ISSN: 1231-4005
e-ISSN: 2354-0133
DOI: 10.5604/01.3001.0010.3143

EVALUATION OF TRANSMISSION SECURE METHODS IN ITS SYSTEMS

Mirosław Siergiejczyk

Warsaw University of Technology, Faculty of Transport
Koszykowa Street 75, 00-662 Warsaw, Poland
tel.: +48 22 2347040
e-mail: msi@wt.pw.edu.pl

Abstract

The essence of the operation of all ITS systems is to make decisions based on the information obtained and available. Under these assumptions, these systems are expected to utilize telecommunication, IT, automation and measurement technologies, which, in conjunction with advanced control methods, improve communication. Each ITS subsystem has specific requirements for communications channels that have to be tailored to the needs of the subsystem, its topology, and users, taking into account the costs of both the construction and operation of the system. The article presents issues related to information security analysis in ITS systems. Some selected aspects of risk prevention, which may be an important factor affecting the safety of the transport system, will be analysed. The analysis and evaluation of secure data transmission methods will also be conducted. This analysis and evaluation will select secure transmission methods using VPN virtual tunnelling technologies.
In the article, 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 problem affecting the communication system architecture is signalled. The methods for secure transmission in ITSs are secure transmission methods commonly used in systems, which require the confidentiality and security of information transmission between the data source and its recipient.

Keywords: *transport, ITS systems, security, information, threats, technologies*

1. Introduction

ITS (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 use of ITS is an affordable and easier method for improving the transport conditions than the communication infrastructure expansion in its current form 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 [1, 14, 19].

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 article, 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. 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. An analysis of information transmission threats in ITS systems

The European Framework Architecture was created on the basis of recommendations of the high-level specialists of telematics. The European Commission decided to finance the KAREN (Keystone Architecture Required for European Networks) project, whose goal was to create ITS European Framework Architecture. 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 adding items to its own additional needs. However, the needs result in functions, 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 [20, 21].

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,
3. Communication Architecture – defines the connection between locations and functions, and it is closely linked with the characteristic requirements and restrictions for given implementation.

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.

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, 5-7, 9, 12, 16, 18]. 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.

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 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 – 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 – 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, 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 the possibility of uncontrolled use of any intranetwork services and resources by third parties, the third parties' uncontrolled use of services, which principally should be made available only to selected external partners, 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 [6, 7, 15, 16, 18].

The protection of information transmission is evident in the design process of a new ITS that 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. Of course, it is impossible clearly to 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 preventing 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.

3. Evaluation of information security mechanisms in ITS systems

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. This requires the use of appropriate devices, tools and protocols [5].

In connection with the threats listed in Chapter 2, 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 [4-7, 12, 16]:

- 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.

The presentation of advantages and disadvantages of the demonstrated security methods can be consolidated, assessed and showed with the use of a multi-criteria comparative analysis method. This method involves leading the founded on arranging the objects on the basis of the adopted cumulative assessment based on partial criteria. Due the importance of the criteria, this method leads the rates of decision-making variants to the state of comparability and their further aggregation. The characteristic feature is determination of the most and least desirable states, that is the preferred directions of changes referring to all criteria. Each of the variants at the end of the algorithm receives a rate for each criterion. The selected maximum cumulative assessment is an optimal or suboptimal variant [2, 4]. This method will be used for supporting the comparison and selection of the most comprehensive data security method within VPN.

In the face of the continuous technical progress and the increasing number of technologies 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.

The assessment will be based on the following criteria:

- Construction and operation costs. Within the framework of these costs, 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, are considered;
- Scope of application. The applications are considered in terms of a multitude of the network types, in which technology can operate correctly, the types of devices, on which it can operate, and the implementation type of the system control unit – hardware (dedicated equipment) or an application (software);

- Application of cryptographic techniques. In this case, the types of cryptographic techniques; availability of algorithms, their quality: expansion capabilities, operational speed, and the available sizes of cryptographic keys, are taken into account;
- Application of authentication techniques. The measure of application will include security assessments of available standard authentication algorithms and new implementation possibilities: currently available, such as Kerberos, Radius etc.;
- Ease of monitoring, identification of events and the system's gaps. Monitoring and identification will be considered in terms of the availability of tools that facilitate operation, identification, log analysis, and the possibility of monitoring the system operation;
- Configuration and required technical knowledge. At this point, the level of the system complexity and the possibility of its easy configuration, the time needed by an engineer for necessary changes in parameters and updates, as well as technical knowledge and the required level of trust in the system engineer (a local engineer working in the company or a specialist, who is locally available on request, hired within the subcontracting company). The engineer's skills should be understood as contractual. In every situation concerning the network security system management, the service personnel's expertise is required. It directly affects the security level of a given network;
- Susceptibility to attacks. This criterion related to the possibility of carrying out an effective attack on security is difficult to assess. It will be based on the author's knowledge, available materials, and his subjective assessment;
- Potential expansion capabilities. Another difficult criterion – it is impossible to predict the direction of technological advances in the digital security systems. This criterion is based on the assessment, which takes into account the current demand for a given type of security and a possible effective scope of each of the security systems.

