International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CYBER SECURITY RISK ANALYSIS FOR INTELLIGENT ROAD AND RAIL TRANSPORT

Mohammed A. Althamir[1*], Abdullah Khalid Bazaid[2]

[1*,2]King Fahd Causeway Authority, Khobar , 34619, Kingdom of Saudi Arabia [1*]Email Id:- malthamir@kfca.sa, Ochid Id: 0009-0003-3151-7512 [2]Email Id:- abazaid@kfca.sa, Orchid Id: 0009-0003-0463-6874

Abstract

Transport infrastructure has evolved from the standard electro-mechanical vehicles and trains to an interconnected machine capable of communicating with other vehicles and trains, and external infrastructure built to share information with the vehicles. The interconnection of vehicles helps with traffic control and management and the efficient use of transport infrastructure and energy. However, interconnecting vehicles raises a security concern, as a cyber attacker can penetrate the network used by the vehicles to launch an attack on them by misdirecting them, stealing information, or jamming the communication. In most situations, a cyber-attack on vehicles or trains can lead to loss of lives as the attacker controls the vehicle or train. The current paper conducts a risk analysis on intelligent transport systems and connected and automated vehicles to determine the likelihood of cyber-attacks and their impact on passengers and the transport infrastructure. The research further suggests solutions to the problem and offers insight into topics for further research on protecting connected vehicles on the roads.

Index Terms – Transport, cyber-attack, Intelligent Transport System, jamming, information, interconnection

Table 1: List of Abbreviations Used

ACRONYM	MEANING
AODV	Ad hoc On-demand Distance Vector
GPS	Global Positioning System
IDS	Intrusion Detection Systems
ITS	Intelligent Transport System
KNN	K-Nearest Neighbor
LiDAR	Light Detection and Ranging
LoRaWAN	Long Range Wide Area Network
RSU	Road Side Unit
SVM	Support Vector Machine
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle

1. Introduction

Intelligent transport system (ITS) is one of the pillars of smart cities. An interconnected transport system improves the safety of passengers, increases mobility, and uses the existing transport infrastructure efficiently. ITS also reduces environmental degradation through data exchange between vehicles or trains, users, infrastructure, and the environment [1]. ITS systems rely on the interconnection of vehicles and trains with their transport infrastructure, such as roads and railways, with roadside units placed strategically to transmit information from the vehicles to the infrastructures and vice versa. Though the interconnection improves traffic, safety, and mobility, it has its limitations, with cybersecurity being the major hurdle to a secure and safe ITS. The networks used in ITS are prone to attacks that can lead to catastrophic consequences for the people involved.

The core components of ITS include RSUs, GPS, mobile networks, and intelligent vehicles communicating with each other (V2V) and with the infrastructure (V2I). Figure 1 below shows an ITS. The Connected and Autonomous Vehicles (CAVs) have sensors, GPS, and communication systems that enable them to communicate with each other and the RSUs, enabling them to navigate traffic, optimize their routes, and thus reduce congestion. The data from CAVs and RSUs is analyzed in the cloud in real-time to reduce congestion and optimize traffic flow [1]. An ITS offers many benefits to users through better transport management and reduced congestion and accidents.

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

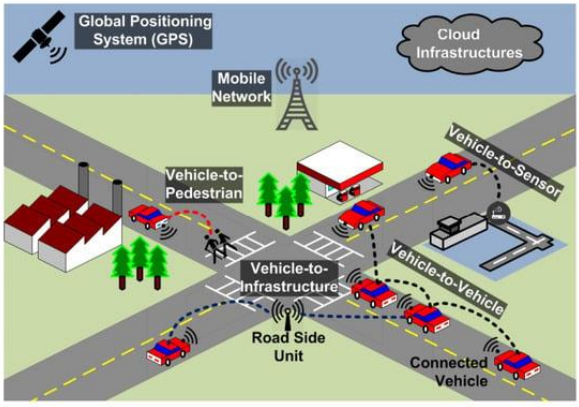

Figure 1: Overall Design of Intelligent Transport System [1].

The Intelligent Railway System is no different as it uses the same concepts as ITS, with cloud computing, network communication, data analysis, and intercommunication between trains and the infrastructure shaping its architecture, as shown in Figure 2. The system is a closed-loop model with people, environment, equipment, and management forming the four pillars of the loop. The use of intelligent systems and networks in railway and road transport has also led to the use of artificial intelligence for fault diagnosis, data analysis, and security [2].

