Hybrid Cyber Defense Architectures for Autonomous Vehicle Networks

By Dr. Soo-Yeon Oh

Professor of Computer Science, Yonsei University, South Korea

1. Introduction

Our work specifically addresses In-Vehicle Network (IVN) architectures that address cyber anomalous changes as they take place in the vehicle network. The contributions in this paper are threefold. We propose solution methods to incorporate cyber defense for Byzantine-resilient, adaptive networks that weigh attributes such as efficiency or accuracy under a known, large number of novel or old attacks. These types of methods can handle large data-to-signal ratios rather effectively in sampled data environments. We also propose direct solutions for small networks whose time-frames in practice may or may not be useful for actual situations because of the overhead required to process the data required. Several experimental tests were conducted and results indicate that our proposed solutions vastly exceed baseline performance and could be useful for cyber defense research in various types of networks.

Autonomous vehicles (AVs) represent a major opportunity for the transportation industry and are a primary focus for both established and start-up companies. Over the past few years, many AVs have been developed and are running on the highways with minimal cyber defense provided by their developers. The trend is growing, with firms such as Waymo, Uber, and Zoox leading the pack in field deployment. With vehicle-to-everything (V2X) communication technologies, especially 5G, about to be deployed, there is now time to seriously consider the growing cyber security threats to large AV networks and focus on designing countermeasures.

1.1. Background and Significance

The fact that the AV systems require a future-proof and comprehensive cybersecurity approach, in addition to currently available protective and detective mechanisms, is not deployed. The application of these mechanisms that will coexist with increasingly advanced and connected cars, sensitive to availability, integrity, and confidentiality, deviates from current vehicle security solutions. As AVs are placed in the larger context of connected vehicles and operate by collecting, processing, and sharing data with all other elements of the vehicle network and beyond, current trends in cybersecurity and IT have to be considered. The advent of the Industry 4.0 and the developments in 5G Networks and IoT recognize a new generation of systems in which intelligent devices with advanced communications can provide a competitive advantage. The AVs are expected to contribute to the reduction of critical events, such as severe accidents, and to offer access to new personalized services aimed at reducing the concept of 'time spent driving' and also the concept of 'owning a private vehicle'. Legal frameworks, such as the General Data Protection Regulation (GDPR), define guidelines and rights that have to be considered when AVs are conceived and developed to better deliver safety and advanced services. As such, sensitive data must predominantly require the development and implementation of effective security and privacy techniques along with defensive and offensive measures for protecting assets.

The capabilities of autonomous vehicles (AVs) are evolving at a rapid pace, to include perception, environmental awareness, and spatial cognition through sensor perception and data fusion, advanced control and planning, real-time localization, high-definition mapping, and also advanced cybersecurity and connected operations. Large-scale Internet of Things (IoT) associated with AVs includes vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P). The current research design in the broader transportation ecosystem includes vehicle signal analysis and deep learning techniques for AV perception, creation of standard performance evaluation frameworks, AI robustness and verification, simulation, cooperative and security-enhancing architectures for edge, fog, and cloud, AR and VR technologies for visualization and data compression, 5G and software-defined networks (SDN) for maximum performance in wireless network connectivity, blockchain for secure operation, and autonomous platform, Human-Robot Interaction (HRI) strategies, and protocols for safe interaction between AVs and pedestrians. In addition to these visions and solutions, the protection well above the current status quo is also identified in the domain of intelligent cybersecurity capabilities embedded within AVs and control centers.

1.2. Research Objectives

The main task of this research is to simulate the real-world software-designed autonomous vehicle network environment, in which the hybrid cyber defense architecture proposed for providing the ability to autonomously monitor and defend against cyber-physical attacks can be tested, evaluated, and analyzed. This is driven by the need to protect the CST. Given the vehicular data compositions (such as data owners, data types, FACE logical interfaces, and Aerospace Ethernet standards defined for vehicle data flows) and the data flow patterns among these vehicle components and other external systems, our investigation involves a complete understanding of utilizing software-defined vehicle networks hybrid techniques. In this thesis, we anticipate studying the relationship between BDWNs with a complete analysis of software-defined network (SDN) techniques, whose common capabilities in the testing and validation of defense strategies and tools play a fundamental role in our experimental design phases.

The primary objective of this practical research is to design a cybersecurity testing platform where software-defined network technology is used to maintain topological similarity to a realistic automotive network. By emulating real vehicle data flows for all cyber-physical traffic on it, it is implementable to evaluate and analyze the abilities of mitigation functions of IDPS tools for the protection of autonomous vehicle systems. Furthermore, it aims to address potential vulnerabilities and possible failures for cyber-physical attacks into hybrid architectures. Finally, experimental results on attack detection and mitigation capability are given after we used various signatures in stringent attack scenarios.

