Service Quality Management in the ITS Telecommunications Systems

Tomas ZELINKA
Faculty of Transport Sciences, Czech Technical University in Prague
Prague, 110 00, Czech Republic

and

Zdenek LOKAJ
Faculty of Transport Sciences, Czech Technical University in Prague
Prague, 110 00, Czech Republic

and

Martin SROTYR
Faculty of Transport Sciences, Czech Technical University in Prague
Prague, 110 00, Czech Republic

ABSTRACT

Guaranteed selected quality of telecommunication service and wide area coverage are typical requirements of the ITS (Intelligent Transport Systems) applications. Extensive range of wireless data services with reasonable coverage is provided by public wireless services operators, however, mostly no guaranteed relevant range of quality and security is available. ITS services require cost-effectively solution which can be resolved by combination of the "core" public solution with the other public as well as private services where and when it is needed. Such approach requires implementation of the relevant flexible system architecture supported by the efficient decision processes. ITS specific service security requirements would not underestimated, as well. Special situation is identified in case of the C2I (Car to Infrastructure) and C2C (Car to Car) communication namely if the vehicle on board unit is interconnected with the vehicle CAN (Controlled Area Network) based network. Such configurations significantly increase potential of dangerous intruders´ attacks. Probability of the critical hazards appearances grows if the ITS data are accessible in the wide area networks. That is also the main reason why relevant telecommunications security support is understood as one of the crucial part of the ITS telecommunications solution.

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

1. INTRODUCTION

ITS system can be described as a final automaton defined by mapping the system inputs with respect to the internal state plus mapping the inputs and internal state with respect to the system outputs. System can be split in several subsystems. A subsystem must be describable through an identical methodology like a system; in its substance the subsystem is a system to be described at a more detailed distinguishing level.

An identification process reflects the chained events within a system. An event may mean a change of a system state brought about either by an initiation on inputs (transfer of input values), initiation of the internal system state or the "only" in the course of the time. A set of all activated processes at possible environmental conditions defines the system behavior.

ITS solutions have been associated with serious expectations and getting ITS applications in the real practice is understood as the essential potential to significantly faster resolve many transport challenges. The main afford of the ITS research is to prepare actual conditions to integrate ITS architectures in the real practice with aim to support different transport optimization tasks.

This paper is concentrated on the communications issues of the ITS architectures, and, the same principles adopted in the ITS applications are applied in the communication solution design. Such decomposition simplifies both analysis as well as synthesis of the systems including security parameters being accepted as the critical ones.

2. TELEMATIC SUB-SYSTEM REQUIREMENTS

The methodology for the definition and measurement of following individual system parameters has been developed in frame of the ITS architecture and it is described in [1] - [5]. Individual system parameters – performance indicators - were accepted and de facto standardized in frame of the ITS architecture to enable to simply compare different subsystems parameters and their behavior to enable efficient and secure synthesis of the whole system:

- 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 the telematic chains in accordance to the various criteria (optimization of the information transfer between a mobile unit and processing center, maximum use of the existing information and telecommunication infrastructure, etc.). It is obvious that quantification of the requirements on the 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]):

- 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 telecommunications 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 [8] are presented details of proposed iterative method.

3. COMMUNICATIONS SOLUTION

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 case such parameters do not meet requirements under specific conditions. Table 1 describes typical behavior of private/public telecommunications solutions.

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.

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)

Mobile data services - GSM– GPRS, EDGE and UMTS
Fig. 1 and 2 present GPRS and EDGE service in area close to their critical level of the signal to noise ratio (C/I). In this critical conditions (S/N) service delay represented by Round Trip Delay (RTD) rapidly grows and significant Packet Loss Ratio (PLR) dependence on the C/I value (light grey) can be identify, as well. Displayed C/I critical conditions (S/N) represent service status when replacement by the alternative technology must be processed, of course only in case such situation is not resolvable by tools of applied solution.

