

Article

Performance Analysis of Sigmoid-Enhanced OSPF for Risk-Aware Adaptive Routing in Secure Networks

Chakadkit Thaenchakun and Komsan Kanjanasit * 

College of Computing, Prince of Songkla University, Phuket Campus, Phuket 83120, Thailand;
chakadkit.th@phuket.psu.ac.th

* Correspondence: komsan.k@psu.ac.th

Abstract

Modern communication networks require routing protocols that can adapt to dynamic traffic conditions while accounting for topology-based structural risk. Conventional open shortest path first (OSPF) relies on static or linear link cost metrics, which are often inadequate for capturing the nonlinear behavior of network dynamics and structural risk. This paper proposes sigmoid-enhanced OSPF (SE-OSPF), which integrates topology-based structural risk into the OSPF routing metric through a nonlinear sigmoid function. The proposed framework employs two configurable sigmoid parameters, the midpoint (x_0) and the steepness (k), to provide smooth cost transitions and adaptive routing decisions under varying network conditions. Simulation results on a Barabási–Albert scale-free topology demonstrate that SE-OSPF reduces the average end-to-end delay by 19.7% and packet jitter by 8.6% compared with Standard OSPF. In addition, SE-OSPF increases the average number of successfully delivered packets by up to 16.6% compared with Linear-OSPF while reducing maximum link utilization (MLU), indicating more balanced traffic distribution, improved load balancing, and reduced congestion. These results demonstrate that the proposed sigmoid-based routing metric effectively balances routing efficiency, packet delivery reliability, and network load distribution, establishing SE-OSPF as an effective framework for topology-based structural risk-aware adaptive routing in modern communication networks.

Keywords: sigmoid-enhanced OSPF; topology-based structural risk; adaptive routing; risk-aware routing; nonlinear routing metric

1. Introduction

The rapid expansion of the Internet of Things (IoT) and cyber-physical systems (CPSs) has led to increasingly complex network environments. These systems operate over dynamic, bandwidth-constrained communication networks, where maintaining reliable and efficient data delivery remains a significant challenge due to frequent topology changes, fluctuating link conditions, and the structural importance of critical network nodes. Such conditions can degrade routing performance and network reliability, highlighting the need for adaptive routing mechanisms that account for topology-based structural risk while maintaining efficient communication under dynamic network conditions [1–3].

Open shortest path first (OSPF) is one of the most widely used intra-domain routing protocols due to its scalability, deterministic behavior, and fast convergence [4]. It is widely deployed in enterprise, industrial, and emerging IoT networks. However, conventional OSPF relies on static, hop-based or bandwidth-derived link cost metrics that are not



Academic Editor: Pingyi Fan

Received: 27 May 2026

Revised: 4 July 2026

Accepted: 8 July 2026

Published: 10 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

well suited to dynamic and heterogeneous network environments. These limitations become more pronounced in scale-free network topologies, where the presence of highly connected hub nodes increases structural vulnerability and can significantly affect routing performance under node or link failures.

Recent research has explored enhancements to OSPF through trust-aware routing, anomaly detection, and traffic engineering (TE) techniques. For example, trust-aware routing frameworks have been proposed to improve routing decisions by incorporating node trust into Dijkstra's algorithm [5,6]. Machine learning approaches have also been developed to detect OSPF-specific attacks, such as link-state advertisement (LSA) falsification [7,8]. In parallel, TE-based methods have incorporated risk indicators and load-balancing mechanisms to improve routing robustness under dynamic network conditions [9–12].

Recent studies have explored adaptive routing in various ad hoc network environments. A survey of vehicular ad hoc networks (VANETs) highlights the importance of privacy, authentication, and secure communication mechanisms [13]. Adaptive routing protocols, such as the adaptive context-aware VANET routing (ACAVR) protocol, improve routing performance by exploiting mobility and traffic context [14]. In mobile ad hoc networks (MANETs), trust-based protocols such as TSDR and TCOR enhance routing decisions by detecting misbehavior and incorporating trust information [15]. Similarly, routing in cognitive radio ad hoc networks (CRAHNS) must adapt to dynamic spectrum availability and interference. Recent studies have also emphasized energy-efficient adaptive routing [16], while the MARP protocol improves IoT network performance by reducing delay and extending network lifetime [17].

Despite recent advances, many routing protocols still rely on fixed thresholds or static routing metrics, limiting their adaptability to dynamic network conditions. Most existing approaches lack smooth, real-time cost adaptation, and the use of nonlinear functions, such as sigmoid models, remains limited. Although adaptive routing has been widely studied in reactive protocols such as AODV, its application to proactive protocols, particularly OSPF, remains relatively unexplored.

1.1. Research Gap

Recent research has improved OSPF by incorporating adaptive routing metrics based on quality of service (QoS) indicators, including delay and congestion. Motivated by the smooth transition characteristics of sigmoid functions, our earlier work [18] introduced a sigmoid-based routing metric for QoS-aware optimization. Extending this approach, the proposed sigmoid-enhanced OSPF (SE-OSPF) framework integrates topology-based structural risk into a nonlinear sigmoid-based cost model to enable adaptive, risk-aware routing. By jointly employing the midpoint (x_0) and steepness (k) parameters, SE-OSPF enables adaptive, risk-aware routing while preserving compatibility with the conventional OSPF protocol. The primary application of the proposed framework is risk-aware routing, whereas the previous study focused on performance optimization. The key differences are summarized in Table 1.

Table 1. Comparison between the previous sigmoid-based OSPF study [18] and the proposed SE-OSPF framework.

Aspect	Previous Work [18]	This Work
Objective	Sigmoid routing metric	Risk-aware SE-OSPF
Routing input	QoS metrics	Structural risk (R_{ij})
Risk model	None	BA topology
OSPF	Metric evaluation	Risk-aware cost
Parameters	k	k, x_0

1.2. Objective

The objective of this study is to develop a SE-OSPF framework that incorporates topology-based structural risk into OSPF routing using a nonlinear sigmoid-based cost metric. The proposed framework aims to enhance adaptive routing by jointly considering node importance and network performance while maintaining compatibility with the conventional OSPF protocol. The effectiveness of the proposed approach is validated through NS-3 simulations on Barabási–Albert scale-free network topologies using end-to-end delay, jitter, packet delivery success (PDS), and maximum link utilization (MLU) as performance metrics.

1.3. Contributions

The main contributions of this work are summarized as follows:

1. We develop a topology-based structural risk model for Barabási–Albert scale-free networks and integrate it into OSPF cost computation.
2. We introduce a sigmoid-based adaptive routing mechanism that enables topology-aware path selection through configurable midpoint (x_0) and steepness (k) parameters.
3. We investigate the effects of the sigmoid parameters on routing performance under different network traffic conditions.
4. We implement the proposed framework in NS-3 and evaluate its performance using end-to-end delay, jitter, MLU, and PDS, demonstrating improved performance over Standard OSPF and Linear-OSPF.

2. Literature Review

Enhancing OSPF for dynamic, large-scale, and risk-sensitive networks has been extensively studied, encompassing adaptive metrics, trust-aware routing, traffic engineering, SDN- and quantum-assisted OSPF variants, and diverse performance evaluation frameworks. This section reviews and categorizes the most relevant contributions.

2.1. Adaptive Metric Designs in OSPF

Traditional OSPF employs static routing metrics based on link bandwidth or hop count, which are often inadequate for dynamic network environments. To address this limitation, several studies have proposed adaptive cost models. For example, an inverse coupled simulated annealing (ICSA) approach was developed to optimize Hello intervals and improve convergence in large-scale OSPF-based IoT networks [19]. Other studies have investigated step, linear, and exponential cost functions to enhance routing performance under varying traffic conditions [20]. In addition, OSPF has been modeled as a self-adaptive system in which mechanisms such as Hello packet exchange and link-state advertisement (LSA) flooding form a feedback control loop for adaptive route computation [21].

2.2. Trust-Based and Secure Routing Enhancements

Several studies have incorporated trust metrics into routing decisions to improve routing robustness. For example, modified Dijkstra algorithms have been proposed to prioritize trusted nodes in OSPF networks [5,6]. Similarly, trust-aware routing protocols, including CONFIDANT [22], Ariadne [23], and SEAD [24], have been developed for AODV- and DSR-based networks to identify and isolate misbehaving nodes.

More recently, anomaly detection techniques have been investigated for OSPF, particularly to identify falsified link-state advertisements (LSAs). These approaches include machine learning-based detection models [7,8] and formal model-checking techniques [25]. However, these methods typically operate independently of the routing process and do not directly integrate detection results into adaptive OSPF cost computation.

2.3. Secure-Aware Traffic Engineering

Traffic engineering (TE) models that incorporate risk-related metrics have also been investigated. For example, flow-based TE models have been extended to consider link compromise probabilities, confidentiality requirements, and traffic class sensitivity [11,12]. These approaches improve routing robustness by diverting traffic away from high-risk paths. However, they typically rely on static thresholds or binary link-blocking mechanisms and do not provide continuous cost adaptation in response to varying risk levels.

2.4. Hybrid SDN-OSPF and Control Plane Extensions

The emergence of software-defined networking (SDN) has enabled hybrid control frameworks that combine centralized SDN controllers with distributed OSPF routers. Studies have shown that hybrid SDN-OSPF architectures improve path management and traffic optimization while preserving existing network infrastructure [26–29]. However, these frameworks generally rely on conventional routing cost models and do not incorporate topology-based structural risk-aware adaptive routing metrics.

2.5. Quantum and Risk-Aware OSPF

The evolution of OSPF toward quantum networking has motivated the development of routing metrics that extend beyond conventional bandwidth-based costs. Previous studies have shown that routing in quantum key distribution (QKD) networks should consider key generation rate to prevent rapid key depletion [30].

More recently, QKD-enabled OSPF architectures have introduced dynamic, key-aware link cost metrics to support distributed and scalable quantum key relay without centralized control [31]. These studies demonstrate the growing importance of adaptive routing metrics and motivate the development of nonlinear cost models that improve routing adaptability under dynamic network conditions.

2.6. Complementary Approaches in OSPF Evolution

OSPF-ICSA [19], QKD-enabled OSPF [31], and the proposed SE-OSPF all extend the conventional OSPF protocol but address different aspects of routing, making them complementary approaches. OSPF-ICSA improves convergence by optimizing control-plane timing without modifying routing costs, whereas QKD-enabled OSPF incorporates quantum key availability into the routing metric to support key relay in QKD networks. In contrast, SE-OSPF integrates topology-based structural risk into the OSPF routing metric through a nonlinear sigmoid-based cost function, enabling adaptive path selection under dynamic network conditions.

As summarized in Table 2, these approaches enhance OSPF at different levels, including control-plane optimization, quantum resource awareness, and routing metric adaptation. Unlike the other approaches, SE-OSPF directly adapts routing costs according to topology-based structural risk, improving end-to-end delay, packet delivery success, jitter, and maximum link utilization without requiring additional protocol messages or specialized hardware.

Table 2. Comparison of OSPF-ICSA, QKD-Enabled OSPF, and SE-OSPF.

