The safety of modern and traditional communication protocols in vehicles

Andrzej Sumorek

Lublin University of Technology, Department of Structural Mechanics
Poland, 20-618 Lublin, Nadbystrzycka 40, e-mail: a.sumorek@pollub.pl

Received July 18.2016: accepted July 25.2016

Abstract. Communication infrastructure of vehicles sub-assemblies has undergone three phases of development. The first phase was initiated by the need to reduce emission levels. The function of vehicle sub-assemblies health monitoring was introduced simultaneously. This phase took place in the 70s and 80s of the 20th century. The second phase was focused on the elimination of redundant sensors and implementation of new functions of the vehicle. This phase has been particularly noticeable since the beginning of the 21st century. At the moment, there are 2 directions of development. On the one hand, the works are being continued in the scope of autonomous movement of vehicle and, on the other hand multimedia solutions are being introduced in order to make the time spent in a vehicle more attractive (multimedia, the Internet, …).

The present study is focused on the mechanisms of protection applied in communication protocols used in vehicles. Furthermore, it contains the classification of communication methods, characteristics of the basic methods of protection incorporated in the described protocols and the practical cases of security breach. Therefore, it is possible to answer the question why it is possible for third persons to interfere into the communication network of a vehicle and to indicate potential methods of protection against the functioning disturbance in such communication networks.

Keywords: Vehicle Communication Protocol, Protocol Safety.

INTRODUCTION

Communication systems of vehicles sub-assemblies have undergone three phases of development. The first phase was initiated by the United States Congress which approved „Clean Air Act" and established Environmental Protection Agency (EPA) in 1970. The principal goal of legislator was to reduce emission levels. As a result of introduction of „Clean Air Act" two new functions have been introduced by motor vehicles manufacturers. On the one hand, the manufacturers commenced to provide motor vehicles with controllers ensuring reduction of emission levels. Simultaneously, they also commenced to install the sockets enabling the diagnostics of vehicle condition in a manner independent on the manufacturer.

The second phase of communication networks development was focused on the elimination of redundant sensors and implementation of new functions. As a result of the elimination of redundant sensors, it was possible to reduce the costs of motor vehicle production. Another effect is the introduction of multiple driver assistance systems e.g. Anti-Lock Braking System (ABS), Electronic Stability Program (ESP) or Acceleration Slip Regulation (ASR). Increased performance of electric and electronic systems (micro-controllers) combined with reduced prices resulted in the introduction of new functions, i.e. temperature measurement in multiple points of vehicle cabin, introduction of several airbags, possibility to adjust the settings of air-conditioning, seats or mirrors by means of pushbuttons.

Currently, 2 directions of development are visible. On the one hand, the works are continued in the scope of autonomous movement of a vehicle and, on the other hand multimedia solutions are introduced in order to make the time spent in a vehicle more attractive (multimedia, the Internet, …). The commonly used parking assistant enables parallel parking without touching the steering wheel. The scope of other driver assistance systems encompasses forward collision warning, lane depth warning, auto steering road edge or pedestrian detection [20]. Less known is the more advanced BMW solution „Remote Valet Parking Assistant" enabling autonomous travel of a parked vehicle to the driver or automatic parking without the driver presence in a motor vehicle [10, 37]. Complete or partial hands-off solutions are applied in Google and Audi motor vehicles. At the time of this writing, autonomous travel of Audi vehicle on highways was equal to almost 1000 km [10]. The travel of autonomous Google motor vehicle has been equal to about 2 million kilometers [18]. Google motor vehicle seems to be the closest to introduction to everyday use. Mr. Stanley from Stanford University, a co-author of the autonomous vehicle, was the first manager of the autonomous vehicle construction project. Stanley vehicle won the first competition for the autonomous vehicle construction arranged by United States Department of Defense (DARPA). The first winner of DARPA competition in the year 2005 and Google motor vehicle in the year 2016 is illustrated in Fig. 1 [28]. As a result of dynamic development, communication networks previously dedicated for various applications are applied in the same motor vehicle.

Fig. 1. The first model (2005) and actual prototype Google motor vehicle (2016) [16, 28]

AUTOMOTIVE NETWORKS AND PROTOCOLS

Before the introduction of data bus communication into a motor vehicle, data exchange was carried out on the basis of simple cable connections between sensors and actuators of the vehicle as well as signaling devices and switches accessible to the driver. Initially, 3 classes of protocols (A, B, and C) were introduced by SAE J1850 standard which were dedicated to various applications between 10 Kbps and 1 Mbps [6, 24, 36]. As early as at the start of the 21st century, the protocols with higher complexity and data baud rate marked as C+, D or Infotaiment began to be used [3, 6, 22, 32, 34]. The structures of every currently manufactured vehicle incorporate simple A class networks (LIN – Local Interconnect Network), as well as D class networks (Medium Oriented System Transport), as illustrated in Fig. 2.

