ARTIFICIAL INTELLIGENCE FOR PREDICTIVE HEALTHCARE: A COMPARATIVE STUDY OF MACHINE LEARNING

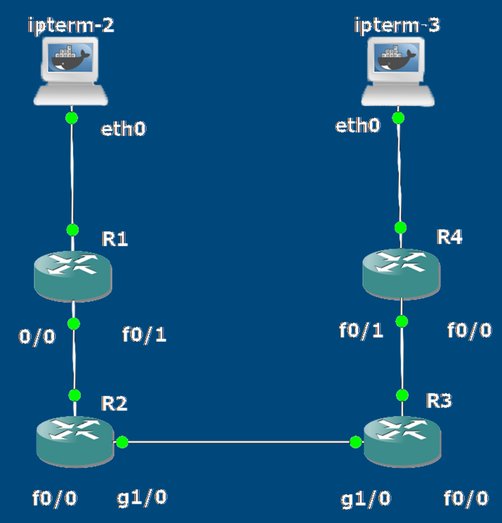
Dr. Sarah A. Al-Harbi
Department of Computer Science, College of Computer and Information Sciences
King Saud University

Introduction

Modern data centers and communication infrastructures use optical networks for unsurpassed bandwidth and speed. However, vulnerabilities can threaten data confidentiality and integrity in these networks. Data transmission is threatened by signal eavesdropping and data tampering which calls for necessitating strong encryption.

Optical Transport Network (OTN) encryption protects optical network data. OTN encryption provides strong security with low latency, but large-scale systems struggle to meet ISO 27001 information security standards. Many optical networks lack security features, emphasizing the necessity for strong encryption frameworks to protect data confidentiality, integrity, and availability.

OTN, OTN over IPsec, and GRE over IPsec are compared in this ISO 27001-compliant optical network encryption study. The project mimics these frameworks in an optical network environment using GNS3 and other tools to test encryption latency, throughput, and network performance. The findings aim to help current optical networks balance security and efficiency.



This topology are used to simulate various network configurations and test protocols, such as encryption frameworks (e.g., OTN over IPsec and GRE over IPsec) in a controlled environment.

Methods

GNS3 was used to carefully design and construct the network topology. The configuration used four routers and two terminal devices to simulate real-world communication. For accurate data flow and network dynamics simulation, the topology was configured.

Three encryption frameworks were deployed across the simulated network topology for comparative analysis. These included a baseline setup with no encryption, OTN over IPsec, and GRE over IPsec. Each framework was meticulously configured to align with industry standards.

Data traffic generation was performed using iperf3, a versatile tool for simulating real-world network conditions. Various traffic patterns and data rates were introduced to measure the impact of encryption frameworks on performance.

Performance metrics such as throughput, latency, jitter, and packet loss were collected under each encryption framework.

Results were analyzed to determine how each encryption framework impacted network performance and compliance with ISO 27001.

ISO 27001 compliance evaluation was conducted to ensure secure transmission while maintaining optimal network functionality.

Metric	Baseline (No Encryption)	OTN Only	OTN Over IPsec	GRE Over IPsec
Average Latency (ms)	115.24	108.99	0.05	0.069
Throughput TCP (Mbps)	0.21	0.11	2.34	2.23
Retries (TCP)	37	5	18	29
Throughput UDP (100 Mbps)	100 Mbps	100 Mbps	99.8 Mbps	96.7 Mbps
Packet Loss UPD (%)	0%	0%	0.08%	0.09%
JITTER (UDP)	64.925 ms	6.172 ms	0.8 ms	4.1 ms

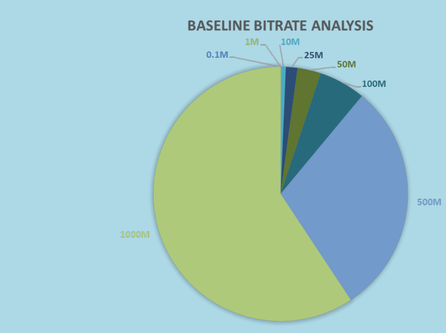
The aimed results should show how to evaluate encryption systems using average delay, throughput, retries, packet loss and jitter for all frameworks

