**1.Eavesdropping attacks:** Eavesdropping attacks happen when people who aren't supposed to, can listen in on car messages.[1] Since the car network sends out messages for anyone on the network to see, once these attackers get into the car's network, they can secretly listen to these messages. They can even start to notice regular patterns in the messages that are supposed to be private.

Data that do not match the rest of the dataset's data are known as outliers [2]. Anomalous data concealed within a typical data collection is identified by outlier detection. Anomaly detection is comparable to a classification challenge in certain ways. There are two types of network flow: normal and aberrant. Finding the most suitable type for the observed data stream is our aim. The conclusion that follows is that anomaly detection works better at identifying variants of known assaults than it does at identifying new malicious activities.[3].In this situation, the system can be taught using frequent background traffic and known attack samples to facilitate a more dependable decision-making process.

**2. TPMS Exploitation:**

The Tire Pressure Monitoring System (TPMS), which lack of crucial security measures, is a well-documented target for attack. One can target the tire pressure monitoring system (TPMS) passively or actively. The TPMS interfaces with the vehicle's Electronic Control Unit (ECU) and continuously checks tire pressure. While active attacks use wirelessly injected spoof signals to fool the ECU, passive attacks use captured TPMS signals to track the movement of the vehicle. False tire pressure readings may be displayed as a result of these attacks, putting the safety of the vehicle at serious risk. To overcome these vulnerabilities, countermeasures include using encrypted signal transmissions and hardware pairings.

 Approximately three miles of wire are present in modern cars, and as we add more on-board electronic components, such as entertainment systems, navigation systems, and in-car sensors, to make our cars smarter, the amount of wire in them will only grow. Car weight and wiring complexity are directly impacted by an increase in wires, which reduces fuel efficiency and makes troubleshooting more difficult. Because of this, wireless technologies will be utilized more often inside and outside of cars to gather status and control information about their electronics.

The procedures will considerably reduce the security risks associated with TMPS and include recommendations for cryptographic protocols along with relatively simple design adjustments. The creation of additional new wireless in-car sensing systems can profit from the knowledge gained. [4]

**3. Lock Picking Attack on Keyless Entry Systems:** The lock picking attack takes use of a weakness in keyless entry systems, which are commonly utilized for garage openers and automobile doors. Using a gadget that intercepts the key fob's sent signal and simultaneously transmits a jamming signal on the same frequency, the attack employs a man-in-the-middle technique. The attacker's device records the second code transmission when the key fob user attempts again, allowing it to open the door with the first code and store the second code for future illegal entry. Sales of these devices have increased despite their general availability and potential for misuse, raising worries and leading manufacturers to demand for stronger security measures.

One of the earliest methods is fixed-code RKE, in which a key fob transmits the instruction along with a predefined authentication code. While fixed-code RKE makes design and manufacturing simpler, replay assaults can easily exploit it. To put it another way, it would be quite simple for an attacker to intercept the broadcast signal, extract the predefined code, and then utilize it to get unauthorized access. In order to get around the fixed-code RKE's limitations, rolling code RKE was created [5]. Rolling-code RKE uses a synchronized counter that is kept in sync between the key fob and the receiver to determine the authentication code that the fob should broadcast at each connection attempt, or press. The fob communicates an encrypted version of the current counter value on each attempt, incrementing it once the transmission is complete. The value of the synchronized counter is retrieved by the receiver using code decryption, and it is then compared to the value of its own counter. The receiver's counter value is increased and the fob is verified to execute the desired action if both matches. It is important to remember that the secret key that is needed for both encryption and decryption is never shared. The receiver matches not only the current counter value but also a few more following ones in order to resolve this issue. To get back into in sync, the receiver changes the counter value in accordance with any matches it discovers. Lastly, the code will be rejected and the fob will not be verified if the recipient receives a counter value that is less than expected.

**4. Road Infrastructure Attacks:** Road infrastructure components are now vulnerable to potential cyber-attacks due to the growing connection of automobiles. New attack vectors are presented by vehicle-to-infrastructure (V2I) connectivity, which includes components like smart traffic lights and road signs. In one famous case, networked traffic signals across several states were compromised and began to show messages indicating they had been hacked. Even though these attacks are first thought of as jokes, they have significant consequences, particularly in times of need. Tight password management and secure sensor design for V2V and V2I communications are necessary to mitigate these threats.

Implementing multiple approaches focused on at reducing potential threats is essential when solving road infrastructure security. This includes putting in place surveillance devices to keep an eye out for any odd activity. Additionally, the establishment and implementation of strict regulatory structures function as a barrier against intentional acts of damage. Campaigns for public education and awareness are essential because they give the public the skills necessary to identify and report such risks. Additionally, securing against and quickly recovering from attacks depends critically on the incorporation of technology into infrastructure design, including resilience-enhancing elements. To create a safe and responsive environment for road infrastructure, law enforcement, governmental organizations, and the community must work together.

**5.CAN Bus Specific Attacks:**

Cars can be vulnerable to attacks if someone gets access:

**CAN Sniffing:** This is when attackers quietly watch the data moving through the car's CAN system. They use special tools to understand this data and can then create fake messages that look real.

**CAN Fuzzing:** In this case, attackers send random data to the car's CAN system to see what happens. This can cause unexpected changes, like the car speeding up or slowing down, because the system gets confused by the strange messages.

There are various ways to defend against assaults on CAN bus systems in automobiles. Encrypting data transferred over the CAN bus is a crucial strategy to prevent attackers from understanding or replicating the messages. Strict access control implementation can also restrict who is able to connect to the CAN system, lowering the possibility of unwanted access. Frequent monitoring and anomaly detection can aid in the early detection of aberrant behavior, enabling prompt intervention.[6] Lastly, increasing general security can be achieved by teaching car mechanics and users about these threats and countermeasures.

**References**

[1] J. Liu, W. Sun, Yongpeng Shi, In-vehicle network attacks and countermeasures: challenges and future directions, IEEE Netw. 31 (2017) 50–58.

[2] H. C. Mandhare and S. R. Idate, ‘‘A comparative study of cluster based outlier detection,distance based outlier detection and density based outlier detection techniques,’’ in Proc. Int. Conf. Intell. Comput. Control Syst. (ICICCS), Jun. 2017, pp. 931–935.

[3] Learning Based Adaptive Network Immune Mechanism to Defense Eavesdropping Attacks MINGYUAN LIU, DEYUN GAO, GANG LIU, (Student Member, IEEE), JINGCHAO HE, LU JIN, CHUNLIANG ZHOU, AND FUCONG YANG

[4] Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study Ishtiaq Roufa, Rob Millerb, Hossen Mustafaa, Travis Taylora, Sangho Ohb Wenyuan Xua, Marco Gruteserb, Wade Trappeb, Ivan Seskarb ∗ a Dept. of CSE, Univ. of South Carolina, Columbia, SC USA

[5] A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic. Kyle Greene, Deven Rodgers, Henry Dykhuizen, Quamar Niyaz, Khair Al Shamaileh, Vijay Devabhaktuni Purdue University Northwest. JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015

[6] Cybersecurity attacks on CAN bus-based vehicles: a review and open challenges. Faten Fakhfakh, Mohamed Tounsi, Mohamed Mosbah Library Hi Tech ISSN: 0737-8831 Article publication date: 12 August 2021