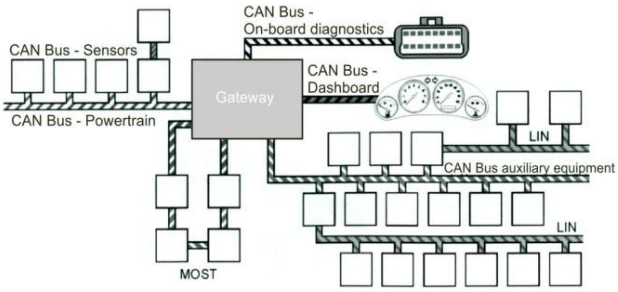

Fig. 2. Conventional communication infrastructure of motor vehicle sub-assemblies [3]

The diagram of communication infrastructure of higher class vehicles is shown in Fig. 3. The diagram illustrates the majority of conventional communication networks from Fig. 2 and additional communication systems. The additional communication systems can be subdivided into two groups. The first group is represented by FlexRay protocol. This group consists of protocols dedicated for automotive sector applications. The representatives of the second group are show in Fig. 3 in the vicinity of Telematics Head Unit (THU). Often, they are solutions associated with typical IT technology i.e. Ethernet network, WLan (Wireless LAN), USB (Universal Serial Bus). This group is supplemented with the solutions enabling the access to mobile telephony networks or to Global Navigation Satellite Systems e.g. GPS (Global Positioning System). Their task is to make vehicle use more comfortable through facilitated vehicle driving (GPS), communication (mobile telephony networks and Bluetooth), multimedia data exchange and entry into motor vehicle from portable devices and the Internet.

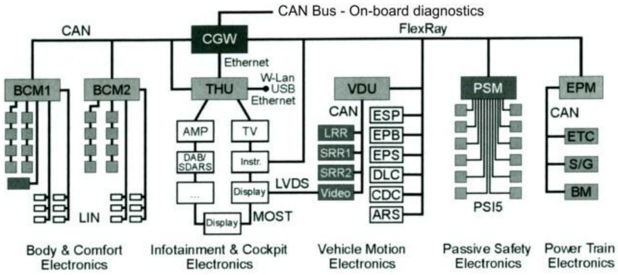

Fig. 3. Example of an advanced communication infrastructure of vehicle sub-assemblies [3]

Elements of communication structures illustrated in Fig. 2 and Fig. 3 are characterized by a high variety of communication methods. A single motor vehicle contains „slow" protocols enabling an exchange of small messages between a precisely defined number of motor vehicle sub-assemblies (e.g. LIN protocol). On the other hand, the multimedia devices can communicate with unknown external multimedia sources (e.g. Wireless LAN) in a fast and wireless mode. The vehicle communication structure integrates the systems dedicated for motor vehicle sub-assemblies control (e.g. FlexRay protocol) and general type systems (e.g. Universal Serial Bus).

The dynamic development in the scope of networks and protocols dedicated for various applications is reflected in the diversified architecture of protocols. Fig. 4 illustrates the basic layer structure based on ISO-OSI model and accompanied by selected structures applied in case of MOST (Medium Oriented System Transport), CAN (Controller Area Network) and Bluetooth protocols. In case of protocols it is not necessary to specify and use all the layers. In case of a protocol serving a single and separated network segment, there are no communication problems between modules regardless the incomplete description of protocol. A diversified structure of many motor vehicles network would require consistency between the protocols, for instance consisting in similar security levels to be ensured in individual layers. Stacks of protocols illustrated in Fig. 4 confirm that various solutions are applied in practice. There are protocols defined in all the 7 layers of ISO-OSI model (e.g. MOST) as well as protocols defined in only one physical layer (e.g SAE J1850 PWM - Pulse Width Modulation and SAE J1850 VPW - Variable Pulse Width) or in several layers – physical layer and data link (e.g. CAN). Diversified communication methods within a motor vehicle are caused by the absence of any technical guidelines in the scope of communication in the initial period of data bus development; only expected emission levels and types of data accessible by means of diagnostic equipment were determined by the legislator. The current problems result from the necessity to make the product, i.e. a motor vehicle, more attractive and to immediately introduce digital technique solutions which could be unsuitable for motor vehicles. Software errors in “household” computers can be eliminated through corrections of successive program versions but software errors in motor vehicle controllers may lead to collisions and accidents.

