Archives of
Transport System
Telematics

Volume 10

Issue 3

September 2017

Analysis of information secure transmission methods in the intelligent transport systems

M. SIERGIEJCZYK
WARSAW UNIVERSITY OF TECHNOLOGY, Faculty of Transport, Koszykowa 75, 00-662 Warsaw, Poland
EMAIL: msi@wt.pw.edu.pl

ABSTRACT

The essence of operation of all the ITSs is to make decisions on the basis of the obtained and available information. The relevance of taken decisions depends on the quality of available information, its accuracy and up-to-dateness. It is important to pay attention to the fact that requirements for up-to-dateness of information as well as the consequences of delays in their transfer or in connection with their loss are different depending on the subsystem. The paper presented the issues related to the analysis of the ITS telecommunications environment. The selected aspects of prevention from risks, which may be an important factor affecting the security of the transport system functioning, will be analysed. Moreover, the analysis of methods for the secure data transmission will be also carried out. The transmission security methods will be selected within the framework of VPN virtual tunnel technologies. The mechanisms, the implementation of which will allow to increase the security and availability of information transmission in ITSs, were offered.

KEYWORDS: information, transmission, security, intelligent transport systems

1. Introduction

ITSs (Intelligent Transport Systems) are defined as systems designed to improve transport activities through the reduction of operating costs, the increase of the level of security, and optimisation of using the existing road infrastructure by moving vehicles. Based on the assumption, these systems should use telecommunications and IT technologies, and also the automation and measurement devices, which in conjunction with advanced control methods, affect the road transport improvement.

The ITS has an impact on the improvement of travelling conditions in the multimodal range – dealing with public and private means of road, sea and air transport. The use of ITS is an affordable and easier method for improving the transport conditions than the communication infrastructure expansion in its current form [1], [2]. Each subsystem of ITS has specific requirements for communication channels, which must be chosen adequately to the needs of a given subsystem, its topology, users, and taking into account the costs of the construction and operation of the system.

A key element of ITSs includes the information sent via various means of communication. This basic functionality has been a serious problem until today because of the diversity, validity, and impact, as well as the way of obtaining and distributing information. The lack of sufficient communication can be a source of many alarming phenomena, which are manifested through the lack of information about the traffic situation, the loss of synchronisation of multimodal transport means, disturbances in the smooth traffic management and many others. The use of telecommunications and IT devices makes it possible that ITSs are, in fact, ICT systems. Hence, the issue on the information security of ITSs becomes significant. In the paper, the selected problems related to the security and confidentiality of information transmission between ITS elements and the provision of protecting access to the IT systems' resources and their stored data, the aspects of this problem affecting the communication system architecture (additional devices for ensuring the data flow security are required) will be signalled. The methods for secure transmission in ITSs are, in fact, secure transmission methods commonly used in systems, which require the confidentiality and security of

information transmission between the data source and its recipient [3], [4], [5], [6]. The ITSs in this area are characterised by emphasis on specific aspects of such transmission. Therefore, it is secure transmission with the use of solutions commonly known among specialists, and at the same time, a group of solutions specialised in terms of application in conditions and adapted to the requirements of application in intelligent transport systems.

2. ITS communication architecture

2.1. European Framework Architecture of Intelligent Transport Systems

The European Framework Architecture was created on the basis of recommendations of the high-level specialists of telematics. FREME is high-level architecture. This means that it is a set of the most popular and the main functions and facilities within the defined division. At the design stage of architecture with the use of the data flow diagrams, their choice is possible. Referring to the creation schema of ITS architecture recommended in case of FRAME, downstream systems are obtained when the aspects specific to given implementation are defined. It is possible because FRAME assumes a flexible basis, which can be used in order to implement own requirements on a national or regional scale.

The range of functions, which can be provided by FRAME in its original version, is usually more comprehensive than the requirements, which are needed for a specific entity – it is a selected set of the user's needs. There are also the situations, where the original architecture does not have a certain set of functions. Then, FRAME allows to add items to its own additional needs. However, the needs result in functions, and some of them, included within FRAME, will be selected as a final set of functions, and the remaining ones will be separately defined by stakeholders and added to the final collection. By combining the aspect of needs and defined functions, the complex ITS national system architecture is created.

