World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity and defense in intelligent transportation systems

Sunday Ebenezer Aluko *

Department of Electrical and Computer Engineering, Binghamton University, State University of New York.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 871–879

Publication history: Received on 29 August 2024; revised on 05 October 2024; accepted on 08 October 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0469

Abstract

Intelligent Transportation Systems (ITS) have become increasingly crucial for enhancing transportation networks' efficiency, safety, and security. ITS includes advanced technologies such as electronic sensors, data transmission, and intelligent control technologies, providing better driver and rider services. However, these technologies pose significant security and privacy risks, in which attackers can easily disrupt transportation systems. This paper presents a survey of the challenges with ITS, the engineering requirements, attack challenges, and related work of securing ITS. This survey also discussed the elements of ITS, including advanced traffic management systems, connected and automated vehicles, intelligent infrastructure, and integrated data analytics, as well as the role of government policies, public-private partnerships, and stakeholder engagement. The aim is to look at present security challenges associated with ITS and provide better ways to the system. which is critical for creating smart cities and increasing the importance of individual and public transportation systems.

Keywords: ITS; Security; Privacy; Transportation; Cybersecurity; Defense; Attack; Blockchain

1. Introduction

Intelligent Transportation Systems (ITS) is an essential technology in transportation systems. Several methods have been used to secure ITS. This system helps improve transportation networks' efficiency, safety, and security. Some traditional techniques use advanced electronic sensor technologies, data transmission technologies, and intelligent control technologies. ITS is essential for creating smart cities and increasing the importance of individual and public transportation systems[1]. However, the vulnerabilities in ITS technologies make it easier for attackers to disrupt transportation systems, posing significant security and privacy risks [3]. Therefore, this survey reviews the benefits and challenges associated with deploying ITS and the engineering requirements, attack challenges, and related work of securing ITS. It examines the elements of ITS, including advanced traffic management systems, connected and automated vehicles, intelligent infrastructure, and integrated data analytics. By exploring the security challenges associated with ITS, this survey aims to provide a comprehensive understanding of securing intelligent transportation systems. This survey reviews potential attacks on ITS technologies, the engineering requirements, specifications to make them secure, goals, recent developments, and applications of ITS technologies, including advanced traffic management systems, connected and automated vehicles, intelligent vehicle infrastructure, and integrated data analytics. The benefits and challenges associated with deploying ITS, including safety, mobility, efficiency, and environmental sustainability improvements, as well as cybersecurity, privacy, and equity concerns. It also examines the Elements of intelligent transportation systems, the role of government policies and regulations, public-private partnerships, and stakeholder engagement in shaping the future of ITS.

* Corresponding author: Sunday Aluko.

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

2. Overview of ITS

2.1. Benefits Of Intelligent Transportation System

ITS offers many benefits for transportation systems. Some benefits are that it significantly improves safety, which measures the overall reduction and mitigation of accidents. Increased vehicle connectivity helps expand roadway infrastructure capacity, enhance traffic flows, and provide more personal mobility options for disabled and aging populations, i.e., improved emergency response. The system also enhances productivity and accessibility by providing real-time information on accessible transit and connecting riders with transportation services.

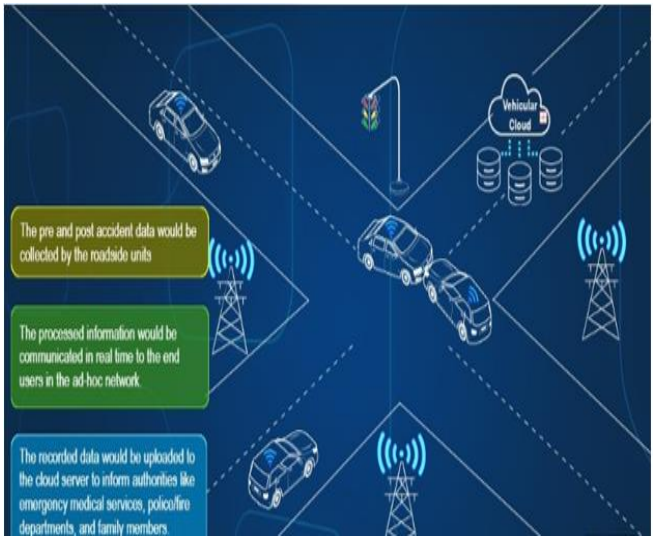

Figure 1 Accident in ITS intersection

Fig. 1. shows an intersection equipped with an intelligent transportation system. In this scenario, an accident occurs where two vehicles collide. Immediately after the event, three things would follow:

- The roadside units would collect the pre and post-accident data.
- The processed information would be communicated in real-time to the end users in the ad hoc network.
- The recorded data would be uploaded to the cloud server to inform authorities like emergency medical services, police and fire departments, and family members as prescribed.

