Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 181-188

Performance and Resilience Analysis of GRE over IPsec Tunnels in Dynamic Routing Networks

Penka Markova
Computer Science and Engineering
Technical University of Varna
Varna, Bulgaria
penkamarkova5@gmail.com

Georgi Markov
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
g.markov@naval-acad.bg

***Abstract*— This paper presents the design and experimental evaluation of Generic Routing Encapsulation over Internet Protocol Security tunnels in dynamic routing networks. The study is motivated by the need to provide secure inter site connectivity while preserving support for dynamic route exchange between remote network segments. A laboratory topology is developed to examine the behavior of the proposed tunnel architecture under normal operation and during network failures. The evaluation focuses on key indicators including throughput, delay, jitter, packet loss, and routing convergence time. In addition, resilience is assessed through controlled disruption and recovery scenarios in order to measure tunnel stability, service continuity, and network reconvergence. The results are used to analyze the balance between secure communication and the performance impact introduced by encapsulation and tunnel protection. Particular attention is given to the practical suitability of this approach for distributed networks that require both protected traffic transmission and flexible routing operation. The study shows that GRE over IPsec remains an effective solution for secure dynamic routing environments when performance limitations and recovery characteristics are properly considered in network design and deployment.**

Keywords*— *dynamic routing protocols, GRE over IPsec, resilience analysis, routing convergence, secure inter-site connectivity, tunnel performance.

I. Introduction

Modern distributed networks are often required to exchange routing information across geographically separated sites while maintaining confidentiality, integrity, and controlled access to operational traffic. In such environments, secure site-to-site connectivity must support not only data forwarding but also the reliable operation of the routing control plane. Internet Protocol Security (IPsec) is a widely adopted framework for protecting IP communications by providing confidentiality, integrity, authentication, and anti-replay protection [1]. At the same time, Generic Routing Encapsulation (GRE) offers a flexible mechanism for transporting network-layer traffic over an overlay tunnel [2]. When these two technologies are combined, it becomes possible to build secure logical links that also preserve support for dynamic routing protocols.

This combination is especially relevant in networks where redundancy, topology changes, and automatic path recovery must be supported without frequent manual intervention. Dynamic routing protocols such as OSPF rely on the continuous exchange of control messages and on the logical visibility of routed paths between remote sites [3]. GRE over IPsec provides a practical means of enabling such routing exchanges over protected inter-site connections, thereby making the tunnel interface appear as a normal routed link from the perspective of the routing process [4].

Despite these advantages, GRE over IPsec introduces additional encapsulation overhead and processing cost. The layered use of GRE and IPsec increases packet size, reduces effective payload efficiency, and may create sensitivity to Maximum Transmission Unit (MTU) limitations, packet fragmentation, and additional cryptographic processing [5]. These factors can influence key operational indicators such as throughput, delay, jitter, packet loss, and routing recovery behavior. As a result, the use of GRE over IPsec involves a practical trade-off between improved security and the performance penalties associated with nested tunneling and encryption.

For these reasons, this paper investigates the performance and resilience of GRE over IPsec tunnels in dynamic routing networks. Rather than proposing GRE over IPsec as a new tunneling mechanism, the study provides a controlled experimental assessment of its operational behavior when dynamic routing, encryption,

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol3.53

encapsulation overhead, and link recovery are considered together. The laboratory implementation evaluates tunnel behavior during normal operation and under controlled failure and recovery conditions. The analysis focuses on throughput, delay, jitter, packet loss, and routing convergence time in order to assess the balance between communication security, routing flexibility, and operational robustness.

The main contribution of the paper is an experimentally grounded evaluation of GRE over IPsec in a reproducible laboratory scenario, with emphasis on measurable performance impact and service continuity during routing changes. The scope is intentionally limited to a compact test topology that allows the influence of tunneling, encryption, and dynamic routing behavior to be isolated. Evaluation of larger multi-site topologies and comparison with newer overlay VPN approaches are identified as directions for future work.