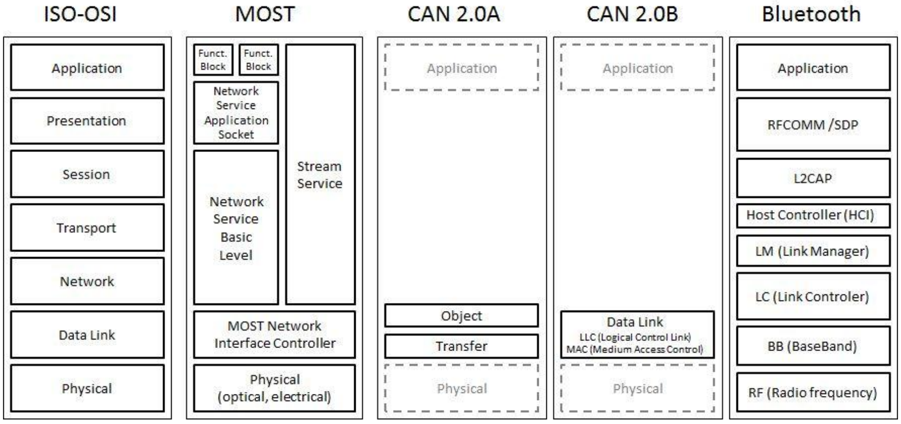

Fig. 4. Layers in the ISO-OSI model and layers in selected communication methods [13, 34]

Examples of communication structures of motor vehicles information network illustrated in Fig. 3 and 4 are associated with more than ten protocols and networks. The characteristics of the 3 selected data buses and protocols representative for networks in A, B and C classes are presented below.

LIN Bus. LIN bus/ protocol (Local Interconnect Network) depending on the baud rate (between 1 and 20 Kbps) can be classified in A or B protocols class. Its first practical implementation took place in 2001. LIN is applied in BCM (Body Control Module) as illustrated in Fig. 3. It is also applied in control and adjustment systems for windows, seats, doors and mirrors [34, 38].

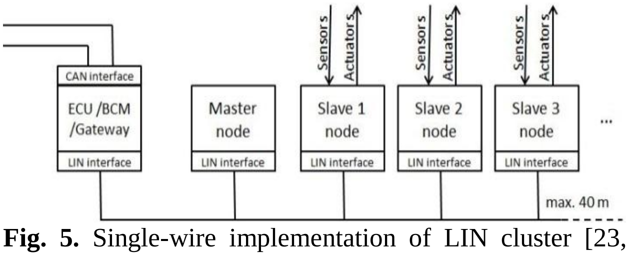

Fig. 5. Single-wire implementation of LIN cluster [23, 32]

LIN bus is operated in single-wire implementation configuration. Maximum 16 nodes can be attached to a single wire bus. The bus should not be longer than 40 meters. Single-wire implementation incorporates a master node and up to 15 slave nodes. Such an arrangement is called cluster (Fig. 5).

The functioning of the whole cluster is based on one or more”schedule tables”. A ”schedule table” contains the list of successive orders including the time and conditions of their transmission by the master node. Communication of cluster nodes is initiated by the master node in accordance with the “schedule table”. The cluster nodes use messages (frames) with the structure shown in Fig 6. The frame is divided into two parts. The first part called the header contains an identifier i.e. a number to which slave node activity is assigned. Responding to the identifier, the slave node may: a) receive and complete the order of master node which is contained in „response” part, b) send data determined by means of the identifier in „response” part to the master node, c) receive the data determined by means of the identifier from another slave node.

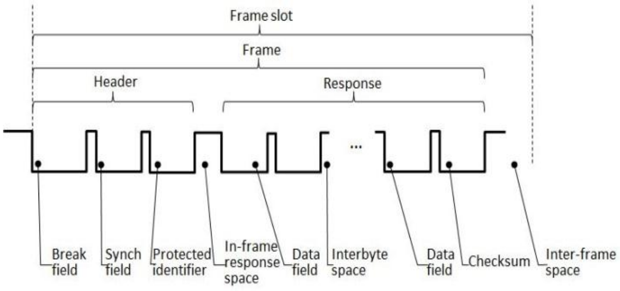

Fig. 6. LIN message frame [23, 34]

Commands of a master node contained in the identifier in the header are secured by means of two additional check bits. Data transmitted to and from a slave node in response are secured by means of an additional byte of checksum. In later protocol versions it is possible to enter an additional bit confirming the correctness of data receipt. There are no advanced mechanisms of data protection in the course of a normal operation of LIN network cluster. In case of identifier or data bytes error detected in the frame, such frame is ignored. In case of lack of declared additional checking procedures, the headers and data with incorrect checksums will not be identified by the cluster. The cluster area does not contain any mechanisms verifying whether the received frame has really originated in the master node. Each node which is physically connected to the bus line is able to generate messages disturbing the operation of the whole cluster. An external device connected to the diagnostic port is able to generate messages for LIN cluster by means of a gateway. The lack of nodes authentication is one of the reasons of LIN bus use in the systems in which high security level is not required.

CAN Bus. Currently, Controller Area Network shall mean the communication protocol, data bus, communication method. Originally, CAN was developed as the communication protocol. It has been introduced for the first time in the year 1991. CAN protocol specification describes Data Link Layer only (Fig. 4). Due to its common application on the market, multiple CAN specifications occurred in the physical and application layer. Therefore, CAN can be applied as B and C class protocol. Unless significant transmission rate is required, it is possible to use the CAN described in ISO 11898-3. In such case, the bandwidth is lower than 250 Kbps. High Speed CAN described in ISO 11898-2 is used in the systems with the bandwidth reaching 1 Mbps. Additional descriptions introduced by ISO standards mainly relate to the physical layer requirements enabling to achieve the required rate of data exchange [3, 30, 31, 36,38]. On the other hand, CAN has been extended by the description of functioning in the application layer and DeviceNet, CANOpen and CAN Kingdom specifications have been created.

