SECURITY OF COMMUNICATION IN THE SPECIAL COMMUNICATIONS SYSTEMS

Grzegorz Różański
Military University of Technology, Faculty of Electronics, Institute of Communications Systems,
gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
e-mail: grzegorz.rozanski@wat.edu.pl

ABSTRACT

The importance of the CIS (Communications and Information System) for supporting the processes of command and management of components of the Armed Forces under the so-called special secure communications systems are discussed. Next, basic communication technologies used in telecommunications systems/networks are briefly characterized. NATO strategies for secure communication in networks were presented, and the importance and role of SCIP (Secure Communications Interoperability Protocol) for End-to-End communication by heterogeneous networks was discussed. Attention was drawn to various concepts and solutions of organization of communication systems in order to ensure the communication systems of the Armed Forces ready for the implementation of specific tasks.

Keywords: military communications, heterogenous networks technologies, security E2E protocols

1. INTRODUCTION

The Armed Forces' communications systems and networks (so-called private or special communications systems), in which the exchange of information is carried out at various levels of confidentiality, play a special role in the state security system. Different types of the Armed Forces use separate, but characterized by interoperability, information systems as part of a joint strategy for management and command of armed forces and cooperating with other components of the state defence system. In the types of Armed Forces, from the operational and functional point of view, basic components of combat units (companies, battalions, brigades, divisions, etc.) are organized, which have their own command systems (command posts) and the necessary information infrastructure (communications systems). Figure 1, in a simplified way, shows the relationship between the command system and reconnaissance systems (reconnaissance sensors, e.g., radio, radiolocation, imaging, etc.) and executive systems (means of destruction, e.g. artillery, rocket, anti-aircraft, etc.).

Radioelectronic Systems Conference 2019, edited by Piotr Kaniewski, Jan Matuszewski, Proc. of SPIE
Vol. 11442, 114420S · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2565307

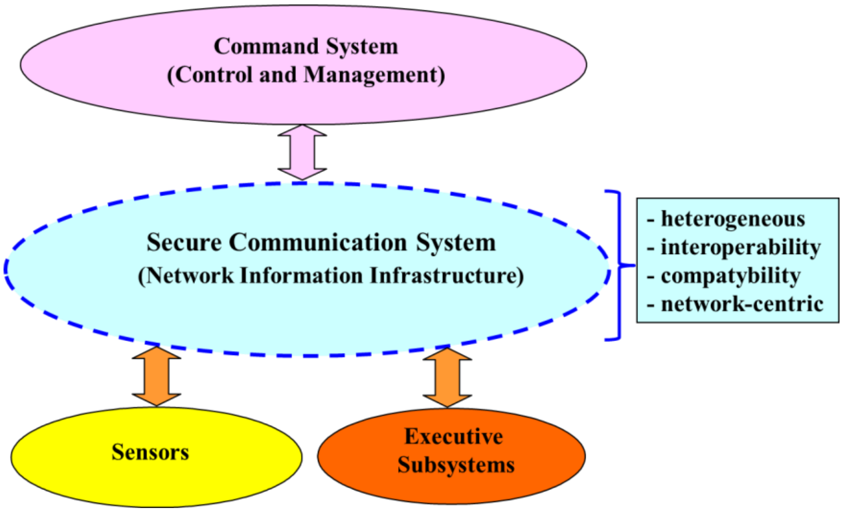


Figure 1. Command, reconnaissance and combat control system and network information infrastructure [1]

The above architecture is referred to as C4ISR, and now as C5ISR (Command, Control, Communications, Computers, Combat System, Intelligence, Surveillance and Reconnaissance).

Communication systems/networks ensuring the organization of information systems at particular command levels are characterized by high *heterogeneity* of architecture, topology and applied technical solutions. They must ensure the interoperability and compatibility necessary to guarantee secure communication with specific traffic and quality requirements for data, voice and video exchange services. *Heterogeneity* concerns various fields of science and technology, including a special role Communications and Information Systems (CIS) in telecommunications systems/networks using different technologies for wired or wireless media. *Heterogeneity* is associated with the concept of *interoperability* as an opportunity for cooperation of different, separate entities to achieve agreed and mutually beneficial goals, while sharing information and knowledge between these entities, through the exchange of information through appropriate communication systems/networks. A special role in the networks is played by the interoperability of Information and Communications Technologies (ICT) understood as the ability of networks to effectively cooperate in order to ensure mutual access of users to services provided in these networks. In contrast, the concept of *compatibility* means the ability of a specific functional element of the system without the need to significantly modify it.

In military systems (but not only), the concept of “network-centric" is also important, which in command systems refers to all projects related to the search for alternatives to traditional organization of battlefield processes - the concept of Network Centric Warfare (NCW). The concept of "network-centric" is often presented as the idea of action, through the large-scale application of modern systems for acquiring, transmitting and managing information to effectively achieve the objectives of military operations. It should be noted, however, that the effectiveness of military operations largely depends on the ability of command systems and the integration of its components to quickly and effectively achieve the intended goal, i.e. the possibility of obtaining the so-called Network Enable Capability (NEC). The above process is implemented both in the cognitive and technical dimension. In particular, the technical context of network-centric capability should take into account both existing and newly proposed solutions in the field of information technology. One of the important aims of the work [2] was to try to answer the following problem: "How to adapt rapidly developing techniques and information technologies to the requirements of operations on the modern battlefield."

