Scientific Research Publishing

World Journal of Engineering and Technology, 2022, 10, 1-27
https://www.scirp.org/journal/wjet
ISSN Online: 2331-4249
ISSN Print: 2331-4222

Paper the Resilience of ITS: Variable Message Signs Contribution to Road Network Resilience under Incident and High Congestion Conditions: A State of the Art Review

Hashmatullah Amiri, Hongtao Li

School of Transportation, Lanzhou Jiaotong University, Lanzhou, China
Email: hashmatullahamiri1993@gmail.com

How to cite this paper: Amiri, H. and Li, H.T. (2022) Paper the Resilience of ITS: Variable Message Signs Contribution to Road Network Resilience under Incident and High Congestion Conditions: A State of the Art Review. *World Journal of Engineering and Technology*, **10**, 1-27.
https://doi.org/10.4236/wjet.2022.101001

Received: October 11, 2021
Accepted: February 11, 2022
Published: February 14, 2022

Abstract

Any failure or disruption in traffic flow can propagate through the road network. However, the server of such disruption and its consequences depends on the robustness and resiliency of transportation systems. In this context, traffic management (TM) measures will help the traffic stream to prevent the occurrence of such conditions or recover faster after experiencing the disruption. The main objective of this paper was to elaborate the contribution of TM measures to the resiliency of transportation systems, as well as, their vulnerability against external threats. Furthermore, a concept design for variable message signs (VMS) is developed and evaluated in terms of contribution to the resiliency of road networks. As well, new vulnerabilities associated with the implementation of VMS are investigated. The result of this study pointed out that ramp-metering, variable message signs, variable speed limits, and autonomous vehicles are valuable tools to mitigate the severity of traffic disruptions. VMS is one of the most effective approaches that enhance traffic resiliency by reducing traffic inflow to congested areas. However, these measures have opened new vulnerabilities to threats, especially cyber-attacks. Several cases of VMS hacks have occurred in the world and provided false messages to road users. It gets even worse with using an integrated wireless communication interface. Therefore, it is necessary to consider the security of such systems in advance, before practical application.

Keywords

Resilience, Robustness, Intelligent Transportation Systems (ITS), Variable Message Signs (VMS)

1. Introduction

In modern cities, robustness and resiliency of transportation systems are critical [1]. Any failure or disruption in the road network can propagate through the whole network and causes a large-scale breakdown. There are a large number of factors that influence the ability of traffic to maintain a certain speed, serviceability, and overall performance of flow, locally and within the whole network. Climate factors such as rain, snow, and wind, poor road surface, inappropriate road geometry, different speed regimes, and cyber-attacks on intelligent transportation systems can lead to disturbance in traffic flow. Although the local effect of disruption would be minimal, it has a direct relation with the whole network [2]. It means that any local disruption influences the overall performance of the road network. In this case, transportation systems are required to have enough resilience to ensure the operational continuity and absorption of the disturbance effect.

The concept of resilience has been studied in a wide range of fields such as engineering, sociology, business, and economics. In infrastructure, it is defined as the ability to mitigate the magnitude and/or duration of a disruption [3]. In the field of transportation, [4] define it as "the characteristics that enable the system to compensate for losses and allows the system to function even when infrastructure is damaged". In other words, resilience is the ability of a system to deal with variable and unexpected conditions without any catastrophic failure [5]. In general, transportation resiliency represents the ability of the system to function during and after major disruption to an acceptable level of service and minimum consequences on the other parts of the network [6]. The occurrence of disruption on the network put adverse effects on traffic flow which often leads to congestion. The measurement of disturbance takes into account the probability of disturbance or the consequence of happening or both. Whenever congestion occurs as a result of disturbance, the speed of recovery to the original or at least acceptable level of service is very important. The ability to recover from such a condition is referred to the level of resiliency of the system. According to Burneau, the existence of extra capacity in the system, alternative choice, inter-modality and coordination between different modes, and dynamic information sharing are crucial in traffic management to handle traffic disruption. Moreover, advanced technologies like intelligent transportation systems (ITS) need to be robust and resilient against disruptions.

ITS refers to the application of communication and information technologies to the real-time management of vehicles and networks which carry people and goods [7]. However, the system which is controlled remotely or interacts with other remote-control systems is vulnerable to remote hackers. The potential vulnerability of these systems can attract the attention of malicious attackers who can control from a long distance [4]. Therefore, cyber threats would be called a general challenge for the transportation network. Improving security can only reduce the risks but cannot eliminate them. On the other hand, the lev-

el and source of the treats are mostly unknown. Therefore, taking beforehand action is somehow impossible. However, increasing the resiliency of transportation systems would be a more efficient approach compared to allocating time and money to improve the systems' security [4]. It refers to the ability of the system to handle the changes of conditions.

There are four underlying dimensions that determine the properties of an ITS measure [7]. 1) Robustness, which refers to the quality and strength of the system to handle a given level of disruption without degradation or loss of functionality. 2) Redundancy, which represents the ability of a system to fulfil the functional requirement via alternative options in case of disruption and loss of functionality. 3) Resourcefulness of the system states the capability of a system to identify the source of disruption, prioritize problems, and mobile resources to recover the functionality of the system. In transportation, it represents the number of available repair units in post-disaster operation [8]. Finally, rapidity refers to the speed to overcome a disruption, and re-achieve the safety, serviceability, and stability of the system.

Within the current paper, it is aimed to explore how traffic management measures including ramp-metering, variable speed limit (VSL), variable message signs (VMS), and autonomous vehicles help the transportation system to be more robust and resilient against traffic disruptions. The main goal of this paper is to give an overview of the vulnerabilities and resilience of dynamic traffic management measures. Furthermore, developing a concept design for VMS and how it can contribute to congestion management that occurred due to incidents or bottlenecks is another objective of this study. Moreover, a new set of vulnerabilities such as cyber-security associated with such a system and what measures can reduce the risk of VMS failure are going to be discussed in this paper.

The remaining parts of the report are structured as follows: Section 2 performance components (resiliency and vulnerability) are reviewed. The next two sections present ITS measures and their contribution to the resiliency of the transportation network and associated vulnerabilities. Later on, VMS concept design is discussed which follows by another section named cyber-security of VMS. Finally, a conclusion is written at the end.

2. Robustness and Resiliency of ITS

When talking about performance and disturbance of traffic flow of a specific road or network, robustness, vulnerability, and resilience are three components that should be defined first hand.

2.1. Robustness

According to [9], robustness refers to "the inherent strength or resistance in any system to withstand a given level of stress or demand without degradation or loss of functionality". [10] defines it as "the ability of a system to resist a change without adapting its initial stable configuration". In terms of the road network,

[11] have given a different definition. The authors define it as "the extent to which, under pre-specified circumstances, a network can maintain the function for which it was originally designed". In general, the robustness of a transportation system refers to the prevention of adverse effects of disturbance [2]. It means that a robust transportation system has the ability to handle the deterioration of performance as far as it is in an acceptable range.

2.2. Resilience

Resilience is a concept that is being studied widely in different fields but less researched in the traffic domain [2]. Generally, it is defined as the ability of a network to recover from disruptions. In the field of the transportation system, resilience can be defined from two perspectives: 1) the ability to maintain functionality under disruption, and 2) the time and resources required to recover acceptable performance levels after disruption [8]. The intensity of disturbance and the speed at which the system restore from disruption determine the resiliency of the transportation system [12]. There are many other interpretations of resilience; most of them, however, based on the same idea that resilience is the ability of the system to restore back to its normal condition after disruptions that changed its state. A well-designed transportation system can absorb disruptions and maintain its function to a stable state. As shown in **Figure 1**, the first phase refers to disruptions, which indicates the happening of disruption up to the maximum value. The second phase reflects the recovery of the system from a disruption. It starts from the recovery point until returning to normal conditions [8]. It should be noted the graph presented below relates to seismic resilience. In transportation, the maximum disruption may remain for some time before going through the recovery phase [8].

2.3. Vulnerability

The term vulnerability refers to the improper working of a system [2]. [13] defines the vulnerability of transportation systems as "susceptibility to incidents

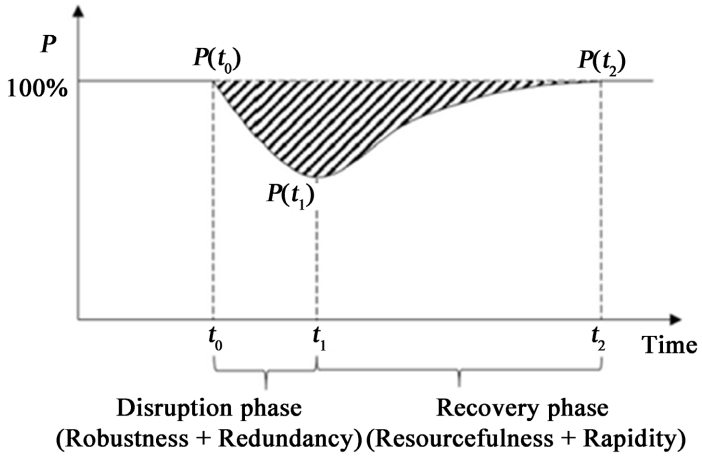

Figure 1. Two phases of resilience (source: [8]).

that can result in a considerable reduction in road network serviceability". The susceptibility in this definition indicates the probability of occurrence of disruption. In this case, the probability of susceptibility and the consequent effect on serviceability are the two main attributes of vulnerability. A big disadvantage with the aforementioned definition is its difficulty in the estimation of probabilities of uncertain events [2]. However, the difficulty of prediction reduces while studying regular traffic disturbances.

