# A LIGHTWEIGHT SECURE BORDER GATEWAY PROTOCOL FOR INTERNET SERVICE PROVIDERS' NETWORKS

**Steve Barongo Mong'are**

**A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science of Murang'a University of Technology**

**August, 2026**

## DECLARATION

**Student Declaration**

I hereby declare that this thesis is my original work and, to the best of my knowledge, has not been presented with a degree award at this or any other university. I understand what plagiarism is and am aware of the University's policy in this. I understand that any false claim regarding this work shall result in disciplinary action in accordance with the University Anti-Plagiarism Policy.

_____ _____

Steve Barongo Mong'are Date

SC400/5822/2022

**Supervisor's Approval**

The undersigned certify that they have read and hereby recommended for acceptance of Murang'a University of Technology a thesis entitled **"A Lightweight Secure Border Gateway Protocol for Internet Service Providers' Networks."**

_____ _____

Dr. Stephen Njenga Date

Department of Computer Science

Murang'a University of Technology

_____ _____

Dr. Daniel Makupi Date

Department of Computer Science

Murang'a University of Technology

## DEDICATION

This thesis has been prepared in honor of all the supporters and encouragers who have graced this research endeavor. To my supervisors, whose important support, ideas, and motivation contributed significantly to the present research on the Design of a lightweight and secure Border Gateway Protocol (BGP) for the ISPs. The researcher owes most of this to your knowledge and criticism, which have provided the background for this work. I am grateful to all my colleagues and friends for supporting, collaborating with, and encouraging me to maintain my concentration and commitment to the principal network security community, whose investigations and efforts to enhance the security of Internet infrastructure underpin this community's advancement. Finally, this work is dedicated to my family- my parents, siblings, and friends because their support and sanctions have contributed greatly towards the achievement of this work. Your belief in me has been a source of motivation, and I am happy to take this as a group achievement; it represents the effort and commitment of all of us.

## ACKNOWLEDGEMENT

I am pleased to thank all my supervisors and colleagues for their invaluable support throughout the thesis process for this study. Their knowledge and ideas have been useful in guiding this work to enhance BGP security, with a particular focus on making the protocols lightweight within ISPs. I would also like to acknowledge individuals who have made the simulation tools used to evaluate A Lightweight Secure BGP protocol available, including Network Simulator-3 and Google Colab. Finally, I would like to thank the ISP professionals who shared their experience, thereby helping make this work relevant to the real world. All these parties would not have come together and contributed so much to this project had it not been for their collaborative efforts. Our future pieces will be as well-received as this one, especially with the much-appreciated encouragement you have given.

## ABSTRACT

The Border Gateway Protocol (BGP) is the foundation of inter-domain routing on the Internet; however, its lack of built-in security makes it vulnerable to routing attacks such as prefix hijacking and route manipulation. Although secure routing protocols such as Border Gateway Protocol Security (BGPsec) improve routing security through cryptographic validation, their high computational overhead, increased convergence time, and scalability limitations hinder their practical deployment within Internet Service Provider (ISP) environments. This study therefore proposed a Lightweight Secure Border Gateway Protocol (L-SBGP) that enhances routing security while reducing the computational complexity associated with existing secure BGP implementations. The study was guided by three objectives: to analyses the parameters influencing lightweight secure BGP protocols in reducing computational overhead, to develop a lightweight secure Border Gateway Protocol for ISP environments, and to evaluate the performance of the proposed protocol. experimental research approach was adopted. A Systematic Literature Review (SLR) was conducted to identify the key factors influencing secure BGP performance, followed by an expert survey to validate the identified parameters. The findings from both approaches established CPU utilization, routing convergence time, and scalability as the principal parameters guiding the design of the proposed protocol. Based on these findings, L-SBGP was formally specified using a lightweight hash-based route validation mechanism, routing update classification, selective verification, mathematical modelling, protocol workflow, and routing algorithms. The proposed protocol was implemented using a Python-based simulation prototype executed in Google Colab and evaluated against conventional BGP and BGPsec. Performance evaluation was conducted using the average results obtained from twenty independent simulation runs under identical network conditions. The results demonstrated that L-SBGP achieved a routing convergence time of 0.0101 s compared with 0.1904 s for BGPsec, representing a 94.7% reduction in convergence delay. The protocol also reduced CPU utilization from 84.20% in BGPsec to 28.40%, corresponding to a 66.3% reduction in computational overhead. In addition, L-SBGP maintained equivalent routing scalability, routing correctness, memory utilization, and control-plane message overhead while achieving 100% suppression of simulated prefix hijacking attacks, comparable to BGPsec. The findings demonstrate that lightweight hash-based validation provides an effective alternative to computationally intensive cryptographic mechanisms for secure inter-domain routing. The study contributes a formally specified lightweight secure routing protocol and provides empirical evidence that routing security can be strengthened without significantly increasing computational requirements. The proposed L-SBGP offers a scalable, computationally efficient, and secure solution suitable for deployment within modern ISP environments and provides a foundation for future research on lightweight secure Internet routing.

