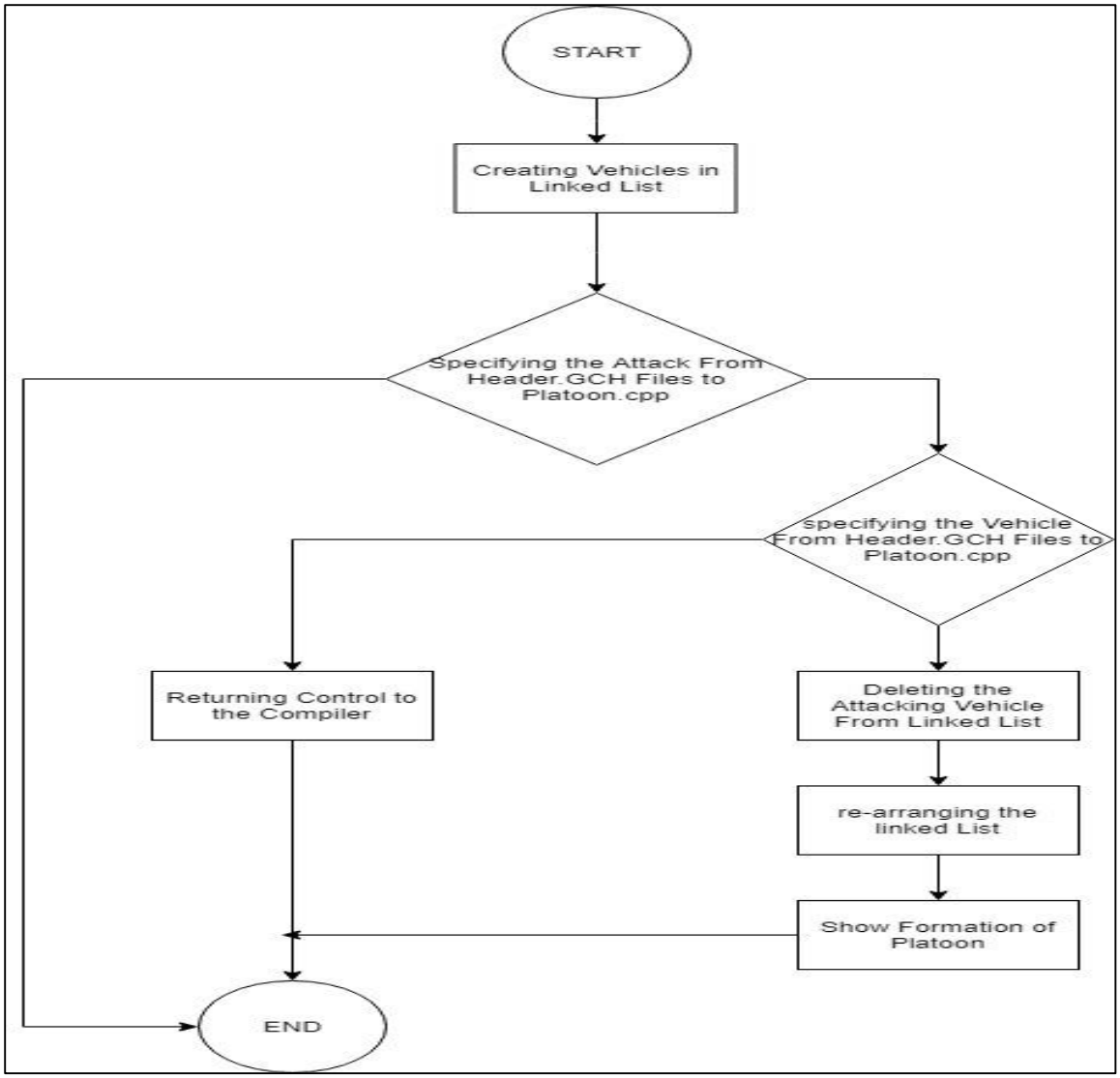


**Figure 4.4:** Threat Detection and Elimination.

## 4.3 RESULTS

In this section we will demonstrate the execution of our program from the formation of the platoon to scanning for attacks and ends with eliminating the threat.

### 4.3.1 First Sample Output

The sample output in which user specifies the number of vehicles in the platoon shown in Figure 4.5, after specifying the number of vehicles in the platoon the user given an ID to the vehicles. The user can take or set as much vehicles in the platoon as much as he/she wants. The first

vehicle which is platoon leader will always be on this linked list. There could be no attack that can intrude the platoon leader. The linked list links all the vehicles by using pointers in a formation. If the user press 0 that's mean the scanning of vehicle and attack will not happen as shown in the figure below.

