A Risk Based Approach to Intelligent Transportation Systems Security

Kaveh Bakhsh Kelarestaghi

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Civil Engineering

Kevin Heaslip, Chair
Alireza Ermagun
Ralph Buehler
Kathleen Hancock
Ryan Gerdes

May 13, 2019
Falls Church, VA

Keywords:

Intelligent Transportation Systems, Cyber Security, Cyber-Physical Systems, Vulnerability Assessment, Attack Tree, Dynamic Message Sign, Risk Assessment, Impact Assessment, Travelers Behavior, Distracted Driving, Speed Variation, Route Divergence Behavior

A Risk Based Approach to Intelligent Transportation Systems Security

Kaveh Bakhsh Kelarestaghi

ABSTRACT (Academic)

Security threats to cyber-physical systems are targeting institutions and infrastructure around the world, and the frequency and severity of attacks are on the rise. Healthcare manufacturing, financial services, education, government, and transportation are among the industries that are the most lucrative targets for adversaries. Hacking is not just about companies, organizations, or banks; it also includes critical infrastructure. Wireless Sensors Networks, Vehicle-to-everything communication (V2X), Dynamic Message Signs (DMS), and Traffic Signal Controllers are among major Intelligent Transportation Systems (ITS) infrastructure that has already been attacked or remain vulnerable to hacking. ITS has been deployed with a focus on increasing efficiency and safety in the face of dramatic increases in travel demand. Although many studies have been performed and many security primitives have been proposed, there are significant concerns about flawless performance in a dynamic environment. A holistic security approach, in which all infrastructure performs within the satisfactory level of security remains undiscovered. Previously, hacking of road infrastructure was a rare event, however, in recent years, field devices such as DMS are hacked with higher frequency. The primary reason that transportation assets are vulnerable to cyber-attacks is due to their location. A more dramatic scenario occurs when hackers attempt to convey tampered instructions to the public.

Analyzing traveler behavior in response to the hacked messages sign on the basis of empirical data is a vital step toward operating a secure and reliable transportation system. There may be room for improvement by policymakers and program managers when considering critical infrastructure vulnerabilities. With cybersecurity issues escalating every day, road users' safety has been neglected. This dissertation overcomes these challenges and contributes to the nascent but growing literature of Intelligent Transportation System (ITS) security impact-oriented risk assessment in threefold.

- First, I employ a risk-based approach to conduct a threat assessment. This threat assessment performs a qualitative vulnerability-oriented threat analysis. The objective is to scrutinize safety, security, reliability, and operation issues that are prompted by a compromised Dynamic Message Signs (DMS).
- Second, I examine the impact of drivers' attitudes and behaviors on compliance, route diversion behavior, and speed change behavior, under a compromised DMS. We aim to assess the determinants that are likely to contribute to drivers' compliance with forged information. To this extent, this dissertation evaluates drivers' behavior under different unauthentic messages to assess in-depth the impact of an adversarial attack on the transportation network.
- Third, I evaluate distracted driving under different scenarios to assess the in-depth impact of an adversarial attack on the transportation network. To this extent, this dissertation examines factors that are contributing to the manual, visual, and

cognitive distractions when drivers encountering fabricated advisory information at a compromised DMS.

The results of this dissertation support the original hypothesis and indicate that with respect to the forged information drivers tend to (1) change their planned route, (2) become involved in distracting activities, and (3) change their choice speed at the presence of a compromised DMS. The main findings of this dissertation are outlined below:

1. The DMS security vulnerabilities and predisposing conditions allow adversaries to compromise ITS functionality. The risk-based approach of this study delivers the impact-likelihood matrix, which maps the adverse impacts of the threat events onto a meaningful, visual, matrix. DMS hacking adverse impacts can be categorized mainly as high-risk and medium-risk clusters. The safety, operational (i.e., monetary losses) and behavioral impacts are associated with a high-risk cluster. While the security, reliability, efficiency, and operational (i.e., congestion) impacts are associated with the medium-risk cluster.
2. Tech friendly drivers are more likely to change their route under a compromised DMS. At the same time, while they are acquiring new information, they need to lowering their speed to respond to the higher information load. Under realistic-fabricated information, about 65% of the subjects would depart from their current route. The results indicate that females and subjects with a higher driving experience are more likely to change their route. In addition, those subjects who are more sensitive to the DMS's traffic-related messages and those who use DMS under congested traffic condition are more likely to divert. Interestingly, individuals with lower education level, Asians, those who live in urban areas, and those with trouble finding their direction in new routes are less likely to pick another route rather the one they planned for.
3. Regardless of the DMS hacking scenarios, drivers would engage in at least one of the distractive activities. Among the distractive activities, cognitive distraction has the highest impact on the distracted driving likelihood. Meaning, there is a high chance that drivers think of something other than driving, look at surrounding traffic and scenery, or talk to other passengers regarding the forged information they saw on the DMS. Drivers who rely and trust in technology, and those who check traffic condition before starting their trips tend to become distracted. In addition, the result identified that at the presence of bogus information, drivers tend to slow down or stop in order to react to the DMS. That is, they would either (1) become involved in activities through the means of their phone, (2) they would mind wander, look around, and talk to a passenger about the sign, and (3) search for extra information by means of their vehicle's radio or internet.
4. Females, black individuals, subjects with a disability, older, and those with high trust in DMS are less likely to ignore the fabricated messages. In contrary, white, those who drive long hours, and those who see driving as a tedious task are more likely to ignore the bogus messages. Drivers who comply with traffic regulations and have a good driving record are likely to slow down under the tampered messages. Furthermore, female drivers and those who live in rural areas are more likely to slow down under fabricated advisory information. Furthermore, this dissertation identifies that planning for alternative route and involvement in distractive activities cause speed variation behaviors under the compromised DMS.

This dissertation is the first to investigate the adverse impact of a compromised DMS on the road users and operators. I attempt to address the current gap in the literature by assessing and evaluating the impact of ITS security vulnerabilities. Broader impacts of this study include (1) to systematically raising awareness among policy-makers and engineers, (2) motivating further simulations and real-world experiments to investigate this matter further, (3) to systematically assessing the adverse impact of a security breach on transportation reliability and safety, and drivers' behavior, and (4) providing insights for system operators and decision-makers to prioritize the risk of a compromised DMS. Additionally, the outcome can be integrated with the nationwide connected vehicle and V2X implementations and security design.

A Risk Based Approach to Intelligent Transportation Systems Security

Kaveh Bakhsh Kelarestaghi

ABSTRACT (General Audience)

Security threats are targeting institutions and infrastructure around the world, and the frequency and severity of security attacks are on the rise. Healthcare manufacturing, financial services, education, government, and transportation are among the industries that are the most lucrative targets for adversaries. Hacking is not just about companies, organizations, or banks; it also includes critical infrastructure. Intelligent Transportation Systems have been deployed with a focus on increasing efficiency and safety in the face of dramatic increases in traffic volume. Although many studies have been performed and many security primitives have been proposed, there are significant concerns about flawless performance in a dynamic environment. A holistic security approach, in which all infrastructure performs within the satisfactory level of security remains undiscovered. Previously, hacking of road infrastructure was a rare event, however, in recent years, field devices, such as dynamic message signs, are hacked with higher frequency. The primary reason that transportation assets are vulnerable to cyber-attacks is that of their location in public. A more dramatic scenario occurs when hackers attempt to convey tampered instructions to the public. Analyzing traveler behavior in response to the hacked messages sign on the basis of empirical data is a vital step toward operating a secure and reliable transportation system. This study is the first to investigate the adversarial impact of a compromised message sign on the road users and operators. I attempt to address the current gap in the literature by assessing and evaluating the impact of ITS security vulnerabilities.

Dedication

*I dedicate my work to my love, **Mona**, for her kindness, laughter, continues support, and devotion. Thanks for always being there for me.*

Acknowledgments

There are a number of people without whom this dissertation might not have been accomplished, and to whom I am greatly grateful.

My love, Mona. I would like to thank you for being there when I needed you the most. Without you achieving this dream would be impossible. I am a better person because of you. Thank you.

A special thanks to my parents, Soraya and Kioomars, my brothers, Kamran and Keivan, and my family, Simin and Kamran, that supported me through the course of my life. Also, I would like to thank my dearest friends, Aref, Farhad, and Ida, for standing with me in my hardest moments.

My sincerest appreciation goes to Dr. Kevin Heaslip, my advisor, for his outstanding support. You believed in me and helped my dreams come true. You offered me opportunities that helped me boost my skills. You changed my life. I can't thank you enough.

Dr. Alireza Ermagun. A unique friend, and a great collaborator. Thank you for helping me dream big.

Dr. Mansoureh Jeihani. Thank you for supporting me in tough days. I am in debt of your kindness and support.

Dr. Kenneth Wong. Thank you for standing by my side when I needed support.

In addition, I'm thankful for my committee members, Dr. Kathleen Hancock, Dr. Ralph Buehler, and Dr. Ryan Gerdes. Your input improved this work. I also would like to thank Dr. Ronald Fricker for his help and input in my research.

I would also like to thank Deloitte for their generous support in funding my research.

Contents

List of Figures

List of Tables

Chapter 1

1 Introduction

DMS are electronic traffic signs that have been used widely across the United States to convey traffic-related information to road users. These en-route messages might include information related to traffic congestion, road closures, accidents, travel time, amber alerts, work zone areas, and speed limit information. Among early deployments, DMS were employed in 1950s in New Jersey Turnpike to warn drivers to reduce their speed [1]. In the beginning stages, DMS were static signs included with words that would be illuminated depending on the situation. For instants, word *construction* would be illuminated to inform drivers of a work zone area. Later these signs substituted by dot-matrix displays that were capable of displaying a more verity of words. With the progression of technology DMS now use LED displays that are capable of displaying pictograms and colored texts. The programming of the early DMS was possible only when an operator was present physically, while by the progression of the technology this task made possible via wired, wireless, or cellular communication.

Current literature has extensively investigated road users' response and behavior to traffic information displayed by DMS. These studies mainly explored the effectiveness of DMS by assessing four different drivers' behavior. These behaviors include route diversion [2, 3, 4, 5], route choice [6, 7, 8, 9], speed change [10, 11], and lane changing behavior [11]. Evidence indicate that DMS were successful in influencing drivers' behavior in order to increase transportation safety and efficiency. Wang et al., [12] compared different speed control strategies in roadwork zones and found that DMS would decrease the speed of the approaching vehicles in order to maintain the safety of the construction team as well as road users themselves. Similar results found in Garber and Patel [13] study where the impact of DMS was tested by displaying various safety messages. The results of a revealed preferences study confirmed a significant speed reduction behavior for speeding drivers [13]. DMS also were found effective in drivers route choice and route diversion behavior. The main goal for system operators is to increase drivers' compliance with advisory information that are displayed on a DMS. To this extent, many researchers have attended to investigate factors that are contributing to drivers' higher compliance rate. These factors include drivers' socio-economic and attitudinal information, trip characteristics, and message content characteristics. For instance, drivers with higher trust to the DMS, who are traveling to work, and those who have limited driving experience are more likely to comply with advisory information [14, 15, 16, 9, 17, 18, 19, 20, 21]. That is, these drivers are more likely to divert to other routes or to choose routes that are suggested by the DMS.

Despite numerous benefits, DMS might impose negative impacts on the transportation network. Drivers are likely to become distracted if encountering wordy, unfamiliar, and complex messages. These messages could cause conflicting attention demands between acquiring task and driving task and compromise drivers' safety [22, 23]. DMS convey advisory information to drivers but concurrently could distract drivers from driving task. The distraction might ensue, since advanced technology could be distracting for some drivers, or because drivers need to read, comprehend and react based upon the message which can be a distracting process. In addition, attention to the DMS could cause irregular speed reduction behavior that might compromise transportation safety [22, 24]. Even more catastrophic consequences could strike if an adversary fabricates the DMS message content. A compromised DMS not only undermines the reliability of

the ITS system but also biases drivers' decisions by coaxing them with forged information. A malicious adversary could purposely shunt drivers to other routes. That is different forged message could trigger different consequences with different impact levels.

Analyzing traveler behavior in response to the hacked messages sign is a vital step toward operating a secure and reliable transportation system. For the purpose of the proposed study we aim to scrutinize the impact of a compromised DMS on the transportation network. Cyber-physical attacks on the ITS infrastructures are expected to levy risks to the transportation system [25]. Indications of the preceding remote and physical security attacks on DMS are sufficient to evince this fact. Various threat events around the nation illustrated that forging the content of a DMS could harmfully influence system efficient operation and drivers' behavior [26, 27, 28, 30]. In our previous study [25] we conducted an impact assessment by undertaking a risk-based approach to perform a qualitative vulnerability-oriented threat analysis with aim at identifying issues that are caused by physical or cyber-attacks that are exploiting DMS security vulnerabilities. The results indicated that safety and behavioral adverse impacts are associated with the high-risk cluster, while operational, security and system efficiency concerns are associated with medium-risk cluster [25]. Herein, the proposed study takes into consideration the previous results and conducts a stated preference analysis to investigate the impacts of a compromised DMS on drivers' compliance and route choice behavior.

1.1 Research question

Intelligent transportation system expected to enhance transportation safety, efficiency, and to provide solution for the adverse environmental impacts of the system, but in the presence of security vulnerabilities the ITS's benefits could dim. In the presence of any vulnerabilities, adversaries might exploit DMS availability, and integrity security goals. Exploiting DMS' vulnerabilities could harm transportation network that is many questions need to be resolved for better security incident response management. That is, system operators and traffic engineers better mitigate the risks of a compromised message sign. For instance:

i. What are the consequences of cyber-physical attacks on transportation?
ii. Would an adversary be able to manipulate road users' decisions by compromising a DMS functionality?
iii. Would an adversary be able to cause safety hazards by compromising a DMS functionality?
iv. What types of forged message content have the most adverse impact?
v. Could a bogus DMS message cause driver inattention?
vi. Could an adversary perpetrate an attack to coax driver's decision to shunt them from certain routes?
vii. Could an adversary engineer traffic speed choice behavior?

Security is a fundamental prerequisite of the intelligent transportation system that if not properly preserved, would adversely impact drivers and system operators. Lessons learned from the current literature portray that drivers' safety, security, and privacy would be compromised due to ITS security vulnerabilities. Malicious adversaries not only might distract drivers but might sway road users' decision in order to, for instance, divert traffic.

1.2 Research problem and general approach

This study conducts an impact-oriented assessment with aims at identifying issues that are caused by adversaries exploiting DMS security vulnerabilities. To this extend we perform both qualitative and quantitative impact-oriented risk assessments to (1) identify adverse impacts that are caused by a malicious adversary exploiting DMS security vulnerabilities, (2) assess drivers' route divergence behavior to the compromised DMS, (3) investigate distracted driving behavior that is caused due to the fabricated messages displayed by a DMS, and (4) investigating traffic speed variation at the presence of a fabricated information.

As far as the qualitative assessment is concerned, we employed the National Institute of Standard and Technology (NIST) risk-based approach to carry a qualitative vulnerability-oriented risk assessment. The qualitative risk-based approach of this dissertation intends to classify adverse impacts that are caused by malicious adversaries exploiting DMS security vulnerabilities. This dissertation provides a rating of the adverse impacts probability through a qualitative risk-based approach for measuring risks and communicating the results for policy consideration. In this study, we synthesize current literature and real-world DMS hacking incidents to determine potential impacts of exploiting ITS security vulnerabilities. We then map safety, operation, reliability, and security issues ensued by DMS hacking incidents into a visual, matrix for risk prioritization purposes.

A rigorous data-driven analysis could be conducted, but this is a difficult task because to this date statistical data (i.e., revealed or stated preference data) is mainly unknown. As DMS security risk analysis in the field of ITS is active research with lacking data of the perpetrated attacks, a comprehensive quantitative risk assessment methodology cannot be conducted. That is, in this dissertation we conduct a stated preference approach to collect road users' perception toward a compromised DMS. In order to examine factors contributing to (1) road users compliance behavior, and (2) distracted driving when drivers encountering fabricated information at a compromised DMS, this study undertakes a stated preference approach. We randomly selected about 4,700 participants from States that experienced the DMS hacking incidents. According to the surveyed threat events occurred around the nation [25].

1.3 Major research theories

The main motivation behind this research is that driver behavior changes as an adversary compromises the functionality of a DMS. We argue that a fabricated message displayed on a hacked DMS could directly/indirectly influence drivers' behavior and causes conflicting attention demands between the acquiring task and driving task. By exploiting DMS security vulnerabilities an adversary could coax drivers to change their route or destination in order to gain benefit from that behavioral change. In addition, an adversary could lure drivers to pay attention to tasks other than driving. These tasks might include using cellphone to call someone, adjusting radio, and talking to a passenger. The current literature have not yet focused on the issues that are likely to ensue due to security vulnerabilities of the message sings. The goal of this Dissertation is to test the following hypotheses:

1. A compromised DMS would adversely impact drivers' behavior.

2. Driving at the presence of a compromised DMS would cause speed variation, unplanned route divergence behavior, and distracted driving.
3. Under various scenarios, speed variation, route divergence, and distracted driving behaviors would be different.
4. The speed variation, route divergence, and distracted driving behaviors would be different across the subjects.
5. Drivers' attitude toward compromised DMS would differ across various bogus content.

There is a gap in the current literature to appraise the consequences of cyber-physical attacks on the transportation system. This dissertation attempts to scrutinize the impacts of DMS security vulnerabilities and adds to the literature of ITS security, by examining conceivable consequences of an adversary compromising a message sign. To this extent, we aim to contribute to the nascent but growing literature of ITS security impact-oriented risk assessment. This dissertation is devoted to identifying security attacks against DMS, to propose defense and protection security mechanisms, identify the impacts of a DMS hacking event from both quantitative and qualitative points of view. The understanding of possible security attacks and the performance of the security mechanisms is still rudimentary. This deficit urges the need for a data driven impact-oriented assessment to detect system-level threats. The research in this dissertation is a continuation of Kelarestaghi et al., [25] study (Chapter 2) which employed the NIST risk model to perform impact-oriented risk assessment for the case of a compromised message sign. The Chapter 3, 4, and 5 of this dissertation take into account the results of the Kelarestaghi et al., [25] study (Chapter 2) and conduct a quantitative impact assessment to uncover issues concerning drivers' behavior encountering a fabricated information displayed by a hacked messages sign.

1.4 Research contributions

This dissertation is the first attempt to systematically evaluate the risks of a compromised DMS in the field of transportation. We challenge this problem and contribute to the current literature of ITS security and resiliency in four papers. In which the first paper has been published and the other three will be submitted to the top-tier journals. In this section, a summary of all papers is provided. The remaining chapters discuss the contribution and outcome of each paper in more details.

1.4.1 Intelligent transportation system security: hacked message signs

"It cannot happen to us" is one of many common myths regarding cybersecurity in the transportation industry. The traditional view that the threats to transportation are low probability and low impact keep agencies from mitigating security threats to transportation critical infrastructure. Current transportation systems depend on closed proprietary systems, which are enhanced by connected cyber-physical systems. A DMS deliver advisory information to road users to ensure safe and efficient trips. Since the first DMS physical hacking more than a decade ago, the importance of DMS security has been a pressing one. DMS hacks can include physical and remote breaches due to the weak protection of the signs and cyber-physical systems. In 2014, multiple cyber-attacks on signs by "Sun Hacker" pushed the Department of Homeland Security (DHS), which includes the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the Federal Highway Administration (FHWA) to investigate breaches more seriously.

It is known that hackers breach cyber systems daily, but white hat hackers have given transportation officials information to help them rethink ITS infrastructure security gaps to prevent harm to road users and financial losses. This study employs a risk-based approach to conducting a threat assessment. This threat assessment performs a qualitative vulnerability-oriented threat analysis. The objective is to investigate safety, security, reliability, and operation issues that are triggered by compromised DMS. Additionally, countermeasures are proposed to prevent the failure of critical infrastructure. The outcome is anticipated to be of special interest and usefulness to policymakers and engineers concerned with the potential vulnerabilities of the ITS's infrastructure.

1.4.2 Cyber-physical attack on DMS and its impact on drivers' route divergence behavior

In this chapter, we explore drivers attitudes toward a compromised DMS in order to understand their route departure behavior. Recently DMS have been hacked with higher occurrence in the US with uncommon en-route information to convey amusing, funny, and offensive message. In this study, we argue that an adversary is able to display fabricated-realistic traffic related information on DMS to coax drivers' decisions. We conducted stated preference research to assess about 4,700 subject's behavior under such forged information. To this extent, we developed latent based ordered probit regression models to scrutinize driver's behavior as far as the route divergence behaviors are concerned. The results of this study support the original hypothesis and indicate that in compliance with the fabricated-realistic message drivers will change their planned route in response to the compromised DMS. The findings pinpoint that female, experienced drivers, subjects familiar with the DMS, and tech-friendly drivers are more likely to comply with the forged information. While white, subjects in rural areas and those who have prior knowledge of DMS hacking phenomena are more likely to ignore the advisory information. The outcome of this study can be a guide to policymakers concerned with developing incident response plans and preparedness plan to mitigate risks that are associated with the security vulnerabilities of intelligent transportation systems infrastructure.

1.4.3 Does DMS bogus content cause distracted driving?

In the real-world DMS hacking events, the fabricated messages rendered funny, offensive, and political information. In this study, we focus on scenarios in reference to the previous threat events to form a set of creative forged messages to assess drivers' decision. In addition, we take a step forward and examine drivers' distraction behavior under a fabricated realistic message as well. This approach helps us to not only compare different messages impact on subjects' behavior but to understand what will happen if an adversary displays bogus realistic messages rather common funny/offensive context. This dissertation is the first study to assess the impact of a compromised DMS with realistic and fictitious related content on travelers' distraction behavior. The main objective of this study is to understand to what extent the drivers are receptive to the fabricated DMS content, and how the fabricated messages adversely impact the drivers' behavior. To test if a cyber-physical attack on DMS would cause drivers' distraction we developed Structural Equation Modeling (SEM) to examine the association between distraction and drivers' objective and subjective attributes. The outcome of this research would be of special help to policymakers,

emergency responders, and engineers who are concerned with developing incident response plans and the safety, security, and resiliency of the ITS network.

1.4.4 Choice of speed under A compromised dynamic messages sign

En-route advisory information supposed to facilitate road users with safe and efficient travel. In this study, for the first time, we argue that not only DMS would not be lucrative to road users but would detriment the safety and operation of the transportation system. An adversary could compromise the security vulnerabilities of a DMS and display his/her desirable message to the drivers. Depends on the message the behavior of the road users could differ. This study investigates travelers' speed choice behavior under realistic and fictitious fabricated DMS content. The statistical models consider about 4,700 subjects' characteristics information and stated speed choice behavior. The results affirm traffic speed variation behavior at the presence of a compromised DMS. We further identify route change behavior and involvement in distraction activities as significant factors to contribute to the subjects' choice of speed. Also, we identify females, reckless and anxious drivers, highly educated subjects and tech-friendly drivers among the individuals that comply with false information.

The remainder of this dissertation is structured as follows. In the second chapter we explore the adverse impacts of a compromised DMS by conducting a qualitative risk-based approach. In the third chapter we investigate whether an adversary could shunt divers from their planned route. We study route divergence behavior of the drivers under four different scenarios. In the fourth chapter, we discuss distracted driving, and determinants of distractive activities while road users encountering an advisory information displayed on a DMS. In the fifth chapter of this dissertation, we explore drivers' speed choice behavior under a compromised DMS. We conclude the dissertation in the Chapter 6.

Chapter 2

2 Intelligent Transportation System Security: Hacked Message Signs

Abstract

"It cannot happen to us" is one of many common myths regarding cybersecurity in the transportation industry. The traditional view that the threats to transportation are low probability and low impact keep agencies from mitigating security threats to transportation critical infrastructure. Current transportation systems depend on closed proprietary systems, which are enhanced by connected cyber-physical systems. A DMS deliver advisory information to road users to ensure safe and efficient trips. Since the first DMS physical hacking more than a decade ago, the importance of DMS security has been a pressing one. DMS hacks can include physical and remote breaches due to the weak protection of the signs and cyber-physical systems. In 2014, multiple cyber-attacks on signs by "Sun Hacker" pushed the Department of Homeland Security (DHS), which includes the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the Federal Highway Administration (FHWA) to investigate breaches more seriously. It is known that hackers breach cyber systems daily, but white hat hackers have given transportation officials information to help them rethink ITS infrastructure security gaps to prevent harm to road users and financial losses. This chapter employs a risk-based approach to conducting a threat assessment. This threat assessment performs a qualitative vulnerability-oriented threat analysis. The objective is to investigate safety, security, reliability, and operation issues that are triggered by compromised DMS. Additionally, countermeasures are proposed to prevent the failure of critical infrastructure. The outcome is anticipated to be of special interest and usefulness to policymakers and engineers concerned with the potential vulnerabilities of the ITS's infrastructure.

2.1 Introduction

Attacks to cyber-physical systems have targeted institutions and infrastructure around the world, and the frequency and severity of attacks are on the rise [31, 32, 33, 34]. Healthcare manufacturing, financial services, education, government, and transportation are among the industries that are the most lucrative targets for adversaries [35, 36, 37]. Hacking is not just about companies, organizations, or banks; it also includes transportation critical infrastructure. Wireless Sensor Networks (WSN), V2X, DMS and Traffic Signal Controllers (TSC) are among major ITS infrastructure that has already been attacked or remain vulnerable to hacking.

ITS has been deployed with a focus on increasing efficiency and safety in the face of dramatic increases in travel demand [38]. Any threat to ITS functionality compromises the system at many levels, including regionally, nationally, and internationally [39]. Although many studies have been performed and many security primitives have been proposed, there are significant concerns about maintaining a flawless performance in a dynamic environment. A holistic security approach [39], in which all infrastructure performs within a satisfactory level of security, remains undiscovered.

Previously, hacking of road infrastructure was a rare event; however, in recent years, field

devices, such as DMS, are hacked with higher frequency [40]. The primary reason that transportation assets are vulnerable to cyber-attacks is their location in the transportation network. Dramatic scenarios occur when hackers attempt to convey tampered messages to the road users [40]. Conceivable future attacks using wireless communication could lead to more sophisticated cyber-attacks, similar to the case of WSN, in which the hacker exemplified a passive attack to compromise a traffic signal by accessing a WSN [41]. There is room for improvement by policymakers and roadway operators when considering critical infrastructure vulnerabilities. With cybersecurity issues escalating every day, road users' safety has been neglected [42]. Although manufacturers have attempted minimal protection (i.e., isolation, hard-coded password), pranksters have been able to successfully manipulate critical infrastructure (e.g., DMS, TSC, Vehicles, WSN).

This chapter attempts to examine the impacts of DMS security vulnerabilities, and contributes to the literature of ITS security and resiliency, by exploring possible consequences of an adversary hacking a DMS. To this aim, we synthesize the current literature and real-world DMS hacking events' evidence that has been described in the current literature and news reports, to pinpoint possible impacts that those attacks can impose on the transportation network.

Additionally, this study undertakes a risk-based approach to perform a qualitative vulnerability-oriented threat analysis with aims at identifying issues that are caused by adversaries exploiting ITS security vulnerabilities. We will present a literature review of the importance and effectiveness of DMS in the ITS network, followed by identifying threat sources and surveying threat events which have occurred around the nation; we then explore safety, operation and security issues ensued by DMS hacking incidents; finally, we suggest countermeasures to prevent the failure of ITS critical infrastructure.

2.2 DMS importance in ITS network

DMS or Changeable Message Signs (CMS), also known as Dynamic Message Signs (DMS), have been used for more than 50 years in the United States [43]. Advanced Traveler Information Systems (ATIS), such as DMS, offer real time information to enhance drivers' route choice by giving information on road traffic conditions, avoiding congestion, selecting better departure times, and increasing network performance by prescribing diversion decisions to motorists [2].

In contrast to traditional speed regulatory signs that have minimal influence on drivers' speed in work zone areas, implementation of DMS caused significant reduction in vehicle speed [13]. Further analysis revealed changes in DMS's efficiency corresponding to message content [13]. Another study [12] comparing different speed control strategies in work zone areas indicated that DMS could significantly reduce the speed of an oncoming vehicle and increase safety for construction crews as well as drivers themselves, thus maximum efficiency is achieved by locating DMS in highly visible areas [44].

Route choice, speed changes, and braking behavior have been investigated for drivers in which road closure information has been provided through DMS. The analysis indicated a dramatic reduction in speed, and almost all drivers avoided the closed road section [10]. Likewise, the investigation specified that message content and location of the accidents displayed on the DMS are important factors about drivers' diversion behaviors [45]. Peeta et al. investigated the relation

of DMS message type and drivers' behavior. The results showed that the influence of the message content has a strong correlation with system performance [2].

Conventionally, real-time communication between DMS and Traffic Management Centers (TMC) is conducted by voice-grade telephone lines, either wire-based or cellular, including fiber optic cable and copper twisted pair cable [46]. The recent emergence of technology sought traffic engineers to deploy advanced communication equipment. Kosch et al. proposed DMS as part of Roadside Equipment (RSE) and should be equipped with communication hardware [47]. The DMS using the connection to the ITS integrated network and the Internet, offers to relay information to passing vehicles.

The credibility of DMS is extremely important to achieving efficient operations. Drivers eventually will not pay attention to messages they distrust [43]. DMS that have been tampered with provide unsanctioned information, which distracts motorists and affects the credibility of the system. Recent DMS targeted by hackers were mainly carried out by physical attacks and were perpetrated for the attackers' amusement.

2.3 Methodology of risk assessment

The risk assessment approach comprises basic steps common to National Institute of Standard and Technology (NIST) Special Publication 800-30 publication [48]. Implementing NIST SP 800-30 provides a guide for conducting an organizational risk assessment. The risk assessment process take-a-ways will be a key constituent of a risk management process [49]. The risk-based approach employs NIST SP 800-30 risk model to conduct a risk assessment to perform qualitative vulnerability-oriented threat analysis. To conduct the vulnerability-oriented risk assessment, this study (1) identifies exploitable security gaps of the system, (2) identifies threat events that could exercise those security gaps, and (3) seeks impacts or consequences of a DMS hacking incident.

The methodology of risk assessment (Figure 1) comprises of (1) identification of threat sources and event, (2) identification of the system vulnerabilities and predisposing conditions, and (3) determination of the adverse impacts and magnitude of impact. To this aim, physical and cyber-attacks will be represented in a tree structure [50] (i.e., attack tree), with the goal of tampering DMS content and different ways of achieving that goal. The attack tree, proposed by Schneier [50], specifies a range of actions that an adversary undertakes to exploit the vulnerabilities of the DMS. Representing the attack in a tree structure provides a better understanding of all different ways that an adversary can compromise the system.

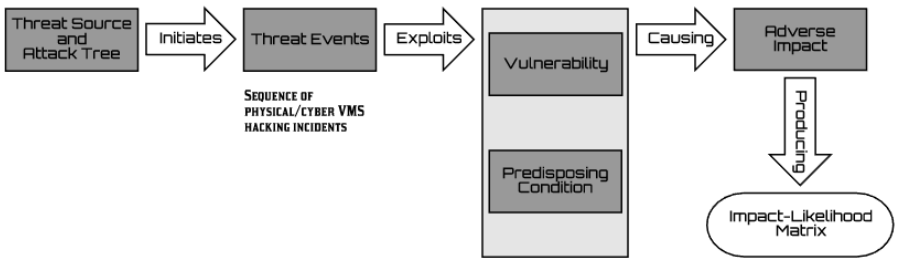


Figure 1 Methodology of risk assessment (adapted from NIST SP 800-30 [20])

Following the threat source and attack tree, threat events will be identified through a comprehensive survey of the DMS hacking incidents occurred throughout the United States. Threat events then will be accompanied by the identification of system vulnerabilities and predisposing conditions, and determination of impacts of those vulnerabilities being exploited.

2.4 Threat source and attack tree

An outsider adversary can compromise DMS functionality through physical and cyber-attacks. In a physical attack, an adversary with limited resources and expertise gains physical access to the portable DMS cabinet by either breaking the lock or using a key, which the attacker may purchase online. Subsequently, by entering the default usernames and passwords, the attacker can override a DMS message [51, 52, 53]. In the case of cyber-attack, an outsider adversary with moderate resources and expertise alters DMS' content with no need for physical access. This attack can be initiated by gaining remote access through the Telnet port 23 or the Simple Network Management Protocol (SNMP) [26, 27]. Then the attacker needs to brute force the password (e.g., guessing a default password or using a password breaker tool) and alter the DMS message. To alter the DMS content remotely, the adversary can employ LCD simulator software. A high-level graphical representation (i.e., attack tree) and term-based syntax for both the physical (Figure 2.A) and cyber-attacks (Figure 2.B) are presented to understand the risk potential systematically. The following section surveys DMS hacking events.

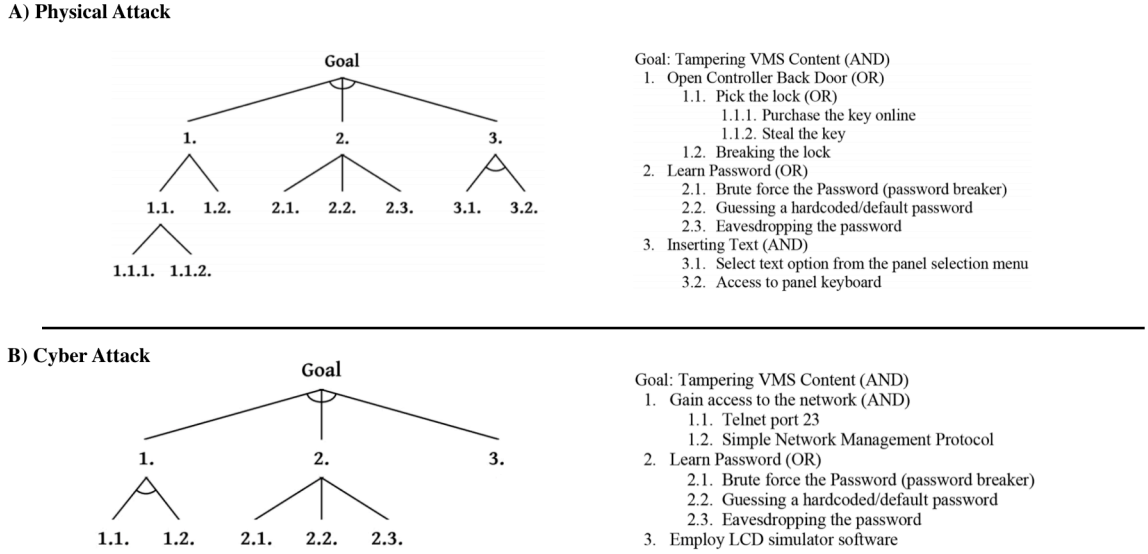


Figure 2 Physical (A) and cyber attack trees

2.5 Threat events and system vulnerabilities

2.5.1 Physical-attacks

One of the early incidents of DMS hacking took place in Boston, Massachusetts in April 2007. MIT students tampered the message to read, "This sign has been hack[e]d" (Figure 3) [54]. Although the intention was not malicious, and no one was hurt, authorities considered it as a future potential threat [55].

In February 2009, hackers tampered with the messages on two portable DMS [55]. It was more about entertainment than the actual message. It was not difficult to gain access to a portable DMS. The control unit uses a simple password and user interface protection, making it easy to hack. A hacker could easily gain the knowledge to gain access from the internet [51, 52, 53] . Also, the portable DMS cabinet can be unlocked effortlessly [55] because the keys are available for purchase. A similar event happened in January 2009, when another DMS was broken into and manipulated to display the message "Zombies Ahead." Officials declared that it was the first time that one of these signs was hacked [56, 57].

In January 2009, hackers were able to tamper with the DMS in Collinsville, Illinois during the morning peak period [58, 59]. A legitimate warning message was altered to read, "Daily Lane Closures Due to Zombies." Such behavior alerted authorities to the drawbacks of ITS's infrastructure security. This deficit in security should be noted and worked on by traffic safety engineers and transportation officials [58]. In February 2009, drivers in Indianapolis, Indiana dealt with a hacked road sign displaying similar language. The sign stated, "Raptors Ahead Caution." Although one of the drivers claimed that he did not pay attention to the sign, another was excited about the content but was skeptical regarding the truth of the message [60].

In 2009, several hacks happened in New York, where three DMS were hacked in one day [61]. The signs should have warned drivers to decrease their speed due to construction activities ahead of them. However, because of their messages (e.g. "PARTY AT JULIE'S"), drivers did not pay attention to the signs, which could have resulted in hazardous consequences for drivers and pedestrians [61]. It is worth noting if the attacks were performed on a weekday instead of the weekend the results might have been different.

Figure 3 Hacked road sign in Boston, MA (courtesy of C. Pentacoff) [54]

In December 2009, during the morning rush hour in Gainesville, Florida, two signs were hacked using a similar message. Before this occurrence, the University of Florida website displayed information regarding a Zombie awareness plan as a joke [62]. The sign was tampered

with to read “Zombie Attack! Evacuate”. Some drivers presumed the sign might be authentic [63]. The Florida Department of Transportation (FDOT) believed that the hack could have been perpetrated using a telephone or by actual physical involvement. The following year, Miami-Dade County in the Florida suffered a hacking incident, where the sign message should have warned drivers of a road closure on Northwest 25th Street [64] but instead displayed an offensive message.

In October 2012, Portland, Maine experienced a tampered message board that worried drivers with the message “Zombies Ahead” instead of “Nightwork 8pm-6am” [65]. A similar event took place in November 2012 in Loomis, California where a message board displayed “Caution Loose Gorilla” [66]. In February 2014, a message board in a work zone area was hacked in California. The construction company was forced to shut down the sign until they could reprogram it. Such behavior is not just offensive; it can put construction crews’ and drivers’ lives in danger [67].

In September 2015, another occurrence happened in Mililani, Hawaii where a DMS was hacked with an offensive message that created confusion for drivers. An investigation revealed that hacking such infrastructure is not complicated since security countermeasures are not sophisticated enough to prevent such malicious behaviors [68]. In October 2015, a DMS in Sacramento, California was hacked by a physical-attack that involved breaking into the DMS cabinet and tampering with the computer [30].

Principally, hacking DMS generates two main problems. First, drivers can get distracted which can lead to a crash. Second, drivers do not see the message that they are supposed to read. Missing traffic information may cause severe consequences not just to drivers but also to construction crews at work. Table 1 provides a survey of hacking cases (sorted by date) across the US. Beyond the cases provided in Table 1, additional DMS hacking events can be found in [69].

Although many people consider hacking message boards a rare occurrence, the difficulties and issues are serious, and the hacking itself is not particularly complicated. Instructions are accessible to anyone who wants to behave maliciously [51, 52, 53] . Watch Dogs (released on May 2014), a home console video game, also teaches gamers how to hack critical infrastructure [26]. Watch Dogs pinpoints security vulnerabilities and allow a player (hacker) to outwit smart cities’ operating systems (e.g., security cameras, power grids and traffic lights) for the hacker’s gain [28]. All the scenarios above are conducted by “Threat Agents: Group One”; individuals that breached the signs aim for “fun or notoriety” [70]. These individuals use their technical knowledge to manipulate and breach systems such as DMS [71].

2.5.2 Cyber-attack: “Sun Hacker”

Vulnerabilities of cyber systems need to be identified, reduced, mitigated, and eliminated throughout the entire supply chain, to ensure the physical security of assets [42]. Protection must be addressed throughout entire system lifespan. Most of the cases reported in Table 1 were physical hacks. However, in Asheville, NC, someone using the pseudonym “Sun Hacker” claimed responsibility for the tampering (Figure 4). Five overhead DMS were hacked in North Carolina in the Ashville, Winston-Salem, and Mount Airy areas on Friday, May 30, 2014 [26, 27, 28]. During the same period, from May 27 to June 2, DMS in three other states (New Jersey, Iowa, and Wyoming) were also hacked by the same entity [26]. The hacked DMS were operated using a web-based interface, which allowed the hacker was able to access them remotely. The hacker stated in his twitter account that he used Telnet Port 23 and a password breaker to breach the signs –there

is evidence suggesting video game "Watch Dogs" was a direct inspiration for "Sun Hacker" [26, 72].

The hacker [73] claimed that the tampering was accomplished by accessing the Virtual Private Network (VPN) of the DMS [74]. The Department of Homeland Security (DHS), based on communication with DMS manufacturer, stated that the password was not hard-coded [27, 75]. Subsequently, the Federal Highway Administration (FHWA) provided guidelines to prevent such an incident. Several recommendations concerned with weak device's password, the accessibility of the IP addresses, and privacy of the network and web pages [76].

Although some states used precautions such as Friend List (New Hampshire), VPN Tunnel (New Hampshire, Nevada), Firewalls (Nevada), Message Validation and Authentication (Maryland), the consistencies of these strategies should be tested and validated to ensure that they are robust enough to secure the network from cyber-attacks.

Interestingly, similar tampering could have more benefits than drawbacks. Instead of hardening systems against attacks by hackers with mischievous intention – so-called black hats –, authorities could encourage white hat hackers – people with non-destructive motives – to try to break into these systems. Hackers breach cyber systems daily, but concurrently they could bounce hints to authorities to rethink ITS's infrastructure security gaps to prevent any harm to road users and financial losses. Subsequently exercising white hat hackers' knowledge to identify network vulnerabilities would be essential.

Figure 4 DMS hacked by "Sun Hacker" in Ashville, NC (courtesy of WNCN) [26]

2.6 Discussion

Although most of the reported hacking events range from amusing to mildly offensive, these are cases that compromise road safety. DMS provide necessary information to drivers regarding traffic conditions and the road ahead of them. Such information might be related to road conditions and

closures, construction zones, accidents, and detours, among other things. Losing or neglecting such information could lead to a disaster. The hacking which happened in Austin (February 2009) [55], was close to a high-density trafficked boulevard. Although no incidents were reported for that particular message, potential impacts that DMS hacking might impose on driver's behavior need to be investigated. It is noteworthy that many studies presented results demonstrating the significant correlation between the content of the DMS message and driver behavior [2, 10, 12, 13, 45, 77].

Hacked DMS were investigated with regards to the impact on vehicles' location in a roadway and the function of their travels. Olofsson [78] defined DMS hacking as "a means of combating the disciplinary regimes of roadways" that can destabilize the correlation between vehicles' location in the roadway, possible events ahead of their trip, their destination, and ultimately jeopardize the institutionalized function of the travel. Such an example can be seen in the Austin case (June 2010), when drivers looked twice when confronting the sign reading, "NAZI ZOMBIES AHEAD!" on a DMS. Some slowed down, and some even took pictures [79]. This reaction is concerning because driver distraction can cause an increase in the risk of a crash, carbon emissions, energy consumption. Security threats on DMS are inevitable, yet we cannot say for sure what consequences such an attack can impose. Although researchers have attended to the security aspect of the ITS, unfortunately very little attention has been dedicated to assessing the impact of security breaches on the transportation network, more specifically on the system's operators and users.

The threat events listed in Table 1 indicate that most of the DMS were seeking to promote awareness regarding an upcoming construction zone. DMS not only provide information regarding slower speed in work zones, but they are also able to enhance safety, especially related to rear-end accidents, by displaying real-time information of a queue-end location to alert drivers of upcoming slow-moving or stopped traffic [80]. Information provided by DMS in work zones should warn drivers to take necessary precautionary actions. Such situations can be even more complicated when dealing with different types of vehicles and emphasize the importance of functioning DMS [81].

