2021

SEE-TREND: SEcurE Traffic-Related EveNt Detection in Smart Communities

Stephan Olariu
Old Dominion University

Dimitrie C. Popescu
Old Dominion University

Original Publication Citation

Olariu, S., & Popescu, D. C. (2021). SEE-TREND: SEcurE Traffic-Related EveNt Detection in smart communities. *Sensors*, *21*(22), 1-24, Article 7652. https://doi.org/10.3390/s21227652 sensors

MDPI

Article

SEE-TREND: SEcurE Traffic-Related EveNt Detection in Smart Communities

Stephan Olariu [1] and Dimitrie C. Popescu [2,*]

[1] Department of Computer Science, Old Dominion University, 3300 Engineering & Computational Sciences Bldg., Norfolk, VA 23529, USA; olariu@cs.odu.edu

[2] Department of Electrical and Computer Engineering, Old Dominion University, 231 Kaufman Hall, Norfolk, VA 23529, USA

* Correspondence: dpopescu@odu.edu

Abstract: It has been widely recognized that one of the critical services provided by Smart Cities and Smart Communities is Smart Mobility. This paper lays the theoretical foundations of SEE-TREND, a system for Secure Early Traffic-Related EveNt Detection in Smart Cities and Smart Communities. SEE-TREND promotes Smart Mobility by implementing an anonymous, probabilistic collection of traffic-related data from passing vehicles. The collected data are then aggregated and used by its inference engine to build beliefs about the state of the traffic, to detect traffic trends, and to disseminate relevant traffic-related information along the roadway to help the driving public make informed decisions about their travel plans, thereby preventing congestion altogether or mitigating its nefarious effects.

Keywords: smart cities; smart communities; smart mobility; congestion support; cyber–physical systems

check for updates

Citation: Olariu, S.; Popescu, D.C. SEE-TREND: SEcurE Traffic-Related EveNt Detection in Smart Communities. *Sensors* **2021**, *21*, 7652. https://doi.org/10.3390/s21227652

Academic Editor: Enrico Meli

Received: 18 October 2021
Accepted: 12 November 2021
Published: 18 November 2021

1. Smart Cities and Smart Communities

This introductory section is intended to offer a succinct review of Smart Cities and Smart Communities. Specifically, Section 1.1 reviews key concepts related to Smart Cities; Section 1.2 reviews a few attributes of Smart Communities; finally, Section 1.3 takes a look at smart mobility, one of the fundamental services provided by Smart Cities and Smart Communities.

As a help to the reader, Table 1 provides the definitions of all acronyms used in the paper.

1.1. Smart Cities

Visionaries have invented the Smart City metaphor almost 30 years ago to give expression to the idea that urban communities were benefiting from the most recent advances in technology, innovation, and globalization [1]. Recently, the National Academies of Sciences, Engineering, and Medicine [2] defined Smart Cities as "urban centers that use intelligent, connected devices and automated systems that maximize the allocation of resources and the efficiency of services".

Inspired by recent urbanization reports, the United Nations predicted that, if the current trends continue, by 2050, well over 68% of the world population will live in metropolitan areas [3]. In the light of this, and of the above-mentioned urbanization reports, the relevance of Smart Cities will increase tremendously.

The visionaries have defined Smart Cities in myriad different ways [4–8], As it turns out, however, these definitions have three characteristics in common:

- First, the Smart Cities will adopt an anticipatory governance style aligned with the real needs of the citizens;

- Second, they provide their citizens with timely access to high-quality information and services;
- Third, they rely on a broad-based participation of the citizens in the co-creation, in partnership with the local government, of services needed by the community.

These two fundamental characteristics of Smart Cities can be summarized by saying the Smart Cities will "put their citizens first" or, equivalently, that they will be citizen-centric communities [9]. The citizen-centric characteristic of Smart Cities is aligned with the open e-government services proposed in the past two decades by the European Union [10] and permeates the work of [11,12]. Importantly, providing their citizens with unrestricted access to high-quality information and services will naturally lead to the co-creation of new services aligned with the needs and wants of the citizenry [9,13].

Table 1. A guide to the acronyms used in the paper.

Acronym	Description
AID	Automated Incident Detection
CPS	Cyber Physical System
DEM	Distributed Expectation Maximization
DSRC	Dedicated Short-Range Communications
EDR	Event Data Recorder
GPS	Global Positioning System
ICT	Information and Communications Technology
ILD	Inductive Loop Detector
ITS	Intelligent Transportation Systems
MANET	Mobile Ad hoc Networks
NHTSA	National Highway Traffic Safety Administration
PATH	California Partners for Advanced Transit and Highways
TMC	Traffic Monitoring Centers
TMU	Traffic Monitoring Unit
US-DOT	United States Department of Transportation
VANET	Vehicular Ad hoc Networks
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle

The transition from the urban communities of today to the Smart Cities of the near future, predicted by the visionaries, will be enabled by the incredible technological advances that we are witnessing every day. One of the challenges involved in this transition is to understand how ICT can be used to empower the people, protect the environment, take action is response to climate change, attend to the needs of all segments of the population, support and promote economic vitality, etc. [13–15]. By leveraging ICT, the Smart City will deliver a large array of "Smart Services" including, *Smart Government* [10–12], *Smart Healthcare* [16,17], *Smart Homes* [18,19], *Smart Mobility* [20], *Smart Parking* [21], *Smart Transportation* [22,23], and *Smart Workplaces* [24], among many similar ones.

Recently, the authors of [9] have drawn attention to the fact that, in a very strong sense, Smart Cities are Cyber–Physical Systems wherein the Physical component is represented by the deployed infrastructure represents the Physical, while the Cyber component involves the people, their administration, and the apps they use. The Cyber and the Physical components of the CPS are locked in a dialectic relationship where they feed, condition, and learn from each other. An interesting corollary of this is that the Cyber and Physical components thrive or fail together. Consequently, the Smart Cities of the near future will continually evolve and enhance the services they offer to the citizens. This will lead to the evolution of diverse Smart Cities based on their own characteristics and the needs of their citizens. Furthermore, of course, this is confirmed by the challenge of running Smart Cities. Should the Cyber and Physical components of a Smart City run away from each other, the entire entity is bound to suffer. In recent years, we have witnessed a large number of urban communities call themselves Smart Cities. Many of these communities were Smart Cities in name only because their two components did not work together well.

It is reasonable to expect the Smart Cities of the near future to provide the socio-economic foundation for sustainable material well-being and prosperity based on an advanced service platform. This will be provided through various forms of cooperation and co-work ranging from human-to-human, to human-to-machine, and eventually to machine-to-machine [25,26]. Most of these forms of cooperation are novel, especially those arising between humans and machines or between autonomous machine systems, have yet to be adequately formalized and understood [14,27–29].

1.2. Smart Communities

In a recent solicitation [30], the U.S. National Science Foundation described Smart Communities as "*communities that synergistically integrate intelligent technologies with the natural and built environments, including infrastructure, to improve the social, economic, and environmental well-being of those who live, work, or travel within it*". The NSF definition of a Smart Community is consistent with the vision and stated goals of Society 5.0 recently publicized by the Japanese Government [13]. Aligned with this definition, Eltoweissy et al. [14] argued that a Smart Community should be motivated by the goal of satisfying most of the reasonable needs of their citizens through the co-creation and provisioning of high-quality services. Eltoweissy et al. [14] pointed out that in a Smart Community the resources and services will be valuated through a *Marketplace of Goods and Services* that will act as an impartial arbiter between producers and consumers of services. Unlike a Smart City that assumes a geographical co-location, a Smart Community is only logically co-located and not geographically. The vision expressed by [14] was to take the idea of utility computing to the next level of generality. Specifically, ref. [14] envisioned future Smart Communities as offering a large variety of evolving services packaged and sold as utilities and managed by a marketplace.

1.3. Smart Mobility—A Key Service in Smart Cities and Smart Communities

We anticipate that the transition for present-day communities, whether urban or otherwise, to the Smart Cities and Smart Communities of the near future, will offer challenging opportunities for the creative and efficient use of all the available or contemplated resources and services. Among the services offered by Smart Cities and Smart Communities, *Smart mobility* is, and in all likelihood will remain, one of the most challenging to provide in a coherent and sustainable fashion. Smart mobility involves the creative use of the latest advances in ITS in order to make traffic more fluid, better adapted to the needs of the driving public while, at the same time, minimizing its societal and environmental footprint. For example, Smart mobility should be designed in an inclusive rather than exclusive way. Smart mobility should elevate the pedestrian and cyclist experience, making them first-class citizens [22,31,32].

Smart Transportation has two key components, namely *Smart Mobility* [6] and *Smart Parking* [33,34]. In a very recent paper, Aljohani et al. [33] devoted their attention to Smart Parking solutions in Smart Cities. Their goal was to identify, among the many published papers dealing with parking, innovative solutions for parking-related problems that can be employed in the Smart Cities of the near future. In this paper, we are devoting our attention exclusively to Smart Mobility solutions that make traffic more fluid and more efficient, elevating the experience of the driving public. Specifically, we show how SEE-TREND can provide innovative solutions to Smart Mobility.

2. SEE-TREND—Motivation

Statistical data for 2019 (the last year for which data are currently available) originating with the US-DOT and NHTSA show convincingly that, contrary to popular belief, 45% of all traffic fatalities were attributable to highway traffic-related incidents rather than to rush-hour traffic in big cities [35,36]. In addition to the loss of life and property caused by traffic accidents, the US-DOT has shown that traffic-related congestion results in 2.9 billion gallons of wasted fuel, 5.5 billions hours of wasted productivity, and is also responsible for the release into the atmosphere of more than 56 billion pounds of CO_2 [37]. Not surprisingly, reducing the number of traffic incidents and making our roadways safer and more environmentally friendly is recognized as one of the key challenges of Smart Cities and Smart Communities [21,38].

Since on most American roadways traffic volumes are close to capacity, congestion is a common occurrence triggered by random fluctuations in traffic flow [37]. Traffic engineers have argued that given sufficient advance notification of traffic flow *trends*, drivers could make educated decisions about taking alternate routes, thus reducing congestion, saving time and drastically curtailing CO_2 emissions [39–42]. Unfortunately, no mechanism for detecting traffic trends well in advance is available at the moment [43,44].

In order to promote Smart Mobility in the Smart Communities of the near future, there is a critical need to *detect* trends in traffic flow, including premonitory signs of imminent slowdown and congestion. Such a system would allow drivers to make more informed decisions about their travel, therefore preventing congestion altogether or mitigating its nefarious effects.

To address this critical need, the main *objective* of this paper is to lay the theoretical foundations of SEE-TREND: a system for Secure Early Traffic-Related EveNt Detection in Smart Cities and Smart Communities. SEE-TREND implements an anonymous, probabilistic collection of traffic-related data from passing vehicles. The collected data are then aggregated and used by its inference engine to build beliefs about the state of the traffic, to detect traffic trends, and to disseminate relevant traffic-related information along the roadway.

SEE-TREND was designed to investigate issues related to the integration of wireless networking with lightweight roadside infrastructure into a CPS that enables efficient, secure, and privacy-preserving detection of traffic-related events and the timely dissemination to the driving public of relevant information about them. The key novelties of SEE-TREND are that, in sharp departure from existing approaches, our system:

1. Detects existing traffic conditions and discovers discernible trends in the traffic flow; this allows SEE-TREND to predict imminent traffic events and to alert interested parties to their likely occurrence;
2. Intelligently disseminates relevant traffic-related information using a recently-developed information decay model. This model developed by [45], captures the rate at which the value of traffic-related information decays as a function of time and distance;
3. Is secure, privacy-aware and non-intrusive. Being non-intrusive, the deployment of SEE-TREND will not adversely affect the durability and structural integrity of our roadways, as ILDs do.