In most cases, CAN bus is built in the form of double-wire implementation (Fig. 7). Linear and star topology is applied. Linear bus topology is commonly used in motor vehicles (Fig. 7). The number of nodes connected to the bus is limited by electric parameters only. The bus is operated in a multi-master mode i.e. the priority of all the nodes is identical. There are no master and slave nodes like in the case of LIN bus. All the nodes can commence transmission at the same time. All the nodes can access the data transmitted by the bus.

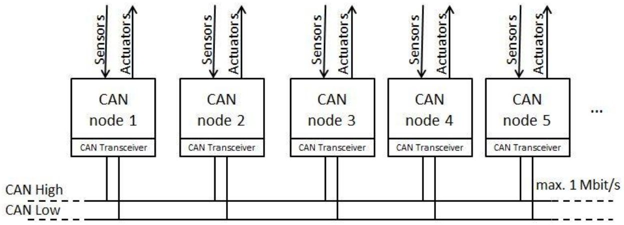

Fig. 7. Double-wire implementation of CAN Bus [13, 32]

Access to data is controlled by arbitration field of CAN message frame (Fig. 8) [33]. In case of simultaneous start of transmission by several nodes, the transmission is continued by the node with greater number of prevailing bites in the arbitration field of CAN message frame. Such a mechanism of the access to CAN bus makes it possible to easily attach new nodes. When entering new messages and new frames, it is only required to avoid collisions with previously used messages.

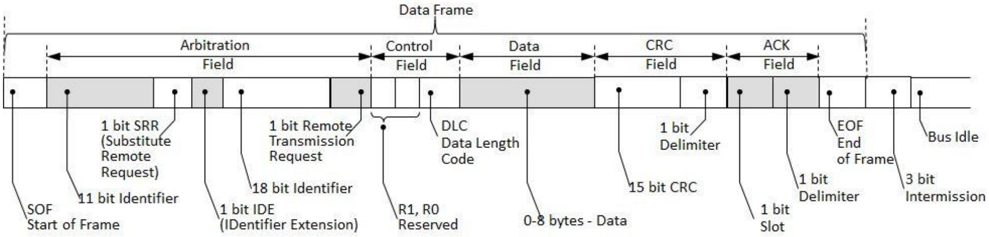

Fig. 8. CAN message frame [3, 31]

There are several mechanisms ensuring security within CAN network. Two methods are used to reduce errors level in the physical layer. Node transceivers are capable to check the bits emitted and present on the bus. In case of non-conformity of the bit emitted and present on the bus, transmission error is detected. In order to avoid bus saturation condition, „bit stuffing" mechanism has been introduced. When five identical bits are transmitted to the bus successively, the sixth bit is automatically transmitted as an opposite bit and automatically eliminated by the receivers. The occurrence of six identical bits despite destuffing will automatically result in the detection of transmission error. Frame structure makes it possible to introduce four additional methods of errors detection (Fig. 8). DLC field indicates the length of data contained in Data Field. CRC field makes it possible to enter checksum consisting of 15 fields for data from Data Field. Inconsistency of sums in the transmitting node and receiving node will result in the transmission of CRC error to the bus. The acknowledging of a bit in ACK field transmitted by the frame recipient will assure the sender that the transmission has been effective. CAN protocol frame has a constant format (equal sizes of fields in the frame). In case of a non-conformity of the bits number with the assumed ones, "frame error" will be generated by any frame recipient.

Presented characteristics of CAN bus and protocol may indicate a high CAN resistance to errors. The estimated number of non-detected errors in relation to the number of bytes transmitted included between 10^{-11} and 10^{-6} [35, 35]. The presented mechanisms do not protect against the introduction of any unknown nodes and additional messages to the bus if the new messages will conform to the required frame format. We could easily imagine that there is a node which will monopolize the bus through continuous transmission of top priority messages.

FlexRay Bus. FlexRay bus is the latest solution dedicated to motor vehicles communication networks which has been applied in practice. The purpose of FlexRay Consortium established in the year 2000 was to develop a solution enabling the communication with a rate higher than in the case of CAN bus and simultaneously ensuring higher security. The bus is mainly dedicated for the supporting of driving systems and active safety systems [3, 38].

The bus can be operated in point – to point topology, star topology, active star topology and hybrid topology, constituting the combination of 3 preceding topologies. Each node can support 2 communication channels. Depending on the applied interface, data transmission is possible by means of 2 wires or fibre optic link. Each channel supports a bandwidth from 10 Mbps. Therefore it is possible to achieve data exchange rate of 20 Mbps or to have a reserve communication channel. The connection between the nodes should not exceed 24 meters.