Queue propagation speed, geometric conditions, and the familiarity of drivers are important factors correlated with an accident's intensity. Lack of real-time information makes drivers more vulnerable to unforeseen traffic conditions [81]. One of the consequences of an information deficit is rear-ended crashes. A naturalistic driving study comprised of 100 cars found that almost 78% of total crashes and 65% of near-crashes were related to driver inattention [82]. Out of all rear-end crashes, 87% involved driver distraction [83]. In 2012, more than 1.7 million rear-end crashes that caused more than 1,700 fatalities were reported in the U.S. [84]. In addition to driver distraction, the unpreparedness of drivers to decrease speed in work zones were identified as another cause of rear-end crashes [84].

Implementation of Automated Work Zone Information Systems (AWIS) is reported to be a reliable and effective way to enhance work zone safety [85, 86]. However, the comparison of AWIS information and the field observation revealed that, in situations where information is not accurate, drivers become confused and some behave based on their judgment and experience [87]. The discrepancy between provided information and the actual condition results in drivers performing evasive behaviors in work zones that increase the likelihood of a crash [88].

Table 1 Summary of known hacking events in the U.S.

Date	Location	Warning Message	Type of Tampered Message	Short term Consequence	Reference
Cyber Attack					
May-Jun. 2014	Asheville, NC Winston-Salem, NC Mount Airy, NC State of New Jersey State of Iowa State of Wyoming	Traffic Information	Amusing /Fame	Driver distracted and confused	[26, 27, 28]
Physical Attack					
Oct. 2015	Sacramento, CA	Work Zone Ahead	Amusing/Offensive	Driver distracted	[30]
Sept. 2015	Mililani, HI	Work Zone Ahead	Offensive	Driver confusion	[68]
Jul. 2015	Tucson, AZ	Road Closure	Amusing	Driver double-take	[89]
Jan. 2015	Los Angeles, CA	Work Zone Ahead	Amusing /Offensive	Drivers distracted	[90, 91, 92, 93]
Feb. 2014	Granite Bay, CA	Work Zone Ahead	Offensive	Driver distracted	[67]
Nov. 2012	Loomis, CA	Road Closure	Amusing	Driver distracted	[66]
Oct. 2012	Portland, ME	Work Zone Ahead	Amusing	Driver worried and distracted	[65]
Aug. 2011	Flagstaff, AZ	Traffic Information – No left turn at intersection	Amusing	Driver confusion	[94, 95]
May 2011	Falls Church, VA	Warning Message for bicyclist and hikers	Amusing	Driver distracted	[29]
May 2010	Miami, FL	Work Zone Ahead	Offensive	Driver distracted	[64, 96]
Dec. 2009	Gainesville, FL	Work Zone Ahead	Amusing	Driver distracted	[63]
Mar. 2009	New York, NY	Work Zone Ahead	Amusing	Driver distracted	[61]
Feb. 2009	Hamilton County, IN	Work Zone Ahead	Amusing	Driver confusion	[60]
Feb. 2009	Collinsville, IL	Work Zone Ahead	Amusing	Driver distracted	[59]
Feb. 2009	Austin, TX	Work Zone Ahead	Amusing	Destabilized traffic norm	[55]
Jan. 2009	Austin, TX	Work Zone Ahead	Amusing	Driver distracted and confused	[56]
Apr. 2007	Boston, MA	Work Zone Ahead	Amusing	Driver distracted	[54]

2.7 Adverse impact and countermeasures

A valid concern might not be over a single hacking scenario; rather about the penetration of an integrated ITS network from the point that is most susceptible to a cyber-attack. As the necessity for inclusive ITS implementation increases, the security issues regarding cyber-attacks have gained more attention. In some cases, conventional DMS were only threatened by physical attacks, and protection was not difficult. However, an integrated ITS network requires an advanced communication setup [47, 97], making security far more difficult. Some challenges that security advancements face may include driver distraction or confusion, incidents, congestion, fatalities, financial losses, and harm to agencies and their employees. Dealing with cyber-attacks demands enhanced coordination and management, as these are serious matters that affect people's lives.

Once a hacker breaches the system, the DMS becomes a malicious node in the TMC network.

From this first foothold, hackers could easily penetrate further and expand their reach into the network. Spyware could be installed to steal usernames and passwords, and later that information could feed Group 2 (e.g., ransomware viruses) and Group 3 (terrorists engaged in cyber warfare) threat agents for exploitation and egress [70]. It is best to create a robust security system in advance, rather than to consider after DMS implementation, to save time and money. Moreover, with the rise of the connected vehicle technology, adversaries could exploit vulnerabilities in existing, traditional ITS installations, thus being able to compromise V2X installations despite their build in security measures. Fabricated information could mislead vehicles to cause adverse impacts (e.g., crashes) on road users and operators [98].

This survey is of special interest and usefulness to engineers concerned with safety, operation and security issues that have been ensured by DMS hacking incidents. Lessons learned from almost all the cases above depict that drivers were distracted by the messages displayed on DMS; they either stopped or reduced vehicle speed and lost concentration on the road for a short period. Driver distraction (e.g., to outside persons and events) is one of the main causes of driving errors leading to crashes. On the other side, tampered DMS need to be fixed by authorities (e.g., Police, TMC) and will dictate unexpected operational costs (e.g., labor costs) to the system. Besides, delay to adjust the issues would affect system operational success and results in road users' distrust of a system. Consequently, DMS' security shall design-fitted instead of retrofitted which possibly costs considerably higher.

A 3×3 impact-likelihood matrix represented in Figure 5, attempts to map adverse impacts of the DMS hacking events onto a meaningful, visual, matrix for risk prioritization purposes. Three impact and likelihood classes (Low, Medium and High) were identified to assist decision-makers to prioritize the risks that are associated with hacked DMS. The impact-likelihood matrix maps the adverse impacts of DMS hacking into high (colored in dark gray), medium (colored in light gray) and low-risk zones. Risk assessment result indicates that (1) safety, operational (i.e., monetary loss) and behavioral impacts are associated with the high-risk cluster, and (2) security, reliability, efficiency and operational (i.e., congestion) impacts are associated with the medium-risk cluster. Noteworthy that the impact-likelihood matrix is concluded based on the highest-level attacks, which represented in Figure 2.

IMPACT	LIKELIHOOD: Low	Medium	High
High	**Security Impact:** DMS becomes a malicious node in the TMC network	**Behavioral Impact:** Impulsive drivers' behavior	**Safety Impact:** Crashes with severity level form Property damage to Injuries and fatalities
Medium		**Operational Impact:** Traffic congestion, increase in travel time	**Operational Impact:** System operators' financial losses
Low		**Efficiency Impact:** Increase in energy consumption	**Reliability Impact:** Road users' distrust of a system

Figure 5 The impact-likelihood matrix maps the adverse impacts of DMS hacking into high (colored in dark gray), medium (colored in light gray) and low-risk zones (colored in white).

A few countermeasures should be considered by manufacturers and system operators, to mitigate against threats to DMS [27]. These recommendations include:

1) to place the display on a private network or VPN,

2) to deactivate unnecessary telnet, webpage and LCD interfaces,
3) to avoid using hard-coded/default passwords, but instead secure the access with strong and complex password,
4) to minimize network exposure,
5) to isolate control network from business network,
6) to secure the remote access for authorize users,
7) to implement an authentication mechanism against physical attacks,
8) to upgrade SNMP to the most current version,
9) to enable remote logging and Monitor the logs, and
10) to change all SNMP community string from the default.

This study aimed to raise awareness among traffic engineers to comprehend and utilize best practices of cyber hygiene (steps to enhance cybersecurity), access control, risk management, information security and monitoring [42]. Network redundancy is required in advance to prevent the failure of critical infrastructures. Intrusion detection systems (IDS) are effective in identifying odd activities in the network. Also, encryption methods can secure the network communications and stop hackers from easily manipulating the infrastructures. More prominently a practical approach would be to exercise white hat hackers' skills to constantly monitor vulnerabilities of the ITS critical infrastructure before adversaries could breach the system.

The result of this study supports risk response decision and might affect (1) ITS security practices, policies, and guidance, (2) selection of common ITS security controls, (3) ITS design, implementation and operational decisions, and (4) development of risk-aware training. The main objective of this study is not to comprehensively study such dynamic subject but is to raise awareness among policy-makers and engineers systematically. Awareness is a fundamental step in making transportation secure and resilient against cyber-physical attacks. Secure and resilient transportation infrastructure enables people and goods to be transported without significant disruption and frees resources to make transportation safer and more efficient.

2.8 Conclusion

As more and more intelligence is applied in the field of transportation, cybersecurity threats are more serious than ever before. These shifts in intelligence include introducing connected vehicle and automated vehicle technologies. Broad integration of such intelligent transportation systems, can make transportation faster, safer, more reliable, and more convenient. However, unanswered controversies remain, including security issues that demand attention before any large-scale implementation should take place. The assumption of the trustworthiness of ITS network fails at the presence of any vulnerability, leading to brittle protection. For a future integrated ITS network, a hacked DMS is a malicious node where group two and three threat agents would prolong their reach into the network. Once access to a single node in a network is gained, adversaries can launch various attacks that eventually can fail the system dramatically. In this study, we outlined potential consequences of the DMS security breaches due to the cyber and physical attacks. The concerns above need to be assessed more in-depth through crowdsourcing or simulation studies. There is a

gap in literature to assess and evaluate the impact of security vulnerabilities on the road users and the system operators. The result of this study endorses the necessity of impact assessment on the DMS security breach.

Risk assessment is a key component of the risk management process, and since risk management is an ongoing process, risk assessment should be conducted throughout the system development lifecycle. In this study, we employed the NIST SP 800-30 risk model to conduct a risk assessment to perform qualitative vulnerability-oriented threat analysis. We summarize the key findings as follows:

5. The risk-based approach of this study delivers the impact-likelihood matrix, which maps the adverse impacts of the threat events onto a meaningful, visual, matrix. The result provides insights for system operators and decision-makers to prioritize the risk of a DMS hacking event.
6. DMS hacking adverse impacts can be categorized mainly as high-risk and medium-risk clusters. The safety, operational (i.e., monetary losses) and behavioral impacts are associated with a high-risk cluster. While the security, reliability, efficiency, and operational (i.e., congestion) impacts are associated with the medium-risk cluster.
7. The DMS security vulnerabilities and predisposing conditions allow adversaries to compromise the ITS functionality. System operators should consider adequate physical and cyber security measures to improve transportation critical infrastructure security and resiliency. Moreover, at the same time, since threats on ITS are inevitable, impact assessment could guide decision-makers on the adverse impact of a security breach.

It needs to be understood that with the progression of technology, the operator's understanding must also change. With the increasing complexity and the integration of the system, operators have to look at this situation on a system level instead of as a collection of isolated incidents. Future ITS implementations need to be designed with adequate security in mind from inception. At this time, it can be concluded that the physical and cyber hackings of DMS create the slowdown of traffic, they also have the potential to threaten road users' safety and to create financial losses in the affected communities. Crashes, fatalities, congestion, and public chaos are among the possible outcomes of tampering with transportation network critical infrastructures. Sudden changes in drivers' behavior while passing a tampered message sign could lead to devastating incidents. Also, from an operation and security standpoint, authorities need to foresee the situation to plan efficient countermeasures to minimize the risk of partial or complete losses of the system. Further research is needed to assess the risk conferred by hacked DMS and the messages they convey. Also, countermeasures proposed here (e.g., encryption and IDS) need to be studied and prioritized as potential long-term and short-term strategies.

Chapter 3

3 Cyber-Physical Attack On DMS And Its Impact on Drivers' Route Divergence Behavior

Abstract

This study is the first to investigate drivers' route divergence behavior under a bogus en-route advisory information. In this study, we explore drivers attitudes toward a compromised Dynamic Message Signs (DMS) in order to understand their route departure behavior. Recently DMS have been hacked with higher occurrence in the US with uncommon en-route information to convey amusing, funny, and offensive message. In this study, we argue that an adversary is able to display fabricated-realistic traffic related information on DMS to coax drivers' decisions. We conducted stated preference research to assess about 4,700 subject's behavior under such forged information. To this extent, we developed latent based ordered probit regression models to scrutinize driver's behavior as far as the route divergence behaviors are concerned. The results of this study support the original hypothesis and indicate that in compliance with the fabricated-realistic message drivers will change their planned route in response to the compromised DMS. The findings pinpoint that female, experienced drivers, subjects familiar with the DMS, and tech-friendly drivers are more likely to comply with the forged information. While white, subjects in rural areas and those who have prior knowledge of DMS hacking phenomena are more likely to ignore the advisory information. The outcome of this study can be a guide to policymakers concerned with developing incident response plans to mitigate risks that are associated with the security vulnerabilities of intelligent transportation systems infrastructure.

Key words: cyber-physical attacks, dynamic message signs, travelers' behavior, route divergence

3.1 Introduction

Advanced Traveler Information System (ATIS) has been used as a means of transferring traffic, safety, and informative-related messages to the drivers with the objective to make transportation safer and more efficient. The majority of current literature found drivers responsive to en-route instructions supplied by the DMS. Compliance rate to the en-route information is dependent on various factors. These factors include, information (i.e., message type and format) [6, 15, 99, 100, 101, 102, 103, 104], drivers (i.e., demographic and attitudinal characteristics) [2, 3, 6, 7, 11, 19, 99, 100, 105, 106, 107], and trip (i.e., travel time, trip purpose) [4, 19, 102, 107, 108] characteristics. Several researchers have attempted to investigate the determinants that influence drivers' behavior under en-route real time information. But none have attempted to assess drivers' behavioral change under a fabricated message.

In recent years, adversarial attacks to the cyber-physical systems have raised a great concern on ITS infrastructures security. These infrastructures include, but not limited to, DMS, traffic signal controllers, and Vehicular ad-hoc Networks (VANET) [25, 109, 110, 111]. To this date, the main focus of the literature was to enhance the security measures of the ITS

infrastructures while limited studies focused on the negative impacts that an adversarial attack could impose on the transportation system. The gap in the current literature is more conspicuous for the case of a compromised DMS. That is, to the best of this authors' knowledge no previous study undertakes a quantitative impact-oriented analysis to assess drivers' behavior under a compromised DMS. That is understanding drivers' behavior to the DMS hacking phenomenon on the basis of empirical data is a must that needs to be addressed.

Cyber-physical attacks on the ITS infrastructures are likely to impose risks to the transportation system [25]. Pieces of evidence from the previous cyber and physical attacks on DMS are enough to evince this fact. For instance in Kelarestaghi et al., study [25] safety, behavioral, operational, security and reliability issues have been identified to occur in case of an adversarial attack. Various threat events around the US illustrated that fabricating the content of a DMS could detrimentally impact drivers' behavior [26, 27, 28, 29, 89, 30]. The thought-provoking fact about DMS compared to other ITS infrastructures (e.g., traffic signal controller), is that through an adversarial attack a meaningful message could be conveyed en-route to the drivers. That is, an adversary could impact drivers' decision and behavior. A compromised DMS not only undermines the reliability of the ITS system but also biases drivers' decisions by coaxing them with forged information.

There is a necessity to a data-driven approach to assess driver's likely behavior under a compromised DMS and to associate socio-demographic and attitudinal information to subject probable responses. In this study, we tackle this challenge and contribute to the literature of the ITS security and resiliency in threefold. First, we conducted a stated preference survey to capture a fair amount of data from eleven States in which some of them have experienced many cyber and physical attacks on DMS. Second, we developed univariate latent based ordered probit models to understand subjects route divergence behavior under fabricate en-route advisory information. Third, we explored the association between speed and route divergence behavior. More specifically we aim to provide answers to the following concerns:

- Could an adversary perpetrate an attack to coax driver's decision to shunt them from certain routes?
- What are the explanatory factors that contribute to the route divergence compliance and noncompliance behavior under a compromised DMS?
- Does DMS hacking phenomena destabilize traffic pattern?

The proposed study aims to assess the impact of a compromised DMS on the drivers' compliance behavior with the fabricated content. For this purpose, a survey questionnaire was designed with the aim to perceive about 4,700 drivers' attitude toward route divergence behavior under a cyber-physical attack on DMS. We built four latent based ordinal models using the perception information of drivers from eleven States which was collected in November and December of 2018. This modeling structure allows us not only to account for analyses of the ordinal dependent variable but also to explore drivers' characteristics that are not clearly recognized by the subjects, which influence their behavior. Here in, we aim to augment the literature of Intelligent transportation system security and resiliency by assessing possible consequences of an adversary attacking the DMS security vulnerabilities. That is, in this study, we

attempt to contribute to the embryonic but growing literature of ITS security and resiliency through data-driven impact-oriented risk assessment. Considering the current policy interventions, the outcome of this study could back policy development process with the aim to mitigate risks of a cyber-physical attack on the transportation network.

The remaining part of this study is organized as follows. First, we survey current literature on traveler's compliance behavior with en-route advisory information displayed on a DMS. Second, we discuss the survey structure and the data that we used in this study. Third, we developed univariate latent based ordered probit models to assess drivers route divergence behavior. We close the paper by summarizing significant discoveries and proposing future research path.

3.2 Background

The current literature have well-investigated the drivers' behavior at the presence of en-route information. However, the literature is mainly focused on drivers' route choice and diversion behavior under the authentic advisory information but a fabricated information. In this section, we aim to review the current literature considering two viewpoints: (1) determinants of drivers' compliance with en-route information, and (2) DMS hacking phenomenon. The succeeding subsections provide a detailed synthesis review on the aforementioned outlooks. A summary of the previous studies is provided in Table 2 with focus on drivers' compliance behavior including the method of data collection, sample size, a location of the study, and the analysis approach.

3.2.1 Determinants of driver response to DMS

Analysis of the drivers' response to the supplied information in the case of ATIS has been a focus of many studies (Table 2). A wide range of determinants found as a contributory factor to the drivers' compliance and inertia with the supplied advisory information. The determinants that impact drivers' behavior under en-route information can be classified into four different categories. These categories include (1) drivers' socioeconomic characteristics, (2) drivers' attitude and perception, (3) trip characteristics, and (4) message content characteristics.

Drivers' socioeconomic characteristics, attitude, and perception explore drivers' characteristics such as age, and drivers' mentality and attitude toward DMS and the supplied information. Trip characteristic refers to conditions that drivers are likely to encounter during their trip. That is, include the purpose of the trip, the time of a trip, trip flexibility, and road network characteristics. Information characteristics include the format and wording of the DMS content. The information might convey only travel time information (i.e., descriptive information), and/or might suggest an alternative route for optimal route-choice decision (i.e., prescriptive information) [112]. As far as the message format is concerned, a graphic indication can be incorporated into the message in addition to the text, in order to improve ATIS performance [18]. The remaining of this section surveys the determinants that are remarked in previous studies with influence on drivers' response to the ATIS.

Table 2 Summary of previous studies.

1st Author	Year	Data collection	Assessed Behavior	Sample size	Location	Analysis	Reference
Studies with focus on Route choice and diversion behavior							
Khattak	1993	SP - Mail-back	Route Diversion	700	Chicago, Illinois	Ordered probit model	[102]
Khattak	1996	SP / RP - Mail-back	Route Diversion, departure time change, modal change	2,703	Bay area, California	Multinomial Logit (improved)	[4]
Wardman	1997	SP-paper questionnaires handed out to individuals	Route choice	289	Warrington, England	Multinomial Logit	[6]
Peeta	2000	SP- on-site survey	Route Diversion	248	Borman Expressway, Indiana	Binary Logit	[2]
Dia	2002	SP - Mail-back and traffic simulation	Route Diversion	167	Brisbane, Australia	Multinomial Logit	[3]
Chatterjee	2002	SP / RP - paper questionnaires	Route Diversion	229 / 203	London, England	Logistic regression	[99]
Peng	2004	SP- on-site survey	Route Diversion	306	Milwaukee, Wisconsin	Ordinal Logistic	[15]
Jou	2005	SP - interview	Route choice	557	Taiwan	Multinomial probit	[7]
Abdel-aty	2006	SP-Driving Simulator	Route diversion and route choice	539 / 218	Orlando, Florida	Binomial and Multinomial generalized extreme equations	[8]
Foo	2006	RP - field observation	Route Diversion	38,866 vehicles	Toronto, Canada	Descriptive statistics	[16]
Peeta	2006	SP- Mail-back, Internet, and on-site survey	Route Diversion	402, 34 and 248	Borman Expressway, Indiana	Binary Logit	[100]
Tsirimpa	2007	SP - Interview	Route Diversion	234	Puget Sound Region, Washington	Mixed Logit	[103]
Richards	2007	SP- Mail-back	Route Diversion	660	Southampton, England	Descriptive statistics	[5]
Choocharukul	2008	SP / RP - Mail-back	Route Diversion	388	Bangkok, Thailand	Structure Equation Modeling	[105]
Kattan	2010	SP- on-site survey	Route Diversion	500	Calgary, Canada	Latent variable model	[17]
Ben-Elia	2010	SP- computer-based survey and Laboratory experiment	Rout choice	49 participants / 14,553 observations	Haifa, Israel	Mixed Logit	[9]
Zhong	2012	SP with simulation scenario	Route choice	246	Beijing, China	Ordinal Logistic with complementary log-log link function	[18]
Spyropoulou	2014	SP- on-site survey	Route Diversion	120	Athens, Greece	Random-effect ordered probit	[101]
Yan	2014	SP-Driving Simulator	Rout choice, Speed control and Lane changing	52	Beijing, China	Logistic regression	[11]
Bifulco	2014	SP- Web-based travel simulator	Rout choice	90	Naples, Italy	Non-parametric test	[113]
Ma	2014	SP - on-site survey	Route Diversion	8,477	Beijing, China	Multinomial logit	[14]
Basheer	2018	SP – offline and online survey	Route Diversion	402	Chennai, India	Logistic regression	[19]

3.2.2 Driver's characteristics

For many years, researchers have attended to identify determinants that are influencing drivers' behavior in response to the en-route information (Table 3). The current literature implies that socioeconomic characteristics play a significant role in drivers' behavior at the presence of en-route information (e.g., [2, 3, 6, 7, 11, 19, 99, 100, 105, 106, 107, 18]). However, the impacts of socioeconomic factors on drivers' behavior varies from one study to another. Age factor found in many studies as an indication to justify drivers' inertia or compliance with the supplied information [3, 100, 114, 6, 17, 105] . Younger drivers have been categorized as drivers that are in compliance with the given information due to their (1) limited driving experience, (2) limited knowledge of network, and (3) the fact that younger drivers are risk-willing in order to find an efficient route [3, 100, 114]. Accordingly, limited driving experience was also found as an indication of drivers compliance with the en-route information [9, 14, 17, 18, 19, 20, 21]. On the opposite side, several studies found younger drivers reluctant to comply with the DMS information [6, 17, 105]. The reason might be that younger drivers depend more on their own knowledge and experience than supplied en-route information [105]. Similar contradiction also remarked in the case of an increase in drivers' age. Several studies found that older drivers are more likely to comply with the supplied information [17, 18, 101, 114]. While others [7, 11, 106], observed older drivers inertia to the supplied information, due to (1) established driving habits and preferences, and (2) risk-unwilling attitude that inhibits older drivers en-route switching behavior.

The majority of the studies found female drivers with a lower compliance rate to the DMS information compared to their male counterparts [2, 3, 6, 7, 11, 19, 99, 100, 105, 106, 107]. A possible explanation is that male drivers are more attentive to the displayed information [105]. In the contrary, several studies (e.g., [14, 108]) found female drivers more responsive to the DMS content. The driving experience is another determinant that has an impact on drivers' behavior. Experienced drivers might not comply with the given information completely [22]. For instance, in the case of Erke et al. experiment [22], a DMS displayed information of a closed road section which recommended an alternative route to drivers. Observation indicates that a large number of vehicles chose alternative routes to the suggested one. However, experienced drivers were interested in more efficient routes (i.e., faster, shorter) than the one advised by the DMS.

Higher income and education are among the factors that are likely to contribute to drivers' higher compliance rate. Several researchers [7, 17, 18, 102, 100]found that drivers with higher income and education are more likely to comply with the DMS information, that is, they have a higher value of time and are prone to diverge in order to choose more efficient routes. In contrast, Spyropoulou and Antonio [101], and Basheer et al. [19] found drivers in a wealthier household less likely to divert. Choocharukul [105] also concluded that well-educated drivers are less attentive to the DMS, and rely on other sources of information, thus are less likely to comply with the en-route information. In addition, other factors were found to influence driver's response to the DMS information. These include (1) infrequent travelers indicated less tendency to comply with the en-route information [6, 18, 100, 101], (2) drivers of a company-owned vehicle are less likely to diverge under the en-route information [115], and (3) professional drivers are more prone to comply with the DMS information [11].

Familiarity with the road network and DMS are also important factors that influence drivers' decision-making process. Familiarity with alternative routes found as a contributing factor

to influence drivers' compliance with a supplied information [4, 14, 17, 102]. While familiarity with the road network contributes to higher divergence rate, some drivers might prefer to stay on their predetermined route even under real-time en-route information [18]. Familiarity with DMS also increases the likelihood of a driver complying with en-route information [6, 7, 15, 107]. This could also be the case for the drivers who are not familiar with the DMS [101]. That is, those who are more familiar might not trust the content because of their past experience with DMS [101].

Drivers' attitude toward DMS and supplied information contribute to their decision of whether to comply with the DMS or not. Drivers trust in the ATIS is a significant explanatory factor to justify drivers' behavior. The majority of the current literature suggests that drivers with higher trust in DMS information, have a higher compliance rate [4, 7, 14, 15, 16, 18, 19, 100]. Meaning that higher information accuracy increases the drivers' perceived reliability of the ATIS, thus drivers tend to comply more with en-route information. Driver's trust in the DMS basically lies in the driver's experience. Drivers with negative experience are unlikely to follow the supplied information to comply with suggested information [7]. This mainly implies that to increase the ATIS performance, system operators should improve the message content and the accuracy of that message.

3.2.3 Trip characteristics

Trip characteristics concern with the nature of the trip (e.g., trip flexibility) and the prevailing conditions (road network characteristics) that are associated with that trip. The purpose of the trip has been found as a governing factor to influence drivers' compliance behavior. Drivers with flexible work schedule found to be more compliant with supplied information [3]. Dia [3] modeled drivers' response to the DMS in a commuter corridor in Australia using a behavioral survey and concluded that drivers who had flexible work schedules are more likely to diverge to another route under quantitative delay information. School- and work-related trips were also found among contributory factors to influence driver compliance behavior. Kattan et al. [17] assessed the route-switching behavior of drivers under en-route information using latent discrete choice model. Investigating the behavior of 500 respondents indicated that during school/work related trips drivers are less likely to divert from their original route. The Choocharukul study [105] suggested the similar results, that is participants whose trip purpose were work or education, trusted their usual routes which they presume are more efficient. Aligned with this result, Foo and Abdulhai [16] found that drivers tend to comply with DMS information with higher propensity during afternoon and evening trips as compared to morning trips. Similarly, Kattan et al. [17] found a negative correlation between diversion rate and trips which occurs during morning rush hours. Inconsistently, several studies indicating an opposing result [4, 19, 102, 107, 108]. The reason behind this contradiction might be due to the trust drivers have in the supplied information [19].

Increase in travel time is another factor that effects drivers' compliance behavior [99, 100, 105, 17]. Peeta and Ramos [100] concluded that commuter individuals whose trip is longer than 30 minutes are more likely to divert under en-route information. These individuals are more sensitive to more efficient routes and are likely to trust the information in order to minimize their travel time. In contrary, Kattan et al. [17] analysis suggested that participants during a longer trip (i.e. more than 45 minutes) are less prone to diversion. That is, these type of travelers might not be familiar with the road network –specifically the middle section of the trip– and are less likely to take the risk and divert from their planned route [17]. The prevailing conditions are another

major contributor that influence divers' diversion behavior. Urban settings and the presence of a traffic signal are factors that sometimes prevent drivers to comply with DMS guidance [8, 116]. The amount of traffic signals in the original route and the recommended route impact the propensity of diversion. Abdel-Aty and Abdalla [8] used a driving simulator to study drivers' route diversion/choice patterns under DMS information. Analysis of route diversion pattern indicated that (1) drivers tend to divert from their original routes that have a higher number of traffic signals, and (2) under ATIS guidance drivers' compliance increases if the advised route contains a lower number of traffic signals.

Table 3 Determinants of driver response to DMS.

Category factor	**Impact on drivers' compliance behavior**	
	Negative	*Positive*
Information characteristics		
Delay (no reason specified)		[6]
Delay (reason specified)		[6]
Information indicating high severity (long delays or avoid area)		[6, 15, 99, 100, 101, 102, 103, 104]
Information related to accidents or roadwork		[4, 15, 99, 102,
Content format: Text + graphics		11, 14]
Drivers' characteristics		
Younger Drivers	[6, 17, 105]	[3, 100, 114]
Older drivers	[7, 11, 106]	[17, 18, 101, 114]
Female	[2, 3, 6, 7, 11, 19, 99, 100, 105, 106, 107]	[14, 108]
Income	[19, 101]	[7, 17, 18, 102,
Education	[105]	[100]
Familiarity with DMS	[101]	[6, 7, 15, 107
Familiarity with the network	[18]	[4, 14, 17, 102]
Infrequent travelers	[6, 14, 18, 100, 101]	
Limited driving experience		[9, 14, 17, 18, 19, 20, 21]
Professional drivers		[11]
Risk-based driving style	[18]	
Calm driving style	[14]	
Trust in DMS accuracy		[4, 7, 14, 15, 16, 18, 19, 100, 113]
Drivers who seek for external traffic information (e.g., via radio)		[17, 101]
Trip characteristics		
Queue visibility	[102]	
Speed under DMS	[11]	
Trip occurs during morning	[16, 17]	
Travel time	[17]	[99, 100, 105]
Drivers with flexible work schedule		[3]
School/work related trips	[17, 105]	[4, 19, 102, 107, 108]
Urban settings & presence of traffic signals	[8, 116]	

3.2.4 Information characteristics

En-route information can be displayed in three formats. These formats include (1) passive message that only contains descriptive information (2) informational content that adds more details to the passive content (e.g., accident ahead, 15 minutes delay), and (3) active guidance that includes detailed prescriptive information [101, 112, 117]. In the case of prescriptive information, a message provides detail information on traffic condition along with advisory information, for instants, of an alternative route. Whereas in the case of descriptive information, a message provides limited information such as travel time statistics and warning of an accident. Informational content includes more details than the descriptive content but the content does not guide drivers of a better alternative. Overall, prescriptive messages found to increase drivers' compliance rate [100]. That is, they transfer quantitative information (e.g., delay, travel time) and diversion strategies (e.g., alternative route) which perceived better by drivers.

Besides other determinants, (e.g., driver's characteristics) DMS content is the most influential factor to impact drivers' route diversion behavior [17]. Accident, delay, and congestion-related information displayed on a DMS could significantly impact drivers' compliance behavior. Erke et al. [22] investigated the impact of a road closure message on drivers' speed, route choice, and braking behaviors. The results indicate that [22] almost all drivers avoided the road closure section of the roadway by choosing another route; 20% of the drivers chose the suggested alternative route; and drivers significantly reduced their speed. In Peng et al. study [15] drivers were asked to rank the importance of different DMS messages. Traffic- and informative-related messages concerned with accidents, congestion, road construction, and hazardous conditions (e.g., natural disasters) were ranked among the most important messages. Implying that, drivers' response with higher rate to the DMS with the aforementioned related messages content.

Apart from the type of a message, format, and wording of the DMS messages influence drivers compliance behavior [118]. An effective message on the DMS should be familiar and standard to the drivers [119]. The message contents that are legible, short and concise are easier to follow and will improve the ATIS efficiency [119]. Incorporating graphics indications (i.e., pictograms) in the message content conveys information that is more likely to perceived by drivers. Symbols and pictograms provide language-independent content that is easy to understand. On the other side, text-only messages demand higher drivers' attention and could have a lower impact compared to the messages that contain clear symbols and pictograms [120]. The current literature suggests that incorporating pictorial message would improve ATIS performance [121, 122, 123, 124]. Ullman et al. [123] investigated the pictorial message effect on conveying information to the drivers. The results suggest that pictorial messages, compared to text messages, assist drivers to read and comprehend the messages better, and allows system operators to communicate unusual operational information effectively. Alkim et al. [124] investigated the impact of graphical route information on drivers behavior and found that (1) graphical information does not compromise drivers' safety, (2) drivers comprehend the information easily, and (3) route choice decision made better compared to alphanumeric information.

3.2.5 DMS hacking phenomenon

While DMS provide en-route information to road users, a forged content might compromise the road users' safety and security if a malicious adversary exploits DMS security vulnerability [25].

Depends on the DMS communication medium and attacker's capabilities and motivation, threats to the DMS could be classified as physical and remote attacks. To the best of our knowledge, the remote attack occurred only in one specific time frame (i.e., May 27th – June 2nd, 2014) but in multiple States (NC, NJ, IO, WY). While the physical attack occurred more frequent for over 10 years. Noteworthy that physical attack is a dominant attack and can be executed on any DMS, while the remote attack can happen only for DMS that are operable remotely (i.e., remotely controlled by TMC) [25].

Kelarestaghi et al., [25] surveyed the DMS hacking incidents that occurred around the nation. In most of the cases, adversaries compromised DMS with funny and offensive messages that caused distraction among the road users. In this study, we argue that a malicious adversary could take a step forward to cause more harm to the transportation operators and road users. A significant negative impact can be achieved by an adversary who attempts to impersonate false information that resembles a realistic message. The message that could directly convey traffic, informative, funny, political, terrorism-related information to the road users. Depend on the wording and format of such content, drivers' behavior could differ significantly. This implies that adversarial attacks cause uncertainties to the drivers' behavior. To elucidate uncertainties, we undertake an SP approach to assess drivers' response to various hypothesized scenarios. The scenarios aim to measure drivers' perception of a compromised DMS impact on transportation's safety, reliability and drivers' behavior (i.e., distraction and route diversion).

3.3 Methodology

3.3.1 Survey design

Investigation of the drivers' response to the DMS information can be undertaken throughout SP and RP approaches. These approaches include (1) survey questionnaire [2], (2) driving simulator [77], (3) network monitoring [125], and (4) traffic network modeling [126]. In the SP approach, drivers can be given a set of hypothetical choices and asked to indicate their response to those choices. While in the case of RP approach an actual behavior of the drivers at the presence of a real DMS is assessed. In the context of drivers' behavior assessment at the DMS, most of the studies employed SP approaches [113]. While RP experiments, attempt to represent real-life drivers' behavior they have several shortcomings that make SP approach a lucrative alternative for this study. The main shortcomings include (1) RP approach is not the best alternative for assessing drivers' behavior for the case of a new hypothetical choice, (2) DMS Hacking is a rare event and it is unlikely to observe drivers' behavior at the time of such event, (3) it is difficult to collect driver's related characteristic, and (4) it is unlikely to capture drivers' behavior at hacked DMS with different fake messages– almost impossible to assess the impact of all types of fake messages through the observation study. The most popular methodology to assess the drivers' behavior under delivery of en-route information is the SP methods. These methods include Mail-back (e.g., [102, 100, 5]), on-site survey (e.g., [2, 15, 100]), interview (e.g., [7, 103]), Internet-based/ survey (e.g., [100, 19]), laboratory experiments (e.g., [127, 9, 18]). Incorporation of the Reveal preferences (RP) and SP methods also found beneficial in order to assess drivers' behavior more accurately (e.g., [4, 99, 105]).

On the basis of the aforementioned concerns, to assess drivers' behavior at the hacked DMS we employed the SP approach, carried out by means of an online survey questionnaire.

Wherein, we attempt to investigate the adverse impact of a compromised DMS on distracted driving, drivers' compliance behavior, transportation safety, and reliability. The survey questionnaire is designed in three distinct sections Figure 6. In the first section, we asked socio-demographic related questions (e.g., age and income). In the second section, we provided questions targeting to understand participants' characteristics (e.g., sense of direction). The third section of the questionnaire aims at exploring the attitude and perception of participants toward forged messages.

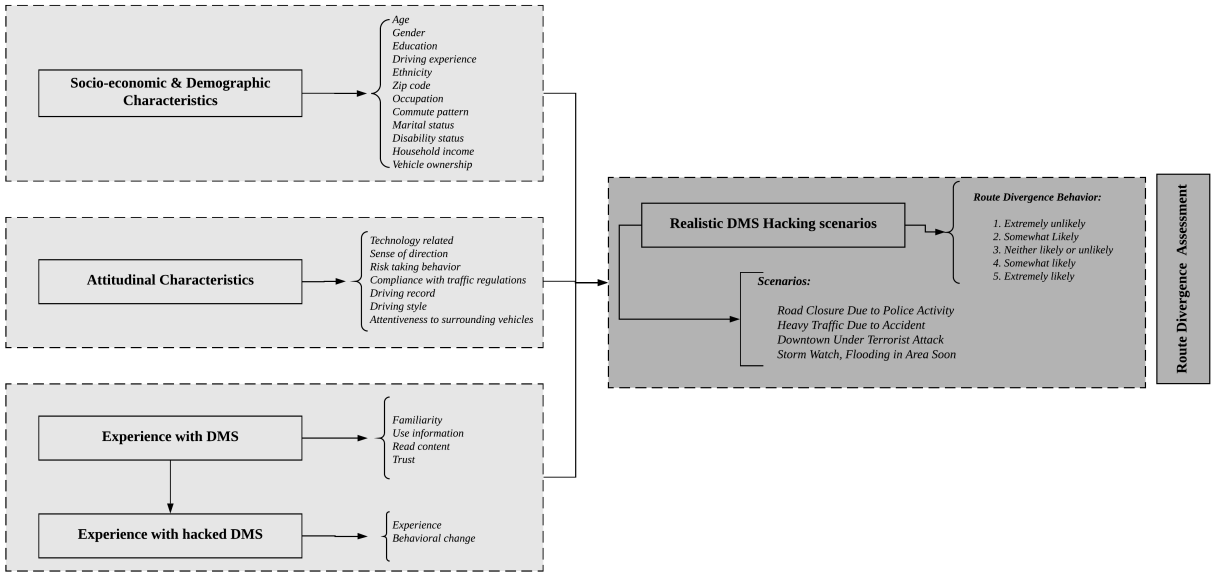


Figure 6 Questionnaire structure.

3.3.2 Tool for data collection

The Amazon Mechanical Turk (mTurk) is an online crowdsourcing marketplace that enables researchers to employ human intelligence in order to collect individuals' attitudes and perception toward different Human Intelligence Tasks (HITs). During the past few years, mTurk has gain popularity in stated preference based studies e.g. ([128, 129]). The mTurk web-based tool has been used to explore various topics especially in the social science domain. Several studies examine the representativeness of the data that has been collected using the mTurk. Huff and Tingley evaluated the data collected from mTurk and found that mTurk respondents demographics are mainly similar to other survey platform respondents [130]. Buhrmester et al., [131] evaluated the quality of the mTurk and found that (1) mTurk respondents compare to other web-based crowdsourcing platforms, are more demographically diverse, (2) and the reliability of the data is similar or better than the traditional methods (paper-based methods). Other studies also indicated that mTurk represents the US population better than other web-based crowdsourcing tools, however, the data is not flawless. More precisely, the respondents might be skewed toward the female, young, and low-income individuals [132]. To avoid biases, data collection process could be controlled to ensure data that is representative of the US population. In this study, we collect the data across different samples to control the demographic diversity of the population.

For the purpose of this study, we used the mTurk web-based service. We used mTurk as a means to recruit respondents. A request specifying the length and the monetary compensation for taking the survey will be advertised on mTurk which will allow workers from mTurk to access and fill out the survey. Note that we will be allowed to accept or reject responses coming from mTurk. That is, if the research team chose not to approve their response, workers will not be compensated. Workers from mTurk are aware of the case and rules.

3.3.3 Data

Following the first and second drafts of the survey IRB approval was obtained and the survey questionnaire distributed in the States of California, Texas, and Florida. The main reasons for the pilot study were to improve the quality of the survey and to collect a sample of data to statistically analyze the validity and reliability of the survey and study hypothesis. The result of the pilot study approved the study hypothesis and indicates an increase in distracted driving and drivers' compliance with forged information.

In result of a 2-month data collection effort (during November and December of 2018), we received 4706 completed online responses. However, following the data preprocessing we removed about 8.5% of incorrect and erroneous data records. In total we collected responses of participants in 11 States including California (CA), District of Columbia (DC), Florida (FL), Iowa (IA), Maryland (MD), Mississippi (MS), North Carolina (NC), New Jersey (NJ), New York (NY), Texas (TX), and Virginia (VA) with 1176, 29, 636, 101, 187, 82, 328, 277, 526, 692, and 268 valid records, respectively. In this study we considered our sampling size to account for roughly 5% of the population of licensed drivers [133] in each of the aforementioned States.

The final data contains 2,301 female drivers that account for 53.5% of the sample. Most of the subjects are under 34 years old (55.3% of the sample), 35.8% are between 35 and 54 years old and the remaining sample size comprise of subjects which are 54 to 84 years old. Above half of the participants have an associate degree or lower (e.g., high school diploma, professional certificate), 37% of them earned a Bachelor degree and about 15% hold a graduate degree. The household income of more than half of the subjects are below $60K, about 24% of the subjects earn more than $90K in which about 400 of them lives in a household with income over $135K. While many researchers have observed that mTurk workers are mainly comprised of low-income induvial in this survey we were able to attract high-income individuals by limiting our data collection to those with higher income- a higher compensation also was offered for these cases. As far as the race of the participants is concerned, we collected the majority of responses from individuals who were White (66% of the sample), Black or African American (9.4%), Asian (9%), Hispanic, Latino, or Spanish origin (9.81%). In this study, we collected the information regarding subjects' driving style which has been categorized into four groups based on the results of the Taubman-Ben-Ari et al. study [134]. These groups and their share of the sample includes Anxious (23.34%), Reckless and careless (2.28%), Angry and hostile (4.39%), and Patient and careful (70%). Table 4 summaries the description and basic statistics of variables used for the modeling purposes.

In previous DMS hacking events, the fabricated messages rendered funny, offensive, and political information [25]. While in this study, we are focused on messages that sounds realistic and convey traffic and informative related information to the drivers. We aim to understand to what extent the drivers are complying with the fabricated supplied information, and how this

compliance could adversely impact the transportation network. To this extent, we designed four scenarios in which DMS displayed fabricated-realistic messages encouraging drivers to change their choice of route. These messages were "Heavy Traffic Due to Accident" (STrf1), and "Road Closure Due to Police Activity" (STrf2), "Downtown Under Terrorist Attack" (SInf3), and "Storm Watch, Flooding in Area Soon" (SInf4).

Table 4 Description of explanatory variables.