Travel time and its consequences on the environment are other dimensions to assess the resiliency of the transportation systems. As a result of any disruption in the system, how much increase in travel time will occur and the environmental impact due to delay defines the level of resiliency. To integrate resiliency in the system, there should be a reduction in vulnerability, an increase in adaptive capacity, agile response, and effective recovery [14].

2.4. Robustness and Resilience vs Vulnerability

As discussed in the previous section, the terms robustness and resilience are closely related to each other. Although argues that robustness and resilience should be considered synonymously, there are some differences between them. Robustness mostly represents the ability of the system to withstand under a certain condition despite uncertainties, while resilience states the ability of the system to recover from disturbances [2]. It focuses more on performance and recovery when facing inevitable disruptions to deal with day-to-day fluctuations [8]. A system is robust for an event if it is resilient for that event under defined states [14]. It means that a system can be resilient but not robust. According to Calvert and [8], robustness is like an umbrella that includes the resilience of all parts.

On the other hand, vulnerability and robustness are opposites of each other. The more the system becomes vulnerable to external threats, it loses its robustness. [15] discusses four types of assessment indicators for road network: network characteristics, traffic flow, threats, and neighborhood attributes. The network characteristics show the overall characteristics of transportation infrastructure. Traffic flow refers to the demand on the network. Threats refer to the possible weakness and risks and neighborhood attributes present the connectivity and accessibility of links in the network.

Figure 2 shows the relationship between traffic performance components discussed previously.

3. TM Measure and Resiliency of Road Network

Vulnerability in traffic networks causes the loss of capability to serve demand. In fact, there is a general lack of adaptiveness in the system to handle major traffic overloads [16]. Since transport planners use long-term forecasts of land and traffic demand under uncertainties, it is likely that, over time, there will be an imbalance in travel demand and the capacity of the roads. The situation gets worse

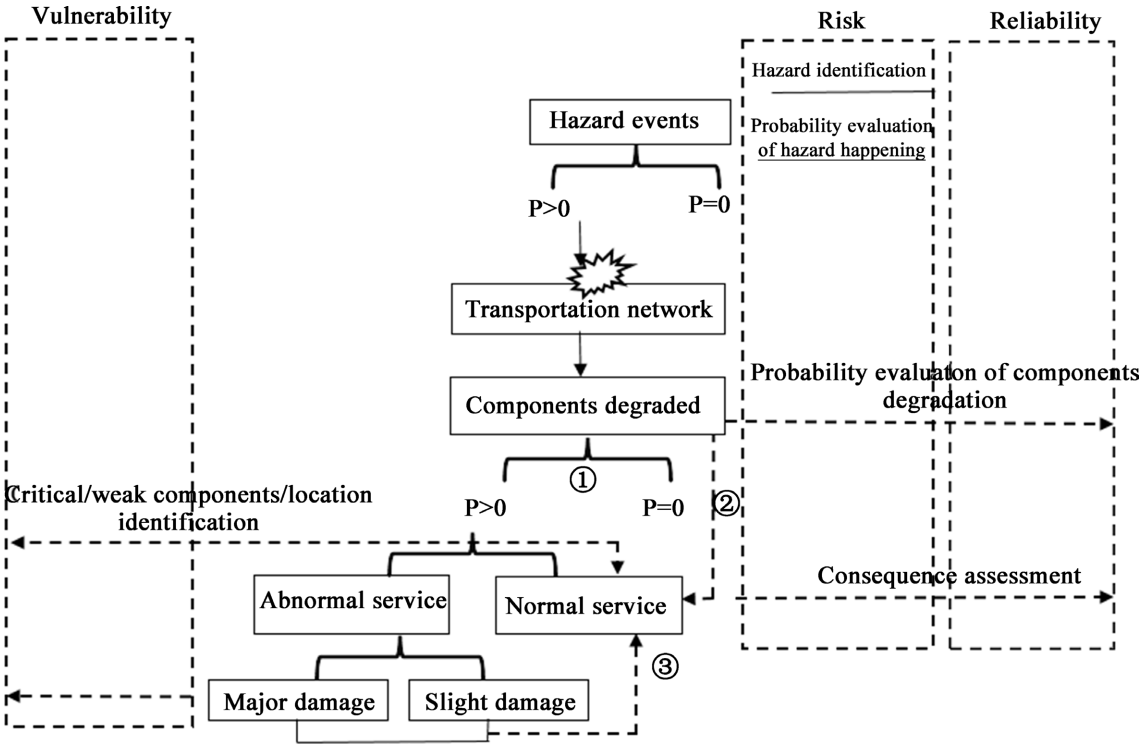

Figure 2. Relationship between performance concepts [8].

when the network possesses less flexibility to handle traffic overloads caused by stochastic events which cannot be predicted beforehand [16]. Such events like incidents, weather, construction/maintenance, special events, and signal time cause capacity drop and trigger congestions in the network [17]. About 50% of delay refers to this type of congestion [16].

Traffic congestions can be recurrent due to demand exceeding the capacity or non-recurrent caused by occasional events. However, an incident can potentially cause another incident. For instance, in the US about 20% of the total car crashes happen because of previous incidents [17]. The consequence of such disturbance in the transportation systems would be serious travel delay, economic loss, injuries, and deaths. The consequence of traffic congestions is even intensified during peak hours; as such it may take up to fifty minutes to clear one-minute congestion on the highway [18]. While it may take only 4 - 5 minutes during off-peak hours.

How fast a transport system returns to its normal situation depends on how much the system is resilient. In this context, dynamic traffic control refers to tools, procedures, and methods that are used in traffic management to improve the traffic flow in the short-term, *i.e.* minutes to hours. They aim to increase safety and traffic flow, decrease travel time and emission, and more stability in traffic states, and more reliability in travel time [19]. Currently, many tools are being used in dynamic traffic management such as traffic signs, VSL, VMS, radio broadcast messages, in-vehicle informing systems, and etcetera. These are effective operational strategies to mitigate the severity of traffic disturbance, as well as, restore to normal conditions faster and smoother.

3.1. Ramp Metering

Ramp metering is a traffic signal which controls the rates of vehicles entering a freeway from an on-ramp [17]. The main objective of introducing ramp-metering is to reduce the entering vehicles and facilitate a smooth merging of these two traffic flows (highway and on-ramp). The ramp-metering can be fixed-time based on historical data, local traffic responsive and system-wide responsive operation. Within a fixed-time strategy, the operation of ramp-metering is based on the static model without any real-time measurements which have many shortages like variation in demand [20], while the local responsive strategy is based on the demand capacity of the highway. In this case, the traffic condition is kept close to some pre-determined thresholds by analyzing real-time data near the on-ramp location [20]. The main objective is to find an optimal metering rate for each ramp individually [17]. On the other hand, wide-system or coordinated strategy refers to the optimization of multiple ramp controls. For instance, Heuristic Ramp Metering Coordination (HERO) is an approach that controls 4 to 6 ramps simultaneously to not exceed the length of queue on the ramps beyond capacity [20].

Ramp-metering has the potential to improve the overall performance of the road network if good alternatives exist for on-ramp demand [21]. In case of congestion on the highway, it can contribute to the resilience of the highway to mitigate congestion faster [22]. As a result, the throughput and congestion duration would be improved by the implementation of ramp metering. The best results can be achieved when all overflow queues behind meters could be shifted to alternate routes [21]. In case of high demand on the on-ramp and highway, the ramp-metering just alleviates congestion from the highway to the on-ramp, as so, it does not have a significant impact on the overall performance of the road network due to overflow queue behind the meters.

3.2. Variable Speed Limits

Variable speed limit (VSL) is another TM measure to reduce the adverse impact of traffic disturbance by adjusting highway speed limits accordingly to real-time traffic conditions [17]. An inductive loop detector is used to collect data of speed and flow with additional equipment of weather-sensing [23]. All the information goes to a central computer which aggregates and processes the data to determine the condition of the road. In case of unusual conditions such as incidents, congestions, construction, or bad weather situations, the VLS displays a speed limit to smooth and optimize road traffic flow and increase the throughput of the road (**Figure 3**). After happening of congestion, the VLS help to dampen traffic congestion by reducing inflow to the congested node [24]. While before the occurrence of traffic breakdown, the VSL aims to prevent or postpone breakdown by reducing inflow and achieving uniform distribution of speed and flow. As a result, the road network becomes more robust and resilient against traffic disruptions.