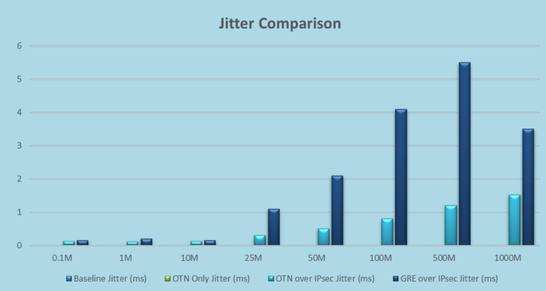
Results & Discussion

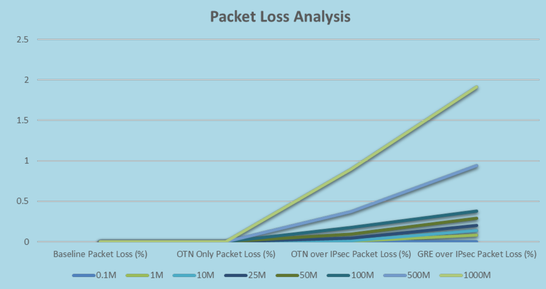
Pie chart represents the distribution of bitrate across various bandwidth categories in the baseline scenario. Most of the traffic was concentrated in the 1000M range, highlighting the network's capacity under unencrypted conditions. Lower bitrate categories showed minimal traffic, indicating efficient bandwidth utilization in the absence of encryption overhead.

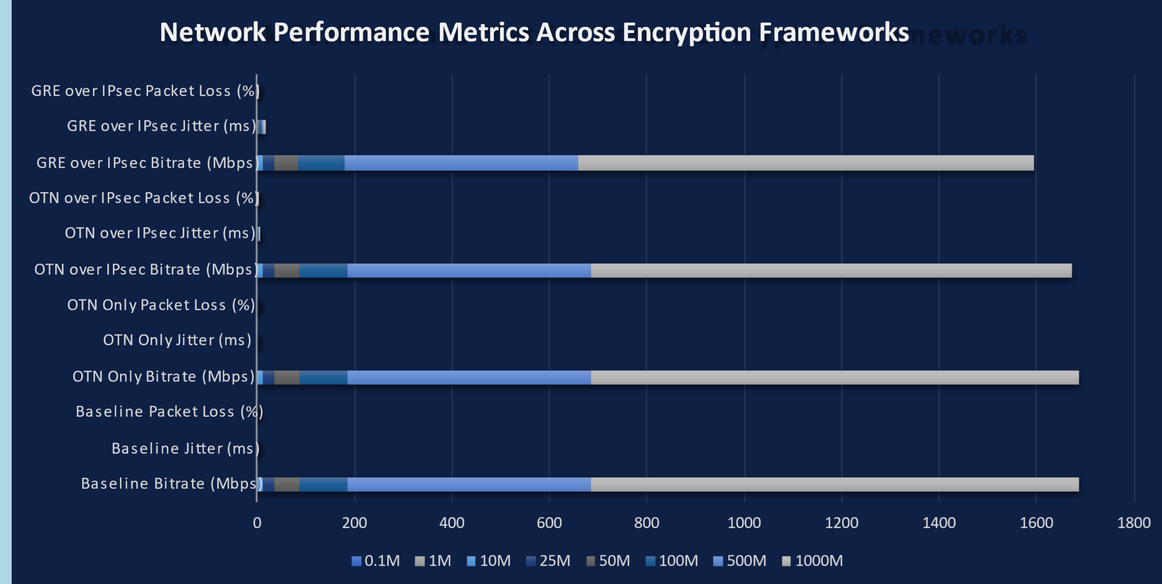
Bar chart compares jitter across different encryption frameworks and baseline. Baseline demonstrated significantly higher jitter values compared to other frameworks. OTN-only exhibited minimal jitter, while OTN over IPsec and GRE over IPsec showed moderate jitter increases as encryption complexity and packet encapsulation levels grew.