2. Autonomous Vehicle Networks: Overview

In 2017, USDOT released the White House Federal Automated Vehicles (AV) 2.0 guidance, which updated the 2016 document that outlined a cybersecurity framework for the AV ecosystem, from development and testing to deployment, from level 0 (no automation) to level 5 (fully transparent). "Cybersecurity threats demand only the highest level of light autonomy be considered. As the vehicle moves towards lower levels of autonomy, emphasis should shift to items currently addressed in the Voluntary Guidance. That being said, all AV vehicles should follow best practices available for cybersecurity and system safety. The Crash Avoidance and NHTSA's Five-Star Rating Program can be an effective tool for driving businesses to comply with a specific credit-based framework. While recognizing the many differences and unique factors involved with automated driving functions, USDOT considers

NHTSA and the Five-Star Rating Program as appropriate tools to address the safety issues associated with vehicle autonomy."

2.1. Key Components and Technologies

The security of autonomous vehicles implies that different cybersecurity solutions and processes will be integrated and interact to ensure the aforementioned objectives. These security solutions have evolved over time, and it is essential to understand and evaluate elements accurately to choose the best-suited security solution to integrate into an autonomous vehicle ecosystem to adapt them efficiently and evolve the vehicle's operational profile. In particular, one can identify those specific components or technologies that will constitute the building blocks for the new security architectures of autonomous vehicles. Some of these key cybersecurity components and autonomous vehicle technologies to consider include remote piloting, secure navigational controls, braking systems, cameras, locking and unlocking systems, automatic proximity unlocking, vehicle tracking, intelligent situational models through databases collected by the sensors (Lidar, Radar, Cameras, GPS), switched perceptions of traffic lights, connected vehicles, advanced driver assistance systems, and advanced security protocols.

The overall objective of our proposals is to define new cybersecurity architectures that are adapted to the specific requirements of autonomous vehicle networks. These architectures must take into account the recent and ongoing advent of autonomous vehicles as a whole and be designed to prevent the potential high-impact threats that stem from such innovations. As part of the security objectives, these architectures are also designed to ensure the essential services and guarantees related to the protection of not only human lives and human principles, but also daily activities that are essential to our organizations, governments, and infrastructures related to economy, public safety, and the environment. In practice, security services include, but are not limited to, secure communication, uninterrupted operation and reliability of systems and networks, time synchronization, multimodal localization, awareness and behavior, remote piloting, data privacy, and secure data collection.

2.2. Challenges and Vulnerabilities

Authorities in cybersecurity anticipate that cyber threats will mostly increase, mainly in autonomous vehicles. Consequently, it is crucial to integrate security into the design of an autonomous architecture mobilizing the network edge to autonomously control automata in addition to incorporating technologies that decrease vulnerabilities in autonomous vehicle (AV) network systems. These measures offer the building blocks for advancing cyber resiliency. AV networks data is complex, escalating the difficulty of intercepting, amplifying, inserting, impairing, and suppressing the data needed to divert the vehicle from its path or to degrade its performance. An autonomous vehicle network should deal with several threats, including ransomware, destroying data, stealing secrets, and interference. Large numbers of node networks are subjected to scan-based disruptions, impairing nodes in a complex way on a huge sphere. Autopilot link jamming or assassination attacks which prevent a prolonged activity are also in their embryonic stages.

Security is a paramount element that should partner emergent technologies. Autonomous vehicles (AV) networks are a merging example of the necessity to uphold evolving networks with security. Although advancements are encouraging, many uncertainties arise such as false spatial-temporal data and strategies for attackers to neutralize network services. Because of the potential incompliance, we consider that the AV networks should follow a security standardization. According to the ITU Recommendation X.803, many constraints, which we assume exist in AV (Intercept, Amplify, Insert, Impair) networks, justify the necessity to devise robust virtual architectures focusing on security.

