A Review on Intelligent Transportation Systems Safety and Challenges

M. KAVITHA
Ph.D Research Scholar
Department of Computer Science
Gobi Arts & Science College
Gobichettipalayam
kavithalakshmi.m@gmail.com

DR. G.T. PRABAVATHI
Associate Professor
Department of Computer Science
Gobi Arts & Science College
Gobichettipalayam
gtpraba@gmail.com

***Abstract*—Integration of intelligence is becoming an increasinglyimportant part of the transportation system. Attacks on the transportation communications have been limited, but as more vehicles become connected, the threat for cyber attacks increases and hence theneed to secure Intelligent Transportation Systems (ITS) for individual vehicles and public transportation is essential. Defending the attacks iscrucial for the safe and efficient transportation. Various solutions are proposed by researchers to deal with the vulnerabilities of systems, overcome the outside threats and to diminish the risks of attacks that can be faced by ITS. The motive of this paper is to review ITS security, challenges and solutions.**

Keywords—*Intelligent Transportation Systems, Attacks, Security, Authorization.*

I. INTRODUCTION

Integration and communication technologies play an important role in transportation and traffic management systems. Integration of intelligence to transportation and traffic management systems is needed to improve the safety, efficiency, and sustainability of transportation networks, to reduce traffic jamming and to enhance drivers' experiences. The grouping of intelligence, information and communication technologies results in Intelligent Transportation Systems (ITS). These additional technologies get added to the transportation and traffic management systems, the facade area for the attack increases. The concept of cyber security is applied in multiple areas. Considering the scratch these attacks can allow to run free, it is very crucial to have a robust protection measures, that to address the Vulnerabilities of systems, to overcome the external threats to the systems, and to reduce the risks of attacks that can be faced by ITS [2]. Research in the field of Intelligent Transportation Systems is very active and is varied in multiple areas. Technology used in vehicles and transportation management continues to evolve and improve.

The objective of this paper is to provide a survey of security challenges and solutions in regards to securing intelligent transportation systems. As Per the literature review, there is limited research regarding cyber security threats against ITS. This survey focuses about the challenges faced by ITS security and the solutions to these challenges. There are a wide range of avenues that ITS security can be breached and one common solution cannot be used for all systems. The rest of the manuscript is organized as follows: Section 2 describes the security challenges for ITS. Section 3 describes the background study of various researches in ITS security. Section 4 outlines the solutions to protect the ITS and lists out the open issues. Section 5 concludes the review.

II. SECURITY CHALLENGES

It is important to identify the risk factor for ITS. Intelligence from other nations, criminal gangs, hacktivists, cyberterrorists, insiders, unscrupulous operators, and natural disasters are all described as prospective attackers to ITS. Criminal gangs use different schemes to hack ITS for the purpose of generating illegal income. Cyber terrorists attack ITS to cause damage of property, life loss, and spreading terror. Insiders attack an organization that they are currently or were parts of, with the attack indirectly acting against the insider's personal interests. Unprincipled operators could hit ITS to evade fines and fees, avoid traffic, sabotage competitors, among other intentions. ITS systems are slightly unusual in that they are highly visible and results in a large impact when the systems are attacked. The attackers motive may be data theft, information warfare, system gaming and theft, or retribution and violence. The message can be acquired by physical, wireless, or network attacks. When a ransom attack occurs, attacks will encrypt data and systems. Decryption keys are not given until a rescue is paid. Attacks can access a connected car and disable functioning until a ransom is paid. Stolen information can be used for a variety of reasons.Individual gains are intended for a data pilfering.

