Automotive Network Cybersecurity through Artificial Intelligence

JAYENDRAN G
TATA ELXSI

Network Connectivity has enabled automobiles to add a significant amount of features and functionality to the vehicle. Security of the data and communication is a significant attendant risk. In addition to the traditional security techniques, Artificial Intelligence and Machine Learning (AI/ML) could be useful in adding cybersecurity features to a connected car.

Different Types of Automotive Networks

A typical vehicle has multiple networks.

1. Controller Area Network (CAN) is a bus protocol that enables the communication between in-vehicle sub-systems. The information exchanged between these sub-systems can be used to communicate with, configure, and control various car parts. In some cases, FlexRay or Ethernet might also be used for in-vehicle networks.
2. The Telematics Network includes those information-intensive components that enable various applications by combining Telecommunications and Informatics. These include Remote Vehicle maintenance, Fleet management, emergency assistance, Location-based services, advanced driver assistance systems, etc. This is part of the Connected Car network where the automobile is connected to one or more servers, typically over a cellular wireless network.
3. Vehicle-to-vehicle and Vehicle-to-Infrastructure networks, referred to by the umbrella term Vehicle-to-everything (V2X networks), are peer-to-peer networks that enable enhanced collision avoidance, vehicle safety, traffic efficiency, etc. Again, this would be over an external network to the outside world as, for example, a wireless network.

All of these networks are interconnected, and data continuously flows from one to the other.

Figure 1: Intelligent Connected Vehicle

Security Challenges and Threats:

In 2015, Charlie Miller and Chris Valasek demonstrated that it was possible to remotely hack into a running Jeep Cherokee from several hundreds of miles away and take control of its operation. They were able to disable the transmission and abruptly engage the brake. Earlier this year (2020), hackers could gain control of an autonomously driven Tesla car and accelerate it significantly.

These are just examples of cyber-attacks that threaten a vehicle's security and passengers and others' safety. There are many ways in which these attacks happen. Malware, short for malicious software, has gained unauthorized access to a car network and has been installed in one or more of its sub-systems. With multiple remote applications connecting to the car and communicating to various sub-systems, there is always room for malware installed within the vehicle. This malware may then continuously operate within the vehicle network, either providing confidential information to a third party or denote a potentially dangerous set of actions that might threaten the safety of the vehicle and its passengers. A denial-of-service attack

would systematically use up a vehicle network's resources, typically by sudden flooding with traffic, thus denying network access to legitimate vehicle sub-systems. Identity exploits would help malicious users gain unauthorized access to various parts of the vehicle network.

The increasing complexity of vehicles and the progressive use of more and more software to control or enhance the functionality of sub-systems within a vehicle increases the attack surface, which is the number of different vehicle points that are vulnerable to a cyber-attack.

A significant challenge is the so-called "zero-day attack," which is an attack that exploits a vulnerability that may not have been identified earlier. The pattern of such an attack would not be known, and no defense would have been planned for it. A conventional software solution is impossible for a zero-day attack since no detail about the attack is known a priori. Only an AI/ML solution is possible, which can learn the normal patterns of data and detect anomalies in the network data. The anomaly detected could be a malicious activity or a rare type of activity which need not necessarily be malicious. The alerts from the AI-based anomaly detection model serve as way of shortlisting network data to be further inspected by Security Experts. It would otherwise be impossible for Security Experts to analyse the entire volume of data collected from an automobile network without a mechanism to shortlist potential malicious activities.

Data that can be analyzed:

A large amount of network traffic flows through the CAN, Telematics, and V2X networks. This network data would still follow a particular pattern of behavior. The information being exchanged within these network messages, the types of commands given to the car remotely, the remote servers being accessed, the kind of information from the car requested for monitoring purposes, etc. can be captured and analyzed. Also, logs are maintained at multiple locations, containing information regarding the various transactions between the communicating entities, the state of different sub-systems of the vehicle at other points in time, the manner of driving, etc. The different applications that the vehicle uses would maintain their log, both within the vehicle and at a server. These logs can serve as a significant information source for analyzing the vehicle's behavior at any point in time.

Network traffic data from all the vehicle networks and Sub-system and Application logs would serve as input to AI modules.

How AI/ML would work:

AI-based malicious activity detection models can be a hybrid composed of supervised classification models to detect known malwares or their minor variants and anomaly detection models to detect any anomalous activity which could be potentially malicious. Anomaly detection models have the potential to detect zero day attacks unlike signature-based traditional tools or supervised classification models. Training a supervised classification model requires labelled training data to be available. That is, we need to have a significant amount of normal network data samples and many samples of each type of malware to train a supervised classification model. Anomaly detection models on the other hand can be trained using normal data that gets captured from the network without any labelling.

The AI/ML framework for Automotive Network security would have to be such that the AI models are present within the car and remote application servers. Automotive controllers that are present in-vehicle have semiconductor support for AI/ML and data analytics. Some of the analytics can be done in-vehicle and the remaining in a remote server.

In-vehicle analytics would be done on CAN network traffic within the vehicle and log data collected. The effectiveness can be enhanced if the AI module maintains an extensive profile and detailed knowledge about each vehicular sub-system's working and performs independent and separate analytics on each one of them. This detailed, granular analytics level would enable even a slight deviation from the normal to be accurately detected.

When a vehicle communicates with a remote server, extensive data and logs are collected on the server. AI based anomaly detection models can learn normal patterns of behaviour of various components within the vehicle by training on the data collected on the server. Any pattern deviating from the normal patterns could be potentially malicious and can be detected by the anomaly detection model.

The AI models can also to be customised for particular drivers and their style of driving. This would enable the models to detect even the slightest deviation from the normal and identify potential problems.

Summary

In the end, security in an automobile is a safety question for passengers and other vehicles and pedestrians. Human lives are at stake and vulnerable to malicious intruders. The absolute power of Artificial Intelligence and Machine Learning needs to be brought to Automotive Network Cybersecurity. It is mandatory to do so as AI/ML is the only way to combat the myriad and diverse threats that make an automotive network vulnerable and help strengthen and protect them against attack. ❑

AUTHOR

Jayendran G
General Manager, Next Generation Business Unit
Tata Elxsi

Jayendran has worked on Communications technologies for over 25 years. He has led teams that have built several products in the areas of Routers and Wireless Communications and has worked with Networking & Communications OEMs and Service Providers across the world. He heads the Cybersecurity practice at Tata Elxsi.