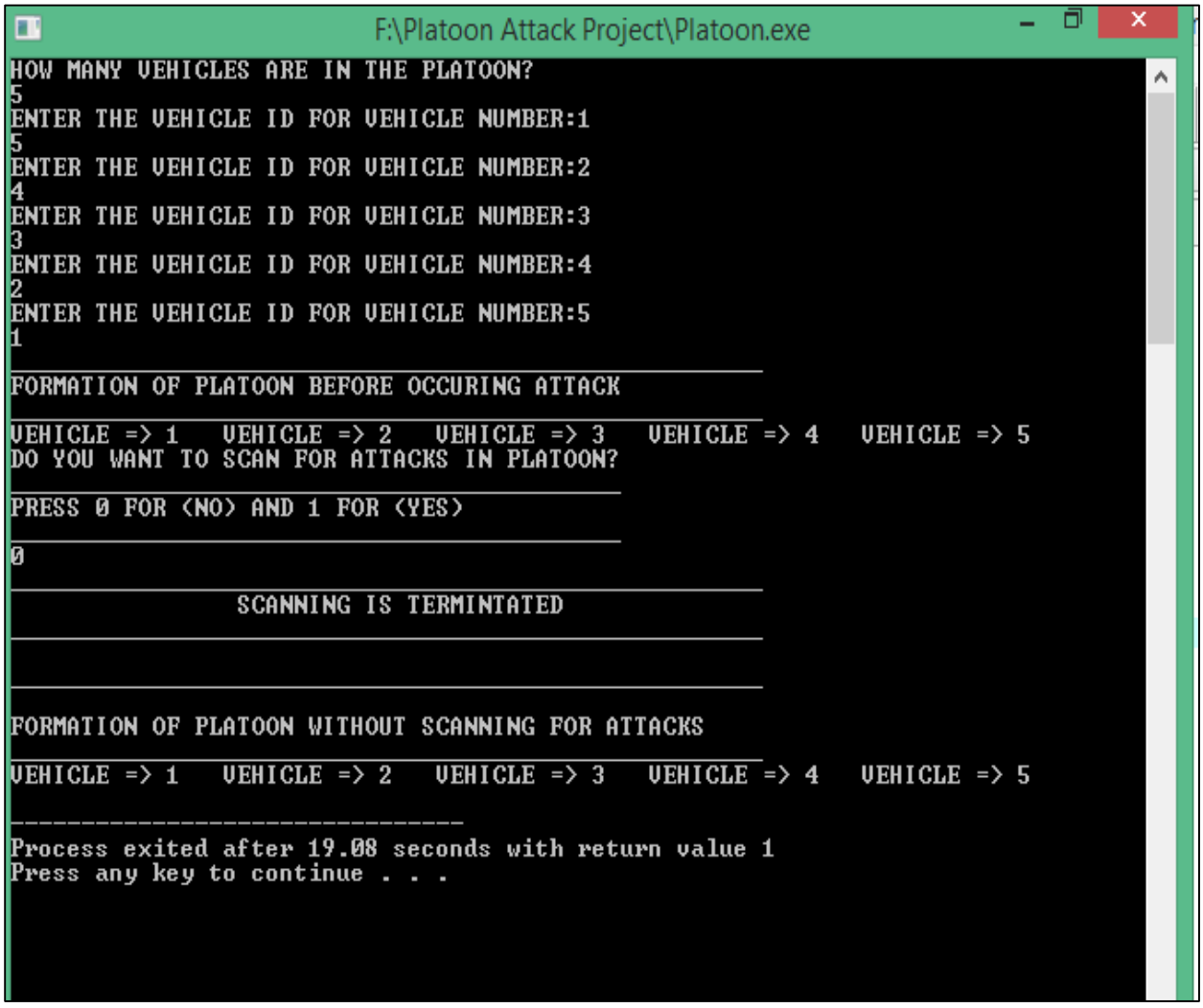


**Figure 4.5:** Formation of The Platoon.

### 4.3.2 Second Sample Output

The sample output in which user specifies the number of vehicles in the platoon, after specifying the number of vehicles in the platoon the user given an ID to the vehicles. The user can take or set as much vehicles in the platoon as much as he/she wants. The first vehicle which is platoon leader will always be on this linked list. There could be no attack that can intrude the platoon

leader. The linked list links all the vehicles by using pointers in a formation. If the user press 1 that's mean the scanning of vehicle and attack will happen as shown in the Figure 4.6. The type of attack and vehicle is identified by its position based on the warning/flags generated by the header files connected to the main file. Then user will have a choice of removing the attacking vehicle. The user will press 0 if the user doesn't want to remove the attacking vehicle from the formation of platoon and program will display the linked list without removing an attacking vehicle after scanning of attack being done.

