

# Intelligent Highway Infrastructure for Planned Evacuations

Michele C. Weigle and Stephan Olariu  
Department of Computer Science  
Old Dominion University  
Norfolk, VA 23529, USA  
{mweigle, olariu}@cs.odu.edu

## Abstract

*Disasters, natural and man-made alike, pose a serious threat to the nation by taking a heavy toll in human lives, destroying the public infrastructure and production capacity, interrupting supply lines, and stalling economic activity. One of the time-honored strategies for dealing with predictable natural disasters is a planned evacuation of the population from the afflicted area. Thus, evacuation strategies and supporting infrastructure are of the highest importance for mitigating the effects of such events. The main contribution of this work is to propose an intelligent highway infrastructure in support of planned evacuations. Specifically, we show that the recently-proposed Architecture for the Notification of Traffic Incidents and Congestion (NOTICE) can be enhanced to support the needs of large-scale evacuations.*

## 1 Introduction

In cases of predicted disasters, such as hurricanes, *massive planned evacuations* are often necessary in order to minimize the impact of the predicted disaster on human lives. There are several issues involved in a large-scale evacuation. For example, once an evacuation is underway, finding available gasoline, drinking water, shelter and medical facilities quickly becomes an issue [5, 8]. In its recent report on hurricane evacuations [19], the US Department of Transportation (US-DOT) found that emergency evacuation plans often do not consider availability of resources such as gas, hotel rooms, food, etc. The recent hurricane evacuations in New Orleans and Houston have confirmed that there is no room for mistakes or misjudgments here. Otherwise, the evacuation routes are likely to be strewn with stranded or abandoned vehicles as happened recently in the Houston evacuation for Hurricane Rita [5, 8, 19].

During a massive evacuation, many major roadways are converted to contraflow, using all available lanes in both di-

rections for evacuation [18, 21]. Residents who are hesitant to leave at the appropriate time may find themselves stuck in traffic during the storm, which could be more dangerous than if they had remained at home. In order to make good decisions about when to evacuate, residents should have an estimate of the distance they would be able to safely travel before the storm hits. In high population areas that are limited in the number of roads leaving the coast, such as the Hampton Roads area in Southeastern Virginia, reliable and timely information about traffic conditions along evacuation routes is essential.

To facilitate this exchange of information, the US-DOT has suggested that emergency managers need a method for communicating with evacuees during the evacuation in order to provide updated information [19]. In addition, *traffic monitoring* equipment needs to be deployed to provide real-time traffic information along evacuation routes.

The most widely-used practice in traffic monitoring is to embed Inductive Loop Detectors (ILDs) in well-traveled highways every mile (or half-mile) [7, 17]. ILDs measure traffic flow by registering a signal each time a vehicle passes over. Each individual ILD (including the hardware and controllers) costs around \$8,200. In addition, the ILDs are connected by optical fiber that costs \$300,000 per mile [17]. Worse yet, statistics show that in some locations about 50% of the installed ILDs are inoperable [20]. Not surprisingly, transportation agencies are looking for less expensive and more reliable methods for traffic monitoring.

The rapid advances in wireless networking technology that we have witnessed in the last decade are enabling the development of innovative solutions. Indeed, systems using Vehicular Ad-hoc Networks (VANETs), employing a combination of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) wireless communication, have been proposed to give drivers advance notification of traffic incidents. V2V systems use the government-mandated Dedicated Short Range Communications (DSRC) operating in the 5.9GHz band. In DSRC the communication range is limited to 300-400 meters. This implies that pure V2V