Aspect	OSPF-ICSA	QKD-Enabled OSPF	SE-OSPF (This Work)
Primary Goal	Fast convergence	Quantum key relay	Risk-aware routing
Optimization Layer	Control-plane timing	Key-resource routing	Routing metric adaptation
Secure Basis	Reliability	QKD cryptography	Network-layer risk awareness

Table 2. *Cont.*

Aspect	OSPF-ICSA	QKD-Enabled OSPF	SE-OSPF (This Work)
Routing Resource	Hello/dead intervals	Key pool and SKR	Risk indicators
Metric Modification	No cost change	Discrete key thresholds	Continuous sigmoid cost
OSPF Integration	Hello interval tuning	QKD-specific LSAs	Standard LSAs, cost only
Path Selection	Shortest path	Avoid low-key links	Avoid high-risk paths
Performance Focus	Convergence time	Key sustainability	Delay, jitter, utilization, PDS
Hardware	None	QKD hardware	None
Key Limitation	No risk awareness	High cost	Risk modeling accuracy

2.7. Simulation, Emulation, and Evaluation Tools

Several platforms support the evaluation of routing protocol performance, including GNS3, OPNET, and the SEED Internet Emulator [32–35]. These tools are widely used to evaluate routing performance, including topology convergence, delay, and packet loss. Some studies have also employed these platforms to investigate OSPF performance under different network conditions [10]. However, there is currently no evaluation framework specifically designed for sigmoid-based adaptive routing in OSPF or for topology-based structural risk-aware routing in scale-free networks. Therefore, this study employs the Barabási–Albert (BA) model to represent realistic scale-free network topologies with highly connected hub nodes.

The BA model is well suited for analyzing topology-based structural risk because highly connected hub nodes play a critical role in maintaining network connectivity. Owing to these characteristics, the BA model has been widely adopted for network resilience analysis and topology-aware routing studies. Tools and frameworks such as BAT [36], LineageBA [37], and EvoCut [38] utilize BA-based topologies to analyze network connectivity, identify structurally important nodes, and evaluate network robustness. In this work, the BA model is used to simulate scale-free IoT networks, analyze node connectivity, and derive topology-based structural risk indicators for adaptive routing.

3. Materials and Methods

3.1. Topology-Based Structural Risk Model

The proposed SE-OSPF framework employs a Barabási–Albert (BA) scale-free topology to model realistic communication networks. Owing to the preferential attachment mechanism, BA networks naturally comprise a small number of highly connected hub nodes and many sparsely connected peripheral nodes, reflecting the structural characteristics of many real-world communication networks. In this study, topology-based structural risk denotes the relative importance of a node within the network topology rather than its probability of being compromised. Consequently, hub nodes are assigned higher structural risk because their failure or overload can have a greater impact on network connectivity and routing performance.

The simulated BA topology comprises 10 core routers and 16 host devices (H1–H16), resulting in a total of 26 nodes, as illustrated in Figure 1. During topology generation, each new node establishes $m = 2$ links according to the preferential attachment probability.

$$\Pi(k_i) = \frac{k_i}{\sum_j k_j} \quad (1)$$

where k_i denotes the degree of node i . This process produces the characteristic power-law degree distribution

$$P(k) \sim k^{-\gamma}, \quad 2 \leq \gamma \leq 3. \quad (2)$$

Node degree is adopted as the structural risk indicator because it directly reflects node connectivity and can be efficiently computed. The normalized structural risk of node i is defined as

$$R_i = \frac{d_i}{\max_{k \in V} d_k} \quad (3)$$

where d_i is the degree of node i , V denotes the set of network nodes, and $\max(d_k)$ is the maximum node degree in the network. Since routing decisions are performed on communication links, the corresponding link-level structural risk is given by

$$R_{ij} = \frac{\max(d_i, d_j)}{\max_{k \in V} d_k} \quad (4)$$

where R_{ij} denotes the normalized structural risk of the link connecting nodes i and j . Consequently,

$$0 \leq R_{ij} \leq 1 \quad (5)$$

where larger values indicate links connected to structurally more important nodes. The normalized risk value is subsequently used as the input to the sigmoid-based routing cost function described in the next subsection. Although node degree is adopted in this study, the proposed framework can be readily extended to incorporate dynamic risk indicators, such as trust scores, intrusion detection alerts, anomaly scores, or historical failure statistics.

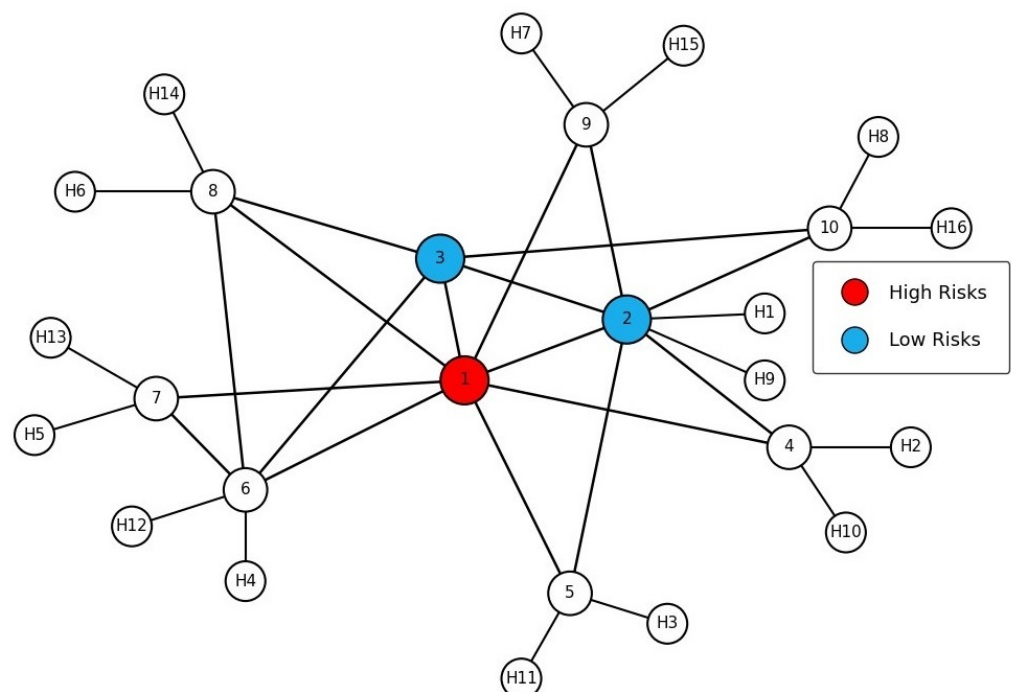


Figure 1. Barabási–Albert topology used in simulations, consisting of 10 core routers and 16 host nodes (H1–H16), totaling 26 nodes, Node 1 (red) classified as high-risk, Nodes 2–3 (blue) as low-risk, and all remaining nodes (white) as neutral based on degree-driven performance analysis.

3.2. Sigmoid-Based Cost Model

Conventional OSPF relies on static link costs that are unable to effectively capture nonlinear variations in network conditions or topology-based structural risk. The proposed SE-OSPF framework addresses this limitation by mapping the normalized structural risk to the routing cost through a nonlinear sigmoid function. Compared with conventional linear cost models, the sigmoid function enables smooth cost transitions, thereby reducing abrupt routing changes and improving routing adaptability.

The sigmoid-based routing cost factor is defined as

$$f_r = \frac{1}{1 + e^{-k(x-x_0)}} \quad (6)$$

where x denotes the normalized structural risk indicator R_{ij} , x_0 is the midpoint, and k is the steepness parameter. The corresponding routing cost is computed as

$$\text{Cost}_{ij} = C_{\min} + (C_{\max} - C_{\min})f_r \quad (7)$$

where $C_{\min}$ and $C_{\max}$ specify the minimum and maximum routing costs. This formulation ensures that routing costs remain within predefined bounds while remaining compatible with the standard OSPF shortest-path computation.

Sensitivity analysis was performed by varying the sigmoid midpoint (x_0) and steepness (k) to investigate their effects on routing decisions and responsiveness to topology-based structural risk. Figure 2 illustrates the routing costs generated by the proposed sigmoid model under different parameter settings. The upper subfigure represents a low-cost routing profile with $C_{\min} = 50$ and $C_{\max} = 200$, whereas the lower subfigure represents a high-cost routing profile with $C_{\min} = 100$ and $C_{\max} = 400$. Three midpoint values ($x_0 = \{30, 50, 70\}$) are evaluated together with five steepness values ($k = \{0.1, 0.2, 0.3, 0.4, 0.5\}$). Smaller values of x_0 shift the sigmoid transition toward lower structural risk, causing routing costs to increase earlier, whereas larger values delay the cost transition until higher risk levels are reached. Increasing k produces steeper transitions around the midpoint, enabling faster adaptation to changes in structural risk, while smaller values yield smoother cost variations that improve routing stability. Although the routing cost ranges differ between the two subfigures, the nonlinear relationship between structural risk and routing cost remains unchanged, demonstrating the flexibility of the proposed sigmoid model for networks with different routing cost scales.

In practical deployments, the parameters x_0 and k may be configured according to network management policies or topology statistics. Although this study derives the structural risk indicator from the node degree, the proposed framework is independent of the underlying risk source and can readily incorporate information from trust management systems, intrusion detection systems (IDS), anomaly detection algorithms, or historical network statistics.

For each simulation run, the topology-based structural risk values are computed once after topology generation and used as static inputs to the sigmoid-based cost model. The corresponding OSPF link costs are then calculated using (7) before route computation and remain fixed throughout the simulation, providing a consistent basis for performance evaluation while avoiding routing oscillations caused by frequent metric updates. The proposed framework can be extended to support periodic risk updates and adaptive routing cost recomputation in network environments.

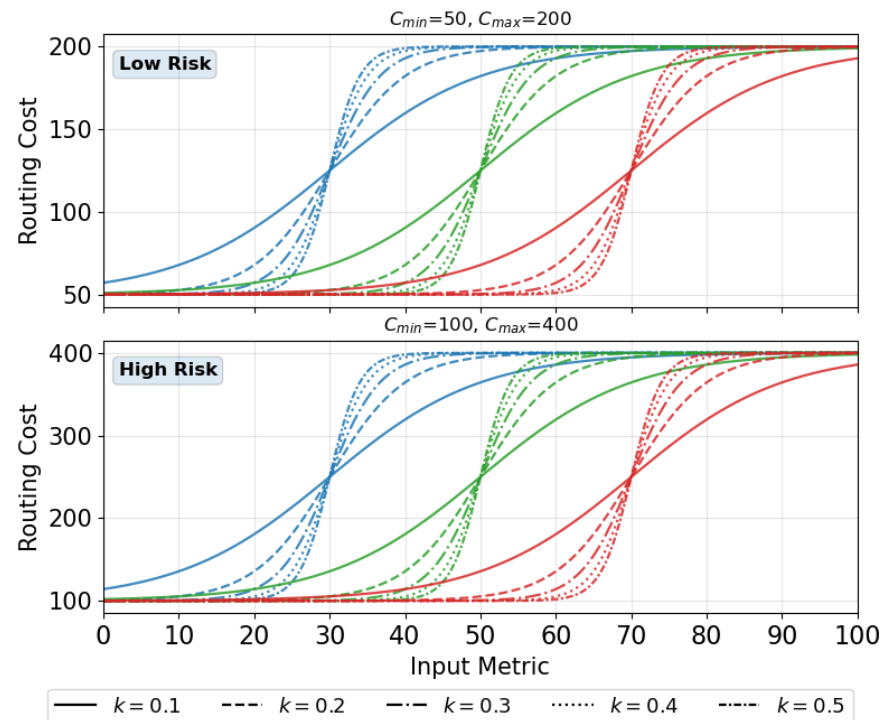


Figure 2. Sigmoid-based routing cost under different midpoint (x_0) and steepness (k) parameters. The upper figure shows the low-risk configuration ($C_{\min} = 50$, $C_{\max} = 200$), while the lower figure represents the high-risk configuration ($C_{\min} = 100$, $C_{\max} = 400$). The midpoint parameter $x_0 \in \{30 \text{ (blue)}, 50 \text{ (green)}, 70 \text{ (red)}\}$ determines the cost escalation threshold, and the steepness parameter $k \in \{0.1, 0.2, 0.3, 0.4, 0.5\}$ controls the transition sharpness.

