ASEAN
Journal of Scientific and Technological Reports
Online ISSN:2773-8752

Research article

A Comparative Study of OSPF Metrics in Routing Algorithms for Dynamic Path Selection in Network Security

Chakadkit Thaenchaikun[1], and Komsan Kanjanasit[2*]

[1] College of Computing, Prince of Songkla University Phuket Campus, Phuket, 83120, Thailand
[2] College of Computing, Prince of Songkla University Phuket Campus, Phuket, 83120, Thailand
* Correspondence: komsan.k@psu.ac.th

Citation:
Thaenchaikun, C.; Kanjanasit, K. A Comparative study of OSPF metrics in routing algorithms for dynamic path selection in network aecurity. *ASEAN J. Sci. Tech. Report.* **2025**, *28*(2), e256556. https://doi.org/10.55164/ajstr.v28i2.256556.

Article history:
Received: November 1, 2024
Revised: February 24, 2025
Accepted: March 12, 2025
Available online: April 1, 2025

Abstract: Open-path first (OSPF) algorithms optimize paths using shortest-path metrics, often overlooking security considerations and adaptability in dynamic network environments. Many OSPF implementations use fixed cost values that do not adapt to network conditions. Research is needed to develop adaptive cost functions that dynamically respond to security threats. This paper compares cost metrics in OSPF routing algorithms to evaluate their effectiveness in dynamic path selection within network security contexts. By incorporating diverse cost functions and assessing their performance across security conditions, this study seeks to identify metrics that evaluate performance. To achieve this, OSPF routing algorithms were analyzed using different cost metrics, including step, linear, and exponential functions. Through simulations, the algorithms were tested under a Barabási-Albert topology, from routine operations to threat-prone scenarios, to evaluate their capabilities in dynamic path selection and resilience against security threats. The numerical results highlight a trade-off among the step, linear, and exponential cost functions, with average delays of 0.553 ms, 0.653 ms, and 0.517 ms, respectively, and average jitters of 0.210 μs, 0.201 μs, and 0.205 μs. The packet delivery success (PDS) rates are also recorded at 87.64%, 86.76%, and 86.18% for the step, linear, and exponential cost functions, respectively. This approach facilitates an analysis aimed at balancing performance with security considerations.

Keywords: Open shortest path first; Routing algorithm network security; OSPF metric; OSPF cost

1. Introduction

The open shortest path first (OSPF) protocol is an interior gateway protocol (IGP) widely adopted for its efficient link-state routing capabilities in large IP networks [1]. Since its inception, OSPF has gained traction since its inception due to its hierarchical structure and ability to manage routing tables efficiently. OSPF uses Dijkstra's algorithm to calculate the shortest path for data packets, minimizing latency and improving network throughput. Although effective for performance, traditional OSPF lacks mechanisms to consider security in path selection, making it susceptible to attacks, especially in dynamic [2, 3]. As networks become more complex and exposed to security threats, relying on traditional shortest-path routing reveals vulnerabilities, such as exposure to man-in-the-middle and denial-of-service attacks. These limitations necessitate a reevaluation of cost metrics in OSPF to enhance adaptability and secure path selection without sacrificing performance.

The default cost metric in OSPF is often calculated based on link bandwidth or delay, assuming that the shortest path correlates with optimal performance. While this assumption holds in stable environments, it is less effective in scenarios with security threats. Based on minimum path cost, OSPF's static metric system may inadvertently route data through compromised nodes if those nodes are part of a shorter path [4]. Research shows that static metrics do not adapt to real-time network changes, such as node failures or attacks. Traditional OSPF metrics fail to account for compromised paths, potentially leading to significant security risks [5]. Therefore, exploring alternative cost metrics prioritizing secure paths alongside shortest-path metrics could reduce these risks and enhance network robustness in dynamic environments.

Adaptive routing addresses the limitations of dynamic routing by dynamically adjusting paths in response to changes in network conditions. Numerous studies explore adaptive routing in various protocols, including OSPF, to improve resilience against congestion and link failures [6]. Adaptive OSPF algorithms have shown the potential to enhance network stability under varying traffic loads and node availability. Dynamic path selection has also gained attention for applications in high-security settings. Adaptive routing mechanisms can significantly improve data flow in congested networks [7]. When applied to OSPF, dynamic path selection ensures that traffic is rerouted efficiently, especially in high-risk or congested networks. However, few studies have extended adaptive routing to include security-based metrics in OSPF, highlighting a gap in the literature.

The need for security-oriented metrics in routing protocols is well-documented, particularly in protocols like multiprotocol label switching (MPLS) and software-defined networking (SDN). Protocols incorporating trust-based or risk-sensitive metrics have shown promising results in securing paths and minimizing threat exposure [8–11]. These approaches dynamically assess paths based on security risks, enabling the routing protocol to avoid compromised nodes. Studies on mobile ad-hoc networks (MANETs) and vehicular ad-hoc networks (VANETs) have proposed trust-based routing models that select paths based on node reputation and historical reliability [12–15]. These security-driven models have demonstrated increased resilience to attacks in wireless and decentralized networks. Applying similar principles to OSPF could enhance network security, particularly in environments where nodes may be compromised or eavesdropping is a risk.

The related studies investigate secure network routing by leveraging traffic engineering principles to mitigate security risks [16, 17]. The proposed routing model integrates cost functions with traffic engineering strategies to enhance network performance while addressing security vulnerabilities. By optimizing traffic distribution and mitigating congestion at critical nodes, the model contributes to improved network stability. Additionally, the research highlights the significance of risk-aware mechanisms in secure routing, demonstrating their effectiveness in preventing network vulnerabilities. The works suggest that incorporating security-aware traffic distribution into routing decisions can enhance network resilience and reduce potential attack surfaces, ultimately strengthening overall network security and reliability.

Despite advancements in adaptive and security-driven routing, research on integrating such metrics into OSPF remains limited. While alternative protocols have successfully employed security-based metrics, studies on dynamic, security-sensitive cost functions in OSPF are sparse. Most security research in OSPF has focused on improving encryption and authentication mechanisms, with little exploration of dynamic cost adaptation. There is also a lack of research explicitly comparing the effectiveness of step, linear, and exponential cost functions within OSPF for high-security applications. Studies indicate potential for these models in other protocols, but comprehensive comparisons within OSPF are needed to validate their efficacy under varying network and security conditions. This research gap calls for further studies on security-enhanced OSPF models, particularly those that adapt to changing network threats.

This study is motivated by the limitations of OSPF's traditional cost metric, which is focused exclusively on the shortest path, particularly in high-risk environments. Static path selection based solely on distance or latency may expose data to insecure routes, significantly when nodes can be compromised. Network security issues can be mitigated by integrating security-focused metrics into the OSPF routing process, creating a need for a dynamic routing approach that adapts to changing security conditions by actively avoiding compromised nodes and routing data through more secure paths. This study addresses these

challenges by performing a comparative analysis of various cost metrics to enhance performance. The main objectives of this study include conducting a comparative analysis of different cost metrics in OSPF routing to assess their impact on performance and investigating the adaptability of these metrics under network conditions, including traffic loads, node compromises, and standard operations. The study aims to identify cost metrics supporting performance optimization and threat mitigation, contributing to a more resilient and secure OSPF-based routing model.

This work holds significance for network administrators, cybersecurity experts, and organizations reliant on secure data transmission. It contributes to advancements in secure networking by providing insights into how cost metrics can be tailored to balance performance with security concerns. The potential applications of this study are particularly relevant for critical infrastructure, government networks, and industries where secure data handling is essential. The findings could guide the development of adaptive OSPF algorithms more responsive to security risks, ultimately leading to a broader adoption of secure routing practices. The paper is organized as follows: Section 2 details the methodology, including the experimental setup, network simulation environment, selected cost metrics, and performance parameters. Section 3 presents the simulated results of analyzing the findings from computation under network conditions. Finally, Section 4 presents the conclusion, summarizing key findings and outlining potential research directions for integrating comparative metrics in OSPF routing.

