NOTICE: An Architecture for Notification of Traffic Incidents

Mahmoud Abuelela Stephan Olariu Michele C. Weigle
Department of Computer Science, Old Dominion University, Norfolk, VA 23529–0162
{eabu,olariu,mweigle}@cs.odu.edu

***Abstract*—We introduce NOTICE, a secure, privacy-aware architecture for the notification of traffic incidents. Using sensor belts embedded in the roadway, traffic-related messages and advisories are carried between belts by passing cars. NOTICE moves the responsibility for making decisions about traffic-related information dissemination to the infrastructure rather than leaving those decisions with the vehicles, which may have incomplete or incorrect knowledge. Extensive simulation showed that NOTICE can provide "up-to-the-minute" notification of road incidents.**

Keywords: traffic-related incidents, incident notification, privacy

I. Introduction

The US Department of Transportation (US-DOT) estimates that over half of all congestion events are caused by highway incidents rather than by rush-hour traffic in big cities [1]. The US-DOT also notes that in a single year, congested highways due to traffic incidents cost over $75 billion in lost worker productivity and over 8.4 billion gallons of fuel. Further, the NHTSA indicates that congested roads are one of the leading causes of traffic accidents, and in 2005 an average of 119 persons died each day in motor vehicle accidents [2].

Given sufficient advance notification of traffic incidents, drivers could make educated decisions about taking alternate routes. This would improve overall traffic safety by reducing the severity of congestion while saving both time and fuel in the process. On most US highways, congestion is a daily event and advance notification of imminent congestion is unavailable [2].

A. State of the art

The most widely-used devices for traffic monitoring and incident detection are Inductive Loop Detectors (ILDs) embedded in well-traveled highways every mile (or half-mile). ILDs measure traffic flow by registering a signal each time a vehicle passes over them. Each 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. Worse yet, official statistics show that about 50% of the installed ILDs are defective. Not surprisingly, transportation departments are looking for less expensive and more reliable methods for traffic monitoring and incident detection.

Recently, Vehicular Ad-hoc Networks (VANET) employing a combination of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) wireless communication have been proposed to alert drivers to traffic events including accidents, lane closures, slowdowns, and other traffic-safety issues. In most of these systems, individual vehicles are responsible for inferring the presence of an incident based on reports from other vehicles. This invites a host of serious and well-documented security attacks [3], [4] intended to 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 well-deserved attention [3]–[5].

In the light of the fact that most of the insecurities in VANET can be traced back to unbridled V2V communications, much of the recent work assumes that VANETs will rely on a pervasive and costly roadside infrastructure that acts as encryption key distribution points or authentication authorities [3], [4]. Unfortunately, in addition to being prohibitively expensive to build and to maintain, this roadside infrastructure 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. It was recently argued [6] that even if pseudonyms are used, detecting the true identity of the driver and, therefore, invading their privacy appears to be difficult to prevent.

B. Our contributions

The main contribution of this work is to propose NOTICE, a secure and privacy-aware architecture for the *Notification Of Traffic InCidEnts* that provides drivers with up-to-the-minute notification about highway conditions. The *underlying philosophy* of NOTICE is that the decision about traffic-related information dissemination should rest with the infrastructure and not with individual vehicles.

Instead of relying on vulnerable roadside infrastructure, we propose to embed *sensor belts* in the road at regular intervals (*e.g.*, every km or so), as illustrated in Figure 1.

Each belt consists of a collection of pressure sensors, a simple aggregation and fusion engine, and a few small transceivers. For robustness and fault tolerance, roadside solar panels of the type currently used on US highways can supplement the energy needs of the belts. We expect this

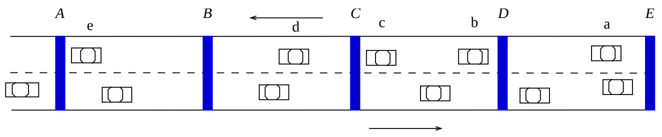

Fig. 1. A collection of belts on a two-lane road. Belts are labeled with capital letters, and cars are labeled with lowercase letters. The figure is not drawn to scale as belts are placed at least 1 km apart.

