Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges

Dalton A. Hahn, Arslan Munir, *Senior Member, IEEE,* and Vahid Behzadan

Abstract—Intelligent Transportation Systems (ITS) aim at integrating sensing, control, analysis, and communication technologies into travel infrastructure and transportation to improve mobility, comfort, safety, and efficiency. Car manufacturers are continuously creating *smarter* vehicles, and advancements in roadways and infrastructure are changing the feel of travel. Traveling is becoming more efficient and reliable with a range of novel technologies, and research and development in ITS. Safer vehicles are introduced every year with greater considerations for passenger and pedestrian safety, nevertheless, the new technology and increasing connectivity in ITS present unique attack vectors for malicious actors. Smart cities with connected public transportation systems introduce new privacy concerns with the data collected about passengers and their travel habits. In this paper, we provide a comprehensive classification of security and privacy vulnerabilities in ITS. Furthermore, we discuss challenges in addressing security and privacy issues in ITS and contemplate potential mitigation techniques. Finally, we highlight future research directions to make ITS more safe, secure, and privacy-preserving.

Index Terms—Intelligent Transportation Systems, Security, Privacy

1 Introduction and Motivation

Intelligent Transportation Systems (ITS) are changing the way our roadways and cities look and function. The ITS has the potential to create a more efficient, safer, and enjoyable experience for travelers all over the world. Numerous companies and cities have started initiatives to support and foster development of ITS technologies (e.g., IBM's Smarter City initiative [1] and British Telecom's CityVerve project [2]). With innovations in traffic prediction algorithms [3][4] as well as autonomous or semi-autonomous vehicles to enhance the safety and efficiency of road travel, the future of transportation will look vastly different than it does today. Furthermore, advancements in *infotainment* systems, such as navigation systems, Bluetooth connectivity, hands-free text messaging and phone calls, etc., continue to integrate modern comforts into the vehicles. This technology integration in transportation systems provides new opportunities to perform work in a mobile environment as well as enhances the ability to travel more comfortably and for longer distances [5]. However, advancements made in ITS and the new technologies being introduced to roadways and infrastructure also bring additional challenges [6].

Increasing integration of loosely secured devices and applications with the transportation systems present opportunities for attackers to exploit these systems. Attacks on ITS have implications within the physical world and can result in damage to infrastructure, delay of emergency response, fatalities, and even threats to national security. Due to the possibility of extensive physical and personal damage, risk assessments for ITS have been carried out and risk models have been created but many of these models still contain unanswered questions and thus require further research [7]. With such risks, development of a secure and privacy-conscious framework for ITS is necessary to ensure the safety and privacy of travelers worldwide.

Figueiredo et al. [8] discuss the conception and developments in ITS through the late 1990's. Due to the relative youth of research in ITS, there are many issues and concerns yet to be addressed. Particularly within the spheres of security and privacy, there are a range of problems that will be necessary to investigate before ITS can have its full impact. Governmental efforts and investments have also been made in regards to ITS, with research programs and funds proposed for projects aiming to enhance the viability and practicality of such technologies. Efforts for standardization have been made with the introduction of the IEEE 1609.X family of standards [9]. These standards relate directly to the communication capabilities between vehicles in ITS. The standards presented by the IEEE are further enhanced by the addition of SAE J2735 Directed Short Range Communications (DSRC) message set dictionary [10], which outlines a framework for message types and their structure for use over the IEEE 1609.X communication standards. In the past, projects such as EVITA [11] and OVERSEE[12] worked to expand on the security and privacy of ITS, but these projects have lost pace with advancements in technology.

This paper presents the current state of research in ITS and highlights security and privacy issues in current deployments. We examine ITS from a system-wide perspective and discuss long-term security and privacy issues that may arise as the field of ITS continues to grow. This study aims to provide a comprehensive analysis on current ITS trends within security and privacy as well as future research directions within the field. The main contributions of our paper are as follows:

- We analyze the current state-of-art in ITS research,

with a focus primarily on security and privacy of ITS.
- We provide a comprehensive classification for security and privacy issues in ITS.
- We discuss challenges in addressing security and privacy issues in ITS and contemplate potential mitigation techniques to alleviate shortcomings and vulnerabilities.
- We have identified numerous future work directions to help engineers and researchers in ITS to explore and tackle the pressing challenges for making ITS more safe, secure, and privacy-preserving.

The remainder of this paper is organized as follows. Section 2 presents an overview of ITS and discusses the main elements and technologies present in ITS. Section 3 reviews the related work in ITS. Section 4 provides a classification of security and privacy issues in ITS. Challenges in addressing security and privacy issues in ITS are discussed in Section 5. Section 6 proposes potential mitigation techniques to alleviate security and privacy issues in ITS. Section 7 identifies future research work directions related to security and privacy in ITS. Finally, Section 8 concludes this work.

2 ITS Overview

ITS, while relatively young as a field of research, has been transforming with new ideas and innovations at a rapid pace. Smart vehicles, while an incredibly important component of ITS, are not the sole constituent of these systems and there are other components of ITS that have received relatively lesser attention. This section provides an overview of main components as well as fundamental enabling technologies for ITS.

2.1 ITS Components

2.1.1 *Smart Vehicles*

ITS is most often associated with smart vehicles, whether they possess driver-assistance technology, are semi-autonomous, or even fully autonomous. Smart vehicles are a major component of ITS due to the sheer volume of personal vehicles on the roadway. As the transportation industry continues to evolve, smart vehicle developments have the largest impact on the way we travel and the underlying infrastructure of transportation. As shown in Fig. 1, smart vehicles can create "convoys" using Vehicle-to-Vehicle (V2V) communication technology in order to improve travel efficiency. This communication and clustering of vehicles has been made possible due to research in vehicular ad-hoc networks (VANETs) [13]. A VANET is a communication network organized by vehicles through wireless communication devices that enables vehicles to exchange data, such as emergency situations, distance between vehicles, etc., [14] to enhance safety and efficiency of transportation systems.

Besides smart vehicles communicating with one another, the components within vehicle, such as electronic control units (ECUs), need to communicate

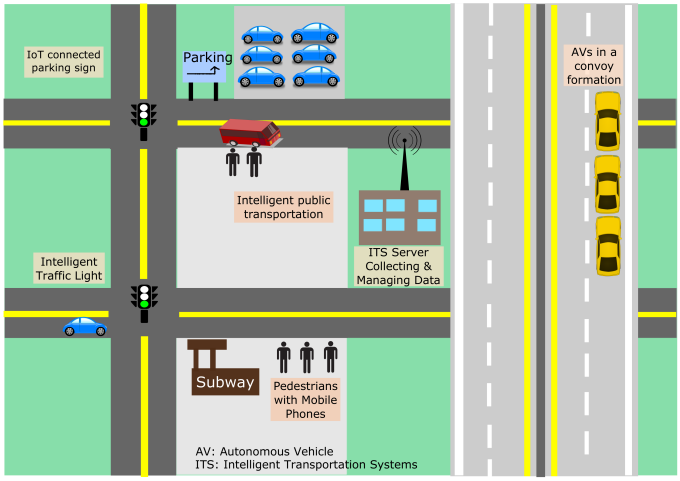


Fig. 1: Intelligent transportation systems.

with each other to implement various distributed control functions. This in-vehicle communication is accomplished through in-vehicle networks, such as Controller Area Network (CAN), CAN with Flexible Data-Rate (CAN FD), and FlexRay [15]. Previous research has shown that in-vehicle networks are susceptible to security attacks where an adversary can remotely control the vehicle while completely ignoring the driver's input [16].

2.1.2 *Public Transportation*

Currently, public transportation systems in many cities are a major means of navigating metropolitan areas. Rail and bus routes operate nearly around the clock in order to provide efficient and economical travel facility to citizens. ITS has the potential to increase the efficiency and the throughput of public transportation systems. Smart bus stops can provide waiting passengers with information regarding the bus schedule (arrival and departure times) and delays, as depicted in Fig. 1. Optimization of routes that takes into account real-time traffic conditions (e.g., congestion caused by other vehicles and accidents) can enhance the passengers' comfort and decrease the travel time. Furthermore, bus and rail systems can also benefit from interaction with the Internet of Things (IoT) devices in ITS that relay information such as passengers waiting at a stop or destination point.