communications will break down under sparse traffic conditions. In V2V systems, each vehicle is responsible for inferring the presence of an incident based on reports from other vehicles. This invites a host of security attacks [1, 13, 15] that could cause vehicles to make incorrect inferences, possibly resulting in increased traffic congestion and a higher chance of severe accidents. Not surprisingly, the problem of providing security in VANETs is starting to attract attention in the literature [1, 9, 10, 13, 15, 22]. In order to address the short-range communication and security problems that afflict pure V2V communications, it has been suggested that VANETs rely on a pervasive roadside infrastructure to act as encryption key distribution points or authentication authorities. Unfortunately, this roadside is extremely costly to deploy and even if deployed, it is very likely to be the target of vandalism that will hamper its intended functionality. Worse yet, the roadside infrastructure may be hacked and injected with malicious code, rendering it not only useless but outright dangerous. Because of their reliance on unreliable V2V and on vulnerable V2I communications, most VANET systems proposed thus far have serious security and privacy problems. Indeed, the way in which current systems are set up, the driver of a vehicle that participates in the traffic will not be able to preserve their privacy and may be subject to impersonation or Sybil attacks [3]. The problem stems from the fact that V2V communications can be traced back to individual vehicles. It was recently argued [14, 16] that even if several pseudonyms are used, detecting the true identity of the driver and, therefore, invading their privacy appears to be hard to avoid.

Our work is concerned with proposing a secure, privacy-aware architecture for traffic monitoring and advisory propagation in support of evacuations. We have recently proposed to enhance our roadways with an *Architecture for the Notification of Traffic Incidents and Congestion* (NOTICE) [12], intended to make travel safer. Although NOTICE was intended to handle day-to-day traffic, in this paper we show that with a minor modification, NOTICE can support the communications needs of large-scale evacuations. With the proposed enhancement, NOTICE will provide estimates of travel time, location of available resources, and information about roadways employing contraflow. While this is work in progress, we are in the process of building a NOTICE simulator and prototype, including its enhanced version in support of planned evacuations and disaster management.

The remainder of this paper is organized as follows: Section 2 reviews the main issues involved in a planned evacuation; Section 3 offers a survey of the main features of NOTICE; Section 4 suggests ways in which NOTICE can be enhanced to help with planned evacuations; Section 5 surveys related work, and Section 6 offers concluding remarks.

## 2 Evacuation Issues

Any system designed to assist travelers during an evacuation should be able to provide estimates of travel times, identify locations of needed resources, alert drivers to contraflow, and help authorities with roadway management.

### 2.1 Travel Time

An important aspect of evacuation is determining travel time in advance. In the event of a hurricane that could affect a large geographic area, residents do not want to be traveling during dangerous weather. Most residents would be safer staying in their homes than being stuck for hours in traffic during the storm. To make the decision of whether to leave or stay involves estimating how much time remains before the storm hits and how long it would take to reach somewhere safe. Traffic congestion plays a very large part in this decision. Typically residents have no information about the state of congestion on the roadways except through the news media, which may focus exclusively on problem areas.

### 2.2 Available Resources

Many residents often need to evacuate to areas several hours away from their homes. Traffic congestion can cause this trip to last considerably longer than anticipated, thus increasing the amount of gasoline needed for the trip. With increased demand (from all of the vehicles that are evacuating), some stations may run out of gasoline. In order to avoid stranded vehicles, drivers should be notified of stations that have gasoline remaining.

Another set of valuable resources includes available hotel rooms, open shelters, and hospitals. Notifying drivers of available shelters could help them in the event that they are not able to reach their final destination before the storm hits. Being in a shelter would be much safer than being stranded on the highway. Up-to-the-minute information about the availability of these resources at interchanges or highway exits must be available to the evacuees if they are to make informed decisions about when to refuel, seek shelter or get medical attention.

### 2.3 Contraflow

One effective method used for facilitating major evacuations is *contraflow*, where all lanes of traffic are moving in the same direction. In 2005, the evacuation of Houston for Hurricane Rita was problematic because the emergency officials delayed the decision to use contraflow. Houston officials cited the complexity of the interstate system and the numerous entrance and exit points as reasons why contraflow was avoided [5]. Contraflow can be a very effective

method of moving large numbers of vehicles out of an evacuation zone. However, it is a complex decision for emergency managers, because it requires a large commitment from state and local agencies to control and direct traffic.