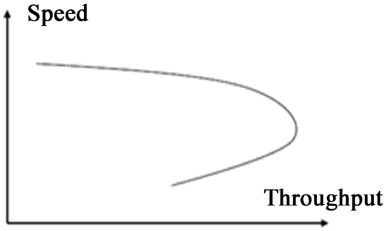

Figure 3. Highway traffic throughput as a function of operating speed [23].

The VLSs' algorithm is based on simple statistics and analysis of the average vehicle speed [23]. For instance, in the Netherlands, the VLS system control is based on the one-minute average of speed and volume across all lanes. In case of an incident, the speed limit displays 50 km/h. If the posted speed limit is shown with a red circle, it is an enforced speed limit, if not then, it is only an advisory speed limit [23].

3.3. Variable Message Signs

Variable message signs (VMS) are assigned to reduce the friction of frequent lane changes and undesirable jams by separate vehicles and allow them to change routes/lanes only in the designated section of the road [17]. The main objective is to increase the use of route/lane occupancy according to the detection of a queue in the network. The route diversion and lane change information are sent through VMS which can allocate traffic demand on the routes/lanes where no disturbance occurred or less congestion exists. By doing this, the congested condition will be solved sooner since fewer vehicles are approaching the blocked route/lane in case of an accident or high congestion.

However, the effectiveness of VMS depends on how many drivers can see the messages. Thus, it is very important to find the optimal location for VMS, so the right drivers receive the right information [17]. Furthermore, drivers' reaction to the provided information is also a critical attribute to be taken into account. Many factors can stimulate their behavior such as message content, update frequency, gender, and route familiarity [17]. To effectively implement VSM to increase transportation system resilience, it is required to carefully operate VMS, otherwise, it will have an adverse impact [15].

3.4. Automation in Driving

Automated vehicle technologies enable a vehicle to assist and make decisions for a human driver [16]. It can be partially automated (levels 1 & 2) or fully automated driving (levels 3 & 4). The partially automated system contributes to dangerous conditions whenever the driver is not capable of being highly distracted. While fully automated vehicles have complete control over driving tasks. Furthermore, autonomous vehicles are also equipped with subset technologies such as crash warning and sharing information with other vehicles and infrastructure. In such a case, the shared information can be used for traffic management purposes [16]. Throughout the vehicle-to-vehicle (V2V) information

sharing, the vehicle increases the resilience in the road network by traffic jam ahead warning, electronic braking light, and the emergency vehicle approaching. A vehicle-to-infrastructure (V2I) contributes to network resilience by notifying hazardous location, road work warning, weather conditions, shock wave damping, in-vehicle speed limits, in-vehicle signage, and time to green [16]. By this, the autonomous vehicle provides the opportunities to avoid congested routes and lines, therefore, help to the resilience of the network [16].

In highly congested situations, autonomous vehicles will reduce the adverse impact of stop-and-go traffic operations. Human drivers mostly exaggerate braking and acceleration responses in such conditions while automated vehicles have more controlled braking and acceleration systems [16]. Shortening of headways between a platoon of vehicles without compromising safety will improve travel time. A human driver may decelerate to avoid collation with the lead vehicle, sometimes applies brakes for some unknown reason. In such a case, the driver sends a big shock wave to the traffic stream which results in the reduction of throughput of the road network, while an automated vehicle can easily adjust its speed and deceleration accordingly to the leading vehicles and avoid aggressive driving and distraction. In addition, the introduction of autonomous vehicles on roads will reduce successive accidents. It means that automated vehicles can drive at a safe and efficient distance even in case of incidents [16].

Moreover, there are some other traffic measurements, especially in European countries e.g. tidal flow, dynamic lands, congestion pricing, and traveler information system [17]. Tidal flow reverses the direction of traffic on the highway during peak hours. The dynamic lane which is implemented in the Netherlands and Germany changes the number and width of lanes using lights similar to cats' eyes set on the surface of the road to increase the road capacity [17].

4. Vulnerabilities of TM Measures

Existing transportation infrastructure usually lacks connectivity therefore, vehicles are operating independently. With the introduction of wireless technology such as Dedicated Short-Range Communication (DSRC) and Cellular Network, this shortcoming has been solved to some extent. Despite the fact that ITS has contributed to the safety and efficiency of traffic flow, it has been associated with a new type of vulnerability [25].

The introduction of ITS brings benefits, but also a new set of vulnerabilities and risks to operators and public society as a whole [7]. Hacking is not only about companies, organizations, and banks, but also ITS measures that rely on wireless sensor networks including VMS have already experienced cyber-attacks or remain vulnerable to cyber-threats [26]. The ITS is vulnerable in the area of communication due to inadequate security protocols, inadequate authentication mechanisms, energy constraints, poor security, and unreliable communication [7]. Although many studies have been done in this regard and many solutions are proposed, still significant concerns exist about maintaining flawless perfor-

mance of transportation systems within a satisfactory level of security [26]. It indicates the presence of cyber threats to traffic management systems that use vulnerable sensors. Figure 4 shows the element of ITS which is vulnerable to cyber-attacks.

Lack of cybersecurity consciousness allows attackers to easily take control of traffic systems and provide fake information or deteriorate the normal performance [25]. As a result, it can cause traffic congestion and increase crash risks. The main challenge in cyber-attacks is uncertainties about the sources and types of threats. Traffic control systems can be targeted through an infrastructure-to-infrastructure (I2I) or vehicle-to-infrastructure (V2I) communication interface. The consequence of such disturbance in traffic flow would be minor to critical failure [25]. Generally speaking, there are three major weaknesses in TM measures: lack of encryption for the network, lack of secure authentication, and vulnerability to known exploits [27]. Furthermore, an increase in automation including autonomous vehicles introduces new potential vulnerabilities. This is due to an increase in the number of system access points and, therefore, cyber-attacks increase simultaneously [7]. To mitigate the cyber-threats and design resilience systems, cyber-tampering of the traffic management system should be analyzed beforehand [27].

Traffic signals at the intersection are the most widely used traffic control measure that attacker can generate inefficient signal timing plan and in some extreme cases, it can lead to disastrous congestions [25]. The attackers take control

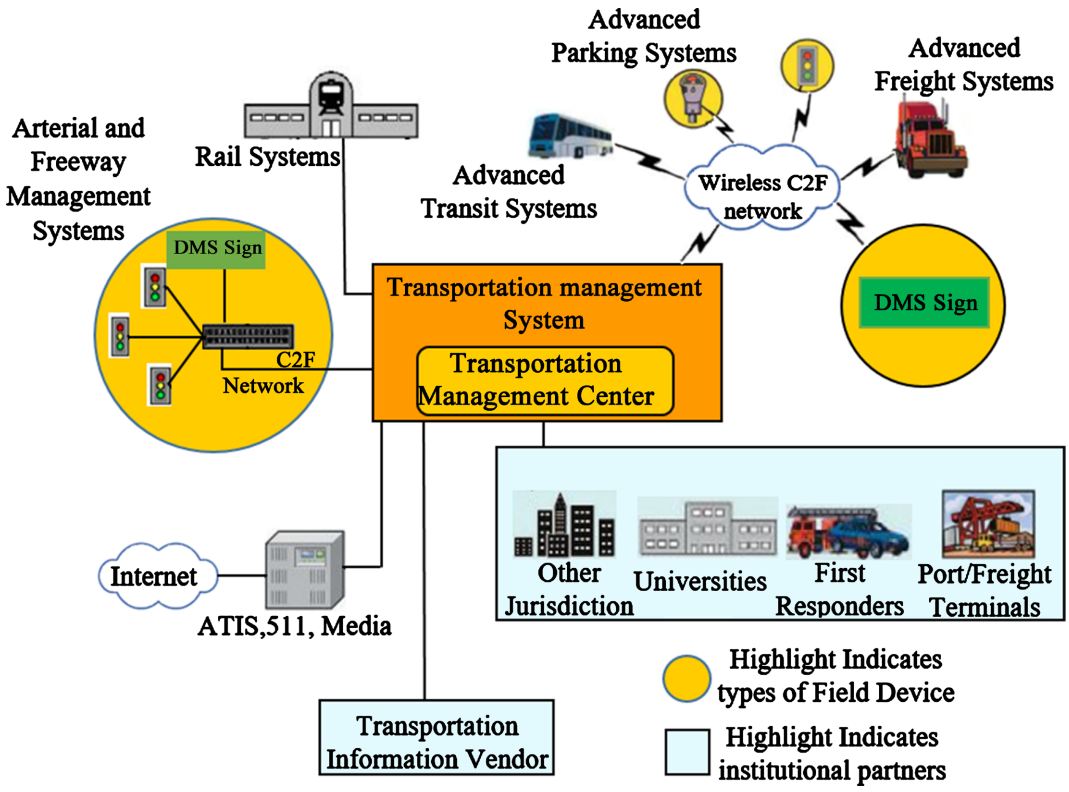

Figure 4. The common element of transportation systems [38].

of these sensors by directly compromising sensors or by gaining control over the communication network [27]. As these signals work based on the fixed-time algorithm, cyber attackers can formulate new programming with different objectives. For instance, a study by [28] revealed that the signal timing of wireless sensors is vulnerable to being manipulated. As well as, it would be vulnerable to falsifying input data to influence control decisions under actuated signals [25].

