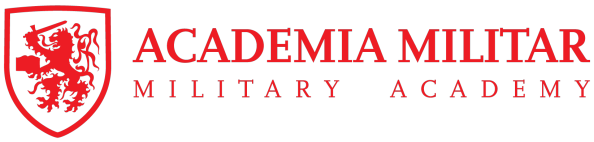

Extending Secure Military Tactical Networks

Daniel Sampaio dos Reis Almeida

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisors: Prof. Ricardo Jorge Fernandes Chaves
Lt. Col. Pedro Manuel Monteiro Fernandes

Examination Committee

Chairperson: Prof. João Luís Da Costa Campos Gonçalves Sobrinho
Supervisor: Prof. Ricardo Jorge Fernandes Chaves
Members of the Committee: Doutor Luís Filipe Xavier Cavaco de Mendonça Dias
Prof. Fernando Mira da Silva

November 2023

Declaration

I declare that this document is an original work of my own authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Acknowledgments

I would like to express my heartfelt gratitude to several individuals who have played pivotal roles in the completion of this academic cycle. Their support, encouragement, and contributions have been instrumental in making this endeavor possible.

First and foremost, I am profoundly grateful to my family, whose unwavering love, support, and belief in me have been a constant source of inspiration throughout this journey. Without them it wouldn't be possible.

I would like to extend my thanks to my friends, colleagues, and comrades who provided valuable insights, feedback, and motivation during all this years of study.

Special appreciation goes to my supervisors, Professor Ricardo Chaves and Lieutenant Colonel Pedro Fernandes, for their guidance, expertise and crucial help in terminating this academic cycle.

Sincere thanks to Captain Rui Gomes, Captain Tiago Gouveia and Captain Nelson Costa for their significant contributions to this work. Their expertise and insights were crucial in understanding the nature of military tactical networks and in finding innovative solutions to the challenges at hand. Their support was indispensable to the success of this thesis.

To everyone mentioned I extend my heartfelt appreciation for being a part of this academic journey. Your support and encouragement have made this achievement possible.

Abstract

In modern military operations, secure communication and data exchange play a pivotal role in ensuring the success of military operations. This thesis presents a exploration of the feasibility of extending classified domains to lower tactical units, since the amount of information soldiers have access to is increasing.

The study is structured into three key stages. An review of academic literature provides the foundational understanding of secure communications and military networks, in order to comprehend what technologies exist and what can be done to improve network security. After this, a fieldwork was conducted to gather real-world insights and requirements essential for the extension of classified domains to lower tactical units. This process involves direct engagement with military personnel and command structures. Finally, a tactical network emulation is employed to simulate the conditions and constraints of operational military networks. This allows for a practical assessment of the potential for integrating encryption and secure channels within bandwidth-constrained tactical networks using cipher machines. The results of the emulation reveal that while the addition of encryption is indeed possible, it is essential to recognize the inherent limitations of these networks. As we descend through the network hierarchy, the need for lightweight encryption becomes increasingly pronounced.

The thesis also outlines potential avenues for future research, including the implementation of encryption protocols and automatic key sharing in tactical military networks.

Keywords

Military Communications; Secure networks; Cipher machines;

Resumo

Nas operações militares modernas, a comunicação segura e o intercâmbio de dados desempenham um papel fundamental para garantir o êxito das operações militares. Esta tese apresenta uma exploração da viabilidade de alargar os domínios classificados às unidades tácticas inferiores, uma vez que a quantidade de informação a que os soldados têm acesso está a aumentar.

Este estudo está estruturado em três fases principais. Uma revisão da literatura académica fornece os conhecimentos fundamentais sobre comunicações seguras e redes militares, a fim de compreender as tecnologias existentes e o que pode ser feito para melhorar a segurança das redes. Em seguida, foi realizado um trabalho de campo para reunir conhecimentos e requisitos reais essenciais para a extensão de domínios classificados a unidades tácticas inferiores. Este processo envolve o envolvimento direto com pessoal militar e estruturas de comando. Por fim, é utilizada uma emulação de rede tática para simular as condições e os condicionalismos das redes militares táticas. Isto permite uma avaliação prática do potencial de integração, através de máquinas de cifra, de encriptação e da criação de canais seguros nas redes tácticas com limitações de largura de banda. Os resultados da emulação revelam que, embora a adição de encriptação seja efetivamente possível, é essencial reconhecer as limitações inerentes a estas redes. À medida que descemos na hierarquia da rede, a necessidade de uma encriptação leve torna-se cada vez mais pronunciada.

A tese também delineia potenciais caminhos para investigação futura, incluindo a implementação de protocolos de encriptação e partilha automática de chaves em redes militares tácticas.

Palavras Chave

Comunicações Militares; Redes Seguras; Máquinas criptográficas

Contents

List of Figures

List of Tables

Acronyms

AH	Authentication Header
AN	Access Node
BCC	Battalion Communication Centre
BLOS	Beyond Line of Sight
CA	Trusted Certificate Authority
CC	Colored Cloud
CCC	Company Communication Centre
CORE	Common Open Research Emulator
C2	Command and Control
DES	Data Encryption Standard
EI-R	Routing-domain-to-routing-domain Information Exchange Interface
EI-RO	Routing Protocol Information Exchange Interface
EI-M	Routing Function and the Modem Exchange Interface
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
FMN	Federated Mission Networking
GPS	Global Positioning System
HMAC	hash-based MAC
HTTP	Hypertext Transfer Protocol
HSM	Hardware Security Module
IEG	Information Exchange Gateway
IP	Internet Protocol
IPSec	IP Security Protocol

ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
IKE	Internet Key Exchange
KDC	Key Distribution Center
KMS	Key Management System
LOS	Line of Sight
MAC	Message Authentication Code
NATO	North Atlantic Treaty Organization
NDN	National Defense Network
OSI	Open Systems Interconnection
OTAR	Over-the-air rekeying
TCP	Transport Control Protocol
TDCIS	Tactical Deployable Communications and Information System
TN	Transit Node
TLS	Transport Layer Security
TGT	Ticket-granting Ticket
UDP	User Datagram Protocol
RAP	Radio Access Point
RL	Rear Link
SA	Security Association
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
SPI	Security Parameter Index
PRT-A	Portuguese Army
PRNG	Pseudorandom Number Generator
PCN	Protected Core Networking
VoIP	Voice over IP
WLAN	Wireless Local Area Network

1

Introduction

Contents

1.1 Context and Motivation

In an era defined by ever-evolving technological landscapes, the role of secure and efficient communication within military operations cannot be overstated. The battlefield is not only a theater of strategy and valor but also a terrain where data and information are pivotal in shaping the outcome of missions. Military tactical networks, the lifelines of modern armed forces, serve as the conduits through which vital information is transmitted. These networks, however, operate in an environment where performance is challenged by the constraints of rugged terrains, limited resources, and the constant threat of adversarial interference.

The security of these networks is of vital importance to military operations, and this thesis seeks to find ways to improve the security of the most sensitive data that is managed by the soldiers close to enemy lines.

This study encompasses a multifaceted approach, incorporating both real-world observation and in-depth emulation, to gain a holistic understanding of the unique challenges and opportunities that military tactical networks present. It explores the delicate balance between implementing robust encryption protocols and navigating the performance limitations inherent to these networks. Additionally, the research extends its reach to the realm of key distribution protocols, further illuminating the path toward a more secure tactical environment.

Throughout this exploration, the thesis emphasizes the importance of encryption and data security in military operations while recognizing the need to maintain network efficiency. It provides a clear plan for future research, which involves assessing new encryption technologies and considering the incorporation of physical encryption devices into the tactical network environment.

Ultimately, this thesis serves as a search for more secure and high-performance military tactical networks. The research endeavors to shed light on the complexities and potential solutions that lie at the intersection of secure communication and tactical operations, and it lays the groundwork for a future where military networks are fortified with robust security measures without compromising operational agility.

1.2 Goals and Requirements

The main goal of this work is to expand a military tactical network security domain taking in account the existence of low-cost and light, while still accredited, encryption devices.

The requirements of this work are to evaluate if the usage of cipher machines still maintain the performance of the existing network and there is no impact on user experience while keeping the costs low.

1.3 Document Outline

This report is composed of this introduction chapter, and 5 more chapters, each of them will approach the following topics:

In the second chapter background concepts are presented, they are essential to understand how computer networks work, cryptographic principles and how secure channels can be established in computer networks. It also presents background to basic military concepts needed to understand tactical networks.

In the state of the art chapter it's shown how the Portuguese military tactical network is structured, followed on how tactical networks are being established by North Atlantic Treaty Organization (NATO).

The proceeding chapter will present three topologies proposed to improve the security to the tactical units of a military tactical network, these topologies vary in implementation complexity, equipment quantity and security design.

The fifth chapter is based in a tactical network emulation to give network metrics to understand if there is possibility to add encryption to these already constrained networks, and how much space there is for this added constraint.

Finally, conclusions are taken of this work and proposal of future work to be developed.

2

Background

Contents

2.1 Computer Networks Principles

Computer networks allow devices such as computers, smartphones, and tablets to communicate with each other and exchange data over a shared medium. They enable us to connect and communicate with others, access and share information and resources.

There are many different types of computer networks, ranging from small, local networks that connect devices in a single location to large, global networks that connect devices all over the world. No matter the size or scope of the network, they all work in a similar way [8].

To provide ”a common basis for the coordination of standards development for the purpose of systems interconnection.” the International Organization for Standardization (ISO) created the Open Systems Interconnection (OSI) Model [9].

It is a conceptual framework that standardizes the functions and communication processes of computer networks and data communication systems. It is not a specific network protocol but a guideline for understanding and designing network architecture and divides network communication into seven distinct layers, each responsible for specific tasks and functions. These layers work together to facilitate data transmission from one device to another. Here's an overview of each layer in the OSI model, starting from the bottom layer (Layer 1) to the top layer (Layer 7) [10]:

Physical Layer (Layer 1): This is the lowest layer, dealing with the physical transmission of data over a physical medium. It includes specifications for cables, connectors, switches, and other physical hardware. The physical layer is responsible for transmitting raw bits over the network.

Data Link Layer (Layer 2): The data link layer is responsible for error detection and correction in the data, as well as the framing of data into frames for transmission. It also manages access to the physical medium and can address hardware-level issues.

Network Layer (Layer 3): The network layer is responsible for logical addressing and routing of data between different networks. It deals with logical addressing, such as IP addresses, and routing protocols to determine the best path for data to travel between source and destination.

Transport Layer (Layer 4): The transport layer is responsible for ensuring end-to-end communication, error detection, and correction. It also manages flow control and segmentation of data into smaller packets. Common examples of transport layer protocols are Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

Session Layer (Layer 5): The session layer is responsible for establishing, maintaining, and terminating communication sessions between two devices. It manages dialog control and synchronization.

Presentation Layer (Layer 6): The presentation layer deals with data translation, encryption, and compression. It ensures that data is presented in a format that the application layer can understand, regardless of the encoding used.

Application Layer (Layer 7): The application layer is the topmost layer and is closest to the end-user.

It provides a platform for applications and network services to interact with the network. Examples of application layer protocols include Hypertext Transfer Protocol (HTTP) for web browsing, Simple Mail Transfer Protocol (SMTP) for email, and File Transfer Protocol (FTP) for file transfer.

Each layer of the OSI model interacts with the layers above and below it. Data is passed down through the layers from the application layer to the physical layer when transmitting, and it is passed up through the layers in the reverse order when receiving. The OSI model helps in the understanding, design, and troubleshooting of network communication by providing a structured framework for communication protocols and functions.

2.2 Principles of Cryptography

In cryptography, a secret key is a piece of information that is used to encrypt and decrypt messages or data. Keys are a critical part of modern cryptography, as they are used to protect the confidentiality and integrity of data transmitted over networks or stored on computers.

Encryption is the process of converting plaintext (unencrypted) data into a form that is difficult to understand without a secret key or password. It is a way of protecting data from unauthorized access or tampering by encoding it in such a way that it can only be decrypted (converted back into plaintext) with the correct key, guaranteeing confidentiality [11].