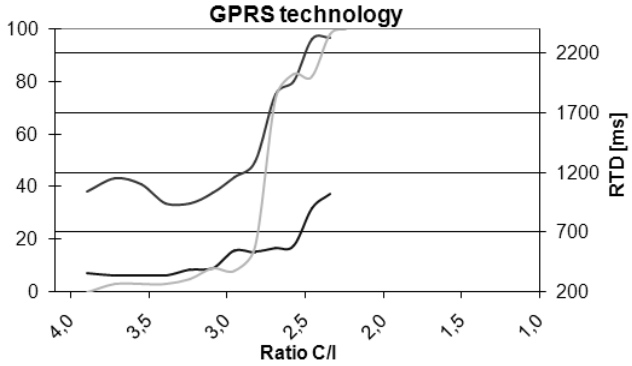

Figure 1. PLR and RTD - GPRS technology

GPRS technologies are applicable for "less demanding" applications where long delays (RTD) being in average 1000 ms is not critical for served application. It must be combined with alternative technology on CALM principles as described below. EDGE service due to its technical solution improvement (if compared with GPRS) could appear in a slightly more demanding telematic solutions, however, service provider would be forced (practically impossible) to guarantee appropriate priority of service provisioning. Anyhow, RTD would not be required to be better than approximately 700ms.

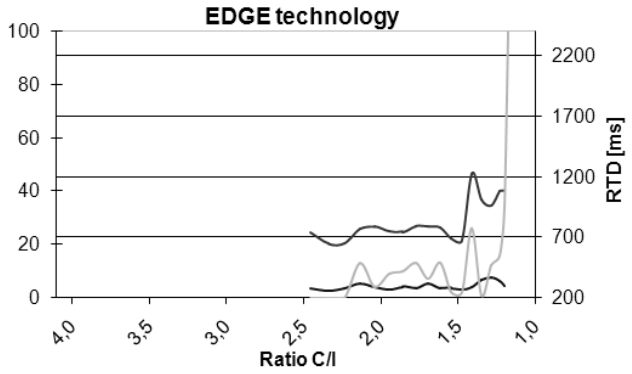

Figure 2. PLR and RTD - EDGE technology

Figure 3 present parameters of the UMTS basic service. UMTS RTD is reaching approximately 200ms allowing extend number of applications. However, there are not many countries in Europe where UMTS is served in the rural areas, and, mostly UMTS providers afford is concentrated on the Urban areas, i.e. areas where also other alternative solutions for the ITS services can be easily available.

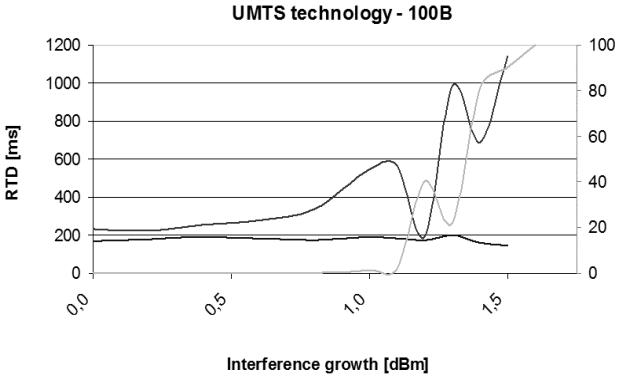

Figure 3. PLR and RTD - UMTS technology

WiFi – IEEE 802.11

Basic „a“, „b“ and „g“ amendments with CDMA/CA collision protocol and public spectra applied have not got delicious reputation and technology oriented application were not expectable. Basic dynamical system parameters with CDMA/CA collision protocol being eliminated are quite reasonable “– see Figure 4.

