# Security Issues in a Future Vehicular Network

Magda El Zarki, Sharad Mehrotra, Gene Tsudik and Nalini Venkatasubramanian

Department of Information and Computer Science, University of California, Irvine
Irvine, CA. 92697-3425 USA
e-mail: {magda,sharad,gts,nalini@ics.uci.edu}

**ABSTRACT**
*In this paper we present a novel infrastructure for vehicular communication on highways (DAHNI) and propose some potential applications aimed at assisting drivers. Certain unique features of the envisaged infrastructure and applications result in equally unique and interesting security challenges. We discuss these challenges and outline some possible solutions.*

## 1 INTRODUCTION

Both modern high-speed motorways and vehicles that drive upon them are becoming increasingly intelligent. In particular, communication devices are being installed in more and more cars and roadside infrastructure components. In the not-too-distant future, traveling vehicles will be able to communicate while forming ephemeral, rapidly changing ad hoc networks. At the same time, they will have direct access to a fixed roadside network infrastructure with information flowing both ways. This network environment motivates the need for an infrastructure that will provide drivers with access to a variety of vital vehicular and roadside information. The resulting enhanced situational awareness has the potential to not only facilitate the decision making tasks of the drivers (e.g., trip planning based on traffic congestion on the road), but also to improve highway safety (by bringing information about catastrophic events and road conditions to the driver's attention). Our objective in this paper is to explore the security-related challenges in this envisaged setting.

While this paper presents no solid technical results, we believe that it provides a valuable analysis of an environment that is very likely to become real in the near future. In particular, it describes one instantiation of an information infrastructure for highway driver assistance: **DAHNI** (**D**river **A**d **H**oc **N**etworking **I**nfrastructure). The paper starts with the brief overview of some key technology assumptions in the next section. We then consider a couple of promising applications (Section 3) and turn to the discussion of specific security issues.

## 2 ASSUMPTIONS

The main elements and assumptions of the envisaged DAHNI infrastructure are as follows:

- **Location awareness**: we expect that, in the near future, most vehicles will be equipped with GPS receivers providing fairly accurate geographical position coordinates. (Note that many SUVs are already being outfitted with GPS receivers.)
- **Ad hoc networking**: many high-end vehicles are already being equipped with sophisticated computing components interconnected via a LAN. This trend will very likely extend into wireless networking. In particular, we assume that short-range wireless ad hoc networking for inter-vehicle communication will become ubiquitous.
- **Access to fixed infrastructure:** a fixed infrastructure **--** comprised of (at least) a number of base stations strategically positioned in close proximity to the highways **--** is necessary to facilitate the upload of data from the vehicles. This data can be used for monitoring current traffic conditions, as well as managing traffic. Vehicles elsewhere can also query the fixed infrastructure for trip planning purposes.

## 3 POTENTIAL APPLICATIONS

The DAHNI infrastructure provides numerous possibilities to revolutionize the automotive and transportation industry of the future. For example, data captured by DAHNI, when properly aggregated, can be fed into the traffic monitoring and flow control system for real-time traffic management. Alternatively, such information can be archived for off-line analysis to understand traffic bottlenecks and devise techniques to alleviate traffic congestion.

There are numerous application possibilities and scenarios some of which may spark debates over privacy rights and apprehensions over undue monitoring. However, the **only** applications we consider are of the non-invasive, assistive variety.

One of the most compelling DAHNI application examples is what we call "**V**ehicle **I**mmediate **V**icinity **A**wareness" or **VIVA** for short. VIVA aims to communicate to each vehicle *vital signs* of other vehicles that are traveling in close proximity. Proximity in this context means the area that falls within direct range of transmission of the wireless networking device found in each vehicle. Such vital signs may include the status of: turn signal indicators, brake application, relative/absolute speed, headlights, etc. It is important to note that all of these signs are, in any case, intended for external display, e.g., the status of the turn signal is always in plain view. In other words, no new information that might be construed as private is intended for communication outside a vehicle.

We anticipate that the information collected by VIVA will assist the drivers by offering them better awareness of their immediate surroundings as well as of the current and intended behavior of the nearby vehicles. Drivers will be able to better concentrate on the road ahead if they no longer have to look sideways to observe flanking and tailgating vehicles. Also, notorious blind spots can be effectively eliminated if drivers are continuously made aware of the surrounding space. Furthermore, traffic conditions ahead can be observed faster if drivers are warned of braking activity one or two vehicles ahead. Consequently, we expect VIVA to increase highway safety by preventing some accidents.