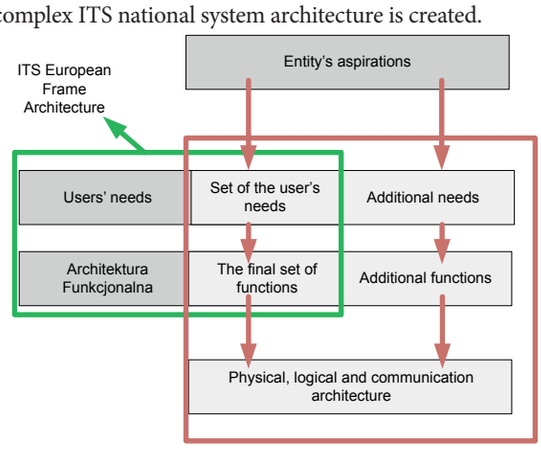

Fig. 1. Process of formation of ITS Architecture [own study based on 8]

The architecture of such a defined system consists of three perspectives:

1. Functional Architecture – describes the processes in a given system.
2. Physical Architecture – illustrates the location of processes in a given environment. Its form is closely associated with specific requirements and restrictions for given implementation;
3. Communication Architecture – defines the connection between locations and functions, and it is closely linked with the characteristic requirements and restrictions for given implementation.

2.2. Sample communication architecture of ITS subsystem

According to FRAME, the communication architecture defines and describes the measures that support the exchange of information between various parts of the system. This exchange is carried out with the use of physical data flows, which are described in the Physical Architecture. By dealing with a communication perspective, it is possible to meet two complementary aspects: the requirement to provide information from one point to another in a manner that is suitable for given application taking into account the costs, possibilities of changing information, its size and delays; as well as the requirement of using languages, interfaces and protocols which allow for the proper understanding of receiver modules. In accordance with FRAME, the data flows (and related operations) between subsystems, and also between subsystems and terminators will be used in defining the communication perspective. In this part of the paper, the main information flows, which determine the communication architecture of the highway emergency communication subsystem (Fig. 2), will be presented in detail [9].

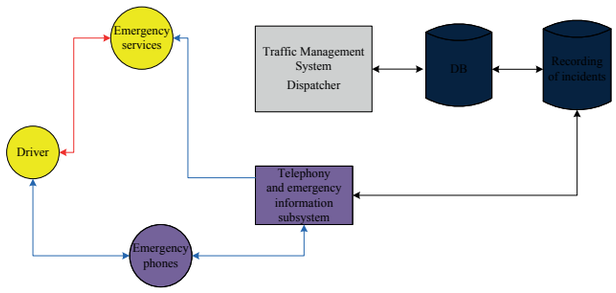

Fig. 2. Diagram of the information flow in the highway emergency communication subsystem [9]

The highway emergency communication subsystem plays roles related to the provision of telephone communication to any place within the equipped highway's section. At a distance of a few hundred metres from each other, the emergency phones (terminators of this subsystem), which connect a driver directly with an operator with VolP (Voice over Internet Protocol) technology that uses a dedicated optic fibre only for this application, are located on both sides of the road. At the operator's side, there are IP phones and the workstation of the emergency subsystem available, where it is possible to check the technical condition of each device and the battery capacity, and to call to a chosen emergency phone. All the calls are saved in the database of the recorders of incidents in the .wav or mp3 format depending on the call duration. The software recorder built into

the telephony server records and keeps the recordings for 60 days from the date of the recording creation. It is possible to play the recordings at any time. The subsystem enables to communicate with emergency services.

The direct links between terminators can be implemented outside the system's infrastructure using mobile telephony or other media available by the driver/passenger. In the central system's GUI (highway traffic management system), technical data related to the condition of each VoIP phone within a given area is displayed. All the complex operations, configurations and the option of calling are possible thanks to a dedicated operator station. Along with the built-in modem supporting 2G and 3G mobile networks, the subsystem makes it possible to quickly direct via phone with emergency services. In the highway emergency communication subsystem, they are used as transmission media, xWDM optic fibre transmission and 5e category twisted-pair and Datex II, XML, TCP/IP, and VoIP protocols.