3.3. Secure Path Selection Using Risk-Aware Sigmoid Cost

Algorithm 1 summarizes the proposed SE-OSPF routing procedure. The algorithm first computes the normalized structural risk of each node from its degree in the BA scale-free topology. The corresponding link-level risk, denoted by R_{ij} , is then determined from the higher normalized degree of the two endpoint nodes, providing a topology-based measure of link importance.

Each link-level risk value is transformed into a routing cost using the sigmoid function described in the previous subsection. The resulting sigmoid output provides a smooth scaling factor that is mapped to the OSPF routing metric through predefined minimum and maximum cost bounds. This nonlinear mapping enables continuous cost adaptation while avoiding abrupt metric changes that could otherwise introduce routing instability.

The weighted network graph is subsequently constructed, and the shortest paths are computed using Dijkstra's algorithm, consistent with the conventional OSPF shortest-path-first procedure. In the current implementation, the topology-based structural risk and the corresponding routing costs are computed once after topology generation and remain fixed throughout each simulation run. This design isolates the effect of the proposed sigmoid-based cost model while preserving routing stability.

By incorporating topology-based structural risk into the OSPF cost computation, SE-OSPF enables topology-based structural risk-aware adaptive routing without modifying the underlying shortest-path algorithm. Consequently, routing decisions consider both network connectivity and node structural importance while remaining fully compatible with the conventional OSPF framework.

Algorithm 1 SE-OSPF Path Selection Using Topology-Based Structural Risk**Require:** Graph $G(V, E)$, where V is the set of nodes and E is the set of links**Require:** Node degree d_i for each node $i \in V$ **Require:** Sigmoid parameters: midpoint x_0 and steepness k **Require:** Cost bounds: $C_{\min}$ and $C_{\max}$ **Require:** Source node s and destination node d **Ensure:** Selected path $P(s, d)$ based on sigmoid-enhanced OSPF cost

```

1:  $d_{\max} \leftarrow \max_{i \in V} d_i$ 
2: for all nodes  $i \in V$  do
3:    $R_i \leftarrow d_i / d_{\max}$  // Normalized node structural risk
4: end for
5: for all links  $(i, j) \in E$  do
6:    $R_{ij} \leftarrow \max(R_i, R_j)$  // Link-level structural risk
7:    $f_r \leftarrow 1 / (1 + e^{-k(R_{ij} - x_0)})$  // Sigmoid scaling factor
8:    $\text{Cost}_{ij} \leftarrow C_{\min} + (C_{\max} - C_{\min})f_r$ 
9: end for
10: Build weighted graph  $G'(V, E)$  using  $\text{Cost}_{ij}$ 
11: Compute routing table using Dijkstra's shortest-path algorithm on  $G'$ 
12: Extract path  $P(s, d)$  from the computed routing table
13: return  $P(s, d)$ 

```

3.4. Linear to Sigmoid Cost Models

In [20], existing OSPF extensions employ a linear routing metric in which the routing cost increases proportionally with a network parameter such as link risk. The linear cost model can be expressed as

$$C_{ij}^{\text{linear}} = c_{\min} + (c_{\max} - c_{\min})x \quad (8)$$

where x denotes the normalized metric associated with link (i, j) and $(c_{\min}, c_{\max})$ represents the allowable routing cost range. Although this formulation is simple and computationally efficient, it assumes constant sensitivity across all network conditions and may not accurately capture nonlinear degradation in dynamic environments.

To improve adaptability, a sigmoid-based routing metric is proposed, enabling non-linear cost scaling. Around its midpoint x_0 , the sigmoid behaves approximately linearly, indicating that the linear metric represents a local approximation of the sigmoid model. The sigmoid formulation therefore generalizes the linear metric by introducing adaptive sensitivity through the parameters x_0 and k . Table 3 summarizes the conceptual differences between the linear routing metric and the proposed sigmoid-based metric in terms of adaptability and congestion response.

Table 3. Conceptual interpretation of linear and sigmoid-based metrics.

Property	Linear Metric	Sigmoid Metric
Cost growth	Constant rate	Adaptive rate
Sensitivity	Uniform	Threshold-based
Adaptability	Moderate	High
Congestion response	Gradual	Rapid near threshold

3.5. Simulation Environment

The performance of the proposed SE-OSPF protocol was evaluated using the NS-3 network simulator. A BA scale-free topology was adopted to emulate realistic communication networks characterized by a small number of connected hub nodes and many peripheral nodes. Such topologies exhibit connectivity and traffic concentration, providing a practical environment for evaluating risk-aware adaptive routing algorithms.

The simulated network consists of 10 core routers and 16 host nodes (26 nodes in total) interconnected through point-to-point wired links. Each communication link was configured with a bandwidth of 1 Gbps, representing the maximum link capacity, and a propagation delay of 1 ns. Traffic was generated using UDP-based Poisson applications with a packet size of 560 bytes. To investigate routing behavior under different traffic conditions, the offered traffic rate, representing the packet generation rate of each application flow, was varied from 100 to 700 Mbps per flow. Routing tables were initialized at the beginning of each simulation and recomputed after topology-based risk evaluation at 0.06 s. The proposed SE-OSPF was compared with Standard OSPF and Linear-OSPF using the same network topology and traffic scenarios.

Table 4 summarizes the simulation parameters used throughout this study.

Table 4. Simulation parameters.

Parameter	Value
Simulator	NS-3
Topology model	Barabási–Albert scale-free topology
Number of core routers	10
Number of host nodes	16
Total nodes	26
Link type	Point-to-point wired links
Link bandwidth	1 Gbps (link capacity)
Link propagation delay	1 ns
Traffic type	UDP Poisson traffic
Number of active traffic flows	26
Packet size	560 bytes
Traffic rate	100, 300, 500, and 700 Mbps (application rate)
Maximum packets per flow	100,000 packets
Queue type	NS-3 default
Queue size	NS-3 default
Simulation length	200 s
Routing update time	0.06 s
Routing update mechanism	Routing table recomputation
Risk update mechanism	Static topology-based structural risk
Random seeds	1–3
Repeated runs	5 simulation runs
Compared protocols	Standard OSPF, Linear-OSPF, and SE-OSPF

4. Results and Discussion

This section evaluates the proposed SE-OSPF framework against Standard OSPF and Linear-OSPF using end-to-end delay, jitter, maximum link utilization (MLU), and packet delivery success (PDS). The performance is analyzed under different bandwidths and sigmoid parameter settings, followed by hypothesis validation based on the experimental results.

4.1. Hypothesis Validation

The experimental evaluation aims to assess the effectiveness of the proposed SE-OSPF framework under topology-based structural risk conditions. The following hypotheses were formulated to guide the performance analysis:

Hypothesis 1. *SE-OSPF reduces average end-to-end delay by employing an adaptive sigmoid-based cost mechanism that proactively mitigates congestion and avoids structurally critical paths.*

Hypothesis 2. *The proposed sigmoid-based cost model reduces packet jitter and improves PDS by enabling fine-grained differentiation of high-risk links during routing decisions.*

Hypothesis 3. SE-OSPF improves load balancing, as evidenced by lower MLU, through continuous sigmoid-based cost adaptation that prevents traffic concentration on highly utilized links.

These hypotheses provide a foundation for evaluating the applicability and effectiveness of SE-OSPF in performance-critical network environments.

4.2. End-to-End Delay Performance Analysis

End-to-end delay is defined as the average packet delivery time from the source to the destination, including transmission, queuing, and processing delays, and is given by:

$$\text{Delay}_{\text{avg}} = \frac{1}{N} \sum_{i=1}^N (t_{\text{recv},i} - t_{\text{send},i}) \quad (9)$$

where N is the number of received packets, and $t_{\text{send},i}$ and $t_{\text{recv},i}$ denote the packet transmission and reception times, respectively. Lower delay indicates better routing performance.

Figures 3–5 illustrate the CDFs of end-to-end packet delay for sigmoid midpoint values of $x_0 = 30, 50$, and 70 , respectively. The midpoint parameter x_0 determines when routing costs increase. A smaller x_0 applies routing penalties earlier, reducing congestion under heavy traffic, whereas a larger x_0 preserves shorter paths under light traffic but may increase delay as network load grows.

The steepness parameter k controls the sensitivity of the routing cost around the threshold. Smaller values provide smoother and more stable routing adaptation, while larger values respond more aggressively to structural risk, improving congestion avoidance at the cost of potentially longer routes. Table 5 summarizes the effects and trade-offs of the sigmoid parameters. The results reveal a trade-off between congestion avoidance and path efficiency. Smaller x_0 or larger k improve delay performance under moderate and heavy traffic, whereas larger x_0 or smaller k better preserve path efficiency under light traffic. These findings support Hypothesis 1, demonstrating that the proposed sigmoid-based cost model effectively balances structural risk and routing performance.

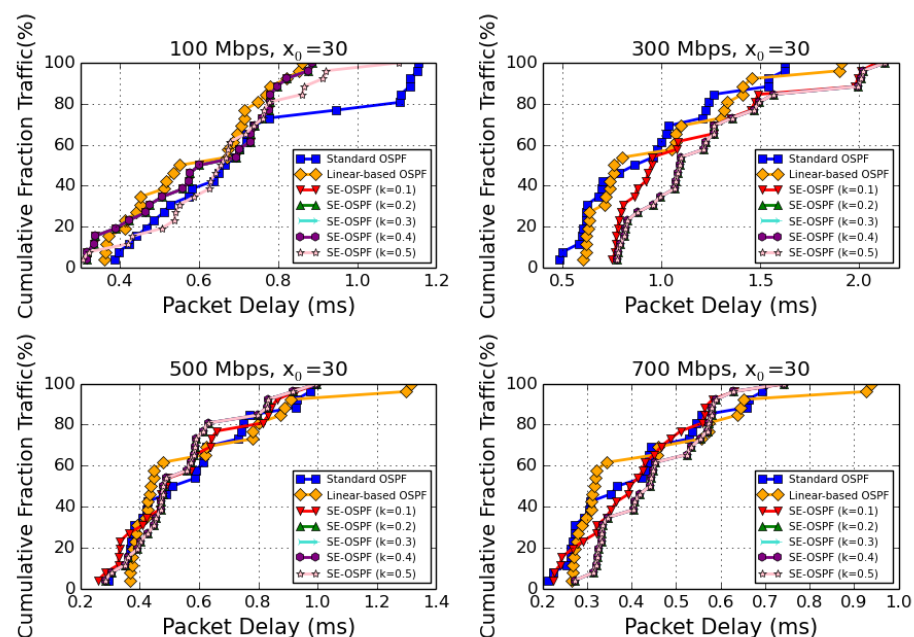


Figure 3. Cumulative distribution functions (CDFs) of end-to-end packet delay for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps with a sigmoid midpoint of $x_0 = 30$ and varying steepness values ($k = 0.1$ – 0.5).

