Featured Articles

Security Operation Management Initiatives in Cooperative Vehicle-Infrastructure Systems for Safe Driving

Akira Mizutani
Mai Kawamura
Eriko Ando
Toru Owada

OVERVIEW: There has been growing awareness in recent years of the potential for the implementation of self-driving vehicles to deliver benefits such as reducing traffic accidents and alleviating congestion. The techniques for obtaining the information about the surrounding environment that is required for autonomous driving include autonomous techniques, which obtain information from the vehicle's own sensors, and cooperative techniques, which obtain information from external sources via wireless communications. Japan has reserved the 700-MHz band for wireless communications using cooperative techniques, and work is progressing on implementing a 700-MHz CVIS to support safe driving using this band. This article describes Hitachi's work on the 700-MHz CVIS and its views on the future of ITS.

INTRODUCTION

THERE has been growing awareness in recent years of the potential for the implementation of self-driving vehicles to deliver benefits such as reducing traffic accidents and alleviating congestion. Autonomous driving involves onboard systems that perform the awareness, decision-making, and actuation functions that were previously performed by the human driver.

Progress is being made on the implementation of autonomous techniques for recognition by onboard systems that use cameras, radar, or other vehicle-mounted sensors. The problem with using autonomous techniques for autonomous driving is how to obtain, at an early stage, the sort of information that conventional sensors find difficult to acquire, such as what is happening out of sight, around a corner, or at an intersection, for example. In response, investigations are being conducted into cooperative techniques for obtaining information about what is happening outside the area that is visible from the vehicle by using wireless communications with roadside and other infrastructure, or with other vehicles.

Japan has reserved the 700-MHz band[(1)] for wireless communications using cooperative techniques, and work is progressing on implementing a system that provides driver assistance services using this band (hereinafter referred to as the "700-MHz cooperative vehicle-infrastructure system" or "700-MHz CVIS").

The provision of information to vehicles via wireless communications is intended foremost to enhance things like safety and environmental functions and performance. Vehicles that are equipped with sensors, actuators, wireless communications, and other such functions can be thought of as Internet of things (IoT) devices, with significant potential for being used as a means of collecting data in big data systems.

In other words, by using cooperative techniques to utilize the data (position and speed, etc.), communication logs, and other information from vehicles as big data, Hitachi believes that further advances are possible in intelligent transport systems (ITSs), such as the monitoring and control of traffic flows over wide areas in realtime (see Fig. 1).

This article describes Hitachi's work on the 700-MHz CVIS and its views on the future of ITS.

DEVELOPMENTS RELATING TO 700-MHZ CVIS

The 700-MHz CVIS works by using communications between vehicles and between roadside infrastructure and vehicles to exchange vehicle information and infrastructure information (signal information, regulation information, pedestrian information, etc.), to help ensure driving safety by warning the driver of hazards such as the approach of other vehicles at intersections or the approach of emergency vehicles.

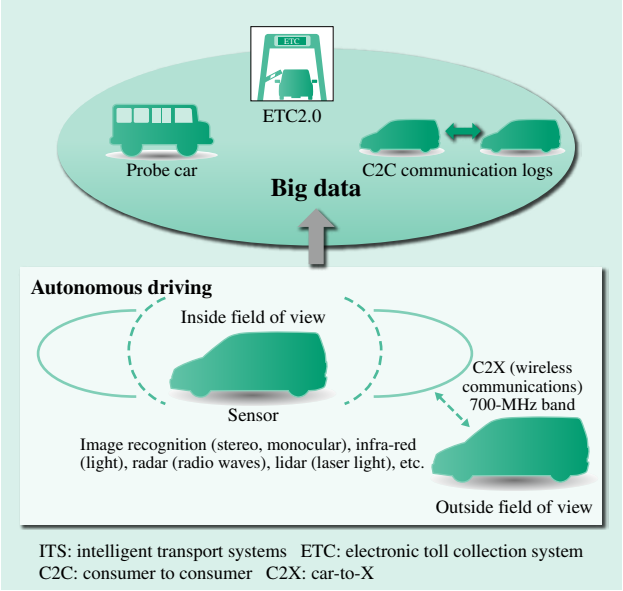

Fig. 1—Hitachi's Vision for Future ITS.
Future ITSs will create new value by utilizing the information collected from vehicles using both autonomous and cooperative techniques as big data.