## TABLE OF CONTENTS

**DECLARATION** ..... **ii**
**DEDICATION** ..... **iii**
**ACKNOWLEDGEMENT** ..... **iv**
**ABSTRACT** ..... **v**
**LIST OF TABLES** ..... **ix**
**LIST OF FIGURES** ..... **x**
**ACRONYMS AND ABBREVIATIONS** ..... **xi**
**CHAPTER ONE: INTRODUCTION** ..... **1**
1.1 Background of the Study ..... 1
1.2 Problem Statement ..... 2
1.3 Research Objectives ..... 3
1.3.1 General objective ..... 3
1.3.2 Specific objectives ..... 3
1.4 Research Questions ..... 3
1.5 Significance of the Study ..... 3
1.6 Scope of the study ..... 4
1.7 Limitations of the study ..... 5
1.8 Contributions of the Thesis ..... 5
1.8.1 Contributions to Theory ..... 5
1.8.2 Contributions to Practice ..... 6
1.9 Organization of the Thesis ..... 6
**CHAPTER TWO: LITERATURE REVIEW** ..... **8**
2.1 Introduction ..... 8
2.2 Overview of Internet Service Providers ..... 8
2.3 Parameters for Enhancing BGPSec ..... 9
2.4 Existing Gateway Protocols ..... 10
2.4.1 Border Gateway Protocol (BGP) ..... 11
2.4.2 Routing Information Protocol (RIP) ..... 12
2.4.3 BGP Secure Routing Extension (BGPsec) ..... 15
2.4.4 Pretty Good BGP (pgBGP) ..... 28
2.4.5 Secure Origin BGP (BGP) ..... 29
2.4.6 GoBGP ..... 31
2.4.7 Machine Learning for Secure Routing ..... 33

2.4.8 Machine Learning for Secure Routing....37
2.4.9 Software Defined Networking (SDN) and Secure BGP....42
2.5 Parameters for reducing complexity overhead in routing protocols in an ISP.48
2.5.1 Convergence Time....48
2.5.2 CPU Utilization....48
2.5.3 Protocol Overhead....48
2.5.4 Memory Utilization....49
2.5.5 Scalability....49
2.5.6 Security Effectiveness....49
2.6 Existing Simulation Tools....49
2.6.1. NS-3 (Network Simulator 3)....50
2.6.2 OMNeT++....51
2.6.3 C-BGP....51
2.6.4 BGPsim....52
2.7 Performance Metrics....55
2.7.1 Packet delivery ratio (PDR)....55
2.7.2 Routing Convergence Time....56
2.7.3 Throughput....56
2.7.4 CPU Utilization....57
2.8 Conceptual Framework....57
2.8.1 Theoretical Foundation of the Conceptual Framework....57
2.8.2 Explanation of the Conceptual Framework....60
2.9 Summary....61
**CHAPTER THREE: METHODOLOGY....63**
3.1 Introduction....63
3.2 Research Design....63
3.3 Research Process....65
3.4 Research Method....66
3.5 Simulation Environment and Architecture....70
3.6 Simulation Topology and Population....71
3.7 Data Collection....71
3.8 Data Analysis....72
3.9 Ethical Issues....73
3.10 Summary....74
**CHAPTER FOUR: RESULTS AND DISCUSSION....75**

4.1 Introduction ..... 75
4.2 Parameters Identified from the Systematic Literature Review ..... 75
4.2.1 Inclusion Criteria ..... 76
4.2.2 Exclusion Criteria ..... 77
4.2.3 Data Extraction and Synthesis ..... 77
4.3 Expert Validation Results of the Identified Parameters ..... 78
4.4 Designing and Development of a Lightweight Secure Border Routing Protocol ..... 83
4.4.1 Design of Lightweight Secure Border Gateway Routing Protocol ..... 87
4.4.2 Development of a lightweight secure border gateway routing protocol ..... 90
4.5 Simulation Results ..... 98
4.5.1 Initial Simulation Parameters ..... 98
4.5.2 Performance Metrics ..... 98
4.6 Results ..... 99
4.6.1 Quantitative Results ..... 100
4.6.2 Convergence Time Analysis ..... 102
4.6.3 Control-Plane Overhead ..... 104
4.6.4 CPU Utilization ..... 104
4.6.5 Memory Usage ..... 106
4.6.6 Routing Table Consistency ..... 106
4.6.7 Security Performance (Hijack Suppression) ..... 106
4.7 Discussion ..... 107
4.8 Summary ..... 110
**CHAPTER FIVE: CONCLUSION, RECOMMENDATIONS AND FUTURE WORK ..... 112**
5.1 Conclusion ..... 112
5.2 Recommendations ..... 114
5.2.1 Recommendations for Practitioners ..... 114
5.2.2 Recommendations for Standards Bodies and Policy Makers ..... 114
5.3 Future Research ..... 115
5.3.1 Short-Term Priorities (0–6 Months) ..... 115
5.3.2 Medium-Term Priorities (6–12 Months) ..... 115
5.3.3 Long-Term Priorities (1–2 Years) ..... 115
**REFERENCES ..... 116**
**APPENDICES ..... 124**