The nodes communicate by means of frames with the structure presented in Fig. 9. This structure is similar to CAN protocol frame structure. In this case it is also possible to detect errors at the frame structure level. Frame ID indicates frame location in communication cycle. „Payload length” field contains the information on utility data. The header and data are secured by means of checksums.

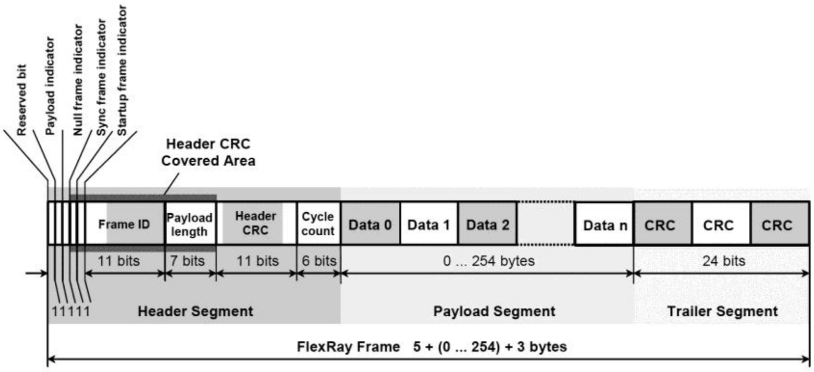

Fig. 9. FlexRay frame format [8]

In case of FlexRay, the control of access to the bus combines the methods applied in LIN and CAN buses. The communication cycle can be subdivided into 4 segments: static, dynamic, symbol window and network idle time. Fig. 10 illustrates a communication cycle without „symbol window”. In the static part, the nodes can transmit data in time slots precisely determined for them (like in case of LIN). In the dynamic part, the nodes communicate depending on their priorities (like in case of CAN). This communication method enables a deterministic data transfer, simultaneously ensuring quick support in case of unexpected events.

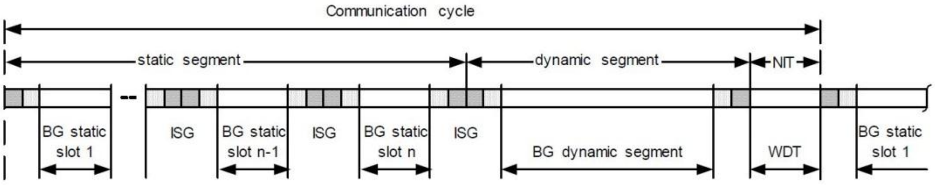

Fig. 10. Bus guardian communication schedule with static and dynamic segment [7]

Bus Guardian module presence in the bus controllers is essential for security assurance [7]. The task of this module is to permit the controller to communicate only in the slots assigned to this controller in communication cycle. Therefore, the possibility of communication disturbance by a single controller on the whole bus is excluded. Additionally, in case of active star topology, it is possible to cut off nodes or network segments generating interfering signals. Owing to these features, FlexRay bus is the fastest and most secure communication bus from among the buses described herein.

PRACTICAL VIOLATION OF SECURITY

The three most common data buses used in motor vehicles and described in the preceding chapter are based on protocols which seem to be resistant to errors to a various degree. The present chapter contains the descriptions of practical experiments consisting in cracking into communication systems in vehicles, descriptions of methods used to disturb the operation of sub-assemblies being the elements of the communication network of a motor vehicle.

Disturbance of motor vehicle functioning by OBD diagnostic port. OBD diagnostic port is an element installed in each manufactured vehicle. Pursuant to ISO 15031-5, diagnostics tester connected to this port can be operated in 9 modes. Most frequently, modes 3 and 4 are most commonly used in vehicle servicing. The modes 3 and 4 consist in reading and deleting permanent defects recorded in the controller. Simultaneously, there are operation modes making it possible to obtain the information on the current parameters of the driving assembly and to take over the control in order to check the correctness of its operation. Additionally, SAE J2534 and ISO 23248 standards define the manner of controllers reprogramming by means of diagnostic protocols [38]. This property is used by a person who wants to disturb motor vehicle operation. False data frames supplied by means of a diagnostic port are not distinguished from frames generated by the vehicle network nodes. Obviously, there is a problem of physical access to the vehicle in order to make the connection to OBD diagnostic connector. Therefore, malice reprogramming is possible only in the case of the vehicle owner's absence. It is unnecessary to use any special diagnostic tester for reprogramming. It is possible by means of software running on PCs communicating with OBD system by means of RS, USB port, Bluetooth network and WiFi. A potential impact on the functioning of motor vehicle controllers has been reported many times [4, 15, 19]. It was also possible to modify the controllers functioning in the course of a vehicle's motion [19].

