Security Extension of Automotive Communication Protocols Using Ethernet/IP

Ján Laštinec*
Institute of Computer Engineering and Applied Informatics
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova 3, 842 16 Bratislava, Slovakia
jan.lastinec@stuba.sk

Abstract

Current vehicles are increasingly depending on Electronic Control Units (ECUs) that control virtually every system of the vehicle. To enable more advanced features automotive embedded systems are opening to external world which raises security concerns. This work deals with the design of a novel approach to secure In-vehicle Systems by taking advantage of Ethernet/IP technology and proven security mechanisms from TCP/IP model. The focus is oriented mainly on the widespread Controller Area Network (CAN). The main goal is to design an efficient solution that meets requirements for latency without requiring high amounts of processing power and provides secure exchange of control signals. The presented solution is based on encapsulation of CAN traffic into UDP datagrams with added authenticity, integrity, and (if required) confidentiality of communication using IPsec protocol in transport mode which creates a âĂIJsecure tunnelâĂİ across backbone Ethernet network in a vehicle. Next part of the paper presents extensive tests both on hardware and in simulation in order to evaluate the characteristics of the designed security extension. The results indicate that using IPsec is a viable solution for securing in-vehicle communications.

Categories and Subject Descriptors

C.2.0 [**Computer-communication Networks**]: General—*Security and protection (e.g., firewalls)* ; C.2.1 [**Computer-communication Networks**]: Network Architecture and Design—*Network communications*; C.2.5 [**Computer-communication Networks**]: Local and Wide-Area Networks—*Buses*; C.3 [**Special-purpose and application-based systems**]: Real-time and embedded systems; C.4 [**Performance of systems**]: Performance attributes

Keywords

Automotive Ethernet, Security, TCP/IP, Controller Area Network, Automotive Embedded Systems

1. Introduction

Communication buses and networks have become a must for today's vehicles. Computations in advanced driver assistance systems are distributed over several Electronic Control Units (ECUs) and sometimes over several different networks. Although the automotive networks have very good safety and reliability properties, there are very few, if any built-in security features in them.

With the rise of external connectivity of today's "connected car" and increasing complexity of software in today's vehicles, they are becoming vulnerable to various IT security threats and attacks [12]. Successful attacks targeting the infrastructure of production vehicles have been demonstrated [6, 10]. Because of the criticality of vehicle control systems it is important to study the security of automotive embedded systems and in-vehicle communication networks.

The remainder of this Section is concerned with explaining state of the art, thesis goals and assumptions. Next Section describes performance case study of TCP/IP security protocols. Section 3 introduces presented solution followed by its evaluation. Possible applications of the proposed security extension are in Section 5 and the final Section gives concluding remarks.

1.1 State of the Art

Vehicle manufacturers and suppliers as well as academic sector have already began to explore the possibilities of increasing vehicle security. Multiple works as well as large European projects between academic and industrial partners emerged in recent years. Research in the area of security of in-vehicle networks focuses mainly on 1) hardware security of control units (especially Hardware Security Modules – HSMs); 2) protecting the firmware of ECUs against unauthorized reprogramming; 3) adding security features (authenticity, confidentiality) to existing technologies; 4) innovative security mechanisms and architectures for existing and probable future technologies, particularly Ethernet/IP. CAN receives the most attention because it is currently the most used technology for

*Recommended by thesis supervisor: Assoc. Prof. Ladislav Hudec
Defended at Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava on [To be specified later].

in-car networks but unfortunately it does not provide sufficient bandwidth for direct application of security mechanisms which results in significant security overhead of proposed solutions.

On the other hand TCP/IP stack provides several mature solutions in the area of maintaining secure communication in the Internet that rely on symmetric and asymmetric cryptography. The identity and authentication of communicating parties is usually achieved using asymmetric cryptography through digital certificates, whereas confidentiality and integrity of exchanged data is by using symmetric cryptography thanks to its computational efficiency.

1.2 Thesis Objective

The central thesis of this dissertation is to design a security extension of existing in-vehicle bus protocols that will allow secure and authentic transmission of communication frames between automotive domains.