Elements of Intelligent Transportation System

- ***Automation***: with automation features, the intelligent transportation system provides all connected vehicles on the network the exact speed and distances of all other vehicles on the road in real-time, traffic and accident information, and the choice of the optimum route to follow, helpful closed-circuit television (CCTV) images to provide contexts, even weather details and local events that might affect traffic[2]. All this happens in real-time, within automated features.
- ***Information Technology****:* This helps to provide many services to the participants in the vehicular network. Such examples are the ability to access information relevant to the vehicle operation route, the current location, the vehicle operating speeds at each of the locations traveled, the estimated arrival time given all factors, and the level of traffic congestion on the road.
- ***Security Credential Management System*****:** Credential management system is specifically designed for vehicles to its communications. The Crash Avoidance Metrics Partners developed it under a cooperative agreement with the United States Department of Transportation[5]. It issues digital certificates to participating vehicles and infrastructure notes for reliable communications for safety and mobility applications based on Vehicle V2X Communications.
- **Spectrum Knowledge Transfer:** Spectrum knowledge transfer relates to information delivery regarding roadside sensing, which brings together tools and mechanisms that directly capture and convey data measurements from the road. The system can obtain valuable metrics such as speed, direction, traffic flow, and vehicles traversing a road segment[12]. The system also provides structured static data, which refers to data

sources that provide information on elements that directly impact transportation, such as public transportation lines and timetables or municipal bike rental services.

- ***Roadway Reporting*:** Roadway Reporting is to make traffic movement efficient and improve road safety for traffic. Road operators must constantly monitor traffic and current roadway conditions using cameras and sensors for real-time traffic control, such as bus lane cameras, Speed cameras, Roadside weather stations, and Vehicle detection systems. With roadway reporting, we can provide road operators with timely and accurate information.
- ***Traffic Flow Controls*:** Traffic flow controls are a major goal of any intelligent transportation system, similar to roadway reporting systems. Traffic flow on the road helps make high-volume traffic more efficient and makes roads safer. Road operators monitor traffic and roadway conditions in real time and use gathered data to manage traffic flow using various flow control mechanisms. Examples include traffic signal control systems, roadway crossing barriers, dynamic message signs, and automated toll collection. There are several ways in which traffic flow can be controlled in ITS, such as Dynamic Message signs, Traffic Signal Control, Variable speed limits, Ramp Metering, lane control, etc.
- ***Payments Applications and Systems*:** Payment applications and systems are critical in the ITS system. With the help of this system, tolls and fees are being collected by reducing the time required for toll collection and fare payment. With smart payment application systems, ITS operators can incorporate existing systems to increase their revenue stream while reducing. Examples include Radio Frequency Identify (RFID) payments and tags, kiosk payment machines, and e-ticket applications. By combining CCTV with license plate recognition systems, we are using an existing system in collaboration with a new system. All of this system will improve the efficiency of the ITS system.
- ***Communications Applications and Systems:*** Communications applications and the relevant systems provide the necessary information exchange, which is core to the ITS ecosystem. Data is used to make traffic flow more efficient, improve road safety, increase revenue, and reduce the ecological and environmental impact. The users of ITS services also consume data to improve their transit options and experiences. Such uses include smart apps, Social media websites, road obstacles, and accident alerts

2.2. Benefits of Intelligent Transportation System

It offers many benefits for transportation systems. Some of the benefits are that it creates vast improvement in safety, which measures the overall reduction and mitigation of accidents. Increased connectivity of vehicles which helps to expand the capacity of roadway infrastructure, enhances traffic flows and provides more personal mobility options for disabled and aging populations, i.e., improved emergency response; the system also enhances productivity and increased accessibility by providing real-time information on accessible transit by connecting riders with transportation services.

2.3. Attack Challenges On Intelligent Transportation System

like anything else in the ITS domain, intelligent transportation systems face a lot of malicious attacks because they contain valuable data and information as well as valuable targets with many potential vulnerabilities that hackers can exploit. They are several ways an attack can occur in the ITS system.