Generally, cyber-attacks on dynamic traffic signals such as ramp-metering, VMS, and VSL can be classified in three groups. 1) Worst-case network accumulation attack, in which the attacker's goal is to destabilize the whole network as much as possible to cause the worst possible traffic congestions. 2) Worst-case lane accumulation attack, in which the attacker's goal is to maximize the accumulation rate of a specific lane, or to minimize its corresponding service rates as much as possible. 3) Risk-averse target accumulation attack, which refers to the strategy of reaching a target accumulation rate by making minimum perturbations [27].

5. Real-Time VMS

Advanced traveler information systems (ATIS) are an important part of the ITS which help drivers in their decision-making processes such as departure time, congestion avoidance, route choice, and lane changes [29]. Such a system can also be used by traffic managers to improve network performance. VMS or Changeable Message Signs (CMS), also known as Dynamic Message Signs (DMS) is the most common type ATIS which provides the possibility to be programmed by traffic controllers [29]. VMS are electronic message boards installed alongside the roadways to disseminate information to drivers who do not have in-vehicle equipment to receive personalized real-time information, either as advisory or pro-active guidance [15], especially under congested conditions [29]. In contrast to traditional speed limits that have minimal influence on drivers' speed, VMS has a significant impact on oncoming drivers' decisions including speed reduction [26]. Thus, VMS should be located in highly visible areas to achieve maximum efficiency. The information can be controlled from a remote centralized location or locally at the site [30]. By this, the drivers are informed in real-time about the traffic conditions of the road ahead.

The general function of VMS would be as follows: 1) information about travel time between known destination, 2) congestion along the highway, 3) construction and maintenance notice, 4) special events notice and instruction, 5) weather condition and 6) incident notification [30]. The main objective is to prepare drivers for unavoidable conditions or give directions to properly allocate vehicles through the network. However, the efficiency of VMS in real-time traffic operation is highly dependent on drivers' interaction with the displayed messages [29].

The messages displayed in VMS are classified into two categories. The passive message provides descriptive information about the traffic condition on the road

which a driver may encounter. Within qualitative information, the situation on the road is described generically e.g. accident, work zone, congestion. Whereas quantitative information is more specific such as expected delay, location, etc [29]. However, this paper does not only focus on passive messages, as well as providing explicit route guidance such as the best alternative route for avoiding congestion. This is called active information.

5.1. VMS is Currently in Operation

The existing VMS is based on algorithms that target specific networks and lack the ability to display messages consistent with driver diversion response attitude. It provides information on surrounding traffic conditions such as weather, work zone, control access to high occupancy vehicle (HOV) lanes, and notify drivers about incidents and other public events and level of congestion. A common disadvantage of them is not considering the interaction between drivers and displayed messages [15]. It is a critical attribute to enhance the overall performance of the network ensuring the acceptance of the guidance, as well as, improving the credibility of the VMS information among drivers [15]. Furthermore, most of the current VMS displays messages in static or quasi-static algorithms, not dynamically reflecting the changes in traffic conditions, especially during incidents and unpredicted congestions. Moreover, the current VMS lacks spatial and temporal consistency of displayed messages. A frequent variation in the displayed messages, inconsistency between consecutive messages, and route prescription which leads to unfavorable experience will degrade the overall efficiency of VMS.

5.2. Real-Time VMS Concept Design

The VMS developed in this paper works on the basis of incident or high congestion in a network where the downstream flow is zero or less than upstream. Thus, a shock wave forms backward. In this context, VMS is an approach that can direct vehicles to alternative routes in case of complete blockage or highly congested and divert to an alternative lane in case of lane blockage. Thus, the VMS system relies on the analysis of traffic conditions before and after the occurrence of an incident or congestion and their adverse impact on the traffic flow (**Figure 5**).

In this regard, three terms are defined as follows:

Current State

The current state of a traffic stream shows free traffic flow. If no incident happened or the flow is less than the capacity of the road, the traffic stream is in normal condition. Therefore, no action is needed in terms of traffic management.

Incidents/High congestion

It shows the situation when an incident or high congestion due to phantom jam or bottleneck occurred. In case of incident/high congestion, the normal

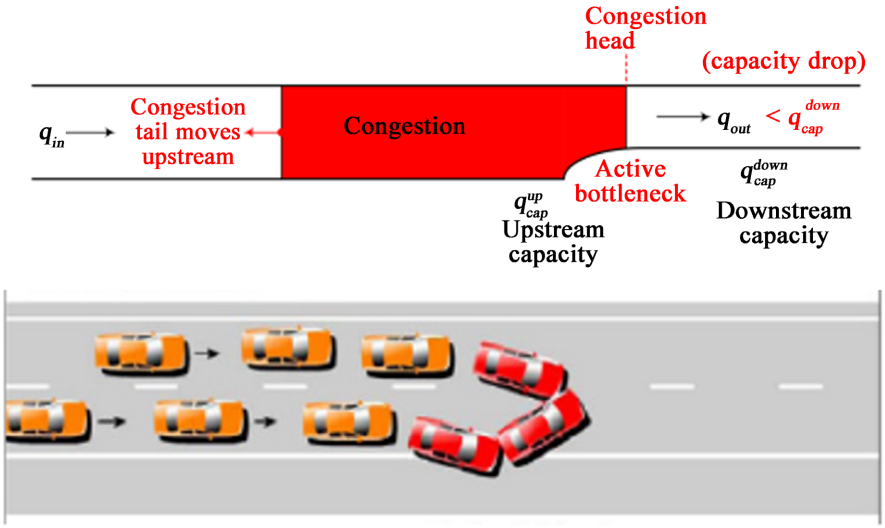

Figure 5. Top: bottleneck congestion, down: incident congestion [15].

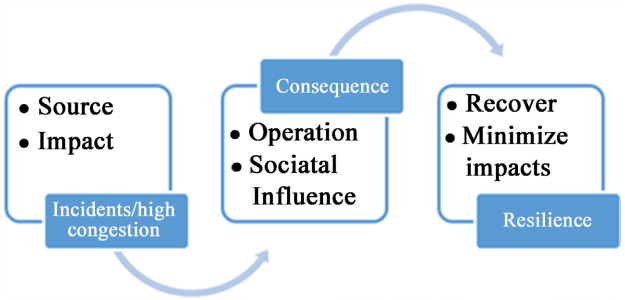

Figure 6. Incident/high congestion in the network [14].

stream of traffic flow deteriorates. Such events may happen to transport infrastructure or operation conditions, or both of them. However, the transportation system needs to be robust enough to handle such disturbance.

Consequences and resilience

Consequences of an event in topology or operating conditions can be defined as the deviation from the original performance of the system [14]. The congestions influence many aspects of the transportation system including the movement of goods and passengers, as well as society. Thus, the traffic stream should be restored to its normal situation to mitigate the consequence of disruption (**Figure 6**).

In this context, the VMS contributes road network to reduce the consequences of congestions and recover to the original state as soon as possible by guiding drivers to take the most appropriate route (lane in case of partial blockage) where the incident/bottleneck did not happen, and traffic flow is low. It should be noted that the concept developed in this paper is similar to the concept designed by [15]. However, the algorithm for congestion detection is different here. Furthermore, [15] based their approach on the incident and assumed complete blockage of the route in all cases. While in reality, this is not true. An incident may only block one or more lanes, not all existing lanes. Thus, the approach proposed in this study covers both scenarios. In addition, the VMS algo-

rithm proposed in this study works with high congestion which was not covered in previous studies.

The VMS heuristic developed here determines when the VMS should be activated, what messages should be displayed, and how frequently the messages should be updated. Within this approach, the system is computationally tractable online, consistent with driver behavior, and responsive to the fluctuation of traffic situations. Its implementation framework uses a hybrid combination of off-line and online components to determine the diversion rates that would optimize system performance under an incident or high congested condition. The system deactivates five minutes after complete clearance of the congestion. Dynamic traffic assignment (DTA) model used to determine desired diversion rates which look for consistency between system and driver response behavior. The message updates frequency differs over time based on the status of the congestion. It means if the intensity of congestion decreases or increases, the content of the VMS changes accordingly to the traffic conditions. It should be noted the drivers who obtain this information through their smartphone applications, the system will not influence their behavior since it is a generic VMS while they already receive personalized messages.

Figure 7 represents the overall algorithm of how VMS works. Whenever congestion happens, the prediction model identifies the level of congestion and possible clearance time. Later on, the traffic control center (TCC) analysis the current state of traffic stream on specific lane or lanes. Then, the DTA model determines the desired diversion rates simultaneously to the objective of the system. Consequently, several VMS are activated. The displayed message is an optimal match between desired diversion rates and the diversion rate obtained from the drivers' response model. The VMS's information is updated by VMS control heuristic. Finally, the loop ends when the congestion is cleared.

