INTERNATIONAL JOURNAL OF COMMUNICATIONS
Issue 4, Volume 5, 2011

Security of transport telematic solutions

Tomas Zelinka, Miroslav Svitek, Zdeněk Lokaj, Martin Srotyr

***Abstract*—**Intelligent Transport Systems (ITS) solutions require availability of the secure seamless communications solutions and coverage of the widely spread areas is typically demanded. Different solutions require different levels of the telecommunications service quality. These parameters are linked with ITS service performance parameters used to quantify services parameters. Even though quite extensive range of wireless data services with reasonable coverage are provided by public telecommunications providers practically all services are provided with no guaranteed data service quality and security. ITS requirements can be better resolved if typically used public solution can be combined with both other public and private services where and when it is needed. Such solution requires implementation of the relevant flexible system architecture supported by the efficient decision processes. This paper is, however, primarily concentrated on the telecommunications security issues quantified by specific security performance parameter. Level of telecommunications service security depends on the ITS service requirement and its mutual relation is not typically trivial to be identified. "Car to Infrastructure" and "Car to Car" communication as well as vehicles on board data communication via Controlled Area Network (CAN) bus are areas with progressive growth of transferred data volumes. Such type of networking increase potential of the appearance of the intruder attacks, namely, if the security of the wide area networks is not carefully enough treated. Probability of hazards appearances principally grows if these networks are integrated in the dynamically organized wide area ones. That is also reason why relevant telecommunications security treatment is more and more understood as the crucial part of the ITS telecommunications solution. Besides of available "off shelf" security tools solution based on the non-public universal identifier with dynamical extension and data availability control according to the actor role or category is presented.

***Keywords*—**Intelligent Transport System, Telematics, system performance, moving object identification, data security.

I. Introduction

PRESENTED results are related to projects e-Ident, DOTEK and SRATVU.

The processes in the ITS architecture are defined by chaining system components through the information links – see Fig. 1. The system component carries the implicit system function (like F1, F2, F3). The terminator (e.g. driver, consignee, emergency vehicle) is often the initiator and also the terminator of the selected process.

T. Zelinka, M. Svitek, Z. Lokaj and M. Šrotýř are with the Faculty of Transportation Sciences, Czech Technical University, Konviktska 20, 110 00 Prague 1, Czech Republic (e-mails: zelinka@fd.cvut.cz, svitek@fd.cvut.cz, lokaj@fd.cvut.cz, srotyr@fd.cvut.cz)

The chains of functions (processes) are mapped in physical subsystems or modules. Second process is defined e.g. by chaining the functions G1, G2 and G3 and information flows between functions specify the communication links between subsystems or modules. If time, performance or other constrains are assigned to different functions and information links, the result of presented analysis is represented by table of system requirements assigned to each physical subsystem (module) and physical communication link between subsystems.

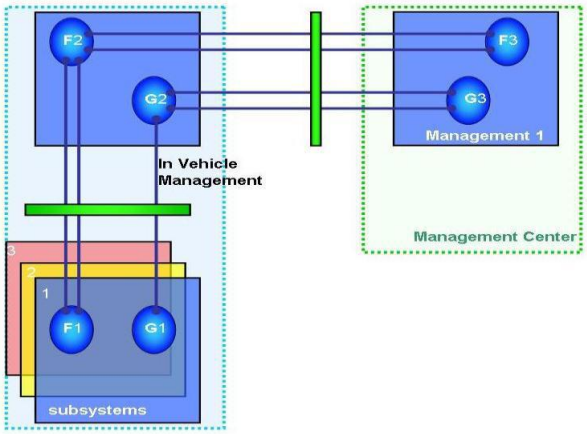

Fig. 1 ITS architecture

It is feasible to consider creation of several subsystem classes of the modular sub-system structure. In this case addition of appropriate optional module can extend or improve system parameters. The same principles are applied in the communication solution design. Such decomposition also simplifies analysis as well as synthesis of the systems where security parameters are accepted as the critical criteria.