2.3.1. *Physical Attacks*

The ITS infrastructure is physically exposed on roadways and roadsides, making it accessible to anyone who walks up to it and attacks the system. One of the ways an attacker can attack the system is by connecting to exposed ports. A hacker is physically connecting to exposed ports such as USB [4], as some of these ports may be open and create availability for users. Another cyberattack is the sniffing attack. This is a scenario where an attacker intercept data by capturing the network traffic; if the attacker can successfully capture the network traffic, they use the data to carry out further attacks. Also, an attacker can use scanning method to discover the topology. This is when a hacker scans the secured closed network to discover its topology to carry out man-in-the-middle (MiTM) attacks, where any exposed wires or cables are utilized to intercept data, or by physically tampering with a device to steal or compromise data or modifying a device, etc. [9].

Wireless Attacks. Wireless attacks on the ITS infrastructure can be numerous. One of the attacks could be Spoofing Vehicle-to-Vehicle communication (V2V) and Vehicle-to-Infrastructure (V2l). This is an act of disguising a communication from an unknown source as being from a known, trusted source. MiTM attack is one of the oldest forms of cyber-attacks. In this case, hackers use wireless transmissions to intercept or modify data. Compromised traffic is stripped of encryption to steal, change or reroute that traffic to the attackers. An attacker can also come into the system by using Wireless Fidelity (Wifi) as an entry point into the communication system made for internal vehicle

communication into the controller area. Once the hackers access that, they can move on to the onboard diagnostics, the telematics control unit, and in-vehicle infotainment. All sorts of damage can be accomplished when the Vehicle's high-integrity serial bus system for networking intelligent devices is compromised.

2.3.2. Network Attacks

These attacks typically require some form of psychological manipulation, fooling otherwise unsuspecting users like spearfishing.

Different Types Of Network Attacks in ITS

- The Traditional network-based attack of identifying and abusing device misconfigurations.
- Installing malware or spyware on systems to jeopardize the Integrity of individual vehicular systems or even the entire Vehicle.
- Targeted attacks or advanced persistent threats.

These are stealthy computer attacks, typically launched by a nation, state, or state-sponsored group. They aim to gain unauthorized access to the vehicular network and remain undetected for an extended period until the time comes to strike Social engineering. The vehicular network remains undetected for an extended period until the time comes to strike Social engineering attacks. These attacks typically require some form of psychological manipulation, fooling otherwise unsuspecting users like spearfishing.

Figure 2 Real-world ITS Attacks

Figure 2 shows an example of a real-world ITS attack. Where a man hacked into a sign read and changed it to use caution Zombies Ahead, there are hundreds of similar Real-world cyber attacking incidents against ITS systems.

Engineering Requirements Specifications of Intelligent Transportation Systems

There are two engineering requirements specifications for intelligent transportation systems: user and system requirements. The user requirements are typically statements and diagrams written for customers. In contrast, the system requirements are structured documents containing system functions, services, operational constraints, and the contract between the client and the development team. Engineering requirement specifications for ITS can also be categorized as functional and non-functional requirements[11]. The Functional Requirements explain the system services software type, expected users, and system type work system and also define the input and expected output of the system. At the same time, the Non-functional requirements explained the quality attributes such as usability, efficiency, dependability, security, environment, and regulatory requirements.

3. Related Work

As the ITS becomes so important, to ensure the safety and efficient transportation of people and goods becomes very necessary. Many studies have investigated different ITS security approaches, focusing on specific applications including smart vehicle security or vehicular ad-hoc networks (VANETs)[15]. However, several challenges associated with securing ITS need to be addressed. Nevertheless, a more comprehensive approach is necessary to examine the interactions between various ITS elements, including smart vehicle components, communication networks, and analytics[6]. One approach to securing ITS is using cryptography and encryption techniques to protect the data and communication channels used by ITS[13]. This traditional approach may not be practical for all ITS devices, and Intrusion Detection and Prevention Systems (IDPS) may be vulnerable to false positives and negatives. Addressing these challenges requires a better approach incorporating physical and cybersecurity measures. Measures such as secure hardware modules, secure boot and firmware update mechanisms, and machine learning and artificial intelligence techniques can be used to detect anomalies and potential security threats. Additionally, a risk-based approach can be employed to prioritize security measures based on the level of risk associated with each ITS component.