3. Identification of information hazards in ITSs

A key element of ITSs includes the information sent via various means of communication. The use of telecommunications and information technology devices makes that ITSs are, in fact, ICT systems (mostly based on IP protocol), which are vulnerable to the same threats [3, 4, 5, 11, 12, 13].

The information security of ITSs can be threatened by a variety of threats evolving in time, and it is affected by many factors, so different criteria of their classification are used. The following fundamental division of threats is most often adopted:

- hardware and software,
- intentional and unintentional,
- external and internal.

The hardware threats are physically caused by the hardware (e.g. equipment failure), however, the software threats are caused by the computer software (e.g. programme error).

Any threat can be defined as intentional or unintentional (accidental). If a threat was automatically caused as a result of e.g. hardware failure, software error or unintentionally as a result of e.g. human error, distraction, insufficient knowledge, etc. we deal with an unintentional (accidental) threat.

The intentional threats are carried out by people, and they constitute conscious interference in hardware and/or software, aimed at destruction, interception or modification of the computer system. It is possible to counteract such threats only through the greatest hindering in the access to the system by unauthorised people, monitoring of the conduct of people authorised to use the system, and increasing awareness of the computer security among users (e.g. training).

Regardless of a type of the threat, it can include an internal threat, which is caused by the users authorised to use the system, or external one. External threats cannot be generally expected, and it it not possible to be properly prepared for them while internal threats are usually unexpected, and therefore, they are particularly dangerous. Therefore, the supervision over authorised users (e.g. keeping records of operations carried out by them) is so important. Threats can cause various effects and lead, inter alia, to:

- interruption - partial or complete destruction of the IT system's access to information or its incapacity for use, e.g. by physical destruction of a part of the computer, network or the entire system, and the drive damage. It is an attack resulting in the breakdown of the user's connection with the ITS service (e.g. call centre, web site demonstrating the status of road conditions). It can be e.g. accidental or intentional physical damage to a specific network element (e.g. server, cable).
- interception, that is the achievement of the access to resources by unauthorised people, e.g. by stealing the documents, playback of packets in order to intercept data in the network, or illegal copying of files or programmes. This type of threat is dangerous only because of the fact that the attacker obtains the access to confidential data, however, in comparison to other types of threats, does not interfere with their content or data transfer itself,
- modification, that is the achievement of the access to resources by an unauthorised person and introduction of changes to them, e.g. changes in the file with data, changes in the programme in order to activate a different type of operation, modification of messages sent to the network, which involves the modification of data sent by the user to the system by changing the files, and entering other false data.
- forgery – is an attack that involves the falsification of sent data. In this case, the intruder enters false information. The modification and falsification are the most dangerous types of attacks due to the fact that the intruder can cause dozens, hundreds or thousands of false notifications of accidents, paralysing the operators' work in CZR, provide false data concerning courses of public transport vehicle, and also indicate incorrect information on variable message signs.

The solutions and protocols used for the network construction should be publicly available and open. The connection using a stack of TCP/IP protocols for transmission in public networks or in networks, which are not fully controlled by the user, poses a serious risk. Such a situation takes place especially when the communication partners are connected with each other via the public Internet, as in case of GPRS. After connecting the network or computer system with the external network, there are threats related to [5, 14, 15, 16]:

- the possibility of uncontrolled use of any intranetwork services and resources by third parties,
- the possibility of the third parties' uncontrolled use of services, which principally should be made available only to selected external partners,
- the possibility to manipulate the data flow between the subsystems and partners by third parties
- and the possibility of the third parties' interception of confidential data (e.g. passwords etc.) exchanged between devices included in the ITS subsystems, and between the ITS and partners that use data provided by ITS subsystems.

The protection of information transmission is evident in the design process of a new ITS than meets the requirements in terms of information security. All the internal and external elements,

which comprise each subsystem, should be subjected to the inspection of the data security status and its transmission.

The system's contact points are one of critical points due to the fact that they need to connect two LAN networks, usually separated from each other, with the use of the network part, which is widely available, e.g. connection of the highway and national road traffic management system with the urban traffic management system. Both systems operate independently and change information on the transmitted traffic from the city or to the city. They also implement the connection between the personnel of both Systems. Currently, these systems can be connected with the use of VPN (Eng. Virtual Private Network) virtual tunnels with appropriately configured ports on firewalls of both local networks. In this area, only the appropriate transmission encryption, the use of efficient network devices and suitable policy of IT networks can stop most potential intruders, who would like to take advantage of the joint part of the network in order to affect the system from the outside.