Another, very different, application has to do with trip planning. We refer to it as "**Hi**ghway **T**raffic **C**ondition **H**elper" or **HITCH** for short. In it, vehicles communicate directly to the fixed infrastructure (base stations) and report their vital signs (as above) as well as the speeds of surrounding vehicles. This information is then efficiently gathered and coalesced into regional traffic snapshot databases. Vehicles, both on and off the highway, can query these databases and obtain immediate information on traffic conditions towards intended destinations. Of course, wired clients, i.e., Internet users at home, can also use HITCH.

## 4 System Overview

In Figure 1 we depict a typical scenario for our system. Several cars travel on a highway while communicating locally, via an ad hoc wireless network, and globally, via a fixed infrastructure wireless network. Each car is outfitted with a laptop or PDA equipped with a wireless LAN card (e.g., 802.11) for local communication, and a wide-area wireless device (e.g., a cellular phone) for the connectivity to the infrastructure network.

Each car forms, around itself, a *local* area of communication. Cars that are further away, although they may constitute part of a neighbor's local area, are not part of that particular car's communication network. All cars broadcast information omni-directionally and receive data from all directions. There is no point-to-point communication link. The purpose of the ad hoc network is to impart information, i.e., the car's *vital* signs, to vehicles in close proximity and to receive the same data from them. The information is processed locally to provide the driver with a map indicating the status of each car in the immediate vicinity, e.g., acceleration, turning signal status, braking, etc. A sample VIVA screen is depicted in Figure 2; it shows some potential vital signs that may be reported.

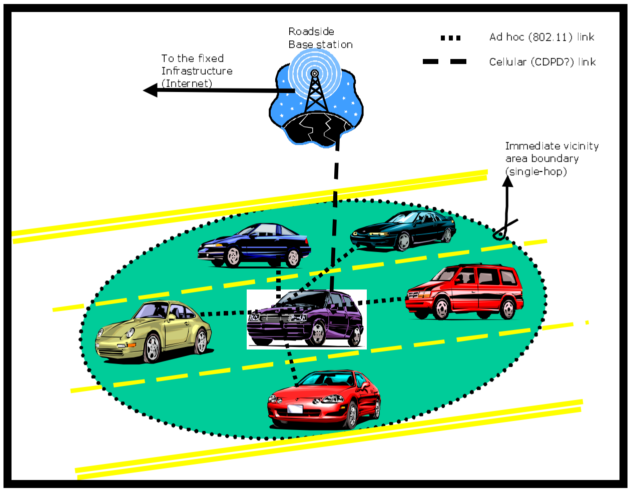

**Figure 1**

In addition to the local ad hoc network, each vehicle also communicates, at a much lower frequency rate, with the infrastructure network in order to upload its vital signs. This data is used by the infrastructure for maintaining up-to-date traffic conditions and for performing traffic management. It also constitutes the highly dynamic database that users (drivers) can query to extract traffic and trip planning information. This refers to the HITCH application mentioned earlier.

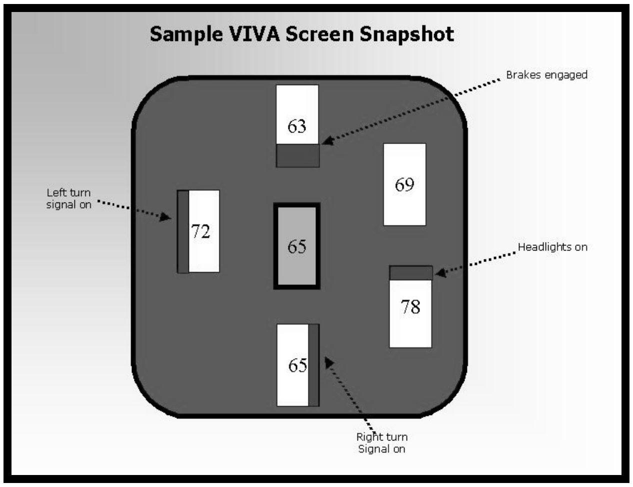

**Figure 2**

We envision that, in addition to communication and processing devices, each vehicle will also be outfitted with a GPS receiver and sensors that collect information regarding the *vital* signs of the vehicle. Furthermore, each vehicle will have, on each of its four sides, a simple detection device that will monitor the presence (or absence) of another vehicle in the immediate vicinity. This feature is necessary to ensure a safe system that is not prone to the vagaries of wireless communication. Figure 3 illustrates a sample unit (i.e., laptop or PDA) that will be fitted into each vehicle with its corresponding communication, GPS links and sensor feeds.