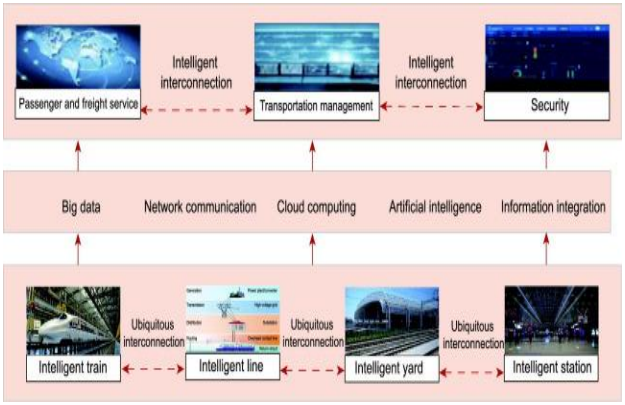

Figure 2: An Intelligent Railway System [2]

Despite the many advantages of intelligent transport systems, they expose the infrastructure and people to new attacks. Previously, most vehicles and railway systems were made of electro-mechanical systems and sensors that could not be controlled outside the car or train. Modern vehicles and trains can be controlled remotely as they are interconnected to other infrastructure through a network. Cyber attackers are now targeting vehicular and railway systems for sabotage and financial gains. In 2023, the Polish railway system suffered a cyber-attack that interfered with its radio frequencies, with a "radio-stop" command forcing about 20 trains to trigger their emergency stop function [3].

In New Zealand, the Auckland Transport system was attacked twice in 2023, disrupting ticketing services and later a DDoS attack. Estonian national railway carrier was attacked in 2023, with DDoS disrupting its ticketing system, resulting in passengers traveling for free. Transport for London was attacked in 2024, with personal details, including bank accounts of 5,000 customers being compromised, and another 30,000 employees being affected as they had to reset their passwords with the help of IT professionals in person [3]. Such examples show the vulnerabilities of using an intelligent and interconnected transport system. The shift to the use of networks, cloud, and interconnection exposes trains and vehicles to cyber-attacks.

Some attacks can lead to collisions, accidents, and loss of lives. Cyber attackers can access the braking systems and steering and control the car's acceleration, with untold consequences [4]. Such access gives the attacker total control of the vehicle, steering it to their desire which can include making an accident. Such control can be disastrous on a national scale for trains, gauging by the number of passengers on a single train.

A risk analysis of the transport systems considers the likelihood of the risk occurring and the consequences of the risk [5]. The risk analysis also helps identify mitigation techniques for the risk elements. Table 1 below shows the risk assessment tool showing the risks and their ratings. From the table, both rail and road transport systems paint a grim picture where a cyber-attack is an extreme risk as it is almost certain a cyber-attack will occur, and the consequences can be catastrophic (Table 2) for some risks.

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 1: Risk Rating Assessment Tool

Consequences					
Rating	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	High	High	Extreme	Extreme	Extreme
Likely	Medium	High	High	Extreme	Extreme
Possible	Low	Medium	High	Extreme	Extreme
Unlikely	Low	Medium	Medium	High	Extreme
Rare	Low	Low	Medium	High	High

Table 3: Risk Consequences [5]

Rating	Description
Insignificant	Impact can be easily absorbed without requiring management effort
Minor	Impact can be readily absorbed but some management effort is required
Moderate	Impact cannot be managed under normal operating conditions; requiring moderate level of resource and management input
Major	Impact requires a high level of management attention / effort and resources to rectify
Catastrophic	Disaster with potential to lead to business collapse and requiring almost total management attention / effort to rectify

Controlling a car or railway will undoubtedly lead to accidents or loss of lives for the occupants. The risks involved in intelligent transport systems are technological, as they involve the introduction of new technological innovations that make it difficult to estimate the overall impact of their use on passengers, drivers, and the general public [6].
Risk analysis shows the severity of the risk, which in this case is the consequences and severity. The consequences of most cyber-attacks on intelligent transport systems are catastrophic. One of the reasons for such a conclusion is the severity of the risk, which factors in the blast radius of the damage from the problem [7]. A compromised vehicle or node in the ITS transmits false information received by all vehicles and infrastructure it is communicating with, increasing the blast radius of the wrong information and, thus, the consequences of incorrect data. Also, the attack vector determines the severity of the attack, with a compromised vehicle's control system affecting the passengers in the vehicle, while a compromised train affects hundreds of passengers in the train and thousands of other passengers waiting for the train at the station.
The current research aims to investigate the risks posed by transport systems in road and rail transport systems due to the introduction of interconnectivity. The study explores the severity of the risk, the probability of a cyber-attack, and its impact. The study also shows methods to mitigate against the risks, proposing security technologies to use to reduce cyber-attacks on transport systems which are part of critical infrastructure of any nation.

2. Problem Statement

Intelligent transport systems have ushered in a new era of vehicle interconnectivity, with vehicles acting as nodes and transmitting information to other vehicles or RSUs. The vehicles are interconnected using a wireless network that requires low latency due to the nature of the information transmitted. However, introducing an interconnected transport infrastructure exposes the entire infrastructure, consisting of vehicles, RSUs, and traffic monitoring systems, to cyber-attacks. The whole system is also exposed to a wide blast radius as a compromised vehicle transmits wrong information to all vehicles and RSUs in the vicinity, leading to incorrect data that can lead to traffic congestion or accidents. CAVs are prone to cyber-attacks and are thus a risk. There is a need to assess and analyze the risks posed by interconnecting the entire transport system, which helps determine mitigation strategies.