2.1.3 *Internet of Things (IoT) Devices*

According to a report published by Pew Research group [17], over 77% of Americans now own a smartphone. Smartphones, an instance of IoT devices, are an important component of ITS, which not only enable integration with smart vehicles (e.g., for infotainment) but also allow for connection with another vital part of ITS, that is, pedestrians. Within all major cities, there are pedestrians utilizing the roadways, via crosswalks, bridges, etc. Pedestrians can be a major hazard for vehicles or vice versa and, hence, traffic signals and routing algorithms also need to consider pedestrian traffic. Through mobile devices, smart traffic

controllers can be alerted of pedestrians waiting to cross the street. Similarly, through mobile devices, public transportation systems can be alerted of pedestrians waiting to board a subway or a bus.

Fig. 1 shows the role that mobile phones can play when carried by pedestrians in an example system. As pedestrians wait for and utilize public transportation systems, they have the ability to receive updates about weather, traffic, hazards, emergency events, etc., from the network of sensors and signals dispersed throughout the ITS. Sensor devices and microcontrollers are instances of IoT devices that are being employed more and more in ITS for various sensing and computation tasks. For instance, these IoT devices are being leveraged to collect and process valuable analytics data for use in traffic and routing algorithms in smart traffic controllers. As depicted in Fig. 1, IoT devices are increasingly used in various facets of ITS ranging from the public transportation systems to the parking signs that relay vacancy information to the travelers looking for a place to park. While these IoT devices are simple and serve their intended purpose in a very economical and efficient way, these devices struggle to implement basic security and privacy standards due to resource constraints [18].

2.1.4 *Controllers*

The controllers of ITS are those components that administer, control, or change the dynamics of the transportation system. The controllers within ITS manifest the acknowledgement, response, and/or physical action of the system to the observed data. Examples of controllers include traffic lights, traffic announcement systems, digital road signs, and railroad switches. Controllers make decisions based on the observed data from the sensors in ITS [19]. Controllers within ITS are often extremely simple state machines that implement basic logic such as an if-then-else structure [20]. As studied in [20], some controller devices have innate vulnerabilities that may allow attackers to modify traffic patterns. In Fig. 1, control input of controllers can take many forms such as a bus responding to a pedestrian waiting at the bus stop or signals from the parking spot sensors that enable controllers to change the parking availability sign (e.g., from vacant to full when it senses that the last available parking spot has been occupied by a vehicle).

2.2 Enabling Technologies

2.2.1 *Sensing*

Sensors are distributed throughout the ITS to collect relevant data ranging from the number of vehicles waiting at a specific traffic light to the temperature and precipitation conditions of an area. The sensing capabilities provide an opportunity to ITS to make informed and correct decisions about how to change the system state (dynamics) to improve efficiency and/or safety [21]. Without the distributed network of sensors within ITS, analytics and decision-making would be poorly informed. Although sensing enables awareness, informed decision-making, and apt responses in ITS, sensing is also susceptible to security vulnerabilities as discussed in Section 4.

2.2.2 *Computation*

Computation is a key component of ITS and is used in nearly every element and process within the system. For example, cryptographic computations required for many of the communication protocols within ITS need microcontrollers or on-board computers (a.k.a ECUs in case of smart vehicles) to perform these computations so that messages can be transmitted over the network confidentially. Cloud computing has emerged as a potential solution to the large-scale processing required to handle the large amounts of data being generated by ITS [22][23][24]. Recently, fog computing has surfaced as a new computing paradigm wherein majority of the information is processed near the source at the edge of the network instead of the distant cloud. Edge servers send the information with the global scope to the cloud for archival or global analytics. Munir et al. [25] have proposed an integrated fog, cloud, IoT architecture, and illustrated the potential benefits of fog computing for ITS. The authors have discussed that how fog computing can offer higher availability, reliability, flexibility, and quality of service in ITS as compared to using only cloud computing.

2.2.3 *Analytics*

In ITS, the analytics component is vital to providing the "intelligence" to the system. Using a range of data such as traffic delays, congestion rate, pedestrian traffic, etc., ITS can derive information on the health of the system as a whole, and then make decisions to alleviate congestion and minimize delays [26]. Leveraging the capabilities provided by cloud or fog computing, a hierarchical analytics network can be realized wherein regional traffic decisions can be made by intermediary analytics servers whereas system-wide decisions can still be made by a central traffic authority [25].

2.2.4 *Vehicle-to-Everything (V2X) Technology*

Vehicle-to-Everything (V2X) technology is the approach of leveraging the communication networks of ITS in order to broadcast and relay information, such as safety warnings, weather information, traffic congestion, and routing information from vehicles to various components of ITS and vice versa. V2X comprises of V2V and V2I (Vehicle-to-Infrastructure). In V2V technology, vehicles communicate with each other as in VANETs [13] and share information about speed and position of vehicles as well as road hazards. The V2I communication is wireless and bidirectional exchange of information between vehicles and road infrastructure, such as overhead RFID (Radio-Frequency Identification) readers and cameras, lane markers, traffic lights, street lights, road signs, and parking meters. As smart vehicles travel along roadways, On-Board Units (OBUs) within smart

vehicles communicate with Road-Side Units (RSUs), IoT devices, and other OBUs that are positioned nearby [27]. Using the V2X framework, a range of signals and messages can be broadcast or received in order to make roadways more efficient and safer for all the travelers. However, while V2X promotes connectivity across the system, it also presents another attack surface which can be exploited by malicious actors.

2.2.5 *Communication Networks*

Communication networks form the backbone of ITS as the communication networks not only link individual components of ITS together but also connect application spheres. There are two main types of communication in ITS: V2V and V2I. Communication standards exist for V2V and V2I. The IEEE 1609.X family of standards, based on the IEEE 802.11p (the IEEE standard for wireless access in vehicular environments - *WAVE*), standardize V2V communication within VANETs. However, there are alternative communication network technologies available besides 802.11p. The Long Term Evolution Device-to-Device (LTE D2D) technology has shown promise as an alternative communication standard for providing low latency in V2X communications [28]. V2V communication standards can be used to relay safety information between vehicles, and thus provide smart vehicles insights into traffic status, road conditions, and other hazards. Both V2V and V2I rely on DSRC, which is resistant to interference and harsh weather, to transmit and receive information. Additional communication networks are required to relay the information from RSUs in V2I to the central traffic servers that control routing information and inform traffic control devices of updates to traffic patterns [27]. The traffic information from RSUs travels through the Internet infrastructure to the central traffic authority [4]. We point out that the communication in V2V and V2I as well as from V2I to the central traffic servers is susceptible to security and privacy attacks.

2.2.6 *Smart Traffic Control*

Smart traffic controllers implement decision-making actions generated by the analytical/intelligent components of ITS. Routing algorithms and traffic schemes, which are adapted based on the observations made by smart vehicles, public transportation, and IoT devices, are sent to the smart traffic controllers for implementation [19]. Smart traffic controllers are not only responders to the observed data but are also a part of the data generation process. For instance, modern traffic signals are often equipped with camera sensor systems to detect the presence of vehicles at road intersections. Additionally, variable message signs [29][30] are another form of smart traffic control on highways and interstate systems that are growing in popularity in the United States. These signs can be modified to alert drivers of events, such as inclement weather conditions, accidents, hazards, slow downs, etc.

By connecting multiple smart traffic controllers together over a communication network, the data observed by one controller can be propagated to the rest of the system to further enhance the systems' ability to respond to traffic dynamics including emergency events in an efficient way. For instance, by alerting the remainder of the system of an emergency event, first responders can reach the point of emergency more quickly, thus affording them a greater opportunity to perform the needed actions. At the center of smart traffic control are the traffic management centers that combine and synthesize data from the rest of the system into a useable form that can be utilized by traffic algorithms and artificial intelligence (AI) components of ITS [31].

3 Related Work

Previous work in ITS has centered on specific applications, whether that be in relation to smart vehicle security or VANETs. Our work differs from these past studies in that rather than focusing on one aspect of ITS (smart vehicle elements, communication network elements, or analytics), we broaden the scope to examine the system-wide interactions that these elements have on one another. In this section, we discuss previous works related to security in smart vehicles and VANETs, and also discuss relevant funded projects.

3.1 Smart Vehicle Security

Previous work has examined a range of different applications and features of vehicles ranging from driver-assistance technology to fully autonomous vehicles. Specifically relevant to this work is the research on smart vehicles' security and privacy. In-vehicle security is particularly challenging due to the CAN bus as CAN does not provide built-in security. The messages within the CAN bus are transmitted without encryption and authentication [16]. Other works have studied the vulnerability of ECUs such as those in tire-pressure monitoring systems to eavesdropping and spoofed packets [32]. Physical access to the car also creates vulnerabilities such as those shown in [33]. Checkoway et al. [33] have demonstrated that access to the On-Board Diagnostics (OBD-II) port of a vehicle grants full access to the CAN bus and ECUs of the vehicle. As vehicles are progressing towards greater levels of autonomy, there have been a range of studies that explore various safety and security applications of fully autonomous vehicles. Many of these studies rely heavily on assumptions of correct data transmission and trust among vehicles [34][35][36][37][38]. Progressing research in ITS security and privacy from a system-wide perspective is of paramount significance to ensure that security is maintained not only within one application sphere, but across multiple application spheres.