### 3 Our Intelligent Highway Infrastructure

Motivated by the need to provide a secure and reliable system for *traffic safety-related information dissemination*, NOTICE shifts the main locus of communication from Vehicle-to-Vehicle (V2V) to a special form of Vehicle-to-Infrastructure (V2I). The infrastructure in NOTICE is obtained by embedding *sensor belts* in the road at regular intervals (*e.g.*, every mile or so), as illustrated in Figure 1. Each belt consists of a collection of piezoelectric pressure sensors, a simple aggregation and fusion engine, and a few small transceivers. The pressure sensors in each belt allow every message to be associated with a physical vehicle passing over the belt, eliminating the need for vehicles to be uniquely identified while avoiding the security problems outlined in the VANET literature [1, 9, 10, 13, 15, 22]. There are two immediate benefits of using belts over roadside infrastructure. First, the belts are far less prone to tampering and, second, they are better placed to detect passing cars and to interact with them in a simple and secure fashion.

#### 3.1 Underlying Philosophy

The underlying philosophy of NOTICE is that the decision about traffic-related *information dissemination* rests with individual belts and not with individual vehicles, as is currently the case. By using their pressure sensors (or suitable radio communications) the belts can detect passing vehicles and initiate interaction with them. In this arrangement, each passing vehicle will exchange data with the belt. It will drop off traffic-related messages originating with the vehicle or uploaded by the previous belt, and it will pick up encrypted messages to be propagated to the next belt. Each adjacent pair of belts shares a common encryption key, which allows them to communicate securely. In addition, because the messages carried by vehicles from one belt to another are encrypted, they cannot be tampered with by the vehicles. Thus, passing vehicles act as *data mules* between the belts, contributing to the overall traffic-related knowledge in the system. If the information received by the belt from a passing vehicle is corroborated by a sufficient number of other vehicles, the belt decides to disseminate the information by alerting passing cars to a traffic-related condition. NOTICE can provide efficient and timely propagation of traffic-related information to interested vehicles while, at the same time, protecting driver privacy.

#### 3.2 A Brief Overview

As is customary in the VANET literature [4, 9, 15], we assume that cars are fitted with a tamper-resistant *black box* which is the locus of vehicle-based communications. In NOTICE, the box receives sensory data from vehicle sub-assemblies as well as queries from the belts.

A few milliseconds after the pressure sensors have detected the front wheels of a passing car, the radio transceivers in the belt send a "Hello" beacon on the control channel containing the ID of the belt, a specific frequency channel  $\lambda$  on which data is to be exchanged, and a one-time session key  $\alpha$  valid for the duration of the communication session between the belt and the passing car. If the car confirms the handshake, the belt will send on channel  $\lambda$  a query encrypted with the session key  $\alpha$ . This query will prompt the car to drop off the message uploaded at the previous belt and report relevant traffic-related data collected by the car. The belt may upload traffic-related information for the car and an encrypted message destined for the next belt.

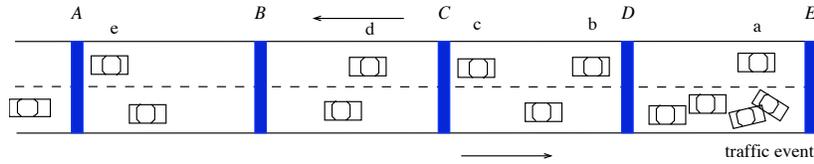
It is worth noting that the data exchange just mentioned is perfectly anonymous and does not interfere with vehicle or driver privacy. Indeed, the pressure sensors in the belts allow NOTICE to associate every message with a physical vehicle passing over the belt. We note that a given vehicle cannot interact with a belt more than once in a reasonable time interval and, consequently, impersonation and Sybil attacks are very hard to perpetrate. In addition, because messages carried by vehicles from one belt to another are encrypted, these messages cannot be tampered with.

Each lane on the roadway has its own dedicated belt. For example, belt  $C$  in Figure 1 consists of two *logical sub-belts*, each serving one lane. In the case of a divided highway, belts on opposite sides of the median are connected by direct wired connection under the median. It is assumed that the sub-belts can communicate directly in a secure way.

