Secure traffic engineering routing framework under normalized link-blocking constraints in softwarized networks

Oleksandr Lemeshko[1,†], Oleksandra Yeremenko[1,*,†] and Anatoliy Persikov[1,†]

[1]Kharkiv National University of Radio Electronics, Nauky Ave, 14, Kharkiv, 61166, Ukraine

Abstract

The paper presents a Secure Traffic Engineering Routing Framework for softwarized networks, emphasizing normalized link-blocking constraints to enhance network security. The proposed framework builds on a flow-based secure routing model with load balancing, incorporating key Traffic Engineering principles while accounting for network security metrics. Secure routing with load balancing is formulated as a linear programming optimization problem, which ensures predictable computational complexity and low processing demands on routing devices, including routers and controllers. A novel aspect of this framework is its adaptation of the exponential link-blocking model using normalized conditions, which prevents secure links from unnecessary blocking and optimizes link resource use. Experimental results demonstrate the model's responsiveness to network topology, flow characteristics, link bandwidth, utilization level, and link compromise probabilities, redistributing traffic to more secure paths and reducing utilization of vulnerable links. Comparative analyses show that the NormSecTE model, an advanced secure TE variant, balances Quality of Service and security metrics. While NormSecTE marginally increases end-to-end delay, it significantly lowers packet compromise probability relative to the SecTE model, achieving an effective trade-off between security and QoS in softwarized network environments.

Keywords

Secure routing, Link compromise, Normalized link blocking, Traffic Engineering

1. Introduction

The growing complexity of modern networks necessitates innovative approaches to managing both Quality of Service (QoS) and security [1, 2, 3]. Software-defined networks (SDNs) enable flexible traffic management, integrating QoS and security requirements [2]. However, this flexibility presents challenges for routing protocols, which must adaptively meet diverse QoS and security demands to determine optimal traffic routes. Effective adaptability to network changes is essential in complex environments, enabling fast failure recovery and maintaining high QoS and security levels within an integrated traffic management framework [3, 4].

The use of mathematical tools is essential for developing optimized routing solutions that address load balancing and security challenges, forming the basis for new strategies suited to modern, programmable networks. Traditional IP routing protocols, such as RIP and OSPF, rely on graph models and shortest path algorithms, which, while effective with limited computing power, do not consider flow characteristics or security [5, 6, 7]. Advances in softwarized network architecture now allow for more sophisticated routing models that handle multi-flow traffic and optimize both QoS and security, prompting recent research to focus on QoS methods incorporating security indicators [8, 9, 10, 11, 12].

A promising direction in secure routing is the application of Traffic Engineering (TE) principles to balance network resource usage, avoiding overload on individual network segments and preventing QoS degradation [13, 14, 15]. Several solutions in this area adapt load balancing to include security

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.

†These authors contributed equally.

oleksandr.lemeshko@nure.ua (O. Lemeshko); oleksandra.yeremenko@nure.ua (O. Yeremenko); anatolii.persikov@nure.ua (A. Persikov)

0000-0002-0609-6520 (O. Lemeshko); 0000-0003-3721-8188 (O. Yeremenko); 0000-0002-8744-7619 (A. Persikov)

