Technical Solutions inV2X

Objective

- Applications
- Security issues and Attacks

Introduction

purpose of V2X technology is to improve road safety, energy savings, and traffic efficiency on the roads.

In this lesson, we discuss the security challenges and requirements in V2X

Learning Outcomes

At the end of this lesson, students are expected to:

- Enumerate the types of Applications
- Describe each type of Security Challenges
- Infer why some areas are more vulnerable to use v2x technology

What are the Applications and Challenges in v2x?

Applications

traffic management applications, road safety applications and comfort and infotainment applications

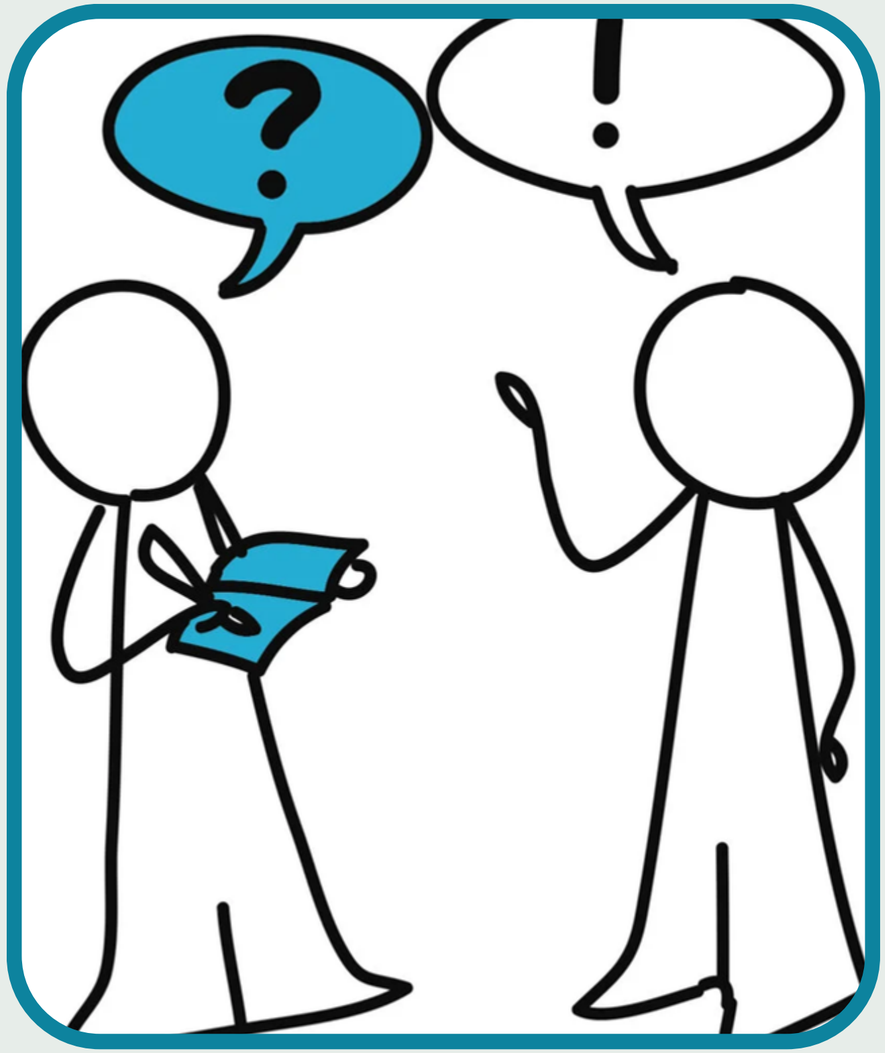
Challenges

User's Trust and Privacy, Attack Prevention, Data Priority, Adoption to Future Platforms,Communication Latency

