Cyber Attacks Towards Autonomous Transportation System and Assessing Future Threats with Their Solutions

Shobhit Kumar[1], Dr. Arun Kr Rai[2], Hradesh Kumar[3]
[1,3]*Assistant professor, Galgotias University*
[2]*Associate Professor, Galgotias University*

***Abstract*—To increase mobility, comfort, safety, and efficiency, intelligent transportation systems (ITS) integrate sensing, control, analysis, and communication technology into travel infrastructure and transportation. Automobile producers consistently develop the experience of travelling is changing as a result of improvements in transportation technology and infrastructure. With the advent of numerous unique technologies as well as ITS research and development, travelling is becoming more reliable and efficient. Every year, safer cars are developed with increased attention to the safety of pedestrians and passengers. ITS, however, has novel attack vectors due to new technology and growing connectivity. The data gathered about passengers and their travel preferences in smart cities with connected public transportation systems raises significant privacy issues. We present a thorough classification of security and privacy risks in ITS in this study. We also talk about the difficulties in dealing with security and privacy concerns in ITS and think about various mitigation methods. Finally, we highlight future research directions to enhance the security, privacy, and safety of ITS.**

I. INTRODUCTION

Tesla, a maker of electric vehicles, unveiled the most cutting-edge autopilot transport system in October 2014. This system enables a car to independently detect impediments, navigate highways, avoid people, and keep up with traffic. This created a whole new context for how road networks will be used in the future and altered the driving experience forever. Although it will take some time and effort, there are currently more and more internet-connected cars on the road. However, it will be tough to properly adapt fully autonomous vehicles to become an everyday transportation system. It is reasonable to anticipate that in the Industrial Internet of Things (IIoT) era, roads will eventually be transformed into Smart Roads that are fully linked with today's internet-connected cars and tomorrow's autonomous vehicles.

The larger picture of Intelligent Transportation Systems includes many different components, including this future scenario of Smart Roads (ITS). Future urban planning and development, especially in nations with high urban population densities, aims to make high-volume traffic movement more efficient, improve road safety, create new economic opportunities, and reduce ecological and environmental impact. Smart roads and ITS are poised to play a critical role in this process. Because of this, several governmental entities (at the municipal, state, and federal levels) in Asia, the European Union (EU), and North and South Americas are actively funding the creation of ITS technology and regulations.

Along with government organisations and politicians, the IT security sector has acknowledged the significance of ITS and its parts. The study of automotive hacking techniques has led to the discovery of attack vectors against contemporary connected cars and trucks as well as upcoming autonomous vehicles, giving criminals the ability to seize control of vehicle functions, steal data, or both. In this study paper, we looked at cyberthreats against the entire system because it is essential to the safe functioning of both current and future vehicles that the road operating environment be fully understood. This system contains cyberthreats against some other ITS, threats against Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communications. Attacks on ITS infrastructure have been quite rare up until this point.

However, as the number of internet-connected automobiles increases. Attacks against the ITS ecosystem can:

- Lead to vehicle accident and damages
- Lead to traffic jams that can affect essential services, freight movements, and daily commutes
- Lead financial losses to individuals, businesses, and municipalities
- Privacy and Data issues

In this essay, we will first examine actual ITS cyberattacks and their consequences. In order to create and analyse potential future cyberattack scenarios against ITS and Smart Roads, we will first apply our knowledge and expertise of current cyberattacks. We have classified the ITS systems into various Severity Levels, which include public safety, daily operations, privacy, data security, and vital operations, based on the likely worst-case scenario and its consequences.
To evaluate the cybersecurity threats posed to ITS devices and systems, we used the accepted DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) threat model. Finally, we offer a set of recommendations for safeguarding the ITS ecosystem from cyberattacks, including technical discussions for IT security teams and political debates for significant decision-makers.

II. THE ITS ARCHITECTURE

A strategic framework is needed for the design and deployment of extremely complex systems, such as integrated ITS applications, as well as the identification of potential future investment areas. The blueprint for all the technological components of ITS, the ITS framework architecture enables designers and planners to see the organizational, legal, and business requirements. Additionally, it makes sure that the resulting ITS deployment is properly thought out, seamlessly interfaces with other systems, and satisfies the performance and behavior demands of its users and stakeholders. The ecosystem as a whole is easier to manage, maintain, and develop thanks to an ITS framework architecture. Multiple applications will be able to communicate with one another, even at a global scale, thanks to compliance with a standard ITS framework architecture.