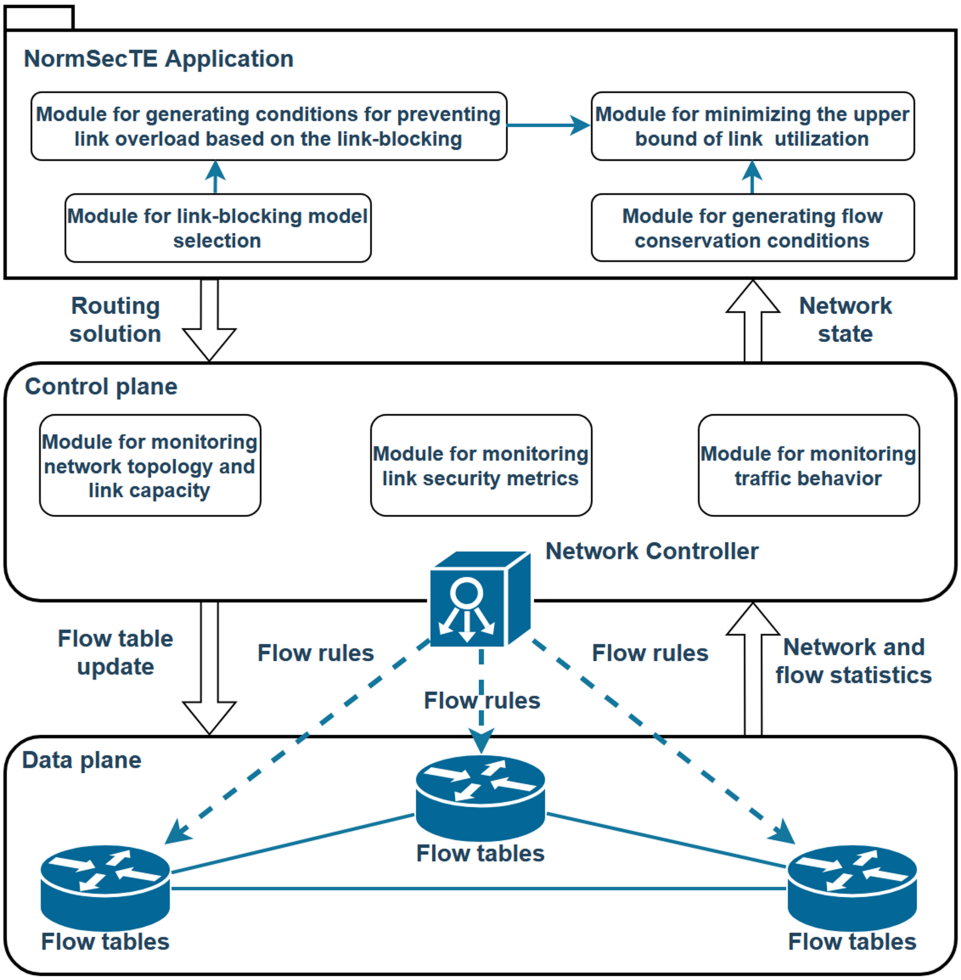

Figure 1: Modular architecture of secure Traffic Engineering routing framework.

considerations [16, 17, 18, 19, 20]. The secure TE routing model proposed for the developed framework in this paper advances solutions [21, 22, 23, 24, 25] by focusing on load balancing and traffic blocking under potential network link compromises.

This paper addresses a critical scientific and applied problem in developing a secure Traffic Engineering routing framework under normalized link-blocking constraints in softwarized networks. The proposed framework aims to optimize network performance by incorporating enhanced load balancing conditions and a normalized model for blocking compromised communication links, thereby increasing the overall levels of both QoS and security.

2. Secure traffic engineering routing framework under normalized link-blocking constraints

Building on the research results of various secure Traffic Engineering routing models in communication networks [21, 22, 23, 24, 25] and an analysis of current technological solutions [2, 13, 14], this paper proposes recommendations for the structural and functional design of advanced SDN solutions. Fig. 1 illustrates a modular representation of the secure Traffic Engineering routing framework architecture, designed with normalized link-blocking constraints to enhance QoS and network security in softwarized networks. This framework is based on the practical implementation of the NormSecTE model [26].

The generalized modular architecture depicted in Figure 1 operates across three functional levels, each responsible for distinct tasks:

- the data plane (network infrastructure);
- the control plane (represented by the controller);
- the application plane (implemented as the NormSecTE Application).

Within the controller architecture, data from modules monitoring network topology, communication link bandwidth, and security metrics, as well as traffic characteristics, are transmitted to the NormSecTE Application. This information enables the application to formulate routing solutions according to the secure Traffic Engineering routing model [26].

The data collected from monitoring modules is essential for establishing conditions to ensure flow conservation and prevent link overload. The processed results are subsequently transmitted to a module responsible for minimizing the upper bound of network link utilization. Through optimized secure routing processes with load balancing, routing solutions are calculated and subsequently translated into flow tables by the controller, which then distributes them to the network‘s forwarding elements (Figure 1).

Next, this paper presents the rationale for selecting the exponential normalized link-blocking model for use within a secure Traffic Engineering routing framework. The model's performance is assessed through simulation and compared with existing models.

3. Secure TE routing model under exponential normalized link-blocking constraints

This section explains the basics of the secure TE routing model under exponential normalized link-blocking constraints and Table 1 contains a model notation summary.