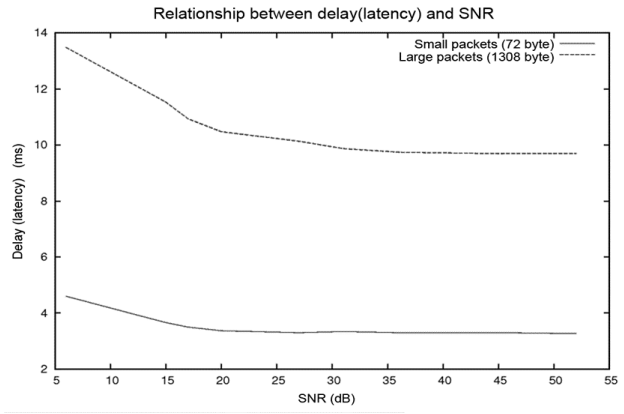

Figure 4. Latency in wiFi system

New Amendments extend existing system parameters in the extensive way. Amendment “e” supports TDM (Time Division Multiplex) based Quality of Service (QoS), management, Amendment “r” defines handover processes (the first generation) in the cellular architecture and Amendment “p” is dedicated specifically for the ITS C2C and C2I applications. Basic dynamical WiFi parameters supported by listed Amendments have got ability to support demanding technological applications like ETC (Electronic Toll Collection) or e-safery. IEEE 802.11p has been e.g. incorporated in the IEEE 1609 standard – applied for C2C and C2I applications.

WiMax – IEEE 802.16

Technology based on IEEE 802.16d/e standards known as (Mobile) WiMax represents robust alternative to WiFi. Figure 5 and 6 preset RTD spectra for two completely different radio configuration described by SNR values and radio visibility (see LOS). Its remarkable adoptability is evident from these results.

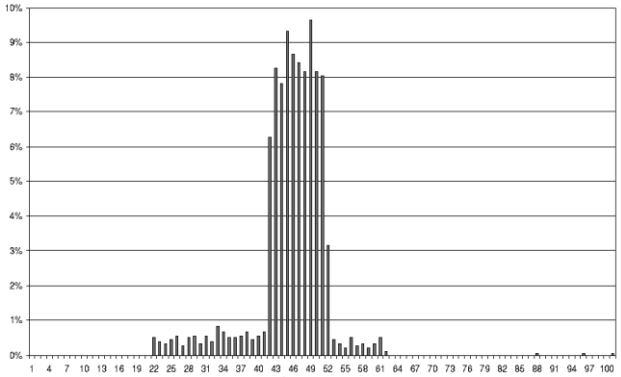
Figure 5. RTD spectra of LOS - SNR =+33db - WiMax

Just coming “beyond 3rd” mobile service technology LTE adopted substantial part of the WiMax like principles. Designers goal was to introduce robust technology dedicated for the mass telecommunications services provisioning with even improved selection of parameters. RTD, PLR as well as other important parameters represent product which will be able to resolve significant part of in these days unsolvable ITS services.

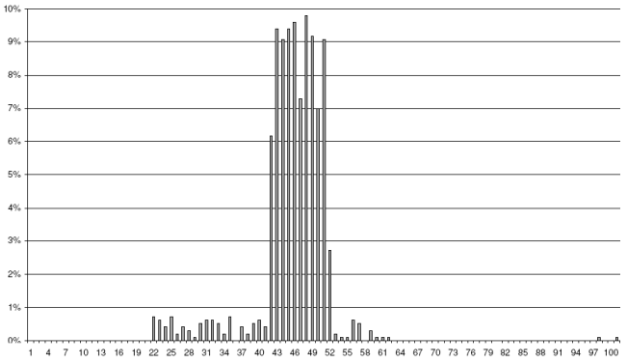
Figure 6. WiMax RTD spectra of NLOS - SNR=-27db

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. 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. [11] - [13]. 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) – see [14]. 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 with smart decision adaptive processes process replacing commonly used PBM (see [15] – [17]). 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 [18] - [32].

5. DATA SECURITY

Security performance indicator 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 and e.g. basic 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.

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 7.