Software change by means of multimedia system elements. One of the elements of Medium Oriented System Transport shown in Fig. 2 and Fig. 3 is often used as CD or more frequently DVD player. In order to improve the functionality of players, their manufacturers make it possible to update firmware. A properly prepared CD or DVD disc makes it possible to change the player software without the awareness of user. As in the case of "household" players, in selected models update process is triggered by pressing of indicated combination of buttons or updating is carried out automatically [25, 26]. The compromised player constituting an element of MOST bus is still able to affect the multimedia system elements which are frequently used to establish phone, Internet and Bluetooth connections. Changed software can disturb on-board networks systems if it is permitted by multimedia network gate.

Local and remote breaking into vehicle. Variable coding is applied in the central lock systems of vehicles. Therefore it is impossible to open the motor vehicle by means of a known intercepted code. „Man-in-the-middle" attack carried out by an expert in the scope of IT security proved that all the locks with radio pilots are insufficient protections [9]. Samy Kamkar built RollJam device (Fig. 11). RollJam incorporates three antennas. Two antennas are used to disturb the key fob (remote control) signal and the third antenna intercepts this signal at each button pressing. The first key fob signal is intercepted and recorded but not received by the receiver in the vehicle. When the second signal is transmitted, the first recorded signal opening the locks is transmitted by the device. The second recorded signal can be used for locks opening in future [9, 12]. Remote attack methods are based on Telematic systems of exclusive vehicles. The thief knowing the vehicle data and the manner of owner's verification can establish phone connection with vehicles fleet management centre and enforce the vehicle opening in remote mode. Another method of vehicle protection consists in keyless systems and immobilizers based on RFID technology. Practical tests proved that it is possible to build a device effectively simulating RFID transponder operation. In executed tests, apart from the immobilizer blocking removal from the vehicle, it was possible to make the payments verified by means of the device using RFID transponder [1].

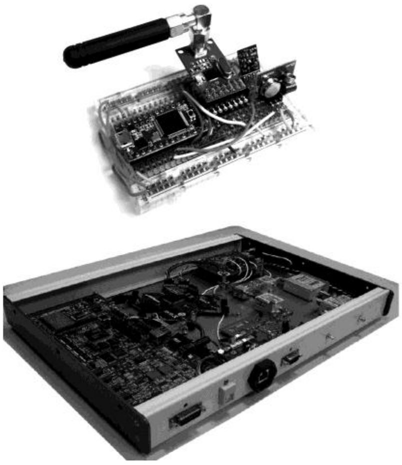

Fig. 11. Universal "remote control" – RollJam (on the left) [11]. Hardware platform for the false GPS transmitter (on the right) [15]

Attack on Bluetooth network. Bluetooth Network support is included in Infotaiment and Cockpit Electronics system (Fig. 3) of each currently manufactured vehicle. The task of Bluetooth interface is to ensure short range wireless communication for personal devices. The present version of standard 1.0 with the bandwidth of 15 Kbps has been upgraded to version 4.2 in December 2014. Multi-functionality of Bluetooth has been reflected in the complex structure of protocols stack illustrated in Fig. 4 and consequently in increased sensitivity to external attacks. The following types of attacks have been reported in the course of Bluetooth development:

- Bluebug – establishing of connections, sending of SMS messages, acquisition of information from the device (e.g. directory) without the user's awareness [29];
- Bluesnarf – acquisition of information e.g. address directory, photos, schedule from a device with Bluetooth interface [14];
- Bluejack – spam transmission / received in the form of visit cards from the devices within radio range after the receipt of properly prepared visit card [29];
- Car whispering – voice interception and sending to car kits or audio devices [14, 27, 29].

The described attacks has been eliminated by later version of protocols in Bluetooth protocols stack, authentication mechanism has been corrected and PIN codes have been made longer. However, it is still possible to listen to a non-encrypted transmission or to record an encrypted transmission in order to decrypt this transmission later. An active Bluetooth interface will be exposed to „Big POLL" attack consisting in continuous responding to POLL packages transmitted by an attacker preventing the devices switchover to low power sleep mode [29].

Attack on satellite navigation system. GPS system considered the first generally accessible navigation system achieved its full functionality in the year 1993. This navigation system facilitates motor vehicle driving performing the role of dynamic chart, facilitates vehicles fleet management and supports the localization of stolen vehicles. Navigation signal disturbance practically makes the vehicle motion impossible. The disturbance of satellite signal seems to be impossible. In practice, GPS receiver prefers the strongest satellite signal. However, a portable transmitter built in the year 2008, is capable to generate information about erroneous position (Fig. 11) [5, 15]. Such device is not capable to disturb the signal for fast moving car but is capable to affect the determination of the route for a parked autonomous vehicle. The presence of such transmitter sending "own" GPS signal can mislead the systems localizing stolen vehicles. It is hard to determine the behaviour of Web VANET network in case of occurrence of a vehicle with deformed position coordinates [17].