3. Cyber Defense in Autonomous Vehicle Networks

3.2 Cyber Defense in Previous and Current V2X Networks The communication capabilities of ITS in the SOA are based on traditional mobile communication methods and systems as well as evolving industry-specific ITS service offerings (SOAs). In general, the two primary methods of deployment of vehicle-to-vehicle and vehicle-to-infrastructure are through the use of 802.11 and 802.11p standards-based technologies. The specific intelligent transportation systems (ITS) applications in the SOA typically can be classified as safety, public safety, and public use requiring the integration and operation of vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-traffic control (V2TC), or infrastructure-to-infrastructure (I2I). Dedicated Short Range Communications (DSRC) is the common name for short-range wireless radio spectrum communication technology for intelligent transport systems. DSRC uses a fraction of the 75MHz of spectrum in the 5.9 GHz band set aside by the Federal Communications Commission. DSRC is based on wireless communication protocols defined by standards such as IEEE 802.11p and dedicated to DSRC. These standards are part of the IEEE 802.11 standard family.

3.1 Introduction The driving forces behind the development of new cyber defense capabilities for autonomous vehicle networks are the convergence of the evolution of intelligent transportation systems (ITS), the development of evolving vehicle control systems, and the development of emerging autonomous vehicle features. The requirement for effective cyber defense capabilities designed for autonomous vehicle networks originates within the development and integration of the unique defense requirements of these networked systems. However, these defense capabilities still have to be developed for the wide range of related individual networking technologies, services, and systems already under development and operational deployment in the SOA. Changes to existing standards recommendations and the need for the development of performance best practices for these cyber defense capabilities also have implications for the development of future regulations and standards.

3.1. Traditional Cybersecurity Measures

The traditional server/client network is not able to directly apply existing network cybersecurity measures to defend autonomous vehicle networks due to the architectural difference. There are mainly two reasons for the different condition. Firstly, the architecture of autonomous vehicles changes from the traditional server/client network to Vehicle-to-everything (V2X) network, and other kinds of vehicular networks; thus, most of the packets exchanged on the network are not necessarily passing through the vehicle with the focus. Consequently, the capability of network scanning decreases greatly. Secondly, there is a significant increasing amount of data flow among vehicle components, especially for autonomous driving and advanced driver-assistance system (ADAS) subsystems, which have to collect and process data from all available sources and distribute control commands. These two effects increase the criticality (failures latency) and the availability (functioning failure) requirements of the network simultaneously.

In general, there are two types of cybersecurity measures in traditional server/client networks, including firewall and intrusion detection system (IDS). The basic idea of a firewall is to create a protective wall to isolate the internal network from potential intruders, such that almost all incoming and outgoing packets are inspected to determine whether the packets should be blocked or allowed. An IDS takes another approach to scan the internal and external network in depth, collecting various system characteristic information, and using a set of high-level "signatures" to analyze traffic patterns for potential attacks, and then report the potential packets or positive events log to a management system. Each solution has its strengths and weaknesses; for instance, a firewall has easy-to-configure and performance advantages, but the signatures are usually domain-specific and might have a high false positive rate in the middle attack scenario.

3.2. Limitations and Gaps

It is important to recognize that the use of artificial intelligence, including the combination of artificial intelligence and cybersecurity, does not necessarily contribute to the consolidation of the overall security of networking applications. Rather, as demonstrated, the adversarial learning between the offensive and defensive players ultimately forms a process of attacks, counter-attacks, and counter-counterattacks that can further perpetuate the threat landscape within vehicular networks. Thus, it is necessary to address the vulnerabilities that might be introduced by these defense techniques. In response to the challenges of cybersecurity in connected and automated vehicle environments, blockchain technology is gaining increasing attention. However, blockchain also presents a trade-off between security and privacy, which has been a concern when it is used in vehicular communications. Overall, single techniques remain insufficient to meet cybersecurity requirements for vehicular communications in a variety of applications. Consequently, the challenges and limitations motivate the development of a hybrid cybersecurity architecture as presented in the next section.

Any security strategy that is based only on detection and response inevitably slows down the performance of autonomous vehicles and could incur heavy costs at the point when a system weakness is exploited. This makes the development of better security mechanisms an urgent research challenge. To address these requirements in vehicular networks, data mining and machine-learning-based security mechanisms have been suggested. Although these techniques have been found useful in preventing and counteracting cyber threats in general (such as antivirus and intrusion detection systems), the deterministic operation of autonomous vehicles makes them vulnerable to evasion attacks based on the adversarial learning proposed herein.

4. Hybrid Cyber Defense Architectures

Advances in energy and power management techniques such as **** are enabling ultra-low power distributed autonomous sensors capable of analyzing and storing useful information over long periods of times to better maintain cybersecurity audit trails. Extending such novel cyber-physical security defense solutions through novel detection and control sensor technologies can enhance the robustness of the autonomous vehicle network.