In order to fulfil the main thesis, the following partial objectives have been defined:

- Design a method to allow transmission of automotive-bus frames by means of Internet Protocol (IP) or Ethernet technology respectively.
- Design particular security mechanisms in order to ensure the authenticity and integrity of the transmitted messages.
- Implementation of the designed method for a specific automotive bus (e.g. CAN).
- Comparison of performance with existing solutions in the corresponding field.
- Comparison of performance with unsecured communication.

1.3 Assumptions

From the security point of view, the most vulnerable part of the CAN protocol is the messages being broadcasted to every node on the bus without any means to verify the origin of the message. Therefore maintaining the authenticity and integrity of the messages is a priority. The revealing of data flowing on the control bus is not a problem as long as they cannot be maliciously altered by a potential attacker which means that demanding mechanisms to guarantee data confidentiality are not necessary.

In our thesis we assume that attacker does not have physical access to the vehicle's CAN bus. In other words the aim is to secure the on-board networks against attacks from outside (Internet, malicious devices, etc.). No additional restrictions are placed on the attacker.

A "domain-based" architecture of in-vehicle network with Ethernet backbone where respective subsystems are divided into several domains according to their functionality is considered. The communication within domains is managed by so-called "domain controllers" that provide access to/from the underlying networks. This architecture is considered a probable candidate for future in-vehicle network [9].

1.4 Specification

Based on the analysis related work and the dissertation thesis, the requirements that should be satisfied by our solution have been identified as follows:

- Provide integrity and authenticity of the exchanged messages,
- Provide protection against so-called replay attacks,
- Full backward compatibility with current CAN technology,
- Support for next generation "Domain controller" architecture based on the Ethernet/IP,
- Taking advantage of the possibilities provided by Ethernet technology in terms of available bandwidth, payload length, addressing scheme and others,
- Minimal security overhead introduced by the security mechanisms and minimising the impact on processing/memory requirements and timing (usable for real-time communication),
- 10 ms maximal latency of secured traffic between two domains,
- Re-using of existing (and proven) security solutions known from "traditional computing" (such as IPsec) where possible and adapting them for automotive use.

2. Case Study: Performance of TCP/IP Security Protocols

In order to determine performance of standard security protocols from TCP/IP model we conducted a case study. The goal of the experiment was analysis and comparison of performance characteristics of TCP/IP security protocols in in-vehicle application by measuring the round-trip-time (RTT) of message sent between two CAN segments interconnected by Ethernet backbone. For the purpose of the experiment a CAN-Ethernet Gateway was implemented that is based on dual-core ARM Cortex-A9 CPU (1 GHz), 1 GB RAM and GNU/Linux OS. Three topologies were considered but because of minimal influence on the resulting delay, analysis was oriented on topology with one Ethernet switch (Figure 1).

Methodology of the measurement consists of sending 1000 successive messages from CAN node 1 to CAN node 2 (see Figure 1) and back. GW1 encapsulates received CAN messages into secured Ethernet frames and sends them to GW2 where they are decapsulated and sent to CAN interface (CAN2). Then the response traffic travels the reverse path until it is received by the sending node on CAN1. The notion is similar to ICMP echo messages.

The following protocols are evaluated in separate runs of the experiment:

- TCP, UDP – unsecured traffic,
- TCP/AH, TCP/ESP, UDP/AH, UDP/ESP – traffic secured with IPsec AH and ESP respectively (transport mode),
- TLS, DTLS – traffic secured with TLS and DTLS respectively.

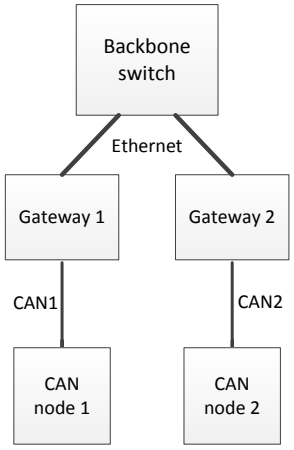

Figure 1: Diagram of Domain Gateway behaviour.

The results show that TLS and DTLS are less suitable for real-time applications. Furthermore, protocols based on connection-oriented TCP have considerable overhead of opening and closing the relations. The assumption that IPsec/AH in combination with UDP transport provides the best performance was confirmed by the measurements. However, we note that other protocols based on UDP or TCP using only one connection are suitable alternatives and the particular solution depends on the traffic characteristics and system requirements.