II. Telematic sub-system Requirements

The methodology for the definition and measurement of following individual system parameters is being developed in frame of the ITS architecture and it is described in [1] - [5]. Individual system parameters – performance indicators - were accepted in frame of the ITS architecture:

- Reliability - the ability to perform required function under given conditions for a given time interval.
- Availability - the ability to perform required function at the initialization of the intended operation.
- Integrity - the ability to provide timely and valid alerts to the user when a system must not be used for the intended operation.

- Continuity - the ability to perform required function without non-scheduled interruption during the intended operation.
- Accuracy - the degree of conformance between a platform's true parameter and its estimated value, etc.
- Safety - risk analysis, risk classification, risk tolerability matrix, etc.

Decomposition of system parameters enables application of the follow-up analysis of telematic chains according to the various criteria (optimization of the information transfer between a mobile unit and processing centre, maximum use of the existing information and telecommunication infrastructure, etc.). It is obvious that quantification of requirements on relevant telecommunication solutions within telematic chains plays one of key roles in this process.

Mobility of the communication solution represents one of the crucial system properties namely in context of specific demand on availability as well as security of the solution.

Following communications performance indicators quantify communications service quality (see e.g. [6] - [10]):

- Availability – (Service Activation Time, Mean Time to Restore (MTTR), Mean Time Between Failure (MTBF) and VC availability),
- Delay is an accumulative parameter and it is effected by either interfaces rates, frame size or load/congestion of all in line active nodes (switches),
- Packet/Frames Loss (as a tool which not direct mean network failure),
- Security.

Performance indicators applied for such communications applications must be transformable into telematic performance indicators structure and vice versa. Indicators transformability simplifies system synthesis. Additive impact of the tecommunications performance indicators vector $\overrightarrow{tci}$ on the vector of telematics performance indicators $\Delta\overrightarrow{tmi}$ can be expressed as $\Delta\overrightarrow{tmi} = TM \cdot \overrightarrow{tci}$, where TM represents transformation matrix. It is valid, however, only under condition that probability levels of all studied phenomena are on the same level and all performance indicators are expressed exclusively by parameters with the same physical dimension – typically in time or in time convertible variable (see e.g. [7]). Transformation matrix construction is dependent on the detailed communication solution and its integration into telematic system. Probability of each phenomena appearance in context of other processes is not deeply evaluated in the introductory period, when specific structure of transformation matrix is identified. In [7] - [10] are presented details of proposed iterative method.

III. COMMUNICATIONS SOLUTION

Figure 2 presents telecommunications chain diagram, originally applied within the pilot project at Airport Prague (see e.g. [7]). We accepted this structure as typical architecture of ITS telematic solutions. On Board Units (OBU), GNSS Sensing System (SS) and set of Wireless Units (WL) are installed in the moving object. SS applies now exclusively GPS (Global Positioning System with no SLA publicly available), but there is expected launch of the European Galileo GNSS services as well as the second generation of the GPS services with guaranteed quality of service. OBU represents not only control but also display and human communication services and WLi represents i-th cellular technology of the wireless complex solution. Terrestrial communication part consist of set of mobile cellular Base Stations (BSij) (i-th bases station of the j-th cellular system) integrated by the terrestrial network based on L3/L2 switches/nodes (TNi) interconnected with Servers (Si). E2E (End to End) service is provided based on

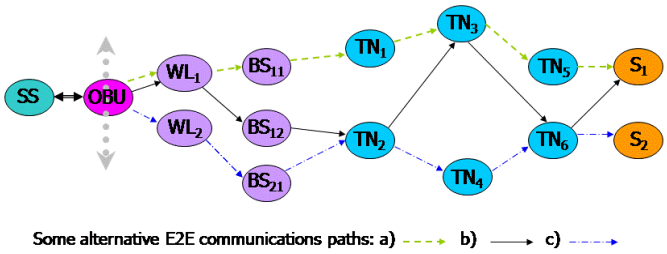

Fig. 2 Telecommunication scheme in chain diagram

One preferred core access wireless technology would be accepted (if possible) as the core solution to be combined with alternative solutions when and where it is needed. Principles of procedures supporting selection of the best possible communications solution quantified both by performance indicators and some other parameters e.g. like service cost, company policy as well. ISO TC204, WG16.1 "Communications Air interface for Long and Medium range" (CALM) group presented their complex approach to resolve described procedures – see e.g. [11] or [12]. Complexity of the ISO approach offers solution with transparent RM OSI compatible architecture, however, such approach also represents highly demanding implementation phase requiring most probably some additional years to reach the market in reasonable pricing.