Element of VMS Algorithm

The data used for the process of the VMS system generates from dual loop

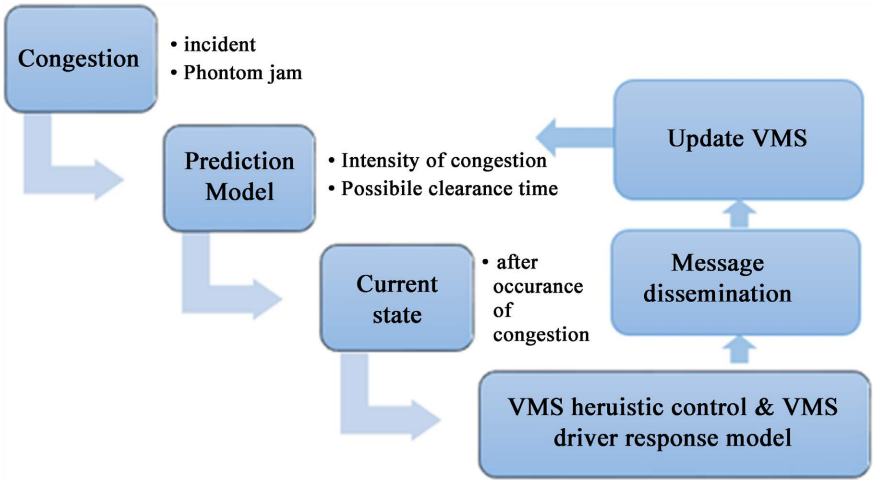

Figure 7. VMS algorithm [19].

detectors which are already being used on the roads for other traffic management purposes. The loop detectors measure flow, speed, and occupancy within a 20 second time interval. Later on, All-purpose Incident Detection (APID) algorithm is used to identify incident/high congestion in the network.

The APID algorithm was developed for the use of the COMPASS advanced traffic management system in Metropolitan Toronto [31]. It uses a combination of different algorithms to identify incident/high congestion conditions at low to high traffic flows [32]. It expands and incorporates the major components of the California algorithm into a single structure [31]. A major difference with the California algorithm is using algorithms under different traffic conditions. This algorithm uses three main routines: a low volume routine, medium volume routine, and high-volume routine. While the California algorithm uses only a high-volume routine. The algorithm includes the following parts [31]:

- General incident detection algorithm under heavy traffic conditions;
- General incident detection algorithm under light traffic conditions;
- Medium volume incident detection algorithm;
- Incident termination detection routine;
- Routine for testing the presence of compression waves;
- Routine for testing the persistence of incident conditions.

The basic algorithm uses compression wave testing whenever it is detected [32] Persistency testing is also applied to identify the end of congestion and time returning to normal traffic conditions. Typical parameter thresholds used in the APID algorithm are shown in **Table 1**.

In addition to the use of occupancy as a traffic stream indicator, the APID takes into account the variation of speed obtained from volume and occupancy. Thus, its reliability is about 95% - 98% and is fairly reliable [31], while the California algorithm is sometimes unreliable.

VMS Driver Response Model

Although drivers' response depends on the availability of alternative routes and the extent to which they are close to change, type of the information provided by

Table 1. Measures used by APID algorithm.

Description	Measure
Special difference in occ (OCCDF)	occdf(i,t)=occ(i,t)=occ(i+1,t)
Relative spatial difference in occ (OCCDF)	occdf(i,t)/occ(i,t)
Relative temporal difference in d/s occ (DOCCTD)	docctd(i,t)=(occ(i+1,t-2)-spd(i,t))/spd(i,t-2)
Downstream Occupancy (DOCC)	doc(i,t)=(occ(i+1,t)
Relative temporal diff in speed (SPDTDF)	spdtdf(i,t)=(spd(i,t-2)-spd(i,t))/spd(i,t-2)
Persistency threshold (PERSYH)	Threshold to be exceeded in persistency check
Medium Traffic Threshold (MEDTRFTH)	The threshold to be exceeded to use med flow alg
Clearance Threshold (CLRTH)	The threshold to be exceeded to clear incident

Adopted from: [32].

VMS about traffic conditions ahead has a significant influence on the route choice [33]. Most driver response model in the network scale is based on the assumption that drivers are looking forward to minimizing objective function like travel time [33]. Previous studies have identified a number of underlying factors which influence the decision-making of drivers in route selection including, journey time, congestions and delays, signposted routes, safety hazards, and unfamiliarity with the network. Whenever information such as incident, delay, and congestion are displayed in VMS, it has an important impact on route choice [19]. However, the effectiveness of the VMS is dependent on the phrasing of the message as well.

One of the approaches mostly used in literature is the stated preference (SP) technique. Within the SP model, a series of hypothetical scenarios are offered in the form of discrete choices between alternative routes and variables which influence the route choice [33]. However, revealed-preference responses (drivers who actually took alternative route after seeing VMS messages) is lower than ST responses (drivers who said they would take alternative routes) [34]. Moreover, socioeconomic characteristics (gender, age, education level, and household size), network spatial knowledge (e.g. familiarity of the network), trip type (work or non-work), amount of delay, and trust in VMS information are other effective factors in the decision-making of drivers. Within this paper, the driver response model is adapted from a study by [29] in which the content of provided information via VMS acts as an independent variable. **Table 2** represents the result of the stated preference (SP) survey conducted in Borman Expressway of Indiana by [29]. Level 5 means the high willingness and 1 indicates a low willingness of route diversion. It can be inferred that expected delay, best detour, location of accident, and occurrence of the accident are valuable information to be displayed in VMS. As the information content increases, the propensity of drivers increases simultaneously to divert their route.

Table 2. Effect of VMS message content.

VMS Message Type	Message Content	Relative Willingness to Divert				
		1%	2%	3%	4%	5%
1	Occurrence of accident only	13.7	33.9	26.6	13.3	12.5
2	Location of the accident only	20.2	33.1	22.6	11.3	12.9
3	Expected delay only	9.3	12.9	39.5	23.8	14.5
4	The best detour strategy only	7.7	18.5	30.2	25.0	18.5
5	Location of accident and the best detour	2.0	4.0	22.6	35.1	36.3
6	Location of the accident and the expected delay	0.8	0.8	19.8	38.3	40.3
7	Expected delay and the best detour strategy	2.0	2.0	13.7	33.5	48.8
8	Location of the accident expected delay, and the best detour strategy	1.2	2.0	5.6	19.8	71.4

Source: [29].

VMS Control Heuristic

VMS heuristic control ensures the activation of appropriate VMS and determines the optimal diversion rates at the activated signals. It explores new alternative routes in proportion to the initial route/lane where congestion is happening. The activated VMS locations are specified by comparing diversion rates with the threshold criteria. Then, the information is updated accordingly to the clearance status of the route. It helps traffic management (congestion management) by diverting the upstream traffic flow to other paths. While in case of no information, all drivers would continue along their initial route and this makes the situation worse.

The framework used for the VMS control heuristic is a hybrid model consisting of online and offline elements. The offline element represents the computationally intensive aspects that determine the benchmark for time-dependent vehicle path assignment proportion via deterministic DTA algorithm for probable congestion condition and mean of O-D demand [35]. The sets of path assignments are later on used by the online element. In case of an incident or other high congestion, the online VMS control heuristic is executed to determine the desired diversion rates and the messages for displaying [35]. If there is no congestion on any of the links, the deterministic DTA model is used to find the optimal route assignment. The process repeats until all VMS are deactivated which means the clearance of the congestion in the network [15].

In this context, the algorithm used in this paper is divided into three sub-algorithms as follows:

1) VMS activation

The activation algorithm works based on diversion rates compared to a predefined threshold (**Figure 8**). The system scans all origin-destination pairs in the

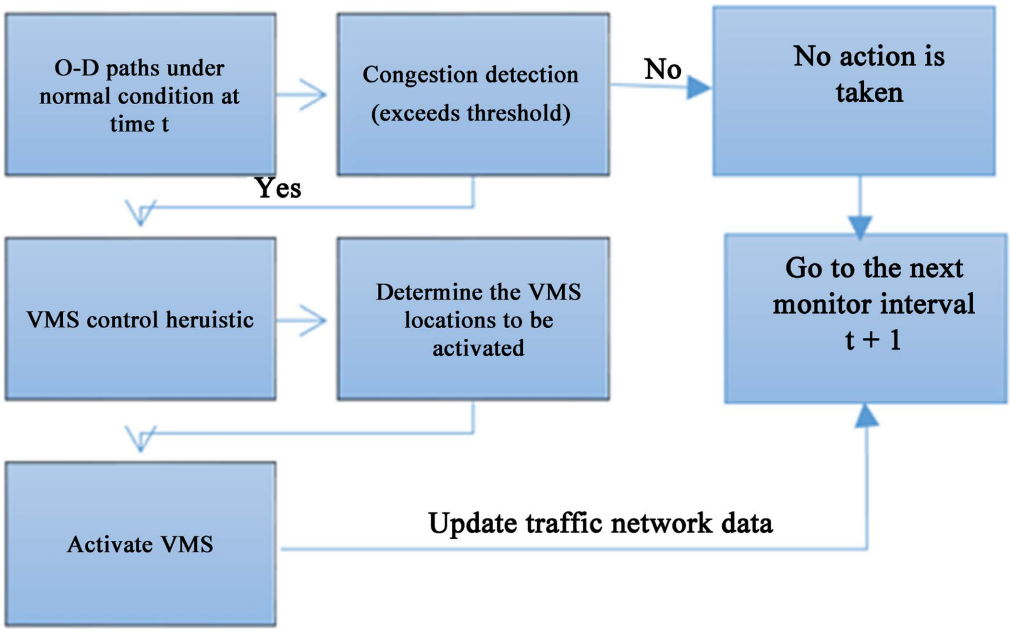

Figure 8. VMS activation algorithm [15].

network to find out where congestion has occurred. In case of an incident or any other congestion on a specific route, the VMS activates. The number of VMS that should be activated depends on the traffic manager to define the threshold. Time and distance-dependent thresholds are common approaches in the field. [15]. For instance, n minutes from the congested location is a time-dependent measure based on average travel time from an incident location toward upstream. The distance-dependent approach can be used if the time-dependent measure is not applicable. It refers to a specific distance from the incident location.