Problem Statement

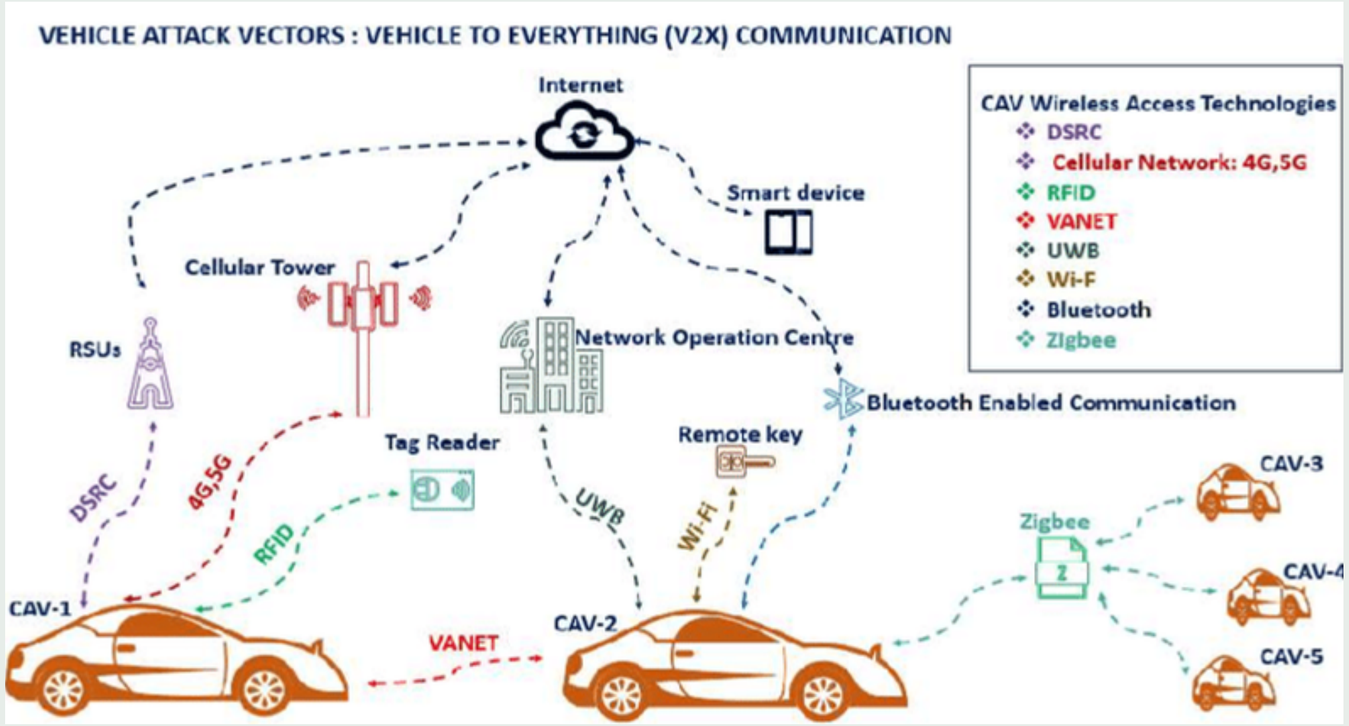
What are the technical issues in traffic management in modern world

we present a comparative study of the different attacks on V2X



Attacks in V2X

There basis of five categories:
1. Attacks based on the behavioral
2. Attacks on software and hardware
3. Attacks on infrastructure
4. attacks on privacy
5. Data trust attacks