Our Contributions

SEE-TREND is a transformative, next-generation distributed system that will help promote sustainable Smart Mobility is the context of the Smart Cities of the near future. SEE-TREND will contribute to aggregating traffic-data collected by the huge fleet of vehicles on our roadways into a comprehensive, near real-time synopsis of traffic conditions nationwide.

Our contributions can be summarized as follows:

- We have developed techniques for setting up and managing secure data collection. SEE-TREND collects traffic-related data from vehicles participating in the traffic flow. Since, in general, these data are highly correlated, there is no need to collect data from *all* passing cars, especially in dense traffic. In support of privacy and security of data collection, every message will be associated *anonymously* with a physical vehicle, eliminating the need for IDs or pseudonyms;

- SEE-TRENDS detects trends in the traffic flow by aggregating the collected data: SEE-TREND aggregates traffic flow data collected from participating vehicles and uses the resulting information to *anticipate* trends in the traffic flow and to infer the likely occurrence of traffic events including imminent slowdowns and congestion;
- SEE-TRENDS enables efficient traffic-related information dissemination. SEE-TREND provides two integrated modalities for information dissemination. For non time-critical information dissemination, SEE-TREND relies on vehicles in the oncoming traffic; however, time-critical messages are disseminated directly by the SEE-TREND roadside infrastructure. One of our key objectives is to further extend the model of information decay both in time and distance [45]. Such a model can be used to optimize the dissemination of relevant traffic-related information thus reducing network traffic;
- SEE-TRENDS supports information dissemination in planned evacuations and emergencies. SEE-TREND allows emergency management personnel to disseminate important information to drivers. This feature of the system is vital during large-scale evacuations, allowing emergency managers to alert drivers to estimated travel times, to the availability of resources, and to contraflow policies.

This paper is organized as follows: in Section 1 we begin by offering a short introduction to Smart Cities, Smart Communities, and Smart Mobility. Next, Section 2 motivated SEE-TREND as a key catalyst for enabling Smart Mobility. Section 3 offers a review of technical issues that will facility the presentation. Specifically, in Section 3.1 we present our vehicular model; in Section 3.2 we introduce vehicular networks and the wireless communication model assumed throughout the paper; in Section 3.3 we discuss briefly security issues in vehicular networks; in Section 3.4 we introduce Intelligent Transportation Systems; in Section 3.5 we review smart-phone based systems for detecting traffic-related events. Next, in Section 4 we outline the architecture of SEE-TREND. Specifically, in Section 4.1 we introduce the TMU, the work-horse of SEE-TREND; Section 4.4 discusses the coverage area of TMUs. Section 4.2 discusses secure TMU to TMU communications. This is followed by Section 4.3 that discusses secure vehicle to TMU communications and by Section 4.5 discussing role-based vehicle-to-TMU Communications. Next, Section 4.6 discusses a probabilistic data collection strategy. Following this, Sections 4.7 and 4.8 discuss, respectively, how to make SEE-TREND secure and fault-tolerant. Section 5 discusses various strategies that SEE-TREND employs to disseminate traffic-related information to the driving public. Specifically, Section 5.1 presents the dissemination of non-time critical information. This is followed, in Section 5.2 by strategies if time-critical information dissemination; further, in Section 5.3 we discuss role-based information dissemination, while in Section 5.4 strategies for information dissemination in planned evacuations is discussed. Section 6 presents a case study of how SEE-TREND can be used for the early detection of potholes on highways. Finally, Section 7 offers concluding remarks and identifies challenges ahead.

3. State of the Art

SEE-TREND straddles a number of research areas ranging from exploiting vehicular on-board resources, to vehicular networks, to ITS, and to security and privacy, to name just a few. The main goal of this section is to offer a succinct synopsis of relevant recent developments in these areas, focusing particularly on previous work on which we build.

3.1. The Vehicle Model

We assume that vehicles have the following on-board capabilities:

- GPS receiver;
- A short-range, DSRC-compliant, wireless transceiver;
- A tamper-resistant Event Data Recorder (EDR). The EDR is responsible for recording mobility attributes including acceleration, deceleration, lane changes, etc. [46]. Each such transaction is associated with an instantaneous GPS reading (in its 2006

ruling [47], the NHTSA has mandated that starting September 2010 an EDR will have to be installed in vehicles with an unloaded weight of less than 5000 lbs). All of the vehicle's sub-assemblies feed their readings into the EDR [48,49].

With millions of new cars sold in the US each year [35], we will soon have millions of these advanced vehicles on our roadways and city streets.

3.2. Vehicular Networks

The original impetus behind VANET, a variant of MANET, was to provide the driving public with real-time notification of traffic and road conditions. The promise of VANET has intrigued the wireless networking research community over the past three decades. Over the years, a number of applications were developed, various standards were written, and many useful protocols were proposed and implemented.

In the past three decades a number of VANET prototypes have been deployed in Europe and Japan by consortia involving car manufacturers [50–52], government agencies and various standardization bodies [53,54]. In the US, the PATH initiative has investigated fundamental issues ranging from platooning, to various forms of automated driving, and to collision warning systems [39,41]. Recently, the US-DOT inspired by the reality of present-day vehicles endowed with a vast panoply of on-board sensors and powerful radios, has launched the Connected Vehicles Initiative [55,56] whose stated goal is to investigate the integration of ITS with vehicular communications. The idea behind the Connected Vehicles Initiative is that connected vehicles, using V2V and/or V2I communications, could have a tremendous potential on traffic monitoring and incident detection [57–59].

3.3. Security and Privacy Issues in VANET

Privacy and security issues are of fundamental importance in VANET. The bulk of security solutions proposed for VANET use standard cryptographic techniques that rely on encryption to promote trust between communicating vehicles or between vehicles and the roadside infrastructure with which they are communicating. Recently, a number of protocols have been developed for key agreement supporting confidentiality and authentication services in VANET [41,60,61]. There seems to be a consensus in the Cyber-security community that while symmetric-key-based protocols tend to be simpler, they are not sufficiently flexible for use in dynamically reconfigurable networks. Public key-based protocols offer more flexibility and scalability but tend to be slow and to consume a great deal of computational resources. In order to avoid vehicle identification, several approaches advocate the use of time-varying pseudonyms. To implement this solution, vehicles need to contact periodically either roadside infrastructure or a certificate authority to obtain new pseudonyms, or preload many pseudonyms into a tamper-proof on-board device [62,63]. However, even with the use of pseudonyms, tracing communication to the owner of the vehicle is often difficult to prevent [64–67].

3.4. Intelligent Transportation Systems

One of the main goals of ITS is to offer the driving public a host of traffic state monitoring and data collection facilities. This is achieved by using a combination of legacy technologies and more recent initiatives leveraging V2V and/or V2I communications and sensor technologies [68–72]. It is fair to say that the past decade has witnessed a convergence of vehicular networking technology with ITS, promising to revolutionize the way we drive by creating a safe, secure, and robust ubiquitous and pervasive computing environment that will eventually encompass our highways and city streets [37,73].

Well known traffic monitoring and incident detection techniques proposed in the past forty years, many of which are still in use today, employ ILDs, video detection systems, acoustic tracking systems and microwave radar sensors [74–76]. Of these, the most prevalent are the ILDs used to measure traffic flow by registering a signal each time a vehicle passes over them. Each ILD, including hardware and controllers, costs around USD 8200; in addition, adjacent ILDs are connected by optical fiber that costs USD 300,000 per mile [77]. Unfortunately, official statistics show that, at any moment in time, over 50% of the installed ILD base and 30% of the video detection systems are defective or otherwise unavailable [78,79]. Moreover, by the extensive use of wireless communications have raised security and privacy concerns, very similar to those encountered in VANET. Not surprisingly, transportation departments worldwide are looking for more reliable and more cost-effective solutions for traffic monitoring and incident detection [37].

3.5. Smartphone-Based Systems

The widespread adoption of smartphones has suggested enlisting these and other similar portable devices such as iPads, FitBits, Smart Watches, Smart Glasses and the like to supplement legacy traffic monitoring by allowing the driving public to provide input in the form of ad hoc incident reports. An early implementation of this idea has resulted in *511 Traffic* intended to offer an at-a-glance view of road conditions in a given geographic area [80]. However, one of the key limitations of 511 Traffic is that it is a *centralized* system that accumulates and aggregates traffic-related feeds at TMCs. Due to inherent delays, 511 Traffic often displays out-of-date traffic information [81].

The recently-completed Mobile Millennium project at the University of California Berkeley harvested and exploited traffic-related information collected by probe vehicles to infer information about the state of the traffic [82]. A lesson learned from the Mobile Millennium project is that relying solely on traffic data collected by probe vehicles seems to work best in urban environments that experience a high concentration of vehicles and less well on highways where the number of probe vehicles is smaller [83].

Finally, Google maps is a GPS-based geographical navigation application program for smartphones with GPS support and display screens which provides traffic status information from driver-submitted location-dependent traffic status information along with travel times and route details. Waze is a centralized system where the entire communication takes place over the mobile telephone network.

All smartphone-based systems known to us rely on the existence of a predeployed cellular phone systems. As a result, these systems may fail to work when they are most needed, that is, in the case of emergencies, whether human-made or natural, where some of the infrastructure may no longer operational. Such is the case, for example, in evacuation scenarios in the wake of a hurricane, a terrorist attack, an earthquake and the like [28,84]. In comparison, SEE-TREND is energetically self-sufficient and does not rely on predeployed infrastructure support.

4. The Details of SEE-TRENDS

This section presents the details of SEE-TREND and discusses the integration of its various components.

4.1. The TMU—The Workhorse of SEE-TRENDS

The workhorse of SEE-TREND are lightweight roadside TMUs that are positioned along the roadway at uniform distances (e.g., every kilometer or so) and are designed to be independent of the power grid, with minimal maintenance and service requirements. Furthermore, adjacent TMUs along the roadway are not connected with each other, which will result in significant cost savings when compared to the existing ILD technology that requires expensive optical fiber for interconnecting the ILDs. Figure 1 presents for illustration a roadway segment with three TMUs, A, B and C in one direction paired with A', B', C' in the opposite direction.

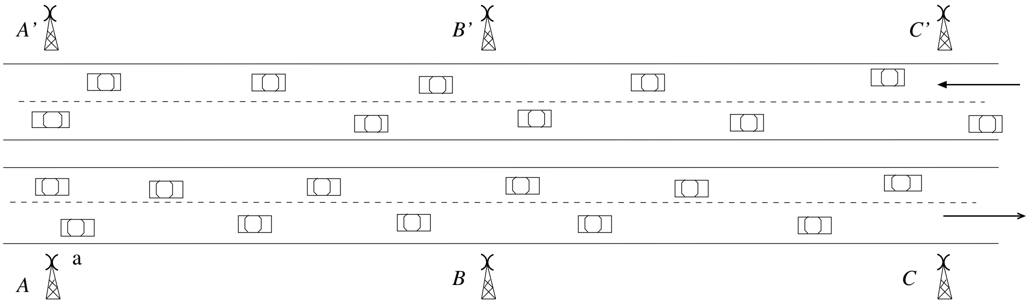


Figure 1. Illustrating a highway segment with several TMUs [85] ©IEEE.