The multipath routing constraints have a form [21]:

$$0 \leq x_{i,j}^k \leq 1. \tag{1}$$

The flow conservation conditions ensuring the route connectivity [21, 26]:

$$\begin{cases} \sum_{j:E_{i,j}\in E} x_{i,j}^k - \sum_{j:E_{j,i}\in E} x_{j,i}^k = 0, & k \in K, \quad R_i \neq s_k, d_k; \\ \sum_{j:E_{i,j}\in E} x_{i,j}^k - \sum_{j:E_{j,i}\in E} x_{j,i}^k = 1, & k \in K, \quad R_i = s_k; \\ \sum_{j:E_{i,j}\in E} x_{i,j}^k - \sum_{j:E_{j,i}\in E} x_{j,i}^k = -1, & k \in K, \quad R_i = d_k. \end{cases} \tag{2}$$

The next formula estimates link utilization [26]:

$$\alpha_{i,j} = \frac{\sum_{k\in K} \lambda^k x_{i,j}^k}{\varphi_{i,j}}. \tag{3}$$

The enhanced load balancing conditions are the following [21, 26]:

$$\sum_{k\in K} \lambda^k x_{i,j}^k \leq \alpha v_{i,j}(p_{i,j})\varphi_{i,j}, \quad E_{i,j} \in E; \tag{4}$$

$$0 \leq \alpha \leq 1. \tag{5}$$

The function $v_{i,j}(p_{i,j})$ models link blocking during secure TE routing, indicating the portion of link capacity used or blocked due to increased compromise probability.

We proposed the modifications of the conditions [26] when compromise scenarios and link probability bounds are known:

$$v_{i,j}(p_{i,j}) = \begin{cases} 0, & \text{if } p_{i,j} = p_{\max}; \\ 1, & \text{if } p_{i,j} = p_{\min}, \end{cases} \tag{6}$$

Table 1
Notations

Notation	Meaning
$G = (R, E)$	Network graph
$R = \{R_i; i = \overline{1, m}\}$	Nodes (routers)
$E = \{E_{i,j};$ $i, j = \overline{1, m}; i \neq j\}$	Directed edges (links)
$\varphi_{i,j}$	Link capacity (packets per second)
K	Number of flows
s_k	Source router
d_k	Destination router
λ^k	Average flow intensity (packets per second)
$x^k_{i,j}$	Routing variables (portion of a flow's intensity on a specific link $E_{i,j} \in E$)
$\alpha_{i,j}$	Link utilization
$v_{i,j}$	Weighting coefficients
p_{min}	Compromise probability of the most secure link
p_{max}	Maximum allowable compromise probability beyond which the link is blocked
p^k_{E2E}	End-to-end probability of packet compromise for the kth flow
τ^k_{E2E}	Average end-to-end delay of packets in the kth flow

$$0 \leq p_{\text{min}} \leq p_{i,j} \leq p_{\text{max}} \leq 1. \tag{7}$$

In a secure TE routing model, we aim to minimize this boundary value α [26, 27]:

$$\min_{x,\alpha} \alpha. \tag{8}$$

In a further study of secure TE routing using the model (1)-(8), we will focus on the exponential link-blocking model:

$$v_{i,j}(p_{i,j}) = \exp\left(-n\frac{p_{i,j} - p_{\text{min}}}{p_{\text{max}} - p_{\text{min}}}\right). \tag{9}$$

Figure 2 illustrates the dependencies of $v_{i,j}(p_{i,j})$ (9) for $n \geq 1$ and the values of $p_{\text{min}} = 0.3$ and $p_{\text{max}} = 1$.

4. Numerical research

This study analyzed and compared four TE routing models:

- the Sec model, which identifies the most secure route for packet transmission;
- the TE model, which does not consider network security parameters [27];
- the SecTE model, which incorporates network security parameters across the full range of link compromise probabilities ($p_{\text{min}} = 0$ and $p_{\text{max}} = 1$) [21, 22];
- the NormSecTE model, an enhanced version of the SecTE model that incorporates normalized network security parameters (Figure 2), represented by the model (1)–(9) ($p_{\text{min}} = 0.3$ and $p_{\text{max}} = 1$).

Further research enabled a comparison of the effectiveness of the proposed secure TE routing model with existing models based on three key indicators: the upper bound of network link utilization α_{max} [21]; the end-to-end packet compromise probability for the kth flow p^k_{E2E} across all utilized paths; and the average end-to-end packet delay of the kth flow τ^k_{E2E} [21, 23].