Variable	Description	Category	Mean	Std. Dev.
DrivDur	Driving duration (year)	1: < 1; 2: 1-5; 3: 6-10; 4: 11-15; 5: 16-20; > 20	4.25	1.52
Female	–	1: Yes; 0: Otherwise	0.53	0.50
Age	Age (year)	1: 18-24; 2: 25-34; 3: 35-44; 4: 45-54; 5: 55-64; 6: 65-84; 7: >85	2.61	1.20
Hssms	Some school and High school	1: Yes; 0: Otherwise	0.09	0.28
AbMaster	Above Master's degree	1: Yes; 0: Otherwise	0.15	0.36
Asian	–	1: Yes; 0: Otherwise	0.09	0.29
Black	Black or African American	1: Yes; 0: Otherwise	0.09	0.29
White	–	1: Yes; 0: Otherwise	0.66	0.47
Student	–	1: Yes; 0: Otherwise	0.06	0.24
Income	Household Income level	1: < 15; 2: 15-30; 3: 30-45; 4: 45-60; 5: 60-75; 6: 75-90; 7: 90-105; 8: 105-120; 9: 120-135; 10: 135-150; 11: > 150	4.94	2.71
Disbl	Disable subjects	1: Yes; 0: Otherwise	0.06	0.23
DisabilityM	Mobility disability	1: Yes; 0: Otherwise	0.02	0.15
Rural	–	1: Yes; 0: Otherwise	0.13	0.34
Urban	–	1: Yes; 0: Otherwise	0.34	0.47
Dhr	Driving hours (per week)	1: 0; 2: 1-5; 3: 6-10: 4: 11-15: 5: 16-20; 6: 21-25; 7: > 25	4.40	2.05
Dhr1620	Driving hours between 16-20 hr (per week)	1: Yes; 0: Otherwise	0.07	0.26
Anxus	Anxious	1: Yes; 0: Otherwise	0.23	0.42
Reckless	Reckless and careless	1: Yes; 0: Otherwise	0.02	0.15
Patient	Patient and careful	1: Yes; 0: Otherwise	0.70	0.46
InvAcc	Involved in accident	1: Yes; 0: Otherwise	0.61	0.49
Dfam	Familiarity with DMS	1: Not familiar at all – 5: Extremely familiar	3.96	1.02
Dread	Read DMS in daily commute	1: Never – 5: Always	4.28	0.89
UVCR	Use DMS information on congested roads	Continues (1–5)	3.97	1.15
ATrM	Attention to DMS traffic information	1: Not at all – 5: Completely	4.31	0.82
RlyTech	Rely on technology for daily trips	1: Extremely Unlikely – 5: Extremely Likely	3.23	1.45
Newrote	Take new routes to reach destination sooner	1: Extremely Unlikely – 5: Extremely Likely	3.81	1.08
Trbldir	Trouble understanding directions	1: Extremely Unlikely – 5: Extremely Likely	2.18	1.17
Accom	More accomplished because of technology	1: Extremely Unlikely – 5: Extremely Likely	4.03	0.92
Bored	Driving makes me bored	1: Extremely Unlikely – 5: Extremely Likely	2.63	1.16
Upnews	Up-to-date with news	1: Extremely Unlikely – 5: Extremely Likely	3.78	1.02
Blinker	I use blinker when changing the lanes	1: Extremely Unlikely – 5: Extremely Likely	4.64	0.73
AtnVeh	Pay attention to vehicles around me	1: Extremely Unlikely – 5: Extremely Likely	4.70	0.62
TrfReg	Comply with traffic regulations	1: Extremely Unlikely – 5: Extremely Likely	4.52	0.74
SmArnd	Driving the same way as the others	1: Extremely Unlikely – 5: Extremely Likely	3.36	1.09
Grec	I have a good record of driving	1: Extremely Unlikely – 5: Extremely Likely	4.46	0.81
TrsArd	Trust drivers around	1: Extremely Unlikely – 5: Extremely Likely	2.42	1.09
Lost	Get lost in an unfamiliar area	1: Extremely Unlikely – 5: Extremely Likely	3.10	1.29
Chctrf	Check traffic before hitting the road	1: Extremely Unlikely – 5: Extremely Likely	3.19	1.38
Trstch	I trust technology to assist in my travel	1: Extremely Unlikely – 5: Extremely Likely	4.17	0.94
PFmRt	I prefer taking familiar routes	1: Extremely Unlikely – 5: Extremely Likely	4.30	0.86
Ignore	STrf1	1: Extremely Unlikely – 5: Extremely Likely	1.64	0.90
	STrf2	1: Extremely Unlikely – 5: Extremely Likely	1.86	0.99
	SInf3	1: Extremely Unlikely – 5: Extremely Likely	1.37	0.81
	SInf4	1: Extremely Unlikely – 5: Extremely Likely	1.73	1.04
Slow Down	STrf1	1: Extremely Unlikely – 5: Extremely Likely	3.78	1.15
	STrf2	1: Extremely Unlikely – 5: Extremely Likely	3.96	1.04
	SInf3	1: Extremely Unlikely – 5: Extremely Likely	3.57	1.34
	SInf4	1: Extremely Unlikely – 5: Extremely Likely	3.27	1.34
Stop	STrf1	1: Extremely Unlikely – 5: Extremely Likely	1.49	0.84
	STrf2	1: Extremely Unlikely – 5: Extremely Likely	1.64	0.95
	SInf3	1: Extremely Unlikely – 5: Extremely Likely	2.15	1.29
	SInf4	1: Extremely Unlikely – 5: Extremely Likely	1.55	0.89
Route Divergence	STrf1	1: Extremely Unlikely – 5: Extremely Likely	3.51	1.27
	STrf2	1: Extremely Unlikely – 5: Extremely Likely	3.69	1.17
	SInf3	1: Extremely Unlikely – 5: Extremely Likely	4.24	1.09
	SInf4	1: Extremely Unlikely – 5: Extremely Likely	3.15	1.39

The current study was developed around the route divergence behavior question. The outcome variable comprises of five categories in order to mimic driver's behavior under each of the scenarios. These categories are from extremely unlikely to extremely likely. Figure 7 illustrates the details of subjects stated preference for all the scenarios. Under the SInf3 scenario, subjects are willing the most to divert from their current route (above 80%). The departure likelihood is the lowest under fabricated message in SInf4. As far as the traffic related scenarios are concerned, 64% and 67% of the subjects are likely to divert under STrf1 and STrf2, respectively.

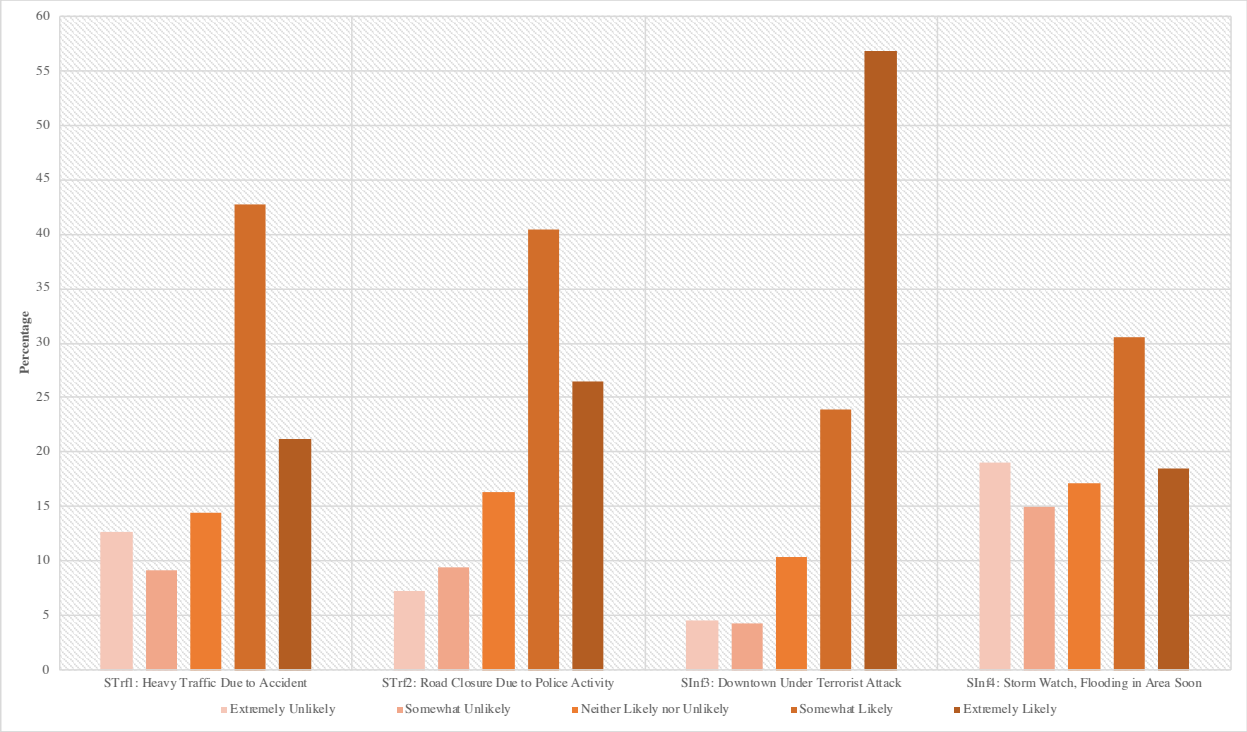


Figure 7 Road users speed route divergence behavior under fabricated-realistic information.

3.3.4 Does data represent the population?

Amazon Mechanical Turk (mTurk) is a great tool that facilitate a collection of quality data within a short period of time. While mTurk offers many benefits, several researchers have questioned its capabilities to collect an unbiased data. Since mTurk workers could mainly comprised of young, low income, and female individuals one should control the sample distribution to assure for data preventiveness. We recognized the similar issue in our data collection process. Meaning that while we were collecting the data we noticed that the sample was skewed toward younger, female, and low-income individuals. Thus, we attempted to control the data collection process according to the age, gender, and income. To do so, we continuously compared the sample demographic information with the State actual data. To test whether the collected data is a representative sample of the States, we compared the aforementioned variables stat between this study data and the states actual data. We judged the significance of difference through the means of t-test.

To test whether the income distribution of the sample correspond with the States distribution, we used Census median household income information by States, for 2017 [135]. We

calculated the exact median income and conducted the two-tailed t-test to identify if there is a significant difference between our sample and Census data. the result of the t-test proved that our data represents the population income distribution. To test for age, we used the data of a total number of licensed drivers by age for each State [136]. Then we conducted a State by State comparison and found that our data matches the age distribution of the licensed population of all the States. As far as the gender distribution is concerned, we used the same source (Federal Highway Administration) [136] data and found that our sample gender distribution is a representative of the eleven States' gender.

3.3.5 Modeling approach

The outcome variables (route divergence behavior) of this study are all ordinal variables with categories of (1) extremely unlikely, (2) somewhat unlikely, (3) neither likely nor unlikely, (4) somewhat likely, and (5) extremely likely. For the purpose of this study, we developed univariate latent based ordered logistic regression model with the probit link function. Basically, in addition to the observed variables, we tested the association between unobserved variables (latent factors) with the outcome variable. The utility function would be $Y_i^* = Z_i + \varepsilon_i$, where Z represents the observed and unobserved characteristic of subjects. The group membership of subject n, would be chosen based on threshold (cut point) values ($\tau_1, \dots, \tau_{P-1}$) relativeness to the utility (Eq. 2). And P is the total number of categories of the ordinal dependent variable of the study. In this study P is equal to 5.

$$Y_{n,i} = \begin{cases} 1 & if\ Y_1^* < \tau_1 \\ 2 & if\ \tau_1 < Y_2^* < \tau_2 \\ \vdots & \vdots \\ P & if\ \tau_{P-1} < Y_p^* \end{cases} \quad \text{(Eq. 2)}$$

In order to develop the models, we undertook the following steps:

- We conducted bivariate regression between the explanatory variables and the dependent variable.
- We tested the association between of the latent factors, and explanatory variables and the dependent variable.
- Based on two-tail t-test we examined the significance level of the model observed and unobserved variables.
- We tested the explanatory power of the highly correlated variables one by one and kept the one that resulted in a model with better goodness of fit. We mediated the better model by means of Akaike Information Criterion (AIC).

3.3.6 Factor analysis

In this study in order to retain the explanatory influence of the indicator variables and to investigate the lower number of unobserved variables, we performed an explanatory factor analysis. The explanatory factor analysis is conducted to identify an optimum number of latent factors that have the potential to group subjects' attitudinal characteristics. For this purpose, we estimated the

measurement of each latent factor based on Eigenvalue of greater than one. We tested factorability of 17 variables and found 11 of them with the potential to form 3 latent variables. These latent variables include (1) driving habit, (2) driving attitudes, and (3) tech friendly (Table 5). We found the Kaiser-Meyer-Olkin Measure of sampling adequacy equal to 0.758 which indicates an adequate sampling [137] and Bartlett's test of sphericity significant with a *p-value* lower than 0.001.

The main indicators of these 3 latent variables are identified (in bold) as those with values equal and greater than 0.4. Driving habit latent variable includes variables that explain drivers' attentiveness to the traffic regulation (i.e., Comply with traffic regulations) and surrounding traffic (i.e., Pay attention to vehicles around me) in addition to their driving records. Driving attitude latent factor explores subjects' characteristics such as the sense of direction (i.e., Trouble understanding directions, Get lost in an unfamiliar area), and their willingness to take new routes to lower their travel time. While tech friendly driver latent factor is formed by indicator variables that measure to what extent subjects are rely upon (i.e., rely on technology for daily trips) and trust (i.e., trust technology to assist in my travel) on technology, and check traffic before starting their trips.

Table 5 Factor loading.

Indicators	Factors		
	Driving Habit (DriHabt)	**Driving attitude (DriAt)**	**Tech friendly (Tech)**
AtnVeh	**0.798**	-0.190	0.086
TrfReg	**0.775**	-0.051	0.024
Blinker	**0.761**	-0.067	0.075
Grec	**0.669**	-0.204	0.037
RlyTech	-0.099	0.115	**0.730**
Trstch	0.203	0.130	**0.692**
Accom	0.261	0.054	**0.594**
Chctrf	-0.016	-0.163	**0.500**
PFmRt	0.494	**0.429**	0.083
Lost	0.077	**0.752**	0.232
Trbldir	-0.127	**0.714**	0.131
Newrote	-0.027	**-0.550**	0.350
Upnews	0.273	-0.324	0.154
Bored	-0.127	0.301	0.124
SmArnd	0.121	0.067	0.315
TrsArd	-0.118	-0.086	0.200

3.4 Result

To assess the route divergence behavior of this study subjects we built four univariate latent based ordered probit regression models. Out of three latent factors, we found only tech-friendly and driving habit latent factors with significant relationship to the outcome variable. We anticipated that driving attituded latent factor would have negative linkage with route change behavior, but we did not find that latent factor significant in the models. That is, we removed it from the modeling process. As indicated in the Table 6 Tech latent factor had positive significant

contribution to the drivers' route divergence behavior in STrf1, STrf2, and SInf4 scenarios. This implies that to what extent subjects' involvement with technology could sway their decision of route change behavior. While the DriHabt construct was found with positive relationship in the traffic-irrelevant scenarios. In addition, we confirmed that there is a strong link between route divergence and speed variation behaviors. We argue that drivers tend to lowering their speed in order to react to the DMS information. Speed reduction behavior provides adequate time frame for drivers to pay enough attention and decide whether they should change their route under the en-route information.

We assessed the models' goodness of fit via McFadden's Pseudo R-Square, according to the following equation (Eq.1). We calculated the McFadden's Pseudo R-Square of 0.59 and 0.6, 0.51, and 0.39 for STrf1, STrf2, SInf3, and SInf4 scenarios, respectively. Which indicate models with a good fit to the data (McFadden's Pseudo R-Square > 0.2). Thresholds (cut points) values that indicate group membership for categorical outcome variables are listed in Table 6.

$$R^2_{McFadden} = 1 - {Fitted\ model\ Log\ Likelihood}/{Null\ model\ Log\ Likelihood} \quad \text{(Eq.1)}$$

During the development of the route divergence models, we tested the association between explanatory variables and latent factors and the outcome variables. We considered variables collinearity in order to not include highly correlated explanatory variables concurrently. The models that we reported here contain only significant variables (at 90% confidence interval) that ensure models' goodness of fit. Table 6 outlines the results for route divergence behavior models. The signs of the significant variables included in all four models are consistent with the theoretical expectation of this study. Several explanatory variables are common between models. That is, they have a significant association with two or more outcome variables. For instance, gender, race, familiarity with DMS, education level, driving style, and attitudinal variables are common variables in most of the models. To build upon this result, we also assessed the linkage between subjects' speed variation and their divergence behavior under a compromised DMS information (Table 6). In the remaining part of this section, we discuss the results of the route divergence behavior models.

3.5 Discussion

The route divergence models assess the effect of latent factors and explanatory variables with the outcome variable. We tested the association in four scenarios to examine subjects' behavior change under different DMS content. Traffic related scenarios (STrf1, STrf2) have more variables in common. As far as the explanatory variables are concerned, the third scenario has some variables in common with the traffic related scenarios, but the scenario SInf4 has no common ground with the first two scenarios. As far as the speed variation behavior is concerned, the modeling result provides the opportunity to compare subjects' behavior under all the scenarios.

To assess whether drivers would pay attention to the fabricated en-route information, we included "ignore" variable in the models. The result indicated that in STrf1, STrf2, and SInf3 scenarios subject would not ignore the message. The effect of "Ignore" entails that subjects would pay the most attention to the "Downtown Under Terrorist Attack" message under SInf3 scenario. That is, adversaries could have a higher chance to destabilize traffic pattern under the third

scenario. Compared to the other scenarios, subjects stated the lowest sensitivity with respect to the "Heavy Traffic Due to Accident" message (Figure 8). We did not locate a significant correlation between "Ignore" and the last scenario.

The majority of variables of the STrf1 model were found significant in the STrf2 scenario as well. These variables are related to the driving duration, gender, subjects who are more sensitive to the DMS information on congested roads, driving style, those who in general pay more attention to the traffic related information and, tech friendly driver latent factor. The explanatory power and the sign of the aforementioned variables are roughly the same between both scenarios.

On the other hand, there are several variables that are not common in both scenarios. For instance, we found several socio-demographic information with association to the outcome variable of the heavy traffic scenario. Race (i.e., Asian), education, subjects' location (i.e., urban area) and household income (Est. = 0.02) are among those variables. Asian and low educated subjects have negative attitude toward the sign. While individuals with higher income are more likely to divert under the DMS content in STrf scenario. This is consistent with [7, 17, 18, 102] where high income drivers found with positive compliance toward the en-route information. This might indicate their sensitivity to slow travel speed and delay that might occur by not changing their route. In addition, we found a significant association between attitudinal variables and route divergence behavior in the road closure scenario. Those subjects that would take a new route in order to optimize their travel (Est. = 0.08) are more likely to depart from their planned route. This is also true for subjects that pay more attention to the DMS information in congested routes.

With respect to the SInf3 scenario, we identified several variables with positive and negative impact on drivers' compliance behavior. Subjects who saw a hacked DMS before, indicated a negative attitude toward route divergence behavior. That is, drivers who speculate that the information could be fabricated, indicated less tendency toward changing their behavior. That is, educating drivers of the DMS hacking phenomena could benefit the system immensely. This result affirms policy implications that aim to familiarize drivers with the DMS common practices. These policies would encourage drivers to question the integrity of the message before taking any action. Furthermore, higher education also was found with negative association to the fabricated content. Female drivers, and subjects who in general are familiar with the DMS would attempt to change their routes under the SInf3 scenario. Attitudinal characteristic of the subjects also plays a significant role in their decision-making process. Drivers who are more sensitive to the news, those who trust and rely on technology and those who comply with traffic regulations are likely to depart from their current route.

Subjects' behavior in regards to the last scenario is different. First, we did not find as many significant variables as the other models. Second, the four explanatory variables that we identified had negative association with the route divergence behavior. These variables relate to subjects who have disability, who are students, live in rural areas, and who are white. Interesting that subjects who live in an urban or suburban area are more likely to divert under SInf4 scenario. In addition, we identified that more conservative drivers who comply with traffic regulations and have better driving record are more likely to change their route under the "Storm Watch, Flooding in Area Soon" message.

Table 6 Route divergence behavior under compromised DMS.

Variables	STrf1: Heavy Traffic Due to Accident			STrf2: Road Closure Due to Police Activity			SInf3: Downtown Under Terrorist Attack			SInf4: Storm Watch, Flooding in Area Soon		
	Estimate	**z**	**P-Value**	**Estimate**	**z**	**P-Value**	**Estimate**	**z**	**P-Value**	**Estimate**	**z**	**P-Value**
Female	0.130	3.754	≤ 0.001	0.055	1.610	0.107	0.208	5.577	≤ 0.001		–	
DrivDur	0.041	3.483	≤ 0.001	0.046	3.971	≤ 0.001		–			–	
AG1824		–			–		0.083	1.557	0.119		–	
Dhr1620		–		-0.154	-2.413	0.016		–			–	
AbMaster		–			–		-0.125	-2.479	0.013		–	
Hssms	-0.156	-2.615	0.009		–			–			–	
White		–			–			–		-0.102	-2.911	0.004
Student		–			–			–		-0.142	-2.037	0.042
Asian	-0.094	-1.564	0.118		–			–			–	
Rural		–			–			–		-0.141	-2.888	0.004
Urban		–			–			–			–	
Income	0.020	3.091	0.002		–			–			–	
Dfam	0.047	2.725	0.006	0.032	1.908	0.056	0.048	2.457	0.014		–	
Dread		–			–		0.062	2.768	0.006		–	
UVCR	0.033	2.034	0.042		–			–			–	
ATrM	0.062	2.670	0.008	0.083	3.800	≤ 0.001		–			–	
Newrote	0.080	4.998	≤ 0.001	0.082	5.176	≤ 0.001		–			–	
DisablityM		–			–			–		-0.204	-1.838	0.066
Upnews		–			–		0.033	1.769	0.077		–	
Patient	-0.058	-1.569	0.117	-0.089	-2.406	0.016		–			–	
SawHckd		–			–		-0.061	-3.027	0.002		–	
Slow	0.054	3.533	≤ 0.001	0.166	9.784	≤ 0.001	0.179	12.104	≤ 0.001	0.360	27.129	≤ 0.001
Stop	0.098	4.822	≤ 0.001	0.154	8.330	≤ 0.001	0.140	8.491	≤ 0.001	0.180	9.191	≤ 0.001
Ignore	-0.211	-10.463	≤ 0.001	-0.318	-17.323	≤ 0.001	-0.476	-21.419	≤ 0.001		–	
Tech	0.132	3.247	0.001	0.194	4.713	≤ 0.001	0.114	2.596	0.009		–	
DriHabt		–			–		0.185	4.251	≤ 0.001	0.147	4.079	≤ 0.001
Thresholds (cut-points)												
Cut 1	-0.026	-0.167	0.867	-0.359	-2.338	0.019	-1.152	-7.804	≤ 0.001	0.352	6.200	≤ 0.001
Cut 2	0.352	2.273	0.023	0.181	1.181	0.238	-0.738	-5.039	≤ 0.001	0.896	15.479	≤ 0.001
Cut 3	0.802	5.168	≤ 0.001	0.774	5.048	≤ 0.001	-0.137	-0.941	0.347	1.401	23.671	≤ 0.001
Cut 4	2.021	12.921	≤ 0.001	1.970	12.734	≤ 0.001	0.716	4.921	0.000	2.380	37.911	≤ 0.001
Tech												
Accom	Constant			Constant			Constant					
Trstch	1.297	23.742	≤ 0.001	1.337	24.244	≤ 0.001	1.305	24.021	≤ 0.001		–	
RlyTech	1.380	20.863	≤ 0.001	1.498	20.682	≤ 0.001	1.360	21.463	≤ 0.001			
Chctrf	0.676	12.242	≤ 0.001	0.715	12.066	≤ 0.001	0.658	12.399	≤ 0.001			
DriHabt												
Blinker							Constant			Constant		
AtnVeh		–			–		0.939	42.305	≤ 0.001	0.941	42.003	≤ 0.001
TrfReg							1.006	39.428	≤ 0.001	1.015	39.241	≤ 0.001
Grec							0.931	33.637	≤ 0.001	0.937	33.526	≤ 0.001

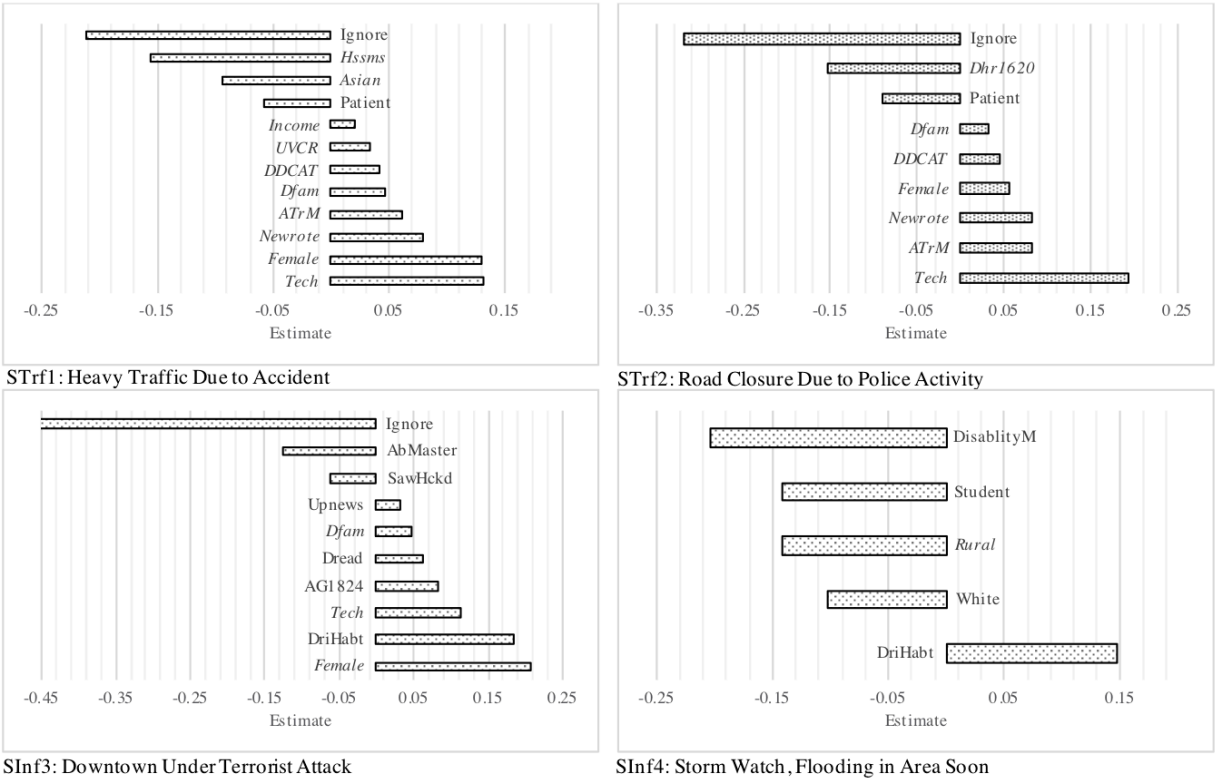


Figure 8 Determinants of route divergence under STrf1, STrf2, SInf3, and SInf4 scenarios

As far as all scenarios are concerned, we expect drivers to comply with the bogus information and divert from the planned route under the compromised DMS. While this study focuses mainly on drivers' compliance behavior under a compromised DMS, we have identified some results that are comparable with the current travel behavior literature. Current literature has a mix result over the association between gender, age, income, education, and drivers' attitude toward DMS. In the route change model, we divulged that females are more likely to comply with the forged information compared to their male counterparts. This is consistent with [14, 108] studies while contradicting with [2, 3, 6, 7, 11, 19, 99, 100, 105, 106, 107].

In [7, 11, 106] older drivers identified as drivers with inertia to the supplied information while in the STrf1, STrf2 scenarios we identified that drivers with more years of driving experience (i.e., older) are more likely to comply with the information to divert from their current route. This result is in agreement with [17, 18, 101, 114] studies that classified older drivers as drivers who comply with DMS information. Higher household income and education are among the variables that have been investigated significantly in travelers' behavior studies. These type of drivers could have a higher value for their time thus more sensitive to the DMS traffic related information [7, 17, 18, 102, 100] . The result of this study confirms this and indicates that subjects with higher income ware more likely to change their route under heavy traffic scenario and low educated subjects are less likely to do so. It is worth mentioning that we did not find a significant association between income and education level under the SInf4 scenario.

Familiarity with DMS is another important factor that contributes to the drivers' compliance behavior. Here we discovered that drivers who are more familiar with the DMS, in

general, are more likely to divert under STrf1, STrf2, and SInf3 scenarios. This is inconsistent with most of the current literature [6, 7, 15, 107] but [101] in which authors found these type of drivers with inertia to the given en-route information. Tech friendly drivers are drivers who seek for additional traffic information to find optimum route. This study result indicates that such drivers are more likely to divert under road closure and heavy traffic messages which is consistent with [17, 101] studies. in addition, we identified a positive reaction to the route change behavior under 'Downtown Under Terrorist Attack' message.

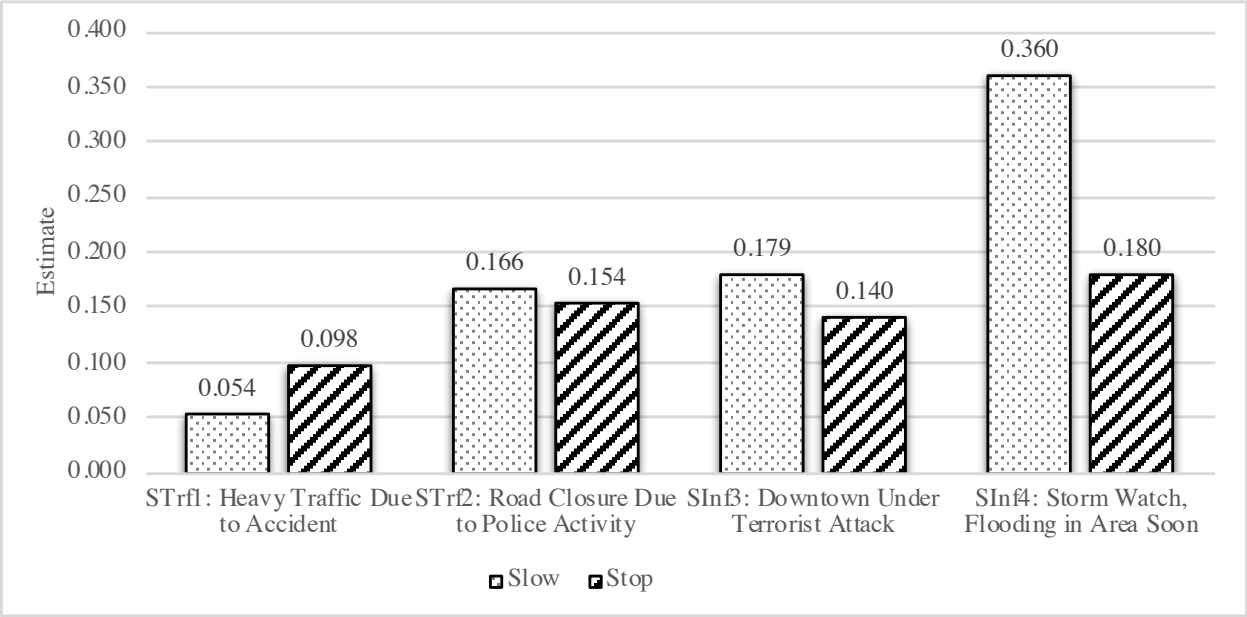


Figure 9 Speed association with route divergence under STrf1, STrf2, SInf3, and SInf4 scenarios

In this study, we anticipate that drivers in order to react to the fabricated information would lower their speed. We tested this hypothesis by measuring the impact of slow down and stopping behavior on route divergence behavior (Figure 9). The result indicates that in STfr2, SInf3, and SInf4 scenarios drivers are more likely to slow down rather stop. However, in the first scenario the correlation between stopping and route divergence is higher. Overall, the likelihood of both slowing down (Est. = 0.36) and stopping (Est. = 0.18) behavior are higher in the last scenario. In the speed variation is higher in response to the traffic-irrelevant messages compared to the traffic related messages. This might be because drivers are more familiar with the traffic related information and it is easier for them to respond to those messages. Besides, drivers could become involved in other activities under the SInf3 and SInf4 scenarios. These activities might include, checking the news, calling/texting someone, changing destination, and talking to a passenger.

In this study, we tested the hypothesis that an adversary could coax drivers route decision by impersonating them through fabricated-realistic en-route information. We constructed four models to mimic drivers' behavior under two realistic scenarios. Our assessment entails that adversaries could sway drivers' decision to their benefit. That is, adversaries could destabilize traffic pattern and shunt drivers from particular routes by displaying realistic traffic related information. We argue that a simple traffic related message could impose a significant impact on the transportation network. This is very concerning when considering system reliability disputes. An adversary not only could adversely impact the efficiency of the transportation network he/she

could undermine the reliability of the system by causing distrust among system users. That is, road users will question the integrity of the service that could mar the credibility of the ITS infrastructures.

3.6 Conclusion

Dynamic message signs are one of the most important and commonly used components of the ITS infrastructure. In this study, we divulged that an adversary could destabilize traffic pattern through compromising the integrity of the DMS message. We presented that road users are likely to slow down in order to comply with a fabricated-realistic message. Later we discovered that the reason behind this behavior is that drivers tend to lower their speed to engage with the en-route information and to find a better route to lower their travel time.

Researchers found that drivers interested the most in the information that guides them to the more efficient route (e.g., [15]). An adversary can use this fact and alter the message to divert drivers to other routes deliberately. The bogus information can inform drivers of traffic congestion in certain routes with an aim to shunt traffic from that particular roadway in order to execute a malicious attack. As far as the type of a message is concerned, to gain higher reward, an adversary can inject a bogus message that impersonates real-world scenario. Integration of a pictorial indication in the bogus message is more likely to increase the impact of an attack. In this study, we used the gain knowledge in order to construct scenarios in which a set of forged information was presented to drivers. The forged messages contained, realistic information included with a pictorial indication, to assess the behavior of the drivers.

To this point, no previous research attempted to tackle the problem of this study. Here, we augmented the results of Kelarestaghi et al., [25] study that undertook a qualitative risk assessment approach. In [25] authors argued that a driver's decision could be affected by a forged message and that the driver is likely to comply with the en-route information which is phony. The results of this study support this premise and indicate that drivers are more likely to slow down under the fabricated information with a likely reason for departing from their planned route. As depicted in Table 13, drivers with higher desire to divert from their current route are extremely unlikely to ignore the messages and are likely to slow down under the fabricated-realistic information. We summarize the primary outcome of this study as follows:

- The latent based ordered model developed with two latent factors. Tech friend driver latent factor was significant in three of the models indicating that those drivers who rely on technology and feels more accomplished with it are more likely to slow down and depart from their planned route. That is, they are more comfortable in changing their route through the secondary sources' suggestions. At the same time while they are acquiring new information, they need to lowering their speed to respond to the higher information load. Drivers who respect traffic regulation also found with positive attitude toward changing their route under traffic-irrelevant scenarios. This type of drivers has higher trust in the DMS information and would comply with the sign to higher degree.
- We assessed the behavior of the drivers under four fabricated messages. These messages include "Heavy Traffic Due to Accident heavy traffic", "Road Closure Due

to Police Activity", "Downtown Under Terrorist Attack", and "Storm Watch, Flooding in Area Soon". As far as the road closure scenario is concerned, approximately 67% of the respondents indicated that they would change their routes under the road closure scenario. As far as the heavy traffic scenario is concerned, 64% stated that it is probable for them rather to pick another route to reach their destination faster. This rate was 81% and 49% for the SInf3 and SInf4 scenarios. Indicating an extremely high sensitivity toward the "Downtown Under Terrorist Attack" content.

- As far as the STfr1 and STfr2 route divergence models are concerned, we identified several variables with a significant impact on compliance and noncompliance behavior. Under the road closure scenario, we found females and subjects with higher driving experience more likely to change their route. In addition, those subjects who are more sensitive to the DMS's traffic related messages and those who use DMS under congested traffic condition are likely to divert. Under heavy traffic forged information, a similar pattern for experienced and female drivers are true. In addition, we found higher income a factor that contributes to higher divergence rate. Interestingly, individuals with lower education level, Asians, those who live in urban areas, and those with trouble finding their direction in new routes are less likely to pick another route other than the one they planned.
- With respect to the traffic-irrelevant scenarios, higher education and previous knowledge over DMS hacking phenomena instigated a negative attituded toward route divergence behavior. living in a rural area, and being a student also associated with a non-compliance behavior. But, similar to the scenarios with traffic related information subjects who are more familiar with DMS, and tech friendly drivers are more likely to trust the message and change their route. Subjects with good record of driving also indicated a positive attituded toward route change behavior under both SInf3 and SInf4 scenarios.

This study investigated drivers' perception toward a hacked DMS. The modeling approach enabled us to capture subject socio-economic and demographic, and attitudinal characteristics toward route divergence behaviors. The approached allowed us to understand how respondents with a different background, driving style, driving habit and attitude toward DMS would react to a fabricated-realistic en-route message. This study suggests a need for future research. For instance, we recommend research to take the step forward and conduct a driving simulation study to assess the speed change and route divergence behavior of the drivers in more details. Such study paves the road for a collection of more data on speed quantities and also allows researchers to observe route divergence behavior. Considering the current policy interventions, the outcome of this study could back policy development process with the aim to mitigate risks of a cyber-physical attack on the transportation network.

Chapter 4

4 Does DMS Bogus Content Cause Distracted Driving?

Abstract

In the real-world Dynamic Message Signs (DMS) hacking events, the fabricated messages rendered funny, offensive, and political information. In this study, we focus on scenarios in reference to the previous threat events to form a set of creative forged messages to assess drivers' decision. In addition, we take a step forward and examine drivers' distraction behavior under a fabricated realistic message as well. This approach helps us to not only compare different messages impact on subjects' behavior but to understand what will happen if an adversary displays bogus realistic messages rather common funny/offensive context. This study is the first to assess the impact of a compromised DMS with realistic and fictitious related content on travelers' distraction behavior. The main objective of this study is to understand to what extent the drivers are receptive to the fabricated DMS content, and how the fabricated messages adversely impact the drivers' behavior. To test if a cyber-physical attack on DMS would cause drivers' distraction we developed Structural Equation Modeling (SEM) to examine the association between distraction and drivers' objective and subjective attributes. The results indicate that regardless of DMS fabricated information, drivers would engage in at least one of the distractive activities. Among the distraction latent factors, cognitive distraction has the highest impact on the distracted driving likelihood. The outcome of this study would be of special help to policymakers, emergency responders, and engineers who are concerned with developing incident response plans and the safety, security, and resiliency of the ITS network.

Key words: cyber-physical attack, dynamic message signs, travelers' behavior, distracted driving

4.1 Introduction

Dynamic Message Signs (DMS) have been installed widely throughout the US to provide traffic management information to improve the safety and efficiency of the transportation network. The information could include traffic, warning, informative, safety-related content. To this date, many studies have been conducted to assess the effectiveness of DMS through the means of revealed and stated preference (SP) studies. For instance, DMS found compelling to divert traffic from a congested or closed road [2, 45, 77, 138], to create homogeneous speed pattern [139], to decrease traffic speed at construction zones [12, 13], and warn drivers of an adverse weather condition [140]. Although DMS add significant benefits to the transportation system, one should not overlook their negative impacts on road users' safety.

Attention to the DMS content might compromise drivers' safety [22, 23]. The supplied en-route information increases the frequency of distraction [141], that is, ensued due to three reasons. First, advanced technology can cause distraction for some of the drivers [142], second, drivers need to read the message, comprehend, and decide based on the message content [143, 144], and third drivers might tend to take a picture, call or text someone, talk to a passenger, think of something other than the driving task, and look at other vehicles [25]. All of these could cause

conflicting attention demands between the acquiring task and driving task. The risk will be significant in cases where drivers need more time to react to the information and draw a decision [145]. Drivers' attentional overload to the en-route information could create traffic speed variation. Such behavior could cause impulsive braking behavior, short headways, and lane changing maneuvers which are factors that are likely to trigger safety hazards [24].

While DMS provide beneficial en-route information to road users, a forged content might compromise the road users' safety and security if a malicious adversary exploits DMS security vulnerability [25]. Depends on the DMS communication medium and attacker's capabilities and motivation, threats to the DMS security could be classified as physical and remote attacks. To the best of our knowledge, the remote attack occurred only in one specific time frame (i.e., May 27th – June 2nd, 2014) but in multiple States (NC, NJ, IO, WY). However, the physical attack occurred more frequently for over 10 years. Noteworthy that physical attack is a dominant attack and can be executed on any DMS, while the remote attack can happen only for DMS that are operable remotely (i.e., remotely controlled by TMC) [25].

Kelarestaghi et al., [25] surveyed the DMS hacking incidents that occurred around the nation, and found that in most of the cases, adversaries compromised DMS with funny and offensive messages which caused distraction among the road users. In this study, we argue that a malicious adversary could take a step forward to display more deliberate content in order to cause more harm to the transportation system. A significant negative impact can be achieved by an adversary who attempts to impersonate false information that resembles a common traffic management information. The bogus content could directly convey traffic, informative, funny, political, terrorism-related information to the road users. Depend on the wording and format of such content, drivers' behavior could differ significantly [25]. This implies that an adversarial attack could cause uncertainties to the drivers' behavior. To elucidate uncertainties, we undertake an SP approach to assess drivers' response to two hypothesized scenarios. The scenarios aim to measure drivers' perception of a compromised DMS impact on transportation's safety, and drivers' behavior.

Transportation system resiliency, efficiency, and reliability are highly dependent on the Intelligent Transportation Systems (ITS) infrastructure functionality. The cyber-physical attack on the ITS infrastructures imposes risks to the drivers and system operators. An adversary could convey a meaningful message to the drivers via the means of a DMS. Analyzing traveler behavior in response to the hacked message signs on the basis of empirical data is a vital step toward operating a secure and reliable transportation system. With cybersecurity issues escalating every day, road users' safety has been neglected [42]. There may be room for improvement by policymakers and program managers when considering critical infrastructure security vulnerabilities.

In this study, we focus on traffic relevant and irrelevant content inclined toward a congestion, road closure, political and funny type content. We explore how a theses bogus messages could impact drivers' attentional overload for the traffic that approaches a compromised DMS. Therefore, the main question of this work is whether a hacked DMS with realistic and fictitious information could compromise drivers' safety in the transportation network. In particular, we attempt to test the following hypotheses:

1. A bogus DMS content causes distraction while driving

2. Attention-averting distraction (i.e. cognitive distraction) would have the highest impact on distracted driving behavior
3. Drivers with positive attitude toward technology would become engaged in distracting activities
4. Gender, race, education, and driving style have a contributory impact on distraction behavior
5. Speed variation and distraction behaviors are associated with each other

The main concern is that distracted driving increases the crash risk of traffic adjacent to a compromised DMS. The distraction could emerge due to any of the visual, manual, or cognitive distractions. The more a driver pay attention to an activity other than driving (i.e., take a picture, mind wandering, texting) the likelihood for that driver to involve in a crash would increase [146]. Measuring the distraction likelihood as a consequence of forged en-route information is a hard task because DMS hacking phenomena is a rare event and it is impractical to observe an unsafe driving behavior while the DMS is being hacked. That is, in this study, we contribute to the literature of ITS security by conducting a state preference methodology to identify drivers' distraction behavior through a self-reported questionnaire.