II. Background and Related Work

GRE over IPsec is an established tunneling approach used when a network must combine flexible traffic encapsulation with protected inter-site communication. In this architecture, GRE performs the logical encapsulation of routed traffic, while IPsec protects the encapsulated packets during transport across the external network [4]. Therefore, the novelty of recent research in this area is not associated with the existence of the mechanism itself, but with its measured behavior under specific routing, security, and failure-recovery conditions. This layered design remains relevant in environments where dynamic routing protocols, multicast traffic, or additional protocol flexibility must be preserved across a secure tunnel [6].

The relevance of GRE over IPsec in dynamic routing environments is directly related to routing protocol support. Conventional site-to-site IPsec deployments may secure traffic successfully, but they do not always provide the same flexibility for transporting routing updates and maintaining a routed overlay between remote sites. GRE addresses this limitation by creating a logical point-to-point tunnel over which routing adjacencies can be formed and maintained [4], [7]. In this way, the combination of GRE and IPsec is well suited to distributed networks in which secure transport and dynamic route exchange must coexist.

Recent studies on overlay networking and VPN performance further support the need for experimental analysis of tunnel-based secure connectivity. Existing research shows that overlay design choices have measurable effects on round-trip time, bandwidth efficiency, and service stability [8]. Other studies have emphasized that VPN performance is strongly influenced by packet processing overhead, protocol stack behavior, and virtual interface implementation [9]. These findings are directly relevant to GRE over IPsec, where GRE encapsulation and IPsec protection operate together and therefore jointly affect communication efficiency.

A central practical issue in GRE over IPsec deployments is the impact of encapsulation overhead. The addition of GRE headers, followed by IPsec processing and protection headers, increases packet size and reduces the proportion of useful payload in each transmitted frame. This may amplify MTU sensitivity, increase the risk of fragmentation, and degrade performance under load. Consequently, any realistic assessment of GRE over IPsec should not treat tunnel establishment as the sole success criterion, but should also evaluate the impact of the solution on throughput, delay, jitter, and packet loss [8], [9]. For reproducibility, such assessments should also specify the IPsec profile, routing protocol parameters, traffic generation method, and measurement tools, since these factors can significantly affect the observed results.

Another important aspect concerns deployment limitations and alternative overlay approaches. GRE over IPsec is typically implemented as a point-to-point solution and is subject to practical restrictions regarding scalability and session design [4]. These characteristics distinguish it from more advanced multipoint or policy-driven overlay architectures, such as DMVPN, FlexVPN, route-based IPsec/VTI deployments, WireGuard-based VPNs, and SD-WAN solutions [10]. Such technologies may offer better scalability, simplified tunnel management, or centralized policy control in larger networks. However, GRE over IPsec remains relevant in compact and medium-sized deployments because of its wide platform support, clear tunnel semantics, and compatibility with dynamic routing. For this reason, the present paper focuses on the operational behavior of GRE over IPsec itself, while a direct comparative evaluation with newer overlay VPN technologies is left for future work.

Recent work on routing resilience also justifies the focus on convergence and recovery behavior in this study. Research comparing dynamic routing protocols under failure conditions has shown that convergence time, traffic redistribution, and recovery stability are critical indicators in routed environments [11]. Similarly, recent studies involving GRE-based routing deployments have reported measurable effects on jitter, packet loss, and recovery time during link disruption [7]. These findings suggest that tunnel-based secure communication should be evaluated not only in steady state, but also during service interruption and restoration.

Based on the reviewed literature and practical platform guidance, the main research gap is not whether GRE over IPsec can provide secure routed connectivity, since this capability is already well established, but how effectively it performs and recovers under defined dynamic routing and failure conditions. The existing literature discusses tunnel overhead, VPN performance, and routing convergence, but fewer studies combine these aspects in a reproducible GRE over IPsec laboratory scenario. This gap motivates the experimental focus of the present study on performance metrics and recovery behavior in a controlled deployment.

III. Materials and Methods

A. Testbed Topology and Network Architecture

The experimental environment was designed as a small-scale inter-site network intended to emulate secure communication between two geographically separated

local area networks connected through an external IP transport infrastructure.

