Secure Wireless Vehicle Monitoring and Control

Huaqun Guo, Lek Heng Ngoh, Yong Dong Wu, and Joseph Chee Ming Teo
Institute for Infocomm Research, A*STAR
1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632
Email: {guohq, lhn, wydong, cmteo}@i2r.a-star.edu.sg

Abstract—The availability of real-time CAN-ECU data and the emerging vehicular networks are critical for advanced vehicle monitoring and control. This paper presents our integrated info-security scheme, real-time hardware/software solutions and their application scenarios. The core is the Integrated Info-Security Circuit Board to communicate with ECUs and sensors inside a vehicle through CAN Bus, LIN Bus, FlexRay and MOST Bus with wire interfaces, and to communicate with other vehicles, road-side infrastructure and mobile phones with wireless interfaces. We have built the first prototype with two circuit boards which communicate directly with CAN network and process CAN messages. One circuit board is used for monitoring and control Vehicle Functions via real-time CAN messages, while another circuit board is used to monitoring and control vehicle itself to against the theft. The demonstrations in the first prototype show that our solutions work very well.

Keywords—Vehicle Monitoring and Control; Controller Area Network; Circuit Board; Anti-theft; Integrated Info-Security

I. INTRODUCTION

Information technology is the driving force behind innovations in the automotive industry. In recent years, control systems of automobiles have moved from the analog to the digital domain. In particular, x-by-wire systems are appearing and have driven research efforts of the whole automotive industry for the recent decade. Networked Electronic Control Units (ECUs) are increasingly being deployed in automobiles to realize diverse functions such as engine management, airbag deployment, and even in intelligent brake systems. For example, at least 70 networked ECUs are employed in a Mercedes S-Class car [1, 2].

In automotive electronics, an ECU is an embedded system which controls one or more of the electrical systems or subsystems in a vehicle. Output signals from an ECU contain information about the current state of the vehicle as the driver interacts continuously with the vehicle. Some of these ECUs are independent, but communication between ECUs is essential. An actuator control ECU may need to receive data from an input ECU. For example, the brake light will be turned on when a driver steps on the brake.

Due to the complexity of the modern vehicle design, the Intra-Vehicle (InV) networks are requested for communications among ECUs. Among number of InV networks, CAN (Controller Area Network) [3] is typically used by the most car manufacturers. Furthermore, the emerging Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructures (V2I) communications are quickly becoming reality. DSRC (Dedicated Short Range Communication) [4] is the recent technological trends to support both public safety and private operations for V2V and V2I communication environments. The examples of InV, V2V and V2I are shown in Fig. 1 [5].

In Fig. 1, InV provides communications among ECUs and sensors within a vehicle while V2V and V2I provide communications among nearby vehicles and between vehicles and nearby fixed roadside equipments. By enabling vehicles to communicate with each other via InV communication, the emerging vehicular networks will contribute to safer and more efficient road usage by providing timely information to drivers and concerned authorities. The availability of real-time CAN-ECU data and the emerging vehicular networks are critical for advanced vehicle telematics such as, active safety, traffic efficiency, driver assistance, infotainment, remote diagnosis, etc.

Figure 1. Example of InV, V2V and V2I communications.
Thus, the primary objective of this paper is to design an Integrated Info-Security scheme and develop real-time hardware/software solutions that interface and communicate directly with CAN network and process CAN messages for secure wireless vehicle monitoring and control purposes.

The rest of paper is organized as follows. Section II introduces related CAN and DSRC technologies. Section III describes the proposed integrated info-security while its application scenarios are introduced in Section IV. Section V presents the initial prototype. Finally, Section VI outlines our conclusions and future works.

II. RELATED TECHNOLOGIES

A. Controller Area Network (CAN)

To add new functionality and reduce the design and wire cost, the CAN protocol was introduced by Robert Bosch GmbH in 1986 [6]. CAN is a multicast shared serial bus system for connecting ECUs. Each controller connected to the network is called a node and is able to transmit and receive messages from the network. CAN was specifically designed to be robust in electromagnetically noisy environments.