Each TMU contains an embedded low-power computing device with a GPS and a radio transceiver, and is powered by an energy harvesting system consisting of solar panels and a battery pack that ensures the TMU energy self-sufficiency [86]. Assuming that the TMU is powered by a 12 V/200 Ah battery that holds a total of 2400 Wh of energy, and that it consumes about 15–20 W, the energy required for daily operation does not exceed 480 Wh of energy in a 24 h period. This leads to a daily battery discharge of about 20%, and the energy required to fully recharge the battery can be obtained from a 0.9 m^2 100 W solar panel (or two 50 W panels) with as little as 4 h of sunlight per day [87,88]. Moreover, with current rechargeable batteries supporting approximately 2000 charging cycles over their lifetime, the 20% per day discharge rate of the battery translates into a 6+ years of battery life, which represents a conservative estimate based on existing battery and solar panel technologies [89,90]. We note that, for practical implementations, more accurate calculations are necessary, which should consider additional details that are beyond the scope of the paper, such as the reliability of the solar energy for example, which is dependent on the geographic location of the system, weather patterns, as well as other factors.

As the central components of SEE-TREND the TMUs collect and aggregate traffic-related data from passing vehicles, as well as by exchanging information, intermittently, with adjacent TMUs. When they become aware of confirmed traffic *trends*, the TMUs disseminate this information to the vehicles that travel on the roadway. When no vehicles are present and no traffic information needs processing, the TMUs enter in a low-power vigilant mode where they only transmit periodic identification information to alert approaching vehicles, which will result in additional power savings extending the lifetime of the TMU battery.

4.2. Secure Data Exchange between Adjacent TMUs

For normal operation, adjacent TMUs are not expected to exchange information directly, and they rely instead on passing vehicles to carry information from one TMU to the other when the traffic conditions are normal. However, whenever time-critical information needs to be exchanged between adjacent TMUs, they have the ability to communicate directly for short periods of time using a DSRC-like radio interface that covers distances up to 1 km [91].

To secure the communication link between them, adjacent TMUs, say A and B, along the roadway (see Figure 1) share a *time-varying* symmetric key $\mu(A, B, t)$ that is used to encrypt, at time t, the data exchanged between them, and using GPS synchronization, the TMUs switch from one key to the next in a pre-established order based on their local time. Thus, SEE-TREND implements a robust scheme that will allow adjacent TMUs to communicate securely.

To illustrate the data exchange between TMUs A and B shown in Figure 1, let us consider that a non time-critical message m must be transmitted from A to TMU B. The process will start with the encryption of message m by TMU A with $\mu(A, B, t)$ followed by upload of encrypted message m onto passing vehicle a. When a arrives at TMU B, it will drop off message m for decoding by B. If TMU B has to send a message to TMU C, it would apply a similar process using a symmetric key $\mu(B, C, t)$, known only to B and C. We note that if the key chain contains a sufficiently large set of keys, the encryption keys used for TMU to TMU communication will appear random to an external observer.

The TMU radios will use multiple access technology to communicate with vehicles traveling in different lanes that are within the coverage area of a TMU at the same time, as shown in Figure 2. In this instance, distinct lanes in the TMU coverage area will be assigned non-interfering radio channels to allow vehicles in adjacent lanes to communicate with the TMU in parallel. The use of multiple access schemes also enables the TMU to communicate with several vehicles that are in the same lane within the TMU coverage area. We note that the length D of the TMU coverage area depends on various factors that are discussed in Section 4.3, and indicate that for vehicles traveling speeds of 70 mph a value of D = 45 m should be sufficient and may be covered by available short-range wireless technologies such as ZigBee or UWB [92–96].

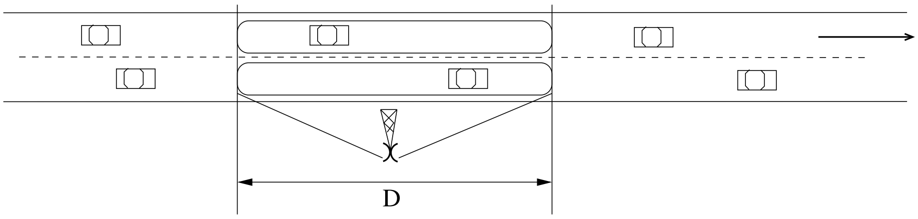


Figure 2. Illustrating the coverage area of a TMU [85] ©IEEE.

4.3. Secure Vehicle to TMU Communication

A vehicle approaching a TMU is either allowed to drop off its collected EDR data with the TMU or else is considered to be a "new" vehicle and is not authorized to do so. To be more precise, those vehicles that have correctly handshaken with the previous TMU have received a one-time session key α that allows them to drop off their EDR data, upon correctly handshaking with the next TMU. On the other hand, those vehicles that just entered the highway or have failed to handshake with the previous TMU are considered "new" vehicles and are not allowed to drop off their EDR information with the TMU. Since, by assumption, the TMUs are synchronized, a TMU can easily check for validity an alleged session-key α. It is easy to see that using one-time session keys issued by the previous TMU, precludes malicious vehicles (including rogue vehicles stationed by the roadside) from mounting a credible Sybil attack on the TMU. Furthermore, it is important to note that the session key is independent of the identity of the vehicle (and driver). In effect, this allows for *privacy-aware* communications between passing vehicles and TMUs.

As illustrated in Figure 3, a connection between a vehicle and a TMU is established when the vehicle enters the TMU's coverage area and receives, on a control channel λ, a beacon containing handshaking information [85]. Having received the handshaking information, the vehicle answers with a "HELLO" message containing

- λ encrypted with the one-time key α, or else
- Only λ if the vehicle is "new" and does not have a session key α.

The TMU then replies with an "ACK" message either encrypted with α or else issues to the vehicle a one-time session key β representing the exact contact time encrypted with the symmetric key between the current and next TMU down the road.

Consider a vehicle that was issued a one-time key β. When this vehicle reaches the next TMU it will upload β to the TMU and, upon successful validation, will be allowed to drop off data collected by its EDR. As a precautionary measure, the TMU verifies that the time at which the vehicle passed the previous TMU as recorded by its EDR corresponds to the value β properly decrypted. If the two match, the credentials are accepted and the data exchange proceeds. Otherwise, the credentials are rejected and the vehicle is, again, considered "new" and is not allowed to drop off EDR data. We note that even "new" vehicles are entitled to download any notification and warning messages that the TMU has available. However, since they are not trusted entities, they are not allowed to drop off EDR data with the TMU.

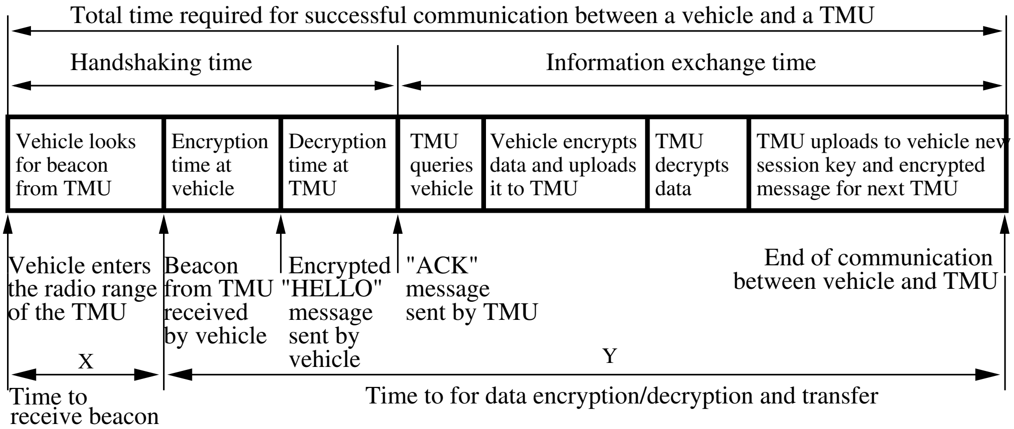

Total time required for successful communication between a vehicle and a TMU
Handshaking time
Information exchange time
Vehicle looks for beacon from TMU
Encryption time at vehicle
Decryption time at TMU
TMU queries vehicle
Vehicle encrypts data and uploads it to TMU
TMU decrypts data
TMU uploads to vehicle new session key and encrypted message for next TMU
Vehicle enters the radio range of the TMU
Beacon from TMU received by vehicle
Encrypted "HELLO" message sent by vehicle
"ACK" message sent by TMU
End of communication between vehicle and TMU
X
Y
Time to receive beacon
Time to for data encryption/decryption and transfer

Figure 3. Illustrating the details of vehicle to TMU communication [85] ©IEEE.

Next, consider a vehicle whose one-time session key α is recognized as valid. The "ACK" message returned by the TMU contains a random frequency channel σ (encrypted with α) on which subsequent data exchange is to take place; in addition, a secure one-time key may be established for the purpose of the data exchange. The vehicle switches to channel σ and proceeds to the data exchange with the TMU by:

- First, dropping off its EDR data along with encrypted data from the previous TMU;
- Second, downloading any notification and warning messages that the TMU has available.

It is important to note that the data exchange between vehicle and TMU requires that a wireless radio link be established and that data be successfully transmitted. The former requirement depends on the TMU beacon spacing (that is how often the beacon signal is sent by the TMU) and on the time required to encryption/decryption the "HELLO" message sent by the vehicle. The latter requirement depends on the encryption/decryption times and the data rate of the wireless link.

4.4. Reasoning about the TMU Coverage Area

It should be clear that successful information exchange between vehicles and TMUs depends on the amount of time the vehicles spends within the coverage area of the TMUs. For simplicity, we assume that vehicles travel at a constant speed s and that each TMU has a coverage area of size D meters. Using the notation in Figure 3 let the random variable X, with distribution function F, keep track of the time between the moment a vehicle enters the TMU coverage area and the time it receives the first beacon. We assume that X is uniformly distributed in $[0, \frac{D}{s}]$. Similarly, let the random variable Y, with *general* distribution function G, keep track of the time it takes to perform the information exchange between the vehicle and TMU. We further assume that X and Y are independent.

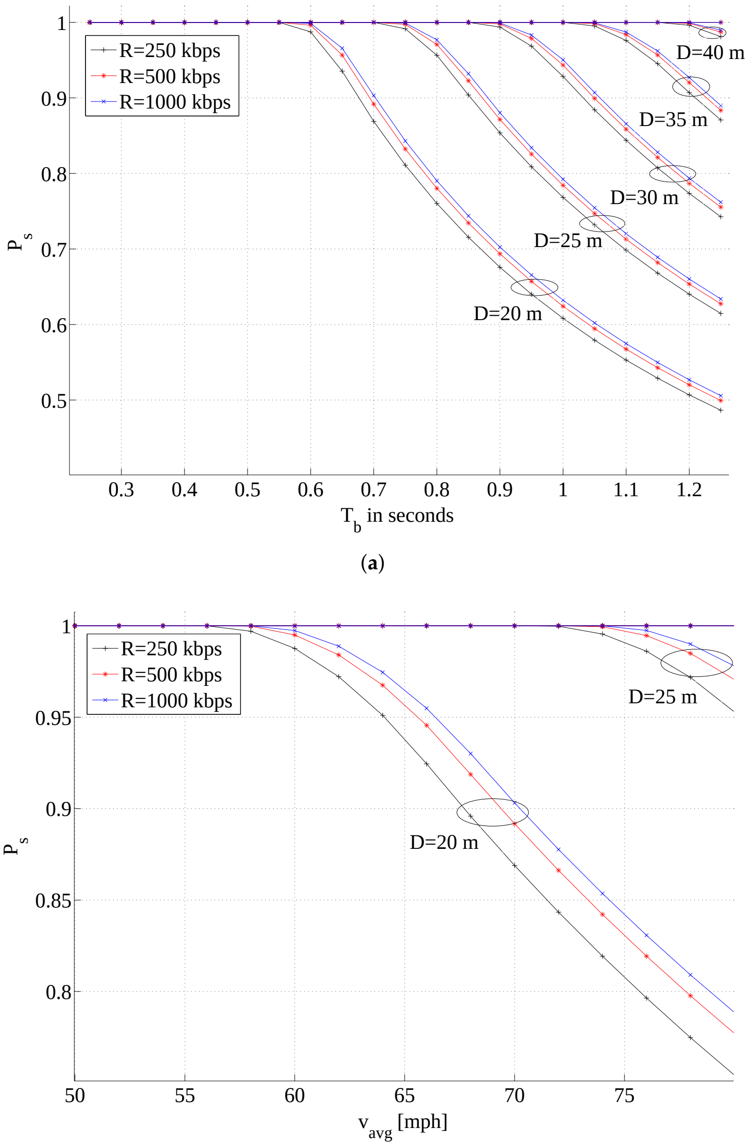
Now, the probability of the event, $P_{success}$, that the information exchange is successful is described by the conditional distribution of $X + Y$ given that the event $\{X \leq \frac{D}{s}\}$ has occurred. By the assumed independence of X and Y, we have that

$$\begin{aligned} P_{success} &= \Pr\left[X+Y \leq \frac{D}{s} \mid X \leq \frac{D}{s}\right] \\ &= \int_0^{\frac{D}{s}} P\left[X+Y \leq \frac{D}{s} \mid X = u\right] \mathrm{d}F(u) \\ &= \frac{s}{D}\int_0^{\frac{D}{s}} \Pr\left[Y \leq \frac{D}{s} - u\right] \mathrm{d}u. \end{aligned} \tag{1}$$

