Acta
Technica
Jaurinensis

Vol. 9, No. 3, pp. 216-236, 2016
DOI: 10.14513/actatechjaur.v9.n3.419
Available online at acta.sze.hu

Enhancing Traffic Safety with Mobile Applications

H. Kaartinen, J. Jämsä

Centria University of Applied Sciences, Research and Development
Vierimaantie 7, 84100 Ylivieska, Finland
Phone: +358 40 729 9951
e-mail: heidi.kaartinen@centria.fi

Abstract: Intelligent Transportation Systems (ITS) have great potential and market on modern traffic environment. Technologies of the day enable the real-time data transfer and presentation for the actors in traffic and outside of it. Inter-cognitive communication is a form of communication where an information system gathers data and processes it to a form of which users can benefit on their decision making. In this paper we will present how deploying new cognitive elements on mobile applications can increase traffic safety. The most important point of view in sharing the traffic data is how to present it for the driver and how to make the data transfer reliable and safe. New vehicles have built-in solutions, such as comprehensive infotainment systems, to present the information and warnings, but older vehicles do not have this option. Therefore the modern devices, such as smartphones and tablet computers can be utilized for these purposes. This paper describes Centria's research work on developing mobile applications for improving the traffic flow and safety by real-time support for the driver's decision making. Also, the data security has been studied and tested at Centria, and will be reported in this paper.

Keywords: 4G/LTE; 802.11p; AES-128; ITS; V2I; adaptive user interface; authentication; vehicular communication; situation awareness; encryption

1. Introduction

Cognitive infocommunications (CogInfoCom) creates a link between human and device, where information systems assist human decision making [1]. Modern vehicles have many factory-installed communication technologies and sensors in them. Using these technologies, the vehicles are connected to the networks to receive external information as well as to provide data to the others. Infotainment systems with large displays enable viewing the data from external sources and from the vehicle itself for driver to use for making decisions in the traffic. Still, there are some issues to be taken into account, when utilizing these technologies.

The general theme of this paper is safety – but when it comes to traffic applications, there are multiple points of views in safety. In creating the applications for drivers, the goal of Centria University of Applied Sciences (hereafter Centria) has been to provide information for drivers for them to make better driving decisions and therefore improve the safety of traffic. This data has to be presented for the driver in as safe way as possible, so that the viewing of the traffic information will not distract the driver's observation on traffic. Lately, the research of Centria has focused increasingly on traffic applications for authorities, such as emergency vehicles. This has evoked the specific need for the reliable solutions of data security.

Information technology (IT) point of view divides reliability into two categories: the safety and security of IT systems. Safety of IT systems is provided by the protection against technical failures. Such failures can occur on e.g. power feed. Also, unbreakable connections to the communications network, are an essential part of data safety. Data security includes protection against attacks on the system. When connected to the network, vehicles use modern applications, and it is fundamental for them to immediately verify the validity of the received data. In case of emergency vehicle, the data security and safety are literally matters of life and death.

On its projects, Centria has built applications to connect the vehicles to the infrastructure (V2I) to receive and provide traffic data for decision making. On these applications, Centria has used Wireless Access in the Vehicular Environment (WAVE) radios as instruments of connection. Centria has designed simple and informative user interfaces for the applications in a way that they can be applied either on the vehicle's pre-installed infotainment systems or used on mobile device, such as a smartphone of a tablet computer. Also, testing of the encryption on WAVE has been executed lately by Centria.

2. Background

As been said before, the modern vehicles have many kinds of communication, sensor and visualization technologies installed in them, and providing of safety services is relatively simple. When designing and developing new traffic safety applications, the focus must be put above all on data security and drivers' safety as they use the applications. Also, the reliability of these services is crucial. When it comes to the services used by authorities, such as emergency vehicles, the service must be available and reliable at all times.

The Vehicular Ad hoc Network (VANET) is an unstructured network of vehicles communicating with each other. The vehicles form a network with each other, with roadside units and the Internet. VANET uses typically short range communication for the data transfer, but also cellular technologies are being used. WAVE radios operate on the dedicated short-range communication (DSRC) 5.85–5.925 GHz bandwidth. WAVE has two sets of protocols for connections, IEEE 802.11p for physical and MAC layers and IEEE 1609.x for security and connection management [2].

Havelt and Oliviera divide the use of VANETs into safety applications and non-safety applications. Safety applications include features to help drivers on executing the tasks of driving. Such features are e.g. drive-assisting solutions and automated message signs. Non-safety applications include road tolls etc. The authors have also compiled the protocols and standards of WAVE into one table (Table 1) [3].

Table 1. WAVE Standards [3]

Protocols	***Standards***		***OSI Layer***
WAVE PHY and MAC	IEEE 802.11p	PHY and MAC functions for an IEEE 802.11p device to function in a vehicular environment	Layers 1 and 2
Multichannel operation	IEEE 1601.4	Enhancements to the 802.11p MAC to support multichannel operation	Layer 2
WAVE Networking Services	IEEE 1609.3	Addressing and routing	Layers 2, 3, and 4
WAVE Resource Manager	IEEE 1609.1	Definition of the application that allows communication from remote sites to on-board units	-
WAVE Security Services	IEEE 1609.2	Secure messaging format and processing	-

IEEE standard 1609.2TM-2013 defines the methods for securing WAVE management messages and application messages. It acknowledges that many WAVE applications are safety-critical and the processed data must be authenticated and encrypted. The authentication is required to be scalable and flexible. The message is encrypted with AES-CCM with 128-bit keys, and Elliptic Curve Integrated Encryption Scheme (ECIES) is used as the encryption of the public key [4].

VANET requires authentication, plausibility, availability, non-repudiation, privacy, and real-time constraints for data security. The legitimacy of sent messages is evaluated by authentication of the senders and messages. Messages have to be consistent with similar ones to be legitimate. The availability of the data must be secured, if the network crashes. For this, the alternative communication methods are needed. The identification method of the vehicles sending the information must be reliable, but not intrusive towards individual privacy. The real-time data distribution enables the information to reach the driver in time [5].

Car-to-car (i.e. vehicle-to-vehicle, V2V) connections have been studied in the European PRESERVE project. In this research the possibility of attacks using the modules in the cars is brought up. In the worst case, the whole vehicle can be hijacked by a malicious person. The researchers of this study were also concerned about the autonomous vehicle solutions, on which combining of safety and security is a challenge. They also highlighted other objects of infrastructure, such as traffic lights, having an effect on traffic safety. These objects need robust built-in security applications to maintain the safety of the system. At this point the attacks against telematics applications are rare, but they are very likely to happen in the future. As the amount of vehicles with built-in technologies is increasing, the people willing to do harm within traffic will have a tempting situation ahead of them [6].

