Use of Intrusion Detection Systems in Vehicular Controller Area Networks to Preclude Remote Attacks

Anthony J Monge, Todd Andel
University of South Alabama, Mobile, Alabama, USA

ajm902@jagmail.southalabama.edu
tandel@southalabama.edu

Abstract: Security is always at the forefront of our thoughts whether we know it or not. Mindlessly, people go about their daily lives with security a part of everything performed. Is the house door locked? Is the phone off and upside down on the table so no one can see it? Is the computer at home/work logged out and secure? However, when thinking about our vehicles, the normal person stops at locking the door. Problem is that our vehicles' electronic systems are unprotected. Vehicles today are essentially personal computers with wheels. It is arguable that vehicles are incredibly safe, but that safety is an illusion. The computers that control our cars have essentially zero security in place to protect them. It is a chilling notion to have the knowledge your brakes could be rendered useless while moving at a high rate of speed. On top of that, this could be done and leave essentially no trace it had been performed. The main crux of this insecurity is the Controller Area Network (CAN) utilized by the vehicles' electronics. This paper outlines the current vulnerabilities that vex this network system and why those issues have remained unsolved. It also outlines a plausible solution to get the security community moving in the right direction. While this solution is a mere small step toward a robust network, it does alert the operator to a potential network attack. With this knowledge, the driver of the vehicle may get it to a safe location prior to more damage being inflected on themselves or others.

Keywords: Controller Area Network, Security, Analysis, Monitoring, Automatic Socket Closure

1. Introduction

The present incarnations of vehicular CAN Bus is nothing short of a security (and safety) catastrophe (Sakhuja et al., 2021). There exists designers, developers, and engineers taking great pains to ensure the safety of personnel in nearly every endeavor thought possible. This could be as simple as walking across the street to putting human beings into the hostilities of space. Even in the most dangerous situations, such as those faced in military operations, safety reigns supreme (US DoD, 2014). Through most of human history, this concept of safety has been followed in one form or another (sometimes begrudgingly). However, up until recently, these safety concepts were only limited to tangible effects on someone. Tangible as in have a physical presence that can be touched or felt directly. Now, you no longer need a tangible interface to affect safety. It is possible to affect someone or something from distances never thought possible over thirty years ago without physical constructs.

All critical systems connect through the CAN Bus. It is chosen due to having robust availability, high accuracy, and near-immunity to data corruption caused by a vehicle's electrically noisy environment. However, it is extremely difficult to secure as there are several inherent limitations. One of these is that the available computational power of the attached Electrical Control Units (ECUs) is limited. Another is the requirement for near-real-time reactions to inputs allows inadequate time to scrutinize traffic. All units connected to the bus must assume that each system-level command is authentic. The significance caused by this void in vehicle security is apparent once a person realizes that all vehicle controls depend on a secure CAN Bus. This is similar to the human body's central nervous system. If this communication network is compromised, a person will not be able to control their own vehicles or may even lose control caused by an unknown third-party. This devolves into an uncontrolled slug of metal and wire speeding along our roadways haphazardly.

The application of security measures without violating these system requirements is daunting. Until technology reaches a point where it is economically feasible to apply normal solutions, creativity must be used to find ways to reduce incoming threats. One way is to eliminate attack vectors. By removing the remote vectors from wireless sources, security remits to only the physical vectors. This can be done by sensing the CAN Bus for attack anomalies and then determining if the incident originated from a wireless source. In doing so, it may then remove the threat by halting that signal from being received and allowing the system to inherently recover.

Our approach in this research requires a conglomerate Intrusion Detection System (IDS) apparatus with the ability to perform three actions. First, it will determine if the CAN Bus was attacked. When this is detected, the

IDS will sense what the last grouping of signals were that was received from the wireless interface. It will then p determine if the attacking signal was received via wireless. Next, if it does detect an attacking wireless signal, the fingerprint or ID of that wireless signal will be blocked from reception. Lastly, an indication of the attack will be sent to the vehicle operator via a light, a sound, a haptic, or a multiple of the three. It is imperative the alert occur *before substantial* damage occurs to the vehicle or renders the operation of the vehicle beyond safe recovery. The haptic could be a vibration into the steering wheel or a section of the headrest. Performing this as a proof-of-concept and demonstrating its scalability is the motive for this research.

