11TH INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2024
Serbia, Tara, 9-11 October 2024

GRE TUNNEL UTILIZATION FOR MINIMIZING MULTI-VENDOR NETWORK EQUIPMENT ISSUES FOR VARIOUS TRANSMISSION CHANNELS

MARKO MARKOVIĆ
School of Electrical Engineering & Vlatacom Institute, Belgrade, marko.markovic@vlatacom.com

LARA KAŠCA
School of Electrical Engineering & Vlatacom Institute, Belgrade, lara.kasca@vlatacom.com

ĐORĐE NEŠKOVIĆ
School of Electrical Engineering & Vlatacom Institute, Belgrade, djordje.neskovic@vlatacom.com

STEFAN STANKOVIĆ
School of Electrical Engineering & Vlatacom Institute, Belgrade, stefan.stankovic@vlatacom.com

MIROSLAV PERIĆ
Vlatacom Institute, Belgrade, miroslav.peric@vlatacom.com

MLADEN KOPRIVICA
School of Electrical Engineering, Belgrade, kopra@etf.rs

GORAN MARKOVIĆ
School of Electrical Engineering, Belgrade, gmarkovic@etf.rs

Abstract: *In the realm of battlefield operations, where seamless communication is paramount, the utilization of all available networking equipment is indispensable. However, the diverse array of vendor equipment often poses compatibility challenges across different transmission channels. These issues are frequently rooted in the varying limitations of packet length among the equipment, leading to undesirable packet fragmentation and potential loss. To mitigate these challenges, we have explored the efficacy of GRE (Generic Routing Encapsulation) tunnel utilization. By employing GRE methodology, we can tailor packet length to optimize performance across specific transmission media and service types. Our focus lies particularly on high-interactivity applications crucial for battlefield environments, such as file transfer and video streaming, for both encrypted and unencrypted scenarios. We present the results of comprehensive experiments that have enabled us to identify optimal configurations for various scenarios, ensuring efficient communication.*

Keywords: *Multi-Vendor Network Equipment, GRE Tunneling, Battlefield Communication, Optimization.*

1. INTRODUCTION

In the dynamic and high-stakes environment of battlefield operations, the importance of seamless and reliable communication cannot be overstated. Effective communication systems are the backbone of strategic coordination and operational success. However, the integration of networking equipment from various vendors often presents significant compatibility challenges, particularly across different transmission channels. One of the primary issues encountered is the disparity in packet length limitations among diverse equipment, which can lead to undesirable packet fragmentation and potential data loss. These fragmentation issues can critically impair the efficiency and reliability of communication, putting mission outcomes at risk.

To address these challenges, our research has focused on the utilization of Generic Routing Encapsulation (GRE) tunnels. The principle of tunnels is to create a virtual network (overlay network) on top of a physical infrastructure (underlay network). This provides a logical interface that emulates a direct physical link connecting two sites, [1]. GRE tunnels allow for the encapsulation of a wide variety of network layer protocols, facilitating more flexible and efficient data transmission. By leveraging GRE methodology, we can customize packet lengths to align with the optimal performance parameters of specific transmission media and service types. Our investigation emphasizes high-interactivity applications that are essential in battlefield settings, such as file transfer and video streaming. These applications are

Corresponding author: M.Marković;
E-mail: marko.markovic@vlatacom.com
DOI: 10.5937/OTEH24072M

analyzed in both encrypted and unencrypted scenarios to ensure comprehensive understanding and applicability. In particular, the analysis focuses on the implementation of GRE over IPSec (Internet Protocol Security) to facilitate secure communication between multi-vendor environments. GRE over IPSec combines the flexibility of GRE tunneling with the robust security features of IPSec, providing a secure and versatile solution for network traffic encryption.

Our experimental approach involved using the File Transfer Protocol (FTP) to transfer a file while systematically varying the Maximum Transmission Unit (MTU) size to identify the fastest transfer rates. These tests were conducted under conditions with and without IPSec encryption to evaluate the impact of security protocols on performance. In parallel, we conducted video streaming experiments using VLC (VideoLAN Client), assessing video quality based on subjective user experiences to determine the optimal MTU settings for both encrypted and unencrypted scenarios.

