A Safety and Security Architecture for Reducing Accidents in Intelligent Transportation Systems

(Invited Paper)

Qian Chen
Department of Electrical and
Computer Engineering
University of Texas at San Antonio
San Antonio, TX, USA
guenevereqian.chen@utsa.edu

Azizeh Khaled Sowan
School of Nursing
University of Texas Health Science
Center at San Antonio
San Antonio, TX, USA
sowan@uthscsa.edu

Shouhuai Xu
Department of Computer Science
University of Texas at San Antonio
San Antonio, TX, USA
shouhuai.xu@utsa.edu

ABSTRACT

The Internet of Things (IoT) technology is transforming the world into Smart Cities, which have a huge impact on future societal lifestyle, economy and business. Intelligent Transportation Systems (ITS), especially IoT-enabled Electric Vehicles (EVs), are anticipated to be an integral part of future Smart Cities. Assuring ITS safety and security is critical to the success of Smart Cities because human lives are at stake. The state-of-the-art understanding of this matter is very superficial because there are many new problems that have yet to be investigated. For example, the cyber-physical nature of ITS requires considering human-in-the-loop (i.e., drivers and pedestrians) and imposes many new challenges. In this paper, we systematically explore the threat model against ITS safety and security (e.g., malfunctions of connected EVs/transportation infrastructures, driver misbehavior and unexpected medical conditions, and cyber attacks). Then, we present a novel and systematic ITS safety and security architecture, which aims to reduce accidents caused or amplified by a range of threats. The architecture has appealing features: (i) it is centered at proactive cyber-physical-human defense; (ii) it facilitates the detection of early-warning signals of accidents; (iii) it automates effective defense against a range of threats.

KEYWORDS

Intelligent Transportation System, Safety and Security Architecture, Internet of Things, Connected Vehicles, Human Factor

ACM Reference Format:
Qian Chen, Azizeh Khaled Sowan, and Shouhuai Xu. 2018. A Safety and Security Architecture for Reducing Accidents in Intelligent Transportation Systems, *(Invited Paper)*. In *IEEE/ACM INTERNATIONAL CONFERENCE ON COMPUTER-AIDED DESIGN (ICCAD '18), November 5–8, 2018, San Diego, CA, USA.* ACM, New York, NY, USA, Article 4, 7 pages. https://doi.org/10.1145/3240765.3243462

1 INTRODUCTION

The Internet of Things (IoT) technology is changing the world by impacting every aspect of the society, economy, and business. The automobile sector will play an important role in this transformation. This can be justified by the following forecasts: more than 94 million vehicles in 2021 will be connected [1]; autonomous and IoT connected Electric Vehicles (EVs) will dominate the roads by 2030 [2, 3]; more changes are expected in the transportation industry in the next five to ten years than the changes that have been made in the past 50 years [4, 5]. Numerous benefits of the new technology are expected, such as:

(1) Safety Benefits: today, the safety of our roadways mainly depends on the human drivers; however, human drivers alone are not trustworthy because each year, 1.3 million people around the world die in road crashes [6], and 94% of these accidents are caused by human errors [7]. In the future, communications among vehicles (i.e., Vehicle to Vehicle or V2V), transportation infrastructures (i.e., Vehicle to Infrastructure or V2I) and other components of an ITS (i.e., V2X) are expected to help reduce or prevent accidents. The National Highway Traffic Safety Administration estimates that in the United States, the ITS and connected vehicles technology annually will reduce up to 80% of the non-impaired-driving crashes, potentially reducing 400,000 to 600,000 crashes and saving 780 to 1,080 human lives [8, 9].
(2) Mobility Benefits: the United States highway users waste more than 6.9 billion hours in traffic congestion [10]. It is anticipated that connected vehicles together with V2I applications will improve the traffic signal system to reduce traffic congestions and travel delay. For example, up to 23% transportation time will be saved for an emergency vehicle; vehicle travel time on freeways will be reduced by 42% when cooperative adaptive cruise control and speed harmonization (along with V2V and V2I) technology are effective [11].
(3) Environmental Benefits: Highway fuel consumption in the United States has increased 86% since 1970 [12]. ITS connectivity and V2X communication environmental applications are expected to provide real-time "green" transportation options for drivers. By applying eco-signal operations, each year drivers can reduce 11% of carbon dioxide emission and 3.1 billion gallons of fuel consumption [11]. By 2050, connected autonomous vehicles can reduce fuel consumption by 44% for passenger vehicles and 18% for trucks [13].

ICCAD '18, November 5–8, 2018, San Diego, CA, USA
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5950-4/18/11...$15.00
https://doi.org/10.1145/3240765.3243462

(4) Financial Benefits: The United States used nearly nine billion barrels of petroleum in the year of 2017, two-thirds of which consumed for transportation purposes [14]. The uncertainty in oil price and supply disruptions can cause significant financial losses. The situation is anticipated to get much better because a connected EV requires a much lower running cost, while being more efficient than a conventional gasoline vehicle [15]. The wide adoption of connected EVs can also diversify the choice of fuels, effectively reducing our reliance on petroleum [14]. Moreover, it is anticipated that ITS and connected EVs can reduce personal and societal costs of transportation, while creating many opportunities in the automobile and electric power industries [16].