To illustrate the approach to secure TE routing, we consider the network structure shown in Figure 3. This model simulates the routing of a single packet flow, where packets are transmitted from the first

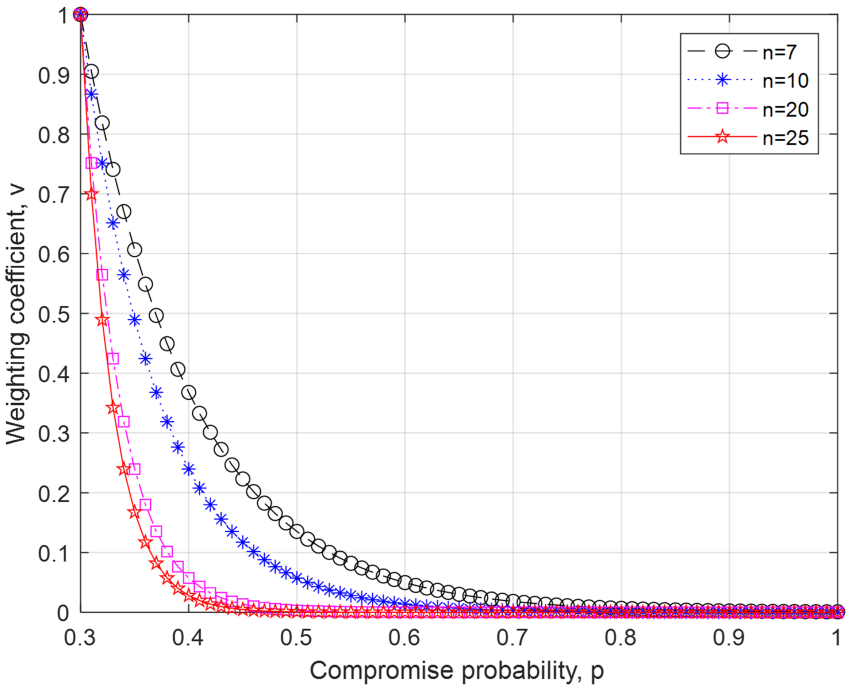

Figure 2: Exponential link-blocking model behavior under $p_{\min} = 0.3$ and $p_{\max} = 1$.

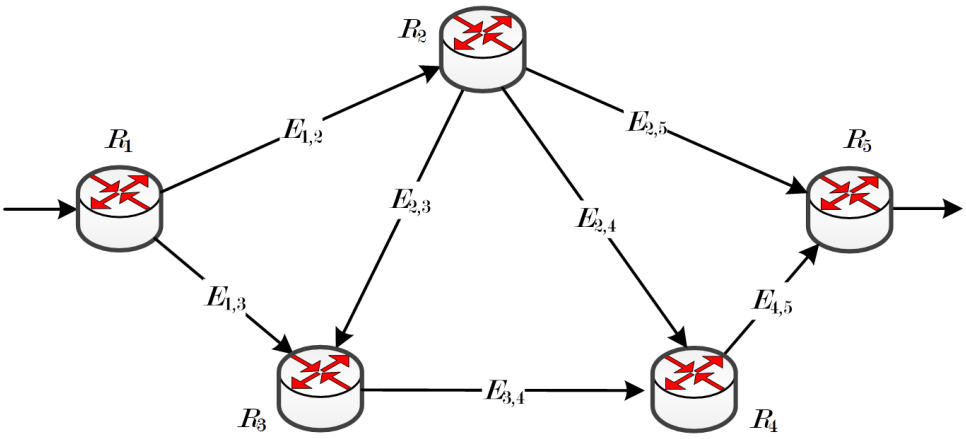

Figure 3: Studied Network Structure.

router to the fifth. Consequently, the flow number is omitted in the analysis below. Table 2 lists the bandwidths of the communication links and their respective compromise probabilities. Based on the network structure (Figure 3) and link characteristics, Table 3 displays the available routes between the source R_1 and destination R_5 routers, along with their compromise probabilities.

Thus, based on the data in Table 2, the dependencies shown in Figure 2 apply to the example under study. Table 4 presents the calculation results for the TE routing models under analysis at a rate of $\lambda = 250$ packets per second and $n = 7$, simulating the routing of a single packet flow. For the Sec model, all packets were transmitted via the first route, as it was the most secure option among the available paths.

Based on the network structure (Figure 3 and Table 2), the flow rate of specific network links determines the packet flow rate on each route: link $E_{2,5}$ affects the first route (λ_1), link $E_{1,3}$ affects the second route (λ_2), link $E_{2,3}$ affects the third route (λ_3), and link $E_{2,4}$ affects the fourth route (λ_4).