Another weak area is HMI (Human – Machine Interface) interface. The threats arising at the point of the human interaction with a machine, in most cases, can be illustrated in the relationship of the personnel – operated device by presenting, e.g. operator of the traffic management system, who inserts an external hard drive unconsciously infected with malicious software. Good quality and regularly updated antivirus programmes as well as other software and hardware security of computers used by employees (e.g. blocking USB ports, the use of filtering according to identification addresses of devices available in the system, etc.) are possible to protect from the majority of unexpected failures, damaged registers, configuration files and databases.

Of course, it is impossible to clearly present all the areas, which result in a risk to integrity and reliability of the transmission. The first step that should be taken is a selection of right people, who will be a design team of ITS architecture created according to FRAME methodology. Only well designed and constructed architecture has a chance to be secure. FRAME assumes that everyone can join the design team, in any case, the membership should be supported by expertise. It will allow to prevent from errors or delays in defining the areas of the designed system. The same applies to the aspect, which is missed in most guides within FRAME, related to the existence of negative stakeholders – people who can cause some inconsistencies of functionality or the system's construction in achieving the goals.

Therefore, at every stage, beginning with the earliest one – defining the system's functionality, it is important to carry out the verification of undertaken arrangements or actions, the tests of action mechanisms of systems as well as quality and transmission tightness.

4. Analysis of information secure transmission mechanisms in ITSs

4.1. Mechanisms to ensure the information transmission security

From the perspective of ensuring the continuity of the information transmission network's operation in ITSs, the possibility of the transmission implementation with the use of bypass roads becomes an important issue. The system should enable the implementation of connections with a specific level of securing operational correctness and reliability. One of the methods includes the planning of bypass roads. In any case, it is crucial to strive for the implementation of a redundant network. However, the costs related to the provision of full redundancy can be significant. Therefore, the analysis of needs and costs for each of the ITS subsystems is required. When the collected information has a little impact on the current operation of the system or does not cause a life threat, a method for the local backup of data and its storage until the time of restoring the connectivity can be adopted. In a place, where the systems related to the security operate, it is crucial to strive for such configuration of the network that it will be resistant to failure of individual connections, individual interfaces or devices. Such a failure does not result in the disconnection of other devices or nodes. Therefore, the communication network's operation in the topology of rings is also preferred.

By taking into account the fact that the topology of separated ITS communication networks will be initially tied in with the course of highways, then, the flat ring topology that is not resistant to the cable's cuts, will be virtually used. Therefore, it is possible to additionally connect with the public data transmission network, that is the Internet network, at the ends of the highway sections operated by such a network. Such connections can be used as an additional independent way of transferring key data in the event of a failure. In general, in any case, it is important to carry out the analysis of the failure results and to prepare actions in order to minimise the impact of the failure on the system operation. The bypass roads do not have to provide a full bit rate that is identical as in the effective system – it should result from the validity of provided information and the analysis of costs. The most desirable ones include the system's automatic switching to the by-pass road. This requires the use of appropriate devices, tools and protocols [3, 12].

In connection with the threats listed in Chapter 3, it is possible to take the appropriate security measures:

- creation of secure transmission channels,
- control of collected and transmitted data and limitation of the access only to specified and necessary data for partners,
- mutual authentication of partners,
- securing the integrity and confidentiality of data.

Due to the fact that the above-mentioned security measures must be used not only in the communication subsystem (transport layer), but also in the application layer, only some aspects of this

problem, which have an impact on the communication system architecture (additional devices required to provide the data flow security) will be signalled in this document.

The flow of data between networks and computer systems can be controlled or restricted using the firewall on the connections between individual networks and subnets, or computer systems. The firewall programmes can be configured in a way that third parties do not have access to intranetwork services and resources, and external partners have access only to the services provided for them.

