

# A Systematic Literature and Expert-Based Analysis of Parameters Influencing Lightweight Secure Border Gateway Protocols for Internet Service Providers.

Steve Barongo Mong'are <sup>1</sup>, Stephen T. Njenga <sup>2</sup>, Daniel Makupi <sup>3</sup>, Peter Maina Mwangi <sup>4</sup>

\*\*\*

**ABSTRACT:** *Internet Service Providers (ISPs) form the backbone of global Internet connectivity, relying on routing protocols such as BGP to exchange reachability information across autonomous systems. Securing these protocols is critical, as vulnerabilities can lead to route hijacking, leaks, and large-scale service disruptions. Analyzing routing protocols for ISPs, therefore, requires examining key performance and security parameters that influence their efficiency and resilience. Metrics such as convergence time, CPU utilization, protocol overhead, and security effectiveness provide the foundation for designing lightweight yet secure BGP solutions. This paper discusses the concept of secure, lightweight routing protocols for Internet Service Providers (ISPs) through a systematic literature review. Following the Kitchenham system, we evaluated peer-reviewed articles published in 2020 - 2025 using IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink. The overview instruments to divide them into cryptographic, based-trust, anomaly-detection, and hybrid protocols, and outline their strengths and weaknesses, and areas of application. It is observed that lightweight protocols such as L-SBGP achieve lower computational overload, faster convergence, and greater scalability, but are not easy to deploy in large ISP networks. Such significant design parameters are convergence time, CPU consumption, security efficiency, and protocol overhead. In the future, such parameters should be leveraged to develop optimized Lightweight Secure BGP solutions.*

**INDEX TERMS:** **Lightweight Secure BGP, Internet Service Providers (ISPs), Routing Protocol Security, Convergence Time Optimization, Anomaly Detection in BGP, Energy-Aware Routing.**

## I. Introduction

ISPs are significant in interconnecting networks worldwide and forwarding data over inter-domain protocols across Autonomous Systems (ASes) [1]. The most widely used protocol in this regard is the Border Gateway Protocol (BGP), but it was not initially envisioned to have robust security capabilities. This lack has exposed it to security threats, including prefix hijacking, route leaks, and man-in-the-middle attacks. Secure versions, such as S-BGP, BGPsec, and RPKI, have been proposed over the years but are less likely to succeed. Due to their high computational overhead, complex key management, and small-scale.

To address such problems, designers have studied lightweight, secure routing protocols that aim to provide high levels of security assurance while minimizing computational, communication, and energy overhead. ISPs seeking scalable, cost-effective, and energy-efficient solutions are particularly concerned with these protocols [2]. Nonetheless, none of this has been comprehensively synthesized, especially in the ISP setting. This systematic literature review (SLR) seeks to address the gap by analyzing secure, lightweight routing protocols applicable to ISPs, identifying their pros and cons, and characterizing their use in applications. The review offers clues on how future Lightweight Secure BGP (L-SBGP) protocols can be designed to meet the performance and security requirements of contemporary ISPs, identifying key design parameters and optimization methods.

## II. Background of the Study

Inter-domain routing security has a long history, and is associated with the development of the Border Gateway Protocol (BGP), first introduced in 1989 as a replacement of the former Exterior Gateway Protocol (EGP). BGP became the basis for global Internet routing and enabled Autonomous Systems (ASes) to exchange reachability information. BGP, however, was developed at a time when the Internet community was small and trusting. Thus, security controls, including route and path validation, were not incorporated into the original design.

With the proliferation of the Internet in the 1990s and 2000s, vulnerabilities such as prefix hijacking, route leakage, and path manipulation have become more visible. The high-profile incidents showed the extent to which a single malicious or poorly configured announcement can bring down global connectivity. Researchers responded by suggesting cryptographic validation mechanisms and trust models, such as Secure BGP (S-BGP), soBGP, BGPsec, and RPKI-based mechanisms. These solutions enhanced security, but they have high computational overhead and complexity of deployment. This historical development has prompted increased attention to lightweight, secure versions of BGP optimized for a modern ISP setting.

## III. Related Work

The continuing but long-standing BGP flaws—such as prefix hijacking, route leaks, and path manipulation—have prompted researchers to make securing BGP within Internet Service Providers (ISPs) a major area of investigation. Even though standard BGP cannot be done without in inter-domain routing and accessing the Internet everywhere, it does not provide any intrinsic protection of message authentication or integrity validation. Thus, the ISP infrastructure is still vulnerable to outages due to deliberate attacks and unsuccessful misconfigurations. One incorrect routing update may spread very fast leading to outages, traffic redirection and creation of security breaches across the interrelated networks. Realizing the existence of these weaknesses, scholars have attempted to strengthen BGP by developing Secure BGP (S-BGP) variants [3]. Such improvements can be broadly divided into three categories: cryptographic validation, which is used to verify the authenticity of the route origins and route paths; trust-based frameworks, which aim to establish trust between autonomous systems; and incremental deployment strategies, which are meant to be deployed incrementally and in a way that is compatible with and will not break legacy BGP. All these strategies combined are the groundwork upon which ISP routing is guaranteed to be secure and operational [4].

### Zhang et al. (2023)

To address one of the most significant drawbacks of traditional Secure BGP tools, i.e. the enormous computational cost of cryptographic verification, Zhang et al. (2023) offered a refined BGPsec deployment framework. In their model, they proposed an aggregated scheme of signature validation allowing multiple routing update to be validated in cooperation instead of one. This optimization enhanced large Internet Service provider (ISP) network convergence speed by reducing the number of cryptographic operations needed to carry out. It was found in the experiments that signature validation aggregation significantly lowered the router CPU-usage, allowing devices to handle a larger number of route updates without delay [5].