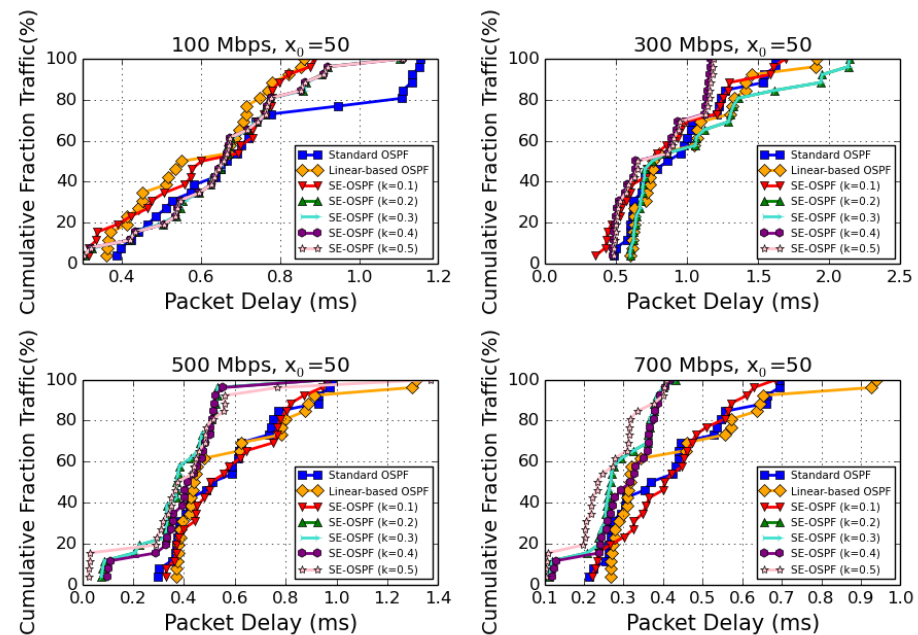


Figure 4. Cumulative distribution functions (CDFs) of end-to-end packet delay for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps with a sigmoid midpoint of $x_0 = 50$ and varying steepness values ($k = 0.1$ – 0.5).

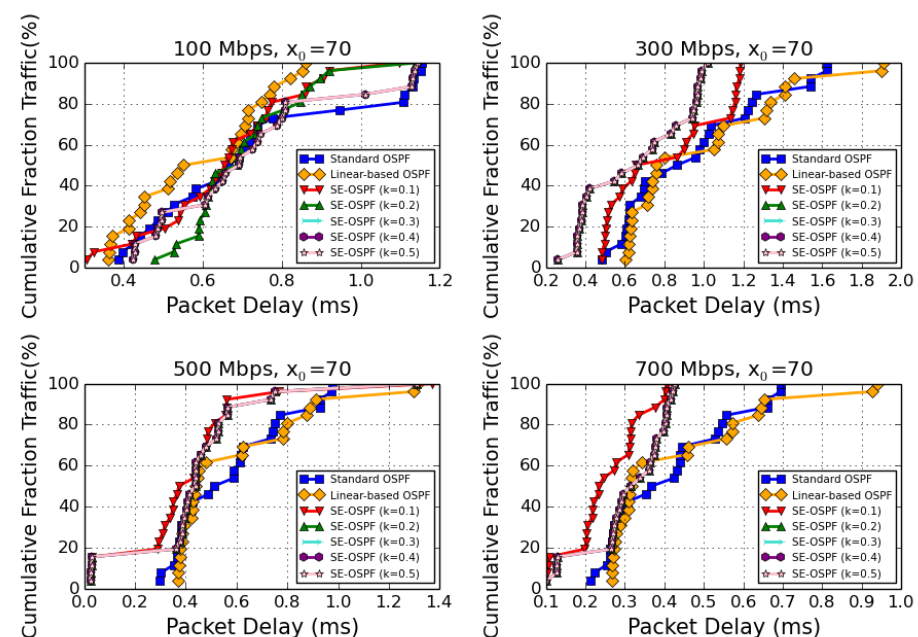


Figure 5. Cumulative distribution functions (CDFs) of end-to-end packet delay for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps with a sigmoid midpoint of $x_0 = 70$ and varying steepness values ($k = 0.1$ – 0.5).

Table 5. Effects of sigmoid parameters on routing behavior.

Parameter	Effect	Benefit	Trade-Off
Small (x_0)	Early penalty	Less congestion	Longer paths
Large (x_0)	Late penalty	Better hub usage	Higher delay
Small (k)	Smooth transition	Stable routing	Slow adaptation
Large (k)	Sharp transition	Fast adaptation	Longer paths

4.3. Average End-to-End Delay Analysis

Figure 6 compares the average end-to-end delay of Standard OSPF, Linear-OSPF, and SE-OSPF with different sigmoid steepness values. Standard OSPF records the highest delay (0.66 ms), while Linear-OSPF shows only a marginal improvement. In contrast, SE-OSPF consistently reduces delay as the sigmoid steepness increases.

A larger k produces a steeper sigmoid cost function, allowing routing costs to rise more rapidly once the structural risk exceeds the threshold. This enables earlier traffic diversion from congested hub nodes, reducing queueing delay and improving load balancing. Smaller k values provide smoother cost transitions, resulting in slower adaptation and slightly higher delays. SE-OSPF with $k = 0.5$ achieves the lowest average delay (0.53 ms), approximately 20% lower than Standard OSPF. These results demonstrate that increasing the sigmoid steepness enhances routing responsiveness and effectively reduces end-to-end delay.

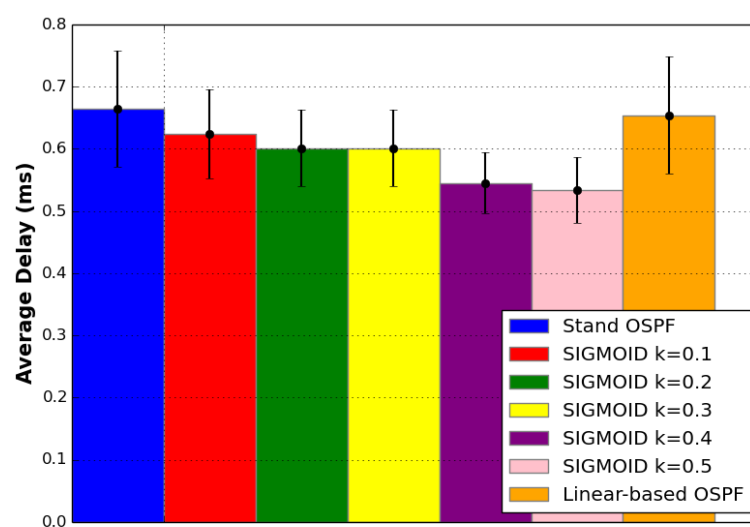


Figure 6. Average end-to-end delay for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1$ – 0.5). Error bars represent the standard deviation of the measured end-to-end delay across the simulation runs.

4.4. Jitter Performance Analysis

Jitter measures variations in packet arrival times and is critical for real-time applications. It is given by:

$$\text{Jitter}_i = |(t_i - t_{i-1}) - (t_{i-1} - t_{i-2})| \quad (10)$$

where t_i , t_{i-1} , and t_{i-2} are the arrival times of consecutive packets. Lower jitter indicates more stable routing and packet delivery.

Figures 7–9 illustrate the CDFs of end-to-end jitter for sigmoid midpoint values of $x_0 = 30$, 50, and 70, respectively. A left-shifted CDF indicates lower jitter and more stable packet delivery. SE-OSPF consistently achieves lower jitter than the baseline protocols, especially under moderate and heavy traffic.

The midpoint parameter x_0 determines when routing costs increase. Smaller x_0 values trigger earlier traffic redistribution, reducing congestion but potentially increasing route changes, whereas larger x_0 values preserve routing stability but may increase jitter under heavy traffic. The steepness parameter k controls routing responsiveness. Smaller k values provide smoother and more stable adaptation, while larger k values react more quickly to congestion, reducing jitter at the cost of more aggressive route updates. Table 6 summarizes

the effects of the sigmoid parameters on jitter performance. Smaller x_0 or larger k improve jitter performance through faster congestion avoidance, whereas larger x_0 or smaller k favor routing stability. These results support Hypothesis 2 that SE-OSPF reduces packet jitter by balancing routing responsiveness and stability.

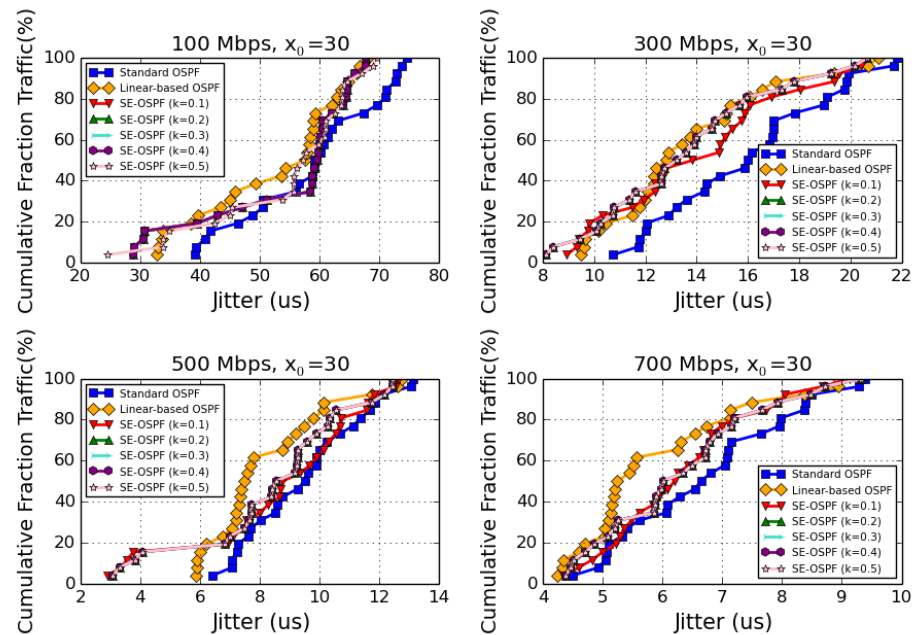


Figure 7. Cumulative distribution functions (CDFs) of packet jitter for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps, with the sigmoid midpoint fixed at $x_0 = 30$ and the steepness parameter varied from $k = 0.1$ to 0.5.