Therefore, the starting point for activities in a network-centric environment is to have a network information infrastructure that binds all its participants and enables the acquisition, integration and use of a wide spectrum of information in real time to make the necessary decisions and quickly achieve the desired effect. In particular, ensuring secure End-to-End (E2E) communication for the exchange of information on various classified levels (e.g. NATO clauses: Top Secret, Secret, Confidential, Restricted) is a significant challenge for designers and operators of information systems. An information system that provides support for the command process in a network-centric environment can therefore be seen in the context of the evolution of network infrastructure solutions for ICT systems [3].

The above premises, concerning the nature of the separability of information systems solutions developed for the purposes of national defence, have a significant impact on the architecture of telecommunications systems/networks, in particular in the so-called special (military) communication systems. This applies not only to the abovementioned system-technical aspects of *heterogeneity*, *interoperability* or *compatibility* in an operational “network-centric" environment at the contemporary theater of military operations, but also results from the organization of command systems at individual hierarchical levels of the armed forces, in particular at the tactical level. Common features of information system solutions for military communications systems are not only security of information exchange and user mobility, but also scalability, reliability, survivability, etc. of network infrastructure at various levels of command.

The integration of command, reconnaissance and logistic security systems for combat operations, as well as the implementation of the NCW concept for effective operational decision making, require secure real-time transmission, collection and analysis of many data from a wide range of sensors and other information sources. Figure 2 presents the general conditions for the organization of communications systems in various segments (domains) of the telecommunications network.

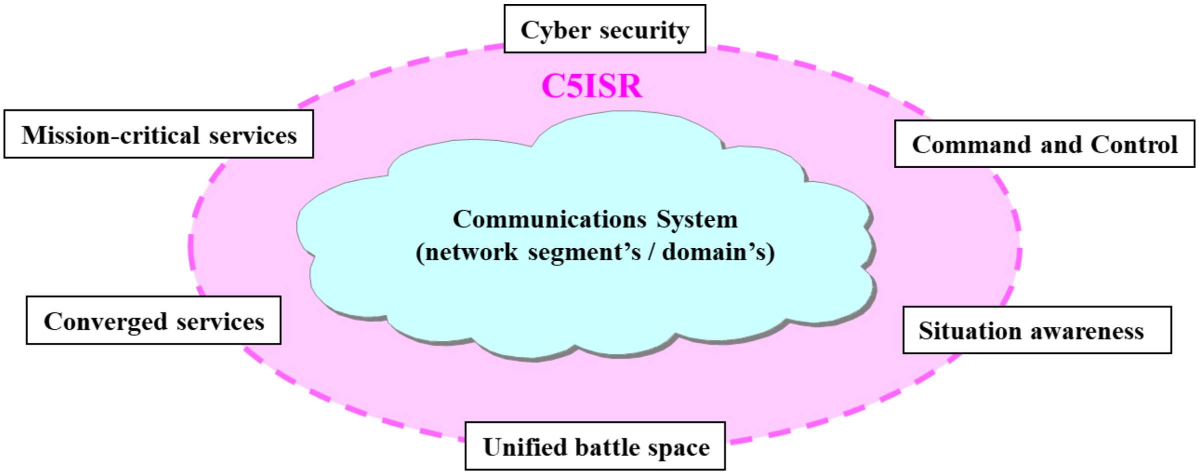


Figure 2. Conditions for the organization of communication systems/networks in the context of the C5ISR architecture

It should also be noted that in the process of organizing the communication system at particular hierarchical levels of command, in the context of the C5ISR architecture, many conditions arising from the specifics should be taken into account: the command and control system, situation awareness, unified battle space, as well as the provision of mission-critical services and their convergence (converged services), with particular emphasis on communication security (Cyber security). The widespread use of the Internet Protocol (including migration to the IPv6 version) and other commercial

protocols, secure access to Internet resources (including military options, the so-called Internet of Things), guarantees of security and quality of services in E2E communication are just some of the challenges posed by contemporary systems.
In view of the above, the rest of the article will briefly discuss modern communication technologies, secure communication strategies (mainly for voice services) proposed by NATO and SCIP protocol (Secure Communications Interoperability Protocol) for secure E2E communication in a heterogeneous environment will be characterized. At the end of the discussion, new proposals (concepts) of solutions for information systems will be presented, including the architecture of FMN (Federated Mission Networking) to ensure communication systems of armed forces with constant readiness to perform specific tasks. It should be noted that the problem of secure communication discussed in the paper applies to the so-called special (separate) communication systems are also based on the considerations presented in the article [1].

2. COMMUNICATION TECHNOLOGIES

The turn of the twentieth and twenty-first century, and in particular the beginning of the twenty-first century is inextricably linked to the emergence of the information society and the development of information and communications technology, closely related to electronics, telecommunications and IT. In all these disciplines, great progress has been observed in basic, research and implementation works. The most important thing is to notice that the driving force behind the development of all these disciplines are two basic values, namely convergence and synergy. Convergence is associated with the tendency to create systems with universal features, as well as similar structure and functional properties. In the case of information technology, it is evident in the modern IT systems offering various services and applications, so far typical of classic solutions. Synergy, in turn, means the interaction of various elements of the system leading to strengthening the efficiency and effectiveness of the entire system, as well as the appearance of new, previously unknown properties or possibilities. Figure 3 illustrates the basic communication technologies currently used in networks in terms of the concept of the so-called overlay networks.