Assuming that X has a uniform distribution in the interval $[0, \frac{D}{s}]$ and that Y has a general distribution $G(\cdot)$ expression (1) can be written as

$$P_{success} \quad = \quad \frac{s}{D}\int_0^{\frac{D}{s}} G\left(\frac{D}{s} - u\right) \mathrm{d}u = \frac{s}{D}\int_0^{\frac{D}{s}} G(x)\,\mathrm{d}x. \tag{2}$$

To get a handle on $P_{success}$, we have considered the worst-case scenario where the maximum amount of information $I_{\max}$ is always exchanged between a vehicle and the TMU and have experimented with the following estimates (see Figure 3): 8 kb maximum data transferred between vehicle and TMU at data rates, R, of 250, 500, and 1000 kbps; $Y(y) = I_{\max}/R$ for all y; beacon intervals T_b starting from 100 ms (typical for 802.11-based wireless systems) to around 1.1 s; 50 ms for encrypting and decrypting a 1 kbyte "HELLO" message. Using these values we calculate $P_{success}$ given in Equation (2) and plot its values in Figure 4, from which we note that a value of $D \simeq 45$ m ensures $P_{success} \approx 1$ for data rates achievable with various short-range wireless technologies. The TMU coverage distance can be reduced if the requirement that the TMU successfully exchange information with all vehicles is relaxed. For example, when $P_{success} = 0.8$ (i.e., the TMU exchanges information with 80% of the passing vehicles) the TMU coverage distance D can be reduced to about 30 m or less.



(**a**)

(**b**)

Figure 4. Illustrating $P_{success}$ for various data rates R and coverage distances D. (**a**) Varying beacon interval with $v_{avg} = 70$ mph, (**b**) Varying average vehicle speed with $T_b = 0.7$ s.

4.5. Role-Based Vehicle to TMU Communications

In special situations, communications between SEE-TREND and a number of authorized vehicles such as police cruisers, ambulances, fire-fighter trucks and the like is necessary. In these cases, the communication between TMUs and passing vehicles needs to be augmented to allow authorized vehicles to interact with SEE-TREND in a predetermined, *role-based*, fashion. As mentioned, this is essential to the interaction with first responders including ambulances, fire fighters, and local police. To accommodate these special needs, authorized vehicles using a special encryption key will be allowed to upload essential information to individual TMUs. For example, police cruisers may upload information related to various types of alerts, planned lane closures, contraflow, suggested detour routes, as well as the availability of essential resources at various interchanges [97].

4.6. Enabling Probabilistic Data Collection

Recall that SEE-TREND becomes aware of traffic-related conditions by collecting EDR data from passing vehicles. Not surprisingly, these data are highly correlated simply because the vehilces in a local cohort see roughly the same traffic conditions. Thus, there is no need to collect data from *all* passing vehicles, especially in dense traffic, and one of the important issues we will investigate is *probabilistic data collection*.

Assume that, instead of collecting data from every passing vehicle, the TMU tosses a biased coin that turns up heads with probability p and collects data from a given passing vehicle with probability p. Assume, further, that the data collected from k vehicles leads to the correct detection of a raffic-relayed event with probability $1 - e^{-\theta k}$, for some application-dependent parameter $\theta > 0$ [98,99]. Let A_n be the event that, under the assumptions above, n passing vehicles suffice for the purpose of detecting correctly a traffic event.

Let H be the random variable that keeps track of the number of vehicles that have contributed traffic-data among the n passing vehicles. By conditioning on the event H we have

$$\begin{aligned}\Pr[A_n] &= \sum_{k=0}^{n} \Pr[A_n \mid H = k] \Pr[H = k] \\ &= \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} \left(1 - e^{-\alpha k}\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} - \sum_{k=0}^{n} \binom{n}{k} \left(pe^{-\alpha}\right)^k (1-p)^{n-k} \\ &= 1 - \left[1 - p\left(1 - e^{-\alpha}\right)\right]^n.\end{aligned} \tag{3}$$

Of course, the value of n depends on the vehicle arrival rate which, in turn, depends on the traffic flow. If a particular TMU is aware of the intensity of the traffic flow, it can determine the number n of arrivals per unit time. In turn, this will allow the computation of p. In fact, the TMU can deliberately forgo data collection from a number of vehicles provided the traffic flow intensity permits. This will reduce TMU power consumption without impacting the time to detect a traffic-related condition.

4.7. Implementing Security Solutions in SEE-TREND

By design, SEE-TREND allows anonymous data collection while preventing impersonation attacks. We now describe possible approaches to providing security against confidentiality and DoS attacks.

SEE-TREND provides built-in security against confidentiality attacks. This is because, as discussed in Section 4.3, the handshaking protocol between a TMU and a passing vehicle involves encrypted data and is not intelligible to the adversary, even positioned by the roadside. An intrinsic part of the handshake is the establishment of a frequency on which subsequent communication between the TMU and the passing vehicle will be conducted. This, ensures that the subsequent data exchange is not understood by the adversary.

Even with these security safeguards in place, a number of problems remain open and will be investigated in this proposal. DoS attacks can take several forms and mitigating their effects is one of the key challenges of SEE-TREND. One form of DoS attack occurs when two adversaries, X and Y, working together, each positioned by the roadside close to adjacent TMUs A and B attempt the following scheme: X will pick up the all the keys β that TMU A provides to "new" vehicle and transmits them to Y. Y then will transmit to B pretending to be a valid vehicle. TMU B will detect that the use of β is fraudulent (since the time stamp does not match); when the vehicle that was issued key β attempts to contact TMU B the attempt will be rejected since the one-time key has already been used by the adversary. If the number of "new" vehicles is large, this form of DoS attack may result in artificially thinning out the traffic seen by TMU B and, as a result, delaying the time it takes SEE-TREND to detect an event.

4.8. Making SEE-TREND Fault-Tolerant

Another important issue in SEE-TREND is fault tolerance. The basic questin here is this: how can the functionality of SEE-TREND be preserved when a TMU is disabled as a result of a malfunction or power failure. Consider the two-lane highway segment shown in Figure 5 and assume a vehicle a traveling between TMUs D and E which share the time-varying symmetric key $\mu(D, E, t)$ used to encrypt, at time t, all the messages carried between the two. If E is disabled, the messages uploaded by D are lost, since they cannot be decoded by the next active TMU, F. This, in effect, renders vehicle a "new", which may adversely impact the timeliness of data collection in SEE-TREND.

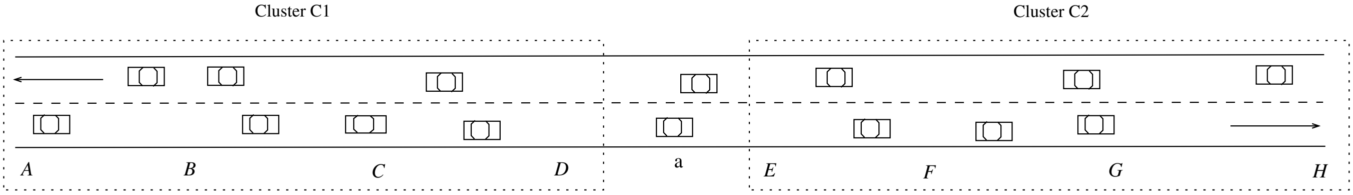


Figure 5. Illustrating clustering and fault tolerance in SEE-TREND.

We now discuss A possible approach to providing fault tolerance in SEE-TREND. The idea is to induce a simple cluster structure on the set of TMUs by grouping k, $(k \geq 2)$, adjacent TMUs into a cluster, as shown in Figure 5. We shall refer to k as the *clustering factor*. In this clustering scheme, every TMU belongs to exactly one cluster and, therefore, the resulting clusters are disjoint. The idea is that as long as each cluster contains an active TMU, messages can be correctly propagated end-to-end in accord with the SEE-TREND semantics. The clustering of the TMUs can be static or dynamic. In either case, each TMU is informed about the identity of the cluster to which it belongs. Figure 5 illustrates two adjacent clusters, with clustering factor $k = 4$ where TMUs A, B, C, D belong to cluster $C1$ while TMUs E, F, G, H belong to $C2$.

In the clustered version of SEE-TREND, all TMUs in cluster C_i know two keys, $\mu(C_{i-1}, C_i, t)$ and $\mu(C_i, C_{i+1}, t)$. Symmetric key $\mu(C_{i-1}, C_i, t)$ is used to encrypt, at time t, messages originating in cluster C_{i-1} and destined for some TMU in clusters C_{i-1} or C_i. Symmetric key $\mu(C_i, C_{i+1}, t)$, used to encrypt, at time t, messages originating in cluster C_i and destined for some TMU in clusters C_i or C_{i+1}.

Referring again to Figure 5, vehicle a carries a message encrypted by TMU D with key $\mu(C_1, C_2, t)$. If TMU E is active, then upon reaching this TMU, the messages is properly encrypted and a new (or the same) message encrypted with the key $\mu(C_2, C_3, t)$ is uploaded onto a. However, if E is disabled, then a fails to establish communication with E and carries the message to the next TMU, F. Assuming that F is active, it correctly decrypts the message and uploads to a a new message encrypted with key $\mu(C_2, C_3, t)$ informing subsequent TMUs in the same cluster that E is disabled. Observe that key $\mu(C_2, C_3, t)$ must be used since F does not know the number of remaining active TMUs in its own cluster.

To determine the amount of fault tolerance afforded by our clustering scheme let us consider a SEE-TREND consisting of n consecutive TMUs with a clustering factor of k, $(1 \leq k < n)$. A good measure of fault tolerance is the probability of the event X that SEE-TREND will fail to propagate messages end-to-end. To evaluate this probability, we assume that TMUs fail independently of each other with some technology-dependent probability p and look at the sequence of n TMUs as a string σ of n symbols A and D, with A denoting an active TMU and D representing a disabled one. Assuming all $\binom{n}{k}$ possible arrangements of σ equiprobable (i.e., adopting the Fermi–Dirac statistics [100] (p. 54)), the probability of a given k-TMU cluster to be disabled is $\binom{n}{k}^{-1}$. Thus, $P[X] = \lfloor \frac{n}{k} \rfloor \binom{n}{k}^{-1}$ and the probability that an entire cluster is down is p^k, which implies that the probability that there is no end-to-end connection is given by

$$\sum_{i=1}^{\frac{n}{k}} \binom{\frac{n}{k}}{i} p^{ki}(1-p^k)^{\frac{n}{k}-i} = 1-\left(1-p^k\right)^{\frac{n}{k}} \approx 1-e^{-\frac{np^k}{k}}. \qquad (4)$$

For example, for $n = 30$, $k = 4$ and $p = 0.1$, this probability evaluates to 0.0749%.