Attacks based on Behavioral Patterns

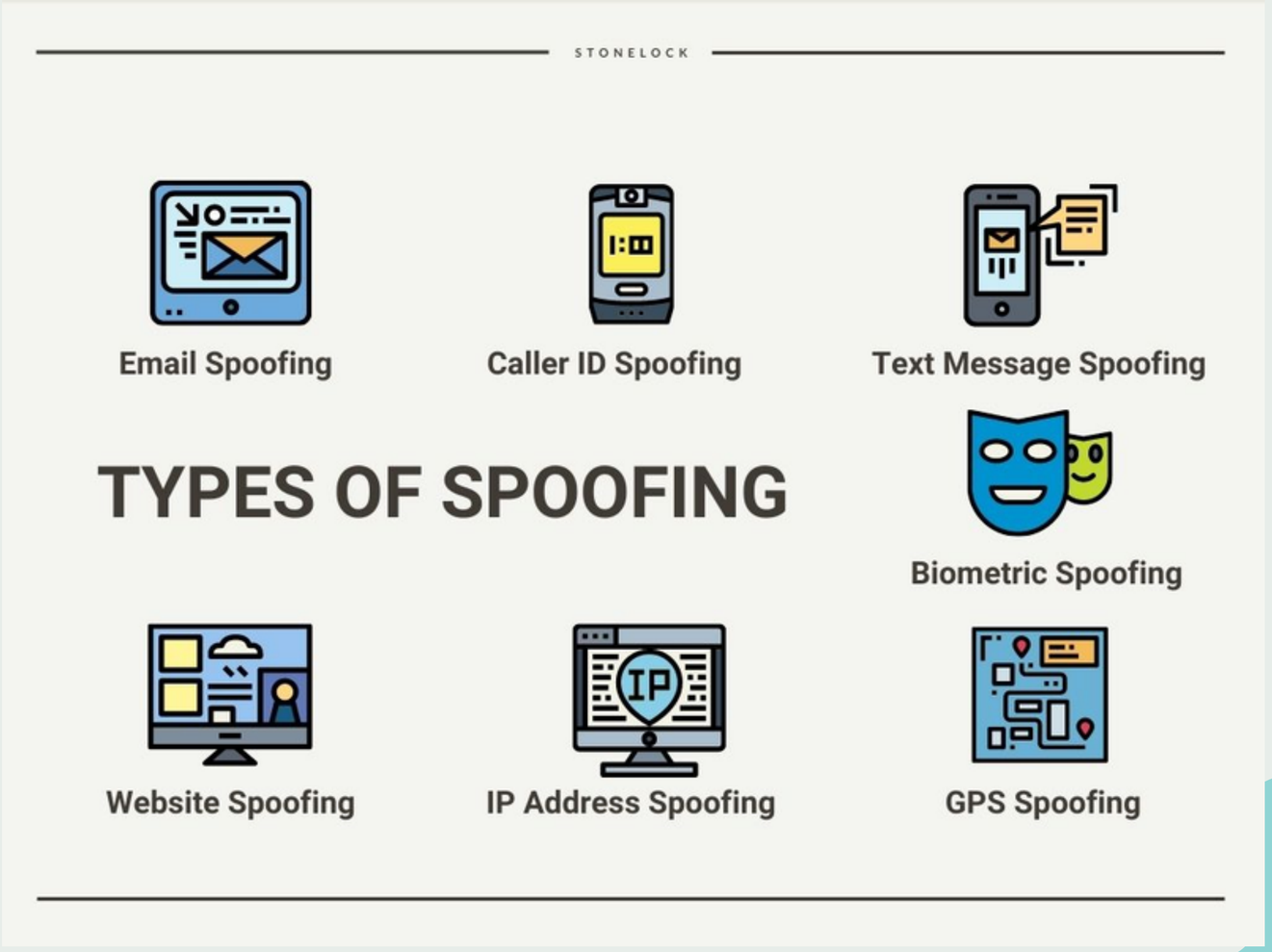
There are two types:
1.Selfish Attack
These attacks perform selfish behaviour where nodes may not forward 480 packets or do not perform verification function

2. Malicious Attacks:
exhibit malicious activities in the network, such as, modification and replaying of messages

Message Spoofing Attack.