Information conflict includes denial-of-service attack on the ITS infrastructure. This causes the systems to collide and causes confusion on roadways. It can also be used to send messages of political positions, protests, or high jinks. This can hurt the company's name and effect in economic loss. Traffic chaos can be created if a false vehicle-to-vehicle (V2V) communication is transmitted. V2V information toxin can be initiated by this attack. Map hacking can also be used to conciliation position transmitters, GPS receivers, and GPS signal spoofing. The ITS systems are also exploited to evade paying fees and service charges. Self-governing vehicles can be hacked and instructed to a remote location where a theft of valuables, vehicle parts, the whole vehicle, or abduction is possible. Paying service charges can be avoided by a utilization of an ITS system. Mobile Infrared Transmitters(MIRT) can alter a traffic light, controlled by a PC, using a distant activator. A competitor's car may be hacked to undermine rivalry and build the vehicles occupied. A circumstance can be created where self-governing vehiclesneed to make way for a hacked vehicle that has been assigned high precedence. False orders for rideshares can be

placed to charge unsuspicious customers. Driving functions can be compromised and used as weapons. Envisage and protecting against these types of attack is very difficult. Hacking ITS systems is usuallydone for the goal of using the ITS system as an access point into the ITS environment. A victorious assault on the ITS system gives right of entry to the ITS ecosystem that is connected via the internet or VPN [9]. Gaining right of entry deep inside the network is achieved with little effort. Attacks can be launched from inside the network when an attacker has access to the network. Substantial attacks are easily conducted for the reasonthat the ITS infrastructure is exposed on the roadways. A device can be accessed using monster force or guessing credentials. Topology can be exposed by scanning a protected or closed network. An ITS device or system can be compromised by deleting files. Firmware can be installed to recover credentials and configurations. Man-in-the-middle attacks capture data using exposed wiring or cables and can send false information to the backend servers. Devices can also be compromised or tampered through trusted operators' abuse of authority. Wireless attacks pose a major IT security warning to and ITS infrastructure. Spoofing communication can be transmit, sniffing wireless transmissions can be complete, wicked firmware can be remotely transmitted and installed, wireless transmissions and vehicle safety systems can be electronically jammed, man-in-the-middle attacks can be conducted to intercept and modify data, vulnerabilities canbe exploited, and Wi-Fi can be used to gain access to controller area network (CAN) bus and the on-board diagnostics, infotainment, and the telematics control unit.[10] The CANbus can be conciliation by remote hijacking and malicious third party apps can be installed. Network attacks are a danger because ITS systems areexposed to the Internet and discoverable on IoT search enginesmaking them vulnerable to cyber attacks [7].The attacker discards the data packets and communication is mislaid in the network. False location information is an attack whereby false location information is broadcast by vehicles. Safety-related application and systems turn into compromised because motor vehicle location information will respond wrongly. This results in lost data packets because the data packets are forwarded to phantom vehicles. Sensor deception involves simulating false driving conditions. In-vehicle sensors can be deceived by an assailant. Passive snoop attacks happen when the network is being monitored by an attacker to track vehicular movement, or listen to communications in vehicles. Attacker vehicles intercept messages and the messages are examined. Information is gathered regarding the motor vehicles and message patterns to use in future attacks.

III. Related Works

M. Alam, J. Ferreira et al. [9] suggested as the volume and density of vehicles increases, technological advancements have developed new way to manage traffic. The Intelligent Transportation Systems applies these technological advancesto road transport. Information is collected from sensors and equipment in vehicles and infrastructures. This information can be used to improve the current transportation systems. Road and traffic safety, traffic efficiency, and value-added applications aim to improve the transportation system.

A Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey was proposed by Vaibhav, D. Shukla et al. [5] V2V information is used to reduce the risk of car accidents and minimize the damage that results from accidents that are unavoidable. The applications that are used for traffic efficiency aim to improve the flow of traffic by helping to reduce travel time and congestion of vehicles. Value-added applications include infotainment, information on travel, trip planning, and access to the Internet. Wireless communications among and between vehicles and the road side infrastructure are required for ITS.

Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges was presented by Dalton A. Hahn, Arslan Munir et al. [11]. A common approach to security classification is used with the scheme CIA (Confidentiality, Integrity, and Availability) and it avoids the confusion with the Central Intelligence Agency. Here the author classified the common security issues in ITS in the CIA dimension. Virtually all of the machine learning techniques are prone to intrinsic vulnerabilities that can be exploited to compromise the security of ITS. While AI safety and security research is gaining traction, it would be of interest to study the relevant aspects of this research to ITS technologies.