Examples of services that could be implemented using this system include helping to avoid collisions when turning or when entering or passing through an intersection, helping with awareness of nearby vehicles such as providing notification of approaching ambulances or other emergency vehicles, or providing information about passengers getting on or off a bus[2], with the potential to significantly decrease the frequency of traffic accidents due to inattention or bad decisions by drivers.

On the other hand, because these systems handle information associated with driver awareness and decision making, they need to take account of cyber-attacks and incorporate adequate protection.

One example involving the 700-MHz CVIS is the potential for causing confusion among other road users if someone with malicious intent causes incorrect vehicle data to be transmitted in an attempt to pass their vehicle off as an emergency vehicle[3]. To prevent this, information exchanged via the 700-MHz band needs to adopt countermeasures including proof of integrity such as an electronic signature or message authentication code (MAC). The maintenance of security also requires the management of resources such as the keys used to generate and verify electronic signatures or MACs[4].

In preparing for the introduction of the 700-MHz CVIS, the Ministry of Internal Affairs and Communications of Japan published the Security Requirements for 700 MHz Band Driving Safety Support Systems[5] (hereinafter referred to as the "Security Requirements") in June 2014 and the Security Guidelines for Construction of 700 MHz Band Safe Driving Support System[6] (hereinafter referred to as the "Guidelines") in July 2015. The Security Requirements specify requirements for the entities (onboard system vendors, etc.) involved in the implementation and management of the 700-MHz CVIS. The Guidelines specify policies for implementing the 700-MHz CVIS based on the Security Requirements. Demonstration projects have also been undertaken under the Development of V2V, V2I Communication Technology toward the Automated Driving Systems[7] FY2014 Cross-ministerial Strategic Innovation Promotion Program (SIP) established by the Cabinet Office, and the subcontracted investigation of communication technologies toward the establishment of next-generation ITS[8], a Ministry of Internal Affairs and Communications budget process. In the private sector, the ITS Connect Promotion Consortium was established in October 2014 to promote the implementation and widespread adoption of the 700-MHz CVIS. The activities of the Consortium have included technical discussions on the security specifications required to satisfy the Security Requirements and support for operational management (see Fig. 2).

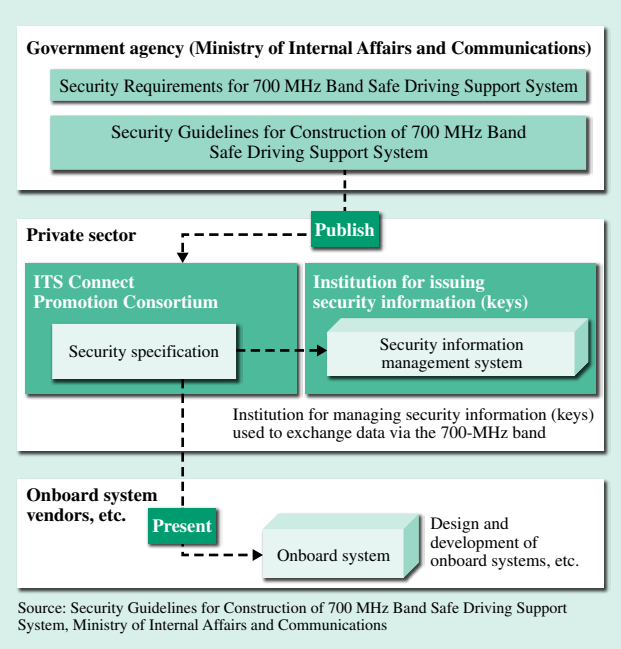

Fig. 2—Public- and Private-sector Developments in Security for the 700-MHz CVIS.
The introduction of the 700-MHz CVIS is progressing through collaboration between the public and private sectors.