The comprehensive data collected from these experiments has enabled us to pinpoint the most effective MTU settings for these applications, thereby enhancing the overall efficiency and reliability of communication systems in battlefield operations. These findings are crucial for ensuring that high-priority communications, such as confidential documents, orders in text form, and real-time video feeds, are transmitted with minimal delay and maximum fidelity. This is essential for supporting the success of military missions.

The remainder of this article is organized as follows: Section 2 provides an overview of the experimental setup and network and device configuration. This section details the hardware and software components used, the network topology, and the specific configurations applied to the devices involved in the experiments. Section 3 presents the results of our study, including performance metrics for file transfers over TCP and video streaming over UDP. The analysis covers both unencrypted and encrypted traffic, highlighting the differences in performance and any observed impacts on data integrity and transmission efficiency. Finally, Section 4 concludes the paper, summarizing the key findings and discussing their implications for future research and practical applications in network security and performance optimization.

2. EXPERIMENTAL SETUP AND NETWORK CONFIGURATION

In this section, we will provide a detailed overview of our work environment, covering network and device configurations. Operating in a multi-vendor setup, we use GRE tunnel to securely extend connectivity between different parts of our network. This configuration ensures dependable performance and secure communication across our infrastructure.

2.1. Experimental setup

Since we are discussing a multi-vendor environment and GRE tunnels, the main idea is to have two private Local Area Networks (LANs) communicating over a (secured) GRE tunnel, isolated from the rest of the network. Therefore, we require two endpoint routers (which are multi-vendor) whose interfaces connect their respective local private networks on one end, while their interfaces on the other end serve as the endpoints between which the GRE tunnel is established. On one side, we have a physical router in the form of a Linux device running Ubuntu, the Xilinx® Kria™ KR260 Robotics Starter Kit, further in the text, Kria. On the other side, there is a Cisco 3745 Router implemented in the GNS3 (Graphical Network Simulator-3) emulator environment, further in the text, RCisco.

GNS3 allows for the integration of virtual and physical devices to simulate complex networks. It utilizes Dynamips emulation software, originally designed to emulate Cisco routers, [2], to simulate Cisco IOS, [3]. This setup facilitates multi-vendor communication over GRE tunnel across a specific "complex" network topology between them. Figure 1. illustrates the experimental setup used for this purpose.

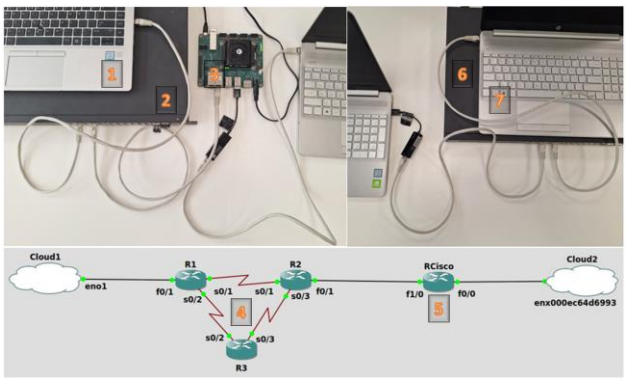

Figure 1. Experimental setup

On the figure above, the following are sequentially depicted:

- PC1 (1),
- DCN L3 Switch DCRS-5960; Switch1 (2),
- Kria (3),
- “Complex” Network (4),
- RCisco (5),
- DCN L3 Switch DCRS-5960; Switch2 (6),
- PC2 (7).

PC1 and Switch1 belong to the private network on the Kria side. The switch is included to demonstrate the expandability of the private network, though simplified for our case. Similarly, this applies to the private network on the RCisco side. Since these two PCs represent the communication endpoints, the GNS3 emulator runs on a third PC. The upper branch in the "complex" network between the GRE tunnel endpoints represents the current and main traffic path, while the lower branch serves as a backup path in case of main path failure, as a likely

scenario in military operations.