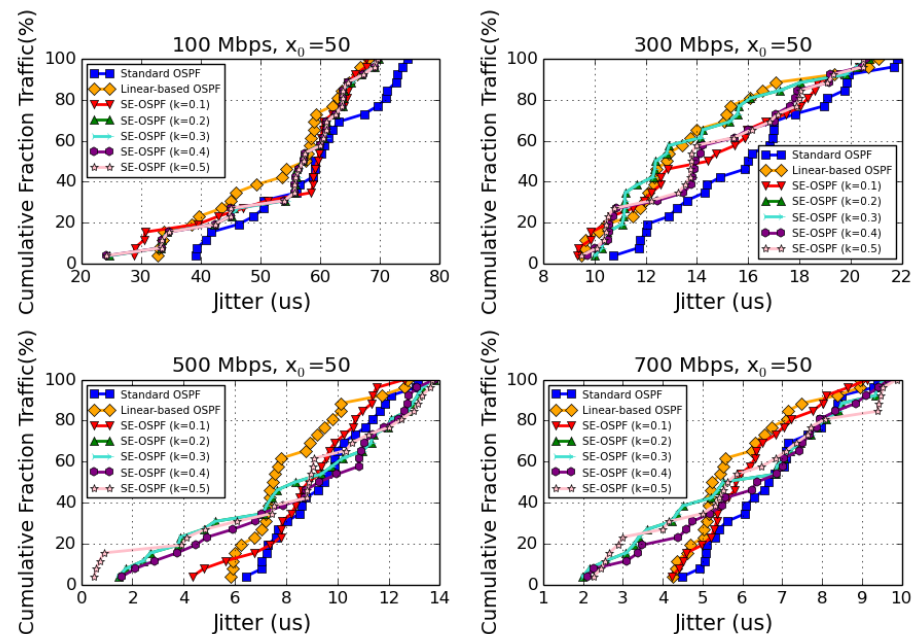


Figure 8. Cumulative distribution functions (CDFs) of packet jitter for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps, with the sigmoid midpoint fixed at $x_0 = 50$ and the steepness parameter varied from $k = 0.1$ to 0.5.

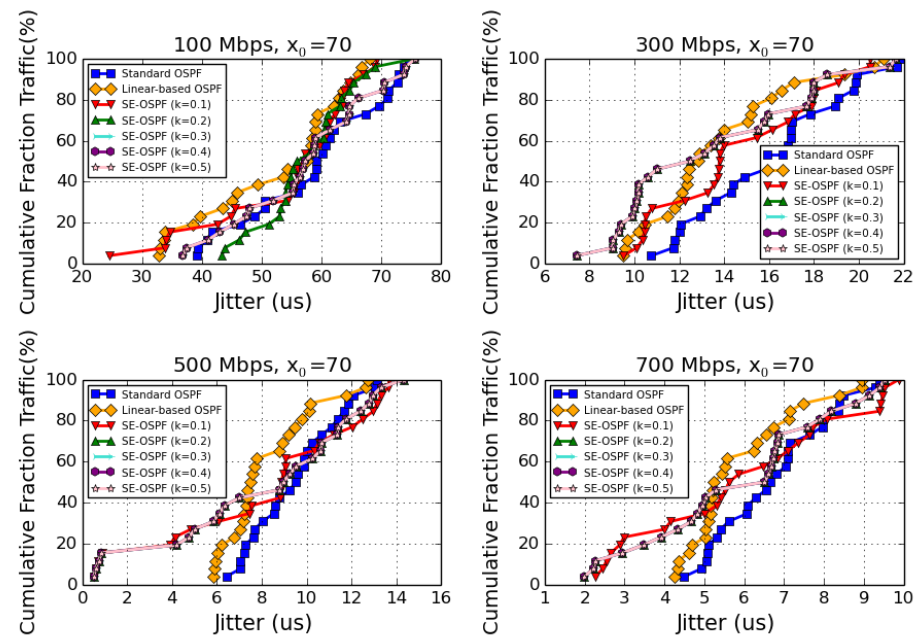


Figure 9. Cumulative distribution functions (CDFs) of packet jitter for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps, with the sigmoid midpoint fixed at $x_0 = 70$ and the steepness parameter varied from $k = 0.1$ to 0.5.

Table 6. Effects of sigmoid parameters on jitter performance.

Parameter	Effect	Benefit	Trade-Off
Small (x_0)	Early adaptation	Lower jitter	Less stable routes
Large (x_0)	Late adaptation	Stable routing	Higher jitter
Small (k)	Smooth transition	Stable routing	Slow adaptation
Large (k)	Sharp transition	Lower jitter	Frequent updates

4.5. Average Jitter Analysis

Figure 10 compares the average jitter of Standard OSPF, Linear-OSPF, and SE-OSPF with different sigmoid steepness values. Standard OSPF exhibits the highest jitter, while all SE-OSPF configurations reduce jitter. The lowest jitter is achieved with moderate steepness ($k = 0.2$ – 0.3), providing the best balance between routing responsiveness and stability.

The steepness parameter k controls routing adaptation. Small values respond gradually, allowing congestion to increase jitter, whereas large values trigger more aggressive route updates that may slightly increase packet delay variation. Moderate values effectively balance congestion avoidance and routing stability, resulting in the lowest jitter. These results support Hypothesis 2, demonstrating that SE-OSPF improves jitter performance through risk-aware adaptive routing.

4.6. Maximum Link Utilization (MLU) Analysis

Network load balancing is evaluated using the MLU, which represents the highest utilization among all network links. Lower MLU indicates more balanced traffic distribution and reduced congestion, whereas higher MLU reflects traffic concentration and an increased risk of bottlenecks.

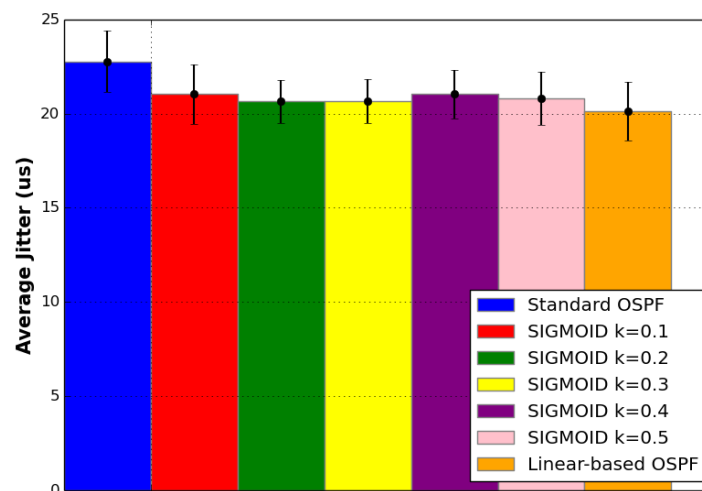


Figure 10. Average packet jitter for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1$ – 0.5). Error bars represent the standard deviation of jitter measurements across the simulation runs.

Per-link utilization is defined as

$$U_l = \frac{B_l}{C_l T} \quad (11)$$

where B_l is the total number of transmitted bits, C_l is the link capacity, and T is the simulation time. The MLU is then computed as

$$U_{\max} = \max_{l \in \mathcal{L}} U_l \quad (12)$$

where $U_{\max}$ denotes the maximum utilization among all links in the network.

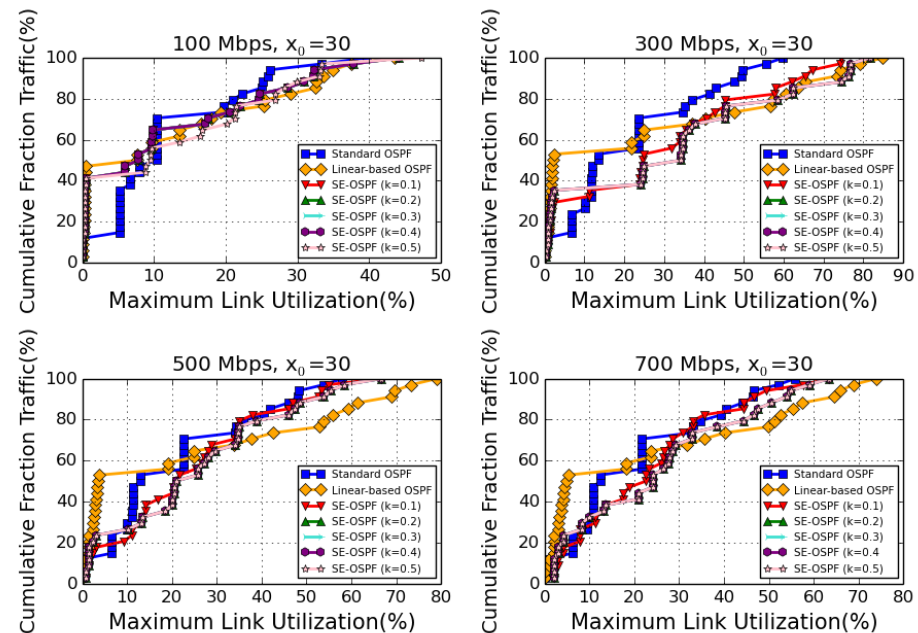
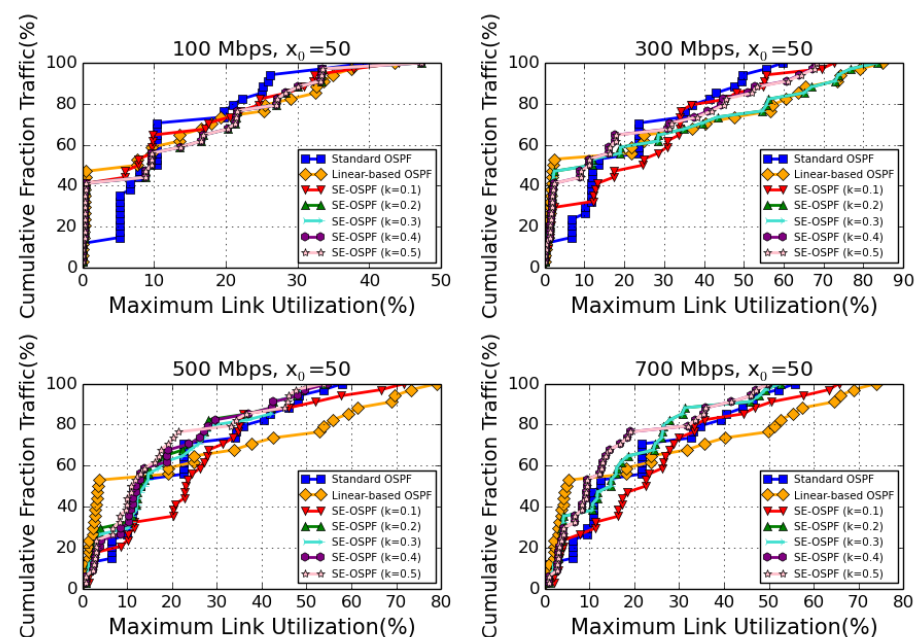
Figures 11–13 present the CDFs of MLU for sigmoid midpoint values of $x_0 = 30$, 50, and 70, respectively. Lower MLU indicates better load balancing by preventing excessive traffic concentration on individual links. SE-OSPF achieves lower MLU than Standard OSPF, particularly under moderate and heavy traffic, demonstrating more balanced traffic distribution.