2. Materials and Methods

This section describes the methodological framework used to compare cost metrics in OSPF routing algorithms for dynamic path selection within a network security context. The primary objective of this study is to evaluate the effectiveness of alternative cost metrics—specifically, step, linear, and exponential functions—in enhancing both performance and security in OSPF routing. The methodology involves setting up a simulated network environment to analyze the behavior of different OSPF cost metrics under various network conditions, including normal operation, high traffic, and security-compromised nodes. To accurately assess the impact of each cost function on network performance and security, the simulation environment was designed to mimic real-world network conditions. Multiple scenarios were created to measure the adaptability and resilience of each OSPF cost metric, analyzing metrics such as delay, maximum link utilization, and jitter. The study used network simulation tools, predefined network topologies, and specific evaluation metrics to compare each cost function's performance.

2.1 Network Simulation Environment and Tools

The network simulations were conducted in network simulator-3 (NS-3), an open-source tool that enables complex network configurations and testing in virtualized environments. NS-3 provides robust support for OSPF configurations and integrates real-world networking devices, which is essential for accurately simulating OSPF behavior under different cost metrics. NS-3 was used to simulate OSPF networks with varying topologies and scenarios, supporting close-to-reality simulation of OSPF routing. A network protocol analyzer was integrated within NS-3 to capture and analyze packet flows in real time, allowing for monitoring OSPF protocol behavior and packet handling under different cost metrics.

The network modeling was implemented with automation scripts to conduct specific simulations, introduce security threats such as node compromise, and extract relevant performance data. A network topology generator was created to simulate standard and Barabási-Albert topologies, commonly found in large-scale networks with high centrality. These topologies were programmatically generated to allow for reproducibility and variations in network scale. The network configuration consists of three main parts: First, the network scale included varying node counts of up to 26 nodes to observe the scalability of each OSPF cost metric. Second, network topology is based on the Barabási-Albert topology to simulate different levels of node centrality and path redundancy. Third, security conditions are that nodes were configured to represent compromised and secure states, allowing for a dynamic assessment of OSPF path selection in response to security changes.

2.2 Barabási-Albert Topology Setup

This study employs a Barabási-Albert topology to investigate network performance under security-focused routing conditions. The Barabási-Albert model, which is commonly used to represent scale-free networks, emphasizes high connectivity among a few core nodes (routers), reflecting realistic network structures often found in large-scale or corporate environments where certain nodes serve as central hubs. This model is particularly suitable for assessing network resilience and security because it inherently contains highly connected nodes that, if compromised, could significantly impact the network. The simulated network consists of 26 nodes, including 16 host nodes (H1 to H16) acting as edge nodes and 10 core nodes serving as routers. As shown in Figure 1, this topology is generated using the Barabási-Albert model and implemented in the NS-3 environment to evaluate the OSPF routing algorithm's performance accurately. NS-3 provides robust support for dynamic traffic flow and real-time analysis of delay and jitter, making it ideal for simulating network performance under security conditions.

The compromised nodes in the network are categorized into two risk levels—high risk and low risk—corresponding to different degrees of node compromise. These scenarios were modeled to reflect real-world conditions where network nodes may become malicious or vulnerable. High-risk nodes were modeled as nodes under significant adversarial control. They were configured to simulate harmful behaviors such as packet drops, where high-risk nodes dropped a substantial portion of incoming or outgoing packets. These nodes also introduced packet delays, intentionally forwarding packets with delays to degrade network performance. On the other hand, low-risk nodes were modeled to simulate limited vulnerabilities or minor compromises. While these nodes did not exhibit overtly malicious behavior, they could experience reduced performance due to vulnerabilities. For instance, minor packet losses or delays might occur due to partial compromise. Furthermore, low-risk nodes may act as intermediaries for high-risk nodes, potentially amplifying the overall risk to other network parts.

For traffic flow, four out of eight source hosts (H1 to H8) are selected to initiate traffic flows, sending data to destination hosts (H9 to H16). Each source sends traffic to four destinations, excluding directly adjacent nodes, ensuring a diverse spread of data transmission across the network. For example, nodes H1 to H4 send data traffic to nodes H13 through H16, ensuring traffic patterns that test different routing paths across the topology. Routers are assigned different risk levels to assess network security under realistic risk conditions. Specifically, Node 1 is designated as a high-risk router, while Node 2 and Node 3 represent low-risk nodes. This risk categorization allows the simulation to evaluate OSPF's adaptive cost metrics in routing traffic through secure paths, focusing on minimizing delay and jitter when rerouting around high-risk nodes. This Barabási-Albert topology simulation highlights how well each OSPF cost metric manages traffic in a security-sensitive network environment, balancing efficient routing with adaptive measures to bypass high-risk routers. The topology's emphasis on highly connected nodes presents a valuable framework for examining the network's resilience against potential security threats and the overall performance impact of different routing strategies on delay and jitter.

2.3 Proposed OSPF-Based Algorithm

This evaluation of the OSPF routing algorithm assesses performance across four distinct cost metrics—Legacy, Step, Linear, and Exponential cost functions—to determine their effectiveness in optimizing network security. Each cost function offers a unique approach to path selection: the Legacy metric focuses on shortest-path routing without dynamic adjustments, the Step function introduces threshold-based rerouting to manage load and security risks, the Linear function gradually adjusts costs for a balanced adaptation to traffic and threats, and the Exponential function rapidly increases costs with congestion or security risk to avoid high-risk paths. By comparing these cost functions, the study aims to identify which approach best supports efficient performance and enhanced network security in dynamic environments.

Figure 2 shows Algorithm 1, the Secure Routing Algorithm, which outlines a method for selecting secure paths based on pre-established cost metrics (step, linear, and exponential functions) while minimizing security risks. Initially, all links are active, and the total flows in the network are defined by $F = (f_1, f_2, \ldots, f_N)$. The algorithm establishes a path using pre-determined cost metrics (step, linear, or exponential) for each flow

and selects a secure path. $P_{xy}(i)$ between the source (x) and destination (y). Each link on the path is evaluated using the Kronecker delta function δ, depending on risk levels (high or low), which assigns a value of 1 if a link is part of the selected path and 0 otherwise. Links identified as security risks are deactivated (set to 0), while active links are maintained (set to 1). The algorithm iterates through all flows, updating the network state to avoid risky links.

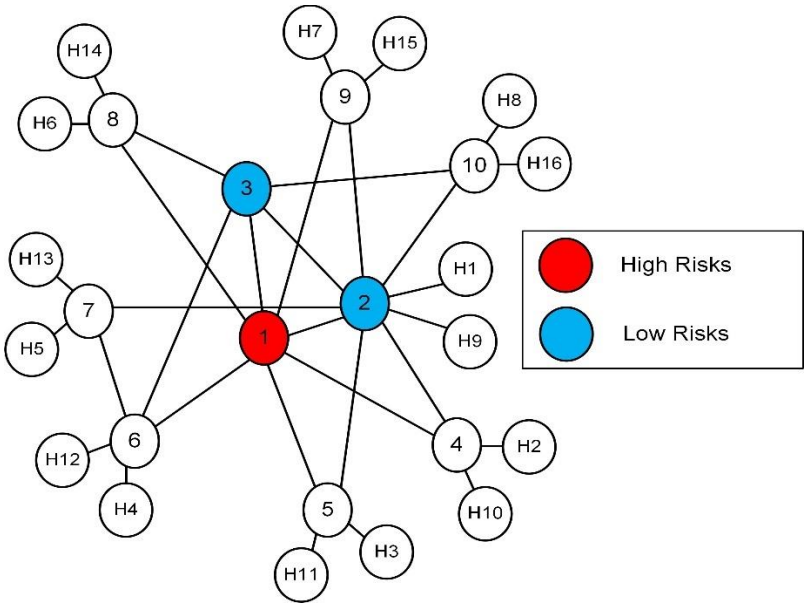

Figure 1. Barabási-Albert topology risk analysis with identifying high-risk and low-risk nodes.