configuration to be less expensive than a single ILD, even without the expensive optical fiber needed to interconnect the ILDs. The pressure sensors in each belt allow every message to be associated with a physical vehicle passing over the belt. Thus, no one vehicle can pretend to be multiple vehicles and there is no need for an ID to be assigned to vehicles. There are three immediate benefits of using belts over roadside infrastructure. First, the belts are far less prone to tampering; second, they are better placed to detect passing vehicles and interact with them in a simple, secure and privacy-preserving fashion; and, third, a recent prototype [7] has confirmed that suitably encased belts are more robust, more reliable and longer-lived than ILDs.

The remainder of this paper is organized as follows: In Section II we discuss the details of NOTICE; Section III presents our simulation model and simulation results. Finally, Section IV offers concluding remarks.

II. NOTICE - THE DETAILS

As has been suggested elsewhere [5], [6], [8], we assume that vehicles will be fitted with a tamper-resistant *Event Data Recorder* (EDR), much like the well-known black-boxes onboard commercial aircraft. The EDR provides tamper-resistant storage of statistical and private data. The EDR is also responsible for recording essential mobility attributes. For this purpose, all of the vehicle's sub-assemblies, including the GPS unit, speedometer, gas tank reading, tire pressure sensors, and sensors for outside temperature, feed their own readings into the EDR. These sub-assemblies can report such attributes as the current geographic position, current speed, momentary acceleration or deceleration, lane changes, and swerving. As a consequence, given a time interval I of interest, the EDR can store information such as the highest and lowest speed during I, the position and time of the strongest deceleration during I, as well as location p, time t and target lane in a lane change.

The EDR is also fitted with a cell-phone programmed to call predefined numbers (including E-911) in the case of an emergency. For example, a driver may be incapacitated as a result of the accident and may be physically unable to place the call. This feature exists already on some vehicles and is useful for reporting, upon the deployment of an airbag, that the vehicle was probably involved in a collision. This allows the authorities to be alerted in real-time to major traffic events and, ultimately, saves lives.

Importantly, the driver can provide input to the EDR, using a simple menu, either through a dashboard console or through verbal input. This is useful feature that allows individual cars to alert NOTICE of traffic incidents that are otherwise hard to detect, such as roadway icing and the presence of stray animals on the roadway. Unfortunately, using this mechanism the driver can, in fact, inject incorrect or malicious information. However, in NOTICE the driver cannot alert directly other cars, since event reporting is restricted to car to belt communications, as opposed to unbridled car to car communications as in standard VANET. To prevent malicious or careless users from inserting invalid information into the system, a belt will not assume that one driver-input notification is accurate, but will wait for confirmation from k other cars. Once a sufficient number of cars have reported the incident, the belt decides that the event is probably real and proceeds to disseminate the information.

NOTICE uses the government-mandated Dedicated Short Range Communications (DSRC) operating in the 5.9 GHz band. The EDR has a secure connection to two radio transceivers, one placed just behind the front axle and a second transceiver placed in a tamper-proof box at the rear of the vehicle. The front transceiver is essential to ensuring correct handshaking with a belt on the roadway; the second transceiver is responsible for data transfer between the vehicle and the belt that will be discussed in Subsection II-B.

A. Belt to belt communications

Each belt is fitted with a few transceivers, at least one per lane of traffic, with a maximum communication range of 5 m. Consequently, the belts do not communicate with each other directly. Instead, adjacent belts rely on passing vehicles to communicate. Referring back to Figure 1, featuring a two-lane roadway, each lane on the roadway has its own dedicated belt. For example, belt C 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, therefore, that the sub-belts can communicate directly in a secure way.