The CAN bus is based on the “broadcast communication mechanism”, which is based on a message-oriented transmission protocol. This means that all nodes can “hear” all transmissions. There is no way to send a message to just a specific node; all nodes will invariably pick up all traffic. The CAN hardware, however, provides local filtering so that each node may react only on the interesting messages. Every CAN message has a message identifier, which is unique within the whole network since it defines content and also the priority of the message. The priorities are laid down during system design in the form of corresponding binary values and cannot be changed dynamically [3].

The CAN standard further defines four different message types.

- **Data frame**: a frame containing node data for transmission
- **Remote frame**: a frame requesting the transmission of a specific identifier
- **Error frame**: a frame transmitted by any node detecting an error
- **Overload frame**: a frame to inject a delay between data and/or remote frames

The messages use a scheme of bit-wise arbitration to control access to the bus, and each message is tagged with a priority. A CAN message transmitted with highest priority will ‘win’ the arbitration, and the node transmitting the lower priority message will sense this and back off and wait. This is achieved by CAN transmitting data through a binary model of “dominant” bits and “recessive” bits where dominant is a logical 0 and recessive is a logical 1. If one node transmits a dominant bit and another node transmits a recessive bit, then the dominant bit “wins” (a logical AND between the two).

So, if you are transmitting a recessive bit, and someone sends a dominant bit, you see a dominant bit, and you know there was a collision. (All other collisions are invisible.) The way this works is that a dominant bit is asserted by creating a voltage across the wires while a recessive bit is simply not asserted on the bus. If anyone sets a voltage difference, everyone sees it, hence, dominant. Thus, there is no delay to the higher priority message, and the node transmitting the lower priority message automatically attempts to re-transmit 6 bit clocks after the end of the dominant message.

If two or more devices start transmitting at the same time, there is a priority based arbitration scheme to decide which one will be granted permission to continue transmitting. The CAN solution to this is prioritised arbitration (and for the dominant message delay free), making CAN very suitable for real time prioritised communications systems.

B. 2.2 DSRC

Within IEEE 802.11, DSRC is known as IEEE 802.11p WAVE [7]. DSRC standards and communication stack are shown in Fig. 2 [5, 7].

IEEE 802.11p is not a standalone standard. It is intended to amend the overall IEEE 802.11 standard. IEEE 802.11p is based on its predecessor ASTM Standard E2313-03, and it is draft standard currently. IEEE 802.11p is a draft amendment to the IEEE 802.11 standard to add wireless access in vehicular environments. It defines enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE) is a higher layer standard on which IEEE 802.11p is based [8]. 802.11p will be used as the groundwork for DSRC. IEEE 802.11p supports physical layer management entity (PLME), lower MAC (Medium Access Control) layer management entity (L_MLME), Wireless Access in Vehicular Environments physical layer (WAVE PHY) as well as WAVE lower MAC in DSRC technology.

III. INTEGRATED INFO-SECURITY

Components of the proposed solutions for secure vehicle monitoring and control are shown in Fig. 3. The core is the Integrated Info-security Circuit Board with wire interfaces and wireless interfaces. Within a vehicle, the Circuit Board will communicate with sensors and CAN Bus, LIN Bus [10], FlexRay [11] and MOST (Media Oriented Systems Transport) Bus [12] through gateways. With wireless interface, the Circuit Board will have a capability to communicate with other vehicles, road-side infrastructure and mobile phones.

In the core, the project will design and develop an Integrated Info-Security Circuit Board with wire interfaces, and wireless interfaces. The Circuit Board must be tamper-proof and will take care of storing all the cryptographic material and performing cryptographic operations, especially signing and verifying safety messages. Furthermore our solutions will embed trust for device security. These solutions will be prototyped and tested with a single-board computer equipped with interface to internal vehicle networks and wireless communication capabilities with an aim to ensure that data exchanged with-inside and with-outside the vehicle is protected from abuse and security attacks.

