Data security in Intelligent Transport Systems

Tomas ZELINKA
Czech Technical University in Prague, FTS
110 00 Praha 1, Czech Republic

Miroslav SVITEK
Czech Technical University in Prague, FTS
110 00 Praha 1, Czech Republic

Zdenek LOKAJ
Czech Technical University in Prague, FTS
110 00 Praha 1, Czech Republic

Martin SROTYR
Czech Technical University in Prague, FTS
110 00 Praha 1, Czech Republic

ABSTRACT

Intelligent Transport Services expect availability of the secure seamless communications solutions typically covering widely spread areas. Different ITS solutions require different portfolio of telecommunications service quality. These parameters have to correspond with ITS service performance parameters required by specific service. Even though quite extensive range of public wireless data services with reasonable coverage are provided, most of them are provided with no guaranteed quality and security. ITS requirements can be in most parameters easier reached if multi-path communications systems are applied core solution is combined with both public as well as private ones where and when it is needed. Such solution requires implementation of relevant flexible system architecture supported by the efficient decision processes.

This paper is concentrated the telecommunications security issues relevant to the ITS wide area networking. Expected level of security varies in dependence on relevant ITS service requirements. Data volumes transferred both in private data vehicle on board networks as well as between vehicles and infrastructure (C2I) or other vehicles (C2C) progressively grow. Such trend upsurges the fatal problems appearance probability in case security of the wide area networks is not relevantly treated. That is reason why relevant communications security treatment becomes crucial part of the ITS solution. Besides of available "off shelf" security tools we present solution based on non-public universal identifier with dynamical extension (time and position dependency as an autonomous variables) and data selection according to actor role or category.

Presented results were obtained within projects e-Ident[1], DOTEK[2] and SRATVU[3].

1 INTRODUCTION

Telematics is a result of convergence and following progressive synthesis of telecommunication technology and informatics. The effects of telematics are based on synergy of both these disciplines. Telematics is applied in wide spectrum user areas, from an individual multimedia communication towards intelligent use and management of large-scale networks. Advanced telematics solutions provide an intelligent environment for knowledge society and allow expert knowledge description of complex systems. It also includes legal, organizational, implementation and human aspects.

Transport Telematics/Intelligent Transport Systems (ITS) connects information and telecommunication technologies with transport engineering to achieve better management of transport, travel and forwarding processes with no additional requirements placed on the existing transport infrastructure.

2 ITS AND ITS ARCHITECTURE

The ITS system model was adopted within ITS society to support design process of the ITS applications. ITS solution is expected to be designed under principles described on Figure [1] – i.e. following the ITS System Model rules.

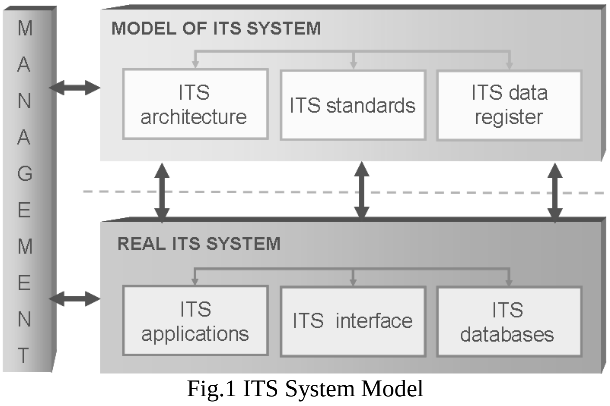


Fig.1 ITS System Model

Management process on Figure 1 represents the methodology of smart ITS design and its maintenance based on application of well-tuned ITS system models.