The IEEE 802.21 presents handover in heterogeneous networks standard known as Media-Independent Handovers (MIH) – see [18]. The standard is designed to enable mobile users to use full advantage of overlapping and diverse of access networks. IEEE 802.21-2008 provides properties that meet the requirements of effective heterogeneous handovers. It allows transparent service continuity during handovers by specifying mechanisms to gather and distribute information from various link types. The collected information comprises timely and consistent notifications about changes in link conditions and available access networks. Scope of IEEE 802.21-2008 is restricted to access technology independent handovers and additional activities in this area are on the way. Handover decision and target assessment constitute a multiphase process where the assistance of IEEE 802.21 is essential. However, the actual handover execution is outside

the scope of the IEEE 802.21 standard.

Authors of this paper recently introduced easily implementable alternative solution applicable namely for compact solutions like On Boar Units (OBU) where all telecommunications technologies units are integrated into one compact system. This alternative was adoptable in much shorter time horizon if compared with system based on complex ISO CALM approach or IEEE 802.21 standard. Authors´ research team goal is to enable its solution for implementations in time period before solutions based on accepted CALM or 802.21 standards are commercially available in reasonable pricing. Authors adopted L3 "intelligent" routing which allows fast implementation namely in compact units like vehicle OBUs. It is based dominantly on the SW package system integration with minimal or no additional requirements on HW specific support. Results of the research are summarized e.g. in [31].

IV. Data security

Security performance indicator (see e.g. [15]) describes ability of the system to ensure that no material damage or loss of human life will occur in cases of any non-standard events like e.g. fake transaction. It means that system detects the forgery on a defined level of probability.

$$P\left(\left|W_i - W_{m,i}\right| \le \varepsilon\right) \ge \gamma \qquad (1)$$

This equation describes that the absolute value of difference between desired risk situation W_i and real situations of risk $W_{m,i}$ does not exceed ε on the probability level γ.

There are many parameters which describe properties of the system which are derived from telematic performance indicators like

- Continuity,
- Integrity,
- Security.

On the other hand the identification can by described as through identification indicators such as:

- Success of identification,
- Accuracy of identification,
- Unique identification,
- Authenticity of the identification.

Properties of the vehicle identification as a part of the telematic chain are influenced by:

- Speed (reader vs. receiver),
- Distance,
- Data volume,
- Weather conditions,
- Communication medium (access network),
- Method of securing the communication channel,
- Transaction security method.

"Car to Infrastructure" (C2I) and "Car to Car" (C2C) communication as well as vehicles on board data communication via Controlled Area Network (CAN) bus are areas with progressive growth of transferred data volumes. If private on board network solution is not connected to any communication cannel than such system can remain reasonably secure and no additional security treatment is typically needed and implemented. However, vehicle private data network security and integrity can be violated in a moment when this network is connected to any other device or network. It is absolutely necessary to take in account that most of vehicles with the CAN based network architecture are minimally equipped with interface for diagnostics purposes, nevertheless, above that interconnection of the CAN bus to the C2C or C2I communications structures becomes "trendy". Data available on the CAN interface are applicable for remote wireless identification of the car or its parts identity or car elements functionality and history of each part status. However, in such applications data security represents sensitive issue to be carefully studied and treated.

Most of vehicle units interconnected via CAN which can be attacked by hackers with the potential of even fatal consequences. The reliable and secure identification of both partners for remote communication represents one of important security tools to prevent unauthorized exchange of any data. It must be combined with other security tools like encryption. Authentication of two actors for mutual communication based on identifier like VIN code or OBU-ID, however, is not acceptable as sufficient tool and extended approach is strongly required.

Second security aspect which follows authentication is data privacy and actors authorization to provide relevant data. Authors´ approach is based on selective data transmission according to the actor role/category. Proposed security approach is based on two steps – reliable and secure authentication and the only relevant to actor's rights data exchange (data which can be provide to the actor). These tools must be combined with other available security tools.