Table 5 presents the calculated performance metrics for each routing model, highlighting load-balancing efficiency and aspects related to network security and quality of service. A comparative

Table 2
Link Characteristics

Link	$\varphi_{i,j}$	$p_{i,j}$
$E_{1,2}$	900	0.4
$E_{2,5}$	300	0.3
$E_{1,3}$	400	0.4
$E_{3,4}$	700	0.42
$E_{4,5}$	900	0.5
$E_{2,3}$	800	0.35
$E_{2,4}$	300	0.3

Table 3
Route Compromise Probability

Number	Path	Compromise Probability
1	$R_1 \to R_2 \to R_5$	0.58
2	$R_1 \to R_3 \to R_4 \to R_5$	0.826
3	$R_1 \to R_2 \to R_3 \to R_4 \to R_5$	0.8869
4	$R_1 \to R_2 \to R_4 \to R_5$	0.79

Table 4
Comparison of the Obtained Solutions for Secure TE Routing

Link	$\lambda_{i,j}^{TE}$	$\alpha_{i,j}^{TE}$	$\lambda_{i,j}^{SecTE}$	$\alpha_{i,j}^{SecTE}$	$\lambda_{i,j}^{NormSecTE}$	$\alpha_{i,j}^{NormSecTE}$
$E_{1,2}$	187.5	0.2083	214.0711	0.2379	196.2364	0.218
$E_{2,5}$	62.5	0.2083	143.6954	0.479	177.8086	0.5927
$E_{1,3}$	62.5	0.1563	35.9289	0.0898	53.7636	0.1344
$E_{3,4}$	145.8333	0.2083	35.9289	0.0513	72.1914	0.1031
$E_{4,5}$	187.5	0.2083	106.3046	0.1181	72.1914	0.0802
$E_{2,3}$	83.3333	0.1042	0	0	18.4278	0.023
$E_{2,4}$	41.6667	0.1389	70.3757	0.2346	0	0

analysis is provided for $n = 7$, aligning with the results shown in Table 5 for packet flow rates of $\lambda = 250$ pps and $\lambda = 200$ pps.

The comparative analysis (Table 5) shows that the Sec model prioritizes the most secure paths, limited by available bandwidth. The TE routing model focuses on improving QoS metrics (Figure 4), such as average end-to-end delay. In contrast, the SecTE (Figure 5) and NormSecTE (Figure 6) models balance both QoS and security (Table 5). Under the exponential link blocking model (9), link blocking intensifies as n increases (Figure 2), leading the SecTE and NormSecTE models to prioritize security. Conversely, as n decreases, QoS considerations gain importance in load balancing. The NormSecTE model achieved a higher level of network security than the SecTE or TE models, although with a slight trade-off in QoS.

The Sec model achieved the highest network security level ($p_{E2E}^{k} = 0.58$), while the TE model increased packet compromise probability by 34%. The SecTE and NormSecTE models offered intermediate security, increasing packet compromise probability by 15.83% and 13.4%, respectively. Although the TE model minimized average end-to-end delay (6.1 ms and 5.8 ms), the Sec model significantly increased it by 1.96 to 3.5 times. The SecTE and NormSecTE models resulted in moderate delay increases of 13.21% to 20.41% and 21.75% to 39.57%, respectively.

5. Discussion

The findings of this study highlight the critical role of integrating security considerations into Traffic Engineering routing models to enhance network resilience and performance. The proposed model

Table 5
Comparison of Routing Models Performance Metrics

Model	$\alpha_{\max}$	p_{E2E}	τ_{E2E} (ms)
	$\lambda = 250$ pps		
Sec	0.8333	0.58	21.5
TE	0.2083	0.7788	6.1
SecTE	0.479	0.6745	7.3
NormSecTE	0.5927	0.6555	8.5
	$\lambda = 200$ pps		
Sec	0.6667	0.58	11.4
TE	0.1667	0.7788	5.8
SecTE	0.3832	0.6745	6.6
NormSecTE	0.4742	0.6555	7.1