2.1. Data security

Wolf, Weimerskirch, and Wollinger describe the important protection methods against attacks in IT systems. Data security is based on encryption and decryption of the transferred data. Also, filtering, anomaly detection, and vulnerability scanning are essential for securing the data within the networks. The sent data is typically encrypted with symmetric or asymmetric cryptographies. Asymmetric cryptography uses a public key, and all the users with the public key can encrypt the data using it. Only the receiver of the data has a private key to decrypt the received data. In symmetric cryptography the sender and the receiver have the same secret key for encrypting and decrypting the data. This type of encryption is definitely secure, but the sharing of the key is a threat for data security. It also includes many keys to be stored securely for future use, as every communicating pair uses its own set of keys. Choosing the length of the key depends on the purpose of the encryption. Systems with public keys need longer keys than private-key systems, because the public-key systems are attacked with more force. The recommended key lengths for public and symmetric cryptographies are shown in Table 2 [7].

Table 2. Recommended Key Lengths for Cryptographies [7]

Security	***AES/DES***	***ECC***	***RSA***
Short-term	64 bits	128 bits	700 bits
Middle-term	80 bits	160 bits	1024 bits
Long-term	128 bits	256 bits	4096 bits

2.2. Related research on 802.11p and data security

The reliability of IEEE 802.11p-based vehicle-to-vehicle communications (V2V) was tested by Wang, Hu, Zhang, and Xu on Chinese expressway near Beijing. They confirmed that the reliability of IEEE 802.11p is affected by the road slope and traffic density. However, they did not take any data security issues into account. No encryption or authentication was used on the data transfer, and therefore their impact on data transfer was not reported [8].

Zhang, Boukerche, and Ramadan defined the transmission range of 208.11p to be only 1000 meters, which is relatively short. They claim the usability of this protocol not to be ideal for transmitting data. Also, the high speed of the vehicle requires the frequent switching of access points and sets special demands for the used protocols used. As the solution, a secure handoff with a lightweight authentication scheme is suggested. The authors' scheme suggests that access points and service providers are divided into groups with a group session key for authentication of the joining vehicle [9].

Biswas and Mišić have created an anonymous ID-based user authentication scheme and a cross-layer verification approach to 802.11p for the VANETs' safety messages. The scheme verifies the messages based on their MAC traffic class and traffic intensity, enabling the most important messages to be delivered, even in case of congested data traffic. The authors justified their approach to WAVE-enabled communications by conducting the security analysis and performance evaluation [10]. Tsai showed this scheme to be vulnerable to a private key reveal attack. He suggested a scheme based on the Elliptic Curve Digital Signature Algorithm (ECDSA) for supporting the authentication and non-repudiation. He claimed that this scheme can withstand such well-known attacks as the private key forging etc. In this scheme the identity revocation and trace are supported, and enables the verifier (OBU/RSU) to check if the received signature was generated by a revoked vehicle [11].

On their study, Kumar and Whyte reported a performance analysis of existing 1609.2 encodings using Abstract Syntax Notation 1 (ASN.1). They used four encoding alternatives and compared the encoding size and encoding/decoding time and claimed that using ASN.1 does not have a significant effect on performance. They proved that using Packet Encoding Rules (PER) or Octet Encooding Rules (OER) increases the size of the encoded message compared to 1609.2, but only slightly, and there is no significant difference between PER and OER encoded messages. The authors defined an acceptable duration for data transfer. The decoding of 1609.02 took about 0.2 % of the available time, whereas OER took 0.1–0.3 % [12].

As his bachelor's thesis on electrical engineering, Muikkula studied the 802.11p WAVE radios. A connection was established between two radios in his tests, but a compliant Intelligent Transport System (ITS) could not be established due to the lack of support standards. Muikkula used the UDP protocol of the Internet Protocol v.4 (IPv4) on the testing. He did not use any encryption in his testing, but acknowledged the data security standard of WAVE in his paper [13].

Table 3. Centria's DSRC Measurements on WAVE Radios [13]

Speed km/h	***Measurements***			
	Packets Sent pcs	Packets Received pcs	Throughput kbit/s	Goodput kbit/s
70	780.0	645.8	8.820	7.737
80	683.7	534.7	8.754	7.728
90	604.5	493.8	8.723	7.652
100	545.2	434.8	8.506	7.462

The Research and Development of Centria University of Applied Sciences has tested the impact of speed of the vehicle on the number of packets delivered on WAVE radios. Testing was done on the Ylivieska airfield, to have an opportunity to drive with a large variety of speeds without interfering the road traffic. Continuously numbered data packets were transmitted in the test to a moving vehicle's on-board unit (OBU) from a roadside unit (RSU) and the received data packets were analyzed. RSU was equipped with a global positioning system (GPS), and a 3G radio for connections to the infrastructure. The OBU had an Ethernet RJ-45 connection for the local area network (LAN) within the car, and a USB connector for the flash drive. The testing proved driving at higher speeds to decrease the number of packets that get through the connection. The maximum range of the data transfer (2000 meters) was also verified during the tests using a 12 dBi omnidirectional antenna. The executed tests have verified the WAVE radio equipment to be suitable for transferring traffic data. Table 3 presents the results of the DSRC measurements on Centria's tests [14]. During this test round no encryption was used. The WAVE radios were also tested by Centria on the rebuilt Tallinn-Tartu highway E263 in Kose, Estonia during the Celtic-Plus project Co-operative Mobility Services of the Future (CoMoSeF).

2.3. Related research on data gathering, sharing and presentation

According to CogInfoCom, data collecting and storing applications are infocommunication systems. These information systems can be evaluated by their cognitive capabilities – how they acquire and process data [15]. The solutions of traffic data acquirement and sharing feature the cognitive sciences and infocommunications, as they provide information for assisting the human decision making. Baranyi and Csapó describe the mode of communication to be either intra- or inter-cognitive communication. Intra-cognitive communication happens between two equal actors, such as two human beings – or two machines. Unequal communication takes place between a human being and an artificially intelligent system, two naturally unequal entities. Both actors of the communication need to share the same sensory modality and/or representation. For communication the actors need a common language [1].

An essential part of the design process for a traffic application's user interface is to make the functions and visualizations informative, but also as simple as possible to ensure the safe use of the application. Users should be able to observe and use the application so that they do not stop paying attention to the traffic.