The preceding benefits will improve the quality of societal lives. However, impaired and unimpaired automobile accidents caused by human factors and Cyber-Physical Attacks (CPAs) cannot be ruled out without being adequately understood and addressed. From a safety's point of view, two causes of crashes are drivers' misbehavior and medical conditions [17], which respectively include (i) drugs, alcohol, drowsiness and distraction, and (ii) sudden medical conditions (e.g., heart attack), complicationss of a current disease (e.g., hypoglycemic in diabetic patients, seizures attach in epilepsy patients), and side effects of medications (e.g., psychotic treatment or agents with central nervous system side effects that can cause symptoms as drowsiness, blurred vision, lack of concentration, muscle weakness or lack of control, and slowed reaction time) [18]. From a security's point of view, recent research demonstrates that computer systems controlling modern vehicles can be compromised by either physical or remote (cyber) attacks [19, 20], which are consequentially a big threat to safety. In particular, terrorists can exploit vehicles to wage cyber attacks; for example, since 2016, the vehicle-ramming attack has killed or injured hundreds of people in 10 major incidents across Europe [21]; there were more than 20 vehicle-as-a-weapon attacks in 2017 [22]; and the van attack in Toronto killed 10 pedestrians [23].

Our contributions. The anticipated huge impact of the ITS and EVs technology highlights that the research community must have a deeper understanding of the threats of unintentional human errors (i.e., misbehavior and medical conditions), malfunctions of ITS components, and cyber-physical security attacks against transportation safety. In this paper, we conduct a systematic investigation on this problem and propose a preliminary design of solutions. Specifically, we make the following contributions.

- We analyze the threats against ITS safety and security, while considering both the threats posed by human factors and the threats posed by cyber attacks that are waged against ITS infratructures and EVs.
- We propose a novel safety and security architecture for protecting ITS and EVs from those threats and ultimately for reducing transportation accidents to save human lives.

To the best of our knowledge, both the threat analysis and the safey and security architecture represent the first of their kinds.

Paper outline. In the following sections, we analyze a systematic threat model against road traffic safety in Section 2, we present a novel and systematic ITS safety and security architecture in Section 3, review the state-of-the-art research methods and technologies related to our study in Section 4, and conclude the paper in Section 5.

2 CYBER-PHYSICAL-HUMAN (CPH) THREAT MODELS AGAINST INTELLIGENT TRANSPORTATION SYSTEMS

ITS safety and security threats can originate from three domains: human factors, physical systems, and cyberspace. As illustrated in Figure 1, cyber-physical threats can cause ITS mechanical failures or malfunctions (e.g., cyber attacks may directly cause cars to run into each other or break traffic lights); human factors (e.g., human errors and driver medical conditions) are critical reasons for car crashes; medical conditions can make driver lose control of vehicles and therefore cause accidents. In the rest of this section we elaborate these threats.

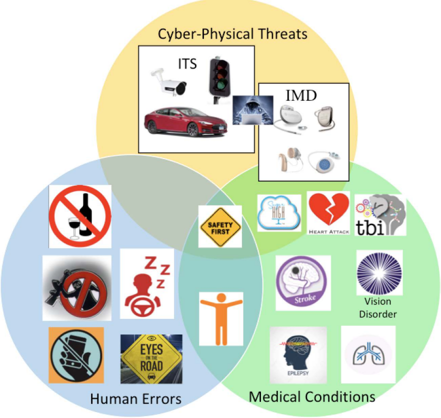

Figure 1: CPH threat models against ITS

2.1 Modeling Threats in the Driver (Human) Domain

Driver misbehaviors (e.g., impaired driving, distracted driving, drowsy driving) and terrorist attacks (i.e., abusing vehicles as a weapon) are the leading causes of car collisions. A single misbehavior, or a combination of them, can significantly increase the fatality rate. For instance, studies have showed that drivers consumption of a low and legal dose of alcohol with moderate sleep restriction can still undermine driving performance and reaction time [24–27]. Moreover, drivers suffering from chronic illness — such as cardiovascular disease, epilepsy, cerebrovascular accident (stroke), alcohol abuse and alcohol dependence, anemia, traumatic brain injury, diabetes mellitus, vision disorder, psychotic disorders, and asthma — can experience loss of consciousness and body control or even sudden death in the course of driving [28, 29].

Medical conditions often necessitate wireless Implantable Medical Devices (IMDs) for diagnostics, monitoring (e.g., glucose and neuro monitors, smart bandages to monitor wound healing), treatment purposes (e.g., insulin pumps, defibrillators), or a combination of them (e.g., cardioverter defibrillators are used to monitor heart rhythms and treat arrhythmias). Cyber-physical threats to drivers' wireless IMDs are big threats to their medical conditions. Therefore, threats against wireless IMDs intersect with both cyber-physical and medical condition domains are shown in Figure 1. That is, deadly crashes caused by human errors, misbehaviors, chronic medical conditions and unexpected medical emergencies must be considered and included in the road safety and security threat model.