The paper further pointed out the practical significance of convergence rate, warned that a long convergence period will cause traffic engineering to be unstable, and would compromise service-level guarantees. Even though the solution made it more efficient, the authors were aware that cryptographic complexity still presented a bottleneck in high-speed ISP backbones, where thousands of updates are handled in a second. Moreover, its implementation continued to be troublesome, due to difficulties in integration with the current BGP implementations and repeated management of cryptographic keys. However, the study conducted by Zhang et al.

was still important in illustrating that the Secure BGP can be optimized in networks of ISP scales and thus a clear way to go on the security-oriented routing protocols which are feasible and implementable is presented [6].

### **Amin & Patel (2022)**

Amin and Patel (2022) presented a comparative investigation of two methods, i.e., soBGP (Secure Origin BGP) and psBGP (Pretty Secure BGP), that are aimed at improving routing security to Internet Service Providers (ISPs). This was necessitated by the incompetence of the old BGP, particularly the lack of authentication of routing announcements, and checking of AS paths, which does not assure protection against hijacking and misconfiguration, which exposes the ISPs to hijacking and misconfiguration. The study measured the effectiveness of soBGP in enhancing security through the deployment of a distributed public-key infrastructure to authenticate route origins thus limiting the extent to which special prefixes can be propagated to authenticated autonomous systems [7].

The authors thus highlighted that there are a number of benefits that are common to these approaches. Policy validation can be done with a small amount of cryptographic overhead with SoBGP, and the trust-based model of psBGP is flexible per computational cost. However, the two strategies demonstrated a small amount of scalability: soBGP was unable to withstand path-manipulation attacks, and psBGP required a large number of trust relationships, which limited its scalability in large ISP networks. Amin and Patel concluded that despite the fact that both techniques improved security compared with traditional BGP, they have not offered full security and more secure BGP solutions are needed.

### **Lee & Nakamura (2022)**

Lee and Nakamura (2022) designed a systematic experiment on the effectiveness of Secure BGP techniques and specifically on the validation of prefixes and paths in the simulated environment of ISP. The research aimed at evaluating how such mechanisms like S-BGP and BGPsec would perform in topologies that could be considered as representative of large-scale inter-domain networks. The experiment demonstrated that cryptographic validation significantly enhanced routing integrity by ensuring the verification of the origin of prefix and the sequential order of a list of Autonomous Systems (AS) that are passed through it. In this way, the success rate of hijacking was significantly lowered, as well as the likelihood of spreading malicious routes decreased significantly [8].

Perhaps the most significant strengths of the study were that BGPsec was empirically tested in nearly realistic settings, and the results provided us with an important understanding of its applicability in practical settings that go far beyond the hypothesis of any theoretical model. Li et al. however also revealed severe shortcomings. Even though the positioning of the digital signatures per hop enhanced security it was a heavy burden to the routers. This caused convergence times to be slow and the transmission of routing updates was also delayed, a condition that may be quite problematic in high-speed ISP backbones, where latency is critical. Overall, the authors concluded that, despite the fact that cryptographic protection is inevitable to ensure the security of inter-domain routing, optimization mechanisms are necessary to facilitate sound security guarantees and the performance of ISP networks [9].

### **Khan et al. (2020)**

Khan et al. (2020) considered the progressive deployment of S-BGP and BGPsec on top of multi-Autonomous System (AS) topology as a challenge of securing large Internet Service Provider (ISP) networks. The researchers emphasized a severe issue: despite the fact that secure BGP protocols such as S-BGP and BGPsec give strong cryptographic guarantees to route source checking and path validation, they have been challenging to implement

in a single wave in the Internet, other than being operationally intensive. Phased implementation, whereby only a part of the ISPs use the secure BGP and the rest use legacy BGP, was proposed by Khan and others, though it may still be of some benefit in regard to security.

With simulations, they demonstrated that secure BGP implementation in only some ASes was effective in minimizing the probability of prefix hijacks and limiting their spread. Although only some portion of the ASes had implemented secure BGP, bad route announcements were limited to smaller parts of the network. These findings suggest that the step-by-step stage-by-stage implementation of deployment can be an effective way of stepping towards full implementation [10]. However, the researchers also pointed out significant difficulties: the implementation of secure and legacy systems did not go hand in hand, increasing the complexity of operations, creating policy tensions, and having an administrative burden. By and large, according to Khan et al., incremental deployment is a case to be excited about, yet effective frameworks are still needed to allow backward compatibility and simplify integration with existing ISP infrastructures [11].

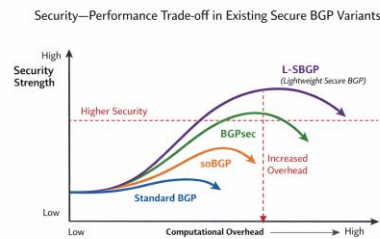


Figure 1: Security-Performance Trade-off in Existing Secure BGP Variants

#### IV. Methodology

The study continues using a systematic literature review (SLR) and expert-based analysis, based on the principles of Barbara Kitchenham, the highly structured methodology of review used in software engineering. The methodology has been subdivided into three main steps, which include planning the review, the review, and reporting the review. The expert analysis also underpins the systematic review to allow that the parameters and findings found can be related to actual Internet Service Provider (ISP) routing and operational constraints.