2.2. Network and device configuration

The following Table 1. displays the assigned IPv4 addresses for each of the devices/interfaces of interest. This is essential for network configuration, ensuring clarity in IP address allocation across key components.

Table 1. Assigned IPv4 addresses

Device/interface	IPv4 address with the prefix length
PC1	192.168.1.10/24
eth0 on Kria	192.168.1.1/24
USB on Kria	172.16.1.1/30
gre1 on Kria	10.0.0.1/30
f0/1 on R1	172.16.1.2/30
s0/1 on R1	172.16.3.1/30
s0/2 on R1	172.16.4.1/30
f0/1 on R2	172.16.2.2/30
s0/1 on R2	172.16.3.2/30
s0/3 on R2	172.16.5.1/30
s0/2 on R3	172.16.4.2/30
s0/3 on R3	172.16.5.2/30
f0/0 on RCisco	192.168.2.1/24
f1/0 on RCisco	172.16.2.1/30
tunnel0 on RCisco	10.0.0.2/30
PC2	192.168.2.20/24

To establish a GRE tunnel between the two multi-vendor routers, it is necessary to create a physical connection between them, i.e., between the USB interface on the Kria and the f1/0 interface on the RCisco. Initially, the OSPFv2 protocol is configured on R1, R2, and R3 (single area). OSPFv2 is a link-state routing protocol that employs a version of Dijkstra's shortest path first algorithm and is an open standard, [4]. In this way, traffic rerouting to the backup path is also enabled, in case of a main path failure. Currently, the Kria has only one static route defined to the network 172.16.2.0/30, via the USB interface as the outgoing interface, i.e., the next-hop IP address being the f0/1 interface of router R1. Similarly, the RCisco has only one static route defined to the network 172.16.1.0/30, via the f1/0 interface as the outgoing interface, i.e., the next-hop IP address being the f0/1 interface of router R2. After setting these static routes, the necessary physical connectivity is established. It is important to note that before establishing the GRE tunnel, the two private LANs must not be exposed to the rest of the network in any way to maintain the confidentiality of both private networks.

Now follows the configuration of the GRE tunnel. On the Kria side, the physical source of the tunnel will be the USB interface (IP address 172.16.1.1), while the physical destination will be the f1/0 interface on the RCisco (IP address 172.16.2.1). Conversely, on the RCisco side, the physical source of the tunnel will be the f1/0 interface (IP address 172.16.2.1), while the physical destination will be the USB interface (IP address 172.16.1.1) on the Kria. The virtual interface gre1 on the Kria will be assigned the IP address 10.0.0.1/30, while the virtual interface tunnel0 on the RCisco will be assigned the IP address 10.0.0.2/30. Once the GRE tunnel is established, it is necessary to define one static route on each router. For the Kria, a static route to the network 192.168.2.0/24 (the private LAN on the RCisco side) needs to be defined via gre1 as the outgoing interface, i.e., 10.0.0.2 as the next-hop IP address. Similarly, on the RCisco, a static route to the network 192.168.1.0/24 (the private LAN on the Kria side) needs to be defined via tunnel0 as the outgoing interface, i.e., 10.0.0.1 as the next-hop IP address. This configuration enables communication between the LANs over the GRE tunnel. This brings us to our initial setup, where we will be able to examine the impact of changing the MTU on the traffic behavior of our applications.