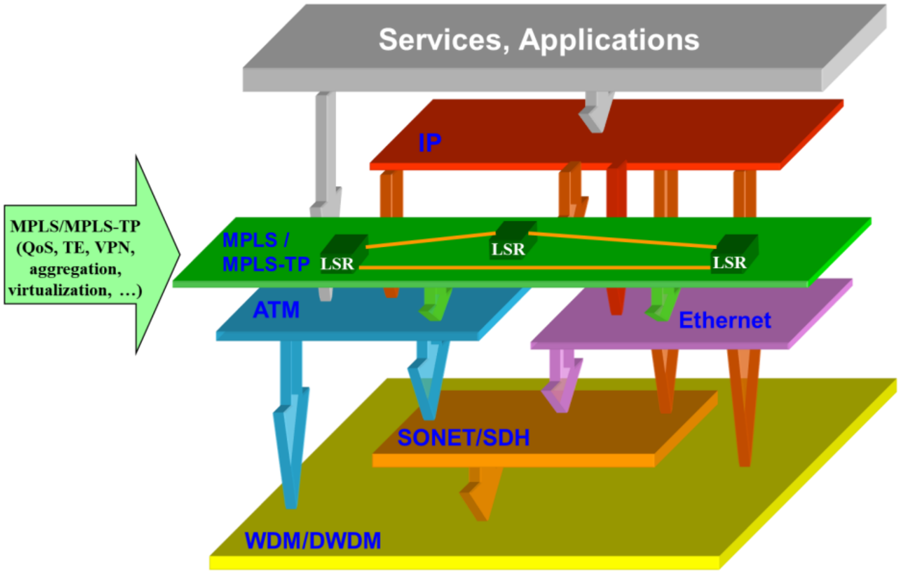


Figure 3. Basic communication technologies

It should be noted that the above drawing is limited to showing only the basic technologies within layers 1-3 of Open Systems Interconnection (OSI) model in the context of the implementation of services/applications (vertical arrows).

The network layer solutions are based on the IP protocol (connectionless communication), cooperating both with routing protocols (RIP, OSPF, BGP, ...), as well as with various mechanisms of service quality support (IntServ, DifServ) and communication security (e.g. IPsec). The networks with a stack of TCP/IP protocols are relatively “simple” in operation (for example, in the implementation for the Internet), and IP is the basic solution in the network layer, while the implementation of any services requires the adaptation of higher layers (in particular in the application layer) to support its functionality (capabilities). The phrase "*All over IP*" means the implementation of any services/applications using the IP protocol stack.

However in the data link layer it is used a whole range of various communication techniques/technologies, starting with the dominance of the Ethernet standard and its evolution, not only in terms of transmission speed (from 10 Mbps to 100 Gbps and more), but also proposals for Provider Bridging solutions (IEEE 802.1ad specification - the so-called "Q-in-Q") and solutions towards connection-oriented Ethernet in backbone networks – Provider Backbone Bridging solution (IEEE 802.1ah specification - so-called MAC-in-MAC), in particular with TE and QoS support.

Since the end of the 1990s, intensive work has been carried out on a new approach to support the TCP/IP protocol stack using the Multi-Protocol Label Switching (MPLS - RFC 3031 specification), especially in backbone networks. MPLS is a specific example of a solution supporting the transport of packets from the network layer (IP over MPLS solutions), but also ensuring the organization of Virtual Private Networks with mechanisms for guaranteeing QoS and service security. MPLS technique introduces the so-called "Label" for marking data units (in an additional header between headers of the network and the data link layer) and creates virtual paths (LSP) in the backbone network with the possibility of aggregating using "tunnels". It should be emphasized that MPLS (similar to the ATM technique) belongs to connection-oriented communication solutions, using network virtualization mechanisms in the network, in cooperation with classic FR, Ethernet, ATM access networks (AToM architecture: Any Transport over MPLS). Therefore, ATM technology is increasingly being replaced by the MPLS due to its better implementation properties in networks with the IP protocol. In addition, standardization processes carried out since 2006 by IETF and ITU-T have led to the development of an extended version of MPLS as a so-called MPLS-TP (MPLS-Transport Profile) with the properties necessary for transport networks (including additional OAM mechanisms). Currently, there are many publications, for example [4], [5], [6], [7], on the application of the MPLS and MPLS-TP solutions not only in backbone networks, but also in access networks.

Next generation networks (NGNs) as a new approach in the design process of telecommunications network architecture leads to the consolidation of many specialized - overlay communication technologies (X.25, FR, ATM, ...) into one solution based on IP (packet switching) with migration to multimedia services based on the IP protocol (Voice over IP services, Video on Demand, ...). This approach applies to both backbone/core and access networks. The next generation of network service capabilities are influenced by mechanisms for creating paths/tunnels in the network, procedures for guaranteeing service quality and communication security, and user mobility. Figure 4 presents the essence of the tunnel creation mechanism by the backbone network (PN - Provider Network).