Analysis and evaluation of the security system will be carried out for the following technologies:

- IPSec (IP Security);
- SSL / TLS (Secure Socket Layer / Transport Layer Security),
- SSH (Secure Shell),
- PPTP (Point to Point Tunnelling Protocol);
- L2TP (Layer 2 Tunnelling Protocol).

In the further part of the analysis, only L2TP protocol will be considered without taking into account its subordination and use with IPSec forming L2TP over IPSec. IPSec assessment is carried out separately, in case of IPSec support; L2TP protocol partly inherits advantages and disadvantages of IPSec method itself.

While selecting the appropriate transmission security system, the construction and maintenance costs usually play the least significant role in initial phases of the system's life. In this case, it is also crucial to take into account the content of the set analysis objective [9]. Therefore, the criterion Construction and operation costs have the lowest weight. The most important aspects of the security system are the principle of its operation, which results in any omitted command functions in the algorithm structure, which contributes to effectiveness in detection of attacks, overall tightness of the system and the level of effort that must be taken by an aggressor in order to gain access to such secured transmission. Therefore, the Susceptibility to attacks criterion has the highest value. Application of cryptographic techniques, Application of authentication techniques and Ease of monitoring, identification of events and the system's gaps criteria have lower values, however, the weights are similar to the previously discussed criterion. The level of advancement and efficiency of cryptographic algorithms and authentication directly affects the previously mentioned value of the aggressor's effort into attack, effectively withdrawing it from the network access. In this case, the Ease of monitoring, identification of events and the system's gaps criterion plays a special role because all the shortcomings resulting from the construction and operation rule

of the security system can be significantly mitigated by active control of the security system and efficient identification of the system's elements potentially susceptible to attacks. The Scope of application criterion responsible for the possibility of using in different network architectures has a relatively high rate. It occurs despite the fact that each method of the network security is individually selected according to the application requirements and affects Potential expansion capabilities. The latter criterion plays an important role, due to the set analysis objective on the expansion capabilities and modernisation of security methods. The last of the set criteria, i.e. Configuration and required technical knowledge is an important value from the perspective of the personnel's ease of work. It is not crucial at selection of the optimal method, because one of the obligatory functioning assumptions/transmission security method requirements includes properly trained personnel maintaining and servicing a given network infrastructure.

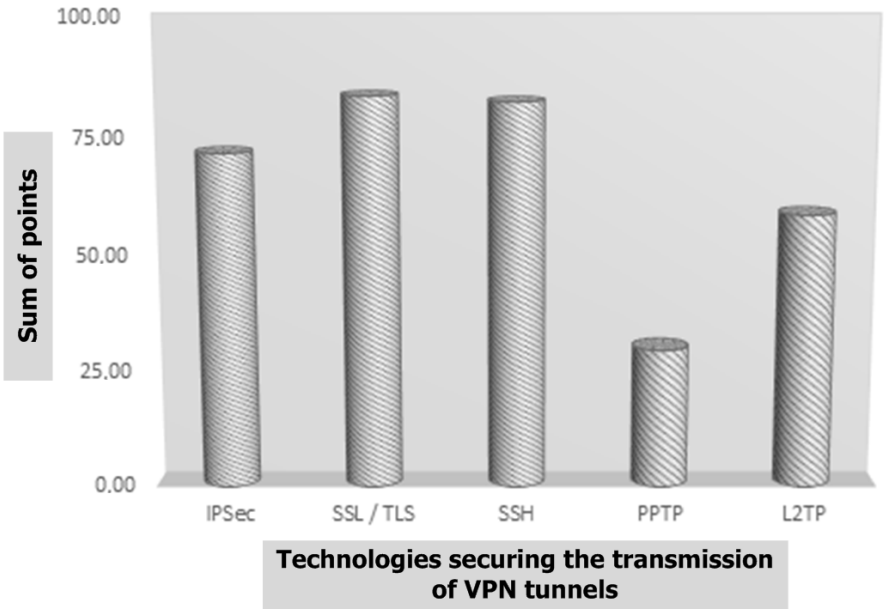

Fig. 1. Final results of analysis of selected methods of data transmission protection

As it can be observed in the analysis results, the security with the use of PPTP is the worst solution in terms of security and expansion capabilities. However, it should not be treated as a fact that PPTP is not suitable as a method. As each of the mentioned ones, PPTP has its own; in this case, narrow range of application with a certain level of the link security, and it is used in this area (dial-up connections). In PPTP protocol, it is seen that L2TP is a more universal and secured solution, which can be recommended as a better PPTP substitute. In case of selecting the optimal or suboptimal method, it is important to choose among IPSec, SSL and SSH [9].

Despite some differences in points, all three methods are characterised by good stability of partial rates (Fig. 2), which shows a certain good level of complexity that these methods represent [9].

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. 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 at the same time, specialisation in a narrower spectrum of useful application. It all depends on the direction, in which the security technologies will 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.