This topology was intentionally kept compact in order to focus on the behavior of a single GRE over IPsec tunnel in realistic operating conditions. The design supports direct observation of traffic forwarding, routing updates, tunnel status, and recovery behavior while avoiding the additional complexity of multi-path or large-scale environments. Although the topology does not represent a large multi-site deployment, it provides a controlled environment in which the effects of GRE encapsulation, IPsec protection, and OSPF-based recovery can be isolated and measured.

The experimental topology used in the study is illustrated in Fig. 1.

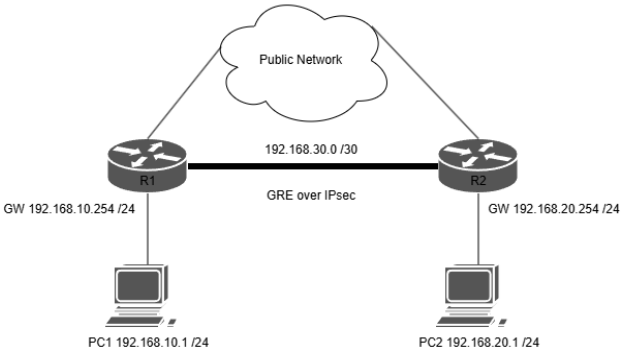

Fig. 1. Experimental topology of the GRE over IPsec inter-site testbed.

The first local segment, LAN1, contains a host with IP address 192.168.10.1/24, while the LAN-facing interface of R1 is configured with address 192.168.10.254/24. The second local segment, LAN2, contains a host with IP address 192.168.20.1/24, while the LAN-facing interface of R2 is configured with address 192.168.20.254/24. The tunnel endpoints communicate across an external IP transport network through WAN-facing interfaces. Over this transport path, a GRE tunnel is created, and IPsec is applied to protect the GRE traffic exchanged between the routers.

This topology was intentionally kept compact in order to focus on the behavior of a single GRE over IPsec tunnel in realistic operating conditions. The design supports direct observation of traffic forwarding, routing updates, tunnel status, and recovery behavior while avoiding the additional complexity of multi-path or large-scale environments.

B. GRE over IPsec Tunnel Design

The implemented tunnel architecture combines GRE and IPsec in order to preserve support for routing protocol exchange while simultaneously securing traffic across the interconnecting network. GRE serves as the logical transport mechanism between the remote routers, allowing the tunnel to carry both user-plane and control-plane traffic. IPsec provides confidentiality and integrity for the GRE-encapsulated packets transmitted over the WAN-facing path [1].

The tunnel was configured as a point-to-point logical connection between R1 and R2. From the perspective of the routing process, the GRE interface behaves as a normal routed link, which makes it possible to establish dynamic routing adjacency across the secure overlay. This architecture reflects a practical deployment model for secure inter-site communication where traditional site-to-site IPsec alone may not provide sufficient flexibility for routing protocol transport.

The main GRE and IPsec configuration parameters used in the experiment are summarized in Table 1. These parameters were kept constant across all protected-tunnel measurements in order to ensure comparability between the traffic scenarios.

TABLE 1 GRE OVER IPSEC CONFIGURATION PARAMETERS

Parameter	Value
GRE tunnel mode	Point-to-point GRE tunnel
Tunnel source/destination	WAN-facing interfaces of R1 and R2
Tunnel addressing	Routed point-to-point tunnel subnet
Routing protocol over tunnel	OSPF
IPsec protection target	GRE traffic between R1 and R2
IKE version	IKEv2
Encryption algorithm	AES-256
Integrity / hash algorithm	SHA-256
Authentication method	Pre-shared key
Diffie-Hellman group	Group 14
IPsec mode	Tunnel mode
SA lifetime	86000

The operational state of the tunnel and the associated IPsec protection were verified on the tunnel endpoint, as shown in Fig. 2.

```
R1#sh int tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.30.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source [redacted]  destination [redacted]
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:32, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 100 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     141 packets output, 14084 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
R1#sh cry
R1#sh crypto se
R1#sh crypto session
Crypto session current status

Interface: GigabitEthernet0/2
Session status: UP-ACTIVE
Peer: [redacted] port 500
  IKEv1 SA: local [redacted] /500 remote [redacted] /500 Active
  IPSEC FLOW: permit 47 host [redacted] host [redacted]
        Active SAs: 2, origin: crypto map
```

Fig. 2. Verification of GRE tunnel status and active IPsec session on router R1.