2) Message Display

The message displayed on the activated VMS is based on the system controller objectives. The route/lane assignment is computed to determine the desired diversion rates, then the simultaneous message to be displayed in the VMS for drivers to switch their route/lane. The percentage of diversion from the route/lane where VMS is activated represents the desired diversion rate. It should be noted there should be a single message for all activated VMS. Thus, a combined measure of the diversion rates should be taken into account to reach an optimal situation during operation [15]. **Figure 9** shows the algorithm and related steps for displaying the VMS messages.

3) Message Update

The messages should be updated accordingly to the changes in the traffic condition since the intensity of congestion reduces over time [15]. Clearance of the congestion on the route increases its capacity thus, it requires updating the displayed message which was shown on the VMS in the vicinity of the congested area. The frequency of the update depends on the congestion clearance and flow condition of upstream. For instance, the difference between the capacity of the link at the congested location at time t and t-1 exceed a pre-set time-dependent threshold, then the message should be updated (**Figure 10**). Reduction in travel time along affected links can also be used as an indicator of changes in the traffic condition of the route. For example, if the travel time in the congested link differs x minutes from time t to t − 1, then the information in VMS needs to be

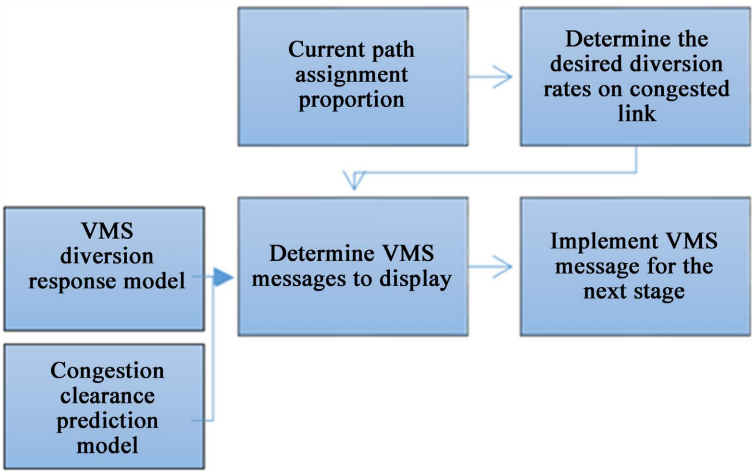

Figure 9. Message display algorithm [15].

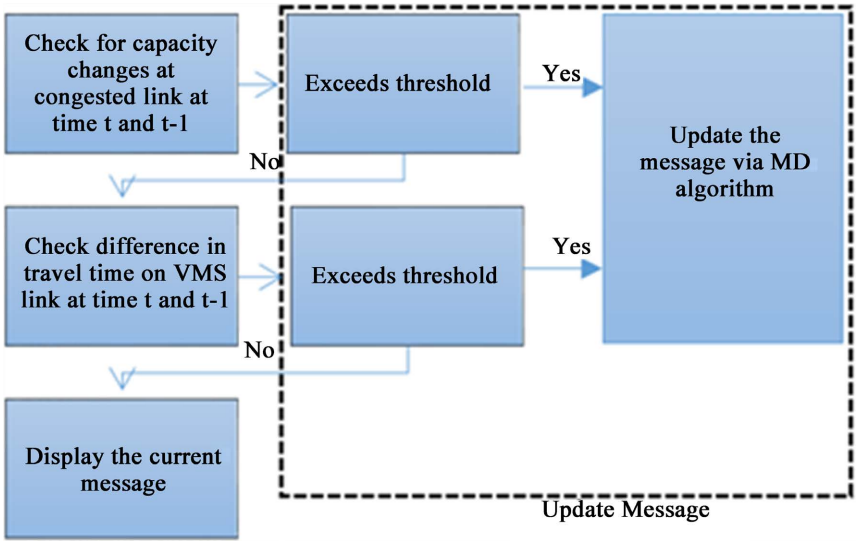

Figure 10. VMS update algorithm [15].

changed. In case of no requirement for an update based on the aforementioned criteria, the messages are retained.

6. Vulnerabilities of VMS

ITS has been deployed with a focus on increasing efficiency and safety in case of traffic flow disturbance [26]. It indicates the resilience of transportation systems to restore to normal condition after experiencing failure as soon as possible. Furthermore, the credibility of traffic signs is extremely important to effectively operate, otherwise, drivers eventually will not pay attention to messages they distrust [26]. However, these systems including VMS are associated with a new type of vulnerability named cyber-attack. Despite several studies regarding the promotion of cybersecurity of traffic measures, holistic security solutions somehow remained undiscovered [36].

The VMS proposed in this study is not apart from other ITS measures. The primary reason for its vulnerability to cyber threats is its location on the transportation network. The VMS cabinet can be unlocked effortlessly [37]. Problematic scenarios happen when hackers send tampered messages to road users [38]. It becomes even worse since wireless communications such as Wireless Sensor Network (WSN) become more common in the transportation network, and cyber-attack can lead to a more sophisticated condition [26]. The first time VMS hack happened in April 2007 in Boston, Massachusetts [37]. MIT students hacked the sign and wrote, "this sign has been hacked" (**Figure 11**). Although the intention was not malicious, the vulnerability of the system was revealed to authorities. In January 2009, attackers hacked VMS in Texas and manipulated it to display the message "Zombies Ahead" [39]. In the same month, another VMS was hacked in Collinsville, Illinois during morning peak hours and displayed "Daily lane closures due to Zombies" [40]. Moreover, several VMS hacks happened in New York during 2009 while displaying a similar message [41]. Due to

Figure 11. Hacked road sign in Boston.

false messages, drivers did not pay attention to the signs which could have caused hazardous consequences for drivers and pedestrians [41].

There are many other examples that VMSs are being hacked and providing fake information to road users. **Table 3** presents a number of cases where the VMS hack occurred in US cities.

However, most of the cases shown in **Table 3** were physical attacks in which the attackers gained access via the internet and portable VMS cabinet. A fully cyber-attack or passive attack is another serious problem for VMS. Through cyber-attack, the hackers do not show up at all since they gain access to the programming base from anywhere [26]. In this case, a VMS hack is similar to a bank hack in which authorities rarely realize the source of threats. Using the web-based interface allows the hacker to access them remotely. For instance, five VMS were hacked in North Carolina in the Ashville, Winston-Salem, and Mount Airy areas on May 30, 2014, by someone, called a "sun-hacker" (**Figure 12**) [42]. The hackers claimed that the tampering was done by accessing the Virtual Private Network (VPN) of VMS [43]. Therefore, the vulnerability of the system to cyber-threats needs to be identified, reduced, and eliminated throughout the entire supply chain and entire system lifespan [26]. Practically, such a system requires huge investment since hacking is accomplished for many purposes.

Moreover, the scale and complexity of transportation networks also induce a new set of vulnerabilities. As discussed in section 5, the VMS heuristic control analysis traffic condition of the whole network to find the congested point and appropriate alternatives thus, mapping and securing the connectivity of the entire system is difficult [7]. Access to real-time information is another source of vulnerability in the VMS and other ITS measures. VMS requires nonstop access to real-time data which leads to higher associated costs regarding maintenance and service downtime. Therefore, it puts the system in higher vulnerability [7].

Table 3. Known Hacking Events in the US.

