Secure Inter-Vehicle Communications

Syed Masud Mahmud, Shobhit Shanker and Srinivas Reddy Mosra
Department of Electrical and Computer Engineering, Wayne State University

Reprinted From: In-Vehicle Networks and Software, Electrical Wiring Harnesses, and Electronics and Systems Reliability (SP-1852)
Secure Inter-Vehicle Communications

Syed Masud Mahmud, Shobhit Shanker and Srinivas Reddy Mosra
Department of Electrical and Computer Engineering, Wayne State University

ABSTRACT
The study done by the U.S. National Highway Traffic Safety Administration (NHTSA) shows that developing automotive collision warning and avoidance systems will be very effective for reducing fatalities, injuries and associated costs. In order to develop an automotive collision warning and avoidance system, it will be necessary that the vehicles should be able to exchange (in real time) their dynamic information such as speed, acceleration, direction, relative position, etc. The only way to exchange the vehicles’ dynamic information will be through wireless communications. The communication links among vehicles must be secured. Otherwise, hackers may inject some misleading data into the inter-vehicle messages to make the vehicle systems malfunction. In this paper, we have presented a technique for exchanging vehicles’ dynamic information in a secure mode. We also investigated the feasibility of implementing secure inter-vehicle communication links using today’s technology. Our study shows that current technology will allow us to build such a system.

INTRODUCTION
The aim of this paper is to provide an architecture to enable information exchange between vehicles in a secure way. The federal government incurs losses of millions of dollars every year in terms of vehicle accidents, and 90% of these losses are due to collisions [1].

During the last several decades, the improvements in seat belts, air bags, crash zones, and lighting have significantly reduced the rate of crashes, injuries and fatalities. In spite of these improvements, each year in the United States, motor vehicle crashes still account for about 40,000 deaths, and over 130 billion in financial losses [1]. A significant focus and interest has risen to develop active safety technology and collision avoidance systems. In order to develop an automotive collision avoidance system, it becomes imperative that the vehicles exchange their dynamic information such as speed, acceleration, position and direction in real time. With the advent of wireless ad hoc networking technologies, this can be done in a fairly accurate and feasible manner. The goal of the Automotive Collision Avoidance Systems (ACAS) is to detect and warn the driver of potential hazard conditions. Therefore, it is of extreme importance that the data integrity should be taken care of, which means that the system should be immune to security attacks. It should be ensured that all communication between various vehicles is done in a secure fashion. Otherwise, a person with malicious intent might inject incorrect information into the inter-vehicle wireless links leading to a disaster, not only for the driver but also for the hundreds of others on the road.

For two devices (in our case, two vehicles) to communicate securely, it is necessary that they share some kind of secret key(s). In a client-server based architecture, this is done by the server using protocols such as SSL, VPN tunneling [2], etc. However in ad hoc networks there is no client-server architecture. The topology of ad hoc networks is dynamic and is constantly changing [3].

Ronald Miller and Qingfeng Huang have done some work in the area of ACAS using wireless communication technologies [4], but their systems are not secure, and can easily be attacked by hackers. In our architecture, security aspects such as authentication, authorization, and data integrity have been implemented. In our proposed architecture, we have suggested a device known as an NDM (Network Device Monitor). The concept of using an NDM has been proposed earlier in our previous work [5]. For an in-vehicle (intravehicle) network, the NDM acts as a key distribution center located inside the vehicle. The NDM acts as a gateway device, which all the devices use to communicate with each other. The NDM is also responsible for maintaining the sessions of the in-vehicle wireless network. The detailed operations of the NDM have been explained in the subsequent sections of this paper.

In our earlier work, we proposed having an NDM in a vehicle for taking care of the security of intravehicle networks. In this paper, we have proposed to have another level of Network Device Monitors to take care of the security of intervehicle networks. This new level of NDMs should be embedded in towers that will be alongside the roads. These towers, known as the Intelligent Transportation Towers, are responsible for providing seamless secure communication between the
vehicles on the roads. An ITT (Intelligent Transportation Tower) will function in the same way as a cell phone tower. Since cell phone towers cover almost all road systems, the contracts for maintaining ITTs can be given to the companies that maintain the cell phone towers. In that case, the same set of towers can serve both purposes: maintaining cell phone networks as well as providing secure communication mechanisms among intelligent vehicles.