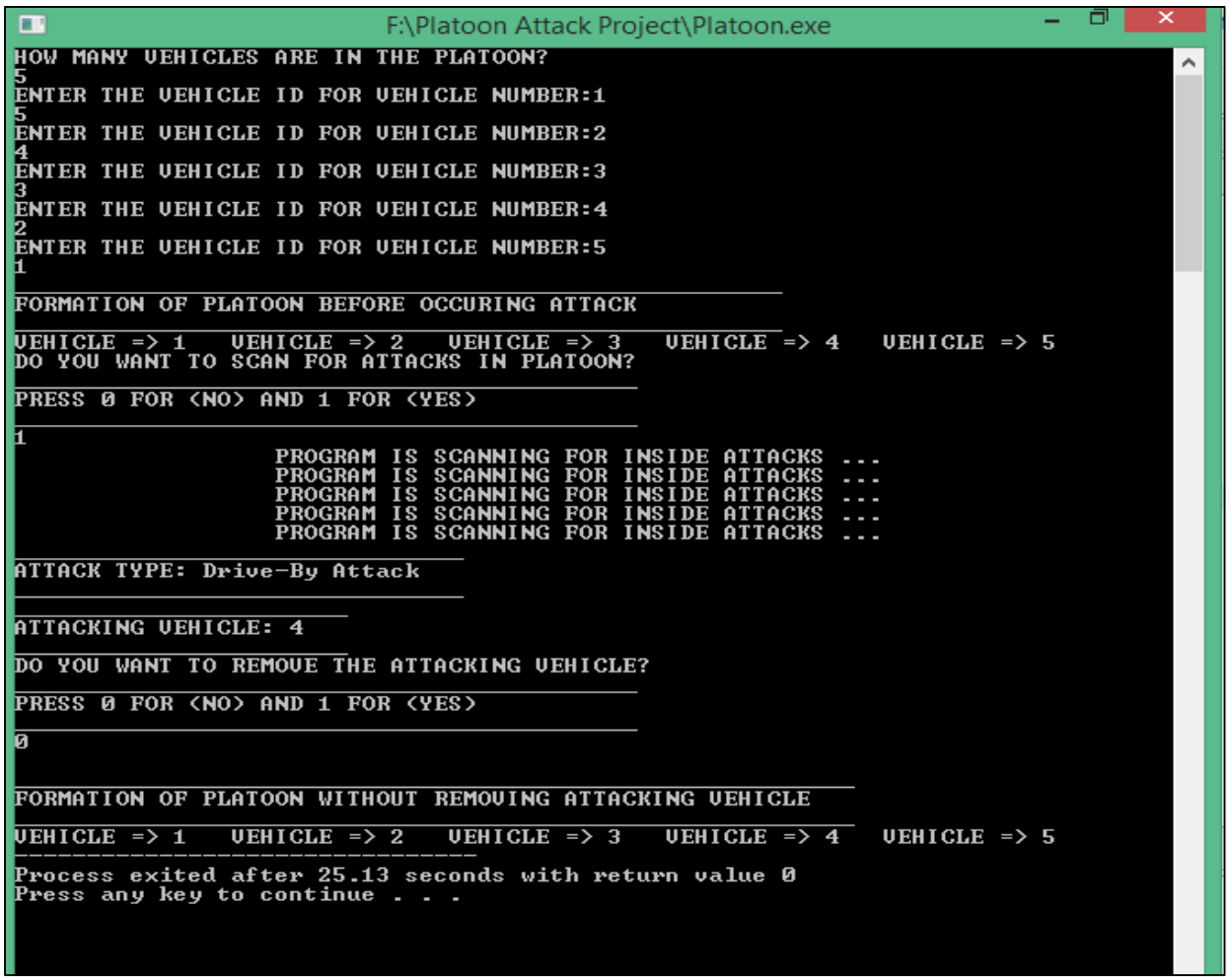


**Figure 4.6:** Detect the Attack and Identify The Attacking Vehicle.

### 4.3.3 Third Sample Output

The sample output in which user specifies the number of vehicles in the platoon, after specifying the number of vehicles in the platoon the user given an ID to the vehicles. The user can take or

set as much vehicles in the platoon as much as he/she wants. The first vehicle which is platoon leader will always be on this linked list. There could be no attack that can intrude the platoon leader. The linked list links all the vehicles by using pointers in a formation. If the user press 1 that's mean the scanning of vehicle and attack will happen. The type of attack and vehicle is identified by its position based on the warning/flags generated