Encryption is commonly used to protect data in transit (such as when it is being transmitted over a network) or at rest (such as when it is stored on a device). It is an important aspect of computer security and is used in a wide range of applications, including email, instant messaging, file transfers, and online banking [8].

Decryption is the reverse of encryption, it is the process of converting ciphertext (encrypted) data back into its original form, known as plaintext. It requires the use of the secret key which was used to encrypt the data in the first place. It is commonly used to access data that has been encrypted for security purposes, such as to protect data in transit or at rest [8].

There are many different decryption algorithms, and they are designed to work with specific encryption algorithms. In order to decrypt data, the correct decryption algorithm and key must be used.

2.2.1 Symmetric key cryptography

Symmetric key cryptography, also known as secret key cryptography, is a type of encryption in which the same secret key is used both to encrypt and decrypt the data. This means that the same key is used to encode the data before it is transmitted, and to decode it after it is received.

One of the main benefits of symmetric key cryptography is that it is relatively fast and efficient, making it well-suited for encrypting large amounts of data. However, there are some drawbacks to

symmetric key cryptography as well. One of the main challenges is how to securely distribute the secret key to the parties that need it. If the key is intercepted by an unauthorized party, they can decrypt the messages [12].

The implementation of these algorithms is achieved by block cipher or stream cipher. While the first use plaintext blocks to encipher the content, the second uses individual characters.

Block cipher

A block cipher is a type of symmetric key cryptographic algorithm that encrypts data by dividing it into fixed-size blocks and then applying a series of mathematical operations to each block.

To encrypt a message using a block cipher, the next steps are typically followed: the message is divided into blocks of a fixed size (e.g. 128 bits). Next a key is chosen with a typical size between 128 and 256 bits. Each block of the message is encrypted using the key and a series of mathematical operations. The specific operations used will depend on the specific block cipher algorithm being used. Finally, the encrypted blocks are then combined to form the encrypted message.

To decrypt the message, the same key and mathematical operations are used in reverse order, revealing the original message.

Stream cipher

A stream cipher is a symmetric cryptographic algorithm that encrypts data by continuously combining it with a stream of random or pseudo-random data, called a keystream, to produce an output one element at a time.

1. A key is chosen that will be used to generate the keystream. The key is typically much shorter than the message, and it is used to seed a Pseudorandom Number Generator (PRNG).

2. The PRNG is used to generate a keystream, which is a sequence of random or pseudo-random data. The keystream is typically the same length as the message.

3. The message is combined with the keystream using a bitwise exclusive OR (XOR) operation. This creates the encrypted message, also known as the ciphertext.

To decrypt the message, the same key is used to regenerate the keystream, and the ciphertext is combined with the keystream using the XOR operation again. This allows the original message to be recovered [12].

Symmetric key distribution

The key distribution has an important play in the strength of any cryptography system. If Alice and Bob want to share a key, this can be obtained through the following methods [12]:

1. Alice can choose a key and physically deliver it to Bob;
2. If Carlos is a third person, he can choose the key and physically deliver it to Alice and Bob;
3. If Alice and Bob have shared a key in a recent past, one of them can use that previous key to encrypt a new key and transmit it to the other;
4. If Alice and Bob already have an encrypted connection with Carlos, he could deliver a key through those secure channels to Alice and Bob.

In the last option, Carlos acts as a Key Distribution Center (KDC). When a connection between two systems is approved, the key distribution center generates a temporary session key for that connection [12].

Kerberos

Kerberos is a network authentication protocol that is designed to provide secure, mutually authenticated communication between two parties over an insecure network. It was developed by the Massachusetts Institute of Technology as a solution to the problem of securely authenticating users over a network.

In a Kerberos authentication exchange, a client wants to authenticate to a server and request access to a service. The client first sends a request to the authentication server, which responds with a Ticket-granting Ticket (TGT). The client then uses the TGT to request a service ticket from the authentication server, which is used to authenticate to the service [13].

One of the key features of Kerberos is that it uses secret key cryptography to encrypt all communication between the client and the server. This ensures that the communication is secure and cannot be intercepted and read by an attacker.

Kerberos is widely used in enterprise networks and other environments where secure, authenticated communication is required. It is an important part of many security systems and is used to protect a wide range of services and resources.

2.2.2 Public key cryptography

Public key cryptography, also known as asymmetric key cryptography, is a type of encryption in which a pair of keys is used to encrypt and decrypt the data. The keys consist of a public key, which is used to encrypt the data, and a private key, which is used to decrypt the data.

The public key can be shared freely, while the private key must be kept secret. This allows for secure communication between two parties, even if they have never met before and do not have a shared secret key [12].

Public key algorithms are relatively slow and are not well-suited to encrypting large amounts of data. However, they offer a number of advantages over symmetric key algorithms, including the ability to securely exchange keys, and producing digital signatures.

Message Authentication Codes

A *Message Authentication Code (MAC)* is a cryptographic checksum that is computed based on the contents of a message, and is used to verify its authenticity and integrity.

To generate a MAC, two inputs need to be given, a symmetric key and a message, then a cryptographic algorithm is applied to the message [14].

Because ”cryptographic hash functions generally execute faster in software than conventional encryption algorithms” [12], hash-based MAC (HMAC) are widely used insted of block-cipher MACs like Data Encryption Standard (DES).

A *hash function* is a mathematical function that takes an input (or ’message’) and returns a fixed-size string of characters, which is called the hash value or message digest. The input to a hash function can be of any size, and the output (the hash value) is always of a fixed size.

One of the basic properties of a good hash function is that it is one-way, meaning it is computationally infeasible to obtain the original input from the hash value. In other words, given a hash value, it is very difficult to determine what the original input was. Other key property of a hash function is that it is very fast to compute.

Another important property of a good hash function is that it should be collision-resistant, meaning it is very difficult to find two different inputs that produce the same hash value [15].

Digital signatures

Digital signatures are a way to verify the authenticity and integrity of digital documents or messages. When Alice wants to send a signed document or message to Bob, she uses her private key to create a digital signature of the content, then sends it with the document to Bob. Bob will use Alice’s public key to perform a mathematical operation and will use its output to verify the content’s integrity and authenticity [16].

2.3 Hardware Security Modules

Hardware Security Module (HSM) play a crucial role in the cryptographic process by collecting, storing, and protecting private-public key pairs and their associated secret values. They find extensive application in critical infrastructure, including payment solutions, internet encryption systems, and certificate management systems. HSMs are specialized devices that perform cryptographic operations, generate key pairs using random number sources, and securely store them. While most HSMs store data on the device itself, some can back up secret values externally on USB storage devices, hard disks, smart cards, or other digital media. In addition to logical protection, HSMs offer physical protection, incorporating features like tamper-proofing, logging, alerting mechanisms, and the ability to wipe contents when tampering is detected, rendering the device inoperable. Moreover, HSMs isolate cryptographic processes from other operations, enhancing efficiency and overall security [17].

Progress in hardware security modules (HSMs) employed for key storage and the development of both high-end and cost-effective random number generators for key generation point towards a bright future in secure and affordable key management [18].

2.4 Secure Channels

The creation of secure channels through an insecure network can be established through several mechanisms, in this section Transport Layer Security (TLS) and IP Security Protocol (IPSec) are presented.

Transport Layer Security

TLS is a Transport Layer protocol that provides secure communication between two applications over the internet. TLS is the successor to Secure Sockets Layer (SSL), which is a similar protocol that was widely used for secure communication over the internet, and both terms are often used equivalently.

TLS is used to establish a secure connection between two parties, typically a client and a server. It uses a combination of public key and symmetric key cryptography to authenticate the parties and to negotiate a shared secret key that can be used to encrypt and decrypt the data exchanged between the parties, it also adds message tampering detection [8].

When the client connects to a server requesting a secure connection, it presents the supported chipers and hash functions. The server picks one of each he also supports and informs the client. It also supplies a digital certificate containing the server name, the Trusted Certificate Authority (CA) that certifies the authenticity of the certificate, and the server's public encryption key. The client will confirm the validity of the certificate and after that does one of two things: it will encrypt a random number with the server's public key and send it to the server and both sides use the random number to generate a

unique session key to encrypt and decrypt the subsequent data exchanges, or it uses Diffie-Hellman key exchange to securely generate a random and unique session key, this latter method adds forward secrecy [19]. After all these steps are concluded, the client securely sends the private data to the server, using symmetric encryption and the shared key. An example of the messages exchanged to establish a SSL/TLS session is depicted in Figure 2.1.

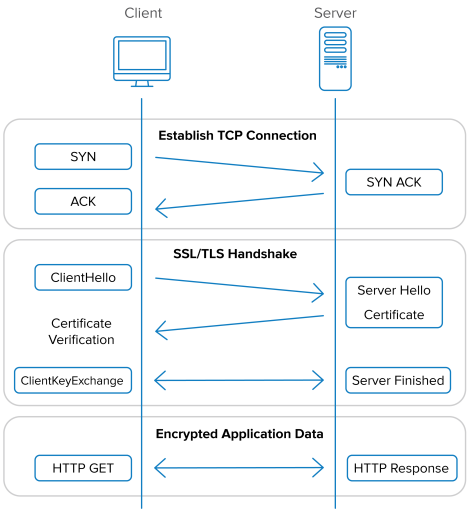

Figure 2.1: TLS session creation [1]

TLS is designed to be transparent to the application layer, it runs ”on top of some reliable transport protocol (e.g., TCP),” [20] meaning that it can be used with a wide range of applications without requiring any changes to the underlying application code. This makes it easy to add security to existing applications and to deploy new applications with built-in security.

TLS is widely used to provide secure communication for a variety of applications, including web browsing, email, and Voice over IP (VoIP). It is also used to protect other types of internet traffic, for example to create VPNs.

Internet Protocol Security

IPSec is a suite of protocols and algorithms used to secure communication over the Internet and other networks. It provides security by encrypting data at the network layer, so that it can be securely transmitted over a public network such as the Internet. It provides security between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host) [21].

It consists of two main protocols, the *Authentication Header (AH)* and the *Encapsulating Security Payload (ESP)*. The first provides user authentication and integrity protection for the transmitted data,

while the second provides confidentiality, as well as authentication and integrity [22].

Both of these two protocols have a tunnel and a transport mode. In tunnel mode, the entire original Internet Protocol (IP) packet is authenticated and/or encrypted and a new IP header is added, while in transport mode only the payload of the original packet is encrypted, while the IP header is not modified.

The *AH header*, which is appended to the original IP packet is depicted in Figure 2.2. It is composed of several fields, such as: *Next Header*, containing the IP protocol with the next packet payload; *Payload Length*, which contains the length of the payload in 4-byte increments, minus 2; *Reserved*, for future use. *Security Parameter Index (SPI)* acting as a unique identifier for the connection, used to determine which Security Association (SA) is being used.*Sequence Number* assigned to each packet, to provide protection against replay attacks. Finally, the *Authentication Information* is composed of the MAC output providing integrity protection [22].

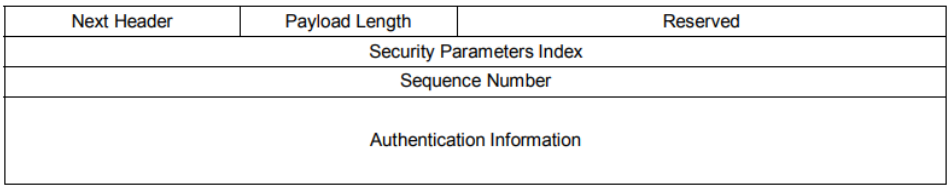

Figure 2.2: AH Header

ESP has two fields around each packet's payload, a header and a trailer. The ESP header contains a *Security Parameters Index* to uniquely identify the connection, making possible to determine which SA is utilized. It also has a *Sequence Number* to provide protection against replay attacks. Whereas the ESP trail may contain *Padding* to make the encrypted data an integral multiple of the block size (because ESP uses block cipher). It carries a *Padding Length* to indicate how many bytes long the padding is. Then comes a *Next Header*, and if integrity protection is active, an *Authentication Information* field composed by the MAC output is added [21].

Figures 2.3 and 2.4 represent how a IP packet is transformed after ESP is applied, both in transport mode and tunnel mode, respectively.