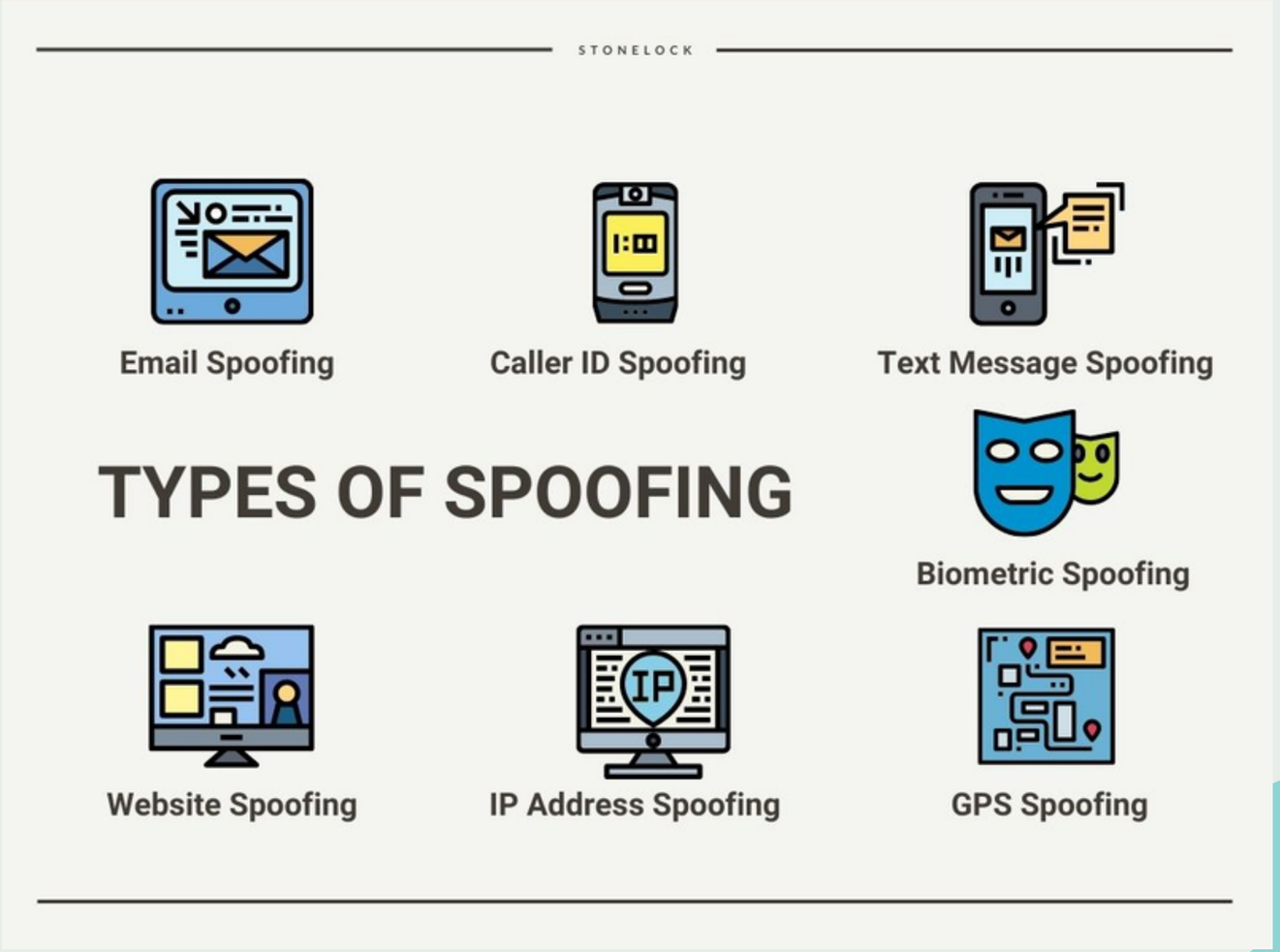
The attacker in the spoofing attack provides incorrect location information to the vehicles in the network.

Spoofing attacks may facilitate other attacks where vehicle identification is used as the tool for launching attacks.



Solution for Message Spoofing Attack.

For defending message spoofing attack, the possible solutions are using vehicular public key infrastructure for communication between vehicles, or by using sign warning messages or forming group communications, or by including a non-cryptographic checksum with each sent message and applying plausibility checks on the receiving message. or by using cryptographic certificate or on-board radar, for assisting the vehicle in detecting the actual position of malicious vehicles.