IV. APPLICATION SCENARIOS

With the advent of Vehicular Ad-Hoc Network that allows vehicles within reasonable proximity to connect wirelessly to one another via DSRC, vehicles are able to share information with each other.

An example is to use extracted CAN messages from vehicles to establish the reliable route for messages to take in order to reach its destination. We describe a scenario where many cars are travelling along a highway (Fig. 4). Cars that will turn right will signal right, hence effectively dividing the cars into two groups. If the CAN messages that govern the signaling lights are collected and then sent to other cars still travelling along this highway, these “peers” are thus now wiser in constructing the reliable data route to relay messages among themselves. With this information they can exclude all cars belonging to the other group – cars that are exiting the highway [13].

Other examples could be extracting CAN data about the current state of vehicle for real time diagnosis and recording CAN data in a black box for post accident analysis.

V. SOLUTIONS & PROTOTYPE

We have built the first prototype of secure wireless vehicle monitoring and control (Fig. 5). In this prototype, two circuit boards have been designed to interface with CAN Bus and ECU nodes.
A. Circuit Design for CAN Bus Monitoring and Control of Vehicle Functions

This first circuit board is used for processing CAN messages and communicating with the Control Center via wireless communication. The circuit board can capture the real-time CAN messages and send them to the Control Center. Thus, the Control Center can monitor the current status of vehicle. The Control Center can also send the command CAN message to the circuit board to control the vehicle.

Fig. 6 shows the block diagram of circuit board which is within dotted lines. The circuit board mainly consists of two microcontrollers: dsPIC30F4012 and 18F2455 chips. The specifications of both chips are found in [14] and [15] respectively. The dsPIC30F4012 chip contains one CAN stack which provides the capability for the board to interpret CAN signal extracted from the CAN Emulator. Furthermore, transceiver chips (MCP2551) are required to connect the circuit board itself to the CAN bus. The extra MCP2515 chip provides a second CAN interface to the circuit board. Thus, the circuit board can access two CAN buses at any one time. The 18F2455 chip is responsible for maintaining the USB (Universal Serial Bus) connection from the circuit board to the Host PC. Data are transferred between the dsPIC30F4012 chip and the 18F2455 chip via the SPI (Serial Peripheral Interface) interface. SPI is a synchronous full duplex data link that transfers data serially between two chips. The software algorithms are firmware programmed for the dsPIC30F4012 and 18F2455 microcontrollers.

Fig. 7 shows the completed circuit board. The RS232 serial port interface, which can be clearly seen in the figure, transfers core dumps to a terminal that aids in debugging during the design process.

The capturing real-time CAN messages are shown in the monitoring GUI (Fig. 8). It captures a total of 26 different CAN messages that are being sent around by the ECUs on the CAN Emulator. In this way, it monitors the current state of the vehicle.

The control CAN message can also be sent out to control a vehicle. Besides the manual input of control CAN messages, the command control tab gives users convenience to control over various functionalities of the CAN Emulator with the simple clicks of buttons. For example, when a user clicks the Signal Left button, the CAN messages for Signal Left is sent to the CAN Emulator and causes the left signal lights on the CAN Emulator to light up; when the user clicks the Wiper Low button, the CAN messages for Wiper Low is sent to the CAN Emulator and the logo is turning to emulate the wiper moving (Fig. 9).

Figure 5. The first prototype of secure wireless vehicle monitoring and control.
B. CAN-based Solution for Anti-theft

We have also built another circuit board (Fig. 10). We use a single board computer (SBC), Soekris Net4801, to act as a core platform. D-Link DWL-G520 wireless card and iTegno GPRS modem are connected to Soekris Net4801. Soekris Net4801 also has serial port interface that connects to networked ECUs inside a vehicle. Finally, Gentoo Linux is adopted as OS (operating system) for the SBC because of its ease of usage, configuration and updatability. C programs is been developed to realize the communication between ECUs to SBC and SBC to GPRS modem.