Definition of set of the individual system parameters was accepted within ITS society, as well:

Accuracy is the degree of conformance between system true parameters and its measured values that can be defined as the probability

[1] e-Ident – Electronic identification systems within transport process – grant 2A-2TP1/108.of Ministry of Industry and Trade of the Czech Republic (MPO),

[2] DOTEK – Communication module for transport telematic applications –grant 2A-2TP1/105 of MPO,

[3] SRATVU – "System Requirements and Architecture of the universal Telematic Vehicle Unit" is grant 2A-1TP1/138 of MPO,

$$\mathrm{P}\left(\left|\mathrm{p_i} - \mathrm{p_{m,i}}\right| \leq \varepsilon_1\right) \geq \gamma_1 \qquad (1)$$

that the difference between the required system parameter p_i and the measured parameter $p_{m,i}$ will not exceed the value ε_1 on probability level γ_1 where this definition is applicable for all N system parameters $p_1, p_2, .., p_N$.

Reliability is the ability to perform a required function (process) under given conditions for a given time interval that can be defined as the probability

$$\mathrm{P}\left(\left|\vec{\mathrm{v}}_\mathrm{t} - \vec{\mathrm{v}}_\mathrm{m,t}\right| \leq \varepsilon_2\right) \geq \gamma_2, \mathrm{t} \in \langle 0, \mathrm{T} \rangle \qquad (2)$$

that the difference between required system functions (processes) represented by parameters $\vec{v}_t$ and the vector of measured parameters $\vec{v}_{m,t}$ will not exceed the value ε_2 on probability level γ_2 in each time interval t from the interval $\langle 0, T \rangle$.

Availability is the ability to perform required functions (processes) at the initialization (triggering) of the intended operation that can be defined as the probability

$$\mathrm{P}\left(\left|\mathrm{q_i} - \mathrm{q_{m,i}}\right| \leq \varepsilon_3\right) \geq \gamma_3 \qquad (3)$$

that the difference between the required rate[4] of successful performing of the function *i* (process *i*) q_i and the measured $\mathrm{q_{m,i}}$ will not exceed the value ε_3 at the probability level γ_3.

Continuity is the ability to perform required functions (processes) without non-scheduled interruption during the intended operation that can be defined as the probability

$$\mathrm{P}\left(\left|\mathrm{r_i} - \mathrm{r_{m,i}}\right| \leq \varepsilon_4\right) \geq \gamma_4 \qquad (4)$$

that the difference between the required rate of successful performing of the function *i* (process *i*) without interruption $\mathrm{r_i}$ and the measured $\mathrm{r_{m,i}}$ will not exceed the value ε_4 at the probability level γ_4.

Integrity is the ability to provide timely and valid alerts to the user, when a system must not be used for the intended operation, that can be defined as the probability

$$\mathrm{P}\left(\left|\mathrm{S_i} - \mathrm{S_{m,i}}\right| \leq \varepsilon_5\right) \geq \gamma_5 \qquad (5)$$

that the difference between the required rate of successful performing of the alert limit (AL) *i* not later than predefined time to alert (TTA) $\mathrm{S_i}$ and the measured $\mathrm{S_{m,i}}$ will not exceed the value ε_5 on the probability level γ_5.

Safety can also be covered among the performance parameters, but the risk analysis and the risk classification must be done beforehand with a knowledge of the system environment and potential risk, and then the safety can be defined as the probability

$$\mathrm{P}\left(\left|\mathrm{W_i} - \mathrm{W_{m,i}}\right| \leq \varepsilon_6\right) \geq \gamma_6 \qquad (6)$$

that the difference between the required rate of *i* risk situations $\mathrm{W_i}$ and the measured ones $\mathrm{W_{m,i}}$ will not exceed the value ε_6 on the probability level γ_6.

A substantial part of the system parameters analysis is represented by a decomposition of system parameters into individual sub-systems of the telematic chain. One part of the analysis is the establishment of requirements on individual functions and information linkage. Then, the whole telematic chain can comply with the above defined system parameters.

The completed decomposition of system parameters enables the development of a methodology for a follow-up analysis of telematic chains according to various criteria (optimization of the information transfer between a mobile unit and a processing center, maximum use of the existing information and telecommunication infrastructure, etc.).