Having presented the components of SEE-TREND, in the next section we describe how SEE-TRENDS realizes its stated objectives.

5. Enabling Efficient Traffic-Related Information Dissemination in SEE-TREND

SEE-TREND provides two integrated modalities for information dissemination that depend on the nature of information to be disseminated, which can be non time-critical or time-critical. The latter refers to information that needs to be disseminated urgently to allow the driving public to make timely decisions, as is the case with information about a crash, for example, which, when suitably disseminated, allows drivers to take alternative exits sparing them the trouble of being stuck in traffic waiting for the crash to clear. We note that, for non time-critical information dissemination, SEE-TREND relies on vehicles in oncoming traffic, while time-critical messages are disseminated directly by TMU to TMU communication. We begin by discussing the dissemination of non time-critical information such as travel time estimates, traffic flow statistics, average speed, road work information as well as minor congestion.

5.1. Non Time-Critical Information Dissemination

For the dissemination of non time-critical traffic information SEE-TREND uses vehicles as data mules to relay encrypted traffic information between consecutive TMUs. Once they receive the relevant information, the TMUs will share it with the passing vehicles, as discussed in Section 4.3. We use Figure 6 to illustrate the backwards information propagation of non time-critical information and note that, by aggregating data from passing vehicles, TMU E becomes aware of a minor slowdown and disseminates this information to TMUs, A, B, C, D which, in turn, inform the passing vehicles. Referring to Figure 6, TMU E begins by passing the information to TMU E'. Next, TMU E' uploads onto vehicle a slowdown information destined for TMU D'. Once TMU D' learns about the slowdown it will inform D and will also upload the information onto vehicle b. The same process is then continued until TMU A receives the information. Finally, TMUs A, B, C, D inform passing vehicles about the slowdown so that they can take appropriate action.

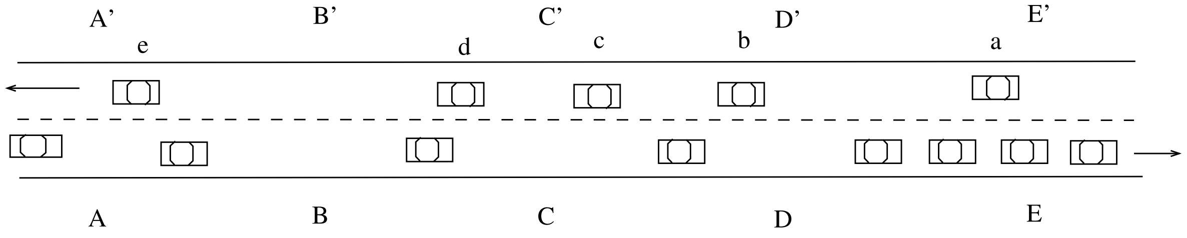


Figure 6. Illustrating non time-critical information dissemination on a two-lane roadway.

5.2. Time-Critical Information Dissemination

In order to be effective at reducing incident-related congestion, SEE-TREND must be able to quickly disseminate information to the vehicles that have not yet reached the incident area. Referring to Figure 7 imagine that TMU *E* sees a sudden significant drop in traffic volume. At the same time, TMU *D* sees stopped or crawling traffic. The other TMUs still see free flowing traffic. It is essential to determine that an accident has occurred between TMUs *D* and *E*. One approach for accomplishing this is the following. Upon seeing a sudden drop in traffic, TMU *E* sends a query to TMU *D* on a control channel. TMU *D* sees a significant increase in traffic volume and a significant reduction in speed and is also tuning in to the control channel. It is important to note that the other TMUs are not yet aware of the accident and they do not tune in to the control channel. Now it is a simple manner for TMUs *D* and *E* to establish that an accident must have occurred between them. This information is time-critical and will be disseminated to the other TMUs.

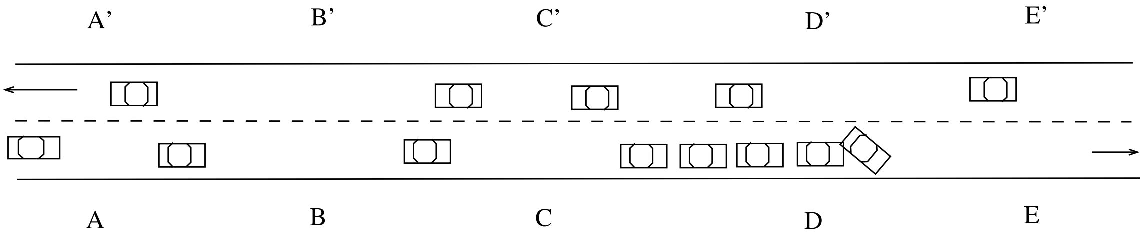


Figure 7. Illustrating time-critical information dissemination on a two-lane roadway.

5.3. Enabling Role-Based Information Dissemination

At various times, emergency management personnel and police officers need to provide drivers with important information. Since SEE-TREND is, at its most basic level, an information dissemination tool, it seems natural to allow these personnel to insert information into the system. As mentioned earlier, authorized vehicles will be given special encryption keys, used to facilitate communication with the TMUs. One of the most frequent uses of the role-based mode is when police have verified a traffic accident and are driving to the scene. As they pass TMUs, the police can input additional information about the accident that will be provided to drivers approaching the accident, validating and corroborate the findings in Section 6.

5.4. Supporting Information Dissemination in Planned Evacuations and Emergencies

As already mentioned, SEE-TREND is engineered to allow first responders and other traffic management personnel to disseminate important information to drivers. This feature is vital during large-scale evacuations, allowing emergency managers to alert drivers to estimated travel times, to the availability of resources, and to the implementation of various contraflow policies [97].

In order to minimize impact of human lives and property, massive evacuations are often necessary in the face of predictable natural disasters such as hurricanes and tsunamis. However, it is well known that there are several issues involved in a large-scale evacuation. For example, once an evacuation is underway, finding resources, such as gasoline, drinking water and shelter, quickly becomes an issue [101,102]. In two reports to Congress on hurricane evacuations [103,104] the US-DOT found that emergency evacuation plans often do not consider availability of such resources. The US-DOT also determined that emergency managers need a method for communicating with evacuees during the evacuation in order to provide updated information. The reports cited above suggested that traffic monitoring equipment should be deployed to provide real-time traffic information along evacuation routes. Aligned with this need, SEE-TREND can provide travel time estimates, notification of available resources, such as gasoline, food, and shelter, and notification of contraflow.

To facilitate this type of monitoring and information dissemination using SEE-TREND, emergency officials can place temporary hardware in the form of support infrastructure, sturdy tamper-proof devices, or mini-towers in the median, about every 10 miles in advance of an evacuation. It is important to note that these devices are temporary and would only be deployed in an emergency. The temporary devices would plug into the TMU system and connect SEE-TREND to the emergency management center overseeing the evacuation. This would provide the TMUs with important information that cannot determined solely by SEE-TREND. In addition, these devices can use powerful radios send backward messages in the case of contraflow traffic, where all lanes travel in the same direction, away from the evacuation zone.

Using the temporary hardware, SEE-TREND can query vehicles about travel times and upload that information to the emergency management center. This vital travel time information could then be released to the public via the news media (TV and radio) and the Internet, which would allow potential evacuees to make informed decisions about if and when to leave the area. In addition, this aggregated information would be fed back into the TMU system to give drivers the same information as they pass over the TMUs.

To determine open gas stations, the EDR monitors the gas tank and determines when gas was added. In addition, the vehicle knows how far it has traveled since the last fill-up. The TMU closest to each highway on-ramp can query traffic to see when and where they last added gasoline. SEE-TREND could then use this information to inform travelers of nearby available gas stations. To facilitate the dissemination of additional information, state emergency agencies could require that gas station operators, hotel operators, and restaurants who remain open during the evacuation provide accurate information to the central server, which would then provide this information to drivers via SEE-TREND. In this same way, emergency managers can upload information about open shelters to the central server. It is important to note that this system would be used to facilitate an evacuation before a disaster strikes, so we assume that electricity and network connections are available.

In addition to having state and county authorities send information to the TMUs about evacuations or contraflow policies, using role-based communication as described earlier, the TMUs themselves could determine the direction and speed at which traffic is flowing. Drivers entering on-ramps onto contraflow roadways (these ramps would likely have been used as exit ramps previously) could be alerted to the direction the traffic is moving. TMUs on one roadway could also alert drivers to upcoming on-ramps that were previously used as exit ramps during non-contraflow travel. As an additional feature, since the TMU system can monitor traffic flow, SEE-TREND could offer recommendations for which roadways are being heavily traveled in only one direction. These roadways are likely good candidates for contraflow.

6. A Case Study: Pothole Detection

Current traffic monitoring techniques perform some amount of Automated Incident Detection (AID) using established ITS algorithms [105–109]. Most of the algorithms, though, are threshold-based, meaning that traffic must be monitored for some amount of time to determine what "normal" is. After that, conditions that are different from "normal" are flagged as incidents. Unlike existing systems which use standard traffic models that describe normal traffic intensity variations to detect significant changes in traffic intensity, we plan to use the unique communications between TMUs to develop AID algorithms that are self-calibrating. In this direction, we note that SEE-TREND aggregates traffic-related data collected from passing vehicles and uses this data to detect traffic-related events and to anticipate trends including imminent slowdowns and congestion. For example, TMUs can monitor the speed of passing vehicles and share that information with neighboring TMUs. A TMU detecting a sudden drop in the average speed, but not in the volume of traffic, can infer that congestion is imminent. We propose to study the use of a Distributed Expectation Maximization (DEM) algorithm that performs local computations at each TMU and passes a small set of sufficient statistics to neighboring TMUs in the iteration process.

For a preliminary analysis let us consider M TMUs and the m-th TMU records N_m speed measurements $(y_{m,1}, \ldots, y_{n,N_m})$. Let $\mathcal{N}$ denote the Gaussian density function with mean μ and covariance σ. The measurements are assumed to follow a Gaussian mixture distribution of the form

$$y_{m,i} = \sum_{j=1}^{J} \alpha_{m,j} \mathcal{N}(\mu_j, \sigma_j), \quad i = 1, \ldots, N_m \tag{5}$$

where the mixing parameters $\{\alpha_{m,j}\}$ are potentially unique at each TMU, but the means $\{\mu_j\}$ and covariances $\{\sigma_j\}$ are common at all TMUs. The goal of the proposed DEM algorithm is to estimate these parameters from the data $y = \{y_{m,i}\}$.

For $j = 1, \ldots, J$, we define $\phi = \{\mu_j, \sigma_j\}$ as the set of means and covariances, $\alpha_m = \{\alpha_{m,j}\}$ as the mixing probabilities for each TMU m and $\theta = \phi \bigcup \{\alpha_m\}_{m=1}^{M}$. The DEM algorithm computes a Maximum-Likelihood (ML) estimate, i.e., θ maximizing the log-likelihood function

$$L_y(\theta) = \sum_{m=1}^{M} \sum_{i=1}^{N_m} \log \left(\sum_{j=1}^{J} \alpha_{m,j} \mathcal{N}(y_{m,i} | \mu_j, \sigma_j) \right) \tag{6}$$

where $\mathcal{N}(y|\mu, \sigma)$ denotes the evaluation of a Gaussian density with mean μ and covariance σ. We note that our measurements are highly correlated and hence the maximum-likelihood can be interpreted as a "pseudo-likelihood" whose estimates tend to the true ML estimates as the data tends to infinity [110].