##### 3.2.1 Detection of Traffic-related Events

NOTICE can detect cars traveling in the wrong direction or lane, the average traffic speed at various moments, the traffic intensity and other data that may be of interest to highway administrations. Using a Bayesian discriminator NOTICE can reliably filter out spurious data. NOTICE works well in both sparse and dense traffic even though the security needs of traffic in these scenarios are vastly different.

The belts can use their collective knowledge to detect slowdowns. A belt can monitor the speed and number of vehicles passing through at any time and communicate that information to later belts. Thus, a later belt detecting a much lower count or speed of vehicles than the previous belt could infer that congestion is occurring. In addition, the belts could also use the *rubberneck* effect that often



**Figure 1.** Illustrating information propagation in NOTICE.

afflicts drivers in lanes opposite an accident. This occurs when drivers who are not hindered slow down to look at the accident. Since belts in opposite lanes are connected, one belt seeing very little traffic and the opposite belt seeing a traffic slowdown could infer that there has been an incident. In these cases, the incident would be assigned an uncertainty probability until it had been verified by an outside source (say, a first responder using a special encryption key, as will be described later).

### 3.2.2 Information Dissemination

NOTICE propagates traffic-event information to vehicles before they arrive at the place of the incident. In NOTICE, vehicles act as messengers, passing encrypted information between belts. Referring to Figure 1, as car  $c$  passes belt  $C$  it picks up information intended for its own use, along with information to be propagated to belt  $B$ . Each pair of adjacent belts shares a common key that allows them to communicate securely.

Using Figure 1, we now give an example to illustrate both detection of traffic incidents and the related backwards information propagation in NOTICE. Belt  $E$  notices a sudden traffic decrease and infers that an event has taken place. It then uploads onto car  $a$  a message for belt  $D$  informing it of local traffic density. Since belt  $D$  does not see stopped traffic it infers that there must have been a traffic event between it and belt  $E$  or beyond  $E$ . This information is then uploaded onto car  $b$  with the “urgent” bit set. At this time, car  $b$  is allowed to broadcast this information, using an encryption key specific to belts  $C$  and  $D$ . The only car that can pick up this message is car  $c$  who is also between belts  $C$  and  $D$ . Upon reaching belt  $C$ , car  $c$  will drop off the information. Belt  $C$  will immediately propagate the information about the potential accident to the cars passing it in the direction towards  $D$ . In this way, the information about the accident is propagated backwards to cars that have not yet reached the traffic event. At the same time, belt  $C$  will task car  $c$  to further propagate the information. At this point, using an encryption key corresponding to belts  $C$  and  $B$ , the information is propagated to car  $d$  which, in turn will drop it off with belt  $B$ . This is then continued in such a way that the cars approaching the accident area get fair notice of the event and have a chance to make alternate travel plans.

### 3.2.3 Role-based Vehicle to Belt Communication

There are exceptional cases where the communication between belts and passing vehicles needs to be augmented to allow authorized vehicles to interact with the belts in a predetermined, *role-based*, fashion. This feature is essential to the interaction of NOTICE with first responders, ambulances, fire fighters, local police, and traffic management personnel in case of emergency operations. In such scenarios, authorized vehicles using a special encryption key will be allowed to load, in a role-based fashion, essential information onto individual belts. For example, police cars may load messages that ambulances are not allowed to load. This information could be related to planned lane closures, major traffic incidents, suggested detour routes, as well as the availability of resources.

## 4 Using NOTICE during Evacuations

We now take a critical look at NOTICE in order to set the stage for our enhancements of the system. We begin by enumerating the traffic-related monitoring for which NOTICE has built-in capabilities.

### 4.1 Capabilities of NOTICE

In addition to providing drivers with safety-related advisories, NOTICE can also perform tasks related to traffic monitoring. For example, NOTICE can detect and aggregate various types of traffic-related data on a per-lane or global basis. This information includes traffic intensity, vehicles moving in the “wrong direction”, average speed of traffic, and the percentage of multi-axle vehicles in the traffic flow. The black boxes in each vehicle also report specific information about occurrences between two consecutive belts. This information, such as average speed, minimum speed, and abrupt changes of direction (swerving, for example), can be used to help NOTICE infer traffic congestion or obstacles in between two belts.