Centria has been working on several projects to improve traffic safety by developing software and solutions for gathering and utilizing the traffic data. Modern mobile devices, such as tablets and smartphones, enable the possibility of acquiring and distributing real-time traffic information. Smartphones are physically right size and include universal interfaces, many usable sensors and connection options that provide a foundation for various applications. Gartner reported more than 1.2 billion smartphones sold during 2014, of which the vast majority (one billion) use the Android operating system [16]. Utilizing the existing mobile devices for distribution of the applications increases the coverage among drivers. There is no actual need for launching a new, possibly high-priced device.

Big data gathered from the sensors of vehicles and smartphones is a perfect source of real-time traffic-related information for the purposes of traffic safety. Gathering and sharing traffic-related data require an infrastructure of mobile technologies for data transfer and modification of sensor data into warnings and notifications. Some research has been done lately in this field and various research projects have studied sensors, technologies and connections. Shi and Abdel-Aty claim that data mining methods have high accuracy in predicting traffic events, such as car crashes [17]. The processes that refine this huge amount of data must be fast, efficient and reliable, in addition to the above mentioned data security issues.

Manolopoulos, Tao, Rodriguez, and Rusu have studied using mobile devices as sensors for gathering traffic data and providing real-time congestion information to drivers [18]. Their model provides the driver with personalized and dynamic information for supporting driving decisions. The study also acknowledges the great prospects of using the large screens of modern smartphones for presenting information to the driver.

Various projects have tested the connections, middleware and hardware for improving traffic safety. In Swedish tests, 3GPP LTE connections were proven feasible for traffic broadcasting [19]. However, the amount of traffic is an issue to be addressed, since in an urban environment with data congestion the delays in the data transfer will increase.

Bai and Krishnan tested the reliability of dedicated short-range communication (DSRC) based on an 802.11p connection for V2V data transfer [20]. Their conclusion is that the method is sufficient and reliable enough for the purpose. Cailean, Cagneau, Chassagne, Popa and Dimian also studied DSRC communication and compared it with visible light communication (VLC) [21]. As a result, they claim VLC to be more reliable in heavy traffic, but the coverage of DSRC is better. As a solution for communication in traffic applications, they suggest a combination of them.

Some commercial manufacturers have designed solutions for a connection between the vehicle's infotainment systems screen and an application of a smartphone. These solutions make it easier and safer to observe and use the phones applications. Car Connectivity Consortium's MirrorLink® is an application that utilizes standard technologies connect smartphones with vehicles. The phone connects to the vehicle's infotainment system to enable the use of certain applications. These applications are standardized with special certification for access during driving [22]. Apple Inc. is co-operating with various car manufacturers with an iPhone 5 and 6 series compatible CarPlay [23]. Also, Google has launched Android Auto [24]. Map service HERE claims to be the leader in navigation, mapping and location experiences. Their application combines high definition maps with cloud technology and provides a navigation service for both pedestrians and drivers [25]. HERE HD Live Map adds vehicle's sensor data to traffic information, weather, congestion, road conditions and lane closures to the map data and helps the driver make driving decisions for a route as safe as possible [26].

A responsive data system for traffic-related information helps drivers to optimize their routes and driving style to save time and money. Also, it is possible to decrease the amount of emissions. By adding intelligent solutions with data communication systems to vehicles, Centria has fostered the concept of cognitive infocommunications: designing and developing information technology solutions to assist drivers with decision making [15]. Some of these solutions are designed for providing traffic-related information, such as weather forecasts or traffic congestion notices, while others are for warning about events that may lead to accidents. (Fig. 1)

In its previous projects, Centria has been working with situation awareness systems and push notifications for sending messages to mobile applications [14]. Communication protocols SOAP and JSON were tested for transferring the sensor data [27]. Centria has a great opportunity to utilize its own 4G LTE network with an active antenna system (AAS) for research purposes and has carried out successful testing on the connections of the mobile solutions developed in its traffic-related projects [28].

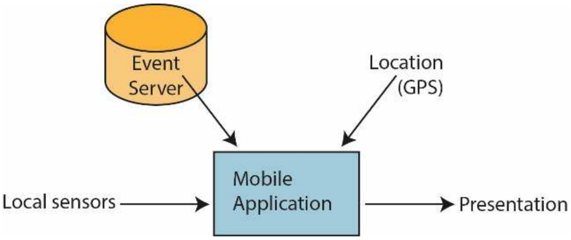


Fig. 1. Mobile application gathers and shares information required for the decision making.

In CoMoSeF project Centria has also tested combining the technologies needed to provide advanced traffic information for the driver with a wireless network within a vehicle. This vehicular area network enables the data to be received from WAVE radio equipment and external sensors, such as Noptel's laser distance sensor, by the adaptive user interface on a smartphone or tablet.

3. Testing the encryption at Centria

To fulfill the need for reliable and secure traffic communication in the Data to Intelligence project, the requirements for cyber-secure connections were defined: data confidentiality, data integrity, and sender authentication. These requirements are often presented as the basics of information security along with data availability [29]. For testing the attack and defense mechanisms, Centria launched the laboratory of Cyber Security in 2015. It will simplify and speed up the development process by making it possible to develop and test the needed protocols within a secure and closed environment before bringing them to real-life production use.

As described earlier, various methods already exist and have been tested. Centria decided to employ AES-128-encryption in the V2I environment. It is a robust encryption method and generally used on Internet. It also enables an end-to-end encryption: the message is not decrypted on routers or other network nodes during the transfer. The hypothesis before the tests was that encryption would extend the connection establishing time and increase the use of energy and time. The created solution is universal and efficient, and it was tested in the laboratory before the tests were set up on the road.

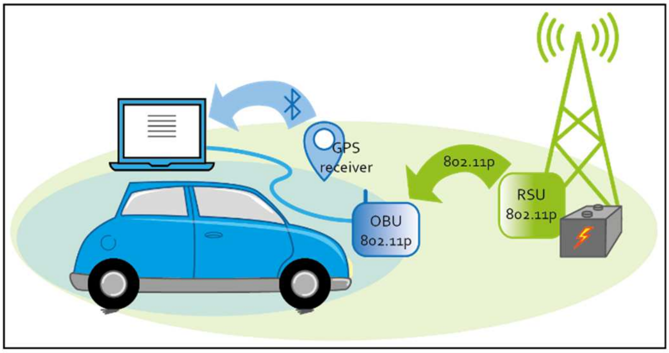


Fig. 2. The setup for the 802.11p testing. The RSU set included a WAVE radio, a power supply, and an antenna (green). The OBU set included a WAVE radio, an external GPS receiver with a Bluetooth connection, and a laptop connected to the radio (blue).