The third aspect of security is to use the approach to prevent the legalization of stolen cars, which are dismantled after the theft to the individual parts as well as parts from stolen vehicles. VIN code and the other identifiers can be included in the new vehicle documents, however, by implementation of the electronic authentication of key parts of each vehicles via CAN bus by in vehicle integrated OBU such crime activities can be substantially limited.

A. Unique identifier

Presented approach is based on usage of Universal Identifier of Vehicle (UIV) is generated as set of all important partial vehicle identifiers where each of them describes non-changeable part of the car detailed identification.

Choice of important identifiers and characteristics of the vehicle must be based on an analysis of the vehicle as a system, which is a purposefully defined as a set of parts or elements and set of links of certain attributes which determine the characteristics, behavior and function of the system as a whole. The vehicle as a system decomposition is performed in order to find basic elements of the vehicle and links between them, as shown in Figure 3.

Based on vehicle decomposition there are examples of partial identifiers and vehicle properties which describes vehicle as a whole:

- VIN (Vehicle Identification Number),
- No. of axles,
- Emission class,
- Vehicle weight,
- Year of its manufacture,
- Optional list of key identifiers and characteristics of the vehicle like:
  - Chassis Ident. No.
  - Engine type and Ident. Number, No.,
  - Transmission type and Ident. No.,
  - Front axes and suspension,
  - Rear axle/-s and suspension,
  - Wheels and tires.

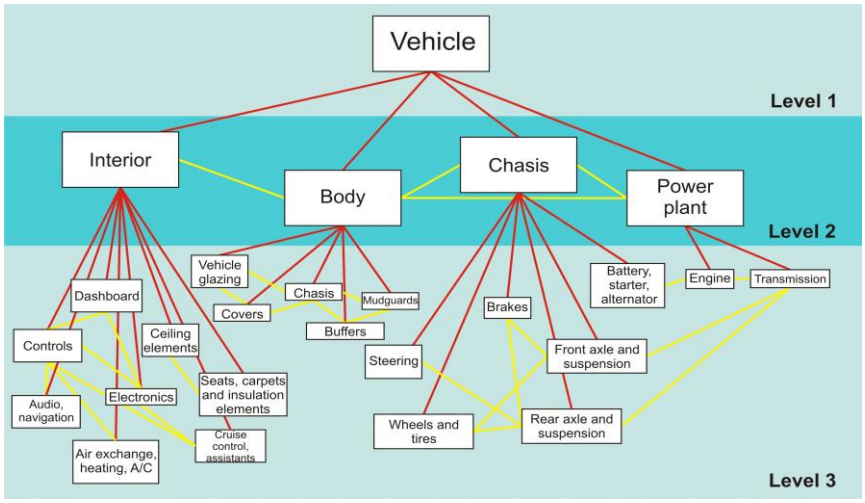

Fig. 3 Vehicle decomposition

The UIV represents set of partial identifiers extended by unique non-public part generated from agreed data by standard cryptography algorithm (e.g. AES or SHA-2) to prevent possibility of UIV algorithm identification in case set of identifiers is for any reason known to the hacker. Check part at the end of identifier is connected for fast check of identifier validity (like validity check of credit card number). The example of UIV is on the Fig. 4.

Fig. 4 Example of unique identifier

It is not necessary to take care of UIV uniqueness because this functionality is ensured by unique VIN code. Advantage of such approach is in fact that complex information about vehicle integrated in the UIV can be used for different telematic applications. Threat of sensitive data abuse is prevented by the data selection availability to the user in dependence on the service class assignment to each one. System allows to use the only that parts of identifier which is dedicated to identified service class – like emergency, public and commercial services.

A. Communication and secure identification

As we described above due to high sensitivity on data privacy exchanged between vehicle and service infrastructure UID must be reasonably protected against potential hackers´ attacks. Three categories of telematic system security in ITS are provided:

- Identifier and data security in vehicle (vehicle environment),
- Identifier and data security for data transmission (wireless environment),

- Identifier and data security in receiver part (server area).

