Security of Wireless Networks in Intelligent Vehicle Systems

Syed Masud Mahmud and Shobhit Shanker
Department of Electrical and Computer Engineering, Wayne State University, Detroit, MI 48202

ABSTRACT
During the last several years, the interest in wireless networking has grown significantly due to the availability of many wireless products, such as cell phones, wireless mice, wireless keyboards, wireless modems, Bluetooth enabled laptops, etc. Bluetooth is a new technology standard for short-range (10-100m) wireless communications. Having a Bluetooth network in a vehicular system will allow dealers and law-enforcing people to access (remotely) different types of vehicle parameters, such as speed, acceleration, position, emission, tire pressure, etc, through Bluetooth enabled devices. In-vehicle Bluetooth networks will also allow vehicles to communicate with other nearby vehicles on highways and freeways in order to avoid impending collisions and safely change lanes. The passengers of a vehicle can also access private information, e.g. email, fax, banking transactions etc., using Bluetooth enabled access points to the internet. The problem with standard Bluetooth systems is the security. In this paper we have presented a technique to build a secured in-vehicle wireless network.

INTRODUCTION
Wireless networking using Bluetooth technology is becoming very popular. Bluetooth is a new technology standard for short-range (10-100m) wireless communications. Many consumer products such as cell phone, PDA, laptop, personal computer, keyboard, mouse, etc. are being manufactured with built-in Bluetooth features. Auto manufacturers are also looking into Bluetooth technology to provide customers with a better way of using cell phones, PDAs, laptops, etc. within a vehicle. General Motor’s 2003 Saab 9-3 model car came up with a Bluetooth network [1]. In a vehicular system, Bluetooth can be used in conjunction with the vehicle’s wired network (e.g. CAN) to build a hybrid network. Such a hybrid network will allow consumers, dealers and law-enforcing people to access different types of vehicle parameters, such as speed, acceleration, position, emission, tire pressure, etc, through Bluetooth enabled devices. Having Bluetooth networks in vehicles, will also allow vehicles to communicate with other nearby vehicles on highways and freeways. These intelligent vehicles can exchange information among themselves, through Bluetooth devices, in order to safely change lanes and avoid any impending collisions. Some researchers have started looking into the use of wireless networks for peer-to-peer collision warning [2] and cooperative driving systems [3]. Furthermore, a Bluetooth network in a vehicle will also allow passengers to access internet through Bluetooth enabled laptops, receive fax through Bluetooth enabled fax machines, listen to music through Bluetooth enabled headsets, etc.

During the last decade, the interest in designing intelligent vehicles and intelligent highways has grown significantly. Bluetooth networks can play a major role towards achieving the goals and objectives of intelligent transportation systems. Future intelligent transportation systems can be made very safe by using Bluetooth technology in conjunction with X-by-wire technology.

The in-vehicle wireless network should support two types of messages: private message and public message. Private messages will be used to transmit and receive private information, such as a fax, financial transaction, email, etc. On the other hand public messages will be used to exchange a vehicle’s dynamic information with other nearby vehicles. The private messages must be transmitted in secured mode so that no personal information is compromised with other people.

The problem with standard Bluetooth systems is the security. For Bluetooth systems, the authentication, authorization and encryption techniques are all based on some vital piece of information e.g. PIN and Bluetooth device address. The Bluetooth device address is a public domain information. Any Bluetooth device can know the address of any other neighboring Bluetooth devices using an inquiry process. Thus, if the PIN of a set of devices for certain applications is compromised, then the security of that set of devices is also compromised as well.

In this paper we have proposed a technique for building secured in-vehicle wireless networks. Our technique can be easily implemented in a vehicle with marginal costs and very little user interface. The next section of this paper presents a brief description of the standard Bluetooth security techniques. Then we presented our proposed technique and conclusion.

BLUETOOTH SECURITY
The Bluetooth technology provides peer-to-peer communications over short distances. In order to provide usage protection and information confidentiality, the system has to provide security measures both at the application layer and the link layer. These measures shall be appropriate for a peer environment. This means that in each Bluetooth unit, the authentication and encryption routines are implemented in the same way. Four different entities are used for maintaining security at the link layer: a public address which is unique for each user, two secret keys, and a random number which is
different for each new transaction [4]. The four entities and their sizes as used in Bluetooth devices are shown in Table I.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>BD_ADDR</td>
<td>48 bits</td>
</tr>
<tr>
<td>Private authentication key</td>
<td>128 bits</td>
</tr>
<tr>
<td>Private encryption key</td>
<td>8-128 bits</td>
</tr>
<tr>
<td>RAND</td>
<td>128 bits</td>
</tr>
</tbody>
</table>

Table I. Entities used in authentication and encryption procedures.