3. Selection of Papers for Literature Review

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.1. Search String

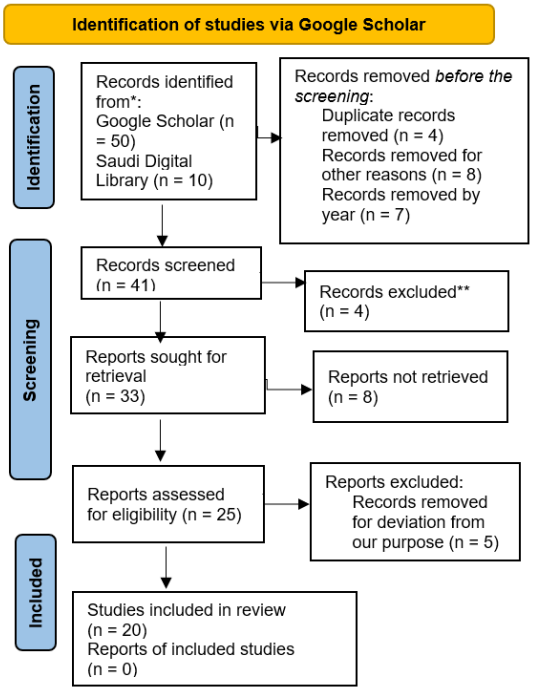

Figure 3: Criteria Used to Select Research Papers Using PRISMA

The PRISMA model shown in Figure 3 above was used in the search for scholarly journals to use in the present study. More than 60 peer-reviewed journals were used in the study, out of which only 20 articles were chosen for the final literature review. The inclusion criteria for the final 20 papers included papers discussing the following:

1. The year of publication
2. Technical vulnerabilities in modern interconnected transport system
3. Causes of security vulnerable in vehicles and railway systems
4. Year of publication

The exclusion criteria used included:

1. Research papers discussing human errors.
2. Articles do not peer reviewed.
3. Research papers discuss the working of transport systems as the research focuses on cybersecurity only.
4. Articles written more than five years ago, as they do not have current information about technology used in intelligent transport systems.

3.2. Research Paper Selection

The scholarly journals had to meet the following terms germane to the study: cybersecurity of intelligent transport systems, security of railway systems, cybersecurity of intelligent railway systems, security challenges of interconnected railway systems, cybersecurity of connected and autonomous vehicles, and cyber-attacks on connected and automated vehicles.

4. Background and Context

The security of modern transport systems is critical for nations as people's lives are at stake. Intelligent transport system is made to reduce congestion, save energy, provide information about the status of roads, and thus avoid some paths when traveling. However, as they are being implemented, it is not secure, and a lot needs to be done to ensure passengers are safe. Over the last few years, the world has witnessed various cyber-attacks on transport systems in different countries, exposing the vulnerabilities in the infrastructure used by millions of people in any given country. Technology has improved the transport sector but exposed its underbelly as the entire industry has relied on electromechanical equipment for centuries and thus has no clue on how to deal with an interconnected and highly mobile system. A risk analysis shows the levels of risks and their impact on people and economy.

5. Challenges and Techniques

The study [8] conducts a risk analysis of ITS, which has varying security threats. Among the most common threats are eavesdropping to determine the type of vehicle and its communication systems. Impersonation attacks are common, where

a vehicle pretends to be another vehicle and spoofing attack which also impersonates another vehicle. Jamming can happen in vehicles to deny them communication, resulting in a denial of service, while flooding overloads the communication system to deny vehicles communication. In some instances, a man-in-the-middle attack can happen where attackers receive information from one vehicle, read it, at times change its contents, forward it to the other vehicle, or drop it altogether (blackhole). The study classifies the threats as critical, with high levels of occurrence, and can cause damage to people. The study proposes different solutions, such as encrypting all communications, authentication using cryptographic digital signatures, and secure routing protocols.

The study [9] exposes the security risks of integrating cyber and physical systems in railway systems. The new system has led to the overdependence of rail operations on cyber and IoT technologies to cut costs and for business growth. However, such systems expose the entire train network to cyber attackers whose sole purpose is sabotaging train operations, damaging physical components, injuries, and losing lives. The study suggests threat identification using technical decomposition, where each interaction is investigated to determine attack flows. Consequence analysis is later performed for risk management and to determine the solution to the problem. The risk factor of a railway systems attack is extreme, as the study shows in the cyber-attacks on Iran's, the UK's, U.S, and Polish rail systems.

The research [10] studies common attacks and solutions that affect ITS. Vehicular networks suffer from security attacks targeting different layers of the network protocols. There is the manipulation of routing protocols to redirect traffic in wormhole attacks, relaying information, or destroying incoming packets to ensure the receiver does not receive and read the message. Jamming attacks also occur at the physical and MAC layers, blocking all communications within the range of the jammed signal. Constant and random jamming attacks are easy to detect as they broadcast constantly or randomly without following communication rules. However, reactive jamming happens in the physical channel communications, preventing information flow. The article suggests using pre-trained machine learning models to detect reactive jamming, which perfectly matches communication activities. The risk posed by reactive jamming is critical, as the impact of jamming communication between vehicles and transport infrastructure is catastrophic. People's lives are at stake, as jamming can lead to accidents.