The remainder of this study is structured as follows. First, we review current literature with a focus on the negative impacts of a DMS. Second, we discuss the data and the structure of this study. Third, we discuss explanatory and confirmatory factor analysis, and we develop structural equation models and provide in-depth conversation over the determinants of distraction. We close the paper by pinpointing the results of the study and promoting future research avenues.

4.2 Background

Distracted driving has been determined as a significant contributory factor to crash risk [147, 148, 149, 150]. Stutts et al., [151] examined 70 driver's distraction behaviors during one week to determine key distractive factors that contribute to the lane changing, lane busting and hard braking behavior. They identified extinguishing cigarette, passenger related distraction, and reading and writing during driving as three factors that caused distracted driving. McCartt et al., [150] reviewed the literature focused on cellphone use during driving, and concluded that cellphone use contributes to higher crash risk among drivers regardless of their age or gender. Campbell et al., [147] used the General Estimates System crash database and identified that drivers' inattention associated with half of the rear-end, and lane change crashes. Klauer et al., [148] used the 100-car naturalistic driving study database to explore more than 9,000 crashes, near-crashes, and incidents in Washington DC. The results of their study discerned that distracted driving contributes to more than 75% of the crashes occurred over a 12-month period [148].

The literature focuses on the effectiveness of the DMS (e.g., [139, 152, 153]) however, the negative impacts of en-route messages have not been adequately assessed. There are several concerns associated with messages displayed on a DMS that might negatively impact drivers' safety. Format and wording of the messages influence drivers' compliance behavior [118]. The Manual on Uniform Traffic Control Devices (MUTCD) states that messages that are displayed on the DMS should be "simple, brief, legible, and clear." An effective message should be standard and familiar to drivers [119]. Message contents that are legible, short and concise are easier to follow for drivers thus will improve their compliance rate [119]. On the other hand, wordy, unfamiliar, and complex messages might demand higher drivers' attention to read, comprehend

and decide based on the content [143, 144]. Unfamiliar and complex messages could cause conflicting attention demands between acquiring task and driving task and compromise drivers' safety.

In general, drivers are receptive to acquire knowledge about accidents, traffic jams, and guidance to an alternative route in order to make their trip more efficient. The main purpose for the supplied en-route information is to improve transportation performance, however excessive attention to the DMS could compromise drivers' safety [22, 23]. Electronic boards have been identified as a source of drivers' inattention and a factor to increase crash injury severity [149]. A DMS conveys en-route information to drivers but on the other hand, might increase the frequency of drivers' distraction [141]. The distraction could strike due to two main reasons. These reasons include (1) advanced technology can cause a distraction for some of the drivers [142], and (2) drivers need to focus on the message to read, comprehend and decide based on the content [143, 144]. Both of these could cause conflicting attention demands between acquiring task and driving task. Safety concerns arise due to the effect of drivers' distraction [22].

Bergeron [154], indicated that irrelevant information (e.g., advertisement) displayed on DMS cause attentional overload which affects drivers' reaction time. That is, DMS have the potential to increase the risk of a crash especially in high-volume high-speed roads. Erke et al., [22] studied advisory information (road closure related content) impact on drivers' speed variability and braking behavior. They revealed that at the presence of the information the traffic braking maneuver increased caused the majority of vehicles to slow down under the en-route information. They suggested that this behavior instigated due to the drivers' high cognitive demand. That is, drivers lowered their speed to pay more attention to the displayed information rather driving task. Worth mentioning that some of the braking maneuvers occurred in response to the traffic slow down behavior in order to avoid accident [22].

While the current literature has vastly investigated drivers' distraction behavior and its impact on transportation safety, there is no previous study with focus on evaluating a compromised DMS impact on distracted driving. In this study, we argue that a fabricated realistic or fictitious content displayed on a DMS would create an attentional overload. The increase in drivers' cognitive demand triggers (1) unsafe headways, (2) slower reaction time, and (3) increase in braking maneuvers. All these are major factors that contribute to higher crash rates.

4.3 Methodology

4.3.1 Data

For the purpose of the proposed study, a survey questionnaire was designed with the aim to perceive drivers' attitude and behavior toward a compromised DMS. The survey questionnaire was distributed online to approximately 5,000 drivers in the States of California (CA), District of Columbia (DC), Florida (FL), Iowa (IA), Maryland (MD), Mississippi (MS), North Carolina (NC), New Jersey (NJ), New York (NY), Texas (TX), and Virginia (VA). Participants were given a set of scenarios to measure their possible behavior regarding likely manual, visual, and cognitive distraction activities.

We collected drivers' responses to four DMS hacking scenarios comprise of fictitious and realistic content. In fictitious scenarios, the DMS were displaying messages with political and funny related content. These messages were 'Read The News Today, Oh Boy!' (scenario 1:

ReadNews), and 'Zombies ahead run!' (scenario 2: Zombieahead). The first scenario (ReadNews) was designed with the intention to encourage drivers to use their cellphone or their vehicles' infotainment system mainly to check the news. While the latter scenario (Zombieahead) was designed in order to assess whether drivers are likely to for instance (1) use their cellphone to take a picture of the sign, (2) talk to someone about the sign, or/and (3) think about something other than their driving task. Worth adding that many adversaries have hacked DMS with similar content for over 10 years around the US [25]. That is, it is not unlikely for many US drivers to saw a similar message on the DMS before. Figure 10 represents the structure of this study.

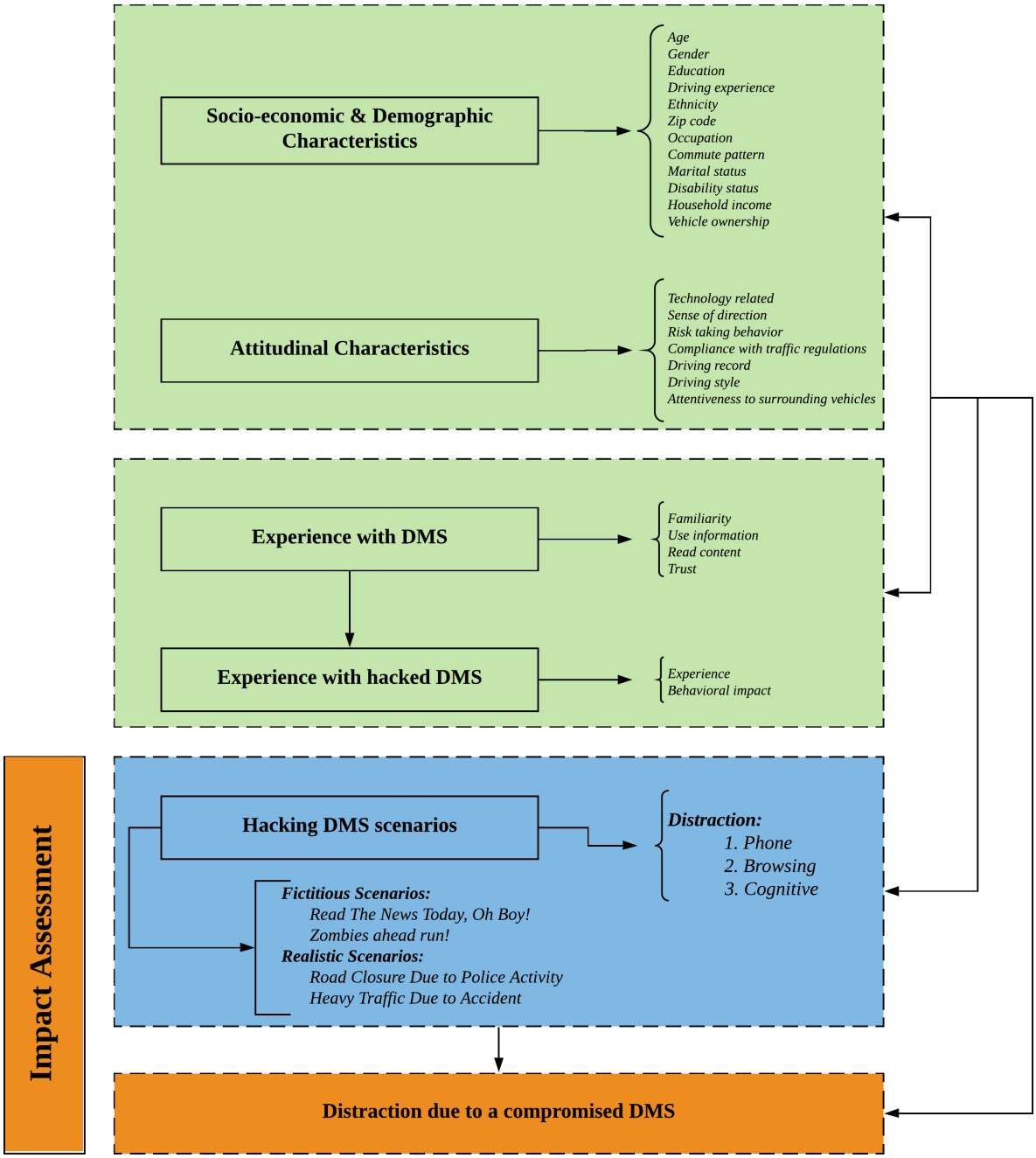


Figure 10 Study structure**.**

In the realistic scenarios, the DMS illustrated traffic-related information. The contents of the DMS were 'Heavy Traffic Due to Accident' (scenario 3: HeavyTraffic), and (2) 'Road Closure Due to Police Activity' (scenario 4: RoadClosure). These scenarios were planned with the objective to cause distraction by stirring drivers to use their phone to check the traffic and find a better route. These messages, on the other hand, could increase drivers' cognitive demand and avert their attention from the driving task. To study distraction behavior of the subjects four folds of data were collected: subjects' socio-economic and demographic characteristics, attitudinal characteristics, experience with DMS and hacked DMS, stated behavior under a compromised DMS, and individuals' risk perception toward the DMS hacking phenomena (Figure 10).

A web-based survey was conducted during November and December 2018, targeting about 5,000 US licensed drivers. We conducted two sets of a pilot study in order to assess the quality of the survey and to optimize the questions format, wording, length, and quantity. We also used domain expert knowledge to shape the final version of the survey prior to the full distribution. We used Amazon Mechanical Turk in order to distribute the survey at the States mentioned above. After confirming the integrity of each assignment, each worker was given a unique code to prevent him/her from retaking the survey.

Based on the study budget and timeline we aimed for roughly 5% of the above-mentioned States population of licensed drivers. During the two-month data collection process, we collected 4,706 web-based responses. We removed about 8.5% of the incorrect responses in the data processing step. The majority of the subjects are from CA, FL, NY, TX which comprise 70% of the data. Females include more than 53% of the data, and most of the participants are between 25 and 44 years old. Majority of the participants hold a Bachelor's degree and above, and about 70% of them have an income of $90k and lower. Important to note that in this study we were able to collect responses from individuals with income higher than $100k as well (about 20% of the data).

As far as the attitudinal and driving characteristics are concerned, majority of the subjects categorized themselves as patient and careful driver, about a quarter of them categorized themselves as anxious drivers and the remaining part claimed to be reckless and careless, and angry and hostile type driver. In addition, we asked a set of question to evaluate subjects' dependency on technology, driving attitude, and sense of direction. For instance, (1) 55% of the subjects indicated that they rely on technology for their daily commute, (2) more than 75% claimed that they would feel more accomplished because of technology, (3) driving is a boring for about 25% of the subjects, (4) only 3% indicated that they are not complying with traffic regulations, and (5) roughly 50% of the subjects would driver the same as the surrounding traffic. For additional information, we refer readers to Table 7.

Table 7 Data description summary.

Variable	Description	Category	Mean	Std. Dev.
Female	–	1: Yes; 0: Otherwise	0.53	0.50
Age	Age (year)	1: 18-24; 2: 25-34; 3: 35-44; 4: 45-54; 5: 55-64; 6: 65-84; 7: >85	2.61	1.20
Ag1824	Age: [18-24]	1: Yes; 0: Otherwise	0.15	0.36
Ag2535	Age: [25-35)	1: Yes; 0: Otherwise	0.40	0.49
Ag3545	Age: [35-45)	1: Yes; 0: Otherwise	0.24	0.43
DrivDur	Driving duration (year)	1: < 1; 2: 1-5; 3: 6-10; 4: 11-15; 5: 16-20; > 20	0.07	0.25
Hssms	Education: Some school and High school	1: Yes; 0: Otherwise	0.09	0.28
ABachlr	Education: Bachelors and above	1: Yes; 0: Otherwise	0.52	0.50
Asian	–	1: Yes; 0: Otherwise	0.09	0.29
Black	Black or African American	1: Yes; 0: Otherwise	0.09	0.29
White	–	1: Yes; 0: Otherwise	0.66	0.47
Student	–	1: Yes; 0: Otherwise	0.06	0.24

VehMotr	Motorcycle / scooter	1: Yes; 0: Otherwise	0.01	0.08
Rural	–	1: Yes; 0: Otherwise	0.13	0.34
Urban	–	1: Yes; 0: Otherwise	0.34	0.47
Dhr	Driving hours (per week)	1: 0; 2: 1-5; 3: 6-10: 4: 11-15: 5: 16-20; 6: 21-25; 7: > 25	4.40	2.05
Dhr1	Driving hours: 0	1: Yes; 0: Otherwise	0.03	0.17
Dhr16	Driving hours: [1-6) hr/week	1: Yes; 0: Otherwise	0.28	0.45
Anxus	Anxious	1: Yes; 0: Otherwise	0.23	0.42
Reckless	Reckless and careless	1: Yes; 0: Otherwise	0.02	0.15
Angry	Angry and hostile	1: Yes; 0: Otherwise	0.04	0.20
Patient	Patient and careful	1: Yes; 0: Otherwise	0.70	0.46
InvAcc	Involved in accident	1: Yes; 0: Otherwise	0.61	0.49
AccDst	Accident due to distraction	1: Yes; 0: Otherwise	0.12	0.33
RlyTech	Rely on technology for daily trips	1: Extremely Unlikely – 5: Extremely Likely	3.23	1.45
Trbldir	Trouble understanding directions	1: Extremely Unlikely – 5: Extremely Likely	2.18	1.17
Lost	Easily get lost in unfamiliar roads	1: Extremely Unlikely – 5: Extremely Likely	3.10	1.29
PFmRt	Prefer taking familiar routes	1: Extremely Unlikely – 5: Extremely Likely	4.30	0.86
Accom	More accomplished because of technology	1: Extremely Unlikely – 5: Extremely Likely	4.03	0.92
Bored	Driving makes me bored	1: Extremely Unlikely – 5: Extremely Likely	2.63	1.16
UpNws	Up-to-date with News	1: Extremely Unlikely – 5: Extremely Likely	3.78	1.02
Blinker	I use blinker when changing the lanes	1: Extremely Unlikely – 5: Extremely Likely	4.64	0.73
AtnVeh	Pay attention to vehicles around me	1: Extremely Unlikely – 5: Extremely Likely	4.70	0.62
TrfReg	Comply with traffic regulations	1: Extremely Unlikely – 5: Extremely Likely	4.52	0.74
SmArnd	Driving the same way as the others	1: Extremely Unlikely – 5: Extremely Likely	3.36	1.09
Grec	I have a good record of driving	1: Extremely Unlikely – 5: Extremely Likely	4.46	0.81
Chctrf	Check traffic before hitting the road	1: Extremely Unlikely – 5: Extremely Likely	3.19	1.38
Trstch	I trust technology to assist in my travel	1: Extremely Unlikely – 5: Extremely Likely	4.17	0.94
Dfam	Familiarity with DMS	1: Not familiar at all – 5: Extremely familiar	3.96	1.02
Dsee	See DMS in daily commute	1: Never – 5: Always	3.02	1.21
Dread	Read DMS in daily commute	1: Never – 5: Always	4.28	0.89
Vtg	Trust in DMS	Continues (1–5)	4.09	0.82
Vtg68	60-80% trust in DMS	1: Yes; 0: Otherwise	0.30	0.46

Seven types of distraction (different combination of manual, visual, and cognitive distraction) is considered in this study: call/text someone (CalTxt), take picture of the DMS (Pic), browse internet/social media (Internet), talk to a passenger (Talk), mind wandering (MindW), look at surrounding traffic or scenery (Look), and pick up on radio (Radio). Overall, above 36%, and 21% of the respondents indicated that a compromised DMS with political/funny, and realistic context, respectively, could cause distracted driving.

In reference to the ReadNews DMS hacking scenario, results indicated that overall: (1) 24% of the individuals are likely to adjust their radio, (2) about 60% of the individuals are likely to talk to the other passengers, (3) 14% of the individuals are likely to use their cell phones to call or text someone, (4) about 30% of the individuals are likely to take a picture of the DMS, (5) 22% of the individuals are likely to browse social media or news in accordance with the message, (6) about 32% of the individuals are likely to mind wandering, and (7) more than fifth of the individuals are likely to look at the other vehicles to observe their reaction to the DMS. The stats for the Zombieahead scenario are 18%, 70%, 33%, 57%, 19%, 38%, and 31%, respectively.

As far as the realistic scenarios are concerned, in respect to the third scenario (HeavyTraffic), in average, (1) about 40% of the subjects indicated that they would engage in one of the cognitive distraction activities (i.e., talk to passenger, mind wandering, and look around), (2) more than 10% would use their phone, and (3) about 45% of the subjects would pick up on the radio to seek more knowledge about the advisory information. In respect to the last scenario, in average, about half of the subjects would become engage in cognitive activities, more than 45% would engage in manual distraction activity to browse for news from radio or internet, and about 20% would call or text someone about the information provided on the sign. Clearly, the data shows that all four scenarios have a potential to engage drivers in a distractive activity and could

compromise the safety of the transportation. Figure 11 illustrates the impact of various forged messages on distracted driving.

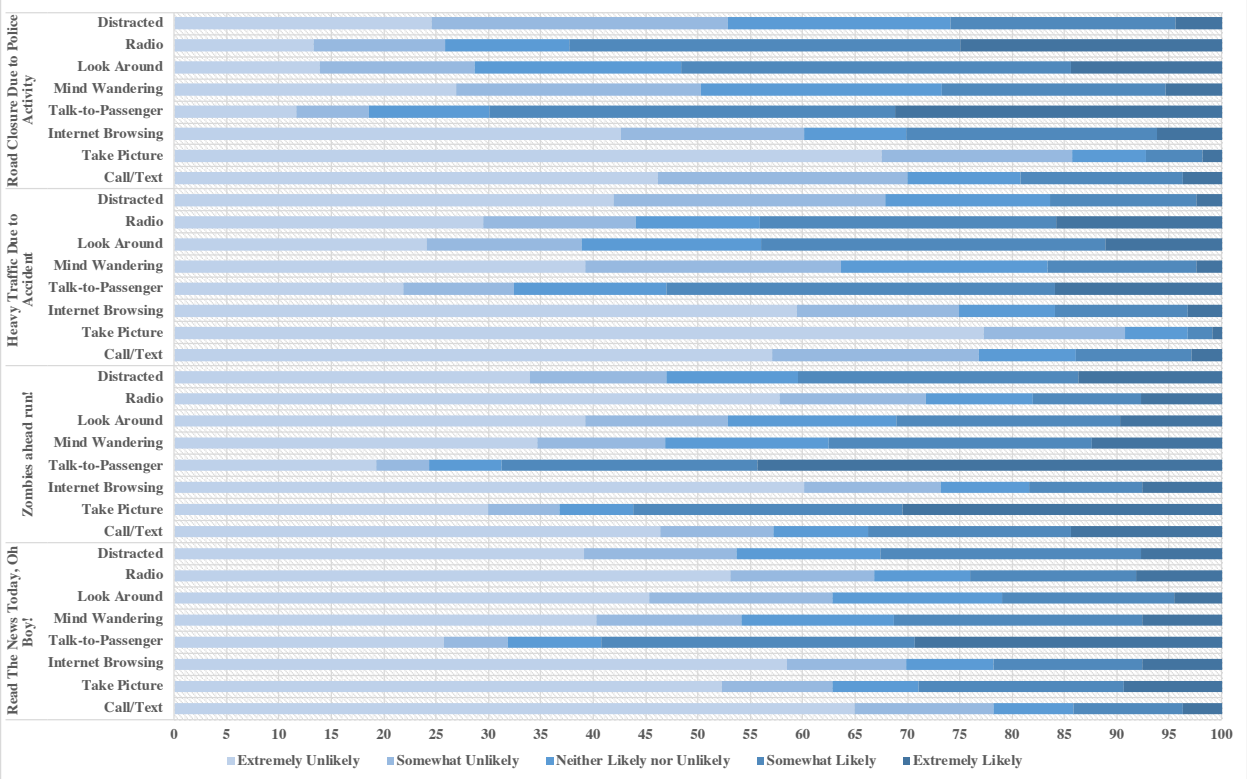


Figure 11 Road users distraction choice and behavior under fictitious hacking scenarios.

4.3.2 Factor analysis

In order to construct significant latent factors from attitudinal and distraction-related variables, we conducted an explanatory factor analysis (EFA). This statistical analysis assists us to identify a group of unobserved latent factors that could account for covariance among observed variables (indicators). In this study, we conducted the EFA using Maximum Likelihood (ML) method with Geomin oblique type rotation. As far as the attitudinal latent factors are concerned the result of the analysis identified three factors. These factors are tech-friendly drivers (L-Tech), driving habit (L-DriHabt), and direction understanding (L-Direct) related factors. The L-Tech regards to the drivers who rely and trust in technology and tend to use it in order to find an efficient route in their daily commute. The L-DriHabt concerns with drivers who have a good record of driving, comply with traffic regulations and are attentive to their surrounding traffic. Moreover, the L-Direct latent factor attempts to cluster subjects that have difficulties understand direction, especially in an unfamiliar route. The result of the factor loading for both of the latent factors is provided in Table 8.

Table 8 Factor loading: explanatory factor analysis (attitudinal factors).

Indicators	Attitudinal Latent Factors		
	L-DriHabt	***L-Tech***	***L-Direct***
Use blinker when changing the lanes	**0.712**	0.187	0.012
Pay attention to vehicles around me	**0.794**	0.176	-0.068
Comply with traffic regulations	**0.706**	0.133	0.006
Good record of driving	**0.599**	0.114	-0.109
Accomplished because of technology	0.274	**0.527**	0.149
Trust technology to assist in travel	0.242	**0.649**	0.250
Rely on technology for daily trips	0.006	**0.627**	0.203
Check traffic before hitting the road	0.083	**0.350**	-0.036
Trouble understanding directions	-0.174	0.135	**0.595**
Get lost easily in an unfamiliar route	0.010	0.282	**0.844**
Prefer Familiar Routes	0.338	0.193	**0.329**
Driving is boring	-0.112	0.059	0.223
Up-to-date with News	0.266	0.116	-0.181
Driving the same way as the others	0.130	0.204	0.074
Trust drivers around	-0.059	0.075	-0.060

As far as the distraction-related latent factors are concerned, the EFA analysis identified three factors (Table 9). These factors include phone use (L-Phone), news and social media browsing (L-Browsing), and attention-averting (L-Cognitive) latent factors. The L-Phone construct is related to the observed variables which indicate whether drivers tend to use their cellphone to call/text someone, take a picture, or check social media and news in response to the displayed information. The L-Browsing latent factor regards to the drivers who tend to gain more knowledge of the given information from radio or by browsing social media and news with their cellphone. It should be noted that L-Phone and L-Browsing latent factors have browsing variable (Social media or news browsing) in common. The L-Cognitive latent factor includes observed variables that represent activities that avert drivers' attention from their primary task (driving). These variables include looking at the scenery and surrounding traffic, thinking of something other than driving (mind wandering), and talking to the vehicle passengers about the forged information. Table 8 and Table 9 outlines the results of the EFA analysis. We accounted for the root mean square error of approximation (RMSEA) to test the EFA goodness of fit. For all five EFA models, the results indicated the RMSEA of lower than 0.08, meaning that EFA models satisfy the goodness of fit criteria.

Table 9 Factor loading: explanatory factor analysis under each scenario (distraction related factors).

Indicators	Read The News Today, Oh Boy!			Zombies ahead run!			Heavy Traffic Due to Accident			Road Closure Due to Police Activity		
	L-Phone	*L-Browsing*	*L-Cognitive*	*L-Phone*	*L-Cognitive*	*L-Browsing*	*L-Phone*	*L-Cognitive*	*L-Browsing*	*L-Phone*	*L-Cognitive*	*L-Browsing*
Call/Text someone	**0.802**	0.256	0.423	**0.749**	0.388	0.448	**0.600**	0.223	0.367	**0.665**	0.188	0.271
Take picture of sign	**0.711**	0.163	0.385	**0.767**	0.417	0.238	**0.853**	0.166	0.203	**0.721**	0.210	0.068
Social media or news browsing	**0.615**	**0.408**	0.435	**0.526**	0.282	**0.723**	**0.551**	0.207	**0.575**	**0.625**	0.224	**0.408**
Talk to passengers about sign	0.394	0.180	**0.528**	0.460	**0.583**	0.140	0.130	**0.410**	0.400	0.202	**0.251**	0.399
Mind wandering	0.455	0.240	**0.840**	0.442	**0.764**	0.310	0.320	**0.649**	0.212	0.258	**0.780**	0.158
Look at scenery/traffic	0.405	0.271	**0.553**	0.380	**0.626**	0.481	0.143	**0.591**	0.237	0.211	**0.418**	0.333
Check radio	0.467	**1.460**	0.439	0.315	0.257	**0.875**	0.184	0.264	**0.659**	0.277	0.118	**0.539**

It should be noted that we tested the results of a 2-factor extraction for distraction-related factors, but the model did not satisfy the goodness of fit criteria. To confirm the results of the EFA models we developed confirmatory factor analysis (CFA) models for each scenario. We developed the CFA models using the ML method in order to test whether the data fit the measurement models resulted from the EFA analysis. The value of the RMSEA was found equal to 0.063, 0.067, 0.066, and 0.063 (< 0.08), for scenario 1 to 4, respectively. That is, the identified constructs presented in Table 8 and Table 9 are a good fit to the data.

4.3.3 Structure equation model approach

In order to model the outcome variables of this study, we developed four structural equation modeling (SEM) for each of the scenarios discussed before. To assess the impact of drivers' attentional overload on distracted driving, we developed four SEM models for the four scenarios of this study. The outcome variable is an ordinal variable comprises of five categories that indicate subjects' perception of the distracted driving at the presence of a compromised DMS. The categories of the outcome variables include extremely unlikely, somewhat unlikely, neither likely nor unlikely, somewhat likely and extremely likely. Higher values are associated with the subjects that found DMS hacking phenomena with a higher likelihood to cause a distraction while driving. We used factor analysis in order to form meaningful constructs from distraction activities. The result of the factor analysis model is discussed in the previous section (4.3.2).

We modeled distracted driving using SEM approach by taking into account a set of hypotheses regarding the impact of subjects socio-economic and demographic and attitudes toward L-Phone L-Browsing, and L-Cognitive latent variables and subjects' perception of the distracted driving outcome variable. The conceptual framework of the proposed model is illustrated in Figure 12. We tested the association of two sets of observed and unobserved (latent factor) variables and distraction latent variables (i.e., L-Phone L-Browsing, and L-Cognitive) and the outcome variable. The descriptive stat of the observed variables is provided in Table 7. Also, discussion related to the unobserved variables used in this modeling approach can be found in the previous section and Table 8.

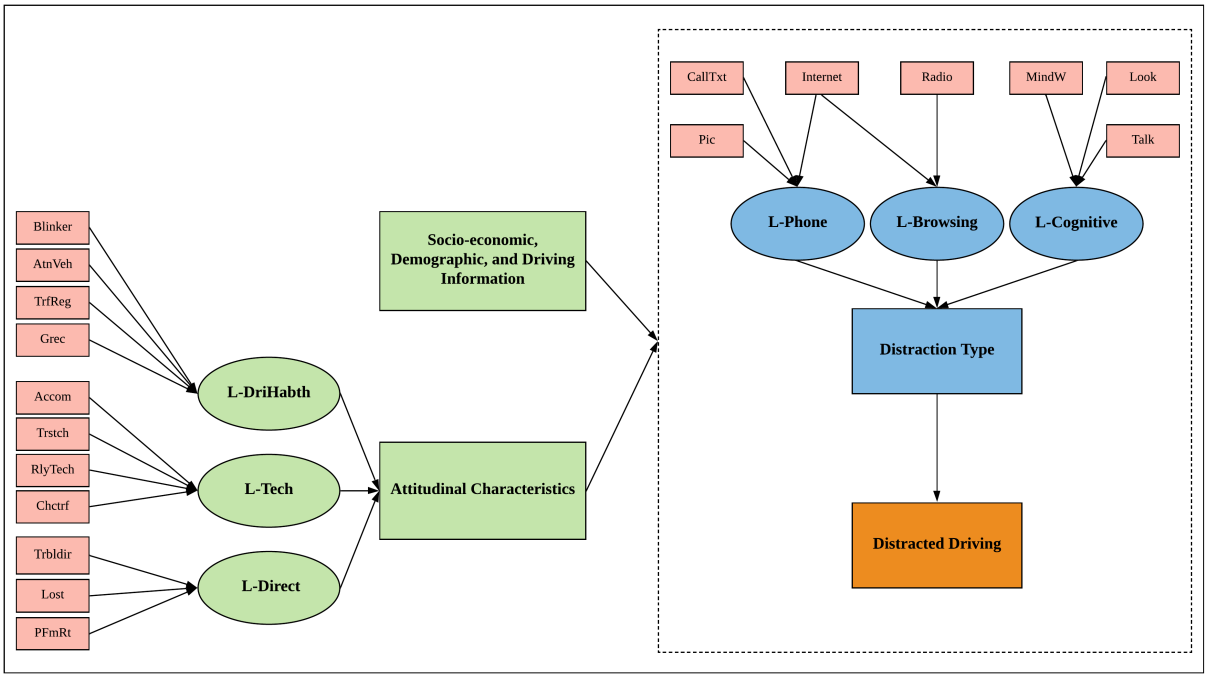


Figure 12 SEM model conceptual framework

The SEM modeling approach and variable selection comprise of four main steps. These steps include:

(1) Conducting bivariate regression between distracted driving, indicator variables and the observed variables of this study,

(2) We tested background variables and latent factors (L-Tech, L-DriHabt, L-Direct) association with the distraction related latent factors (e.g., L-Phone) and the distracted driving,

(3) We used the two-tailed t-test to assess the significance level of the model variables. Direction effects and variables that were significant at 90% confidence interval were only inserted.

(4) Among highly correlated variables we kept the variable that resulted in a model with better goodness of fit to the data. We judged by comparing the Akaike Information Criterion (AIC) value between the two models.

4.4 Results

To explore hacked DMS phenomena we investigated the impact of the bogus information on road users in three folds: (1) determinants of distracted driving, (2) association of background variables, attitudinal latent factors with the three distraction latent factors, and (3) determinants and causation factors of distracted driving under a compromised DMS. We hypothesized that a hacked DMS would increase drivers' attentional overload and increase the chance of driving under distraction. We developed four SEM models with ordinal outcome variable to investigate the hypothesis of this study. Following sections provide in-depth discussion over the modeling result.

4.4.1 Distraction model

To explore the determinants of distraction perception at the presence of a hacked DMS we developed an SEM model by taking into account five unobserved latent factors. To construct the model, we tested the association between latent factors and the likelihood of distracted driving. Out of the six latent factors, we found L-Phone, L-Cognitive, L-Browsing, and L-Direct associated with the risk of distraction at the 90% confidence interval. We identified a significant link between L-Tech and L- DriHabt latent factors and the three distraction types. Table 10 and Table 11 outline the results of the SEM models developed for the 4 scenarios of this study.

Three attitudinal latent factors were identified as significant in the SEM model: L-Tech, L-DriHabt, and L-Direct. The L-Tech comprises of indicators that explain subjects' attitude toward technology. The L-Tech latent includes four indicators: Accom, RlyTech, Trstch, and Chctrf. These variables indicating subjects' dependency on technology and the extent technology (e.g., Google Map) could assist them in their day to day commute. For instance, Chctrf explores whether participants of this study would check the traffic before starting their commute. The Trstch, RlyTech and Accom variables indicated the highest contribution to the L-Tech latent factor. L-Direct represents subjects with trouble finding their direction, who prefer familiar routes for their commute and get lost easily in an unfamiliar area. This type of drivers is likely to use secondary sources such as GPS device to get assistant for their trips. Also, at the presence of traffic-related advisory information that suggests travelers change their route this type of drivers might stay on their planned routes.

L-DriHabt, on the other hand, explore Subjects' Driving habits. This latent incorporates information concerning subjects' compliance with traffic regulation (TrfReg), their traffic records (Grec), and their attentiveness to the surrounding traffic (AtnVeh). The AtnVeh, and Blinker designated the highest contribution to the L- DriHabt latent factor. The attitudinal factors represent a total of 24.6% to 53.57% of the variance. We expect this type of drivers to follow safety measures while they are approaching a DMS with a political or funny related content. That is, we hypothesize that drivers with a good habit of driving are less likely to become involved in a distractive activity. While, we expect that tech-friendly subjects, to use their cellphones or vehicles infotainment system more frequently in response to the fabricated information. We argue that these type of drivers are more prone to attention overload and risky driving behaviors.

For each of the scenarios, we developed an SEM model separately. To decide on models' goodness of fit, we used McFadden's Pseudo R-Square using the following equation (E.q. 1). In which, LL_{fit} is a log likelihood value for the fitted model and LL_{Null} is the log likelihood value of the null model. Closer this value is to one, the better the model fits the data. We estimated the McFadden's Pseudo R-Square equal to 0.36, 0.4, 0.3, and 0.32, for scenario 1 through 4, respectively. The reported values indicate that models have satisfactory goodness of fit indices.

$$R^2_{McFadden} = 1 - {LL_{fit}}\Big/{LL_{Null}} \quad \text{(E.q. 1)}$$

As far as the realistic scenarios' models are concerned, in average distraction-related latent factors explain 50% of the "call/Text someone" indicator variance, 54.3% of its "take picture of sign" indicator, 42% of its "social media or news browsing" indicator variance, and 84.1% of its "check radio" variance. The attention-averting latent factors also explain 21%, 54.7%, and 27% variance of its "Talk to passengers about sign", "Mind wandering", "Look at scenery/traffic" indicators, respectively.

As far as the fictitious scenarios are concerned, the L-Cognitive latent factors explain, in average, 62.6% of the "Mind wandering" indicator variance, 24.3% of its "talk to passengers about sign" indicator, and 33.3% of its "look at scenery/traffic" indicator. The other two latent factors explain 50.6%, 59.2%, 40%, and 96% variance of its "call/Text someone", "take picture of sign", "social media or news browsing", and "check radio" indicators, respectively.

Other than the last scenario we did not identify a significant relationship between attitudinal latent factor and likelihood of distraction. Subjects with direction trouble indicated that "Road Closure Due to Police Activity" message would increase the likelihood of their distraction while driving. As depicted in Table 11 we can discern that, in all the scenarios, the attention-averting activities contribute the most to the likelihood of distracted driving. The L-Phone and L-Browsing latent factors indicated a mixed impact on distracted driving. For the ReadNews scenario, distracting activities involving phone use have the higher impact on distracted driving. While, in the realistic scenarios, L-Browsing latent factor contribute with higher degree to the risk of distraction.

Interestingly, in the second scenario (Zombieahead) L-Browsing latent factor did not have a significant contributory effect on distraction. The attention-averting latent factor plays almost a similar role in explaining the risk of distraction under a hacked DMS, for all scenarios. Its impact on distraction is the highest with respect to the first scenario and is the lowest with respect to the RoadClosure scenario.

Table 10 SEM unobserved latent factors.

Latent	Exogenous variables	Read The News Today, Oh Boy!		Zombies ahead run!		Heavy Traffic Due to Accident		Road Closure Due to Police Activity	
		Estimate	*Est./S.E.*	*Estimate*	*Est./S.E.*	*Estimate*	*Est./S.E.*	*Estimate*	*Est./S.E.*
Distraction Related factors									
L-Phone	Call/Text someone	*Constant*		*Constant*		*Constant*		*Constant*	
	Take picture of sign	1.168	35.960	0.876	39.420	0.957	32.529	0.922	28.858
	Social media or news browsing	0.646	27.502	0.694	36.458	0.866	27.050	0.946	27.627
L-Cognitive	Look at scenery/traffic	*Constant*		*Constant*		*Constant*		*Constant*	
	Mind wandering	1.685	29.668	1.427	36.368	1.138	24.414	1.250	19.385
	Talk to passengers about sign	1.258	25.773	0.973	29.497	0.794	19.669	0.674	14.878
L-Browsing	Social media or news browsing	*Constant*		–		*Constant*		*Constant*	
	Check radio	2.267	37.026			3.830	17.028	3.451	10.909
Attitudinal Related factors									
L-Tech	Accomplished because of technology	*Constant*		*Constant*		*Constant*		*Constant*	
	Trust technology to assist in travel	1.282	24.563	1.284	24.665	1.346	25.382	1.334	25.840
	Rely on technology for daily trips	1.345	21.312	1.335	21.446	1.399	22.042	1.406	21.978
	Check traffic before hitting the road	0.653	12.413	0.642	12.364	0.636	12.058	0.653	12.255
L-DriHabt	use blinker when changing the lanes	*Constant*		*Constant*		*Constant*		*Constant*	
	Pay attention to vehicles around me	0.939	42.314	0.938	42.283	0.945	42.516	0.941	42.443
	Comply with traffic regulations	1.007	39.411	1.004	39.420	1.000	39.479	1.003	39.460
	good record of driving	0.932	33.641	0.930	33.622	0.934	33.765	0.936	33.776
L-Direct	Get lost easily					*Constant*		*Constant*	
	Prefer Familiar Routes	–		–		0.207	13.774	0.215	15.852
	Trouble understanding directions					0.507	15.984	0.530	20.034

Note: All the estimated are significant at the 90% confidence interval.

The Tech-friendly and L- DriHabt latent factors did not have a significant association with the distraction likelihood outcome variable of the SEM model. We also tested whether those who would slow down or stop under the compromised DMS would perceive the risk of distraction under a compromised DMS high. The estimates indicated that slow down behavior positively correlated with the distraction risk while the stopping behavior did not have a significant association with the distraction risk. In addition, we explored the correlation between slow down and stop speed choices with distraction latent factors, and found a significant linkage between those. Meaning that as a result of drivers' attentional overload they tend to lower their speed or stop their vehicle to manage the excessive cognitive demand. This finding is consistent with previous studies [22, 155, 156]. In the following section, we provide more details on the models' results and findings.

4.5 Discussion

In this study, we focused on the scenarios where DMS display unrealistic (i.e., fictitious) and realistic (i.e., traffic-related) information. We aim to understand to what extent the drivers are attentive to the supplied information, and how this attention increases the likelihood of distraction while driving. In this study, we argue that a compromised DMS not only undermines the reliability of the ITS system, could engineer drivers' decisions by persuading them with fake information.

While developing the SEM models for each scenario, we account for the association between explanatory variables, attitudinal latent factors, distraction latent factors and the outcome variable of this study–likelihood of distracted driving under a compromised DMS. In the modeling process, we consider the collinearity between variables in order to not include two or more highly correlated variables in one model. The final models only comprise of significant variables (90% confidence interval) and latent factors that ensure the model's goodness of fit. Table 11 represents the SEM results of all the scenarios, and indicate the linkage between the observed and unobserved variables of this study.

As far as the sign and the coefficient of the observed and unobserved variables are concerned they are congruous with the theoretical expectations. We found several of the explanatory variables of this study with a direct effect on two or three distraction constructs. These variables include, but not limited to race, education level, driving experience, age, speed choice behavior, driving style, and subjects general trust in DMS information. In addition, we found several background variables with a significant correlation with the likelihood of distraction while driving. The impact of the variables that are common in different scenarios models are mainly similar (Figure 13). In scenario 1, 3, and 4 all the attention-averting related constructs were found to have a contributory impact on the distraction likelihood. While the distraction related constructs have a similar impact, the magnitude is different among different scenarios. The L-cognitive construct has its highest positive impact on distraction risk in the first scenario (i.e., ReadNews). Its impact is the lowest in respect to the last scenario where subjects are given fabricated information regarding road closure due to police activity.

The effect of the other latent factors on the outcome variable of different scenarios is more diverge than the L-Cognitive. In respect to the fictitious scenario 1, the subjects who would use their cellphone increase the risk of distracted driving more than the ones seeking the news via radio. We did not identify a significant association between the L-Browsing construct and the likelihood of distraction. For the case of the realistic scenarios, subjects are rather to gain

secondary knowledge regarding the traffic condition through radio, social media, or the internet. This distinction is higher for the last scenario where a DMS displays "Road Closure Due to Police Activity". That is, L-Browsing latent factor has more impact on the risk of distraction compare to the L-Phone latent factor.

Interestingly, only one of the attitudinal latent factors has a significant linkage with distraction while driving. The L-Direct factor (drivers with direction trouble) indicated a positive contribution to the outcome variable of the last scenario. It should be noted, that its impact is the lowest compared to the distraction-related latent factors.

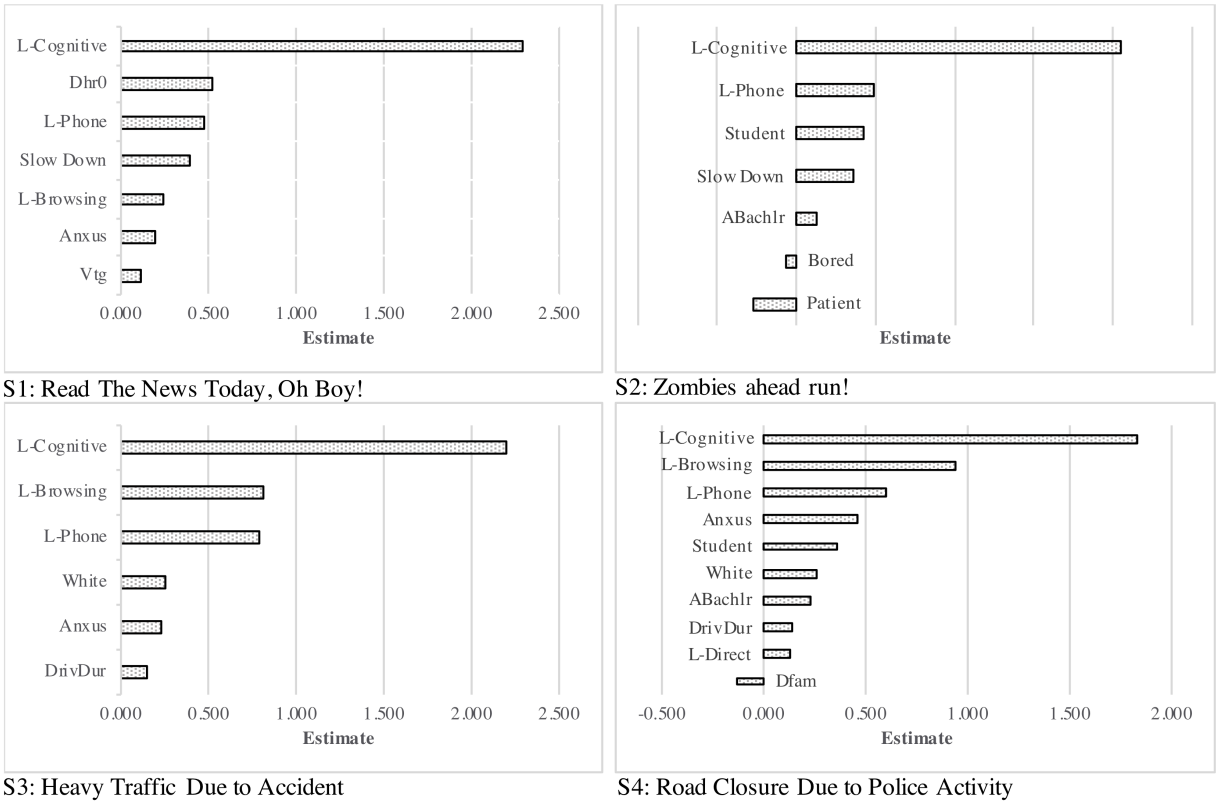


Figure 13 Distracted driving under different scenarios

Observed variables also contribute to the subjects' risk of distraction while driving. We found that students are more likely to become involved in distracted driving behavior in both scenario 2 and 4. Drivers with anxious driving style (i.e., those who feel alertness and tension during driving), and those with the education of Bachelor's degree and higher are more prone to the distracted driving behavior. The anxious drivers would distract the most in the last scenario where the road is closed. Experienced drivers (those with many years of driving experience), and those with high trust in DMS information are more likely to increase the risk of distraction. Subjects with white race would also increase the risk of distracted driving compared to the other races. The SEM models of the scenario 2 and 4 identified 3 explanatory variables with a negative effect on distracted driving. These variables relate to (1) patient and careful drivers, (2) subjects that feel driving is a boring activity, and (3) those subjects who are more familiar with the DMS. Among these subjects, those who are patient and careful drivers have the highest negative impact and those who perceive driving as a tedious task have the least negative contribution to the risk of distracted driving.