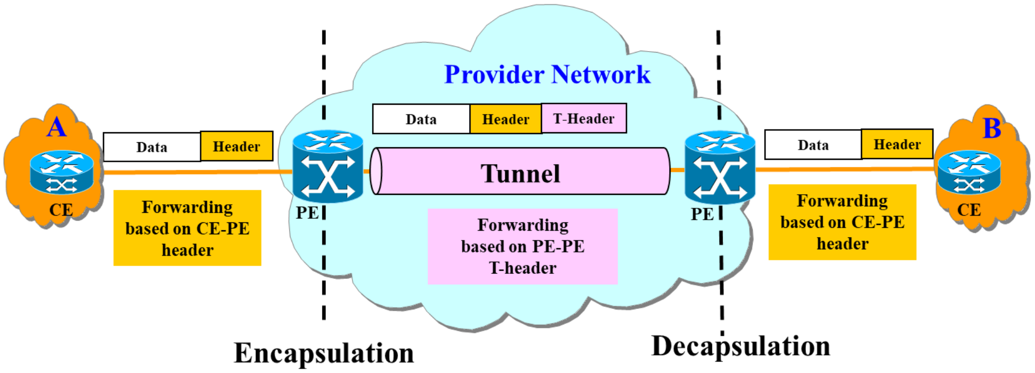

Provider Network
A
B
CE
CE
PE
PE
Data
Header
Data
Header
T-Header
Data
Header
Tunnel
Forwarding based on CE-PE header
Forwarding based on PE-PE T-header
Forwarding based on CE-PE header
Encapsulation
Decapsulation

Figure 4. The tunneling mechanism through the PN backbone network

Data sent from the Customer's network edge (CE) at location A is supplemented ("Enacapsulation" procedure) at the edge of the backbone network (PE) with an additional header (T-header) and transmitted via the backbone network (tunnel created in the PN network) in based on the parameters contained in the additional header. At the exit from the PN, this additional tunnel header is removed ("Decapsulation" procedure) and the data is sent to the edge of the user network at location B.

The mechanism of tunneling through the backbone briefly discussed is of fundamental importance in the design Virtual Private Network (VPN). Currently used tunneling protocols are based on mechanisms both in layer 3 (GRE, IPSec protocols) and in layer 2 (L2TP protocols) of the OSI model, as well as in MPLS VPN solutions - VRF, VPWS, and VPLS mechanisms. Therefore, it is important to emphasize the significant impact of the NGN concept on the strategy of using new communication technologies, including for special communication systems (networks).