Another traditional approach to securing ITS is network segmentation, which involves dividing the system into smaller, more manageable network segments[10]. While this can help to reduce the attack surface and limit the potential impact of a security breach, it requires constant maintenance. It needs to address the increasing complexity of modern ITS. These challenges can be overcome by using blockchain technology[7] because it is a distributed ledger technology that helps maintain a secure and decentralized record of transactions. Blockchain-based smart contracts can automate ITS operations, such as toll collection and parking payments, and ensure secure, transparent transactions. It can help create secure and tamper-proof records of vehicle ownership, maintenance history, and accident reports, improving safety and reducing fraud[8].

3.1. Physical and Cybersecurity Measures in ITS

To ensure the safety and efficiency of ITS, incorporating physical and cybersecurity measures is crucial. The security of ITS devices can be improved by using some hardware components, such as Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs) are examples of secure hardware modules that provide secure storage of encryption keys and prevent unauthorized access to sensitive data. Another important security measure is implementing secure boot and firmware update mechanisms.

Advanced techniques such as machine learning and artificial intelligence can also detect potential security threats in ITS data and communication channels. Machine learning algorithms can be trained on large datasets of normal and abnormal ITS behavior to identify patterns of suspicious activity. In contrast, artificial intelligence techniques such as neural networks and deep learning can detect and classify potential security threats in real-time.

3.2. Blockchain Technology in ITS

This is a distributed ledger technology that can help maintain secure and decentralized records of transactions. In ITS, operations, such as toll collection and parking payments, can be automated using blockchain-based smart contracts, ensuring secure and transparent transactions. Blockchain technology also secures communication channels in ITS by providing authentication, authorization, and encryption mechanisms. This saves vehicle ownership records, maintenance history, and accident reports, improving safety and reducing fraud.

3.3. Network Segmentation and Risk-Based Approach in Its Security

Implementing network segmentation is crucial to reduce the attack surface and limit the potential impact of a security breach in ITS. Network segmentation involves:

- Dividing the ITS into smaller, more manageable network segments.
- Isolating critical components.
- Containing the impact of a security breach.

Appropriate security measures can be implemented in these network segments to reduce the attack surface further. The appropriate level of network segmentation can also be determined for each ITS component based on its level of risk. In addition to enhancing security, network segmentation can improve the performance and reliability of the ITS by reducing network congestion and improving traffic flow. Regular monitoring and assessment of network segmentation and security measures are also critical to minimize the impact of potential security threats. We can create a more secure and efficient transportation system by combining network segmentation and a risk-based approach to ITS security.

3.4. Self-Adaptive System

A self-adaptive system fulfills an objective by sensing the environment, analyzing it, and making the best decision, according to its requirements. It can make its own decisions in real-time, which requires a strong understanding of all the tradeoffs between the satisfaction of different requirements.

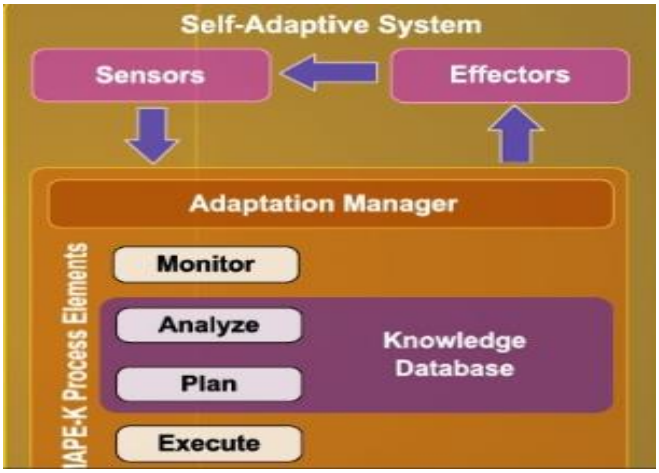

Figure 3 Self-Adaptive System**.**

Figure 4 Self-adaptive using MAPE-K

Self-adaptive systems can be aware of their architecture and thus reconfigure autonomously at runtime to activate only the required modules for a certain environmental state.

This is a system connected to the cloud ITS platform. It relies on sensors that collect data and a special software device combination that can respond to stimuli and execute decisions. They are thousands of sensors in vehicles and the vehicular environment in general, and multiple factors that can act and make decisions. The adaptation manager monitors, analyze plans and executes the decisions. All these decisions are derived from the knowledge database. The model is known from the first letters of each action. Monitor, Analyze, Plan, and Execute (MAPE-K). The letter K stands for the Knowledge Database. The adaptation is implemented through a continuous feedback loop.