2.2 Modeling Threats against the ITS Cyber-Physical System (CPS)

We classify these threats into three categories according to the attack points: connected vehicles, V2X security, and wireless implantable medical devices.

Threats against connected vehicles. The In-Vehicle-Network (IVN) of modern connected vehicles contains two subsystems: the *infotainment* system and the *Vehicle Control System* (VCS). Using the Tesla Model S [30] EV as an example, its infotainment system is built on a 17-inch touchscreen Center Information Display (CID) and an Instrument Cluster (IC). Similar to all modern vehicles, Tesla Model S has a central gateway functioning like a router to separate VCS data from the infotainment system's data. The central gateway can prevent an attacker from controlling a vehicle via the compromised infotainment system. However, the connector below the CID of the Tesla EV can let malicious users "enter" the VCS via an Ethernet cable [31]. Therefore, the CAN bus, which is the primary network protocol for communicating messages between processors, sensors, and actuators of the EV, can be monitored, hijacked and fabricated. The malfunction of EV hardware can cause deadly crashes. The EV cybersecurity vulnerabilities are elaborated as follows.

(1) Threats against communication links: The network protocols of the Tesla EV infotainment system and of the VCS are UDP-based and CAN bus, respectively. Vulnerabilities in the IVN communication protocols include the lack of confidentiality, integrity, or authentication of messages, which may allow an attacker to control the EV in question, extract vehicle measurements, and display spoofed vehicle information about the IC and CID. The infotainment system can also be connected to, and accessed by, a smart phone, meaning that vulnerabilities in Bluetooth and Wi-Fi should be considered as well.

(2) Threats against vehicle hardware (i.e., sensors and actuators): Sensors (e.g., cameras, GPS, radar, and LIDAR) and actuators (e.g., autopilot) of EVs are not attack-proof. Cybersecurity vulnerabilities in their firmware should be assessed and attack vectors should be taken into account.

(3) Threats against Operating System (OS): Tesla EV OS is modified from the Ubuntu operating system and runs on two NVIDIA Tegra processors. Therefore, the vehicle OS might be compromised by exploiting its software vulnerabilities.

Threats against V2X security. Vehicle Wireless Communication Technologies, such as Dedicated Short Range Communications (DSRC), 4th and 5th generation wireless technology, are developed to support ITS V2V and V2I communications. DSRC, a two-way medium range wireless communication channel, is highly dependent upon cooperative standards for interoperability, and can significantly reduce crashes through real-time alerts to imminent hazards [32, 33].

The DSRC protocol stack consists of four layers, including physical (PHY), data link, network, transport and application layers. The physical protocol is defined in IEEE 802.11p, an amendment protocol for wireless access in vehicular environments (WAVE). The data link standard is divided into MAC (Medium-Access Control) and LLC (Logical Link Control). The MAC sublayer uses the IEEE 802.11p protocol and IEEE 1609.4 standard, whereas the LLC sublayer follows the IEEE 802.2 standard to switch the connected vehicles and Road Side Units (RSUs) of the ITS among radio channels when they are operating in a multi-channel environment.

DSRC middle layers employ a suite of IEEE 1609 standards. The network and transport layer adopts IEEE 1609.2 for security services and IEEE 1609.3 for network services, respectively. At the top of the DSRC stack is the DSRC message sublayer that uses the SAE J2735 Message Set Dictionary standard to support a variety of vehicle applications. The SAE protocol consists of 15 message types for V2V and V2I communications. For example, the Basic Safety Message (BSM) type packet conveys critical vehicle state information, such as the vehicle's position, dynamics, system states, and size to ITS smart transportation infrastructures. In addition, connected vehicles can send common safety request messages to check their neighboring vehicles' states. RSUs send geographic description of an intersection, traffic signal states, and hazardous traffic conditions to connected vehicles in real time, and can also manage the collection of probe data from vehicles via six types of messages specified in the SAE J2735 standard [33].

DSRC-equipped V2V and V2I communications use one-to-many unencrypted broadcast communication, which is an efficient way to disseminate safety-critical information. However, the trustworthiness of messages and their confidentiality are two major concerns because anyone in the ITS can receive and read broadcast messages. For instance, a malicious user can spoof as a legitimate RSU and can manipulate traffic signals or publish fake traffic conditions to control vehicles. False vehicle state information sent to its neighbors may cause fatal car crashes. The threat model of V2X communications must include the following aspects.

(1) Threats against authentication: There is no or little authentication in the DSRC protocols, meaning that attackers can spoof a legitimate vehicle or RSU to send false or misleading messages to control ITS.

(2) Threats against message confidentiality and integrity: The IEEE 1609.2 standard uses a combination of symmetric-key and asymmetric-key cryptosystems to protect messages from eavesdropping and sniffing attacks. Similarly, the SAE J2735 standard uses digital signatures to secure messages in their transmission. However, these mechanisms may impose significant overhead, especially when a vehicle is at a high speed.