3.1. Execution of the Tests

A new testing round on Componentality FlexRoad WAVE radios was carried out on the highway in Kose, Estonia. RSU was connected to the antenna raised next to the road on a height of 2.5 m. The energy required by RSU was supplied with an external battery.

As there was no external antenna available for the OBU, it was placed on the dashboard of the test car for the best possible connection. A laptop computer was connected to the OBU with an Ethernet cable and to an external GPS receiver with Bluetooth connection. OBU was plugged into the car's cigarette lighter for power. The connection to the RSU was opened with PuTTY, and the scripts for saving the data were controlled from Windows' built-in command prompt (Fig. 2 and 3).

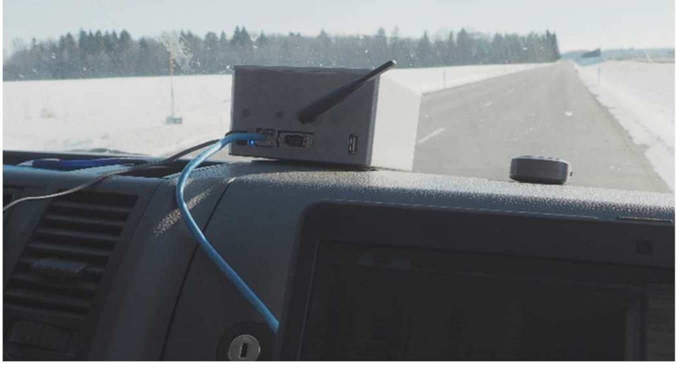


Fig. 3. Testing vehicle passing by the RSU, seen on the left side of the road. The OBU can be seen on top of the dashboard next to the external GPS receiver (on the right). Information about the data transferred during the tests is instantly seen on the laptop screen.

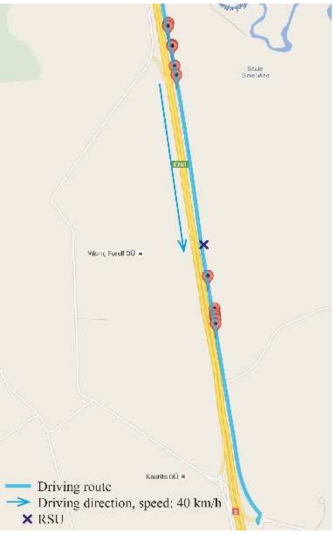
The tests drives were executed in two rounds, without encryption and with encryption to verify the loss in the received packets. The driving speeds were defined to be 70 km/h and 40 km/h. The drives were repeated several times in order to get reliable results from the testing. During the test drives, some random events to affect the results occurred, such as a big truck passing by the test vehicle and blocking out the data transfer. These events were noticed during the drives, and the data were removed from the analysis material as a whole. In these cases, extra drives were performed to get reliable data for the analysis.

3.2. Analysis of the Gathered Data

On the analysis of the measured data, we defined the timestamps and the GPS coordinates of the stable connection, where only a few individual failed packets occurred. The start and end points of the GPS coordinates were placed on a map (Fig. 4 and 5) to see how the stable connection area varied between the tests with and without encryption. Observing these maps proved that the encryption seemed to scatter the start and end points of the test rounds further away from each other.

According to the GPS information and the timestamps, the actual average speed during the tests with the speed of 40 km/h was 38.8 km/h. With the speed of 70 km/h, the actual speed was 64.8 km/h. The average area of the stable connection while testing without encryption was 946 m (91 sec) at the speed of 40 km/h and 910 m (51 sec) at the speed of 70 km/h. The corresponding areas with encryption were 981.5 m (88 sec, speed of 40 km/h) and 917.5 m (51 sec, speed of 70 km/h). This indicates, that the encryption slightly widens the area of stable connection.

The verified stable connection area with and without encryption is encouraging for applications that require high data security. The transfer distance of almost one kilometer is more than sufficient for sending and receiving data packets in suburban and city areas. As seen on the maps (Fig. 4 and 5), the connection starts to cut off after the vehicle passes by the RSU. This results from the metal body of the vehicle blocking the signal from WAVE radio on the dashboard. Using an external antenna will remove this problem, and the connection will be stable to all directions from the RSU.



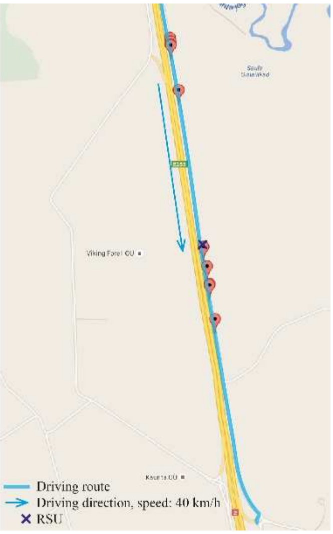


Fig. 4. The GPS start and end points of stable connection at the speed of 40 km/h on the map. Testing without encryption is on the left and with encryption is on the right.

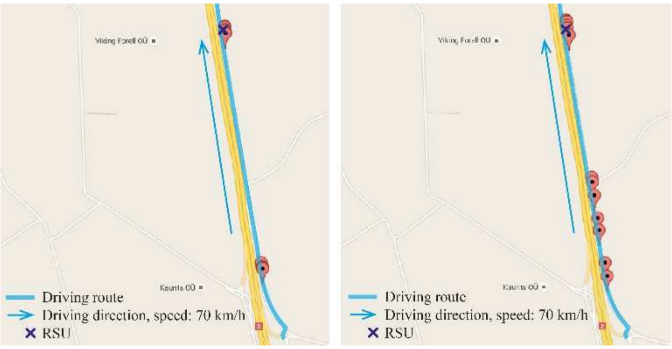


Fig. 5. The GPS start and end points of stable connection (speed of 70 km/h) on the map. Without encryption on the left, with encryption on the right.

The impact of the speed difference on the total number of sent packets was found significant: reduction of approximately 55 % from speed of 40 km/h to 70 km/h (see the packet amounts in Table 4). Testing with encryption and without it led to the same result. However, the encryption slowed down the data transfer process and reduced the total number of sent packets by approximately 21 %. In contrast, the decreased number of sent packets while using the encryption led to an improved stability of the connection at both speeds. When the encryption was used, the failing percentage decreased by about two percentage points or even more.