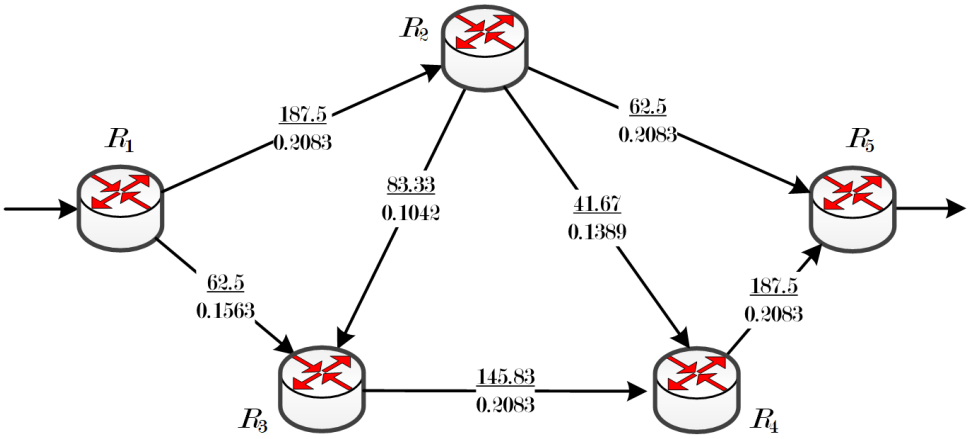

Figure 4: TE routing solution.

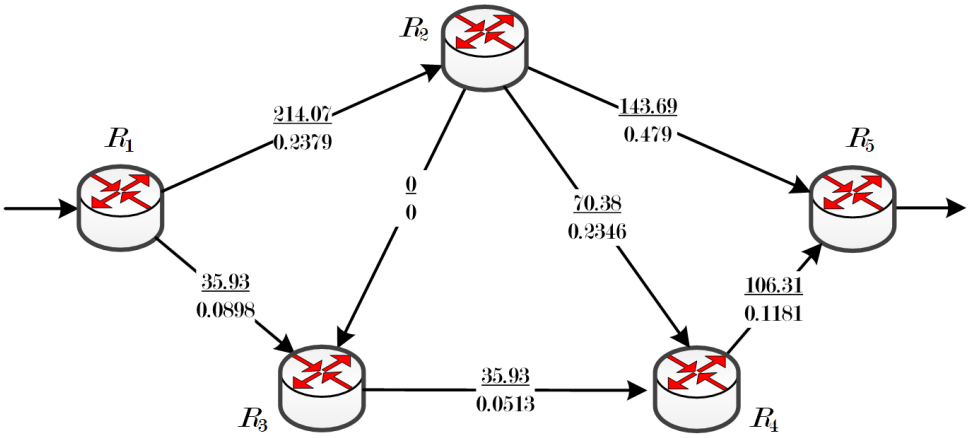

Figure 5: SecTE routing solution.

addresses traffic load balancing and secure routing challenges by extending the TE framework to incorporate network security parameters. This novel approach models secure routing under normalized link-blocking constraints, formulating an optimization problem as linear programming to ensure computational predictability and low demands on network devices. A key enhancement lies in modifying the exponential link-blocking model (9) to avoid inefficient resource use by preventing unnecessary blocking of secure links. Testing confirmed the model's efficacy in adapting routing based on network

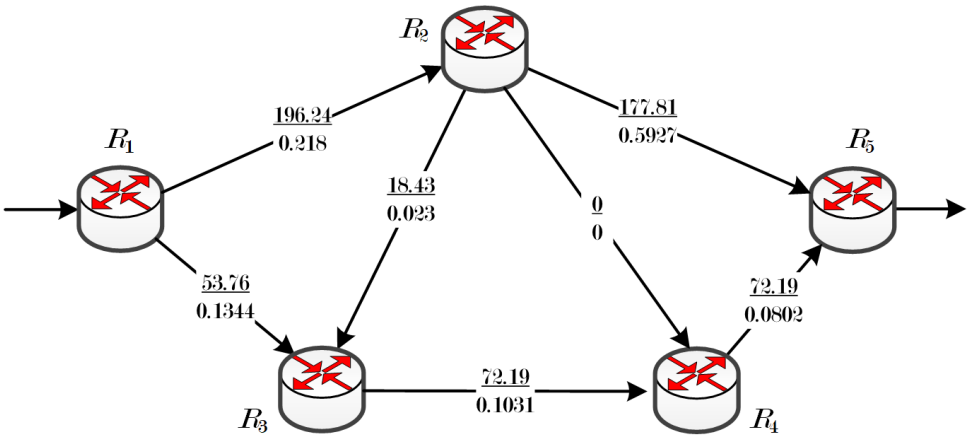

Figure 6: NormSecTE routing solution.

conditions, such as topology, link utilization, bandwidth, and compromise probability. The model effectively redistributes traffic away from high-compromise links, achieving a balanced load on secure links.