As a result of these efforts, preparations for the 700-MHz CVIS are proceeding and introduction of the service is imminent.

SECURITY OPERATION MANAGEMENT INITIATIVES FOR 700-MHZ CVIS

This chapter describes Hitachi's work on system security operation management aimed at helping encourage the wider adoption of the 700-MHz CVIS.

Past Work by Hitachi

Hitachi has been involved in work on specification reviews and the implementation of security operation management in the lead up to commercialization of the 700-MHz CVIS.

(1) Participation in ITS Connect Promotion Consortium

As a member of the ITS Connect Promotion Consortium, Hitachi has participated alongside other members in a review of the specifications of systems for managing keys and other security resources (security information management systems) and a study of security management schemes, including people's movements.

(2) Work as a system vendor

In its role as a system vendor, Hitachi has developed a security information management system that complies with the ITS Connect Promotion Consortium specifications. This development was based on an analysis of potential threats and drew on Hitachi's know-how from similar systems in the ITS field. Hitachi is also looking at management procedures that are based on the management schemes defined by the ITS Connect Promotion Consortium.

Upcoming Hitachi Activities

As noted in the introduction to the Security Requirements, implementing appropriate countermeasures that keep up with changing social and technical factors is important to maintaining and improving security[5]. In response to the need to maintain and improve the security of the social infrastructure that underpins public and corporate (economic) activity, Hitachi has devised and is working on the implementation of Hitachi's concept for social infrastructure security[9].

This section describes security operation management for the 700-MHz CVIS in terms of Hitachi's concept for social infrastructure security and the key issue of responsiveness that Hitachi will consider proposing in the future (see Fig. 3).

Overview of Hitachi's Concept for Social Infrastructure Security

Hitachi's concept for social infrastructure security identifies trends associated with social infrastructure security: the growing diversity of threats, the importance of post-incident follow-up, and the expanding scale of interdependence, and focuses on the three requirements of adaptability, responsiveness, and cooperativeness.

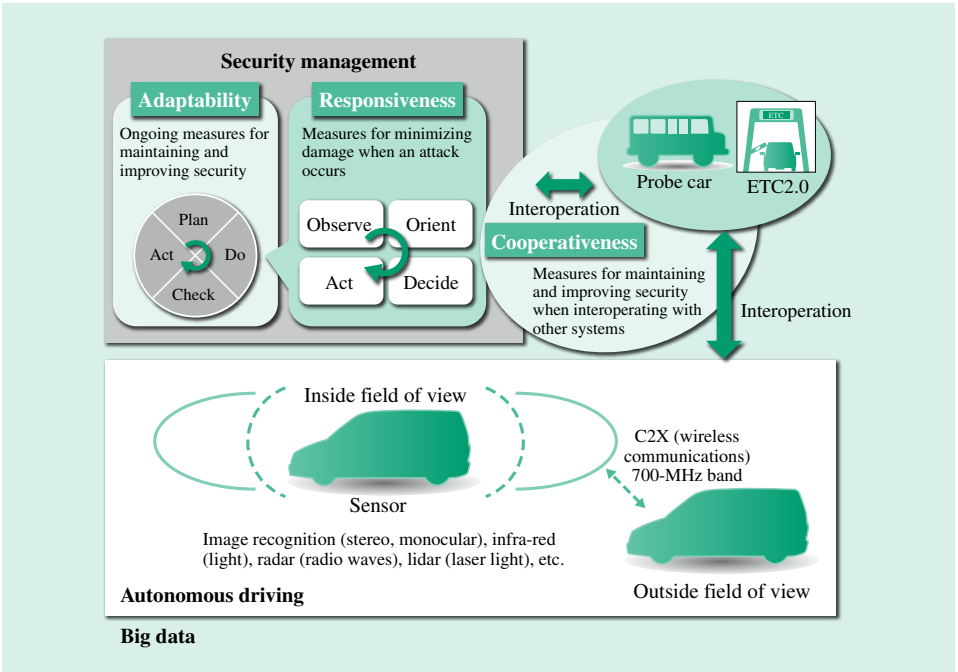

Fig. 3—Hitachi Proposal based on its Concept for Social Infrastructure Security. Hitachi is proposing an approach to security management, based on its concept for social infrastructure security, which considers the medium- to long-term development of the 700-MHz CVIS.