Table 4. The Average Number of Sent and Received Packets, Failed Packets and Failing Percentages

Speed 40 km/h, without encryption	
Average, sent: 668.3	Average, received: 557.8
Average, failed: 110.5	Failing percentage: 16.5
Speed 40 km/h, with encryption	
Average, sent: 522.6	Average, received: 452.8
Average, failed: 69.8	Failing percentage: 13.4
Speed 70 km/h, without encryption	
Average, sent: 298.8	Average, received: 231.7
Average, failed: 67.2	Failing percentage: 22.5
Speed 70 km/h, with encryption	
Average, sent: 235.6	Average, received: 186.8
Average, failed: 48.8	Failing percentage: 20.7

4. Applications designed and developed at Centria

On the field of ITS, Centria has concentrated on traffic applications for supporting the driver's decision making. They created applications for data gathering and converting the data to a readable form. Also, visualizations for presenting the traffic information to the user were designed. The customer needs defined the operating system on which the applications were programmed: even though the Android is popular among consumers [16], companies often prefer using Windows operating system.

The created traffic applications can be divided into three categories according to the purpose for which they were created. They gather data from sensors for the use of other applications. The sensors can be one of those integrated in the vehicle or the smartphone or they can be added sensors, such as a laser sensor for measuring distances, mounted to the vehicle. Other applications collect data from different sources, such as the applications mentioned before, or other databases. These databases can include, e.g. weather information or the user data by other road users. The applications represent the data by creating a visualization of it, enabling the driver to view the processed information. They can also warn the driver about the possible hazards. The last application category, server-based information interchange applications, allow users to add information to the databases. They also enable the administrators to view and validate the information before sharing it for common use.

4.1. Information-gathering applications

The OBD2 DTC application is designed for the use of professional vehicle fleets, such as transport companies. The application makes queries for diagnostic trouble codes (DTCs) from the vehicle's on-board diagnostics (OBD2) port and shares them for the fleet management. The daily routines are created for obtaining the important information of the maintenance needs of the vehicle. The driver can be notified in cases of changing circumstances and of critical need for service. Also, the drivers' driving habits can be traced and stored into a database for management purposes and evaluation of economical driving.

A data acquisition application connects the mobile phone to sensors. The research studied the phones' local area connections, such as Wi-Fi, Bluetooth and IrDA for interconnection with sensors. The created application enables the transfer of data from sensors to a smartphone with a Windows 8 operating system.

Centria created a box (Fig. 6) that has connectors for up to four analog inputs and eight digital inputs. The box also has four switching outputs to control auxiliary devices. The smartphone and sensor box are connected using the Bluetooth serial port profile and the smartphone phone acts as a real-time display and a router between the sensors and the server. The connection box itself is not connected with the vehicle, but with the sensors installed on the vehicle, as the Bluetooth-connection can be established with only one device at a time, in this case the smartphone.

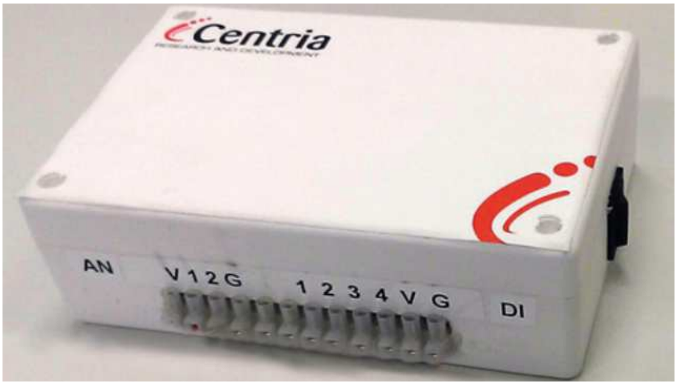


Fig. 6. Bluetooth sensor connection box.

4.2. Information-representing applications

The only information to be shown at all times on the dashboard of a motor vehicle, required by Finnish legislation [30], is the speedometer. For a visually effective and adaptive user interface Centria designed a Dashboard Demo. This application is based on HTML5 and CSS3, and replaces a vehicle's conventional dashboard, enabling the visual notifications and warnings to be shown as needed. To meet the requirement of the law, Centria designed a dashboard application enabling the visualization of the critical information on the dashboard without losing the legally restricted speedometer. As the important notification needs to be shown, it appears in the center of the dashboard and replaces the speedometer indicator, which will be relocated on one side of the dashboard. On the design process, the warnings were designed to be as informative as possible – keeping in mind the drivers not to lose their attention paid to the traffic.

The adaptive dashboard connects to the vehicle's OBD2 port with a Bluetooth ELM327 device, which enables the viewing of the information of the vehicle itself on the dashboard. The presentable information from OBD2 includes engine revolutions per minute, vehicle speed, coolant temperature and fuel level (Fig. 7).

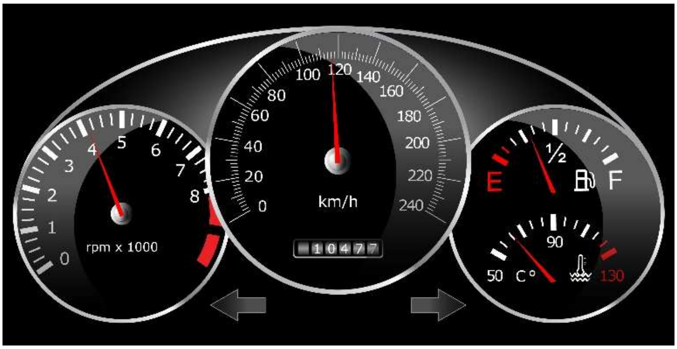


Fig. 7. Adaptive dashboard responds to changing information. Warnings are displayed when needed.

Centria has also added some equipment to a vehicle and tested receiving distance readings and warnings on the adaptive dashboard, if the distance to the vehicle ahead is too short to be safe (Fig. 8). For this test, the added devices were a Noptel laser distance sensor for defining the distance to the vehicle ahead and a Wi-Fi connection to transfer the data to the dashboard. GPS coordinates were used for the location of the vehicle and based on them the Finnish Meteorological Institute (FMI) based on the coordinates supplied the prevailing friction factor for calculating the needed braking distance [31].

