Extending Secure Military Tactical Networks

Daniel Almeida

Academia Militar
Instituto Superior Técnico
almeida.dsr@exercito.pt

***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.

***Index Terms*—Military Communications; Secure networks; Cipher machines.**

I. Introduction

In an ever-evolving technological landscape, secure and efficient military communication is vital. Tactical networks are lifelines in modern warfare, facing challenges like rugged terrain and security threats. This study aims to enhance security for sensitive military data near enemy lines. It combines real-world observation and emulation, exploring encryption, performance, and key distribution. The focus is on securing military operations while maintaining network efficiency. The thesis proposes future research on encryption technologies and physical security devices. It seeks to create more secure and high-performance military tactical networks that balance robust security and operational agility.

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.

II. Background

A. 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.

To provide ”a common basis for the coordination of standards development for the purpose of systems interconnection.” the ISO created the OSI Model [1]. 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 anothe, starting from the bottom layer (Layer 1) to the top layer (Layer 7) [2]:

B. 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 data into a secure, unreadable form that can only be decoded with the correct key, ensuring confidentiality [3]. It is widely used to protect data during transmission over networks and while stored on devices, playing a vital role in computer security across applications like email, instant messaging and file.

Decryption is the process of reversing encryption, turning encrypted data (ciphertext) into its original, readable form (plaintext). It requires the use of the same secret key used for encryption. Decryption is commonly used to access securely encrypted data, whether for data in transit or at rest. Different

decryption algorithms are designed to work with specific encryption methods, and the correct decryption algorithm and key must be used to decrypt data effectively [4].

1) Symmetric key cryptography: Symmetric 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 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 [5].

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.

2) 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 [5]:

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. When a connection between two systems is approved, the key distribution center generates a temporary session key for that connection [5].

3) 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 Token (TGT). The client then uses the TGT to request a service ticket from the authentication server, which is used to authenticate to the service [6].

4) 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 [5].

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 (MAC): A 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 [7].

Because "cryptographic hash functions generally execute faster in software than conventional encryption algorithms" [5], HMAC are widely used insted of block-cipher MACs like DES

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

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 [8].

5) Hardware Security Modules (HSM): HSMs 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 [9].

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 [10].

6) Secure Channels: There are several ways of establishing secure channels in a network, these include:

7) Transport Layer Security: TLS is a Transport Layer protocol that provides secure communication between two applications over the internet. TLS is the successor to 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 [4].

8) 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) [11].

It consists of two main protocols, the *AH* and the *ESP*. The first provides user authentication and integrity protection for the transmitted data, while the second provides confidentiality, as well as authentication and integrity [12].

Both of these two protocols have a tunnel and a transport mode. In tunnel mode, the entire original 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.

C. 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.

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 (Figure 1)

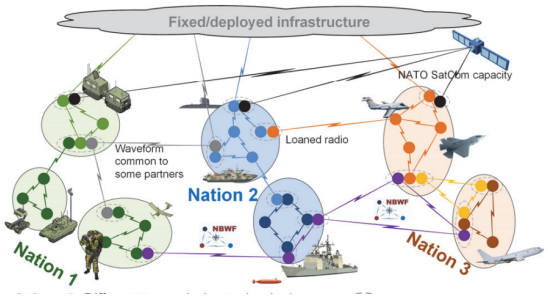

Fig. 1. Meshed Network Topology [13]

Portuguese Army Units: To better understand how TDCIS works, it is necessary to understand how the units are hierarchically structured in the Portuguese Army. From the bigger to the smaller unit there are brigades, battalions, companies, platoons, sections and squads. Several battalions belong to a brigade, several companies belong to a battalion, and so forth [14].

1) Services in Tactical Networks: 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.

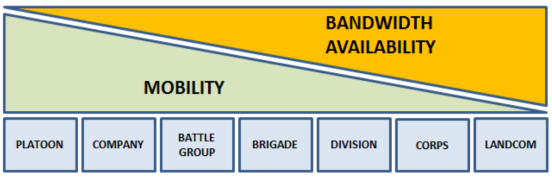

Fig. 2. Mobility vs Bandwidth [15]

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

TABLE I
COMMUNICATION SERVICES AT DIFFERENT LEVELS [15]

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		

2) 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 ”red” typically representing unclassified or less sensitive information, and ”black” representing classified or highly sensitive information.

The red network is the less secure network where unclassified or non-sensitive data is processed and transmitted.