The output confirms that the GRE tunnel interface was operational and that an active IPsec session had been established between the peers. The verification included tunnel interface status, crypto session state, encapsulated and decapsulated packet counters, and the presence of protected GRE traffic between the two WAN-facing endpoints.

C. Dynamic Routing Operation

Dynamic routing was enabled across the GRE tunnel using OSPF in order to evaluate not only basic connectivity, but also the suitability of the solution for routed inter-site operation. The OSPF configuration used a single routing area and formed adjacency over the GRE tunnel interface. The LAN networks behind R1 and R2 were advertised through OSPF, allowing end-to-end reachability to be restored automatically after tunnel recovery. The same OSPF parameters were maintained throughout the experiments in order to avoid changes in convergence behavior caused by routing configuration differences. OSPF Hello traffic was observed traversing the GRE tunnel, confirming that routing protocol exchanges were successfully carried over the protected logical path. This behavior demonstrates that the tunnel architecture supports the control plane required for adaptive routing between the two remote LAN segments.

In the context of the present study, dynamic routing is treated as a core functional property of the tunnel environment rather than as an auxiliary feature. The presence of routing protocol traffic allows the experiment to assess not only data forwarding performance, but also convergence and recovery after transport disruption.

Packet capture analysis further confirmed the presence of both routing control traffic and end-to-end user traffic in the experimental environment, as illustrated in Fig. 3.

The observed OSPF hello packets and successful ICMP exchanges support the conclusion that the tunnel carried both control-plane and user-plane traffic.

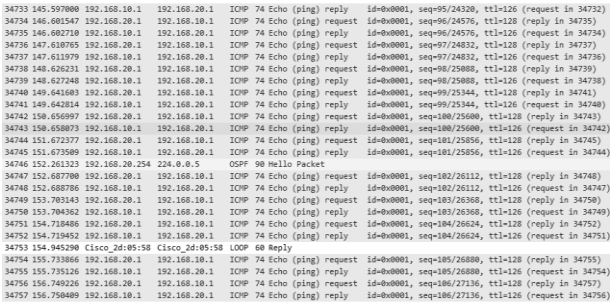

Fig. 3. Verification of GRE tunnel status and active IPsec session on router R1.

D. Measurement Metrics and Traffic Scenarios

The methodological focus of the study is not limited to successful tunnel establishment. Instead, the objective is to quantify the operational impact of layered encapsulation and encryption on network behavior. For this reason, the evaluation considers throughput, end-to-end delay, jitter, packet loss, and routing convergence time as the main performance indicators [11], [12].

The measurements were performed using iperf3 for TCP and UDP traffic generation, ICMP echo tests for reachability and delay observation, Wireshark for packet capture analysis, and Cisco IOS diagnostic commands for tunnel, routing, and IPsec verification. Router CLI outputs were used to monitor tunnel state, OSPF adjacency, crypto session status, and encapsulation/decapsulation counters during normal operation and recovery.

The measurements are structured around several comparative traffic scenarios. First, baseline measurements are collected without tunnel protection in order to establish reference values for the underlying network path. Second, equivalent traffic is transmitted across the GRE tunnel without IPsec in order to isolate the effect of GRE encapsulation. Third, traffic is measured over the complete GRE over IPsec configuration in order to assess the additional impact of encryption and tunnel protection. This staged methodology allows the individual and combined effects of encapsulation and security processing to be interpreted more clearly.

Both TCP and UDP traffic scenarios are included in the evaluation. TCP traffic is used to examine the impact of the tunnel architecture on reliable data transfer and effective throughput, while UDP traffic is used to assess delay, jitter, and packet loss under controlled offered load. This combination provides a balanced view of tunnel performance for both connection-oriented and real-time traffic patterns.