3.2 Vehicular Ad-Hoc Networks (VANETs)

Current work on VANET security strategies and applications has been surveyed and summarized by de Fuentes et al. [13], and more recently by Engoulou

TABLE 1: **Problems Addressed by Relevant Projects**

Problem Area	Relevant Project
Secure/Reliable Inter-Vehicle Communication	EVITA [11]
Application Isolation	OVERSEE [12][47]
Reduction of Traffic Incidents	TIMELI [48], CVES [49]
User Privacy and Security	CIMEC [50]
Secure V2V and V2I Communication	CCAM [51], SPMD [52]
Accurate/Efficient Traffic Control	MMITSS [52]

et al. [39] and Mejri et al. [40]. Due to the fact that VANETs require wireless network technology to operate, VANETs face many of the same challenges as wireless network systems, and thus attacks such as denial-of-service, Sybil [40], and replay attacks can all be found within VANETs as well [41]. The security issues that are faced by VANETs are also relevant to other components of ITS. The propagation of security vulnerabilities to other parts of the system poses a massive risk to the overall security of ITS, and hence a top-down approach to securing ITS is vital.

The VANETs have also been studied in regards to maintaining privacy among the participants and preventing the exposure of participants' private credentials to malicious parties. Most of the work regarding privacy in VANETs relies upon the idea of using *pseudonyms* (fictitious names) or pseudo IDs, as a way of providing privacy to travelers, while also maintaining strong non-repudiation mechanisms for ITS [42][43][44][45]. Kchaou et al. [46] have investigated clustering mechanisms for VANETs in order to create a distributed trust management scheme. However, despite the recent work in VANET pseudonyms, it appears that there are still areas of privacy preservation in VANETs that need further exploration.

3.3 Relevant Funded Projects

Work in ITS has been flourishing in recent years with opportunities for research funding in ITS security and privacy among other research areas. Table 1 depicts some relevant projects and highlights the problems addressed by these projects.

The National Science Foundation (NSF) has various funded projects related to ITS. One such project, TIMELI, aims to reduce traffic incidents and avoid costly congestion events related to traffic incidents through large-scale data analytics [48]. Another ongoing research project [49] at NSF aims to enhance ITS by developing Cooperative Vehicle Efficiency and Safety (CVES) systems to reduce traffic incidents and improve efficiency within autonomous vehicles and ITS.

Within the European Union, there are currently a range of ongoing projects related to ITS technology and strategies [53]. EVITA [11] and OVERSEE [12] are two such projects that have been completed. Specifically, EVITA aimed to develop secure and reliable communication between vehicles. The OVERSEE project provided an environment for isolation of independent applications ensuring that functionality and safety of the vehicle is protected for any application [47]. Within the European Union, there have been many efforts for developing Cooperative Intelligent Transportation Systems (C-ITS) [54][55]. Projects that fall under this theme, such as CIMEC [50] and CCAM [51], are shown in Table 1. Another European project HIGHTS (high precision positioning for cooperative ITS applications) [53] aims to provide new technologies that can be used for extremely accurate position detection systems in order to insure the safety of pedestrians and other vulnerable road users such as motorcyclists.

The United States Department of Transportation (DOT) is also currently running projects focused on ITS. One such project is the Multi-Modal Intelligent Traffic Safety System (MMITSS) [52], which aims to improve efficiency in traffic signals and collects accurate traffic information for all types of transportation [52]. Additionally, the National Highway Traffic Safety Administration (NHTSA) within the United States conducted the Safety Pilot Model Deployment (SPMD) usdot:mmitss project in 2011 to 2014. The goal of this project was to advance and evaluate V2V and V2I technology for potential use in real-world deployment [52].

4 Classification of Security and Privacy Issues

In this section, we provide a framework for classification of various security and privacy issues that exist currently in ITS, as well as those that may arise during the research and development of new ITS technologies.

4.1 Classification of Security Issues in ITS

A common approach to security classification is to use the CIA (Confidentiality, Integrity, Availability) scheme as performed in previous work [13][39]. Here, we classify common security issues in ITS in the CIA dimension as well as additional dimensions such as authentication, identification, and non-repudiation.

4.1.1 Confidentiality

When dealing with sensitive information in a communication network, confidentiality is clearly one of the necessary security services that require consideration in ITS. Confidentiality enables devices and parties within ITS to communicate with one another in a secure and private way without disclosing information to uninvolved parties [39]. For example, a smart vehicle and a public transportation bus traveling together may relay proximity information to one another in order to keep a safe distance. Confidentiality provides a means for secure communication for these ITS components over an insecure channel to send their data while preventing third parties and potential adversaries from eavesdropping on the exchanged information. In addition to encryption mechanisms for providing confidentiality, recent works in *steganography* and

TABLE 2: **Attack Surface Analysis of ITS** (within the Security Dimension column: C, IN, AV, ID, AU, and NR stand for confidentiality, integrity, availability, identification, authentication, and non-repudiation, respectively)

Functional Surface	Attack Example	Security Dimension	Attack Type
Sensing	Denial-of-Service [13]	AV	Active
	Spoofing [56]	IN, AV, ID, AU	Active
Computation/Processing	Denial-of-Service [13]	AV	Active
	Race Condition/Timing Attacks [40]	IN, AV, AU	Active
Communication Networks	Sybil Attacks [13]	IN, AV, ID	Active
	Jamming/Denial-of-Service [40]	AV	Active
	Man-in-the-Middle [40]	C, IN, AV, ID, AU	Active/Passive
	Eavesdropping [13]	C	Passive
	Loss of Event Data [40]	NR	Passive
AI/Machine Learning	Adversarial Examples [56]	IN, AV	Active
	Policy Manipulation [56]	IN, AV	Active
	Data Poisoning [39]	IN, AV	Active
	Environmental Perturbations [57]	IN, AV	Active
	Model Identification [56]	C	Active/Passive
Analytics	Data Poisoning [39]	IN, AV	Active
	Exploiting Model Constraints [58]	IN, AV	Active
	Loss of Event Data [40]	NR	Passive
Controllers	Denial-of-Service [13]	AV	Active
	Parameter/Dynamic Inference [56]	C	Passive

covert channels have investigated how these alternative methods can be used to conceal information when malicious actors can have access to the communication channel [59][60].

As shown in Table 2, communication networks present an attack surface vulnerable to both passive and active attacks. Specifically, confidentiality is imperative for V2X technology to prevent a variety of passive and active attacks on the sensitive information transmitted in V2X communication. Confidentiality incorporation in ITS is challenging due to a wide variety of devices involved in ITS ranging from sophisticated smart phones and smart vehicles to extremely simple IoT devices with minimal computation capabilities. Maintaining confidential communication across the entire spectrum of ITS devices is a challenging endeavor.

4.1.2 *Integrity*

Maintaining data integrity across messages and computations between vehicles, infrastructure, traffic controllers, etc., is critical for correct functionality of ITS. As shown in Table 2, at every point (functional surfaces) in ITS, integrity has the potential to be compromised. For example, a malicious vehicle in an ITS can execute a man-in-the-middle attack by intercepting safety messages between the two vehicles and altering the content before forwarding the messages on to other vehicles. Consequently, the legitimate vehicles will not have the correct positioning information of other vehicles, which can create catastrophic scenarios as this incorrect information will be used by legitimate vehicles in various calculations and decision-making. However, work in sensor fusion has been shown to offset incorrect information from corrupting computations beyond acceptable bounds [61]. Sensor fusion is already commonly used in many modern automobiles.

Another attack against integrity that has been shown to be successful is Global Positioning System (GPS) spoofing [62]. In GPS spoofing, attackers broadcast false GPS signals in order to cause travelers to change their routes based on the corrupt/malicious data. Sybil attack [40] is another common form of attack in which a malicious actor impersonates as multiple parties within a VANET and injects false broadcast messages into the network. This type of attack has been studied in [39][40][46] but still remains one of the common issues within VANETs and ITS. Recent research by Singh et al. [63] has examined the use of blockchain as a mechanism for performing secure data sharing between parties within ITS, however, the proposed blockchain-based approach requires further research in order to establish its viability in real-time environments. Similarly, integrity attacks on other functional surfaces exist, some of which have been summarized in Table 2.