The study [11] delves into the application of blockchain in VANET. The network systems lack trust, making communication between vehicles questionable and unreliable. Systems used to build trust require a repetitive process that affects the communication system's performance. To differentiate between malicious and trusted messages, a vehicle in VANET has a trust system that provides a vehicle with rewards or sanctions. The study proposes using an Optimized Link State Routing (OLSR) protocol. However, OLSR suffers from security challenges, such as the need for multi-point relays and a repetitive process of executing security mechanisms on each node individually. Blockchain solves the two issues by providing a secure technology that motivates vehicles to collaborate, avoiding the repetitive detection process. Malicious messages pose a critical threat as the message contains important information about the vehicles, such as when to slow down, take turns, or the road to use. The probability of malicious messages being transmitted is high, with the impact being catastrophic.

The authors [12] conduct a literature review on cyber threats faced by CAVs. CAVs have features such as using different technologies, communication between vehicles and infrastructure, and sharing data such as their position, movement, and speed. Attacks on CAVs include jamming GPS and attacking sensors such as those found in the engine control system, infrared, and LiDAR. Some attacks target the electric control modules of the car to rewrite the firmware, changing the functionality of various systems in the vehicle. CAVs also have actuators that control brakes, throttle, and steering. An attack on any device can be catastrophic, as the attack controls the brakes, steering, engine, and all sensors, controlling the vehicle to his wishes. The risk is extreme, with the impact being catastrophic.

The study [13] discusses cybersecurity challenges in the railway sector. Due to increased passenger traffic, railway systems have witnessed the integration of Information technology, IoT, and operational technology to control and manage railway signaling systems, control centers, and trains themselves. Such levels of interconnected systems pose a considerable risk to people and a nation's economy. Also, technological advances have led to more sophisticated attacks on the railway system. The study proposes both proactive and reactive measures, such as security policies, risk management, technical solutions, and consequence management to combat the ever-increasing threat to railway systems. The risk posed by cyber-attacks on railway systems is extreme, with catastrophic results in case of cyber breach.

The authors [14] propose a deep reinforcement learning system to detect impersonation attacks on device-to-device communications. ITS is device-to-device communication as the vehicles act as nodes, interacting with other nodes to form a communication network that shares information between the nodes. One of the disadvantages of such networks is their decentralized nature, which differs from the centralized systems that are robust and secure. Physical layer security overcomes wireless network vulnerabilities by authenticating the users. However, the channels used in the networks are dynamic, and an attacker can easily penetrate the network and pretend to be an authentic user. The authors suggest reinforcement learning, where each user acquires optimal solutions without awareness of the system or network they are using. The risk associated with impersonation attacks is high as the attacker is disguised and thus can do anything, including deleting security messages, misdirecting traffic, leading to congestion on roads or accidents. The probability of occurrence is high, with the results being catastrophic.

Received: August 05, 2025

The study [15] discusses ITS models and security challenges. The ITS architecture consists of a roadway and a traffic management system, with traffic operations personnel managing the systems. The roadway system includes surveillance, equipment coordination, traffic information dissemination, and variable speed limit adjustments. The study explains the implementation of ITS in a smart city project in Wolfsburg, Germany, where Wi-Fi and LoRaWAN are used for interconnectivity, and IDS is used to protect the system from DoS attacks and monitor suspicious devices. All traffic generated by vehicles and other IoT devices is monitored and analyzed at the radio and network levels to identify anomalies. The cyber-attack risk in the smart city and ITS in the city is low, as security measures are in place. The probability of cyber-attack occurring is medium since zero days still exist, and attackers continue to invent novel methods to attack systems. However, the impact is low, as the ITS system has anomaly detection systems that prevent catastrophic events.

The authors [16] delve into cybersecurity's role in approving safety standards in railways. Often, cybersecurity is not an essential component of railway operations, with safety and efficiency being the two most important aspects. The outcome of such thinking is cybersecurity flaws in the railway systems, as the security teams have a culture of rigid approval processes that cannot work in the world of frequent security updates and patches required in the system. Besides, the railway system has physical and cybersecurity threats aiming to disrupt its operations. The authors show the safety approvals, such as the CENELEC standard (based on the European Committee for Electrotechnical Standardization), required to protect railway systems from cyber-attacks. The probability of railway systems having security flaws is high, with the risk of an attack being high. However, the risks may not be catastrophic as some security vulnerabilities may not affect core

The study [17] discusses data poisoning attacks (DPA) on intelligent transport systems which attack training data. Today's transport systems rely on intelligence from trained systems using data. However, cyber attackers can inject malicious data during training, leading to inaccurate results. If the data is used in real-time decision-making, it can lead to adverse effects such as (vehicle) queue estimations at intersections, leading to delays and improper signal timing. Malicious data can also mislead vehicles to choose congested paths, causing more congestion. The risk posed by DPA is critical due to the actors involved and their motives. Some of the attackers are APTs sponsored by foreign governments to instill fear; others sabotage infrastructure or cause economic and social instability, while for some, attacks on ITS are to steal sensitive data. The probability of the risk occurring is high, and the impact can be catastrophic in case of infrastructure and economic sabotage.