### 4.2 Limitations of NOTICE

There are, however, tasks that are crucial in the context of a planned evaluation and that NOTICE was not *à priori* designed to perform. These tasks include propagating

information backwards in the context of contraflow traffic (where there is no oncoming traffic) and tabulating the availability of resources, such as hotel rooms and hospital facilities. In order to use NOTICE in support of planned evacuations, we need to provide additional hardware. The added hardware, discussed in the next subsection, should be *temporary* in nature and easy to deploy.

### 4.3 Enhancing NOTICE in Support of Evacuations

Before an evacuation, emergency officials can place temporary hardware in the form of support vehicles, sturdy tamper-proof devices, or mini-towers along the median every 10 miles or so, as illustrated in Figure 2. It is important to note that these devices are temporary and would only be deployed in an emergency. The temporary devices would be directly connected to the nearest belt and connect NOTICE to the emergency management center overseeing the evacuation. This would provide the belts with important information that cannot be determined solely by NOTICE. In addition, these devices can use powerful radios to send backward messages in the case of contraflow traffic. For security, these temporary devices would share time-varying symmetric encryption keys. In addition, the device that plugs into a particular belt will share an encryption key with that particular belt. Even though the communication between the device and belt will not be wireless, this encryption key would prevent a malicious attacker from impersonating a piece of this temporary emergency infrastructure.

#### 4.3.1 Estimating Travel Time in Advance

Using the temporary hardware introduced above, NOTICE can query vehicles for travel times and upload that information to the emergency management center through the temporary hardware. This 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 belt system to give drivers the same information as they pass over the belts.

#### 4.3.2 Detecting Available Resources

To determine stations with available gasoline, the black box in a vehicle can monitor its gas tank and determine when gas was added. In addition, the vehicle will know how far and for how long it has been driven since the gas tank was last filled. The belt closest to each highway on-ramp can query traffic to see when and where vehicles last added gasoline. NOTICE could then use this information to inform travelers of nearby available gas stations.

As an example, suppose that car *b* in Figure 2 has recently filled its gas tank and is re-entering the highway. As it crosses belt *A*, car *b* notifies the belt about the addition of gasoline to the tank, including the location of the gas station. Belt *A* then transmits this information to tower *X*, which can then propagate that information to the other towers and belts. If car *c* is low on gas, it can obtain information about the available gas station at least by the time it passes belt *B* and then can exit to refuel.

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 NOTICE and the temporary emergency infrastructure. 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.

#### 4.3.3 Alerting Drivers to Contraflow

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

## 5 Related Work

Recently, there has been much attention paid to how to achieve efficient evacuations. Researchers at Oak Ridge National Labs [6] have developed a traffic model for simulating emergency evacuations. They also proposed using fixed digital cameras at various points along an evacuation route to monitor traffic in real-time. Chiu [2] has also developed a modeling system for emergency evacuations, including estimation of travel time and evacuation routes. A report from the Minnesota Department of Transportation [11] discusses issues involved in travel time estimation and the result that the accuracy of the estimation depends on the length of road travel that is being estimated.

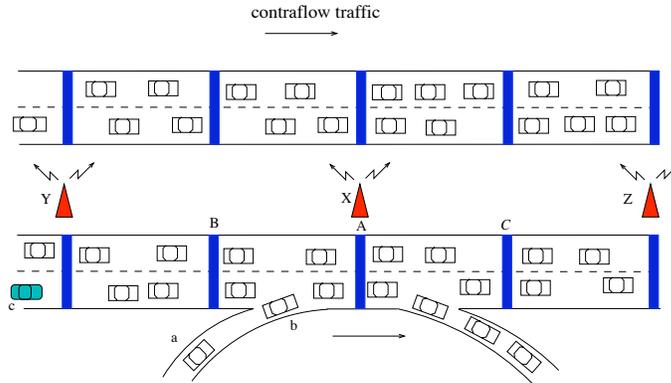


Figure 2. Illustrating the extension of NOTICE in support of evacuations.