4.1.3 *Availability*

The availability of devices to operate and communicate with other components of ITS is critical to maintaining the safety of travelers. Denial-of-service attacks [40] are the major attacks on the availability of ITS components and services. Table 2 shows that the denial-of-service attacks are prevalent in most of the attack surfaces present within ITS. Attacks on availability are especially dangerous for ITS due to the real-time operational requirements of many ITS components. Some of the existing solutions against denial-of-service attack include signature-based authentication [14] and proof-of-work [64] as shown in Table 3.

4.1.4 Authentication and Identification

Within ITS, it is extremely necessary to authenticate and identify the parties involved in communication and data transfer. As shown in Table 3, common approaches to solving authentication and identification issues involve using Message Authentication Codes (MACs) [39] or challenge-response protocols. Both of these solutions provide verification of a sender, but both of the approaches also add additional computation overhead to the system which may introduce new challenges. Many of the devices present within modern smart vehicles, as shown in Fig. 2, rely upon authentication and identification in order to function properly. However, as mentioned before, the strain of additional computation overhead due to authentication mechanisms may infringe upon real-time constraints or resource limits of these devices.

In addition to the MACs and challenge-response solutions, much of the research in regards to VANET authentication and identification has moved to the idea of utilizing pseudonyms in place of vehicle identifiers to provide greater privacy [42][43][44][45][65]. However, this shift in using pseudonyms requires additional overhead and computation during the processing of safety messages within ITS because the pseudonym must first be verified by a trusted authority. The attribute-based credentials, as studied in [66][67][68], have been proposed as a substitute to psuedonyms and are as discussed in Section 4.3.1.

4.1.5 Non-Repudiation

Non-repudiation is a key security service in ITS and is a focus especially within the study of VANETs and V2V communication, where non-repudiation prevents the deniability of malicious actions by members of the system. Most of the works on non-repudiation [13][39][40] involve a trusted third party to verify the real-world identity of pseudonyms commonly used in VANETs. These third parties are referred to as *regional trusted authorities* and may take the form of physical infrastructure or groups such as governmental authorities. The tradeoff between non-repudiation and privacy adds additional challenges for incorporating security services in ITS.

4.2 Attack Surface Analysis of ITS

Due to the assortment of various technologies and devices that make up ITS, a range of surfaces are present for malicious actors to target for attacks. Table 2 categorizes a sampling of attacks against each surface for confidentiality, integrity, availability, identification, authentication, and non-repudiation dimensions that the attacks are attempting to disrupt. Further, we describe each of the potential attacks as either active or passive to show the involvement of attackers in performing each type of attack. Attacks such as denial-of-service can occur in many of the technologies or functional surfaces within ITS, while others such as eavesdropping

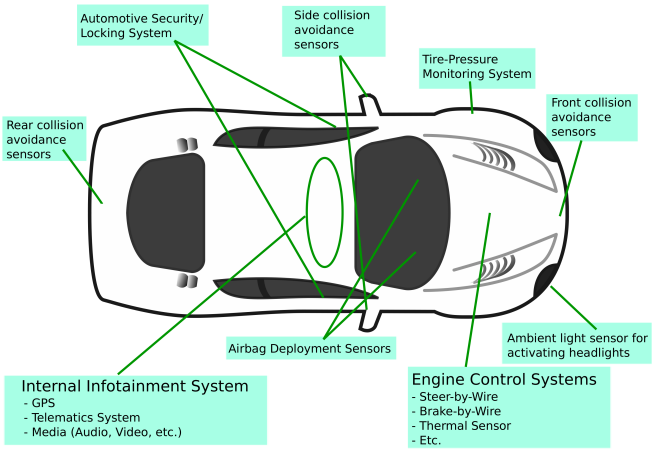


Fig. 2: Attack surface of a smart vehicle.

may only occur in communication networks. As additional technologies and components are added to ITS, it is imperative to consider the additional attack surfaces these new components/technologies present to malicious actors.

A major element in current and future ITS technologies is AI-enabled autonomy. From driver-assistance technologies to city-level analytics and planning, AI and machine learning form a core pillar of ITS. Recent research [69] has shown that all types of machine learning (supervised, unsupervised, reinforcement learning, or hybrid) are vulnerable to various exploitations at any stage of the learning process, namely: training, testing, and deployment. For instance, many of the control applications present within an autonomous vehicle have been trained to detect objects through sensor input, as shown in Fig. 2, such as road signs and interpret them to form intelligent and appropriate responses to keep passengers and pedestrians safe in roadways. However, these AI algorithms are subject to *adversarial examples*, which are carefully modified inputs, also known as perturbations, crafted to manipulate the system into generating a particular output. In the context of classification (a widely used application of AI), adversarial examples are crafted to force a target AI model to cause misclassification in a category different from their legitimate class [57].

Work by Behzadan et al. [70] demonstrates that not only supervised classifiers, but even reinforcement learning techniques are prone to adversarial perturbations. Their work explores the idea of attacking the emerging technique of deep reinforcement learning [71] and training the model to behave in ways dictated by a malicious actor. For example, a reinforcement learning-based autonomous navigation system can be manipulated to halt whenever it observes an exit sign on highways. Furthermore, in analytics components of ITS, adversarial manipulation of observations (e.g., traffic flow) can lead to incorrect modeling of the environment, thus causing catastrophic

failures in management and optimization. The security threats posed by adversarial AI can have catastrophic consequences in ITS.

In addition to AI-enabled autonomy, ITS contains other attack vectors such as tire-pressure monitoring systems as studied by [32] in which in-car wireless sensor networks are compromised. Due to the lack of authentication in the CAN bus, once an attacker has gained access to the network via spoofing the static identifier, other ECUs within the network (e.g., those associated with engine control, airbag control, power steering systems, x-by-wire systems, etc.) can be attacked [32]. Additionally, more complex systems such as infotainment systems with GPS for on-board navigation may be targeted by attackers as shown in [62]. Exfiltration of data from on-board sensors and systems may lead to the exposure of privacy issues as well.

4.3 Classification of Privacy Issues in ITS

Privacy is an extremely necessary consideration for ITS. In this section, we define privacy issues along three overarching categories: identity privacy, behavioral privacy, and location privacy.

4.3.1 *Identity Privacy*

Identity privacy in relation to ITS refers to the privacy of a driver, traveler, passenger, pedestrian, or participant's real-world identity. This can take the form of their first and last name, driver's license number, car registration number, etc. Recent research in VANETs has pushed for the idea of using *pseudonyms*, also known as pseudo IDs, in place of linking real-world identities to vehicles that are a part of VANET systems. Research has shown that pseudonyms have the ability to protect the link between message broadcasts in VANETs that carry safety information, such as vehicle position, and the identity of the sender of these messages [42][43][44][45][65] [68]. However, research has also shown that it is still possible for malicious actors to track specific vehicles when using basic pseudonym implementations [65]. In response to this, pseudonym research in VANETs has advanced to incorporate more interesting approaches as to when and how to change a vehicle's pseudonym.

As an alternative to using psuedonyms for privacy-preserving identification, attribute-based credentials have been proposed. Privacy-enhancing attribute-based credentials allow users to authenticate to verifiers such that users are not linkable between authentication events and only reveal those attributes from their credentials that are relevant to the verifier [72]. However, attributed-based credentials have high resource requirements and also necessitate creation of shared secrets/attributes for all desired services. In short, there exists a tradeoff between preserving privacy of ITS participants and providing security service of non-repudiation, which is needed to correctly identify users of the system in cases of vehicular accidents and/or crimes.

4.3.2 *Behavioral Privacy*

With abundant and detailed information of users in ITS ranging from financial information to location information as well as users' habits within the system, there is a massive opportunity for invasion of individuals' behavioral privacy. Finn et al. [73] have studied classification schemes for various types of privacy. Within the scope of ITS, behavioral privacy refers to the privacy of data that describes various aspects of a group or individuals and their actions within ITS. For a system to maintain behavioral privacy, it must have the ability to anonymize and protect collected user data from exposure as well as to mask common behavioral patterns of users of ITS.

Preserving privacy of actions taken by ITS users is necessary to avert attackers from tracking and drawing inferences on specific individuals within the system. As ITS collects information on travelers' routing patterns to make the routes safer and more efficient, movement patterns of individual travelers are also recorded in the system, the analysis of which can provide inferences about the behaviors of individuals. For example, the origin and destination points of individual travelers can lead to privacy issues as it can enable a malicious actor to infer the residence or workplace of a traveler.