In this paper the only intermediate part - wireless environment - will be discussed.

The communication channel can be secured e.g. by application of a VPN (Virtual Private Network) or a cryptographic SSL (Secure Sockets Layer). If the attack is successful than misuse transferred data can be misused by hacker. Proposed approach to the data security yields lies in the dynamical component extension (time and position dependency) and symmetric or asymmetric encryption, which is chosen depending on the application.

For Point to Point (P2P) communication symmetric encryption can be effectively applied. In such case e.g. the Diffie-Hellman (D-H) key exchange or any other newer algorithms based on the D-H principles can be used, i.e. a cryptographic protocol that allows to establish the encrypted connection over an unsecured channel between two communicating parties, without the first explicit agreement of both parties on the encryption key. Result of this process allows generation of the unique symmetric encryption key which can then be used to encrypt further mutual communication. The key advantage of such approach lies in the fact that such symmetric encryption key cannot be identified based on the exclusively "listening". All keys are constructed by participants case by case and communication is never processed in an open form.

The main disadvantage of this protocol is an attack via "man in the middle". Solution on described principles cannot be applied without combination with other methods whenever the attacker can actively interfere with communication channels.

In case of Point to Multipoint (P2M) communications namely if large number of active terminals are served, asymmetric cryptography can be efficiently used, as well.

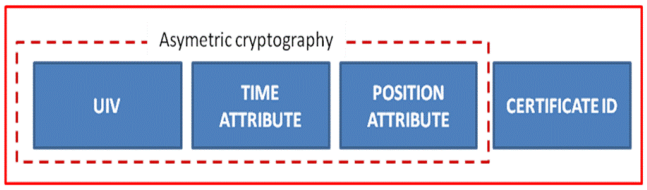

Fig. 5 Dynamic version of the identifier

In this solution the identifier is concatenated by actual time, current GNSS coordinates (i.e. exclusively in direction from by GNSS equipped vehicle to infrastructure) and finally by the user ID. Identifier is than encrypted by either asymmetric or symmetric cryptographic algorithm. Examples described on the Figure 5.

Encryption of the UIV is described as follows:

$$M1 = EK\ (UIV\ II\ T_i\ II\ P_i), \qquad (2)$$

where UIV means Universal Identifier of the Vehicle, EK - asymmetric encryption with public key K, T_i - clock state in time of message generation, P_i - position in time of message generation, UIV II Ti II P_i - identifier with link to current time and position

After receiving the request by the central system, the message M1 is decrypted and UIV is read in „static form" - received time T_i and P_i are checked for validity.

It means, that the message is not older than n seconds and the message has been sent from area with maximum of m meters tolerated difference. Data message with identifier in dynamic format is not impacted by this process and this approach doesn't influence usage of the other security tools.

The goal of this approach is to highly secure data against attacks mainly like eavesdropping and usage of the data for forgery.

Identifier extended by the transaction time and location in a dynamic form is usable for transaction validation. It is possible to apply this information also in the other telematics applications like traffic management.

V. Service Categories

Proposed approach covers categorization of the telematic services. Each category has defined set of data allowed to user application. Because the unique identifier includes complex information about the vehicle there must be special tool implemented on both sides (sender and receiver) which process incoming identifier and transfers and publish the only relevant data to user. On Figure 5 this component is described as an "Interface". This component also covers "dynamisation" of the message content as it was already described above.

Three service categories were defined:

- Security services – e.g. emergency, fire dept., police,
- Public services (public authorities) – e.g. customs,
- Commercial services.

Example on Figure 6 describes public services support dedicated for public institutions. Set of available data is identified by the unique identifier. Hand reader operated by customs officer generates request for identification and sends it to the vehicle unit - encrypted message contains user Public Encryption Key (PEK). Vehicle unit processes the request and sends relevant service category data according to the rights of customs administrations. Category is identified by PEK. User requires for example emission class, number of axles, license plate number, country of origin and OBU ID. Even though the other "public class" data are included in a sent UIV, the interface component splits the unique identifier and the only relevant data are publish, i.e. in this case just emission class, number of axles, license plate number, country of origin and OBU ID. Remaining data from the identifier are suppressed and are kept unreadable for the system.

