Authentication and Data Security in ITS Telecommunications Solutions

Tomas ZELINKA
Faculty of Transportation Sciences, Czech Technical University in Prague
Prague, 11000, Czech Republic

and

Michal JERABEK
Faculty of Transportation Sciences, Czech Technical University in Prague
Prague, 11000, Czech Republic

and

Zdenek LOKAJ
Faculty of Transportation Sciences, Czech Technical University in Prague
Prague, 11000, Czech Republic

ABSTRACT

Paper presents telecommunications security issues with dynamically changing networking. Paper also presents performance indicators of authentication as an integral part of the approach to non-public information. Expected level of security depend on relevant ITS services requirements, different solutions require different levels of quality. Data volumes transferred both in private data vehicle on board networks as well as between vehicles and infrastructure or other vehicles significantly and progressively grow. This trend leads to increase of the fatal problems if security of the wide area networks is not relevantly treated. Relevant communications security treatment becomes crucial part of the ITS telecommunications solution because probability of hazards appearances grow if vehicles networks are integrated in the dynamically organized wide area networks. Besides of available "off shelf" security tools solution based on non-public universal identifier with dynamical extension and data selection according to actor role or category is presented including performances indicators for the authentication process.

Keywords: Intelligent Transport System, Telematics, System Performance, Authentication, Performance Indicator, Object Identification, Data Security.

1. INTRODUCTION

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.
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.
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.

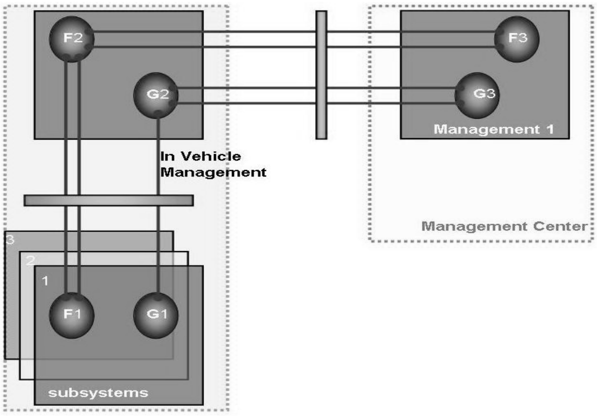


Fig. 1 ITS architecture

2. REQUIREMENTS OF TELEMATIC SUB-SYSTEM

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
- availability
- integrity
- continuity
- accuracy
- safety

Thanks to decomposition of system parameters the application can follow-up analysis of telematic chains according to the various criteria. It is obvious that quantification of requirements on relevant telecommunication solutions within telematic chains plays one of key roles in this process.
Following communications performance indicators quantify communications service quality (see e.g. [6] - [10]):

- availability – (Service Activation Time, Mean Time to Restore, Mean Time Between Failure 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. 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.

3. 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 occurs in cases of non-standard events (e.g. fake transaction). It means that system detects the forgery on a defined level of probability.

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

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 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.

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.
The UIV represents set of partial identifiers extended by unique non-public part generated from agreed data by standard cryptography algorithm 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).
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.

Communication and secure identification
Due to high sensitivity on data privacy exchanged between vehicle and service infrastructure VID must be reasonably protected against potential hackers attacks. In this paper will be discussed identifier and data security for data transmission only.
The communication channel can be secured by standard cryptography methods (VPN or SSL). If this protection is broken and the attack is successful than potential hacker can misuse transferred data. Proposed approach to data security yields in dynamical component extension (time and position dependency) and symmetric or asymmetric encryption, which is chosen depending on aplication.
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 Fig. 2.

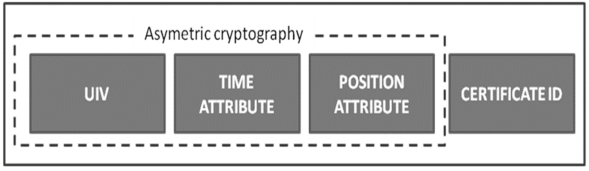


Fig. 2 Dynamic version of the identifier

Encryption of the UIV is described as follows:

$$M1 = EK\ (UIV \mid\mid Ti \mid\mid Pi), \qquad (2)$$

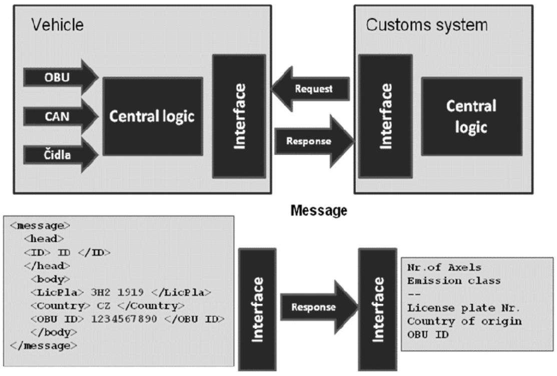
where

UIV - Universal Identifier of the Vehicle,
EK - asymmetric encryption with public key K,
Ti - clock state in time of message generation
Pi - position in time of message generation,
UIV || Ti || Pi - 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.