III. COMPONENTS OF INTELLIGENT TRANSPORTATION SYSTEM

Cars, trucks, buses, and other types of vehicles are essential elements of transportation, and an ITS discussion would be lacking without mentioning them. Two categories of vehicles are the focus of this study:

- Connected car: A car that has internet connection and a wireless Local Area Network (LAN) that enables it to share internet access with other devices inside and outside the car.
- Autonomous car – A more sophisticated form of linked vehicle, able to sense its surroundings and navigate without a driver's assistance by utilising a number of technologies as LIDAR, RADAR, GPS, stereoscopic cameras, etc.

V2V and V2I: Using the wireless network, vehicles or vehicles and infrastructure can communicate directly or indirectly to improve user safety and mobility.
In some circumstances, we can use a 3G, 4G, or 5G mobile network to connect with infrastructure and vehicles, but its use is constrained by the cost and network performance.
Technology for roadside cameras (RSC): This kind of camera is used to manage traffic and stop accidents. To extract the data from the image and video, the camera is connected to a central computer.
One of the fundamental technologies utilised in vehicles for route direction and navigation is GPS. With the use of this technology, we can specify the position of the vehicle

IV. INTELLIGENT TRANSPORT SYSTEM ATTACKS

Where there are possibilities, there are also trespassers who use the system for their own personal and professional advantage, including monetary gain, retaliation, and protest. The many categories of offenders who pose dangers to ITS infrastructure are covered in this section.

4.1. Physical attacks and risks

Threat evaluations rate physical attacks as the least serious, yet physical damage to infrastructure results in significant financial losses and recovery time. Roadside and highway exposure makes ITS facilities physically accessible to everyone. Physical elements including exposed ports, gauges, and network antennae are vulnerable to malicious actors' tampering, which might result in errors when uploading and reporting data.

4.2. Network attacks and risks

The biggest threat to the development of smart cities and transportation systems is network attacks against ITS. The routine operational processes of devices and equipment are the focus of network assaults and threats, which disrupt services and may result in data breaches and information theft. Cybercriminals frequently utilise malware to spread other malicious payloads that can result in distributed denial of service (DDoS), man-in-the-middle attacks (MiTM), privilege escalation, and other problems.

In addition to causing unneeded and unlawful use of precious resources, intrusions into the systems governing and monitoring these transportation systems can also result in lost money and stolen items.

4.3. Wireless attacks and risks

The backbone of smart transportation and city operations will be wireless communications for V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), and I2I (infrastructure-to-infrastructure), particularly in the interchange of real-time data and reaction deployment. However, as the well-known Jeep hack in 2015 demonstrated, it is neither unheard of or impossible to remotely compromise automobiles using embedded or linked electronics. Unencrypted public wifi connections and flaws in the vehicles or their peripherals can be utilised to take control of moving automobiles. Additionally, server-side security would need to advance from the design stage to distribution, as vulnerable websites, lax passwords, and searchable app data can easily reveal manufacturer customers' data, traffic-control information, or software flaws that enable automated vehicles to unlock and start.

Given the gadgets that manufacturers are incorporating, like voice-activated assistants, known flaws and hacking methods of these linked and smart devices can likewise be utilised to compromise these automobiles. App flaws and gaps can be exploited to hack into, scan for, and seize control of connected transportation and cars as well as vital industries and infrastructure.