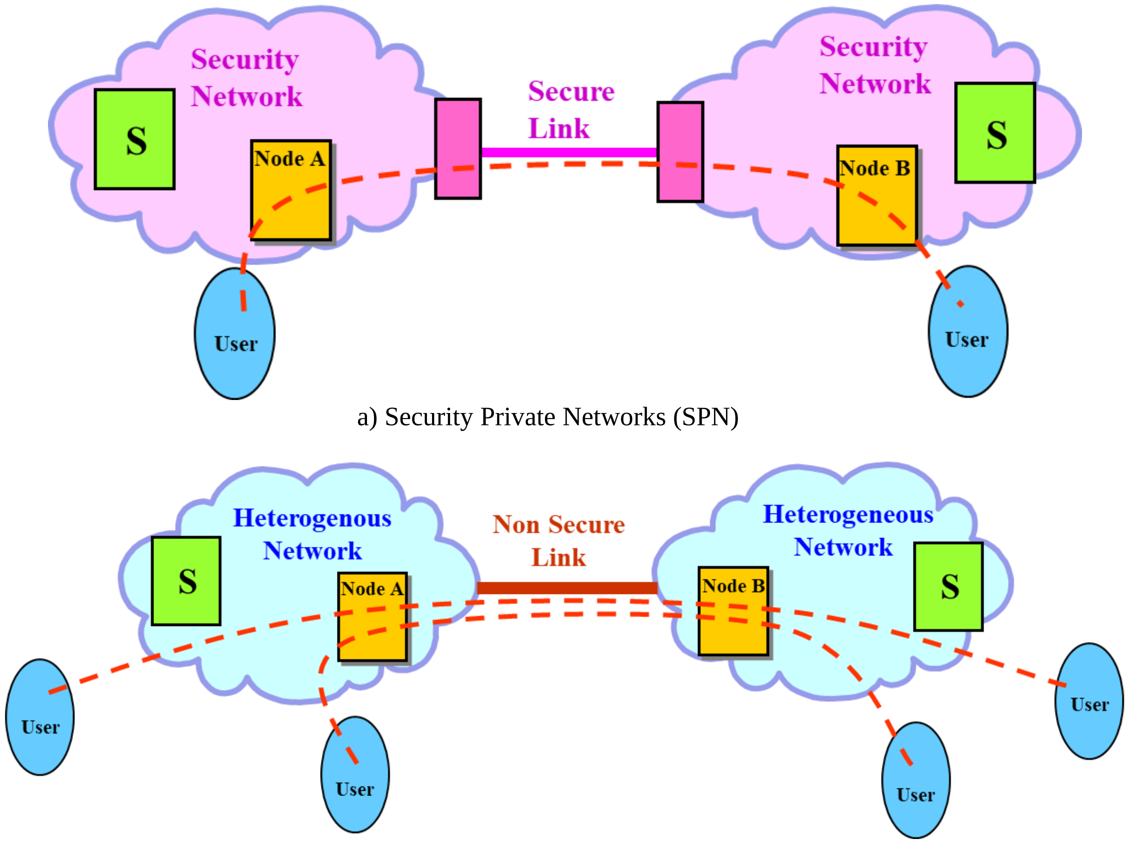
3. COMMUNICATION SECURITY STRATEGIES

The issues of security of information systems, computer networks and telecommunications networks have been given a lot of attention almost from the very beginning of the existence of communication services. This applies not only to the classic telephone service, but also to data and image transmission services as well as broadly understood multimedia services, in particular those implemented in wireless systems and networks. Basics of security architecture in relation to the security dimensions in the plane-layer approach have been included in the recommendation X.805 ITU-T [8], and security issues have been developed and characterized to this day in the context of protocols/techniques/technologies used in telecommunications networks.

Communications and Information Systems Security (CISS) includes many different organizational, system and technical mechanisms, including those related to:

- ✓ assessing the security architecture of information systems and their integrity analysis under threat conditions,
- ✓ analysis of used technologies/communication protocols and security assessment of the technical infrastructure of the telecommunications network,
- ✓ correlation between CISS and NCW,
- ✓ introducing various security management mechanisms/procedures, including the use of various algorithms for cryptographic information security,
- ✓ conducting research in the field of interoperability and compatibility of information systems, including e.g. disclosing emissions, etc.

The heterogeneity of telecommunications systems and networks has a significant impact on solutions in the field of communication security between users in an end-to-end relationship (E2E). Figure 5 presents two concepts for ensuring secure communication: in multi-domain separated Security Private Networks (SPNs), for example with IPSec solution and open Heterogeneous Public Networks (HPNs), for example without IPSec protocol.



a) Security Private Networks (SPN)

b) Heterogeneous Public Networks (HPN)

Figure 5. Secure communication in the E2E relationship [1]

In both solutions, user authentication servers (S) play an important role, and the difference lies in either creating a secure network architecture (Figure 5a) or creating secure E2E communication channels (Figure 5b). However, the introduction of a Secure Link between domains (Figure 5a) requires the use of complex cryptographic conversion mechanisms.

Modern solutions, e.g. for secure voice communication in networks, use the IP protocol and are based on Voice over IP (VoIP) architecture. NATO for military systems suggests several variants of solution such as Voice over Secure IP (VoSIP), Secure Voice over IP (SVoIP) and the Secure Communications Interoperability Protocol (SCIP) and in the document the NATO Secure Voice Strategy (NATO SVS) [9] presents two strategies:

- Voice over Secure IP (VoSIP), where security mechanisms are implemented in the network mainly using **N**etwork and **I**nformation Infrastructure IP **N**etwork **E**ncryptor (NINE) with the IPSec protocol (solution for SPNs - Figure 5a),
- Secure Voice over IP (SVoIP), where network security mechanisms are implemented using Secure Communications Interoperability Protocol (SCIP) for E2E communication (solutions for HPNs - Figure 5b).

Secure Voice over Secure IP option is also possible, but it is not considered or proposed in the NATO SVS strategy. NATO normative documents published in subsequent years (2010-2014): BI-SC Secure C2 Data Strategy (SDS) [10], NATO Secure Voice Strategy (SVS) [9], ADatP-34 (G/H): NATO Interoperability Standards and Profiles (NISP) [11] refer to both strategies.

The strategy of secure data exchange, discussed in the document [10], based on the assumptions of the NATO Network Enabled Capability (NNEC) concept, is to ensure effective and secure mechanisms for transporting and timely delivery of information, its distribution, storage, etc., at various levels of the command system in NNEC environment. This also applies to information lifecycle protection issues in all heterogeneous data exchange environments. The use of NNEC capabilities by NATO forces in conducting new missions raises a number of challenges for introducing new requirements to support C4ISR / C5ISR systems.

It should be emphasized that currently SCIP and NINE are the basic security standards introduced by NATO for the secure exchange of information. They provide information protection, e.g. by encrypting voice, files and messages, in line with the cryptographic interoperability strategy proposed by NATO.

The NINE standard is designed to efficiently support large data traffic flows in IP networks, using the IPSec protocol (including the new IDP protocol - IPSec Discovery Protocol) and new mechanisms/procedures for distributing keys - Multicast Internet Key Exchange (MIKE). It is proposed to use NINE to ensure effective, secure information transfer in command systems, in particular in the FMN concept. The NINE standard is to be based on High Assurance Internet Protocol Encryptor (HAIPE) cryptographic devices, whose interfaces will ensure secure data transmission at speeds above 1 Gbps.

The SCIP protocol, on the other hand, provides encryption in point-to-point or point-to-multipoint relationships through the created communication channels for the VoIP service, but does not support secure routing mechanisms, e.g. using IPsec. More information about the SCIP protocol will be presented in section 4.

Attention should also be paid to the extremely important problem, critical for effective secure communication, which is the key management system. Just as there is a need to develop more effective secure algorithms, e.g. encryption of information directly at the user, also the key management system requires adaptation to different variants of key transfer. Therefore, the requirement for interoperability of Security Management Infrastructure (SMI) to support both proposed strategies will be important. Solutions in this area are largely based on the ITU-T X.509 specification [12].