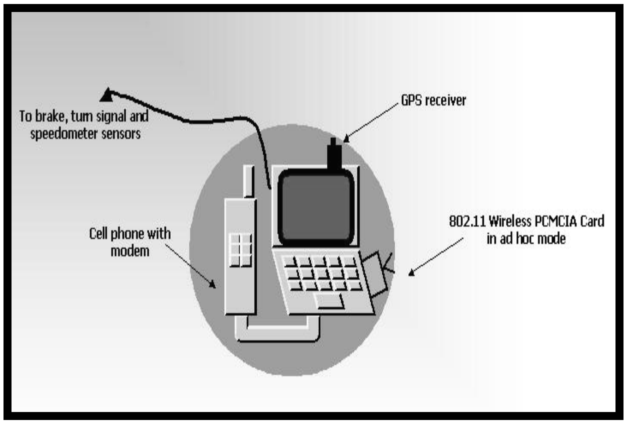
To brake, tum signal and speedometer sensors
GPS receiver
Cell phone with modem
802.11 Wireless PCMCIA Card in ad hoc mode

**Figure 3**

## 5 Challenges

We now outline the set of challenges in developing the envisaged network and information infrastructure.

First and foremost, we are dealing with an environment that is very dynamic and composed of high-motion vehicles. This results in rapidly changing network topologies. In addition, data exchanged between the vehicles is extremely time sensitive. The number of nodes involved is much larger than any system that has been proposed to date (e.g., sensor environments). On the other hand, since the communication devices are mounted in vehicles, the power supply is unlimited. This makes it possible to use fairly large antennas and on-board GPS devices. Also, data is only of interest to a small set of neighboring vehicles.

At first, the above appears to simplify the problem since all data is broadcast one hop and no routing is involved. There are, however, some concerns. Primarily, the throughput of the system and the delays involved are important since the data is time sensitive, and in many cases, of urgent nature (e.g., speeding vehicle approaching in left lane). Therefore, the system must be robust and must have the capacity to support the traffic load and its time-critical needs (i.e., how far can the system can be pushed before reaching the point at which chaos prevails and data flow comes to halt). More complex, multi-channel systems that can handle the traffic load and its delay constraints, pose a different set of problems associated with the speed with which vehicles can associate themselves to the different channels and maintain an up to date picture of their surroundings.

From the information infrastructure perspective, DAHNI can be seen as a highly distributed and dynamic database where a large number of data sources (e.g., vehicles) generate vehicular information which is then consumed at different levels of aggregations (i.e., individual vehicle level in the context of VIVA applications, and, at a more aggregated form, in HITCH applications). The data sources may themselves store information acting as smaller (light-weight) databases, or alternatively, periodically migrate the information to the backbone storage and computation units.

The additional intelligence embedded in VIVA must be capable of expedited processing of critical path control messages -- information that can impact immediate vehicular control. In conjunction with the selective processing of messages, VIVA will implement appropriate information collection policies and algorithms that determine how and when to probe and process incoming and outgoing information. Inter-node VIVA interfaces and protocols will allow for customized processing of messages received from other vehicles. VIVA-HITCH interfaces and protocols will implement techniques to determine the transfer of information between the vehicle and the fixed wired infrastructure.

The HITCH layer assumes a hierarchical architecture where information flows from the vehicles to databases supported at the fixed infrastructure (reachable through roadside base stations). Information may also flow (at various levels of aggregation) from the infrastructure to the vehicles to support, queries that originate at the vehicles. An example of such a query corresponds to traffic information on a given route. Many aspects of such a query are interesting. First, the DAHNI infrastructure may attempt to answer such a query based on data cached at the vehicle. Since data cached at vehicles can be rapidly outdated in the dynamic environment, techniques to correlate quality of results based on quality/age of data will need to be developed. If the data does not satisfy the quality requirement of the query, the vehicle will need to communicate with the fixed infrastructure, the base stations and/or other vehicles to get more accurate information. In general, query computation will be shared between the vehicles and the databases residing at the base stations as well as the fixed infrastructure [7-12]. Another interesting aspect of such queries is their continuous nature. Traditionally, a database query is issued explicitly; the database evaluates it and returns all results in one time. In contrast, in the DAHNI environment a user (e.g., a driver) may monitor events/traffic continuously en-route. Implemented naively, the vehicle will generate a fresh query every time its location changes or an event occurs that changes the result set of the previous query. Given the continuity of motion in space and time, it is possible to optimize such continuous queries extensively [8].