Differential privacy can be used to preserve privacy of ITS users. The goal of differential privacy is to preserve information privacy by furnishing ways to maximize the accuracy of queries from statistical databases while minimizing the probability of identifying its records [74]. However, differential privacy faces challenges when being used across recurrent or time-series data [74]. Furthermore, development of ϵ-differentially databases becomes challenging as $\epsilon \to 0$.

4.3.3 *Location Privacy*

Using Finn et al.'s [73] definition of privacy, location privacy within ITS would be classified as "privacy of location and space", or the right of a user to travel or move about the system without concern of his/her location information being exposed. While precise location information is beneficial for ITS to provide location-aware services, such information can also be used to attack the privacy of individuals. By utilizing this location information, attackers can launch attacks that are focused on an individual. It is extremely challenging for GPS-based navigation systems to provide service while also preserve location privacy of users. Hence, what is crucial is to find a balance between providing beneficial and accurate services to users while also preserving location privacy. Location obfuscation or location cloaking [75] is a technique employed in privacy-preserving location-based services. *Location cloaking* protects a user's location privacy by slightly altering or generalizing the user's location to avoid disclosure of the user's actual position.

TABLE 3: **Comparative Analysis of Contemporary Approaches to Security and Privacy Issues in ITS**

Category	Current Approaches	Advantages	Disadvantages	References
Confidentiality	Symmetric Key Cryptography	Low computation overhead	Key distribution problem	[9][13][14] [39][40][76][77]
	Asymmetric Key Cryptography	Symmetric key distribution	High computation overhead	[9][14][39][40] [66][76][77]
	Steganography	Secure information sharing	High computation overhead	[59][60]
Integrity	Message Authentication Codes	Verification of message contents	Additional computation overhead	[9][14][32][39][40] [41][76][77][78]
Authentication	Challenge-Response Protocols	Verification of sender	Challenge-Response verification time requirement	[39][40][41]
	Message Authentication Codes	Verification of sender	Computation overhead	[9][14][32][39][40] [41][76][77][78]
Non-Repudiation	Digital Signatures	Link message to sender	Difficult in pseudonymous systems	[9][14][39] [40][41][66]
Availability	Signature-based Authentication	Avoids unnecessary signature computations	Requires additional infrastructure and rekeying scheme	[14][40][41][44]
	Proof-of-Work	Prevents false message flooding	Additional computation overhead	[64]
Identity Privacy	Pseudonym	Disguise true identity	Vulnerable to pattern analysis	[13][14][39][41][42] [43][44][45][65]
	Attribute-based Credentials	Restrict access to information based on shared secrets	Require shared secrets for all desired services	[13][42][66][67] [68][79]
Behavioral Privacy	Differential Privacy	Limit privacy exposure	True user-level privacy of single data record still challenging	[74][79]
	Public-Key Cryptography	Integratable with hardware	Computationally intensive	[9][14][39][40] [66][76][77]
Location Privacy	Location Cloaking	Personalized privacy	Requires additional infrastructure	[75][79]
	Homomorphic Encryption	Distributed analysis of data	Computation overhead	[80]

4.4 Analysis of Contemporary Approaches to Security and Privacy Issues

Table 3 displays a sampling of current approaches to various security and privacy issues relevant to ITS. We perform a comparison across different solutions by examining their advantages and disadvantages in ITS implementations. For example, a common solution for incorporating message integrity in ITS is using MACs, which provide verification of message contents, however, MACs require additional computation overhead for the verification process. Each of the discussed approaches provides valuable benefits to ITS, nevertheless, the approaches also introduce additional challenges to the system that must be considered.

5 Challenges

Addressing security and privacy issues in ITS presents numerous challenges for the engineering and development of practical solutions. While many of these challenges overlap with those of the similar paradigms such as IoT and Mobile Ad hoc Networks (MANETs), there are multiple aspects that remain unique to the domain of ITS. This section presents an overview of such challenges from a system design perspective.

5.1 Heterogeneity

ITS comprises of numerous technologies and components with different diverse functionalities and objectives. This inherent heterogeneity exacerbates the task of analyzing and ensuring the secure adoption and integration of such components within ITS. Besides the vulnerabilities that may already exist in each component, the interactions of different components can also give rise to new vulnerabilities and exploitable threats. Moreover, components from different vendors that are designed for the same task may follow different designs and standards, which leads to further complications in comprehensive security analysis and defensive solutions. For instance, different implementations of the same V2X communication protocol may present vulnerabilities that arise from the interaction of communicating devices, which can be exploited to compromise the security of ITS [81].

5.2 Scalability and Extendability

The growing rate of adoption and advancements in ITS technologies presents two fundamental constraints on security solutions. The first is that of scalability: ITS security solutions must provide the means for seamless compatibility with the expanding scales of their deployment. As an example, any key distribution mechanism or intrusion detection system needs to remain feasibly effective in very large ITS deployments. The second constraint is extendability: due to the young age of the ITS field, security solutions must be designed such that the ITS evolution and extension over time do

not come at the expense of major overhauls and changes to the dependent components.

5.3 Distributed Network Architecture

Similar to IoT, ITS is envisioned as a network of heterogeneous sensors, controllers, and computational units whose interactions are not managed through central infrastructure. The high degree of heterogeneity and the distributed nature of ITS escalate the complexity of monitoring and control of such systems. For instance, employing central or system-wide defenses is often not practically feasible. Furthermore, the mobility of most ITS components results in the dominance of wireless communication links, which are inherently insecure and prone to a variety of attacks [82]. Therefore, security solutions for ITS need to account for unreliability of the underlying communications infrastructure as well.

5.4 Complexity

ITS as a whole is comprised of numerous interacting components of heterogeneous types and nonlinear dynamics. Such features form the defining characteristics of Complex Adaptive Systems (CAS) [24]. In CAS, the interdependence and interaction of constituent components generate higher-order behavior and phenomenon that are not present in individual components, but are emergent from the system as a whole. Analysis and control of such higher-order events is often complicated and intractable [83]. Hence, providing guarantees on the reliability and security of such emergent behavior in ITS is also a challenging problem - particularly under adversarial conditions [56]. An instance of such emergent vulnerabilities in ITS is presented in [84], which shows that sequential tampering with traffic flow sensors can result in major traffic jams in urban areas.

5.5 Resource Constraints

Sensors, processors, and devices employed in ITS applications are often required to be inexpensive, low-energy, and small form-factor. Therefore, many ITS devices have limited memory, storage, computing power, and communication range [85]. Such constraints greatly limit the space of feasible security and privacy solutions. Often times, tradeoffs with security must be made because of a device's limited resources. For example, limited computational resources in current in-vehicle ECUs may render the use of cryptographic and authentication schemes infeasible for providing secure CAN communications. Also, resource limitations may give rise to new vulnerabilities, such as increased susceptibility to denial-of-service and man-in-the-middle attacks [86].

5.6 Delay Sensitivity

Many ITS applications require (near) real-time responses to events occurring in the environment [85]. Due to factors such as the high mobility of vehicles and the demand for timely adjustment of large-scale transportation systems, the processing of sensory measurements must be performed in a short amount of time dictated by the time constraints of the application. In such conditions, utilization of limited resources for security and privacy mechanisms may be challenging for many ITS devices. Furthermore, stringent time constraints may require ITS components to rely on incomplete information or suboptimal approximations, which may lead to further vulnerabilities. An instance of such vulnerabilities is presented in [87], where the real-time constraints of sense and avoid mechanisms in autonomous vehicles give rise to myopic avoidance decisions, thus enabling an adversary to manipulate the trajectory of such vehicles by invoking short-term evasion maneuvers.

5.7 Secure Storage and Distribution of Secret Keys

Integration of security primitives, such as confidentiality, integrity, and authentication, in ITS agents relies on secure secret keys [88]. Many of the ITS devices are likely to not have the capability or resources to securely store and manage secret keys generated for secure communication or data transfer with other ITS agents, which puts the security of ITS at risk and makes the privacy of collected traveler data vulnerable. Besides secure storage of secret keys, secure key distribution of secret keys between ITS agents involved in a given application presents another challenge. Resource constraints of many ITS agents makes it difficult to implement complex secret key exchange protocols with large key lengths required to provide adequate security. Considering the resource constraints of ITS agents, new lightweight techniques for secure key exchange are being developed, which present new risks and vulnerabilities for ITS agents.