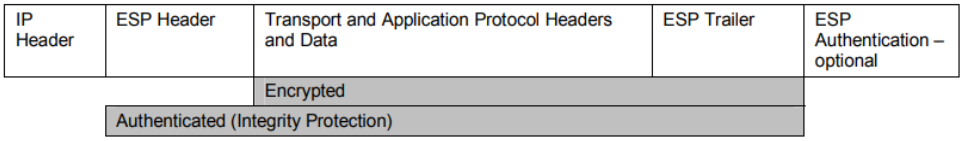

Figure 2.3: IPSec datagram with ESP in Transport Mode

A SA is a unidirectional connection between a sender and a receiver that offers security to the traffic that occurs between them. If both want to be senders and receivers, two SA have to exist. It is uniquely identified by three parameters: the *SPI* that is carried in the AH or ESP header; The *IP Destination Address*; And a *Security Protocol Identifier* which indicates if the association is AH or ESP [23].

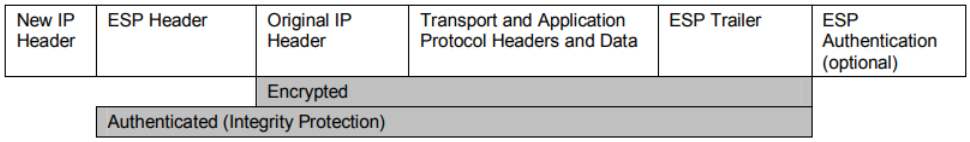

Figure 2.4: IPSec datagram with ESP in Tunnel Mode

A *Security Association Database* is present in each device to define the parameters related with each SA and has the following parameters: a *Security Parameter Index* that uniquely identifies the SA to map traffic to the correct SA; a *Sequence Number Counter* to generate the Sequence Numbers for the AH or ESP header; a flag *Sequence Counter Overflow* to indicate if there has been an overflow of the Sequence Number Counter; a *Anti-Replay Window* to check if an incoming packet is a replay; *AH Information* with the parameters of the AH such as authentication algorithm, keys, key lifetimes, etc. *ESP Information* with the parameters of the ESP like authentication and encryption algorithms, keys, key lifetimes, etc. *Lifetime of this Security Association*; a *IPSec Protocol Mode* which can be tunnel, transport or wildcard; and *Path MTU* which corresponds to the maximum size a packet can have without being fragmented [12].

The security associations of IPsec are established using the Internet Security Association and Key Management Protocol (ISAKMP), which can be manually configurated with pre-shared secrets for small VPNs. For large implementations the Internet Key Exchange (IKE) protocol is usually designated as a secure mechanism to establish security associations.

IKE consists of two phases: the first phase serves to negotiate a bidirectional secure channel known as IKE SA so the subsequent IKE exchanges can occur through it. An IKE SA can be established with main mode or aggressive mode. And the second phase creates a unidirectional IPSec SA through the quick mode [24]. The modes mentioned earlier won't be explained in this report.

In summary, the creation of an IPSec tunnel with IKE can be seen in figure 2.5.

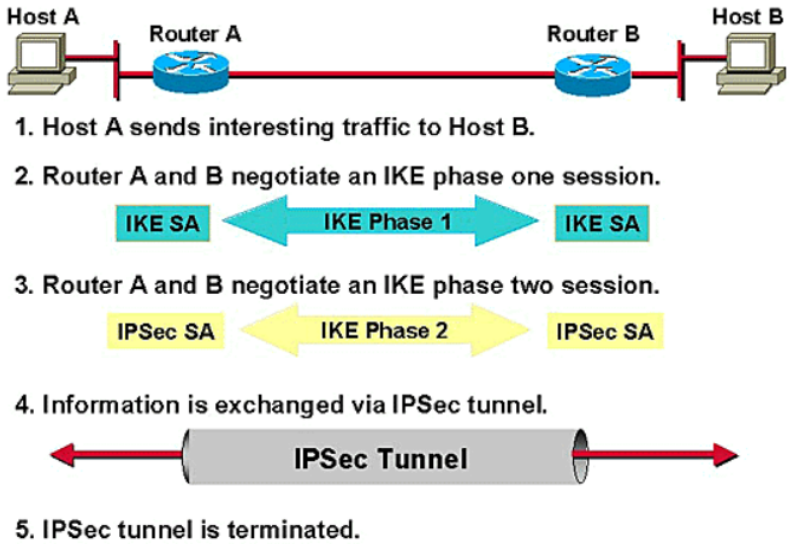

Figure 2.5: IPSec tunnel created with IKE [2]

2.5 Military Networks

Nowadays a core hub-based topology is adopted in the majority of military networks, it has several advantages such as being easier to implement with the existent technologies and organizational structure. It has the disadvantage that its bandwidth is inefficient since traffic usually flows up and down the hierarchical node structure [25].

A mesh network topology is a more very flexible and robust design because any network act as a transit network, and any edge can be used to perform shortest paths routes from one domain to another. In Figure 2.6 is possible to verify that many interconnection platforms can exist and connect different transmission technologies and routing domains. Not relying in a backbone makes the mesh topology very robust. However, it is also far more challenging to implement given the state of network technology and military communication systems today [25].

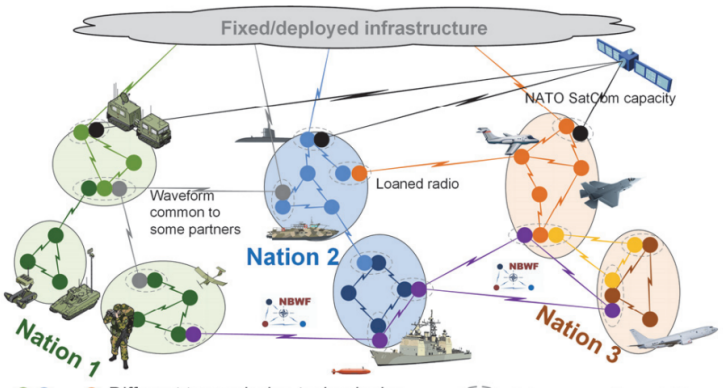

Figure 2.6: Meshed Network Topology [3]

Portuguese Army Units

To better understand how Tactical Deployable Communications and Information System (TDCIS) works, it is necessary to understand how the units are hierarchically structured in the Portuguese Army. From the bigger to the smaller unit:

Brigade: It's a special unit composed of various subunits besides the battalions. There are three brigades in the Portuguese Army (PRT-A).

Battalion: Composed of approximately 500 soldiers

Company: Composed of approximately 110 soldiers

Platoon: Composed of approximately 35 soldiers

Section: Composed of approximately 11 soldiers

Squad: Composed of approximately 5 soldiers

Several battalions belong to a brigade, several companies belong to a battalion, and so forth [26].

Services in Tactical Networks

As a Command and Control (C2) entity approaches the immediate vicinity of its own troop positions, bandwidth limitations may become more apparent. However, it remains crucial for that specific entity to maintain access to essential services. The way these necessary services are provided and the presentation of the Graphical User Interface to users will vary depending on where the user is situated within the land C2 hierarchy. For instance, entities positioned higher up in the Land C2 chain will have a more sophisticated and interactive GUI, whereas those located further down in the chain will encounter a more standardized and text-based service presentation. Nevertheless, the overarching principle is that, regardless of its place in the chain of command, a Land C2 entity should have access to the same core functionality [4].

The need for lower tactical forces to be highly mobile and operate while on the move is expected to reduce available bandwidth in direct correlation with the level of mobility of ground assets, as depicted in Figure 2.7.

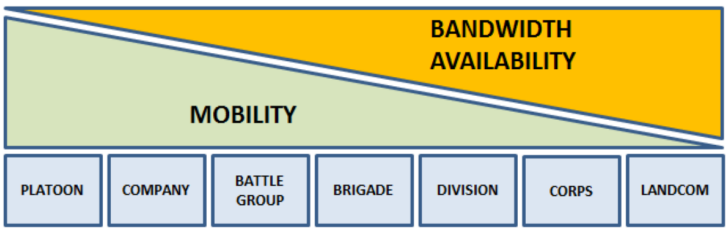

Figure 2.7: Mobility vs Bandwidth [4]

C2 information can be consumed and disseminated using standard file transfer protocols that adhere

to existing STANAGs (e.g., STANAG 5066, Reference Q). Templated messages in message text format following APP11/AdatP3 standards can also be transferred via these protocols.

Verbal orders are commonly employed at the lower tactical levels for the delivery of operational plans, orders, and situational updates. These verbal orders are transmitted over secure tactical voice radio networks or delivered in person by commanders visiting higher command locations.

Tactical radios deployed to support units at the companies and lower levels should have the capability to automatically broadcast their location details, determined using a Global Positioning System (GPS), to their immediate higher command entity [4].

Services that should be available at each unit are specified in Table 2.1.

Table 2.1: Communication Services at Different Levels [4]

Service	Company Level	Battalion Level	Brigade Level
Audio-based Communication (Voice)	- Line of Sight (LOS) and Beyond Line of Sight (BLOS) Wireless narrowband transmission services.	- LOS and BLOS wireless narrowband transmission services	- LOS and BLOS wireless narrowband transmission services
Informal Messaging (Email)	- Not available as a routine service	- Not available from battalion level down to company level	- By establishing a high-capacity data radio network with SMTP servers.
Text-Based Collaboration (Chat)	- By chat function in tactical radios	- By chat function in tactical radios	- Tactical chat IP based software applications or chat functions in tactical radios
Video-Based Collaboration	- Generally not available due to bandwidth constraints	- Not required from battalion to company	- Below Brigade is not a mandatory requirement
Ground to Air	-Company and below required to communicate directly with air entities, e.g. medical evacuation and Close Air Support. -Wireless LOS mobile narrowband transmission services		

RED/BLACK Network

In military networks, the ”red/black concept” refers to a security model that segregates and controls the flow of information to maintain the confidentiality and integrity of sensitive data. The model is named after the colors ”red” and ”black,” with ”black” typically representing unclassified or less sensitive information, and ”red” representing classified or highly sensitive information.

The black network is the less secure network where unclassified or non-sensitive data is processed and transmitted. This network is typically connected to the internet and may handle routine communications and information that does not require a high level of security.

The red network is the highly secure network where classified or sensitive data is processed. It is isolated from the black network to prevent unauthorized access. This network handles classified

communications and information that requires the highest level of security.

To enable controlled and secure communication between the red and black, there is the need to have a set of hardware, software, and policies that facilitate the transfer of information between networks of different security classifications while maintaining strict security controls. It ensures that data can move from the red network to the black network (and vice versa) without compromising security [27].

Military Radios

Military radios are layer 3, meaning they enable the use of standard network protocols, making it possible to connect them to existing IP networks and infrastructure [5].

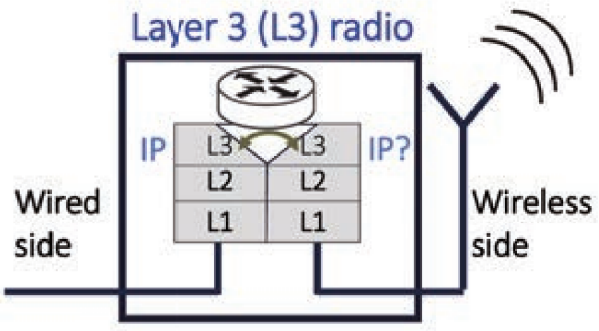

Figure 2.8: Layer 3 Radio Model [5]

In tactical networks, a combination of radios with varying characteristics is usually found. Some are long-range and narrowband, while others have shorter ranges but higher bandwidth capabilities. Certain radios come equipped with built-in cryptographic protection (Z), while others rely on external crypto devices. The nodes within these networks exhibit a wide range of differences, spanning from dismounted soldier nodes, each carrying a single radio, to vehicle-mounted nodes with multiple users and radios, and stationary headquarters setups. Additionally, these radios can function at different OSI layers, with some operating as Layer 3 routers and others as Layer 2 modems.

Figure 2.9 illustrates the radio model. It is assumed that a traditional IP protocol stack is used on the wired side, while the wireless side may employ either a proprietary radio stack or an IP stack.