(3) Threats against bandwidth: 75 MHz of bandwidth at 5.9 GHz of frequency is allocated for DSRC communications, but a connected vehicle can communicate 4,000 GB of data per day [34]. The ITS network thus will be the victim of Distributed Denial of Service (DDoS) attacks when vehicles and RSUs are compromised.

(4) Threats against ITS network and component segmentation: Current ITS networks have no segments. Malicious users can

undermine ITS security by launching catastrophic stepping stone attacks via the compromised ITS components.

(5) Threats against ITS component firmware: RSUs firmware would rarely be updated after initial installation, so are the vehicle's OS and firmware. Attackers can exploit vulnerabilities in unpatched ITS components to send fabricated DSRC messages to cause traffic collisions.

(6) Threats against ITS component hardware: The hardware of the ITS components are not tamper-resistant. For example, the open ports and open password prompts of vehicles and RSUs can be exploited as the entry points to penetrate into ITS.

Threats against wireless implantable medical devices (IMDs) security. Hundreds of millions of drivers have life-supporting or life-sustaining wilress IMDs [35, 36], such as cardiac pacemakers, defibrillators, cochlear implants, and insulin pumps. These IMDs can monitor drivers' health conditions, enhance disabled driver's quality of life, and prevent drivers from sudden deaths. With the fast development of the Internet of Medical Things (IoMT) technology, modern IMDs adopt the wireless technology to connect to physician offices, where health professionals can monitor drivers' health, adjust IMDs, and deliver medications remotely. However, this new technology also brings new threats. For example, cyber attacks can alter the driver's heartbeats via a vulnerable implanted cardiac pacemaker, can deliver random shocks to driver's hearts, can maliciously adjust program settings of cochlear implants, and can abuse the insulin pump to tamper with the delivery of medications. Threats against IMD security are dlaborated as follows.

(1) Threats against battery: Most IMDs are powered by batteries. Cyber attacks can drain the battery to stop the IMDs maliciously [37]. In addition, the rapid drainage of a battery may cause overheating in the body of the patient in question, which can be life-threatening [38].

(2) Threats against IMD firmware: Cyber attacks can exploit firmware vulnerabilities to remotely access the IMD, reboot or turn off the IMD, and/or manipulate the dispense amount of fluid or highly-sensitive medication.

(3) Threats against communication links: Various communication methods are in use or proposed for communicating with implantable devices, such as near-field communication [39], body-coupled communication [40], and ultrasound [41]. However, all of these methods have security and safety implications [42]. Modern IoT-enabled IMDs sending data via Bluetooth and Wi-Fi have exacerbated this problem because threats against wireless protocol can cause malfunctioning of IMDs and can endanger human lives when patients are driving.

3 A SAFETY AND SECURITY ARCHITECTURE

In order to mitigate the CPH threats discussed above, we propose a safety and security architecture as shown in Figure 2. The architecture includes an intelligent use of a collection of functions such as encryption, cyber-physical vulnerability analysis, intrusion detection, behavior prediction, and machine learning technologies. As elaborated below, the architecture consists of (i) safety and security (S2) modules at ITS components, and (ii) a cloud-based road traffic S2 automated control center (S2 ACC for short).

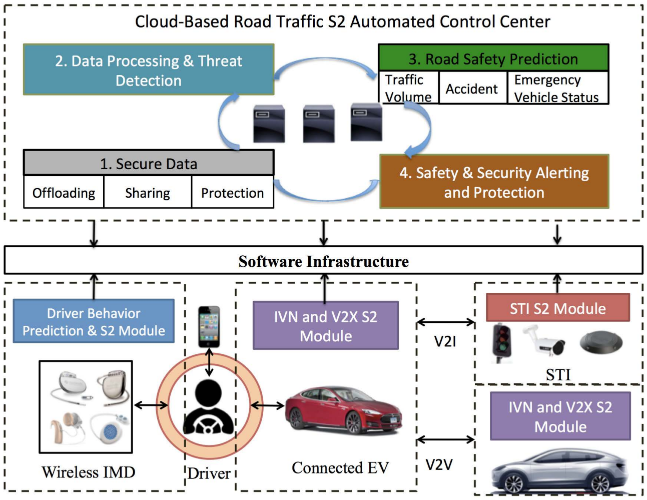

Figure 2: ITS Safety and Security (S2) Architecture

3.1 S2 Modules at ITS Components

ITS components include connected vehicles, connected drivers, and smart transportation infrastructures (STI) (i.e., traffic signals, cameras, and smart parking systems). The functions of S2 modules are described as follows.

3.1.1 Driver Behavior Prediction & S2 Module. As discussed earlier, human errors and cyber-physical attacks against wireless IMD are big threats to ITS safety and security. This module is responsible for assuring normal operations by authenticated drivers and protecting drivers with chronic medical conditions and unexpected medical emergencies.

Assuring driver authentication.