The DAHNI environment also poses a number of security- and privacy-related research challenges. In particular, vehicle-specific information exchanged as part of VIVA or reported as part of HITCH must be provided strictly at the discretion of the owner/driver, i.e., participation in inter-vehicle (and vehicle-infrastructure) networking must be voluntary. At the same time, all information provided – whether by the vehicles or by the infrastructure -- must be authentic, i.e., both the source and the integrity of the information must be evident and verifiable. We now consider these challenges in more detail.

## 6 SECURITY AND PRIVACY ISSUES

Issues of security and privacy are fairly common to most mobile and wireless network settings: authentication, data integrity, resistance to various denial-of-service attacks and so forth.

At first glance, it may seem as if the network environment envisaged in this paper might not have any unique features or challenges related to security and privacy. However, a closer look reveals some important differences:[1]

- **No confidentiality**: the issue of data secrecy or confidentiality is not of concern in this network environment; none of the application scenarios we consider require any data to be kept secret. This is quite unusual in mobile networks. For example, in many modern cell phone networks (GSM [3], CDPD [4], etc.) a secure channel is maintained between the cell phone and the nearest base station and/or local subscriber registry
- **No key distribution**: most mobile network security architectures include provisions for key distribution. This is not only the case when an encrypted channel is set up; many settings require a key to be shared for authentication and data integrity reasons. In our case, key distribution is unnecessary for two reasons: 1) there will be no bulk data transmitted (on a continuous basis) either among cars or between cars and roadside infrastructure, and, 2) vehicles traveling at high speeds (as most do on highways) will likely spend little time within a cell of a given base station. Also, vehicles communicating in an ad hoc network broadcast their data, thus, pair-wise (or group-wise) key distribution is not needed.
- **No hand-over**: typically, one of the notable security features of mobile networks is the secure hand-over protocol [3, 4], e.g., as a node moves from one cell to another, its state (including any on-going connection data) is handed over from one base station to the next. However, explicit hand-over is not needed if communication is largely one-way, i.e., vehicles reporting current speed and other parameters to the base stations.
- **No battery power concerns**: this is actually the most important distinguishing factor of the network environment outlined in this proposal. In practically all mobile networks, power (CPU) consumption is a paramount concern. This includes not only power utilized for reception and transmission but also the power necessary to perform (usually expensive) cryptographic operations on weak and battery-challenged computing devices such as small PDAs, packet radios or cell phones. In our case, power consumption is not relevant since a running vehicle provides an ample source of battery power.
- **No CPU speed issues**: a related concern in many mobile networks is the low CPU speed of the mobile node. Hence, there is usually a goal to minimize the use of cryptography because of the relatively long delays it imposes (e.g., an average Palm Pilot or Handspring PDA [1] takes seconds to generate a digital signature). This often results in security protocols that are "contorted" to minimize the use of cryptography; sometimes, with disastrous consequences, e.g., the original GSM security architecture [5]. Since "nodes" in our context are vehicles, more powerful (faster) CPUs can be assumed.
- **Extreme Time Sensitivity:** as mentioned earlier, all data is very much time-sensitive. In applications such as VIVA, the needs for timeliness are only part of the problem. Time synchronization is also extremely important (although we can perhaps count on the GPS devices to provide accurate and uniform clock readings). Moreover, the system must be intolerant of replays (hostile and otherwise).

Taking the above differences into account leads us to a fairly simple security architecture with the following notable features:

- **Digital Signatures**: we require all broadcasts in VIVA as well as all "reports" in HITCH to be digitally signed by the originating vehicle. Since each vehicle (and the roadside infrastructure) will receive many more messages that it will send, the cost of signature verification is of more importance than that of signature generation. Therefore, at least at the beginning, we are likely to use RSA-based digital signatures (as opposed to, say, DSA). Of course, an appropriate message and signature format will be defined.
- **Time-stamping and sequencing**: all communication in both applications will include both sequence numbers as well as timestamps. Clock synchronization is a non-issue, for the time being, as all vehicles and fixed infrastructure components are

[1] The above list is not meant to be exhaustive; there are possibly other, more subtle differences.

(per our assumption) equipped with GPS receivers and GPS is also a time service.