The MAPE-K model can provide secure communication in vehicular environments in real time. This is because it can give self-adaptive solutions for different security challenges such as liability identification, message authentication, Integrity, non-repudiation, and attacks against privacy. Figure 4 shows that Intelligent Vehicle A receives a message from Intelligent Vehicle B. Vehicle A can directly communicate back to Vehicle B using the adaptive MAPE-K security model. This model gives effective results regarding security based on specific rules. The adaptation manager can use the monitoring part to check the center's validity. So, in this case, IV(A) can check whether IV(B) is a legal vehicle registered with the certificate center. In addition, it can directly check IV(B)'s certificate in its maintained database containing log information of all previously communicated intelligent vehicles on the cloud. It can also verify the validity with the help of a certification such as a digital signature. Both vehicles IV(A) and IV(B) can use the analysis part of the adaptation manager to analyze the authentication of the messages exchanged. What is analyzed is whether the originator's message is authentic and guaranteed that the message is not intercepted while in transit. The receiver vehicle IV(A) depends on secure communication with the sender vehicle IV(B) using cryptographic protocols that maintain the receiver's privacy. The messages for both vehicles are sent according to plan. They cannot be repudiated, which means that neither the sender nor the receiver cannot deny any message exchange between them[16].

3.5. Methods to Reduce Security and Privacy Risks

Incorporating security features within ITS devices ensures their success and widespread adoption. Additionally, privacy concerns must be addressed during the design phase to safeguard ITS users' personal information and data. This section discusses several possible approaches to mitigate security and privacy vulnerabilities in ITS.

- **Secure ECU Architecture:** Many ITS components are resource-limited, making integrating more robust security protocols challenging[19]. Some researcher has attempted to tackle this issue by proposing innovative Electronics Control Units (ECU) architectures for modern vehicles. They have shown that by incorporating security and dependability at the architectural level, the real-time constraints of automotive control functions can be met in a power-efficient manner. Moreover, the EVITA project has suggested using HSMs to implement security for vehicle ECUs. Although TPMs have been considered a solution for securing vehicular communications, they are costly and must be more robust for ITS use.
- **Secure Generation and Storage of Secret Keys:** In ITS, cryptographic systems' security relies on secret keys, whose disclosure can compromise the entire system's security[17]. Storing secret keys securely poses challenges. Secret keys can be kept in tamper-resistant memories. Nevertheless, numerous attack vectors, such as side-channel, reverse engineering, fault injection, and software attacks, have been developed to assess, clone, and extract secret keys stored in nonvolatile memory. Public key cryptography can be employed to generate secret keys securely.
- **Intrusion Detection Systems (IDS):** It can be implemented in ITS to prevent attacks and safeguard the security and privacy of ITS and travelers. By setting up the rules correctly and including new signatures, IDS can be an effective defense mechanism in ITS against potential attacks. Furthermore, adaptive and evolving IDS inspired by machine learning that relies on statistically detecting anomalies and attack indicators can further mitigate security and privacy breaches.
- **Implementing Security in Resource-Constrained Devices:** Integrating security features in resource-limited ITS devices is complex. Several papers have explored the implementation of security protocols that balance security with the constraints imposed by devices. Additionally, the resource constraints of ITS devices present device management challenges. Sehgal et al. [18] have investigated the requirements of IP-based network management protocols for resource-limited devices. Finally, embedding security features in hardware architecture can help meet the security requirements of devices with limited resources while adhering to the real-time demands of ITS agents.
- **Privacy-Preserving Computing:** Collecting traffic data from thousands or even millions of contributing nodes is necessary for traffic optimization and traffic pattern analysis in ITS. However, the privacy of these nodes must be protected. Privacy-preserving computing can help to preserve data privacy while performing computations on the vast amounts of data collected in ITS-like settings. [15] have proposed new techniques for preserving the privacy of participating parties, which can be adapted to protect the confidentiality and anonymity of parties involved in data contribution for ITS.

4. Conclusions

Intelligent Transportation Systems are a promising technology that can revolutionize the transportation sector by enhancing efficiency, safety, and security. The benefits of ITS range from reducing traffic congestion and improving transportation services to decreasing environmental impacts. However, implementing ITS poses significant security and privacy challenges that must be addressed. This survey has highlighted various approaches to secure ITS, including secure ECU architecture, intrusion detection systems, privacy-preserving computing, and network segmentation. Technology such as Blockchain, Machine Learning applications, Artificial Intelligence can be incorporated to secure the modern ITS ecosystem. As more implementation and integration of ITS systems into transportation, it is crucial to continue exploring innovative solutions to ensure the security and privacy of transportation systems.