SECURE VEHICULAR COMMUNICATIONS

In this section, we first present background material including our prior work on building secure in-vehicle network, and then we present our proposed technique for building secure inter-vehicle networks. After that we present system requirements for our proposed technique.

BACKGROUND MATERIALS

During the last several years, interest in using wireless communication technologies have grown significantly. Bluetooth features are becoming very common in cell phones, PDAs, laptops, etc. More and more homes are getting broadband connections and using Wi-Fi technology for in-home wireless networking. The automotive industry has also started introducing Bluetooth technologies to build in-vehicle wireless networks. The Bluetooth-enabled cell phone fitted in the 2003 Saab 9-3 car can access any other Bluetooth-enabled devices in the car, such as a PDA [6]. We hope, in the future, other automobile companies may also introduce wireless networking technologies in their vehicles. If intra and inter-vehicle wireless networks can be implemented at reasonable costs, then the government may also require all auto manufacturers to have wireless networking features in every vehicle, so that the vehicles can exchange messages among themselves (in real time) to issue pre-crash warnings. The vehicles must communicate among themselves through secure wireless links to avoid any disasters from hackers.

Securing any type of communication links involves three key requirements. First, the links must be protected from eavesdropping, so that unauthorized persons can’t access private information. Second, the end users must be authenticated before anything is sent to or received from them. Third, the communication links must be protected from tampering by hackers.

If all information is transmitted in encrypted form, then that should protect the communication links from eavesdropping. If standard techniques, such as Cyclic Redundancy Check (CRC) [7], [8] Check Sum [8], Hamming Code [9], etc. are used with the information before it is encrypted, then that should protect the links from tampering. Yet the most vital task in establishing a secure communication link is authenticating the parties on both sides of the communication link and exchanging their encryption keys.

In our earlier work, we developed a technique for securing an in-vehicle network [5]. A brief description of our earlier work is presented in the following subsection to make the readers familiar with the technique for developing a secure in-vehicle network. After that we present the technique for building inter-vehicle secure wireless networks.

![Figure 1: Registration process of a device to the NDM](image)

A Secure In-Vehicle Network:

For in-vehicle devices to securely communicate with each other, they should use some secret keys. The length of the keys should be sufficiently large so that the keys are not susceptible to attacks such as brute force attacks. In order to build a secure in-vehicle network, we used a device called the Network Device Monitor (NDM). The NDM is responsible for distributing secret keys to all the in-vehicle devices. All devices to be used in the vehicle are initially registered to the NDM through a password protected user interface. The user interface could be a keypad, an infrared link or a very short-range (say, a few inches) wireless link. For every wireless device to be used in the vehicle, the password-protected human interface is used only once during the lifetime of the device. During the registration process of a device, the NDM sends a set of authentication keys to the device, and also keeps a copy of the keys in its own memory. Figure 1 shows the registration process of a device to the NDM. When a device wants to join an in-vehicle communication session, the NDM authenticates this device using one of its authentication keys. Different in-vehicle devices are given different sets of authentication keys, so that the keys of other devices can’t be obtained by using a lost or stolen device. A lost or stolen device can also be deregistered from the NDM using the password-protected user interface. This deregistration process is necessary to protect the in-vehicle wireless network from unauthorized users who may have the lost or stolen device in their possession.
The NDM sends a session key to the device.

The device starts talking to other in-vehicle devices using the session key.

Figure 2: Authentication of a device by the NDM

Assume that the authentication keys of a device are \( k_1, k_2, \ldots k_n \), where, \( n \geq 1 \). Later on, when the device will try to join a wireless communication session, the NDM will use one of the keys of the device to authenticate the device. Different authentication keys will be used for different communication sessions of the device. Key \( k_i \) will be used during the \( i^{th} \) session of the device after the device has been registered. During the \( n^{th} \) session of the device, the NDM will send another set of authentication keys to the device, for the device to join future sessions.