The remainder of this paper is organized as follows: The next section will discuss the problem faced in securing vehicles. In section 3, the current state of vehicular CAN Bus is discussed and the attack vectors present. Section 4 covers the current state of Intrusion Detection Systems as related to CAN Bus. Section 5 presents the concept of the detect-detect-react methodology proposed in this paper and how it processes potential attacks. The impact discussion, conclusion, and path forward are presented in section 6.

2. Inherent Security Issues with CAN Bus

Even though great emphasis is placed on the near-real time communication network, it is hampered by the ease in which it is to degrade the availability or negatively modify communication integrity. Typical networks have time to detect and sufficient computational power to manage the situation before an attack on them is fatal. There is a significant lack of both in the CAN Bus protocol and set-up (required real-time communication and paltry computer power). The main hinderance to treating CAN Bus communications as a normal network communications is the near-real-time requirement (Wu et al., 2020). There is not sufficient time-overhead to allow for adequate security checks. In addition, current vehicle configurations from OEM's oblige us to install security equipment after the fact. While manufacturers have decidedly put forth safety as their number one consideration, they have fallen short in an extreme way. The main reason is the rabid insecurity that grips the CAN Bus. As stated before, safety has been designed, engineered, and litigated into each vehicle allowed on our roadway's sans the networks. *However, without proper security for the vehicle systems, all the safety mitigations taken could be in vain.* Without proper security, it could bring the main method of personal transportation to a standstill. With modern over-the-air updates, it is possible to convert a fleet of autonomous vehicles into a vehicle equivalent of a botnet (Bagloee et al., 2016).

Now, over thirty years later from when the CAN Bus made its debut, there are over 275 million vehicles registered in the United States (US DoT, 2019, States, 2022). The average age of those vehicles has surpassed 11.5 years (Culver, 2020, Bomey, 2019, Carlier, 2021, Deerwester, 2022). Assuming normal statistical distribution, that would place vehicles on the older part of the curve being made in 1997 and later. This equates to over 200 million vehicles present on U.S. roadways that have unsecured networks.

The protocol used on the CAN Bus does not hold well to the tenants of security. When measuring this protocol against the appeal of the CIA model, it falls short. These are the three essential security criteria. *Confidentially* entails providing information only to those people or entities that are required or cleared to access it. The CAN protocol does not include any mechanism or cryptographic ability to prevent unauthorized persons from accessing all information contained on the bus. *Integrity* deals with the exactitude, legitimacy, and comprehensiveness of the data. The CAN protocol does contain error checking mechanisms at a rudimentary level. However, these methods cannot detect the injection of false data onto the bus. Without that ability, the data on the bus will never attain full integrity. *Availability* involves the system always being accessible by authorized users. With the presence of priority-based messaging system, if a message with a higher or the highest priority is inserted onto the bus, lower priority messages will be barred access to the network. Incidentally, availability is one of the primary strengths of the CAN Bus, but it is easily turned into one of its weaknesses.

3. Controller Area Networks

3.1 Computer Solution for Vehicles

The normal progression of computing led to reducing the physical size of computational devices. It was only a matter of time before microprocessor size became trivial enough to find themselves embedded into everything, including automobiles. When Karl Benz invented what would pass as the first car in 1886, it was little more than a frame, an internal combustion engine, and three wheels (Jardine, 2022). At the turn of the 20th century, cars were still a simple mix of mechanical parts put together to get someone from point A to point B faster than a

horse drawn carriage. As time wore on, they became increasingly more complex. In the sixty years between 1911 and 1971, cars saw the implementation of electronic ignition, air conditioning, power steering, and anti-lock brakes. The additional features were enhanced using electronics and more wiring was needed. This led to increased weight. This affected fuel mileage which became an issue during the 1973-1974 oil embargo. With the federal government prompting cars have better fuel mileage, a solution was needed (Day, 2016).