by the header files connected to the main file as shown in Figure 4.7. Then user will have a choice of removing the attacking vehicle. The user will press 1 if the user wants to remove the attacking vehicle from the formation of platoon and program will display the linked list after removing an attacking vehicle.

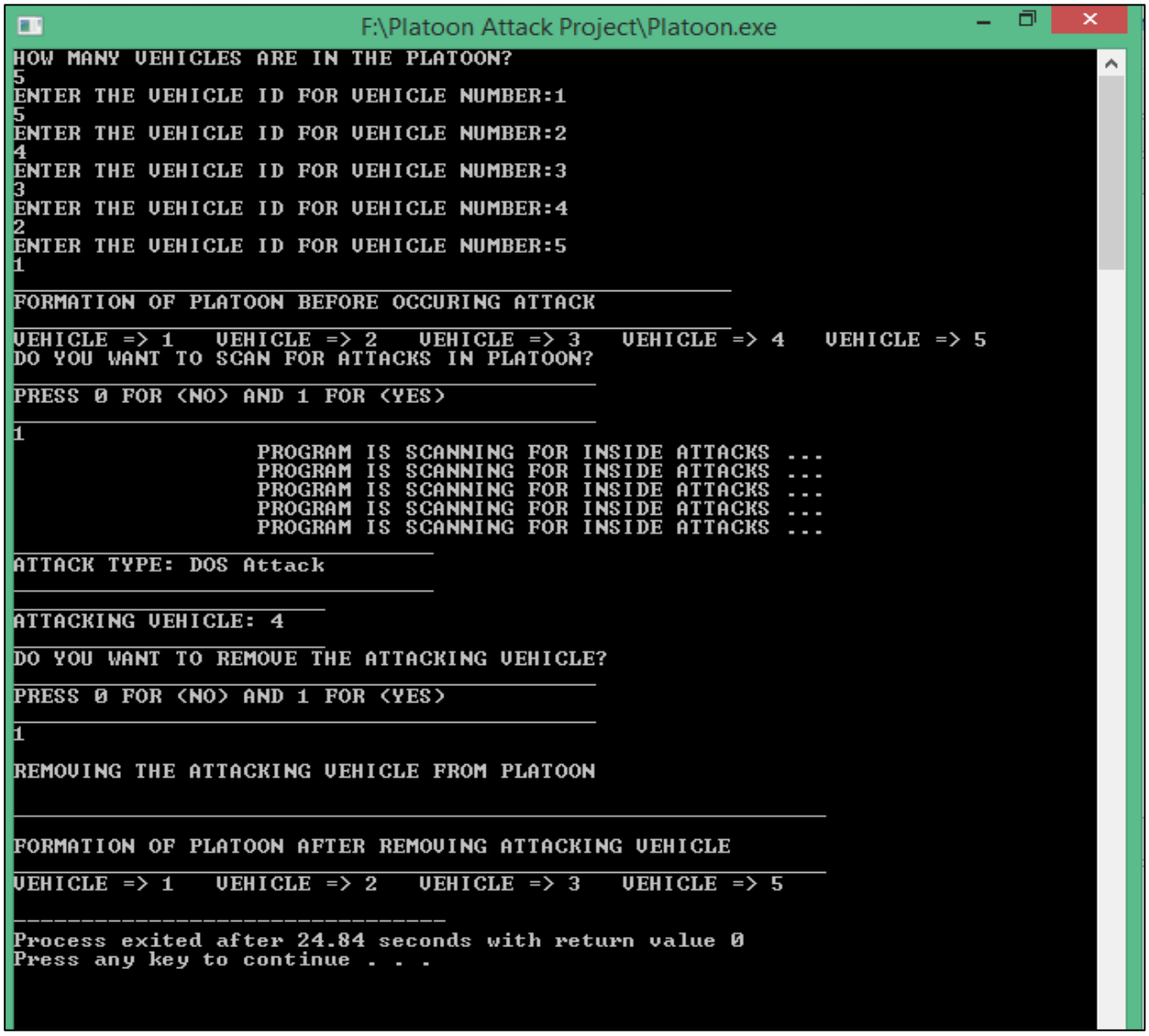


**Figure 4.7:** Eliminate the Threat by Rearranging The Platoon.

Figure 4.8 will show the program executing time for each attack from formation of the platoon to the elimination of the threat. Our result shows that Drive-by attack will take more time that the other three attacks in term of detection the followed by DoS, Botnet and finally Ad-hoc attack. Figure 4.9 will demonstrate the procedure of the program execution.