PROPOSED TECHNIQUES FOR BUILDING SECURE INTER-VEHICLE WIRELESS NETWORKS

In this section of the paper we have presented a technique for building secure inter-vehicle wireless networks. This technique requires that every vehicle must be equipped with a wireless device to communicate with the neighboring vehicles as well as with the Intelligent Transportation Towers (ITTs). An ITT will be responsible for authenticating the vehicles when the vehicles come within the range of the ITT. If the contract for maintaining the ITTs is given to companies that maintain the cell phone towers, then the same tower can be used for providing service to the cell phone networks as well as to the intelligent transportation networks. An intelligent vehicle will have three different types of wireless links: 1) a link for the in-vehicle wireless network, 2) a link for inter-vehicle wireless networks, and 3) another link for the vehicle to ITT communications. Our goal is not to advocate a particular wireless technology to be used in the vehicles. Any wireless technology, such as Bluetooth, Wi-Fi, etc. can be used for communications. Bluetooth or any similar technology that allows devices to form ad hoc networks can be used for in-vehicle as well as for intervehicle wireless networks. A short-range (say 10-meter) technology can be used for in-vehicle networks, and a long-range (say a couple of hundred meters) technology can be used for intervehicle networks. The links for vehicle to ITT communications must have a longer range so that a vehicle will be able to communicate with at least its nearest ITT. Wi-Fi or Cell Phone technology can be used for the vehicle to ITT communications. The protocol for vehicle to ITT communications can be a client-server protocol, where the vehicles are the clients and the ITTs are the servers.

When a vehicle is manufactured a wireless device will be installed in it. After the wireless device has been installed, a set of keys will be given to it. A copy of these keys will also be kept in a secure central server. The secure central server can be maintained by any one of the following organizations: a) the manufacturer of the vehicle, b) the supplier which makes the wireless device, c) the company which is responsible for maintaining the intelligent transportation towers, or d) any other trusted organizations. Different vehicles will be given different sets of keys. These keys will be securely kept in the central server. Authorized organizations will be able to access the keys of a vehicle by using the vehicle’s ID (VID) number. If the central servers are maintained by the auto companies, then the VID of a vehicle will indicate which server to go to for accessing the keys.

Authentication Process:

Every ITT will be equipped with a device called the Network Device Monitor (NDM). When a vehicle enters a road, it will send its VID to the nearest ITT. The NDM of the ITT will then check its own memory to determine whether or not the keys of the vehicle are locally available. If the keys are not locally available, then the ITT will check to see whether or not the keys are available in the adjacent ITTs. If the keys are not available in the adjacent ITTs either, then the ITT will access the central server of the vehicle to access the
keys. The ITT will then try to authenticate the vehicle using one of the keys. Based on a built-in protocol, both the vehicle and the central server know which key to use for the current authentication. If the keys were locally available in the NDM of the ITT, then the ITT also knows which key to use for authentication. After a vehicle is authenticated by an ITT, both the vehicle and the ITT will generate a common encryption key. After that, all communications between the vehicle and the ITT will take place in encrypted form. The ITT will use different encryption keys for different vehicles, so that the communication between a vehicle and an ITT remains private.

After all authentication keys of a vehicle are used, the central server of the vehicle will issue a new set of authentication keys to the vehicle via the network of ITTs. This new set of keys will be used for future authentications.

A vehicle needs a session key in order to communicate with its neighboring vehicles. The session key is given to the vehicle by the ITT after the vehicle has been authenticated. The ITT sends the session key to the vehicle in encrypted form. The vehicle then talks to other neighboring vehicles using the session key.

If the authentication of the vehicle by the ITT fails, then the ITT will not send any session key to the vehicle. The ITT will warn all vehicles within its range about the presence of an unauthorized vehicle on the road. The ITT will also send a warning message to the highway patrol officers informing them about the presence of an unauthorized vehicle. Figures 3a, 3b and 3c show the entire authentication process of a vehicle by an ITT.