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

A set of hardware, software, and policies to transfer information between networks of different security classifications must exist [16].

3) 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 [17].

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.

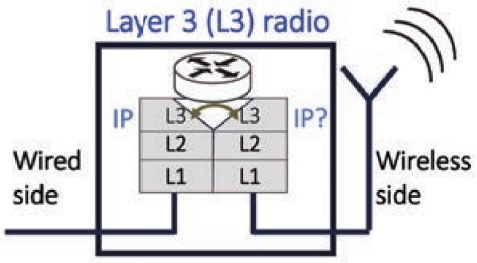

Fig. 3. Layer 3 Radio Model [17]

Figure 4 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 [17].

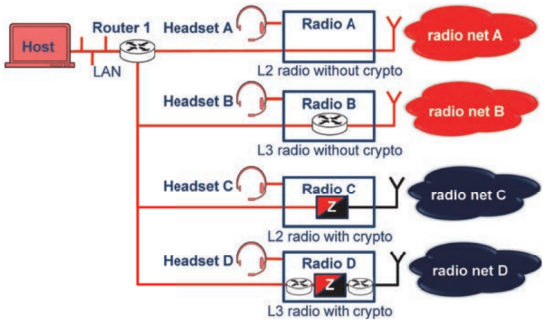

Fig. 4. Tactical network node [17]

III. State of the Art

A. Tactical Deployable Communications and Information Systems

The Portuguese Army (PRT-A) is a well-structured force focused on protecting Portugal. A key element of PRT-A operations is the Tactical Deployable Communications and Information Systems (TDCIS).

The objective is to provide PRT-A with secure, modular, and interoperable communication within the Portuguese NDN or with NATO FMN partners.

TDCIS consists of these node types:

- AN for Brigade support;
- BCC for Battalion support;
- CCC for Company support.

TDCIS also includes nodes for the tactical and reach-back Wide Area Network:

- TN for node communication;
- RAP for mobile user communication;
- RL for reach-back to the NDN.

B. 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 [18]. 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.

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 [19].

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.

1) Protected Core Networking (PCN): PCN aims to create a secure and versatile military IP transport infrastructure. It connects diverse national network segments to form a worldwide core network. PCN emphasizes security and quality of service, currently undergoing NATO standardization as STANAG 5637.

PCN uses various network service classes to address performance and security requirements. It features advanced knowledge, management, and control capabilities. The network structure is depicted in Figure 5.

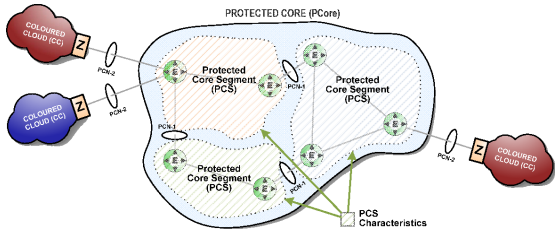

Fig. 5. Protected Core Networking [20]

PCN includes Colored Clouds (CC) connecting to a central entity called the Protected Core. The Protected Core consists of multiple segments, forming a collaborative federation. Segments conform to PCN principles and interconnect via E-nodes over the PCN-1 interface [21].

The Protected Core serves as a transport network, with end-users connecting via CCs. Cryptographic isolation ensures communication only between CCs of the same color, denoting specific security domains. Nodes connecting via PCN-1 or

PCN-2 interfaces undergo authentication for network security and integrity.

2) 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 [22].Each of these architectures depend on different information exchange interface.

On a *flat architecture* (Figure 6), 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 an EI-M between the routing function and the Modem is [17].

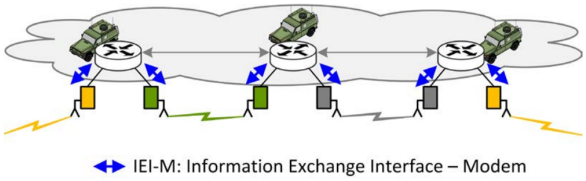

Fig. 6. Flat Architecture [17]

The *interconnected-flat architecture* (figure 7) 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 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 [19].

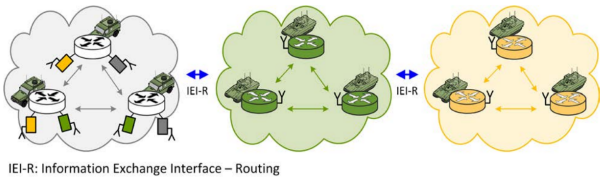

Fig. 7. Interconnected-Flat Architecture [17]

Interconnect-overlay architecture (Figure 8) 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 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 [17].