AI techniques may prove to be of significant value in automating the discovery, mitigation, and defense against security threats within the highly complex ITS. Further researchon such techniques can facilitate more efficient approaches to the design and management of secure ITS technologies. Incorporating AI techniques for tackling Transportation threats was given by V. Behzadan and A. Munir et al.[12].

Roopa Ravish Shanta Ranga Swamy et al.[13] revealed that ITS used wireless network systems to gather the data about vehicles and performed significantly well. However, high expense of antennas limits its application. Further, variousstudies with different technologies in managing traffic indicated that the application of a specific technique relies on the nature of location, where the traffic needs to be managed. The review pertained to the application of different technologies in managing traffic revealed that the application of deep learning technologies and certain optimization algorithms like Ant and Bee algorithms provided better results in managing traffic. The various technologies used for predicting accurate travel time through the detection of traffic congestion signposted that technologies designed on two models provide a better accuracyin the detection of vehicular congestions, thereby predicting travel time with a high degree of accuracy.

Huq, Rainer Vosseler, and Morton Swimmer et al. [14] suggested Cyber attacks and breaches are inevitable, but embattled attacks that are state sponsored and advanced persistent threats are possible. Wicked firmware can be uploaded and installed. Distributed Denial of Service (DDoS) attacks can be launched on the ITS communications and backend servers that are bare to the internet. Malicious draft can

be injected as advertisements. Hazard to ITS can contain cross-site scripting (XSS), where malicious script is inserted into the network. Structured query language (SQL) injection is one of the

most common webs hacking technique. Meeting hijacking involves exploiting a suitable computer session. DNS spoofing and hijacking involves the name server returning a wrong IP address. Trusted operators could abuse their authority and compromise the systems or devices. Computers of a third-party outworker can be compromised and used to access the corporate network. Vehicular Ad hoc Networks (VANETs) are vulnerable to attacks that can affect roadway safety [15]. Sybil attacks are one of the most hazardous attacks and can be very difficult to detect. They involve a motor vehicle appearing to have more than a single identity. Data received from this vehicle cannot be determined if it is coming from one vehicle or multiple. Attackers use this to form the network according to their purpose. A black hole assault involves data packets being routed through the attacker. False location information is an attack whereby false location data is broadcast by vehicles.

Targeted attacks that are state sponsored and advanced persistent threats are possible. Malicious firmware can be uploaded and installed. Distributed Denial of Service (DDoS) attacks can be launched on the ITS infrastructure and backend servers that are exposed to the internet. Malicious script can be injected as advertisements [16]. Risks to ITS can include cross-site scripting (XSS), where malicious draft is inserted into the network. Structured query language (SQL) injection is one of the most common webs hacking technique. Meeting hijacking involves exploiting a legal computer session. DNS spoofing and hijacking involves the name server returning a wrong IP address. Trusted operators could abuse their authority and conciliation the systems or devices. Computers of an intermediary contractor can be compromised and used to access the corporate network. Vehicular Ad hoc Networks(VANETs) are vulnerable to attacks that can distress roadway safety. Sybil attacks are one of the most hazardous attacks and can be very hard to detect. They involve a motor vehicle appearing to contain more than a single uniqueness. Data received from thismotor vehicle cannot be determined if it is coming from one motor vehicle or many. Attackers use this to form the network according to their goals. A black hole assault involves data packets being routed through the attacker [5].