The purpose of this circuit board is to make security in CAN bus systems by using embedded device security and cryptography. This solution provides vehicle physical security through tamper-resistant software in embedded devices for the protection of vehicle components and their ECUs. [16]. This circuit board is used to monitoring and control vehicle itself to against the theft. Once an owner realizes his vehicle is lost, all he needs to do is to send a “Stop engine” SMS from his mobile phone to a secret and specific phone number which is dedicated to the electronics on the vehicle. The circuit board will send the disable CAN message to the CAN bus so that the vehicle cannot be started again after it stops. If someone tampers the security system in a vehicle, the circuit board will send an alert...
message to inform the owner. The owner mobile phone can also automatically forward the alert message to inform the Control Center. With our solution, the owner has the monitoring and control capability even after his vehicle is lost.

In order to determine the feasibility of the proposed solution, we conducted experiments by measuring time $T_1$ taken from the mobile phone sending out a “Stop engine” message to ECUs disabling the engine to be started. We also took time measurements in the software to determine time $t_2$ from the time GPRS modem receiving the message to when the ECUs disables the engine. Furthermore, since we embed security features in ECUs, if an ECU is being tampered, the security system will send out the alert message via the GPRS modem at once to inform the owner. Thus, we also measured time $T_2$ from when an ECU is tampered to when the mobile phone receives the alert SMS message. We further measure time $t_4$ from when an ECU is tampered to when the GPRS modem sends out an alert message. Therefore, $(T_1 - t_2)$ and $(T_2 - t_4)$ are the messages communication time between mobile phone and GPRS modem. The experimental results are shown in Table I. We conducted each of the experiments five times and the value in the last row is the average time of the five experiments. From the results, it is clear that the time spent in our embedded software is relatively low, thus we conclude that the proposed anti-theft solution is technically feasible and under normal circumstances, the owner can securely control his vehicle within a few seconds.

<table>
<thead>
<tr>
<th>TABLE I.</th>
<th>TIME MEASUREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stop Engine</strong></td>
<td></td>
</tr>
<tr>
<td>$T_1$ (second)</td>
<td>$t_2$ (second)</td>
</tr>
<tr>
<td>6.6</td>
<td>2</td>
</tr>
<tr>
<td>5.5</td>
<td>1</td>
</tr>
<tr>
<td>8.5</td>
<td>1</td>
</tr>
<tr>
<td>4.7</td>
<td>1</td>
</tr>
<tr>
<td>8.6</td>
<td>3</td>
</tr>
<tr>
<td><strong>6.78</strong></td>
<td><strong>1.6</strong></td>
</tr>
</tbody>
</table>

| **Tamper Detection** |  
| $T_1$ (second) | $t_2$ (second) | $(T_1 - t_2)$ (second) |
| 12.8 | 4 | 8.8 |
| 12.3 | 4 | 8.3 |
| 12.4 | 4 | 8.4 |
| 14.7 | 4 | 10.7 |
| 14.9 | 4 | 10.9 |
| **13.42** | **4** | **9.42** |

VI. CONCLUSIONS

Networked ECUs are increasingly being deployed in automobiles to realize various functions and CAN network is used for the communications among ECUs. The availability of real-time CAN-ECU data and the emerging vehicular networks are critical for advanced vehicle monitoring and control.

This paper presents our integrated info-security scheme, real-time hardware/software solutions and their application scenarios. The core is the Integrated Info-Security Circuit Board with wire interfaces and wireless interfaces. Within a vehicle, the Circuit Board will communicate with sensors and CAN Bus, LIN Bus, FlexRay and MOST Bus through gateways. With wireless interface, the Circuit Board will have a capability to communicate with other vehicles, road-side infrastructure and mobile phones. We have built the first prototype of secure wireless vehicle monitoring and control with two circuit boards. One circuit board is used for monitoring and control Vehicle Functions via real-time CAN messages. Another circuit board is used to monitoring and control vehicle itself to against the theft. The demonstrations in the first prototype show that our solutions work very well.

In the near future, we will continue working on integrated Info-Security solutions such as data timeliness and minimize network delays to realize reliable secure car communications.

REFERENCES