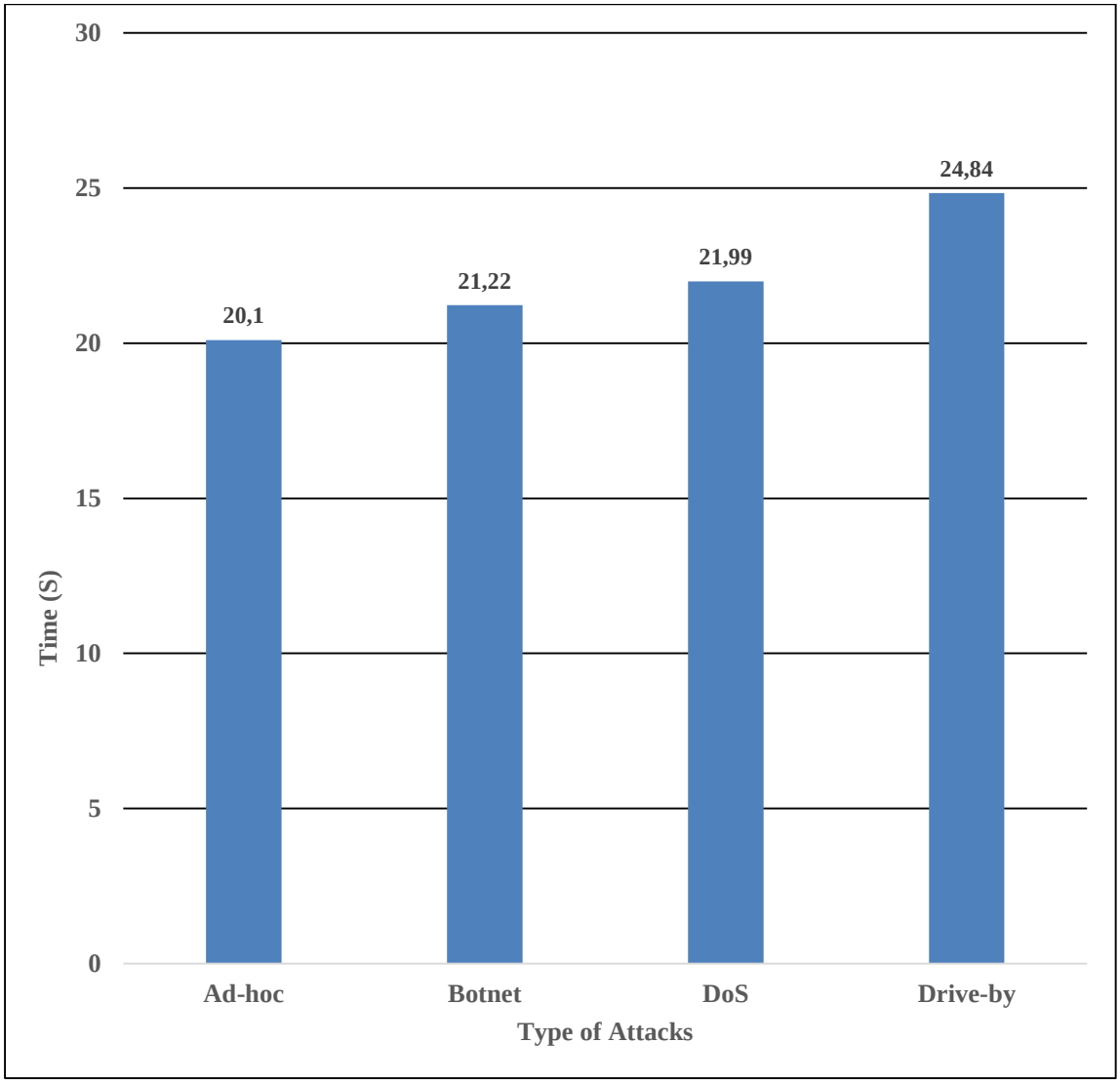


**Figure 4.8:** Time of Executing of Each Attack.

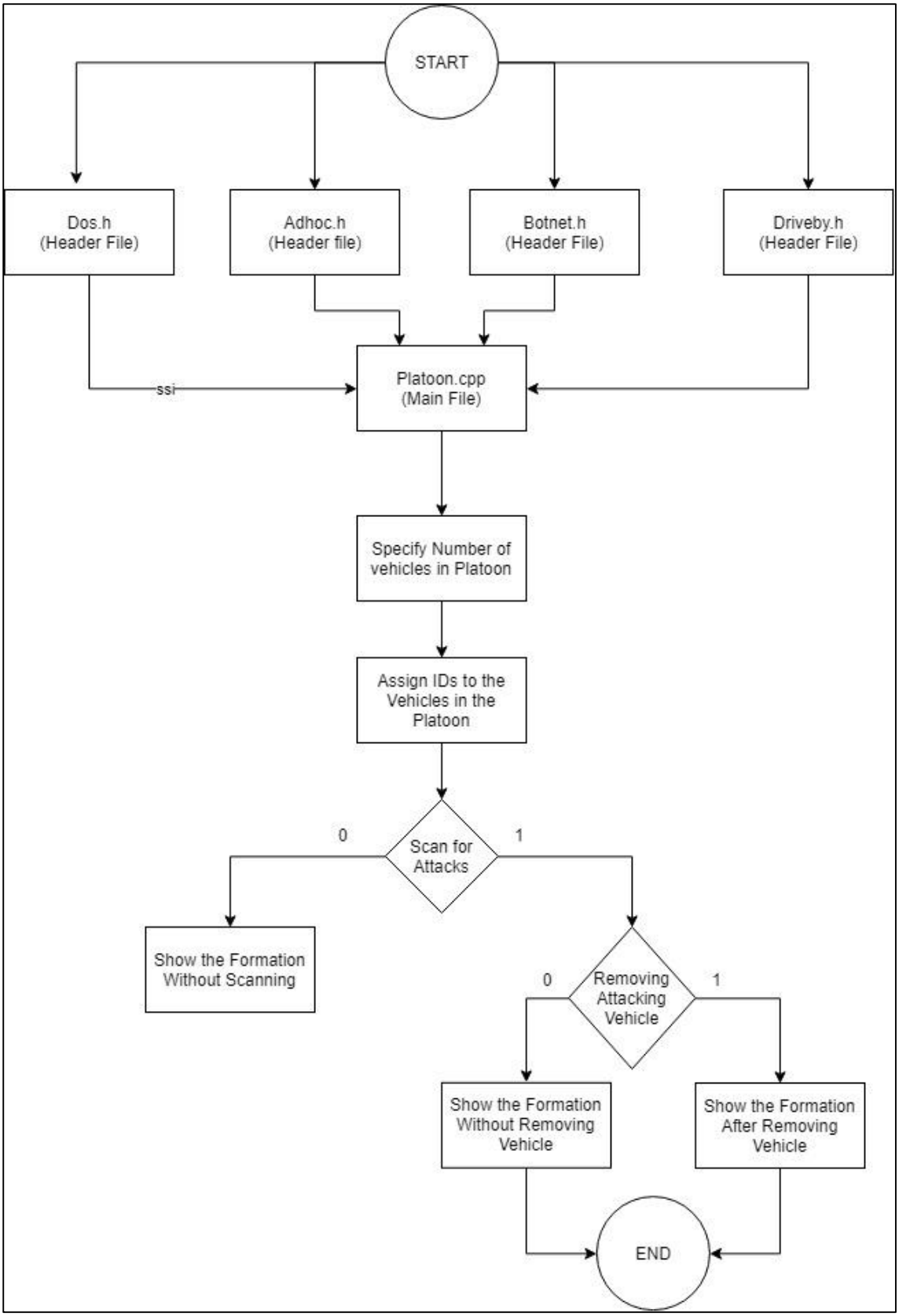


**Figure 4.9:** Program Execution.

# 5. CONCLUSIONS

## 5.1 OUTSIDE ATTACK

In term of outside attacks, we have taken steps to explained how to overcome (sybil, dos, delay) attacks with some security algorithms such as encryption, hashing and message authentication code. Our result show that these techniques can efficiency solve these attacks. To ensure the validity of these steps we have set up a simulation system to measure the extent and number and timing of the impact of vehicles attacks. The result shows that the most serious attack is sybil attack followed by the DOS then comes in the last rank in terms of direct risk is timing attack as shown in Figure 5.1 and Figure 5.2.