In order to authenticate the partners and ensure the integrity and confidentiality of data, it is necessary to use advanced security. For this purpose, it is possible to use the following technologies [13, 14, 15, 16, 17, 18, 19]:

- IPSec / Virtual Private Network (VPN)
- SecureShell (SSH)
- Secure Socket Layer (SSL) / Transport Layer Security(TLS)
- PPTP (Point to Point Tunneling Protocol);
- L2TP (Layer 2 Tunneling Protocol)

The mentioned technologies should be used when transferring data through public networks or networks that are not under the control of administration of national roads and highways. These technologies interfere with different layers in the data flow in a similar manner and can ensure mutual authentication as well as the integrity and confidentiality of data with proper configuration.

A set of IPSec/Virtual Private Network (VPN) protocols

A set of IPSec protocols makes it possible to connect two physically connected networks or a network and a computer system, in a secure manner, with the use of a public network and without affecting the action of the application operating in these networks. In general, both parties use VPN routers, which after the mutual authentication, encode the whole data flow between these two networks.

Due to the fact that IPSec functions in the network layer, which as a result, allows for the data flow between connected networks, the firewall programme is most often installed in order to limit and control the data flow between these networks or computer systems. It is crucial to remember that the security measures provided by IPSec include only the data flow between two connected networks through the channel created in the public network, and the data flow within the networks, which are connected with the channel, is not subject to security. The IPSec configuration itself is associated with great expenditure and cause problems, in particular, when the products of different manufacturers are used, and also during the use of the Internet through Network Adress Translation (NAT) [16, 17, 21].

IPSec can be applied in host-host, host-gateway or gateway-gateway connections. The first type requires either a transport mode or a tunnel mode, while the other two connection types require the tunnel mode. Thanks to the authentication and encryption of IP packets, IPSec allows to entirely secure the data transmission based on a stack of TCP/IP protocols [16, 17].

Secure Shell (SSH) Protocol

SSH (Secure Shell) is a network protocol created for being used in the security of connections in the computer systems of a client-server type. It secures login sessions and remote control of workstations at a distance. In this case, the cryptographic algorithms, which secure connections, data transmission and authentication of the server and the client, are used. The principle of the SSH protocol's operation is based on RSA cryptographic technology and is as follows: each of the computers, on which the SSH software is installed, has a pair of keys: the so-called private key available only for the computer administrator (and of course, the system software that supports SSH protocol), and the public key available for all network users. These keys are constructed in a way that information encrypted with the private key can be deciphered only with the public key, and vice versa, the information encrypted with the public key can be deciphered using only the private key. Therefore, keys are interrelated, but any of them can be recovered on the basis of knowledge of the other. The SSH connection is initiated by the programme - SSH client. The client connects with the server and receives the own public key from it. This key is compared with the one preserved in the internal database of the client, from previous connections. In case of detecting the keys' inconsistency, a special warning, which allows to break down the connection, is displayed. Then, the client passes his/her public key to the server, generates a random 256-bit number, encrypts it using his/her private key and the server's public key. The server after receiving a number coded in this manner will decode it using its private key and the client's public key. As a result, the obtained number is random, and moreover, known only to the client and the server. It is used as a key for encoding during further communication. SSH allows to protect the network from attacks of the following types [3, 5, 12]:

- IP spoofing,
- IP source routing,
- DNS spoofing,
- interception of the users' passwords sent through the network in the explicit form,
- based on tapping and falsifying the authorisation at the level of X-Windows protocol.

Many remote services, which use TCP/IP protocol, can be protected with the use of SHH. Among others: applications of the client-server users, database systems and services such as HTTP, TELNET, POP, and SMTP. By using SSH, it is crucial to remember that transferring the connection to a different host, on which the terminal session is not open, will be coded only to the host, on which the terminal session currently takes place. The connection from this host to a target host will not be coded. Therefore, the target host should be always in a secure network or should constitute a host where the terminal session is.

SSL (Secure Socket Layer)/TLS(Transport Layer Security) VPN

SSL (Secure Socket Layer) is a secure transport protocol, which is commonly used to ensure the confidentiality and security of transactions, e.g. in banking or e-commerce. The SSL and VPN networks are often called "clientless" networks, because most web browsers support SSL/TLS protocol, and they are used as the client's software. This is an opposite of the IPSec-based solution, where the client's software provided by the producer must be installed on each computer that uses remote access. TLS (Transport Layer Security) is a protocol of the transport layer developed by IETF and recommended to be used in SSL and VPN networks. The solution of SSL VPN normally means remote access to the network via SSL VPN gateway, but it can also include the applications supporting SSL, e.g. of e-mail clients (MS Outlook, Eudora) [21].