## LIST OF TABLES

Table 2.1: Comparison Table: BGP Variants ..... 18
Table 2.2 Comparison of Simulation Tools ..... 54
Table 3.1 Objective Table ..... 68

## LIST OF FIGURES

Figure 2.1: Border Gateway Protocol ..... 11
Figure 2.2: Route Information Protocol ..... 15
Figure 2.3: BGP Secure Routing Extension ..... 17
Figure 2. 4: Secure Origin BGP ..... 31
Figure 2. 5: GoBGP ..... 33
Figure 2.6 : Conceptual Framework ..... 61
Figure 3.1: Research Process ..... 66
Figure 4.1: Flow chart for selecting the articles ..... 78
Figure 4.2: Parameter ranked by Experts on importance for each, according to expert opinion ..... 82
Figure 4.3: A diagram showing the elements of the control plane, the update classification module, and the validation process ..... 85
Figure 4.4: L-SBGP Routing Update Validation Process. A diagram of the routing update processing flow from reception, through validation, to update the routing table ..... 86
Figure 4.5: shows how L-SBGP Routing Process Validation Flows in a chart to explain the algorithm ..... 88
Figure 4.6 : L-SBGP Routing Process Validation Flowchart ..... 89
Figure 4.7: Convergence Time Bar Graph ..... 104
Figure 4.8: CPU Utilization Bar Graph ..... 106
Figure 4.9: Hijack Suppression Graph ..... 107

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **AS**: | Autonomous System |
| **BGP**: | Border Gateway Protocol |
| **BPS**: | Board of Postgraduate Studies |
| **C-BGP**: | Border Gateway Protocol Simulator |
| **L-SBGP**: | Lightweight Secure Border Gateway Protocol |
| **ISPs**: | Internet Service Providers |
| **NACOSTI**: | National Council of Science and Technology |
| **pgBGP**: | Pretty Good BGP |
| **RPKI**: | Resource Public Key Infrastructure |
| **soBGP**: | Secure Origin Border Gateway Protocol |

# CHAPTER ONE
# INTRODUCTION

## 1.1 Background of the Study

Modern communication, commerce, and information exchange are based on the Internet, and the Border Gateway Protocol (BGP) is the fundamental mechanism for inter-domain routing among autonomous systems. Although it plays an essential role, BGP is under pressure due to rapid growth in network traffic and the number of Internet Service Providers (ISPs), which puts additional strain on its effectiveness and operational capacity [1].

With the expansion of routing tables and the increasing complexity of network dynamics, BGP has been constrained by performance, leading to slower convergence, higher latency, and greater processing overhead. Their nature is enhanced by the protocol's reliance on policy-based decision-making and frequent route updates, which make it more difficult to select a path and scale to large networks [2].

Current optimization methods, including route aggregation, policy refinements, and secure extensions such as BGPsec, aim to enhance performance and security. Nonetheless, these remedies usually entail high computational overhead, configuration, and operational inefficiencies, which limit their use in ISP settings [3]. Furthermore, more sophisticated approaches like distributed routing models and algorithmic optimizations might offer some apparent benefits, but require greater amounts of resources (and/or architectural complexity) [4][5].

To address these limitations, this paper suggest a new protocol called Lightweight Secure Border Gateway Protocol (LSBGP) which is intended to address those limitations in the context of ISP networks. LSBGP focuses on using minimal routing mechanism, minimal overhead and modular design in order to achieve the dynamic scalability of the mechanism. The protocol is enhanced by applying the effective use of cryptographic techniques, but does not compromise the performance of the solution [6].

Finally, LSBGP should be a more well-balanced protocol that will enhance the performance of routing and lower the utilization of resources and will also not be impractical or unscalable, as the traditional BGP implementation is [7].

### 1.2 Problem Statement

The backbone of inter-domain routing is Border Gateway Protocol (BGP), which allows Autonomous Systems (ASs) to share reachability information. Nonetheless, its architecture poses major problems for Internet Service Providers (ISPs). The protocol provides no intrinsic security measure and is not easy to operate, causing routing management problems. However, within ISPs, there are often inefficiencies in the network switching from static to dynamic, which can result in instability and scalability problems [8][9].