Communication among vehicles:

Figure 4 shows a snapshot of a road with thirteen vehicles (V1 through V13) and two ITTs (ITT-1 and ITT-2). All thirteen vehicles are moving from the left to the right. Vehicles V1 through V7 are within the range of ITT-2, and vehicles V7 through V13 are within the range of ITT-1. The thirteen vehicles form three clusters. Vehicles V1 through V4 are in Cluster 1, vehicles V5 through V9 are in Cluster 2, and vehicles V10 through V13 are in Cluster 3. It is assumed that the clusters are far away from each other, so that the vehicles of one cluster don't need to form a network with the vehicles of
the other clusters. The vehicles of Cluster-1 will use the session key of ITT-2 to communicate among themselves. The vehicles of Cluster-3 will use the session key of ITT-1 for communicating among themselves. The vehicles of Cluster-2 are in the range of both ITT-1 and ITT-2. Since vehicles V5, V6 and V7 are in the range of ITT-2, they will communicate using the session key of ITT-2. Similarly, since vehicles V7, V8 and V9 are in the range of ITT-1, they will communicate using the session key of ITT-1. Since vehicles V5 and V6 moved into the range of ITT-2 from the range of ITT-1 just a while ago, they still know the session key of ITT-1. Thus, V5 and V6 will communicate with V8 and V9 using the session key of ITT-1. From time to time, every ITT will change its session key in order to protect the inter-vehicle communications from Brute Force attacks.

Figure 4. A road with two ITTs and three clusters of vehicles.

The communication between a pair (vehicle, ITT) is private. Hence, when a vehicle talks to an ITT, no other vehicles can understand that conversation. Thus, when a session key is sent from an ITT to a vehicle, it is sent in a secure mode. If the session key is long enough, and also if the ITT changes the session key from time to time, then it will be difficult for someone to crack the key using some kind of external hacking device (not a part of the vehicle electronics). Unauthorized vehicles, such as stolen vehicles, unidentified vehicles, vehicles without valid registration, suspended vehicles (vehicles that have lost the privilege of being on the road due to prior violations), etc. will not be issued any session keys by the ITTs. In fact, an ITT can issue warning messages to all authorized vehicles and highway patrol officers within its range, informing them about the presence of an unauthorized vehicle within the neighborhood. The drivers of the authorized vehicles can then take extra precaution in driving their vehicles. If the authorized vehicles are equipped with Automatic Collision Avoidance System (ACAS), then these vehicles can automatically disable their ACASs and go back to manual mode after receiving warnings about the presence of unauthorized vehicles on the road.

SYSTEM REQUIREMENTS FOR BUILDING SECURE INTER-VEHICLE WIRELESS NETWORKS.

In this section we present an estimate of memory and bandwidth requirements for an ITT. The memory and bandwidth requirements have been determined for the worst-case scenarios. In order to determine the memory requirement of an ITT, we assumed that the road system is completely jammed. This means that traffic is bumper-to-bumper. In order to determine the bandwidth requirement of an ITT, we assumed that a vehicle maintains a distance of one second (distance traveled in one second) from the vehicle in front of it. Note that, for safe driving, a distance of at least two seconds is recommended behind the vehicle in front of you, but we used a distance of one second to determine the worst-case requirement.
**Memory Requirement:**

Let's assume that each tower covers a distance of \( r \) miles of the road, each vehicle takes up a space of \( d \) feet, and there are \( k \) lanes on the road. Then the total number of vehicles within the range of an ITT on a road is \( \frac{5280r}{d}k \). Let's assume that the length of each key is \( x \) bytes and an ITT must keep \( y \) number of keys per vehicle within its range. Then the size of memory required to keep the keys of the vehicles of a road is \( \frac{5280r}{d}kxy \) bytes. If there are \( n \) such roads within the range of an ITT, then the total size of memory required to keep the keys of all the vehicles within the range of an ITT is

\[
M = \frac{5280mrkxy}{d} \text{ bytes.} \tag{1}
\]

We have determined the size of memory assuming that the traffic on the road is bumper-to-bumper (worst-case scenario), as shown in Figure 5. For such a case, we assumed that the average space needed by a vehicle is 25 feet (\( d = 25 \)). We also assumed that each key is 128 bits (16 bytes) long and at any given time four keys need to be kept for every vehicle within the range of the ITT. Table I shows a list of all the parameters used to determine the memory and bandwidth requirements.