Comparative analysis of TE routing models revealed that, while the classical TE model optimizes link utilization and packet delay, it lacks any security provisions, resulting in a higher compromise probability. In contrast, the SecTE and NormSecTE models, particularly the latter, offer a balanced solution by integrating both security and quality of service requirements. Specifically, the NormSecTE model enhances network security by redistributing traffic to less vulnerable links, with a minor trade-off in packet delay. These findings underscore the importance of adopting security-aware routing strategies that protect network integrity without significantly impacting performance.

6. Conclusions

This research presents the NormSecTE model as a significant advancement in secure Traffic Engineering, integrating both QoS and security metrics within a single framework to enhance routing in softwarized networks. The model's linear programming formulation supports efficient computational processing, ensuring low resource demands while effectively prioritizing security in routing decisions. Comparative results highlight the limitations of conventional TE models, which, although optimized for performance metrics like delay and utilization, neglect critical security considerations. In contrast, the NormSecTE model reduces the probability of packet compromise through load balancing and traffic redistribution toward more secure links.

The study validates the NormSecTE model's effectiveness in balancing network performance and security and emphasizes the need for further research to expand its capabilities. Future work should incorporate a broader range of link-blocking models and explore diverse network topologies and compromise scenarios. These developments will strengthen the model's ability to address complex routing demands in softwarized networks, supporting a robust and secure infrastructure that balances QoS with enhanced security.

NormSecTE model offers valuable insights for the broader cybersecurity ecosystem. In case when security metrics are included in routing decisions, compromise prevention becomes an integral part of the logic behind routing, rather than an additional task requiring a separate solution. This approach can serve as the basis for designing cyber-resilient infrastructures with proactive cybersecurity logic. In this way, the NormSecTE model supports the development of secure-by-design networks, which are crucial to the growth and development of a robust cybersecurity ecosystem.

Acknowledgments

This paper was published due to work on the Erasmus+ Project Jean Monnet module "Integrating the future-proof EU cybersecurity ecosystem in Ukraine" Project No.: 101177024 – ERASMUS-JMO-2024-HEI-TCH-RSCH. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] S. A. Mohammed, A. L. Ralescu, Future internet architectures on an emerging scale—a systematic review, Future Internet 15 (2023) 166. doi:10.3390/fi15050166.

[2] M. D. Tache, O. Păscuțoiu, E. Borcoci, Optimization algorithms in sdn: Routing, load balancing, and delay optimization, Applied Science 14 (2024) 5967. doi:10.3390/app14145967.

[3] M. Ali, F. Naeem, G. Kaddoum, E. Hossain, Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions, IEEE Communications Surveys Tutorials 26 (2024) 1238–1278. doi:10.1109/COMST.2023.3347172, secondquarter.

[4] J. S. Al-Azzeh, M. A. Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10 (2017) 328–336. doi:10.15866/iremos.v10i5.12009.

[5] D. Medhi, K. Ramasamy, Network routing, Morgan Kaufmann, San Francisco, CA, USA, 2017.

[6] P. Gargano, S. Empson, CCNP and CCIE Enterprise Core CCNP Enterprise Advanced Routing Portable Command Guide, Cisco Press, Portable Resource, 2020.

[7] D. Savage, J. Ng, S. Moore, D. Slice, P. Paluch, R. White, Rfc 7868: Cisco's enhanced interior gateway routing protocol (eigrp), 2016. URL: https://datatracker.ietf.org/doc/html/rfc7868.

[8] Y. Xu, J. Liu, Y. Shen, X. Jiang, Y. Ji, N. Shiratori, Qos-aware secure routing design for wireless networks with selfish jammers, IEEE Transactions on Wireless Communications 20 (2021) 4902–4916. doi:10.1109/TWC.2021.3062885.

[9] C. Li, Y. Liu, J. Xiao, J. Zhou, Mceaaco-qsrp: A novel qos-secure routing protocol for industrial internet of things, IEEE Internet of Things Journal 9 (2022) 18760–18777. doi:10.1109/JIOT.2022.3162106.

[10] A. Pathak, I. Al-Anbagi, H. J. Hamilton, An adaptive qos and trust-based lightweight secure routing algorithm for wsns, IEEE Internet of Things Journal 9 (2022) 23826–23840. doi:10.1109/JIOT.2022.3189832.

[11] S. Soundararajan, R. Prabha, M. Baskar, T. J. Nagalakshmi, Region centric gl feature approximation based secure routing for improved qos in manet, Intelligent Automation Soft Computing 36 (2023) 267–280. doi:10.32604/iasc.2023.032239.