The estimated mean, variance, and mixing parameters mirror the characteristics of the traffic intensity in a quantitative manner. In the case of congested roads (lower speed distributions), the mean quantifies the severity of congestion and for un-congested roads (higher speed distributions), the mean may be used to define the acceptable/normal traffic intensity. The measure of variance represents the consistency in traffic intensity while the mixing parameters represent the congestion index on a scale of 0 to 1.

We propose a probabilistic technique to detect both temporary incidents (e.g., accidents, disabled vehicles, etc.) and long-lived anomalies (e.g., potholes) using vehicle-to-TMU communications. The proposed technique, which is the first of its kind to detect such traffic-related events, starts with some *beliefs* about the road, such as assuming that the probability of having an incident has a very small value.

When SEE-TREND notices a number of lane changes due to temporary incidents and/or abnormal road conditions, the corresponding data collected will be correlated in both time and location, and will provide *evidences* for the system to update beliefs by computing the *posteriori* probability using Bayesian inference techniques with the arrival of each *evidence* as

$$Bel(Incident) = \frac{P(incident) * P(Evidence|Incident)}{P(Evidence)} = \alpha * P(incident) * P(Evidence|Incident) \tag{7}$$

where $P(incident)$ is the *a priori probability* of an incident at a given location, $P(Evidence|Incident)$ is the likelihood, α can be computed as

$$\alpha = 1.0/[P(Incident) * P(Evidence|Incident) + P(NoIncident) * P(Evidence|NoIncident)] \tag{8}$$

and, finally, *Evidence* represents any evidence such as changing lane or passing over a pothole.

Accumulated empirical evidence has confirmed that in order to avoid a lane occlusion, most vehicles change lanes at a moderate distance away from it and that, under most traffic conditions, the distance to the occlusion at which the lane change occurs is *normally* *distributed*. We formally define the conditional probability of a lane change at location x given that an occlusion exists at location y as

$$P_{x,y} = \frac{1}{\sqrt{2\pi}} e^{\frac{-(x-y)^2}{2}}. \tag{9}$$

On the other hand, drivers may notice potholes at the last minute and hence we expect them to change lanes, if at all, very close to the pothole. Thus, we define the conditional probability of a lane change at location x given that a road condition exists at location y as

$$P_{x,y} = \frac{I(A = true)}{\sqrt{2\pi}} e^{\frac{-(x-y)^2}{2}} \tag{10}$$

where $I(A = true)$ is an indicator function returning 1 if the driver had the ability to change lanes and x was near y, and 0 otherwise. This reflects the fact that some drivers may pass over potholes and not change lanes.

Each TMU maintains a list $ManMade$ storing information about human-made road "anomalies" including rail-road crossings, speed ramps and road work. In addition, each TMU maintains two tables $TempProb[m][n]$ and $PermProb[m][n]$ where m is the number of lanes and n is the number of *segments* between two consecutive TMUs. Here, a segment is an atomic unit of length, say, around 10 m. The purpose of these tables is to record the probabilities of a temporary (respectively permanent) incident at any given segment. For example, $TempProb[i][j] = 0.8$ indicates that there is a probability of 0.8 of having some form of a temporary occlusion of lane i at segment j between two given TMUs, where all probabilities were initialized to some very small value representing the normal probability of having an incident on that road.

Define those segments that a vehicle has traversed as "passed over segments" and the others as "avoided segments". When a TMU receives an EDR report from a passing vehicle, it applies Bayes' theorem to update the posterior probabilities for different road segments, for both tables, based on the new EDR data as follows.

For each segment $p = (i, j)$ that a vehicle x has passed over, the following steps are performed.

- If x's EDR has a record for a suspected road section at location p, $p \notin ManMade$, then we need to compute the a posteriori probability of having an actual road condition at this location, update our beliefs, as

$$PermProb[i][j] = \alpha * PermProb[i][j] * P(Detection|Pothole) \tag{11}$$

  where α is computed as before. The term $P(Detection|Pothole)$ is industry–dependent and reflects how the probability of successfully detecting a road condition given that one actually exists.
- If x's EDR shows that x has significantly decelerated around location p, $p \notin ManMade$, this means that there might be a pothole at location p that the driver wanted to avoid or reduce its effect on their vehicle.

$$PermProb[i][j] = \alpha * PermProb[i][j] * P(Reduce|Pothole) \tag{12}$$

  where α is computed as described before. The term $P(Reduce|Pothole)$ represents the probability that a driver slows down when he sees a pothole. This depends on many factors including driver response.
- If x's EDR shows nothing about p, then either p is clear or x's driver avoided the pothole.

In all cases above, since x has passed over location p, there is no temporary incident at p and hence the probability of such an incident at this location should be re-initialized, i.e., we set $TempProb[i][j] = InitialProbability$. Next, assume that vehicle x has changed lanes at location $y < j$ avoiding $p(i, j)$. Observe that the lane change was due to a pothole, a temporary accident or a slow-moving vehicle. Thus, we need to compute the a posteriori probabilities as follows:

- First, we recompute the a posteriori probability of having a temporary incident at p that forced x to change lanes as $tempprob[i][j] = \alpha * tempprob[i][j] * P_{y,j}$ $(0 < i < y)$, where $P_{y,j}$ is the probability of changing lanes at location y given an incident at location j and can be computed as above;
- Furthermore, x may have changed lanes at p; we compute the a posteriori probability of having a pothole based on this new evidence: $permprob[i][j] = \alpha * permprob[i][j] * P_{y,j}$, $(0 < i < y)$, where $P_{y,j}$ is the probability of changing lanes at location y given a pothole at location j and can be computed as above.

Observe that the proposed technique cannot be deceived by slow-moving vehicles or other false positives.

After the TMU has processes data from a number of vehicles, if for some $p(i, j)$

- $PermProb[i][j] > T$ for some threshold T, infer the presence of a pothole at location (i, j). The larger the value of the threshold T, the more conservative the TMU is;
- $PermProb[i][j] = InitialPotholeProb$ and $TempProb[i][j] > T$, then infer the presence of a temporary incident at location (i, j) where $InitialPotholeProb$ is the initial belief of having a temporary incident.

7. Concluding Remarks and Challenges Ahead

In this paper, we have laid the theoretical foundations of SEE-TREND, an innovative, next-generation computing and communication paradigm. We are confident that many other applications of SEE-TREND will be discovered which could have a profound and lasting societal impact. What makes SEE-TRENDS stand out, is that it aims to accomplish the following novel goals:

- First, our goal is to build a distributed system that detects existing traffic conditions and anticipates discernible trends in highway traffic flow. This allows our system to predict traffic events and to alert interested parties to their likely occurrence;
- Second, we will intelligently disseminate relevant traffic-related information using a decay model of the value of information based on time and distance;
- Third, SEE-TREND is a secure, privacy-aware, and non-intrusive system.

There are many ways in which SEE-TREND can be extended and enhanced. The most intriguing challenges include:

- Emergency vehicle preemption is one of the well-known causes of congestion. It is important to extend role-based interaction between emergency vehicles and SEE-TREND, while limiting the impact on traffic flow;
- Yet another intriguing question is: What is the most efficient way to manage contraflow, while reserving one incoming lane for ambulances, fire trucks, and the like?
- What are the tradeoffs between TMU energy and the quality of collected data in a planned evacuation?
- Fault tolerance is a key issue in emergencies and planned evacuations. We will investigate ways in which fault tolerance will be increased in support of such events.
- Extending SEE-TREND to detect traffic trends in urban settings, which may use alternative hardware such as traffic light controllers for example, instead of TMUs, and may employ strategies based on Vehicular Clouds [15,111] or Vehicular Crowdsourcing [29].

Furthermore, it would be very important to put to work Big Data analytics using computing resources that are available on-board modern vehicles. Big Data analytics in conjunction with Vehicular Crowdsourcing [29], Vehicular Clouds [15,111], and Machine Learning [112] could enable groups of vehicles to process more traffic-related data faster and more accurately. One of the promising directions is the potential for designing and implementing efficient hardware algorithms for basic operations including prefix computation, fast sorting and searching, as well as vision algorithms using various parallel architectures such as, for example, reconfigurable architectures [113–116] or parallel architectures with various fast bus systems [84,117–121]. Using parallel architectures to harvest Big Data analytics promises to extend the capabilities of SEE-TREND. This is a worthwhile area for future work.

Author Contributions: Conceptualization, S.O. and D.C.P.; methodology, S.O.; validation, D.C.P.; formal analysis, S.O. and D.C.P.; writing–original draft preparation, S.O. and D.C.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors are grateful to the anonymous reviewers for their comments and suggestions, which improved the presentation of this work.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Gates, B. *The Road Ahead*; Viking Penguin: New York, NY, USA, 1995.
2. National Academies of Sciences, Engineering, and Medicine. *Information Technology and the U.S. Workforce: Where Are We and Where Do We Go from Here?* National Academies Press: Washington, DC, USA, 2017.
3. United Nations. *World Urbanization Prospects: The 2014 Revision, Highlights. Department of Economic and Social Affairs*; Population Division, United Nations: New York, NY, USA, 2014.
4. Harrison, C.; Donnelly, I.A. The theory of smart cities. In Proceedings of the 55th Annual Meeting of the International Society for the Systems Sciences (ISSS'2011), Hull, UK, 17–22 July 2011.
5. Hatch, D. Singapore Strives to Become the Smartest City is Using Data to Redefine What it Means to Be a 21st-Century Metropolis. 2013. Available online: https://drjdbij2merew.cloudfront.net/GOV/GOV_Mag_Feb13.pdf (accessed on 11 October 2021).
6. Lakakis, K.; Kyriakou, K. Creating and intelligent transportation system for smart cities: performance evaluation of spatial-temporal algorithms for traffic prediction. In Proceedings of the 14th International Conference on Environmental Science and Technology, Rhodes, Greece, 3–5 September 2015.
7. Litman, T. Autonomous vehicle implementation predictions: Implications for transport planning. In Proceedings of the 2015 Transportation Research Board Annual Meeting, Washington, DC, USA, 11–15 January 2015.
8. Townsend, A.M. *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*; W. W. Norton: New York, NY, USA, 2013.
9. Iqbal, A.; Olariu, S. A survey of enabling technologies for smart communities. *Smart Cities* **2021**, *4*, 54–77. [CrossRef]
10. European Commission. *Analysis of the Value of New Generation of eGovernment Services and How Can the Public Sector Become an Agent of Innovation through ICT*; Publications Office of the European Union: Luxemburg, 2016. [CrossRef]
11. Johansson, D.; Lassinantti, J.; Wiberg, M. Mobile e-Services and Open Data in e-Government Processes—Concept and Design. In Proceedings of the 12th International Conference on Mobile Web and Intelligent Information Systems, MobiWis'2015, Rome, Italy, 24–26 August 2015; pp. 149–160.
12. Johansson, D.; Lassinantti, J.; Wiberg, M. Mobile e-Services and Open Data in e-Government Processes—Transforming Citizen Involvement. In Proceedings of the 17th ACM International Conference on Information Integration and Web-Based Applications and Services, iiWAS'2015, Brussels, Belgium, 11–13 December 2015.
13. Shiroishi, Y.; Uchiyama, K.; Suzuki, N. Society 5.0: For Human Security and Well-Being. *IEEE Comput.* **2018**, *51*, 91–95. [CrossRef]
14. Eltoweissy, M.; Azab, M.; Olariu, S.; Gracanin, D. A new paradigm for a marketplace of services: Smart communities in the IoT era. In Proceedings of the International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT'2019), Sakhier, Bahrain, 22–23 September 2019; pp. 173–186.
15. Olariu, S. A survey of vehicular cloud computing: Trends, applications, and challenges. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 2648–2663. [CrossRef]
16. National Research Council. *Computational Technology for Effective Health Care: Immediate Steps and Strategic Directions*; National Academies Press: Washington, DC, USA, 2009.
17. Zhao, W.; Luo, X.; Qiu, T. Smart Healthcare. *Appl. Sci.* **2017**, *7*, 1176. [CrossRef]
18. Cicirelli, F.; Fortino, G.; Giordano, A.; Guerrieri, A.; Spezzano, G.; Vinci, A. On the design of smart homes: A framework for activity recognition in home environment. *J. Med. Syst.* **2016**, *40*, 1–17. [CrossRef]