Algorithm 1: Secure Routing Algorithm

$X = (1, 1, ..., 1) \rightarrow$ Initially all the link are active
$F = (f_1, f_2, ..., f_N) \rightarrow$ Total flows in Network = N
`/* Secure Costs and Selecting links to Security risk */`
for *each flow,* $f_i \in F(i = 1, 2, ..., N)$ **do**
  $S(i) \leftarrow$ Pre-established Path (calculate with STEP, LINER and EXP)
  $P_{xy}(i) \leftarrow$ Select Path (x,y) (denote Path between source (x) and destination (y)
  $P \leftarrow P_{xy}(i)$
  for *each link,* $l_k \in L(k = 1, 2, ..., N)$ **do**
    $X_k \leftarrow \delta(P_{xy}(i), l_k)$
    \\ Risk Links are selected by Kronecker delta function (δ).
    \\ Kronecker delta function returns 1 if the link k belong to $P_{xy}(i)$ and 0 otherwise.
    \\ keep active link = 1 and Security risk link =0 at $X_k \in X(k = 1, 2, ..., L)$
  end
  Update(X)
end

Figure 2. A secure routing algorithm for calculating paths using step, linear, and exponential function cost metrics.

2.4 Cost Metric Models

This study evaluates three primary cost function models in OSPF routing: the step, linear, and exponential functions—each with unique characteristics suited to different performance and risk requirements.

2.4.1 Step Cost Function

Figure 3 depicts the step-type OSPF cost function versus throughput percentage for two risk levels: high and low. The high-risk OSPF cost (red) follows a four-level step pattern, with significant cost increases at

approximately 25%, 50%, and 75% throughput, reaching the maximum cost of 100 at higher throughput levels. This stepped increase discourages routing through high-risk paths as the network load intensifies. In contrast, the low-risk cost (blue) follows a more gradual step pattern, with smaller increases at each level, ultimately reaching a lower maximum cost. This configuration incentivizes routing through lower-risk paths under higher throughput conditions, balancing performance and security considerations.

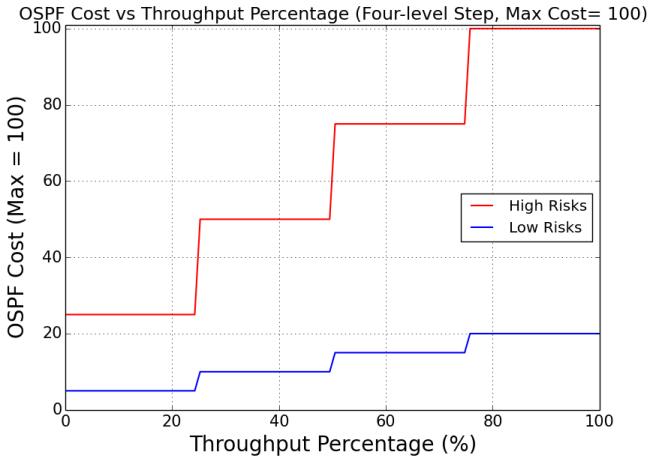

Figure 3. Step-type OSPF cost function versus throughput percentage for high-risk and low-risk paths.

2.4.2 Linear Cost Function

Figure 4 shows the linear-type OSPF cost function versus throughput percentage for two risk levels: high and low. The high-risk cost (red) increases linearly with the throughput percentage, reaching the maximum cost of 100 at 100% throughput. This linear growth indicates a proportional increase in routing cost as load rises, making high-risk paths progressively less favorable. In contrast, the low-risk cost (blue) also increases linearly but at a much lower slope, resulting in a modest rise in cost even at maximum throughput. This design encourages routing through lower-risk paths as network load increases, promoting balanced load distribution with a focus on security.

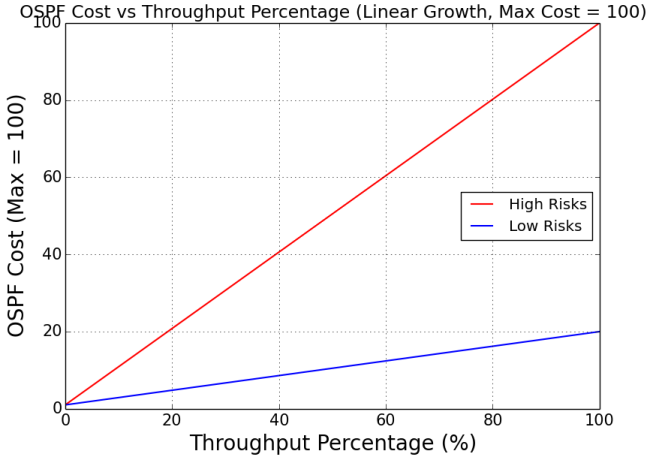

Figure 4. Linear-type OSPF cost function versus throughput percentage for high-risk and low-risk paths.

2.4.3 Eponential Cost Function

Figure 5 illustrates the exponential-type OSPF cost function versus throughput percentage for two risk characteristics: high risk and low risk. As the throughput percentage increases, the OSPF cost associated with high risk (red) rises sharply, reaching near the maximum value of 100 at higher throughput levels. This steep increase reflects a strategy to disincentivize routing through high-risk paths as the network load

intensifies. Conversely, the OSPF cost for low-risk (blue) increases gradually, remaining well below the maximum threshold even at high throughput percentages, thereby favoring low-risk paths under increased load conditions.

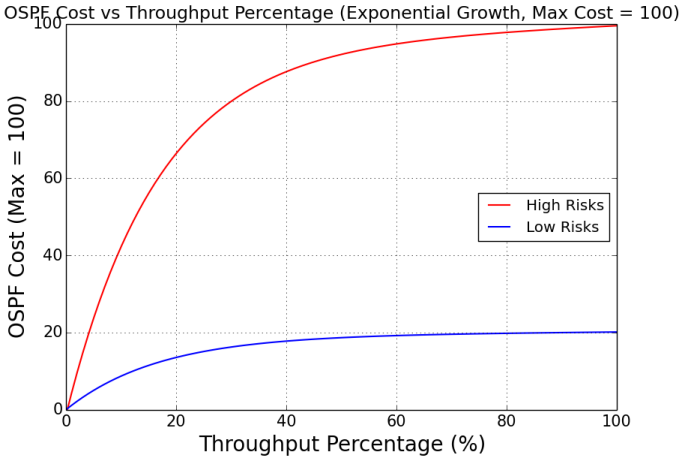

Figure 5. Exponential-type OSPF cost function versus throughput percentage for high-risk and low-risk paths.

Each cost function was simulated in separate instances, with results measured and compared to determine which model networking parameters with performance in dynamic network environments.

2.5 Experimental Scenarios

The experimental setup models node compromise by simulating delays, mean link utilization (MLU), and jitter. Security metrics, including packet delivery rate and success, are measured to evaluate network performance.

2.5.1 Normal Operation as Legacy

The normal operation as a legacy scenario represents a baseline OSPF routing environment with traditional cost metrics focused on shortest-path selection without adaptive security-focused adjustments. This setup allows for comparing the standard OSPF behavior and the enhanced scenarios with modified cost metrics designed to optimize security and performance. The network topology for this scenario is designed as A typical topology with 26 nodes, representing a balanced network without excessive complexity. This topology allows for redundancy in path selection and simulates a network structure commonly found in corporate or service provider environments. Nodes in the network represent routers with OSPF configurations connected by multiple links with standardized bandwidth and delay values. Links are assumed to be stable, with no link failures or intentional disruptions. OSPF is configured in its default settings, where path selection relies purely on shortest-path metrics calculated based on link bandwidth. The OSPF cost metric remains static, with no modifications or additional weighting factors for security. No adaptive routing strategies are applied, meaning routing tables are updated only in response to network topology changes (security risks).