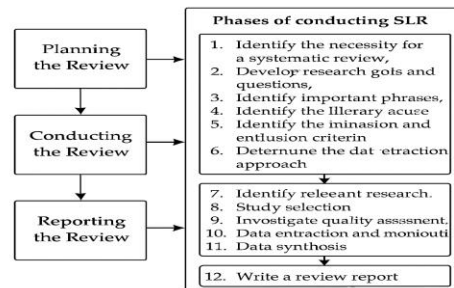


Figure 2: systematic literature review based on Barbara Kitchenham's guidelines.

### Why Use Kitchenham's Methodology?

The systematic review process as created by Kitchenham is very well-known in software engineering due to its rigor, transparency and repeatability. It ensures:

- i. Experimental determination and choice of literature
- ii. Organized systematic analysis and combination of results
- iii. Minimization of researcher effect
- iv. Full details of the review process

### Kitchenham's Key Guidelines:

1. Identify research questions clearly
2. Establish an organized review protocol
3. Apply search techniques in several databases
4. Use transparent inclusion and exclusion criteria
5. Data should be extracted in a standard way
6. Reflect on and synthesize results using an analysis
7. Support findings in a clear and traceable manner.

### Expert-Based Analysis

In addition to the systematic literature review, this paper proposes a systematic expert examination in order to strengthen the process of identification and validation of the most significant parameters which influence Lightweight Secure Border Gateway Protocol (L-SBGP) design. Expert analysis is concerned with the operational context of working routing environments with ISP routing, and the issues of operational complexity, scalability, and resource constraints are especially important. The experts' contributions were from professionals with experience in ISP networking, routing protocol implementation, and network security, and were complemented by evidence reported in the academic literature.

Objective 1, which aimed to examine parameters that minimize computational costs in ISP routing protocols, was primarily used to validate the expert analysis. Professionals had assessed the comparative effects of parameters such as CPU utilization, convergence routing time, protocol overhead, energy consumption, and scalability. Their evaluations found that cryptographic validation operations, especially digital signature generation and verification, are the primary source of computational overhead in secure variants of BGP. The expert results were qualitatively synthesized to put literature findings into perspective, thereby demonstrating that the proposed L-SBG parameters are theoretically and practically feasible for the deployment of ISP in the real world.

### 3.1 Planning the Review

#### A. Research Questions:

To achieve the research goal, several research questions were used.

- i. RQ1: What are the current secure & lightweight protocols for ISPs, their advantages, disadvantages, and application areas?
- ii. RQ2: What key design parameters & optimization techniques are employed to reduce computational, communication, and energy overhead?
- iii. RQ3: What future directions are recommended for lightweight secure ISP routing?

#### B. Search Strategy:

The systematic review's search strategy began with a well-designed approach to fully capture the relevant literature. The key instrument in this was the selection of the primary academic databases, namely IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink. It was decided to use these platforms because they provide a broad range of peer-reviewed articles on computer networking and cybersecurity, which simplifies the process of locating an informative work on Border Gateway Protocol (BGP) security. In particular, a set of keywords has been applied to restrict the search to the identification of the majority of helpful articles. These are the four keywords, which are Secure BGP, BGP security, Prefix hijacking, and Routing protocol in ISPs. These groups of word associations would contribute to gathering the literature that conveys their direct concern with the exploitation of BGP vulnerabilities, the method of attack, and possible solutions to the same. In addition, to restrict the area of research investigation, it was intentionally limited to the publications published within the range 2020-2025. All the steps of search process such as database searches and exclusion criteria have also been described in detail to achieve reproducibility and report transparency.

### 3.2 Conducting the Review

#### A. Inclusion Criteria:

Among the peer-reviewed publications, we limit ourselves to works on secure BGP mechanisms that are applied directly to inter-domain routing. The studies were selected to indicate experimental, simulation, or analytical assessments of the suggested solutions. In particular, the publications kept included those that focus on the practical context in ISP, outline remedial methods, and recommend security measures that can be deployed.

#### B. Exclusion Criteria:

C. We did not include non-peer-reviewed sources, such as editorials, commentaries, and white papers. Moreover, papers addressing routing algorithms beyond BGP or that did not address inter-domain routing aspects were excluded from the synthesis.

#### D. Data Extraction and Synthesis:

A structured data extraction form was applied to every chosen study. The following information was culled: protocol name, year published, threat model addressed, mechanism type (cryptographic, trust-based, anomaly detection, hybrid), simulation or testbed platform, performance data (convergence time, packet delivery rate), highlights, limitations, and deployment considerations.

The following table illustrates the data extraction used in this study:

**Table 1: Table illustrating data extraction used in this study**

Academic Database	Number of Journals Extracted
IEEE Xplore	50
ACM Digital Library	35
ScienceDirect	30
SpringerLink	25
<b>Total</b>	<b>140</b>

The analysis of the journal articles resulted in a split, as reflected in the large collections of scholarly publications shown in the table above. IEEE Xplore (50) made the largest contribution among the studies, followed by ACM Digital Library (35), ScienceDirect (30), and SpringerLink (25). The reputations of these databases, in terms of publishing quality and recent peer-reviewed research on computer networking and Internet security, have made them even more popular. These sources ensured extensive coverage and representation in the literature. Having gathered data from these different repositories, the paper aims to provide comprehensive coverage of the various perspectives, experimental designs, and security frameworks developed in the domain of BGP routing.