The study [18] discusses smart cities and their security challenges. Transport interconnectivity is one of the main aspects of smart cities, besides healthcare, utilities, and the environment. One of the features of smart cities is the use of actuators that adjust or control physical things such as heating elements, filters, valves, and switches. The actuators have replaced sensors that measure things. Actuators can be compromised, leading to physical damage to the system they control. Besides, the entire industrial control system and infrastructure network can face a cyber-attack that leads to DoS shutting down services such as train ticket systems, payment systems, or computer systems managing city buses. Such attacks disrupt transportation, with the operator’s losing revenue in the process. The risks involved range from extreme to medium. In case of an attack on actuators that control critical systems such as traffic systems, the impact is extreme as it can lead to accidents and loss of life. For DoS, the risk is medium as the effects are financial. The probability of cyber-attacks on transport infrastructure, specifically DoS and actuator attacks, is high.

The research [19] delves into the challenges of introducing networks and interconnection in railway systems. Legacy railway systems operated in an air-gapped environment, with the devices being electro-mechanic. However, newer systems use commercial-off-the-shelf devices to build the network interconnecting trains and operational systems. The security consequence of such systems is the increased attack surface of the rail network and reducing the knowledge required to break into the rail networked system. The railway network provides a large attack surface, implying a vast area for lateral movement for the attackers. The risk posed by the cybersecurity threats is high, as attackers gain entry to the systems and conduct any malicious activity they desire. The probability of occurrence is high. The authors propose using encryption in communication and security standards and frameworks to protect railway systems. Cyber range, where a virtual representation of the entire infrastructure system is simulated, can help security personnel analyze different security challenges and scenarios and proactively develop solutions.

The research [20] is based on experiments on applying KNN and SVM in detecting impersonation attacks in VANETs. Impersonation attacks are common in vehicular networks as VANETs cannot identify the authenticity and source of messages transmitted, leaving vehicles vulnerable to receiving messages from attackers and thus causing untold havoc. The research notes that IDS is the best technology for detecting malicious messages and vehicles in the network. Machine learning can improve the detection capability of IDS, with KNN having a 98% accuracy while SVM shows 93% accuracy in detecting attacks. The models can be incorporated into the IDS. The risk of impersonation attacks is extreme as the message receiver can receive the wrong information and take the wrong action, leading to accidents or traffic disruptions.

The research [21] explores the use of AODV to detect black hole attacks in VANET. VANET network controls traffic jams and road security and allows communication between vehicles and between vehicles and infrastructure. Vehicles are nodes in a VANET network. However, any node can function as a router for other nodes. The issue arises when a malicious node injects spoofed routing tables in the network, which are transmitted to other nodes and affect the entire network. The solution to the problem involves modifying the AODV routing protocol by improving the route request

(RREQ) and route reply (RREP) packets. The modified version also incorporates cryptography for encrypting and decrypting communication to identify authentic nodes. The risk posed by black holes is extreme, as malicious nodes can inject routing tables, leading to unimaginable problems, such as traffic jams, accidents, and shutting down communication. The probability of occurrence is high as any vehicle or electronic device acting as the vehicle can act as a node and thus router.

The article [22] discusses the cybersecurity infrastructure of the railway system. The most important systems are the Interlocking system and automatic train supervision system. The Interlocking system tracks moving parts and ensures multiple trains do not use the same track simultaneously. On the other hand, the automatic train supervision system makes all decisions regarding routing and train traffic. In modern railway infrastructure, such systems are interconnected, with some parts being hosted in the cloud, making them vulnerable to cyber-attacks. Railways are critical infrastructure and, thus, an ideal target for APTs and cyber attackers interested in causing havoc. The risk posed by cyber breaches of railway systems is critical, as the outcome is catastrophic, to say the least. Any cyber-attack either leads to delays, disruption of traffic, or accidents that lead to loss of human life. Since thousands use railways to millions of people daily, the result is catastrophic. The authors suggest incorporating international standards such as CENELEC as security guidance for rail applications.

The research [23] builds a system that detects malicious RSUs and tampered messages from Intelligent Vehicles. The rise of the Internet of Vehicles has improved road safety and traffic flow. However, intelligent vehicles are prone to cyber-attacks as the network requires low latency but has no security mechanism to determine the integrity of the messages sent or received. A compromised RSU can tamper with data sent or received by an intelligent vehicle, giving the vehicle the wrong information, which can be catastrophic as the messages contain basic safety and emergency information. Types of attacks include DoS, Sybil attack, jamming, eavesdropping, wormholes, and Man-in-the-Middle. The research proposes a special authentication method using a probabilistic model to identify malicious RSUs with 99% detection accuracy. The probability of a cyber-attack on RSUs is high, with the impact being catastrophic.