Referring again to Figure 1 consider the lane wherein the traffic is moving right-to-left. If belt C wants to communicate a message m to the next belt, B, it will encrypt m with a time-varying shared key $\mu(C, B, t)$ known only to belts C and B, with t representing the time parameter. We assume that the belts are roughly synchronized in time and that they switch from one key to the next in a pre-established key-chain based on their local time. Tight time synchronization between belts is not essential, given the inherent delays in communications. It is important to note that, given a sufficiently large set of keys in the key-chain, the use of the belt to belt encryption keys appear random to an external observer.

To pass the encrypted message m to belt B, belt C will upload m onto passing car d (as will be described below). When car d reaches belt B, the message m will be dropped off and decoded by belt B. In turn, belt B may decide to send a message to belt A. This would be done using the symmetric key $\mu(B, A, t)$, known only to belts B and A.

B. Belt to car communications

We now give a succinct description of the communication between a belt and a passing car. Referring, again, to Figure 1, consider car c traveling at 100 km/h (approximately, 65 mph – the legal interstate speed in most US states). Once the pressure sensors in belt C have detected the front wheels of car c, a radio transceiver in the belt will send, at a very low power (range of about 1 m), a "Hello" beacon on a standard control channel containing the ID, C, of the belt, as well as handshaking information. This information includes a frequency channel λ on which data is to be exchanged. Once car c receives this information, it will have roughly 36 ms (time to travel 1 m and thus out of communication range) to respond. As the handshaking response will be very short and will not be encrypted, a NOTICE-equipped car will have no problem responding in time. If belt C does not receive a reply to the handshake, it will not communicate further with car c.

If car c confirms the handshake before it leaves radio range, belt C will send on channel λ a query that will received by the vehicle's transceiver. 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's EDR, including driver input, if provided. Car c will then drop off the encrypted message from belt D and the relevant data collected by its EDR in the time interval $I(D, C)$, which is the time spent traveling between belts D and C.

If there is traffic-related information that concerns car c, belt C will upload this information to the car. Belt C may also upload a message m destined for the next belt, B. Message m is encrypted with the symmetric key $\mu(C, B, t)$, a time-varying shared key between belts B and C that we introduced in Subsection II-A. The message is stored in the EDR and will be dropped off with belt B at the appropriate time. The car does not know the key $\mu(C, B, t)$ and, consequently, cannot decrypt the message destined for belt B.

For the data exchange between the belt and the car, the belt uses a transceiver with slightly higher range than that of the handshaking transceiver, about 3 m. Since the transceiver on the car that will perform data exchange is placed at the rear of the car, there will be a total range of 6 m (as the car passes over the belt) for data exchange. This gives the belt and the car about 216 ms to complete the communication.

Here we show that 216 ms is a feasible communication time period for the data exchange between the belt and the car. Let s be the transmission time for a single message, d be the encryption/decryption time for a single message, and p be the processing time for the belt to incorporate new information. There are a total of 5 messages sent after handshaking (belt sends initial query, car sends message from previous belt, car sends EDR data, belt sends new information for car, and belt sends message for next belt) and 2 encryption/decryption events (belt decrypts message from previous belt and encrypts message for next belt). This results in a total communication time $T = (5s + 2d + p)$ ms. If we set $p = 50$ ms, $d = 20$ ms, and $s = 1$ ms (corresponding to a 750-byte message at 6 Mbps, the lower end of DSRC [9], then $T = 95$ ms. These are conservative estimates, as we anticipate messages to be much smaller than 750 bytes, at least for the first query sent by the belt. Even with these conservative estimates, for 95 ms to be too little time for communication, the car would have to be traveling at 227 km/h (141 mph), an illegal, not to mention an unsafe, speed on US highways.

The very short-range radio transmission used in the car to belt communication is deliberate. It renders the communication strictly *local* and, therefore, reduces the chances of eavesdropping by malicious entities positioned by the roadside. It is worth noting that the belt to car and car to belt data exchanges discussed above are perfectly *anonymous* and do 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 car cannot interact with a belt more than once in a reasonable time interval and, consequently, impersonation and Sybil attacks are difficult to perpetrate. In addition, because messages carried by vehicles between belts are encrypted, these messages are secure.