3.2 CAN Bus is Created:

Robert Bosch GmbH created the CAN Bus in 1985 providing a solution for electronic devices to communicate without the requirement of separate lines (Corrigan, 2016) (Automation, 2018). The result allowed components to communicate without needing dedicated physical wires between them. The components could share one medium. This eliminated the need for additional wires for each communication line and lowered cost and weight. In 1991, Mercedes Benz was the first to utilize this framework in the mass production of vehicles (the W140) (Daimler, 2016).

The CAN Bus is an asynchronous serial communications network. The physical characteristics of the CAN Bus is exceedingly unassuming. This is one of the motivations for its appeal. There must be two or more Electronic Control Units (or ECU's) on the bus for the protocol to function correctly. Each node is connected to the conventional two-wire, twisted pair bus. Both wires have a potential of 2.50V that flow in opposite directions to each other. Along with the twisted pair, the current flowing in opposite directions ensure that electronic noise effects are minimized. This configuration provides near immunity to the electronic noise that is prevalent in a car's environment. There is not a central hub or routing system, just a continuous flow of information that's always available (Wojdyla, 2012).

3.3 Attacks and Vulnerabilities

Contemporary intrusions and vehicular attacks have been physical attacks that require hands-on access to the vehicle (cutting a brake line or hotwiring a car) (Nilsson, 2008). These types of infiltrations normally leave some residual evidence that, upon inspection, will reveal that a malicious incident has been exercised or has been attempted. It is entirely different when it comes to attacks on the car's CAN Bus. Physical manifestations of these types of attacks are not as clear. Since these attacks do not rely on physical contact, they can be executed and leave little to no evidence. These attacks would be similar to SYN-Flood attacks on a Wi-Fi network (Lutkevich, 2022). Attack detection is possible. However, it takes more effort and ability than what is required for a simple visual inspection of the attack site. The inspector would need full understanding of how the attack took place and what to look for in reviewing logs. In a sense, without cause to think what had happened, these attacks could occur without leaving a noticeable trace.

Attack vectors on the CAN Bus have two overarching classifications. One is physical and the other is not (wireless). Physical attacks require access to the vehicle. Wireless attacks do not. Securing the wireless portion would result in the possible removal of that vector. That would essentially return cybersecurity to that of a physical issue as it was prior to the proliferation of installed wireless technology in vehicles. Therefore, the focal point is decreasing the possibility of success through the CAN Bus wireless attack vector (Nilsson et al., 2008).

According to (Wu et al., 2020), CAN Bus attacks generally have three steps. First step is to target the vehicle. This can be done either physically or wirelessly. The second step is to compromise the CAN Bus itself or a device on the CAN Bus. This may be performed by flashing firmware on an ECU or by transmitting bogus frames. The final step is what the attacker wants to do with the control. Do they want to start/stop/damage the vehicle, steal information, or just to wreak havoc? It is vital when researching the attack potential of the CAN bus, as well as individual ECUs, that all pathways into and out of the system in question be evaluated. The most critical attacks are replay, injection, and/or denial of service (Batmaz and Pete, 2018). The assumption is made that an attacker is not limited to the computational power of an ECU but can use more powerful devices for attacks (Luo and Hou, 2019b).

The aggregate of attack research performed on the core of the CAN Bus is extensive. The notion of placing an Intrusion Detection System (IDS) in this communication network is not a novel approach. Table 1 below outlines several attacks performed during past CAN Bus security research. Please note, two-thirds of the attacks do not require access to the vehicle.