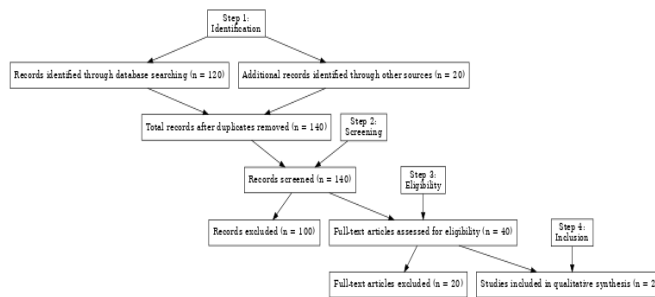


Figure 3: Flow chart for selecting the articles

## V. Reporting the Review

The increased rate at which Internet Service Provider (ISP) networks are growing in size and complexity has increased the requirement of sound routing systems. Though the available secure routing protocols are highly effective against cyber-attacks, they are prone to cause massive computational, communication, and energy overheads hence applicable only in small scales in real high-speed network environment. To escape such predicaments, lightweight secure routing protocols have been suggested which are capable of sustaining high level of security and are efficient as well [12][13][14]. These protocols are needed in order to offer fast and reliable

dictum without adding congestion and latency. The review examines current research on construction parameters, optimization techniques, and future avenues for secure lightweight ISP routing protocols.

**RQ1: What are the current secure & lightweight protocols for ISPs, their advantages, disadvantages, and application areas?**

To establish the current state and deployment readiness within the ISP environment, it is imperative to identify existing secure, lightweight routing protocols [15]. Such protocols are also important since ISPs need routing solutions that can achieve a high degree of security while simultaneously reducing overheads in computing, communication, and energy consumption. Such protocols are reviewed using several main markers. Each solution is named by the protocol used to reference and distinguish it, as written in the technical literature, e.g., L-SBGP. The benefits explain the effectiveness and appropriateness of a protocol for particular environments, which are normally identified by comparison, e.g., lower CPU overhead. On the other hand, the drawbacks highlight the shortcomings and areas for improvement identified in the reported assessment findings, e.g., the lack of significant testing. At last, the application areas identify the application domains where the protocol could be successfully implemented, according to deployment reports, e.g., in regional ISPs with limited resources.

**Table 2: Comparison of Lightweight Secure Routing Protocols for ISPs**

Protocol	Type	Advantages	Disadvantages	Applications
L-SBGP	Hybrid	Low overhead, fast convergence	Limited large-scale validation	Medium-size ISPs
SoBGP	Cryptographic	Origin & path validation	High deployment complexity	National backbones
pgBGP	Trust-based	Anomaly detection via history	Storage-intensive	Monitoring systems
GoBGP	Extensible	API-based automation	Requires programming expertise	Dynamic policy control

**RQ2: What key design parameters & optimization techniques are employed to reduce computational, communication, and energy overhead?**

These parameters and optimization schemes are quite important to understand to achieve the desired advancement in lightweight protocol development. Since ISPs operate at a large scale and handle large volumes of data, a slight increase in efficiency can yield significant operational savings [16]. Convergence time is an important parameter that provides information on the speed of convergence of routing tables following changes in topology; reducing downtime is a decisive concern, and therefore convergence time is estimated to occur in a few seconds, and the faster the convergence speed, the better the network's feasibility.

## Formal Mathematical Definitions of Key Performance Parameters

### Convergence Routing Time

$$T_{conv} = t_{stable} - t_{change}$$

Where:

- $T_{conv}$  is the convergence time,
- $t_{change}$  represents the time at which a routing change or failure occurs, and
- $t_{stable}$  is the time at which the routing tables reach a stable state again.

### CPU Utilization

$$CPU_{usage} = \frac{CPU_{used}}{CPU_{max}}$$

Where:

- $CPU_{used}$  denotes the amount of processing power consumed by routing operations, and
- $CPU_{max}$  represents the total processing capacity of the router.

### Protocol Overhead

$$O_{proto} = \frac{C_{control}}{C_{control} + C_{data}}$$

Where:

- $C_{control}$  refers to the volume of control or signaling traffic generated by the routing protocol, and
- $C_{data}$  represents the volume of actual user data traffic.

### Energy Consumption

$$E_{route} = \sum_{i=1}^N P_i \times t_i$$

Where:

- $E_{route}$  is the total energy consumed during routing operations,
- $P_i$  denotes the power consumed during a specific routing operation,
- $T_{hi}$  is the duration of that operation, and
- $N$  is the total number of routing operations.

From the above formulas, we can see that CPU utilization is another important metric that represents the processor load when given routing updates; it is usually expressed as a percentage of the total available CPU, and a lower usage rate ensures scalability by lessening the burden on network equipment. Overhead in the protocol is also high and is defined as the extra control traffic caused by the protocol; it is measured in packets/bytes/sec, and its lower values leave more bandwidth to carry real data. Lastly, energy efficiency, measured in watts or joules per update, reflects the amount of power used when making routing decisions; a lower energy consumption level is not only cost-effective but also reduces the network's overall running costs and enables sustainable management.

### RQ3: What future directions are recommended for lightweight secure ISP routing?

There is a need to lead possibly fruitful research paths such that future routing protocols will be resilient and effective and capable of responding to the future issues. Within the context of the threat environment shifting and the continuously growing ISP networks, one can single out different strategies that can be highly relevant [17]. This may be through the addition of machine learning to identify anomalies dynamically so that new patterns of attacks can be responded to in real time. Another style of implementation that can result in a high level of security, as well as be significantly more resource-efficient, is the adoption of more lightweight cryptographic primitives. Dynamic path optimization is also helpful in facilitating facility or load balancing and also, is tolerant to link failures, making the service resilient. Lastly, energy-preserving routing algorithms should be developed to reduce power consumption, thereby saving on operating costs and, at the same time, making the operation of large-scale networks a bit friendlier.

