Security in the ITS Telecommunications

Tomas Zelinka, Michal Jerabek, Zdenek Lokaj, & Martin Srotyr

Abstract— Guaranteed 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 offered by public wireless service providers, however, mostly no guaranteed relevant range of quality and security has been available. As ITS services require cost-effectively solution, as well, requirements can be resolved by seamless switched combination of public and private services selected in accordance to agreed criteria realized by implemented decision processes. Specific 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 dynamically developing telecommunications solution touching public networks significantly increase potential of dangerous intruders’ attacks. That is also the main reason why relevant telecommunications security support is understood as one of the crucial part of the ITS telecommunications solution and it is discusses in detail in this paper.

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 telecommunications issues of the ITS architectures, and, the same principles adopted in the ITS applications are applied in the telecommunication 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 tci; on the vector of telematics performance indicators Δmti can be expressed as

\[ Δmti = TM · tci \]  

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. Telecommunications Solution

Range of mobile data services with wide area coverage is available for ITS. These are namely GPRS, EDGE, UMTS and coming LTE, but also namely locally applicable WiFi, WiMax. Specific role play DSRC 5.8 and coming DSRC 5.9.

Most of services dedicated for public market do not guarantee quality, i.e. defined range of theirs performance indicators. To improve conditions for ITS implementations and service provisioning combination of different services with automatic seamless switching (second generation of handover) was introduced.

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 standard 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 introduced recently easily implementable alternative solution applicable namely for compact solutions like On Board 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 is adoptable in much shorter time horizon if compared with system based on complex ISO CALM approach or IEEE 802.21 standard. Authors applied 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].

4. 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.

\[ P(\left| W_i - W_{m,i} \right| \leq \varepsilon) \geq \gamma \]  

Equ. 2

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

“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 channel 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.

A. Unique Identifier

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

Choice of important identifiers and characteristics of the vehicle must be based on an analysis of the vehicle as a system, which is a purposefully defined as a set of parts or elements and set of links of certain attributes which determine the characteristics, behavior and function of the system as a whole. The vehicle as a system decomposition is performed in order to find basic elements of the vehicle and links between them, as shown in Fig. 1.

![Fig. 1 Vehicle decomposition](image)

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 axles 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. 2.

![Fig. 2 Example of unique identifier](image)

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.

B. 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:

\[ M_1 = EK \text{(UID II Ti II Pi)} \]  
\[ \text{(Equ. 3)} \]

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.

C. 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.

5. Authentication Performance Indicators

The authentication system is an integral part of any information system. Different information systems have different requirements on functionality of applied authentication and determination of the metrics enables easier different authentication systems comparison and specifies the required parameters for authentication system. Following authentication performance indicators quantify authentication service quality.

Transformation between telecommunications and telematics system of performance indicators was summarized in chapter 2. Equation (1) is applicable, 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. We therefore primarily define performance indicator Duration of authentication.
effectively applicable with other communications performance indicators. Than other even more representative indicators are introduced, as well.

**A. Duration of Authentication Process**

Duration of authentication, i.e. 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 $K_{KA}$).

$$\text{duration of authentication} = \text{duration } Z_k + \text{duration } Z_A + \text{duration } K_{KA} \quad (\text{Eq. 4})$$

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

$$\text{duration of authentication} = \sum_{i=0}^{k} d_i K_i + \sum_{i=0}^{k} d_i K_A + \sum_{i=0}^{k} d_i A_i \quad (\text{Eq. 5})$$

where

- $d_i K_i$ is duration of the i-th processing on the client side,
- $d_i K_A$ is duration of the i-th communication between the client and the authenticator,
- $d_i A_i$ 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

$$\text{duration of authentication} = t \left( \sum_{i=0}^{k} d_i K_i + \sum_{i=0}^{k} d_i K_A + \sum_{i=0}^{k} d_i A_i \right) \quad (\text{Eq. 6})$$

For those authentication protocols that must be repeated n times in order to reduce the likelihood that an attacker fraud an authenticating, their drawback is being longer duration authentication (theoretically n-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

$$\frac{\text{duration of authentication}}{\text{duration of transaction}} \quad (\text{Eq. 7})$$

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

$$\text{duration of authentication} = \text{duration } Z_{ta} + \text{duration } K_{DA} + \text{duration } Z_A + \text{duration } Z_{DA} + \text{duration } K_{DA} + \text{duration } K_{DAK} \quad (\text{Eq. 8})$$

The duration as performance indicator may be approached from the perspective of two requirements. The first request is 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

$$P \left( t_{R,i} - T_R \leq \varepsilon_{\text{DAP}} \right) \geq \gamma_{\text{DAP}} \quad (\text{Eq. 9})$$

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 $\varepsilon_{\text{DAP}}$ on the probability level $\gamma_{\text{DAP}}$.