[12] A. Gehlot, S. Kumar, Trust-based safe qos routing in mobile ad hoc networks, in: 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing Communication Engineering (ICATIECE), Bangalore, India, 2022, pp. 1–6. doi:10.1109/ICATIECE56365.2022.10047396.

[13] A. Farrel, Rfc 9522: Overview and principles of internet traffic engineering, 2024. URL: https://datatracker.ietf.org/doc/rfc9522/.

[14] A. Wang, B. Khasanov, Q. Zhao, H. Chen, Rfc 8821: Pce-based traffic engineering (te) in native ip networks, 2021. URL: https://www.rfc-editor.org/rfc/rfc8821.html.

[15] Z. Hu, Y. Khokhlachova, V. Sydorenko, I. Opirskyy, Method for optimization of information security systems behavior under conditions of influences, International Journal of Intelligent Systems and Applications 9 (2017) 46–58. doi:10.5815/ijisa.2017.12.05.

[16] X. Yuan, Secure low-energy routing protocol based on dynamic trust awareness and load balancing in wireless sensor networks, Security and Communication Networks 6772435 (2023) 1–12. doi:10.1155/2023/6772435.

[17] U. Palani, G. Amuthavalli, V. Alamelumangai, Secure and load-balanced routing protocol in wireless sensor network or disaster management, IET Information Security 14 (2020) 513–520. doi:10.1049/iet-ifs.2018.5057.

[18] R. Cyriac, M. A. S. Durai, Lmh-rpl: a load balancing and mobility aware secure hybrid routing protocol for low power lossy network, International Journal of Pervasive Computing and Communications 20 (2022) 561–578. doi:10.1108/ijpcc-05-2022-0213.

[19] G. Thahniyath, M. Jayaprasad, Secure and load balanced routing model for wireless sensor networks, Journal of King Saud University - Computer and Information Sciences 34 (2022) 4209–4218. doi:10.1016/j.jksuci.2020.10.012.

[20] T. Selvan, P. Malathi, S. Freeda, An efficient method for adjustable load equalization for reducing traffic in routing for mobile ad hoc networks, Wireless Personal Communications 110 (2020) 2149–2164. doi:10.1007/s11277-019-06834-9.

[21] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, O. Baranovskyi, Complex investigation of the compromise probability behavior in traffic engineering oriented secure routing model in software-defined networks, in: M. Klymash, M. Beshley, A. Luntovskyy (Eds.), Future Intent-Based Networking, Lecture Notes in Electrical Engineering, volume 831, Springer, Cham, 2022, pp. 145–160. doi:10.1007/978-3-030-92435-5_8.

[22] O. Lemeshko, Z. Hu, A. Shapovalova, O. Yeremenko, M. Yevdokymenko, Research of the influence of compromise probability in secure based traffic engineering model in sdn, in: Z. Hu, S. Petoukhov, I. Dychka, M. He (Eds.), Advances in Computer Science for Engineering and Education IV. ICCSEEA Lecture Notes on Data Engineering and Communications Technologies, volume 83, Springer, Cham, 2021, pp. 47–55. doi:10.1007/978-3-030-80472-5_5.

[23] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, V. Lemeshko, M. Persikov, Analysis of secure routing processes using traffic engineering model, in: 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems, 2021, pp. 951–955. doi:10.1109/IDAACS53288.2021.9660980.

[24] O. Lemeshko, O. Yeremenko, A. Shapovalova, M. Yevdokymenko, S. O. Omowumi, A. M. Hailan, Secure routing with power link blocking model and load balancing, in: 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), Lviv, Ukraine, 2021, pp. 216–219. doi:10.1109/AICT52120.2021.9628938.

[25] O. Lemeshko, O. Yeremenko, A. Shapovalova, M. Yevdokymenko, A. Akulynichev, V. Porokhniak, Research of secure routing with load balancing and compromise probability behavior account, in: IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, Lviv, Ukraine, 2021, pp. 296–299. doi:10.1109/EUROCON52738.2021.9535642.

[26] O. Lemeshko, A. Persikov, O. Yeremenko, Secure aware traffic engineering routing in communication network, in: 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 2024, pp. 1–5.

[27] Y. Lee, Y. Seok, Y. Choi, C. Kim, A constrained multipath traffic engineering scheme for mpls networks, in: 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333), New York, NY, USA, 2002, pp. 2431–2436. doi:10.1109/ICC.2002.997280.