Table 1: Attacks Performed on CAN Bus

Research	Interface	Physical Access	Method
(Zhang et al., 2016)	OBD-II	Yes	ELM327 OBD-II Bluetooth device and malicious application on a smartphone
(Kang et al., 2018)	OBD-II	Yes	Arduino UNO with CAN bus connects to OBD-II port
(Studnia et al., 2013)	USB	Yes	Connect to media systems by using smartphone
(Oka et al., 2014)	Bluetooth	No	Using the PIN vulnerability while paring
(Josephial and Adepu, 2019)	Wi-Fi	No	Scanning vulnerabilities through appropriate tools such as Nmap, Nessus, and Metasploit
(Woo et al., 2015)	3G/4G	No	Transmit controlling frames by smartphone connecting to CAN via 3G/4G network
(van der Heujden et al., 2017)	V2X	No	DoS at data injection against VANET
(Chattopadhyay et al., 2018)	V2X	No	Injection and packet drop attacks
(Petit et al., 2015)	Sensors	No	Attacking LiDAR, radar, and camera sensors remotely based on physical vulnerabilities

4. Intrusion Detection Systems (IDS)

Overall, the current literature discusses three overall possibilities to provide CAN Bus security. First is the use of cryptography. It has been discussed as a possible way of ensuring frame integrity and confidentiality. Another is the insertion of a firewall between critical and non-critical sections of the CAN Bus. Third is adding an IDS at the entry points of the CAN Bus (Wu et al., 2020). With our current technology, application of the first two increase the required response times to an unacceptable level. It is in the third extent that this paper dwells to find a possible solution.

To adequately detect an event on the CAN Bus, three requirements must be met. First, there must be a device to detect the event. This can be one of the detection mechanisms already presented in the literature or a combination of a few of them. Second, there must be a device that can store the information found during the detected event. This could be volatile or non-volatile. In addition, the amount of needed storage will fluxuate depending on how much past information is desired to be kept. Finally, there must be a device that can interpret the bus traffic for storage on the device. This has been referred to as a “decision engine” in the current intrusion detection literature. These requirements may be met with a single device or combination of devices (Moustafa et al., 2019).

Figure 1 (Luo and Hou, 2019b), provides a basic diagram of the vehicle network and how it interfaces with external sources. There are three distinct layers or areas to note. The first is the External Wireless Interface layer which comprises of the transmission and reception of all the wireless signals. The demarcation for this layer is just inside the Wireless Gateway/Central Gateway. It encompasses the wireless signals as well as the physical connections. The second layer, called the Internal Vehicle Network (IVN) layer by the authors, contains all the network systems. This incorporates not only the target CAN Bus but also the other various networks. The third is External Physical Interface layer. This involves the connections to the physical items that an operator or a person can physically attach to the IVN layer. Potential cyberattacks are then analyzed at each layer and corresponding countermeasures are presented.