The measurements are reported as representative observations obtained under stable laboratory conditions. Since the experiments were performed in a controlled environment with fixed topology, fixed configuration parameters, and limited background traffic, the results are suitable for comparative interpretation within the tested scenario. However, repeated measurements over longer observation periods would be required for stronger statistical generalization.

E. Failure and Recovery Procedure

In addition to performance measurements, the study includes a resilience assessment under failure conditions. Controlled disruption is introduced at the WAN-facing side of the tunnel environment in order to observe the response of the protected tunnel, the routing process, and end-to-end communication. The recovery phase is then monitored in order to determine the time required for restoration of the IPsec security association, re-establishment of the GRE tunnel, recovery of OSPF adjacency, and stabilization of user traffic.

The disruption was introduced by administratively disabling the WAN-facing interface, and recovery was initiated by restoring the same interface. The recovery interval was measured from the moment of transport restoration until stable end-to-end communication between LAN1 and LAN2 was observed again. During this interval, tunnel state, IPsec session state, OSPF adjacency, and user traffic restoration were monitored.

This procedure makes it possible to distinguish between several different phases of recovery: transport restoration, tunnel restoration, routing reconvergence, and traffic stabilization [11]. Such separation is important because a tunnel may return to the up state before communication quality fully returns to steady-state conditions.

F. Scope and Limitations

The developed topology is intentionally limited to a single protected logical path between two routers. As a result, the resilience analysis in this paper focuses on service continuity, tunnel recovery, and routing reconvergence rather than on redundancy-based failover through alternative underlay links. The study therefore addresses operational resilience in the sense of automatic recovery after transient interruption, but not high-availability behavior based on path diversity.

Within this scope, the main methodological contribution of the study is the combined evaluation of performance and recovery behavior in a dynamic routing environment using GRE over IPsec. The experimental design provides a practical basis for assessing the suitability of this architecture for secure routed inter-site communication. A direct performance comparison with DMVPN, FlexVPN, VTI-based IPsec, WireGuard, or SD-WAN overlays is outside the scope of the present study and is considered future work.

IV. Results and Discussion

A. Performance Assessment

The results obtained in the laboratory network environment show that GRE over IPsec provides stable and functionally correct communication between the two remote LAN segments under the tested conditions. The tunnel successfully carries both user-plane and control-plane traffic, including OSPF exchanges, thereby confirming its suitability for routed inter-site operation in the evaluated topology.

At the same time, the measurements clearly indicate that the use of GRE encapsulation and IPsec protection introduces measurable communication overhead. Compared with plain IP forwarding, the protected tunnel produces lower effective throughput, increased delay, higher jitter, and a slight increase in packet loss. These effects are consistent with the additional header overhead and processing requirements imposed by GRE and IPsec.

The comparative scenarios also show that GRE alone introduces a moderate performance cost, while the full GRE over IPsec configuration results in the most visible degradation. This confirms that the additional headers, encryption, integrity protection, and cryptographic processing associated with IPsec contribute significantly to the total performance impact of the architecture. From an engineering perspective, the findings demonstrate that secure tunneling should be evaluated not only in terms of functionality, but also in terms of transport efficiency and service quality under expected traffic load.

The reported values should be interpreted as representative measurements obtained under stable laboratory conditions with fixed topology, fixed configuration parameters, and limited background traffic. The detailed numerical results for TCP and UDP traffic are presented in the corresponding tables:

Table 2 Results for TCP Traffic

Operating mode	Average throughput (Mbps)
No tunnel	94.8
GRE without IPsec	91.6
GRE over IPsec	84.9

Table 3 Results for UDP Traffic at 20 Mbps Offered Load

Operating mode	Actual received traffic (Mbps)	Average delay (ms)	Jitter (ms)	Packet loss (%)
No tunnel	19.98	3.3	0.42	0.0
GRE without IPsec	19.74	4.4	0.71	0.3
GRE over IPsec	18.92	6.8	1.36	1.2