SSL or TLS that is also used, are protocols which operate in connection modes with the use of TCP protocol. A simplified diagram of the creation of SSL session is illustrated in Figure 3.18. In common with IPSec, there is an initial phase, before the connection, in which several parameters are negotiated and verified:

- server authentication by the client using digital certificates,
- optional authentication of the client by the server with the use of digital certificates (or other methods),
- secure generation of session keys used for encrypting and checking the integrity of data.

There are two ways of the remote access implementation with the use of SSL protocol. In the first case, the individual servers, using SSL software, individually apprenticeship the tunnels compiled by remote users. An alternative to this approach is VPN gateway, which on the one hand, is the interface that apprenticeships VPN tunnels of remote users, communicating with the internal server in its natural format.

The connection to SSH server proceeds in several stages:

- server authentication (authenticity is confirmed by two public keys, which change periodically);
- establishing a secure connection (256-bit session key is created and encrypted with received public keys);
- authentication of the client using a given connection (client's identification files and/or his/her RSA public keys or password are used);
- client's login on the server (after successful authentication, the client is logged on the server).

SSH-2 which constitutes a more modern version (which will be considered in case of evaluation) can tunnel any TCP sessions through single encrypting of Secure Shell connection. More importantly, tunnelling makes it possible to secure the communication tunnel for other applications and protocols not affecting their operation and modification of the applications. It is frequently used in the transmission of data packages in the network that applies different protocols in relation to transmitter and receiver networks (virtual channels). SSH-2 supports some of the most powerful encryption algorithms. The data integrity is ensured thanks to HMAC (Hash Message Authentication Codes), and the whole is supported by the X.509 standard, that is architecture of the public key. The SSH-2 protocol consists of three elements. The transport layer protocol, which is responsible for the server's authentication, confidentiality and integrity. The authentication protocol of users that authenticates the client to the server and the connection protocol separating the encrypted tunnel for a few logical channels.

PPTP (Point-to-Point Tunnelling Protocol)

PPTP is an extension of PPP (point-to-point Protocol) standard. By working in the data link layer, it is used for authentication and securing point-to-point connection of a dial-up type in IP networks. PPTP encapsulates and encrypts data with the use of standard methods before their tunnelling. The so-called PPTP control connection creates, configures, and maintains the tunnel, through which data is transmitted. The PPTP operation essentially involves the encryption of PPP data and the provision of PPP, GRE (Generic Routing Encapsulation), and IP headers and data links. Due to the use of GRE protocol, PTP operates only in IP networks. Authentication is based on the protocols resulting from the use of PPP, that is: EAP (Extensible Authentication Protocol), MSCHAP (Microsoft Challenge Handshake Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), SPAP (Shiva Password Authentication Protocol) PAP (Password Authentication Protocol). However, for the purposes of encryption, MPPE (Microsoft Point-to-Point Encryption), which uses MSCHAP (in 1 and 2 versions) and EAP-TLS, is applied. The encryption is carried out with the use of 40, 56 or 128 bit keys. PPTP is used only in IP networks, because it requires the network transport layer to be based on IP. At the same time, it is possible to compile only one tunnel between the VPN server and the client. PPTP does not support the header's compression mechanisms.

Layer 2 Tunnelling Protocol (L2TP / L2TP and IPSec)

L2TP () is a further extension of PPP protocol. L2TP was created as a result of connection of two protocols, PTPP and L2F (Layer 2 Forwarding), and it inherits their best properties. The same as the previous one, L2TP allows for the communication through Dial-up connection. However, this time, its advantage includes the possibility of implementation in networks operating in the IP protocol and in ATM Asynchronous Transfer Mode), X.25 and Frame Relay networks [22].