Furthermore, we tested the relationship between distraction risk and subjects' choice of speed. The hypothesis is that under a compromised DMS, drivers tend to slow down or stop in order to react to the supplied information. As far as the fictitious scenarios are concerned, we indicated a positive correlation between slow down behavior and risk of distraction. This result is consistent with theoretical anticipation. We did not find a significant association between choice of speed and distracted driving behavior in realistic scenarios. Figure 13 provides more detail regarding the impact differences of the observed and unobserved variables between the four scenarios of this study.

4.5.1 Distraction type: phone use

In all of the scenarios, attitudinal latent variables were found significantly correlated with the L-Phone construct. Regardless of the scenarios, tech-friendly drivers are the ones who would use their cellphones to take a picture, call text someone, or brows social media. The L-Tech latent factors have the highest positive impact on the L-phone distraction construct in regard to the second scenario where a DMS warns drivers of a Zombie attack. Interestingly, this result is consistent with drivers real-word encounter [25]. That is, in reaction to a similar message, drivers are likely to slow down, or stop to take a picture of the sign. This behavior could cause unsafe traffic condition as a consequence of frequent braking, and lane changing behaviors. Drivers with a good record of driving and those who comply with traffic regulation are less likely to engage in phone use related activities. The L-DriHabt latent factor, in all scenarios, has negative linkage to the L-phone construct. This negative effect is the highest for subjects at the presence of the "Road Closure due to Police activity" sign. These type of drivers are more prone to the fictitious messages rather realistic ones (Figure 14).

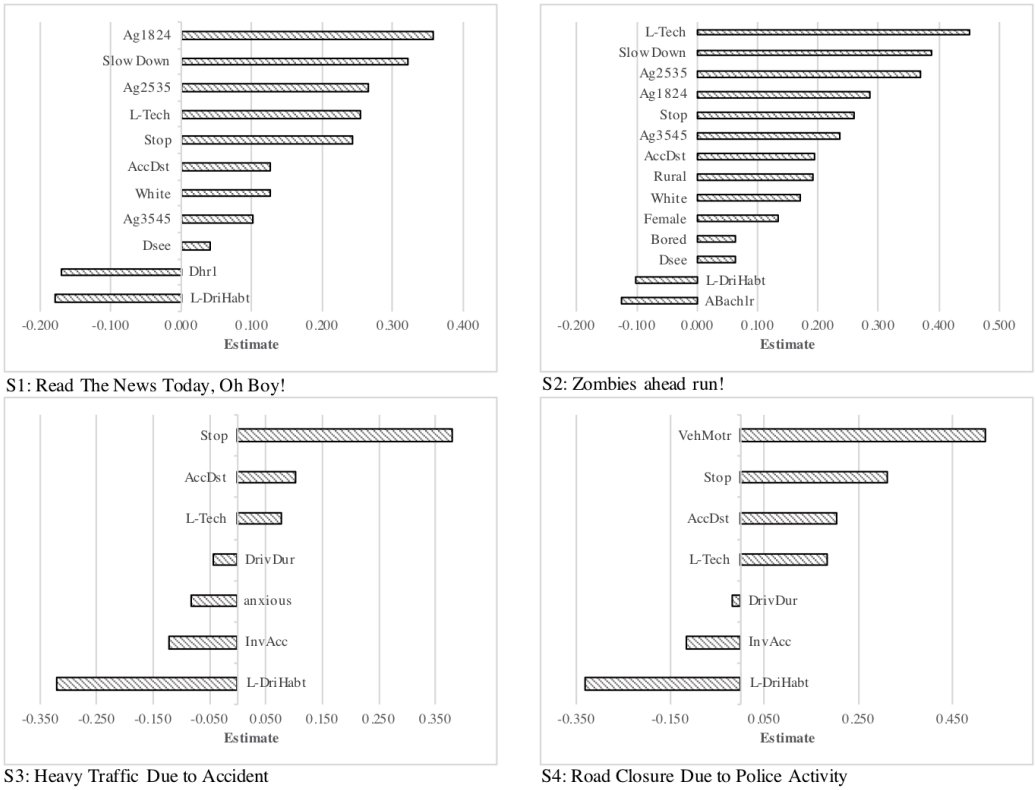


Figure 14 L-Phone distraction under the 4 scenarios

Table 11 Determinants of distraction.

Latent Variables	Read The News Today, Oh Boy!			Zombies ahead run!			Heavy Traffic Due to Accident			Road Closure Due to Police Activity		
	Estimate	Est./S.E.	P-Value	Estimate	Est./S.E.	P-Value	Estimate	Est./S.E.	P-Value	Estimate	Est./S.E.	P-Value
Distraction												
L-Phone	0.475	8.756	0.000	0.489	12.091	0.000	0.795	12.402	0.000	0.597	11.070	0.000
L-Cognitive	2.289	20.717	0.000	2.046	23.891	0.000	2.200	18.281	0.000	1.829	15.023	0.000
L-Browsing	0.246	4.045	0.000		–		0.814	7.384	0.000	0.942	6.553	0.000
L-Direct		–			–			–		0.126	3.815	0.000
ABachlr		–		0.129	1.851	0.064		–		0.230	3.563	0.000
DrivDur		–			–		0.146	5.723	0.000	0.134	5.252	0.000
White		–			–		0.249	3.081	0.002	0.257	3.471	0.001
Patient		–		-0.277	-3.621	0.000		–			–	
Bored		–		-0.071	-2.250	0.024		–			–	
Student		–		0.428	2.920	0.004		–		0.360	2.586	0.010
Anxus	0.193	2.382	0.017		–		0.234	2.664	0.008	0.461	6.078	0.000
Dfam		–			–			–		-0.133	-4.130	0.000
Dhr0	0.521	2.590	0.010		–			–			–	
Vtg	0.108	2.580	0.010		–			–			–	
Slow Down	0.389	10.500	0.000	0.353	10.590	0.000		–			–	
L-Phone												
L-Tech	0.253	6.969	0.000	0.451	9.056	0.000	0.078	2.989	0.003	0.183	5.388	0.000
L-DriHabt	-0.178	-5.112	0.000	-0.101	-2.164	0.030	-0.321	-12.407	0.000	-0.332	-10.370	0.000
Female		–		0.135	3.450	0.001		–			–	
DrivDur		–			–		-0.044	-5.653	0.000	-0.020	-2.088	0.037
Ag1824	0.357	7.167	0.000	0.286	4.173	0.000		–			–	
Ag2535	0.265	6.724	0.000	0.370	6.844	0.000		–			–	
Ag3545	0.102	2.390	0.017	0.237	4.043	0.000		–			–	
ABachlr		–		-0.125	-3.144	0.002		–			–	
anxious		–			–		-0.083	-3.365	0.001		–	
White	0.126	4.138	0.000	0.171	4.079	0.000		–			–	
Rural		–		0.191	3.278	0.001		–			–	
Dhr1	-0.169	-1.969	0.049		–			–			–	
VehMotr		–			–			–		0.520	3.018	0.003
InvAcc		–			–		-0.123	-5.187	0.000	-0.115	-3.821	0.000
AccDst	0.126	2.428	0.015	0.193	3.221	0.001	0.103	3.123	0.002	0.203	4.772	0.000
Dsee	0.040	3.442	0.001	0.064	3.957	0.000		–			–	
Bored		–		0.064	3.802	0.000		–			–	
Slow Down	0.322	21.406	0.000	0.388	20.596	0.000		–			–	
Stop	0.243	9.875	0.000	0.260	8.681	0.000	0.379	24.088	0.000	0.310	19.720	0.000
L-Cognitive												
L-Tech	0.210	6.976	0.000	0.285	8.273	0.000	0.121	3.457	0.001	0.196	5.880	0.000
L-DriHabt	-0.115	-4.136	0.000		–		-0.163	-5.113	0.000	-0.100	-3.424	0.001

L-Direct		–			–		0.053	3.879	0.000	0.035	2.707	0.007
Ag1824	0.132	3.955	0.000		–			–			–	
Hssms	-0.207	-4.969	0.000	-0.151	-2.914	0.004	-0.219	-4.704	0.000	-0.204	-4.725	0.000
asian		–			–		0.158	3.116	0.002		–	
black		–			–			–		-0.126	-2.760	0.006
White	0.187	7.441	0.000	0.187	6.006	0.000	0.145	4.503	0.000	0.103	3.414	0.001
Urban		–			–		-0.055	-1.965	0.049		–	
DrivDur		–			–			–		-0.050	-5.389	0.000
Dhr		–			–		-0.014	-2.111	0.035	-0.016	-2.744	0.006
Dhr16	0.101	3.856	0.000	0.111	3.417	0.001		–			–	
Vtg6080		–		0.075	2.375	0.018		–		0.054	2.084	0.037
Patient		–		-0.143	-4.376	0.000		–			–	
Anxus	0.106	3.725	0.000		–		0.081	2.437	0.015		–	
InvAcc		–		0.057	1.894	0.058		–			–	
AccDst	0.114	2.669	0.008		–		0.074	1.850	0.064		–	
Bored	0.047	4.606	0.000	0.082	6.318	0.000		–		0.062	5.823	0.000
Slow Down		–			–		0.078	6.222	0.000	0.116	8.764	0.000
Stop		–			–		0.179	10.579	0.000	0.096	7.042	0.000
L-Browsing												
L-Tech	0.074	3.585	0.000					–		0.035	2.375	0.018
L-Direct		–						–		-0.020	-3.391	0.001
DrivDur		–					0.033	6.015	0.000		–	
Black		–					-0.070	-3.499	0.000		–	
Urban	-0.051	-2.724	0.006					–			–	
Student		–					-0.046	-1.808	0.071		–	
Hssms		–			–			–		-0.040	-1.940	0.052
Reckless		–						–		-0.116	-2.928	0.003
Dfam		–						–		0.025	4.127	0.000
UpNws	0.024	2.827	0.005					–			–	
Slow Down	0.150	15.121	0.000				0.035	5.302	0.000	0.072	8.477	0.000
Stop	0.144	9.630	0.000				0.079	8.417	0.000	0.039	5.636	0.000
Thresholds (cut-points)												
Cut 1	1.876	8.773	0.000	0.243	3.999	0.000	2.192	10.688	0.000	0.576	2.630	0.009
Cut 2	2.970	13.672	0.000	0.643	10.524	0.000	3.982	18.080	0.000	2.317	10.234	0.000
Cut 3	3.973	17.874	0.000	0.992	16.208	0.000	5.301	22.631	0.000	3.595	15.303	0.000
Cut 4	6.594	26.776	0.000	1.891	29.909	0.000	7.978	28.833	0.000	6.078	23.360	0.000

In both fictitious scenarios, age has a significant impact on phone use related activities. In respect to the first scenario, subjects with age of 18 to 24 years old have the highest chance to become involved in distraction involving their phone. While, in the second scenario, this is true for those who age between 25 and 34 years old. Age is not a contributory variable in realistic scenarios. Female and White subjects and those who live in a rural area are likely to use their phone under the fictitious scenarios. We did not find a significant correlation between these type of drivers and L-Phone construct in the realistic scenarios. Experienced drivers and those drivers with less than 1 driving hour in a week have a negative association with the L-Phone latent factor.

We found two interesting results involve the subjects that had previous accident experience. Those who were involved in an accident in general, were less likely to use their phone under realistic scenarios. But the ones who were involved in an accident involving a distraction would contribute positively to the L-Phone latent factors. In addition to the aforementioned observed and unobserved variables, we investigated the direct correlation between speed variation and L-Phone latent factors. The models result indicate that subjects' slow down and stopping behavior is highly correlated with the phone use activity. Meaning that subjects are highly likely to change their speed in response to the fabricated messages. This behavior could occur due to several reasons. As far as the fictitious scenarios are concerned these reasons include (1) take picture of the sign, (2) call/text someone about the sign, and (3) browse social media in order to upload the information about the hacked DMS. However, with respect to the realistic scenarios, the rescans could be different. The subjects might reach to their phone in order to check the traffic condition, and also find a more efficient route to minimize their commute delay. Figure 14 illustrates the similarities and differences of different scenarios determinants.

4.5.2 Distraction type: cognitive

Cognitive-related distractions were found with the highest positive effect on distracted driving risk. That is, it is imperative to know what type of driver is more likely to become involved in such distraction activity. Similar to the L-Phone latent factor, tech-friendly drivers (subjects associated with L-Tech) are more prone than other drivers to engage in a cognitive type of distraction activity. This could be thinking about something other than driving (mind wandering), looking at the surrounding traffic or scenery or talking to a passenger.

We found L-DriHabt with negative impact on the L-Cognitive construct in three of the scenarios. Meaning that drivers who respect traffic regulations are not likely to pay attention to something other than driving. Interestingly, in the realistic scenarios, subjects with trouble in finding their direction in an unfamiliar road, and those who get lost easily are more prone to this type of distraction. This is mainly due to the fact that this type of drivers is willing to commute through familiar routes to lower the risk of longer travel times.

White, anxious drivers, and drivers with high trust in DMS (60-80% trust) would involve in a cognitive type of distraction under both fictitious and realistic scenario. it is very likely for subjects who were involved in an accident and for those that distraction was the reason of their accident to become involved in a related cognitive distraction. In addition, Asians and subjects who see driving as a tedious task would positively contribute to the L-Cognitive latent factor.

The modeling result also indicates that several variables have a negative association with the L-Cognitive construct. These variables define subjects who are (1) patient and careful, (2) have low education, (3) black, (4) live in an urban setting, and (5) experienced drivers. Hssms has a

similar negative impact on L-Cognitive in all the scenarios. Its impact is the highest regarding the first and third scenarios. In addition, with respect to the fabricated realistic scenarios, those subjects with higher commute hours are less likely to become distracted.

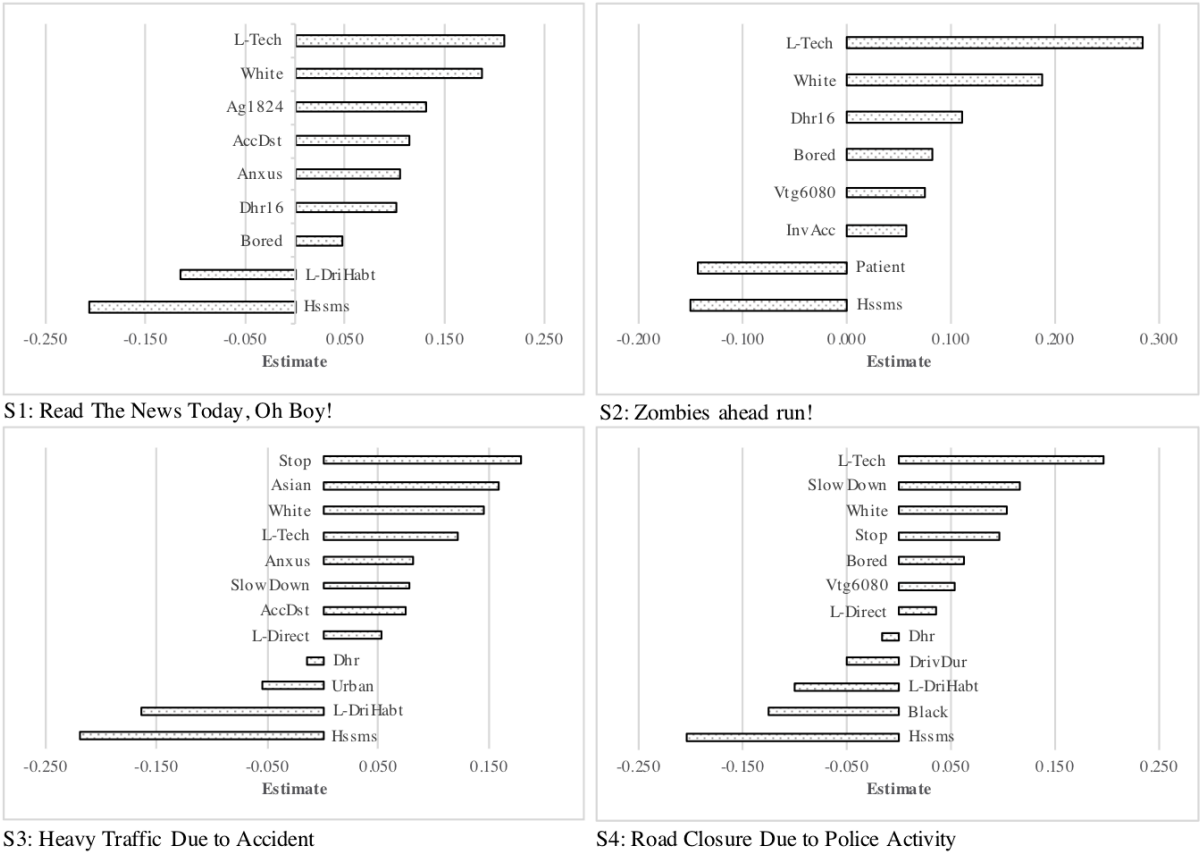


Figure 15 L-Cognitive distraction under the 4 scenarios

4.5.3 Distraction type: browsing

The L-Browsing construct mainly concerns those subjects who would pick up on the radio to acquire extra information about the DMS content. In this study, L-Browsing latent factor contributes positively to a higher risk of distraction in scenario 1, 3, and 4. Two attitudinal latent constructs were identified with a significant direct effect on L-Browsing (Table 11). These factors include L-Tech and L-Direct. The tech-friendly subjects are more likely to reach out to their vehicle infotainment system. The L-Tech association is higher concerning the fictitious scenario. This is similar to their behavior as far as the L-Phone and L-Cognitive distraction types are concerned.

Interestingly, the subjects with trouble finding their direction in an unfamiliar road are less likely to check the radio to gain extra information about traffic condition. That is, they might prefer to stay on the same route or either use their phone to find alternative routes. Either way, as we discussed in the previous sections, their chance of becoming distracted under a compromised DMS is high.

Among the observed variables that were found significantly correlated with the L-Browsing construct, subjects who are up-to-date with news, those who are familiar with DMS, and experienced drivers stated a positive attitude toward L-Browsing distraction type (Figure 16). However, subjects who (1) live in an urban area, (2) are students, (3) black, (4) reckless and careless drivers, and (5) those who have low education are less likely to become distracted. Among the explanatory variables with negative impact, reckless drivers have the highest negative impact while low educated subjects have the least negative impact on the L-Browsing.

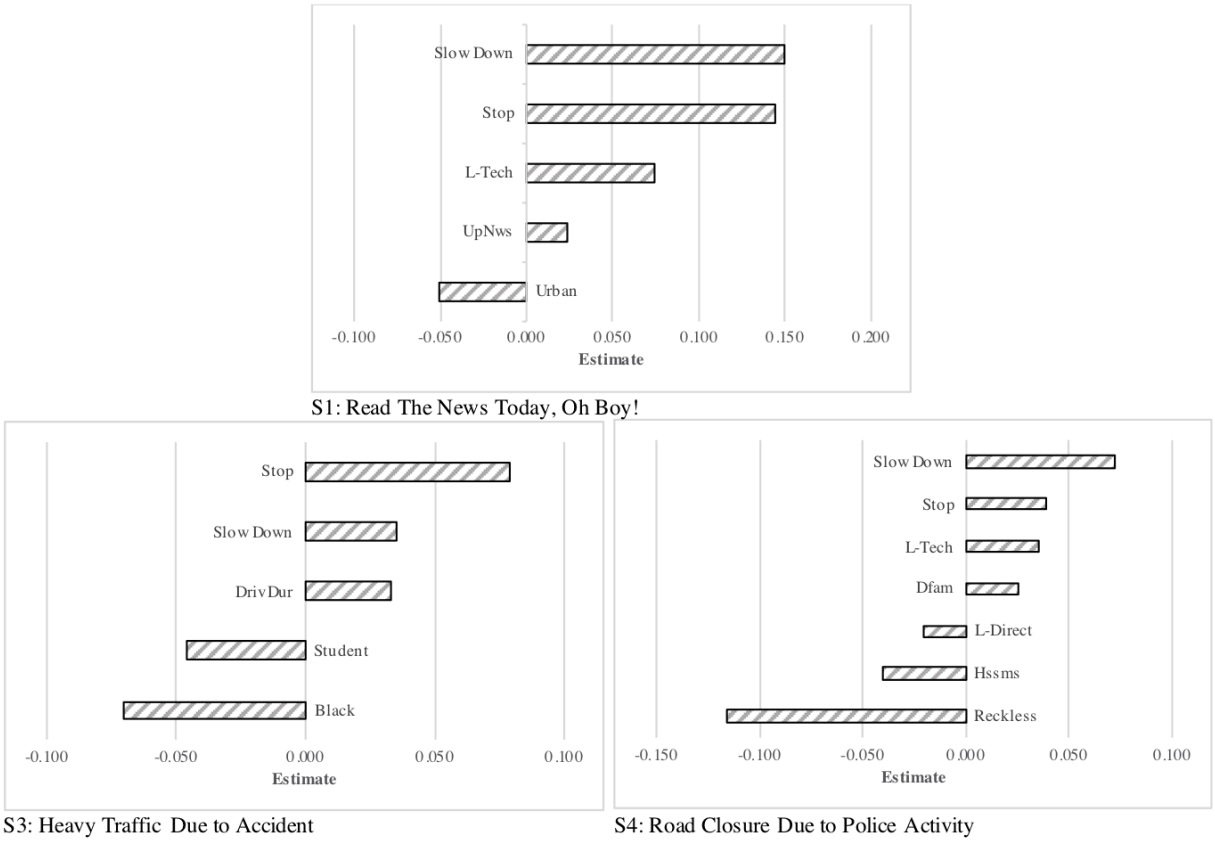


Figure 16 L-Browsing under the 4 scenarios

The slow down and stopping behavior have the highest association in the fictitious scenario. The speed choice trend is a little bit different between the realistic scenarios. Basically, in scenario 3 those subjects who stop their vehicles are more likely to tune their radio, while this is true for slow down behavior in the last scenario. Overall, in both fictitious and realistic scenarios, subjects speed variation behavior is significantly correlated with the L-Browsing constructs. That is, we can infer that distraction under a compromised DMS could lead to an unexpected slowing down and stopping behaviors.

4.6 Conclusion

Understanding drivers' distraction behavior under a compromised DMS is a fundamental step toward operating a safe and reliable transportation system. DMS have been hacked for over a decade, yet no previous study attempted to understand the adverse impacts of such event, on the

basis of empirical data. Previously Kelarestaghi et al., [25] conducted a qualitative risk assessment approach to tackle this problem. The result of their study listed distracted driving as one of the primary outcomes of DMS hacking phenomena [25]. In this study we conducted a web-based questionnaire in order to evaluate US drivers' distraction behavior under two main scenarios. These scenarios included realistic (with traffic-related information) and fictitious DMS content.

The fictitious scenarios were designed to resemble real-world hacking events [25]. The aim was to explore whether subjects are likely to distract under bogus information, and to identify what type of distractions have a higher association with risk of distracted driving. In addition, we developed two SEM models to estimate determinants of different type of distractions in order to provide a better understanding of travelers' behavior under a compromised DMS.

We took a step forward and argued that adversaries are able to display fabricated traffic related information in order to maximize their rewards of a cyber-attack. We tested the impacts of two fabricated-realistic messages on travelers' distraction behavior. These messages were (1) "Heavy Traffic due to Accident", and (2) "Road Closure due to Police Activity". The main hypothesis is that adversaries could create an unsafe traffic condition by encouraging drivers to use their cellphones or paying more attention to activities other than driving.

The design of this study not only assist engineers and policy makers to understand the outcome of cyber-attack on DMS but to compare different type of bogus messages impacts on drivers' behavior. Thus, we developed four SEM models in order to account for observed and unobserved variables that have the explanatory power to scrutinize the problem. These variables included drivers' (1) socio-economic and demographic information, (2) behavioral and attitudinal characteristics, and their experience with DMS in their day-to-day commute. Using Factor Analysis, we constructed three attitudinal latent factors to identify different type of drivers. These latent factors, classified drivers into (1) tech-friendly drivers, (2) drivers who respect traffic regulations, and (3) drivers who have trouble with identifying their direction especially in unfamiliar roads. We then tested the direct and indirect impact of the observed and unobserved explanatory variables on distraction behavior.

To assess travelers' distraction behavior under compromised DMS we grouped–using factor analysis–different distractive activities under 3-main latent factors. These latent factors included (1) phone use related distraction, (2) cognitive related distraction, and (3) distraction as a result of drivers reaching out to the vehicle infotainment system. The aforementioned latent factors were constructed thru the consolidation of the various manual (e.g., picking up on radio), visual (e.g., look at surrounding traffic), and cognitive (e.g., mind wandering) type distracting activities. Ultimately, we tested the direct association between the three distraction latent factors and the outcome variable of this study. The primary outcomes of this study are as follows:

- Regardless of the DMS hacking scenarios, drivers would engage in at least one of the distractive activities. Among the distraction latent factors, cognitive distraction has the highest impact on the distracted driving likelihood. Meaning, there is a high chance that drivers think of something other than driving, look at surrounding traffic and scenery, or talk to a passenger regarding the information that they saw on the DMS.

- Subjects attitudinal characteristics have significant contribution toward distraction risk. Drivers who rely and trust in technology and those who check traffic condition before starting their trips tend to become distracted especially with respect to the realistic scenarios. For drivers with trouble in finding their direction, the result is a mixed one. They have a negative attitude toward the L-Browsing constructs, but they have a positive association with the L-Cognitive latent factor. That is, while they might not use their cellphone or vehicle infotainment system, they are highly likely to, for instance, mind wanders under a compromised DMS. The subject who comply with traffic regulations have a homogeneous behavior toward detractive activities. The result of modeling indicated a negative linkage between L-DriHabt and distraction-related constructs regardless of the bogus information.
- We further assessed how and to what extent the mix of drivers responded to the distraction latent factors. Gender was identified with a positive association only to the L-Phone construct. White subjects were found to have positive linkage with L-Phone and L-Cognitive latent factors. Age was among the most important determinants of distractions. Younger subjects stated a positive correlation with L-Phone and L-Cognitive under the fictitious scenarios. We also learned that driving style is a determinant of drivers' distraction behavior under a compromised DMS. In both fictitious and realistic scenarios, Anxious drivers tend to positively impact the L-Cognitive latent factor. While the reckless and careless drivers stated a negative attitude toward the L-Browsing construct under scenario 4. In addition, the result of SEM models indicated several variables with a negative effect on distraction types. These variables are defining subjects who are less educated, student, black, live in an urban area, experienced drivers, and patient and careful drivers.
- Furthermore, we assessed the linkage between speed and distraction thru testing the association between subjects' slow down and stop behavior, and distraction behavior. we identified that at the presence of a bogus information drivers tend to slow down or stop in order to react to the DMS. That is, they would either (1) become involved in activities through the means of their phone, (2) they would mind wander, look around, and talk to a passenger about the sign, and (3) search for extra information by means of their vehicle's radio or internet. Interestingly this fluctuation in speed is consistent regardless of a scenario.

This study conducted a stated preference approach to asses drivers' distraction behavior under a compromised DMS. We collected data from eleven States by means of a web-based questionnaire. The modeling approach of this study allowed us to account for both subjective attribute and objective determinants of the population. The subjective attributes helped us to test information that are not acknowledged by the subjects directly. The layers of the SEM models also enabled us to understand the attitudes of drivers with different background toward the three-type of distraction. The result of this study identifies future research need to assess the behavior of the drivers under a compromised DMS using a driving simulator. There is a gap in the current literature to scrutinize the adverse impacts of a cyber/physical attack on DMS. The outcome of this study would be of particular help to policymakers, emergency responders, and engineers who are concerned with developing incident response plans and the safety, security, and resiliency of the ITS network.

Chapter 5

5 Choice Of Speed Under A Compromised Dynamic Messages Sign

Abstract

En-route advisory information supposed to facilitate road users with safe and efficient travel. In this study, for the first time, we argue that not only Dynamic Messages Signs (DMS) would not be lucrative to road users but would detriment the safety and operation of the transportation system. An adversary could compromise the security vulnerabilities of a DMS and display his/her desirable message to the drivers. Depends on the message the behavior of the road users could differ. This study investigates travelers' speed choice behavior under realistic and fictitious fabricated DMS content. To do so, we conducted a web-based survey using Amazon Mechanical Turk in eleven States around the nation. The statistical models take into account about 4,700 subjects' characteristics information and stated speed choice behavior. The results affirm traffic speed variation behavior at the presence of a compromised DMS. We further identify route change behavior and involvement in distraction activities as significant factors to contribute to the subjects' choice of speed. Also, we identify females, reckless and anxious drivers, highly educated subjects and tech-friendly drivers among the individuals that comply with false information. The outcome of this study would be beneficial to engineers and policymakers concerned with the safety, security, and resiliency of the transportation system.

***Key words**: cyber-physical systems, dynamic message signs, travelers' behavior, speed variation*

5.1 Introduction

Implementation of DMS has been a successful practice for many years. The DMS provides advisory information to the drivers in order to make the trips more efficient, and safe. One of the widely accepted application is to use DMS in order to control the speed of traffic. Current literature has been in favor of this approach [127, 157, 158, 159]. Previous literature indicate that drivers would comply with the DMS speed control related information and that the application of the DMS would benefit traffic homogeneity [157, 159]. For instance, Lee et al., [127] investigated the impact of variable speed limit signs, a warning messages on driver's speed change behavior. They conducted a driving simulator study and examined 86 subjects' response to the DMS. The result of their study indicated that subjects complied with the signs and lowered their speed. The outcome of this practice could benefit the system by lowering the risk of a crash [127].

While a speed related content displayed on a DMS could be beneficial to the system, traffic speed variation under different DMS would not be lucrative. Excessive attention to the DMS content would create speed variation in traffic. That is, for example, speed reduction behavior might occur mainly due to (1) increased attention demand (i.e., due to drivers' reaction to the message), and (2) following traffic compliance with speed reduction behavior of the lead traffic [22]. The unexpected variation in speed would create impulsive driving behaviors leading to closer spacing between vehicles and frequent lane changing maneuvers. The aftermath would be the creation of an unsafe traffic pattern that could result in a severe crash [24].

A message displayed on a DMS could unintentionally/intentionally affect drivers' choice of speed. The unexpected speed change behavior could increase safety risk. Smiley et al., [149] explored drivers' behavior under a digital billboard to investigate their speed and headway change before and after the sign construction. They found that the installation of the advertisement DMS would cause drivers inattention and cause them to brake more frequently [149]. Consequently, this speed change variability suggested as a reason for unsafe headways that compromise traffic safety.

Kolisetty et al. [160] studied road users speed change behavior using driving simulator and found DMS information effective to decrease drivers speed under adverse weather condition. The result of their study indicated that (1) most of the subjects' speed choice was affected by the DMS, and (2) DMS were effective to change the speed in the range of -2 to 15 km/hr. In a similar study, Yan and Wu studied [11] drivers speed behavior under DMS and found that as drivers move closer to the DMS, they tend to lower their speed. Erke et al., [22] designed a revealed preference study in order to investigate road users route choice and speed behavior under en-route information. They assessed speed change behavior of 3,342 vehicles and concluded that DMS information (road closure and road work related information) significantly sway drivers to reduce their speed. The reduction in speed was comparable with the amount of speed reduction under DMS with messages to warn drivers to lower their speed or warn them of a slippery road.

Harms et al., [155] attempted to explore whether DMS traffic-irrelevant content could harm transportation network. In their study, they collected the driving behavior of 32 subjects using driving simulator in Netherland. The results indicated that vehicles slowed down when approaching the DMS, in order to pay more attention to the DMS content. Drivers' understanding of a DMS content also plays a significant role in their speed choice behavior. Guattari et al., [156] in a similar study, used driving simulator data to investigate speed variation pattern at the presence of a DMS. They found that for cases that drivers were not able to understand the content the speed variation is high. While, when drivers comprehended the content the speed profile was stable.

Speed reduction behavior in response to the messages might compromise roadway safety. Lower driving speed and less driving attention can lead to more distraction [161]. To respond to the higher information load, drivers tend to lower their speed to engage with the supplied information. The speed reduction behavior that is irregular for the adjacent traffic could improvise headway decrease, conflicts, and risky driving behaviors [162]. In compliance with DMS information, drivers might reduce their speed, and this speed reduction behavior instigates the following vehicles to change lane or brake hard accordingly. The risk of unsafe driving would be higher in case drivers need more time to react to the information and draw a decision [145].

Previous literature solely focused on the impact of an authentic DMS content on the traffic speed change. Meaning that no previous study scrutinized a likely behavior of drivers under a compromised DMS. In this research we attempt to fill this gap and contribute to the literature of travelers' behavior in threefold: (1) we explore the impact of a fabricated content on drivers' speed choice behavior, (2) we investigate observed and unobserved determinants of drivers' choice of speed under a compromised DSM, and (3) scrutinize causation factors that are likely to contribute to this speed variation behavior. Mainly, our objective is to provide an answer to the following questions:

- Could adversaries engineer the traffic speed choice behavior?

- What are the critical factors that contribute to the speed choice behavior under a compromised DMS?
- What are the reasons that cause the speed variation pattern?

To answer these questions, we developed multivariate latent based ordered probit regression models to fully assess subjects likely speed choice behavior. We pondered four different forged information with realistic and fictitious related content. The fictitious scenarios were designed in order to mimic the real world DMS hacking events [25]. While the fabricated-realistic messages aimed at portraying scenarios that are conceivable to cause a higher negative impact. The remaining part of this study is organized as follows. First, we discuss the method and data that we used in this study. Second, we develop the multivariate ordered probit regression models. Third, we provide in-depth conversation over the determinants and causation factors of the speed choice behavior. We close the paper by outlining the main findings of the study and suggesting future research lines.

5.2 Method and data

The data collection process involved with a web-based survey questionnaire to capture about 4,700 subjects in eleven States. These States include California, New York, Texas, Florida, New Jersey, Mississippi, Iowa, Virginia, Maryland, North Carolina, and District of Columbia. To fellfield the objectives of the study and to understand the traveler change of behavior under the hacked DMS we designed our questionnaire into four sections. The first section aim was to capture subjects socio-economic and demographic information. The second part of the survey objective was to understand driving related attitudes of the participants. The third part, questioned subjects experience with the DMS, and the last section investigated subjects' behavior under different DMS hacking scenarios.

In this study, to assess the behavior of the subjects we queried several of their demographic, socio-economic and attitudinal related characteristics. These characteristics include age, gender, driving experience, commute hours, education, income, vehicle ownership, and driving style. Also, we question subjects' attitudes toward the use of technology, traffic regulations and their sense of direction, especially in an unfamiliar area. Besides, we wanted to acquire some knowledge of their familiarity with the DMS and to know whether they use the en-route information in their day-to-day commute.

The data that we collated comprise of 2,301 females and 2,001 males. Most of the subjects are younger than 45 years old and above 65% categorized themselves as white. Exactly 2,257 of the participants have a degree of Bachelor's or higher and 30% of these individuals hold a degree higher than Masters. About 2,131 of the subjects live in households with income lower than $60k, and about 20% of these subjects classified themselves in income categories of lower than $30k. In the other hand about 24% of the survey population live in households with income of $90k and higher.

In the survey questionnaire, we ask participants to classify themselves in one of the four driving style categories. These categories include anxious (i.e., feelings of alertness and tension), Reckless and careless (i.e., violations of safe driving norms), Angry and hostile (i.e., tendency to act aggressively on the road), and Patient and careful (i.e., planning ahead; attention, patience).

Subjects mainly cherry-picked patient driving style with 70% frequency, then anxious driving style with 23% and the rest described themselves as a reckless or angry driver. Precisely 2,635 of the subjects had previous accident experience in which the reason for a quarter of those accidents was distracted driving. Additional information regarding the data is listed in Table 7.

The current study was developed around the speed choice behavior that questioned in the survey questionnaire. According to the scenarios, respondents were asked to state their likely speed behavior under four different scenarios. These scenarios include (Sc1) "Road Closure due to Police Activity", (Sc2) "Heavy Traffic due to accident", (Sc3) "Read The News Today, Oh Boy!", and (Sc4) "Zombies ahead run!". In this paper, often we refer to Sc1 and Sc2 as realistic scenarios and to Sc3 and Sc4 as fictitious scenarios. Worth mentioning that Sc2 and Sc4 content comprised of a pictogram to increase cognitive demand for drivers. Subjects stated their likely speed behavior of (1) do-nothing, (2) speed up, (3) slow down, and (4) stop to the extent of extremely unlikely to extremely likely.

Our data show that under "road closure due to police activity" message (1) it is unlikely for participants (above 80% of the participants) to ignore the message, speed up or stop under the DMS information, and (2) most of the respondent slow down under the given scenario. That is approximately 73% of the participants to scale of extremely or somewhat likely slows down at the time they see the fabricated information. Participants indicated the similar speed change behavior under "heavy traffic due to accident" message. Most of them stated that they would slow down while indicating they would not ignore the message nor speed up or stop under the supplied information. Figure 17 illustrates respondents stated preference parallel to their choice of speed concerning scenarios with fabricated content.

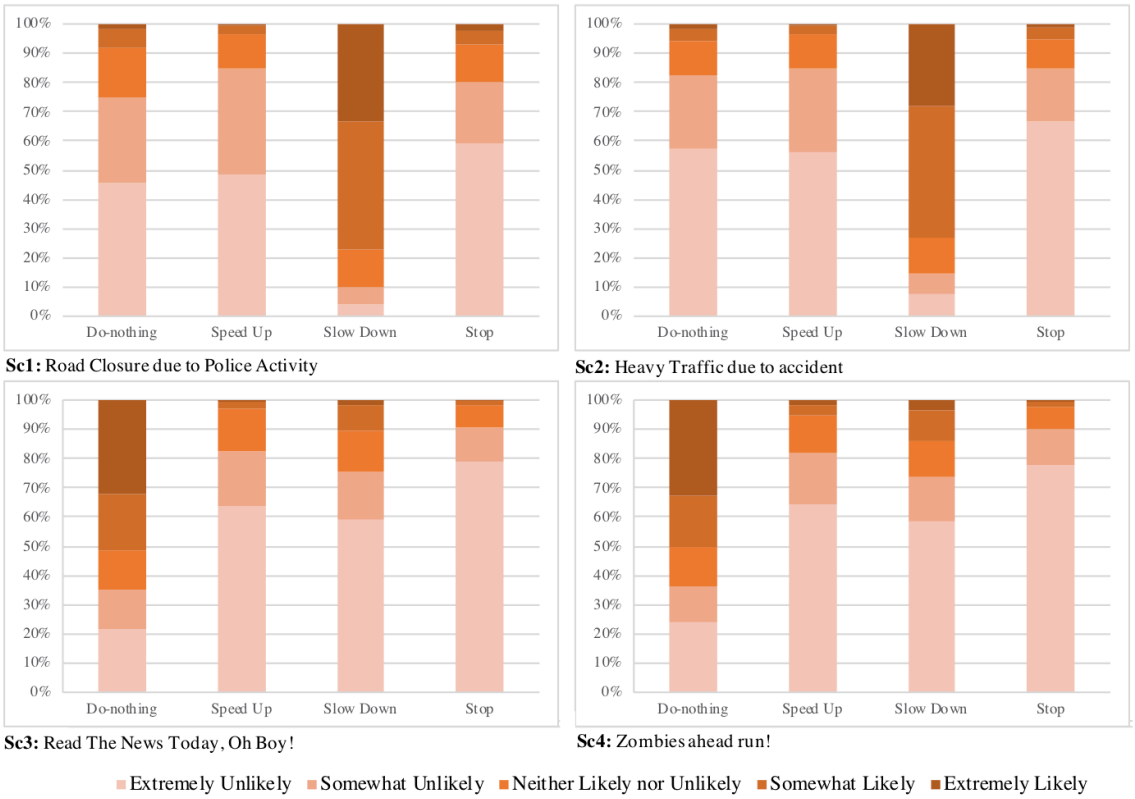


Figure 17 Road users speed choice behavior under a hacked DMS

As far as the fictitious scenarios are concerned, under the Sc3 scenario (i.e., Read The News Today, Oh Boy!) about half of the subjects indicated that they are more likely to ignore the message, 97% indicated that it is unlikely for them to speed up, more than 10% would slow down, and about 2% would stop their vehicle. In the Sc4 scenario (i.e., Zombies ahead run!) 50% of the participants would ignore the message, 95% would not speed up, about 15% of them would slow down, and roughly 3% of the subjects would stop under the compromised DMS.

Table 12 Data description summary.