Existing BGP enhancements address these problems, but have their own drawbacks. In particular, there is a lack of a good security/ease of use compromise in the BGP. This allows ISPs to be left to rely on solutions that improve security at the cost of performance, or on solutions that are efficient but less secure.

BGPsec was created to augment BGP security by cryptographically validating route announcements. Nevertheless, research has revealed that BGPsec incurs processing overhead due to per-hop cryptographic validation and multiple digital signatures. This leads to increased computational requirements, latency, and bandwidth usage, particularly in large or high-traffic networks [10][11][12].

Moreover, BGPsec leads to slower convergence and more difficult policy management in Autonomous Systems with diverse needs. It is expensive to implement, requires significant expertise and resources, and is neither scalable nor adoptable. As a result, the lack of a solution that provides strong security with low complexity makes a lightweight, scalable, secure routing solution evident [13][14][15].

## 1.3 Research Objectives

### 1.3.1 General objective

The general objective of this research is to develop a Lightweight Secure Border Gateway routing protocol to reduce complexity overheads for Internet service providers.

### 1.3.2 Specific objectives

i. To analyze parameters that reduce complexity overheads in routing protocols in Internet service providers.
ii. To design a lightweight, secure border gateway protocol for Internet service providers
iii. To validate a lightweight, secure border gateway routing protocol.

## 1.4 Research Questions

i. How can complexity in routing protocols be minimized to improve efficiency in Internet service providers' networks?
ii. How can a lightweight, secure border gateway protocol be designed to address the challenge of complexity, for instance, routing convergence time and protocol overhead?
iii. How do we validate the proposed protocol?

## 1.5 Significance of the Study

This study examines the complexity and computational cost of implementing BGPsec, particularly for Internet Service Providers (ISPs). It suggests designing a lightweight, secure Border Gateway Protocol (L-SBGP) to enhance routing performance and scalability, as well as routing security and resource consumption (memory and processing time).

The research will benefit ISPs because they will get a realistic and implementable security system which is more efficient and less complex to operate. This makes implementation easier and more straightforward for network engineers, while also reducing the number of configuration mistakes and the resulting instability in routing. In addition, this study will help cybersecurity experts find a balance between security and performance when it comes to inter-domain routing.

It's an important step in filling the knowledge gap between high security and lightweight deployment models. It provides the basis for future studies of optimal secure routing systems. The results may also benefit the policy makers and regulatory authorities by providing evidence-based guidance to create policies and standards for internet security that can be achieved and realistically implemented. The purpose of this study is to come up with a more solid, efficient and widely accepted routing paradigm that will make the internet infrastructure more stable and resilient worldwide and promote a secure routing practice in general.

### 1.6 Scope of the study

The purpose of this research was to create a lightweight and secure, secure BGP with minimal overhead of complexity related and not losing important security attributes. Designing a simple, performance, and scalable protocol with minimum computational cost (memory and processor time) was emphasized. The study was specifically focused on inter-domain routing security in the Internet Service Provider (ISP) environment, with a focus on lightweight mechanisms to enhance routing efficiency and robustness against malicious routing attacks, such as prefix hijacking.

The study involved protocol design, algorithm development, flowchart modeling, implementation and performance evaluation of the algorithms by simulations. To explain the operational structure, route validation, filtering, and routing decision processes of the proposed Lightweight Secure Border Gateway Protocol (L-SBGP), a lightweight route validation algorithm and a routing process flowchart were developed. These metrics were identified as the most significant since they have the greatest impact on protocol efficiency and deployment in a large-scale network environment, including routing convergence time, protocol overhead, CPU utilization, memory usage, packet delivery ratio, and security effectiveness.

The protocol was simulated and tested using python-based models in google colab and network simulation techniques similar to the one used in ns-3 environments. The study also compared the performance of L-SBGP with respect to the conventional BGP and BGPsec under different routing scenarios, network topologies and malicious routing conditions to see if the proposed protocol can achieve a balance between security, scalability and reduced complexity.

The study was not conducted for real-world deployment of the ISPs, performance benchmarking of the hardware, or direct integration with the existing infrastructure of the ISPs. Moreover, this study did not take into account the economic, policy, and regulatory factors of protocol adoption. The results of the study can only be interpreted in the light of these limitations.

## 1.7 Limitations of the study

The results of the study are subject to the following limitations: Routing environment of Internet Service Providers (ISPs) is complex and dynamic. Firstly, the proposed protocol was not implemented in a real-life ISP deployment, it was only tested in a simulated scenario. Although simulation offers an experimental environment, it is not a true representation of the operational requirements of real traffic, administration and real time network interaction.

Secondly, the number of performance and security cases examined was rather limited. Some important parameters such as routing convergence time, protocol overhead, and CPU utilization were measured, but much less testing was performed in terms of attack scenarios (such as coordinated large-scale route hijacking, APTs). This limits the number of times the protocol can be thoroughly tested in various and changing threat and conditions.