- **Certification Infrastructure (PKI)**: public key digital signatures are not particularly useful without a certification infrastructure. Designing a nimble, scalable and secure PKI has been a major challenge in the last decade. (See, for example, IETF PKI efforts [6].) We must take into account the unique aspects of our network environment in designing an appropriate PKI. Moreover, there are some recent and promising results in cryptography that obviate the need to public key certificates. For example, the Boneh/Franklin identity-based encryption system [2] is an elegant method of obtaining public key cryptography without any certificates: in it, an entity's public key is derived from a unique identity string, e.g., an email address or X.500 distinguished name. (This could be a vehicle identification number, in our case.)

## 7 Secure Information Management

The databases at various levels of the DAHNI infrastructure (from those located at the vehicles, to base stations, to back-end servers) store a variety of spatial and spatio-temporal information about vehicles on the move and their ambient environment. Such information includes data about vehicles and their locations at different times, traffic conditions, road signs, traffic signals, and the road network. Ensuring the integrity of the assorted information and providing effective access control mechanisms to prevent unauthorized access and usage of information in the DAHNI environment poses a significant challenge. Data in the DAHNI environment can be classified into:

1) Fixed spatial data that does not change with time (the road network, location of traffic sign);
2) Spatio-temporal data that changes with time (number of vehicles in a given road segment, information about road construction); and
3) Mobile data for which both the value and location changes as a function of time.

There are several problems that must be resolved to enable the secure collection and dissemination of relevant information in a timely manner within the DAHNI infrastructure. One issue is that of providing *real-time access control* to the various VIVA and HITCH databases. Dynamic reconfiguration within the DAHNI environment further complicates data collection. Since the set of VIVA neighbors in the network and the base-stations that a node is connected to changes continuously, access control criteria in the ad-hoc network may need to be continuously reestablished. The degree to which this dynamics must be reflected in the access control policies is application dependant and is an interesting topic for future research.

## 8. SUMMARY

In summary, in this brief paper we sketched out a vehicular communication infrastructure (DAHNI) and discussed several unique security issues and challenges. Although DAHNI is a concocted, artificial setting, we believe that the technology components needed to make it real are already available. Clearly, this paper presents no actual results: it only scratches the surface of what is promising to be a new and fertile area of research both in networking and security.

## References

[1] N. Modadugu, D. Boneh, and M. Kim, "Generating RSA Keys on the PalmPilot With the Help of an Un-trusted Server," *RSA Data Security Conference 2000*.

[2] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *in Proceedings of CRYPTO'2001*.

[3] M. Rahnema, "Overview of the GSM System and Protocol Architecture," *IEEE Communications Magazine, April 1993*.

[4] Y. Frankel, et al., "Security Issues in a CDPD Wireless Network," *IEEE Personal Communications, August 1995*.

[5] R. Molva, D. Samfat and G. Tsudik, "Authentication in Mobile Networks," *IEEE Network, March/April1994. Internet Public Key Infrastructure, Internet RFCs 2459, 2510, 2511*.

[6] I. Lazaridis, S. Mehrotra, K. Porkaew and R. Winkler, "Database Support for Situational Awareness", *Computer Science Handbook, M.S. Vassilou and T.S. Huang (eds.), Army Research Laboratory, 2001*

[7] I. Lazaridis and S. Mehrotra, "Quality Aware Query Processing", *Submitted for publication. 2002*.

[8] I. Lazaridis, K. Porkaew, S. Mehrotra, "Dynamic Queries over Mobile Objects", *To appear in to the 8th International Conference on Extending Database Technology, 2002*.

[9] I. Lazaridis, S. Mehrotra, "Incorporating Aggregate Queries in Interactive Visualization", *5th Annual Federated Laboratory Symposium, 2001*.

[10] I. Lazaridis and S. Mehrotra, "Progressive Approximate Aggregate Queries with a Multiresolution Tree Structure", *2001 SIGMOD Conference on Management of Data, 2001*.

[11] S. Mehrotra, I. Lazaridis and K. Porkaew, "Situational Awareness over Large Spatio-Temporal Databases", *Workshop at the Intersection of Geospatial Information and Information Technology, Computer Science and Telecomm. Board, National Council of Research, Oct 2001.*

[12] K. Porkaew, I. Lazaridis and S. Mehrotra, "Querying Mobile Objects in Spatio-Temporal Databases", *7th International Symposium on Spatial and Temporal Databases, 2001*.