The research [24] discusses federated learning systems in connected and automated vehicles (CAV). Interconnection of vehicles raises new security threats due to the nature of the interconnections. First, there is high-node mobility due to the fast-moving vehicles, leading to a rapidly changing routing topology. Such features are different from the traditional mobile and fixed networks. Vehicles and infrastructure communications rely on Basic Safety Messages (BSMs), which have no personally identifiable information to maintain the sender's anonymity. However, the same security features protecting the vehicle sending messages become a vulnerability. A corrupted device can communicate with other vehicles, leading to false and malicious BSM exchanges between the corrupted device and trusted senders or receivers in the network. Federated learning is not secure as model poisoning happens due to the corrupted device, leading to wrong training in the chief node and, thus, wrong analysis. The risk posed by corrupted devices and the use of federated learning is extreme, as incorrect information, training, and insight affect traffic and congestion. The probability of occurrence is high since most networks used in vehicle communication have no methods of authenticating the vehicles and, thus, nodes.

The authors [25] discuss the architecture, cyber-attacks, and defense strategies used in ITS. The most notable cyber-attacks on ITS include sniffing attacks, where the attacker intercepts data in transit and later uses it for further attacks. A man-in-the-middle attack happens when the attacker scans the network and intercepts the data before it reaches the receiver. The attacker modifies the data or ensures it never reaches the intended recipient. Spoofing attacks happen in wireless communication in the case of V2V and V2I, with the attacker disguising themselves as a trusted and known data source. Malware can also be injected into the network, while state actors can carry out advanced persistent threats or targeted attacks. The authors propose using IDS, incorporating security at the electronics control unit (ECU), encrypting data and secure generation of the secret keys. Privacy-preserving computing protects data obtained from the vehicles and all other devices in the ITS network. The risk posed by the cyber-attacks is extreme, as the spoofed or sniffed data can be used to damage or misconfigure the ITS system, leading to loss of lives or traffic disruptions.

The authors [26] examine the security vulnerabilities of autonomous vehicles (AV). Due to the use of wireless networks to interconnect vehicles, AVs suffer from remote hacking where malicious actors use the wireless network to gain access to the vehicle communication and conduct other malicious activities, such as controlling the vehicle to cause accidents or harm the passengers. The sensors in the AV, such as the cameras or vehicle radar, can also be manipulated. In some cases, attackers are interested in the information from the vehicles and thus access the vehicle communication systems to steal the data. Solutions offered include applying ML in threat detection systems, using advanced encryption methods, developing secure software and hardware, and continuously monitoring the entire AV network system. The risk posed by remote hacking and sensor manipulation is extreme as the impact of the cyber breach is catastrophic, with a high probability of occurrence.

The research [27] examines data falsification in ITS systems. A cooperative ITS (cITS) includes vehicles, RSUs, and backend systems. cITS has the same task as IoT in that all devices work cooperatively to achieve a shared task. Vehicles in the cITS share information with each other, and this makes them vulnerable as a compromised vehicle shares false information with other vehicles and the RSUs in the same network. The wrong information leads vehicles to react to false events or change their security settings, enabling the attacker to penetrate the network further. The research proposes using IDS and Misbehavior Detection Systems (MDS) as security solutions. The research suggests using Artificial Neural

Networks (ANN), SVN, and Logistic Regression for misbehavior detection, with the three algorithms showing high accuracy in detecting anomalies. The risk posed by false information is critical as there is a high probability of the attack occurring, with the impact being catastrophic.

6. Proposed Work

The main problem between ITS and CAVs is their interconnectivity. The systems are electro-mechanical, with sensors and actuators connected to a wireless network that transmits the information to an outside infrastructure. The solution to cyber-attacks targeting transport infrastructure involves encrypting data before transmitting it, authenticating RSUs, and having an outside source for information instead of vehicles being the source.

4.1. Encrypting Communication

Communication between vehicles V2V and V2I is insecure as there are no means to authenticate the source of the message to protect users and their vehicles. The lack of vehicle authentication raises integrity questions about the message received and its source. One solution is to encrypt all messages transmitted to and from cars to eliminate snooping and man-in-the-middle attacks. Encrypting the message does not eliminate cyber-attacks; it reduces attackers trying to infiltrate the message between the vehicle and infrastructure.

4.2. Centralized Data Point and Data Analysis

Having an outside source of information is the best plan to solve the issue of impersonation attacks, the most prevalent form of attack and the most lethal as the impersonator transmits wrong information or takes control of vehicles or operations infrastructure, giving it personal commands. Road transport infrastructure can have a central operations center which relays information to all RSUs in a given area about traffic and related matters, and in turn the RSUs transmit the same information to all vehicles within its vicinity. Such a message can be classified differently from other vehicles (V2V), giving it more trust than the V2V information.