The second requirement is dynamical 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

$$P \left( t_{R,i} - T_{R,(m,n)} \leq \varepsilon_{\text{DAP,(m,n)}} \right) \geq \gamma_{\text{DAP,(m,n)}} \quad (\text{Eq. 10})$$

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 $\varepsilon_{\text{DAP,(m,n)}}$ on probability level $\gamma_{\text{DAP,(m,n)}}$.

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 \( \gamma_{DAP} \) and threshold value \( \varepsilon_{DAP} \). Expression should therefore changed

\[
P \left( \left( T_{R,c} - T_{R,(m,n)} \right) \leq \varepsilon_{DAP} \right) \geq \gamma_{DAP} \quad \text{(Equ. 11)}
\]

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 \( \varepsilon_{DAP} \) equal zero and probability level \( \gamma_{DAP} \) equal 99% the maximum duration \( T_R \) must not be greater than 687 milliseconds (see graph on Fig. 3).

\[
\text{Fig. 3 Graph of measured duration of authentication with specified maximum duration}
\]

\[2\]

B. 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

\[
P \left( \left( \frac{r_{LS}}{r_t} \right) \geq \varepsilon_{SoS} \right) \geq \gamma_{SoS} \quad \text{(Equ. 12)}
\]

\[t \in (0,T)\]

\[\varepsilon_{SoS} \in (0,1)\]

that the percentage of served requests \( r_{LS} \) and the total number of requests \( r_t \) is greater or equal to \( \varepsilon_{SoS} \) on the probability level \( \gamma_{SoS} \) for each time \( t \) interval from \((0,T)\).

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

\[
P \left( \left( \frac{r_{LS}}{r_t} \right) \geq \varepsilon_{SoS,(m,n)} \right) \geq \gamma_{SoS} \quad \text{(Equ. 13)}
\]

\[t \in (0,T)\]

for unified probability level \( \gamma'_{SoS} \).

C. 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

\[
P \left( \left( R_{0,(0,T)} - R_{0,(0,T)} \right) \leq \varepsilon_{LR} \right) \geq \gamma_{LR} \quad \text{(Equ. 14)}
\]

that the difference between the number of really outstanding requests \( r_{n,(0,T)} \) and tolerated the maximum number of outstanding requests \( R_{0,(0,T)} \) will not exceed the value \( \varepsilon_{LR} \) on the probability level \( \gamma_{LR} \) during a time interval \((0,T)\).

D. 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

\[
P \left( \left( \frac{r_{LS} - R_t}{r_t} \right) \leq \varepsilon_{REA} \right) \geq \gamma_{REA} \quad \text{(Equ. 15)}
\]

that the percentage of difference between the number of erroneously accepted authentications \( r_{LS} \) and the number of tolerated erroneously accepted authentications \( R_t \) and the total number of authentication requests \( r_t \) will not exceed the value \( \varepsilon_{REA} \) on the probability level \( \gamma_{REA} \).

E. 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
that the percentage of difference between the number of erroneously rejected authentications $r_e$ and the number of tolerated erroneously rejected authentications $R_e$ and the total number of authentication requests $r_i$ will not exceed the value $e_{RERA}$ on the probability level $\gamma_{RERA}$.

6. Conclusion

“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 channel then 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 integrity and 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. Identification of two actors for mutual communication based on identifier like VIN code or OBU-ID is not acceptable as sufficient tool. Identification based only 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.

Possibility to quantify impact of authentication process on telematics solution performance relates with conditions of presented transformation between telecommunications and telematics set of performance indicators. Such transformation is applicable only if probability levels of all studied phenomena are set on the same level and all performance indicators have the same physical dimension – typically time is applied. Therefore performance indicator Duration of authentication was firstly defined with aim to have effectively integrate-able in processes performance indicator. Than the other specific indicators where introduced, as well.

References

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


[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.