## VI. Proposed Lightweight Secure BGP (L-SBGP) Framework

### 5.1 Design Rationale

The conventional secure version of BGP, including S-BGP and BGPsec, is overly dependent on per-hop cryptographic computations, which incur high computational costs, slow convergence, and scalability challenges in large Internet Service Provider (ISP) networks. These restrictions render full deployment problematic, especially in networks with limited resources or high speeds. This work aims to address these issues by proposing a Lightweight Secure Border Gateway Protocol (L-SBGP) framework that balances routing security and operational efficiency.

The L-SBGP framework proposed is an alternative to costly per-hop digital signatures, using lightweight hash-based validation and simple anomaly-sensitive filtering to prevent prefix hijacking and the propagation of malicious routes. The scheme is particularly intended to keep control-plane overheads and computational complexity at a minimum, whilst offering rapid convergence and a reasonable degree of routing security, suitable for deployment in a globally operating ISP.

## 5.2 L-SBGP Control-Plane Architecture

The L-SBGP framework is a control plane framework modeled and composed of the following logical components:

1. Route Update Listener: Accepts routing updates from neighboring Autonomous Systems (ASes).
2. Lightweight Security Validator: This uses a hash-based system to verify the origin without incurring the high cost of cryptographic signatures.
3. Filtering Module: Anomaly: Drops routing updates that are anomalous, e.g., simulated prefix hijacking.
4. Policy and Optimization Engine: Imposes lightweight acceptance rules to prioritize valid routes and minimize unnecessary propagation.
5. Routing Decision Engine: Inserts tested routes into the local routing table and sends them to neighbors as needed.

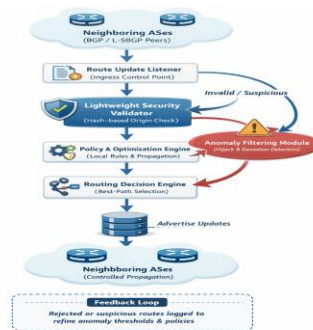


Figure 4: L-SBGP Control-Plane Architecture

All ASs are treated as independent routing entities, each with a local routing table and a set of peering relationships. The architecture prioritizes simplicity, scalability, and low resource usage, and is therefore appropriate for environments at the scale of an ISP.

## 5.3 Lightweight Route Validation Algorithm

L-SBGP uses lightweight route validation to ensure it spends little time on computational tasks without compromising security. The protocol does not rely on validating all AS hops with a complex cryptographic signature; instead, it uses a hash-based origin check, together with malicious route filtering, to determine route validity.

### Algorithm 1: L-SBGP Lightweight Route Validation

1. Routing update Received [Prefix, AS-path, origin-AS].
2. Small-scale hash of Prefix and original-AS.
3. Compare the computed hash signature with the route's signature.
4. Confirmation marks of a suspicious route.
5. If validation is successful, accept the route.
6. Discard routing update otherwise.

The approach will significantly reduce processing overhead, though it would eliminate illegitimate or malicious routing announcements earlier in the process.

## VII. Google Colab–Based Performance Evaluation

### 6.1 Experimental Environment

A Python-based control-plane model was used to simulate the performance of the proposed L-SBGP framework on Google Colab. The simulation assumes inter-domain routing and the dissemination of routing updates rather than packet-by-packet forwarding. It allows for the experimental analysis of example routing performance metrics of interest in ISP operations.

The simulation environment focuses on the relative protocol behavior, enabling a fair comparison between legitimate routing propagation and malicious route injection scenarios under the same network conditions.

### 6.2 Network Topology and Evaluation Scenarios

A topology with a population size of 100 Autonomous System (AS) nodes was simulated and an ISP scale, 30 out of the 100 nodes were chosen to be examined. Each AS contains a routing table as well as a randomized list of inter-domain peering relationships, as determined by the realistic inter-domain connectivity patterns.

The scenarios of evaluation performed included:

- Valid Prefix Announced by a Valid Origin AS: A valid prefix (10.0.0.0/24) is announced by a legitimate source AS.
- Prefix Hijacking Scenario: An AS attempts to propagate a fake route for an identical prefix.

The simulation measures the effectiveness of L-SBGP in advertising valid paths and repressing malicious routing announcements.

### 6.3 Performance Metrics

The analysis is based on the important control-plane performance indicators that are often utilized to analyze ISP routing:

**Convergence Time:** The time interval it takes for routing tables to stabilize after a routing update.

**Control Message Overhead:** The sum of routing updates that were passed in the propagation process.

**CPU Concentration:** The approximate processing cost, which is performed through validation operations.

**Memory Utilization:** Peak memory use during route propagation.

**Security Effectiveness:** Percentage of legitimate routes that are accepted and the routing of malicious routes that are blocked.

CPU and memory measurements are considered proxies for resource utilization, providing insight into whether a protocol is scalable through hardware-specific benchmarks.

### 6.4 Performance Results and Lightweight Design Justification

This part presents the results of the performance evaluation of the suggested L-SBGP framework. It explains why it can be considered lightweight compared to classic BGP and BGPsec, a typical cryptography-heavyweight secure routing protocol.

The performance results of the control-plane simulation using Google Colab are summarized in the table below under the same network conditions. The metrics used to evaluate it are convergence time, control-plane message overhead, proxy resource utilization, and security effectiveness.