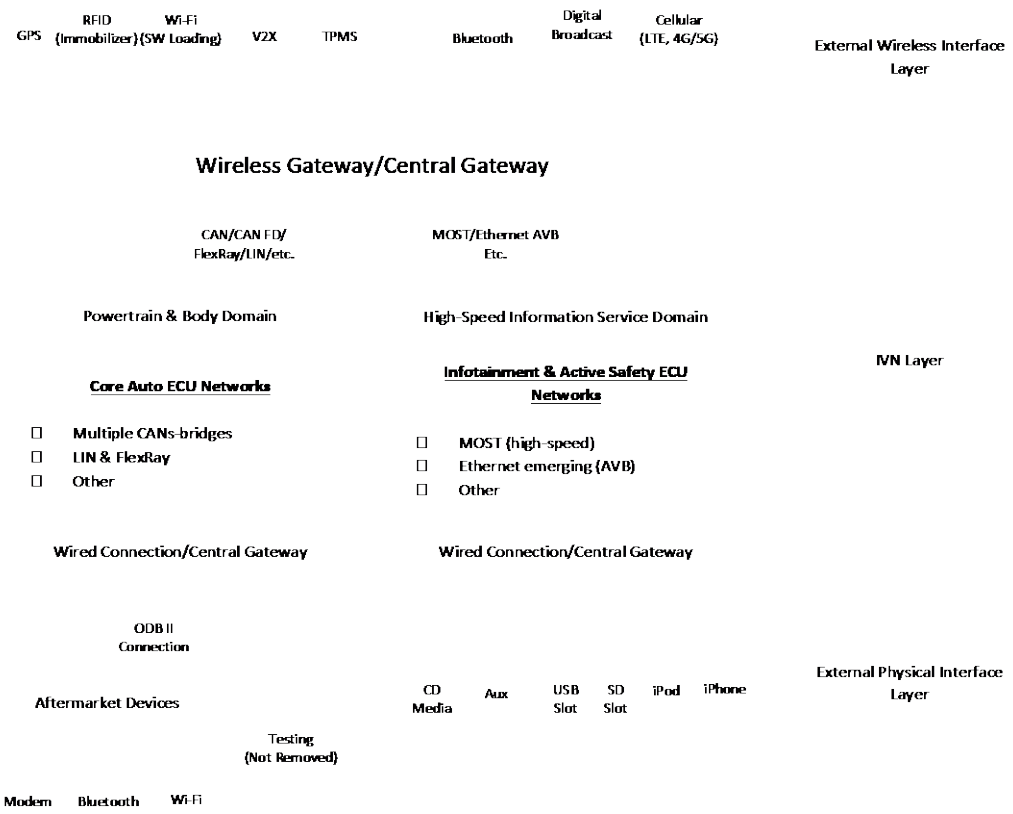

Figure 1: Three-layer structure of the IVN structure from the perspective of external interface (Luo and Hou, 2019a)

Based on current IDS research, there are a few types of sensors that appear to be feasible for CAN Bus (Luo and Hou, 2019b). They are broken down into:

- Dataflow Based: these check only the identification values of CAN frames and thus are more suitable for real-time detection. They can identify cyberattacks but require substantial computing power. Examples include the frequency of communications, ECU fingerprinting, and systematic entropy.
- Payload Based: these check the actual payload of each frame. These methods rely on the utilization neural networks and other forms of machine learning. However, it is not known how well these types would perform in the automotive environment. Examples of these include frame ID checks and checksum verifications.
- Hybrid: methods that extract the best of both worlds in dataflow and payload-based types. These require specialized hardware and are a prime utilization for FPGA's (Luo and Hou, 2019b). These may also employ a total of eight specialized sensors as notated in Table 2.

Table 2: Intrusion Detection Sensors

Sensors	Description
Formality	Correct message size, header and field size, field delimiters, checksum, etc.
Location	Message is allowed with respect to a dedicated bus system
Range	Compliance of payload in terms of data range
Frequency	Timing behavior of messages is approved
Correlation	Correlations of messages on different bus systems adheres to specification

Sensors	Description
Protocol	Correct order, start time, etc. of internal challenge-response protocol
Plausibility	Content of message payload is plausible, no infeasible correlation with previous values
Consistency	Data from redundant sources is consistent

5. Concept of Providing Security

This research focuses on the wireless connectivity of the vehicle. As shown in Figure 1, there are a considerable number of external communication vectors. Intrusion detection occurs on one of the CAN Buses and results in the potential blocking of a communication vector. The perfect answer to the security drawback would be to have confidentially, integrity, and availability (CIA) preserved as is done in standard networking. However, the technology and knowledge in doing that successfully, while overcoming the limitations and restrictions of the system, is currently unavailable. Nevertheless, if it is possible to detect and alert the operator of an intrusion at this gateway, all wireless vectors would be protected.

To provide a graphic explanation of this research, figure 2 shows a functional layout and shows where the sensing and the feedback loops would be connected. In addition, it shows where each element would be located, and demonstrates how the apparatus would be applied. Overall, the concept will continuously monitor the CAN Bus for pre-set anomalies, like how antivirus software utilizes a signature database. If an anomaly is detected, the apparatus will then review the incoming wireless signals to determine if that was the source of the anomalous injection. If it is the source, steps could be taken to pinpoint the port/socket and close it.

5.1 Operational Concept

Figure 2 is a diagram of the proposed research apparatus. It has been adopted from (Luo and Hou, 2019a) and manipulated to suit the needs of this research. There are three main sections. Along the top is the wireless gateway where the universe of RF signals interface with the vehicle. Following from this on the left side are the vehicle's CAN bus that connects the various ECU's. Both items are found already installed in today's vehicles. It is the block diagram to the right where the research is to take place. This block is broken down into various sub-functions which outline what happens. Here, the device will monitor and log the wireless traffic into and out of the vehicle. In addition, the CAN Bus is sensed for any anomalies present. With the current iteration, the checks it does are akin to how a virus scanner performs their inspections. It searches for potential known signatures of attacks.