Thirdly, the simulation environment did not consider the detailed hardware limitations. The router processing and the memory architecture and vendor-specific options were not explicitly modeled. Thus, the performance may not reflect the protocol's performance in a typical real ISP network with a variety of hardware.

Also, BGPsec and Border Gateway Protocol (BGP) were used as benchmark. The full deployment aspects and key management, interoperability, incremental adoption, etc., were not fully tested in the simulated environment. The protocol has several limitations indicating the need for testing and validation in real-life environments, including more varied test environments.

## 1.8 Contributions of the Thesis

### 1.8.1 Contributions to Theory

The study has made the following contributions to theory;

i. The study identified key parameters that reduced complexity overheads in routing protocols in Internet service providers.

ii. The study developed a Lightweight Secure Border Gateway Protocol (LSBGP) optimized for simplicity, performance, and security, tailored to the needs of ISPs.

### 1.8.2 Contributions to Practice

The study has made the following contribution to practice:

i. The study validated the LSBGP through simulation experiments, comparing its efficiency with traditional BGP and BGPsec.

## 1.9 Organization of the Thesis

There are five chapters in this thesis, which are organized in the following order:

Chapter 1, "Introduction," describes the background of the study, the problem statement, the research objectives and questions, the study's significance, the scope, its limitations, and the contributions made by the thesis.

Chapter 2, "Literature Review," emphasizes available studies on Border Gateway Protocol (BGP) security and lightweight routing solutions for Internet Service Providers (ISPs). This review summarizes state-of-the-art secure BGP variants, including cryptographic, trust-based, anomaly-detection, and hybrid designs and methods, along with the techniques used in their design and implementation. It also discusses performance and security evaluation metrics for assessing the routing protocol's efficiency and scalability, including convergence time, CPU utilization, protocol overhead, and security effectiveness.

Chapter 3, "Methodology," outlines a detailed research methodology followed to achieve the objectives of this study. This chapter covers the research design, research process, data acquisition, ethical considerations, and experimental materials.

Chapter 4, "Results and Discussion**,"** describes the results of this study and their implications in the discussion section.

Chapter 5, “Conclusion, Recommendations, and Future Works**,”** presents the study's conclusions, recommendations, and proposed future work, followed by references and appendices.

# CHAPTER TWO
# LITERATURE REVIEW

## 2.1 Introduction

BGP plays a crucial role in Internet routing, as it helps data packets traverse the many Autonomous Systems (ASs). However, BGP lacks intrinsic protection mechanisms, and because of its significance, it attracts significant attention from malicious actors, as illustrated by the following example of route hijacking. In this chapter, the reader compares various elements and approaches to enhance BGP security. It also examines today's gateway protocols, emphasizing their strengths and weaknesses in terms of security. In addition, this chapter revisits the prospects of using simulation to design a better BGP and evaluates its capacity to resist security threats and enhance the Internet's architecture.

## 2.2 Overview of Internet Service Providers

Internet Service Providers (ISPs) play a key role in enabling communication across the globe through their provision of Internet access to individuals, businesses and organisations. They maintain and operate the network of networks that brings end users to the vastness of the Internet, which includes millions of devices and networks. ISPs are available at many different scales, ranging from local providers that provide internet connectivity to small businesses to the large ISP providers which provide high speed and reliable internet connectivity to customers across the globe. The ISPs manage their networks, such as forwarding the packets between various Autonomous Systems (AS) on the Internet. They communicate with one another via a routing protocol called Border Gateway Protocol (BGP) to exchange routing information and help direct data across the Internet in an efficient way. However, with increased traffic, the complexity of BGP, its Scalability and security are increasingly becoming challenges to ISPs [16].

One of the biggest issues for an ISP is getting data delivered quickly, efficiently and securely. The current BGP is currently not scalable enough or dynamic enough to deal with large scale and dynamic traffic flows. Such restrictions are often obstacles to convergence, security threats, and expensive to compute, particularly as the Internet expands and traffic rises. In response to these challenges, ISPs seek new solutions that will make BGP more complex - and yet more efficient and secure. These can be

mitigated by using lightweight secure Border Gateway Protocol (LBGPSec), which reduces the memory and CPU load used to keep current state information about the network and also gives high levels of security when propagating routing information. Optimizing the protocol for performance and Scalability can provide ISPs with a range of benefits, including efficient data transmission, quicker network convergence, and improved network security, which are crucial for meeting the demands of contemporary internet infrastructure [17].

### 2.3 Parameters for Enhancing BGPSec

The design of the routing protocol should consider several parameters to enhance routing performance of the Internet Service Providers (ISPs). The following parameters affect the efficiency, responsiveness and effectiveness of the proposed routing protocol in this article, Lightweight Secure Border Gateway Protocol (LBGPSec). A key parameter is the packet delivery ratio (PDR) which represents the ratio of packets delivered successfully in a network. The higher the PDR the more reliable the routing protocol, as data will not be held in any unnecessary queue or lost. The key is to route the paths optimally and minimise packet loss to ensure steady and reliable Internet connection to the users [18].