5.8 Dynamic Security and Privacy Requirements

Components and users of ITS technologies may have different security and privacy preferences, which may change over time. For instance, the security requirements of an urban ITS deployment may vary in case of threats to national security or natural disasters. With respect to privacy, the preferences of users may vary from requiring absolute privacy and minimal information exposure to voluntarily opting-in to new services that require more user information. Managing these dynamic preferences in an efficient and transparent manner is critical to providing adaptive, resilient, and effective ITS solutions.

6 Mitigation of Security and Privacy Vulnerabilities

Embedding security primitives within ITS devices will be necessary for ensuring the success and adoption of ITS. Furthermore, to protect the personal information and data of ITS users, privacy issues need to be considered in the design of ITS. This section outlines a few potential strategies for mitigating security and privacy vulnerabilities in ITS.

6.1 Secure ECU Architecture

Many of the ITS devices and components are resource constrained, which limits the incorporation of stronger security protocols. Works by Poudel et al. [15][77][78] attempts to address this issue by introducing novel ECU architectures for modern automobiles. In these works, Poudel et al. have demonstrated that by assimilating security and dependability at the architecture level, real-time constraints of automotive control functions can be satisfied in an energy efficient manner. Further, as a part of the EVITA project, hardware security modules (HSMs) have been proposed by Wolf et al. [89] as a way of implementing security for ECUs within vehicles. Trusted Platform Modules (TPMs) have also been explored as a potential solution for securing vehicular communications, but they have been shown to lack the cost efficiency and robustness necessary for use within ITS [15].

6.2 Secure Storage and Generation of Secret Keys

The security of crypto systems in ITS relies on secret keys, the leakage of which can compromise the security of the entire system. The secure storage of secret keys presents challenges. To minimize potential exploits, secret keys can be stored in tamper-resistant memories, however, however, a multitude of attack vectors, such as side-channel attacks, reverse engineering, fault injection attacks, microprobing, and software attacks have been devised for appraisal, cloning, and extraction of secret keys stored in nonvolatile memory [15]. Public key cryptography can be used for secure generation of secret keys. To mitigate the risks of secret key storage, hardware-based security techniques such as physically unclonable functions (PUFs) can be used to generate secret keys on-the-fly instead of storing the keys in nonvolatile memory.

6.3 Intrusion Detection Systems

Rule-based and signature-based intrusion detection systems (IDS) have been used extensively in computer and network security. The IDS provide a "first-line of defense" against attacks and malicious actors. The IDS can be employed within ITS to prevent attacks and attempts at compromising the security of ITS and privacy of travelers [90]. By configuring the rules correctly and incorporating fresh signatures, IDS can serve as a valuable defense mechanism in ITS against potential attacks. Furthermore, machine learning-inspired adaptive and evolving IDS that leverage statistical detection of anomalies and attack indicators can further circumvent security and privacy attacks.

6.4 Implementing Security in Resource-Constrained Devices

Implementing security primitives in resource-constrained ITS devices is a challenging issue. Perrig et al. [91] have discussed the implementation of security protocols that balance security with the resource constraints imposed by devices. Furthermore, resource constraints of ITS devices also present device management issues. Sehgal et al. [18] have explored requirements of IP-based network management protocols for use in resource constrained devices. Finally, integration of security primitives in hardware architecture can also help in meeting security requirements of devices with limited resources while adhering to the real-time requirements of ITS agents [15].

6.5 Privacy-Preserving Computing

The traffic optimization and traffic pattern analysis requires that traffic data be collected from thousands or even millions of contributing nodes, the privacy of which needs to be maintained. Privacy-preserving computing has risen as a potential solution to preserve data privacy while performing computations on the massive amounts of data collected in environments such as ITS. Lu et al. [92] presents new solutions to maintaining the privacy of participating parties, which can be applied to preserve the privacy and anonymity of parties involved in data contribution for ITS.

7 Future Research Directions

Previous sections expanded upon the necessity of further research and development in various aspects of security and privacy in ITS. Of the wide range of problems that require further research and development, some are deemed fundamental and vital. This section presents an overview of such areas and promising venues of research.

7.1 Artificial Intelligence

The adoption of AI and machine learning techniques within ITS technologies is growing at a rapidly intensifying rate. While the advantages of utilizing such approaches are greatly publicized, the security implications of their integration with ITS remain largely unstudied. As discussed in Section 4.2, 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. On the other hand, recent research [84][93] proposes that 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 research on such techniques can facilitate more efficient approaches to the design and management of secure ITS technologies.

7.2 Complex Adaptive Systems

Another venue of research is the security aspects of the ITS as a whole within the abstraction of CAS. As discussed in Section 5, the envisioned paradigm of ITS forms a CAS, in which the interactions of

many constituent components create higher-order effects that can be interpreted as emergent phenomena. Understanding such complex dynamics and controlling emergent behaviors of ITS from a security standpoint is of paramount importance, since in such systems, local failures may give rise to cascades of failures, escalating the problem to the entire system [84].

7.3 Vulnerability Assessment

Vulnerability assessment of ITS requires further research, in particular, there is a pressing need for a comprehensive vulnerability assessment framework. While some studies have focused on vulnerability assessment of particular components of ITS (e.g., [84][93]), there is still no standard and comprehensive framework for analysis and quantification of vulnerabilities in the integrated system, particularly from a CAS point of view. Similarly, the bulk of the current literature focuses on implementing security measures post-development, leaving much to be done in establishing guidelines and frameworks for secure design and development. Finally, considering the growing trend towards complementing cloud-based designs with edge architectures [25], a comprehensive study of the security implications resulting from this shift is necessary.

7.4 Privacy by Design

Privacy by design concept [94] emphasizes on the proactive role of data controllers and processors in addressing the privacy aspects of associated systems not only during the full life cycle of each system, but also throughout the design and planning phases. While the paradigm of privacy by design is not new, it has recently gained increasing attention from researchers and the industry due to the adherence of the General Data Protection Regulation (GDPR) to this concept [95]. While some studies (e.g., [96][97][98]) have applied the principles of privacy by design to the ITS domain, there still remains a wide gap between the state of the art and satisfying the privacy requirements of GDPR in ITS technologies [99]. Promising technical venues to explore in this direction include the recently proposed blockchain-based approaches [100] and homomorphic encryption [80], which can potentially provide a distributed mean for sharing and analyzing data while preserving anonymity and privacy.

8 Conclusions

Although burgeoning revolution of Intelligent Transportation Systems (ITS) presents a myriad of benefits, such as increased comfort and safety, increased energy efficiency, reduced pollution, reduced noise, and reduced traffic congestion, it also poses serious security and privacy issues if not accounted for in the design of ITS. It is imperative that security and privacy be considered in the design of individual ITS agents as well as overall ITS in order to maintain a safe and secure ITS. This paper has provided a comprehensive classification of security and privacy vulnerabilities in ITS. Furthermore, we have identified challenges in addressing security and privacy issues in ITS. The mitigation techniques presented in this paper can help in alleviating security and privacy vulnerabilities of ITS. Finally, we have identified future research directions to help researchers and engineers design safer, secure, and privacy-preserving ITS.

Acknowledgments

The authors would like to thank all the reviewers and the editors that have contributed to improving the content of this paper. This work was supported by the National Science Foundation (NSF) (NSF CNS 1743490). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

[1] IBM, "Smarter Cities," 2017. [Online]. Available: https://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/

[2] B. Telecom, "BT CityVerve Portal," 2017. [Online]. Available: https://portal.bt-hypercat.com/

[3] S. de Luca, R. D. Pace, A. D. Febbraro, and N. Sacco, "Transportation Systems With Connected and Non-Connected Vehicles: Optimal Traffic Control," in *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. Naples, Italy: IEEE, June 2017, pp. 13–18.

[4] H. Qin and C. Yu, "A Road Network Connectivity Aware Routing Protocol for Vehicular Ad Hoc Networks," in *2017 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*. Vienna, Austria: IEEE, June 2017, pp. 57–62.

[5] M. Alam, J. Ferreira, and J. Fonseca, "Introduction to Intelligent Transportation Systems," in *Intelligent Transportation Systems*. Springer, 2016, pp. 1–17.

[6] A. Munir, "Safety Assessment and Design of Dependable Cybercars: For today and the future," *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 69–77, April 2017.

[7] K. B. Kelarestaghi, K. Heaslip, and R. Gerdes, "Vehicle Security: Risk Assessment in Transportation," *arXiv preprint arXiv:1804.07381*, 2018.

[8] L. Figueiredo, I. Jesus, J. A. T. Machado, J. R. Ferreira, and J. L. M. de Carvalho, "Towards the development of intelligent transportation systems," in *ITSC 2001 IEEE Intelligent Transportation Systems.*, Aug 2001, pp. 1206–1211.

