

# IoT devices hacking: Car Hacking

Bashayer Alsharif 4210396

Wafa Habeeb 4210618

Khadija Khan 4111576

Maha Alghamdi 4010134



The background image depicts a person wearing a dark hoodie, their hands positioned as if interacting with a futuristic, glowing digital interface. The interface is composed of several elements: a large, semi-transparent wireframe of a car is visible on the right side; various data visualizations, including bar charts and line graphs, are scattered across the interface; a circular gauge or progress indicator is on the left; and a cluster of hexagonal icons with different symbols (like a cloud, a checkmark, and a question mark) is at the bottom right. The overall aesthetic is high-tech and cybernetic, with a color palette dominated by dark blues, greys, and bright, glowing cyan and orange highlights. In the top left corner, there is a small, solid orange rectangular bar.

# Introduction to Car Hacking:

What is Car Hacking?





# Types of Vehicle Attacks

## - Wireless Attacks

Hackers can remotely exploit vulnerabilities in a vehicle's wireless communication systems, such as Bluetooth or Wi-Fi.

## 1 Replay Attack

A **replay attack** is a type of attack in which an attacker captures valid communication data and retransmits it to impersonate a legitimate signal.

## 2 Remote Start Attack

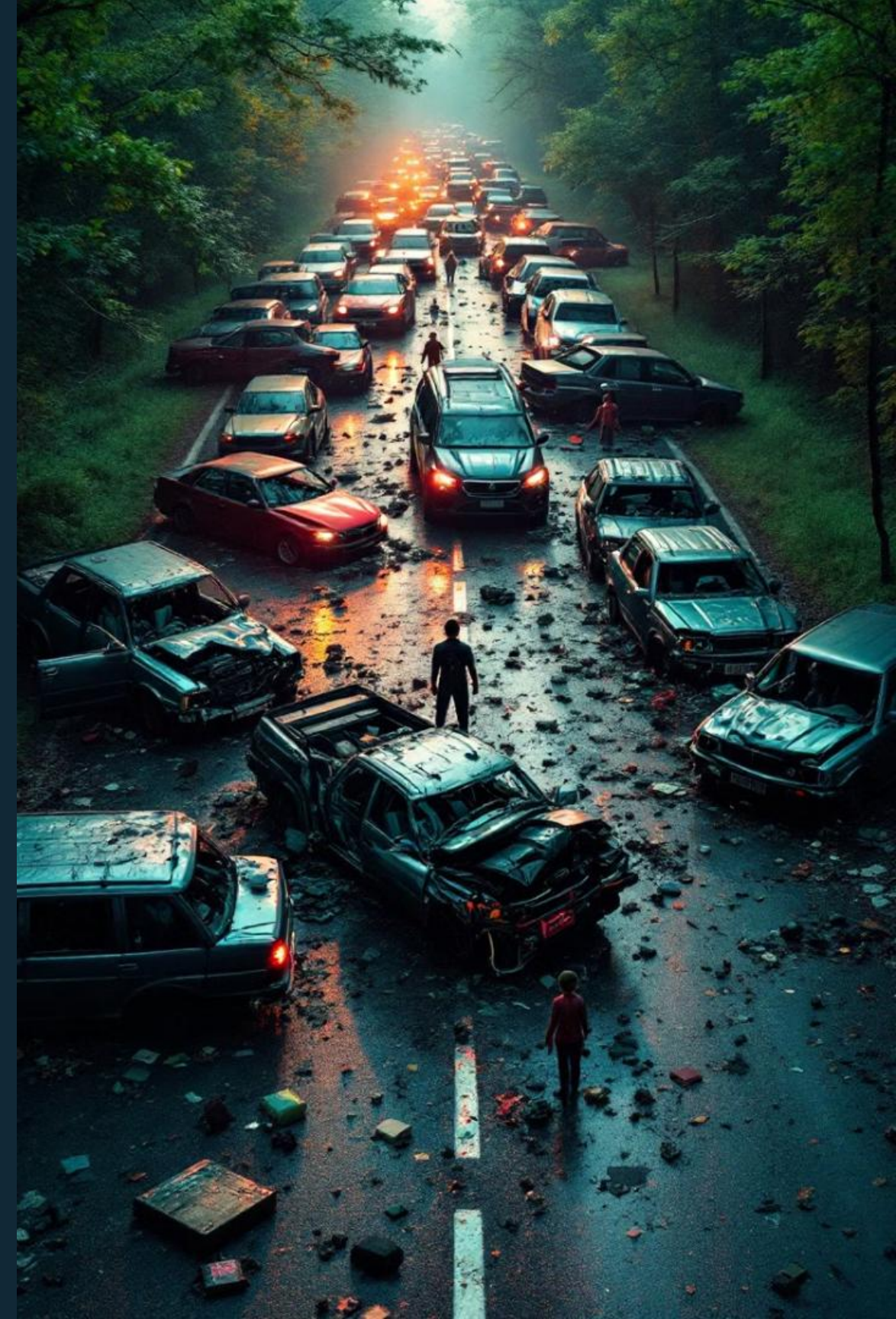
A **remote start attack** is a cyberattack that exploits vulnerabilities in a vehicle's remote start system, allowing an attacker to start the car's engine without proper authorization.