Conclusion

This chapter explains the principles of computer networks, specifically focusing on the TCP/IP layers and the use of cryptography to secure communications. The concepts of symmetric key cryptography, symmetric key distribution, and the use of Kerberos are discussed. Additionally, the chapter delves into the concepts of asymmetric key cryptography, message authentication codes, digital signatures, and hardware security models. It also explains how secure channels can be established through an

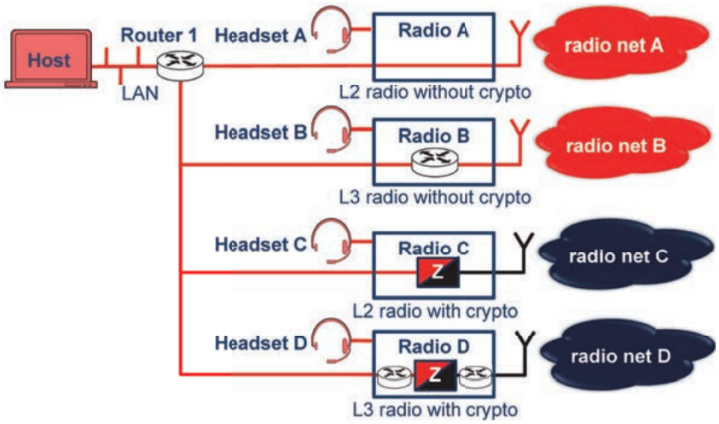

Figure 2.9: Tactical network node [5]

untrusted network and at what layer these security measures are implemented. Next, the chapter covers the specific technologies of TLS and IPSec and their role in securing network communications. And finally, some background to understand how military networks are structured.

3

State of the art

Contents

3.1 Tactical Deployable Communications and Information Systems

The Portuguese Army (PRT-A) is a highly organized and structured force, designed to effectively protect and defend Portugal. One of the key components of PRT-A operations is the Tactical Deployable Communications and Information Systems (TDCIS). This section will provide a look at the structure and composition of the TDCIS and how it supports the overall mission of the Portuguese army. We will explore the various components that make up the TDCIS and by the end of this section, readers will have a comprehensive understanding of the TDCIS.

A project with NATO has recently started to develop a new TDCIS to supplement the existing one. This system is capable of supporting deployments of one entire Brigade at once or multiple sub-elements concurrently in either a Portuguese or international operational role.

The objective is to provide PRT-A with a secure, modular, sustainable and interoperable means of communications and information exchange with other deployed PRT-A units connected to the Portuguese National Defense Network (NDN), or with deployed elements of mission partners connected to a NATO Federated Mission Networking (FMN).

TDCIS is composed of different node types to deliver IT services to users over different domains :

- Access Node (AN) for Brigade level support;
- Battalion Communication Centre (BCC) for Battalion level support;
- Company Communication Centre (CCC) for Company level support.

TDCIS also contains nodes used to build the tactical and reach back Wide Area Network:

- Transit Node (TN) that enables the communication between nodes;
- Radio Access Point (RAP) that enables communication with mobile users;
- Rear Link (RL) that enables reach-back to the NDN.

Figure 3.1 illustrates TDCIS nodes and the relationship between them.

3.2 Tactical Heterogeneous Networks

Seamless cooperation between nations is an important factor in the success of military operations because it allows the different countries involved to pool their resources and expertise in pursuit of a common goal.

NATO realized the importance of a coalition network during the missions in Afghanistan which lead to the definition of FMN [28]. The FMN is a system that allows NATO's member countries to share information and resources in real-time, enabling them to respond more effectively to crises and emergencies.

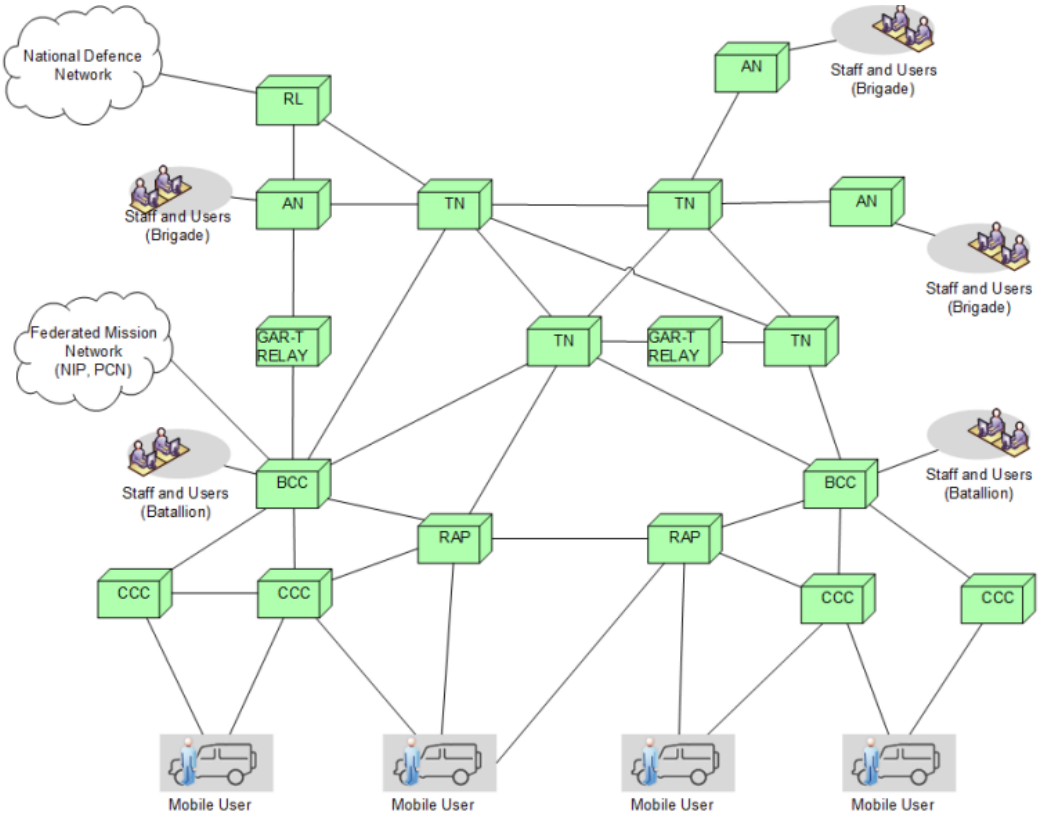

Figure 3.1: TDCIS Overview [6]

The FMN was developed in response to the changing nature of modern warfare, which often involves complex, multi-faceted operations that require the coordination of a range of different military and civilian assets. By enabling member countries to share information and resources in real-time, the FMN allows NATO to respond more effectively to crises and emergencies, and to better protect its member countries and the wider international community.

Recent studies developed by NATO's research group IST-124 revealed that at the lower tactical levels, networks are usually made up of radio networks that utilize different transmission technologies which can vary in terms of bandwidth, frequency, modulation, delay, and range. This can lead to a range of bandwidths, varying levels of connectivity and delay, high bit-error rates, and nodes that must operate in radio silence while behind enemy lines [29].

Radios in nodes can have routing capability or not, making them layer 3 or layer 2 radios respectively. Cryptographic devices can be added outside the radios or built inside them.

Protected Core Networking

The notion of Protected Core Networking (PCN) seeks to create a versatile and secure infrastructure for military IP transport. PCN outlines the necessary specifications to seamlessly link diverse national

network segments, forming a worldwide core network. This approach places paramount emphasis on maintaining a baseline level of security and quality of service. These specifications are currently undergoing standardization by NATO as STANAG 5637.

This objective is achieved through the utilization of multiple network service classes, which cater to both performance and security requirements. PCN is characterized by its sophisticated knowledge, management, control capabilities, and the comprehensive safeguarding of all network components. The network structure based on PCN principles is depicted in Figure 3.2.

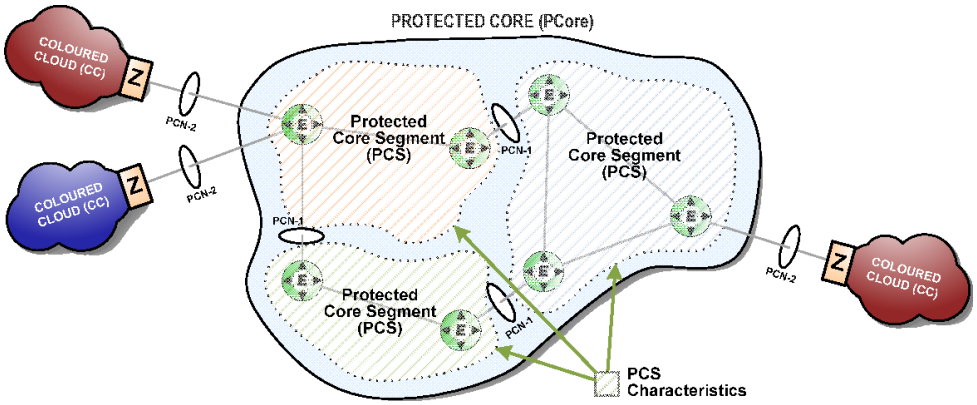

Figure 3.2: Protected Core Networking [7]

In this visual representation, several Colored Cloud (CC) establish connections with a central entity known as the Protected Core. The Protected Core, in turn, comprises multiple Protected Core Segments. The Protected Core functions as a collaborative federation of Protected Core Segments, where each conform to the PCN principles and seamlessly interacts with other protected core segments within this system. The interconnections between different Protected Core Segments within the Protected Core are facilitated through dedicated routers known as E-nodes, operating over the PCN-1 interface [30].

It's important to note that the Protected Core exclusively serves as a transport network, with end-users connecting through the CCs. Cryptographic isolation, represented by the "Z" function in the figure, separates the CCs from the Protected Core transport network. This cryptographic separation, realized through mechanisms like network layer IP encryption, ensures that only users linked to CCs of the same color, denoting specific information/security domains, can communicate.

Furthermore, any node connecting via the PCN-1 or PCN-2 interfaces must undergo authentication to ensure the security and integrity of the network.

3.2.1 Routing Architectures

For the meshed network topology, which has been proven to be the best, there are three distinct routing architectures defined in the NATO's state-of-the-art: flat, interconnect-flat, and interconnect-overlay [31].

Each of these architectures depend on different information exchange interface. On a *flat architecture* (Figure 3.3), a common routing protocol is used by all network segments but with different transmission technology domains. This architecture is usually obtained by connecting Layer 2 radios to a tactical router that runs the common routing protocol, or with Layer 3 radios running the common routing protocol. There is no need to add a information exchange interface on the routing layer but there is the need to have an Routing Function and the Modem Exchange Interface (EI-M) between the routing function and the Modem. A single routing protocol may be beneficial for link break detection and rerouting, but if there is a node operating in radio silence, it must still receive packets but not transmit them. Many standard routing protocols expect periodic heartbeats or acknowledgements, which reduces the list of protocols to use or requires a protocol to be extended [5].

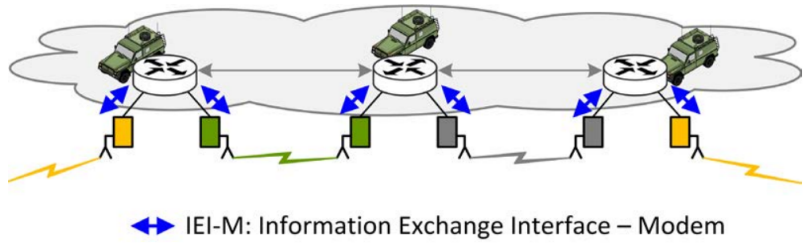

Figure 3.3: Flat Architecture [5]

The *interconnected-flat architecture* (figure 3.4) based on the flat one but where each segment has a different routing protocol or similar protocols on different frequency bands or management domains. The segments connect through an Routing-domain-to-routing-domain Information Exchange Interface (EI-R) and when a node belongs to several routing domains, it's designated as an interconnection platform and have a EI-R between each two routing domains. The purpose of the EI-R is to inform each routing domain of the destinations which can be reached via that domain [29].