References

[1] Y. Zhou, J. Wang and H. Yang, "Resilience of Transportation Systems: Concepts and Comprehensive Review," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 12, pp. 4262-4276, Dec. 2019, doi: 10.1109/,TITS.2018.2883766.

[2] M Veres and M. Mousa, "Deep Learning for Intelligent Transportation Systems: A Survey of Emerging Trends" in IEEE Transaction on Intelligent Transportation Systems. vol. 21, no. 8, pp. 3152-318, Aug. 2020, doi: 10.1109/,TITS.2019.229020 .

[3] L Qi, "Research on intelligent transportation system technologies and applications," in Proc. Workshop Power Electron. Intell. Transp. Syst., 2008, pp. 529–531.

[4] S.-H. An, B.-H. and Lee, Shin, "A survey of intelligent transportation systems," in Proc. Int. Conf. Comput. Intell., Jul. 2011, pp. 332–337.

[5] N.-E. El Faouzi, H. Leung, and A. Kurian, "Data fusion in intelligent transportation systems: Progress and challenges A survey," Inf. Fusion, vol. 12, pp. 4–10, 2011.

[6] J. Zhang, F.-Y. Wang, K. Wang, and C. Chen, "Datadriven intelligent transportation systems: A survey," IEEE Trans. Intell. Transp. Syst., vol. 12, no. 4, pp. 16241639, Dec. 2011.

[7] M. Zichichi, S. Ferretti and G. D'angelo, "A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems," in IEEE Access, vol. 8, pp. 100384-100402, 2020, doi: 10.1109/.ACCESS.2020.2998012.

[8] C. Chen, B. Liu, S. Wan, P. Qiao and Q. Pei, "An Edge Traffic Flow Detection Scheme on Deep Learning in an Intelligent Transportation System," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1840-1852, March 2021, doi: 10.1109/.TITS.2020.3025687.

[9] A. Kashevnik, I. Lashkov and A. Gurtov, "Methodology and Mobile Application for Driver Behavior Analysis and Accident Prevention," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, pp. 2427-2436, June 2020, doi: 10.1109/IITS.2019.2918328.

[10] M. Alam, J. and Ferreira J. (2016). Introduction to intelligent transportation systems. In Intelligent Transportation Systems (pp. 1-17). Springer International Publishing.

[11] Agachai Sumalee, Hung Wai Ho, Smarter and more connected: Future intelligent transportation system, IATSS Research, Volume 42, Issue 2, 2018, Pages 67-71, ISSN 0386-1112,

[12] F.-Y. Wang et al., "Where does AlphaGo go: IEEE/CAA J. Autom. Sinica, vol. 3, no. 2, pp. 113–120, Apr. 2016

[13] F.-Y. Wang, "Artificial intelligence and intelligent transportation: Driving into the 3rd axial age with ITS," IEEE Intell. Transp. Syst. Mag., vol. 9, no. 4, pp. 69, Oct. 2017.

[14] A. P. Athreya and P. Tague, "Network self-organization in the Internet of Things," in Proc. IEEE Int. Conf. Sens., Commun. Netw. (SECON), Jun. 2013, pp. 25–33

[15] H. A. Omar, W. Zhuang, and L. Li, "VMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs," IEEE Trans. Mobile Comput., vol. 12, no. 9, pp. 1724–1736, Sep. 2013.

[16] F. Yu and S. Biswas, "Self-configuring TDMA protocols for enhancing vehicle safety with DSRC based vehicle-to-vehicle communications," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1526–1537, Oct. 2007.

[17] Z. Lu, G. Qu, and Z. Liu, "survey on recent advances in vehicular network security, privacy and trust" IEEE Trans. Intell. Transp. Syst.,vol. 20, no. 2, pp. 760–776, Feb. 2019.

[18] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for V2X communications," IEEE Open J.Veh. Technol., vol. 1, pp. 244–266, 2020.

[19] B. Poudel and A. Munir, "Design and Evaluation of a Reconfigurable ECU Architecture for Secure and Dependable Automotive CPS," IEEE Transactions on Dependable and Secure Computing, 2018