IV. CHALLENGES & SOLUTIONS

Next-generation firewalls and UTM gateways bring multiple systems and services together as a single engine or appliance. Network traffic at line speed analyzes devices with subordinate traffic. Anti-phishing solutions check email for incoming spam and phishing emails and block these emails. Malicious attachments pretense a probable hazard and can be screened using message sandboxes as part of anti-phishing solutions. [16] Man-in-the-Middle (MitM) attacks can be defeated using encrypted network traffic. Physical and virtual scrap organization software updates endpoints, servers, and remote computers. Data fusion software on a motor vehicle canrecognize the true condition of the motor vehicle. It can also provide information about the vehicle's surroundings. Data received from all sources is compiled and reported. Attacks can be identified and compensated for depending on the information that is still available in the vehicle. These data fusion systems can potentially assist in the identification of anomalous inputs from cyber attacks.

Biometrics is an authentication technique that measures physiological and individual characteristics. These characteristics are then automatically verified. Biometric systems are important in the future of security. A biometric system is an automated system. The system collects information about specific characteristics. The information is then distributed, stored and processed within the system. Aresolution is prepared as to whether or not to approve the user. The safety of the whole ITS system is increased with the use of biometrics, and the risk of impersonation is reduced. Information and countermeasures can be shared regarding cyber threats and attacks. A huge amount of daily user information is generated in the ITS ecosystem. Storage space ofthis information needs to be protected and data access usage policies need to be strict. Minimum security standards should be codified by legislation for new ITS applications and systems before approval is given for use on roadways.

The policy recommendation of coordinating ITS frameworks can be challenging because of an unwillingness to collaborate and exchange information. This could be due to reputational costs, pressures from competition, and losses that may results from cyber-crime. Information may not be available for sharing because necessary systems or measure may not have been implemented. Another challenge for solutions is necessary importance is not given to cyber security and as a result, spending is inadequate. There is a lack of awareness and acquaintance of cyber security that is efficient and that which is not effective. Knowledge of the range of cyber threats and being able to secure ITS can be challenging. Cyber security can be implemented, but if there is limited knowledge on how to use the software, it is not as effective as it could be [4]. Countermeasures can be an effective way to prevent and resolve cyber attacks, but if there is resistance to security adoption the ITS is at increased risk as attacks are evolving and penetrating the ITS ecosystem. Balancing the security, convenience and functionality of security vectors needs to be evaluated for use in the ITS ecosystem.

Table.1 Lists out the possible types of attacks and chaos due to attacks.

TABLE 1 ATTACKS AND OUTCOMES

Type of Attack	*Description of Attack*	*Outcome of the Attack*
DDoS Attacks	Vehicle to Vehicle message; Electronic Jamming	Chaos on Roadways; Service not available tolegitimate users
Revenge and Terrorism	Hacking ITS to get theattacker access to the systems	Driving functions are compromised and usedas weapons
System gaming and theft	Hacking the autonomousvehicle	Avoid paying fees andtolls. thieving vehiclesor goods from vehicle
Physical Attacks	Brute force; Reconnaissance and Manin the Middle attacks.	Compromised or Tampered ITS devices.
Wireless Network Attacks	Sniffing wireless communications; Jammingof vehicle safety systems; Man in the middle attacks.	Gain access of controller area networkand on-board diagnostics, infotainment and telematics.
Wired Network Attacks	DNS Spoofing and hijacking; Malware; Spyware; SQL Injectionand Cross Site Scriptingattacks	Targeted state sponsored attacks that pose constant threats.
VANET Attacks	Sybil attacks; Black-hole attacks; Wormhole attacks	Fake location data is broadcast by vehicles;Safety-related applications and systems become compromised.
V2V	Wireless attacks; An ad hoc mesh network attacks	Prevent accidents by allowing vehicles in transit to send position and speed data to one another

V. CONCLUSION

ITS environments are constantly evolving and threats to these systems evolve as well. There is a large scope of improvements that can be made in various areas. Further, security of transportation is an emerging area of research.There is various shortcomings in current models used by ITS environments which are discussed in earlier sections. Additional research is needed to evaluate intelligent solutions that are specific for the various types of ITS systems and applications. Further research is needed on cooperative transportation systems towards identification of cyber threats and the development of strategies to protect against them. Biometric systems are crucialto the future of cyber security of ITS and various researches are there tacking for the solution. This paper attempted to review the Intelligent Transportation Systems Safety and Challenges.