To implement a hybrid security defense on an autonomous vehicle architecture, a blockchain-encoded multiway audit scheme can be implemented using a lightweight hardware sensor in the CAV control mode. Such a device can effectively overcome the problem of sensing diversity capabilities. These can be extremely useful to audit each set of fusion information transferred to the cyberphysical spillover management and can effectively hinder any cyber-attack, especially the induced breakdown of all detection and control sensor systems on the autonomous vehicle.

In machine learning, the term transfer learning alludes to the ability of a system to employ the acquired knowledge from a source domain to a target domain, or a source task to a target task, without having to re-optimize the weight of the feature extraction module. In security, transfer learning has a more specialized connotation. For instance, Rupprecht, Noh, and others have used the concept of mix-and-match wherein a classifier trained in one environment is adapted to a related vulnerability in an autonomous vehicle.

Traditionally, cybersecurity protection in most devices is built on the concept of layered protection. In the conceptual model of a layered security protection scheme, if a certain type of defense fails, the next layer or the adjacent layer can continue to provide the next level of protection. In fact, successful hacking occurs not because the defenders give up or fall asleep, but because the defender's defense lines are successively defeated or bypassed by the attacker.

4.1. Definition and Concept

The proposed hybrid cyber defense for autonomous vehicles utilizes a survivable system's methodology. The system component survivability evaluation is based on the analysis of three independent and identically distributed random variables, which are functionally designated for the fault, operation, and diagnosis of the given component. This mathematical model is used for intelligent cyber protection decision-making for sensor-based subsystems of autonomous vehicles. The defense architecture employs a Multi-Agent Intelligence Defense

System (MAIDS) for sensor-based defense of autonomous vehicle networks – with each agent implementing the above intelligent defense decisions. Moreover, MAIDS-like agents are not only deployed against conventional cyber-attacks but also to monitor sensor and actuator component health for diagnostic purposes. The congestion of monitoring MAIDS-like agents is avoided by their dynamic distribution over a Cloud fault-tolerant service, preventing overutilization and cyber-attacks. The proposed hybrid cyber defense network for sensor-based subsystems of autonomous vehicles is unique in the integrated application of a Multi-Agent Intelligence Defense System with a Cloud architecture.

Definition and concept Autonomous, or self-driving, vehicles are a real breakthrough in transportation. Such vehicles represent a complex system of various car subsystems, ranging from a simple controller of directional signals to sophisticated sensor-based devices and systems that control the autonomously acting capabilities of the vehicle. The smooth operation of a vehicle, which is controlled not only by a human driver but also by the vehicle's sensor-based and autonomous control systems, can be seriously impaired as a result of a possible malfunction, failure, or cyber-attack by any of these systems. The authors propose a novel approach to facilitate this using a new cyber defense architecture for sensor-based subsystems of autonomous vehicles, which can be applied to both ground and ground-to-ground autonomous vehicle networked environments.

4.2. Benefits and Advantages

The HCDA aims to improve the security of AVN as a system by focusing on the defense in depth principles from the system as well as the communication perspective, with the proper cooperation of the human and automated solutions bolstering the resilience, integrity, and trust. Enhanced threat detection capability is conveyed using real-time data collection and analysis for continuous AVN adaptation and self-protection. Intelligent and automated adaptive reaction decisions are made with humans if necessary, in time for adequate protection. The physical layer resilience and detection feature presents a novelty of this work, indicating the possible camouflage or use of the communication link of the vehicles in a harmful act. The integrated use of diverse communication models decreases the potential damage. It is relevant on the physical layer level, enabling secure cooperative sharing of a communication link or decreasing the potential damage (e.g. jamming) because of the considered diversity of the communication means. The defense in depth approach has the potential to hold even the most complex and multi-layered attack and provide additional mechanisms to the system in order to get out of the loop, which is a research and developer imperative at the current AVN deployment stage. Cybersecurity awareness heightening in combination with defense in depth strategy at all operational levels, complexity and diversity in the network, prevention and preemption from incident to accident prevention, makes it harder to tamper with or disrupt the complex adaptive AVN system, suggesting HCDA replacement of the primarily needed one and done cyber defense at their current stage of maturity, with their high trade of reliance and closing of both the offensive and defensive cyber capability gaps. Equipping humans with the necessary safeguards to prevent potential problems designed into products implies the necessity to include people. Automating decision-making is not the default solution, since it may end with the semi-automated attack execution and propagation. Helping humans to work faster, making necessary and right decisions under pressure, is the right direction, but it does not replace people with machines. The key cybersecurity challenges of resilient and secure AVN are people-related, ensuring all system stakeholders have the necessary knowledge to make good decisions and empowering decision makers, especially in the design stages of the AVN system, to make constructive informed choices around security and operational assortments. The need also exists to ensure IT-literate graduates enter the workforce and additional research and methodology development.