2.5.2 Data-Rate Variation

The data rate variation scenario introduces incremental changes in network data rates to examine how different OSPF cost metrics (step, linear, and exponential functions) manage performance and security as network load fluctuates. This scenario assesses each cost function's effectiveness in dynamically balancing performance and security while handling increased traffic levels. In this scenario, four distinct data rates were used to simulate incremental increases in network load:

- At 100 Mbps as a low load, the network experiences a moderate load where no significant stress is applied. This rate allows for optimal path selection without congestion and serves as a baseline for each cost metric.

- At 300 Mbps as a moderate load, the load begins to push network capacity but should still maintain stability without substantial latency or jitter. This rate tests the cost functions' effectiveness in managing moderate data flow while minimizing path congestion.
- At 500 Mbps as a high load, network links are heavily utilized, nearing 50% of total link capacity. This rate evaluates each cost metric's handling of high-load conditions, where path selection should become more strategic to avoid congestion.
- At 700 Mbps as a very high load, the network approaches 70% of link capacity, challenging network stability and potentially leading to congestion on high-demand paths. Each cost metric is tested for its ability to manage traffic effectively under near-saturation, balancing latency and packet delivery against path security and stability.

2.6 Evaluation Metrics

Three key performance and security metrics were selected to measure the performance of each cost metric. These metrics provide insight into network behavior under varying conditions and help identify the balance between security and performance in dynamic path selection.

2.6.1 Average delay

Average delay, or latency, is measured from when a packet is sent from the source until it is received at the destination. Low latency is desirable in routing performance, as it ensures faster data delivery, improving user experience and real-time application efficiency. However, achieving low latency while maintaining secure paths can be challenging in high-security environments. This metric is crucial in comparing how each cost function handles the trade-off between latency and security. The average delay is calculated by averaging the total time taken by each packet to reach its destination across multiple simulation runs:

$$Average\ Delay = \frac{\sum_{i=1}^{N} Delay_i}{N} \tag{1}$$

Where N is the total number of packets and $Delay_i$ Represents the time taken by packet iii. Delay was measured using packet time-stamping at both source and destination points. Timestamp differences were recorded and averaged over the total packets in each scenario.

2.6.2 Average Link Utilization

Average link utilization is a measure of the bandwidth usage on network links. It indicates how much each link's capacity is used during data transmission. High link utilization is generally desirable as it indicates efficient use of network resources. However, excessive utilization can lead to congestion, delay, and packet loss. High link utilization must be balanced with secure path selection in security-sensitive routing to avoid routing through compromised nodes or congested links. Link utilization is calculated as a percentage of the link's bandwidth being used over time:

$$MLU\ (\%) = max\left(\frac{Traffic\ load\ on\ each\ Link}{Link\ capacity}\right) \times 100 \tag{2}$$

Average link utilization across all links in the network is then computed by taking the mean utilization across individual links:

$$Average\ MLU = \frac{\sum_{j=1}^{L} MLU_j}{L} \tag{3}$$

Where L is the total number of links in the network, link utilization was monitored during simulations using network monitoring tools within the NS-3 environment. Link utilization data were collected and averaged across simulation runs.

2.6.3 Average Jitter

Jitter refers to the variation in packet delay over time. Average jitter is calculated as the average change in delay between successive packets. It indicates the stability of the network in delivering packets with consistent timing, which is critical for applications. Maintaining low jitter is essential in a security-sensitive routing environment, especially for real-time services sensitive to delay variation. Excessive jitter can disrupt quality of service (QoS), leading to packet reordering or loss. Assessing jitter helps understand the impact of dynamic path selection on packet timing consistency. Average jitter is calculated by measuring the difference in delay between successive packets and averaging these values:

$$Jitter = \frac{\sum_{k}^{N-1} |Delay_{k+1} - Delay_k|}{N-1} \quad (4)$$

Where N is the total number of packets and $Delay_k$ Is the delay of packet k. Jitter was measured by time-stamping packets at their source and destination points. The variation in delay between successive packets was calculated and averaged for each scenario.

2.6.4 Packet Delivery Analysis

Packet analysis plays a crucial role in network security, with packet delivery rate (PDR) and packet delivery success (PDS) as key indicators of network integrity and reliability. A secure network must maintain high PDR and PDS by implementing robust security mechanisms to prevent packet interception, data loss, and cyberattacks. Monitoring these metrics helps detect security threats early, ensuring safe and efficient data transmission in enterprise and critical infrastructure networks.

PDR is the ratio of successfully received packets to the total number of packets sent within a network. In the security context, a low PDR could indicate packet interception, data manipulation, denial-of-service (DoS) attacks, or packet filtering by firewalls and intrusion detection systems (IDS). The formula for PDR is expressed as

$$PDR = \frac{Packet\ Receied}{Packet\ Sent} \quad (5)$$

PDS focuses on successfully transmitting critical or sensitive packets, ensuring essential data reaches its destination securely. While PDR measures overall packet transmission, PDS emphasizes the security and accuracy of data transmission, particularly in encrypted communication, financial transactions, and mission-critical applications. The formula for PDS is expressed as $PDS = PDR \times 100\%$

In this work, statistical analysis provides data from simulations analyzed using the NS-3 platform. The performance parameters were calculated for each cost metric model under each scenario. Statistical tests were conducted to determine significant differences among cost models. A comparative analysis was performed across all scenarios to identify the cost metric model suitable for balanced performance. Key comparisons included delay assessments, maximum link utilization (MLU), and jitter across varying data delivery rates. Analysis refers to visualizations created to illustrate differences across cost metrics. Key plots included line charts for the delay, MLU, and jitter at different data rates and bar charts for comparative analysis of network topology performance under different conditions.

3. Results

This section provides the results of simulating different OSPFs with varying cost metrics under a network model. The main goal was to evaluate the effectiveness of step, linear, and exponential cost functions in balancing network performance and security. Metrics such as average delay, maximum link utilization (MLU), and jitter were collected across scenarios to gauge each cost model's adaptability. The results demonstrate that each cost metric exhibits distinct strengths and weaknesses under various load conditions and security scenarios. The step function provided robust performance for handling abrupt network changes

but showed limited adaptability in high-load conditions. The linear function offered a balanced approach, maintaining consistent performance with gradual cost adjustments. In contrast, the exponential function proved highly sensitive to security risks but led to increased rerouting and higher latency in congested conditions. These findings provide insight into the suitability of each cost function for specific network security and performance requirements.

3.1 Delay Performance Analysis

Figure 6 displays the delay performance of four OSPF cost metrics—legacy, step, linear, and exponential—across different data rates: 100 Mbps, 300 Mbps, 500 Mbps, and 700 Mbps. At lower data rates (100 Mbps and 300 Mbps), the exponential and linear cost metrics show lower cumulative packet delays than the legacy and step metrics, indicating efficient traffic handling. As the data rate increases to 500 Mbps, the linear and exponential metrics outperform the legacy and step metrics in minimizing delay, maintaining more compact cumulative delay distributions. At the highest data rate of 700 Mbps, the linear metric achieves the lowest delay distribution, followed closely by the exponential metric, while the legacy metric shows the highest delays. Overall, this comparison highlights the superior adaptability of the linear and exponential cost metrics in reducing delay under increasing network load conditions.