At the outset, the incoming wireless signals are parsed out and logged as they are received at the Wireless Gateway. This provides a history of what has been received. It will be used for review in the event an anomaly is detected on the CAN Bus. From there, the CAN Bus is monitored for any anomalous signals. The current iteration of the research contains simple triggers based on what has been observed in the past on that network. This is akin to a signature type of detection. This appears to be the easiest method to ensure the concept works. The CAN Bus is being used as the area for anomaly detection rather than the raw incoming wireless signals. This is due to the relative ease of detecting an abnormality with respect to the incoming wireless signals. CAN Bus communications are predictable and mundane as compared to Wi-Fi, Bluetooth, and cellular signals. In the event a potential anomaly is detected, a decision engine is enacted to see if what has been encountered can be classified as an anomaly. This is done by the detected potential anomaly being compared to a signature of known attacks. Previous research such as that from (Dwivedi, 2022), (Han et al., 2018), and (Marchetti and Stabili, 2017) demonstrate such signatures exist for the CAN Bus anomalies.

Once an attack has been established, the determination is made as to the attack origination. It can either be from an external source or from an embedded internal source. This is done by evaluating the incoming wireless signals that were logged earlier. If a received signal adequately maps to a potential structure that could cause the anomaly, a command is sent to the Wireless Gateway to initiate a closure of that communication socket. For example, imagine there exists an interpreted signal on the CAN Bus that directs the steering wheel to instantly turn 90 degrees while the car is going 80 MPH, that could be determined to be an abnormal signal. This would be especially true if that signal kept repeating and not deviating. The detection system would review the logged

incoming signals to determine if an inbound wireless signal is directing that resulting frame on the CAN Bus. If that is the case, a command is sent to the Wireless Gateway to suspend that communication socket. In addition, the apparatus will alert the operator that an abnormal wireless signal was received and caused irregular indications on the CAN Bus. This can be a simple indicator light on the instrument cluster, an alarm that will interrupt and play through the speakers (maybe a voice), or a haptic all depending on the desires of the operator.