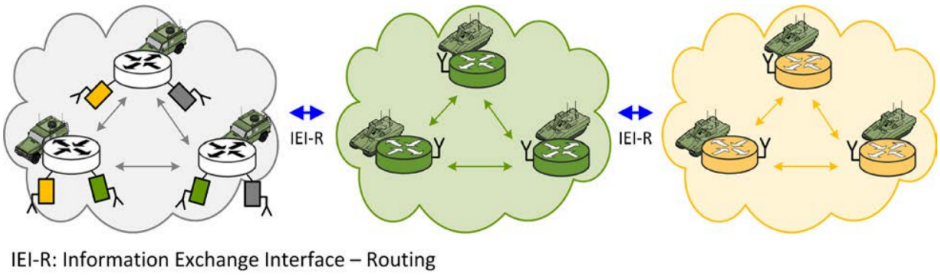

Figure 3.4: Interconnected-Flat Architecture [5]

Interconnect-overlay architecture (Figure 3.5) also includes many network segments with separate routing protocol domains like the latter. This one adds an extra layer of routing in overlay to span

the whole heterogeneous network and connect the separate routing protocol domains.The routers that participate in the overlay network are located on the interconnection platforms.

A Routing Protocol Information Exchange Interface (EI-RO) is added on the routers of the interconnection platforms, between the overlay's routing protocol and the routing domain protocol that work in separate network segments. No EI-R is needed between the different routing protocol domains [5].

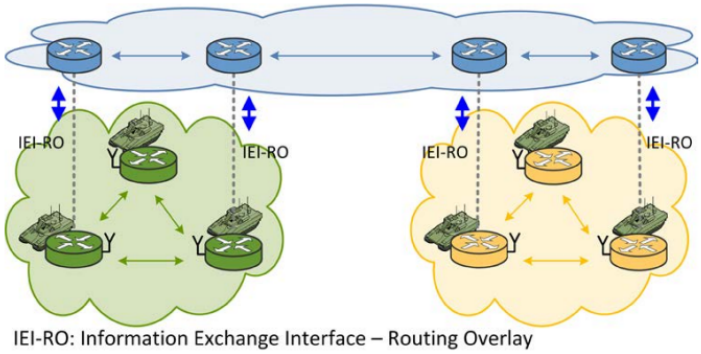

Figure 3.5: Overlay Architecture [5]

3.2.2 Security in Tactical Networks

Cryptographic safeguards can be introduced at various levels within the OSI stack and can be enforced by one or multiple network nodes. These safeguards may find their placement within the originating endhost, within the network infrastructure, or within a radio accessed via a routed network. The impact on the network service hinges on both the specific location within the network – which network node is responsible for applying cryptographic protection – and the layer(s) within the OSI stack where this protection is situated. This subsection explores different options and their associated outcomes, highlighting the advantages and disadvantages of each. For simplicity it is assumed that all radios are layer 3.

Application Level Protection

Application Level Protection includes any type of protection located on the endhosts' network layer or above. It consists of application layer protection mechanisms as well as IPSec or TLS implemented on the host. By using IPSec in the end-host for Application Level Protection, less overhead is needed when using transport instead of tunnel mode.

Some advantages of Application Level Protection is that the user payload is truly protected end-to-end and it has no impact on routing since the cryptographic boundary is outside the tactical network and it's transparent to the communication channel.

One of the main disadvantages is that key management is more complex than the case in where a

single cryptographic device protects multiple hosts, because each host needs a different and valid key for each security association. Another disadvantage is it's very expensive to evaluate, certificate and having security accredited having a large number of endhosts [5].

Network Level Protection

Network level Protection consists on the traditional IPSec approach and is based on network layer encryptors that separate the network into a red side and a black side.

All RED side data is protected end-to-end between the network encryptors.

A advantage of this solution is that a single crypto unit can protect several hosts and applications on a coloured cloud (RED side) and the encrypted data can be transmitted over any unsecured network. Key management is also simpler than the previous case since the same crypto function is used to protect multiple hosts.

Some disadvantages are that this solution introduces more routing domain, in the RED and BLACK sides. And network control and routing information cannot pass freely between the RED side and the black side without compromising the security [5].

Link Level Protection

Link Level Protection embodies a straightforward security framework safeguarding both user payload and vital network management and control data. Moreover, it typically imposes minimal overhead, rendering it a more bandwidth-efficient option than Network Level Protection methods. Notably, it poses no routing challenges since the cryptographic boundary resides at a lower layer within the protocol stack.

Some limitations is that it provides protection on a hop-by-hop basis and necessitates decryption and re-encryption at each hop. Consequently, it implicitly assumes that all traffic belongs to the same security domain [5].

Key Management

Effective encryption implementations hinge on secure key management practices throughout the key's entire life cycle. Failing to handle keys properly at every stage introduces vulnerabilities, potentially leading to unauthorized access, tampering, or interception of sensitive radio communications. Since the majority of encryption algorithms are publicly known, the security of data in transit relies heavily on the safeguarding of the encryption key. The loss or compromise of a key is tantamount to the loss or destruction of the protected data itself.

To ensure the security of encryption keys, organizations employ Key Management System (KMS) or HSM to generate, store, and oversee these keys [32].

Additionally, key distribution protocols can be used to securely transmit keys and certificates. Over-the-air rekeying (OTAR) is a example of this in this strategy, referring to the secure transmission or update of encryption keys within a secure information system, facilitated through encrypted electronic communication channels, ”over the air” [33]. The adoption of these mechanisms serves to make key distribution simpler by reducing the need for physical keying material and the manual loading of cryptographic devices.

Furthermore, a critical component of key management is key and certificate revocation. Keys and certificates should be revoked when they are no longer required, compromised, or when they expire [32]. In manual re-keying systems, the absence of mechanisms to disable keys remotely (i.e., ”over-the-air”) in the event of lost or stolen radios underscores the importance of timely and reliable key revocation. This practice ensures that compromised or unnecessary keys do not pose a threat to the security of sensitive communication systems.

Information Exchange Gateway (IEG) and Cipher Machines

An IEG is a specialized system designed to facilitate secure communication between different security and management domains. In a military context, information exchange is essential to enable seamless human-to-human communication across the force, particularly for mission planning and execution.

IEGs serve as solutions to enable information sharing between diverse security and information domains by offering a managed set of information exchange services. These services aim to bridge the gap between domains that may lack interoperability.

While the exchange of information is essential, it is crucial to maintain the confidentiality and other information assurance aspects of connected information domains. Therefore, suitable information protection services must be implemented to ensure that security and integrity are not compromised during the exchange process [34].

When designing a IEG, some factors demand different requirements depending on the pretended usage. Some of these factors are the level and depth of the inspection of data, what anti-virus or intrusion detection systems are needed, and how data which doesn’t comply with the security policy is to be managed (e.g. quarantine) [35].

In this work, an IEG is an indispensable component of the proposed solution. It makes possible the connection between different levels of classified networks.

Small and cost-effective network encryption devices are currently under development as part of the innovative project DISCRETION [36]. This project sparked the interest and motivation in the improvement of networks’ security particularly in this work in the tactical domain. The emergence of these compact and budget-friendly encryption solutions can open up the possibility for their integration into tactical military communication systems.

Conclusion

This chapter provided a thorough examination of the Tactical Deployable Communications and Information Systems (TDCIS) and their significance within the Portuguese Army (PRT-A). These systems are instrumental in enabling secure, modular, and interoperable communication across various military units.

The concept of Tactical Heterogeneous Networks was introduced, underlining the need for seamless cooperation between nations in military operations, emphasizing the role of the FMN system developed by NATO.

Additionally, the chapter explored the complexities of lower tactical networks, which rely on different transmission technologies, leading to varying bandwidth, connectivity, and delay. It also covered three routing architectures - flat, interconnect-flat, and interconnect-overlay - and their specific use cases.

The PCN concept was discussed, highlighting its role in establishing a secure and versatile infrastructure for military IP transport, emphasizing quality of service and security.

Security measures within tactical networks were addressed, including application, network, and link level protection. Key management was emphasized as a critical aspect of secure communication, along with the role of cryptographic devices like IEGs in secure information exchange.

Furthermore, the potential integration of cost-effective encryption devices, such as those from the DISCRETION project, was identified as a promising avenue for enhancing the security of tactical military communication systems.

In summary, this chapter provided a comprehensive overview of key components and challenges in tactical communication and information systems, setting the stage for further exploration of security architectures in the following sections.

4

Proposed Topologies and Analysis

Contents

In this chapter, our primary focus is to conduct a qualitative study, in ways to enhance the security of lower tactical units using low-cost encryption devices and IEGs to perform the transition between security domains.

Considering that tactical unit radios can transmit data over the air using IP, the concept of creating cryptographic bubbles of different classification domains to segregate the communications of a unit or a group of units was born. It consists on creating clusters of nodes, within which all data packets between them are encrypted and share the same cryptographic key and function. When a packet has to be exchanged between different cryptographic bubbles with a different classification domain, it has to be analysed by an IEG.

This chapter's content was collected in a visit to the PRT-A yearly exercise ORION23. The visit had the focus on understanding how a tactical network is established in the PRT-A and how its security could be improved, having low-cost and certified cryptographic devices. This chapter defines qualitative requirements to the solutions that could make this improvement in the security of tactical networks and some topologies are proposed with a brief explanation on how they could be implemented.

This study was conducted by collecting operational requirements in the field, to understand how low in the hierarchy sensitive information is dealt by military personnel. The scenarios differ in complexity and security level, the first is for situations in where sections deal with more sensitive information, and since they are so close to enemy lines, there is the need on segregating their communications, to revoke their access to the network in case they are compromised. The second can be used in cases where sections don't need access to classified domain and only platoons do, still having their own bubble, so in case they are compromised, their access is also revoked. The final scenario is the least complex and most probable to be implemented, only segregating companies with their platoons, it can be used in the most mobile use cases.

4.1 Scenario 1 - Complete Segregation

Since the battalion and brigade commanders already have access to the Mission Secret classification domain, in this solution we focus on creating cryptographic clusters to the lower units in a cryptographic bubble for each one, as depicted in Figure 4.1

This scenario can be used in cases in which sensitive information is dealt by sections, and since they are very close to enemy lines, a cryptographic bubble is created for them to protect the remaining network in case any section node is captured.

When communication is done between nodes of the same unit, it's encrypted so the packet goes through the air secure. When the communication is between nodes up or down the hierarchy, it has to pass a IEG. This way, if a node has the risk of being compromised or is in fact compromised, the unit

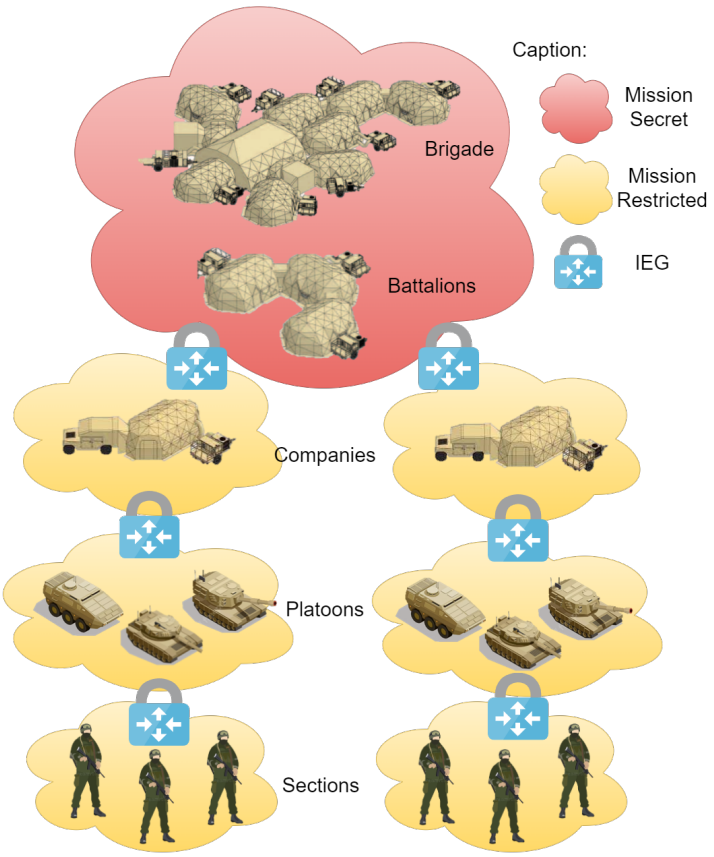

Figure 4.1: Complete Segregation Topology

above can decide what to do to any traffic coming from it (e.g putting it in quarantine or discarding it completely).