C. Car to car communications

As mentioned already, for reasons of security and privacy, NOTICE minimizes the amount of V2V communications. There are, however, instances where V2V communications are useful and, as such, are supported by NOTICE. Referring again to Figure 1, assume that belt D has an emergency message to convey to belt C. Using the belt to car communications discussed in Subsection II-B, belt D can upload the message onto car b in which case it will take slightly less than one minute (assuming a car speed of 100 kmh) for the message to make it to belt C. In fact, in the case of a traffic slowdown, where the traffic moves very slowly or is stopped, it may take considerably longer for the message to reach belt C. In emergency situations, this delay is intolerable. Under such conditions, belt D having encrypted the message with the key $\mu(D, C, t)$ will upload the message unto car b and will also set the "urgent" bit indicating that car b must try to contact cars traveling in the direction toward C forwarding the message by radio. In Figure 1, car b will send a message destined to all cars between belts D and C (car c in the Figure 1) asking them to drop off the urgent message with belt C. This feature is extremely useful for accident notification and for alerting drivers approaching an accident of the corresponding slowdown. More details will be given in Subsection II-F in the context of information dissemination in NOTICE.

D. Role-based car to belt communications

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

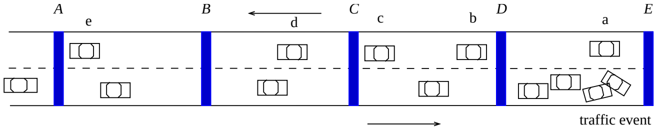

Fig. 2. Information propagation in NOTICE on a two-lane roadway.

vehicles using a special encryption key will be allowed to load essential information onto individual belts.

E. Incident detection

NOTICE relies on accumulated evidence in conjunction with driver input and intelligent data mining to detect traffic-related incidents. Due to stringent page limitations, we restrict our attention to incidents that force cars to change lanes; these include wrecks, objects strewn on the roadway (e.g a mattress) or slow-moving vehicles. Consider two adjacent belts A and B and assume that N cars that pass B report lane changes since passing A. How can belt B infer the presence of an incident? Imagine that the EDR in one car reports n lane changes $(p_1, t_1, 2), (p_2, t_2, 1), \ldots (p_n, t_n, 1)$ between A and B. Assume, further, that the EDR in another car reports m lane changes $(q_1, t'_1, 1), (q_2, t'_2, 1), \ldots (q_m, t'_m, 2)$. If there is to be a traffic incident, there must be a common reason for at least one lane change. Moreover, these lane changes must be *correlated* in time, geographic location, and destination lane. Given input from N cars, belt B can infer the presence of a traffic incident when k reports are correlated as above. Even if there is correlation, a careful further analysis is required. For example, were the lane changes caused by a slow moving vehicle? Again, the answer lies in the k reports corroborated, perhaps, by driver input.

F. Information dissemination

In order to be effective at reducing incident-related congestion, a notification system must be able to quickly disseminate that information to vehicles that have not yet reached the incident. We use Figure 2 to illustrate the backwards information propagation in the event of a traffic incident between belts D and E. (Note that this figure is not drawn to scale as we anticipate putting belts at least 1 km apart.) Assume that belt D is aware of the incident and the slowdown in traffic resulting from it. When car a passes over belt D, the belt will upload information about the incident destined for belt C. As discussed in Subsections II-B and II-C, there are two different modes of message dissemination, normal and urgent. In *normal* mode, car a (and cars that follow for a certain amount of time) will carry the message to belt C, belt B, and belt A, in succession. The message propagation time depends upon the speed of car a. In *urgent* mode, car a will transmit the message to any other cars that are located between belts C and D, such as cars b and c. These cars will then drop off the message at belt C before car a would have reached belt C. This speeds up the message propagation time considerably.

When the information about the traffic incident reaches belt C (and belt B and belt A), it will inform cars traveling towards the incident. these cars in turn may use their navigation system that may suggest alternate route. The severity of the traffic incident and the current traffic conditions will affect how far the message is propagated.