3. Proposed Solution

The proposal extends the concept of hierarchical in-vehicle network architecture with IP-based backbone by adding security services to the communication occurring on the backbone layer.

Main idea is to offload the security processing from regular control units to powerful Domain Gateways and secure the communication that occurs on the Ethernet/IP backbone. Control frames from lower-layer automotive buses are encapsulated into Ethernet/IP packets by the gateways, and therefore it is possible to reuse proven security protocols from TCP/IP model to implement needed security services. The design therefore effectively minimizes processing requirements for ECUs and does not limit the payload size of automotive frames.

3.1 Domain Gateway

The Domain Gateway is an essential element of the security architecture. It performs similar functions as domain controller ECU that is mentioned in literature dealing with automotive Ethernet and domain-based architecture but extends its functionality by providing security services for the forwarded communication. Basic behaviour of the Domain Gateway is shown by a diagram in the Figure 2. Details of the functions performed by the Domain Gateway are discussed in later Sections.

3.2 Encapsulation Protocol

In order to successfully transmit messages from domain network over the backbone network an encapsulation protocol is needed. The specification of existing protocol that supports transmission of CAN traffic via Ethernet was

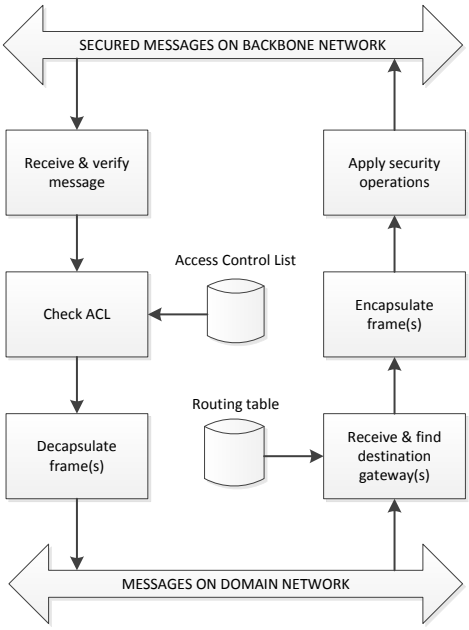

Figure 2: Diagram of Domain Gateway behaviour.

not found during our analysis. Related works either do not explicitly state the protocol used or they are oriented on slightly different goal like for example a method suggested in [8]. The authors do not present exact protocol but rather they are oriented on method to convert CAN messages into UDP segments. On the other hand our goal is to provide a method to tunnel CAN messages over Ethernet/IP-based network.

Therefore a self-designed protocol has been created to allow CAN messages to be encapsulated into Ethernet/IP packets without losing any information. The aim is to provide a method of communicating between several CAN networks through Ethernet network (i.e. tunneling CAN traffic through UDP/TCP). Thanks to the encapsulation into transport layer segments, it is possible to engage security protocols from TCP/IP model to secure the control data.

Main features of the protocol are:

- Support for both UDP and TCP transport thanks to the fact that it operates on the application layer,
- Extensible to support different automotive bus technologies (this document is oriented mainly on CAN),
- Support for N:1 mapping of fieldbus frames into transport layer segments which allows to decrease bandwidth requirements,
- Message priority based on the encapsulated data (CAN ID) which allows advanced strategies to be used when processing multiple messages,

Attention is oriented mainly on the support of CAN Bus due to its widespread use in automotive systems. Due

to the broadcast nature of vehicle protocols it is recommended to use UDP as transport layer protocol.

3.3 Traffic Forwarding

Domain Gateway translates and forwards communication between the backbone and its local bus system according to some scheme given by a gateway strategy.

3.3.1 Gateway strategies

Gateway strategies define a method of encapsulating CAN-Bus frames into Ethernet/IP packets. Essentially there are two possible ways of the transformation – 1-to-1 and n-to-1 mapping. The concept and results from [7] are taken as a reference in this work. The evaluated approaches are listed below for the sake of completeness along with the description of our suggestion to extend the urgency approach by considering the priority of CAN messages also during transmission to destination CAN.