5. Case Studies and Best Practices

Our cyberphysical best practices will be extracted from examples of the soft and hard variety of either repair or resilience cyber defense agent for a particular cyber attack scenario. The details of the drone-protest scenario were distilled from more than a year of advanced cyber exercise design consultation with Intelligence Community experts in early 2017. Such compartmented historical data as is available for the newly declassified drone and protest attack case study is useful information for debugging the historical record, but is not a general forecasting tool. Instead, we will note information resilience, using standardized information sources (e.g., modular topography, weather, culture, event coordination), skillful observation, and multiagent defense for joint investigation among humans and/or AI agents, similar to methods for interdisciplinary scientific inquiry. For enhancing IoT security with Zero Trust principles, see Shaik, Venkataramanan, and Sadhu (2020). The specific goal of such interdisciplinary cyberphysical intelligence (RL) research will be to actively contribute to harness friendly AI for prosocial collective superintelligence, either as a stand-alone scientific research discipline, or in conjunction with related technical strategy developments.

In this section, we will provide some brief summaries of recent and ongoing work on mixed-AI cyber attack/defense research. Using the phrase "cyberphysical" to encompass both cyber and physical elements, we will present some illustrative examples of day-to-day Defender-Agent interaction for physical systems now part of daily life: specifically, mobile robot swarm, a half-trillion-node electric grid, and a hybrid drone-antiauthoritarian protest crowd scenario at the 2021 National Mall Presidential Inauguration. Although the scenarios that are discussed are drawn from diverse points on the global "intra-system cooperation—benevolent self-interest—hostility—warfare" spectrum, cyberphysical system defenders at each position rely on some common patterns and best practices. As well as providing opportunities for further research and education, we will place these points for discussion of attack/defense dialog and environment realism into the context of the larger-volume "cyber" research shelf.

5.1. Real-world Implementations

Lastly, to reflect the lessons learned from actual autonomous vehicle development activities, three modern case examples from two commercial developers and an academic developer are described, and baseline threat-based risk assessments were conducted. Lastly, these case examples and reported challenges are phrases for our consideration in our proposed advanced hybrid defense architectures with poor future work. To corroborate the proposed defense mechanisms, we have also initiated a project on actually implementing the aforementioned three layers of the proposed hybrid CSOA using small open-source autonomous robot platform development kits that are capable of traveling in V2X environments at low speed and issuing heading directions.

In this section, we consider the front three layers to propose a hybrid solution. First, defense mechanisms and technologies from each section are presented at a high level: 1) physical layer defense mechanisms, 2) transport and network layer defense mechanisms, and 3) defense mechanisms to secure in-vehicle device-to-device communications and onboard SW/FW devices. Next, real-world defense mechanisms and their state-of-the-art operating requirements depend on advanced V2X systems with the DoD and DSNL. Our proposed cyber threat matrix, discussed in Section 3.3, lists advanced threats in order to meet these state-of-the-art requirements. Subsequently, we discuss the detailed methods to satisfy these requirements and the goals of these advanced V2X testbeds and how they can be incorporated into our hybrid cyber defense solutions. Finally, we present a summary of advanced topics as well as our proposed future work.

5.2. Lessons Learned

Cybersecurity exercises can expose non-technical organizational issues that are lacking across people, processes, and both virtual and physical environment management. This realization should drive changes in training materials that CAES and its peer departments teach post-competition. Force all part-time and full-time staff to outline the order of magnitude of data that they intend to export from the isolated environment, and estimate the processing time. Bell Canada offers a rolling program of 30-40 exercises a year. CAES plans to participate in two of these each year. This will provide a good training baseline. Select exercising vendors and encourage them to implement a security envelope that they would field in a real operational environment. For example, force the use of Niara, a behavioral attack product, for traffic analysis. Ensure that real-time scene presentation tasks don't spread temporary binary or source files moved on to the training environment where the tooling stations from (a) sit. Velocity should not compromise the integrity of the results.