Table 4 Relative Impact Compared with Plain IP Forwarding for TCP Traffic

Metric	GRE without IPsec	GRE over IPsec
Throughput reduction	3.4%	10.4%
RTT increase	29.0%	100.0%
Jitter increase	56.7%	193.3%
Packet loss increase	+0.1 percentage points	+0.4 percentage points

B. Resilience Assessment

The resilience assessment shows that disruption of the WAN-facing interface leads to an almost immediate interruption of end-to-end communication, followed by loss of the protected tunnel and interruption of routing continuity. The recovery times were derived from the observed event timestamps, router diagnostic outputs, OSPF adjacency state changes, IPsec session status, and end-to-end ICMP reachability. The first failed ping is observed approximately 0.1 s after the interruption, the GRE tunnel enters a down state after about 1.0 s, and OSPF adjacency is lost after about 1.1 s. This confirms that both tunnel availability and routing continuity are directly dependent on the availability of the underlying transport path.

After restoration of the WAN interface, the IPsec security association is re-established within approximately 3.6 s, the GRE tunnel returns to the up/up state after about 4.3 s, and OSPF reaches FULL state after approximately 6.8 s. The total communication outage lasts approximately 14.9 s from the beginning of the disruption, while full service stabilization is achieved approximately 18.0 s after the disruption starts. These results indicate that the implemented GRE over IPsec solution is resilient in the sense of automatic service recovery after temporary failure, although it does not provide path redundancy through an alternative underlay route.

An additional observation concerns post-recovery stability. Although the tunnel becomes operational again within a relatively short interval, communication quality does not immediately return to its steady-state baseline. A short post-recovery phase is observed in which jitter remains elevated and packet loss temporarily increases. This indicates that tunnel restoration, routing reconvergence, and traffic stabilization should be treated as distinct but related phases of recovery.

The resilience-related measurements are summarized in the following tables:

TABLE 5 EVENT TIMELINE DURING CONTROLLED DISRUPTION AND RECOVERY

Event	Time from test start (s)
Normal operation	0–30.0 s
WAN interface disabled on R1	30.0 s
First failed ping	30.1 s
IPsec session begins to fail	30.4 s
GRE tunnel enters down state	31.0 s
OSPF adjacency lost	31.1 s
WAN interface restored	38.0 s
IPsec re-established	41.6 s
GRE tunnel up/up	42.3 s
OSPF adjacency FULL	44.8 s
First successful ping after recovery	45.0 s
Communication stabilized	48.0 s

TABLE 6 MEASURED RESILIENCE INDICATORS

Indicator	Value
Start of disruption	30.0 s
Duration of physical interruption	8.0 s
Time until tunnel failure	1.0 s
Time until OSPF adjacency loss	1.1 s
Time to IPsec re-establishment	3.6 s after link restoration
Time to GRE tunnel recovery	4.3 s after link restoration
Time to OSPF recovery	6.8 s after link restoration
Total communication outage	14.9 s
Time to full service stabilization	18.0 s

TABLE 7 TRAFFIC BEHAVIOR BEFORE, DURING, AND AFTER DISRUPTION

Metric	Before disruption	During disruption	After recovery
TCP throughput	84.9 Mbps	0 Mbps	82.7 Mbps
UDP received rate	18.92 Mbps	0 Mbps	18.45 Mbps
RTT	6.2 ms	timeout	7.1 ms
Jitter	0.88 ms	—	1.94 ms
Packet loss	0.4%	100%	2.8% during first 5 s
OSPF state	FULL	DOWN	FULL

These resilience results are specific to the tested configuration, routing timers, IPsec parameters, router platform, and failure procedure. Therefore, they should not be interpreted as universal recovery times for all GRE over IPsec deployments. Instead, they demonstrate the sequence of recovery phases and the type of operational impact that may occur when the protected underlay path is temporarily interrupted.

C. Discussion of Trade-Offs

Taken together, the results show that GRE over IPsec provides a practical and functionally effective solution for secure communication in networks that require dynamic route exchange between remote sites. The architecture successfully supports both data forwarding and routing control traffic, thereby preserving routing flexibility while securing the communication path.