In summary, both proposals: the SCIP protocol and the NINE standard, form the basis for organizing secure communication in a heterogeneous environment, but further work should be focused not only on their implementation in military communications systems, but also on ensuring their interoperability. In particular, the convergence and synergy of SCIP and NINE devices will be a challenge for manufacturers and operators of secure communication systems.

4. SCIP PROTOCOL

To meet the needs of intensifying work on secure communication systems, International Interoperability Communications Working Group (IICWG) was established within NATO, whose task is to implement and test national solutions using the SCIP protocol. Developed by IICWG and adopted by NATO member states - STANAG 5068 [13] contains the necessary guidelines for implementing the SCIP protocol in the armed forces. The idea of the SCIP protocol is based on the National Security

Agency USA (NSA) proposal developed in Future Narrow Band Digital Terminal (FNBDT) [14] for secure narrowband E2E communication in military and government networks.

Functionalities of the SCIP protocol in the field of secure communication through heterogeneous telecommunications networks (Figure 6) via the IP protocol result from the following premises:

- a low transmission speed of 2.4 Kbps (MELPe codec) is required, to ensure communication via KF/UKF narrowband radio media, and in the case of larger bandwidth resources (broadband radio media), for a transmission rate of 7.2 Kbps, a G.729D codec is proposed,
- providing simplex work (specificity of mobile systems) and point-to-point (P-to-P) or point-to-multipoint (P-to-MP) communication,
- the cryptographic component is an integral part of the SCIP protocol (coalition, mission or national cryptography is proposed),
- in the case of higher bandwidths available, SCIP enables transmission of multimedia data in E2E relation with a speed of up to 10 Mbps.

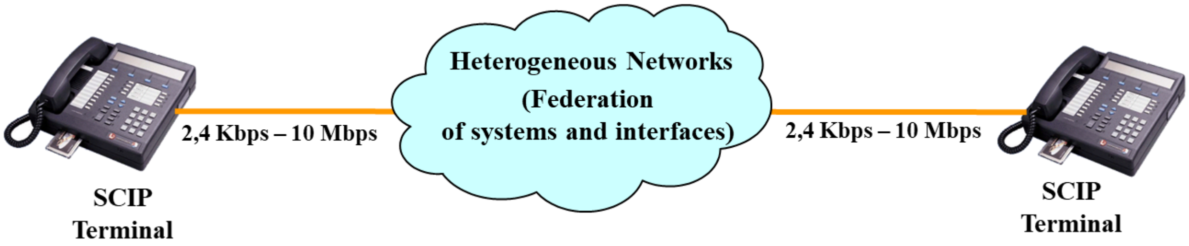


Figure 6. SCIP protocol in E2E communication via heterogeneous networks.

The heterogeneous network environment marked in figure 6 is most often seen as a federation of different systems or interfaces for secure information exchange.

The main features of the SCIP protocol can be characterized as follows:

- ✓ defining channels for signalling and encrypted user data is carried out at the application layer (Layer 7 OSI model),
- ✓ minimum transmission requirements for various technologies and communication protocols are specified below the network layer (Layer 3 OSI model),
- ✓ SCIP channels have their own error control system SCIP Reliable Transport Channel,
- ✓ encryption of user data through the SCIP channel is carried out with minimum requirements for bandwidth (throughput) - the use of different codecs, e.g. MELPe, G.729D, ...,
- ✓ end-to-end E2E encryption requires bit transparency in the channels for sending signalling information and data,
- ✓ SCIP channels can be implemented both through packet and circuit switched networks.

The documentation for the SCIP protocol is very extensive (it contains several dozen different specifications and drafts, constantly updated and developed), but it can be grouped in four basic areas, including:

A. principles of using MELPe (2.4Kbps) or G.729D (7.2 Kbps) codecs for voice signal compression (Voice Compression),

B. principles and methods of encrypting information for each connection implemented in SCIP devices (Encryption - basic document is SCIP231),

C. use of key management infrastructure to ensure secure communication (KMI: Key Management Infrastructure, basic document is SCIP 120),

D. unified connection setup procedures, with the MELPe/G.729D frame stream being sent for voice communications, and the ARQ procedure is used for data transmission (signalling Plane – basic documents is SCIP210); in signalling procedures, information about the type encryption (coalition, mission or national) is also provided.

The advantage of the SCIP protocol is the use of the classic model for the VoIP service (SIP, RTP, TCP, UDP, IP, ... protocols). Figure 7 presents the idea of SCIP implementation in terms of the OSI model and the “overlay” or “peer-to-peer” mode concept.