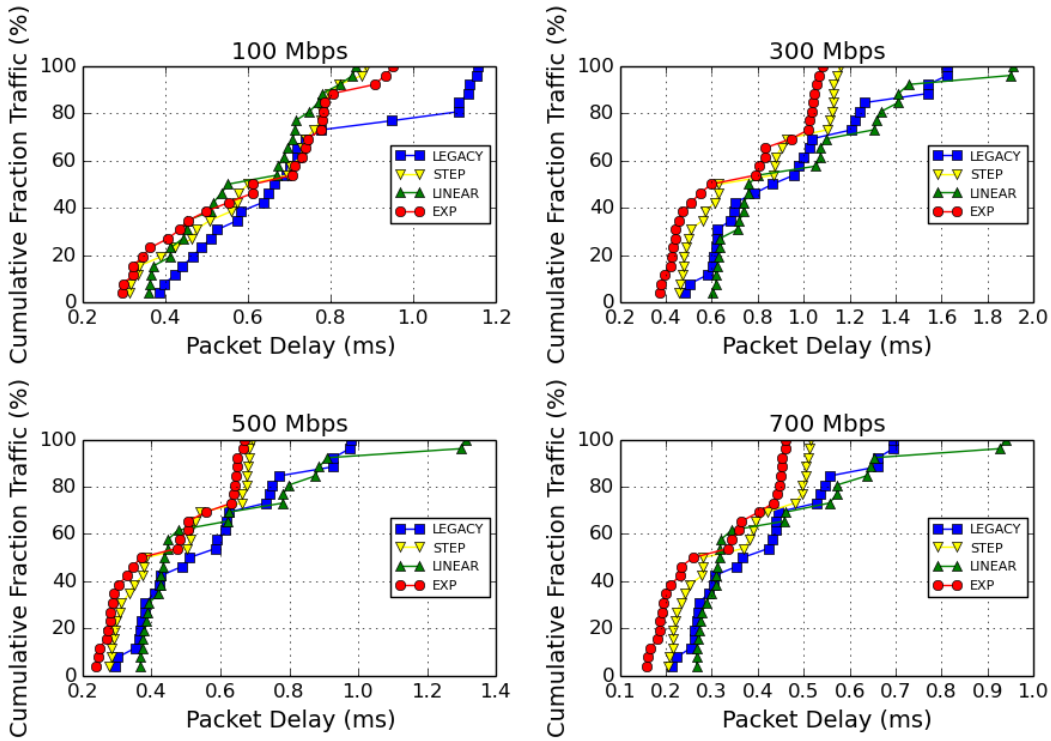

Figure 6. Cumulative fraction of traffic (%) versus packet delay (ms) for different traffic management approaches (Legacy, Step, Linear, Exponential cost functions) at varying bandwidth levels (100 Mbps, 300 Mbps, 500 Mbps, and 700 Mbps). Each subplot illustrates the impact of different strategies on packet delay distribution.

3.2 Maximum Link Utilization Performance Analysis

Figure 7 shows the maximum link utilization (MLU) performance of four OSPF cost metrics— legacy, step, linear, and exponential—across varying data rates: 100 Mbps, 300 Mbps, 500 Mbps, and 700 Mbps. At 100 Mbps, the step and exponential metrics demonstrate lower MLU than the legacy metric, which shows the highest utilization. As the data rate increases to 300 Mbps, the linear and exponential metrics maintain a more even distribution of MLU. In contrast, the Legacy metric exhibits higher utilization peaks, indicating less effective load balancing. At 500 Mbps, the linear and exponential metrics outperform the legacy and step

metrics by distributing traffic evenly across links, reducing MLU. Finally, at 700 Mbps, the linear metric achieves the most balanced MLU distribution, followed closely by the exponential metric, while the legacy and step metrics experience higher peaks. This analysis suggests that the linear and exponential metrics are better suited for efficient load distribution and minimizing MLU under increasing network load conditions.

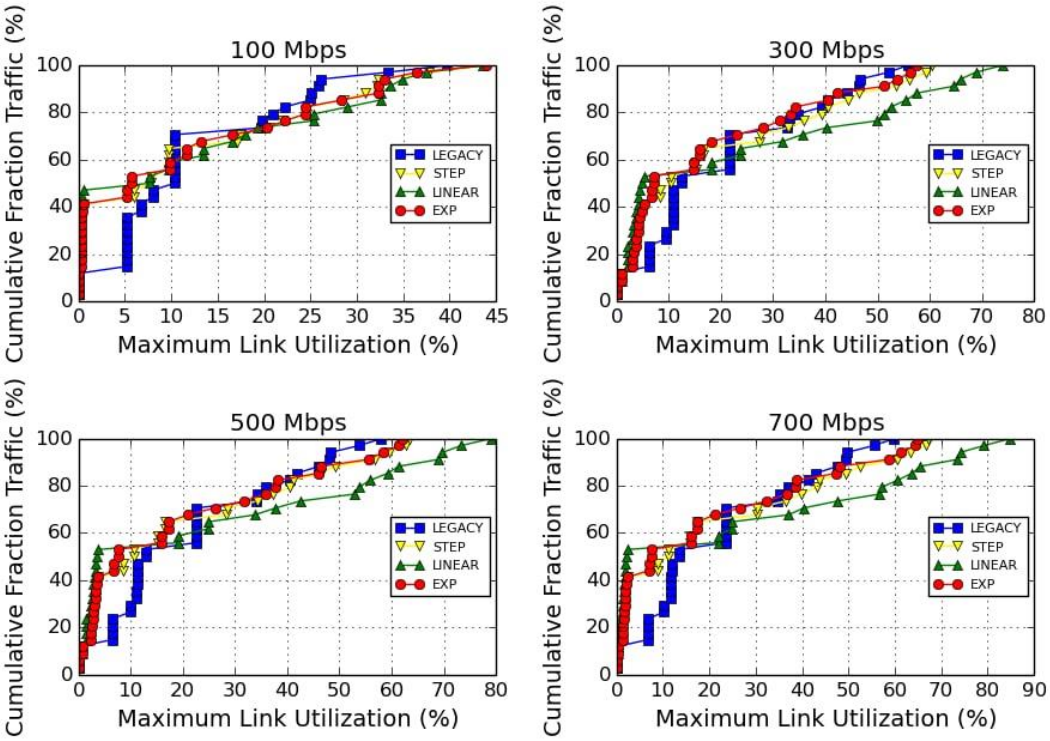

Figure 7. Cumulative fraction of traffic (%) versus maximum link utilization (%) for different traffic management approaches (Legacy, Step, Linear, Exponential cost functions) at varying bandwidth levels (100 Mbps, 300 Mbps, 500 Mbps, and 700 Mbps). Each subplot represents a different bandwidth setting, showing the impact of different strategies on link utilization distribution.

3.3 Jitter Performance Analysis

Figure 8 illustrates the jitter performance of four OSPF cost metrics— legacy, step, linear, and exponential—across varying data rates (100 Mbps, 300 Mbps, 500 Mbps, and 700 Mbps). At the lowest data rate of 100 Mbps, the exponential and linear metrics exhibit lower cumulative jitter values, while the legacy metric shows the highest jitter. As the data rate increases to 300 Mbps, the linear and exponential metrics outperform the legacy and step metrics, achieving lower jitter. At 500 Mbps, the linear metric maintains the most consistent jitter distribution, followed closely by the exponential metric, while the legacy metric remains the highest. Finally, at 700 Mbps, the linear metric shows the best jitter performance, with the exponential metric performing similarly, while the legacy and step metrics display greater jitter variability. This comparison demonstrates the superior capability of the linear and exponential metrics in managing jitter effectively across different network load conditions.