REFERENCS

[1] J. Zhang, F. Wang, K. Wang, W. Lin, X. Xu, and C. Chen. "Data-driven intelligent transportation systems: A survey." IEEE Transactions on Intelligent Transportation Systems 12, no. 4 (2011): 1624-1639.

[2] K. Qureshi, and A. Abdullah. "A survey on intelligent transportation systems." Middle-East Journal of Scientific Research 15, no. 5 (2013): 629-642.

[3] A.S. Elmaghraby, and M. M. Losavio (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research, 5(4), 491-497.

[4] M.A. Javed, B. Hamida, and W. Znaidi, (2016). Security in intelligent transport systems for smart cities: From theory to practice. Sensors, 16(6), 879.

[5] A. Vaibhav, D. Shukla, S. Das, S. Sahana, and P. Johri. "Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey." IJ Wireless and Microwave Technologies 3 (2017): 36-48.

[6] Guerrero-ibanez, J. A., Zeadally, S., & Contreras-Castillo, J. (2015). Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. IEEE Wireless Communications, 22(6), 122-128.

[7] K. Kelarestaghi, K. Heaslip, M. Khalilikhah, A. Fuentes, and V. Fessmann. "Intelligent transportation system security: hacked message signs." SAE International Journal of Transportation Cybersecurity and Privacy 1, no. 11-01-02- 0004 (2018): 75-90.

[8] E. Bubeníková, M. Franeková, and P. Holečko, P. (2013, October). Security increasing trends in intelligent transportation systems utilising modern image processing methods. In International Conference on Transport Systems Telematics (pp. 353-360). Springer, Berlin, Heidelberg.

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

[10] S. Chakraborty, and S. Ramesh. (2016, January). Technologies for Safe and Intelligent Transportation Systems. In VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), 2016 29th International Conference on (pp. 56-58). IEEE.

[11] Hahn, Dalton A., Munir, Arslan; Behzadan, Vahid (2019). Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. IEEE Intelligent Transportation Systems Magazine, 1–1. doi:10.1109/MITS.2019.2898973

[12] V. Behzadan and A. Munir, Adversarial Reinforcement Learning Framework for Benchmarking Collision Avoidance Mechanisms in Autonomous Vehicles (2018). arXiv preprint arXiv:1806.01368, 2018.

[13] Roopa Ravish, Shanta Ranga Swamy Intelligent Traffic Management: A Review of Challenges, Solutions, And Future Perspectives (2021). Transport and Telecommunication, 2021, volume 22, no. 2, 163–182. DOI 10.2478/ttj-2021-0013

[14] Numaan Huq, Rainer Vosseler, and Morton Swimmer Cyberattacks Against Intelligent Transportation Systems: Assessing Future Threats to ITS (2017). TrendLabs Research Paper, 2017 - computing.es.

[15] E. Bubenikova, J. Durech, and M. Franekova. (2014). Security solutions of intelligent transportation systems applications with using VANET networks. In Control Conference (ICCC), 2014 15th International Carpathian (pp. 63-68). IEEE.

[16] Guerrero-ibanez, J. A., Zeadally, S., & Contreras-Castillo, J. (2015). Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. IEEE Wireless Communications, 22(6), 122-128.

[17] J. Chelladhurai, P. Chelliah, and S. Kumar. "Securing docker containers from denial of service (dos) attacks." In 2016 IEEE International Conference on Services Computing (SCC), pp. 856-859. IEEE, 2016.

[18] S. Chakraborty, and S. Ramesh. (2016, January).Technologies for Safe and Intelligent Transportation Systems. In VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), 2016 29th International Conference on (pp. 56-58). IEEE.

[19] S. Kumar, "Classification and review of security schemes in mobile computing." Wireless Sensor Network 2, no. 06 (2010): 419.

[20] S. Kumar, and B. Xu. "Vulnerability assessment for security in aviation cyber-physical systems." In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 145 150. IEEE, 2017.