The midpoint parameter x_0 determines when routing costs increase. Smaller x_0 values redistribute traffic earlier, reducing MLU through proactive load balancing, whereas larger x_0 values retain traffic on preferred routes for longer, potentially increasing link utilization before rerouting occurs. The steepness parameter k controls routing responsiveness. Smaller k values provide gradual traffic redistribution, while larger k values shift traffic more rapidly from highly utilized links, further reducing MLU but increasing routing sensitivity. Table 7 summarizes the effects of the sigmoid parameters on MLU, highlighting the trade-off between load balancing and routing stability.

These results highlight a trade-off between load balancing and routing stability. Smaller x_0 or larger k improve load distribution by lowering MLU, whereas larger x_0 or smaller k preserve more stable routing with slightly higher link utilization. SE-OSPF effectively balances traffic across the network, supporting Hypothesis 3 that risk-aware adaptive routing improves load balancing by reducing maximum link utilization.

Table 7. Effects of sigmoid parameters on maximum link utilization.

Parameter	Effect	Benefit	Trade-Off
Small (x_0)	Early adaptation	Lower MLU	Less stable routes
Large (x_0)	Late adaptation	Stable routing	Higher MLU
Small (k)	Smooth transition	Stable routing	Slower load balancing
Large (k)	Fast adaptation	Lower MLU	Higher routing sensitivity

**Figure 11.** Cumulative distribution functions (CDFs) of Maximum Link Utilization (MLU) for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps, with the sigmoid midpoint fixed at $x_0 = 30$ and the steepness parameter varied from $k = 0.1$ to 0.5.**Figure 12.** Cumulative distribution functions (CDFs) of Maximum Link Utilization (MLU) for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps, with the sigmoid midpoint fixed at $x_0 = 50$ and the steepness parameter varied from $k = 0.1$ to 0.5.

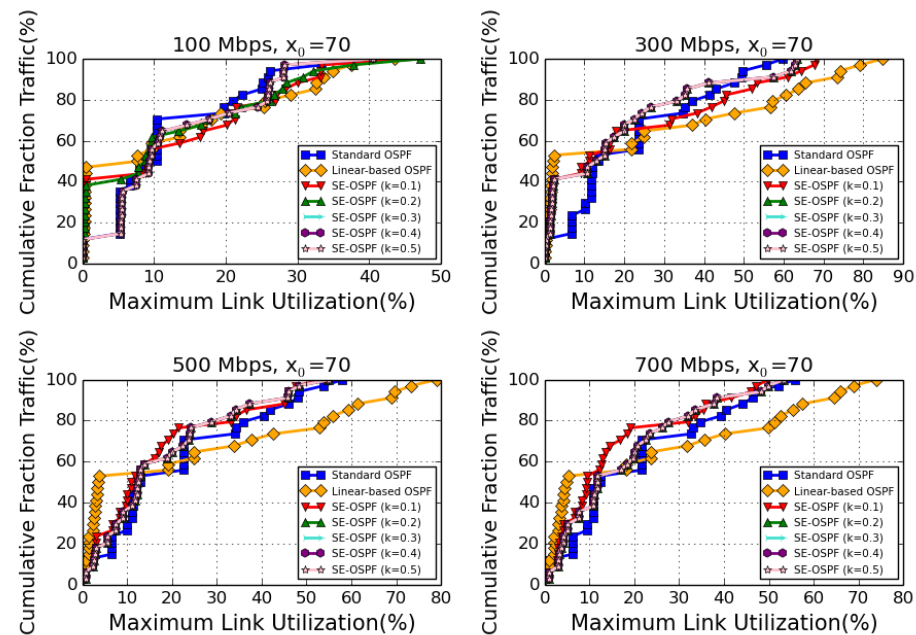


Figure 13. Cumulative distribution functions (CDFs) of Maximum Link Utilization (MLU) for Standard OSPF, Linear-OSPF, and SE-OSPF under bandwidths of 100, 300, 500, and 700 Mbps, with the sigmoid midpoint fixed at $x_0 = 70$ and the steepness parameter varied from $k = 0.1$ to 0.5 .

4.7. Average Link Utilization (ALU) Analysis

The average link utilization (ALU), which measures the mean utilization across all network links, is defined as

$$U_{\text{avg}} = \frac{1}{|\mathcal{L}|} \sum_{l \in \mathcal{L}} U_l \quad (13)$$

where $|\mathcal{L}|$ is the total number of links and U_l is the utilization of link l . Lower ALU indicates more balanced traffic distribution across the network.

Figures 14–16 compares the ALU of three representative nodes for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid parameters. Lower average MLU indicates better load balancing through more even traffic distribution. Standard OSPF concentrates traffic on Node 1, while Linear-OSPF shifts a larger portion of traffic toward Nodes 2 and 3, resulting in uneven link utilization. In contrast, SE-OSPF distributes traffic more uniformly by adapting routing costs according to structural risk, thereby improving overall load balancing.

The midpoint parameter x_0 controls when traffic redistribution begins. Larger x_0 values delay routing penalties, preserving preferred routes while gradually balancing utilization across the network. The steepness parameter k controls the aggressiveness of traffic redistribution. Moderate-to-large values ($k = 0.3$ – 0.5) provide the most balanced utilization, whereas very small values may produce less effective traffic distribution. SE-OSPF achieves more balanced average link utilization than Standard OSPF and Linear-OSPF, demonstrating that risk-aware adaptive routing effectively improves network load balancing while avoiding excessive traffic concentration.

As summarized in Table 8, SE-OSPF exhibits a higher ALU of 30.84% compared to 21.76% for Standard OSPF and 25.18% for Linear OSPF, corresponding to increases of 41.7% and 22.5%, respectively. This increase results from a sigmoid-based nonlinear cost mechanism that intentionally consolidates traffic on secure and reliable paths once risk is exceeded. Rather than indicating inefficiency, the higher ALU reflects a designed

trade-off that enhances routing stability, risk awareness, and resilience in dynamic IoT and CPS networks.

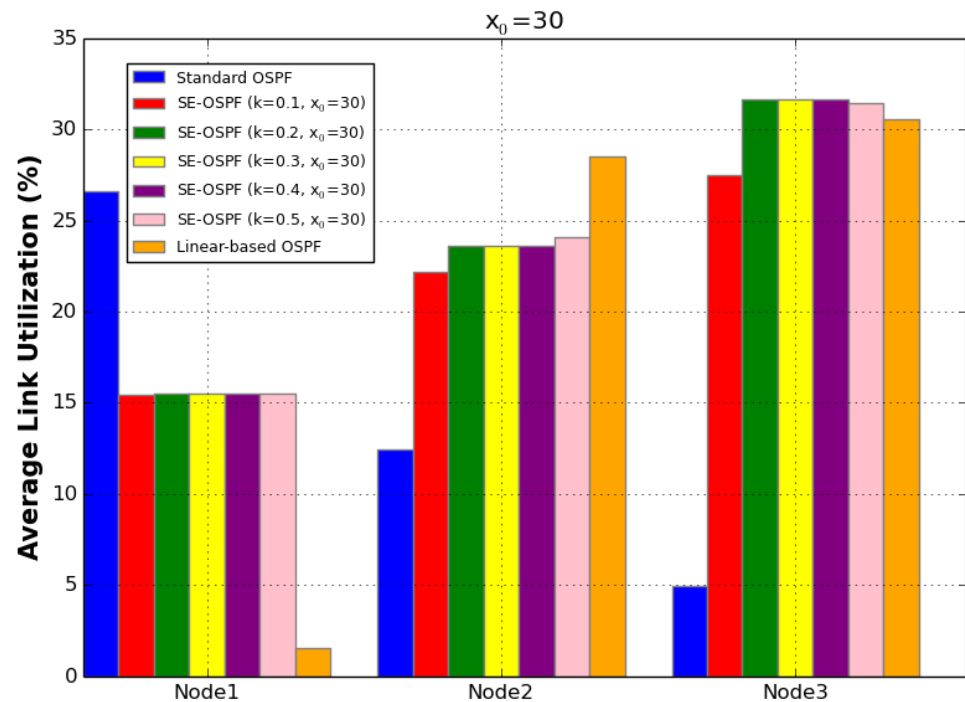


Figure 14. Average link utilization for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1$ – 0.5) with the sigmoid midpoint fixed at $x_0 = 30$.

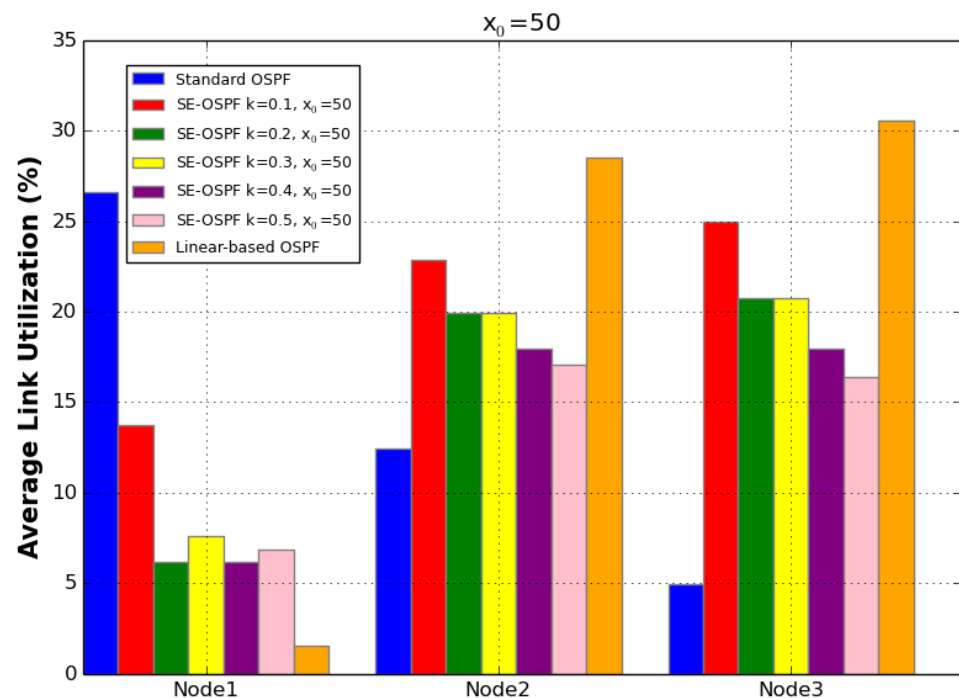


Figure 15. Average link utilization for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1$ – 0.5) with the sigmoid midpoint fixed at $x_0 = 50$.