For **rural driving**, an ITT may have to take care of only one or two highways. Also, the highway may not have more than four lanes. Table II shows the memory required by an ITT in rural areas. This table shows that the size of memory required by an ITT to keep the keys of the vehicles is in the order of a few hundred kilobytes, which is not a significant size.

For **city driving**, especially in the downtown area of a big city, an ITT may have to take care of many roads, and each road may have many lanes. Assume that there are \( m \) roads per mile of a downtown area. If the range of an ITT is \( r \) miles along the East-West and North-South directions, then the ITT will have to take care of vehicles for \( 2mr \) number of roads as shown in Figure 6. Replacing the parameter \( n \), used in Equation (1), by the term \( 2mr \) we get the following expression for the size of memory required by an ITT in a downtown area.

\[
M = \frac{10560mr^2kxy}{d} \text{ bytes} \tag{2}
\]

For downtown areas like New York, Los Angeles, Chicago, etc, we can assume that there are approximately eight roads per mile (\( m = 8 \)) along both East-West and North-South directions. Table III shows
the memory required by an ITT in the downtown area of a big city. This table shows that the size of memory required by an ITT to keep the keys of the vehicles is in the order of a few megabytes, which is not that significant either (by today's standard).

Table II: Memory required by an ITT in rural areas.
(For \( d = 25, \ x = 16 \) and \( y = 4 \))

<table>
<thead>
<tr>
<th>Number of Roads (n)</th>
<th>Range of an ITT in miles (r)</th>
<th>Number of Lanes in the Road (k)</th>
<th>Memory Required in Kbytes (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>52.8</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>4</td>
<td>105.6</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>2</td>
<td>79.2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>4</td>
<td>158.4</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>105.6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>211.2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>158.4</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>316.8</td>
</tr>
</tbody>
</table>

Figure 6. Coverage area of an ITT in a Downtown.

Table III: Memory required by an ITT in a big downtown area.
(For \( d = 25, \ m = 8, \ x =16 \) and \( y = 4 \))

<table>
<thead>
<tr>
<th>Range of an ITT in miles (r)</th>
<th>Number of Lanes in each Road (k)</th>
<th>Memory Required in Mega Bytes (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>1.65</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3.30</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3.71</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>7.43</td>
</tr>
</tbody>
</table>

Note that in addition to the memory size shown in Tables II and III, some more memory is needed by each ITT to keep and run the program for maintaining secure intervehicle networks. The size of this additional memory is fixed and doesn’t depend on the number of vehicles within the range of the ITT.

Bandwidth Requirement:
An ITT will have to communicate (in real time) with all the vehicles entering its range. The ITT will have to exchange several messages with every vehicle to authenticate the vehicle and then issue the session key. Let's assume that every message will contain about 256 bytes including the header, data and checksum, which is a reasonable assumption. Let's also assume that a total of six messages need to be exchanged between a vehicle and the ITT to go through the process of authentication and issuance of the session key. Thus, the ITT needs to exchange about 1.5 Kbytes of data with every vehicle entering its range. If the vehicles are keeping a one-second distance between them and the vehicles in front of them, then the total number of vehicles entering into the range of the ITT in every second will be equal to \( nk \). Hence, the bandwidth necessary from an ITT to communicate with all the vehicles in its range is 1.5 \( nk \) KB/sec (Kilobytes/sec). For a downtown area \( n = 2mr \). Hence, the required bandwidth for a downtown area is \( 3mrk \) KB/sec. Some additional bandwidth is necessary from each ITT to receive the keys of the vehicles from the central server. The additional bandwidth needed from an ITT is equal to \( nkxy \) bytes/sec and \( 2mrkxy \) bytes/sec for rural and downtown areas, respectively. Hence, the total bandwidth needed from an ITT can be expressed as:

\[
B = \left(1.5 + \frac{xy}{1024}\right)nk \text{ KB/sec (for rural areas)} \tag{3}
\]

and

\[
B = \left(1.5 + \frac{xy}{1024}\right)2mrk \text{ KB/sec (for a downtown)} \tag{4}
\]

Table IV shows the bandwidth requirement from an ITT in a rural area. It is seen from Table IV that for two roads and four lanes per road, the bandwidth needed from an ITT is 12.5 Kbytes/sec, i.e. 100 Kbits/sec, which is not a significant requirement.

Table V shows the bandwidth requirement from an ITT in a large downtown area. It is seen from Table V that if the range of an ITT is 3 miles and if every road has four lanes, then the bandwidth needed from an ITT is 300 Kbytes/sec, i.e. 2.4 Mbits/sec, which can be obtained using Wi-Fi or similar technology.

Table IV: Bandwidth required from an ITT in a rural area.
(For \( x = 16 \) and \( y = 4 \))

<table>
<thead>
<tr>
<th>Number of Roads (n)</th>
<th>Number of Lanes in the Road (k)</th>
<th>Bandwidth Required in Kbytes/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3.125</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>6.250</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>6.250</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>12.500</td>
</tr>
</tbody>
</table>
Table V: Bandwidth required from an ITT in a big downtown area.
(For $m = 8$, $x = 16$ and $y = 4$)

<table>
<thead>
<tr>
<th>Range of an ITT in miles ($r$)</th>
<th>Number of Lanes in each Road ($k$)</th>
<th>Bandwidth Required in Kbytes/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>200</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>150</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>300</td>
</tr>
</tbody>
</table>

From our above analysis, it becomes clear that using today’s technology we can build ITTs with sufficient memory to keep the keys of all the vehicles within the range of the ITT. Today’s technology will also allow us to build ITTs with sufficient bandwidth capabilities to support secure communications among intelligent vehicles.

CONCLUSION

Exchanging vehicles’ dynamic information such as speed, acceleration, position, direction, etc. is necessary to build collision warning and avoidance systems. Secure intervehicle communication links are necessary to protect the intervehicle messages from tampering by hackers. In this paper, we presented a technique for maintaining secure communication links among intelligent vehicles on the road. We provided detailed descriptions of the key exchange mechanism for maintaining security. Intelligent Transportation Towers, like cell phone towers, are necessary to authenticate vehicles on the road. We investigated the feasibility of implementing Intelligent Transportation Towers (ITTs) using today’s technology. From our analysis we found that by using today’s technology it is possible to build ITTs with enough memory and bandwidth capabilities.

REFERENCES


CONTACT

Dr. Syed Masud Mahmud has received his Ph.D. degree in Electrical Engineering from the University of Washington, Seattle, in 1984. He received his B.S. degree in Electrical Engineering from Bangladesh University of Engineering and Technology (BUET), Bangladesh, in 1978. He received a Gold Medal for securing the highest percentage of marks among all the recipients of B.S. degree from BUET in 1978. During his doctoral study at the University of Washington, he was one of the four recipients of Physio Control Fellowship. Currently he is an Associate Professor in the Department of Electrical and Computer Engineering of Wayne State University. He published over 60 technical papers in refereed journals and conference proceedings in the area of Vehicle Multiplexing, Hierarchical Multiprocessors, Cache Coherence Protocols, Interconnection Networks, Wireless Security, and Simulation Techniques. In 2002 he received the President’s Teaching Excellence Award of Wayne State University. He has been listed in a number of Who’s Who. (Email: smahmud@eng.wayne.edu, Phone: 313-577-3855)