Variable	Description	Category	Mean	Std. Dev.
Female	–	1: Yes; 0: Otherwise	0.53	0.50
Age	Age (year)	1: 18-24; 2: 25-34; 3: 35-44; 4: 45-54; 5: 55-64; 6: 65-84; 7: >85	2.61	1.20
Ag2534	Age: [25-34]	1: Yes; 0: Otherwise	0.40	0.49
DrivDur	Driving duration (year)	1: < 1; 2: 1-5; 3: 6-10; 4: 11-15; 5: 16-20; > 20	0.07	0.25
DrivDur15	Driving duration: [1-5] yr	1: Yes; 0: Otherwise	0.14	0.35
DrivDurA20	Driving duration: Above 20 yr	1: Yes; 0: Otherwise	0.32	0.47
Hssms	Education: Some school and High school	1: Yes; 0: Otherwise	0.09	0.28
ABachlr	Education: Bachelors and above	1: Yes; 0: Otherwise	0.52	0.50
Black	Black or African American	1: Yes; 0: Otherwise	0.09	0.29
White	–	1: Yes; 0: Otherwise	0.66	0.47
Single	Single, never married	1: Yes; 0: Otherwise	0.43	0.49
IncmA90	Income: above $90k	1: Yes; 0: Otherwise	0.24	0.42
VehMotr	Motorcycle / scooter	1: Yes; 0: Otherwise	0.01	0.08
VehVan	Minivan/Van/MPV	1: Yes; 0: Otherwise	0.05	0.22
VehSUT	Single unit truck	1: Yes; 0: Otherwise	0.00	0.05
Rural	–	1: Yes; 0: Otherwise	0.13	0.34
Urban	–	1: Yes; 0: Otherwise	0.34	0.47
Dhr	Driving hours (per week)	1: 0; 2: 1-5; 3: 6-10: 4: 11-15: 5: 16-20; 6: 21-25; 7: > 25	4.40	2.05
Dhr0	Driving hours: 0	1: Yes; 0: Otherwise	0.03	0.17
Dhr15	Driving hours: [1-5] hr/week	1: Yes; 0: Otherwise	0.28	0.45
Dhr1620	Driving hours: [16-20] hr/week	1: Yes; 0: Otherwise	0.07	0.26
Anxus	Anxious	1: Yes; 0: Otherwise	0.23	0.42
Reckless	Reckless and careless	1: Yes; 0: Otherwise	0.02	0.15
Angry	Angry and hostile	1: Yes; 0: Otherwise	0.04	0.20
InvAcc	Involved in accident	1: Yes; 0: Otherwise	0.61	0.49
RlyTech	Rely on technology for daily trips	1: Extremely Unlikely – 5: Extremely Likely	3.23	1.45
Newrote	Take new routes to reach destination sooner	1: Extremely Unlikely – 5: Extremely Likely	3.81	1.08
Leader	I can be a leader	1: Extremely Unlikely – 5: Extremely Likely	3.99	1.00
Trbldir	Trouble understanding directions	1: Extremely Unlikely – 5: Extremely Likely	2.18	1.17
Accom	More accomplished because of technology	1: Extremely Unlikely – 5: Extremely Likely	4.03	0.92
Bored	Driving makes me bored	1: Extremely Unlikely – 5: Extremely Likely	2.63	1.16
UpNws	Up-to-date with News	1: Extremely Unlikely – 5: Extremely Likely	3.78	1.02
Blinker	I use blinker when changing the lanes	1: Extremely Unlikely – 5: Extremely Likely	4.64	0.73
AtnVeh	Pay attention to vehicles around me	1: Extremely Unlikely – 5: Extremely Likely	4.70	0.62
TrfReg	Comply with traffic regulations	1: Extremely Unlikely – 5: Extremely Likely	4.52	0.74
SmArnd	Driving the same way as the others	1: Extremely Unlikely – 5: Extremely Likely	3.36	1.09
Grec	I have a good record of driving	1: Extremely Unlikely – 5: Extremely Likely	4.46	0.81
Chctrf	Check traffic before hitting the road	1: Extremely Unlikely – 5: Extremely Likely	3.19	1.38
Trstch	I trust technology to assist in my travel	1: Extremely Unlikely – 5: Extremely Likely	4.17	0.94
Dfam	Familiarity with DMS	1: Not familiar at all – 5: Extremely familiar	3.96	1.02
Dread	Read DMS in daily commute	1: Never – 5: Always	4.28	0.89
Vtg	Trust in DMS	Continues (1–5)	4.09	0.82
VtgA8	Above 80% trust in DMS	1: Yes; 0: Otherwise	0.58	0.49
ATrMC	Attention to DMS traffic information	1: Extremely Unlikely – 5: Extremely Likely	4.31	0.82
Rout divergence				
	Sc1	1: Extremely Unlikely – 5: Extremely Likely	3.69	1.17
	Sc2	1: Extremely Unlikely – 5: Extremely Likely	3.51	1.27
	Sc3	1: Extremely Unlikely – 5: Extremely Likely	1.33	0.72
	Sc4	1: Extremely Unlikely – 5: Extremely Likely	1.42	0.88
Call/Text someone				
	Sc1	1: Extremely Unlikely – 5: Extremely Likely	2.07	1.23
	Sc2	1: Extremely Unlikely – 5: Extremely Likely	1.83	1.16
	Sc3	1: Extremely Unlikely – 5: Extremely Likely	1.75	1.19

Sc4	1: Extremely Unlikely – 5: Extremely Likely	2.45	1.56
Take picture of sign			
Sc1	1: Extremely Unlikely – 5: Extremely Likely	1.56	0.97
Sc2	1: Extremely Unlikely – 5: Extremely Likely	1.36	0.77
Sc3	1: Extremely Unlikely – 5: Extremely Likely	2.23	1.47
Sc4	1: Extremely Unlikely – 5: Extremely Likely	3.20	1.64
Pick up on radio			
Sc1	1: Extremely Unlikely – 5: Extremely Likely	3.48	1.34
Sc2	1: Extremely Unlikely – 5: Extremely Likely	2.86	1.49
Sc3	1: Extremely Unlikely – 5: Extremely Likely	2.12	1.41
Sc4	1: Extremely Unlikely – 5: Extremely Likely	1.96	1.34
Look at scenery/traffic			
Sc1	1: Extremely Unlikely – 5: Extremely Likely	3.23	1.26
Sc2	1: Extremely Unlikely – 5: Extremely Likely	2.92	1.37
Sc3	1: Extremely Unlikely – 5: Extremely Likely	2.17	1.29
Sc4	1: Extremely Unlikely – 5: Extremely Likely	2.49	1.43
Social media or internet browsing			
Sc1	1: Extremely Unlikely – 5: Extremely Likely	2.34	1.39
Sc2	1: Extremely Unlikely – 5: Extremely Likely	1.85	1.21
Sc3	1: Extremely Unlikely – 5: Extremely Likely	2.01	1.38
Sc4	1: Extremely Unlikely – 5: Extremely Likely	1.93	1.34

The outcome variables (i.e., speed choice behavior) of this study are all ordinal variables with categories of (1) extremely unlikely, (2) somewhat unlikely, (3) neither likely nor unlikely, (4) somewhat likely, and (5) extremely likely. For the purpose of this study, we developed four multivariate latent based ordered logistic regression models with the probit link function. For the sake of speed change behavior model, we applied the multivariate model to account for heterogeneity in the error structure. The modeling approach allows for correlation between outcome variables error terms.

We hypothesize that the driver's inattention would cause them to change their speed (slow down) in order to manage extra cognitive demand. The multivariate ordered probit is an extension to the multivariate probit regression when the outcome variables have more than two categories. The process that we took to develop the speed choice include (a) test the correlation between the dependent and independent variables using bivariate regression, (b) test the collinearity between variables, (c) assess the significance of observed and unobserved variables in the model, and (d) remove highly correlated variables that result in less efficient models. That is, the models represented in Table 13 and Table 14 are a good fit to the data.

To group attitudinal variables in the meaningful construct, we conducted explanatory factor analysis. The result suggests three attitudinal latent factors. These factors are related to the drivers' attitude toward technology (Tech), their driving habit (DriHabt), and their sense of direction (DriAttitd). The first latent factors include Accom, Trstch, RlyTech, and Chctrf variables. These variables mainly measure to what extent drivers seek traffic information utilizing technology. The tech-friendly driver latent variables comprise of indicators that portraying drivers attituded toward the use of technology in a daily commute. For instance, RlyTech indicator gauges driver's reliance on technology (i.e., use of GPS), and Chctrf indicates to what extent the subjects of this study are dependent to technology to scan their planned route traffic condition before departing. Overall, a tech-friendly driver characterizes subjects who are sensitive to the traffic congestion, travel time, and those who prefer to use secondary sources to gain prior knowledge of the real-time traffic condition rather than relying only on their observation and driving experience. The second latent factors include Blinker, AtnVeh, TrfReg, and Grec variables which indicating drivers respect to traffic regulations and their attentiveness to the surrounding traffic. The latter construct examines drivers' sense of direction. This construct includes three observed variables: Lost, PFmRt, and Trbldir. Next section explains the results of the modeling process.

5.3 Result and discussion

The results of the speed choice models for scenario 1 and 2 are listed in Table 13 and for scenario 3 (Sc3) and 4 (Sc4) are outlined in Table 14. To decide on models' goodness of fit, we used McFadden's Pseudo R-Square using the following equation (E.q. 1). In which, LL_{fit} is a log likelihood value for the fitted model and LL_{Null} is the log likelihood value of the null model. Closer this value is to one, the better the model fits the data. For the first scenario speed choice model, we estimated the McFadden's Pseudo R-Square equal to 0.66, for the second scenario we estimated it equal to 0.64 (> 0.2). The McFadden's Pseudo R-Square value is equal to 0.53 and 0.79 (> 0.2) for Sc3 and Sc4. All values are indicating that models have satisfactory goodness of fit indices.

$$R^2_{McFadden} = 1 - {LL_{fit}}/{LL_{Null}} \quad \text{(E.q. 1)}$$

To construct the models, we examined all three latent factors (i.e., Tech, DriHabt, DriAttitd) discussed in the previous section. We found the tech latent variable significant (at 90% confidence interval) in the Sc1 model with respect to the slow down behavior. We also indicated that DriAttitd latent factor has significant contribution to the slow down behavior under the Sc2 scenario. In regards to the Sc3 scenario model, we did not identify a significant correlation between latent factors and the outcome variables. In the Sc4 scenario, we found DriHabt latent factor with positive linkage to the do-nothing dependent variable.

Table 13 Speed choice under realistic scenarios.

Variables	Sc1: Road Closure due to Police Activity								Sc2: Heavy Traffic due to accident							
	Do-nothing		Speed Up		Slow Down		Stop		Do-nothing		Speed Up		Slow Down		Stop	
	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z
Female	-0.14***	-2.98	–		0.25***	6.61	–		–		–		0.13***	3.43	-0.09**	-2.37
Age	–		–		–		–		-0.08***	-4.41	–		–		–	
White	0.13**	2.4	–		-0.10**	-2.51	–		–		–		-0.14***	-3.52	–	
Black	-0.18**	-1.99	–		–		0.19***	3.12	-0.36***	-4.35	–		–		0.22***	3.2
BlwAsoc	–		–		–				-0.09**	-1.97	–		–		–	
Rural	–		–		–				–		-0.21***	-2.63	0.22***	3.88	–	
Disbl	-0.28***	-2.85	–		–		–		–		–		–		–	
Dread	-0.15***	-5.52	–		–		-0.13***	-6.31	-0.12***	-4.84	–		–		–	
Dfam	–		-0.08***	-3.86	–		–		–		–		–			
DrivDur	–		–		–		-0.09***	-7.49	–		–		–			
InvAcc	–		–		–		–		–		-0.19***	-3.49	–		-0.20***	-4.85
VehVan	–		–		–		–		–		–		–		0.154*	1.76
Vtg	-0.28***	-8.51	-0.27***	-8.91	0.18***	7.49	–		–		–		–		–	
VtgA80	–		–		–		–		-0.21***	-4.44	–		–		–	
ATrMC	-0.28***	-8.85	-0.18***	-6.27	–		–		–		–		–		–	
Dhr1620	0.16*	1.92	–		–		–		–		–		–		–	
Patient	-0.11**	-2.27	–		–		–		–		–		–		–	
Reckless	–		–		–		–		–		0.48***	3.04	–		–	
Upnews	-0.041*	-1.83	–		–		–		–		–		–		–	
Bored	–		–		–		–		0.09***	4.37	–		–		–	
Take picture	-0.05***	-2.65	–		0.04**	2.57	–		–		–		0.06***	4.25	–	
Check radio	-0.09***	-5.18	–		0.13***	8.85	–		–		–		0.07***	5.29	–	
Look around	–		–		0.16***	10.43	–		–		–		0.13***	9.27	–	
Call/Text	–		–		–		0.18***	11.31	–		–				0.28***	16.45
Browsing	–		–		–		0.11***	7.86	–		–		–		–	
Route Change	-0.34***	-16.64	–		0.22***	12.73	0.1***	6.13	-0.23***	-13.02	–		0.08***	5.15	–	
DriAttitd	–		–		–		–		–		–		0.03*	1.94	–	
Tech	–		–		0.11**	2.33	–		–		–		–		–	
Thresholds (cut-points)																
Cut 1	-5.08***	-25.98	-2.22***	-14.25	0.61***	4.62	0.41***	3.56	-1.2***	-8.57	0.22***	4.65	-0.67***	-8.552	0.94***	17.62
Cut 2	-3.83***	-20.13	-0.73***	-4.85	1.13***	8.58	1.11***	9.71	-0.07	-0.529	1.71***	21.4	-0.25***	-3.276	1.68***	29.26
Cut 3	-2.67***	-14.29	0.61***	3.91	1.77***	13.28	1.85***	15.81	0.82***	5.929	3.07***	24.09	0.28***	3.576	2.45***	37.09
Cut 4	-1.58***	-8.29	1.57***	8.05	3.32***	23.25	2.48***	19.98	1.65***	11.087	4.09***	22.13	1.79***	21.41	3.2***	35.65

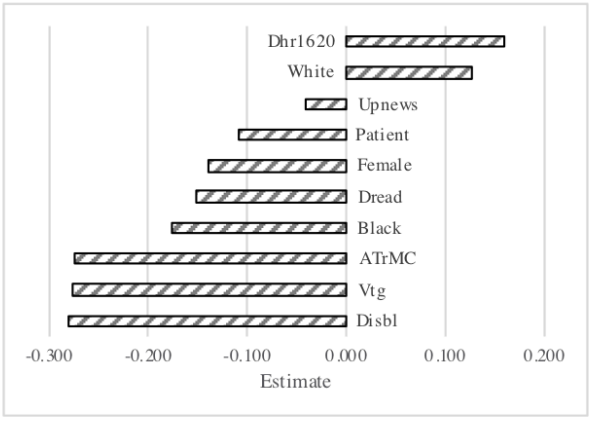
Latent factors indicators

Tech			**DriAttitd**		
Indicator	Coef.	z	Indicator	Coef.	z
Accom	Constant		Lost	Constant	
Trstch	1.33***	24.17	PFmRt	0.19***	17.09
Rlytch	1.49***	20.56	Trbldir	0.46***	26.04
Chctrf	0.71***	11.96		–	

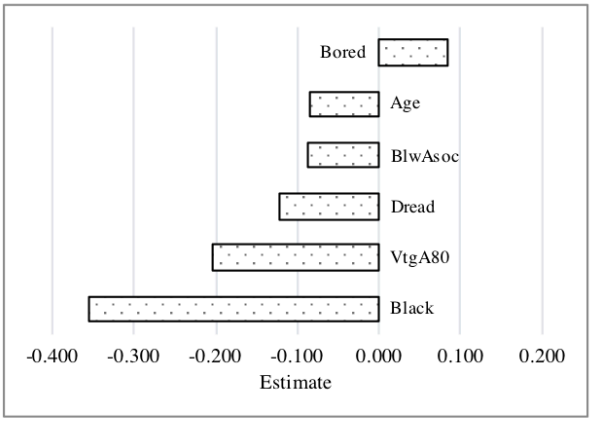
*Note: ***, **, * means significance at 1 percent, 5 percent, 10 percent level.*

The speed choice model result represents the estimates of explanatory variables and latent factor related to the speed choices– ignore (do-nothing), speed up, slow down, and stop. Concerning the Sc1 realistic scenarios, most of the significant variables under the ignore outcome variable indicated a negative association. That is, drivers with higher trust to the DMS (Coef. = -0.28), those who pay more attention to the traffic-related information (Coef. = -0.28), and those with disability have the least intent to ignore the fabricated-realistic information. While white subjects and those with long weekly commute hours tend to ignore the traffic-related messages. That is, the experienced drivers tend to value their experience more than the en-route information. Figure 18 illustrates the effect determinants on do-nothing choice for all the scenarios.

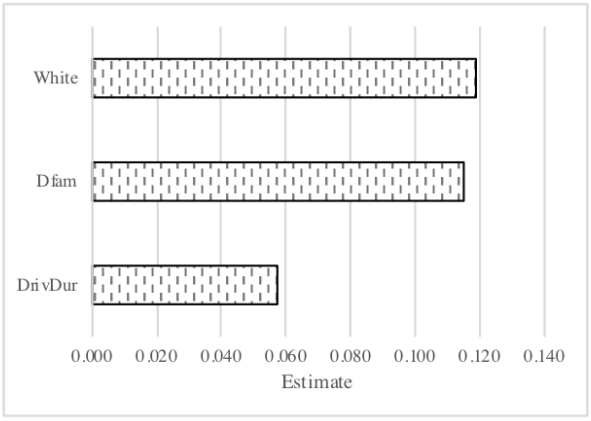
In the first scenario, All the explanatory variables that found significantly correlated to the speed up choice have a negative association with the outcome variable. For instance, subjects who are familiar with the DMS (Coef. = -0.08) are unlikely to speed up under the supplied information. In compliance with the fabricated information, most of the subjects would slow down under the DMS in Sc1. These subjects include female drivers (Coef. = 0.25), drivers with high trust in the DMS (Coef. = 0.16), and tech-friendly drivers (Coef. = 0.11). While the results for the last speed choice (stop) is a mixed one, it is worth remarking that Black (Coef. = 0.24) drivers, subjects who have trouble finding their direction in new routes and those with the patient and careful driving style are more likely to stop under the given information.



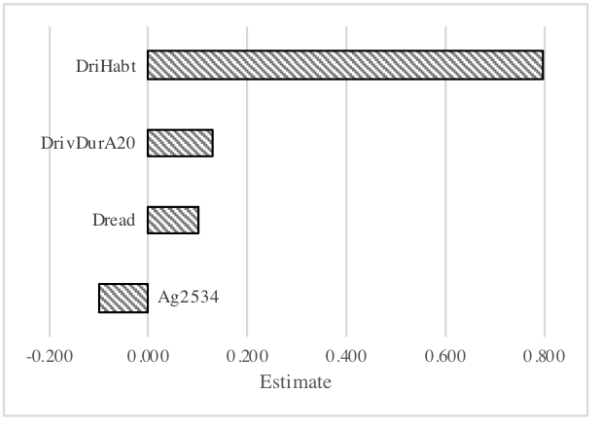
Sc1: Road Closure due to Police Activity



Sc2: Heavy Traffic due to accident



Sc3: Read The News Today, Oh Boy!



Sc4: Zombies ahead run!

Figure 18 Determinants of do-nothing

Table 14 Speed choice under fictitious scenarios.

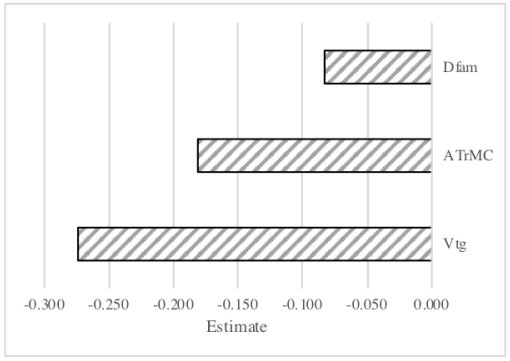
	Sc3: Read The News Today, Oh Boy!								Sc4: Zombies ahead run!							
Variables	**Do-nothing**		**Speed Up**		**Slow Down**		**Stop**		**Do-nothing**		**Speed Up**		**Slow Down**		**Stop**	
	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z	Coef.	z
Female	–		–		–		–		–		-0.08*	-1.64	–		–	
Age	–		–		0.06***	2.89	–		–		–		–		–	
Ag2534	–		–		–		–		-0.09**	-2.13	–		–		–	
White	0.12***	2.82	–		–		–		–		-0.19***	-3.52	–		-0.27***	-3.62
Asian	–		–		–		–		–		–		–		–	
IncmA90	–		–		–		–		–		-0.13**	-2.39	–		–	
ABachlr	–		–		–		–		–		–		0.12***	2.91	–	
Single	–		–		0.12**	2.57	–		–		–		–		–	
Urban	–		–		–		0.19***	2.77	–		–		–		0.18***	2.59
DrivDur	0.06***	4.1	-0.08***	-5.516	–		–		–		–		–		–	
DrivDur15	–		–		–				–		–		0.11*	1.89	0.22**	2.4
DrivDurA20	–		–		–				0.13***	2.58	–		–		–	
VehMotr	–		–		–		0.77**	2.25	–		–		–		–	
InvAcc	–		–		–		-0.23***	-3.28	–		–		–		–	
Vtg	–		–		–		-0.3***	-7.18	–		–		–		–	
Anxus	–		–		0.13***	2.71	–		–		–		–		–	
Reckless	–		–		–		0.46**	2.32	–		–		–		–	
UpNws	–		–		–		–		–		–		–		–	
VehSUT	–		–		0.61*	1.8	–		–		–		–		–	
Bored	–		–		0.05***	2.7	–		–		–		–		–	
Dfam	0.12***	5.88	–		–		–		–		–		–		-0.13***	-4.11
Dread	–		-0.19***	-8.11	-0.1***	-4.24	–		0.1***	4.44	–		–		–	
Take picture	–		–		0.25***	13.91	0.19***	5.95	-0.16***	-11.01	–		0.14***	8.44	–	
Call/Text	–		–		0.19***	8.62	0.33***	8.42	-0.24***	-15.22	–		0.15***	8.89	0.22***	8.95
Check radio	–		–		0.27***	16.24	0.32***	8.75	–		–		–		–	
Browsing	–		–		–		0.1***	3.09	–		–		–		–	
DriHabt	–		–		–		–		0.79***	14.68	–		–		–	
Thresholds (cut-points)																
Cut 1	-0.12***	-1.24	-0.69***	-6.122	1.76***	11.85	2.33***	9.29	-1.52***	-13.51	0.45***	7.83	1.25***	19.74	1.62***	8.88
Cut 2	0.39***	4.09	0.04***	0.358	2.48***	16.07	3.41***	11.72	-1.08***	-9.66	1.3***	19.57	1.89***	27.73	2.66***	12.56
Cut 3	0.79***	8.29	1.21***	9.951	3.23***	20.30	4.96***	13.79	-0.68***	-6.12	2.27***	28.27	2.47***	33.79	3.86***	15.27
Cut 4	1.35***	14.0	2.01***	13.991	4.22***	25.02	6.18***	14.36	-0.15	-1.30	2.77***	30.60	3.34***	39.81	4.71***	16.22

DriHabt Latent factor		
Blinker	constant	
ATNVEHC	0.94***	42.36
TRFREGC	1.01***	39.15
Grec	0.94***	33.59

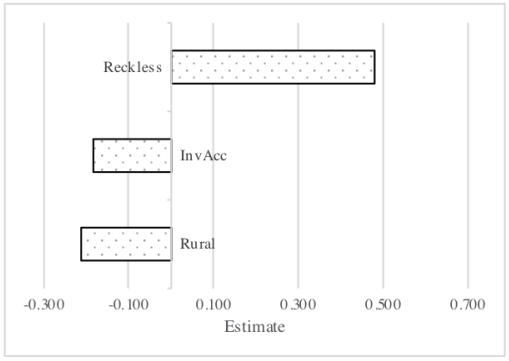
*Note: ***, **, * means significance at 1 percent, 5 percent, 10 percent level.*

As far as the heavy traffic scenario (Sc2) is concerned, similar to the scenario mentioned above, significant explanatory variables have a negative association with the do-nothing outcome variables. That is Black, older subjects, those who have lower education (under Associate degree), and those who read the DMS information more than other drivers are less likely to ignore the fabricated-realistic information. The only variable with a significant positive association with the do-nothing outcome variable is the one that represents subjects that finds driving a tedious activity (Coef. = 0.09). Interestingly those subjects that see driving a tedious task are likely to ignore the heavy traffic message and to continue with their intended choice of speed. Under this scenario, most of the variables have a negative association with the speed up choice but the variable that characterizes reckless and careless drivers (Coef. = 0.54). Figure 19 summarizes the determinants of speed up behavior under all the scenarios.

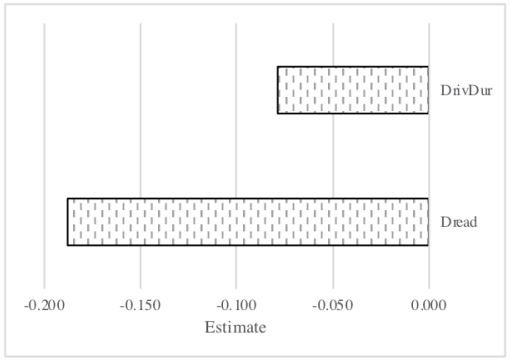
The main hypothesis is that subjects should comply with the message and slow down under the pretentious information. As the model result implies (Figure 20), female drivers (Coef. = 0.13), subjects who live in rural areas (Coef. = 0.24), and those who are not good at finding their direction in unfamiliar routes (Coef. = 0.03) are more likely to slow down under the DMS. This finding is plausible because subjects under the DriAttitd latent factors would need extra time to find a better route through the means of secondary sources. We argue that it is likely for subjects to stop under this information (Sc2) in order to cherry-pick other routes in order to lower their travel time. The results (Figure 21) indicate that while female and drivers who involved in an accident before are not willing to stop under the given information, other drivers might stop. These subjects are those who drive Minivan and Van vehicle (Coef. = 0.21), black and African American subjects (Coef. = 0.2).



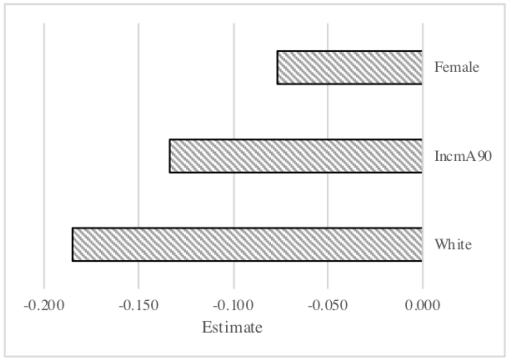
Sc1: Road Closure due to Police Activity



Sc2: Heavy Traffic due to accident



Sc3: Read The News Today, Oh Boy!

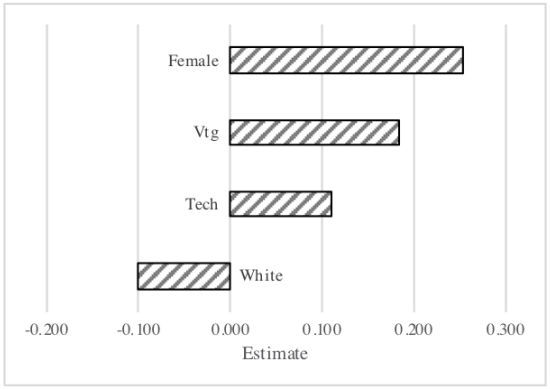


Sc4: Zombies ahead run!

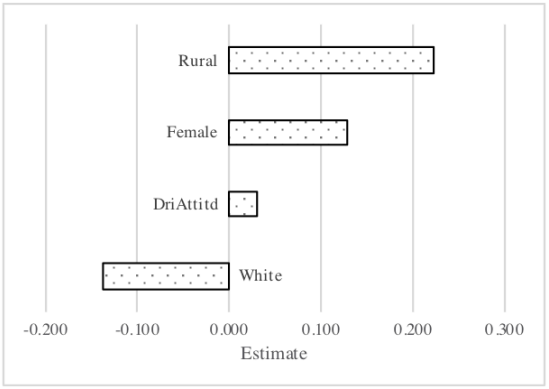
Figure 19 determinants of speed up behavior

In the fictitious scenarios (Sc3 and Sc4) the behavior of the subjects is different. Experienced drivers especially those with higher than 20 years of driving experience (Coef. = 0.13) are likely to ignore both fictitious messages. White subjects, the ones who are familiar with the DMS content in general and those who respect traffic regulations and are attentive to their surrounding traffic tend to ignore the fictitious messages. Surprisingly in the case of younger drivers (between 25 and 34 years old), there is a tendency to not ignore the message (Coef. = -0.1) of the Sc4 scenario. The reason is that the "Zombies ahead run!" is attractive to these subjects and they would pay more attention to the sign compare to the older drivers.

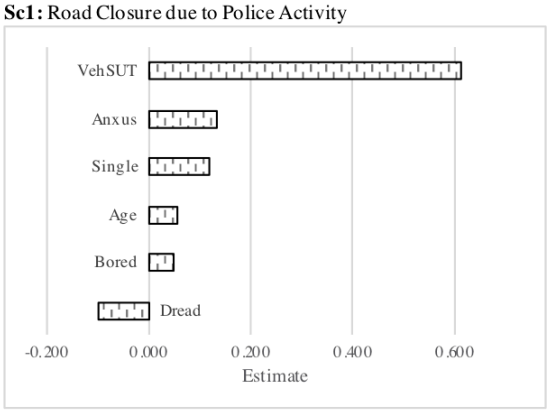
As far as the speed up behavior is concerned, under Sc3 and Sc4, all the significant factors have a negative association with the outcome variable. These variables include DriDur (Coef. = -0.1), Dread, White, IncmA90 (Coef. = -0.13), and Female (Coef. = -0.07). All, but one, of determinants, were found with positive correlation to the slow down behavior under both the "Read The News Today, Oh Boy!" and "Zombie ahead run!" scenarios. Drivers of a single unit truck, anxious drivers, single (never married) and older individuals are the ones that who would pay attention to the signs and slow down in Sc3. This behavior could mainly raise from subjects' sensitivity to the news or simply from their interests in abnormal and infrequent messages. Either way, the sign would cause unexpected slow down behavior with the potential to create unsafe traffic pattern. The interesting fact is that those subjects who read DMS more often in their commute would not slow down under the message.



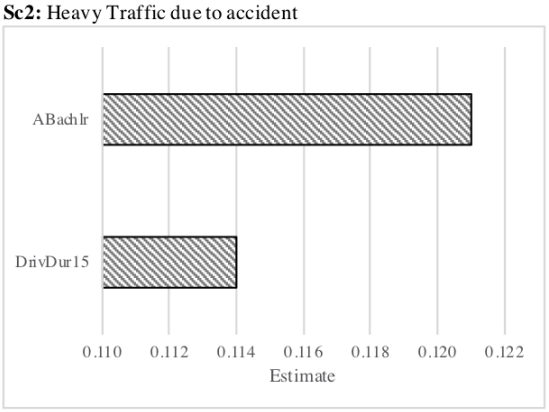
Sc1: Road Closure due to Police Activity



Sc2: Heavy Traffic due to accident



Sc3: Read The News Today, Oh Boy!



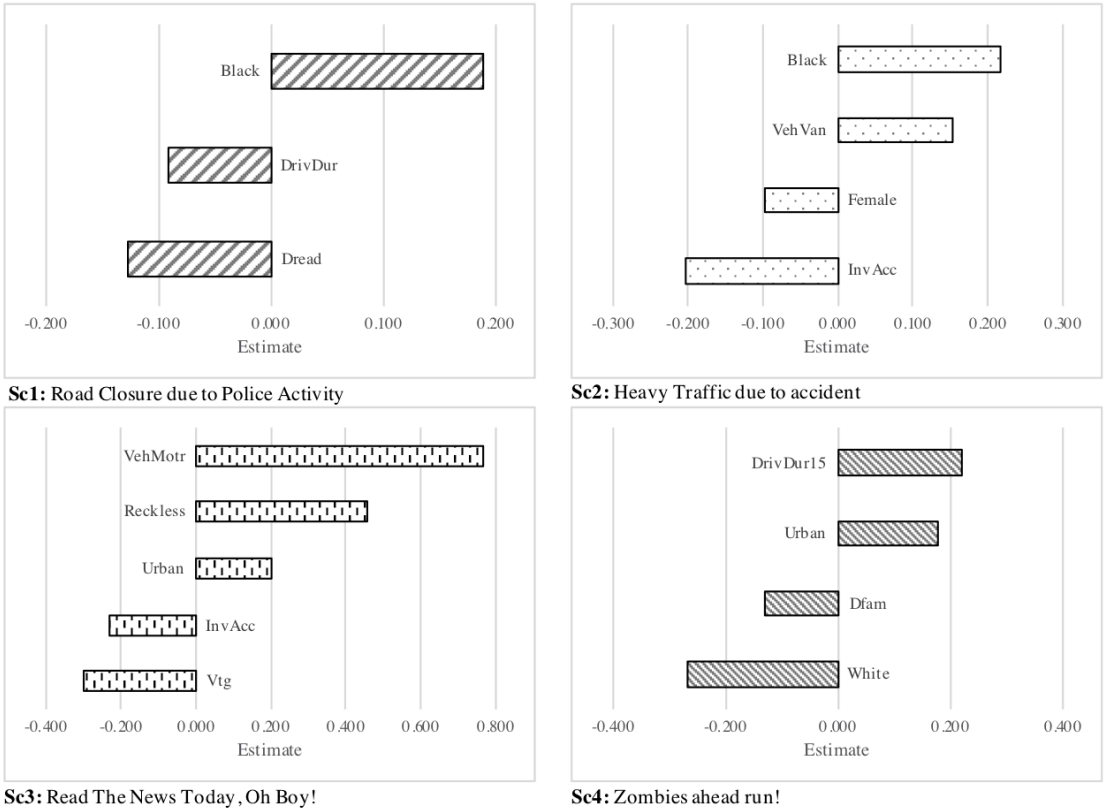
Sc4: Zombies ahead run!

Figure 20 determinants of slow down behavior

Under the last scenario, those who have relatively high education (above Bachelor's degree) and those who have up to five years of driving experience would slow down under the "Zombie ahead run!" message. Subjects stopping behavior under the fictitious scenarios is also interesting to examine. Previous involvement in an accident, high trust to the DMS, and familiarity with the DMS are factors that inhibit subjects from stopping at the DMS with fictitious content. While, living in an urban area, and relatively low driving experience are factors that contribute to the higher chance of stopping under these scenarios. Interesting to note that, reckless drivers and subjects whose primary vehicle is motorcycle are likely to stop under the "Read The News Today, Oh Boy!" message.

5.3.1 Causation factors

In addition to exploring determinants of speed choice, we scrutinize the reasons behind each of the choices that subjects might take. To this extent, we tested the relationship between distracting activity and route change behavior with the speed choice outcome of all the scenarios. The distracting activities include taking a picture of the sign, call/text someone about the sign, talk to a passenger, browse social media or internet after seeing the sign, and picking up on the radio to gain more information about the en-route content. For a better presentation, we separated these variables and compared their impact in Figure 22, Figure 23, and Figure 24.



Sc1: Road Closure due to Police Activity

Sc2: Heavy Traffic due to accident

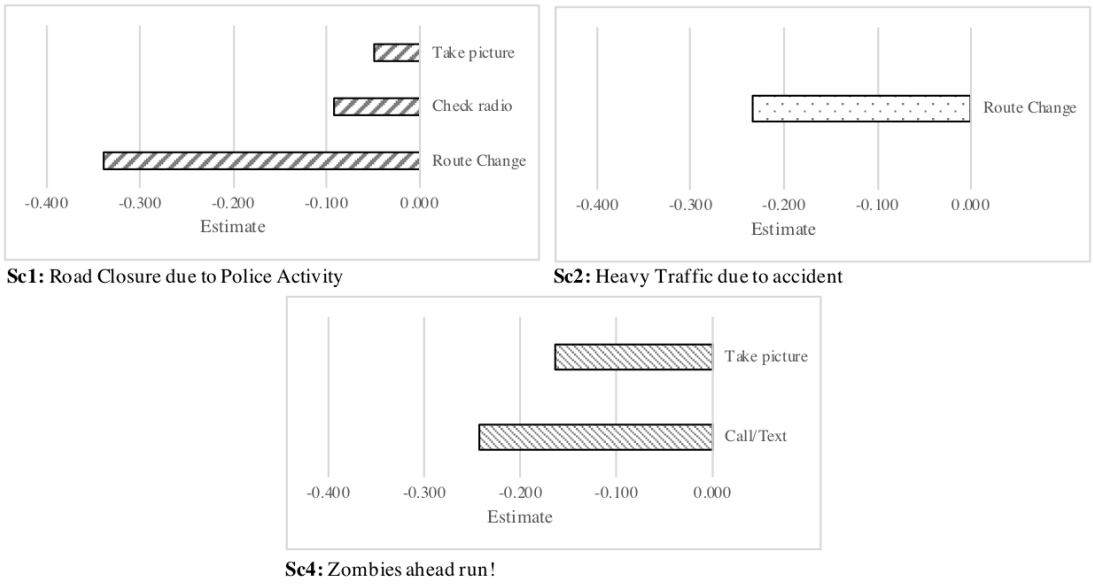
Sc3: Read The News Today, Oh Boy!

Sc4: Zombies ahead run!

Figure 21 determinants of stopping behavior

Do-nothing

We identified several causation factors with negative impact in the ignore models. Indicating that motivation for these types of activities sways subjects to pay attention to the signs. With respect to both scenario 1 and 2, one of the subject's reasons for paying attention to the sign is route change behavior. These signs alert subjects of a fake road closer or heavy traffic ahead of them. However, since the integrity of such messages is not clear to the subjects they consider changing their route. As far as the distracting behavior is concerned, under Sc1 and Sc4 those who want to take a picture, pick up on radio or call/text someone about the sign would not ignore the sign (Figure 22).



Sc1: Road Closure due to Police Activity

Sc2: Heavy Traffic due to accident

Sc4: Zombies ahead run!

Figure 22 Causation factors of do-nothing

Slow down

Slow down behavior is the speed choice behavior that we anticipate under all the fabricated scenarios. We hypothesized that (1) attentional overload would cause drivers to slow down to respond to the excessive cognitive demand, (2) subjects would attempt to find a better route under SC1 and Sc2, thus would slow down, and (3) they would become involved in distracting behaviors. If drivers need extra time under the last two reasons, they will stop under the fabricated content (Figure 23).

In addition to examining the link between explanatory variables and speed choice outcome variables, we tested if it is correct to speculate that subjects are likely to divert from their current route under the bogus information. That is, we included the variable representing the subject stated a preference to the route divergence behavior under all scenarios. The result depicts that route divergence variable has a positive association with subjects' slow down behavior under both Sc1 and Sc2 scenarios. As far as the Sc1 scenario is concerned, route change behavior has the most causation impact on the slow down behavior.

The estimates for route divergence variables under road closure and heavy traffic scenarios are equal to 0.22, and 0.08, respectively. At the same time, there is a negative correlation between do-nothing outcome variable and the route divergence behavior for both scenarios. That is, one can extrapolate that searching for a more efficient route could be the causation of drivers slowing down behavior. This result is consistent with the hypothesis of this study, rendering that it is very likely for an adversary to destabilize traffic by affecting drivers' speed choice and shunt drivers to other routes.

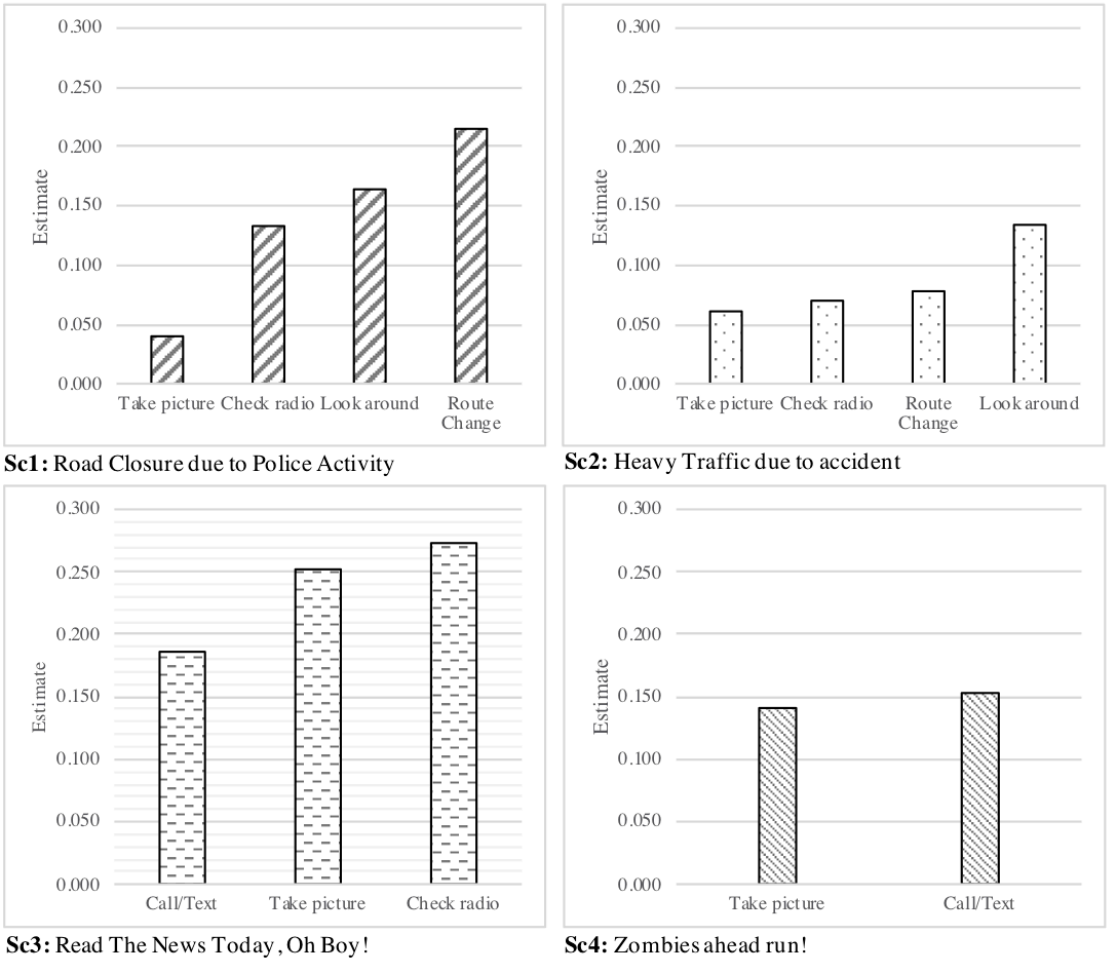


Figure 23 causation factor of slow down behavior

Look at surrounding traffic and scenery (visual distraction), picking up on the radio (manual distraction) and taking a picture of the sign to have a lower contribution to the slow down behavior. The impact of distracting behavior on Sc2 is almost the same as Sc1 with only one difference. Looking at the scenery and surrounding traffic has the most impact, and Route change behavior has the second most significant impact on the slow down behavior.

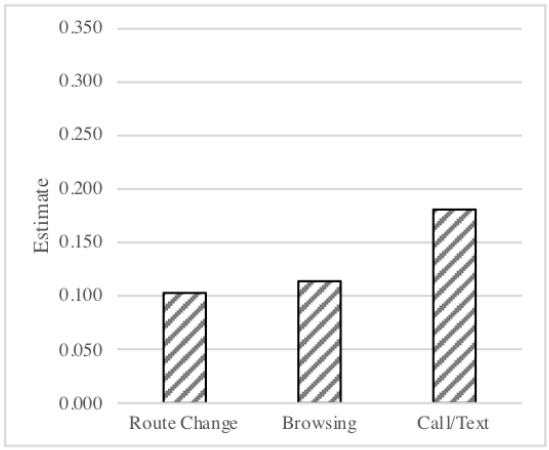
Route change behavior did not have a significant contribution to the slow down behavior under fictitious scenarios. In Sc3, picking up on the radio had the most impact on the slow down behavior. Taking a picture of the sign and call/text someone about the sign

had a lower impact. Interestingly, in the last scenario call/text someone had the most impact on the slow down behavior.