However, this functional advantage is accompanied by measurable performance cost. The combined use of GRE encapsulation and IPsec protection reduces effective throughput, increases delay and jitter, and introduces a modest increase in packet loss compared with plain forwarding. In addition, temporary underlay failure causes complete service interruption, followed by a recovery interval during which the cryptographic session, tunnel state, and routing adjacency must all be restored before traffic fully stabilizes.

These findings suggest that GRE over IPsec should be regarded as a solution that offers an effective balance between security and routing flexibility rather than maximum transport efficiency. In practical deployments, this makes the architecture well suited for protected inter-site communication where moderate performance trade-offs are acceptable. At the same time, the expected recovery interval and short-term post-recovery instability should be considered carefully in networks that carry delay-sensitive traffic or require strict service continuity.

The results also indicate that GRE over IPsec remains a practical solution when dynamic routing support and broad platform compatibility are required, but it should not be considered the only possible secure overlay design. Technologies such as DMVPN, FlexVPN, VTI-based IPsec, WireGuard-based VPNs, and SD-WAN overlays may provide advantages in scalability, centralized policy management, or multipoint connectivity. A direct experimental comparison with these alternatives is outside the scope of the present paper and is identified as future work.

From a practical design perspective, the obtained results suggest that GRE over IPsec is appropriate for controlled inter-site deployments where secure routing exchange is required and where a moderate reduction in throughput and increase in delay can be accepted. For larger networks, delay-sensitive services, or strict high-availability requirements, additional mechanisms such as redundant underlay paths, optimized MTU settings, tuned routing timers, or alternative overlay VPN architectures should be considered.

V. CONCLUSIONS

This paper presented the design, implementation, and experimental evaluation of a GRE over IPsec tunnel in a dynamic routing environment connecting two remote LAN segments through an external IP transport network. The study did not aim to introduce GRE over IPsec as a new tunneling mechanism, since this approach is already well

established. Instead, the contribution of the paper is a controlled laboratory assessment of its performance and recovery behavior when GRE encapsulation, IPsec protection, and OSPF-based dynamic routing are used together.

The practical implementation confirmed that the combined use of GRE and IPsec makes it possible to maintain secure inter-site communication while preserving the exchange of routing control traffic across the tunnel. The tunnel successfully carried both user-plane and control-plane traffic, including OSPF messages, thereby demonstrating its suitability for the evaluated scenario, where protected communication and routing flexibility were both required.

At the same time, the experimental results showed that GRE over IPsec introduces measurable communication overhead. Compared with plain IP forwarding, the protected tunnel resulted in lower effective throughput, increased delay, higher jitter, and a slight increase in packet loss. These effects became more pronounced when IPsec protection was applied on top of GRE, confirming that additional encapsulation, security headers, and cryptographic processing contribute significantly to the total performance impact.

The resilience evaluation further demonstrated that temporary loss of the underlay connection causes immediate interruption of communication, loss of tunnel availability, and disruption of routing continuity. Nevertheless, after restoration of the transport path, the IPsec security association, GRE tunnel state, and OSPF adjacency were re-established automatically without manual intervention. This confirms that the implemented architecture is resilient in the sense of service recovery after transient failure, even though it does not provide redundancy-based failover through alternative paths. The results also showed that communication quality does not return instantly to steady-state conditions after restoration, since a short post-recovery phase with elevated jitter and temporary packet loss was observed.

From a practical perspective, the findings indicate that GRE over IPsec remains a viable solution for secure communication in dynamic routing networks when both traffic protection and routing functionality are required across remote sites. However, the results should be interpreted within the limits of the tested topology, router platform, traffic scenarios, OSPF parameters, and IPsec configuration. The architecture offers an effective balance between security and operational flexibility, but its deployment should be accompanied by prior assessment of the expected impact on traffic quality, MTU behavior, and recovery time.

The main limitation of the present study is the scale of the experimental environment. Because the implementation was based on a single protected logical path between two routers, the work addresses performance and recovery-oriented resilience rather than redundancy-based failover or large-scale overlay behavior. In addition, the study does not provide a direct comparison with newer or more scalable VPN and overlay approaches such as DMVPN, FlexVPN, VTI-based IPsec, WireGuard-based VPNs, or SD-WAN solutions.