(1) Adaptability

Dealing with increasingly diverse threats that include more sophisticated forms of attack requires ongoing measures utilizing the well-known plan, do, check, act (PDCA) method of security management. Because of the significant potential impact of an attack on social infrastructure, it is important to adopt a philosophy of defense in depth and to work through the PDCA cycle for each layer of the system (cyberspace, physical space, and operational management).

(2) Responsiveness

As unexpected attacks can still occur even when pre-emptive countermeasures are in place, it is important to minimize the damage when an attack occurs and quickly restore operation.

To achieve responsiveness, Hitachi has adopted the observe, orient, decide, and act (OODA) loop concept of operational management.

(3) Cooperativeness

In general, social infrastructure systems operated by different service providers and other organizations are increasingly linked together to improve the convenience and efficiency of services. As this makes centralized system management difficult, an attack on one system can have major impacts on other systems. Accordingly, it is important to take steps to minimize damage by having service providers and other organizations cooperate with each other and share a common situational assessment.

700-MHz CVIS Considered in Terms of Hitachi's Concept for Social Infrastructure Security

This section describes work on the adaptability, responsiveness, and cooperativeness of the 700-MHz CVIS in its role as part of the social infrastructure.

(1) Adaptability

The implementation of the 700-MHz CVIS will expose vehicles to risks from a new type of threat. As noted above in "Developments Relating to 700-MHz CVIS," the public and private sectors have been collaborating in preparation for the commencement of 700-MHz CVIS services, working on the "plan" and "do" aspects of security that are necessary for introducing services by identifying requirements that encompass not only cyberspace, but also physical and operational management considerations; reviewing security specifications; and studying management schemes. Once services are up and running, Hitachi intends to propose activities to the ITS Connect Promotion Consortium that cover the "check" and "act" aspects.

(2) Responsiveness

The wider adoption of the 700-MHz CVIS will increase motivation for attacks, which will likely include some of an unanticipated nature. In preparation for the wider use of the 700-MHz CVIS, Hitachi is collating requirements with a view toward proposing security information management systems that incorporate the OODA loop concept. Details are described below.

(3) Cooperativeness

As noted in the introduction, the 700-MHz CVIS is likely to undergo further development in the medium and long term involving greater integration with other systems. In preparation for this more extensive interoperation between systems, Hitachi intends to start looking at techniques for ensuring that systems are cooperative.

Hitachi's Proposal for "Responsiveness" Based on the Company's Concept for Social Infrastructure Security

As noted above, Hitachi is collating requirements for security information management systems that incorporate the OODA loop concept.

(1) Observe

The collection of communication logs from onboard systems and roadside infrastructure will be required to determine the status of the 700-MHz CVIS. Hitachi is undertaking studies and other work looking at things like what data is required for analysis, considering such issues as the impact of driver assistance services that require realtime performance and the processing load on onboard systems.

(2) Orient (situation assessment)

To minimize the damage when an attack occurs, it is necessary to quickly detect unconventional attacks or other failures and accurately assess or predict the damage. To achieve these, Hitachi is undertaking studies with a view to using business intelligence (BI) tools and its own technology for high-speed data access platforms.

Depending on the data being collected, privacy may also be an issue. Hitachi is working on the research and development of privacy technologies such as k-anonymization and searchable encryption, and looking at how they can be deployed.

(3) Decide

To choose the best countermeasures to adopt, it is necessary that the results of analysis (damage updates and urgency, etc.) be presented visually. To achieve this, Hitachi is collating what information other than analysis results is needed for decision making

(available countermeasures, etc.) and investigating matters such as how to present it.