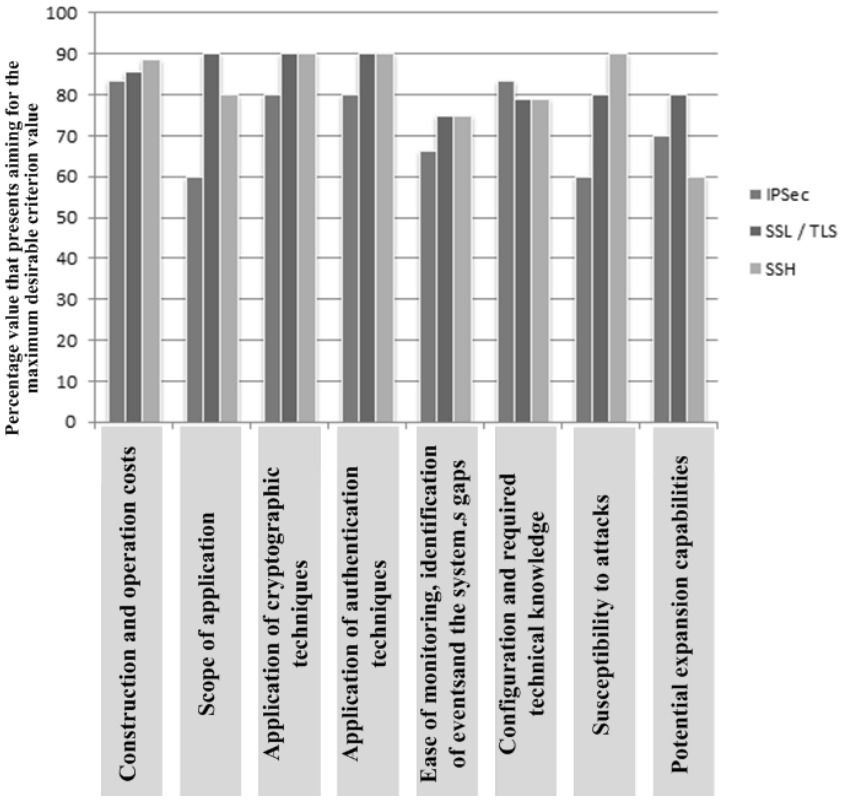

Fig. 2. Percentage value that presents aiming for the maximum desirable criterion value for the best-evaluated technology

4. Conclusion

The information security of ITSs is essential to ensure the operational continuity of ITS services. The article 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.

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.

References

[1] Chowdhury, M. A., Sadek, A., *Fundamentals of Intelligent Transportation Systems Planning*, Artech House ITS Library, Boston, London 2003.

[2] Duchaczek, A., Skorupka, D., Szleszyński, A., *Optimization of the selection of means of transport in the logistics warehouse of building materials* Wyd. WSOWL, Wroclaw 2012.

[3] Fry, Ch., Nystrom, M., *Monitoring and network security,* Wyd. Helion, Gliwice 2010.
[4] Górny, P., *Elements of decision analysis*, Wyd. AON, Warszawa 2004.
[5] Karpiński, M., *Information security*, Wyd. PAK, 2012.
[6] Kowalewski, J., Kowalewski, M., *Information threat in cyberspace, cyberterrorism*, Oficyna Wydawnicza PW, Warszawa 2017.
[7] Liderman, K., *Information security*, Wydawnictwo Naukowe PWN, Warsaw 2012.
[8] Nader, J. C., *VPNs Illustrated: Tunnels, VPNs and IPSec*, Addison Wesley Professional 2005.
[9] Ogórek, P., *The method to ensure a secure transmission of information within the ITS systems*, Master's thesis. Lecturers thesis, M. Siergiejczyk, Faculty of Transport, Warsaw University of Technology, Warsaw 2016.
[10] PN-ISO/IEC 17799:2003 *Information technology. Practical rules of the information security management*.
[11] PN-ISO/IEC 27001:2007. *Information Security Management Systems. Requirements*
[12] Serafin, M., *VPN networks. Remote operation and data security*, Wydawnictwo Helion, Gliwice 2009.
[13] Siergiejczyk, M., *Issues on implementation of virtual private networks of railway companies,* Logistyka, No. 3/2009, Poznań 2009.
[14] Siergiejczyk, M., *Operational efficiency of transport telematics systems*, Scientific Journals of Warsaw University of Technology, Transport series, No. 67, Warsaw 2009.
[15] 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.
[16] Siergiejczyk, M., Wawrzyński, W., *Problem of information security in ITSs,* Logistyka 4/2014, Poznan 2014.
[17] Sosinsky, B., *Computer networks*, Wydawnictwo Helion, Gliwice 2011.
[18] Stallings, W., *Cryptography and security of computer networks. Concepts and methods of secure communication,* Wydawnictwo Helion, Gliwice 2012.
[19] Williams, B., *Intelligent Transport Systems Standards*, Artech House Inc., 2008.
[20] www.frame-online.net: *European ITS Framework Architecture – Communication Architecture D3.3*, Iss. I, April 2004.
[21] www.frame-online.net: *Planning a modern transport system. A guide to intelligent transport system architecture*, Iss. 2, April 2004.