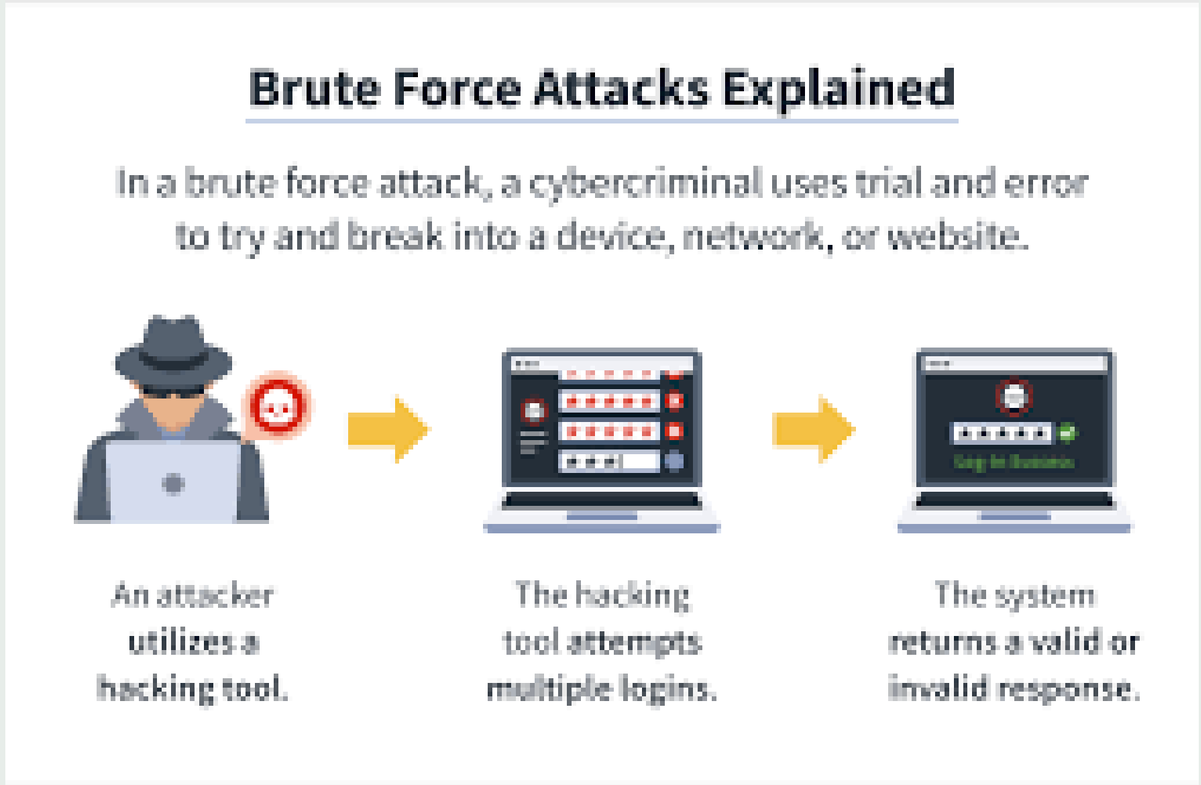
Did You Know?

Libya by far has the highest incidence of car accidents anywhere in the world
At a rate of 73.4 deaths per 100,000 people
the highest death tolls tend to be in African countries, and the lowest in European countries

Brute Force Attack

This type of attack is tough to execute in vehicular networks, due to resource constraints and short connection times, still it can affect such networks in certain scenarios.

The confidentiality of messages and authentication processes may be hampered by launching brute force attacks.



Solution for Brute Force Attack

As brute force attacks are not a vulnerability per se, keeping the software up to date is not enough to protect yourself.
Here are few common methods to prevent these attacks:

Use Strong Passwords

Restrict Access to Authentication URLs

Limit Login Attempts

Use CAPTCHAs

Use Two-Factor Authentication (2FA)

Session Hijacking Attack.

the hackers control the session among nodes resulting in what is known as the session hijacking attack.

Solution for
Session Hijacking Attack.