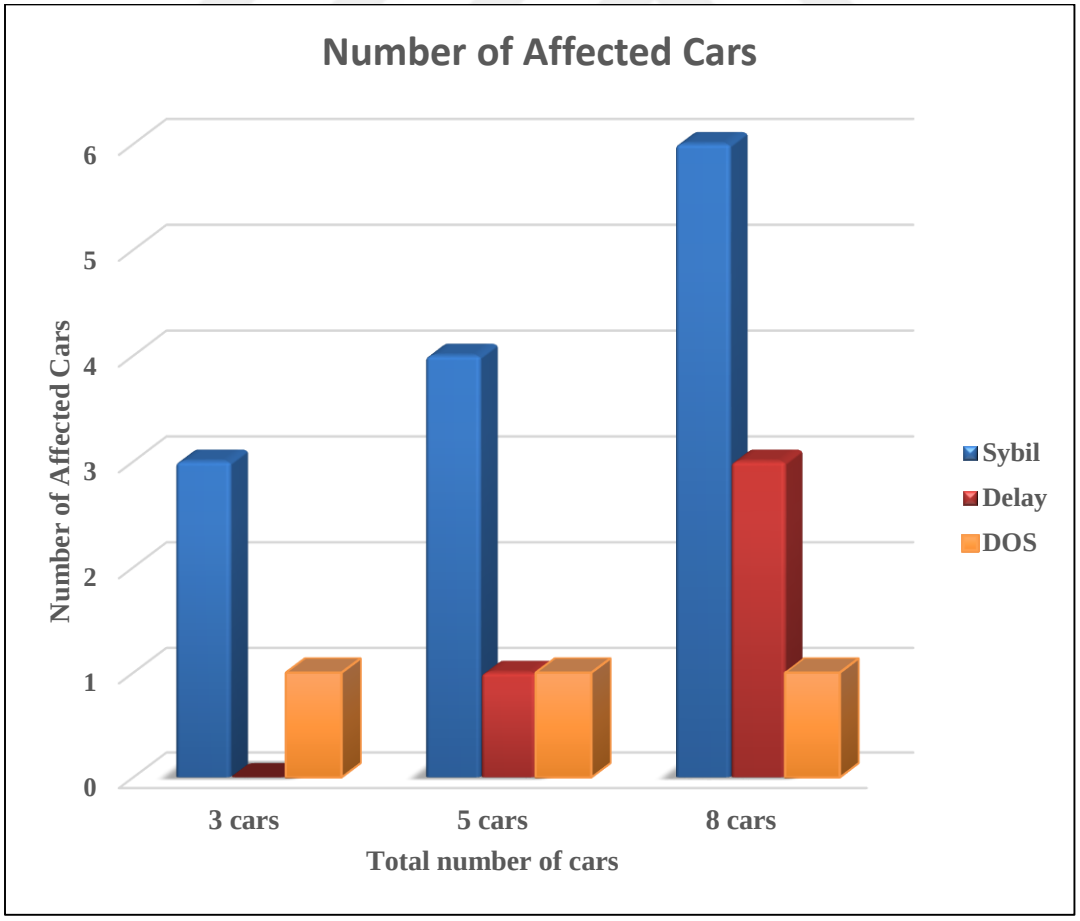


**Figure 5.1:** Statistical Diagram of Affected Cars for Each Attack.

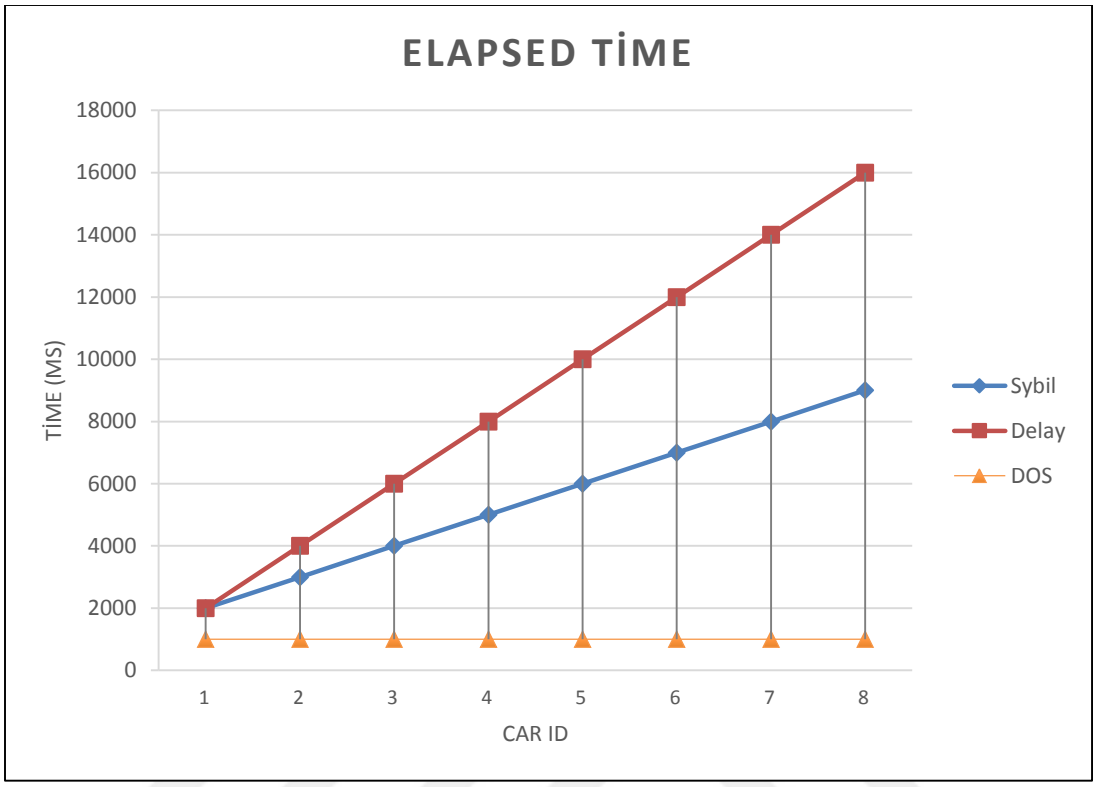


**Figure 5.2:** Statistical Diagram of Elapsed Time in ms For Each Attack.

## 5.2 INSIDE ATTACK

In term of inside attacks, we proposed a way to deal with secure vehicle confirmations and congruity into a platoon by checking physical setting using linked list. Linked list is novel since it use inborn arbitrariness from different vehicles unit and traffic conditions to independently bootstrap a mutual cryptographic key that is utilized by vehicles to safely tie physical setting of different attacks (i.e. dos attack, botnet attack, ad-hoc attack and drive-by attack), or region data to advanced identifiers, or testaments. We executed and assessed the linked list-based check conspire against genuine attacking information gathered from distinct header files of attack type and vehicle information. We exhibited the achievability of adequately separating between contiguous vehicles utilizing C++ programming language which works on low-level comparative to other programming language for verifying the type attack and vehicle information in the platoon. The result shows the program ability to detect the attack, identify the malicious actor

position and secure the platoon from those attackers by eliminate the threat and re-arrange the platoon efficiently.

Figure 5.3 show the time of execution for each attack. In this approach (inside attack) we consider four different attacks (Botnet attack, DoS attack, Ad-hoc attack and Drive-by attack), these attacks consider the most dangerous attacks facing the platooning system.