- Biometric access control for driver authentication: Instead of using a physical key with an addtional layer of protection (e.g., RFID tokens) to defend against theft of vehicle control, biometric information of the user(s)/owner(s) can be validated before the drivers entering a vehicle. Technologies such as 3D face recolonization [43], fingerprints, retinal scans or voice recognition have been used to unlock smartphones. These existing technologies along with biometric-based user authentication methods (e.g., foot motion [44], pulse-response [45], and ECG signles [46]) can be deployed at a vehicle or the users' smartphones, possibly with the assistance of Internet of Medical Things (IoMT) sensors such as Apple watch [47] and Mysignal [48].
- Modeling driver behavior: An attacker can get through the authentication process by stealing biometrics of authenticated drivers. In order to defeat this attack, a driver behavior model can be leveraged to detect this attack. A driver behavior model can be trained from data describing vehicle trajectories, driving characteristics that can be obtained from the IVN Controller Area Network (CAN)-Bus information (e.g., steering wheel angles, brake status, acceleration status, and vehicle speed). Machine learning algorithms such as

Hidden Markov Model [49, 50], K-means clustering cross-validation [51], and support vector machine [52] have been applied to build driving behavior models and detect malicious drivers. Driving behavior models for personal vehicles (<=5 drivers) can be deployed as a part of the IVN S2 module at the vehicle end. Driving behavior models for business vehicles (e.g., a company's vehicles and rental cars) allowing more drivers (> 5 drivers) can be deployed at the S2 ACC. In addition, drivers can choose to save their driving behavior models of personal vehicles in the S2 ACC. When a driver operating a business vehicle for the first time, the driver's behavior can be estimated based on existing behavior models. The new driver's identity can be authenticated in real-time without requiring new learning and training processes.

Protecting wireless IMDs from cyber-physical attacks. These attacks should be detected and filtered in real time. Anomaly and rule-based intrusion detection and prevention systems are deployed at IMDs' gateways (i.e., the paired smartphones) to protect drivers from fatal attacks to their IMDs. The driving behavior model, possibly extended to include drivers' biometric features (e.g., heart rate, blood pressure, respiration rate, temperature, glucose level and sleep quality), can be used to predict human errors, such as a driver's misbehavior and medical condition, and cyber-physical attacks that attempt to bypass the intrusion detectors deployed at the wireless IMDs. This biometric information data can be monitored and collected by IoMT sensors (i.e., the same sensors for biometric access control). Human errors and cyber-physical attacks against wireless IMDs can be detected if the driver's biometric behavior along with the vehicle trajectory and the driving characteristic features deviate. This extended driving behavior model can be deployed at vehicles if an in-vehicle security server is available; otherwise, it should be deployed at the S2 ACC.

3.1.2 IVN and V2X S2 Module.

This module is responsible for assuring security of IVN and V2X communications. One strategy is to use asymmetric key cryptography and the Public-Key Infrastructures (PKI) for the key distribution. The PKI maintains trust through a chain of certificates from an end-entity certificate to the Root Certification Authority's certificate. A chain of trust is established through verification of digital signatures that are included in certificates, which are issued by the immediate higher-level authority in the chain. In addition, intrusion detection system can be deployed at vehicles to monitor messages from/to connected vehicles. Malicious requests/commands to connected vehicles are eliminated before they enter the IVN. Messages originated from a malicious vehicle cannot reach any components in the ITS network (or S2 ACC).

3.1.3 Smart Transportation Infrastructures (STI) S2 Module.

Similar to the IVN and V2X S2 module, this module is responsible for assuring security of the STI. In addition to the intrusion detection systems that identify malicious communication traffic from/to the STI, the STI S2 module monitors failures of the STI. For example, malfunction of traffic cameras and power outage of traffic signals. These failure messages can be sent to the S2 ACC to launch a remote trouble shooting process to automatically repair the malfunctioning STI, or can be sent to local government offices or their contractors. This module is deployed at every STI.

3.2 Cloud-Based ITS Safety and Security (S2) Automated Control Center (ACC)

The S2 ACC is deployed at the ITS cloud server. Its incorporated security mechanisms can include the current standard practice of anti-malware tools, which often operate at the OS kernel-level to detect suspicious activities [53]. The S2 ACC is responsible for extracting new attack information that can be rapidly shared with the other S2 ACCs, in a fashion similar to the architecture described in [54].

