Cybersecurity Attacks in Vehicular Sensors

Zeinab El-Rewini, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj,
Siby Jose Plathottam, Prakash Ranganathan, Shree Ram Abayankar Balaji*
School of Electrical Engineering and Computer Science
University of North Dakota
Grand Forks, ND, USA

Introduction

We are rapidly approaching an age in which both partially and fully-autonomous vehicles will emerge on roadway systems. The National Highway Traffic Safety Administration (NHTSA) has set forth a vision that eventually leads to deploying fully autonomous, self-driving cars sometime after the year 2025 [1]. In the meantime, the NHTSA is encouraging the development of partially automated vehicular functions, such as lane-keeping assist, adaptive cruise control, and self-parking. Auto and technology Original Equipment Manufacturers (OEMs) such as Waymo [2], Tesla [3], GM Cruise [4], and Aptiv [5] have already begun to use vehicular sensors to enable both fully autonomous and semi-autonomous vehicular functions and test those functions on active roads [6]. A survey by Society of Automotive Engineers (SAE) International details the cybersecurity risks in autonomous vehicles [7]. To safely deploy autonomous vehicles with SAE Level 5 autonomous capability [8], it is necessary to analyze the cybersecurity aspects in the decision-making pipeline.

Three-Tier Framework For Automotive Systems

Automotive security threats can be classified through the three-tier hierarchical system shown in Fig. 1. Also known as the AutoVSCC (Autonomous Vehicular Sensing Communication and Control) framework, the sensing layer is the first layer of the hierarchy and is comprised of vehicular sensors. Threats to the sensing layer include jamming the Global Positioning System (GPS), eavesdropping on communication within Tire Pressure Monitoring Systems (TPMSs), and deceiving ultrasonic sensors so that they perceive nonexistent objects. Threats at both sensing and communication layers can adversely influence the functionality of the control layer via the transport-application interface to transport and translate valuable digital data into real-time vehicular applications such as automated steering control, lane change maneuvers, and brake application.

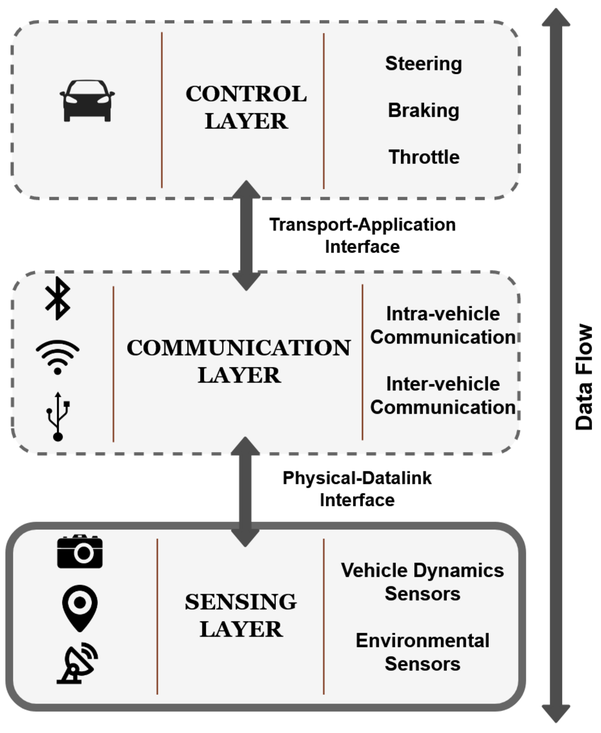

Fig 1. Three-tier connected and automated vehicle architecture (AutoVSCC Framework).

THE SENSING LAYER

The vehicular sensing layer is comprised of vehicular sensors that measure the physical properties of a vehicle's state and surroundings. The sensing layer is critical to smooth vehicle operation since automotive electronic control systems use vehicular sensor measurements to make driving decisions. For instance, distance sensor measurements allow adaptive cruise control systems to determine whether a vehicle can safely increase speed. In partially or fully automated vehicles, human sensing is replaced to some degree by vehicular sensing. Consequently, sensing layer data must have high reliability and accuracy.