The configuration on both the Kria and RCisco establishes a secure (GRE over) IPSec tunnel using IKEv1 (Internet Key Exchange version 1) for encryption and authentication, [5]. On the Kria router, StrongSwan is configured with AES-128 encryption, SHA-1 hashing, and MODP-1024 for Diffie-Hellman key exchange in Phase 1 (IKE). A pre-shared key is used for authentication between the local (172.16.1.1) and remote (172.16.2.1) endpoints. Phase 2 (IPSec) employs the same AES-128 encryption and SHA-1 hashing algorithms to protect traffic between the local subnet (192.168.1.0/24) and the remote subnet (192.168.2.0/24). Similarly, on the RCisco, IKEv1 Phase 1 is configured with AES-128 encryption, SHA-1 hashing, and Group 2 (MODP-1024) for key exchange, using the same pre-shared key for authentication. Phase 2 IPSec settings match those of the Kria – AES-128 for encryption and SHA-1 for hashing within a defined transform set. Next, we create a profile that utilizes this transform set. Finally, we apply the created profile to our tunnel0 (GRE) interface. Together, these configurations establish a robust and secure communication channel between the two networks. This brings us to our second setup, where we will be able to examine the impact of changing the MTU on the behavior of encrypted traffic in our applications.

The aforementioned encapsulations of the payload data, initially via a GRE tunnel and subsequently with IPSec, are illustrated in Figure 2. This figure also provides a comprehensive depiction of the packet structure at each stage of the process.

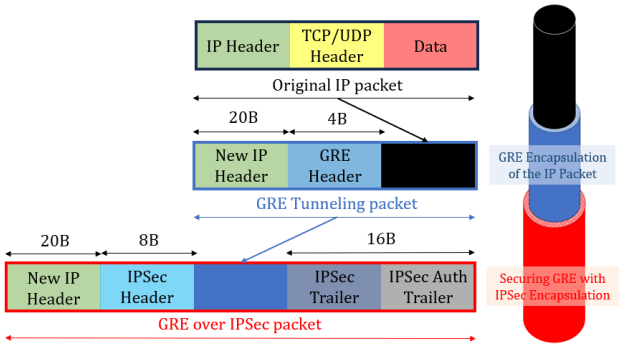

Figure 2. Detailed process of IP packet encapsulation using GRE tunnel and IPSec

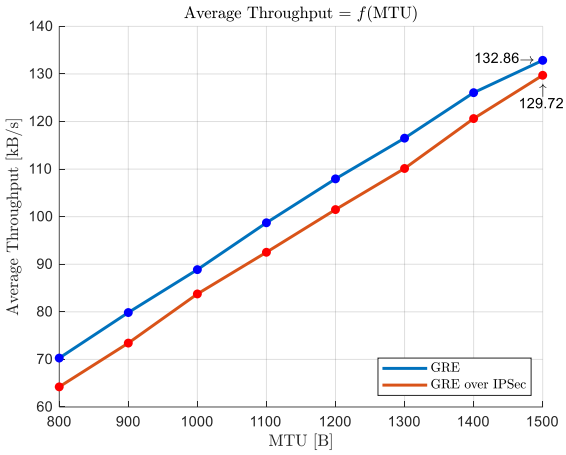

Figure 3. Average Throughput versus MTU

3. RESULTS AND DISCUSSION

The detailed results will now be presented, comparing encrypted and unencrypted traffic in parallel for each application.

3.1. File transfer over TCP

Transmission Control Protocol (TCP) is a fundamental component of the TCP/IP suite, providing comprehensive transport layer services to applications. Positioned within the transport layer of the TCP/IP model, TCP ensures reliable communication by establishing, maintaining, and terminating connections between endpoints. Unlike User Datagram Protocol (UDP), TCP offers a more complex yet robust connection setup that ensures data integrity. TCP breaks down data streams into manageable units known as segments, which are reliably reassembled at the receiving end. This reliability is achieved through mechanisms that maintain the sequence of segments and allow for retransmission of any lost or corrupted data. TCP establishes a logical full duplex connection between application layer processes, ensuring bidirectional communication where data is transmitted in sequence and acknowledged upon receipt, [6].

As a file transfer protocol, FTP has been widely adopted for many years due to its robustness and simplicity in transferring files over networks. It provides a straightforward method for users to upload and download files between their local systems and remote servers, [7]. In our case, a 1MB file was used (generated as a random file of that size) to investigate the behavior of both encrypted and unencrypted traffic when changing the MTU size.