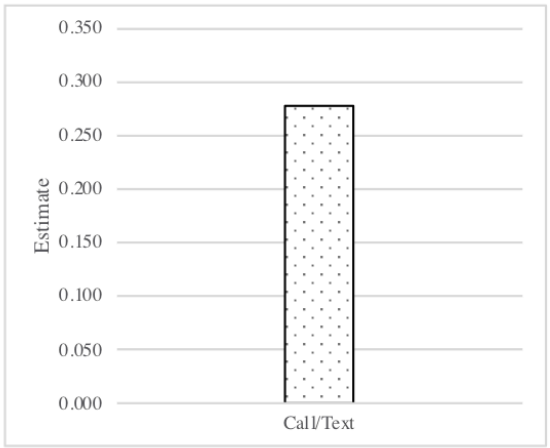
Stop

Several reasons could explain why drivers have a tendency to stop under the realistic and fictitious DMS content (Figure 8). For all the scenarios regardless of the content, call/text someone is the activity with the highest impact on the stopping behavior. This is very interesting since under fictitious content (especially in Sc4) many drivers tend to take a picture of the sign [15]. However, this result indicates that subjects would not stop to take a picture but slow down. We argue that this could raise even more concern regarding safety hazards that could occur due to the DMS hacking phenomena.

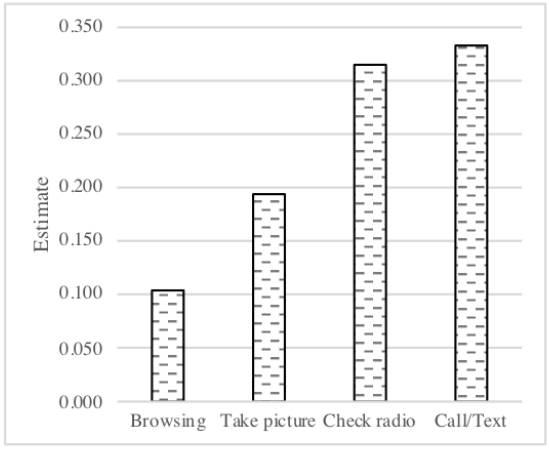
Under Sc1 social media and internet browsing had a lower impact but still, are among the factors that cause drivers to stop. Under the Sc3 scenario, several activities could motivate drivers to stop under the compromised DMS. These activities include (ordered from the highest to the lowest impact) call/text someone, picking up on the radio, taking a picture, and browse social media or internet. These activities are mainly striking since drivers tend to seek additional information from secondary sources.



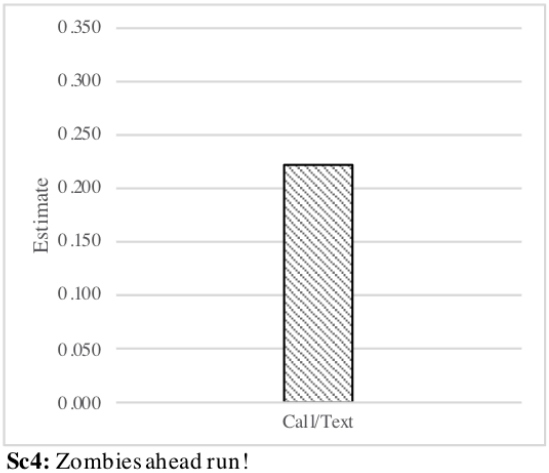
Sc1: Road Closure due to Police Activity



Sc2: Heavy Traffic due to accident



Sc3: Read The News Today, Oh Boy!



Sc4: Zombies ahead run!

Figure 24 causation factors of stopping behavior

5.4 Conclusion

The speed change pattern under advisory information has been investigated in the current literature (e.g., [11, 22, 160]). While the current studies were successful in exploring the speed pattern, their analysis failed to explain the speed change behavior under a hacked DMS. This study is unique in this domain research since it is not only exploring drivers' socio-demographic and attitudes toward a hacked DMS, but it considers four types of speed behavior simultaneously to understand the matter fully. In this paper, we presented speed choice models that investigated the explanatory power of certain variables on choices of speed. Theses choice include do-nothing (ignore the message and continue with current speed), speed up, slow down, and stop. This scrutiny provides valuable insight to policymakers to put in place effective policies to mitigate the risks that are associated with a compromised DMS. We summarized the key points of this study below:

- We developed multivariate ordered probit models to account for four choices of speed (i.e., do-nothing, speed up, slow down, and stop). We applied the multivariate model to account for heterogeneity in the error structure. The modeling approach allows for correlation between outcome variables error terms. In the modeling process, we considered the association of subjects socio-economic, demographic and attitudinal characteristics to the outcome variables. We tested and compared this linkage between four different scenarios under realistic and fictitious type content.
- We further examined the power of explanatory variables to understand various subjects' reaction to the given scenarios. We found many variables significant to different speed choices under both scenarios. We found the female, black, individuals with a disability, older, and those with high trust in DMS are less likely to ignore the fabricated messages. In contrary, white, those who drive long hours (i.e., 16 to 20 hours per week), and those who see driving as a tedious task are more likely to ignore the messages. Drivers who comply with traffic regulations and have a good driving record are likely to slow down under the messages. Furthermore, female drivers and those who live in rural areas are more likely to slow down under fabricated advisory information.
- Furthermore, we investigated whether route divergence behavior and involvement in distractive activities could cause speed variation. The tryout divulged that (a) under realistic scenarios, visual distraction and route change behavior are activities that have the highest impact on slow down behavior, (b) under fictitious scenarios, calling/texting someone, taking a picture of the sign, and picking up on radio are distracting activities which cause drivers to slow down, and (c) under a fabricated message, the calling and texting activities have the highest causation impact on the stopping behavior. Sudden speed change behaviors could impose safety risks [163]. For instance, unexpected slowdown and lane changing behaviors could increase the risk of a rear-end crash. The risk would be higher in high volume and highly congested roads.

This study investigated determinants of drivers' choice of speed under a compromised DSM with bogus content. The approach used in this study not only identified

the linkage of observed and unobserved variables with speed, but assessed the likely reasons behind the variation of speed. The outcome of this study provides promising hints to policymakers and engineers concerned with developing emergency and security incident response plans. We recommend future research to take the step forward and conduct a driving simulation study to assess the speed change behavior of the drivers in more details. Such study paves the road for a collection of more quantitative information on speed variation under a hacked DMS.

Chapter 6

6 Conclusion

Transportation system resiliency, efficiency, and reliability are highly dependent on the ITS infrastructure functionality. The cyber-physical attack on the ITS infrastructures imposes risks to the drivers and system operators. An adversary could convey a meaningful message to the drivers via the means of a DMS. The resiliency of the transportation system relies on the road users' response to the compromised DMS and the risks that these adversarial attacks could impose on the transportation system.

A provocative datum about DMS compared to other ITS infrastructures, is that through an adversarial attack a meaningful message could be conveyed en-route to the drivers. Previous studies have investigated the drivers' behavior in the presence of unreliable advisory information and concluded that drivers' compliance rate decreases in accordance with information reliability level. On the other side, drivers tend to comply with unreliable information and follow the spurious advisory messages.

A compromised DMS not only undermines the reliability of the ITS system but also biases drivers' decisions by coaxing them with forged information. Analysis indicated a significant speed reduction behavior mainly due to (1) increased attention demand (i.e., due to drivers' reaction to the message), and (2) following traffic compliance with speed reduction behavior of the lead traffic. Impulsive braking behavior, short headways, and lane changing maneuvers are likely to trigger safety hazards.

Attention to the DMS content would compromise drivers' safety. The supplied en-route information increases the frequency of distraction, that is, ensued due to three reasons. First, advanced technology can cause distraction for some of the drivers, second, drivers need to, read the message, comprehend, and decide based on the message content, and third drivers might tend to take a picture, call or text someone, talk to a passenger, think of something other than the driving task, and look at other vehicles. Both of these could cause conflicting attention demands between the acquiring task and driving task. The risk will be significant in cases where drivers need more time to react to the information and draw a decision.

6.1 Synthesis of findings

In this dissertation, I investigated the behavior of the road users under a compromised DMS as far as the route divergences, speed variation, and distraction activities are concerned. I postulated that an adversary could (1) coax drivers' decision, (2) engineer their speed behavior, and (3) induce drivers to become engaged with distracting activities. In this dissertation, I identified drivers' compliance behavior, as their positive attitude toward a compromised DMS. That is if a driver behaves in accordance with the fabricated messages, this dissertation presumes this behavior a compliance behavior. Otherwise, I consider it as a noncompliance behavior. The following sections synthesize the outcome of this dissertation with respect to the realistic and fictitious scenarios.

6.1.1 Fabricated-realistic scenarios

This dissertation scrutinized drivers' behavior under four different fabricated-realistic messages. These messages were "Heavy Traffic Due to Accident," and "Road Closure Due to Police Activity," "Downtown Under Terrorist Attack," and "Storm Watch, Flooding in Area Soon." The first two messages are traffic-related information, and the other two messages are informative related information. This section provides a summary of road users' compliance and noncompliance behavior under these four messages.

6.1.1.1 Demographic and socio-economic characteristics

This dissertation identified several socio-economic and demographic information with the association with the outcome variable of the realistic scenarios. Race, education, subjects' location, and household income are among those variables. Asian and low educated subjects have a negative attitude toward the sign. While in the fabricated-realistic scenario, individuals with higher income are more likely to divert under the DMS content. Also, this dissertation found a significant association between attitudinal variables and route divergence behavior in the road closure scenario. Those subjects that would take a new route in order to optimize their travel are more likely to depart from their planned route. This is also true for subjects that pay more attention to the DMS information in congested routes.

Subjects who saw a hacked DMS before indicated a negative attitude toward route divergence behavior. That is, drivers who speculate that the information could be fabricated, indicated less tendency toward changing their behavior. Furthermore, higher education also was found with a negative association with the fabricated content. Female drivers and subjects who in general are more familiar with the DMS would attempt to change their routes under realistic scenarios. Familiarity with DMS is another important factor that contributes to the drivers' compliance behavior. This dissertation discovered that drivers who are more familiar with the DMS, in general, are more likely to divert under fabricated realistic scenarios.

As far as the distraction behavior is concerned, the results found several of the explanatory variables of this study with a direct effect on two or three distraction constructs. These variables include, but not limited to race, education level, driving experience, age, speed choice behavior, driving style, and subjects general trust in DMS information. In addition, this dissertation found several background variables with a significant correlation with the likelihood of distraction while driving. The result indicated that students are more likely to become involved in distracted driving behavior in realistic scenarios. Drivers with anxious driving style (i.e., those who feel alertness and tension during driving), and those with the education of Bachelor's degree and higher are more prone to the distracted driving behavior. The anxious drivers would distract the most under the "Road Closure Due to Police Activity" content. In addition, experienced drivers (those with many years of driving experience), and those with high trust in DMS information are more likely to increase the risk of distraction. Subjects with white race would also increase the risk of distracted driving compared to the other races.

White, anxious drivers and drivers with high trust in DMS would involve in a cognitive type of distraction under the realistic scenarios. This dissertation found two interesting results involve the subjects that had previous accident experience. Those who were involved in an accident in general were less likely to use their phone under realistic scenarios. But the ones who were involved in an accident due to distraction would become involved in phone use, and cognitive-related activities under the compromised DMS. In addition, Asians and subjects who find driving a tedious task would positively contribute to the cognitive distraction. The modeling result also indicated that several background variables have a negative association with cognitive distraction. These variables identify subjects who are (1) patient and careful, (2) have low education, (3) black, (4) live in an urban setting, and (5) experienced drivers.

The main hypothesis is that subjects should comply with the false messages and slow down under the pretentious information. As the model result implies, female drivers, and subjects who live in rural areas are more likely to slow down under the DMS. The results indicate that while female and drivers who were involved in an accident are not willing to stop under the fabricated information, other drivers might stop. These subjects are those who drive minivan and van vehicle, black and African American subjects.

6.1.1.2 Attitudinal characteristics

As far as the attitudinal characteristic of the subjects is concerned. This research identified three groups of characteristics. These groups cluster subjects into drivers who (1) rely and trust in technology, (2) respect traffic regulation, and (3) have trouble understanding directions in unfamiliar routes. This dissertation investigated the correlation between each type of drivers and the outcome variables of this study.

The results indicated that tech-friendly drivers are more likely to comply with the fabricated-realistic content and would divert from their planned route. The modeling result indicated that drivers who rely on technology are more likely to slow down and depart from their planned route. That is, they are more comfortable in changing their route based on suggestions obtained from the secondary sources. At the same time, while they are acquiring new information, they need to decrease their speed to respond to the higher information load. More specifically, under the “Road Closure Due to Police Activity” scenario, tech-friendly drivers indicated a positive attitude toward the slow down behavior. As far as the distracting activities are concerned, I found a positive association between tech-friendly drivers and the three type of distraction– phone use, cognitive, and browsing. That is, tech-friendly drivers are more prone than other drivers to become engaged in distraction activities.

Drivers who respect traffic regulations and pay attention to the surrounding traffic are more likely to depart from their planned route under the realistic messages, notably the “Downtown Under Terrorist Attack,” and “Storm Watch, Flooding in Area Soon” messages. This type of drivers has higher trust in the DMS information and would comply with the sign to a higher degree. Consistent with the primary hypothesis of this study, Drivers who comply with traffic regulations are less likely to become involved in distraction activities. This type of drivers has a negative attitude toward phone-use and cognitive-related distractions activities– they mainly focus on their driving task. The

analysis did not identify a direct association between this type of drivers and speed choice behavior.

Subjects that have difficulties in understanding direction, especially in an unfamiliar route, are more likely to become engage in distractive activities under the "Heavy Traffic Due to Accident," and "Road Closure Due to Police Activity" messages. More specifically, they would become involved in cognitive related activities such as, mind wandering, talking to a passenger, and looking at surrounding traffic or scenery. Interestingly, these drivers are less likely to become engaged in activities such as picking up on the radio and browsing social media and internet under fabricated realistic content. In addition, this type of drivers is more likely to lower their speed at the presence of "Heavy Traffic Due to Accident" message. This finding is conceivable because subjects who have trouble finding their directions would need extra time to find a better route through the means of secondary sources.

6.1.1.3 Behavioral change association

The results confirmed that there is a strong link between route divergence and speed variation behaviors. This dissertation argues that drivers tend to lower their speed in order to react to the DMS information. Speed reduction behavior provides an adequate time frame for drivers to pay enough attention and decide whether they should change their route under the en-route information. Herein, I anticipate that drivers, in order to react to the fabricated information, would lower their speed. I tested this hypothesis by measuring the impact of slow down and stopping behavior on the route divergence behavior. The result indicated that in most of the realistic scenarios, drivers are more likely to slow down rather stop. However, in the "Heavy Traffic Due to Accident" scenario, the correlation between stopping and route divergence is higher. Overall, the likelihood of both slowing down and stopping behavior are higher under the "Storm Watch, Flooding in Area Soon" message.

In addition, I scrutinized the reasons behind each of the choices that subjects might take concerning distracting activities. To this extent, I tested the relationship between distracting activity and route change behavior with the speed choice outcome of the realistic scenarios. The distracting activities include taking a picture of the sign, call/text someone about the sign, talk to a passenger, browse social media or internet after seeing the sign, and picking up on the radio to gain more information about the en-route content. With respect to "Heavy Traffic Due to Accident" and "Road Closure Due to Police Activity" scenarios, one of the subject's reasons for paying attention to the sign is route change behavior. These signs alert subjects of a fake road closer or heavy traffic ahead of them. However, since the integrity of such messages is not clear to the subjects they consider changing their route. Further examination into this matter indicated that subjects tend to decrease their speed, and become engaged with distracting activities such as calling/texting someone, picking up on the radio, taking a picture, and looking at surrounding traffic.

6.1.2 Fictitious scenarios

In addition to the realistic messages, to mimic the real world DMS hacking incidents, this dissertation also considers the fictitious messages impact on drivers' behavior. These messages were "Read The News Today, Oh Boy!", and "Zombies ahead run!". Essentially, the importance of the fictitious messages lies with an understanding of speed choice and distraction behaviors. This section provides a summary of road users' compliance and noncompliance behavior under the fictitious messages.

6.1.2.1 Demographic and socio-economic characteristics

As far as the speed up behavior is concerned, under fictitious scenarios, all the significant factors have a negative association with the outcome variable. These variables are related to the driving experience, the extent that drivers read DMS information, subjects' race, income, and gender. All, but one, of determinants, were found with positive correlation to the slow down behavior under both the "Read The News Today, Oh Boy!" and "Zombie ahead run!" scenarios. Drivers of a single unit truck, anxious drivers, single and older individuals are the ones that would pay attention to the signs and slow down under fictitious message. This behavior could mainly raise from subjects' sensitivity to the news or simply from their interests in abnormal and infrequent messages. Either way, the sign would cause unexpected slow down behavior with the potential to create unsafe traffic pattern. The interesting fact is that those subjects who read DMS more often in their commute would not slow down under the message.

At the presence of the fictitious scenarios, subjects who have high education and those who have up to five years of driving experience tend to slow down under the "Zombie ahead run!" message. Subjects stopping behavior under the fictitious scenarios is also interesting to examine. Previous involvement in an accident, high trust to the DMS, and familiarity with the DMS are factors that inhibit subjects from stopping at the DMS with fictitious content. While living in an urban area, and relatively low driving experience are factors that contribute to the higher chance of stopping under these scenarios.

For all the scenarios, regardless of the content, calling/texting someone is the activity with the highest impact on the stopping behavior. This is very interesting since, under fictitious content, many drivers tend to take a picture of the sign. Results indicated that subjects would not stop to take a picture but slow down. This dissertation argues that this could raise even more concern regarding safety hazards that could occur due to the DMS hacking phenomena.

6.1.2.2 Attitudinal characteristics

The L-Tech latent factors have the highest positive impact on the L-phone distraction construct in regards to the fictitious scenario where a DMS warns drivers of a Zombie attack. Subjects with a good record of driving and those who comply with traffic regulation are less likely to engage in phone use related activities. The L-DriHabt latent factor, in fictitious scenarios, has negative linkage to the L-phone construct. This negative

effect is the highest for subjects at the presence of the "Read The News Today, Oh Boy!" sign. A similar pattern was found concerning the attention-averting distraction.

The results found L-DriHabt with a negative impact on the L-Cognitive construct in three of the scenarios. Meaning that drivers who respect traffic regulations would not pay attention to activities other than driving. Under fictitious scenarios, tech-friendly subjects are more likely to reach out to their vehicle infotainment system. This is similar to their behavior as far as the L-Phone and L-Cognitive distraction types are concerned.

As far as the speed variation behavior is concerned, the result identified a significant association only between L-DriHabt and do-nothing. Subjects who are attentive to the traffic regulations were identified as subjects who would not change their travel speed under the fictitious messages. The other two attitudinal latent factors did not have a significant association with choices of the speed under the fictitious scenarios.

6.1.2.3 Behavioral change association

Route change behavior did not have a significant contribution to the slow down behavior under fictitious scenarios. Under the "Read The News Today, Oh Boy!" message, picking up on the radio had the most impact on the slow down behavior. Taking a picture of the sign and calling/texting someone about the sign had a lower impact. Under the "Read The News Today, Oh Boy!" content, several activities were identified as a motivating factor for drivers to stop under the compromised DMS. These activities include (ordered from the highest to the lowest impact) call/text someone, picking up on the radio, taking a picture, and browse social media or internet. These activities are mainly striking since drivers tend to seek additional information from secondary sources.

This dissertation identified similar results with respect to the divers' distraction behaviors under fictitious scenarios. The result indicated a positive association between slow down and stopping behavior and the phone-use, and browsing activities. For all the models, the slow down behavior has a higher impact than stopping behavior. The slow down behavior has the highest association to the phone use activity under the "Zombie ahead run!" message. Subjects' stopping behavior has the highest association to the phone-use related activates. Meaning that there is a higher chance for subjects to stop under the fictitious messages in order to use their phone rather picking up on vehicle radio.

6.2 Dissertation contributions

This work sets the foundation on how to understand and assess the impact of the cyber-physical attacks on the transportation network by means of qualitative and quantitative risk-based approaches. I summarize the main contribution of this dissertation below.

This dissertation, for the first time, employed a risk-based approach to conducting a threat assessment. This threat assessment performs a qualitative vulnerability-oriented threat analysis. The objective was to investigate safety, security, reliability, and operation issues that are triggered by a compromised DMS. It needs to be understood that with the progression of technology, the operator's understanding must also change. With the increasing complexity and the integration of the system, operators have to look at this

situation on a system level instead of as a collection of isolated incidents. Future ITS implementations need to be designed with adequate security in mind from inception. At this time, it can be concluded that the physical and cyber hackings of DMS create the slowdown of traffic, they also have the potential to threaten road users' safety and to create financial losses in the affected communities. Crashes, fatalities, congestion, and public chaos are among the possible outcomes of tampering with transportation network critical infrastructures. Sudden changes in drivers' behavior while passing a tampered message sign could lead to devastating incidents. Also, from an operation and security standpoint, authorities need to foresee the situation to plan effective countermeasures to minimize the risk of partial or complete losses of the system.

This dissertation, for the first time, investigated drivers' route divergence behavior under a false en-route advisory information. In this study, I explored drivers attitudes toward a hacked DMS in order to understand their route departure behavior. This study investigated drivers' perception toward a hacked DMS. The modeling approach enabled this research to capture subject socio-economic and demographic, and attitudinal characteristics toward route divergence behaviors. The approached allowed this research to understand how respondents with a different background, driving style, driving habit, and attitude toward DMS would react to a fabricated-realistic en-route message.

In this dissertation, for the first time, I focused on scenarios in reference to the previous threat events to form a set of creative forged messages to assess drivers' decision. In addition, I took a step forward and examined drivers' distraction behavior under a fabricated realistic message as well. The modeling approach of this study allowed this research to account for both subjective attribute and objective determinants of the population. The subjective attributes helped this research to test information that is not acknowledged by the subjects directly. The layers of the SEM models also enabled this research to understand the attitudes of drivers with different background toward the three-type of distraction.

In this dissertation, for the first time, I argue that not only DMS would not be lucrative to road users but would detriment the safety and operation of the transportation system. This study investigated travelers' speed choice behavior under realistic and fictitious fabricated DMS content. This study investigated determinants of drivers' choice of speed under a compromised DSM with bogus content. The approach used in this study not only identified the linkage of observed and unobserved variables with speed but assessed the likely reasons behind the variation of speed.

6.3 Dissertation significance

For each problem that I tackled, this dissertation provided an in-depth investigation and uncovered significant outcomes. A summary of the dissertation significance, practical, and research implications are discussed in this section. Additional discussion about this dissertation significance and future research directions are provided in section 6.5.

As far as the research implications are concerned, the broader impacts of this dissertation include to raise awareness among policy-makers and engineers systematically, to motivate further simulations and real-world experiments to investigate this matter

further, and to systematically assess the adverse impact of a security breach on transportation reliability and safety, and drivers' behavior. The outputs of the study are projected to assist traffic engineer and policymakers to enhance the transportation system resiliency and security by means of future research. The qualitative and quantitative impact assessment communicates valuable insights to the system operators to mitigate risks that are imposed on the transportation system. The results infer insights for the identification of the security best practices and development of novel security countermeasures. This dissertation outcome agrees with the fact that ITS components are hackable, regardless of how robust security measures are.

Additionally, the outcome can be integrated with the nationwide connected vehicle and V2X implementations and security design. Understanding the behavior of the road users at the presence of a compromised DMS would assist researchers to mimic drivers' behavior under more significant threats. For instance, with respects to the connected vehicle safety applications, this study outcomes would be of help to scrutinize drivers' behavior under fabricated Basic Safety Messages (BSM).

As far as the practical implications are concerned, the results would be of help for the development of the security and emergency preparedness plans and incident response plans. I believe that transportation management centers need to have a separate division comprised of experts in the security field, to respond to the cyber-physical attacks. Understanding the behavior of the users under such an attack would be a valuable advantage for emergency respondents to mitigate the risk. The result of this dissertation could assist system operators in order to identify the hot spots that could impose the highest cost to the system. The hot spots could be with respect to the drivers' population and the physical distribution of the assets. By knowing how different type of people would react to the sign, authorities could place an education program to familiarize drivers of such event. On the other hand, system operators could elaborate on this research and identify high-risk locations in which DMS hacking would cause the highest dire impact. Prioritizing the locations would pave the road for effective risk management.

6.4 Dissertation limitation

6.4.1 Data

While mTurk offers various benefits to the research community, it suffers from a fundamental limitation. The limitation arises from the fact that mTurk workers population is limited to 100k-200k subjects. That is, the data collected from the mTurk might not perfectly represent the population of a particular geographic area. I encourage future researchers to employ other means of data collection in order to enhance the quality of the data. The fusion of multiple data sources would be another approach that ensures high quality, consistent data. Nonetheless, I encourage the application of the driving simulation studies for in-depth investigation of drivers' behavior at the compromised DMS.

6.4.2 Dimension of the data

Inquiring detailed information regarding subjects' attitudes toward the use of technology is a key to evaluate their reaction to the DMS. That is, in the survey questionnaire of this dissertation, I asked subjects to rate their trust and reliance on technology under four statements. These include (1) I rely on technology for my daily trips, (2) I check traffic condition before hitting the road, (3) I trust technology to assist in my travel, and (4) I feel that I get more accomplished because of technology. For future research, I encourage to expand this dimension via asking supplementary questions. Expanding this topic could have a fruitful impact on the understanding of driver's attitude toward the application of technology. One possible example is to gauge subjects' attentiveness to the in-vehicle GPS (Global Positioning System) device for their day-to-day commute. Also, more in-depth evaluation of subjects' driving style could offer valuable insight to fathom their likely behavior under a compromised DMS.

6.5 Future research avenues

This dissertation aimed to communicate risk outcomes of a compromised DMS to two types of audiences. These audiences include experts with a focus on the security aspect of the ITS network and those who are concerned with the adverse impact of cyber-physical attacks on the transportation network. In this section, I discuss the potential research avenue that needs to be pursued to address the current gaps in literature and practice.

6.5.1 Security standpoint

6.5.1.1 Attack/threat analysis

The comprehensive analysis of security issues related to the DMS physical and communication network vulnerabilities need to be conducted. Identifying the problem areas and classification of the DMS security issues should be implemented as a fundamental step prior to development/employment of security countermeasures. A well-established approach to classify security threats could be the use of Confidentiality, Integrity, and Availability (CIA) scheme. Augmenting CIA scheme through authentication, non-repudiation, and identification security services could provide better insight over the DMS security vulnerabilities. The security classification should be accompanied by attack identification to shed lights on the collection of apt security countermeasure that ensures ITS secure and resilient operation.

6.5.1.2 Vulnerability assessment

There is a need for research effort regarding the vulnerability assessment of the DMS. Most of the ITS components have been designed with no or minimal security development in the design phase. The majority of research aims at post-development of security measures, leaving many gaps in developing guidelines, standards, and cybersecurity frameworks for DMS secure design. Considering the current pressing shift

toward an integrated and connected ITS network, raise the necessity for DMS with adequate security in mind from inception.

6.5.1.3 Countermeasures

This dissertation asserts that it is indispensable for DMS manufacturers and transportation system operators to employ security countermeasures in order to prevent adversaries from compromising the DMS. Cybersecurity best practices could be employed as a short-term solution to the DMS hacking incidents, but not to ensure a resilient and sustainable system for long term practice. Here, this dissertation recommends the application of several cybersecurity best practices and discuss future research line for the development of novel security countermeasures.

Best practices

At the presence of any security footholds, adversaries will be able to compromise the system and cause dire consequences. Thus, the DMS security should be ensured at each layer of the security. As far as the cybersecurity best practices are concerned, this dissertation recommended several countermeasures. These countermeasures include (a) to place the display on a private network or VPN, (b) to deactivate unnecessary telnet, webpage and LCD interfaces, (c) to avoid using hard-coded/default passwords, but instead secure the access with strong and complex password, (d) to minimize network exposure, (e) to isolate control network from business network, (f) to secure the remote access for authorize users, (g) to implement an authentication mechanism against physical attacks, (h) to upgrade SNMP to the most current version, (i) to enable remote logging and Monitor the logs, (j) to change all SNMP community string from the default, (k) whitelisting and blacklisting the keywords, (l) temporal based filtering to prevent DMS content alteration at unauthorized schedule, and (m) network security zoning.

This dissertation aimed to raise awareness to understand and employ security best practices of cyber hygiene, access control, risk management, information security, and monitoring. Network redundancy is required in advance to prevent the failure of critical infrastructures. In addition to the cybersecurity best practices, novel Intrusion detection systems (IDS) are effective in identifying anomalous activities in the network. Also, encryption methods can secure network communications and stop hackers from easily manipulating the infrastructures. More prominently a practical approach would be to exercise white hat hackers' skills to constantly monitor vulnerabilities of the ITS critical infrastructure before adversaries could breach the system. Reminder part of this section discusses advance security-based countermeasures that are needed to be employed for the case of DMS.

Digital solutions

Even though most of the cyber-physical systems are equipped with cryptographic solutions, usually at practice it is left as an optional item for the system users. Using advanced cryptographic techniques such as digital signatures or message authentication codes, along with keys long enough (e.g., 128 as common practice) to provide adequate

protection are the well-known and established solutions. Transportation system operators need to evaluate the current digital solutions and develop security countermeasure compatible with the DMS system. There is a gap in both research and practice to improve current security practices that are not enough to fix security issues. Future research is necessary to identify more expensive security countermeasures to stop future attacks.

Intrusion Detection and prevention System

The intrusion detection system (IDS) is a hardware or software with the aim to detect network intrusion automatically. The intrusion prevention system (IPS) is a supplement to the IDS that could attempt to prevent adversaries from compromising the system. IDS techniques could be classified into anomaly (behavioral), signature (knowledge), and protocol-based methodologies. Currently, there are extensive research efforts available concerning each of the IDS types development, assessment, and implications. However, the development and application of such well-known technology are not mature in the field of ITS, especially as far as the DMS security is concerned. This dissertation endorses future research directions toward the application of the IDS and IPS techniques in order to ensure DMS secure and resilient operation.

Another technique to secure wireless communication is to use physical-layer-identification (PLI) based IDS for the devices that are connected to the DMS communication network. According to this method, also called fingerprinting, certain anomalies in the analog signal (which are caused by manufacturing inconsistencies) are used for generating templates that are unique for each radio hardware. The fingerprints exploiting could be conducted through machine learning techniques. Not only these fingerprints are unique to each device, but also, they are not mimicable. Advantages of PLI based IDS techniques makes them a lucrative alternative in order to secure the DMS system. That is, I encourage future research to investigate the effectiveness of the PLI based IDS to prevent adversaries from compromising the DMS functionality.

6.5.1.4 Machine learning and Artificial intelligence

The application of machine learning (ML) and artificial intelligence (AI) techniques in the security domain is nascent but growing. The adaptation of the ML and AI techniques needs to be investigated in the field of ITS for the purpose of (1) identifying threats (i.e., anomaly detection), (2) mitigating the threats, and (3) defending against security attacks. For instance, in the case of DMS, a difficult task is to authenticate the integrity of the realistic-fabricated messages. Data fusion approaches would be practical in order to feed additional data to the machine learning algorithm. The algorithm then would judge the message alteration incident by taking into consideration various sources of information. Application of the text mining algorithms also would be crucial in validating the integrity of the DMS content.

6.5.2 Transportation system management standpoint

6.5.2.1 Safety measurement

Measuring safety at the presence of the compromised DMS is a difficult task. This dissertation identified safety impact of DMS hacking DMS as a consequence with the high-impact high-likelihood outcome. The qualitative and quantitative analysis indicated that road users are attentive to the fabricated information. The drivers' attentiveness to the false information could cause drivers to become distracted, and change their speed choice behavior unexpectedly. Both behaviors would emerge disturbance in the traffic pattern that triggers safety hazards. Measuring the safety outcome as far as the frequency and severity of the crashes is concerned is very important. Future research could attempt to conduct a safety analysis to identify hot spots and vulnerable road users. The results of such studies would have a policy and design implications with the aim to improve the safety of the transportation system under cyber-physical attack.

6.5.2.2 System reliability

The credibility of DMS is extremely important to achieve efficient operation. Drivers eventually will not pay attention to the messages they distrust. The outcome of this dissertation indicated that road users' trust in the ITS system could drop at the presence of security vulnerabilities. The drivers' distrust in the DMS content would threat the effectiveness of the technology, undermining system operators' effort and expenses. That is, there is a need for future research to systematically analyze the impact that DMS hacking phenomena could have on system reliability.

6.5.2.3 Road users' education

The result of this dissertation indicated that subjects who saw a compromised DMS before are less likely to comply with the fabricated information. To this extent, the outcome of this dissertation supports the efforts to raise awareness among road users and to familiarize them with the DMS hacking phenomena. There is a gap in the literature to assess policy implications that could educate road users about the system vulnerabilities and the potential of an adversarial attack on DMS. Also, there is a need for assessing the importance of education to improve the interaction between drivers and a compromised DMS.

6.5.2.4 Emergency respondent training

To respond efficiently to the future cyber-physical attacks on DMS, transportation agencies need to train emergency respondent and experts. So far, emergency respondent experience and respond to the compromised DMS have not been efficient. There is an eminent need for trained personnel and effective communication between TMC and field responders to mitigate the adverse impact of a cyber-physical attack. Future research could evaluate various strategies to address this issue.

6.5.2.5 Effective communication with affected road users

There is a need for future research for identifying ways to notify the driver in real-time of a fabricated DMS content. Effective communication is crucial to improve drivers' behavior under a compromised DMS. The communication needs to be real-time, fast, secure, resilient, and efficient. At the same time, communication should not cause drivers to become distracted while driving. Thus, the format and wording of the message and the medium in which system operators would communicate to the drivers with the right instruction are of vital importance. Effective communication is more eminent in case of fabricated-realistic messages that could coax drivers' decision.

References

[1] Roads & Bridges, "Amped-up traffic signs imminent for NJ expressways." [Online]. Available: https://www.roadsbridges.com/amped-traffic-signs-imminent-nj-expressways.

[2] S. Peeta, J. Ramos, and R. Pasupathy, "Content of variable message signs and on-line driver behavior," *Transp. Res. Rec. J. Transp. Res. Board*, no. 1725, pp. 102–108, 2000.

[3] H. Dia, "An agent-based approach to modelling driver route choice behaviour under the influence of real-time information," *Transp. Res. Part C Emerg. Technol.*, vol. 10, no. 5–6, pp. 331–349, 2002.

[4] A. Khattak, A. Polydoropoulou, and M. Ben-Akiva, "Modeling revealed and stated pretrip travel response to advanced traveler information systems," *Transp. Res. Rec. J. Transp. Res. Board*, no. 1537, pp. 46–54, 1996.

[5] A. Richards and M. McDonald, "Questionnaire surveys to evaluate user response to variable message signs in an urban network," *IET Intell. Transp. Syst.*, vol. 1, no. 3, pp. 177–185, 2007.

[6] M. Wardman, P. W. Bonsall, and J. D. Shires, "Driver response to variable message signs: a stated preference investigation," *Transp. Res. Part C Emerg. Technol.*, vol. 5, no. 6, pp. 389–405, 1997.

[7] R.-C. Jou, S.-H. Lam, Y.-H. Liu, and K.-H. Chen, "Route switching behavior on freeways with the provision of different types of real-time traffic information," *Transp. Res. Part Policy Pract.*, vol. 39, no. 5, pp. 445–461, 2005.

[8] M. A. Abdel-Aty and M. FathyAbdalla, "Examination of multiple mode/route-choice paradigms under ATIS," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 3, pp. 332–348, 2006.

[9] E. Ben-Elia and Y. Shiftan, "Which road do I take? A learning-based model of route-choice behavior with real-time information," *Transp. Res. Part Policy Pract.*, vol. 44, no. 4, pp. 249–264, 2010.

[10] A. Erke, F. Sagberg, and R. Hagman, "Effects of route guidance variable message signs (VMS) on driver behaviour," *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 10, no. 6, pp. 447–457, 2007.

[11] X. Yan and J. Wu, "Effectiveness of variable message signs on driving behavior based on a driving simulation experiment," *Discrete Dyn. Nat. Soc.*, vol. 2014, 2014.

[12] C. Wang, K. Dixon, and D. Jared, "Evaluating speed-reduction strategies for highway work zones," *Transp. Res. Rec. J. Transp. Res. Board*, no. 1824, pp. 44–53, 2003.

[13] N. J. Garber and S. T. Patel, "Control of vehicle speeds in temporary traffic control zones (work zones) using changeable message signs with radar," *Transp. Res. Rec.*, no. 1509, pp. 73–81, 1995.

[14] Z. Ma, C. Shao, Y. Song, and J. Chen, “Driver response to information provided by variable message signs in Beijing,” *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 26, pp. 199–209, 2014.

[15] Z.-R. Peng, N. Guequierre, and J. Blakeman, “Motorist response to arterial variable message signs,” *Transp. Res. Rec. J. Transp. Res. Board*, no. 1899, pp. 55–63, 2004.

[16] S. Foo and B. Abdulhai, “Evaluating the impacts of changeable message signs on traffic diversion,” in *Intelligent Transportation Systems Conference, 2006. ITSC’06. IEEE*, 2006, pp. 891–896.

[17] L. Kattan, K. Habib, S. Nadeem, and T. Islam, “Modeling Travelers’ Responses to Incident Information Provided by Variable Message Signs in Calgary, Canada,” *Transp. Res. Rec. J. Transp. Res. Board*, no. 2185, pp. 71–80, 2010.

[18] S. Zhong, L. Zhou, S. Ma, and N. Jia, “Effects of different factors on drivers’ guidance compliance behaviors under road condition information shown on VMS,” *Transp. Res. Part Policy Pract.*, vol. 46, no. 9, pp. 1490–1505, 2012.

[19] S. Basheer, K. K. Srinivasan, and R. Sivanandan, “Investigation of Information Quality and User Response to Real-Time Traffic Information Under Heterogeneous Traffic Conditions,” *Transp. Dev. Econ.*, vol. 4, no. 2, p. 8, 2018.

[20] A. Richards, M. McDonald, G. Fisher, and M. Brackstone, “Investigation of driver comprehension of traffic information on graphical congestion display panels using a driving simulator,” *Eur. J. Transp. Infrastruct. Res.*, vol. 4, no. 4, p. 2004, 2004.

[21] E. Ben-Elia, I. Erev, and Y. Shiftan, “The combined effect of information and experience on drivers’ route-choice behavior,” *Transportation*, vol. 35, no. 2, pp. 165–177, 2008.

[22] A. Erke, F. Sagberg, and R. Hagman, “Effects of route guidance variable message signs (VMS) on driver behaviour,” *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 10, no. 6, pp. 447–457, 2007.

[23] D. De Waard and K. A. Brookhuis, “On the measurement of driver mental workload.,” *Traffic Transp. Psychol. Theory Appl.*, pp. 161–171, 1997.

[24] D. Shinar and E. Schechtman, “Headway feedback improves intervehicular distance: A field study,” *Hum. Factors*, vol. 44, no. 3, 2002.

[25] K. B. Kelarestaghi, K. Heaslip, V. Fessmann, M. Khalilikhah, and A. Fuentes, "Intelligent transportation system security: hacked message signs," SAE International Journal of Transportation Cybersecurity & Privacy, vol. 1, no. 2, doi:10.4271/11-01-02-0004, 2018.

[26] Krebs on Security, “They Hack Because They Can.” [Online]. Available: http://krebsonsecurity.com/2014/06/they-hack-because-they-can/comment-page-1.

[27] “Daktronics Vanguard Default Credentials (Update A)," ICS-CERT. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-155-01A.

[28] P. Tassi, “Aiden Pearce, Snooping Superhero: The Strange Moral Compass of ‘Watch Dogs.’” [Online]. Available:

https://www.forbes.com/sites/insertcoin/2014/05/28/aiden-pearce-snooping-superhero-the-strange-moral-compass-of-watch-dogs/#33fb59d95881.

[29] "'Caution Zombies Ahead': N. Va. electronic sign hacked", The Washington Post. [Online]. Available: https://www.washingtonpost.com/blogs/the-buzz/post/caution-zombies-ahead-n-va-road-sign-hacked/2011/05/11/AFPObEsG_blog.html. [Accessed: 15-Dec-2015].

[30] "Dude! What did that traffic sign say?," The Sacramento Bee. [Online]. Available: http://www.sacbee.com/news/local/transportation/back-seat-driver/article39697362.html.

[31] "Cyberattacks are surging and more data records are stolen." [Online]. Available: https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html.

[32] "With Cyber Attacks On the Rise, Here's How Companies Can Mitigate Their Risks," HuffPost. [Online]. Available: https://www.huffingtonpost.com/entry/with-cyber-attacks-are-on-the-rise-heres-how-companies_us_59c1787ae4b0c3e70e742883.

[33] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures," *ArXiv Prepr. ArXiv190301541*, 2019.

[34] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Intelligent Transportation System Security: Impact-Oriented Risk Assessment of In-Vehicle Networks," IEEE Intelligent Transportation Systems Magazine, doi: 10.1109/MITS.2018.2889714, 2019.

[35] "Top 5 Industries At Risk Of Cyber-Attacks." [Online]. Available: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#8831db3715e9.

[36] "What Cyberthreats Do Higher Education Institutions Face?" [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/#24b35d7b640d.

[37] "Ransomware Cyber Attacks: Which Industries Are Being Hit The Hardest?" [Online]. Available: https://www.bitsighttech.com/blog/ransomware-cyber-attacks. [Accessed: 14-Feb-2018].

[38] L. E. Y. Mimbela and L. A. Klein, "Summary of vehicle detection and surveillance technologies used in intelligent transportation systems," 2000.

[39] K. Dellios, D. Papanikas, and D. Polemi, "Information Security Compliance over Intelligent Transport Systems: Is IT Possible?," *IEEE Secur. Priv.*, no. 3, pp. 9–15, 2015.

[40] E. Fok, "An Introduction to Cybersecurity Issues in Modern Transportation Systems," *ITE J.*, p. 19, 2013.

[41] "IOActive Labs Research: Hacking US (and UK, Australia, France, etc.) Traffic Control Systems." [Online]. Available: http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html.

[42] "Protection of Transportation Infrastructure from Cyber Attacks: A Primer," National Academies of Sciences, Engineering, and Medicine, NCHRP Document 221, 2015.

[43] C. L. Dudek, *Changeable message sign operation and messaging handbook*. Federal Highway Administration, Operations Office of Travel Management, 2004.

[44] J. Atkinson *et al.*, "Designing for Transportation Management and Operations: A Primer," 2013.

[45] K. Chatterjee, N. B. Hounsell, P. E. Firmin, and P. W. Bonsall, "Driver response to variable message sign information in London," *Transp. Res. Part C Emerg. Technol.*, vol. 10, no. 2, pp. 149–169, 2002.

[46] "Intelligent Transportation Systems Design Manual," Wisconsin Department of Transportation, Madison, 2000.

[47] T. Kosch, I. Kulp, M. Bechler, M. Strassberger, B. Weyl, and R. Lasowski, "Communication architecture for cooperative systems in Europe," *Commun. Mag. IEEE*, vol. 47, no. 5, pp. 116–125, 2009.

[48] R. S. Ross, "Guide for conducting risk assessments," 2012.

[49] N. J. T. F. T. Initiative, "Managing Information Security Risk: Organization, Mission, and Information System View," *NIST Spec. Publ.*, pp. 800–39, 2011.

[50] B. Schneier, "Attack trees," *Dr Dobb's J.*, vol. 24, no. 12, pp. 21–29, 1999.