The Bluetooth device address (BD_ADDR) is a 48-bit number which is unique for each Bluetooth unit. The Bluetooth addresses are publicly known, and can be obtained automatically, via an inquiry routine by a Bluetooth unit. The secret keys are derived during initialization and are further never disclosed. Normally, the encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size may vary between 1 and 16 octets (8-128 bits). The encryption key is entirely different from the authentication key, even though the latter is used to create the former. The authentication key is also known as the link key.

In order to accommodate for different types of applications, four types of link keys have been defined:

- the combination key $K_{AB}$
- the unit key $K_A$
- the master key $K_{master}$
- the initialization key $K_{init}$

The purpose of separating the authentication key and encryption key is to facilitate the use of a shorter encryption key without weakening the strength of the authentication procedure. There are no governmental restrictions on the strength of authentication algorithms. However, in some countries, such restrictions exist on the strength of encryption algorithms.

GENERATION OF THE INITIALIZATION KEY

The initialization key is the first link key and it is generated when two Bluetooth units meet each other or the first time. It is derived from the Bluetooth address BD_ADDR of the claimant unit, a PIN code, the length of the PIN (L), and a random number RAND_A issued (and created) by the verifier, as shown in Figure 1. The BD_ADDR_B, PIN and L are first converted into PIN’ and L’ using an augmentation process, and then PIN’, L’ and RAND_A are converted to the 128-bit initialization key ($K_{init}$) using the E22 algorithm, as shown in Figure 2. Depending upon the need of the applications, other link keys (unit key, combination key, master key) are generated from the initialization key. The initialization key is also used for authentication when two units have no record of a previous link key. When the units have performed the link key exchange, the initialization key shall be discarded.

AUTHENTICATION

The authentication process in Bluetooth uses a challenge-response scheme in which a claimant’s knowledge of a secret key is checked through a 2-move protocol using symmetric secret keys. The latter implies that a correct claimant/verifier pair share the same secret key. In the challenge-response scheme the verifier challenges the claimant to authenticate a random input (the challenge), denoted by AU_RAND_A, with an authentication code, denoted by $E_1$ algorithm, and return the result SRES to the verifier as shown in Figure 3. The input to the $E_1$ algorithm is a tuple consisting of AU_RAND_A, the Bluetooth address of the claimant (BD_ADDR_B) and the secret link key. The verifier also applies the $E_1$ algorithm on the same input tuple and determines SRES’. If SRES’ is same as SRES, then the authentication process is successful.
PROBLEM WITH BLUETOOTH SECURITY

From Figures 1 and 2 it is understood that the secrecy of a Bluetooth device depends on the PIN. So if someone can get hold of this PIN, then that person can monitor the entire conversation of two Bluetooth units that share the same PIN. If no PIN is available, a default value of zero is used. Sometimes no PIN is used to allow various types of devices to form ad hoc networks. For example, if vehicles are allowed to form ad hoc networks to exchange their dynamic parameters, then no PIN may be used.

OUR PROPOSED TECHNIQUE FOR IMPLEMENTING SECURED IN-VEHICLE WIRELESS NETWORKS

In this paper, we have presented an architecture to provide security in vehicular wireless networks. We have developed our architecture by taking the following measures into consideration:

- The system must keep track which Bluetooth devices are allowed to participate in secured private conversations. Thus, the devices which will be allowed to participate in private conversations must be activated, only once during their entire lifetime, through a password protected human interface,
- The PIN for a set of devices should contain reasonably large number of digits,
- The PIN should be automatically changed from time to time, so that it is not compromised due to a brute force attack,
- A device, called the “Network Device Monitor (NDM)”, will be responsible for distributing PINs among the devices that will participate in private conversations,
- The NDM must distribute PINs to other devices in such a way that the PINs are not compromised due to a man-in-the-middle attack.