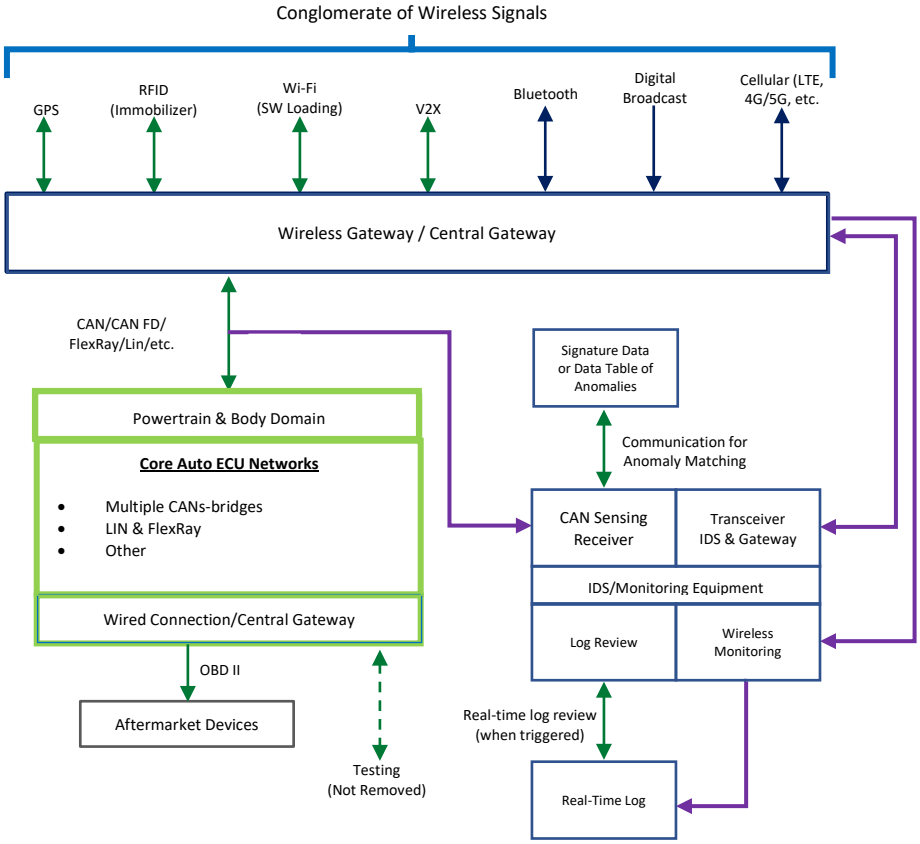

Figure 2: Projected Layout & Function of Research Apparatus

6. Way Forward and Conclusion

The concepts presented in this paper are not new. The act of monitoring and analyzing both CAN Bus as well as wireless signals have been performed exhaustively in the past. The paring of these methods together has not been well documented and researched. As a follow-on to this research, our future work entails the development of a test bed to run experimental evaluation on the concept. When this is successful, the addition of successive actions should be relatively easy. Once able to alert the driver, a wireless cutoff could be installed. These are utilized in Virtual Private Networks (VPN) today when it loses connectivity. This prevents the network protected by the VPN to become active without the VPN in place.

References

AUTOMATION, C. I. 2018. *History of CAN Technology* [Online]. CAN in Automation. Available: https://www.can-cia.org/can-knowledge/can/can-history/ [Accessed 15 April 2022].

BAGLOEE, S. A., TAVANA, M., ASADI, M. & OLIVER, T. 2016. Autonomous Vehicles: Challenges, Opportunities, and Future Implications for Transportation Policies. *journal of Modern Transportation,* 24**,** 284 - 303.

BATMAZ, G. & PETE, I. 2018. Controller Area Network (CAN) Deep Packet Inspection. Nvidia.

BOMEY, N. 2019. Old Cars Everywhere: Average Vehicle Age Hits All-Time High. *USA Today*, 28 June 2019.

CARLIER, M. 2021. Age of U.S. Light Vehicles 2002-2020. *In:* TRANSPORTATION, D. O. (ed.). Statista.com: US Department of Transportation.

CHATTOPADHYAY, A., MITRA, U. & STROM, E. C. 2018. Secure Estimation in V2X Networks with Injection and Packet Drop Attacks. *15th International Symposium on Wireless Commuication Systems (ISWCS).* Lisbon, Portugal: IEEE.

CORRIGAN, S. 2016. Introduction to the Controller Area Network (CAN). Texas Instruments.

CULVER, M. 2020. Average Age of Cars and Light Trucks in the U.S. Approaches 12 Years, According to IHS Markit. IHS Markit.

DAIMLER, C. N. M. 2016. *Mercedes W140: First Car with CAN* [Online]. CAN Newsletter Magazine. Available: https://can-newsletter.org/engineering/applications/160322_25th-anniversary-mercedes-w140-first-car-with-can [Accessed 10 March 2022].

DAY, C. 2016. Computers in Cars. *Computing in Science and Engineering.* IEEE CS American Institute of Physics.

DEERWESTER, J. 2022. The Average Age of a Car in the US is up to 12.2 Years, a New Record. How Old is Yours? *USA Today*, 24 May 2022.

DWIVEDI, A. K. 2022. Anomaly Detection in Intra-Vehicle Networks. arXiv.

HAN, M. L., KWAK, B. I. & KIM, H. K. 2018. Anomaly Intrusion Detection Method for Vehicular Networks Based on Survival Analysis. *Vehicular Communications,* 14**,** 52-63.

JARDINE. 2022. *The History of Car Technology* [Online]. Jardine Motors Group. Available: https://news.jardinemotors.co.uk/lifestyle/the-history-of-car-technology [Accessed 08 March 2022].

JOSEPHIAL, E. F. M. & ADEPU, S. 2019. Vulnerability Analysis of an Automotive Infotainment System's Wifi Capability. *19th International Symposium on High Assurance Systems Engineering (HASE).* Hangzhou, China: IEEE.