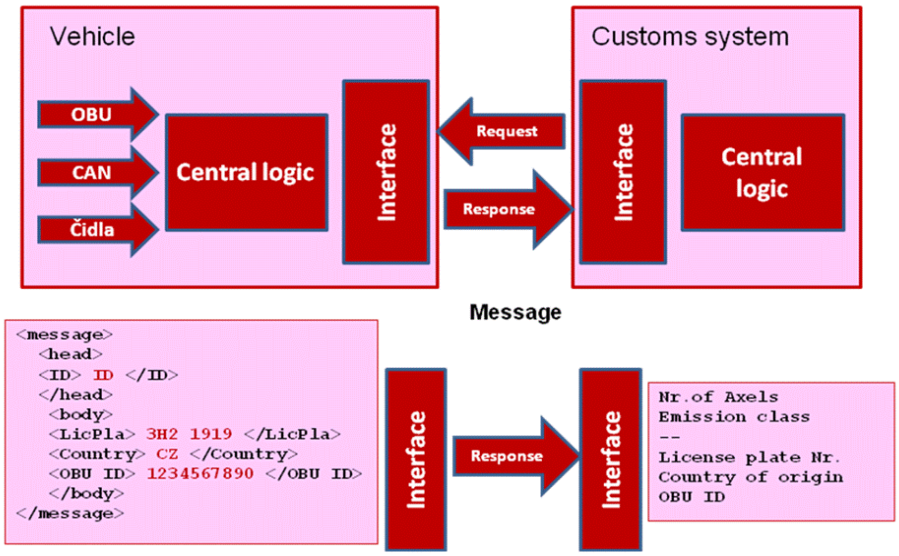

Fig. 6 Public service example – customs administration

Basically the following telematics applications that come into consideration for the use of electronic identification described in this paper:

- Electronic Payment Facilities,
- Safety and emergency Facilities,
- Traffic Management,
- Public Transport Operations,
- Advanced Driver Assistance Systems,
- Traveller Journey Assistance,
- Enforcement systems,
- Freight and Fleet Operation.

I. Acknopwledgement

This project was supported by Ministry of Industry and Business (MPO) and Ministry of Transport (MD) of the Czech Republic via following grants: e-Ident (Electronic identification systems within transport process) MPO 2A-2TP1/108, DOTEK (Communication module for transport telematic applications), MPO 2A-2TP1/105, SRATVU (System Requirements and Architecture of the universal Telematic Vehicle Unit), MPO 2A-1TP1/138, CAMNA (Joining of the Czech Republic into Galileo project), MD 802/210/112.

II. Conclusion

Due to complexity of the ITS services mostly mobile services wide area coverage and selectable classes of services are required. Authors were focused on the wireless access solution designed as seamless combination of more independent access solutions of the same or alternative technology.

Quickly and easily implementable alternative solution to the complex solution based either on family of ISO standards known as CALM or IEEE 802.21 supporting family of standards IEEE 802 and 3G mobile services. Authors adopted software based L3 routing which is relatively simple to be implemented in most of off-shelf OBUs.

C2C and C2I communication as well as vehicles on board data communication via Controlled Area Network bus are areas with progresively growing transfer of data volumes. If private on board CAN based network solution is not connected to any communication cannel than it can be understood as a reasonably secure situation and no additional security treatment is typically needed to be designed and implemented. However, vehicle private data network security and integrity is potentially violated in a moment when internal private vehicle network is connected via wireless service to any other device or any other network. CAN and OBU interconnect will come soon namely due to on private vehicle network representative data availability and their applicability for services like the vehicle and its parts identity and ability to control/influence behavior of any part of the system. However, data security in such applications represents sensitive issue to be carefully studied and treated.

Reliable and secure identification of both partners for remote communication represents between others one of important security tools to prevent unauthorized data exchange. It must be, however, combined with other security tools. Authentication of two actors for mutual communication based on identifier like VIN code or OBU-ID is not possible to accept as a sufficient tool. Identification based on newly designed dynamical Unique Vehicle Identifier UIV is presented as the relevant alternative principally improving

system security integrity.