In telecommunication exists wide range of system parameters definitions. We adopted set of performance indicators as follows:

- **Availability**
  - Service Activation Time,
  - Mean Time to Restore (MTTR),
  - Mean Time between Failure (MTBF) and
  - Virtual Connection Availability
- **Delay** as an accumulative parameter effected by
  - Interfaces Rates,
  - Frame Size, and
  - Load / Congestion of all active nodes (switches) in the line
- **Packet/Frames Loss**
- **Security**

These telecommunications performance indicators were specifically redefined with goal of compatibility with telematics performance parameters. Impact of telecommunication performance indicators on the telematic performance must be indicators transformability simplifies system synthesis. The additive impact of the communications 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 the transformation matrix. It is valid, however, under condition that the 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. The transformation matrix construction is dependent on the detailed communication solution and its integration into the telematic system. The probability of the each phenomena appearance in context of the other processes is not deeply evaluated in the introductory period, when the specific structure of transformation matrix is identified. In [7] – [9] are presented details of the proposed iterative method. This method is designed as broadly as possible with a clear aim to be applied in the widest possible range of telematic application. This method can be also successfully used for identification of the decision processes criteria, i.e. the tolerance range of each performance indicator. Such information represents necessary (but not sufficient) condition to let processes decide which access path represents within the defined time period the best possible alternative.

[4] $q_{m,i} = \frac{Q_i}{Q}$ where $\mathrm{Q_i}$ is the number of successful experiments (successful performing of the function *i*, successful performing of the process *i*) and Q is the number of all experiments (both successful and unsuccessful).

3 COMMUNICATIONS SOLUTION STRUCTURE

Figure 2 presents telecommunications chain diagram, originally applied within the pilot project at Airport Prague (see e.g. [7] – [10]). 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 WL_i represents i-th cellular technology of the wireless complex solution. Terrestrial communication part consist of set of mobile cellular Base Stations (BS_{ij}) (i-th bases station of the j-th cellular system) integrated by the terrestrial network based on L3/L2 switches/nodes (TN_i) interconnected with Servers (S_i). E2E (End to End) service is provided based on IP protocol, L2 switching is Ethernet protocol based.

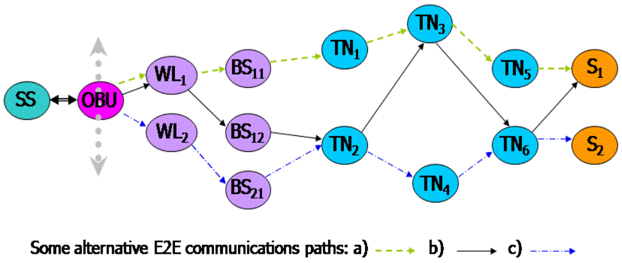


Fig. 2. Telematic telecommunication scheme in chain diagram

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. The core solution would meet dominant service quality and coverage requirements being corrected in the case where such parameters do not meet requirements under specific conditions. Table 1 describes typical behavior of private/public telecommunications solutions.

Tab. 1 Public vs. private services parameters

	Private	Public
Service quality management SLA	Typically Available	Low (if any)
Signal coverage	Cost dependent - Typically low (-er),	High
Pricing/cost	High (-er)	Low (-er)

If we evaluate realistically telecommunications data services market there are only few technology streams available for the ITS demanding applications. Each of these alternatives was studied in detail by authors in specialized laboratories.

4 CALM - SECOND GENERATION HANDOVER PRINCIPLES

Principles of procedures supporting selection of the best possible communications solution quantified both by performance indicators and some other parameters e.g. service cost, company policy. ISO TC204, WG16.1 "Communications Air interface for Long and Medium range" (CALM) group presented their complex approach to resolve described procedures – see. [11] or [12]. A basic tool – the second generation of the handover principles are defined by CALM standards. 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 introduce on the market products with reasonable pricing.

The IEEE 802.21 presents handover in heterogeneous networks standard known as Media-Independent Handovers (MIH). 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 an easily implementable alternative solution. It is applicable namely for compact solutions like On Boar Units (OBU) where all telecommunications technologies units are integrated into one compact system with smart decision adaptive processes process replacing commonly used PBM (see e.g. [14]). 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 has been 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 exclusively on the SW package system integration with minimal or no additional requirements on HW specific support. Results of the research are step by step described in [27] - [31].