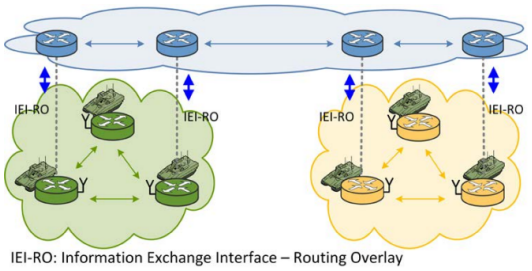

Fig. 8. Overlay Architecture [17]

3) 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 end-host, within the network infrastructure, or within a radio accessed via a routed network. 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 a large number of end-hosts [17].

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 [17].

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 [17].

Key Management: 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 the same as losing the protected data itself.

To ensure the security of encryption keys, organizations employ KMS or HSM to generate, store, and oversee these keys [23].

Additionally, key distribution protocols can be used to securely transmit keys and certificates. OTAR is a example to this in this strategy [24].

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 [23].

IEG and Cipher Machines: IEG systems are specialized for secure communication across diverse security domains. In a military context, they enable seamless human-to-human communication for mission planning and execution. They facilitate information sharing between domains lacking interoperability, ensuring information assurance and confidentiality. Information protection services are essential to maintain security and integrity during exchanges [25].

In this work, IEG are a vital component, connecting different classified networks together with budget-friendly encryption devices from the DISCRETION project [26] can increase the quantity of encryption devices available to use in tactical networks.

IV. Proposed topologies and analysis

This chapter's content was collected in a visit to the PRT-A yearly exercise ORION23. By collecting operational requirements in the field, it was able to understand how low in the hierarchy sensitive information is dealt by military personnel. The scenarios differ in complexity and security level:

A. 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 9

This scenario is suitable for securing sensitive information near enemy lines. Each section forms a cryptographic bubble

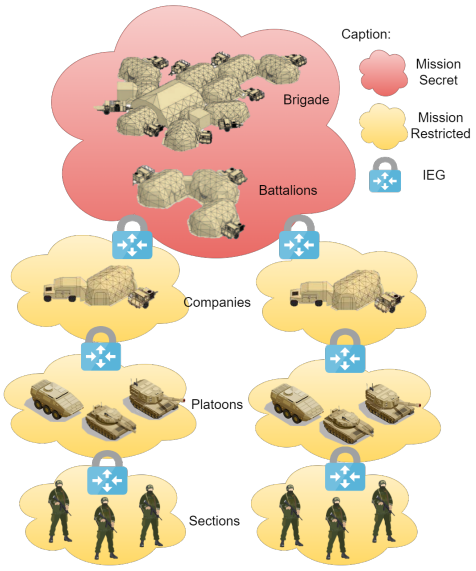

Fig. 9. Complete Segregation Topology

using an IEG to protect the network if a section node is compromised.

Communication within a unit is encrypted for secure transmission. Cross-hierarchy communication passes through an IEG, allowing the higher-level unit to manage traffic from compromised nodes.

Key management is critical. Manual key distribution is an option, but automatic distribution via a secure channel is more efficient.

This topology offers the highest security but is complex and costly to implement. It provides hierarchical control for damage prevention but requires intricate key management due to many nodes.

Equipping a brigade with a 15% backup requires 325 devices, estimated at a thousand euros each.

Consider installation, integration, maintenance, and support costs beyond the device cost.

B. 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 10).

This scenario is suitable for platoons handling sensitive information. Sections' information is considered less critical.

Within the same unit, data is encrypted. Cross-hierarchy communication passes through an IEG, enabling the higher-level unit to manage traffic from compromised nodes.

Key creation can be manual, significantly reducing the number of keys to distribute. This simplifies key management.

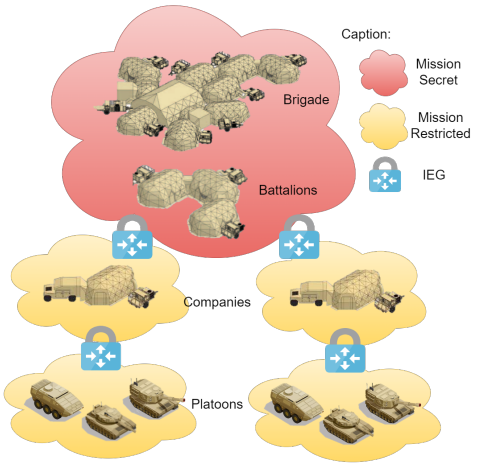

Fig. 10. Simplified Complete Segregation Topology

This simplified setup offers robust security with hierarchical control. In case of compromise, the higher-level unit can swiftly disconnect the compromised unit.