Another security aspect which follows authentication is data privacy and actors authorization to receive any relevant data content. Authors´ approach is based on selective data transmission and delivery in accordance to the actor role/category. These principles described in this paper are combined with other available security tools like discussed asymmetric data encryption. Such carefully selected combination leads to the solution with relevant level of reached system security.

REFERENCES

[1] M. Svitek, Architecture of ITS Systems and Services in the Czech Republic, International Conference Smart Moving 2005, Birmingham 2005, England.

[2] M. Svitek, Intelligent Transport Systems - Architecture, Design methodology and Practical Implementation, Key-note lesson, 5th WSEAS/IASME Int. Conf. on Systems Theory and Scientific Computation, Malta 2005.

[3] M. Svitek,, T. Zelinka, Communications Tools for Intelligent Transport Systems, Proceedings od 10th WSEAS International Conference on Communications, pp 519 – 522, Athens 2006, ISSN 1790-5117, ISBN 960-8457-47-5.

[4] M. Svitek,, T. Zelinka, T., Communications Solutions for ITS Telematic Subsystems, WSEAS Transactions on Business and Economics, Issue 4 (2006), Vol. 3, pp 361 – 367, Athens 2006, ISSN 1109-9526,

[5] M. Svitek,, T. Zelinka, Telecommunications solutions for ITS. Towards Common Engineering &Technology for Land, Maritime, air and Space Transportation – ITCT 2006, CNISF, Paris 2006.

[6] M. Svítek,, T. Zelinka, Communication solution for GPS based airport service vehicles navigation, EATIS'97 ACM-DL Proceedings, Faro (Portugal) 2007, ISBN #978-1-59593-598-4.

[7] T. Zelinka, M. Svitek, Communication solution for Vehicles Navigation on the Airport territory, Proceedings of the 2007 IEEE Intelligent Vehicle Symposium, Istanbul, Turkey, pp 528–534, IEEE Catalogue number 07TH8947, ISBN 1-4244-1068-1.

[8] M. Svitek, T. Zelinka, Communications Environment for Telematic Subsystems, Proceedings of 11-th World Multi-Conference on Systemic, Cybernetics and Informatics, Volume II, pp 362-367, IIIS/IFSR, Orlando, FL, USA, ISBN-10: 1-934272-16-7, ISBN-13: 978-1-934272-16-9

[9] M. Svitek,, T. Zelinka, Communications Challenges of the Airport Over-ground Traffic Management, Proceedings of the 11th WSEAS International Multi-conference CSCC, Volume – Advances in Communications, pp. 228 – 234, Agion Nikolaos, Crete Island, Greece, ISSN 1790-5117, ISBN 978-969-8457-91-1.

[10] T. Zelinka, M. Svitek, Communications Scheme for Airport Service Vehicles Navigation, Proceedings of International Conference TRANSTEC Prague, Czech Technical University, Faculty of Transport Science and University of California, Santa Barbara, Praha 2007, pp. 160 – 166, ISBN 978-80-01-03782-9

[11] B. Williams, CALM handbook V1.0. Document ISO TC204 WG.16.1 CALM, 2004.

[12] N. Wall, CALM - why ITS needs it, ITSS 6 (September), 2006

[13] T. Zelinka, M. Svitek, CALM - Telecommunication Environment for Transport Telematics, Technology & Prosperity, 2006, Vol. XI, special edition (11/06), ISSN 1213-7162.

[14] K. Yang, J. Wittgreffe, M. Azmoodeh: Policy-Based Model-Driven Creation of Adaptive Services in Wireless Environments. IEEE Vehicular technology Magazine, September 2007, pp. 14-20.

[15] M. Svitek, Dynamical Systems with Reduced Dimensionality, Neural Network World edition, II ASCR and CTU FTS, Praha 2006, ISBN:80-903298-6-1, EAN: 978-80-903298-6-7.

[16] A. Dempster, N. Laird, D. Rubin, Maximum likelihood from incomplete data via EM algorithm. J. Royal Stat. Soc. 39, 1977, pp 1-38.