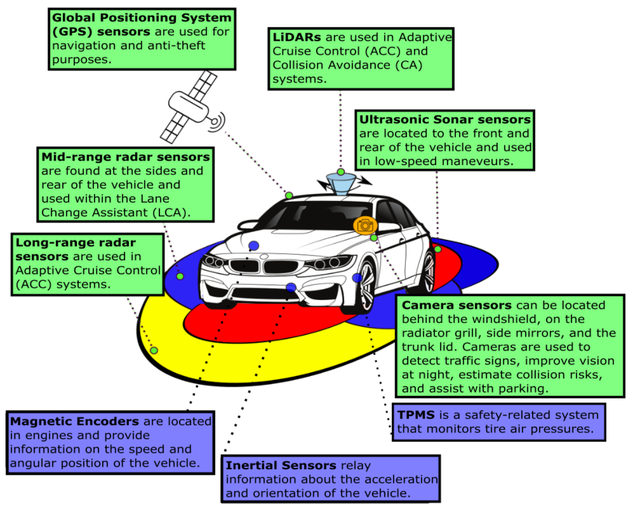

Fig 2. Vehicle dynamics sensors (Blue) and environment sensors (Green) in autonomous and connected vehicles.

Table 1 . Attack Vectors in the Sensing Layer

Attack Vector	Access	Sensor Type	Description
Sensor Components	Physical	Active, Passive	Sensors can be physically tampered with or destroyed.
Receiver	Remote	Active, Passive	Attackers can transmit illegitimate signals to a sensor's receiver.
Emitter	Remote	Active	Emitted signals can be eavesdropped and recorded.
Side Channel	Remote	Active, Passive	External stimuli can be directed at the sensor's transducer to disable sensor functionality.

Table 2 . Comparison of Vehicular Sensor Countermeasures

Countermeasure	Complexity	Robustness	Primary Sensor(s)
Sensor Fusion	Medium-High	Medium	All
Encryption using HSMs and PUFs	High	High	All
Attack Detection	High	High	All
Hardware/Software Modifications & Acoustic Filters	Low-Medium	Low	Inertial
Static Code Analysis	Low-Medium	High	TPMS
Random Probing	Low-Medium	Low	LiDAR
Side Channel Modulation	Medium	Low	LiDAR
Physical Shift Authentication (PSA)	N/A	High	Ultrasonic
Near-IR Light Filters	Low	Medium	Camera
Noise Filters	Medium-High	High	Radar
Sensor Threshold Monitoring	N/A	Low	GPS
Data Multi-routing	N/A	Low	GPS

FUTURE OUTLOOK

A future for autonomous vehicles is quite promising as the automotive industry is racing to provide comfort and safety. As research and development of fully autonomous vehicles are underway, intelligent sensors will play a major role in determining how well these autonomous vehicles run on roads. As each vehicle may contain over 200 sensors with an intelligent onboard infotainment system and state-of-the-art cloud based telematics, data privacy and security are critical for vehicle manufacturers, vendors, and customers. As cyberattacks become a method of warfare, innovative technologies such as machine learning and blockchain will play a significant role in offering cybersecurity solutions.

Blockchain Based Solutions

Though the adoption of the Internet of Things (IoT) in vehicular networks is on the rise, there are still major challenges such as scalability, security, lack of standards, centralized networks, architecture models, and cost. A distributed platform or Distributed Ledger Technology (DLT) such as blockchain has the potential to overcome these challenges and to increase the protection against vehicular cyber-attacks.

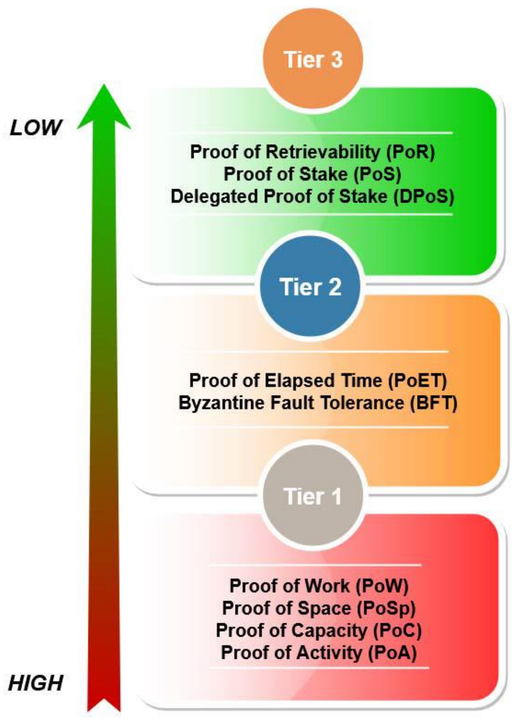

Fig: 3 Hierarchy-based consensus algorithms for blockchains in vehicular environments..