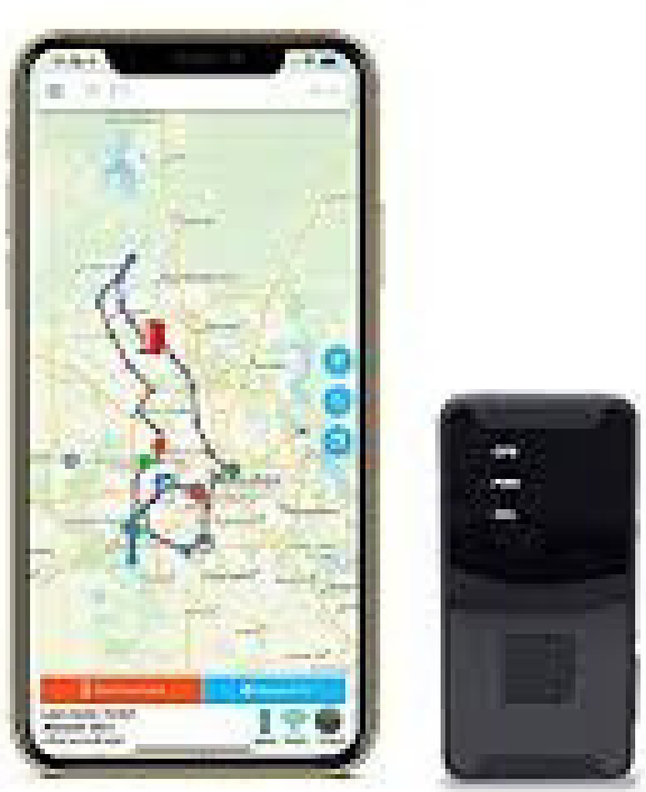
First, we will no about session hijacking?
what is session hijacking?
The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections.

Defensive mechanisms for session hijacking attacks include the use of trust authority and public key infrastructure. The trust authority is aware of the actual identity of every node. Every time a vehicle communicates with a RSU initially validates its identity through the trust authority and subsequently shares the key with the vehicle.

Location Tracking

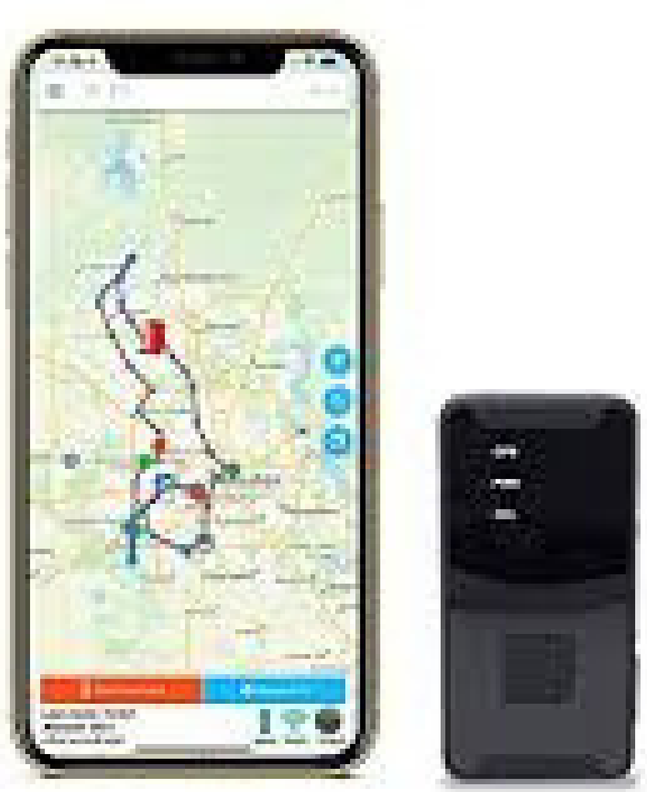
Tracks the location and path followed by the vehicle