V. ATTACKS AGAINST VANETS

The majority of road users will be connected and autonomous vehicles in the future. Vehicular Ad hoc Networks are one of the major technologies linked vehicles will use (VANETs). Smart automobiles and Roadside Units (infrastructure) that are part of VANETs interact using unstable wireless media. Due to their ad hoc nature, VANETs are vulnerable to attacks that could endanger the safety of the road, particularly when vehicles rely on VANET data for important driving choices. The following is a summary of the VANET attack vectors:

- Sybil Attack – A node (vehicle) that assumes many identities. As a result, other vehicles in the network are unable to determine if the data being received is coming from a single vehicle or a group of vehicles. The attacker wants to modify the network to suit their objectives. One of the most deadly attacks on VANETs is the Sybil, which is also one of the hardest to spot.
- A DDoS attack occurs when a system is overloaded with more requests than it is intended to handle. This results in the targeted system crashing or going offline. Attackers may attempt to disable the network built by RSUs in VANETs and halt communications between vehicles and/or RSUs.
- Blackhole Attack – This type of attack involves an attacker node tricking other nodes in ad hoc cooperative networks into sending their data packets through the attacker. Then, the attacker willfully discards the data packets, disrupting

network communication and preventing other vehicles from receiving vital road information.

- Wormhole attacks involve two or more hacked nodes participating in as many routing requests as they can by pretending to know the fastest route to any given location. In order to gather and/or influence significant amounts of network traffic, the attackers want to alter the network's logical architecture and direct all routing requests via themselves.
- False information attacks involve the use of data produced or sent by other vehicles or RSUs by vehicles connected to VANETs. The information sent or received might not be accurate; an attacking vehicle could produce bogus information and send it to the VANET. False information attacks are frequently used to:
- False Location Data—Vehicles are capable of transmitting false location information. This is a major issue since it will generate inaccurate responses from safety-related applications and systems that depend on precise car location data. False position information will also cause data packet loss because it will cause packets to be forwarded to imaginary vehicles.
- Sensor Deception – Attackers can trick in-vehicle sensors by creating fake driving conditions, such as when they brake rapidly over a short distance to create the appearance of a traffic jam so that the car broadcasts an inaccurate traffic jam alert.
- Replay Attack – This type of attack involves storing and then replaying messages to trick other network nodes. The message that is repeated in a replay attack is no longer truthful or valid. By rebroadcasting the cached message, the attacker hopes to recapture and take advantage of the circumstances present at the time the original message was transmitted.
- Attacks that passively eavesdrop on communications or follow the movement of vehicles are referred to as passive eavesdropping attacks. Simple message interception and analysis is all that the attacking node does. The attacker wants to learn more about the cars' communication patterns so they can use that knowledge in future attacks.

VI. COMPARATIVE ANALYSIS OF CONTEMPORARY APPROACHES TO SECURITY AND PRIVACY ISSUES IN ITS

We conduct a comparison analysis of various systems by looking at their benefits and drawbacks in ITS implementations. For instance, employing MACs, which offer message content verification, is a popular method for adding message integrity into ITS. However, using MACs results in significant computing overhead throughout the verification process. Each of the approaches that have been examined has important advantages for ITS, but they also present new difficulties that must be taken into account.

Category	Current Approaches	Advantages	Disadvantage
Confidentiality	Symmetric Key Cryptography	Low computation overhead	Key distribution problem
	Asymmetric Key Cryptography	Symmetric key distribution	High computation overhead
	Steganography	Secure information sharing	High computation overhead
Integrity	Message Authentication Codes	Verification of message contents	Additional computation overhead
Authentication	Challenge-Response Protocols	Verification of sender	Challenge-Response verification time requirement
	Message Authentication Codes	Verification of sender	Computation overhead
Non-Repudiation	Digital Signatures	Link message to sender	Difficult in pseudonymous systems
Availability	Signature-based Authentication	Avoids unnecessary signature computations	Requires additional infrastructure and rekeying scheme

	Proof-of-Work	Prevents false message flooding	Additional computation overhead
Identity Privacy	Pseudonym	Disguise true identity	Vulnerable to pattern analysis
	Attribute-based Credentials	Restrict access to information based on shared secrets	Require shared secrets for all desired services
Behavioral Privacy	Differential Privacy	Limit privacy exposure	True user-level privacy of single data records still challenging
	Public-Key Cryptography	Integra table with hardware	Computationally intensive
Location Privacy	Location Cloaking	Personalized privacy	Requires additional infrastructure
	Homomorphic Encryption	Distributed analysis of data	Computation overhead