- *one-to-one strategy* – uses one-to-one mapping of CAN frames to UDP segments.
- *buffered strategy* – stores received CAN frames in a buffer and transmits them in one UDP segment either if the buffer is full or a timer associated with the buffer has timed out.
- *timed strategy* – adds an option to dynamically decrease the timer value based on the priority of incoming CAN frame in order to lower the latency.
- *urgency strategy* – extends timed strategy with a functionality to instantly send the buffered frames in case a high priority frame is received.
- *priority strategy* – takes advantage of the priority feature of proposed encapsulation protocol to order the encapsulated messages according to their priority. The receiving Gateway processes Ethernet messages with the highest priority first and the decapsulated frames are sent to destination CAN-Bus also from the highest priority to the lowest.

3.3.2 Forwarding to multiple domains

According to the analysis of in-vehicle domains, current vehicles require information exchange between virtually every domain. We propose to split the CAN message set based on the destinations of the messages and use multicast addressing in order to utilize the backbone network bandwidth efficiently and minimize the latency.

3.4 Security Layer

Based on the results of conducted case study and automotive requirements identified during analysis IPsec protocol in transport mode was chosen for providing authenticity, integrity, replay-protection and (optionally) confidentiality for backbone communications. Additional advantage is that IPsec security services are transparent for programmer and he/she does not need to "think" about security during the development of an application – security services can be configured centrally as a service or middleware module. This enables easier implementation of security services and improves manageability and flexibility of the solution as well. During the design of the security extension we proceeded according to the guidelines described in the Best Current Practice document BCP 146 [3].

Another function of Domain Gateway is access control using Access Control Lists (ACL) that filter traffic between domain bus and backbone network. Thanks to ACLs it is possible to mitigate unwanted communication (e.g. in case of compromised node on the local CAN). Implementation of this mechanism is out of scope of this work but we propose following functional requirements: support for defining allowed CAN identifiers for Gateways; support for defining allowed traffic from local network; usage of "white-list" principle; support for different filtering criteria (identifier, message periodicity, etc.).

Because in-vehicle network architecture is practically static it is possible to apply additional configuration to increase security and safety of the backbone network. It is recommended that the IP addresses of Domain Gateways are statically configured to mitigate vulnerability of DHCP protocol to Man-in-the-Middle (MitM) attacks. Another measure is to configure static ARP tables on the backbone which can also increase performance (no need for ARP exchange). Furthermore the encapsulated control traffic should be transmitted on a dedicated Virtual LAN (VLAN) that has suitable quality of service (QoS) configured.

4. Evaluation

We evaluated the proposed solution in OMNeT++ simulation environment [2] using INET, CoRE4INET and FiCo4OMNet models [1, 11, 5].

Goal of the experiment is determining latency of secured communication between two CAN domains and comparing the results with unsecured traffic. The aim to evaluate timing properties of the solution in multiple scenarios including single and bidirectional traffic and impact of background traffic and prioritization on the backbone network. The parameters of simulation model are based on the real-world measurements obtained in case study. We measured latency of communication between nodes one different CAN buses similarly to the case study, however, in order to simulate real-world CAN example, nodes and CAN message sets are generated by using NETCAR-BENCH [4] which is a freely available benchmark generator for automotive communication systems.

Simulation results show that end-to-end latency is influenced by several factors with varying rate. The most significant influence on measured latency values is caused by the choice of gateway strategy – one-to-one strategy provides the best performance in terms of latency and jitter but the overhead on the backbone network is the highest. The next significant factor influencing the results is the rate of traffic that is forwarded between domains. Furthermore the utilization of destination CAN network and the composition of CAN IDs has also noticeable impact on the delay of traffic. The influence of background streams is minimal as long as the backbone network is not overloaded[1].

5. Possible Applications

Proposed security extension is mainly oriented on securing in-vehicle communication. An example of secure Electronic Stability Programme (ESP) system is depicted in

[1] In this case the latency starts to increase linearly due to buffering which leads to exceeding specified 10 ms hard limit.