# Future work:

## Jamming Attack:

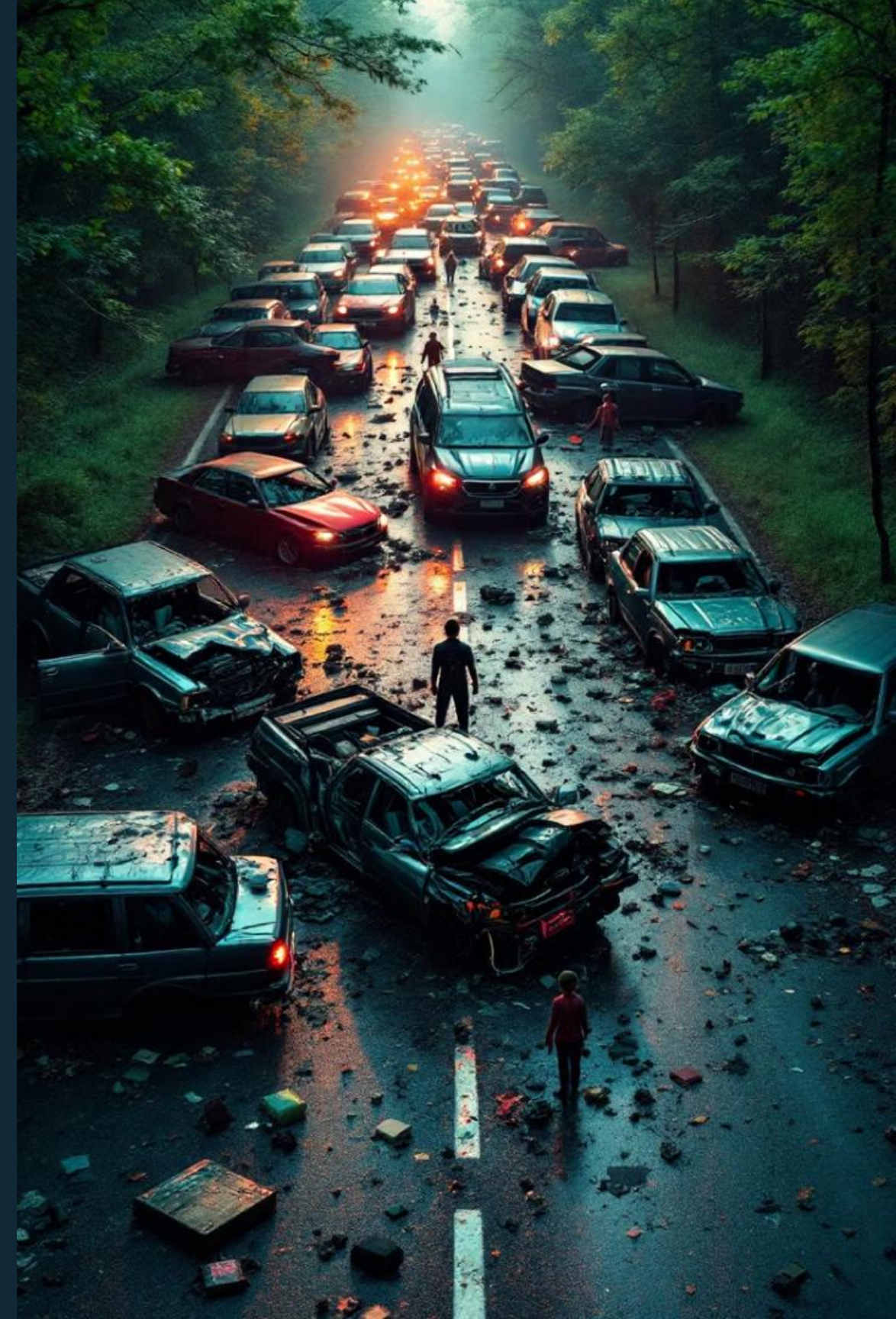
A **jamming attack** involves disrupting wireless communication by emitting interference signals.