RSUs can analyze data collected from vehicles (V2I) to determine the correct information and anomalies. When analyzing data, the RSU can determine the source of information and the lifetime of the device transmitting the information. In most cases, vehicles transmitting information have spent considerable time on the road. On the other hand, most malicious sources tend to be new, and thus, it is easy to categorize them as an anomaly. Also, besides categorizing the source of information (vehicles), data analysis can collect the data from many vehicles transmitting information to the RSU and merge them to check for similarities and anomalies. Most vehicles passing a given area have the same data; thus, similar information has some legitimacy, while those that differ can be treated as anomalies. Machine Learning (ML) algorithms can train a system in the RSU to enable it to categorize data and differentiate trustworthy data and anomalies. The ML system can also be trained on the type of data to expect from vehicles (nodes) and the type to treat as malicious from the start. For instance, directing all vehicles to perform some security function can be treated as malicious if no security warning had been given prior to the message. Also, controlling sensors and actuators in a car can be treated as malicious, and thus such information should not pass through the RSU. An ML system can be trained to detect malicious communication from the start and use previous information communicated from the vehicles to determine the trustworthiness of the message received from any vehicle in a locality.

Analyzed data from each RSU can be transmitted to a central command in the locality where data from all RSUs in the area are merged and analyzed further to provide more insight, with the analyzed data being sent back to the RSUs to be transmitted to the vehicles. The intent of analyzing data from a central point is data integrity, with all RSUs trusting the source of the data. Vehicles receiving the data can be assured of the integrity of the data, and since it is encrypted, there is no man-in-the-middle to tamper with the data. An attacker can only read the data by having an endpoint device that receives the data. However, at this point, the attacker cannot use the data to attack the vehicles or RSUs.

7. Discussion

ML systems are the best defense against cyber-attack on transport infrastructure. Most cyber-attacks in the transport sector exploit known vulnerabilities, such as a lack of message encryption, authentication of messages, and lack of trust in the source of information. Even with such weaknesses, ML systems can learn from data from many vehicles passing a given RSU, analyze it and determine trustworthy data. Malicious information from vehicles aims to control vehicles in a manner that raises the alarm to the vehicle, the RSU, and the passengers or vehicle owner. Information aiming to control vehicle actuators is a clear signal of an attack. Data on traffic that shows different information from that of other vehicles is an anomaly and should be treated as such, with the ML system ignoring such data. An ML system can benefit from encryption, where all messages from the RSU to the central command and from the central command to the RSU and the vehicles are encrypted to ensure their integrity. Since RSUs have no personal information, they can have some form of authentication mechanism for vehicles to know the source of the data, as attackers can also send such data.

Received: August 05, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

8. Real-Life Use Case

CAVs have no way to authenticate the message and its source, making it easy for attackers to send malicious messages to the vehicles. A viable solution is to analyze all data transmitted from vehicles and RSUs to enable vehicles to filter out anomalies in the data. ML systems are the best method to analyze data from vehicles as the systems can learn from massive data sets and provide insight that the vehicles can use when driving. Siemens' solution of an intelligent railway system has some of the features discussed above, such as the use of big data, centralized control for analyzing information and transmitting it to local nodes, and connectivity [28]. Data analysis, centralization of data, and intelligent traffic management will be at the core of every transport system interconnected using modern (wireless) networks.

9. Future Work

The main reason for the lack of vehicle authentication is to protect the vehicle and its owner from cyber attackers who may intend to use ITS to steal personally indefinable information from the vehicle. The system protects the vehicle's owner at the cost of security of the entire transport system. There is a need for more research on how to authenticate the vehicles without revealing their true identity, which can help authenticate all vehicles and, thus, sources of the information transmitted to the RSUs. Also, further research is required on how to protect sensors and actuators from remote control from unauthorized people. Such systems are critical to a vehicle, and remote control can lead to catastrophic consequences as the attacker can cause an accident or even lead to loss of lives for all onboard the vehicle.

10. Conclusion

Cyber security for CAVs and ITS is critical to smart cities. Transport is one of the most crucial aspects of the touted smart city design, with most industrialized nations taking the lead in interconnecting their transport system to their mobile network. However, such interconnectivity has come at a cost, as most rail transport connected to the network has been hacked or exposed to cyber-criminal acts. Security of intelligent transport infrastructure is a necessity for the millions of people who use such infrastructure in each country worldwide. Cyber-attacks common to transport infrastructure include DDoS, phishing, eavesdropping, jamming, and man-in-the-middle, with consequences ranging from moderate to catastrophic. Encrypting data and using ML algorithms to analyze data is necessary for a secure transport system.

References

References must be numbered in order of appearance in the text (including citations in tables and legends) and listed individually at the end of the manuscript. We recommend preparing the references with a bibliography software package, such as EndNote, ReferenceManager or Zotero to avoid typing mistakes and duplicated references. Include the digital object identifier (DOI) for all references where available.
Citations and references in the Supplementary Materials are permitted provided that they also appear in the reference list here.
In the text, reference numbers should be placed in square brackets [ ] and placed before the punctuation; for example [1], [1–3] or [1,3]. For embedded citations in the text with pagination, use both parentheses and brackets to indicate the reference number and page numbers; for example [5] (p. 10), or [6] (pp. 101–105).

[1] Avci and M. Koca, “Intelligent transport system technologies, challenges and security,” Applied Sciences, vol. 14, no. 11, 2024.