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 Fig. 3 this component is described as an "Interface". This component also covers "dynamisation" of the message content as it was already described above.



```
<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. 3 Public service example – customs administration

Example on Fig. 3 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.

4. AUTHENTICATION PROCESS

To access non-public information to competent persons only the information systems used identification, authentication and authorization. During authentication of user it is verified, whether it is same entity, whose identity is proven. After identification and authentication of the user's authorization is done, this allowed him access to information.
Authentication the person may be based on knowledge of "something", ownership "of something" or the user's biometric characteristics. It is suitable to combine these three possible approaches, but the authentication is in practice very often only realized with a password.
The authentication system is an integral part of information systems. It allows access to data and functions of information system only to authorized persons. Poorly functioning authentication system affects the whole information system. Different information systems may be different requirements for the functioning of its authentication system. Determination of the metrics makes it very easy to compare different authentication systems and specify the required parameters for authentication system.
Following authentication performance indicators quantify authentication service quality.

Duration of Authentication Process
Duration of authentication, ie time interval between the client request to the authentication and information on successful/unsuccessful authentication from authenticator is influenced by the complexity of the calculations, both the client and the authenticator side, but also the volume of data exchanged between the parties and mainly used telecommunication connection between the client and the authentication server.
The total duration of authentication can generally be divided into sub-periods

- the processing on the client side ($duration\_Z_K$)
- the processing time for the authenticator ($duration\_Z_A$)
- the communication time between the client and the authenticator ($duration\_K_{KA}$).

$$duration\_of\_authentication = duration\_Z_K + duration\_K_{KA} + duration\_Z_A \qquad \textbf{(3)}$$

All three times are sums of partial times and it is therefore possible to write

$$duration\_of\_authentication = \sum_{i=0}^{j} dzK_i + \sum_{i=0}^{k} dkKA_i + \sum_{i=0}^{l} dzA_i \qquad (4)$$

where
dzK_i is duration of the i-th processing on the client side
$dkKA_i$ is duration of the i-th communication between the client and the authenticator
dzA_i is duration of the i-th side processing on the authenticator side
For those protocols that must be repeated several times (generally t-times), to reduce the probability that an attacker has successfully authenticates fraud, the

$$duration\_of\_authentication = t \cdot \left(\sum_{i=0}^{j} dzK_i + \sum_{i=0}^{k} dkKA_i + \sum_{i=0}^{l} dzA_i \right) \qquad (5)$$

For those authentication protocols that must be repeated several times in order to reduce the likelihood that an attacker fraud an authenticating, their drawback is being longer duration authentication (theoretically t-times). The total time of authentication is to be viewed in the context of the overall time of the transaction. If the user took every request in the order of seconds, it is acceptable if the authentication will take as a few tenths of a second. It is therefore an important aspect

$$\frac{duration\_of\_authentication}{duration\_of\_transaction} \qquad (6)$$

If the authentication protocol is still based on trusted authority, the total time authentication is affected by the processing time on the trusted authority ($duration\_Z_{DA}$) and time communication with the authenticator ($duration\_K_{DAA}$) or client ($duration\_ZK_{DAK}$).

$$\begin{aligned} duration\_of\_authentication = duration\_Z_K \\ + duration\_K_{KA} + duration\_Z_A + duration\_Z_{DA} \\ + duration\_K_{DAA} + duration\_K_{DAK} \end{aligned} \qquad (7)$$