KANG, T. U., SONG, H. M., JEONG, S. H. & KIM, H. K. 2018. Automated Reverse Engineering and Attack for Can Using OBD-II. *IEEE 88th Vehicular Technology Conference (VTC-Fall).* Chicago, IL, USA: IEEE.

LUO, F. & HOU, S. 2019a. Cyberattacks and Countermeasures for Intelligent and Connected Vehicles. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems,* 12**,** 55 — 66.

LUO, F. & HOU, S. 2019b. Cyberattacks and Countermeasures for Intelligent and Connected Veicles. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems,* 12**,** 55 — 66.

LUTKEVICH, B. 2022. *SYN Flood Attack* [Online]. TechTarget. Available: https://www.techtarget.com/searchsecurity/definition/SYN-flooding [Accessed 15 January 2023].

MARCHETTI, M. & STABILI, D. 2017. Anomaly Detection of CAN Bus Messages Through Analysis of ID Sequences. *IEEE Intelligent Vehicles Symposium (IV).* Los Angeles, CA, USA: IEEE.

MOUSTAFA, N., HU, J. & SLAY, J. 2019. A Holistic Review of Network Anomaly Detection Systems: A Comprehensive Survey. *Journal of Network and Computer Applications,* 128**,** 33 - 55.

NILSSON, D. K. 2008. Secure Firmware Updates of the Air in Intelligent Vehicles. *IEEE International Conference on Communications Workshops.* Beijing, China: IEEE.

NILSSON, D. K., LARSON, U. E. & JONSSON, E. 2008. Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes. *!EEE 68th Vehicular Technology Conference.* Calgary, BC, Canada: IEEE.

OKA, D.-K., FURUE, T., LANGENHOP, L. & NISHIMURA, T. 2014. Survey of Vehicle IoT Bluetooth Devices. *7th International Conference on Service-Oriented Computing and Applications.* Matsue, Japan: IEEE.

PETIT, J., STOTTELAAR, B., FEIRI, M. & KARGL, F. 2015. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and Lidar. *Black Hat Europe.* Amsterdam, The Netherlands: Security Innovation.

SAKHUJA, S., DUNNE, M. & FISCHMEISTER, S. 2021. The Boy Who Cried Wolf: On Precision in CAN Bus Instrusion Detection. *Embedded Security in Cars - USA.* Virtual.

STATES, U. 2022. Number of Motor Vehicles Registered in the United States from 1990 to 2020. *In:* TRANSPORTATION, D. O. (ed.). Federal Highway Administration.

STUDNIA, I., NICOMETTE, V., ALATA, E., DESWARTE, Y., KAANICHE, M. & LAAROUCHI, Y. 2013. Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks. *43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W).* Budapest, Hungary: IEEE.

US DOD, D. O. D. 2014. DoD Safety and Occupational Health (SOH) Program. *In:* DEFENSE (ed.). Washington, D.C., USA: U.S. Government.

US DOT, D. O. T. 2019. Highway Statistics 2018. *In:* U.S. DOT, D. O. T. (ed.). Washington, D.C.: Federal Highway Administration.

VAN DER HEUJDEN, R., LUKASEDER, T. & KARGL, F. 2017. Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC). *IEEE Vehicular Networking Conference (VNC).* Turin, Italy: IEEE.

WOJDYLA, B. 2012. *How it Works: The Computer Inside Your Car* [Online]. Hearst Digital Media: Popular Mechanics. Available: https://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/# [Accessed 02 February 2021].

WOO, S., JO, H. J. & LEE, D. H. 2015. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems,* 16**,** 993 - 1006.

WU, W., LI, R., XIE, G., AN, J., BAI, Y., ZHOU, J. & LI, K. 2020. A Survey of Intrusion Detection for In-Vehicle Networks. *IEEE Transactions on Intelligent Transportation Systems,* 21**,** 919 — 933.

ZHANG, Y., GE, B., LI, X., SHI, B. & LI, B. 2016. Controlling a Car Through OBD Injection. *IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud).* Beijing, China: IEEE.