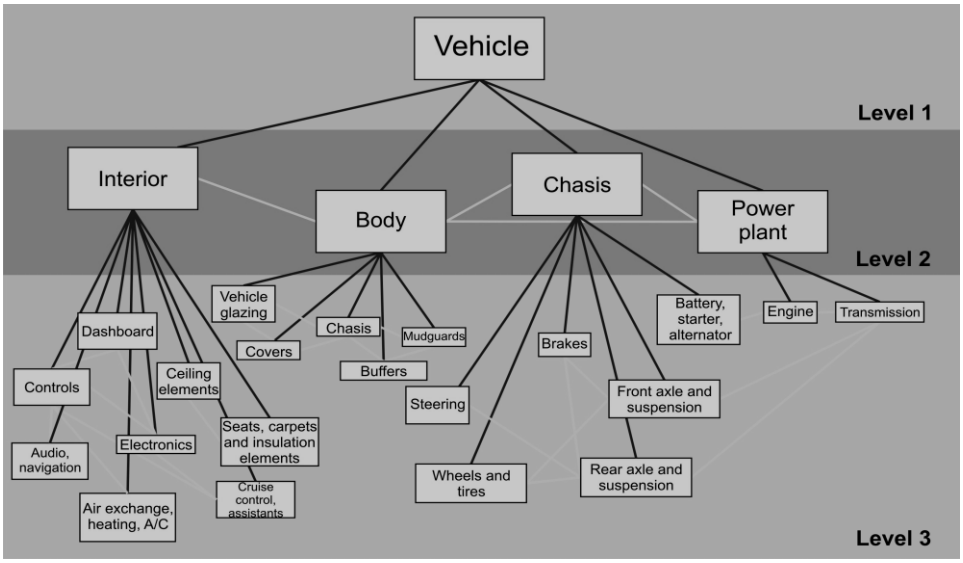

Fig. 7 Vehicle decomposition

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.

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. 8.

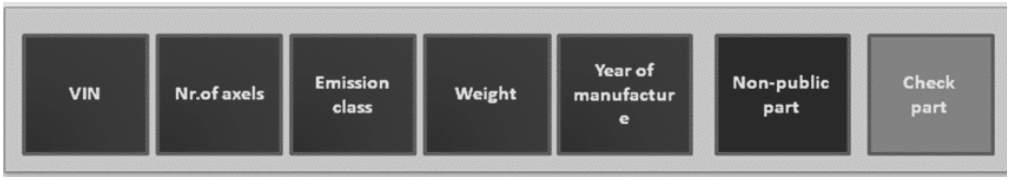

Fig. 8 Example of unique identifier

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.

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.
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. Encryption of the UIV is described as follows:

$$M1 = EK (UIV \text{ II } Ti \text{ II } Pi), \quad (2)$$

where UIV means 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 II Ti II Pi - 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 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.
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.

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. Such component can also cover "dynamisation" of the message content as it was already described above.
Three service categories may be for example defined:

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

Set of available data is identified by the unique identifier. Vehicle unit processes the request and provides defined selection of ITS data dedicated to the service category of the customer.

6. CONCLUSION

Due to complexity of the ITS services mostly mobile services wide area coverage and selectable classes of services are required. Authors focused afford on the wireless access solution designed as a seamless combination of more independent access solutions of the same or alternative technologies. Basic analysis of available technologies applicable for ITS is presented.
Quickly and easily implementable alternative solution to the complex ones based either on family of ISO standards known as either CALM or IEEE 802.21 supporting family of standards IEEE 802 and 3G mobile services is presented. Authors adopted software based L3 routing which is relatively easy to be implemented in most of off-shelf OBUs based on available sets of market available microchips.
C2C and C2I communication as well as vehicles on board data communication via Controlled Area Network bus are areas with progressively 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 volumes will substantially grow. It is due to fact that private vehicle networks contain representative data with applicability for services like the vehicle and its parts identity identification. Available data are also useable to control behavior of the key parts 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 the 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 dynamical Unique Vehicle Identifier UIV is presented as the relevant solution 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.

8. ACKNOWLEDGMENTS

This project was supported by Ministry of Industry and Business (MPO) and Ministry of Transport (MD) of the Czech Republic via 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.

9. 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] IEEE Std 802.21-2008, **IEEE Standard for Local and Metropolitan Area Networks**, IEEE, January 2009

[15] 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.

[16] 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.

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

[18] 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.

[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, 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.

[32] Zelinka, T., Lokaj, Z.: **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.