The duration as performance indicator may be approached from the perspective of two requirements. The first request I call static - it is determined the maximum required duration limit authentication regardless of the load current authentication system. Using this requirement the duration is the ability of authentication system to serve request for authentication to a certain specified maximum duration regardless of the load that can be defined as the probability

$$P\left(\left(t_{R,i} - T_R\right) \leq \varepsilon_{DAP}\right) \geq \gamma_{DAP} \qquad (8)$$

that the difference between the measured duration of i-th authentication process $t_{R,i}$ and the specified maximum duration T_R will not exceed the value ε_{DAP} on the probability level γ_{DAP}.

The second requirement I call a dynamic that takes into account the current authentication system load (number of authentication requests per time unit). For this requirement the duration as performance indicator is the ability of authentication system to serve the authentication request to a specified maximum duration for the current load that can be defined as the probability

$$P\left(\left(t_{R,i} - T_{R,(m,n]}\right) \leq \varepsilon_{DAP,(m,n]}\right) \geq \gamma_{DAP,(m,n]} \qquad (9)$$

where $m < n$

m, n are positive integers

that the difference between the measured duration of i-th authentication $t_{R,i}$ and the specified maximum duration $T_{R,(m,n]}$ for a given load (expressed in an interval $(m,n]$ of the number of requests per time unit) will not exceed the value $\varepsilon_{DAP,(m,n]}$ on probability level $\gamma_{DAP,(m,n]}$. So for different load ranges $(m,n]$ can be defined different threshold values $\varepsilon_{DAP,(m,n]}$ for the relevant probability level $\gamma_{DAP,(m,n]}$, the union would be appropriate probability level γ_{DAP} and threshold value ε_{DAP}. Expression should therefore changed

$$P\left(\left(t_{R,i} - T_{R,(m,n]}\right) \leq \varepsilon_{DAP}\right) \geq \gamma_{DAP} \qquad (10)$$

Performance indicator the duration may be determined from the viewpoint of the client, but also of the server. For real use is preferable to determine this from the viewpoint of the client.

For example when client and server were in the same network (LAN) and it was used Fast Ethernet (100Mb/s) as telecommunications access solution and Fiat-Shamir protocol was repeated 4 times, the average duration of authentication process was 567 miliseconds and standard deviation was 60 miliseconds. When we want to use performance indicator "Duration" then for ε_{DAP} equal zero and probability level γ_{DAP} equal 99% the maximum duration T_R must not be greater than 687 milliseconds (see graph on Fig. 4).

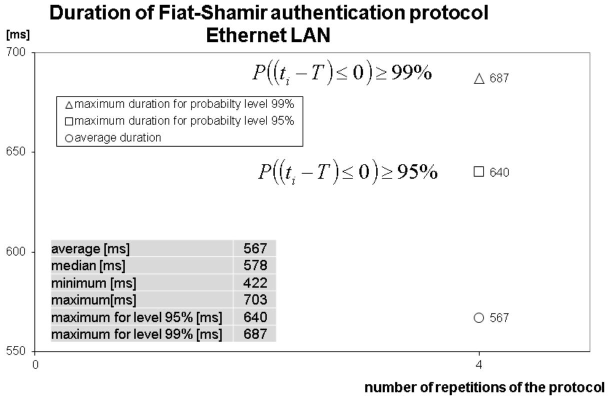


Fig. 4 Graph of measured duration of authentication with specified maximum duration

Stability of Serviceability

Stability of serviceability is the ability of authentication system to process the authenticate requests without loss up to the allowable limit that can be defined as the probability

$$P\left(\left(\frac{r_{t,s}}{r_t}\right) \geq \varepsilon_{SoS}\right) \geq \gamma_{SoS} \qquad (11)$$

$$t \in \langle 0, T \rangle$$

$$\varepsilon_{SoS} \in \langle 0, 1 \rangle$$

that the percentage of served requests $r_{t,s}$ and the total number of requests r_t is greater or equal to ε_{SoS} on the probability level γ_{SoS} for each time t interval from $\langle 0, T \rangle$.

Thus in terms of the stability of serviceability ignores the current workload of authentication system and therefore for different intervals of workload $(m,n]$ can be expressed by the formula

$$P\left(\left(\frac{r_{t,s}}{r_t}\right) \geq \varepsilon_{SoS,(m,n]}\right) \geq \gamma_{SoS} \qquad (12)$$

on condition a unified the probability level .

Loss Rates
Loss rates reflects the ability of an authentication system to don't serve only part of the authenticate requests to a maximum allowable limit that can be defined as the probability

$$P\left(\left(r_{o,\langle 0,T\rangle} - R_{\langle 0,T\rangle}\right) \le \varepsilon_{LR}\right) \ge \gamma_{LR} \qquad (13)$$

that the difference between the number of really outstanding requests $r_{o,\langle 0,T\rangle}$ and tolerated the maximum number of outstanding requests $R_{\langle 0,T\rangle}$ will not exceed the value ε_{LR} on the probability level γ_{LR} during a time interval $\langle 0,T\rangle$.

Rate of Erroneously Accepted Authentications
The rate of erroneously accepted authentications reflects the property authentication system erroneously authenticate to a certain extent that can be defined as the probability

$$P\left(\left(\frac{r_f - R_f}{r_t}\right) \le \varepsilon_{REAA}\right) \ge \gamma_{REAA} \qquad (14)$$