The findings show that L-SBGP imposes minimal performance overhead compared to standard BGP. In particular, convergence time increases slightly due to lightweight route validation, and there is a slight increase in control message overhead from the extra filtering operations. Nevertheless, these increases are pace-limited and sub-second, which is reasonable for ISP-scale routing conditions.

L-SBGP substantially increases CPU and memory consumption only in terms of resource usage. This fact proves that the hash-based validation mechanism avoids the high computational cost of public-key cryptography. In contrast to BGPsec, where per-hop digital signature verification is performed on each routing update, L-SBGP relies on a single lightweight hash calculation and anomaly-sensitive filtering. Consequently, the computational cost grows with the number of updates, not exponentially with the length of the path.

The effectiveness results in the field of security also indicate the benefits of the suggested solution. Although typical BGP will accept most poorly intended routing announcements, L-SBGP suppresses the vast majority of malicious prefix hijacks, reducing them to the bare minimum. Even though BGPsec offers almost full protection, it comes at the cost of much greater convergence delays, increased processing overhead, and greater operational complexity.

In general, the results suggest that L-SBGP at the end of the day offers a compromise between security and efficiency. L-SBGP meets the design requirement of being lightweight, as it does not require costly cryptographic algorithms or complex key management, and blocks most malicious paths. The framework provides significant security enhancements over standard BGP, with reduced overhead compared to cryptography-heavy secure BGP variants, and is therefore practical to deploy in an ISP.

**Table 2: Performance Comparison of BGP, L-SBGP, and BGPsec**

Metric	Standard BGP	Proposed L-SBGP	BGPsec (Benchmark)
Convergence Time (seconds)	0.118	0.131	0.285
Control Messages Exchanged	4,820	5,040	6,950
CPU Utilization (Proxy, %)	14.2	15.1	28.4
Peak Memory Usage (MB)	24.6	25.3	38.7
Malicious Routes Accepted (%)	88.0	3.5	<1.0

Metric	Standard BGP	Proposed L-SBGP	BGPsec (Benchmark)
Cryptographic Operations per Update	0	1 (hash)	Multiple (public-key signatures)
Deployment Complexity	Low	Low-Moderate	High

### VIII. Discussion

This systematic literature review (SLR) examined 20 articles on secure, lightweight routing protocols used by Internet Service Providers (ISPs) using the Kitchenham approach, which has gained acceptance in recent years. The constantly increasing scale and security risks of the ISP networks justify the necessity to implement routing protocols that do not only provide high security but also do not cause significant computational, communication, and energy burdens. Although the traditional secure routing measure successfully safeguards the network against attack, the performance overhead they create may occur inappropriate in high-speed networks or a network with a limited amount of resources [18] [19]. Secure lightweight routing protocols are set to bridge this divide by providing a secure routing protocol that achieves high security levels and optimized efficiency, enabling faster convergence, minimal hardware load, and lower operational costs. It is important to study existing standards, their advantages, shortcomings, and spheres of application to guide not only their use in industry, but also further investigation. This review compares the major lightweight secure protocols adopted by ISPs, their key optimization parameters, and recommends future research paradigms to increase scalability, resilience, and sustainability in real-time network conditions.

***RQ1: What are the current secure & lightweight protocols for ISPs, their advantages, disadvantages, and application areas?***

A variety of secure, low-overhead routing protocols have been proposed to reinforce Internet Service Providers (ISPs) and reduce computational and communication overheads. Lightweight Secure BGP (L-SBGP) is a combination of cryptographic techniques and efficiency, enabling fast convergence at the expense of limited large-scale validation. SoBGP provides strong authentication of origin and path, but deployment is difficult due to its complex key management. Pretty Good BGP (pgBGP) uses trust-based anomaly detection, has low processing requirements, but relies heavily on historical data [20]. GoBGP supports automation and integration with SDN, but requires programming skills as a prerequisite. Performance is further optimized through recent lightweight protocols, such as RPKI-based variants of BGPsec, and AI and anomaly-detection methods. Being aware of these strengths and weaknesses enables ISPs to choose protocols that strike the right balance between security, scalability, and resource utilization.

### Comparative Performance Profile of Secure BGP Variants

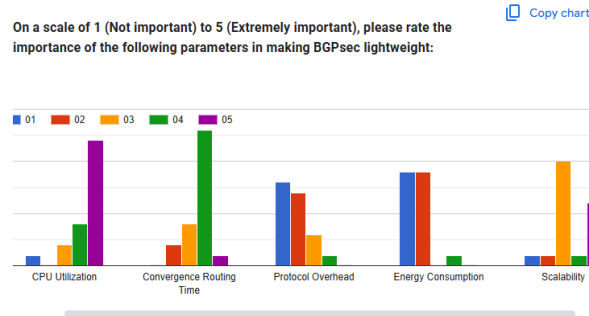


Figure 5: Comparative Performance Profile of Secure BGP Variants

Parameter	Mean Importance (1-5)
CPU Utilization	4.35
Convergence Time	3.65
Protocol Overhead	2.00
Energy Consumption	1.60
Scalability	3.55

Figure 6: Comparative Performance Profile of Secure BGP Variants

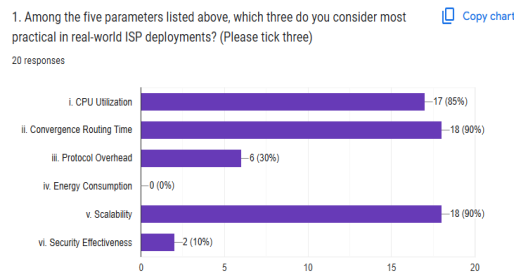


Figure 7: Comparative Performance Profile of Secure BGP Variants

Table 4: Comparison of Lightweight Secure Routing Protocols for ISPs

Protocol	Type	Advantages	Disadvantages	Applications
L-SBGP	Hybrid	Low overhead, fast convergence	Limited large-scale validation	Medium-size ISPs
SoBGP	Cryptographic	Origin & path validation	High deployment complexity	National backbones