In Figure 3, a comparative scenario is depicted for both unencrypted and encrypted file transfers, showing achieved average throughput while varying the MTU size.

Smaller MTU means each packet can carry less data. This results in more packets needing to be sent to transmit the same amount of data compared to a larger MTU. This increased number of packets introduces additional overhead due to packet headers (e.g., IP, TCP/UDP headers) and protocol processing time, which reduce the overall throughput. Since the packet size exceeds the MTU of a network link, it needs to be fragmented into smaller packets that fit within the MTU. Fragmentation adds complexity to the transmission process as the source device has to break the packets down, and the receiving device has to reassemble them. This process can introduce delays and potentially increase the chance of packet loss or errors, further impacting throughput.

Traffic through a GRE tunnel is generally faster compared to GRE over IPSec due to the additional overhead and processing required by IPSec. IPSec provides encryption for the data traveling through the tunnel, which involves computationally intensive operations. Each packet must be encrypted on the sending end and decrypted on the receiving end, which adds processing time and can slow down the traffic. IPSec includes mechanisms for ensuring the authenticity and integrity of the data packets, such as hashing and verification processes. Also, IPSec adds extra headers to each packet for encryption and authentication purposes (see Figure 2). This adds further processing overhead compared to a plain GRE tunnel, which does not include such features.

3.2. Video streaming over UDP

UDP is one of the core protocols in the TCP/IP suite, operating at the transport layer alongside TCP. Unlike TCP, UDP is connectionless and does not provide mechanisms for guaranteed delivery, sequencing, or error checking. Instead, UDP focuses on minimal overhead and high-speed transmission, making it suitable for applications where occasional packet loss is acceptable, such as real-time video streaming. UDP does not establish a connection before sending data. Each UDP packet (datagram) is independent and can be sent without prior communication, [8]. UDP does not guarantee delivery or order of packets. Overall, UDP is valuable in situations

where speed and low latency are critical, and where occasional packet loss can be tolerated without significant impact on application performance.

VLC is a free and open-source cross-platform multimedia player and framework that supports playback of most multimedia files, including DVDs, audio CDs, VCDs and a variety of streaming protocols, [9]. In our case, "BigBuckBunny_320x180.mp4" video was used (it has become a popular example of open-source filmmaking and has been used in various educational and promotional contexts; it can be downloaded from [10]) to investigate the behavior of both encrypted and unencrypted traffic when changing the MTU size, by streaming it via VLC.

While this resolution may seem low by civilian standards, it offers several strategic advantages in military contexts. Firstly, in situations where covert surveillance is crucial, such as reconnaissance missions or movement monitoring, smaller, less conspicuous cameras with lower resolutions are easier to conceal and deploy discreetly. Secondly, lower resolution cameras consume less bandwidth and storage space, which is particularly important in remote or austere environments where resources like power and network connectivity are limited. Additionally, these cameras can operate efficiently in harsh conditions, such as extreme temperatures or rugged terrain, where robustness and reliability are paramount. Lastly, the reduced visual detail of 320x180 resolution may still provide sufficient information for situational awareness and decision-making, especially when coupled with advanced image processing and analytics technologies that enhance the interpretation of captured footage.

The following Table 2. presents the detailed subjective experience observed during video streaming on the client side, capturing insights from both unencrypted and encrypted traffic scenarios. The results show a remarkable similarity between the two cases, highlighting negligible perceptible differences in user experience despite the added encryption overhead.

Table 2. Descriptive subjective experience versus MTU

MTU [B]	Descriptive subjective experience
1500	Perfect viewing experience
1400	Watchable in a satisfactory manner
1300	Watchable, with slightly degraded graphics
1200 & 1100	Almost satisfactory viewing, occasional stuttering occurs
1000 & 900	Blurred scenes have started to appear
800	Significant stuttering during certain scenes
700 & 600	Less frequent appearances of scenes
500	Partially usable
≤ 400	Completely unusable