Future work may extend the evaluation toward more complex topologies involving multiple tunnels, redundant WAN paths, larger numbers of routing nodes, comparative routing protocol analysis, optimized MTU and timer settings, and repeated long-duration measurements. A direct experimental comparison with alternative secure overlay technologies would also provide a broader basis for evaluating the trade-offs between security, scalability, routing flexibility, and recovery performance.

In conclusion, the experimental evidence supports the view that GRE over IPsec is an effective and operationally relevant solution for secure routed communication between remote network segments in controlled inter-site deployments. Although the approach introduces measurable overhead and temporary degradation during recovery, it continues to provide a practical combination of traffic protection and routing support when its performance and resilience limitations are properly considered.

REFERENCES

[1] K. Seo and S. Kent, “Security Architecture for the Internet Protocol,” Dec. 2005, *RFC Editor*. doi: 10.17487/RFC4301.

[2] T. Li, D. Farinacci, S. P. Hanks, D. Meyer, and P. S. Traina, “Generic Routing Encapsulation (GRE),” Mar. 2000, *RFC Editor*. doi: 10.17487/RFC2784.

[3] J. Moy, “OSPF Version 2,” Apr. 1998, *RFC Editor*. doi: 10.17487/RFC2328.

[4] Cisco, “Security Configuration Guide, Cisco IOS XE 17.14.x (Catalyst 9300 Switches) - Configuring GRE over IPsec .” Accessed: Apr. 07, 2026. [Online]. Available: https://web.archive.org/web/20260407185156/https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-14/configuration_guide/sec/b_1714_sec_9300_cg/configuring_gre_over_ipsec.html

[5] P. Savola, “MTU and Fragmentation Issues with In-the-Network Tunneling,” Apr. 2006, *RFC Editor*. doi: 10.17487/RFC4459.

[6] Cisco, “Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - GRE Over IPsec Tunnels.” Accessed: Apr. 08, 2026. [Online]. Available: https://web.archive.org/web/20260407190810/https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-gre-over-ipsec-tunnels.html

[7] M. Huda and W. Andriyani, “Multi-Area OSPF Analysis Using Virtual Link and GRE Tunnel,” *Eduvest - Journal of Universal Studies*, vol. 5, no. 2, pp. 1804–1819, Feb. 2025, doi: 10.59188/EDUVEST.V5I2.1710.

[8] A. F. Gentile, D. Macrì, E. Greco, and P. Fazio, “Overlay and Virtual Private Networks Security Performances Analysis with Open Source Infrastructure Deployment,” *Future Internet 2024, Vol. 16, Page 283*, vol. 16, no. 8, p. 283, Aug. 2024, doi: 10.3390/FI16080283.

[9] C. Fu *et al.*, “A Generic High-Performance Architecture for VPN Gateways,” *Electronics 2024, Vol. 13, Page 2031*, vol. 13, no. 11, p. 2031, May 2024, doi: 10.3390/ELECTRONICS13112031.

[10] J. Dudczyk, M. Sergiel, and J. Krygier, “Analysis of SD-WAN Architectures and Techniques for Efficient Traffic Control Under Transmission Constraints—Overview of Solutions,” *Sensors 2025, Vol. 25, Page 6317*, vol. 25, no. 20, p. 6317, Oct. 2025, doi: 10.3390/S25206317.

[11] K. Shahid, S. N. Ahmad, and S. T. H. Rizvi, "Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems," *Future Internet 2024, Vol. 16, Page 339*, vol. 16, no. 9, p. 339, Sep. 2024, doi: 10.3390/FI16090339.

[12] A. F. Gentile, D. Macrì, E. Greco, and P. Fazio, "IoT IP Overlay Network Security Performance Analysis with Open Source Infrastructure Deployment," *Journal of Cybersecurity and Privacy 2024, Vol. 4, Pages 629-649*, vol. 4, no. 3, pp. 629–649, Aug. 2024, doi: 10.3390/JCP4030030.