[2] Y. Qin et al. “Research on active safety methodologies for intelligent railway systems,” Engineering, vol. 27, pp. 266-279.

[3] James. (2024, Sep. 29). 14 recent cyber attacks on the transport & logistics sector [Online]. Available: https://wisdiam.com/publications/recent-cyber-attacks-transport-logistics-sector/

[4] T. Islam, A. Sheakh, A. N. Jui, O. Sharif, and Z. Hassan, “A review of cyber attacks on sensors and perception systems in autonomous vehicle,” Journal of Economic and Technology, vol. 1, pp. 242-258, 2023.

[5] K. Christian, Keys to running a successful research Projects: All the things they never teach you. London Wall, London, UK: Academic Press, 2018.

[6] A. Gerunov, Risk analysis for the digital age. Cham, Switzerland: Springer, 2023.

[7] I. Tarandach and M. J. Coles, Threat modeling: A practical guide for development teams. Sebastopol. California, US: O'Reilly, 2021.

[8] B. Zeddini, M. Maachaoui, and Y. Inedjaren, "Security threats in intelligent transport systems and their risk levels," Risks, vol. 10, no. 5, 2022.

[9] Z. Wang and X. Liu, "cyber security of railway cyber-physical system (CPS) – A risk Management methodology," Communications in Transport Research, vol. 2, 2022.

[10] H. Nguyen-Minh, T. T. Hoang, and G. P. Thanh, "Machine learning-based jamming detection for safety applications in vehicular networks: Individual detection?" Hidawi: Security and Communication Networks, vol. 2023, 2023.

[11] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J. P. Barbot, "Blockchain-based distributed management system for trust in VANET," Vehicular Communications, vol. 30, 2021.

[12] N. G. Cholli and N. M. Nayak, "Cybersecurity challenges and risks in connected autonomous vehicles: A literature review," SSRN, 2024.

[13] S. G. Predescu, D. Savu, and V. E. Badea, "Cybersecurity in the railway sector," Romanian Cybersecurity Journal, vol. 4, no. 2, 2022.

[14] S. Tu et al., "Reinforcement learning Assisted impersonation attack detection in device-to-device communications," IEEE Transactions on Vehicular Technology, vol. 70, no. 2, 2021.

[15] J. Kolodziej, C. Hopmann, G. Coppa, D. Grzonka, and A. Widlak, "Intelligent transport systems – Models, challenges, security aspects," In Cybersecurity of Digital Service Chains: Lecture Notes in Computer Science, vol. 13300, pp. 56-82, 2022.

[16] E. H. Okstad, R. Bains, T. Myklebust, and M. G. Jaatun, "Implications of cyber security to safety approval in railway," in Proceedings of the 31st European Safety and Reliability Conference, 2021.

[17] F. Wang, X. Wang, and X. Ban, "Data poisoning attacks in intelligent transport systems: A survey," Transport Research Part C: Emerging Technologies, vol. 165, 2024.

[18] H. Habibzadeha, B. H. Nussbaumb, F. Anjomshoac, B. Kantarcid, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," Sustainable Cities and Society, vol. 50, 2019.

[19] S. Soderi, D. Masti, and Y. Z. Lun, "Railway cyber-security in the era of interconnected systems: A survey," Journal of Latex Class Files, vol. 18, no. 9, 2020.

[20] M. S.Savekar and S. A. Thorat, "Identifying impersonation attack in VANET using KNN and SVM approach," International Journal of Future Generation Communication and Networking, vol. 13, no. 3, pp. 1266-1274, 2020.

[21] A. Kumar et al., "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," Microprocessors and Microsystems, 2020.

[22] J. Nunes, T. Cruz, and Paulo Simoes, "Railway infrastructure cybersecurity: An overview," in Proceedings of the 23rd European Conference on Cyber Warfare and Security, vol. 23, no. 1, 2024.

[23] N. V. Abhishek, M. N. Aman, T. J. Lim, and B. Sikdar, "DRiVe: Detecting malicious roadside units in the internet of vehicles with low latency data integrity," IEEE Internet of Things, 2021.

[24] R. Al Mallah, G. Badu-Marfo, and B. Farooq, "Cybersecurity threats in connected and automated vehicles based federated learning systems," in 2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops), 2021.

[25] S. E. Aluko, "Cybersecurity and defense in intelligent transportation systems," World Journal of Advanced Engineering Technology and Sciences, vol. 13, no. 1, pp. 871-879, 2024.

[26] I. Durlik, T. Miller, E. Kostecka, Z. Zwierzewicz, and A. Łobodzinska, "Cybersecurity in autonomous vehicles – Are we ready for the challenge?" Electronics, vol. 13, 2024.

[27] S. A. Almalki and J. Song, "A review on data falsification-based attacks in cooperative intelligent transport systems," International Journal of Computer Science and Security (IJCSS), vol. 14, no. 2, 2020.

[28] Siemens. How digitization is evolving intelligent rail infrastructure [Online]. Available: https://www.mobility.siemens.com/global/en/company/stories/how-digitalization-is-revolutionizing-rail-traffic.html.

Received: August 05, 2025