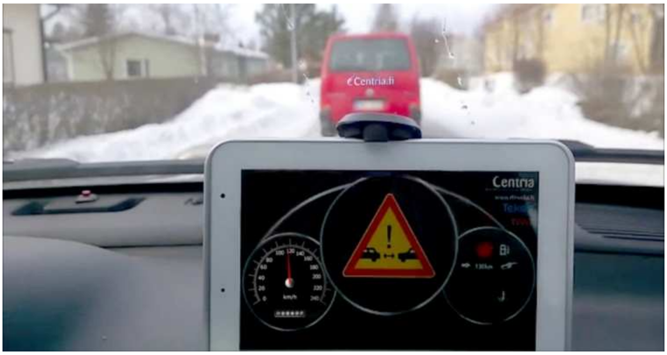


Fig. 8. Adaptive dashboard presenting a warning that the distance to the car ahead is too short to be safe.

A traffic warning system application for the Windows phones was created to speed up the spread time of the events for the public. The users can create events and warn other drivers if something unexpected happens on the road. The service is built of two types of mobile software and one web-based server screen. The three interfaces address the different needs of the traffic warning system and connect users and authorities to the same service. A nearby event can be displayed on the map (Fig. 9). On the right side of the app, there are three buttons to create new events, such as general warning for an obstacle on the road, bad visibility, or an animal on the road – a local and short duration event, such as deer or moose seen near the road.

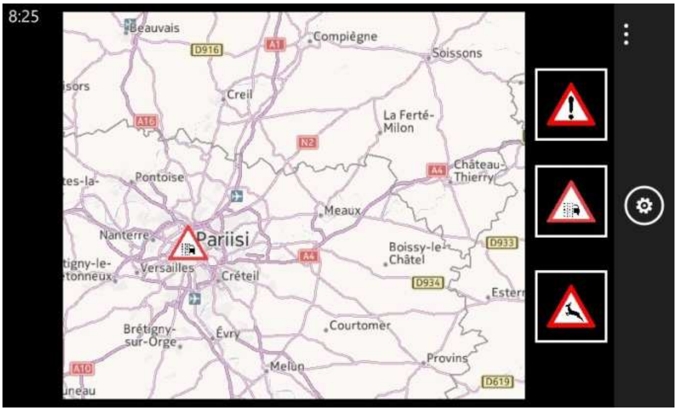
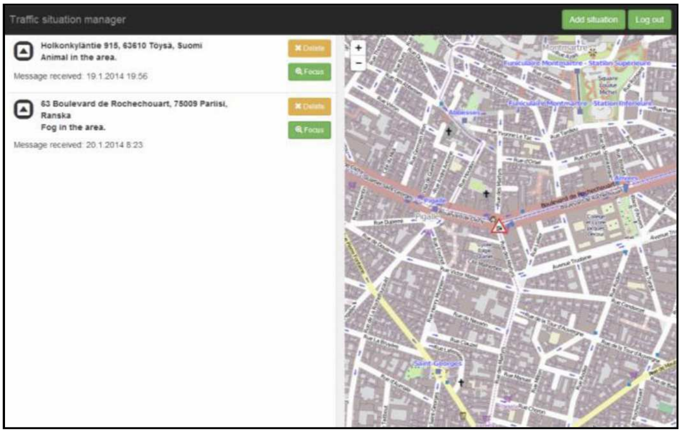


Fig. 9. A driver can add events to the system on the traffic warning application on a smartphone screen.



Holkonkyläntie 915, 63610 Töysä, Suomi
Animal in the area.

Message received: 19.1.2014 19:56

63 Boulevard de Rochechouart, 75009 Pariisi, Ranska
Fog in the area.

Message received: 20.1.2014 8:23

Fig. 10. Manager's view of a web page.

Some commercial applications feature same kinds of properties. Nevertheless, there seem to be some problems with their credibility, when it comes to the use of authorities. Professional drivers prefer an application with simple visualizations, clear objects, good usability and reliable data, instead of cute figurines, such as featured by Waze [32]. Waze relies on crowd sourcing and lacks the collaboration with such official traffic information providers as traffic authorities or meteorological institutions. When relying on the data of masses, a mechanism must be created for making sure the user-added events are real. Counting the user messages from the server application makes it possible to estimate the validity of the events: repeatedly appearing message is probably valid. In CoMoSeF project, the fleet of professional drivers ensured the fast delivery time of the sudden events. Events added by authorized users did not need validation, and they were distributed to the other drivers in the area immediately. Fig. 10 illustrates the managers' view of the web page, where they can either confirm or remove events added by other users.

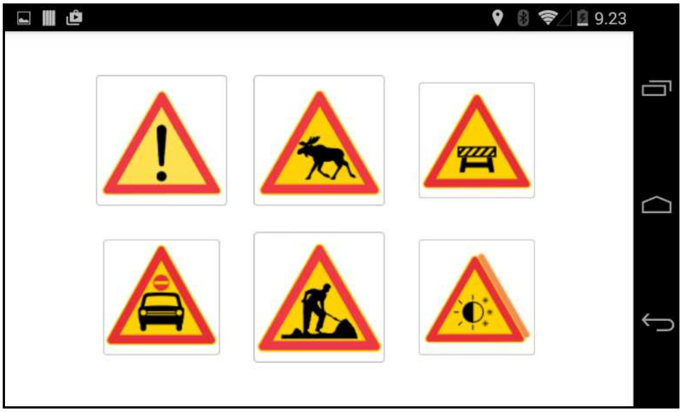


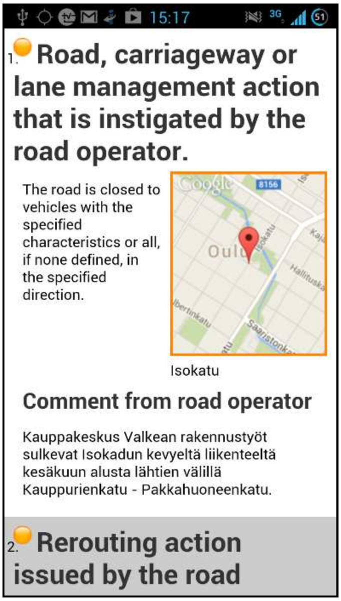
Fig. 11. Smartphone user interface of traffic warning application enables the driver to add notifications to the warning system.

An improved traffic warning system was developed for Android smartphones to meet the needs of a company involved in the project. A simplified user interface allows the driver to add notifications of unpredictable traffic events to the system (Fig. 11). Different user groups are categorized and notifications added by the authorized users, i.e. professional drivers, are presented automatically to the other users. A control panel was also developed for the maintenance of the traffic warning system and for the manager to review and accept or deny the regular users' notifications for broadcasting. The validated notifications and the notifications added by the authorized users are presented to the other drivers on the map.