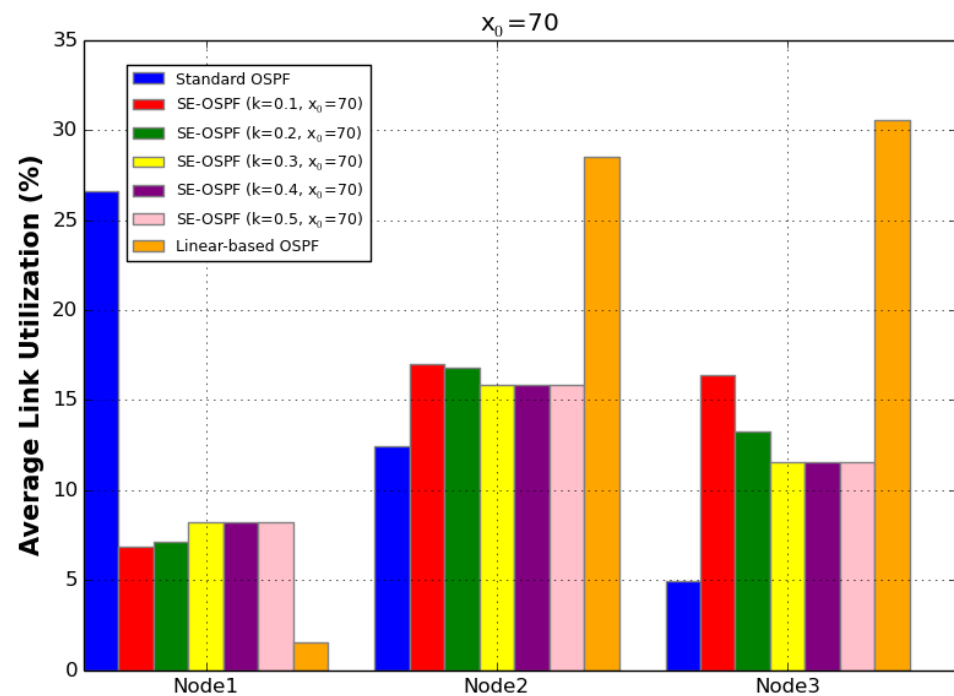


Figure 16. Average link utilization for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1$ – 0.5) with the sigmoid midpoint fixed at $x_0 = 70$.

Table 8. Summary of maximum link utilization comparison. The dash (–) indicates that the comparison is not applicable.

Routing Scheme	ALU (%)	vs. Standard	vs. Linear
Standard OSPF	21.76	–	–
Linear OSPF	25.18	+15.7%	–
SE-OSPF (Avg)	30.84	+41.7%	+22.5%

4.8. Packet Delivery Success (PDS) Analysis

PDS evaluates routing reliability by measuring the proportion of packets successfully delivered to their destinations, where higher PDS indicates better routing performance. Figures 17–19 present the PDS of Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid parameter configurations. The results show that PDS depends on the trade-off between congestion avoidance and routing efficiency. Standard OSPF maintains relatively high PDS under light traffic, whereas Linear-OSPF consistently exhibits the lowest PDS among the evaluated routing schemes.

The midpoint parameter x_0 determines when routing costs increase. Smaller x_0 values reroute traffic earlier, reducing congestion but increasing path length and routing overhead, which lowers PDS. Larger x_0 values preserve efficient routes until structural risk becomes significant, resulting in higher packet delivery. The steepness parameter k controls routing responsiveness. Moderate values ($k = 0.2$ – 0.3) provide the best balance between congestion avoidance and path stability, whereas very small or large values either react too slowly or introduce excessive route changes. Larger x_0 with moderate k achieves the highest PDS by balancing routing efficiency and congestion avoidance, supporting Hypothesis 2 that risk-aware adaptive routing improves packet delivery success.

Table 9 summarizes the effects of the sigmoid parameters on PDS. Smaller x_0 improves congestion avoidance but may reduce PDS, whereas larger x_0 better preserves packet

delivery. Similarly, smaller k favors routing stability, while larger k enhances congestion avoidance at the cost of more frequent route updates.

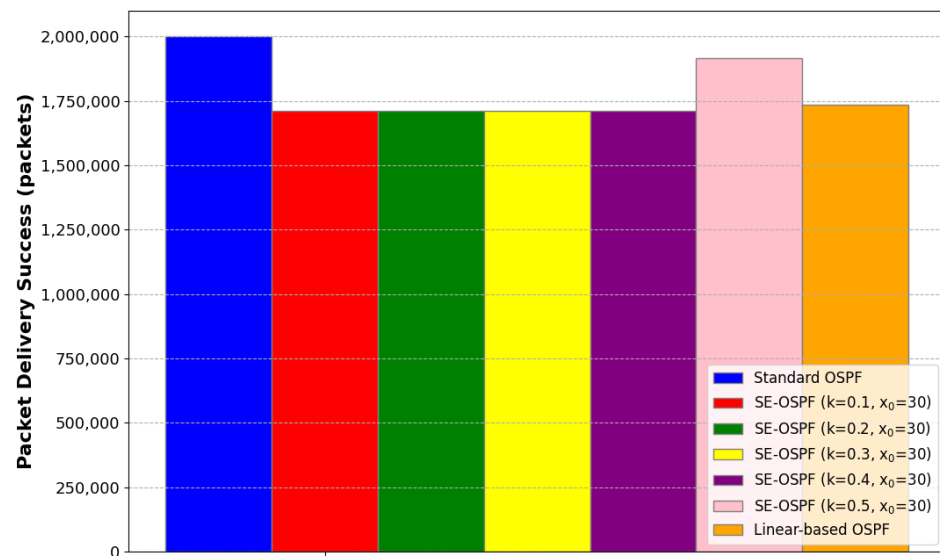


Figure 17. Packet delivery success (PDS) for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1–0.5$) with the sigmoid midpoint fixed at $x_0 = 30$.

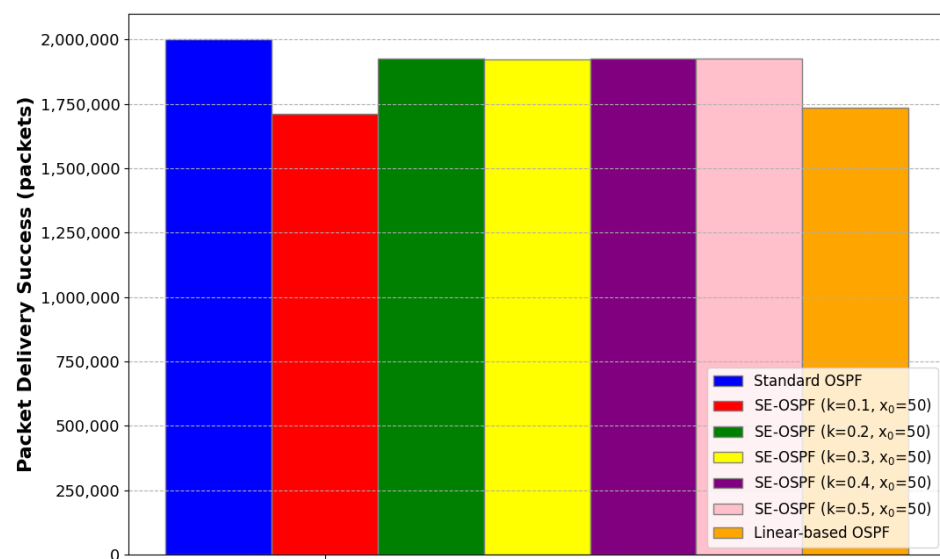


Figure 18. Packet delivery success (PDS) for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1–0.5$) with the sigmoid midpoint fixed at $x_0 = 50$.

Table 9. Effects of sigmoid parameters on packet delivery success.

Parameter	Effect	Benefit	Trade-Off
Small (x_0)	Early	Less congestion	Lower PDS
Large (x_0)	Late	Higher PDS	Higher congestion risk
Small (k)	Smooth	Stable routing	Slow congestion response
Large (k)	Fast	Better congestion avoidance	More route changes

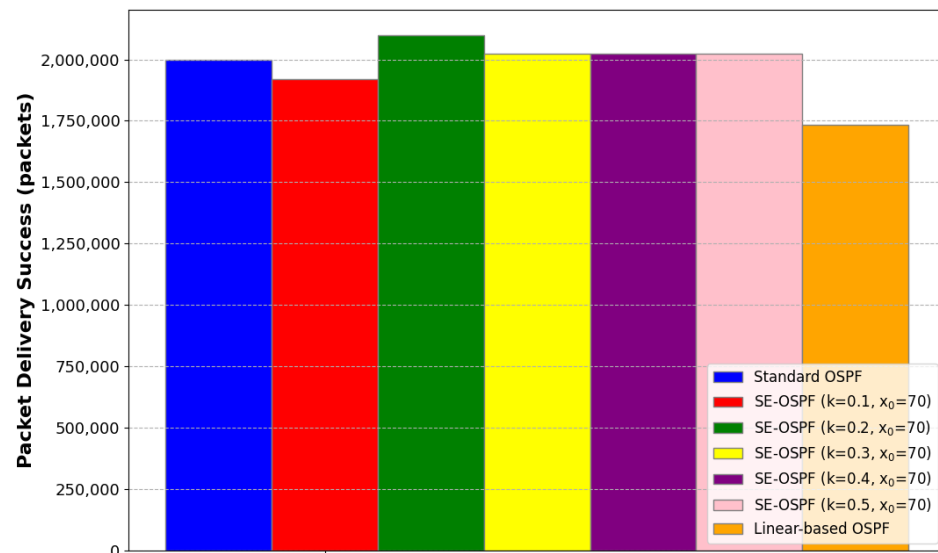


Figure 19. Packet delivery success (PDS) for Standard OSPF, Linear-OSPF, and SE-OSPF under different sigmoid steepness values ($k = 0.1$ – 0.5) with the sigmoid midpoint fixed at $x_0 = 70$.

4.9. Unified Performance Discussion

SE-OSPF outperforms Standard OSPF and Linear-OSPF by reducing end-to-end delay, packet jitter, and MLU while maintaining high PDS. These improvements are achieved through the proposed sigmoid-based cost model, which adaptively redistributes traffic according to topology-based structural risk.

Table 10 summarizes the effects of the sigmoid midpoint (x_0) and steepness (k) on the evaluated performance metrics. It highlights the engineering trade-offs associated with different parameter settings and provides practical guidance for selecting suitable values under varying network conditions.

The sigmoid parameters jointly influence routing performance. Smaller values of x_0 promote earlier traffic redistribution, improving congestion avoidance and load balancing, whereas larger values preserve path efficiency and routing stability. Likewise, moderate values of k provide an effective balance between responsiveness and stability, resulting in higher PDS and lower jitter, while larger values enable faster adaptation under heavy traffic. Consequently, more aggressive parameter settings are better suited to congested networks, whereas conservative settings are preferable under stable operating conditions.

From an engineering perspective, the proposed topology-based structural risk-aware routing framework preserves the conventional OSPF control plane by modifying only the routing cost computation. This design facilitates deployment in existing IP networks, while the configurable sigmoid parameters provide flexibility for different operating conditions and offer opportunities for future optimization using adaptive or machine learning-based techniques.

Table 10. Unified effects of sigmoid parameters on routing performance. Arrows indicate the relative change in each metric ($\uparrow$: increase; $\downarrow$: decrease).