A larger MTU size allows for optimal data transmission without noticeable degradation, providing a seamless viewing experience (MTU = 1500). Slight reduction in MTU starts to show minor impacts on video quality but remains generally acceptable for viewing (MTU = 1400). Further reduction in MTU leads to noticeable degradation in video quality, particularly in visual clarity and detail (MTU = 1300). Occasional interruptions or stutters begin to occur by further reducing the MTU, impacting the smoothness of video playback intermittently (MTU = {1200, 1100}). As MTU further decreases, video content becomes visibly blurry or pixelated, affecting overall viewing experience and clarity (MTU = {1000, 900}). Significant interruptions and delays in video playback become noticeable at MTU = 800. Video content may fail to load or display consistently at MTU = {700, 600}, leading to irregular viewing experiences with missing or delayed scenes. The last possible MTU value set for transmitting the video from which some useful data can be extracted is at a value of 500; video streaming becomes challenging with frequent interruptions or delays, making it difficult to follow content consistently. For the MTU ≤ 400, video content is severely disrupted or fails to load entirely, rendering it impossible to watch due to continuous buffering or playback issues.

4. CONCLUSION

Based on the detailed setup and experimental findings, our study emphasizes the critical role of secure and efficient communication in military operations. The integration of GRE tunnels, particularly when combined with IPSec for encryption, offers a robust solution for maintaining confidentiality and reliability across multi-vendor environments. Our research highlights that while IPSec introduces additional overhead due to encryption and authentication processes, the performance impact is minimal under optimal MTU settings, ensuring that encrypted traffic remains viable for high-priority applications.

For file transfer protocols like FTP, our experiments demonstrate that varying MTU sizes significantly influence throughput, with larger MTUs generally yielding faster transfer rates. Even with IPSec encryption, the highest MTU setting (1500 bytes) proved to be the most efficient, underscoring the balance between security and performance in military communications. Similarly, in video streaming applications, MTU size plays a crucial role in maintaining high-quality transmission, where larger MTUs contribute to better user experiences, albeit with slight performance variations between encrypted and unencrypted scenarios.

In conclusion, configuration of GRE tunnel and GRE over IPSec in a multi-vendor environment, coupled with exploration of optimal MTU values, provides insights crucial for enhancing communication efficiency and reliability in military settings. These findings underscore the importance of adaptive network configurations that accommodate both security requirements and operational performance needs, ensuring mission-critical data is transmitted effectively and securely across dynamic battlefield environments.

Acknowledgment

This paper was funded by Vlatacom Institute of High Technologies under the project P176.

References

[1] El Idrissi, D., Elkamoun, N., Lakrami, F., & Hilal, R. (2018). Study of the impact of routing and the profoundness of GRE tunnels on the performance of the transmission of real time applications in IP networks. *IJCSNS*, 18(7), 76.

[2] https://en.wikipedia.org/wiki/Dynamips (last time accessed on 22.06.2024)

[3] https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3 (last time accessed on 22.06.2024)

[4] W. V. Wollman and Y. Barsoum, "Overview of open shortest path first, version 2 (OSPF V2) routing in the tactical environment," *Proceedings of MILCOM '95*, San Diego, CA, USA, 1995, pp. 925-930 vol.3, doi: 10.1109/MILCOM.1995.483435.

[5] https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html (last time accessed on 22.06.2024)

[6] Orogun, A. O. Brief insight into transmission control protocol (TCP), 2017.

[7] Liu Xia, Feng Chao-sheng, Yuan Ding and Wang Can, "Design of secure FTP system," *2010 International Conference on Communications, Circuits and Systems (ICCCAS)*, Chengdu, 2010, pp. 270-273, doi: 10.1109/ICCCAS.2010.5582002.

[8] V. V. Belkhode and D. M. Dakhane, UDP-Based Multi-Stream Communication Protocol, *International Journal of Innovative Research in Electronics and Communications*, 2015, 2(7), pp. 11-15.

[9] https://www.videolan.org/ (last time accessed on 22.06.2024)

[10] https://download.blender.org/peach/bigbuckbunny_movies/ (last time accessed on 22.06.2024)