(4) Act

To find ways to implement the action chosen by the "observe," "orient," and "decide" process, it is essential that the entities involved in operation and management of the 700-MHz CVIS coordinate with each other. The importance of coordination between entities when an incident occurs has also been highlighted for the Security Requirements, and Hitachi is working on incident response measures in collaboration with the relevant entities through the ITS Connect Promotion Consortium.

CONCLUSIONS

A variety of studies are underway as part of moves toward the introduction of autonomous driving. This article has described what Hitachi is doing in relation to the use of cooperative techniques for security operation management of the 700-MHz CVIS, and its plans for the future. Hitachi is contributing to the wider adoption and development of the 700-MHz CVIS by working on security operation management based on its concept for social infrastructure security.

In the future, Hitachi also plans to pursue the potential for creating useful information and extending the technology to applications such as using the collected log data for things like planning roads, detecting faulty roadside infrastructure, and investigating the cause of accidents and other incidents.

REFERENCES

(1) Association of Radio Industries and Businesses (ARIB), "700 MHz Band Intelligent Transport Systems," ARIB Standard STD-T109 1.2 (Dec. 2013), http://www.arib.or.jp/english/html/overview/doc/1-STD-T109v1_2.pdf in Japanese.

(2) ITS Connect Promotion Consortium, https://www.itsconnect-pc.org/en/

(3) ITS Info-communications Forum, "Security Guidelines for Driver Assistance Communications System," ITS FORUM RC-009 1.2, (Nov. 2013), http://www.itsforum.gr.jp/Public/J7Database/p41/ITS_FORUM_RC009V1_2.pdf in Japanese.

(4) ITS Info-communications Forum, "Operation and Management Guidelines for Driver Assistance Communications System," ITS FORUM RC-008 1.0 (Apr. 2011), http://www.itsforum.gr.jp/Public/J7Database/p38/ITS_FORUM_RC008V1_0.pdf in Japanese.

(5) Ministry of Internal Affairs and Communications, "Security Requirements for 700 MHz Band Safe Driving Support System (Rev. 1.0)," (Jun. 2014), http://www.soumu.go.jp/main_content/000297761.pdf in Japanese.

(6) Ministry of Internal Affairs and Communications, "Security Guidelines for Construction of 700 MHz Band Safe Driving Support System (Rev. 1.0)," (Jul. 2015), http://www.soumu.go.jp/main_content/000367888.pdf in Japanese.

(7) Ministry of Internal Affairs and Communications, "Lecture & Exhibition: ICT for Next Generation ITS," "Development of Vehicle-Vehicle Communications and Vehicle-Infrastructure Communications Technologies for Autonomous Driving System," (Mar. 2015), http://mic-its-conference-2015.net/data/pdf/06_ja.pdf in Japanese.

(8) Ministry of Internal Affairs and Communications, "Lecture & Exhibition: ICT for Next Generation ITS," "Contract Study of Communications Technologies for Establishing Next-generation ITS," (Mar. 2015), http://mic-its-conference-2015.net/data/pdf/11_ja.pdf in Japanese.

(9) M. Mimura et al. "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).

ABOUT THE AUTHORS

Akira Mizutani

Intelligent Transport Systems Business Promotion Center, Government & Public Corporation Information Systems Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in the development of ITS-related systems.

Mai Kawamura

Intelligent Transport Systems Business Promotion Center, Government & Public Corporation Information Systems Division, Information & Telecommunication Systems Company, Hitachi, Ltd. She is currently engaged in the development of ITS-related systems.

Eriko Ando

Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. She is currently engaged in research into information security for automotive systems. Ms. Ando is a member of the Information Processing Society of Japan (IPSJ) and The Institute of Electrical Engineers of Japan (IEEJ).

Toru Owada

Intelligent Transport Systems Business Promotion Center, Government & Public Corporation Information Systems Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in research into information security for automotive systems. Mr. Owada is a member of The Institute of Electronics, Information and Communication Engineers (IEICE).