Parameter	Behavior	Delay	Jit./MLU	PDS	Trade-Off
Small (x_0)	Early	$\downarrow$	$\downarrow$	$\downarrow$	Fast adaptation
Large (x_0)	Late	$\uparrow$	$\uparrow$	$\uparrow$	Stable routing
Small (k)	Smooth	$\uparrow$	Stable	Moderate	Slow response
Large (k)	Fast	$\downarrow$	$\downarrow$	Moderate	Frequent updates

4.10. Comparative Performance Analysis

As summarized in Table 11, SE-OSPF ($k = 0.5$) provides the best overall performance among the evaluated routing schemes. It achieves the lowest end-to-end delay (0.53 ms), corresponding to a 19.7% reduction compared with Standard OSPF. Although Linear-OSPF yields the lowest average jitter, it records the fewest successfully delivered packets (1,734,813), highlighting a trade-off between delay stability and delivery reliability. In contrast, SE-OSPF maintains low jitter while increasing the average number of successfully delivered packets to 2,023,200, demonstrating a more balanced trade-off between latency, reliability, and routing adaptability under dynamic network conditions.

Table 11. Performance comparison of routing schemes.

Metric	Std. OSPF	Linear OSPF	SIGMOID ($k = 0.5$)
Delay (s)	0.66	0.65	0.53
Jitter (ms)	22.76	20.11	20.81
Packet Delivery (Avg)	1,999,595	1,734,813	2,023,200
Adaptivity	Low	Medium	High

5. Conclusions and Future Work

This paper proposed SE-OSPF, a topology-based structural risk-aware adaptive routing framework that integrates a nonlinear sigmoid-based cost function into the conventional OSPF protocol. By incorporating topology-based structural risk into the routing metric, the proposed framework adaptively adjusts routing costs using two configurable sigmoid parameters: the midpoint (x_0) and the steepness (k). This nonlinear cost model enables flexible routing decisions that effectively balance congestion avoidance, routing stability, and path efficiency under varying network conditions.

The effectiveness of SE-OSPF was evaluated through NS-3 simulations on a Barabási–Albert scale-free topology. The results demonstrate that SE-OSPF outperforms Standard OSPF and Linear-OSPF by reducing end-to-end delay, packet jitter, and MLU while maintaining high PDS, thereby improving routing efficiency and load balancing. Sensitivity analysis further shows that routing behavior can be effectively controlled through the sigmoid parameters. Smaller values of x_0 or larger values of k promote earlier traffic redistribution and stronger congestion avoidance, whereas larger x_0 or moderate k provide greater routing stability and improved packet delivery. These findings demonstrate that appropriate parameter selection enables an effective trade-off between routing responsiveness and network efficiency. Since SE-OSPF modifies only the routing cost computation while preserving the standard OSPF control plane, it can be readily deployed in existing IP networks without requiring protocol redesign.

Future work will investigate adaptive optimization of the sigmoid parameters using machine learning techniques to enable autonomous routing under dynamic network conditions. The framework will also be extended to support multi-objective routing by jointly considering congestion, trust, energy efficiency, and topology-based risk indicators. In addition, large-scale experimental validation and dynamic risk-aware routing scenarios will be explored to further evaluate the scalability, robustness, and practical applicability of the proposed framework.

Author Contributions: Conceptualization, C.T. and K.K.; methodology, C.T. and K.K.; software, C.T. and K.K.; validation, C.T. and K.K.; formal analysis, C.T. and K.K.; investigation, C.T. and K.K.; data curation, C.T. and K.K.; visualization, C.T. and K.K.; writing—original draft preparation, C.T. and K.K.; writing—review and editing, 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.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request.

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

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

References

1. Jahangeer, A.; Bazai, S.U.; Aslam, S.; Marjan, S.; Anas, M.; Hashemi, S.H. A review on the security of IoT networks: From network layer's perspective. *IEEE Access* **2023**, *11*, 71073–71087. [CrossRef]
2. Naik, A.C.; Awasthi, L.K.; Sharma, P.R.T.P.; Verma, A. Enhancing IoT security: A comprehensive exploration of privacy, security measures, and advanced routing solutions. *Comput. Netw.* **2025**, *258*, 111045. [CrossRef]
3. Kim, S.; Park, K.-J.; Lu, C. A survey on network security for cyber-physical systems: From threats to resilient design. *IEEE Commun. Surv. Tuts.* **2022**, *24*, 1534–1573. [CrossRef]
4. Moy, J. OSPF Version 2. RFC 2328, Internet Engineering Task Force (IETF). April 1998. Available online: <https://www.rfc-editor.org/info/rfc2328> (accessed on 1 June 2025).
5. Obelovska, K.; Snaichuk, Y.; Liskevych, O.; Mitoulis, S.-A.; Liskevych, R. Mitigation of risks associated with distrustful routers in OSPF networks—An enhanced method. *Computers* **2025**, *14*, 43. [CrossRef]
6. Obelovska, K.; Tkachuk, O.; Snaichuk, Y. Minimizing the number of distrustful nodes on the path of IP packet transmission. *Computation* **2024**, *12*, 91. [CrossRef]
7. 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. [CrossRef]
8. Devir, N.; Grumberg, O.; Markovitch, S.; Nakibly, G. Topology-agnostic runtime detection of OSPF routing attacks. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, Washington, DC, USA, 10–12 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 277–285. [CrossRef]
9. 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)*, New York, NY, USA, 8–12 December 2014; Association for Computing Machinery: New York, NY, USA, 2014; pp. 336–345. [CrossRef]
10. Meredith, R.; Dutta, R. Increasing network resilience to persistent OSPF attacks. In *Proceedings of the IEEE International Conference on Communications (ICC)*, Shanghai, China, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–7. [CrossRef]
11. Lemeshko, O.; Yevdokymenko, M.; Shapoval, M. Routing model with load balancing on the traffic engineering principles based on information security risks. In *Proceedings of the IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 5–7 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 572–576. [CrossRef]
12. 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 International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Cracow, Poland, 22–25 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 951–955. [CrossRef]
13. Singh, K.; Moh, S. Routing protocols in cognitive radio ad hoc networks: A comprehensive review. *J. Netw. Comput. Appl.* **2016**, *72*, 28–37. [CrossRef]
14. Kazi, A.K.; Farooq, M.U.; Asif, R.; Hina, S. Adaptive context-aware VANET routing protocol for intelligent transportation systems. *Network* **2025**, *5*, 47. [CrossRef]
15. Ramkumar, J.; Vadivel, R. Multi-adaptive routing protocol for Internet of Things based ad-hoc networks. *Wirel. Pers. Commun.* **2021**, *120*, 887–909. [CrossRef]
16. Mahamune, A.A.; Chandane, M.M. Trust-based co-operative routing for secure communication in mobile ad hoc networks. *Digit. Commun. Netw.* **2024**, *10*, 1079–1087. [CrossRef]
17. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [CrossRef]
18. Thaenchai, C.; Kanjanasit, K.; Chantara, W. Enhancement of network performance using sigmoid-based metrics on a routing protocol. In *Proceedings of the 22nd International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, Bangkok, Thailand, 20–23 May 2025; IEEE: Piscataway, NJ, USA, 2025; pp. 1–6. [CrossRef]
19. Pan, C.; Lu, H.; Shi, H.; Wang, Y.; Qin, L. Inverse coupled simulated annealing for enhanced OSPF convergence in IoT networks. *Electronics* **2024**, *13*, 4332. [CrossRef]

20. Thaenchakun, C.; Kanjanasit, K. A comparative study of OSPF metrics in routing algorithms for dynamic path selection in network security. *ASEAN J. Sci. Technol. Rep.* **2025**, *28*, e256556. [\[CrossRef\]](#)
21. 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.; Springer: Berlin, Germany, 2009; Volume 5844, pp. 78–89. [\[CrossRef\]](#)
22. Buchegger, S.; Boudec, J.-Y.L. Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile ad hoc Networking & Computing (MobiHoc)*, New York, NY, USA, 9–11 June 2002; Association for Computing Machinery: New York, NY, USA, 2002; pp. 226–236. [\[CrossRef\]](#)
23. Hu, Y.-C.; Perrig, A.; Johnson, D.B. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.* **2005**, *11*, 21–38. [\[CrossRef\]](#)
24. Hu, Y.-C.; Johnson, D.B.; Perrig, A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Netw.* **2003**, *1*, 175–192. [\[CrossRef\]](#)
25. Darville, C.; Höfner, P.; Ivankovic, F.; Pam, A. Advanced models for the OSPF routing protocol. *Electron. Proc. Theor. Comput. Sci. (EPTCS)* **2022**, *355*, 13–26. [\[CrossRef\]](#)
26. 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*, 1395–1405. [\[CrossRef\]](#)
27. Mehraban, S.; Yadav, R.K. Traffic engineering and quality of service in hybrid software defined networks. *China Commun.* **2024**, *21*, 96–121. [\[CrossRef\]](#)
28. Bahnas, A.; Louhab, F.E.; Khat, A.; Badri, A.; Talea, M.; Pandey, B. Smart hybrid SDN approach for MPLS VPN management and adaptive multipath optimal routing. *Wirel. Pers. Commun.* **2020**, *114*, 1107–1131. [\[CrossRef\]](#)
29. 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. [\[CrossRef\]](#)
30. Yao, J.; Wang, Y.; Li, Q.; Mao, H.; El-Latif, A.A.A.; Chen, N. An efficient routing protocol for quantum key distribution networks. *Entropy* **2022**, *24*, 911. [\[CrossRef\]](#) [\[PubMed\]](#)
31. Drif, Y.; Bedhief, I.; Chatzinotas, S. Distributed key relay: OSPF for effective QKD. *IEEE Commun. Standards Mag.* **2025**, *10*, 154–161. [\[CrossRef\]](#)
32. Biradar, A.G. A comparative study on routing protocols: RIP, OSPF and EIGRP and their analysis using GNS-3. In *Proceedings of the 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Jaipur, India, 1–3 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5. [\[CrossRef\]](#)
33. Tsochev, G.; Popova, K.; Stankov, I. A comparative study by simulation of OSPF and EIGRP routing protocols. *Inform. Autom.* **2022**, *21*, 1240–1264. [\[CrossRef\]](#)
34. Nedyalkov, I. Benefits of using network modeling platforms when studying IP networks and traffic characterization. *Computers* **2023**, *12*, 41. [\[CrossRef\]](#)
35. Golightly, L.; Modesti, P.; Chang, V. Deploying secure distributed systems: Comparative analysis of GNS3 and SEED Internet Emulator. *J. Cybersecur. Priv.* **2023**, *3*, 464–492. [\[CrossRef\]](#)
36. Prasad, B.; Yogita; Yadav, S.S.; Kumar, N.; Pal, V. BAT: Barabasi–Albert with Topsis scale-free topology evolution for load-balanced WSNs. *IEEE Sens. J.* **2023**, *23*, 17627–17637. [\[CrossRef\]](#)
37. Park, H.; Kim, M.-S. LineageBA: A fast, exact and scalable graph generation for the Barabási–Albert model. In *Proceedings of the IEEE 37th International Conference on Data Engineering (ICDE)*, Chania, Greece, 19–22 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 540–551. [\[CrossRef\]](#)
38. Jaiswal, S.K.; Pal, M.; Sahu, M.; Sahu, P.; Dev, A. EvoCut: A new generalization of Albert–Barabási model for evolution of complex networks. In *Proceedings of the 22nd Conference of Open Innovations Association (FRUCT)*, Jyväskylä, Finland, 15–18 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 67–72. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.