Only 45 devices, with a 15% backup, are needed in this scenario.

C. 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 11.

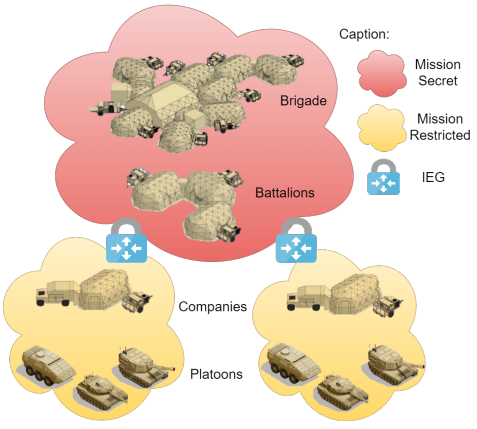

Fig. 11. Company Segregation Topology

This solution is the simplest and most likely use case, as platoons and companies are highly mobile, and their traffic doesn't require an IEG.

Unlike other scenarios, it only needs an IEG between battalions and their companies. The limited available bandwidth for lower units adds minimal constraint due to encryption devices.

This solution simplifies key management and is cost-effective for product acquisition, similar to the second topology.

These topologies are ideal for units involved in Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) missions, Artillery Gun Systems, and Special Forces. They ensure secure communication for highly classified data, data integrity for precision targeting, and confidentiality for operations deep within enemy territory. These scenarios aim to extend secure communications to sensitive information handling troops.

V. Topology Emulation and Evaluation

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.

To conduct our study, we commence 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. Figure 12.

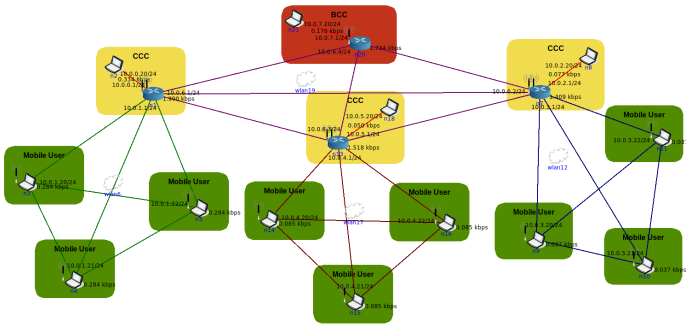

Fig. 12. Emulated Battalion Network

A 2Mbps WLAN simulates real military radio network conditions. This value was gathered in the field work at ORION23 exercise, using wideband radios.

The study analyzes both TCP and UDP traffic. TCP assesses packet loss, network delay, and optimal node count for reliable data transfer. UDP investigates jitter, available bandwidth, and handling time-sensitive data with multiple hosts, offering a comprehensive view of network performance.

A. Network parameters evaluation

The network study aimed to stress test the network by adjusting settings like packet loss, delay, and concurrent traffic between neighbor nodes (e.g., two CCC). This test helps evaluate the network's robustness and flexibility in real-world scenarios and its capacity for encryption.

The widely recognized tool, iperf, was used for performance measurements. One host served as the server ('iperf -s'), and the other as the client ('iperf -c [server's IP] -i 2 -t 300')

for a 5-minute parameter study. The '-i 2' flag provided performance feedback at 2-second intervals, enabling detailed analysis.

Nodal delay: Four sources contribute to packet delay: processing delay (routing and encryption), queue delay (output link congestion), transmission delay ($d_{trans} = \frac{L}{R}$), and propagation delay ($d_{prop} = \frac{D}{c}$). The total delay (d_{nodal}) is given by Equation 1.

$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop} \quad (1)$$

Figure 13 illustrates TCP traffic's maximum nodal delay and corresponding available bandwidth.