3.4 Average Delay Performance Comparison

Figure 9 compares the average delay performance of four cost metrics—legacy OSPF, step cost, linear cost, and exponential cost. The legacy OSPF model shows the highest delay at 0.664 ms, reflecting its limited adaptability under dynamic network conditions. The step cost function improves upon this with a reduced delay of 0.553 ms, benefiting from threshold-based adjustments. The linear cost function achieves a moderate delay of 0.653 ms, providing a balanced approach to load adaptation. The exponential cost function exhibits

the lowest delay at 0.517 ms, demonstrating its high sensitivity to congestion and load variations. The plot indicates that the exponential cost function is the most effective in minimizing delay, followed closely by the step cost function. In contrast, the legacy and linear cost functions show comparatively higher delay values.

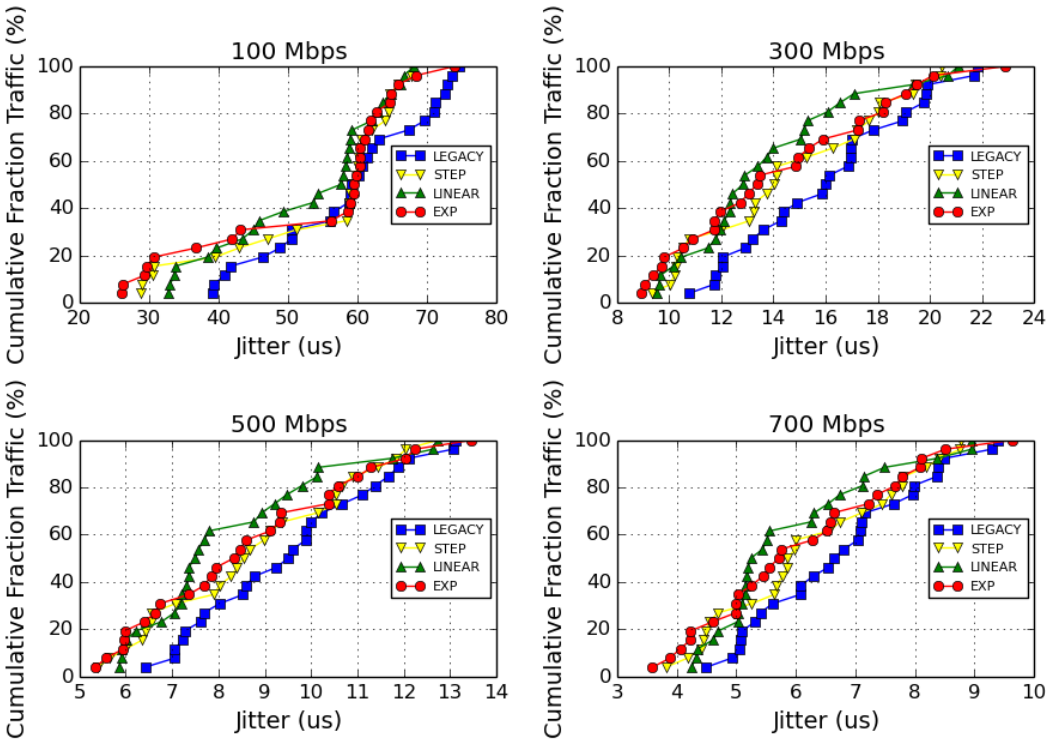

Figure 8. Cumulative fraction of traffic (%) versus jitter (μs) for different traffic management approaches (Legacy, Step, Linear, Exponential cost functions) at varying bandwidth levels (100 Mbps, 300 Mbps, 500 Mbps, and 700 Mbps). Each subplot illustrates the impact of different strategies on jitter distribution.

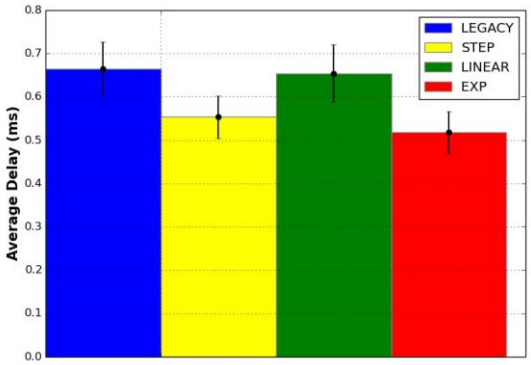

Figure 9. Average delay (ms) for traffic management approaches (Legacy, Step, Linear, Exponential cost functions). The bar chart compares the delay performance of each approach, highlighting variations in latency.

3.5 Average Maximum Link Utilization Performance Comparison

Figure 10 presents a comparative analysis of maximum link utilization (MLU) across four cost metrics—legacy OSPF, step cost, linear cost, and exponential cost—at Node 1, Node 2, and Node 3. For the legacy OSPF metric, MLU at Node 1 is highest, reaching 26.609%, while Nodes 2 and 3 show lower utilizations at 1.535% each. In contrast, Node 2, under the legacy OSPF metric, displays a peak MLU of 12.471%, followed

by utilization values of 23.362%, 28.491%, and 23.413% across the other cost functions. At Node 3, MLU is maximized with the linear cost function at 30.530%, while the legacy OSPF and step functions register lower utilizations of 4.929% and 21.533%, respectively. This plot highlights that while the linear and exponential cost functions effectively distribute the load more evenly across nodes, the legacy and step metrics show significant variations, with legacy OSPF consistently demonstrating lower adaptability across nodes, as shown by its high MLU concentration at specific nodes.

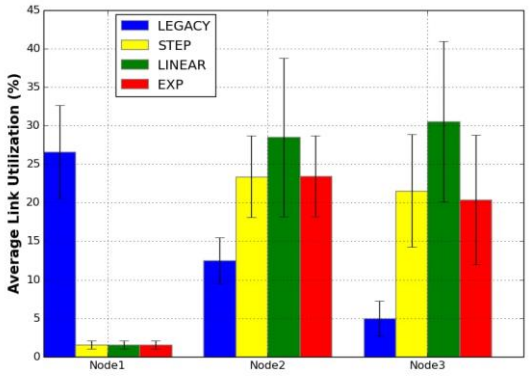

Figure 10. Average link utilization (%) across different nodes (Node1, Node2, Node3) for various traffic management approaches (Legacy, Step, Linear, Exponential cost functions). The bar chart illustrates the utilization distribution among the nodes, highlighting differences in traffic handling efficiency.

3.6 Average Jitter Performance Comparison

Figure 11 presents a comparative plot of jitter performance across four cost metrics: legacy OSPF, step, linear, and exponential. The legacy OSPF model exhibits the highest jitter at 0.227 μs, reflecting its dynamic routing approach that lacks adaptability to changing conditions. The step cost function reduces jitter to 0.210 μs through threshold-based adjustments, while the linear cost function achieves the lowest jitter at 0.201 μs, demonstrating smooth load adaptation. The exponential cost function presents a slightly higher jitter of 0.205 μs, indicating its sensitivity to congestion adjustments. Consequently, the linear cost function outperforms the other metrics in maintaining minimal jitter.

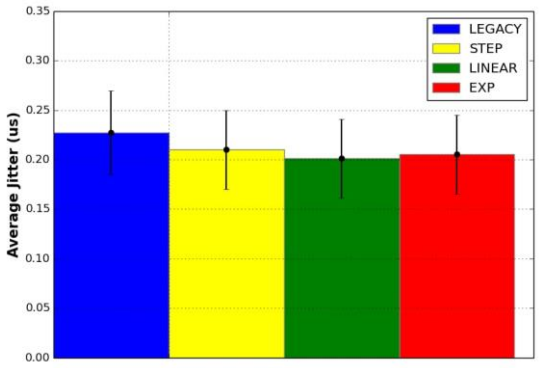

Figure 11. Average jitter (μs) for traffic management approaches (Legacy, Step, Linear, Exponential cost functions). The chart compares the jitter performance of each approach, illustrating variations in delay consistency.