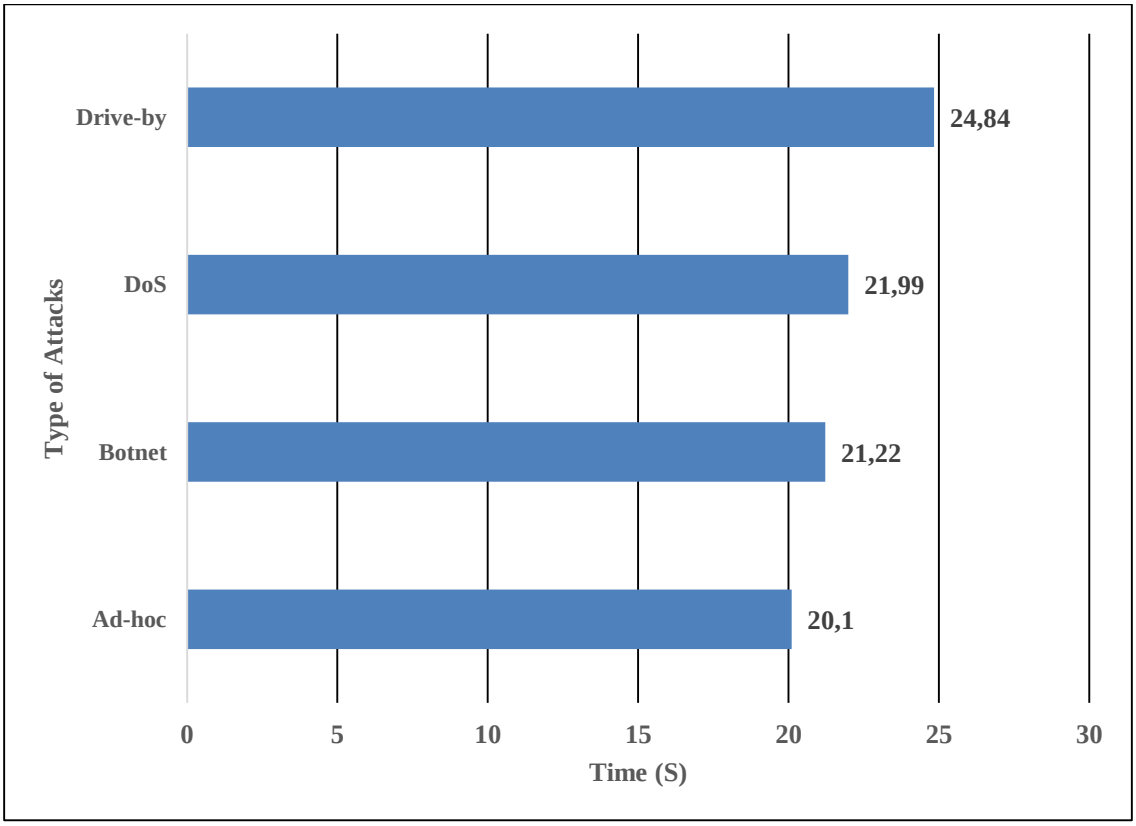


**Figure 5.3:** Time of The Program Executing For Each Attack.

## 5.3 FUTURE WORK

The project has successfully evaluated the security breaches in vehicle platooning and expanding the possibilities of developing scenarios to test these attacks. Therefore, the following proposals for future research are recommended:

- Future design should be more customizable to include other aspects of the vehicle platoon by accommodating customizable simulation parameters. The customization will allow the inclusion of the recommended changes to counter attacks.
- A user-friendly interface can be used for simulating and defining the elements of the vehicle platoon.
- Specialized research into the nature and effects of the various attack modes is recommended. Each attack scenarios should be specially studied and researched where scenario of occurrence being evaluated to create a robust understanding of their effects and security requirements.

In vehicular system there are two types of communications (vehicle to vehicle and vehicle to infrastructure). The infrastructure provides the platoon with sensitive information including road condition, weather condition and shortest path etc. Future work will focus on the threats that facing the infrastructure and its ability to destroy the stability of the platoon by detecting these threats and secure the platoon from any possible threats.

## REFERENCES


[1] V. L. Hybrid, “IEEE 802.11p and Visible Light Hybrid Communication Based Secure Autonomous Platoon,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8667–8681, 2018.

[2] T. Cevik, S. Yilmaz, and E. Engineering, “AN OVERVIEW OF VISIBLE LIGHT,” vol. 7, no. 6, pp. 139–150, 2015.

[3] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” Ad Hoc Networks, vol. 61, pp. 33–50, 2017.

[4] S. Rehman, M. A. Khan, T. A. Zia, and L. Zheng, “Vehicular Ad-Hoc Networks ( VANETs ) - An Overview and Challenges,” vol. 3, no. 3, pp. 29–38, 2013.

[5] A. Yasser, M. Zorkany, N. A. Kader, and A. Yasser, “ELECTRICAL & ELECTRONIC ENGINEERING | RESEARCH ARTICLE VANET routing protocol for V2V implementation : A suitable solution for developing countries,” *Cogent Eng.*, vol. 4, no. 1, pp. 1–26, 2017.

[6] T. J. S. Chowdhury, C. Elkin, V. Devabhaktuni, D. B. Rawat, and J. Oluoch, “Advances on localization techniques for wireless sensor networks : A survey,” vol. 110, pp. 284–305, 2016.

[7] S. Ucar, S. C. Ergen, and O. Ozkasap, “Visible light communication in vehicular ad-hoc networks,” in *2016 24th Signal Processing and Communication Application Conference (SIU)*, 2016, pp. 881–884.

[8] T. Rosenstatter and C. Englund, “Automated Vehicle Control System,” pp. 1–11, 2017.

[9] B. Chen, “A cooperative control method for platoon and intelligent vehicles management,” pp. 1–5, 2017.

[10] A. Petrillo, A. Pescap, and S. Santini, “A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks,” pp. 110–115, 2017.

[11] M. Y. Abualhoul, M. Marouf, O. Shagdar, and F. Nashashibi, “Platooning Control Using

Visible Light Communications : A Feasibility Study," no. Itsc, pp. 1535–1540, 2013.

[12] H. Phuoc, D. Nguyen, and R. Zoltán, "The Current Security Challenges of Vehicle Communication In The Future Transportation System," no. January 2019, 2018.

[13] K. Orkun and V. Erol, "Network Security Issues and Solutions on Vehicular Communication Systems," no. June, 2017.

[14] S. Zhao, T. Zhang, N. Wu, H. Ogai, and S. Tateno, "Vehicle to Vehicle Communication and Platooning for EV with Wireless Sensor Network," pp. 1435–1440, 2015.

[15] X. U. S. H. S. Hen and U. N. O. F. W. Aterloo, "Complementing Public Key Infrastructure To Secure Vehicular AD HOC Networks Albert Wasef And Rongxing L U , University Of Waterloo," no. October, pp. 22–28, 2010.

[16] S. Santini, A. Salvi, A. S. Valente, and A. Pescap, "A Consensus-based Approach for Platooning with Inter-Vehicular Communications," no. PON04a3 00058, pp. 1158–1166, 2015.