Another important consideration is routing convergence time, which is the time it takes a network to converge to a stable routing state after a topology change; typically, the topology change is a link failure or the network is updated. High availability and minimized interruptions in data flow are important because of the rapid convergence times. Thus, a reduced convergence time can help enhance network performance, especially in dynamic and high traffic environments where network changes are required rapidly. Other parameters directly affect routing performance are protocol overhead – amount of additional information that needs to be transmitted to manage and maintain the routing protocol. This enables exchange of routing information and network topology. It is crucial to keep the load in the network resources such as bandwidth and processing power to an absolute minimum, to keep overhead of protocols to an absolute minimum. This overhead can be reduced with the lightweight protocol implementation, which can enhance processing speed and minimize the load on the network especially in highly loaded networks or during high network traffic [19].

Another important factor of network performance is the CPU utilization need of a routing protocol. This is due to a resource intensive protocol that can slow down routers particularly if there is high traffic volume or frequent updates. Under load conditions, routers remain responsive and scalable with a Lightweight Protocol that requires a lower CPU load. In a similar fashion, memory usage is a concern; the memory of the router is limited and is used for storing routing tables, updates and other information. A light-weight routing protocol helps the routers to scale with an increasing number of internet traffic without running out of memory because the protocol does not require much memory to operate [20].

Another important factor is security, and security efficiency can be measured as the degree to which a protocol can achieve high security levels with low computational costs. With efficient cryptographic methods, robust protection can be achieved with minimal performance penalties from attacks like route hijacking and man-in-the-middle. For widespread adoption of such a protocol in different ISPs, it should be lightweight, secure and not be consuming much resources. Finally, Scalability is a basic parameter for any routing protocol which gives an idea about its capacity to process the growing internet traffic and the growth of the number of network nodes [21]. A scalable protocol can grow with network growth and keep the network efficient and performance efficient regardless of the number of routing entries and users. Lightweight protocol leverages Scalability to maintain the pace of the ever-changing internet.

The proposed LBGPSec protocol tries to improve the routing performance of ISPs by optimizing the following parameters: packet delivery ratio, routing convergence time, protocol overhead, CPU utilization, memory usage, security efficiency and scalability. This minimizes complexity, overhead and keeps networks fast, secure and scalable for future growth.

### 2.4 Existing Gateway Protocols

This section examines six existing protocols that ISPs can use to control route hijacking, highlighting their advantages and disadvantages.

### 2.4.1 Border Gateway Protocol (BGP)

BGP remains the kingpin of inter-domain routing or inter-AS routing on the Internet, where it is responsible for the distribution of routing information and the availability and accessibility of networks worldwidewide [22]. However, BGP has its shortcomings, most of which are on the security front, where the protocol is open to various vulnerabilities, including route hijacking. In this section, a critique of BGP is presented, highlighting its pros and cons and identifying a research gap in today's literature to strengthen security. Figure 2.1 shows how BGP processes routing updates, filters routes, maintains tables, and selects best paths across autonomous systems.