Remote taking control over vehicle. Charlie Millerand Chris Valasek are the leading specialists in the scope of intrusions into voice and data transmission networks of motor vehicles [9]. Initial attempts of such intrusions required cable connection with vehicle network. In case of later attempts it was possible in remote mode. A documented attack was carried out to Jeep vehicle. This vehicle was connected with the Internet via UConnect system. Physical connection of UConnect is possible by means of mobile telephony services provided by Sprint company. On the basis of query directed by means of browser it was possible to localize IP address of motor vehicle in Sprint network. Due to a gap in vehicle software it was possible to change firmware of a chip in the vehicle entertainment system. After chip reprogramming to was possible to complete remote commands and to take the control over a majority of a vehicle's sub-assemblies i.e. steering and breaking system, air – conditioning and central lock [9, 11]. In this case, the attack was possible thanks to erroneous software. Therefore it can be classified as the attack to application layer. Remote attack was possible via the link of Spring mobile telephony and Wi-Fi network. This gap has been eliminated from 1.4 million vehicles through software updating.

CONCLUSIONS

Owing to the solutions reducing emission levels, improving safety and comfort of the driver and passengers, the problems associated with vehicle failures are concentrated on electronic systems as well as data processing and transfer systems. Striving for higher comfort and autonomous vehicle motion will intensify the problems associated with on-board computer systems installed in motor vehicles. On the basis of presented functioning analysis for selected communication buses and documented cases of the influence on data exchange influence in vehicles, the following conclusions can be drawn:

1. Protocols and data buses of motor vehicles are characterized by functionality assumed by their authors. The protocols ensure transmission security and rate in accordance with the corresponding classes. They have not been designed in terms of intentional interferences caused by third persons.

2. Newer communication protocols (e.g. FlaxRay) are provided with mechanisms increasing their reliability and security of use (redundant communication channels, increased bandwidth, bus access control by Bus Guardian module).

3. Dynamic development of automotive industry is the source of potential disturbances in data exchange systems operation. Therefore, several electronic, mechatronic and computer sub-assemblies characterized by diversified complexity levels and diversified resistance to disturbances and intrusions and originating from various manufacturers are integrated in the same vehicle.

4. Increased vulnerability of the whole system to disturbances and intrusions is caused by a mix of solutions from various fields of life (automotive industry, consumer electronics, mobile telephony, IT).

5. In most cases, physical vehicle access is required (ODB port, DVD player, Bluetooth communication activating …) to reduce vehicle use safety.

6. The cases of attacks reducing vehicle user safety, analyzed and presented above, require comprehensive theoretical knowledge and research facilities. Attacks are carried out as multi-phase attempts. There is no hazard of fast popularization of effective attacks to computerized vehicles.

REFERENCES

1. **Bono S.C., Green M., Stubblefield A. Juels A., Rubin A.D., Szydlo M. 2005.** Security Analysis of a Cryptographically-Enabled RFID Device. Proceedings of USENIX Security 2005, USENIX Association.
2. **Bosch R. GmbH. 1991.** CAN Specification. Version 2.0, Stuttgart.
3. **Bosch R. GmbH. 2008.** Data exchange network in vehicles. Wydawnictwa Komunikacji i Łączności, Warszawa (in Polish).
4. **Checkoway S., McCoy D., Kantor B., Anderson D, Shacham H., Savage S., Koscher K., Czeskis A., Roesner F., Kohno T. 2011.** Comprehensive Experimental Analyses of Automotive Attack Surfaces. Report for the National Academy of Sciences Committee on Electronic Vehicle Controls and Unintended Acceleration, http://www.autosec.org/pubs/cars-usenixsec2011.pdf.
5. **Cornell University. 2008.** GPS Navigation Devices Can Be Spoofed, Counter Measures Not Effective In Certain Cases. https://www.sciencedaily.com/releases/2008/09/080922122523.htm (23.09.2008).
6. **Fijalkowski B.T. 2011.** Automotive Mechatronics: Operational and Practical Issues. Volume 1. Springer Science+Business Media B.V.
7. **FlexRay Consortium. 2004.** FlexRay Communications System. Bus Guardian Specification, Version 2.0. www.uni-salzburg.at/fileadmin/multimedia/SRC/docs/teaching/SS08/PS_VS/FlexRayCommunicationSystem.pdf.
8. **FlexRay Consortium. 2010.** FlexRay Communications System. Protocol Specification, Version 3.0.1, svn.ipd.kit.edu/nlrp/public/FlexRay/FlexRay%E2%84%A2%20Protocol%20Specification%20Version%203.0.1.pdf.
9. **Gozdek J. 2015.** Hackers without limits. Chip, 11, 104-108 (in Polish).
10. **Gozdek J. 2015.** The spring novelties. Chip, 4, 20-25 (in Polish).