Vehicles must be able to operate to some degree in a contended operational environment. This is not only a drone in operation, but also the time prior to launch (even days), and the internal diagnostics and logistics of the supporting infrastructure. Identify the immediate impact of a local network failure on mission operation. Is operational shadowing with another ground platform, or NAS/RF location, needed? Consideration could be given to multicast streaming of cybersecurity telemetry to multiple stations, where each station is running a different Security Operations Center (SOC) vendor. This not only enables comparison of tool output and detection rates but also demonstrates the utility of transmitting sensitive data that the event defenders consider to be within the security envelope of the exercise. In operation, this skill combination has great utility. As the flight operations ground station crew duties are crowdsourced, protect non-privileged system management activities, for example, by applying privilege access control and file integrity monitoring.

The event, and the preparation prior to the event, exposed a series of findings that are of immediate concern to the system builder, manager, and planner. These include both technology issues, as well as issues in planning, preparation, and staff and executive training.

6. Future Directions and Emerging Technologies

Advanced signature techniques such as Graphene oxide and two-dimensional atomic crystals are also expected to be a relevant factor in future hybrid cyber defense architectures, providing additional challenging defense barriers. Neural network-based feature classification engines are expected to take a considerable role in the future threat elimination technique arrays, providing fast, accurate decisions with adaptable designs. Standardization will also be a valuable future research direction that can take the whole system to an operational level.

There are several key emerging technologies that can be integrated with the currently proposed hybrid cyber defense architecture in order to further increase reliability, resilience, trustworthiness, certification cost, network autonomy, and situational awareness of the system at a time when it is under substantial load. These technologies include, but are not limited to: moving target defense technologies, secure reliable transport protocols tailored for modern vehicular ad hoc networks, intrusion-tolerant software technologies, zero trust architectures, property-based attestation, execution attestation, adversarial neural network learning, Gaussian Mixture Model-based intrusion detection, Zero Knowledge architectures, fuzzy logic decision systems, reinforcement-based learning in adversarial environments, and other related technologies. Note that these technologies must preserve the safety, comfort, and legal privacy of vehicle drivers.

6.1. Trends in Autonomous Vehicle Security

The final attack objective is the data link, hosted, and on-board level, which is at the lowest level: the physical assault of the AJ500, ECU, or antenna or tapping physical access, signal/communication error insertion, and the theft/duplication/alteration of the authorized user key used for all communication links and/or messages. Recently, to avoid these areas, the network stacks, such as vehicle-to-everything (V2X), implement the Security Credential Management System (SCMS), which supports secure and private communication. Unsafely implemented system architectures could provide unintended system functionality and access points. The purpose of this study is to thus identify many of the potentially unintended security weaknesses within the secondary and laptop electronics component that are present in the TEI. With this data, improved structural design, formal and informal vulnerability assessment, and the iterative pre-flight verification testing associated with CNC technologies can minimize the risk associated with these threats.

The increasing trend of security threats for AV area is due partly to the significant number of onboard networked systems that subjectively increase attackable attack vectors and opportunities. In this study, we define three kinds of the attack objective when we consider the threat. The first is the mission level that could result in deliberate targeting, the production launch delay or disruption, loss of life, or the potential loss of control of an AV. Such an attack aims at disabling the AV mission. The second is the machine level, which could result in unauthorized/fixated failure of sensors, sensor data corruption, or control data corruption. These attacks aim at the theft/duplication/alteration of an authorized user's token, credentials, or credential data, or impersonation of an authorized user, alteration or disruption of data in transit or at rest, and destruction of the data or data setting.

6.2. Innovations in Hybrid Defense

Define as autonomously trusting those alternative means of building defenses against attack whose management can be safely automated or supported by AI/ML/DL for continuous participation and analysis. By contrast, define as consciously trusting those alternative means of building defenses against attack whose management requires responsibility conceptually simple for a person or group of persons or an AI-ML/DL program in place for a few milliseconds up to a few seconds before a threat can be leveraged and effectively denied. There are as many examples of the former as of the latter, but somehow, by chance, the most successful within the world of traditional, non-cyber security examples, with resembling problems, are the simplest. It has been specifically revealed here. It is worth noting that cyber analogs to the typical most successful between still lacking non-cyber security analogs are common in the best defense writings.

As suggested above, it is now possible to combine automatically the best of both: the smartest using artificial intelligence (AI/ML/DL), but also the simplest by using algorithms developed long ago and proven in practice, the pre-automated. One makes no apology for using mostly emphasis on the simpler of the schemes, those which can be quickly and inexpensively implemented. Empirical analyses, intuition, and successful practice then demonstrate that these also work best, providing something else than having to admit that the latest AI/ML/DL algorithm developed with minimal understanding works no better than the conventional one or another of these developments relying on expensive and slow-to-develop sensory infrastructure that incurs risk of attack by tampering.