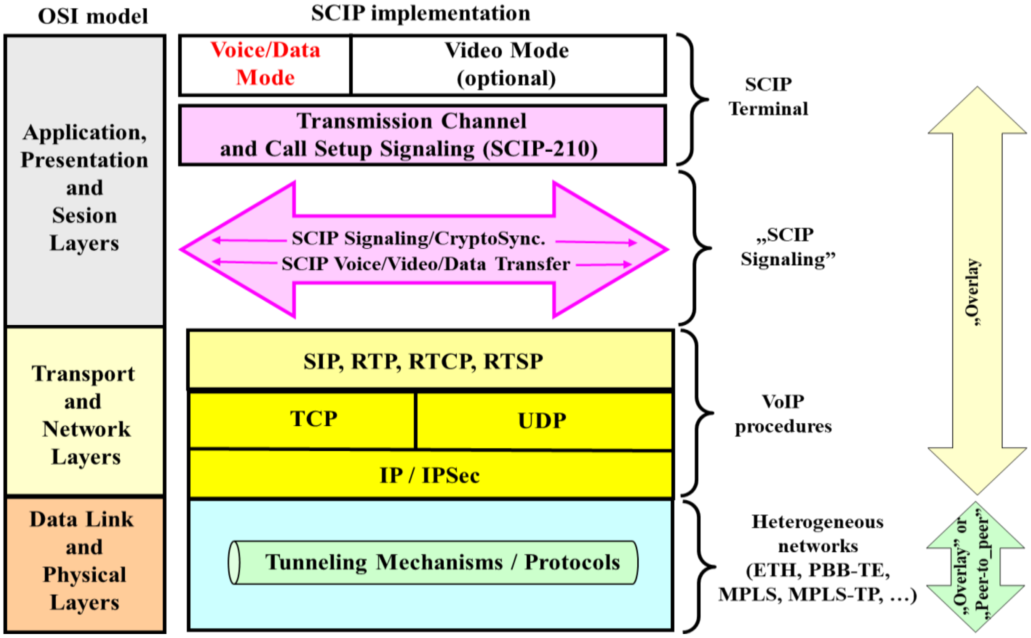

OSI model
SCIP implementation
Voice/Data Mode
Video Mode (optional)
Transmission Channel and Call Setup Signaling (SCIP-210)
SCIP Terminal
Application, Presentation and Sesion Layers
SCIP Signaling/CryptoSync.
SCIP Voice/Video/Data Transfer
„SCIP Signaling”
„Overlay
Transport and Network Layers
SIP, RTP, RTCP, RTSP
TCP
UDP
IP / IPSec
VoIP procedures
Data Link and Physical Layers
Tunneling Mechanisms / Protocols
Heterogeneous networks (ETH, PBB-TE, MPLS, MPLS-TP, …)
„Overlay” or „Peer-to_peer”

Figure 7. Implementation of the SCIP protocol in terms of the OSI model

As indicated in figure 7, SCIP and VoIP protocols, including: signaling and transmission procedures, are implemented in the "overlay" mode, while the organization of communication through segments/domains of heterogeneous networks is based on both the "overlay" and "peer-to-peer" modes". It can therefore be concluded that the implementation of the SCIP protocol at the application layer does not require any modification in the processes of creating end-to-end communication in the lower layers OSI model. This applies to both tunnelling mechanisms through heterogeneous networks as well as the implementation of procedures for the VoIP service using IP/IPSec in the network layer OSI model. In contrast, the SCIP protocol introduces its own signaling mechanisms to ensure the implementation of cryptographic procedures.

The basic implementations of the SCIP protocol relate to the voice service, but the activity of the Polish side deserves to be emphasized in all NATO tests and exercises (as part of IICWG), presenting the use of the SCIP protocol also for the transmission of multimedia services in military (but not only) communication systems in a heterogeneous environment. The signaling and transmission procedures in the SCIP specification have also been modified for video transfer options.

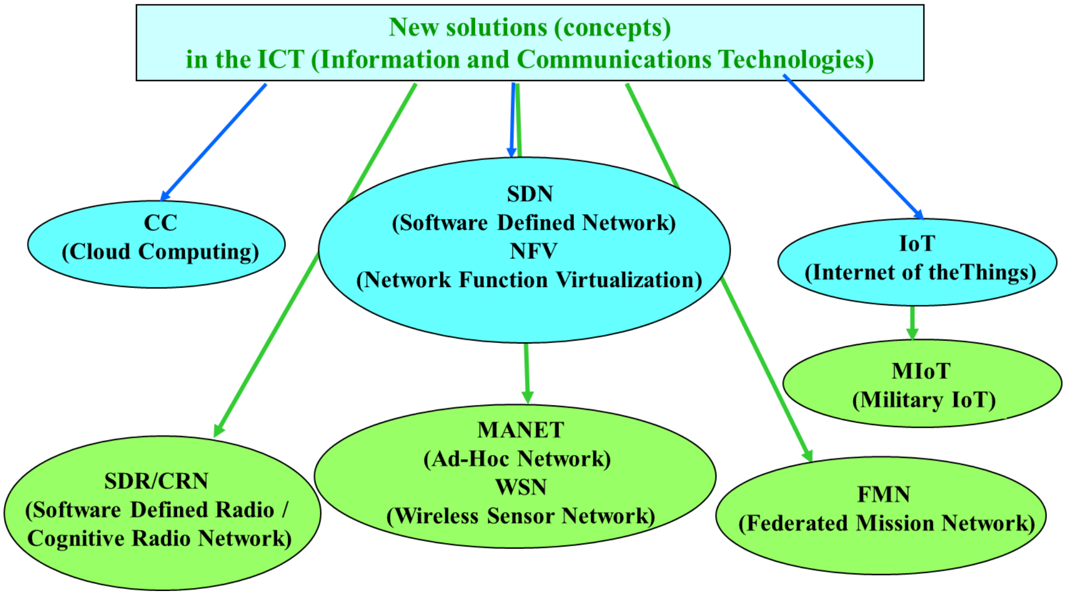
In summary, it should be noted that the SVoIP strategy clearly fits into solutions for information systems, and the SCIP protocol is a good solution for secure voice (as well as multimedia) communication in heterogeneous networks.