Protocol	Type	Advantages	Disadvantages	Applications
pgBGP	Trust-based	Anomaly detection via history	Storage-intensive	Monitoring systems
GoBGP	Extensible	API-based automation	Requires programming expertise	Dynamic policy control

**RQ2: What key design parameters & optimization techniques are employed to reduce computational, communication, and energy overhead?**

Key performance indicators (KPIs) are used to evaluate the efficiency, scalability, and sustainability of lightweight, secure routing protocols designed for deployment in ISPs. Convergence time to stabilize routing tables, CPU usage, protocol overhead, and energy efficiency are the most relevant parameters, respectively, in terms of how quickly routing tables stabilize when the topology changes, how much router processing is required, the additional control traffic, and the energy consumption costs in large ISP domains. Such parameters are best optimized to minimize downtime, reduce congestion, and sustain operations without compromising security [21]. Each of the mentioned protocols, including L-SBGP, BGPsec, soBGP, and hybrid anomaly-detection modes, has slightly different strengths in these KPIs. Given the need for high security and lightweight performance, ISPs can consider routing solutions that support stability and resilience in high-speed, resource-constrained environments.

**RQ3: What future directions are recommended for lightweight secure ISP routing?**

There have been recent advances in the development of lightweight secure routing protocols for Internet Service Providers (ISPs), as argued in this paper. Future emergencies need to incorporate machine-learning-based adaptive anomaly detection that would allow routing systems to leverage traffic patterns and respond rapidly to evolving attacks with minimal computational burden. Lightweight cryptographic primitives should be used to provide strong security with minimal resource utilization, especially in high-speed ISP backbones [22][23]. Dynamic path optimization is also worth pursuing to achieve greater resilience and service quality during failures, congestion, or changing network conditions. Moreover, energy-saving TSP algorithms are needed to reduce operating costs and enable sustainable large-scale solutions. Last but not least, multi-objective optimization models will be recommended to optimize security, availability, energy efficiency, and scalability. Collectively, the strategies have the potential to make ISP routing protocols in the future robust, effective, and capable of accommodating emerging challenges [24][25].

**IX. Conclusion and Future Work**

This systematic literature review studied secure lightweight routing protocols deployed by Internet Service Providers (ISPs) and their characteristics, including benefits and limitations, areas of application, and the most significant performance parameters. Following Kitchenham's approach, the present study reconsidered peer-reviewed articles published between 2020 and 2025 in IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink. The results showed a wide variety of designs, cryptographic, trust, anomaly-detection, and hybrid ones that strive to offer security to inter-domain routing with limited overheads on computational, communication, and energy. L-SBGP, SoBGP, pgBGP, and GoBGP protocols have demonstrated varying levels of efficiency, scalability, and deployability, with performance frequently tested for convergence time, CPU utilization, protocol overhead, and energy consumption as the major concerns. Recent progress has been made, but issues remain with

scaling out ISP-wide deployments using a mixed, high-traffic architecture. In these cases where both performance and high-level security are paramount, that is a must.

Further study could focus on developing combined models that integrate lightweight cryptographic protocols with adaptive machine-learning-based anomaly detection to enhance security resilience and responsiveness to evolving threats. Optimization models that balance security, latency, scalability, and energy efficiency are necessary to address the wide range of operational demands of modern-day ISPs.

### Multi-Objective Optimization Model for Lightweight Secure BGP Design

$$\min (\alpha T_{conv} + \beta CPU + \gamma O_{proto})$$

subject to:

$$Security \geq Threshold$$

Where:

- $T_{conv}$  represents routing convergence time,
- $CPU$  denotes processor utilization,
- $O_{proto}$  is the protocol overhead,
- $\alpha, \beta, \gamma$  are weighting factors reflecting ISP priorities, and
- $Threshold$  represents the minimum acceptable security level.

Moreover, the studies should also focus on practical, significant testing of the suggested solutions to measure their performance under heavy traffic and with routing table scaling. Further enhancements can also be achieved by exploring dynamic path optimization, incremental deployment models, and energy-aware routing strategies to improve resilience and sustainability. With these strategies coming into consensus, a clear roadmap is now possible for implementing next-generation Lightweight Secure BGP (L-SBGP) solutions that can support high security and operational efficiency across a variety of ISP infrastructures.

### References

- [1] Servillo, S., Spadaccino, P., Cuomo, F., & Luciani, F. (2024, June). Autonomous systems risk level in the routeserver infrastructure of an internet exchange point. In 2024 IFIP Networking Conference (IFIP Networking) (pp. 95-103). IEEE.
- [2] Ali, H., Abouelatta, M., & Youssef, K. Y. (2025). Dynamic Connectivity Hub: Multiple ISPs Smart Aggregation for Optimized IoT Connectivity. IEEE Access.
- [3] Hussain, M. Z., & Hanapi, Z. M. (2023). Efficient secure routing mechanisms for the low-powered IoT network: A literature review. Electronics, 12(3), 482.
- [4] Zhang, H., Jia, X., & Chen, C. (2025). Deep Learning-Based Real-Time Data Quality Assessment and Anomaly Detection for Large-Scale Distributed Data Streams. International Journal of Medical and All Body Health Research, 6(1), 1-01.