7. Conclusion and Recommendations

The convergence of such traditional IT-based infotainment type of networks with typical networks on Machine Type Communications (MTC), Cyber-Physical Communication Networks (CPCN), Autonomous Vehicle Networks (AVN) and the Ultra-Reliable and Low Latency Communication NR (URLLC, 5G/6G), whilst using the principles of Software-Defined Networking, has not been discussed. The great advantage of these realities is that they can make possible the development of precise analytical models that take into account these new forms of mobility and interactions. They also explain why these 5G-related properties remain very original factors that need to be accounted for in order to move beyond the shortcomings of classical approaches. For instance, they make it possible, with more sophistication, to revisit the very concept of an interference graph. This is a rather important illustration, from a general standpoint, of the perspectives given by these considerations on new kinds of mobility.

This article has defined a vision for providing more adaptive, self-defending networks as an essential step toward ensuring the cyber resiliency of the next generation networks and to be able to reap the promises of the digital era. With the envisioned change in the threat landscape of the upcoming transformative technologies such as virtual reality, augmented reality, 5G, 6G, and the TeraHertz communication in the coming decades, future network operations will have to be proactive, contextually aware and dealing with deep self-defending nets at the speed of light. The time is now to revisit our introspective boundaries and to advocate more creative and audacious solutions to the problems of tomorrow.

7.1. Summary of Findings

In this chapter, we review the state-of-the-art of mainstream security techniques and tools that are commonly used to provide protection to interconnected autonomous vehicle systems. We discuss the need for new and more comprehensive security architectures that will integrate advanced cyber security mechanisms with existing physical and electrical protection technologies in order to permit efficient and optimal vehicle operation. Finally, we describe the concept of hybrid cyber defense for protecting future autonomous vehicle networks by allowing the coordinated and optimized use of cyber, physical and electrical protection systems. We first present the main network components and the basic communication modes used in modern autonomous and connected vehicle networks. We explain several common communication security mechanisms that are currently employed and then we describe how these mechanisms can be blended and expanded in order to create a secure communication framework. Finally, we discuss the role of protection of the cyber-physical and cyber-electrical vehicle interfaces and propose a new defense in depth security architecture that adjusts the threat exposure window in a flexible and situation-aware manner.

Recent technological advancements in the area of autonomous and connected vehicle networks promise significant benefits not only in terms of road safety but also in optimizing road use, improving fuel efficiency and reducing emissions. However, utilizing various data and communication technologies combined with the increased reliance on sophisticated algorithms and artificial intelligence increases the potential vulnerabilities associated with these systems. In this chapter, we review the state-of-the-art of mainstream security techniques and tools that are commonly used to provide protection to interconnected autonomous vehicle systems. We discuss the need for new and more comprehensive security architectures that will integrate advanced cyber security mechanisms with existing physical and electrical protection technologies in order to permit efficient and optimal vehicle operation. Finally, we describe the concept of hybrid cyber defense for protecting future autonomous vehicle networks by allowing the coordinated and optimized use of cyber, physical and electrical protection systems.

7.2. Practical Recommendations

Hosting candidates for the HIDS can apply virtualization platforms for deploying the legacies in a more secured way. Persistent threats like advanced persistent threat groups require a more flexible methodology to face them. Regional cyber defense can be deployed using a fleet-based coverage solution. The inner edge firewalls should have their rules updated frequently to deny known accessed persistent malicious command and control networks in the drop zone, block identified devices of previous attacks, and deny repeated access from the same place over different physical locations. The outer edge of manual cut-off could be used on the fly for higher security levels. Automatic cut-off requires additional cyber situational awareness features for successful critical traffic restoration. Digital forensics over autonomous vehicles from highly automated and of lower levels, mostly advanced and pre-autopilot cars, is a forbidding reality today, but it is urgent in consequence of the studying of such a critical subject matter.

We have presented three hybrid cyber defense architectures, namely, Cloud Hybrid Intrusion Detection System (C-HIDS), On-the-Marshalling-Yard Hybrid Intrusion Detection System (OMY-HIDS), and Regional Hybrid Intrusion Detection System (R-HIDS). Now we focus on practical implementation recommendations for these and future works. Cybersecurity is expensive and is an enabler for the mass deployment of autonomous vehicles. The hardware and software for real experimental platforms can be implemented through a combination of commercially available off-the-shelf and open source tools. Real cars of the brands that have autopilot or pre-autopilot features are highly connected smart platforms for executing the proof-of-concept on-route level through long-range telecommunication networks.