3.7 Packet Delivery Analysis

Figure 12 illustrates the packet delivery success (PDS) of four network methods: legacy OSPF, step cost, linear cost, and exponential cost. Out of 2,500,000 packets sent, the legacy OSPF method demonstrates

the highest efficiency, successfully delivering approximately 1,999,595. In comparison, the step cost, linear cost, and exponential cost methods exhibit similar performance levels, delivering 1,752,473 packets (87.64%), 1,734,813 packets (86.76%), and 1,723,183 packets (86.18%), respectively, relative to the Legacy OSPF approach. These results highlight the superior reliability of the legacy OSPF method in packet transmission.

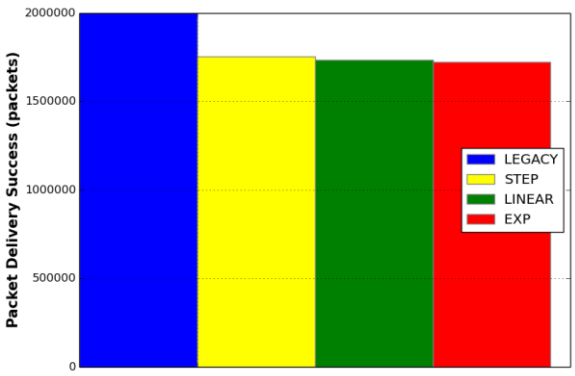

Figure 12. Packet delivery success (PDS) for traffic management approaches (Legacy, Step, Linear, Exponential cost functions). The chart compares the number of successfully delivered packets across the approaches, highlighting variations in reliability.

The comparative study of PDS highlights the inherent trade-off between performance and security. The PDS rate decreases as security measures become increasingly advanced, transitioning from step to exponential functions. This decline is primarily attributed to the increased network congestion and overtaxed devices introduced by these security mechanisms. This trade-off underscores the importance of tailoring routing protocols to meet specific network requirements. For applications where high performance is critical, configurations such as the legacy scheme or step cost function are more appropriate. Conversely, linear and exponential configurations are better suited for security-focused environments, where robust protection takes precedence over performance.

Figure 13 illustrates the number of packets arriving at a high-risk node (Node 1) under four routing configurations. The comparison focuses on the significant impact of routing strategies on the traffic load directed toward high-risk nodes, offering valuable insights into how security measures and optimization techniques influence network behavior. In the legacy configuration, approximately 1,305,800 packets arrive at the high-risk node, representing the highest traffic load among the configurations. This indicates that the legacy routing protocol does not employ mechanisms to mitigate risk or redistribute traffic, resulting in a significant dependence on high-risk nodes. In contrast, the step configuration drastically reduces the number of packets arriving at the high-risk node to 18,469. This sharp decline demonstrates the implementation of security measures aimed at distributing traffic evenly across the network and avoiding excessive reliance on high-risk nodes.

The linear configuration further reduces the number of packets arriving at the high-risk node to 18,446, comparable to the step configuration. This marginal improvement suggests using more refined optimization techniques, such as dynamic routing or advanced load-balancing strategies, to protect high-risk nodes further. Similarly, the exponential configuration directs 18,451 packets to the high-risk node, closely matching the results of the step and linear configurations. Exponential likely represents the most aggressive security model, incorporating advanced measures such as dynamic path randomization and sophisticated traffic analysis to enhance network resilience and mitigate risks to high-risk nodes. The results highlight the effectiveness of advanced routing strategies in reducing high-risk node dependency while emphasizing the importance of balancing security and performance in network design.

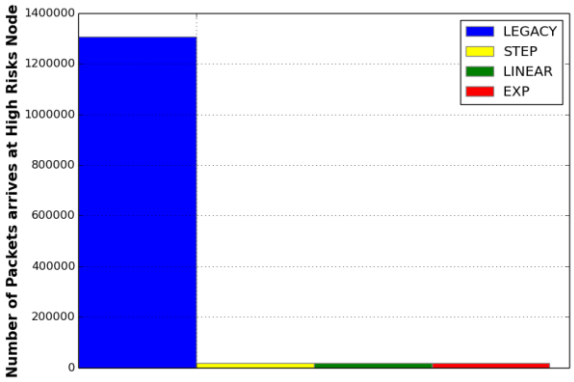

Figure 13. Number of packets arriving at high-risk nodes for different traffic management approaches (Legacy, Step, Linear, Exponential cost functions). The chart illustrates the distribution of packets reaching a high-risk node, showing the effectiveness of each approach in mitigating risk exposure.

4. Conclusions

This study evaluates the OSPF routing algorithm, explicitly analyzing how different cost metrics (legacy, step, linear, and exponential functions) perform under the Barabási-Albert network topology for security concerns. The analysis focused on key performance indicators: delay, MLU, and jitter, as these metrics are critical in ensuring efficient network operation and robustness against security threats. Each cost metric has unique characteristics that influence OSPF's routing behavior, adaptability to load changes, and response to potential risks within the network, particularly in dynamic traffic scenarios.

The legacy cost metric, which relies on traditional shortest-path routing based on bandwidth, serves as the baseline model for OSPF. This dynamic routing approach has shown stable delay, MLU, and jitter performance at lower data rates, such as 100 Mbps and 300 Mbps. Under these conditions, the legacy model maintained low delay, minimal jitter, and balanced link utilization. However, as data rates increased to 500 Mbps and 700 Mbps, the static nature of the legacy metric became a disadvantage. Without adaptive adjustments, the legacy model routed traffic along the same paths regardless of load, leading to congestion on primary links. This congestion caused delays to increase sharply, and jitter became more variable, especially under peak loads. The legacy metric's limitations in handling high data rates or changes in network load highlight its inadequacy in situations where dynamic adaptability and security considerations are essential.

The step cost function introduced threshold-based adjustments, providing OSPF with a more adaptable approach than the legacy model. By abruptly increasing the cost once traffic load or security risk reached predefined thresholds, the step function could reroute traffic more effectively to avoid congestion and compromised paths. The analysis showed that this threshold-based mechanism improved performance at moderate to high data rates (300 Mbps and 500 Mbps), where the step kept delay levels relatively stable by distributing traffic away from highly utilized links. In terms of MLU, the step function maintained a more balanced load distribution than the legacy metric, as it redirected traffic once threshold limits were breached. However, at very high loads (700 Mbps), the abrupt changes in cost led to fluctuations in delay and jitter as traffic rerouting became more frequent. This behavior makes the step function suitable for networks with moderate load conditions and security risks but less ideal for environments requiring consistent delay control and minimal jitter, as sudden adjustments can disrupt timing stability.

The linear cost function offers a gradual, proportional increase in cost based on rising link utilization or security risks, which allows for smoother traffic redistribution and more stable routing adjustments. This function was particularly effective across all data rates, from 100 Mbps to 700 Mbps, providing consistent delay and low jitter performance even under high load. The linear cost model maintained lower MLU by evenly spreading traffic across available paths, preventing any single link from becoming overly congested. The smooth, incremental adjustments in cost allowed the linear function to effectively balance performance

and security concerns, preventing drastic rerouting actions that could destabilize packet timing. With stable jitter and minimal delay fluctuations, the linear function emerges as the most effective option for networks that require dependable timing and efficient load handling. Its gradual adjustment mechanism makes it more robust in high-security environments, as it is less likely to cause abrupt path shifts that may expose data to compromised nodes.

The exponential cost function, designed to respond rapidly to congestion or security risks by exponentially increasing costs with utilization, demonstrated high sensitivity to both load and potential threats. At lower data rates (100 Mbps and 300 Mbps), the exponential function maintained low delay and minimal jitter, performing comparably to other models. However, as network load increased, this sensitivity led to frequent rerouting actions to avoid congestion or high-risk paths. This resulted in elevated jitter and variable delay at high data rates (500 Mbps and 700 Mbps), as the frequent path changes impacted packet timing stability. Despite these fluctuations, the exponential function proved highly effective in prioritizing secure path selection, as it rapidly redirected traffic away from compromised or heavily loaded links, enhancing network resilience in security-sensitive environments. The exponential function is, therefore, well-suited for networks where security is prioritized over performance stability, as its rapid adjustments make it highly responsive to security concerns, albeit with trade-offs in timing consistency under heavy load.