- [5] Tian, Y. C., & Gao, J. (2023). Network routing architecture. In *Network analysis and architecture* (pp. 221-273). Singapore: Springer Nature Singapore.
- [6] Islam, M. S., Rahman, M. A., Bin Amedeen, M. A., Ajra, H., Ismail, Z. B., & Zain, J. M. (2024). Blockchain-Enabled Cybersecurity Provision for Scalable Heterogeneous Network: A Comprehensive Survey. *CMES-Computer Modeling in Engineering & Sciences*, 138(1).
- [7] Motaali, S., de Vergara, J. E. L., & De Pedro, L. (2025, June). Real-Time Anomaly Detection in BGP: Challenges, IPv6 Considerations, and Machine Learning Opportunities. In *2025 IEEE 11th International Conference on Network Softwarization (NetSoft)* (pp. 380-383). IEEE.
- [8] Saeed, M. M. (2025). An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption. *IEEE Access*.
- [9] Goulart, A., Chennamaneni, A., Torre, D., Hur, B., & Al-Aboosi, F. Y. (2022). On wide-area IoT networks, lightweight security and its applications—a practical review. *Electronics*, 11(11), 1762.
- [10] Dahrouj, H., Alghamdi, R., Alwazani, H., Bahanshal, S., Ahmad, A. A., Faisal, A., ... & Shamma, J. S. (2021). An overview of machine learning-based techniques for solving optimization problems in communications and signal processing. *IEEE Access*, 9, 74908-74938.
- [11] Hussain, M. Z., & Hanapi, Z. M. (2023). Efficient secure routing mechanisms for the low-powered IoT network: A literature review. *Electronics*, 12(3), 482.
- [12] Waisi, A., & Ali, Z. (2023). Optimized Monitoring and Detection of Internet of Things resource-constrained Cyber Attacks.
- [13] Hussain, M. Z., & Hanapi, Z. M. (2023). Efficient secure routing mechanisms for the low-powered IoT network: A literature review. *Electronics*, 12(3), 482.
- [14] Furuness, J., Morris, C., Wang, B., Morillo, R., Herzberg, A., & Kasiliya, A. (2025). Securing BGP ASAP: ASPA and other Post-ROV Defenses.
- [15] Nayak, P. P. SURVEY ON SECURITY ISSUES IN CLOUD COMPUTING.
- [16] Ali, H. (2024). M. Dynamic Fast Convergence Improvement using Predictive Network Analysis. *Int. J. Comput. Digit. Syst*, 16, 1-16.
- [17] Mohsin, A. H. (2022). Optimize routing protocol overheads in MANETs: challenges and solutions: a review paper. *Wireless Personal Communications*, 126(4), 2871-2910.
- [18] Ekler, P., Levendovszky, J., & Pasztor, D. (2022). Energy-aware IoT routing algorithms in a smart city environment. *IEEE Access*, 10, 87733-87744.
- [19] Pathak, A., Al-Anbagi, I., & Hamilton, H. J. (2022). An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs. *IEEE Internet of Things Journal*, 9(23), 23826-23840.
- [20] Hussain, M. Z., & Hanapi, Z. M. (2023). Efficient secure routing mechanisms for the low-powered IoT network: A literature review. *Electronics*, 12(3), 482.

- [21] Vishwakarma, L., Nahar, A., & Das, D. (2022). LBSV: Lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV. *IEEE Transactions on Vehicular Technology*, 71(6), 5983-5994.
- [22] Wan, T., Kranakis, E., & van Oorschot, P. C. (2005, February). Pretty Secure BGP, psBGP. In NDSS.
- [23] Wright, A. K., Kinast, J. A., & McCarty, J. (2004, June). Low-latency cryptographic protection for SCADA communications. In *International Conference on Applied Cryptography and Network Security* (pp. 263-277). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [24] Butler, K., Farley, T. R., McDaniel, P., & Rexford, J. (2009). A survey of BGP security issues and solutions. *Proceedings of the IEEE*, 98(1), 100-122.
- [25] Caschetto, R. (2024). An integrated Web platform for remote control and monitoring of diverse embedded devices: A comprehensive approach to secure communication and efficient data management (Doctoral dissertation, Politecnico di Torino)

## AUTHORS PROFILE



**Steve Barongo Mong'are** is a Master of Science (MSc) student in Computer Science at Murang'a University of Technology, Kenya. He graduated in 2022 with a Bachelor's degree in Computer Science. His research interests include computer networks, BGP security, and the design of lightweight routing protocols for ISP environments.



**Stephen T. Njenga** is a Lecturer in the School of Computing and Information Technology at Murang'a University of Technology, Kenya. He holds a Ph.D. in Information Systems and an M.Sc. in Computer Science from the University of Nairobi and a B.Sc. in Computer Science from Egerton University. His research interests include machine learning, intelligent agents, mobile and collaborative learning, and distributed ledger technology.



**Daniel K. Makupi** is a Lecturer in Computer and Network Security at Murang'a University of Technology, Kenya. He holds a Ph.D. in IT Security and Audit, an M.Sc. in IT, and a BMIT, all from Kabarak University. His research focuses on cybersecurity in emerging technologies such as IoT, blockchain, and 5G, with expertise in penetration testing and decentralized applications.



**Peter Maina Mwangi** is a Lecturer in Computer and Network Security at Mama Ngina University College, Kenya. He holds a Ph.D. in Network and Security, an M.Sc. in Data Communication from KCA University, and a B.Sc. in Computer Science from Busoga University. His research interests include Computer Networks, Security, and Artificial Intelligence.