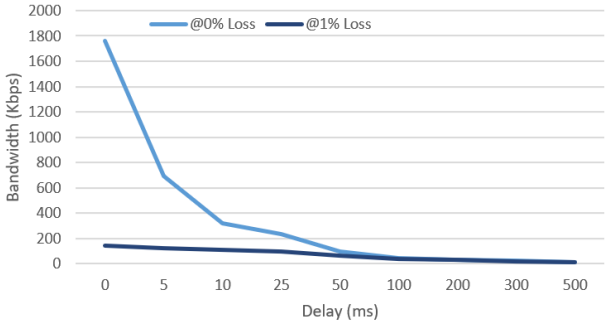

Fig. 13. Available bandwidth vs Delay

Minor delays, especially with packet loss, significantly impact bandwidth, especially in real-time applications. A small increase in loss rate (from 0% to 1%) consistently affects bandwidth at various latency levels, emphasizing the importance of low packet loss.

- Inverse Relationship: As expected, there's an inverse relationship between delay and bandwidth due to TCP's congestion control. - Latency Impact: Bandwidth decreases significantly with delays exceeding 100ms. - Network Resilience: Even at 500ms delay, some bandwidth is retained, indicating network resilience, albeit at a lower rate. - Real-time Applications: TCP's suitability for real-time apps diminishes with higher delays due to reduced bandwidth.

In the case of UDP traffic, increased delay didn't affect available bandwidth. UDP is suitable for real-time applications due to its "fire and forget" approach, but it doesn't adapt to network congestion, potentially leading to packet loss and jitter during network congestion.

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 15.

It can be concluded that tactical networks are very sensitive to link losses, both TCP and UDP protocols experience

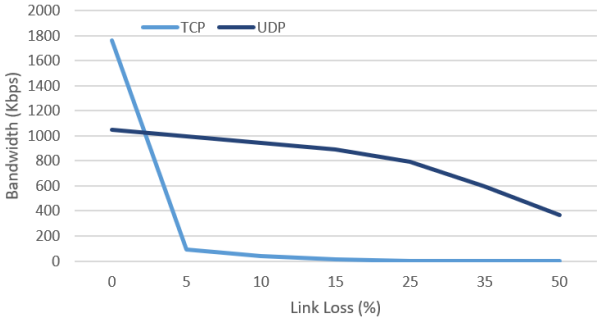

Fig. 14. Available bandwidth vs Link loss

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.

Network congestion: Our study examined the impact of multiple mobile users communicating with a single CCC. We systematically increased the number of users, starting with one user at 100 kbps with a Poisson distribution and scaling up to ten users. A second phase involved users transmitting data at 512 kbps, using the same methodology.

Poisson distribution was chosen for its realistic representation of unpredictable network traffic patterns.

The figures in Figure 15 show the impact of users on available bandwidth. As more users join, available bandwidth per user decreases, leading to congestion. The greatest bandwidth drop occurs when transitioning from 3 to 4 users, indicating significant congestion.

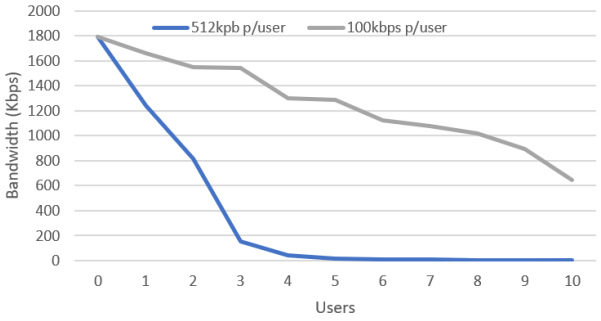

Fig. 15. Available bandwidth vs Network users

For 100 kbps per user, bandwidth reduction is gradual. For 512 kbps per user, bandwidth drops significantly, especially when transitioning from 2 to 3 users and from 6 to 7 users.

In summary, allocating higher bandwidth per user improves individual experience but becomes inefficient with more users. Allocating less bandwidth per user supports more users but may reduce performance.

B. Encryption on the tactical network

This study didn't emulate encrypted network traffic, but some conclusions can be drawn from network characteristics.

Assuming that encryption increases data packet size by around 10-20%, leading to proportional bandwidth reduction. For example, a user with 512 kbps might experience around 435 kbps post-encryption (512 kbps * 0.85). Similarly, a 100 kbps user would have roughly 85 kbps after encryption.

Assuming that ncryption adds processing delay at both the sender and receiver, typically 5-15 ms, potentially increasing network latency from 25 ms to 30-40 ms.

Modern hardware with cryptographic accelerators can mitigate latency impact. Stronger encryption adds overhead but offers better security.