5 DOTEK PROJECT

The main objective of the DOTEK project was motivated by the "CALM family" of standards. However, exclusively routing on L3 layer adopted responsibility in the change to the other path process. Results of the DOTEK project can be summarized as follows:

- Analysis and selection of available wireless services applicable for different studied transport telematics services.
- Design of tools for continuous monitoring and evaluation of services quality,
- Realization of the decision to change to the alternative path decision.

Namely due to limited R&D man power resources the first project phase applied "Extended PBM" principles. The complex version below described statistical approach was due to its implementation complexity above the research team capacity. Nevertheless, simplified approach was successfully implemented and tested and authors identified that the 2nd generation handover time-durations are primarily influenced by the GSM network response times, and obtained results presented in the Table 2 reach the only fraction of the critical transport delay times identified with GPRS or EDGE data services (see Fig. 2 and 3).

Table 2. Results of test scenario focused on the time of handover

Test no.	Handover time [ms)
1	208
2	137
3	41
4	108
5	362

The materialization of the project results represents exclusively the SW package with no additional HW requirements. The SW package has got modular structure and solution is practically technologically independent, i.e. integrate-able in most of on the market available OBUs. Tests results confirmed its wide range of its applicability in telematics, namely, in areas where GSM data services performance is acceptable as core communication service.

6 Data security

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

$$P\left(\left|W_i - W_{m,i}\right| \le \varepsilon\right) \ge \gamma. \qquad (7)$$

This equation describes that the difference between desired or non-standard risk situation W_i and real situations of risk or abnormal $W_{m,i}$ does not exceed the level of probability γ.

"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 it remains 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 CAN based vehicles are minimally equipped with interface for diagnostics purposes, anyhow. Above that interconnection of the CAN bus to the C2C or C2I communications structures becomes "trendy" namely due to on network representative data availability applicable for services like car identity or car units integrity or functionality remote identification. However, data security in such applications represents sensitive issue to be carefully studied and treated.

There are many in vehicle systems interconnected via CAN which can be attacked by hackers with potential of even fatal consequences. Reliable and secure identification of both partners for remote communication represents between others one of important security tools to prevent unauthorized exchange of any data. It must be combined with other security tools like encryption or more effective tunneling. 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 must be applied.

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

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. There are some examples of identifiers:

- VIN
- Nr. of axels
- Emission class
- Weight
- Year of manufacture

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. 3.

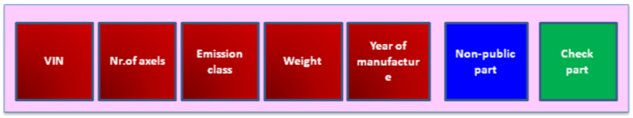


Fig.3. Example of unique identifier

It is not necessary to take care of UIV uniqueness because this functionality is ensured by unique VIN code. Advantage of such approach is that complex information about vehicle integrated in the UIV can be used for different telematic applications. Threat of sensitive data abuse is prevented by data selection availability to user in dependence on 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.

B Communication and security identification

As described above due to high sensitivity on data privacy exchanged between vehicle and service infrastructure VID 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 wireless environment part will be discussed.

The communication channel might be secured by standard cryptography methods, however, insufficient protection might be broken and hacker´s successful attack can misuse transferred data with fatal consequences. Proposed approach to data security yields in dynamical component extension (time and position dependency) and symmetric or asymmetric encryption, which is chosen depending on application.

For Point to Point (P2P) communication typically symmetric encryption is applied - e.g. like radar control on the highway. 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. Such approach is relevant in case communication between systems of different owners with significant difficulties to manage relevant keys distribution.

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 4.