1. Securing data: Offloading, data sharing, and data protection are three functions for protecting data transmission and data sharing between ITS components (e.g., drivers, connected vehicles, and STIs) and the S2 ACC. The offloading function is responsible for securely offloading general programs, cryptographic computations (encrypting/descripting V2X traffic), malware and intrusion detection tasks as we discussed for the S2 modules mentioned above. The data sharing function is responsible for securely sharing data as requested by ITS components/cloud services. Traditional access control methods can be applied for secure data sharing. The data protection function aims to mitigate the damage caused by attacks that have penetrated into the vehicles and STIs. The encrypted ITS component data (e.g., driving data, vehicle information) can be decrypted by the authenticated drivers using their private keys.
2. Data processing and threat detection: This module processes the large volume of data and detects threats against ITS traffic safety. An Information Relative (IR) approach can be applied to extract the most significant features for developing a highly-accurate and low-overhead detection engine to identify collision threats in real time. Machine learning algorithms such as support vector machines, decision trees, neural networks can be used to detect unauthorized drivers, ITS cyber-physical attacks, human errors and driver's sudden medical emergencies that might lead to deadly traffic collisions (similar to the S2 modules deployed at ITS components).
3. Road safety prediction: The detected threat information are sent to the road safety prediction module for estimating traffic volume, possibility and severity of traffic accidents, and the location and status of emergency vehicles. For example, multiple driver errors and compromised vehicles are detected while large traffic volumes are among those misbehavior drivers and malicious vehicles; thus, the possibility of traffic accidents and fatal injuries are predicted as extremely high. In this scenario, the nearby emergency vehicles' location, status (on/off duty or idle) are used to predict how many minutes would the rescue team arrive to save lives if the accident cannot be prevented.
4. Safety and security alerting and protection module: Alerts must be sent to the misbehavior/victim drivers and their neighbors (e.g., drivers, passengers and pedestrians) immediately after the threats are detected. Authorized drivers,

highway patrols, police offices, hospitals, and fire departments should be notified as well. Similar to the alerting system, protection mechanisms must be automatically implemented to prevent from an upcoming crash. For instance, the protection design of a connected vehicle should engage its autopilot system to reduce vehicle speed, get off the highway, and/or pull over when cyber-physical attacks and/or unauthorized driver threats are detected. Smart traffic signals should adjust the timing of the lights depending on real-time traffic volumes. This module should also launch an automatic trouble-shooting process to fix a software failure issue of STI components and send a repair request or an alert to local government offices or their contractors.

4 RELATED WORK

Most vehicle security studies are centered at reverse engineering vehicle communication protocols (e.g., CAN and DSRC) and demonstrating how to take control of vehicles. For example, one can sniff the CAN packets to obtain responses from a compromised vehicle [55]; one can mislead the ECUs and diagnostic devices to make them believe that airbag control modules are absent [56]; one can crash the tire pressure monitoring system, the power steering control, the engineer control, the adaptive cruise control, the electronic parking brake, and the parking assist modules [57–60]; one can block the normal vehicle services by flooding the VIN with garbage, but high priority messages [61, 62].

In terms of defense, most studies focus on investigating how to use Public-Key Infrastructures (PKIs) for distributing and managing cryptographic keys to improve security and privacy in the communications between ITS components. For example, a Security Credential Management System (SCMS) [63] would support bootstrapping, certificate provisioning, misbehavior reporting, and revocation. While it is tempting to revoke misbehaving/malfunctioning vehicles, this approach is limited because it assumes that attacks can be accurately detected — a difficult problem on its own. As an improvement, it has been discussed to use the blockchain technology, which offers a distributed Event Data Recorder (EDR), to provide a compressed global state that can be used to meet the accountability requirements [64]. The accountable revocation mechanism of the blockchain technology allows a collaborative and transparent decision-making process, which prevents the issuance of malicious certificates by misbehaving authority.

In terms of human factors, there have been some studies on understanding driver behaviors. For example, spatiotemporal datasets, such as the New York Taxi Dataset [65] and vehicle trajectory datasets collected by insurance companies [66], have been used to analyze driver behaviors (e.g., potential causes of certain driving patterns in terms of vehicle location, speed, and time). As another example, MIT Autonomous Vehicle Technology recruited 78 participants and captured 3.5 billion video frame of the participants who drove 275,589 miles in 7,146 days; the dataset is used for understanding correlations of car crashes, human interaction, mental models and vehicle automation technology [67]. Despite these efforts, driver behavior is far from being adequately understood, including the interaction between human drivers and the situation surround them.

Compared with the studies reviewed above, we are the first to propose, to the best of our knowledge, a systematic safety and security architecture that accommodates threats against safety and cyber security, while noting that the latter can further cause threats against ITS and EV safety.

5 CONCLUSION

Motivated by the importance to of the emerging Intelligent transportation systems and its huge impact on the future society, we have presented a systematic investigation on the threats against safety and security of these systems. In the threat model, we consider both human factors and intentional cyber attacks. The threat model leads us to propose a systematic safety and security architecture for protecting intelligent transportation systems, with the ultimate goal of reducing transportation accidents and saving human lives.

The present study is still preliminary, and future studies are needed to refine the threat model and the safety and security architecture. Both theoretical and experimental evaluation of the architecture, including the building-block mechanisms the architecture can incorporate, are left as outstanding problems for future research.