[51] "HOW TO - Hack construction signs | Make: DIY Projects, How-Tos, Electronics, Crafts and Ideas for Makers." [Online]. Available: http://makezine.com/2009/01/27/how-to-hack-construction-signs/.

[52] "How To Hack An Electronic Road Sign." [Online]. Available: http://jalopnik.com/5141430/how-to-hack-an-electronic-road-sign?trending_test_d&utm_expid=66866090-62.H_y_0o51QhmMY_tue7bevQ.4&utm_referrer=http%3A%2F%2Fjalopnik.com%2F5144628%2Ftraffic-sign-hacking-spreads-to-indiana%3Ftrending_test_d.

[53] "Road sign hacking | Hackaday." [Online]. Available: http://hackaday.com/2009/01/24/road-sign-hacking/.

[54] "This sign has been hacked," Apr-2007. [Online]. Available: http://hacks.mit.edu/Hacks/by_year/2007/sign_hacked/index.html.

[55] "Austin Road Signs Hacked, Warn of Nazi Zombies and World's End | WIRED." [Online]. Available: http://www.wired.com/2009/02/austin-road-sig/.

[56] "Hackers Crack Into Texas Road Sign, Warn of Zombies Ahead | Fox News." [Online]. Available: http://www.foxnews.com/story/2009/01/29/hackers-crack-into-texas-road-sign-warn-zombies-ahead.html.

[57] "Road Sign Hacking: Harmless Prank or Safety Threat? | Traffic Control Equipment | Flexible High Impact Delineation." [Online]. Available: http://www.impactrecovery.com/resources/road_sign_hacking_harmless_prank_or_safety_threat/.

[58] "Another road sign warns of zombies | Metro News." [Online]. Available: http://metro.co.uk/2009/02/05/another-road-sign-warns-of-zombies-432840/.

[59] "Road sign prank warns drivers of zombies - NY Daily News." [Online]. Available: http://www.nydailynews.com/news/world/midwest-road-sign-prank-warns-drivers-zombies-article-1.388519.

[60] "'Raptors Ahead' Sign Gets Stares, Chuckles - TheIndyChannel.com." [Online]. Available: http://www.theindychannel.com/news/-raptors-ahead-sign-gets-stares-chuckles.

[61] "MAKING LIGHT OF THE LAW | New York Post." [Online]. Available: http://nypost.com/2009/03/17/making-light-of-the-law/.

[62] "Thank goodness! UF has a plan for zombie invasions," Oct-2009. [Online]. Available: http://www.gainesville.com/article/20091002/articles/910021006.

[63] "Don't fear: Zombies are not near," Dec-2009. [Online]. Available: http://www.gainesville.com/article/20091222/articles/912221017.

[64] "Miami construction sign hacked to read 'No Latinos,' 'No Tacos' - tribunedigital-sunsentinel." [Online]. Available: http://articles.sun-sentinel.com/2010-05-26/news/fl-roadsigns-hacked-20100525_1_sign-hacked-construction-site.

[65] "'Zombies Ahead': Construction sign tells Maine drivers to be very afraid - CBS News." [Online]. Available: http://www.cbsnews.com/news/zombies-ahead-construction-sign-tells-maine-drivers-to-be-very-afraid/.

[66] "'Caution Loose Gorilla': Electronic road sign hacked in Northern California - CBS News." [Online]. Available: http://www.cbsnews.com/news/caution-loose-gorilla-electronic-road-sign-hacked-in-northern-california/.

[67] "Construction board hacked in Granite Bay, changed to obscene saying | News - KCRA Home." [Online]. Available: http://www.kcra.com/news/construction-board-hacked-in-granite-bay-changed-to-obscene-saying/24277104.

[68] "Mililani digital road sign hacked with offensive message | KHON2." [Online]. Available: http://khon2.com/2015/09/19/mililani-digital-road-sign-hacked-with-offensive-message/.

[69] "23 Great Hacked Road Signs | Stuff You Should Know." [Online]. Available: http://www.stuffyoushouldknow.com/blog/gallery/hacked-road-signs/.

[70] E. Fok, "Cyber Security Challenges: Protecting Your Transportation Management Center," *ITE J.*, vol. 85, no. 2, 2015.

[71] U.S. Department of Homland Security, "Strategy for Securing Control Systems: Coordinating and Guiding Federal, State and Private Sector Initiatives," U.S. Department of Homland Security, Washington, DC, USA, 2009.

[72] "'Watch Dogs' Video Game Will Inspire More 'Godzilla Attack' Road Sign Hacks, Says Cybersecurity Warning." [Online]. Available: https://www.forbes.com/sites/kashmirhill/2014/06/09/watch-dogs-road-sign-hacks/#78d0489f4e55.

[73] "SUN HACKER (@ISUN_HACKER) | Twitter." [Online]. Available: https://twitter.com/isun_hacker.

[74] "D.O.T. Signs Hacked In Asheville & Statewide - YouTube." [Online]. Available: https://www.youtube.com/watch?v=YJG9fRv_6Js.

[75] "Flaw Lets Hackers Control Electronic Highway Billboards - Nextgov." [Online]. Available: http://www.nextgov.com/cybersecurity/2014/06/flaw-lets-hackers-control-electronic-highway-billboards/85849/.

[76] "'Godzilla Attack' prompts DMS recommendations," 16-Jun-2014. [Online]. Available: http://www.traffictechnologytoday.com/news.php?NewsID=59883.

[77] M. Jeihani, S. NarooieNezhad, and K. B. Kelarestaghi, "Integration of a driving simulator and a traffic simulator case study: exploring drivers' behavior in response to variable message signs," IATSS research, vol. 41, no. 4, pp. 164–171, 2017.

[78] J. Olofsson, "'Zombies ahead!'A study of how hacked digital road signs destabilize the physical space of roadways," *Vis. Commun.*, vol. 13, no. 1, pp. 75–93, 2014.

[79] "Hacked road signs in Austin - YouTube." [Online]. Available: https://www.youtube.com/watch?v=1Lw0WMyChrM.

[80] A. M. Khan, "Intelligent infrastructure-based queue-end warning system for avoiding rear impacts," *Intell. Transp. Syst. IET*, vol. 1, no. 2, pp. 138–143, 2007.

[81] P. B. Wiles, S. A. Cooner, C. H. Walters, and E. J. Pultorak, "Advance warning of stopped traffic on freeways: current practices and field studies of queue propagation speeds," 2003.

[82] S. G. Klauer, T. A. Dingus, V. L. Neale, J. D. Sudweeks, and D. J. Ramsey, "The impact of driver inattention on near-crash/crash risk: An analysis using the 100-car naturalistic driving study data," 2006.

[83] S. E. Lee, E. Llaneras, S. Klauer, and J. Sudweeks, "Analyses of rear-end crashes and near-crashes in the 100-car naturalistic driving study to support rear-signaling countermeasure development," *DOT HS*, vol. 810, p. 846, 2007.

[84] "The Use of Forward Collision Avoidance Systems to Prevent and Mitigate Rear-End Crashes," National Transportation Safety Board, May 2015.

[85] L. Tudor, A. Meadors, and R. Plant, "Deployment of smart work zone technology in Arkansas," *Transp. Res. Rec. J. Transp. Res. Board*, no. 1824, pp. 3–14, 2003.

[86] L. Chu, H.-K. Kim, Y. Chung, and W. Recker, "Evaluation of effectiveness of automated work zone information systems," *Transp. Res. Rec. J. Transp. Res. Board*, no. 1911, pp. 73–81, 2005.

[87] M. Tooley, J. Gattis, R. Janarthanan, and L. Duncan, "Evaluation of automated work zone information systems," *Transp. Res. Rec. J. Transp. Res. Board*, no. 1877, pp. 69–76, 2004.

[88] T. Morris, J. A. Schwach, and P. G. Michalopoulos, "Low-Cost Portable Video-Based Queue Detection for Work-Zone Safety," 2011.

[89] "Tucson digital traffic sign hacked, warns of 'Zombies Ahead' - Tucson News Now." [Online]. Available: http://www.tucsonnewsnow.com/story/29466781/tucson-digital-traffic-sign-hacked-warns-of-zombies-ahead.

[90] "L.A. Traffic Sign Is Hacked to Say 'Read a F——ing Book' (PHOTOS) | L.A. Weekly." [Online]. Available: http://www.laweekly.com/news/la-traffic-sign-is-hacked-to-say-read-a-f-ing-book-photos-5331670.

[91] "Hackers made an LA traffic sign say 'READ A FUCKING BOOK' » MobyLives." [Online]. Available: http://www.mhpbooks.com/hackers-made-an-la-traffic-sign-say-read-a-fucking-book/.

[92] "Los Angeles traffic sign hacked with obscene message (Photo)." [Online]. Available: http://fansided.com/2015/01/11/los-angeles-traffic-sign-hacked-obscene-message-photo/.

[93] "Downtown Los Angeles traffic sign hacked - AOL." [Online]. Available: http://www.aol.com/article/2015/01/10/downtown-los-angeles-traffic-sign-hacked/21127825/.

[94] "Hacked road sign warns Flagstaff drivers of panda rampage." [Online]. Available: http://tucson.com/news/state-and-regional/hacked-road-sign-warns-flagstaff-drivers-of-panda-rampage/article_8c5e1e72-cda7-11e0-a057-001cc4c03286.html.

[95] "Police: No rogue pandas about." [Online]. Available: http://azdailysun.com/news/local/police-no-rogue-pandas-about/article_420be32f-7571-5507-9ce9-58b6f6ea8d4f.html.

[96] "Hacked Miami road sign highlights password and physical security lapses - TechRepublic." [Online]. Available: http://www.techrepublic.com/blog/tr-dojo/hacked-miami-road-sign-highlights-password-and-physical-security-lapses/.

[97] "Wireless M2M Solutions for Changeable Message Signs for Traffic Managers," Jan-2015. [Online]. Available: http://govmobile.com/author/govmobile/.

[98] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for Cellular-assisted V2X Communication," *Veh. Commun.*, 2018.

[99] K. Chatterjee, N. B. Hounsell, P. E. Firmin, and P. W. Bonsall, "Driver response to variable message sign information in London," *Transp. Res. Part C Emerg. Technol.*, vol. 10, no. 2, pp. 149–169, 2002.

[100] S. Peeta and J. L. Ramos, "Driver response to variable message signs-based traffic information," in *IEE Proceedings-Intelligent Transport Systems*, 2006, vol. 153, pp. 2–10.

[101] I. Spyropoulou and C. Antoniou, "Determinants of driver response to variable message sign information in Athens," *IET Intell. Transp. Syst.*, vol. 9, no. 4, pp. 453–466, 2014.

[102] A. J. Khattak, F. S. Koppelman, and J. L. Schofer, "Stated preferences for investigating commuters' diversion propensity," *Transportation*, vol. 20, no. 2, pp. 107–127, 1993.

[103] A. Tsirimpa, A. Polydoropoulou, and C. Antoniou, "Development of a mixed multi-nomial logit model to capture the impact of information systems on travelers' switching behavior," *J. Intell. Transp. Syst.*, vol. 11, no. 2, pp. 79–89, 2007.

[104] D. M. Levinson and H. Huo, "Effectiveness of variable message signs using empirical loop detector data," 2003.

[105] K. Choocharukul, "Effects of attitudes and socioeconomic and travel characteristics on stated route diversion: Structural equation modeling approach of road users in Bangkok, Thailand," *Transp. Res. Rec. J. Transp. Res. Board*, no. 2048, pp. 35–42, 2008.

[106] M. Yun and S. Tang, "Route diversion probability model based on guidance utility and its application," in *Plan, Build, and Manage Transportation Infrastructure in China*, 2008, pp. 627–636.

[107] R. H. Emmerink, P. Nijkamp, P. Rietveld, and J. N. Van Ommeren, "Variable message signs and radio traffic information: An integrated empirical analysis of drivers' route choice behaviour," *Transp. Res. Part Policy Pract.*, vol. 30, no. 2, pp. 135–153, 1996.

[108] C. Caplice and H. S. Mahmassani, "Aspects of commuting behavior: preferred arrival time, use of information and switching propensity," *Transp. Res. Part Policy Pract.*, vol. 26, no. 5, pp. 409–418, 1992.

[109] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: analyzing the security of traffic infrastructure," in *Proceedings of the 8th USENIX conference on Offensive Technologies*, 2014, pp. 7–7.

[110] M. S. Al-kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," in *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, 2012, pp. 1–9.

[111] C. Cerrudo, *Hacking Traffic Control Systems (U.S., UK, Australia, France, etc.)*. DEFCON 22, 2015.

[112] G. N. Bifulco, F. Simonelli, and R. Di Pace, "The role of the uncertainty in ATIS applications," in *Applications of Soft Computing*, Springer, 2009, pp. 230–239.

[113] G. N. Bifulco, R. Di Pace, and F. Viti, "Evaluating the effects of information reliability on travellers' route choice," *Eur. Transp. Res. Rev.*, vol. 6, no. 1, pp. 61–70, 2014.

[114] H. Gan and X. Ye, "Urban freeway users' diversion response to variable message sign displaying the travel time of both freeway and local street," *IET Intell. Transp. Syst.*, vol. 6, no. 1, pp. 78–86, 2012.

[115] H. Gan, X. Ye, and W. Gao, “Drivers’ En Route Diversion Decisions Under Influence of Variable Message Sign Information: Empirical Analysis,” 2008.

[116] K. Chatterjee and M. Mcdonald, “Effectiveness of using variable message signs to disseminate dynamic traffic information: Evidence from field trails in European cities,” *Transp. Rev.*, vol. 24, no. 5, pp. 559–585, 2004.

[117] E. Bekiaris and Y. J. Nakanishi, *Economic impacts of intelligent transportation systems: innovations and case studies*, vol. 8. Elsevier, 2004.

[118] P. W. Bonsall and I. A. Palmer, “VMS signs–the importance of phrasing the message,” *Behav. Netw. Impacts Driv. Inf. Syst.*, 1998.

[119] D. R. Proffitt and M. M. Wade, “Creating effective variable message signs: Human factors issues,” *Contract*, vol. 9816, pp. 040–940, 1998.

[120] E. D. Nuttall, E. Ginsburg, and R. Beerlage, “LEDs spell it out: The future of traffic signs,” *Traffic Technol. Int.*, vol. 1998, pp. 182–184, 1998.

[121] S. Nyg\a ardhs and G. Helmers, *VMS-Variable Message Signs: A Literature Review*. Statens väg-och transportforskningsinstitut, 2007.

[122] P. Rämä, A. Schirokoff, and J. Luoma, “Potential harmonisation of variable message signs in Viking countries,” *Nord. Road Transp. Res.*, no. 3, 2004.

[123] B. R. Ullman, N. D. Trout, and C. L. Dudek, “Use of graphics and symbols on dynamic message signs: technical report,” Texas Transportation Institute, The Texas A & M University System, 2009.

[124] T. P. Alkim, P. H. J. Van Der Mede, and W. H. Janssen, “Graphical route information on variable message signs,” 2000.

[125] S. Tarry and A. GRAHAM, “THE ROLE OF EVALUATION IN ATT DEVELOPMENT. 4, EVALUATION OF ATT SYSTEMS,” *Traffic Eng. Control Vol 36 No 12*, 1995.

[126] M. McDonald and A. Richards, “Urban incident management using integrated control and information systems,” 1996.

[127] C. Lee and M. Abdel-Aty, “Testing effects of warning messages and variable speed limits on driver behavior using driving simulator,” *Transp. Res. Rec. J. Transp. Res. Board*, no. 2069, pp. 55–64, 2008.

[128] M. ABI AAD, “Evaluating Responses to Contraflow for Hurricane Evacuation,” PhD Thesis, Virginia Tech, 2018.

[129] A. J. Berinsky and D. R. Kinder, “Making sense of issues through media frames: Understanding the Kosovo crisis,” *J. Polit.*, vol. 68, no. 3, pp. 640–656, 2006.

[130] C. Huff and D. Tingley, “‘Who are these people?’ Evaluating the demographic characteristics and political preferences of MTurk survey respondents,” *Res. Polit.*, vol. 2, no. 3, p. 2053168015604648, 2015.

[131] M. Buhrmester, T. Kwang, and S. D. Gosling, “Amazon’s Mechanical Turk: A new source of inexpensive, yet high-quality, data?,” *Perspect. Psychol. Sci.*, vol. 6, no. 1, pp. 3–5, 2011.

[132] P. G. Ipeirotis, “Demographics of mechanical turk,” 2010.

[133] Statista, “Total number of licensed drivers in the U.S. - by state 2017,” 2017. [Online]. Available: https://www.statista.com/statistics/198029/total-number-of-us-licensed-drivers-by-state/.

[134] O. Taubman-Ben-Ari, M. Mikulincer, and O. Gillath, “The multidimensional driving style inventory—scale construct and validation,” *Accid. Anal. Prev.*, vol. 36, no. 3, pp. 323–332, 2004.

[135] “United States Census Bureau.” [Online]. Available: https://www.census.gov/en.html.

[136] Federal Highway Administration, “Office of Highway Policy Information,” 2015. [Online]. Available: https://www.fhwa.dot.gov/policyinformation/.

[137] H. F. Kaiser, “An index of factorial simplicity,” *Psychometrika*, vol. 39, no. 1, pp. 31–36, 1974.

[138] H. S. Mahmassani and Y.-H. Liu, “Dynamics of commuting decision behaviour under advanced traveller information systems,” *Transp. Res. Part C Emerg. Technol.*, vol. 7, no. 2–3, pp. 91–107, 1999.

[139] N. van Nes, S. Brandenburg, and D. Twisk, “Improving homogeneity by dynamic speed limit systems,” *Accid. Anal. Prev.*, vol. 42, no. 3, pp. 944–952, 2010.

[140] P. Rämä, “Effects of weather-controlled variable speed limits and warning signs on driver behavior,” *Transp. Res. Rec.*, vol. 1689, no. 1, pp. 53–59, 1999.

[141] T. Vaa, C. Gelau, M. Penttinen, and I. Spyroupolou, “its and effects on road traffic accidents-State of the art,” in *PROCEEDINGS OF THE 13th ITS WORLD CONGRESS, LONDON, 8-12 OCTOBER 2006*, 2006.

[142] P. Rämä, J. Luoma, and V. Harjula, “Distraction due to variable speed limits,” *Traffic Eng. Control*, vol. 40, no. 9, pp. 428–430, 1999.

[143] P. A. Hancock and W. B. Verwey, “Fatigue, workload and adaptive driver systems,” *Accid. Anal. Prev.*, vol. 29, no. 4, pp. 495–506, 1997.

[144] J. Rasmussen, “Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models,” *IEEE Trans. Syst. Man Cybern.*, no. 3, pp. 257–266, 1983.

[145] B. R. Cooper and J. Mitchell, “SAFETY AND EFFECTIVENESS OF THE WIDER USE OF VMS. FINAL REPORT,” *TRL Rep. 526*, 2002.

[146] J. A. Molino, J. Wachtel, J. E. Farbry, M. B. Hermosillo, and T. M. Granda, “The effects of commercial electronic variable message signs (CEVMS) on driver attention and distraction: An update,” Turner-Fairbank Highway Research Center, 2009.

[147] B. N. Campbell, J. D. Smith, and W. Najm, “Examination of crash contributing factors using national crash databases,” United States. National Highway Traffic Safety Administration, 2003.

[148] S. G. Klauer, V. L. Neale, T. A. Dingus, D. Ramsey, and J. Sudweeks, "Driver inattention: A contributing factor to crashes and near-crashes," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2005, vol. 49, pp. 1922–1926.

[149] A. Smiley *et al.*, "Traffic safety evaluation of video advertising signs," *Transp. Res. Rec.*, vol. 1937, no. 1, pp. 105–112, 2005.

[150] A. T. McCartt, L. A. Hellinga, and K. A. Bratiman, "Cell phones and driving: review of research," *Traffic Inj. Prev.*, vol. 7, no. 2, pp. 89–106, 2006.

[151] J. Stutts *et al.*, "Distractions in everyday driving," 2003.

[152] C. Lee and M. Abdel-Aty, "Testing effects of warning messages and variable speed limits on driver behavior using driving simulator," *Transp. Res. Rec.*, vol. 2069, no. 1, pp. 55–64, 2008.

[153] X. Yan and J. Wu, "Effectiveness of variable message signs on driving behavior based on a driving simulation experiment," *Discrete Dyn. Nat. Soc.*, vol. 2014, 2014.

[154] J. Bergeron, "An Evaluation of the Influence of Roadside Advertising on Road Safety," *Doc. Prep. Minist. Transp. Gov. Quebec*, 1996.

[155] I. M. Harms, C. Dijksterhuis, B. Jelijs, D. de Waard, and K. A. Brookhuis, "Don't shoot the messenger: Traffic-irrelevant messages on variable message signs (VMSs) might not interfere with traffic management," *Transp. Res. Part F Traffic Psychol. Behav.*, 2018.

[156] C. Guattari, M. R. De Blasiis, and A. Calvi, "The effectiveness of variable message signs information: A driving simulation study," *Procedia-Soc. Behav. Sci.*, vol. 53, pp. 692–702, 2012.

[157] H. G. Hawkins Jr, W. S. Wainwright, and S. C. Tignor, "Innovative traffic control practices in Europe," *Public Roads*, vol. 63, no. 2, 1999.

[158] P. Rämä and J. Luoma, "Driver acceptance of weather-controlled road signs and displays," *Transp. Res. Rec.*, vol. 1573, no. 1, pp. 72–75, 1997.

[159] J. Luoma, P. Rama, and K. MacLaverty, "Understanding control strategies and technical features of VM signs," *Traffic Eng. Control Vol 42 No 5*, 2001.

[160] V. G. B. Kolisetty, T. Iryo, Y. Asakura, and K. Kuroda, "Effect of variable message signs on driver speed behavior on a section of expressway under adverse fog conditions—a driving simulator approach," *J. Adv. Transp.*, vol. 40, no. 1, pp. 47–74, 2006.

[161] D. De Waard, *The measurement of drivers' mental workload*. Groningen University, Traffic Research Center Netherlands, 1996.

[162] B. Abdulhai and H. Look, "Impact of dynamic and safety-conscious route guidance on accident risk," *J. Transp. Eng.*, vol. 129, no. 4, pp. 369–376, 2003.

[163] N. J. Garber and R. Gadirau, "Speed Variance and Its Influence on Accidents.," 1988.

Attachment

SURVEY QUESTIONNAIRE: ROAD USERS' BEHAVIOR AT HACKED DMS

We are researchers from the Department of Civil and Environmental Engineering at Virginia Tech conducting a study that will help policymakers improve the safety of the transportation network. Our study focuses on the assessment of road users' behavior. Every question is important to our study and responses will be kept strictly confidential. You may choose not to answer any question, but that will affect the quality of our research. This survey should take 15 minutes of your time.

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
Consent Information Sheet for Participants in Research Projects Involving Human Subjects

Title of Project:
Road users' behavior at hacked message sign

Investigators:
Kaveh Bakhsh Kelarestaghi and Kevin Heaslip DMSsecurityimpact@vt.edu

I. Purpose of this Research/Project
This online survey is part of a research project to examine factors affecting road users' behavior when encountering different information at the variable message sign. We are interested to evaluate how road users respond to the content of variable message signs and the factors that affect their behavior. Our study may help researchers and policymakers to improve the safety and reliability of the transportation network.

Results from the study would only be published in aggregate form in a dissertation, academic journals, and presentations at professional conferences.

II. Procedures
The online survey will help us learn about factors affecting road users' behavior when faced with a variable message sign. We would like to request your participation in our 15-minute online survey.

III. Risks
There is minimal risk of a breach of confidentiality. No identifying information is requested.
Your participation is voluntary, and if you decide not to participate, there will be no penalty.

IV. Benefits
The study may help researcher and policymakers by providing them with better knowledge on the impacts of variable message sign content on road users' behavior. However, we are not promising or guaranteeing benefits to encourage you to

participate. You may access a summary of the research results on our website when we complete the research.

V. Extent of Anonymity and Confidentiality
There is minimal risk of a breach of confidentiality. We will use a unique identifier to track response/non-response. No identifying information is requested. We will not link your name to any of your survey responses in the text of study or any other publications.

The investigators will access survey data by computer. We will assign unique identifiers to track responses, but these will be visible only to the project investigators and will be separated from the actual responses. The Virginia Tech Institutional Review Board (IRB) may view the study's data for auditing purposes. The IRB is responsible for the oversight of the protection of human subjects involved in research.

VI. Compensation
We are providing no financial compensation for your participation.

VIII. Freedom to Withdraw
Submission of the survey requires a response to all questions. However, you are free to withdraw from this study at any time without penalty.

IX. Acknowledgment
The investigators would like to thank Dr. Alireza Ermagun, Dr. Ronald Fricker and Dr. Ralph Buehler for their input and help in preparing this survey.

X. Questions or Concerns
Should you have any questions or concerns about the study's conduct or your rights as a research subject, or need to report a research-related injury or event, you may contact the Virginia Tech Institutional Review Board at irb@vt.edu.

Q2 Our study is restricted to drivers 18 years and older who live in the United States. By choosing "yes" please verify that you (1) have read the above consent form and are voluntarily
agreeing to participate in this study, and (2) are **at least 18 years old** and live in the United States?

- Yes
- No

Q3 What type of **US driving license** do you hold?

- State issued drivers license
- Learners permit
- I do not drive

Q4 **How long** have you been **driving**?

- Less than a year
- 1-5 years
- 6-10 years
- 11-15 years
- 16-20 years
- More than 20 years

Q5 How do you identify your **gender**?

- Male
- Female
- Other

Q6 **How old** are you?

- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- 65 - 74
- 75 - 84
- 85 or older

Q7 What is the **highest level of education** you have completed?

- Some high school, No degree
- High school diploma
- Some college, No degree
- Associates degree

- Bachelors degree
- Masters degree
- Professional degree
- Doctoral degree

Q8 Which category describes you the best:

- White
- Hispanic, Latino, or Spanish origin
- Black or African American
- Asian
- American Indian or Alaska Native
- Middle Eastern or North African
- Native Hawaiian or other Pacific Islander
- Multi-racial
- Other

Q9 Where do you **live**?

- Urban area
- Suburban area
- Rural area

Q10 What is the **Zip Code** of your primary residence?

Q11 Which of the following statements about **occupational status** is accurate about you?

- Self-employed
- Employed by someone else
- Student
- Employed and a student
- Unemployed

Display This Question:
If Q11 = Self-employed
Or Q11 = Student
Or Q11 = Employed by someone else

Q12 Which of the following statements about **occupational status** is accurate about you?

- Full time
- Part time

Display This Question:
If Q11 = Employed and a student

Q13 Which of the following statements about **occupational status** is accurate about to you?

- Full time employee and full time student
- Full time employee and part time student
- Part time employee and full time student
- Part time employee and part time student

Display This Question:
If Q11 = Unemployed

Q14 Which of the following statements about **occupational status** is applied to you?

- Unemployed looking for work
- Unemployed not looking for work
- Homemaker
- Retired

Display This Question:
If Q11 = Student
Or Q11 = Employed and a student

Q15 What describes you the most?

- High school student
- Undergraduate student
- Graduate student

Q16 How many hours do you drive in a typical week?

- 0 hours
- 1-5 hours
- 6-10 hours
- 11-15 hours
- 16-20 hours
- 21-25 hours
- More than 25 hours

Q17 How do you describe your driving behavior?

- **Anxious** (i.e., feelings of alertness and tension)
- **Reckless and careless** (i.e., violations of safe driving norms)
- **Angry and hostile** (i.e., tendency to act aggressively on the road)
- **Patient and careful** (i.e., planning ahead; attention, patience)

Q18 Have you ever been involved in any accidents?

- Yes
- No

Display This Question:
If Q18 = Yes

Q19 Was **distraction** (e.g. distracted by phone) the main reason of any of those accidents?

- Yes
- No

Display This Question:
If Q19 = Yes

Q20 In any of those accidents were you the **distracted driver**?

- Yes
- No

Display This Question:
If Q20 = Yes

Q21 What were the **reasons for the distractions**? (check all that apply)

- Looking at Scenery
- Looking at Roadside Incident
- Cellphone
- Sleepiness/Fatigue
- Passenger
- Radio/CD, Navigation Device, Adjusting Vehicle Controls
- Eating/Drinking
- Mind Wandering
- Other

Q22 Please mark the following statements on a scale of strongly agree to strongly disagree (from the left to right).

	Strongly Agree	Somewhat Agree	Neither agree nor disagree	Somewhat Disagree	Strongly Disagree
I rely on technology for my daily trips (GPS, Google map)	O	O	O	O	O
I check traffic condition before hitting the road	O	O	O	O	O
I easily get lost when traveling in an unfamiliar area	O	O	O	O	O
I trust technology to assist in my travel	O	O	O	O	O
I prefer taking familiar routes	O	O	O	O	O
I'm willing to take new routes to get to my destination sooner	O	O	O	O	O
I can be a leader	O	O	O	O	O
I have trouble understanding directions	O	O	O	O	O
For validation purposes, please select strongly disagree for this question.	O	O	O	O	O
I feel that I get more accomplished because of technology	O	O	O	O	O
Driving makes me bored	O	O	O	O	O
I'm up-to-date with news	O	O	O	O	O
I use my blinker when changing the lanes	O	O	O	O	O
I pay attention to vehicles around me	O	O	O	O	O
I comply with traffic regulations given by traffic signs	O	O	O	O	O
I like driving the same way as the other cars around me	O	O	O	O	O
I have a good record of driving	O	O	O	O	O
I can trust drivers around me	O	O	O	O	O

Q23 This part of the survey introduces Variable Message Signs (DMS) and ask several questions regarding your familiarity with the DMS.
DMS are electronic traffic signs that have been used widely across the US to convey traffic-related information such as traffic congestion, road closures, accidents, and travel time to road users. The following sections ask questions related to your experience with these signs.

Q24 How **familiar** were you with the DMS before starting this survey?

- Extremely familiar
- Very Familiar
- Moderately familiar
- Slightly familiar
- Not familiar at all

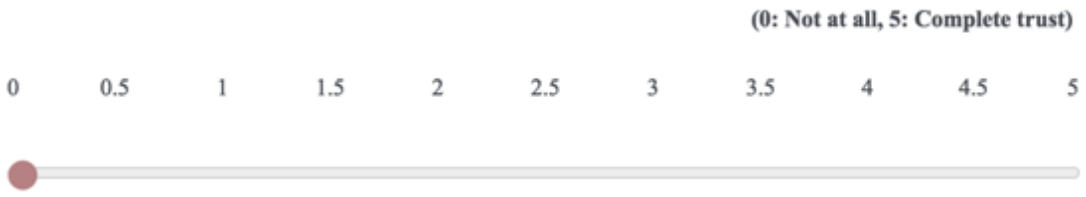
Q25 How often **do you see** DMS on your daily commute?

- Always
- Most of the time
- About half the time
- Sometimes
- Never

Q26 How often do you **read the content** of DMS?

- Always
- Most of the time
- About half the time
- Sometimes
- Never

Q27 In general, how much do you **trust DMS information**?



Q28 On a scale of 0 to 5, to what extent do you **use DMS information** when you are driving in the following conditions?

(0: Not at all, 5: A great deal)

0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5

On an unfamiliar road

At night

On familiar roads

On a congested road

In a bad weather condition

Near a work zone area

On the way to work/school

On the way home

Q29 On the scale of not at all, to complete attention, how much attention do you pay to the following messages? (from the left to right).

	Not at all	Slightly	Moderately	Very	Completely
Traffic-related messages (e.g. Crash Ahead, Choose Other Routes)	O	O	O	O	O
Informative messages (e.g. Hurricane Is Coming, Take Shelter)	O	O	O	O	O
Terrorism-related messages (e.g. State buildings are under attack, avoid downtown)	O	O	O	O	O
Political messages (e.g. Bernie For President!)	O	O	O	O	O
Funny/Offensive/Nonsense messages (e.g. Zombies are coming!)	O	O	O	O	O

Q30 Sometimes DMS is **hacked and its message is changed** like the following pictures. Please answer the following questions regarding the hacked DMS.

Q31 Have you **come across** a hacked DMS before?

- Yes
- No
- The DMS seemed like a hacked one
- I'm not sure

Display This Question:
If Q31 = Yes
And Q31 = The DMS seemed like a hacked one

Q32 At the time you came across the hacked DMS, did any of the following occurred to you? (check all that apply)

- ☐ I called or texted someone
- ☐ I took picture of the sign
- ☐ I thought of something other than driving
- ☐ I talked to a passenger about the sign
- ☐ I checked the radio
- ☐ I checked news or social media
- ☐ I slowed down
- ☐ I stopped the car
- ☐ I changed my route
- ☐ I changed my destination
- ☐ I ignored the message
- ☐ Other _____
- ☐ Please share the hacked message if you remember:

Display This Question:
If Q31 = Yes

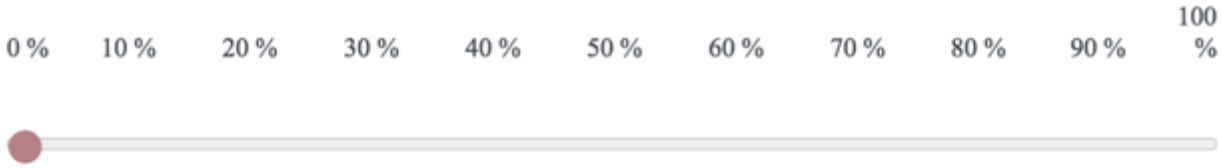
Q33 To what **percent your trust in the content of DMS change** after you experienced the hacked DMS?

(0%: No change, 100%: Completely distrust)

Display This Question:
If Q31 = No
Or Q31 = I'm not sure
Or Q31 = The DMS seemed like a hacked one

Q34 To what percent **<u>your trust in the content of DMS will change</u>** by knowing that DMS can be hacked?

(0%: No change, 100%: Completely distrust)



Q35 In the next few sections, you will be given a set of scenarios to evaluate your behavior when interacting with various DMS. Please provide your answer to the following questions.

Q36 Assume that you are driving on a highway to reach downtown with the speed limit of 60 mph. You come across a DMS that says "Road Closure Due to Police Activity". Please mark the following statements on a scale of extremely likely to extremely unlikely (from left to right).

	Extremely likely	Somewhat likely	Neither likely nor unlikely	Somewhat unlikely	Extremely unlikely
I would call or text someone	O	O	O	O	O
I would take picture of the sign	O	O	O	O	O
I would check social media or news	O	O	O	O	O
I would talk to a passenger about the sign	O	O	O	O	O
I would think of something other than driving	O	O	O	O	O
I would look at other vehicles and scenery	O	O	O	O	O
I would check the radio	O	O	O	O	O
I would not be distracted	O	O	O	O	O
I would slow down	O	O	O	O	O
I would speed up	O	O	O	O	O
I would stop my car	O	O	O	O	O
I would change my route	O	O	O	O	O
I would change my destination	O	O	O	O	O
I would ignore the message	O	O	O	O	O

Q37 Assume that you are driving on a highway to reach downtown with the speed limit of 60 mph. You come across a DMS that says "Storm Watch, Flooding in Area Soon". Please mark the following statements on a scale of extremely likely to extremely unlikely (from left to right).

	Extremely likely	Somewhat likely	Neither likely nor unlikely	Somewhat unlikely	Extremely unlikely
I would call or text someone	○	○	○	○	○
I would take picture of the sign	○	○	○	○	○
I would check social media or news	○	○	○	○	○
I would talk to a passenger about the sign	○	○	○	○	○
I would think of something other than driving	○	○	○	○	○
I would look at other vehicles and scenery	○	○	○	○	○
I would check the radio	○	○	○	○	○
I would not be distracted	○	○	○	○	○
I would slow down	○	○	○	○	○
I would speed up	○	○	○	○	○
I would stop my car	○	○	○	○	○
I would change my route	○	○	○	○	○
I would change my destination	○	○	○	○	○
I would ignore the message	○	○	○	○	○

Q38 Assume that you are driving on a highway to reach downtown with the speed limit of 60 mph. You come across a DMS that says "Downtown Under Terrorist Attack". Please mark the following statements on a scale of extremely likely to extremely unlikely (from left to right).

	Extremely likely	Somewhat likely	Neither likely nor unlikely	Somewhat unlikely	Extremely unlikely
I would call or text someone	○	○	○	○	○
I would take picture of the sign	○	○	○	○	○
I would check social media or news	○	○	○	○	○
I would talk to a passenger about the sign	○	○	○	○	○
I would think of something other than driving	○	○	○	○	○
I would look at other vehicles and scenery	○	○	○	○	○
I would check the radio	○	○	○	○	○
I would not be distracted	○	○	○	○	○
I would slow down	○	○	○	○	○
I would speed up	○	○	○	○	○
I would stop my car	○	○	○	○	○
I would change my route	○	○	○	○	○
I would change my destination	○	○	○	○	○
I would ignore the message	○	○	○	○	○

Q39 Assume that you are driving in a work zone with the speed limit of 40 mph on a highway. You come across a DMS that says "Work Zone Ends, Speed Limit 60 mph". Please mark the following statements on a scale of extremely likely to extremely unlikely (from left to right).

	Extremely likely	Somewhat likely	Neither likely nor unlikely	Somewhat unlikely	Extremely unlikely
I would call or text someone	O	O	O	O	O
I would take picture of the sign	O	O	O	O	O
I would check social media or news	O	O	O	O	O
I would talk to a passenger about the sign	O	O	O	O	O
I would think of something other than driving	O	O	O	O	O
I would look at other vehicles and scenery	O	O	O	O	O
I would check the radio	O	O	O	O	O
I would not be distracted	O	O	O	O	O
I would slow down	O	O	O	O	O
I would speed up	O	O	O	O	O
I would stop my car	O	O	O	O	O
I would change my route	O	O	O	O	O
I would change my destination	O	O	O	O	O
I would ignore the message	O	O	O	O	O

Q40 Assume that you are driving on a highway to reach downtown with the speed limit of 60 mph. You come across a DMS that says "Heavy Traffic Due to Accident". Please mark the following statements on a scale of extremely likely to extremely unlikely (from left to right).

	Extremely likely	Somewhat likely	Neither likely nor unlikely	Somewhat unlikely	Extremely unlikely
I would call or text someone	O	O	O	O	O
I would take picture of the sign	O	O	O	O	O
I would check social media or news	O	O	O	O	O
I would talk to a passenger about the sign	O	O	O	O	O
I would think of something other than driving	O	O	O	O	O
I would look at other vehicles and scenery	O	O	O	O	O
I would check the radio	O	O	O	O	O
I would not be distracted	O	O	O	O	O
I would slow down	O	O	O	O	O
I would speed up	O	O	O	O	O
I would stop my car	O	O	O	O	O
I would change my route	O	O	O	O	O
I would change my destination	O	O	O	O	O
I would ignore the message	O	O	O	O	O

Q41 Assume that you are driving on a highway to reach downtown with the speed limit of 60 mph. You come across a DMS that says "Read The News Today, Oh Boy!". Please mark the following statements on a scale of extremely likely to extremely unlikely (from left to right).

	Extremely likely	Somewhat likely	Neither likely nor unlikely	Somewhat unlikely	Extremely unlikely
I would call or text someone	O	O	O	O	O
I would take picture of the sign	O	O	O	O	O
I would check social media or news	O	O	O	O	O
I would talk to a passenger about the sign	O	O	O	O	O
I would think of something other than driving	O	O	O	O	O
I would look at other vehicles and scenery	O	O	O	O	O
I would check the radio	O	O	O	O	O
I would not be distracted	O	O	O	O	O
I would slow down	O	O	O	O	O
I would speed up	O	O	O	O	O
I would stop my car	O	O	O	O	O
I would change my route	O	O	O	O	O
I would change my destination	O	O	O	O	O
I would ignore the message	O	O	O	O	O

Q42 Assume that you are driving on a highway to reach downtown with the speed limit of 60 mph. You come across a DMS that says "Zombies ahead run!". Please mark the following statements on a scale of extremely likely to extremely unlikely.

	Extremely likely	Somewhat likely	Neither likely nor unlikely	Somewhat unlikely	Extremely unlikely
I would call or text someone	O	O	O	O	O
I would take picture of the sign	O	O	O	O	O
I would check social media or news	O	O	O	O	O
I would talk to a passenger about the sign	O	O	O	O	O
I would think of something other than driving	O	O	O	O	O
I would look at other vehicles and scenery	O	O	O	O	O
I would check the radio	O	O	O	O	O
I would not be distracted	O	O	O	O	O
I would slow down	O	O	O	O	O
I would speed up	O	O	O	O	O
I would stop my car	O	O	O	O	O
I would change my route	O	O	O	O	O
I would change my destination	O	O	O	O	O
I would ignore the message	O	O	O	O	O

Q43 Previously, you saw several scenarios in which the DMS messages were hacked. For instance, in one case the "Work Zone Ahead" message was changed to "Work Zone Ends, Speed Limit 60 mph". Or in another case, a common traffic-related message was changed to "Downtown Under Terrorist Attack".
Given the scenarios that you observed, please answer the following questions.

Q44 Do you believe the hacked DMS increases the chance of a crash?
(0: Not at all, 5: Extremely likely)

(0: Not at all, 5: Extremely likely)

0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5

Q45 Do you believe the hacked DMS causes delay and increases the travel time?

(0: Not at all, 5: Extremely likely)

0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5

Q46 If you have already experienced or experience hacked DMS, how much does it change your trust to the different type of messages provided below come across from 0 (No change) to 5 (Complete distrust).

0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5

Traffic-related messages (e.g. Crash Ahead, Choose Other Routes)

Informative messages (e.g. Hurricane Is Coming, Take Shelter)

Terrorism-related messages (e.g. State buildings are under attack, avoid downtown)

Q47 We are almost done. Please answer to a few short questions before the end of the survey.

Q48 If other drivers react to the DMS information **would you follow them**?

- Extremely likely
- Very likely
- Moderately likely
- Slightly likely
- Not at all

Q49 What is your **household a**nnual income?

- Less than $15,000
- $15,000 - $29,999
- $30,000 - $44,999
- $45,000 - $59,999
- $60,000 - $74,999
- $75,000 - $89,999
- $90,000 - $104,999
- $105,000 - $119,999
- $120,000 - $134,999
- $135,000 - $149,999
- More than $150,000
- Not interested to reveal

Q50 What **kind of vehicle** do you mostly use?

- Passenger car (any type or size)
- Minivan / van / MPV (multipurpose vehicle)
- Pickup / Passenger truck
- SUV (sport utility vehicle)
- Motorcycle / scooter
- Single unit truck

Q51 **How many cars** do you have in your household?

- 0
- 1
- 2
- 3 or more

Q52 Do you have any disability?

- Yes
- No
- I prefer not to answer

Display This Question:
If Q52 = Yes

Q53 Which of the following statements about disability status is applied to you?

- A sensory impairment (vision or hearing)
- A mobility impairment
- A learning impairment (e.g., ADHD)
- A mental health impairment
- Other
- Not interested to reveal

Q54 What's your **marital status**?

- Single, never married
- Married or domestic partnership
- Widowed
- Divorced
- Separated
- Not interested to reveal

Display This Question:
If Q31 = Yes

Q55 We appreciate your time for taking this survey. If you'd like us to contact you for a follow-up survey (with compensation) please provide your email address below.

Q56 We thank you for your time spent taking this survey. Your response has been recorded