19. Curzon, J.; Almehmadi, A.; El-Khatib, K. A survey of privacy enhancing technologies for smart cities. *Pervasive Mob. Comput.* **2019**, *55*, 76–95. [CrossRef]
20. Faria, R.; Brito, L.; Baras, K.; Silva, J. Smart mobility: A survey. In Proceedings of the IEEE International Conference on Internet of Things for the Global Community, (IoTGC'2017), Funchal, Portugal, 10–13 July 2017.
21. USDOT. The Smart/Connected City and its Implications for Connected Transportation. 2014. Available online: https://www.its.dot.gov/itspac/Dec2014/Smart_Connected_City_FINAL_111314.pdf (accessed on 11 October 2021).
22. NHTSA National Highway Traffic Safety Administration. Traffic Safety Facts—Pedestrians—DOT-HS-812-375. 2017. Available online: https://www.nhtsa.gov/road-safety/pedestrian-safety/2015PedestriansTrafficSafetyFactSheet.pdf (accessed on 11 October 2021).
23. NHTSA National Highway Traffic Safety Administration. Traffic Safety Facts—Children—DOT-HS-812-491. 2018. Available online: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812491 (accessed on 11 October 2021).
24. Zhao, W.; Lun, R.; Gordon, C.; Fofana, B.M.; Espy, D.D.; Reinthal, M.A.; Ekelman, B.; Goodman, G.D.; Niederriter, J.E.; Luo, X. A human-centered activity tracking system: Toward a healthier workplace. *IEEE Trans. Hum.-Mach. Syst.* **2017**, *47*, 343–355. [CrossRef]
25. Maglio, P.; Spohrer, J. Fundamentals of service science. *J. Acad. Mark. Sci.* **2008**, *36*, 18–20. [CrossRef]
26. Spohrer, J.; Maglio, P.; Bailey, J.; Gruhl, D. Toward a science of service systems. *IEEE Comput.* **2007**, *40*, 71–77. [CrossRef]
27. Maglio, P.; Vargo, S.; Caswell, N.; Spohrer, J. The service system is the basic abstraction of service science. *Inf. Syst. E-Bus. Manag.* **2009**, *7*, 395–406. [CrossRef]
28. Olariu, S.; Eltoweissy, M.; Younis, M. ANSWER: AutoNomouS netWorked sEnsoR system. *J. Parallel Distrib. Comput.* **2007**, *67*, 111–124. [CrossRef]
29. Olariu, S. Vehicular Crowdsourcing for Congestion Support in Smart Cities. *Smart Cities* **2021**, *4*, 662–685. [CrossRef]
30. U.S. National Science Foundation. Smart and Connected Communities. 2019. Available online: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf18520 (accessed on 11 October 2021).
31. Herrmann, A.; Liu, M.; Pilla, F.; Shorten, R. A new take on protecting cyclists in smart cities. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3992–3999. [CrossRef]
32. NHTSA National Highway Traffic Safety Administration. Pedestrian and Bicyclists Safety. 2019. Available online: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/14046-pedestrian_bicyclist_safety_resources_030519_v2_tag.pdf (accessed on 11 October 2021).
33. Aljohani, M.; Olariu, S.; Alali, A.; Jain, S. A survey of parking solutions in Smart Cities. *IEEE Trans. Intell. Transp. Syst.* **2021**, *20*, 1–18. [CrossRef]
34. Ranjini, R.; Manivannan, D. A comparative review on car parking technologies. *Int. J. Eng. Technol.* **2013**, *5*, 1763–1767.
35. NHTSA National Highway Traffic Safety Administration. Traffic Safety Facts Annual Report Tables. 2019. Available online: https://cdan.nhtsa.gov/tsftables/Introduction.pdf (accessed on 11 October 2021).
36. NHTSA National Highway Traffic Safety Administration. Traffic Safety Facts. 2019. Available online: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813206 (accessed on 11 October 2021).
37. Texas Transportation Institute. 2021 Urban Mobility Report. 2021. Available online: https://static.tti.tamu.edu/tti.tamu.edu/documents/mobility-report-2021.pdf (accessed on 11 October 2021).
38. USDOT. 2015-2019 Strategic Plan Intelligent Transportation Systems (ITS). 2015. Available online: http://www.its.dot.gov/strategicplan.pdf (accessed on 11 October 2021).
39. California Partners for Advanced Transit and Highways. PATH. Available online: www-path.eecs.berkeley.edu (accessed on 11 October 2021).
40. NHTSA National Highway Traffic Safety Administration. Early Estimate of Motor Vehicle Traffic Fatalities for the First Half of 2021. DOT HS 813 199. 2021. Available online: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813199 (accessed on 11 October 2021).
41. Olariu, S.; Weigle, M.C. (Eds.) Vehicular Networks: From Theory to Practice; CRC Press/Taylor & Francis: Boca Raton, FL, USA, 2009.
42. Wu, X.; Michalopoulos, P.; Liu, H.X. Stochasticity of freeway operational capacity and chance-constrained ramp metering. *Transp. Res. Part C* **2010**, *18*, 741–756. [CrossRef]
43. Seo, T.; Bayen, A.; Kusakabe, T.; Asakura, Y. Traffic state estimation on highway: A comprehensive survey. *Annu. Rev. Control* **2017**, *43*, 128–151. [CrossRef]
44. van Erp, P.B.; Knoop, V.L.; Hoogendoorn, S.P. Macroscopic traffic state estimation using relative flows from stationary and moving observers. *Transp. Res. Part B Methodol.* **2018**, *114*, 281–299. [CrossRef]
45. Olariu, S.; Mohrekesh, S.; Wang, X.; Weigle, M.C. On aggregating information in actor networks. *SIGMOBILE Mob. Comput. Commun. Rev.* **2014**, *18*, 85–96. [CrossRef]
46. NHTSA National Highway Traffic Safety Administration. Event Data Recorders. Federal Motor Vehicle Safety Standards 215 Part 49, Code of Federal Regulations Part 563. 2006. Available online: https://www.nhtsa.gov/fmvss/event-data-recorders-edrs (accessed on 11 October 2021).
47. NHTSA National Highway Traffic Safety Administration. 2006 Ruling. 2006. Available online: http://www.injurysciences.com/Documents/NHTSA%20Issues%20Final%20Rules%20for%20Automotive%20EDRs.pdf (accessed on 11 Ocotber 2021).

48. Gabauer, D.J.; Gabler, H.C. Comparison of Roadside Crash Injury Metrics Using Event Data Recorders. 2008. Available online: http://www.sciencedirect.com/science/article/pii/S000145750700139X (accessed on 11 October 2021).
49. Sapper, D.; Cusack, H.; Staes, L. *Evaluation of Electronic Data Recorders for Incident Investigation, Driver Performance, and Vehicle Maintenance: Final Report*; US-DOT, Office of Research: Washington, DC, USA, 2009.
50. Comes, C. Clear Shows Off WiMAX Capabilities at Chicago Auto Show. WiMAX.com. 2010. Available online: http://bit.ly/974xmY (accessed on 11 October 2021).
51. Reardon, M. Chrysler Takes Wi-Fi on the Road. cNet News. 2008. Available online: http://news.cnet.com/8301-10784_3-9978037-7.html (accessed on 11 October 2021).
52. Gruener, W. Chrysler to Put WiMax into its Cars. TG Daily. 2008. Available online: http://www.tgdaily.com/mobility-features/35601-chrysler-to-put-wimax-into-its-cars (accessed on 11 October 2021).
53. Car2Car Consortium. Car-2-Car. Available online: www.car-2-car.de (accessed on 11 October 2021).
54. Hull, B.; Bychkovsky, V.; Zhang, Y.; Chen, K.; Goraczko, M. CarTel: A Distributed Mobile Sensor Computing System. In Proceedings of the ACM SenSys, Boulder, CO, USA, 31 October 2006; Association for Computing Machinery: New York, NY, USA, 2006.
55. USDOT. Connected Vehicles. 2017. Available online: https://www.its.dot.gov/research_areas/connected_vehicle.htm (accessed on 11 October 2021).
56. US Department of Transporation. *Analysis. Modeling, and Simulation for Traffic Incident Management Applications*; Technical Report FHWA-HOP-12-045; Federal Highway Administration: Washington, DC, USA, 2012.
57. Florin, R.; Olariu, S. On a Variant of the Mobile Observer Method. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 441–449. [CrossRef]
58. Florin, R.; Olariu, S. Towards real-time density estimation using vehicle-to-vehicle communications. *Transp. Res. Part B Methodol.* **2020**, *138*, 435–456. [CrossRef]
59. Popescu, O.; Sarwar, S.M.; Popescu, D.C.; El-Tawab, S.; Abdel-Wahab, M. Automatic Incident Detection in Based on V2I Communication and Aggregation of Traffic Parameters. *IEEE Intell. Syst. Mag.* **2017**, *9*, 64–75.
60. Ishihara, S.; Nakamura, N.; Niimi, Y. Demand-based location-dependent data dissemination in VANETs. In Proceedings of the ACM Mobicom, Miami, FL, USA, 30 September 2013; Association for Computing Machinery: New York, NY, USA, 2013; pp. 219–221.
61. Luan, T.; Shen, S.; Bai, F. Integrity-Oriented Content Transmission in Highway Vehicular Ad Hoc Networks. In Proceedings of the IEEE INFOCOM, Turin, Italy, 14–19 April 2013; Institute of Electrical and Electronics Engineers: Piscataway, NJ, USA, 2013.
62. Park, M.; Gwon, G.; Seo, S.W.; Jeong, H.Y. RSU-Based Distributed Key Management (RDKM) for Secure Vehicular Multicast Communications. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 644–658. [CrossRef]
63. Zhou, T.; Sharif, H.; Hempel, M.; Mahasukhon, P.; Wang, W.; Ma, T. A Novel Adaptive Distributed Cooperative Relaying MAC Protocol for Vehicular Networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 72–82. [CrossRef]
64. Yan, G.; Wen, D.; Olariu, S.; Weigle, M.C. Security challenges in vehicular cloud computing. *IEEE Trans. Intell. Transp. Syst.* **2013**, *4*, 6–16. [CrossRef]
65. Yan, G.; Olariu, S.; Wang, J.; Arif, S. Towards providing scalable and robust privacy in vehicular networks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 1895–1906.
66. Calandriello, G.; Papadimitratos, P.; Hubaux, J.P.; Lioy, A. Efficient and robust pseudonymous authentication in VANET. In *VANET '07: Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*; ACM: New York, NY, USA, 2007; pp. 19–28.
67. Xie, H.; Kulik, L.; Tanin, E. Privacy-Aware Traffic Monitoring. *IEEE Trans. Intell. Transp. Syst.* **2010**, *11*, 61–70.
68. Bai, F.; Chen, W.; Letaief, K.B.; Cao, Z. Low Complexity Outage Optimal Distributed Channel Allocation for Vehicle-to-Vehicle Communications. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 161–170. [CrossRef]
69. Nzounta, J.; Rajgure, N.; Wang, G.; Borcea, C. VANET Routing on city roads using real-time vehicular traffic information. *IEEE Trans. Veh. Technol.* **2009**, *58*, 3609–3626. [CrossRef]
70. Roess, R.P.; Prassas, E.S.; McShane, W.R. *Traffic Engineering*, 4th ed.; Pearson Prentice Hall: Prentice-Hall, NJ, USA, 2011.
71. Saad, W.; Han, Z.; Hjørungnes, A.; Niyato, D.; Hossain, E. Coalition Formation Games for Distributed Cooperation Among Roadside Units in Vehicular Networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 48–60. [CrossRef]
72. US Federal Highway Administration. Traffic Incident Management Handbook. 2000. Available online: http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPT_MIS/13286.pdf (accessed on 11 October 2021).
73. Chung, J.M.; Kim, M.; Park, Y.S.; Choi, M.; Lee, S.; Oh, H.S. Time Coordinated V2I Communications and Handover for WAVE Networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 545–558. [CrossRef]
74. Daganzo, C.F. *Fundamentals of Transportation and Traffic Operations*; Elsevier: New York, NY, USA, 1997.
75. May, A.D. *Traffic Flow Fundamentals*; Prentice Hall: Hoboken, NJ, USA, 1990.
76. de Dios Ortúzar, J.; Willumsen, L.G. *Modelling Transport*; Wiley: Hoboken, NJ, USA, 2002.
77. Sreedevi, I.; Black, J. Loop Detectors. California Center for Innovative Transportation. 2001. Available online: http://www.calccit.org/itsdecision/serv_and_tech/Traffic_Surveillance/road-based/in-road/loop_report.html (accessed on 11 October 2021).
78. Fontaine, M. Traffic Monitoring. In *Vehicular Networks, from Theory to Practice*; Olariu, S., Weigle, M., Eds.; CRC Press: Boca Raton, FL, USA, 2009; pp. 1.1–1.28.