[17] T. Zelinka, M. Svitek, Communication Scheme of Airport Over-ground Traffic Navigation System. Proceedings of the International Symposium on Communications and Information Technologies - ISCIT 2007. IEEE Sydney, 2007, pp 329 - 334. IEEE Catalogue No. 07EX1682(C), ISBN 1-4244-977-2, Library of Congress 2007920360.

[18] IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks, IEEE, January 2009

[19] M. Svitek,, T. Zelinka, Monitoring of Transport Means on Airport Surface. Advances in Transport Systems Telematics, Monograph edited by Jerzy Mikulski, Selesian University of Technology, Katowice, pp. 285 – 292, ISBN 978-83-917156-6-6.

[20] T. Zelinka, M. Svitek, Decision processes in telematic multi-path communications access systems. International Journal of Communications, North Atlantic University Network NOUN, Issue 2, Volume 1, 2007, pp.11 – 16.

[21] M. Svitek,, T. Zelinka, Communications multi-path access decision scheme. Neural Network World, ICS AS CR and CTU, FTS, Praha, No. 6., 2008, pp 3 - 14, 2008, ISSN 1210 0552,

[22] M. Svitek,, T. Zelinka, Decision processes in Communications Multi-path Access Systems applied within ITS. Transactions on Transport Science, MTCR, Praha, No. 1, 2008, pp 3-12 , ISSN 1802-971X,

[23] T. Zelinka, M. Svitek, Identification of Communication Solution designated for Transport Telematic Applications. WSEAS Transactions on Communications, Issue 2, Volume 7, Athens, 2008, pp 114 – 122, ISSN: 1109-2742.

[24] T. Zelinka, M. Svitek, Multi-path communications access decision scheme. Proceedings of the 12-th World Multi-Conference on Systemics, Cybernetics and Informatics, Volume III, pp 3233-237, IIIS/IFSR, Orlando, FL, USA, ISBN-10: 1-934272-32-7, ISBN-13: 978-1-934272-33-6.

[25] T. Zelinka, M. Svitek,: Adaptive communications solutions in complex transport telematics systems. Proceedings of the 11th WSEAS International Multiconference CSCC 2008, Volume – New Aspects of Communication, pp. 206 – 212, Heraklion, Greece, ISSN 1790-5117, ISBN 978-960-6766-84-8.

[26] T. Zelinka, M. Svitek, Adaptive communications solutions in complex transport telematics systems. Monograph on Computers and Simulation in Modern Science-Volume II, WSEAS Press, Athens 2009, pp. 234 -241, ISBN 978-960-474-032-1.

[27] T. Zelinka, M. Svitek, Adaptive Wireless Access Environment in Transport Solutions. Proceedings of, 13-th World Multi-Conference on Systemics, Cybernetics and Informatics, Volume IV, pp 310 - 315, IIIS/IFSR, 2009, Orlando, FL, ISBN 978-1-934272-62-6.

[28] T. Zelinka, M. Svitek, M. Vosatka, Adaptive Approach to Management of the Multi-path Wirelesss Solutions. Proceedings of the Symposium Recent Advance in Data Network, Communications, Computers, WSEAS Press, Morgan State University, Baltimore, 2009, pp. 161 – 168, ISBN 978-960-474-134-2.

[29] T. Zelinka, M. Svitek, M. Srotyr, M. Vosatka, Adaptive multi-path Telecommunications Solutions for ITS. Proceedings of, 14-th World Multi-Conference on Systemics, Cybernetics and Informatics, Volume I, pp 89 - 94, IIIS/IFSR, 2010, Orlando, FL, USA, ISBN 978-1-934272-98-5.

[30] T .Zelinka, M. Svitek, Z. Lokaj, Adaptive Decision Processes the Multi-path Wireless Access Solutions Implementable on the IP Routing layer. EATIS'10 Proceedings, Panama City (Panama), 2010, ISBN 978-958-44-7280-9

[31] Zelinka, T., Svitek, M., Srotyr, M., Vosatka, M.: Adaptive Multi-path Telecommunications Solutions for ITS, Journal of Systemics, Cybernetics and Informatics Volume 9, No. 1, pp. 14 – 20, Orlando, 2011, ISSN: 1690-4524.