New graph-based statistical method detects threats to vehicular communications networks

24 November 2020

Credit: Pixabay/CC0 Public Domain

Researchers at the University of Maryland, Baltimore County (UMBC) have worked to create methods for improving the safety of technologically complex vehicles. Now that the majority of new cars operate using sophisticated computing technology, they are vulnerable to malicious attacks on their networks that could lead to disastrous safety issues. Riadul Islam, assistant professor of computer science and electrical engineering, has worked with collaborators at UMBC and the University of Michigan-Dearborn to create a simple, easily adapted method for detecting the breaches in security. The research is published in the Institution of Electrical and Electronic Engineers (IEEE) publication *Transactions on Intelligent Transportation Systems*.

Currently, the most widely used intra-vehicular communications network in the automobile industry is the controller area network (CAN). This network is very simple to use, which makes it appealing for consumers and manufacturers, but this simplicity also renders it vulnerable to potential security threats.

The CAN is essentially a broadcasting network, so any entity has the ability to 'read' the messages coming from a car, and potentially send conflicting messages. It is possible to remotely control a car from another device using the CAN network. This is both a feature and a bug, enabling many new innovations, and also creating security concerns. An entity could take control of the network and send new commands to a vehicle, creating dangerous circumstances, such as disabling the breaks or causing engine failure.

The first step to completely eradicating these possible threats is detecting them. According to Islam, detecting these threats does not require extensive technology. Instead, his method involves the formulation of graph-based anomaly detection techniques that will "easily show the complex relationship between data."

Islam's team took the graphs that were made to demonstrate the data on the network and conducted a simple statistical analysis to detect intruders or threats. This method does not require costly machinery; instead, it relies on methods that are already well understood by statisticians and capable of functioning intuitively.

The main benefit of using a statistical method to detect potential threats in the CAN is that it is cost-effective by "an order of magnitude," according to Islam. "The statistical method requires less energy than machine learning or artificially intelligent methods would," he explains.

As the prospect of self-driving or heavily computerized cars becomes a reality, detecting and addressing network vulnerabilities becomes essential. Islam and his team have shown that this

task does not need to be complex or expensive to be effective. Instead, car manufacturers can maintain simplicity by using data and statistical analysis to identify threats in real time. In the future, the statistical method developed by Islam will be available digitally to best assure accessibility as vehicles are created with more functions than ever before.

More information: Riadul Islam et al, Graph-Based Intrusion Detection System for Controller Area Networks, *IEEE Transactions on Intelligent Transportation Systems* (2020). DOI: 10.1109/TITS.2020.3025685

Provided by University of Maryland Baltimore County