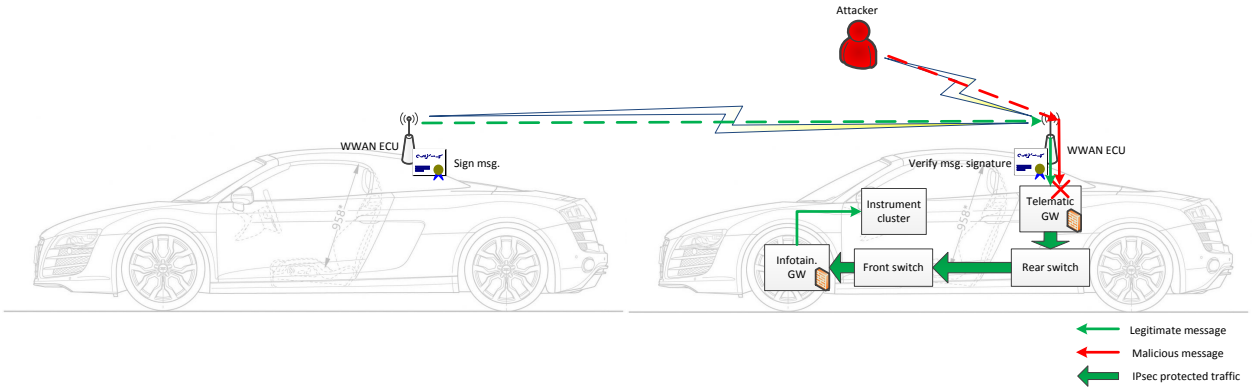

Figure 5: Use-case 3: secure vehicle-to-vehicle communication.

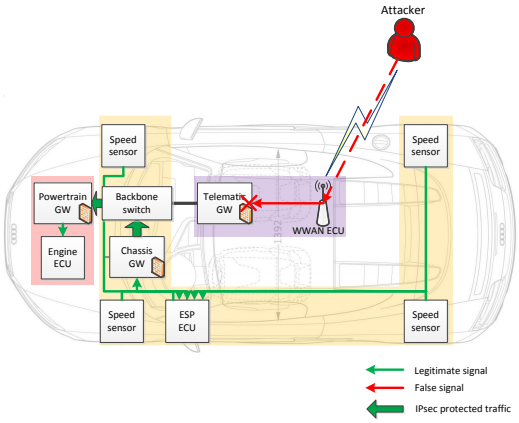

Figure 3: Use-case 1: secure ESP system.

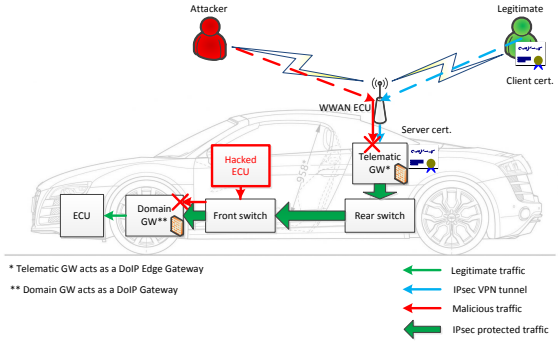

Figure 4: Use-case 2: secure firmware uploading.

the Figure 3. An attempt to inject false signals to Engine ECU is prevented by applying ACL on the Telemtatic Gateway. The authenticity of legitimate signals can be verified by Powertrain Gateway.

The solution is compatible with external communication as well. Use-case 2 (Figure 4) shows a possible way to defend against malicious firmware reprogramming. In this case a certificate authenticated IPsec tunnel is first established to reach the vehicle, effectively blocking the attacker. Furthermore it can be verified that programming messages are transmitted by Telematic GW and not Hacked ECU.

It is also possible to integrate the proposed solution with vehicle-to-vehicle communication as shown in the Figure 5 where messages between vehicles are signed and verified using e.g. asymmetric keys and again the authenticity of messages can be verified at the receiver side.

6. Conclusions and Contribution

In this work we present a security extension of automotive communication protocols that uses Ethernet/IP technology – the most probable candidate for next-generation in-vehicle networking. The presented solution is based on encapsulation of automotive frames into UDP datagrams with added authenticity, integrity and (if required) confidentiality of communication using IPsec protocol in transport mode which creates a "secure tunnel" across backbone Ethernet network. Proposed method and Gateway have been implemented and evaluated for Controller Area Network which is currently the most widespread automotive bus technology. It has been carried out in simulation environment with configuration based on experiments on real hardware to confirm that the solution meets automotive timing requirements and to identify its characteristics. Results of the performance evaluation indicate that implementation of IPsec protocol support in automotive embedded operating systems would be beneficial to improve the security of communication in "connected" vehicles. Moreover the concept is compatible with Car2X communication and provides possibilities to integrate it with security solutions for e.g. vehicle-to-vehicle communication.