[17] M. Segata *et al.*, "Toward Communication Strategies for Platooning : Simulative and Experimental Evaluation," vol. 64, no. 12, pp. 5411–5423, 2015.

[18] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, and J. Rowe, "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving," *IEEE Commun. Mag.*, vol. 53, no. June, pp. 126–132, 2015.

[19] R. Van Der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (CACC)," IEEE Veh. Netw. Conf. VNC, vol. 2018-January, pp. 45–52, 2018.

[20] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A Security Credential Management System for V2V Communications," pp. 1–8, 2013.

[21] H. Menouar, "Visible Light Communication," no. december, pp. 45–53, 2015.

[22] H. Tseng, Y. Wei, A. Chen, H. Wu, H. Hsu, and H. Tsai, "Characterizing Link Asymmetry in Vehicle-to-Vehicle Visible Light Communications," pp. 88–95,

2015.

[23] P. Luo, Z. Ghassemlooy, H. Le Minh, and E. Bentley, “Performance analysis of a car-to-car visible light communication system,” no. March, 2015.

[24] S. Ucar, B. Turan, S. Colen, O. Ozkasap, and M. Ergen, “Dimming Support for Visible Light Communication in Intelligent Transportation and Traffic System,” pp. 1193–1196, 2016.

[25] M. Poonam Barua and M. Sanjeev Indora, “International Journal of Computer Science and Mobile Computing Overview of Security Threats in WSN,” 2013.

[26] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, “Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA),” in *2013 International Conference on Information Communication and Embedded Systems (ICICES)*, 2013, pp. 237–240.

[27] M. Ghosh, A. Varghese, A. A. Kherani, and A. Gupta, “Distributed Misbehavior Detection in VANETs,” in *2009 IEEE Wireless Communications and Networking Conference*, 2009, pp. 1–6.

[28] C. Kolias, G. Kambourakis, and S. Gritzalis, “Attacks and Countermeasures on 802.16: Analysis and Assessment,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 487–514, 2013.

[29] M. M. Joe, R. S. Shaji, and K. A. Kumar, “Computer Network and Information Security,” *Comput. Netw. Inf. Secur.*, vol. 8, no. 8, pp. 55–61, 2013.

[30] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, “Classification of Security Attacks in VANET: A Review of Requirements and Perspectives,” *MATEC Web Conf.*, vol. 150, p. 06038, Feb. 2018.

[31] Deeksha, A. Kumar, and M. Bansal, “A review on VANET security attacks and their countermeasure,” in *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, 2017, pp. 580–585.

[32] V. Nampally and M. Raghavender Sharma, “A Survey on Security Attacks for VA

-NET" IJCSMA. Vol.5 Issue. 10, October- 2017, pg. 58-70

[33] A. Malla and R. K. Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET." 2013.

[34] "How Sensor Fusion for Autonomous Cars Helps Avoid Deaths on the Road" [online]. Availible: https://www.intellias.com/sensor-fusion-autonomous-cars-helps-avoid-deaths-road/

[35] I. A. Sumra, I. Ahmad, H. Hasbullah, and others, "Classes of attacks in VANET," in Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, 2011, pp. 1–5.

[36] V. L. Le, I. Welch, X. Gao, and P. Komisarczuk, "Anatomy of drive-by download attack," Conf. Res. Pract. Inf. Technol. Ser., vol. 138, no. Aisc, pp. 49–58, 2013.

[37] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, "IoDDoS -The internet of distributed denial of sevice attacks A case study of the mirai malware and IoT-Based botnets," IoTBDS 2017 - Proc. 2nd Int. Conf. Internet Things, Big Data Secur., no. IoTBDS, pp. 47–58, 2017.

[38] Electricity Information Sharing and Analysis Center(E-ISAC), "Analysis of the Cyber Attack on the Ukrainian Power Grid Table of Contents," 2016.

[39] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.

[40] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," IEEE Veh. Technol. Conf., pp. 2036–2040, 2008.

[41] B. Jayaraman, J. M. Kannimoola, and K. Achuthan, "Sybil attack detection in vehicular networks," *Secur. Priv. Internet Things Model. Algorithms, Implementations*, vol. 2, no. 4, pp. 35–51, 2016.

[42] X. Bin, Y. Bo, and G. Chuanshan, "Detection and localization of sybil nodes in VANETs," *DIWANS 2006 - Proc. 2006 Work. Dependability Issues Wirel. Ad Hoc*

*Networks Sens. Networks (part MobiCom 2006)*, vol. 2006, pp. 1–8, 2006.

[43] A. M. Malla, "Security Attacks with an Effective Solution for DOS Attacks in VANET," *Int. J. Comput. Appl.*, vol. 66, no. 22, pp. 45–49, 2013.

[44] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-Hoc networks: Evaluating the impact of attackers' strategies," *Sensors (Switzerland)*, vol. 18, no. 11, pp. 1–19, 2018.

[45] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J.-C. Tsou, "Man-in-the-middle-attack: Understanding in simple words," *Int. J. Data Netw. Sci.*, no. January, pp. 77–92, 2019.

[46] M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla, "Congestion Attacks to Autonomous Cars Using Vehicular Botnets," 2015.

[47] M. T. Garip, P. Reiher, and M. Gerla, "Ghost: Concealing vehicular botnet communication in the VANET control channel," *2016 Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2016*, pp. 1–6, 2016.

[48] A. Niki, *IT Security Conference for the Next Generation DRIVE-BY DOWNLOAD ATTACKS : EFFECTS AND DETECTION METHODS Aikaterinaki Niki MSc Information Security , 2008-2009 Royal Holloway University of London Author :*, vol. 44, no. 0. 2009.

[49] M. Egele, E. Kirda, and C. Kruegel, "Mitigating drive-by download attacks: Challenges and open problems," *IFIP Adv. Inf. Commun. Technol.*, vol. 309, pp. 52–62, 2009.