The implementation of the SCIP protocol in various end devices (terminals, radio stations, GSM cells, smartphones, etc.) requires, however, the unification of transmission and signaling procedures as well as methods of speech signal coding and cryptographic mechanisms in individual components of the communication system for secure E2E communication through open heterogeneous networks (concept federation systems, networks and interfaces).

SUMMARY

Due to the wide range of topics related to telecommunications systems/networks, including the so-called special communication systems, the article focuses only on some aspects of a wide range of issues related to the properties and functionality of selected communication solutions and technologies in the context of end-to-end communication security.

It should also be noted that for several years there has been an intensive development of new solutions (concepts) in the area of broadly understood information technology (ICT), both in relation to computer systems and in particular to telecommunications systems/networks - figure 8.



New solutions (concepts)
in the ICT (Information and Communications Technologies)
CC
(Cloud Computing)
SDN
(Software Defined Network)
NFV
(Network Function Virtualization)
IoT
(Internet of theThings)
MIoT
(Military IoT)
SDR/CRN
(Software Defined Radio /
Cognitive Radio Network)
MANET
(Ad-Hoc Network)
WSN
(Wireless Sensor Network)
FMN
(Federated Mission Network)

Figure 8. Concepts (solutions) for information systems [1]

The evolution of technologies and communication protocols for the next generation network (NGN) has a significant impact on the appearance of a number of different concepts in the area of ICT organization of information systems and support of telecommunications systems/networks infrastructure in the context of:

- so-called information processing in the cloud (CC: separated-private or open-public),
- software-defined networks (SDN) and network virtualization functions (NFV),
- the Internet of Things (IoT),

and solutions of particular importance in military systems:

- so-called programmable radio (SDR) or "cognitive" radio network (CRN),
- ad-hoc wireless networks (MANET) or wireless sensor networks (WSN),
- federation mission networks (FMN),
- implementation of the IoT in military systems (MIoT).

In particular, the idea of FMN originates from solutions used in Afghanistan, where for the needs of the multinational mission International Security Force in Afghanistan (ISAF) an Afghanistan Mission

Network (AMN) type network was created based on the resources of the secure NATO backbone network and secure components of national networks [1]. FMN is a set of federal mission networks operating within one, common in the field of security policy, information system Protected Core Networks (PCNs) infrastructure, in accordance with the C5ISR architecture. The concept of "federation" means that it is not a mono-system environment, but ensures the interaction of people, processes and communication technologies to exchange information and provide services for mission operational activities. Therefore, referring to the so-called operational capabilities of the FMN environment should be emphasized that they refer to supporting the process of managing federation networks and services and providing a platform that can be used to create and secure the functioning of an information system for NATO and mission participants. The FMN concept assumes several ways to implement it as:

- a federation of networks having one classified information clause with a separate network infrastructure for each mission,
- a federation of networks having different classified information clauses with a separate network infrastructure for each mission,
- a federation of networks having different classified information clauses with a uniform network infrastructure for all mission participants.

Each of the solutions presented in figure 8 plays an important role in the design of information systems and communications systems/networks in military applications.

BIBLIOGRAPHY

[1] Różański G.: „Strategie bezpiecznej komunikacji w sieciach wydzielonych", Przegląd Telekomunikacyjny nr. 8-9, 2016

[2] Praca zbiorowa pod red. M. Amanowicza: „Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w działaniach sieciocentrycznych", Warszawa, 2010

[3] Różański G.: „Techniki telekomunikacyjne wspierające funkcjonowanie systemu informacyjnego w środowisku sieciocentrycznym", Technologie podwójnego zastosowania – wybrane technologie, Wojskowa Akademia Techniczna, Warszaw, 2012

[4] Minei I., Lucek J.: „MPLS-Enabled Applications: Emerging Developments and New Technologies", J.Wiley&Son, 608p, 2011

[5] Technical Report: „Technical Specifications for MPLS in Mobile Backhaul Networks", Broadband Forum, 99p. 2011

[6] White Paper: „MPLS-TP in Mission Critical Systems", KEYMILE, 8p, 2015

[7] Monge A.S., Szarkowicz K.G.: „MPLS in the SDN Era: Interoperable Scenarios To Make Networks Scale To new Services", Juniper Networks, 919p, 2016

[8] Rec. X.805: „Security Architecture for Systems Providing End-to-End Communications", ITU-T, 2003.

[9] NATO C3B: „NATO Secure Voice Strategy", C3B Annex 1 AC/322-D(2012) 0001,2012

[10] NATO SHAPE CIS: „BI-SC Secure C2 Data Strategy", v.1.0, 2010

[11] NATO C3B: „ADatP-34G – NATO Interoperability Standards and Profiles", vol. 2, 2013

[12] Rec. X.509: „The Directory - Public-key and attribute certificate frameworks", ITU-T, 2012

[13] STANAG 5068: „Secure Communications Interoperability Protocol, NATO classified document Standard AComP-5068 ed. A, 2014

[14] Jodalen V., Solberg B., Haavik S.: „NATO Narrowband Waveform - overview of link layer design", NATO, 2011