11. **Greenberg A. 2015.** Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired, www.wired.com/2015/07/hackers-remotely-kill-jeep-highway, 21.07.2015.
12. **Greenberg A. 2015.** This Hacker’s Tiny Device Unlocks Cars And Opens Garages. Wired, www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages, 06.08.2015.
13. **Grzemba A. 2008.** MOST - The Automotive Multimedia Network. Frazis Verlag GmbH.
14. **Haataja K., Hyppönen K., Pasanen S., Toivanen P. 2013.** Bluetooth Security Attacks. Comparative Analysis, Attacks, and Countermeasures. Springer Berlin Heidelberg.
15. **Humphreys T.E, Ledvina B.M., Psiaki M.L., O'Hanlon B.W., Kintner P.M. 2008.** Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. Proceedings of ION GNSS, The Institute of Navigation, Savanna, Georgia, USA.
16. **Jaffe E., 2015.** Google's New Self-Driving Car Is About to Hit the Streets. CityLab, http://www.citylab.com/tech/2015/05/googles-new-self-driving-car-is-about-to-hit-the-streets/393323.
17. **Joe M.M., Ramakrishnan B. 2015.** Review of vehicular ad hoc network communication models including WVANET (Web VANET) model and WVANET future research directions. Wireless Networks. Springer Science+Business Media New York.
18. **Korn J. 2015.** Computer: The Sorcerer's Apprentice. Chip, 9, 108-111 (in Polish).
19. **Koscher K., Czeskis A., Roesner F., Patel S., Kohno T., Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., Savage S. 2010.** Experimental Security Analysis of a Modern Automobile. Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, May 16–19, 2010, http://www.autosec.org/pubs/cars-oakland2010.pdf.
20. **Kulas T. 2015.** New methods of security. Chip, 8, 100-101 (in Polish).
21. **Larson U.E., Nilsson D.K. 2008.** Securing vehicles against cyber attacks. Mili and Krings editors, CSIIRW ’08, ACM Press.
22. **Leen G., Hefferman D. 2000:** Talking to the car. The Engineneer, http://www.theengineer.co.uk/news/talking-to-the-car/285325.article, 5 October 2000.
23. **LIN Consortium. 2006.** LIN Specification Package Revision 2.1. tge.cmaisonneuve.qc.ca /barbaud/R%C3%A9f%C3%A9rences%20techniques/Bus%20LIN/LIN-Spec_Pac2_1.pdf.
24. **Merkisz J., Mazurek S. 2007.** On-board Diagnostic Systems of Vehicles. Wydawnictwa Komunikacji i Łączności, Warszawa (in Polish).
25. **Panasonic Corporation. 2016.** DMP-BD10 Firmware Download. http://av.jpn.support. panasonic.com/support/global/cs/bd/download/bd10/europe_uk/index.html
26. **Sony Europe. 2016.** Sony Home Audio and Video: Firmware Download. https://www.sony.co.uk/support/en/content/cnt-dwnl/prd-tvhc/sony-rdrhxd-firmware-update-v170/RDR-HXD870
27. **Soppera A., Burbridge T. 2005.** Wireless identification - privacy and security. BT Technology Journal, Vol 23, 4, 54-64.
28. **Stavens D. M. 2011.** Learning to Drive: Perception For Autonomous Cars. Dissertation Submitted to the Department of Computer Science and the Committee on Graduate Studies of Stanford University, http://purl.stanford.edu/pb661px9942.
29. **Stern A. 2013.** Bluetooth Connectivity Threatens Your Security. https://blog.kaspersky.com/bluetooth-security/1637/ (15.04.2013).
30. **Sumorek A. 2010.** Safe Communication Among Vehicle Sub-Assemblies on the Basis of the Embedded Functions of CAN Protocol. Teka (Archives) of the Commission of Motorization and Power Industry in Agriculture, Vol. 10, 432-439.
31. **Sumorek A. 2010.** The Variability of Electrical Parameters of CAN Protocol Signals in Vehicles. Logistyka, 6, 3263-3272 (in Polish).
32. **Sumorek A., Buczaj M. 2011.** The Problems in Fibre Optic Communication in the Communication Systems of Vehicles. Teka (Archives) of the Commission of Motorization and Power Industry in Agriculture, Vol. 11, 363-372.
33. **Sumorek A., Pietrzyk W. 2011.** Controlling of Access of Mechatronic Nodes to the Information Networks of Vehicles. MOTROL - Motorization and Power Industry in Agriculture, Vol. 13, 290-301 (in Polish).
34. **Sumorek A. 2011.** The Variability of Diagnostic, Control and Multimedia Protocols in Vehicles. Logistyka, 3, 2583-2592 (in Polish).
35. **Tran E., Koopman P. (advisor). 1999.** Multi-Bit Error Vulnerabilities in the Controller Area Network Protocol. Carnegie Mellon University, Institute for Complex Engineered Systems, 33. Pittsburgh.
36. **Widerski T., Kędzierski J. 2004.** Automotive information networks (CAN). Auto Moto Serwis, 4, Warszawa, Wydawnictwo Instalator Polski, 38-42 (in Polish).
37. **Wolański R. 2016.** Every car will be able do it in five years. Chip, 3, 106-107 (in Polish).
38. **Zimmermann W., Schmidgall R. 2008:** Bussystems in Automotivetechnology: Protocolls and Standards. Wydawnictwa Komunikacji i Łączności, Warszawa (in Polish).