[9] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, July 2011.

[10] SAE, "Dedicated Short Range Communications (DSRC) Message Set Dictionary," 2016. [Online]. Available: https://www.sae.org/standards/content/j2735_201603/

[11] K. M. Bayarou, "E-Safety Vehicle Intrusion Protected Applications," 2008. [Online]. Available: https://www.evita-project.org/index.html

[12] T. Wollinger, "OVERSEE - Open Vehicular Secure Platform," 2010. [Online]. Available: https://www.oversee-project.com/index.html

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

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

[15] 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.

[16] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*. Berkeley, CA, USA: IEEE, May 2010, pp. 447–462.

[17] Pew Research, "Mobile Fact Sheet," 2018. [Online]. Available: http://www.pewinternet.org/fact-sheet/mobile/

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration Challenges of Intelligent Transportation Systems with Connected Vehicle, Cloud Computing, and Internet of Things Technologies," *IEEE Wireless Communications*, vol. 22, no. 6, pp. 122–128, December 2015.

[23] P. Jaworski, T. Edwards, J. Moore, and K. Burnham, "Cloud Computing Concept for Intelligent Transportation Systems," in *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*. Washington, DC, USA: IEEE, Oct 2011, pp. 391–936.

[24] F. Y. Wang, "Parallel Control and Management for Intelligent Transportation Systems: Concepts, Architectures, and Applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 3, pp. 630–638, Sept 2010.

[25] A. Munir, P. Kansakar, and S. U. Khan, "IFCIoT: Integrated Fog Cloud IoT: A Novel Architectural Paradigm for the Future Internet of Things," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 74–82, July 2017.

[26] J. Zhang, F. Y. Wang, K. Wang, W. H. Lin, X. Xu, and C. Chen, "Data-Driven Intelligent Transportation Systems: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1624–1639, December 2011.

[27] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected Vehicles: Solutions and Challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, Aug 2014.

[28] S. Sun and J. Hu and Y. Peng and X. Pan and L. Zhao and J. Fang, "Support for Vehicle-to-Everything Services Based on LTE," *IEEE Wireless Communications*, vol. 23, no. 3, pp. 4–8, June 2016.

[29] Alena Erke and Fridulv Sagberg and Rolf Hagman, "Effects of Route Guidance Variable Message Signs (VMS) on Driver Behaviour," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 10, no. 6, pp. 447 – 457, 2007.

[30] K. B. Kelarestaghi, K. Heaslip, V. Fessmann, M. Khalilikhah, and A. Fuentes, "Intelligent Transportation System Security: Hacked Message Signs," *SAE Int. J. Transp. Cybersecur. Priv*, 2018.

[31] B. M. Williams and A. Guin, "Traffic Management Center Use of Incident Detection Algorithms: Findings of a Nationwide Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 8, no. 2, pp. 351–358, June 2007.

[32] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in *Proceedings of the 19th USENIX Conference on Security*. Berkeley, CA, USA: USENIX Association, August 2010, pp. 21–21.

[33] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *Proceedings of the 20th USENIX Conference on Security*. Berkeley, CA, USA: USENIX Association, 2011, pp. 6–6.

[34] D. Bevly, X. Cao, M. Gordon, G. Ozbilgin, D. Kari, B. Nelson, J. Woodruff, M. Barth, C. Murray, A. Kurt, K. Redmill, and U. Ozguner, "Lane Change and Merge Maneuvers for Connected and Automated Vehicles: A Survey," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 1, pp. 105–120, March 2016.

[35] T. Kato, C. Guo, K. Kidono, Y. Kojima, and T. Naito, "SpaFIND: An Effective and Low-Cost Feature Descriptor for Pedestrian Protection Systems in Economy Cars," *IEEE Transactions on Intelligent Vehicles*, vol. 2, no. 2, pp. 123–132, June 2017.

[36] A. Kouvelas, J. P. Perrin, S. Fokri, and N. Geroliminis, "Exploring the Impact of Autonomous Vehicles in Urban Networks and Potential New Capabilities for Perimeter Control," in *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. Naples, Italy: IEEE, June 2017, pp. 19–24.

[37] B. Paden, M. p, S. Z. Yong, D. Yershov, and E. Frazzoli, "A Survey of Motion Planning and Control Techniques for Self-Driving Urban Vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 1, pp. 33–55, March 2016.

[38] N. Wang, S. Lv, M. J. Er, and W. H. Chen, "Fast and Accurate Trajectory Tracking Control of an Autonomous Surface Vehicle With Unmodeled Dynamics and Disturbances," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 3, pp. 230–243, September 2016.

[39] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET Security Surveys," *Computer Communications*, vol. 44, pp. 1–13, May 2014.

[40] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, April 2014.

[41] F. Sakiz and S. Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33 – 50, June 2017.

[42] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*. Montreal, Quebec, Canada: ACM, September 2007, pp. 19–28.

[43] H. Lu, J. Li, and M. Guizani, "A Novel ID-Based Authentication Framework with Adaptive Privacy Preservation for VANETs," in *2012 Computing, Communications and Applications Conference*. Hong Kong, China: IEEE, Jan 2012, pp. 345–350.

[44] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, Jan 2012.

[45] Y. Pan and J. Li, "Cooperative Pseudonym Change Scheme Based on the Number of Neighbors in VANETs," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599 – 1609, November 2013.

[46] A. Kchaou, R. Abassi, and S. Guemara, "Toward a Distributed Trust Management Scheme for VANET," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM, 2018, pp. 53:1–53:6.

[47] A. Groll, J. Holle, C. Ruland, M. Wolf, T. Wollinger, and F. Zweers, "Oversee a Secure and Open Communication and Runtime Platform for Innovative Automotive Applications," in *7th Embedded Security in Cars Conf.(ESCAR)*, 2009.

[48] P. Balan, "PFI:BIC- A Smart Service System for Traffic Incident Management Enabled by Large-data Innovations (TIMELI)," 2016. [Online]. Available: https://nsf.gov/awardsearch/showAward?AWD_ID=1632116

[49] R. Wachter, "CAREER: Multi-Resolution Model and Context Aware Information Networking for Cooperative Vehicle Efficiency and Safety Systems," 2016. [Online]. Available: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1664968&HistoricalAwards=false

[50] E. Commission, "Cooperative ITS for Mobility in European Cities (CIMEC)," 2018. [Online]. Available: http://cimec-project.eu/

[51] E. Commission, "Cooperative, Connected and Automated Mobility (CCAM)," 2018. [Online]. Available: https://ec.europa.eu/transport/themes/its/c-its_en

[52] J. S. Debby Bezzina, "Safety Pilot Model Deployment: Test Conductor Team Report," 2015. [Online]. Available: https://www.its.dot.gov/research_archives/dma/bundle/mmitss_plan.htm

[53] E. Commission, "H2020 Transport:Intelligent Transport Systems," 2018. [Online]. Available:

https://ec.europa.eu/inea/en/horizon-2020/h2020-transport/projects-by-field/intelligent-transport-systems

[54] E. Commission, "Innovating for the Transport of the Future," 2018. [Online]. Available: https://ec.europa.eu/transport/themes/its_en

[55] E. T. S. Council, "Briefing: Cooperative Intelligent Transport Systems (C-ITS)," 2017. [Online]. Available: https://etsc.eu/briefing-cooperative-intelligent-transport-systems-c-its/

[56] V. Behzadan and A. Munir, "Models and Framework for Adversarial Attacks on Complex Adaptive Systems," *arXiv preprint arXiv:1709.04137*, September 2017.

[57] P. McDaniel, N. Papernot, and Z. B. Celik, "Machine Learning in Adversarial Settings," *IEEE Security Privacy*, vol. 14, no. 3, pp. 68–72, May 2016.

[58] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," *arXiv preprint arXiv:1412.6572*, 2014.

[59] De Fuentes, José María and Blasco, Jorge and González-Tablas Ferreres, Ana and González-Manzano, Lorena, "Applying Information Hiding in VANETs to Covertly Report Misbehaving Vehicles," *International Journal of Distributed Sensor Networks*, vol. 2014, 02 2014.

[60] Manchanda, Kimi and Singh, Amarpreet, "Covert Communication in VANETS using Internet Protocol Header Bit," *International Journal of Computer Applications*, vol. 123, pp. 10–14, 08 2015.

[61] K. Jo and K. Chu and M. Sunwoo, "Interacting Multiple Model Filter-Based Sensor Fusion of GPS With In-Vehicle Sensors for Real-Time Vehicle Positioning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 329–343, March 2012.