The sketch of the protocol operation presented in the above figure, from the L2TP technical side, can be understood as connection through a modem and a network of the computer with terminal equipment of a given LAC network (L2TP Access concentrator). Behind LAC, there is a LNS network controller (L2TP Network Server), which transmits data directly to the Internet network. L2TP supports the compiled tunnel and sends data with the use of the same message format. UDP (User Datagram Protocol), which uses 1701 source and destination ports, is applied in this case. As in PPTP, the subsequent but different headers are given to the PPP encrypted data package. L2TP is not an independent protocol. For the purposes of the proper security, it is necessary to use the IPSec protocol. In order to carry out the authentication, the local certificates of computers from the certification authority CA are used. However, two protocols are available: PAP (Password Authentication Protocol) which provides the identity control with the use of a password sent in the explicit form (however, it is a safe process because L2TPwith IPSec encrypt the entire session), and MS CHAP, that is the identity control using a call-response method and separation of encryption keys at the user's level from encryption keys at the computer level. The authentication itself is a process of authentication of computers, and then the users. L2TP also makes it possible to encrypt data with the use of HMAC (Hash Message Authentication Code), and MD5 (Message Digest), which use 28-bit keys. However, the encryption is carried out using 3DES (Data Encryption Standard version 3) algorithms. Unlike PPTP, L2TP allows to compress the headers, and therefore, it uses the bandwidth more efficiently, and also allows to create multiple tunnels between endpoints, which creates obvious manoeuvrability of the availability of many tunnels with different levels of QoS (Quality of Service) services, and security levels.

4.2. Evaluation of mechanisms for secure transmission

In the face of the continuous technical progress and the increasing number of the technology securing the transmission within the framework of VPN tunnels, it is necessary to determine such technology that enables the most efficient cryptographic techniques and access to the link, and it will be sufficiently flexible to be developed at relatively minimal resources in the future. In the assessment of the described mechanisms for ensuring secure transmission in ITSs, several aspects were taken into account. These are the costs of equipment or services, update and modernisation of the security system, access to updates, the necessity of maintenance and frequency of the system operation monitoring, and the scope of their application. The possibility of monitoring, identification of events and detection of the system's gaps was also included. The types of cryptographic techniques, as well as the availability of algorithms, their expansion capabilities, operational speed, and the available sizes of cryptographic keys and authentication techniques were also taken into account. The level of the system's complexity and the possibility of its configuration, the time needed by the administrator for necessary changes and updates, and the required level of technical expertise were taken into consideration.

As a result of the analysis carried out with the use of an expert method, it can be observed that IPSec is a very popular protocol within the scope of application mainly of the IP network. The ease of configuration, and hence, also the functions of monitoring, and the availability of many good cryptographic methods, place it on the high third place according to the analysis. The second place occupied by the SSH protocol, which supports strong security and authentication algorithms, is a widely used and popular method of transmission in terms of configuration of devices and in the environments of Linux and Unix operating systems. The TLS and SSL methods, though not much above than SSH, are located at the first place according to the above analysis. Despite the wide use and several versions of these protocols, the percentage share of newer versions is not as widely used as it could be expected. The advantage within this field is the fact that the opportunities to improve newer versions of SSL and TLS are so flexible that the cost of the version update and adaptation to specific applications will be smaller. However, SSL and TLS constitute a strong security field widely used in IP networks as HTTPS applied, inter alia, in bank applications as a reliable method [22].

Thus, the technologies recommended for the development in terms of VPN tunnels include SSH and SSL/TLS. However, by broadening knowledge on each of three leading technologies presented in this analysis, it should be stated that it is impossible to clearly predict one proper technology in relation to a task planned for this analysis. However, this process significantly explained a range of the problem, which would be face by the team trying to improve each of given methods. Each of the variants has the capabilities of the version development, expansion of use and specialisation in a narrower spectrum of useful application. It all depends on the direction, in which the security technologies develop, because other new technologies, which will be more complex and reliable, on the basis of experience resulting from the existing methods, will be developed and implemented.

3. Conclusion

The information security of ITSs is essential to ensure the operational continuity of ITS services. The paper presented the issues related to an analysis of ITS telecommunication environment. The selected aspects of prevention from risks, which may be an important factor affecting the security of the transport system functioning, were analysed.

The requirements, which are currently imposed to the methods of secure information transmission, can be briefly included in the scope of an analysis of several solution variants in VPN networks. Among them, the most important ones include, of course, technical aspects of security, which are cryptography and authentication. There are many transmission security methods within the framework of VPN tunnels. Unfortunately, it is not possible to find the best solution in terms of security among the currently available technologies. It occurs due to the fact that the best operating security system is the one which is individually selected and configured to the application, network architecture, infrastructure of hardware and users, who are supposed to use this network.