Line chart illustrates packet loss percentages across encryption frameworks and baseline. The baseline and OTN-only frameworks exhibited negligible packet loss, while OTN over IPsec and GRE over IPsec showed slight increases. GRE over IPsec had the highest packet loss, likely due to added overhead from encapsulation layers.









The chart provides a comparative analysis of network performance metrics—bitrate, jitter, and packet loss—across different encryption frameworks (Baseline, OTN Only, OTN over IPsec, and GRE over IPsec). Each framework is evaluated at varying traffic rates (0.1M to 1000M), offering insights into their effectiveness in ensuring reliable and efficient data transmission. This visual representation aligns with the study's objective to measure the impact of encryption methods on network performance and security.

Conclusion

The best security-performance balance was OTN over IPsec, with low latency and jitter, high throughput, and little packet loss. While strong, GRE over IPsec increased jitter and packet loss due to overhead. As expected, the baseline setup performed well but lacked encryption, making it unsuitable for secure environments.

ISO 27001 Control	Description	Baseline	OTN Only	OTN Over IPsec	GRE Over IPsec
A.10 Cryptography	Use of encryption to protect information	✗ No encryption	⚠ Partial compliance (physical-layer protection, no explicit encryption)	✓ IPsec ensures data encryption	✓ Similar to OTN over IPsec
A.13 Communications Security	Protecting information in transit	✗ Data Vulnerable	✓ Protection inherent at the physical layer	✓ Secure encryption protects transit data	✓ Enhanced with GRE tunneling and IPsec
A.18 Compliance	Adherence to regulatory requirements	✗ Not aligned	✗ Partially aligned (requires encryption for full compliance)	✓ Aligns with ISO requirements	✓ Aligns with ISO requirements

This study emphasizes the importance of choosing encryption solutions that meet security and performance needs which are highlighted in some key findings through testing:

Findings:

- OTN over IPsec provides the best balance of security and performance, with minimal impact on latency and jitter.
- GRE over IPsec offers strong security but introduces significant overhead, resulting in higher jitter and packet loss.
- The Baseline configuration, while optimal for performance, is unsuitable due to the lack of encryption for secure environments.

Key Insights:

- Encryption frameworks significantly affect network performance metrics, including latency, jitter, and packet loss.
- OTN over IPsec is the most suitable for ISO 27001- compliant secure optical networks, ensuring data confidentiality and integrity.

References

[1] Qian Lv and Zuqing Zhu. 2023. On the Multilayer Planning of Filterless Optical Networks With OTN Encryption. IEEE/ACM Trans. Netw. 31, 6 (Dec. 2023), 2529–2544. https://doi.org/10.1109/TNET.2023.3256409

[2] H. Choi, J. Lee, T. Kim and S. Kim, "Effective management and encryption processing method for security of optical transmission network," 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 1048-1050, doi: 10.1109/ICTC49870.2020.9289595.

[3] F. Chen, M. Song, F. Zhou and Z. Zhu, "Security-Aware Planning of Packet-Over-Optical Networks in Consideration of OTN Encryption," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3209-3220, Sept. 2021, doi: 10.1109/TNSM.2021.3081590

[4] M. Furdek, N. Skorin-Kapov, S. Zsigmond and L. Wosinska, "Vulnerabilities and security issues in optical networks," 2014 16th International Conference on Transparent Optical Networks (ICTON), Graz, Austria, 2014, pp. 1-4, doi: 10.1109/ICTON.2014.6876451.

Email: Abdullah.Alsaffy@ku.edu.kw. Phone: +965 6678 9805