Table 3 . APPLICATIONS AND CONSTRAINTS OF BLOCKCHAIN USAGE IN IoV NETWORKS

Application	Attack	Defense	Challenges
Trust Management & Announcement Network in VANETs	Spoofing, Replay, MITM	Bayesian Rating, PKI, Unique IDs, Consensus Algorithms, Verification & Validation	Data Privacy
Message Handling	DoS, DDoS	PKI, Event Message Authentication	Overhead & Latency
ECU Data Storage & Local/Regional Blockchain, SDVN	Spoofing (Immutability), DoS Eavesdropping	ACL, Symmetric Encryption, Reduce Delay	Cloud Reliance

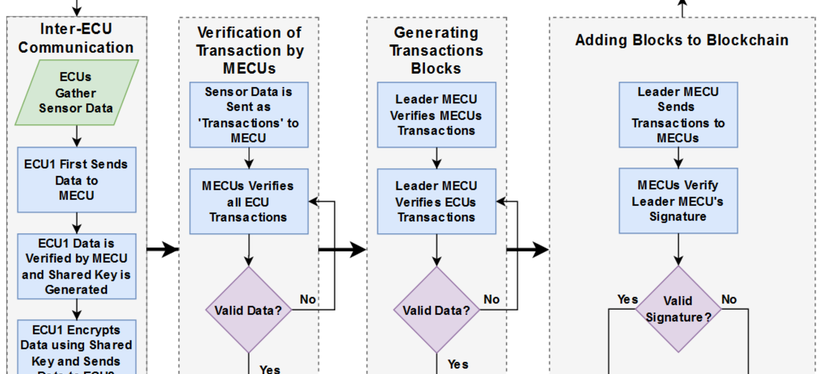

Fig: 4 Blockchain implementation to secure intra-vehicular data from ECUs

Conclusions

The contribution of this paper is to offer a timely review of potential cyber-attacks in autonomous vehicles. Specifically, the article discusses how malicious attackers in the sensing layer can exploit a modern car. Several cybersecurity threats are investigated under vehicle dynamics and environment sensors with their countermeasures. The authors see a transformative automotive industry that will soon adopt disruptive technologies (e.g., real-time machine learning, deep learning, advanced edge/fog computing, encryption, and blockchain) by integrating vehicular data from sensors in IoT platforms to advance the security and safety of vehicular networks.

References

[1] NHTSA. (2018). Automated Vehicles for Safety. [Online]. Available: https://www.nhtsa.gov/technology-innovation/automated-vehicles safety
[2] (2020). Waypoint—The official Waymo Blog. [Online]. Available: https://blog.waymo.com/
[3] (2020). Tesla Autopilot AI. [Online]. Available: https://www.tesla.com/autopilotAI
[4] (2020). Cruise. [Online]. Available: https://medium.com/cruise
[5] (2020). Aptiv—CTO Blog. [Online]. Available: https://www.aptiv.com/newsroom/cto-blog/253985928
[6] (Feb. 2019). Self-Driving Cars Take the Wheel. MIT Technology Review. [Online]. Available: https://www.technologyreview.com/2019/02/15/137381/self-driving-cars-ta%ke-the-wheel/
[7] S. International and Synopsys, "Securing the modern vehicle: A study of automotive industry cybersecurity practices," Ponemon Inst., Traverse City, MI, USA, Tech. Rep., 2019.

Acknowledgements

El-Rewini, Z., Sadatsharan, K., Sugunaraj, N., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity attacks in vehicular sensors. IEEE Sensors Journal, 20(22), 13752-13767.

*Poster Designer(Non - Author)

Contact

Dr. Prakash Ranganathan
Director of Center for Cyber Security Research (C2SR) Associate Professor, IEEE Senior Member of Electrical Engineering College of Engineering & Mines University of North Dakota
prakash.ranganathan@UND.edu | 701.777.4431