79. V-DOT Virginia Department of Transportation. Virginia Smart Road. Available online: http://www.virginiadot.org/projects/constsal-smartrd.asp (accessed on 11 October 2021).
80. 511 Traffic. Latest Traffic News. Available online: http://traffic.511.org/LatestNews (accessed on 11 October 2021).
81. NHTSA National Highway Traffic Safety Administration. An Analysis of Recent Improvements to Vehicle Safety. 2012. Available online: http://www-nrd.nhtsa.dot.gov/Pubs/811572.pdf (accessed on 11 October 2021).
82. Bayen, A.; Butler, J.; Patire, A. *Mobile Millenium Final Report*; Technical Report UCB-ITS-CWP-2011-6; California Center for Innovative Transportation: Berkeley, CA, USA, 2011.
83. Hofleitner, A.; Herring, R.; Abbeel, P.; Bayen, A. Learning the Dynamics of Arterial Traffic from Probe Data Using Dynamic Bayesian Network. *IEEE Trans. Intell. Transp. Syst.* **2012**, *13*, 1679–1693. [CrossRef]
84. Nakano, K.; Olariu, S.; Schwing, J.L. Broadcast-efficient protocols for mobile radio networks. *IEEE Trans. Parallel Distrib. Syst.* **1999**, *10*, 1276–1289. [CrossRef]
85. Daniel, A.; Popescu, D.C.; Olariu, S. A Study of Beaconing Mechanism for Vehicle-to-Infrastructure Communications. In Proceedings of the IEEE ICC 2012 Workshop on Intelligent Vehicular Networking: V2V/V2I Communications and Applications—WIVN 2012, Ottawa, ON, Canada, 10–15 June 2012; pp. 8736–8740.
86. Qutaiba, I. Design, Implementation and Optimisation of an Energy Harvesting System for Vehicular Ad-Hoc Networks' Road Side Units. *IET Intell. Transp. Syst.* **2014**, *8*, 298–307.
87. Del Corso, D.; Passerone, C.; Reyneri, L.; Sansoe, C.; Speretta, S.; Tranchero, M. Design of a University Nano-Satellite: The PiCPoT Case. *IEEE Trans. Aerosp. Distrib. Syst.* **2011**, *47*, 1985–2007. [CrossRef]
88. Crimmins, D.M.; Patty, C.T.; Beliard, M.A.; Baker, J.; Jalbert, J.C.; Komerska, R.J.; Chappell, S.G.; Blidberg, D.R. Long-Endurance Test Results of the Solar-Powered AUV System. In Proceedings of the OCEANS 2006, Boston, MA, USA, 18–21 September 2006.
89. Reddy, T.B.; Linden, D. *Linden's Handbook of Batteries*, 4th ed.; McGraw-Hill: New York, NY, USA, 2011.
90. Boxwell, M. *The Solar Electricity Handbook*; Code Green Publishing: Warwickshire, UK, 2010.
91. Kenney, J.B. Dedicated Short-range Communications (DSRC) Standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182. [CrossRef]
92. Tsai, H.M.; Tonguz, O.K.; Saraydar, C.; Talty, T.; Ames, M.; Macdonald, A. ZigBee-based intra-car wireless sensor networks: A case study. *IEEE Wirel. Commun.* **2007**, *14*, 67–77. [CrossRef]
93. Sha-Mohammad, S.A.; Abdel-Wahab, H.A.; Popescu, D.C. A study of IEEE 802.11 standard for use in vehicle to infrastructure communication. In Proceedings of the IEEE Globecom, Atlanta, GA, USA, 9–13 December 2013.
94. Tufail, A.; Fraser, M.; Hammad, A.; Hyung, K.K.; Yoo, S.W. An Empirical Study to Analyze the Feasibility of WIFI for VANET. In Proceedings of the 12th International Conference on Computer Supported Cooperative Work in Design—CSCWD'08, Xi'an, China, 16–18 April 2008; pp. 553–558.
95. Lee, J.S.; Su, Y.W.; Shen, C.C. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In Proceedings of the 33rd Annual IEEE Conference on Industrial Electronics Society—IECON'07, Taipei, Taiwan, 5–8 November 2007; pp. 46–51.
96. Wheeler, A. Commercial applications of wireless sensor networks using ZigBee. *IEEE Commun. Mag.* **2007**, *45*, 70–77. [CrossRef]
97. Weigle, M.C.; Olariu, S. Intelligent Highway Infrastructure for Planned Evacuations. In Proceedings of the 1st International Workshop on Research Challenges in Next Generation Networks for First Responders and Critical Infrastructures (NetCri), New Orleans, LA, USA, 11–13 April 2007; pp. 594–599.
98. Barria, J.A.; Thajchayapong, S. Detection and classification of traffic anomalies using microscopic traffic variables. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 695–704. [CrossRef]
99. El-Tawab, S.; Alhafdhi, A.; Treeumnuk, D.; Popescu, D.; Olariu, S. Physical layer aspects of information exchange in the NOTICE architecture. *IEEE Intell. Transp. Syst.* **2015**, *7*, 8–18. [CrossRef]
100. Feller, W. *An Introduction to Probability Theory and Its Applications*, 1st ed.; John Wiley and Sons: Hoboken, NJ, USA, 1960; Volume I.
101. Harden, B.; Moreno, S. *Thousands Fleeing Rita Jam Roads From Coast*; Washington Post: Washington, DC, USA, 2005.
102. Feldstein, D.; Stiles, M. *Too Many People and No Way Out*; Houston Chronicle: Houston, TX, USA, 2005.
103. US Department of Transportation. Catastrophic Hurricane Evacuation Plan Evaluation: A Report to Congress. 2006. Available online: http://www.fhwa.dot.gov/reports/hurricanevacuation/ (accessed on 11 October 2021).
104. US Department of Transporation. *Intelligent Transportation Systems for Planned Special Events: A Cross-Cutting Study*; Technical Report FHWA-JPO-08-056; Federal Highway Administration: Washington, DC, USA, 2008.
105. Ahmed, S.; Cook, A. Application of time-series analysis techniques to freeway incident detection. *Transp. Res. Rec.* **1982**, *841*, 19–21.
106. Levin, M.; Krause, G.M. Incident detection algorithms. *Transp. Res. Rec.* **1989**, *722*, 49–64.
107. Michalopoulos, P. Automatic incident detection through video image processing. *Traffic Eng. Control* **1993**, *34*, 66–75.
108. Persaud, B.; Hall, F.; Hall, L. Congestion identification aspects of the McMaster incident detection algorithm. *Transp. Res. Rec.* **1990**, *1287*, 167–175.
109. Stephanedes, Y.; Chassiakos, A. Freeway incident detection through filtering. *Transp. Res.* **1993**, *1C*, 219–233. [CrossRef]
110. Besag, J. On the Statistical Analysis of Dirty Pictures. *J. R. Stat. Society. Ser. B Methodol.* **1986**, *48*, 259–302. [CrossRef]
111. Florin, R.; Syedmeysam, A.; Ghazizadeh, A.; Olariu, S. Big Data in the Parking Lot. In *Big Data Management and Processing*; Li, K.C., Jiang, H., Zomaya, A.Y., Eds.; Taylor and Francis: Boca Raton, FL, USA, 2017; pp. 425–450.

112. Zomaya, A.; Clements, M.; Olariu, S. A framework for reinforcement-based scheduling in parallel processor systems. *IEEE Trans. Parallel Distrib. Syst.* **1998**, *9*, 249–260. [CrossRef]
113. Olariu, S.; Schwing, J.L.; Zhang, J. Fundamental algorithms on reconfigurable meshes. In Proceedings of the 29th Allerton Conference on Communications, Control and Computing, Monticello, IL, USA, 27–29 September 1991; pp. 811–820.
114. Olariu, S.; Schwing, J.L.; Jingyuan, Z. Fast computer vision algorithms for reconfigurable meshes. *Image Vis. Comput.* **1992**, *10*, 610–616. [CrossRef]
115. Olariu, S.; Schwing, J.L.; Zhang, J. Optimal parallel algorithms for problems modeled by a family of intervals. *IEEE Trans. Parallel Distrib. Syst.* **1992**, *3*, 364–374. [CrossRef]
116. Olariu, S.; Schwing, J.L. A novel deterministic sampling sheme with applications to broadcast-efficient sorting on the reconfigurable mesh. *J. Parallel Distrib. Comput.* **1996**, *32*, 215–222. [CrossRef]
117. Hennessy, J.L.; Patterson, D.A. *Computer Architecture a Quantitative Approach*, 6th ed.; Morgan Kaufman: Burlington, MA, USA, 2019.
118. Bhagavathi, D.; Looges, P.J.; Olariu, S.; Schwing, J.L. A fast selection algorithms on meshes with multiple broadcasting. *IEEE Trans. Parallel Distrib. Syst.* **1994**, *5*, 772–778. [CrossRef]
119. Lin, R.; Olariu, S.; Schwing, J.L.; Zhang, J. Sorting in O(1) time on a reconfigurable meshe of size $N \times N$. In Proceedings of the EWPC'92, Parallel Computing: From Theory to Sound Practice, Barcelona, Spain, 23–24 March 1992; pp. 16–27.
120. Lin, R.; Olariu, S. Reconfigurable buses with shift switching: Concepts and applications. *IEEE Trans. Parallel Distrib. Syst.* **1995**, *6*, 93–102. [CrossRef]
121. Nakano, K.; Olariu, S. A survey on leader election protocols for radio networks. In Proceedings of the International Symposium on Parallel Architectures, Algorithms and Networks, I-SPAN'02, Makati City, Philippines, 22–24 May 2002; pp. 71–76.