[62] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, "A Practical GPS Location Spoofing Attack in Road Navigation Scenario," in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*. New York, NY, USA: ACM, February 2017, pp. 85–90.

[63] M. Singh and S. Kim, "Crypto trust point (cTp) for secure data sharing among intelligent vehicles," in *2018 International Conference on Electronics, Information, and Communication (ICEIC)*, Jan 2018, pp. 1–4.

[64] Esther Palomar and José M. de Fuentes and Ana I. González-Tablas and Almudena Alcaide, "Hindering False Event Dissemination in VANETs with Proof-of-Work Mechanisms," *Transportation Research Part C: Emerging Technologies*, vol. 23, pp. 85 – 97, 2012.

[65] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough," in *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*. Kranjska Gora, Slovenia: IEEE, February 2010, pp. 176–183.

[66] J. M. de Fuentes, L. González-Manzano, J. Serna-Olvera, and F. Veseli, "Assessment of Attribute-Based Credentials for Privacy-Preserving Road Traffic Services in Smart Cities," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 869–891, Oct 2017.

[67] G. Neven, G. Baldini, J. Camenisch, and R. Neisse, "Privacy-Preserving Attribute-Based Credentials in Cooperative Intelligent Transport Systems," in *2017 IEEE Vehicular Networking Conference (VNC)*. Torino, Italy: IEEE, Nov 2017, pp. 131–138.

[68] L. Nkenyereye, B. A. Tama, Y. Park, and K. H. Rhee, "A Fine-Grained Privacy Preserving Protocol over Attribute Based Access Control for VANETs," *JoWUA*, vol. 6, no. 2, pp. 98–112, 2015.

[69] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman, "SoK: Security and Privacy in Machine Learning," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018.

[70] V. Behzadan and A. Munir, "Vulnerability of Deep Reinforcement Learning to Policy Induction Attacks," in *Proceedings of the International Conference on Machine Learning and Data Mining (MLDM)*, New York, New York, July 2017.

[71] Y. Li, "Deep Reinforcement Learning: An Overview," *arXiv preprint arXiv:1701.07274*, 2017.

[72] J. Camenisch, A. Lehmann, G. Neven, and A. Rial, "Privacy-Preserving Auditing for Attribute-Based Credentials," in *Proc. of European Symposium on Research in Computer Security*, M. Kutyłowski and J. Vaidya, Eds., 2014, pp. 109–127.

[73] R. L. Finn, D. Wright, and M. Friedewald, "Seven Types of Privacy," in *European data protection: coming of age*. Springer, 2013, pp. 3–32.

[74] F. Kargl, A. Friedman, and R. Boreli, "Differential Privacy in Intelligent Transportation Systems," in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*. New York, NY, USA: ACM, April 2013, pp. 107–112.

[75] E. Yigitoglu, M. L. Damiani, O. Abul, and C. Silvestri, "Privacy-Preserving Sharing of Sensitive Semantic Locations under Road-Network Constraints," in *2012 IEEE 13th International Conference on Mobile Data Management*. IEEE, July 2012, pp. 186–195.

[76] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in Internet of Things: A survey," in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*. Marrakech, Morocco: IEEE, May 2017, pp. 1–6.

[77] B. Poudel, N. K. Giri, and A. Munir, "Design and Comparative Evaluation of GPGPU- and FPGA-based MPSoC ECU architectures for Secure, Dependable, and Real-Time Automotive CPS," in *IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*. Seattle, WA, USA: IEEE, July 2017, pp. 29–36.

[78] B. Poudel and A. Munir, "Design and Evaluation of a Novel ECU Architecture for Secure and Dependable Automotive CPS," in *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*. Las Vegas, NV, USA: IEEE, January 2017, pp. 841–847.

[79] D. Christin, "Privacy in Mobile Participatory Sensing: Current Trends and Future Challenges," *Journal of Systems and Software*, vol. 116, pp. 57 – 68, 2016.

[80] Y. Zhang, Q. Pei, F. Dai, and L. Zhang, "Efficient Secure and Privacy-Preserving Route Reporting Scheme for VANETs," in *Journal of Physics: Conference Series*, vol. 910, no. 1. IOP Publishing, 2017, p. 012070.

[81] M. Vanhoef, "WiFuzz: Detecting and Exploiting Logical Flaws in the Wi-Fi Cryptographic Handshake."

[82] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, June 2004.

[83] M. Mitchell, *Complexity: A Guided Tour*. Oxford University Press, April 2009.

[84] V. Behzadan and A. Munir, "Adversarial Exploitation of Emergent Dynamics in Smart Cities," *Proc. of IEEE International Smart Cities Conference (ISC2), Kansas City, Missouri*, 2018.

[85] A. Munir and F. Koushanfar, "Design and Performance Analysis of Secure and Dependable Cybercars: A Steer-by-Wire Case Study," in *IEEE Annual Consumer Communications Networking Conference (CCNC)*. Las Vegas, NV, USA: IEEE, January 2016, pp. 1066–1073.

[86] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[87] V. Behzadan, "Cyber-Physical Attacks on UAS Networks-Challenges and Open Research Problems," *arXiv preprint arXiv:1702.01251*, 2017.

[88] A. Munir and F. Koushanfar, "Design and Analysis of Secure and Dependable Automotive CPS: A Steer-by-Wire Case Study," *IEEE Transactions on Dependable and Secure Computing*, 2018.

[89] M. Wolf and T. Gendrullis, "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module," in *Proceedings of the 14th International Conference on Information Security and Cryptology*. Springer-Verlag, Nov 2012, pp. 302–318.

[90] M. Khanafer, M. Guennoun, and H. T. Mouftah, "Intrusion Detection System for WSN-Based Intelligent Transportation Systems," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. Miami, FL, USA: IEEE, Dec 2010, pp. 1–6.

[91] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, September 2002.

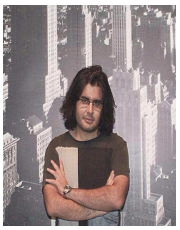
[92] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward Efficient and Privacy-Preserving Computing in Big Data Era," *IEEE Network*, vol. 28, no. 4, pp. 46–50, July 2014.

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

[94] A. Cavoukian, "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era," in *Privacy protection measures and technologies in business organizations: aspects and standards*. IGI Global, 2012, pp. 170–208.
[95] Y.-S. Martin and A. Kung, "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering," in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2018.
[96] A. Kung, J.-C. Freytag, and F. Kargl, "Privacy-by-design in ITS Applications," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*. IEEE, 2011, pp. 1–6.
[97] N. Asaj, F. Schaub, M. Muter, A. Held, and M. Weber, "ProTACD: A Generic Privacy Process for Vehicle Development," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2013, pp. 1675–1682.
[98] M. Kost and J. C. Freytag, "Privacy Analysis Using Ontologies," in *Proceedings of the second ACM conference on Data and Application Security and Privacy*. ACM, 2012, pp. 205–216.
[99] J. Lederman, B. D. Taylor, and M. Garrett, "A Private Matter: The Implications of Privacy Regulations for Intelligent Transportation Systems," *Transportation Planning and Technology*, vol. 39, no. 2, pp. 115–135, 2016.
[100] Y. Yuan and F.-Y. Wang, "Towards Blockchain-based Intelligent Transportation Systems," in *Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on*. IEEE, 2016, pp. 2663–2668.

Dalton Hahn is a Ph.D. student in the Department of Electrical Engineering and Computer Science at the University of Kansas. His research interests include computer security and privacy, with an emphasis on cyber-physical systems. Contact him at daltonhahn@ku.edu or 247N Nichols Hall, 2335 Irving Hill Road, Lawrence, KS 66045.

Arslan Munir is currently an Assistant Professor in the Department of Computer Science at Kansas State University. He obtained his Ph.D. in Electrical and Computer Engineering from the University of Florida, Gainesville, USA. His current research interests include embedded and cyber-physical systems, secure and trustworthy systems, computer architecture, parallel and distributed computing, and artificial intelligence safety and security. He is a Senior Member of IEEE. Contact him at amunir@ksu.edu or 2162 Engineering Hall, 1701D Platt St. Manhattan, KS 66506.



Vahid Behzadan is a Ph.D. candidate in the department of Computer Science at Kansas State University. He received his MS in Computer Science from University of Nevada, Reno, and a B.Eng. in Communications and Computer Systems from the University of Birmingham, UK. His research interests lie in the intersection of artificial intelligence, security, and complex adaptive systems. Contact him at behzadan@ksu.edu or 2184 Engineering Hall, 1701D Platt St., Manhattan, KS 66506.