III. Simulation results and analysis

A traffic simulator has been developed in order to evaluate NOTICE. We have simulated an 8Km four-lane highway with two lanes in each direction. Cars were deployed uniformly at random, then each car has a speed between 65 mph and 75 mph. The inter-belt distance was set to 1km, although later it was varied to measure its impact on the time to detect an incident. Although many kinds of traffic incidents and many incident inferring methods exist, due to space limitation we are presenting only a few experiments to measure the performance of NOTICE. In our simulation,traffic incidents (accident) were generated uniformly at random in one of the lanes between any two belts. All vehicles approaching the accident in that lane must change lanes. We assume that a belt needs to collect $k = 10$ different EDR reports to confirm the occurrence of the accident.

A. Detecting an accident

Our main concern was to evaluate the time it takes a belt to deduce the occurrence of an accident. Naturally, this is impacted by a number of parameters as illustrated in Figure 3. First, the top graph in Figure 3 shows that, as expected, as traffic density increases, the time taken by a belt to detect the accident decreases because many cars will exist to confirm the occurrence of the accident. However, in very dense traffic the speed of vehicles will decrease and the ability to change lanes decreases as well. As a result, the time to infer and accident increases again. Of course, this time could be reduced if we used urgent bit approach. As an illustration, for density of 20 cars/km, it may take about 60 sec to discover the accident.

One of the fundamental design parameters in NOTICE is the inter-belt distance. A large inter-belt distance will reduce the cost to *deploy* NOTICE. However, the larger the inter-belt distance, the longer the time needed to detect an event. The second graph in Figure 3 shows the impact of the inter-belt distance on the time needed to infer an event under different traffic densities. Under sparse traffic, 10 cars/km, and for a large inter-belt distance of 2500m, we found that a belt can infer an event in about 137 sec. For a 1000 m inter-belt distance and reasonably dense traffic, 20 cars/km, it took only about 47 sec. Actually, this problem is an optimization problem that will be studied analytically in future work.

Another fundamental parameter is how *conservative* a belt should be, that is, how many reports should a belt collect,*within some time interval*, in order to be reasonably sure an incident had occurred? The bottom graph in Figure 3 shows the impact of k on the time to infer an event. As k increases, the time to infer an event increases. As a result of this experiment, we suggest that a belt should not be very conservative as it takes longer time to deduce an event. The price to pay for reacting as a result of too few reports is an increase in the number of false alarms.