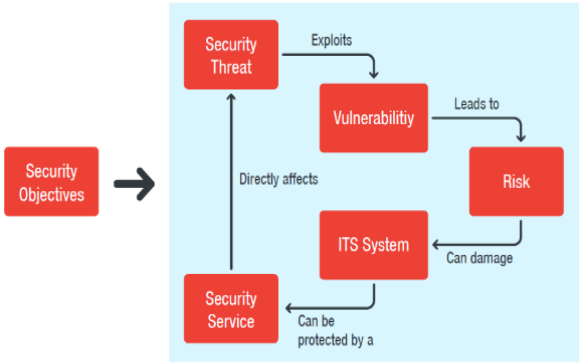
VII. SECURING THE ITS ECOSYSTEM

Since securing the entire ITS system is exceedingly challenging and offering solutions for the entire ecosystem is outside the scope of a single paper, we came to the conclusion that network cyberattacks, followed by wireless attacks and then physical attacks, constitute the greatest threat to ITS. Nation governments, criminal gangs, hacktivists, terrorists, and insiders are some of the perpetrators who target ITS and attack its infrastructure for a variety of purposes.

For ITS operators, cyberattack and data breach prevention techniques should be seen as an essential component of daily business operations. Cyberattacks and data breaches are unavoidable since, in the end, no protection is impregnable against persistent enemies. The complete preservation of an ITS environment depends on having efficient alert, containment, and mitigation systems.

The fundamental tenet of defence is to presume that one has been compromised and to implement the following countermeasures:

- Stop the loss of sensitive data and contain the security breach.
- Secure all potential points of vulnerability to proactively thwart assaults.
- Use the knowledge gained to bolster defences even more and avoid future incidents.



VIII. CONCLUSIONS

Intelligent Transportation Systems (ITS) are undergoing a rapid revolution that offers a plethora of advantages, including improved comfort and safety, increased energy efficiency, decreased pollution, reduced noise, and reduced traffic congestion. However, if security and privacy concerns are not taken into consideration during the design of ITS, it could result in serious security and privacy issues. To maintain a safe and secure ITS, security and privacy must be taken into account while designing both individual ITS agents and the system as a whole. A thorough classification of ITS security and privacy risks has been offered in this study. We have also noted difficulties in dealing with security and privacy concerns in ITS. In following stages, mitigation strategies that can lessen ITS security and privacy risks will be discussed. To help scientists and engineers create ITS that are more secure, safe, and privacy-

preserving, we will conclude by identifying future research directions.

REFERENCES

[1] Swan, M. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self-2.0. J. Sens. Actuator Netw. 2012, 1, 217–253.

[2] M. Javed and E. Znaidi , "Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice," Sensors, vol. 16, pp. 1-25, 2016.

[3] M. Bawangaonwala, D. Wadhwa, U. Nandeshwar, S. Dhurate, S. Ramteke, P. Bante and S. Ansar, "A Review on Development of Intelligent Transport System to Compare with Nagpur Transport System," International Journal of Computer Science and Mobile Computing, vol. 7, no. 4, pp. 12-21, 2018.

[4] J. M. d. Fuentes, A. I. Gonz ´alez-Tablas, and A. Ribagorda, "Overview of Security Issues in Vehicular Ad-Hoc Networks," 2010.

[5] L. He and W. T. Zhu, "Mitigating DoS Attacks Against SignatureBased Authentication in VANETs," in 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE). Zhangjiajie, China: IEEE, May 2012, pp. 261–265.

[6] 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.

[7] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of Resource Constrained Devices in the Internet of Things," IEEE Communications Magazine, vol. 50, no. 12, pp. 144–149, December 2012.

[8] A. Fernndez-Isabel and R. Fuentes-Fernndez, "Analysis of Intelligent Transportation Systems Using Model-Driven Simulations," Sensors, vol. 15, no. 6, pp. 14 116–14 141, 2015.

[9] Branden Ghena and William Beyer and Allen Hillaker and Jonathan Pevarnek and J. Alex Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," in 8th USENIX Workshop on Offensive Technologies (WOOT 14). San Diego, CA: USENIX Association, 2014.

[10] V. J. Hodge, S. O'Keefe, M. Weeks, and A. Moulds, "Wireless Sensor Networks for Condition Monitoring in the Railway Industry: A Survey," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 3, pp. 1088–1106, June 2015