Creating cryptographic keys for secure communication within a brigade is a critical component of the security infrastructure. While one option is for the brigade to generate these keys, the sheer number of keys required and the complexity of securely distributing them poses a considerable challenge.

One approach of managing the key is for the higher-level unit to manually create and distribute sets of keys to its subunits before a mission commences. However, if a stable and adequate bandwidth link can be established between the higher-level unit and its subunits, a more efficient alternative is the cryptographic device performing an automatic key distribution protocol to facilitate a secure key exchange protocol over this potentially insecure channel.

While this topology provides the highest level of security among those discussed in this chapter, it is also the most complex and costly to implement. The primary advantage of this solution is the hierarchical control it offers; if any unit becomes compromised, the unit immediately above it has the capability to disconnect it from the network, thereby preventing further damage. However, a notable drawback is the

Table 4.1: Quantity of cryptographic devices for complete segregation

Unit Type	Quantity
Brigade	1
Battalions	3
Companies	9
Platoons	27
Sections	243
Total (+15% backup)	325

intricate key management process associated with this approach, owing to the vast number of nodes that require valid cryptographic keys.

Estimating the cost of equipping a brigade with cryptographic devices for each unit involves several factors, including the type of cryptographic devices, their capabilities, and the scale of deployment. But a rough cost estimation can be made, and in Table 4.1 the quantity of cryptographic devices is summed.

The cost of cryptographic devices can vary widely. For high-security military-grade devices, you might be looking at a few thousand to tens of thousands of euros per device, depending on the features and capabilities. But since this solution is focused on lower-end devices it should be more budget-friendly, and for simplicity reasons, it's estimated in this work at a thousand euros.

The cost of the equipment is not the only factor to be considered, the cost of installation and integration into the existing communication infrastructure may involve additional equipment and software, and also maintenance and support to maintain and perform updates to the equipment.

4.2 Scenario 2 - Simplified Complete Segregation

In this alternative approach, the configuration significantly differs from the previous one, making it distinct due to the reduced number of nodes that require cryptographic keys and protection. Leaving the communication between the platoons and sections with lesser secure methods already used (Figure 4.2).

This scenario can be used in cases in which sensitive information is dealt by platoons and protecting the information dealt by sections is seen as not critic.

Similar to the previous scenario, communication within the same unit is encrypted to ensure secure data transmission. However, when nodes need to communicate either up or down the hierarchy, the data must pass through an IEG. This setup provides a critical security layer, allowing the higher-level unit to assess and manage the traffic originating from compromised or potentially compromised nodes. Actions may include isolating the compromised node, placing it in quarantine, or discarding the traffic altogether.

Creating cryptographic keys for secure communication remains a fundamental aspect of this security

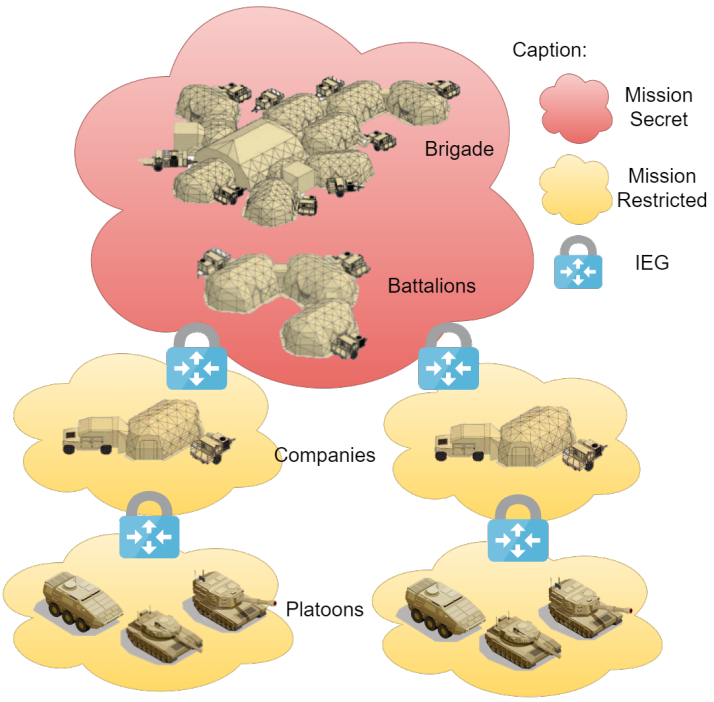

Figure 4.2: Simplified Complete Segregation Topology

infrastructure. One option for generating these keys is for the brigade to create them manually. However, this alternative significantly reduces the number of nodes that require keys, simplifying the process. Unlike the previous complex and costly method, key management in this scenario becomes much more simpler, because the number of keys to be distributed is significantly reduced.

This simplified topology maintains a commendable level of security while offering advantages such as hierarchical control. In the event that any unit becomes compromised, the unit immediately above it possesses the capability to take swift action, disconnecting the compromised unit from the network to prevent further damage. Notably, one of the key benefits of this solution is the streamlined key management process due to the reduced number of nodes requiring valid cryptographic keys.

When estimating the cost of equipping a brigade with cryptographic devices for each unit, several factors must be considered, including the type of cryptographic devices, their capabilities, and the scale of deployment. However, in this scenario, the cost estimation is notably lower due to the reduced number of nodes. As seen in Table 4.2, the quantity of cryptographic devices required for this simplified configuration is summed.

Having around 85% less devices than the first proposed solution, the price of product acquisition is significantly lower than the previous case.

Table 4.2: Quantity of cryptographic devices for a simplified complete segregation

Unit Type	Quantity
Brigade	1
Battalions	3
Companies	9
Platoons	27
Total (+15% backup)	45

4.3 Scenario 3 - Companies Segregation

In this alternative solution, the primary objective remains focused on maintaining the security of the Brigade and Battalions within the Mission Secret classification while creating individual cryptographic bubbles for each Company to communicate securely with their respective subunits, operating within a Mission Restricted classification domain. This approach ensures that sensitive information remains well-protected and isolated from unauthorized access, Figure 4.3.

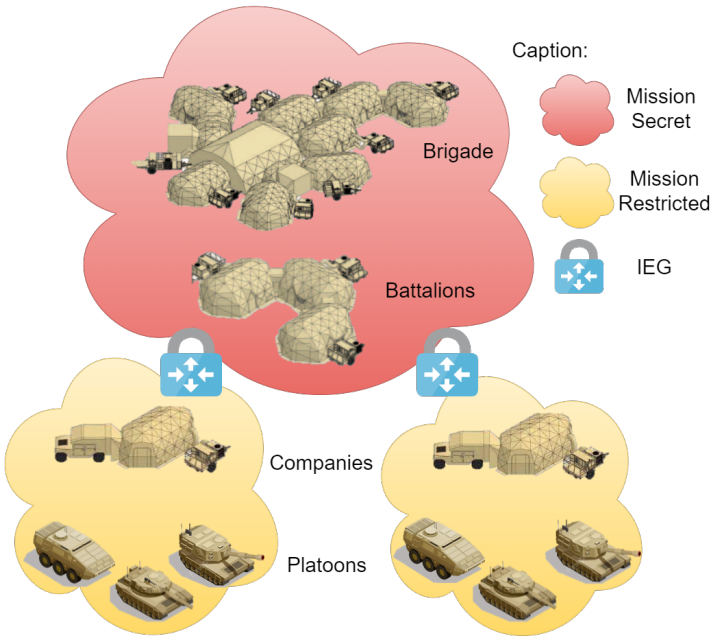

Figure 4.3: Company Segregation Topology

This solution is the most simple to implement and the most probable use case, since platoons and companies are very mobile units the traffic between them is not choked by an IEG.

The hierarchical security structure is still preserved, with the Company serving as the focal point of communication and coordination for its subunits. However, when Company-level communication needs to extend to the Battalion level, a crucial security layer is introduced in the form of an IEG. This gateway acts as a guardian at the border between security domains, ensuring that data crossing this boundary

is suitably protected. This extra layer of security guarantees that sensitive information remains compartmentalized, even within the larger Battalion domain.

The greatest difference between this scenario and the others is that it only requires an IEG between the battalions and their companies, since the available bandwidth for even lower units is very constrained, the encryption devices are the only extra amount of constraint to the already low bandwidth.

One of the standout advantages of this solution lies in its simplicity regarding key infrastructure. With only a handful of nodes within the same security domain, key distribution becomes a straightforward process. Battalions can employ physical key distribution methods or key sharing protocols to establish secure channels over the air, such as via satellite or radio links. Since the number of nodes that need to receive keys is relatively small, this approach is highly efficient and manageable. Battalions can securely share cryptographic keys with their subordinate Companies, ensuring that secure communication is upheld throughout the hierarchy.

When considering costs, this solution is notably cost-effective in terms of product acquisition, akin to the second topology mentioned earlier.

In summary, this alternative solution not only maintains the security of Brigade and Battalion operations within the Mission Secret classification but also streamlines the key management process. It provides a practical and cost-effective approach to ensuring the secure exchange of information, making it a compelling choice for military operations where simplicity and efficiency are paramount.

Conclusion

In conclusion, this chapter has explored three distinct scenarios, each designed to enhance the security of tactical networks. These solutions offer valuable insights into how the military can safeguard sensitive information and maintain operational security in a variety of scenarios.

These topologies hold particular promise for units engaged in Intelligence, Surveillance, Target Acquisition, and Reconnaissance missions. These units often deal with highly classified data, making the need for secure communication paramount. Furthermore, these solutions are well-suited for Artillery Gun Systems, where data integrity and security are essential for precision targeting. Additionally, Special Forces units, which frequently establish communications deep within enemy territory, can benefit from the implementation of these topologies to ensure the confidentiality and integrity of their communications. In summary, these scenarios try to give an insight on how an extension of more secure communications to troops that deal with more sensitive information can be made.

Key to these solutions is the use of lightweight encryptors, which provide a practical and cost-effective means of securing information across various echelons of command. These encryptors not only bolster the security of communications but also streamline the key management process, making secure communication more accessible and efficient.

As modern military operations become increasingly data-centric, the ability to protect sensitive information and maintain secure communication channels is of paramount importance. The topologies presented in this chapter offer versatile solutions that can be adapted to a wide range of scenarios, ensuring the security of critical military operations.

5

Topology Emulation and Evaluation

Contents

In order to study the implications of adding encryption to the tactical units, this chapter focuses on defining the limits that tactical military networks have in terms of performance metrics.

The efficient operation of a battalion tactical network is of paramount importance in modern military scenarios, necessitating an in-depth analysis of network topology and its various parameters. This chapter describes the methodological approach adopted in our research to explore the implications of cryptographic equipment on the communication within a battalion tactical network.

To perform this study, a tool for building virtual networks Common Open Research Emulator (CORE) developed by the U.S. Naval Research Laboratory was used. The main objective of this chapter is to understand the extent to which encryption and packet transformation processes impact key network performance metrics, with a focus on assessing the maximum latency introduced by the cryptographic operations.

To conduct our study, we start with the creation of a network topology that mirrors the structure of a battalion tactical network with some TDCIS nodes represented by a router and a end user. This hierarchical design begins with mobile users as the lowest network entities, connected to their corresponding CCC and every CCC connected to each other and to their BCC, as depicted in Figure 5.1.