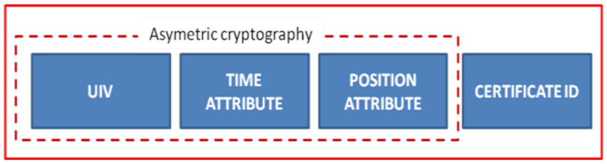


Fig. 4. Dynamic version of the identifier

Encryption of the UIV is described as follows:

$$M_1 = E_K\,(UIV \,\|\, T_i \,\|\, P_i), \qquad (8)$$

where

UIV = Universal Identifier of the Vehicle,
E_K = asymmetric encryption with public key K of the end receiver,
T_i = clock state in time of message generation,
P_i = position in time of message generation,
$UIV \,\|\, T_i \,\|\, P_i$ = identifier with link to current time and position.

After receiving the request by system central system, the message M1 is decrypted and UIV is read in „static form“ - received time Ti and Pi 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.

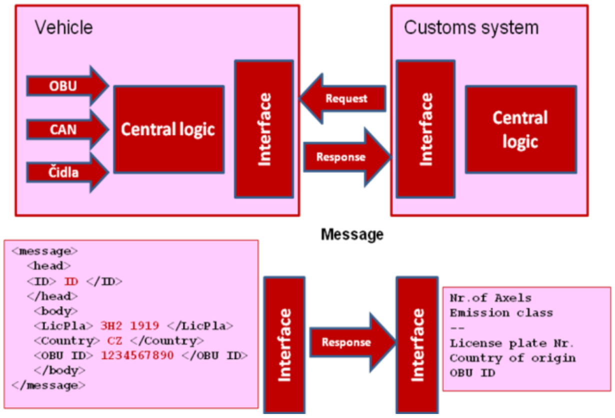
7 Service categories

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 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 5 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).



```
<message>
  <head>
  <ID> ID </ID>
  </head>
   <body>
   <LicPla> 3H2 1919 </LicPla>
   <Country> CZ </Country>
   <OBU ID> 1234567890 </OBU ID>
   </body>
</message>
```

```
Nr.of Axels
Emission class
--
License plate Nr.
Country of origin
OBU ID
```

Fig. 5. Public service example – customs administration

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.

Conclusion

Due to complexity of ITS solutions and implementations typically mobile services wide area coverage and selectable classes of services are required. Authors based on general analysis of ITS architecture and design principles focused their afford on wireless access solution designed as seamless combination of more independent access solutions of the same or alternative technology. Before analysis of the seamless handover/handoff based solution was designed and implemented the detailed analysis of the most frequently used communications solutions was processed in detail. Authors decided to design quickly and easily implementable alternative solution to complex solution based either on family of ISO standards known as CALM or IEEE 802.21. Solution adopts software based L3 routing effective in implementations in compact units like vehicles OBU.

“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 transferred data volumes progressive growth. If vehicle on board network solution is not connected to any communication cannel than system remains 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 via OBU to any other devices or networks.

OBU wireless interconnect (C2I) will be provided more and more frequently namely due to representative data available via the CAN vehicle network applicable for telematics services. However, data security in such applications represents sensitive issue which must be carefully studied and treated.

Security of telecommunications channel can be resolved with wide range of available security tools. Strongly required reliable and secure authentication of the actors and such data privacy are not frequently sufficiently resolvable by standardly available security tools. This paper presents solution based on non-public universal identifier with dynamical extension (time and position dependency as autonomous variables where relevant) as well as provided data selection according to actor role or category.

These tools have been implemented in laboratory OBU and relevant processes have been under procedure of the complex tests.

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] M. Svitek,, T. Zelinka**, Monitoring of Transport Means on Airport Surface.** Proceedings of 7-th International Conference on Transport Systems Telematics, Katovice-Ustron, 2007, pp. 285 – 292, ISBN 978-83-917156-7-3.

[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, 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, 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, IS BN 978-958-44-7280-9

[31] T. Zelinka, M. Svitek,, M. Srotyr, M. Vosatka, **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.

[32] T. Zelinka, Z. Lokaj, **Data security in transportation solutions**, 15-th World Multi-Conference on Systemics, Cybernetics and Informatics, pp 160 - 165, IIIS/IFSR, Orlando, FL, USA, ISBN 978-1-936338-29-0.