Certain encryption protocols may introduce delays during session establishment due to key exchange.

In conclusion, encryption may affect bandwidth and latency, but proper hardware and configuration can mitigate these effects. Thorough testing is essential to ensure user experience remains unaffected, given the network's sensitivity to latency and bandwidth constraints.

VI. Conclusion

This study aimed to explore extending classified domains to lower military units, affirming its feasibility.

The study comprised three phases: literature review, fieldwork, and tactical network emulation. Results show that integrating lightweight encryption is viable, given bandwidth constraints.

Future research can focus on encryption protocols and key sharing within an emulated tactical network to identify suitable options.

The study concludes that encryption must be very lightweight due to low bandwidth, latency, and overhead. This work serves as a foundational step for enhancing tactical military network security and performance.

References

[1] Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. Standard, International Organization for Standardization, Geneva, CH, June 1996.

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

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

[4] James F. Kurose and Keith W. Ross. *Computer networking: a top-down approach*. Pearson, Boston, 6th ed edition, 2013.

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

[6] Dr. Clifford Neuman, Sam Hartman, Kenneth Raeburn, and Taylor Yu. The Kerberos Network Authentication Service (V5). RFC 4120, July 2005.

[7] Peter Gutmann. Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS). RFC 6476, January 2012.

[8] Bruce Schneier. *Applied Cryptography*. Wiley, 2nd edition, 1996.

[9] Gaoliang Ma, Huaguo Liang, Liang Yao, Zhengfeng Huang, Maoxiang Yi, Xiumin Xu, and Kai Zhou. A low-cost high-efficiency true random number generator on fpgas. In *2018 IEEE 27th Asian Test Symposium (ATS)*, pages 54–58, 2018.

[10] Valentin Mulder, Alain Mermoud, Vincent Lenders, and Bernhard Tellenbach, editors. *Trends in Data Protection and Encryption Technologies*. Springer Nature Switzerland, 2023.

[11] Stephen Kent. IP Encapsulating Security Payload (ESP). RFC 4303, December 2005.

[12] S Kent. IP Authentication Header. RFC 4302, December 2005.

[13] Mariann Hauge, Terje Mikal Mjelde, Arjen Holtzer, Floris Drijver, Ronald in't Velt, Anne Marie Hegland, Erik Ørbekk, Christoph Barz, Jonathan Kirchhoff, and Henning Rogge. Inter-network interoperability for heterogeneous networks at the tactical edge. In *2020 Military Communications and Information Systems Conference (MilCIS)*, page 1–7, Nov 2020.

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

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

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

[17] Anne Marie Hegland, Mariann Hauge, and Arjen Holtzer. Federating tactical edge networks: Ways to improve connectivity, security, and network efficiency in tactical heterogeneous networks. *IEEE Communications Magazine*, 58(2):72–78, 2020.

[18] Chad C. Serena, Isaac R. Porche III, Joel B. Predd, Jan Osburg, and Brad Lossing. *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network*. RAND Corporation, Santa Monica, CA, 2014.

[19] Arjen Holtzer, Ronald In't Velt, Floris Drijver, Henning Rogge, Jonathan Kirchhoff, Christoph Barz, Niels Van Adrichem, and Mariann Hauge. Tactical router interoperability: Concepts and experiments. In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pages 647–654, 2018.

[20] Roland Schutz, Sam McLaughlin, Tim Daeleman, Marko Luoma, Markus Peuhkuri, Per Carlen, and John Haines. Protected core networking (pcn): Pcn qos and sla definition. In *2013 Military Communications and Information Systems Conference*, pages 1–9, 2013.

[21] Roland Schutz, Sam McLaughlin, Tim Daeleman, Marko Luoma, Markus Peuhkuri, Per Carlen, and John Haines. Protected core networking (pcn): Pcn qos and sla definition. In *2013 Military Communications and Information Systems Conference*, page 1–9, Oct 2013.

[22] Mariann Hauge, Anders Hansson, Christoph Barz, Arjen Holtzer, Anne Marie Hegland, and Ronald In't Velt. Final report of nato ist-124, annex e – architecture considerations for heterogeneous tactical networks, 2019.

[23] 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].

[24] Scott Tyley. *Over-the-Air Distribution (OTAD)*. 2015.

[25] Martin Cooper. An introduction to information exchange gateways, Jan 2015.

[26] Discretion project will reinforce the autonomy of the european defense in secure communications.