Our architecture requires a wireless device to be permanently fixed in the vehicle, say at the dashboard. This permanent device is called the Network Device Monitor (NDM). The NDM is equipped with a password-protected keypad to be used for human interface. The NDM also as a port, say a serial port or an infrared link, to be used for activating a device only once during its lifetime. The NDM will keep track of only those devices, which want to participate in secured private communications. All other devices, which want to participate only in non-secured communications, need not be activated by the NDM. The devices, which are activated by the NDM, can participate in both secured and non-secured communications. In a Bluetooth network, the PIN of a device is used as one of the parameters to generate an encryption key. In our architecture, we proposed to have two types of PINs: one type of PIN is for non-secured communication and the other type of PIN is for secured communication. The PIN of a device for non-secured communication can be kept the same for the entire lifetime of the device. But the other type of PIN, needs to be changed from session to session so that the security of the communications is not compromised.

If the owner of a vehicle wants to add a wireless device to the vehicle system for secured communications, then the owner must connect the wireless device (e.g. a PDA) to the NDM through the serial port or the infrared link. The owner will then enter a password through the keypad of the NDM. If the password is valid, then the NDM will send a set of keys (PINs), say \( k_1, k_2, k_3, \ldots \), to the connected device. After that, the activation of the device is completed for its lifetime.

Figure 4 shows the algorithm for activating a device by the NDM. Later on, these PINs will be used to establish secured communications. Similarly, other devices, which want to participate in secured communications, will be activated one at a time. The NDM will keep track, which set of keys have been sent to which device.

If a device wants to start a secured communication session, then first it must be authenticated by the NDM. For the authentication process, the NDM will be using the Bluetooth address of the device and one of the PINs that was sent earlier. PIN \( k_i \) will be used if this is the \( i \)th session after the activation of the device by the NDM. Only the NDM and this device know which PIN is going to be used for the authentication purpose. The NDM will then generate an encryption key, based on the current PIN, by using all the necessary algorithms (e.g. E0, E1, E2 ...) built in a Bluetooth device. The NDM and the device can use this encryption key, if they want to continue their secured communication. If another device wants to join in a secured communication, that device will also have to be authenticated by the NDM in a similar manner. When a device is going to be authenticated by the NDM using the last key of the set of keys that was sent to the device by the NDM at the time of activation, the NDM will send another set of new keys to the device to be used for future authentications.

Different devices may communicate with the NDM using different encryption keys, which were generated using their own PINs. Since all the secured devices, except the NDM, don’t know each other’s PIN, two secured devices will not be able to establish a secured communication without the help of the NDM.

The NDM will maintain a session key (another encryption key) for every secured communication session. Every time a new session is established, the NDM will send the session key to all the secured devices of that session. The NDM will send the session key to a device using the device’s own encryption key, that was determined earlier when the device was authenticated by the NDM. During the current session, all the secured devices will communicate among themselves using the session key received from the NDM. The current session will end, if every secured device stops communicating among themselves. At a later time, if the secured devices want to start another session, a new session key will be distributed to the secured devices by the NDM.
Our architecture will also protect the vehicle system from a security attack, using a lost or stolen device. If a device, which was originally activated by the NDM, is lost or stolen, then the owner of the vehicle can disable that device by using the password-protected keypad of the NDM. As a result, the stolen device will not be able to join in a secured communication without being re-activated by the NDM. For certain types of devices (e.g. a PDA and a laptop), additional security measures can be taken by requiring the users to enter a password through the keypad of the PDA or laptop, for the PDA or laptop to be authenticated by the NDM, respectively.

CONCLUSION

In this paper we have presented a technique to build secured wireless networks within a vehicle. Our technique can be implemented at a margin cost. The system can be easily used by all users. The only thing that a user has to know is the procedure for activating a new device by the password protected keypad of the Network Device Monitor.

ACKNOWLEDGMENTS

We would like to thank Mr. Mohammed Tarique for helping us in doing literature search and participating with us during the initial discussions about various aspects of collision avoidance.

REFERENCES


CONTACT

Dr. Syed Masud Mahmud has received his Ph.D. degree in Electrical Engineering from the University of Washington, Seattle. He published over 60 technical papers in refereed journals and conference. 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. Phone: (313) 577-3855, Email: smahmud@eng.wayne.edu.