4.3. Server-based information interchange

HTML5 based CentriaNavi (Fig. 12) is an application for Android user interfaces. It receives and views traffic-related information in standardized DATEX II format. DATEX II is created for the interchange of information between data centers [33] and it includes traffic data, e.g. traffic flow. Also, traffic light systems data, data from public information sources and data provided by partnering companies and institutions are interchanged with DATEX II. Using DATEX II enables rapid spread of the traffic information. Within CoMoSeF, the collaboration with Infotripla Ltd. made it possible to receive DATEX II messages through their interface. CentriaNavi sends a query to the interface every five minutes and adds author comments and map information to the received data. The user sees the information on a map.

A DATEX II-JSON (JavaScript Object Notation) converter developed at Centria converts the heavyweight server-to-server protocol to lightweight mobile use. DATEX II is a heavily transferable data format used for traffic between servers and not usable for mobile connections. Data packets are received and converted to JSON format in Centria's server. This results to lighter calculation processes in the end user application and less traffic to the DATEX II interface. Centria's server stores the DATEX II messages in a local database. It is queried by the mobile application in the vehicle based on its GPS information. For defining the location of the query for DATEX II, Centria's web interface maintains a list of geo coordinates. DATEX II will provide information about any events reported in that specific area. The server replies to the mobile application's query with a JSON-formatted message and includes the status of the traffic on the upcoming route.



1. Road, carriageway or lane management action that is instigated by the road operator.

The road is closed to vehicles with the specified characteristics or all, if none defined, in the specified direction.

Isokatu

Comment from road operator

Kauppakeskus Valkean rakennustyöt sulkevat Isokadun kevyeltä liikenteeltä kesäkuun alusta lähtien välillä Kauppurienkatu - Pakkahuoneenkatu.

2. Rerouting action issued by the road

Fig. 12. CentriaNavi presents traffic-related information on a mobile phone screen.

A WAVE radio demo was also done when the driver warning system was piloted [14]. When the vehicle reached RSU's message coverage area, the type and location of a warning was received by the equipment in the vehicle and displayed to the driver on a screen. Different kinds of warnings were designed: an animal on the road, slippery because of an icy road and slippery because of rainy weather. The driver's ability to notice and react to the warnings was researched and reported on during the testing of the application.

During the notification demo, the connections between the roadside unit and the on-board unit were tested and a push notification application was developed for an Android mobile phone. The driver will get real-time notifications of critical traffic-related events on his or her mobile phone regardless of what he or she is using the phone for at the moment (Fig. 13). In other words, if the driver is using a navigation application on the phone, the push notification application will override the current application and present the warning. The server is based on the Google notification service, where the mobile device introduces itself to the server as a client and after that, is able to get push type messages.

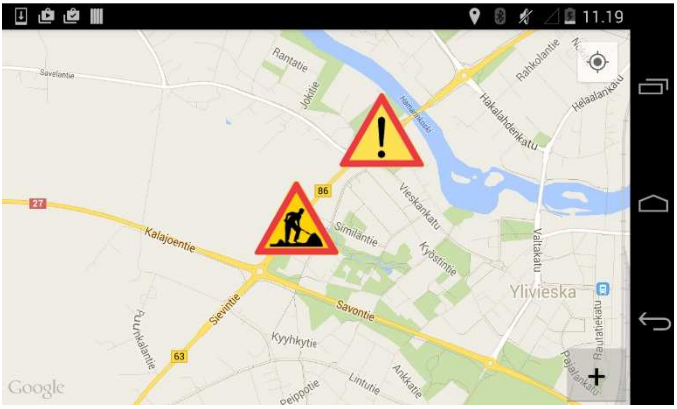


Fig. 13. Notification demo visualizing the warnings on a mobile phone user interface.

5. Conclusion

Centria has been working in collaboration with several Finnish companies and research institutions to create applications within CoMoSeF and Data to Intelligence (D2I) projects for making traffic safer. The created applications were based on the companies' needs, and some of them are already included in their products and services portfolios. By designing a simple user interface for sharing unpredictable traffic events, Centria and its collaborators have been able to create an infocommunication system that significantly improves traffic safety.

While interacting with these user interfaces, the human actor does not have to pay an excessive amount of attention to the application itself, but can focus on the traffic. In its earlier study Centria has collected user-feedback on the presentation method and proven it to be feasible and safe to use for presenting the traffic data. [14] The adaptive dashboard presents the crucial information precisely, clearly and unambiguously for the driver when needed. Also, adding warnings to the system is made as simple as possible to prevent accidents while using the application. The traffic warning application was tested in the Tampere region with approximately ten taxes. The received feedback received from the drivers was encouraging. One of the drivers thought, that the application is "extremely easy to use" and "lives can be saved by using this kind of an application". All the created applications share the same cognitive Centria platform and provide each use case a user-specified interface.

The data security tests performed by Centria showed that using encryption on WAVE radios slows down the broadcast and reduces the total number of sent data packets. In contrast, the reduced number of packets increases the percentage of the received packets, compared to the transfer of unencrypted data. In addition, a change in the speed of the vehicle affects data transfers, but while driving on urban speeds, the operating distance of the WAVE radios is sufficient for transferring traffic data, and delivering warnings and other information to the driver.

In real-life implementations and applications, good visibility from the OBU to the RSU is essential. The antennas must be placed high enough so that other vehicles, buildings or other obstacles will not block the connection. Using an external antenna on the top of the vehicle will help to achieve this goal. The low speeds in urban areas will improve the reliability of the connection.

Acknowledgment

The authors would like to thank the Finnish Funding Agency for Technology and Innovation (Tekes) for their financial support of the projects. The tests were executed and reported at Centria projects: European Celtic-Plus projects Co-operative Mobility Services of the Future (CoMoSeF) and Cyber-security in the Wireless Industrial use case (CyberWI), and a national Digile Ltd. SHOK program Data to Intelligence (D2I). The applications were developed with collaborating companies as part of D2I and CoMoSeF projects. The authors would also like to thank all the other institutions and companies that participated in the projects.

References

[1] Baranyi P, Csapó A: Definition and Synergies of Cognitive Infocommunications, Acta Polytechnica Hungarica, Vol. 9, pp. 67–83, 2012.
DOI: 10.1109/CogInfoCom.2012.6422001

[2] Saxena A: IEEE 802.11p: OVERVIEW. [Online] Available:
https://apoorvsaxena4.wordpress.com/2015/05/16/an-introduction-to-ieee-802-11p-in-vehicular-environment

[3] Havelt R, Oliviera B: Hacking the Fast Lane: Security Issues with 802.11p, DSRC, and WAVE, Black Hat DC 2011. January 2011.