Taking into account that in the day of rapid development of ITC technologies and progress in this area, it is only possible to predict development trends at the macro level. There is a need to systematise the directions of development and specialist research in terms of securing information sent in networks and access to information contained in databases related to the intelligent transport operation. .

Bibliography

[1] CHOWDHURY, M.A., SADEK, A.: Fundamentals of Intelligent Transportation Systems Planning. Artech House ITS Library. Boston, London 2003

[2] WILLIAMS, B.: Intelligent Transport Systems Standards. Artech House, Inc. 2008

[3] KARPIŃSKI, M.: Information security [Bezpieczeństwo informacji]. Publishing House: W.PAK 2012 [in polish].

[4] KOWALEWSKI, M. KOWALEWSKI, J.: Policy of information security in practice [Polityka bezpieczeństwa informacji w praktyce]. Eds. Library IT Professional, 2014 [in polish].

[5] LIDERMAN, K.: Information security [Bezpieczeństwo informacyjne]. Wydawnictwo Naukowe PWN, Warsaw 2012 [in polish].

[6] KRZYKOWSKA, K., SIERGIEJCZYK, M.: The impact of new technologies on the safety level of air traffic in Poland. Safety and Reliability Methodology and Applications, CRC Press 2015 Taylor & Francis Group, London.

[7] www.frame-online.net: European ITS Framework Architecture – Communication Architecture D3.3 Issue I, April 2004.

[8] www.frame-online.net: Planning a modern transport system. A guide to intelligent transport system architecture Issue 2, April 2004.

[9] www.frame-online.net: The FRAME Architecture and the ITS Action Plan.
[10] SIERGIEJCZYK, M., KRZYKOWSKA, K., ROSIŃSKI, A.: Reliability-exploitation analysis of the alarm columns of highway emergency communication system. Journal of KONBiN No. 2(38)2016.
[11] KOWALEWSKI, J., KOWALEWSKI, M.: Cyberterrorism as a particular threat to the national security [Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa]. Telekomunikacja i Techniki Informacyjne [Telecommunications and Information Technologies] 1-2/2014 [in polish].
[12] FRY, Ch., NYSTROM, M.: Monitoring and network security [Monitoring i bezpieczeństwo sieci]. Helion Publishing House Gliwice 2010 [in polish];
[13] STAWOWSKI, M.: Technical bulletin of IT security [Techniczny biuletyn zabezpieczeń IT]. Clico Sp. z o .o 2003 [in polish].
[14] NADER, J.C.: VPNs Illustrated: Tunnels, VPNs, and IPSec, Addison Wesley Professional 2005.
[15] STREBE, M.: Network security foundations [Podstawy bezpieczeństwa sieci]. MIKOM Warsaw 2005 [in polish].
[16] SUTTON, R.J.: Telecommunication security [Bezpieczeństwo telekomunikacji]. WKŁ Publishing House Warsaw 2004 [in polish].
[17] SERAFIN, M.: VPN networks. Remote operation and data security [Sieci VPN. Zdalna praca i bezpieczeństwo danych]. Helion, Gliwice 2009 [in polish].
[18] STALLINGS, W.: Cryptography and network security. Principles and Practice [Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji]. Edition V, Eds. Helion 2012, Gliwice [in polish].
[19] SIERGIEJCZYK, M.: Issues regarding information safety in digital network of railway radio communications, w: Journal of KONBiN, vol. 1, No. 33, 2015.
[20] SIERGIEJCZYK, M.: Issues on implementation of virtual private networks of railway companies [Zagadnienia realizacji wirtualnych sieci prywatnych dla spółek kolejowych]. Logistics No. 3/2009. Poznań 2009 [in polish].
[21] RYŁKO, K.: SSL VPN solutions [Rozwiązania SSL VPN]. Networld 09/2005. IDG Warsaw 2005 [in polish].
[22] Ogórek, P.: The method to ensure a secure transmission of information within the ITS systems [Metoda zapewnienia bezpiecznej transmisji informacji w systemach ITS]. Master's thesis. Lecturers thesis: M. Siergiejczyk. Faculty of Transport, Warsaw University of Technology. Warsaw 2016 [in polish].