## 6 Concluding Remarks

We have described enhancements to our recently-proposed system NOTICE, an Architecture for the Notification of Traffic Incidents and Congestion. These enhancements would provide essential information for residents and evacuees, as well as emergency management personnel, about the state of highways during a planned evacuation. This is currently work in progress, and we are in the process of developing simulations and a prototype to evaluate NOTICE, including the evacuation enhancements.

## References

- [1] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmülle. Attacks on inter-vehicle communication systems - an analysis. In *Proceedings of the International Workshop on Intelligent Transportation (WIT)*, Mar. 2006.
- [2] Y.-C. Chiu. Traffic scheduling simulation and assignment for area-wide evacuation. In *Proceedings of the IEEE Intelligent Transportation Systems Conference*, pages 537–542, Washington, D.C., Oct. 2004.
- [3] J. Douceur. The sybil attack. *Lecture Notes in Computer Science: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, 2429:251–260, 2002.
- [4] S. Eichler, B. Ostermaier, C. Schroth, and T. Kosch. Simulation of car-to-car messaging: Analyzing the impact on road traffic. In *Proceedings of the Conference on Measurement and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2005.
- [5] D. Feldstein and M. Stiles. Too many people and no way out. *Houston Chronicle*, Sept. 25 2005.
- [6] O. Franzese and J. Sorensen. Fast deployable system for consequence management: The emergency evacuation component. Oak Ridge National Labs, 2001.
- [7] J. Gajda, R. Sroka, M. Stencel, A. Wajda, and T. Zeglen. A vehicle classification based on inductive loop detectors. In *Proc. IEEE Instrumentation and Measurement Conference*, Budapest, Hungary, May 2001.
- [8] B. Harden and S. Moreno. Thousands fleeing Rita jam roads from coast. *Washington Post*, Sept. 23 2005.
- [9] J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy Magazine*, 2(3):49–55, 2004.
- [10] J. Luo and J.-P. Hubaux. A survey of inter-vehicle communication. Technical Report IC/2004/24, School of Computer and Communication Sciences, EPFL, 2004.
- [11] Minnesota Department of Transportation. Development of operational strategies for travel time estimation and emergency evacuation on a freeway network. 2004-49 Final Report, 2004.
- [12] S. Olariu, M. C. Weigle, and G. Yan. NOTICE: An architecture for the notification of traffic incidents and congestion. In submission, Feb. 2007.
- [13] B. Parno and A. Perrig. Challenges in securing vehicular networks. In *Proceedings of HotNets*, 2005.
- [14] M. Raya and J.-P. Hubaux. Security aspects of inter-vehicle communications. In *Proceedings of the Swiss Transport Research Conference (STRC)*, 2005.
- [15] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, Nov. 2005.
- [16] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. *IEEE Wireless Communications Magazine*, 2006.
- [17] I. Sreedevi and J. Black. Loop detectors. California Center for Innovative Transportation, Feb. 2001.
- [18] State of Louisiana Office of Homeland Security and Emergency Preparedness. Louisiana citizen awareness and disaster evacuation guides, 2006.
- [19] US Department of Transportation. Catastrophic hurricane evacuation plan evaluation: A report to congress, June 2006.
- [20] P. Varaiya, X.-Y. Lu, and R. Horowitz. Deliver a set of tools for resolving bad inductive loops and correcting bad data. Proposal, [http://path.berkeley.edu/~xyylu/TO6327/TO6327\\_SEMP.pdf](http://path.berkeley.edu/~xyylu/TO6327/TO6327_SEMP.pdf), Oct. 2006.
- [21] Virginia Department of Transportation. Virginia’s hurricane evacuation routes, Oct. 29 2006.
- [22] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security issues in a future vehicular network. In *Proceedings of European Wireless*, Feb. 2002.