The comparative analysis of these four cost metrics reveals distinct strengths and weaknesses, particularly regarding delay, MLU, and jitter. While stable at lower loads, the legacy cost metric lacks the adaptability necessary for high-load or high-security scenarios. The step cost metric provides useful adaptability at moderate loads but introduces delay fluctuations at peak loads due to its abrupt adjustments. In contrast, the linear cost metric effectively balances delay, jitter, and MLU, proving reliable across varying loads by offering gradual adjustments without sudden rerouting, making it a strong choice for secure networks that also demand performance consistency. Lastly, the exponential cost metric is highly effective in security-sensitive contexts, with rapid rerouting actions that prioritize avoidance of congested or compromised paths. However, its aggressive adjustments can increase jitter and delay variability under high load, limiting its applicability where timing stability is a priority.

This analysis underscores the importance of selecting an appropriate cost metric based on specific network objectives and security needs. For environments where network performance consistency and low delay are paramount, the linear cost function emerges as the optimal choice. However, in networks where security risks are the primary concern, the exponential cost metric's rapid response to risk may offer enhanced protection at the expense of some timing stability. While effective in certain conditions, the legacy and step functions show limitations in high-load or security-sensitive scenarios, emphasizing the need for adaptive metrics in dynamic network environments.

Future research could build on these findings by exploring hybrid cost functions that combine elements of linear and exponential models, potentially balancing performance stability with security responsiveness. Additionally, real-world testing in diverse network environments would further validate these results and provide deeper insights into how adaptive OSPF cost metrics can enhance performance and security in modern, risk-sensitive networks.

5. Acknowledgements

The authors would like to thank the College of Computing, Prince of Songkla University, Phuket Campus, Thailand, for their support.

Author Contributions: Conceptualization, C.T. and K.K.; methodology, C.T. and K.K.; software, C.T.; validation, C.T. and K.K.; formal analysis, C.T. and K.K.; investigation, X.X.; writing—original draft preparation, K.K.; writing—review and editing, C.T. and K.K.; visualization, C.T. and K.K..; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Moy, J. OSPF: Anatomy of an internet routing protocol; Addison-Wesley, **1998**.

[2] Devir, N.; Grumberg, O.; Markovitch, S.; Nakibly, G. Topology-agnostic runtime detection of ospf routing attacks. *In Proceedings of the 2019 IEEE Conf. Commun. Netw. Secur. (CNS)*, Washington, DC, USA, **2019**, 277–285. https://doi.org/10.1109/CNS.2019.8802826.

[3] Meredith, R.; Dutta, R. Increasing Network Resilience to Persistent OSPF Attacks. *In Proceedings of the 2019 IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, **2019**, 1–7. https://doi.org/10.1109/ICC.2019.8761838.

[4] Nakibly, G.; Sosnovich, A.; Menahem, E.; Waizel, A.; Elovici, Y. OSPF Vulnerability to Persistent Poisoning Attacks: A Systematic Analysis. *In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14)*, New York, NY, USA, **2014**, 336–345. https://doi.org/10.1145/2664243.2664278.

[5] Al-Musawi, B.; Branch, P.; Hassan, M. F.; Pokhrel, S. R. Identifying OSPF LSA Falsification Attacks through Non-linear Analysis. *Comput. Netw.*, **2020**, 167, 107031. https://doi.org/10.1016/j.comnet.2019.107031.

[6] Basu, A.; Riecke, J. Stability Issues in OSPF Routing. *ACM SIGCOMM Comput. Commun. Rev.*, **2001**, *31*(4), 225–236. https://doi.org//10.1145/964723.383077.

[7] Rétvári, G.; Németh, F.; Chaparadza, R.; Szabó, R. OSPF for Implementing Self-adaptive Routing in Autonomic Networks: A Case Study. *In Modelling Autonomic Communications Environments, Strassner, J. C.; Ghamri-Doudane, Y. M., Eds.; Lecture Notes in Computer Science; Springer: Berlin, Heidelberg*, **2009**, *5844*, 78-89. https://doi.org/10.1007/978-3-642-05006-0_6.

[8] Bahnasse, A., Louhab, F.E., Khiat, A., Badri, A., Talea, M., and Pandey, B. Smart Hybrid SDN Approach for MPLS VPN Management and Adaptive Multipath Optimal Routing. *Wireless Pers Commun*., **2020**, *114*, 1107–1131, https://doi.org//10.1007/s11277-020-07411-1

[9] Mehraban, S.; Yadav, R. K. Traffic Engineering and Quality of Service in Hybrid Software Defined Networks. *China Commun.,* **2024**, *21*(2), 96–121. https://doi.org/10.23919/JCC.fa.2022-0860.202402

[10] Yazdinejad, A.; Parizi, R. M.; Dehghantanha, A.; Srivastava, G.; Mohan, S.; Rababah, A. M. Cost Optimization of Secure Routing with Untrusted Devices in Software Defined Networking. *J. Parallel Distrib. Comput.,* **2020**, *143*, 36–46, https://doi.org//10.1016/j.jpdc.2020.03.021.

[11] Bi, Y.; Han, G.; Lin, C.; Peng, Y.; Pu, H.; Jia, Y. Intelligent Quality of Service Aware Traffic Forwarding for Software-Defined Networking/Open Shortest Path First Hybrid Industrial Internet. *IEEE Trans. Ind. Inform.* **2020**, *16*(2), 1395–1405. https://doi.org/10.1109/TII.2019.2946045.

[12] Ramkumar, J., Vadivel, R. Multi-Adaptive Routing Protocol for Internet of Things based Ad-hoc Networks. *Wireless Pers Commun.,* **2021**, *120*, 887–909. https://doi.org/10.1007/s11277-021-08495-z

[13] Singh, K.; Moh, S. Routing Protocols in Cognitive Radio Ad Hoc Networks: A Comprehensive Review. *J. Netw. Comput. Appl*., **2016**, 72, 28–37. https://doi.org/10.1016/j.jnca.2016.07.006.

[14] Mahamune, A. A.; Chandane, M. M. Trust-Based Co-operative Routing for Secure Communication in Mobile Ad Hoc Networks. *Digit. Commun. Netw.,* **2024**, *10*(4), 1079–1087. https://doi.org/10.1016/j.dcan.2023.01.005.

[15] Manivannan, D.; Moni, S. S.; Zeadally, S. Secure Authentication and Privacy-Preserving Techniques in Vehicular Ad-hoc Networks (VANETs). *Vehic. Commun.*, **2020**, *25*, 100247. https://doi.org/10.1016/j.vehcom.2020.100247.

[16] Lemeshko, O.; Yevdokymenko, M.; Shapoval, M. Routing Model with Load Balancing on the Traffic Engineering Principles based on Information Security Risks. *In Proceedings of IEEE Int. Conf. Probl. Infocommun. Sci. Technol. (PIC S&T),* Kharkiv, Ukraine, **2021**, 572–576. https://doi.org/10.1109/PICST54195.2021.9772193.

[17] Lemeshko, O.; Yeremenko, O.; Yevdokymenko, M.; Shapovalova, A.; Lemeshko, V.; Persikov, M. Analysis of Secure Routing Processes Using Traffic Engineering Model. *In Proceedings of the IEEE Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. (IDAACS*), Cracow, Poland, **2021**, 951–955. https://doi.org/10.1109/IDAACS53288.2021.9660980.