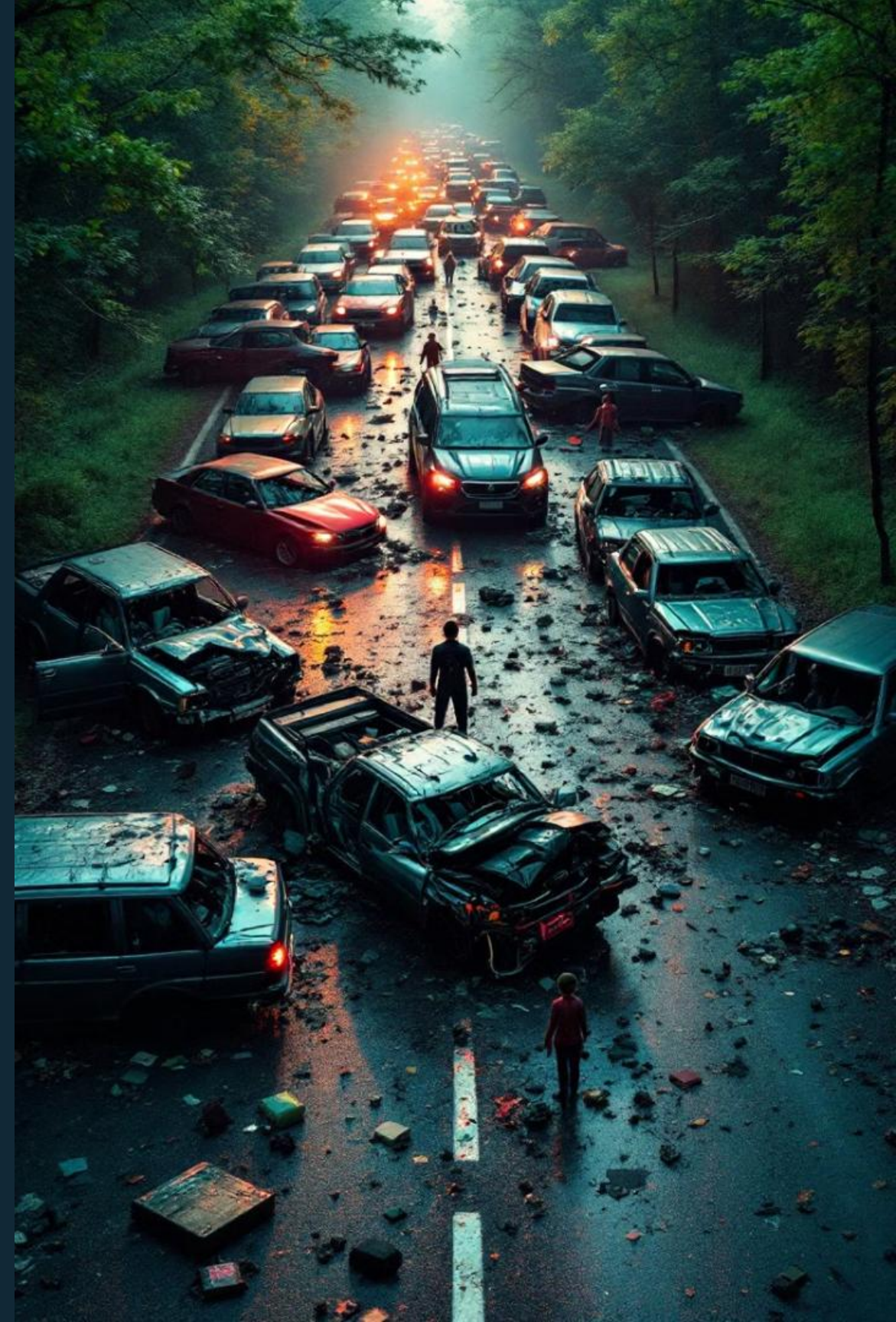
# Types of car used:

- Mercedes-Benz
- Toyota Innova
- Toyota Land Cruiser





Demo:





Thank you for  
listening!