It effects the privacy of the user



Solution for Location Tracking

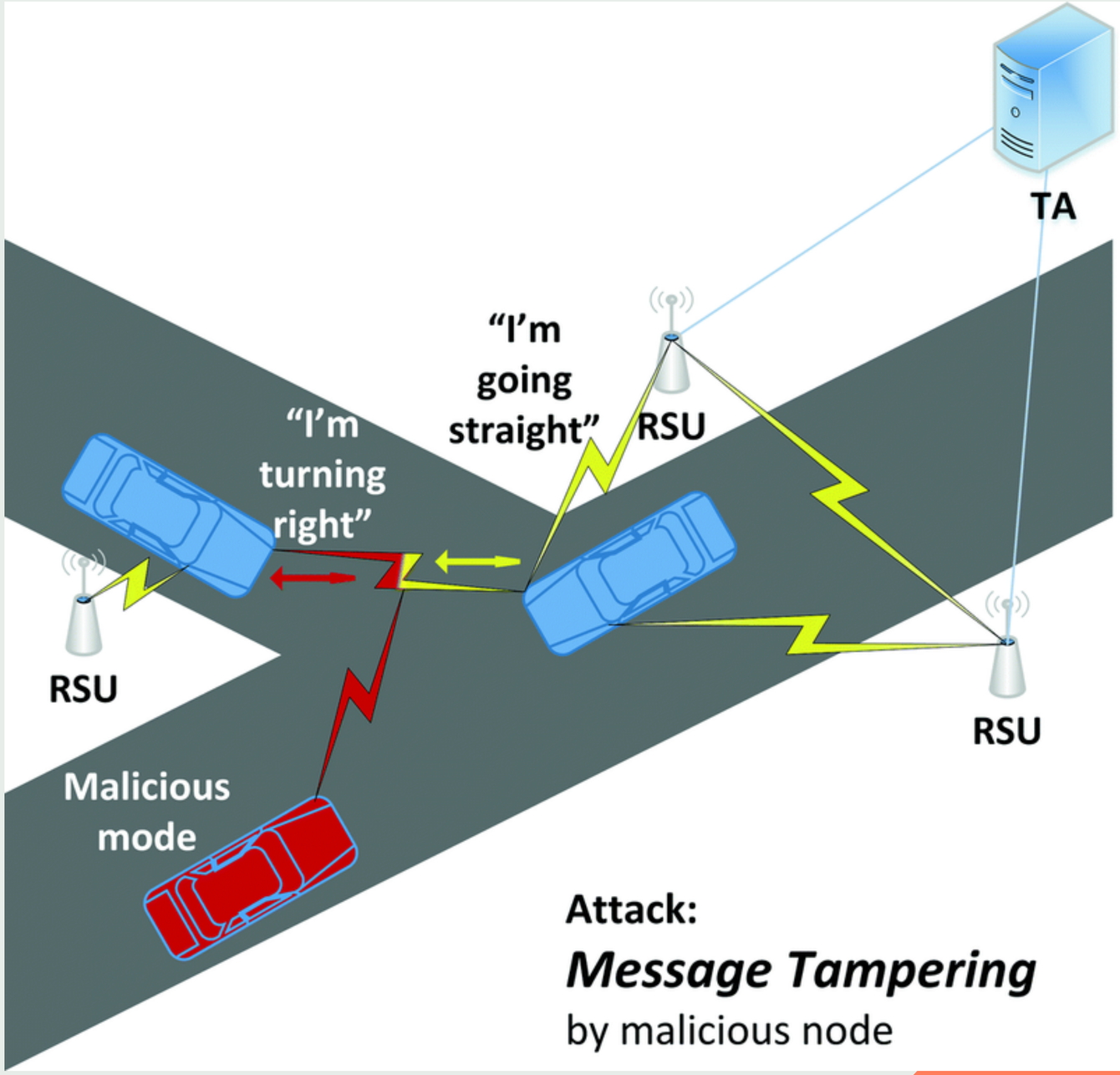
The identity of the user is hidden from illegal access through anonymous and temporary keys. Therefore, the location privacy of the vehicle is maintained and the trajectory of the node cannot be tracked by malicious nodes.



Message Tampering

This attack results in modifying, altering, deleting or constructing the data that is already present

It is a Threat to hardware and software



Solution for
Message Tampering

Review

V2X Technology

Vehicle to Everything (V2X) is a vehicular communication system that supports the transfer of information from a vehicle to moving parts of the traffic system that may affect the vehicle

The main purpose of V2X technology is to improve road safety, energy savings, and traffic efficiency on the roads. The main components of Vehicle to Everything (V2X) include vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication systems.

Reference

https://en.wikipedia.org/wiki/List_of_countries_by_traffic-related_death_rate#cite_note-WHOMap-9
https://corporatefinanceinstitute.com/resources/knowledge/other/vehicle-to-everything-v2x/

THANKYOU