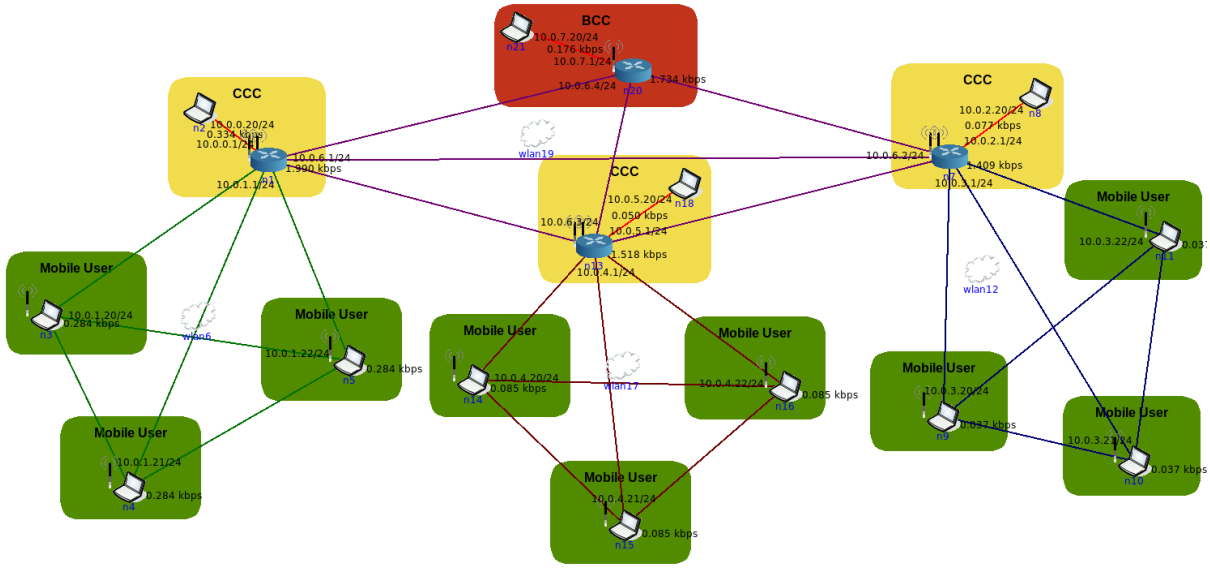

Figure 5.1: Emulated Battalion Network

A Wireless Local Area Network (WLAN) of 2Mbps is established to serve each subunit, to closely emulate the conditions and requirements of wideband military radio networks. This value of 2Mbps was gathered in the field word, since wideband military radios are being acquired and are going to be used by the nodes of the network. This choice enables us to rigorously evaluate the communication systems under conditions that are both realistic and consistent with the demands of military applications.

In this research study, we undertook a comprehensive analysis by considering both TCP and UDP

traffic. When it comes to TCP, the focus was primarily on assessing various critical aspects of data transmission. Aiming to gauge the extent of packet loss, delve into the network delay or latency, and determine the optimal number of nodes that could communicate simultaneously while still maintaining a reasonable level of available bandwidth. This investigation into TCP traffic allowed to gain insights into the reliability and efficiency of data transfer within the network under different conditions.

On the other hand, the exploration of UDP traffic was geared towards understanding how packet loss, network delay, and the number of active hosts communicating concurrently impact the concept of jitter and available bandwidth. Analyzing jitter and available bandwidth in the context of UDP enabled to comprehend the network's ability to handle time-sensitive data and the trade-offs involved when accommodating multiple hosts in such environments.

Together, this investigation provided a holistic view of network performance and the interplay between various parameters when considering both TCP and UDP traffic.

5.1 Network parameters evaluation

To perform the network study the objective was pushing the network to its limits. This is done by increasing different network settings (such as packet loss probability, delay, concurrent traffic), to see just how much stress the network can handle between two neighbor nodes in the tactical network (e.g. between two CCC). It's a stress test for the network, where the goal is to find out what it can take and where it starts to struggle. This helps us figure out how robust and flexible our network is in real-world scenarios, and how much room there is to encrypt the communication.

To evaluate these network performance metrics a widely recognized tool was used, iperf. The iperf utility allowed to conducting rigorous performance measurements by configuring one host as the server and the other as the client. The server host was initiated using the command 'iperf -s,' designating it as the receiver. On the client side, the command 'iperf -c [server's IP] -i 2 -t 300' was executed, serving as the sender. The inclusion of the '-t 300' parameter set the duration of the test to 300 seconds, effectively enabling a 5-minute parameter study of the network connection. Additionally, the '-i 2' flag specified that feedback on the connection's performance would be provided at 2-second intervals, allowing for a detailed analysis of network performance over the duration of the study. This rigorous methodology provided us with valuable insights into the network's behavior and performance characteristics.

Nodal delay

There are four sources of packet delay:

d_{proc} Delay caused by the processing of a node, not only typical routing functionalities such as determining the output link and checking bit errors but in this work the encryption of packets is also

taken in consideration

d_{queue} Corresponds to the time a packet waits at the output link for transmission, depending on the congestion level of the router

d_{trans} Its the size of the packet $L\ (bits)$, over the link bandwidth $R\ (bps)$: $d_{trans} = \frac{L}{R}$

d_{prop} Since tactical links are wireless, this delay is given by the distance between nodes $D\ (m)$, over the speed of light $c\ (m/s)$: $d_{prop} = \frac{D}{c}$

Summing them, the total delay a packet has from one node to another is given by equation 5.1.

$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop} \tag{5.1}$$

To study the maximum nodal delay for TCP traffic, the delay was increased and the available bandwidth was measured, Figure 5.2 depicts the results obtained from the network emulation at 0% and 1% link loss, with delay values in milliseconds (ms) and corresponding bandwidth values in kilobits per second (Kbps).

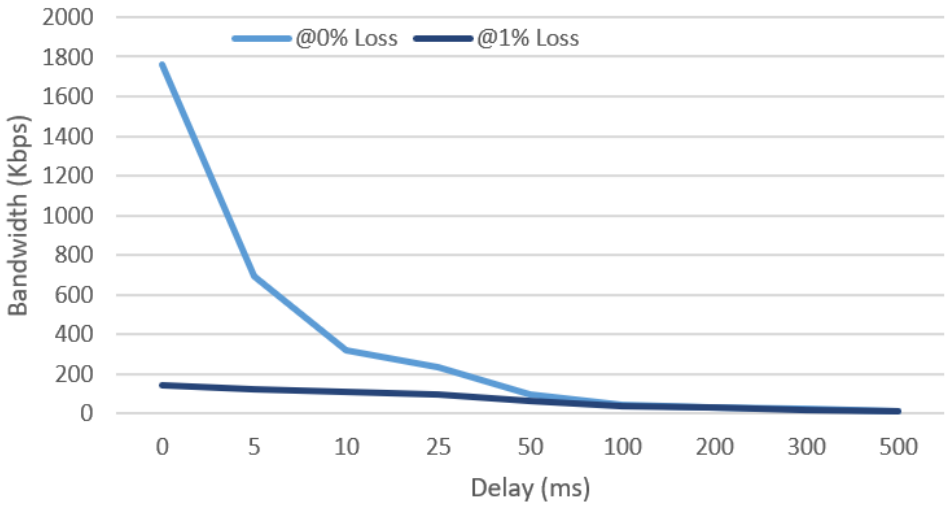

Figure 5.2: Available bandwidth vs Delay

Even minor delays have a pronounced impact on bandwidth, especially when combined with packet loss. For real-time applications, like video conferencing or video streaming, this could be detrimental, leading to lags or disrupted sessions. A minuscule increase in loss rate (from 0% to 1%) has a consistent and noticeable impact on bandwidth across all latency values. This underlines the importance of maintaining a low packet loss rate in this network.

These results reveal important insights into the performance of the network under varying conditions, when there is no link loss:

Inverse Relationship: One notable trend, as expected, is the inverse relationship between delay and bandwidth. As the delay increases, the available bandwidth decreases. This is a common characteristic

of TCP, as it adjusts its transmission rate based on network conditions to avoid congestion.

Latency Impact: The decrease in bandwidth is particularly pronounced as the delay exceeds 100ms. At 100ms delay, the bandwidth is around 46,9 Kbps, which is less than half the bandwidth available with no delay (1,760 Kbps). This demonstrates the significant impact of latency on TCP traffic, where higher delays result in lower throughput.

Network Resilience: The network continues to maintain some level of bandwidth even at 500ms delay, indicating a degree of resilience. However, the bandwidth has decreased significantly to 13,900 Bps. This suggests that the network can still handle data transmission, albeit at a much-reduced rate, even in conditions of relatively high latency.

Real-time Applications: These results highlight the challenges of using TCP for real-time or latency-sensitive applications. As the delay increases, the network's suitability for such applications diminishes due to the decreasing available bandwidth.

In the case of UDP traffic, the increase in delay didn't have impact on the available bandwidth. Which was expectable since it's a connectionless protocol that does not implement flow control, error correction, or congestion control mechanisms like TCP. It simply sends data as fast as possible, without waiting for acknowledgments or retransmitting lost packets. This ”fire and forget” approach makes UDP suitable for real-time and time-sensitive applications, such as audio and video streaming. However, this also means that UDP does not adapt to network congestion, which can result in packet loss and jitter in situations where the network is congested.

Packet loss

Packet loss can be high in military tactical networks due to several unique challenges and operational conditions that these networks often encounter.

In order to investigate the impact of increasing packet loss, the link loss probability was systematically elevated during our study. This involved progressively introducing higher probabilities of packet loss at various stages while simultaneously measuring key network parameters and the results are depicted in Figure 5.4.

It can be concluded that tactical networks are very sensitive to link losses, both TCP and UDP protocols experience reduced bandwidth as link loss increases. However, TCP's performance degrades more rapidly, which is characteristic of its error-checking and retransmission protocols. UDP handles link loss slightly better, but it sacrifices data integrity. This suggests that the network may have some instability or interference that leads to packet loss.

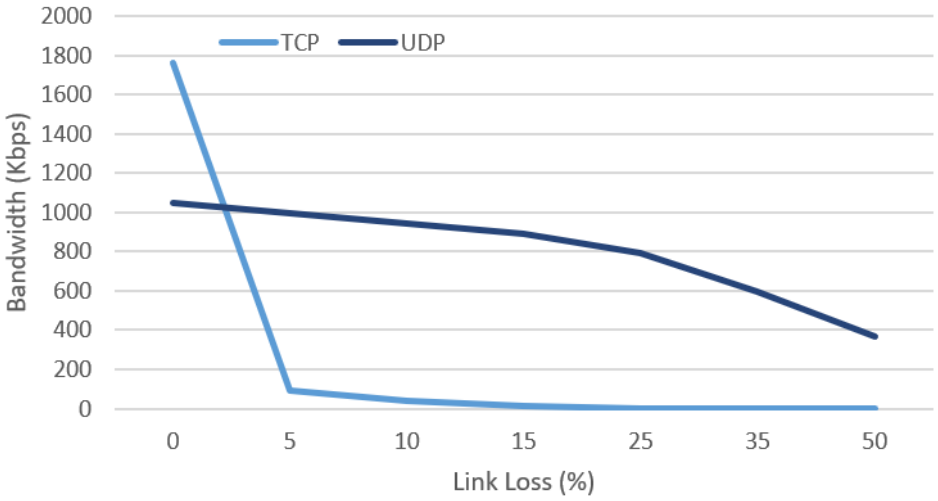

Figure 5.3: Available bandwidth vs Link loss

Network congestion

Our study aimed to investigate the influence of multiple mobile users communicating with a single CCC on the network. To examine this impact, the number of mobile users engaging in communication was systematically increased. Beginning initialy with a single mobile user, transmitting data at a rate of 100 kbps with a Poisson distribution, and subsequently scaling up to ten mobile users. Following this, a second phase was introduced in which mobile users were configured to transmit data at a rate of 512 kbps, and the same methodology was aplied, ranging from one to ten mobile users. The choice of a Poisson distribution for simulating network usage is because it closely mirrors the unpredictability and randomness of network traffic patterns. It effectively models the sporadic and bursty nature of user interactions, making it a valuable tool for assessing network performance and handling varying loads realistically.

The next two plots are referent to TCP traffic, one for each host consuming 100kbps and the other 512kbps, Figure 5.4.

As more users access the network, the available bandwidth per user decreases, leading to potential congestion and slower data transfer rates. On average, the percentage of available bandwidth drops by approximately 6.93% for each additional user added to the network. The greatest drop in bandwidth is noticed when the number of users increases to 4.