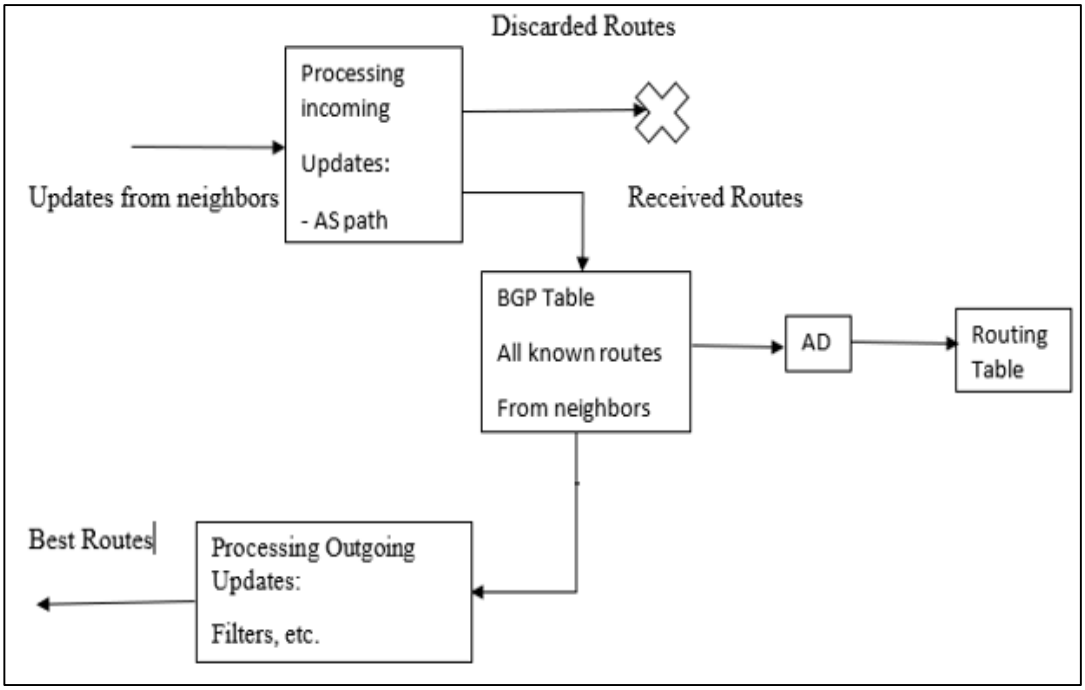



**Figure 2.1: Border Gateway Protocol**

BGP is known to scale very well for similar reasons. Namely, it is an Internet protocol that can process thousands of prefixes and support many peers. This is one of BGP's strongest features, as it enables it to evolve to meet the continually increasing demands of internet traffic worldwide. There are many others, including the policy-based routing capability, which enables a network administrator to apply routing policies based on attributes such as AS path, next hop, and community attributes. This feature allows BGP to make precise decisions on routing and thus adapt well to various

networks and businesses [23]. Furthermore, BGP's path vector mechanism provides AS path information for each network destination, helping protect against routing loops and providing more stable networks. In addition, BGP configuration is flexible, allowing it to establish one or more peering sessions with one or more ASes and to apply several routing policies and business models.

Thus, BGP has disadvantages, and these issues are critical for security on the World Wide Web. In the case of BGP, one of the major challenges, which is the security aspect, cannot go unnoticed. BGP cannot enforce security and is vulnerable to threats like route hijacking, prefix hijacking, and AS path manipulation. All the above vulnerabilities seriously threaten Internet routing security, as miscreants are well-organized in exploiting them to reroute web traffic, leading to data breaches, service disruptions, and other critical issues [24]. Another misfortune often attributed to BGP is that it is highly complex to configure. The naming is extremely flexible, and the BGP configuration process can be intricate. Many decisions and precautions must be taken in advance to ensure the BGP operating process is effective and protected. Because of the above-explained complexity, one could easily get it wrong, thus exposing the networks to security risks. Lastly, it is worth noting that BGP convergence time is comparatively slow. BGP convergence in large-scale networks can take time; thus, routing instability persists for some time, potentially leading to service disruption [25].

Concisely, like any other system, BGP has its strengths and weaknesses: scalability and policy-based routing, path-vector mechanisms, and flexibility are its great strengths, while its shortcomings include security threats, configuration complexity, and slow convergence time. The literature indicates that insufficient attention is given to these security issues. Therefore, improving the protocols complicates the risks already inherent in the BGP [26].

### 2.4.2 Routing Information Protocol (RIP)

RIP is one of the oldest distance-vector routing protocols used to construct complex routing information systems within small, simple networks to build device interconnectivity. While many people know RIP as a simple routing protocol that is relatively easy to implement, it has some shortcomings related to scalability and efficiency in large networks. In this section, an argument is made about RIP to show

that it is effective or deficient in certain ways and to reveal the function of RIP for which such a gap in its functionality can best be described, as needed by further research. Under Routing Updates, RIP works as follows: it sends the entire routing table to all neighboring routers each time, and it uses a metric, the hop count, to define the shortest path to a destination. The maximum number of hops is 15, which eliminates the issue of forming an infinite loop, but the protocol is not very effective for large networks. At the same time, these simple periodic updates result in significant bandwidth utilization and slow convergence during network changes, which are major disadvantages [26].

One of the main advantages of RIP organization is its simplicity. It is very easy to set up and compatible with most routing hardware and software, and is best suited to adding to small networks, or to environments that require little complexity in routing. The simplicity of the distance-vector mechanism is one of the important merits of the protocol. It is very easy to follow including for troubleshooting and debugging for network administrators having little or no experience.

RIP also incorporates some built-in facilities for stability in routing operation such as maximum hop count and split horizon. These mechanisms make sure that RIP can work well for small non-changing networks. Unfortunately, RIP, as a routing protocol has a few big problems that make it undesirable in today's network environment. It has the major drawback of not being scale efficient, first of all. A hop count of 15 means that RIP is not really viable for large geographically distributed networks or networks with numerous routers. Further, the core of RIP is that it must be updated periodically, which wastes bandwidth during updates and, not to mention, takes some time for changes to spread across the network [26]. This slow convergence means that routing loops or routing information may be temporarily outdated during topological changes, affecting services.