8. References

1. L. Chen, Y. Zhang, Y. Wang, and J. Wu, "A Survey of Cyber Security in Smart Grids," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1989-2010, Fourth Quarter 2014.
2. M. M. Hassan, E. Hossain, and A. Alamri, "Cyber Security and Privacy Issues in IoT-Based Healthcare Systems: A Comprehensive Review," in IEEE Access, vol. 5, pp. 6787-6808, 2017.
3. M. S. Hossain, M. Fotouhi, A. Hasan, and R. Hasan, "Cloud-Assisted Industrial Internet of Things (IIoT) - Enabled Framework for Health Monitoring," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1340-1351, Dec. 2017.
4. J. Lin, R. Li, J. Lu, Y. Zhu, and Y. Zhang, "Health-IoT: A Hybrid Health Monitoring Architecture for IoT," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1980-1991, April 2019.
5. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," in Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, Sept. 2013.

6. S. Khan, R. A. Khan, S. U. Khan, and M. A. Aziz, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Information Technology Journal, vol. 12, no. 10, pp. 2477-2484, 2013.

7. T. O. Olwal and C. Odhiambo, "Review of Security Issues in Industrial IoT," in International Journal of Computer Applications, vol. 175, no. 7, pp. 18-24, October 2017.

8. K. Mekki, M. Msakni, and N. Boudriga, "A Survey on Security in Internet of Things: State of the Art and Future Trends," in ACM Computing Surveys (CSUR), vol. 49, no. 4, pp. 1-35, 2016.

9. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized Blockchain for IoT," in Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173-178, 2017.

10. M. M. Alam, M. Rehman, S. U. Khan, and I. U. Khan, "A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts," in IEEE Access, vol. 6, pp. 29847-29857, 2018.

11. K. Yang, X. Chen, P. Sun, H. Wen, and J. Li, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 3144-3154, April 2019.

12. J. Y. L. Loo, R. S. Lee, J. Y. K. Loo, and K. Y. Lam, "A Blockchain-Based Architecture for Secure Data Storage in Decentralized Digital Ecosystems," in IEEE Access, vol. 7, pp. 45470-45485, 2019.

13. Tatineni, Sumanth. "Beyond Accuracy: Understanding Model Performance on SQuAD 2.0 Challenges." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.1 (2019): 566-581.

14. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

15. Shaik, Mahammad, Srinivasan Venkataramanan, and Ashok Kumar Reddy Sadhu. "Fortifying the Expanding Internet of Things Landscape: A Zero Trust Network Architecture Approach for Enhanced Security and Mitigating Resource Constraints." *Journal of Science & Technology* 1.1 (2020): 170-192.

16. Vemori, Vamsi. "Human-in-the-Loop Moral Decision-Making Frameworks for Situationally Aware Multi-Modal Autonomous Vehicle Networks: An Accessibility-Focused Approach." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 54-87.

17. A. A. Gani, S. Khan, A. Y. Zomaya, and M. K. Khan, "Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment," in IEEE Access, vol. 6, pp. 1706-1717, 2018.

18. Y. Xiao, X. Yi, S. Lu, and D. K. Y. Yau, "A Survey of Key Management Schemes in Wireless Sensor Networks," in Computer Communications, vol. 30, no. 14-15, pp. 2314-2341, 2007.

19. H. Zhang, Q. Liu, Z. Chen, and B. Zhang, "E-Health: A Review on IoT-Based Smart Health Monitoring Systems," in Journal of Industrial Information Integration, vol. 18, pp. 100129, 2020.

20. M. M. Hassan, E. Hossain, and A. Alamri, "Cyber Security and Privacy Issues in IoT-Based Healthcare Systems: A Comprehensive Review," in IEEE Access, vol. 5, pp. 6787-6808, 2017.

21. S. S. Kanhere and C. M. R. Prasad, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 55-66, First Quarter 2013.

22. J. Cheng, Z. Zhang, J. Chen, and Z. Jin, "Cooperative Security Defense Framework Against Advanced Persistent Threats in Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2560-2568, June 2018.

23. S. Rahmani, S. Habibi, and J. G. Paredes, "Smart Cities and the IoT: An Investigation of Cybersecurity Challenges," in Journal of Information Security and Applications, vol. 50, pp. 76-90, 2020.

24. A. H. Almohri, F. F. Alharbi, M. A. Jararweh, and M. A. Alzubaidi, "A Survey on the Security of Fog Computing in IoT," in Journal of King Saud University - Computer and Information Sciences, 2020.