This change represents the most substantial decrease in available bandwidth in the given data. The drop from 1,540 kbps to 1,300 kbps reflects a significant reduction in available resources as an additional user is introduced, indicating a point of notable network congestion.

The greatest drop in available bandwidth occurs when transitioning from 3 users to 4 users. Here's the change in bandwidth during this transition:

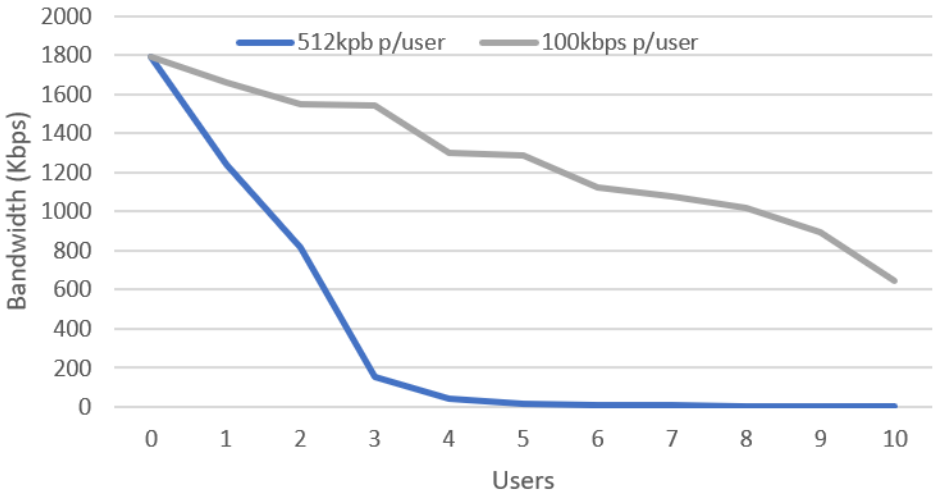

Figure 5.4: Available bandwidth vs Network users

With 3 users, the available bandwidth is 1,540 kbps. When the number of users increases to 4, the available bandwidth drops significantly to 1,300 kbps. This change represents the most substantial decrease in available bandwidth in the given data. The drop from 1,540 kbps to 1,300 kbps reflects a significant reduction in available resources as an additional user is introduced, indicating a point of notable network congestion.

In the first set (100 kbps per user), the available bandwidth decreases as more users are added to the network. This reduction is more gradual due to the relatively lower bandwidth utilization per user.

In the second set (512 kbps per user), the available bandwidth drops significantly with each additional user, especially when transitioning from 2 to 3 users and from 6 to 7 users. This is because each user consumes a larger portion of the total available bandwidth.

It can be concluded that allocating higher bandwidth per user (like 512 kbps/user) might offer a better user experience for individual users, but they'll quickly become inefficient with a growing number of users. Conversely, allocating less bandwidth per user (like 100 kbps/user) can support more users, but each user might experience reduced performance.

5.2 Encryption on the tactical network

It was not possible in this work to delve into the emulation of encrypted network traffic on top of this network but from the study on the network characteristics some conclusions can be taken.

To accurately determine the impact of packet encryption on bandwidth and delay, several factors need to be considered, including the type of encryption, the processing power of the devices in the network, and the size of the data packets.

Encryption increases the size of the data packets due to added headers and trailers. Depending on the encryption method and the packet size, this overhead can vary but lets consider it being around 10-20%. Assuming a 15% overhead for simplicity, the bandwidth would decrease proportionally. For example, for a user with a bandwidth allocation of 512 kbps, the effective bandwidth after encryption might be around 435 kbps (512 kbps * 0.85). Similarly, for 100 kbps, the post-encryption bandwidth would be roughly 85 kbps.

In terms of latency impact, encryption adds processing delay at both the sender (for encryption) and the receiver (for decryption). The exact time depends on the encryption algorithm and the processing power of the involved devices. Assuming an additional delay of 5-15 ms for the encryption-decryption process might be reasonable for many common encryption schemes and average hardware. So, if the network initially had a delay of 25 ms, implementing encryption could potentially increase this to 30-40 ms.

Modern networking hardware often comes with cryptographic accelerators that can speed up the encryption and decryption processes, thereby reducing the latency impact.

Stronger encryption algorithms (e.g., AES-256) provide better security but can be more computationally intensive than weaker ones (e.g., AES-128). This choice will influence both bandwidth overhead and latency, but not so much.

Some encryption protocols, especially those that also provide authentication, can introduce additional delays during session establishment due to key exchange and other processes.

In conclusion, while encryption will impose some bandwidth and latency penalties, these can be mitigated to some extent with the right hardware and configuration. However, given the already sensitive nature of the network to latency and bandwidth constraints, thorough testing should be conducted to ensure that the added encryption does not impact user experience.

6

Conclusions and Future Work

The primary objective of this study was to explore the feasibility of extending classified domains to lower military units, and our findings affirm that this extension is indeed possible.

The thesis comprises three core phases. Initially, we conducted a comprehensive literature review, delving into academic sources to gain insights into secure communications and military networks. This was followed by fieldwork to gather essential requirements for the extension of classified domains to lower units. The final stage involved a tactical network emulation, which allowed us to assess the potential for implementing encryption and secure channels within these bandwidth-constrained networks.

Based on the results obtained from our emulation, it is evident that integrating encryption is a viable option. However, it is imperative to acknowledge that these networks inherently possess limited performance capabilities. As we traverse down the network hierarchy, the need for lightweight encryption becomes increasingly pronounced.

Future endeavors can involve the implementation of encryption protocols and automatic key sharing within an emulated tactical network. Such research can help identify the most suitable encryption protocols and their respective constraints in these network settings.

With the emulation presented in this work, it can be concluded that the latency, and overhead extension added by the encryption devices has to be very lightweight, since these networks are already very low bandwidth due to high link losses, delay and reduced bandwidth.

In summary, this thesis serves as a foundational stepping stone for more in-depth research on enhancing the security and performance capabilities of tactical military networks.

Bibliography

[1] “Establishing a ssl/tls session - transport layer security — okta developer.” [Online]. Available: https://developer.okta.com/books/api-security/tls/how/

[2] “Ipsec overview part four: Internet key exchange (ike),” *Cisco Press*, 2002.

[3] M. Hauge, T. M. Mjelde, A. Holtzer, F. Drijver, R. in’t Velt, A. M. Hegland, E. Ørbekk, C. Barz, J. Kirchhoff, and H. Rogge, “Inter-network interoperability for heterogeneous networks at the tactical edge,” in *2020 Military Communications and Information Systems Conference (MilCIS)*, Nov 2020, p. 1–7.

[4] “Draft mc 0640 – minimum level of communication and information systems capabilities at land tactical level,” 2018.

[5] A. M. Hegland, M. Hauge, and A. Holtzer, “Federating tactical edge networks: Ways to improve connectivity, security, and network efficiency in tactical heterogeneous networks,” *IEEE Communications Magazine*, vol. 58, no. 2, pp. 72–78, 2020.

[6] *Tactical Deployable Communications and Information Systems (TDCIS) for the Portuguese Army*, NCI Agency, NATO, 2022. [Online]. Available: https://www.ncia.nato.int/downloads/115363.pdf

[7] R. Schutz, S. McLaughlin, T. Daeleman, M. Luoma, M. Peuhkuri, P. Carlen, and J. Haines, “Protected core networking (pcn): Pcn qos and sla definition,” in *2013 Military Communications and Information Systems Conference*, 2013, pp. 1–9.

[8] J. F. Kurose and K. W. Ross, *Computer networking: a top-down approach*, 6th ed. Boston: Pearson, 2013.

[9] “Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model,” International Organization for Standardization, Geneva, CH, Standard, Jun. 1996.

[10] “What is the OSI Model? — forcepoint.com,” https://www.forcepoint.com/cyber-edu/osi-model, [Accessed 18-10-2023].

[11] C. C. Gary C. Kessler, Ph.D., “An Overview of Cryptography,” https://www.garykessler.net/library/crypto.html, [Accessed 18-10-2023].

[12] W. Stallings, *Network security essentials: applications and standards*, 4th ed. Boston: Prentice Hall, 2011.

[13] D. C. Neuman, S. Hartman, K. Raeburn, and T. Yu, “The Kerberos Network Authentication Service (V5),” RFC 4120, Jul. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4120

[14] P. Gutmann, “Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS),” RFC 6476, Jan. 2012. [Online]. Available: https://www.rfc-editor.org/info/rfc6476

[15] D. Knuth, *The Art Of Computer Programming, vol. 3: Sorting And Searching*. Addison-Wesley, 1973.

[16] B. Schneier, *Applied Cryptography*, 2nd ed. Wiley, 1996.

[17] G. Ma, H. Liang, L. Yao, Z. Huang, M. Yi, X. Xu, and K. Zhou, “A low-cost high-efficiency true random number generator on fpgas,” in *2018 IEEE 27th Asian Test Symposium (ATS)*, 2018, pp. 54–58.

[18] V. Mulder, A. Mermoud, V. Lenders, and B. Tellenbach, Eds., *Trends in Data Protection and Encryption Technologies*. Springer Nature Switzerland, 2023. [Online]. Available: https://doi.org/10.1007/978-3-031-33386-6

[19] Archiveddocs, “Ssl/tls in detail.” [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811(v=ws.10)

[20] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, Aug 2018, no. RFC 8446. [Online]. Available: https://datatracker.ietf.org/doc/rfc8446

[21] S. Kent, “IP Encapsulating Security Payload (ESP),” RFC 4303, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4303

[22] ——, “IP Authentication Header,” RFC 4302, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4302

[23] P. Willis and I. o. E. Engineers, *Carrier-Scale IP Networks: Designing and Operating Internet Networks*, ser. BT communications technology series. Institution of Engineering and Technology, 2001. [Online]. Available: https://books.google.pt/books?id=5BbTeaFGOIIC

[24] C. Kaufman, “Internet Key Exchange (IKEv2) Protocol,” RFC 4306, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4306

[25] T. Shake and T. Gibbons, “Architectural consequences of domain formation in tactical edge networks,” in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 647–654.

[26] *Quadro Orgânico do Quartel-General da Brigada de Intervenção.*, Ministério da Defesa Nacional, 2015.

[27] *MIL-HDBK-232A - RED/BLACK ENGINEERING-INSTALLATION GUIDELINES*, 2000.

[28] C. C. Serena, I. R. P. III, J. B. Predd, J. Osburg, and B. Lossing, *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network*. Santa Monica, CA: RAND Corporation, 2014.

[29] A. Holtzer, R. In’t Velt, F. Drijver, H. Rogge, J. Kirchhoff, C. Barz, N. Van Adrichem, and M. Hauge, “Tactical router interoperability: Concepts and experiments,” in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 2018, pp. 647–654.

[30] R. Schutz, S. McLaughlin, T. Daeleman, M. Luoma, M. Peuhkuri, P. Carlen, and J. Haines, “Protected core networking (pcn): Pcn qos and sla definition,” in *2013 Military Communications and Information Systems Conference*, Oct 2013, p. 1–9.

[31] M. Hauge, A. Hansson, C. Barz, A. Holtzer, A. M. Hegland, and R. I. Velt, “Final report of nato ist-124, annex e – architecture considerations for heterogeneous tactical networks,” 2019.

[32] “How do you manage encryption keys and certificates in your organization?” https://www.linkedin.com/advice/1/how-do-you-manage-encryption-keys-certificates-1c, [Accessed 20-10-2023].

[33] S. Tyley, *Over-the-Air Distribution (OTAD)*, 2015.

[34] M. Cooper, “An introduction to information exchange gateways,” Jan 2015. [Online]. Available: https://colinrobbins.me/2015/01/19/introduction-information-exchange-gateways/

[35] N. Mainse, “An introduction to information exchange gateways,” Aug 2020. [Online]. Available: https://colinrobbins.me/2015/01/19/introduction-information-exchange-gateways/

[36] “Discretion project will reinforce the autonomy of the european defense in secure communications.” [Online]. Available: https://www.it.pt/News/NewsPost/4748