Data	Location	Warning message	Type of tampered message	Short consequence
Cyber attack				
May-Jun. 2014	Asheville, NC Winston-Salem, NC Mount Airy, NC State of New Jersey State of lowa State of Wyoming	Traffic Information	Amusing/Fame	Driver distracted and confused
Physical attack				
Oct. 2015	Sacramento, CA	Work Zone Ahead	Amusing/Offensive	Driver distracted
Sept. 2015	Mililani, HI	Work Zone Ahead	Offensive	Driver confusion
July 2015	Tucson, AZ	Road Closure	Amusing	Driver double-take
Jan. 2015	Los Angeles, CA	Work Zone Ahead	Amusing/Offensive	Driver distracted
Feb. 2014	Granite Bay, CA	Work Zone Ahead	Offensive	Driver distracted
Nov. 2012	Loomis, CA	Road Closure	Amusing	Driver distracted
Oct. 2012	Portland, ME	Work Zone Ahead	Amusing	Driver worried and distracted
Aug. 2011	Flagstaff, AZ	Traffic Information— No left turn at the intersection	Amusing	Driver confusion
May 2011	Falls Church, VA	Warning message for bicyclists and hikers	Amusing	Driver distracted
May 2010	Miami, FL	Work Zone Ahead	Offensive	Driver distracted
Dec. 2009	Gainesville, FL	Work Zone Ahead	Amusing	Driver distracted
Mar. 2009	New York, NY	Work Zone Ahead	Amusing	Driver distracted
Feb. 2009	Hamilton County, IN	Work Zone Ahead	Amusing	Driver confusion
Feb. 2009	Collinsville, IL	Work Zone Ahead	Amusing	Driver distracted
Feb. 2009	Austin	Work Zone Ahead	Amusing	Destabilized traffic norm
Jan. 2009		Work Zone Ahead	Amusing	Driver distracted and confused
Apr. 2007		Work Zone Ahead	Amusing	Driver distracted

Source: [26].

Figure 12. VMS hacked by "sun-hackers" in Ashville.

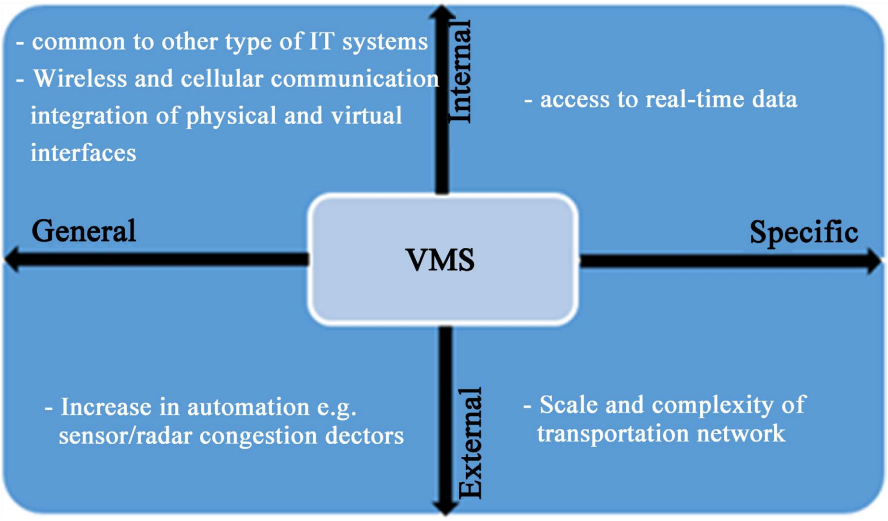

Figure 13. Matrix of VMS vulnerabilities [7].

Figure 13 shows the potential vulnerabilities induced with the implementation of the VMS.

Since the VMS developed in this study works on an integrated form that several VMSs activate at the same time to provide necessary information to drivers, a valid concern would be an integrated hack from the point that is most susceptible to a cyber-attack. If it was a conventional VMS threatened by physical attacks, the protection would not be much difficult. An integrated ITS network requires an advanced communication setup and its securing is far more challenging [30]. Furthermore, there are some other threats including, electricity cutting, low visibility due to foggy weather conditions, loss of internet connection, etc which do not relate to the design of VMS, rather than depend on the overall reliability of the traffic management system of authorities and companies.

7. Adverse Impact of VMS Failure

VMS provides the necessary information to drivers about traffic conditions such as road closure, construction zone, accidents, high congestion due to on-ramp or lane closure, and detours ahead of them. Thus, missing or neglecting such important information could lead to a disaster [26]. In other words, the hacking of VMS can destabilize the correlation between vehicles' location in the roadway, possible events ahead on the road [44]. Generally, the VMS hack results in two problems. First, drivers get distracted by a fake message displayed in VMS which can cause car collisions. Second, drivers do not see the messages that they are supposed to read as they lose their trust in VMS information. Thus, missing information about traffic conditions may cause many problems to not only drivers, but also to traffic management processes such as construction crews [26]. For instance, in the Austin case (June 2010) when drivers were confronting the sign reading "NAZI ZOMBIES AHEAD", some of them slowed down and some took pictures of that [45]. The reaction of drivers can distract them thus, increasing the risk of crashes, carbon emissions, and energy consumption [26].

Furthermore, the VMS enhances safety by providing real-time information about queue end location to alert drivers of upcoming slow-moving or stopped traffic conditions, thus it can prevent rear-end accidents [26]. With the lack of such information, drivers may run carelessly which results in more crashes.

Once the hackers take over control of the system, VMS becomes a malicious node in the traffic management system. Spyware can be installed to steal usernames and passwords, later on, it can be a source of ransomware virus or terrorist attacks [26]. Therefore, it is necessary to develop a robust system in advance, rather than after VMS implementation. Moreover, tampered VMSs need to be fixed by authorities like TM center which will dedicate additional costs, as well as, take some time to restore the system to the normal condition. **Table 4** shows the likelihood and impact of VMS hacking.

However, there are ways to improve the performance of VMS and protect it against cyber threats [42]. By good practices, we can develop effective security measures that should be implemented if they address the weaknesses identified previously. These counter threats can be either technical, policies and standards or organizational. Within the technical practice, the operators would conduct regular risk assessments covering cyber, information, and physical security to identify the critical point of the system [7]. Furthermore, unauthorized physical access to sensitive locations should be fully prohibited. For digital security of the VMS, the operators must ensure robust digital access control by:

- Using private network or VPN for VMS communication, and isolate control network from business network;
- Securing the system with strong and complex passwords;
- Implementing an authentication mechanism against physical attacks;
- Deactivating unnecessary telnet, webpage, and LCD interface;
- Secure the remote access for authorized users.

In addition, the employment of alarms/surveillance for protecting physical and digital assets is another important tool that can reduce the severity of VMS

Table 4. Impact-Likelihood matrix of VMS hacking.

	Low	LIKELIHOOD Medium	High
IMPACT LOW MEDIUM HIG	Security Impact: VMS becomes a malicious node in the TMC network	**Behavioral Impact**: Impulsive drivers behavior	Safety Impact: Crushes with severity level form property damage to injuries and fatalities
		Operational Impact: Traffic congestion, increase in travel time	**Operational Impact**: System operator financial losses
		Efficiency Impact: Increase in energy	Reliability Impact: Road user distrust of the system

Source: [26].

failure by informing the operator as soon as possible.

Moreover, the VMS can be secured through engineering policies and standards [7]. For instance, physical and cyber security should be considered upstream during the engineering process to minimize the potential risk of hacking during operation. As well as, establishing disaster recovery process, defining degraded modes of operation, implementation of information security policy, ensuring redundancy for critical VMS, regular monitor, and record of activity, engaging staff in train and raising awareness of cyber threats are important tools that can prevent VMS and other ITS failures [7].

8. Conclusions

This study aimed to investigate the resilience and robustness of traffic management measures. Ramp-metering, VSL, VMS, and autonomous vehicles are the TM measures that were discussed in this paper. The main objective was to explore how these measures can contribute to the resiliency of the road network. In addition, a concept design for VMS is developed and evaluated in terms of its vulnerability against cyber threats.

Providing advanced information through VMS about traffic conditions ahead on the road can influence the drivers' decision to change their route in case of an incident and bottleneck. Moreover, VMS is effective in directing the vehicle to alternative lanes while partial blockage of the road. As a result, the congestion recovers faster since fewer vehicles approach congested routes/lanes. Therefore, VMS would be called an important ITS measure that contributes to the resiliency of the road network. Although VMS does not have a direct impact on the robustness of transportation systems, it can indirectly enhance by diverting vehicles to alternative routes before the occurrence of congestion. In case of an incident, VMS's information reduces the number of approaching the vehicle to the affected route thus it prevents further congestions.

However, ITS measures depend on several online and offline communication interfaces which make it vulnerable to external threats such as loss of internet connection, power cut, lack of visibility during bad weather conditions, and more important cyber-attacks. The findings of this study pointed out several cases in which VMS was hacked either physically or through cyber hacking. Since ITS is working on the basis of wireless sensors, hackers are able to take over control of the system and program them with new objectives. As result, the system fails. The consequences of such an event would be disastrous. Drivers may get distracted and collide with other vehicles. Furthermore, hackers may use it for malicious intentions like terrorist attacks. Thus, cybersecurity of ITS measures including VMS is a critical point that should be considered before implementation.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Nourzad, S. and Pradhan, A. (2014) The Resiliency of Intelligent Transportation Systems to Critical Disruptions: An Eigen Value-Based Viewpoint. 2014 *International Conference on Computing in Civil and Building Engineering*, Orlando, June 23-25 2004, 1731-1738. https://doi.org/10.1061/9780784413616.215

[2] Calvert, S. and Snelder, M. (2017) A Methodology for Road Traffic Resilience Analysis and Review of Related Concepts. *Transportmetrica A*: *Transport Science*, **14**, 130-154. https://doi.org/10.1080/23249935.2017.1363315

[3] National Infrastructure Advisory Council (2009) Critical Infrastructure Resilience Final Report and Recommendations. National Infrastructure Advisory Council, Washington DC.