The contribution of this work is the development of a novel approach to secure the control communication in automotive systems that takes advantage of emerging Ethernet/IP applications in vehicles and proven security solutions from TCP/IP communication model, notably IPsec protocol. Presented solution contributes to research in the field of Applied Informatics by designing an extensible method to encapsulate automotive bus traffic into IPsec-protected datagrams and experimentally proving that IPsec can be used to protect information exchange in a next generation in-vehicle system architecture.

Acknowledgements. This work was partially supported by research grants VEGA 1/0722/12, VEGA 1/0774/16, Programme for supporting young researchers, and Eset Research Centre.

References

[1] INET Framework for OMNet++. `http://inet.omnetpp.org/`. [Online; accessed Oct 29th, 2014].

[2] OMNet++. `http://omnetpp.org/`. [Online; accessed Oct 29th, 2014].

[3] S. Bellovin. Guidelines for Specifying the Use of IPsec Version 2. BCP 146 (Informational), February 2009.

[4] C. Braun, L. Havet, and N. Navet. NETCARBENCH: a benchmark for techniques and tools used in the design of automotive communication systems. In *7th IFAC International Conference on Fieldbuses & Networks in Industrial & Embedded Systems (FeT 2007)*, Toulouse, France, November 2007.

[5] S. Buschmann, T. Steinbach, F. Korf, and T. C. Schmidt. Simulation-based Timing Analysis of FlexRay Communication at System Level. In *SIMUTools 2013 – 6th International OMNeT++ Workshop*, pages 285–290, New York, USA, March 5-8 2013. ACM DL.

[6] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, pages 6–6, Berkeley, CA, USA, 2011. USENIX Association.

[7] A. Kern, D. Reinhard, T. Streichert, and J. Teich. Gateway strategies for embedding of automotive can-frames into ethernet-packets and vice versa. In *Proceedings of the 24th International Conference on Architecture of Computing Systems*, ARCS'11, pages 259–270, Berlin, Heidelberg, 2011. Springer-Verlag.

[8] A. Kern, T. Streichert, and J. Teich. An automated data structure migration concept - From CAN to Ethernet/IP in automotive embedded systems (CANoverIP). In *Design, Automation Test in Europe Conference Exhibition (DATE), 2011*, pages 1–6, March 2011.

[9] H.-U. Michel. ARAMiS in the Automotive Domain. In *ACROSS Workshop on Integration of mixed-criticality subsystems on multi-core processors at HIPEAC 13*, Berlin, Germany, January 2013.

[10] C. Miller and C. Valasek. Car Hacking: The Content. `http://blog.ioactive.com/2013/08/car-hacking-content.html`, August 2013. [Online; accessed Oct 17th, 2016].

[11] T. Steinbach, H. Dieumo Kenfack, F. Korf, and T. C. Schmidt. An Extension of the OMNeT++ INET Framework for Simulating Real-time Ethernet with High Accuracy. In *SIMUTools 2011 – 4th International OMNeT++ Workshop*, pages 375–382, New York, USA, March 21-25 2011. ACM DL.

[12] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi. Survey on security threats and protection mechanisms in embedded automotive networks. In *Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on*, pages 1–12, June 2013.

Selected Papers by the Author

J.Laštinec, L.Hudec. Approach to Securing In-vehicle Networks using Ethernet-IP. IN *Computer, Information, Systems Sciences & Engineering Conference, CISSE 2014 Online E-Conference. Proceedings.* (In print)

J.Laštinec, L.Hudec. A performance analysis of IPSec/AH protocol for automotive environment. In *Proceedings of the 16th International Conference on Computer Systems and Technologies CompSysTech '15*, pages 299–304, Dublin, Ireland, 2015. ACM.

J.Laštinec, L.Hudec. Comparative Analysis of TCP/IP Security Protocols for Use in Vehicle Communication. In *ICCC 2016 : 17th International carpathian control conference.*, pages 397–403, Tatranská Lomnica, Slovak Republic, 2016. IEEE.