[4] IEEE Vehicular technology Society: IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages, The Institute of Electrical and Electronics Engineers, Inc., 2013.

[5] Raya M, Hubaux JP: Securing vehicular ad hoc networks, Journal of Computer Security, Vol. 15, pp. 39–68, 2007.
DOI: 10.3233/JCS-2007-15103

[6] Wordsworth S: Grid Unlocked, Traffic Technology International, April/May 2013, pp. 22–26, Dorking, 2013.

[7] Wolf M, Weimerskirch A, Wollinger T: State of the Art: Embedding Security in Vehicles, EURASIP Journal on Embedded Systems, Vol. 2007, June 2007.
[Online] Available:
http://www.weimerskirch.org/papers/WolfEtAl_StateOfTheArtVehicles.pdf
DOI: 10.1155/2007/74706

[8] Wang Y, Hu J, Zhang Y, Xu C: Reliability Evaluation of IEEE 802.11p-Based Vehicle-to-Vehicle Communication in an Urban Expressway, Tsinghua Science and Technology, Vol. 20, Issue 4, pp. 417–428, August 2015.
DOI: 10.1109/TST.2015.7173456

[9] Zhang Z, Boukerche A, Ramadan H: Design of a lightweight authentication scheme for IEEE 802.11p vehicular networks, Ad Hoc Networks, Vol. 10, Issue 2, pp. 243–252, March 2012.
DOI: 10.1016/j.adhoc.2010.07.018

[10] Biswas S, Mišić J: A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs," in the IEEE Transactions on Vehicular

Technology, Vol. 62, No. 5, pp. 2182–2192, June 2013.
DOI: 10.1109/TVT.2013.2238566

[11] Tsai JL: An Improved Cross-Layer Privacy-Preserving Authentication in WAVE-Enabled VANETs, in the IEEE Communications Letters, Vol. 18, No. 11, pp. 1931–1934, November 2014.
DOI: 10.1109/LCOMM.2014.2323291

[12] Kumar V, Whyte W: Performance Analysis of Existing 1609.2 Encodings v ASN.1, in the SAE International Journal of Passenger Cars – Electronic and Electrical Systems, May 2015.
DOI: 10.4271/2015-01-0288

[13] Muikkula J: Introduction of 802.11p WAVE radio system," bachelor's thesis, electrical engineering. Centria University of Applied Sciences, Ylivieska, 2014.

[14] Jämsä J: Cognitive communication for traffic safety, in the 5th IEEE Conference on Cognitive Infocommunications (CogInfoCom), pp. 103–108, Vietri sul Mare, 2014.
DOI: 10.1109/CogInfoCom.2014.7020427

[15] CogInfoCom: Cognitive Infocommunications, 29 January 2013. Available: http://www.coginfocom.hu/index.php

[16] Gartner Inc.: Gartner Says Smartphones Sales Surpassed One Billion Units in 2014, 3 March 2015. Available: http://www.gartner.com/ newsroom/id/2996817

[17] Shi Q, Abdel-Aty M: Big Data applications in real-time traffic operation and safety monitoring and safety monitoring and improvement on urban expressways, Transportation Research Part C: Emerging Technologies, Vol. 58, Part B, pp. 380–394, September 2015.
DOI: 10.1016/j.trc.2015.02.022

[18] Manolopoulos V, Tao S, Ismail M, Rusu A: MobiTraS: A Mobile Application for a Smart Traffic System, in the 8th IEEE International NEWCAS Conference (NEWCAS), pp. 365–368, Montreal, QC, June 2010.
DOI: 10.1109/NEWCAS.2010.5604010

[19] Kihl M, Bür K, Mahanta P, Coelingh E: 3GPP LTE downlink scheduling strategies in vehicle-to-infrastructure communications for traffic safety applications, in the IEEE Symposium on Computers and Communications (ISCC), pp. 448–453, Cappadocia, July 2012.
DOI: 10.1109/ISCC.2012.6249337

[20] Bai F, Krishnan H: Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications, in the IEEE Intelligent Transportation Systems Conference (ITSC '06), pp. 355–362, Toronto, Ont., September 2006.
DOI: 10.1109/ITSC.2006.1706767

[21] Cailean AM, Cagneau B, Chassagne L, Popa V, Dimian M: A survey on the usage of DSRC and VLC in communication-based vehicle safety applications, in the IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT), pp. 69–74, Delft, November 2014.
DOI: 10.1109/SCVT.2014.7046710

[22] Car Connectivity Consortium: MirrorLink, 2014. Available: http://www.mirrorlink.com/about-mirrorlink

[23] Apple Inc.: Apple CarPlay, 2016. Available: https://www.apple.com/ios/carplay/

[24] Google: Android Auto, 2016. Available: http://www.android.com/auto/

[25] HERE: HERE, the leading location cloud, 2015. Available: https://company.here.com/here/

[26] HERE: HERE HD Live Map - the most intelligent vehicle sensor, 2016. Available: https://company.here. com/intelligent-car/here-hd-live-map/

[27] Jämsä J, Luimula M: Advanced car navigation—future vehicle instrumentation for situation-aware services, in the 12th IEEE Int. Conf. on Mobile Data Management (MDM), Vol. 2, pp. 7–10, Luleå, 2011.
DOI: 10.1109/MDM.2011.36

[28] Heikkilä M, Kippola T, Jämsä J, Nykänen A, Matinmikko M, Keskimaula J: Active Antenna System for Cognitive Network, in the 5th IEEE Conference on Cognitive Infocommunications (CogInfoCom), Vietri sul Mare, 2014.
DOI: 10.1109/CogInfoCom.2014.7020452

[29] Cisco: CCNA Security 2.0. [Online course material] Cisco Systems 2016.

[30] Ministry of Transport and Communications of Finland: 1090/2002 Vehicles Act, Chapter 4, section 25, § 12, Finnish Ministry of Justice, 1 January 2005. Available: http://www.finlex.fi/en/laki/kaannokset/ 2002/en20021090

[31] Kaartinen H, Jämsä J, Hippi M, Pahkala J: Fact and friction, in Thinking Highways, Vol. 10, No. 1. pp. 40–44, 2015.

[32] Waze Mobile: Real-time maps and traffic information based on the wisdom of the crowd, 2016. Available: http://www.waze.com/

[33] European Parliament: Directive 2010/40/EU, EUR-Lex - Access to European Union law, 7 July 2010. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32010L0040