[4] Ganin, A., Mersky, A., Jin, A., Kitsak, M., Keisler, J. and Linkov, I. (2019) Resilience in Intelligent Transportation Systems (ITS). *Transport Research Part C*, **100**, 318-329. https://doi.org/10.1016/j.trc.2019.01.014

[5] Urena Serulle, N. (2010) Transportation Network Resiliency: A Fuzzy Systems Approach. Utah State University, Utah.

[6] Amdal, J. and Wwigart, S. (2010) Resilient Transportation Systems in a Post-Disaster Environment: A Case Study of Opportunities Realized and Missed in the Greater New Orleans Region, 2010. University of New Orleans Transportation Institute, New Orleans.

[7] Levy-Becheton, C. and Darra, E. (2015) Cyber Security and Resilience of Intelligent Transportation. European Union Agency for Cybersecurity, Athens.

[8] Zhou, Y., Wang, J. and Yang, H. (2018) Resilience of Transportation Systems: Concepts and Comprehensive Review. *IEEE Transactions on Intelligent Transportation Systems*, **20**, 4262-4276. https://doi.org/10.1109/TITS.2018.2883766

[9] Bruneau, M., Chang, S., Eguchi, R. and Lee, G. (2003) A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, **19**, 733-752. https://doi.org/10.1193/1.1623497

[10] Wieland, A. and Wallenburg, C. (2012) Dealing with Supply Chain Risks. *International Journal of Physical Distribution and Logistics Management,* **42**, 887-905. https://doi.org/10.1108/09600031211281411

[11] Snelder, M., van Zuylen, H. and Immers, L. (2012) A Framework for Robustness Analysis of Road Network for Short-Term Variation in Supply. *Transportation Research Part A*, **46**, 828-842. https://doi.org/10.1016/j.tra.2012.02.007

[12] Goldberg, M. (1975) On the Inefficiency of Being Efficient. *Environment and Planning A*: *Economy and Space*, **7**, 921-939. https://doi.org/10.1068/a070921

[13] Bardica, K. (2002) An Introduction to Road Vulnerability: What Has Been Done, Is Done, and Should Be Done. *Transport Policy*, **9**, 117-127. https://doi.org/10.1016/S0967-070X(02)00011-2

[14] Pant, S. (2012) Transportation Network Resiliency: A Study of Self-Annealing. Utah State University, Logan, Utah.

[15] Peeta, S. and Gedela, S. (2001) Real-Time Variable Message Sign-Based Route Guidance Consistent with Driver Behaviour. *Transportation Research Board*, **1752**, 117-125. https://doi.org/10.3141/1752-16

[16] Khan, A., Whelen, M., Elsafdi, O., Snobar, N., Jones, B. and Arnold, P. (2016) Automation in Driving for Enhancing Resiliency in Transportation System. Resilient Infrastructure, London.

[17] Lui, S. and Tuite, P. (2008) Evaluation of Strategies to Increase Transportation Resi-

lience to Congestion Caused by Incidents. Virginia Polytechnic Institute and State University, Blacksburg.

[18] Dia, H. and Cottman, N. (2004) Evaluation of Incident Management Benefits Using Traffic Simulation. Workshop on Traffic Simulation, The University of Queenland, Brisbane, 329-333.

[19] Hegyi, A., Bellemans, T. and De Schutter, B. (2009) Freeway Traffic Management and Control. In: Meyers, R.A., *Encyclopedia of Complexity and Systems Science*, Springer, New York. https://doi.org/10.1007/978-0-387-30440-3_232

[20] Papageogious, M. and Kotsialos, A. (2002) Freeway Ramp Metering: An Overview. *IEEE Transactions on Intelligent Transportation Systems*, **3**, 271-281. https://doi.org/10.1109/TITS.2002.806803

[21] Nsour, S., Cohen, S., Clark, J. and Santiago, A. (1992) Investigation of the Impacts of Ramp Metering on Traffic Flow with and without Diversion. *Transportation Research Record*, **1365**, 116-124.

[22] Shehada, M. and Kondyli, A. (2019) Evaluation of Ramp Metering Impacts on Travel Time Reliability and Traffic Operations through Simulation. *Journal of Advanced Transportation*, **2019**, Article ID: 8740158. https://doi.org/10.1155/2019/8740158

[23] Steel, P., McGregor, R., Guebert, A. and McGuire, T. (2005) Application of Variable Speed Limits along the Trans-Canada Highway in Banff National Park. *Annual Conference of the Transportation Association of Canada*, Calgary, 18-21 September 2005, 6-11.

[24] Darroudi, A. (2014) Variable Speed Limit Strategies to Reduce the Impacts of Traffic Flow Breakdown at Recurrent Freeway Bottlenecks. Florida International University, Miami.

[25] Feng, Y., Huang, S., Chen, Q., Lui, H. and Mao, Z. (2018) Vulnerability of Traffic Control System under Cyberattacks with Falsified Data. *Transportation Research Record*, **2672**, 1-11. https://doi.org/10.1177/0361198118756885

[26] Kelarrestaghi, K., Heaslip, K., Khalilikhah, M. and Fuentes, A. (2018) Intelligent Transportation System Security: Hacked Messages Signs. *SAE International Journal of Transportation Cybersecurity and Privacy*, **1**, 75-90. https://doi.org/10.4271/11-01-02-0004

[27] Ghafouri, A., Abbas, W., Vorobeychik, Y. and Koutsoukos, X. (2016) Vulnerability of Fixed-Time Control of Signalized Intersections to Cyber-Tampering. 2016 *Resilience Week* (*RWS*), Chicago, 16-18 August 2016, 130-135. https://doi.org/10.1109/RWEEK.2016.7573320

[28] Cerrudo, C. (2015) An Emerging Us (and World) Threat: Cities Wide Open to Cyber-Attacks. Securing Smart Cities.

[29] Peeta, S., Ramos, J. and Pasupathy, R. (2000) Content of Variable Message Signs and On-Line Driver Behavior. *Transportation Research Record*, **1725**, 102-108. https://doi.org/10.3141/1725-14

[30] Brian Kary, Department of Transportation (2000) Variable Message Signs. In: *Intelligent Transportation System* (*ITS*) *Design Manual*, Wisconsin Department of Transportation, Wisconsin, 2.1-2.10.

[31] Parkany, E. (2005) A Complete Review of Incident Detection Algorithms and Their Deployment: What Works and What Does Not. The New England Transportation Consortium, New Hampshire.

[32] Thirukkonda, S. (1997) Design and Evaluation of Freeway Incident Detection Algo-

rithms. Indian Institute of Technology, Madras.

[33] Wardman, M., Bonsall, P. and Shires, J. (1997) Driver Response to Variable Message Signs: A Stated Preference Investigation. *Transportation Research Part C*, **5**, 389-405. https://doi.org/10.1016/S0968-090X(98)00004-7

[34] Yim, Y. and Ygnace, J. (1996) Link Flow Evaluation Using Loop Detector Data: Traveler Response to Variable Message Signs. *Transportation Research Record*, **1550**, 58-64. https://doi.org/10.1177/0361198196155000108

[35] Zhou, C. and Peeta, S. (1999) Robustness of the Offline: A Priori Stochastic Dynamic Traffic Assignment Solution for Online Operation. *Transportation Research Part C*, **7**, 281-303. https://doi.org/10.1016/S0968-090X(99)00023-6

[36] Dellios, K., Papanikas, D. and Polemi, D. (2015) Information Security Compliance over Intelligent Transportation System: Is IT Possible? *IEEE Security and Privacy*, **13**, 9-15. https://doi.org/10.1109/MSP.2015.59

[37] Fermoso, J. (2015, October 16) Austin Road Signs Hacked. Warn of Nazi Zombies and World's End.

[38] Fok, E. (2013) An Introduction to Cybersecurity in Modern Transportation Systems. *Inst. Transportation Engineers*, **83**, 18-21.

[39] Miller, J. (2015, December 15) Hackers Crack into Texas Road Sign. Warn of Zombies Ahead.

[40] Metro News (2009, February 5) Another Road Sign Warn of Zombies. http://metro.co.uk/2009/02/05/another-road-sign-warns-of-zombies-432840/

[41] Soltis, A. (2009, November 6) Making Light of the Law. http://nypost.com/2009/03/17/making-light-of-the-law/

[42] ICS-CERT (Industrial Control Systems) (2018, February 12) Daktronics Vanguard Default Credentials (Update A). https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-155-01A

[43] WLOS News (Director) (2015) D.O.T. Signs Hacked in Asheville & Statewide [Motion Picture].

[44] Olofsson, J. (2014) Zombies Ahead! A Study of How Hacked Digital Road Signs Destabilize the Physical Space of Roadways. *Visual Communication*, **13**, 75-93. https://doi.org/10.1177/1470357213507511

[45] KXAN (Director) (2010) Hacked Road Signs in Austin [Motion Picture]. https://www.youtube.com/watch?v=1Lw0WMyChrM