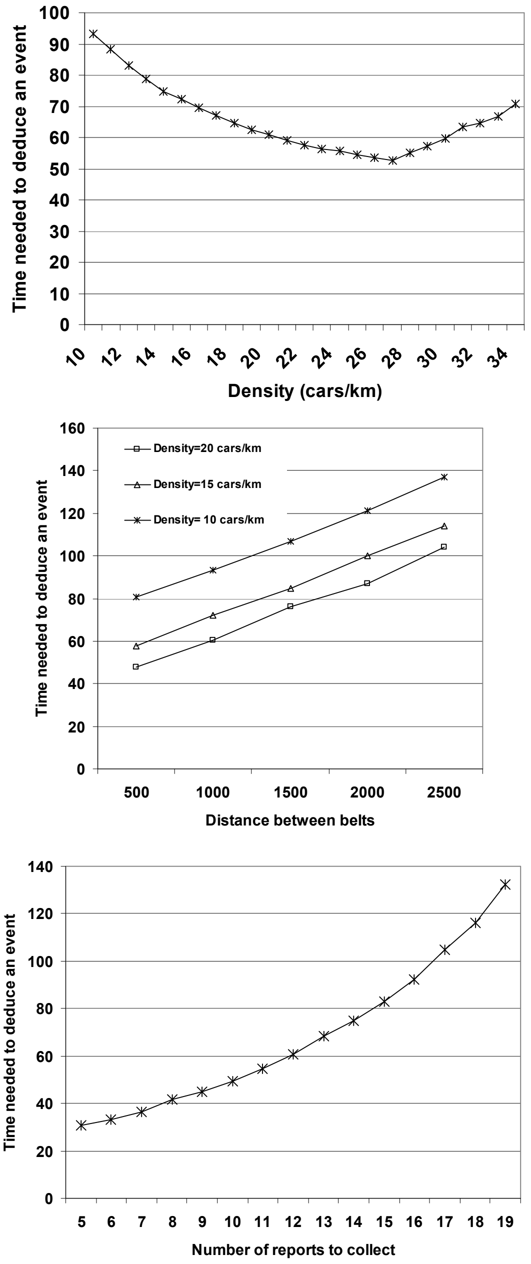

Fig. 3. *Impact of various parameters on the time to infer an accident.*

B. Propagating the information

After inferring an event, the belt must propagate information back to coming vehicles so that they may avoid congestion. Figure 4 shows the impact of traffic density on the time needed to propagate the information. Specifically, we measured the time elapsed between the occurrence of the accident until cars that are 2 km behind are informed about it. As expected, as the traffic density of the other direction increases, more cars will be available to propagate the information. However, for large traffic density, the speed of vehicles will be decreased and hence longer time will be needed to propagate an event. As an illustration, it may take about 2 minutes to propagate information 2 km. due to space limitations, more experiments will be available in subsequent papers.

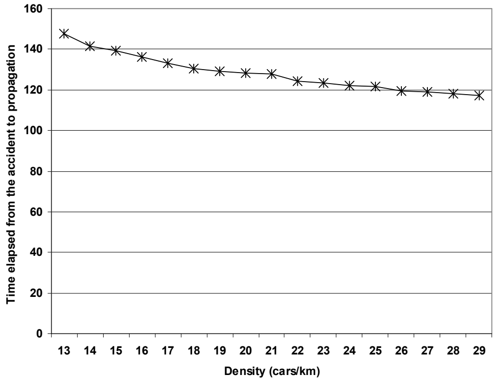

Fig. 4. Illustrating the impact of traffic density on time needed to propagate the information back

IV. Concluding remarks and future work

NOTICE is a secure, privacy-preserving architecture for the automatic inference of traffic incidents and the dissemination of related traffic advisories. NOTICE preserves driver privacy by being able to associate messages with physical vehicles. By using vehicles mainly as data mules to transport information between belts, NOTICE reduces the possibility of malicious attack by individual drivers inserting false messages into the system. In addition, since the NOTICE belts have sensors that detect vehicles passing over them, each belt can independently corroborate information provided by a vehicle with what has been observed by the belt itself. In spite of these encouraging results, more work is needed to enhance the inference engine of NOTICE. Ongoing work includes evaluating various intelligent data mining and inference techniques. Second, enhancing the security of NOTICE is another issue to avoid possible active or passive attacks. Third, and perhaps most important, we look into other causes of incidents including rubbernecking and other human-nature related causes.

References

[1] J. Paniati, Traffic congestion and sprawl, Federal Highway Administration, http://www.fhwa.dot.gov/congestion/congpress.htm, Nov. 2002.

[2] National Highway Traffic Safety Administration, “Traffic safety facts,” http://www-nrd.nhtsa.dot.gov, 2005.

[3] M. Raya and J.-P. Hubaux, The security of vehicular ad hoc networks, *Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005.

[4] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmülle, Attacks on inter-vehicle communication systems - an analysis, *Proc. WIT*, Mar. 2006.

[5] 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.

[6] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing vehicular communications, *IEEE Wireless Communications Magazine*, 2006.

[7] Z.-X. Li, X.-M. Yang, and Z. Li, Application of cement-based piezoelectric sensors for monitoring traffic flows, *Journal of Transportation Engineering*, 132(7), 565–573, 2006.

[8] K. Plößl, T. Nowey, and C. Mletzko, Towards a security architecture for vehicular ad hoc networks, *Proc. First International Conference on Availability, Reliability and Security*, (ARES), 2006.

[9] IEEE, “DSRC FAQ,” http://grouper.ieee.org/groups/scc32/dsrc/faq/.