ACKNOWLEDGMENTS

This material is based on research sponsored by National Science Foundation (NSF) under Grant No.1700391. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

REFERENCES

[1] A. Meola, “Automotive industry trends: Iot connected smart cars & vehicles,” 2016. http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10.
[2] M. Anderson, “Rethinkx: Self-driving electric cars will dominate roads by 2030,” May 2017. https://spectrum.ieee.org/cars-that-think/transportation/self-driving/rethinkx-selfdriving-electric-cars-will-dominate-roads-by-2030.
[3] J. Shankleman, “The electric car revolution is accelerating,” July 2017. https://www.bloomberg.com/news/articles/2017-07-06/the-electric-car-revolution-is-accelerating.
[4] K. Burke, “The auto industry will change more in next five years than prior 50, says gm’s president,” June 2016. https://goo.gl/fw7cem.
[5] M. Barra, “The next revolution in the auto industry,” Jan. 2016. https://www.weforum.org/agenda/2016/01/the-next-revolution-in-the-car-industry/.
[6] A. For Safe International Road Travel, “Annual global road crash statistics,” 2018. http://asirt.org/initiatives/informing-road-users/road-safety-facts/road-crash-statistics.
[7] NHTSA, “Traffic safety facts,” *U.S. Department of Transportation*, 2015. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115.
[8] Autotalks, “Usdot issued nprm mandates v2v,” 2017. https://www.auto-talks.com/nprm-mandates-v2v/.
[9] Bowman and B. M. V. Group, “Vehicle safety in a connected world-nhtsa proposed rulemaking on v2v technology and oem liability,” 2016. https://www.bowmanandbrooke.com/insights/nhtsa-proposed-rulemaking-v2v-communication-tech.
[10] E. Dooley, “Here’s how much time americans waste in traffic,” Aug 2015. https://abcnews.go.com/US/time-americans-waste-traffic/story?id=33313765.
[11] U. DOT, “Connected vehicle benefits,” 2016. https://www.its.dot.gov/factsheets/pdf/ConnectedVehicleBenefits.pdf.
[12] O. of Highway Policy Information-U.S. DOT, “Highway finance data collection: Motor fuel,” 2014. https://www.fhwa.dot.gov/policyinformation/pubs/hf/pl11028/chapter5.cfm.
[13] J. McMahon, “Big fuel savings from autonomous vehicles,” 04 2017. https://www.forbes.com/sites/jeffmcmahon/2017/04/17/big-fuel-savings-from-autonomous-vehicles/#5907d57c4390.
[14] D. of Energy, “Electric vehicle benefits,” 2018. https://www.energy.gov/eere/electricvehicles/electric-vehicle-benefits.

[15] D. of Energy, "Saving on fuel and vehicle costs- egallon: Compare the costs of driving with electricity," 2018. https://www.energy.gov/eere/electricvehicles/saving-fuel-and-vehicle-costs.

[16] A. Mai and D. Schlesinger, "A business case for connecting vehicles executive summary," tech. rep., Cisco Internet Business Solutions Group, 2011.

[17] NHTSA, "Crash stats: Critical reasons for crashes investigated in the national motor vehicle crash causation survey," 2018. https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812506.

[18] A. Hetland and D. B. Carr, "Medications and impaired driving," *Ann Pharmacother*, vol. 48, pp. 494–506, Apr 2014.

[19] A. Greenberg, "Hackers remotely kill a jeep on the highway-with me in it," July 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[20] R. Toews, "The biggest threat facing connected autonomous vehicles is cybersecurity," Aug. 2016. https://techcrunch.com/2016/08/25/the-biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/.

[21] Telegraph, "Timeline of vehicle rampage attacks in europe," Apr. 2018. https://www.telegraph.co.uk/cars/news/timeline-vehicle-terror-attacks-europe/.

[22] B. M. Jenkins, "Navigating the latest terrorism trend," Dec. 2017. https://www.usnews.com/opinion/world-report/articles/2017-12-15/2017-saw-boom-in-use-of-vehicles-in-terrorist-attacks.

[23] E. L. et al., "A van speeds across toronto sidewalks, leaving 10 pedestrians dead," 2018. https://www.cnn.com/2018/04/23/world/toronto-collision-pedestrians/index.html.

[24] J. H. et al., "Driving impairment due to sleepiness is exacerbated by low alcohol intake," *Occup Environ Med*, vol. 60, pp. 689–692, Sep 2003.

[25] A. V. et al., "Effects of moderate sleep deprivation and low-dose alcohol on driving simulator performance and perception in young men," *Sleep*, vol. 30, pp. 1327–1333, Oct 2007.

[26] J. L. et al., "Alcohol and sleep restriction combined reduces vigilant attention, whereas sleep restriction alone enhances distractibility," *Sleep*, vol. 38, no. 5, 2015.

[27] M. L. B. et al., "Impaired inhibition after total sleep deprivation using an antisaccade task when controlling for circadian modulation of performance," *Physiol. Behav.*, vol. 124, pp. 123–128, Jan 2014.

[28] J. L. Charlton, *Influence of chronic illness on crash involvement of motor vehicle drivers.* 2004.

[29] P. C. D. et al., "Medical conditions and car crashes," *Annu Proc Assoc Adv Automot Med*, vol. 44, pp. 335–346, 2000.

[30] "Tesla Model S," 2018. https://www.tesla.com/models.

[31] K. Mahaffey, "Hacking a tesla model s: What we found and what we learned," 08 2015. https://blog.lookout.com/hacking-a-tesla.