that the percentage of difference between the number of erroneously accepted authentications r_f and the number of tolerated erroneously accepted authentications R_f and the total number of authentication requests r_t will not exceed the value ε_{REAA} on the probability level γ_{REAA}.

Rate of Erroneously Rejected Authentications
The rate of erroneously rejected authentications reflects property of authentication system reject authentication an authorized person to a certain extent that can be defined as the probability

$$P\left(\left(\frac{r_d - R_d}{r_t}\right) \le \varepsilon_{RERA}\right) \ge \gamma_{RERA} \qquad (15)$$

that the percentage of difference between the number of erroneously rejected authentications r_d and the number of tolerated erroneously rejected authentications R_d and the total number of authentication requests r_t will not exceed the value ε_{RERA} on the probability level γ_{RERA}.

5. CONCLUSION

Due to complexity of ITS services requiring typically mobile services wide area coverage and selectable classes of services we focused our afford on wireless access solution designed as seamless combination of more independent access solutions of the same or alternative technology.

"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. CAN and OBU interconnect is coming 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.
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 acceptable as sufficient tool. Identification based on newly designed dynamical Unique Vehicle Identifier UIV is presented as relevant alternative.
The authentication system is an integral part of information systems. It allows access to data and functions of information system only to authorized persons. Poorly functioning authentication system affects the whole information system. Different information systems may be different requirements for the functioning of its authentication system.
Second security aspect which follows authentication is data privacy and actors authorization to receive relevant data content. Authors´ approach is based on selective data transmission and delivery in accordance to actor role/category. These described principles are combined with available security tools like in this case applied asymmetric data encryption. Such combination of presented tools leads to solution with relevant level of reached system security.

6. 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, 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, ISBN 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**, Proceedings of the 15-th World Multi-Conference on Systemics, Cybernetics and Informatics, pp 160 - 165, IIIS/IFSR, Orlando, FL, USA, ISBN 978-1-936338-29-0.

[33] V. Fabera: **Transformations of Pairs of FSMs**. In LATEST TRENDS in INFORMATION TECHNOLOGY. Athens: WSEAS, 2012, p. 403-408. ISBN 978-1-61804-134-0.

[34] V. Fabera, J. Zelenka: **FSM Construct with Genetic Algorithm Using Distance Measuring in Mutation**

Operator. In Proceedings of 17th International Conference on Soft Computing (MENDEL 2011). Brno: University of Technology, 2011, pp. 62-66. ISBN 978-80-214-4302-0.

[35] J. Krcal: **Departure model and its mathematical expression**. In Proceedings of First International Conference on Modelling and Development of Intelligent Systems. Sibiu: Lucian Blaga University of Sibiu, 2009, pp. 115-120. ISSN 2067-3965.

[36] J. Krcal: **Parametrization of a Departure Model**. In Proceedings of the 8th WSEAS International Conference on DATA NETWORKS, COMMUNICATIONS, COMPUTERS. New York: WSEAS Press, 2009, pp. 195-198. ISBN 978-960-474-134-2.

[37] P. Bures, Z. Belinova, P. Jesty: **Intelligent transport system architecture - different approaches and future trends**. In Data And Mobility: Transforming Information Into Intelligent Traffic And Transportation Services, Proceedings Of The Lakeside Conference 2010. Berlin:Springer, 2010, p.115-127.ISBN 978-3-642-15502-4.

[38] Z. Belinová, P. Bures, D. Barta, D.: **Evolving ITS architecture, the Czech experience**. In Modern Transport Telematics. Berlin: Springer, 2011, p. 94-102. ISBN 978-3-642-24659-3.

[39] M. Bellare, C. Namprempre, G. Neven: **Security Proofs for Identity-Based Identification and Signature Schemes**. Journal of Cryptology. Volume 22, Number 1. Springer New York, 2009.

[40] A. Menezes, P. von Oorschot, S. Vanstone: **Handbook of Applied Cryptography**. CRC Press, 1996. ISBN 0-8493-8523-7.