[32] U. D. of Transportation, "Dsrc: The future of safer driving," 2018. https://www.its.dot.gov/factsheets/dsrc_factsheet.htm.

[33] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, pp. 1162–1182, July 2011.

[34] "Just one autonomous car will use 4,000 gb of data/day," 2018. https://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html.

[35] B. A. et al., "Power Approaches for Implantable Medical Devices," *Sensors (Basel)*, vol. 15, pp. 28889–28914, Nov 2015.

[36] M. R. et al., "Statistics on the use of cardiac electronic devices and electrophysiological procedures in the european society of cardiology countries: 2014 report from the european heart rhythm association," *EP Europace*, vol. 17, 2015.

[37] X. H. et al., "Defending resource depletion attacks on implantable medical devices," in *GLOBECOM 2010*, pp. 1–5, Dec 2010.

[38] N. S. A. et al., "High-Efficiency Wireless Power Delivery for Medical Implants Using Hybrid Coils," in *EMBC 2012*, (San Diego, CA), Aug-Sep 2012.

[39] X. H. et al., "Poster: Near field communication based access control for wireless medical devices," in *ACM MobiHoc*, pp. 423–424, ACM, 2014.

[40] C. L. et al., "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, pp. 150–156, IEEE, 2011.

[41] K. B. R. et al., "Proximity-based access control for implantable medical devices," in *CCS 2009*, pp. 410–419, ACM, 2009.

[42] T. Halevi and N. Saxena, "On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping," in *CCS*, pp. 97–108, ACM, 2010.

[43] H. Moon and K. Lee, "Biometric driver authentication based on 3d face recognition for telematics applications," in *Universal Acess in Human Computer Interaction* (C. Stephanidis, ed.), (Berlin, Heidelberg), pp. 473–480, Springer Berlin Heidelberg, 2007.

[44] D. G. et al., "User authentication based on foot motion," *Signal, Image and Video Processing*, vol. 5, p. 457, Aug 2011.

[45] I. M. et al., "Authentication using pulse-response biometrics," *Commun. ACM*, vol. 60, pp. 108–115, Jan. 2017.

[46] C. C. et al., "Human identification using compressed ecg signals," *Journal of Medical Systems*, vol. 39, p. 148, Sep 2015.

[47] "Apple watch," 2018. https://www.apple.com/apple-watch-series-3/.

[48] "MySignal-ehealth and medical iot development platform," 2018. http://www.my-signals.com/.

[49] C. Miyajima and K. Takeda, "Driver-behavior modeling using on-road driving data: A new application for behavior signal processing," *IEEE Signal Processing Magazine*, vol. 33, pp. 14–21, Nov 2016.

[50] S. Choi and et al., "Analysis and classification of driver behavior using in-vehicle can-bus information," 2007.

[51] U. F. et al., "Driving behavior analysis through can bus data in an uncontrolled environment," 2017.

[52] A. B. et al., "Driver identification and authentication with active behavior modeling," in *2016 12th CNSM*, pp. 388–393, Oct 2016.

[53] S. Xu, E. P. Ratazzi, and W. Du, "Security architecture for federated mobile cloud computing," 2013. https://pdfs.semanticscholar.org/67ed/c4d4f8385c297b6d54dcd045cf96c28cbbb6.pdf.

[54] L. Xu, G. Tan, X. Zhang, and J. Zhou, "Aclome: Agile cloud environment management platform," in *2013 Fourth International Conference on Digital Manufacturing Automation*, pp. 101–105, June 2013.

[55] C. Valasek and C. Miller, "Adventures in automotive networks and control units," *IOActive*, 2014.

[56] T. H. et al., "Security threats to automotive can networks-practical examples and selected short-term countermeasures," *Reliability Engineering & System Safety*, vol. 96, no. 1, pp. 11–25, 2011.

[57] C. Valasek and C. Miller, "Can message injection," 2016. http://illmatics.com/canmessageinjection.pdf.

[58] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," 2015. http://illmatics.com/RemoteCarHacking.pdf.

[59] C. Miller and C. Valasek, "Adventures in automotive networks and control units," 2014. http://illmatics.com/car_hacking.pdf.

[60] I. R. et al., "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Usenix Security Symposium, Washington, Dc, Usa, August 11-13, 2010, Proceedings*, pp. 323–338, 2010.

[61] B. Elend and T. Adamson, "Cyber security enhancing can transceivers," 2017. https://www.can-cia.org/fileadmin/resources/documents/conferences/2017_elend.pdf.

[62] S. M. et al., "Practical dos attacks on embedded networks in commercial vehicles," 2016.

[63] B. B. et al., "A security credential management system for v2x communications," 2018.

[64] R. W. van der Heijden et al., "Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication," 2017.

[65] "New york taxi dataset," 2009-2017. http://www.nyc.gov/html/tlc/html/about/trip_record_data.shtml.

[66] S. M. et al., "Characterizing driving context from driver behavior," 2017.

[67] L. F. et al., "Mit autonomous vehicle technology study: Large-scale deep learning based analysis of driver behavior and interaction with automation," 2017.