The third issue that affects RIP is security. This is because the protocol does not provide provisions for authenticating the sources of routing updates. This makes RIP networks prone to malicious attacks, including route poisoning, whereby unauthorized updates Flood routers and endanger network stability.

The core architecture of RIP is perfectly aligned with the requirements of the networking system at a different time, which did not consider scaling and efficiency as significant goals. However, features designed to prevent loops offer simple stability, while the protocol's poor security and slow gain rate become problematic in dynamic or aggressive environments. Further investigation could focus on addressing the limitations of the RIP by integrating new trends, such as authentication techniques and optimal upgrade procedures. Even if the networks are mostly running Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP), there remains a need to keep small peripheral systems with limited processing power or running rather primitive routing algorithms alive as a possible solution; in such cases, some minor optimizations in the protocol can go a long way in extending its usefulness. Hence I am summarising the RIP protocol, focussing on its merits: complexity and implementability. If these loopholes can be overcome, its application can be brought back to the area where other routing protocols are desirable due to their simplicity and lightness. The figure 2.2 depicts the flow of route validation and update decisions using RIP, emphasizing rejection logging and route acceptance processes.

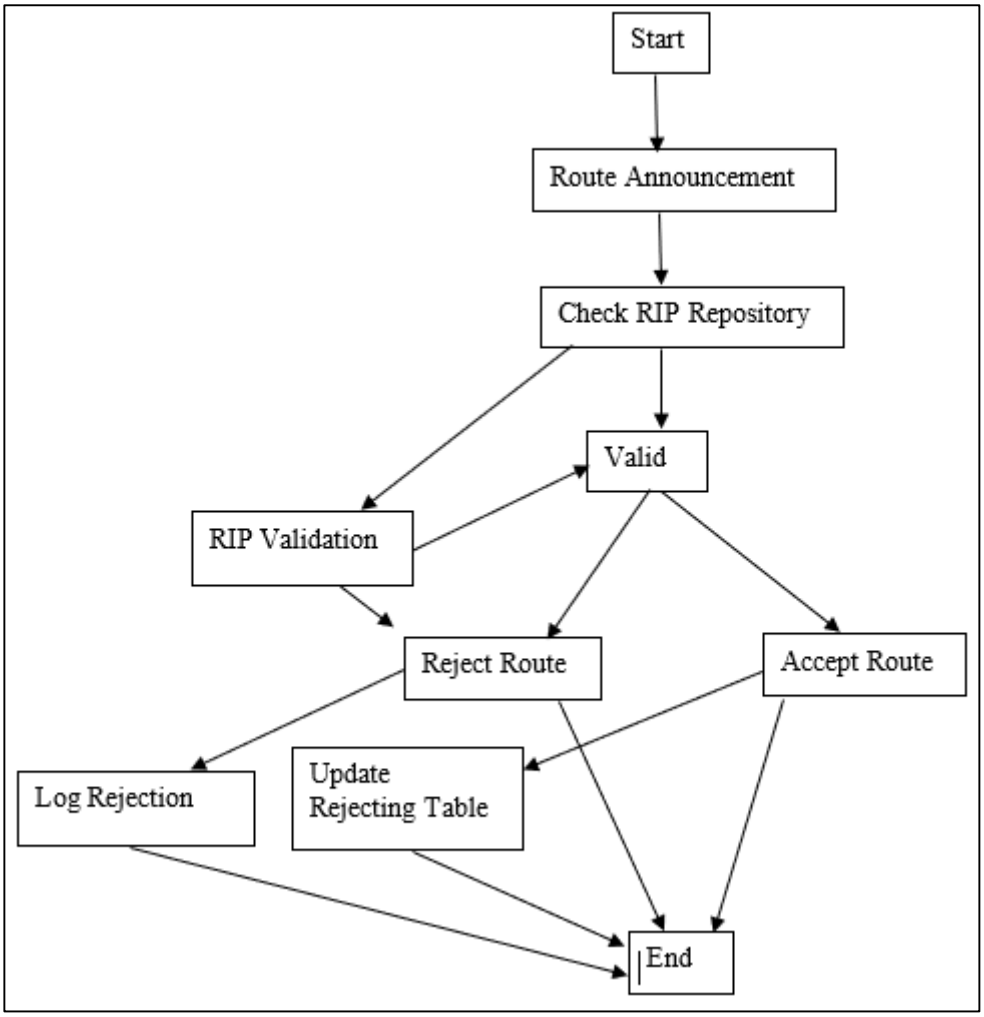



**Figure 2.2: Route Information Protocol**

### 2.4.3 BGP Secure Routing Extension (BGPsec)

BGPsec is an extension of the conventional BGP, which includes substantial enhancements that focus mainly on resolving the root of the security issues that characterize BGP. With the help of additional security points, BGPsec wants to check routing announcements, improving Internet routing security in general [30]. But there are minor or major issues with using BGPsec, depending on the situation.

An important examination of BGPsec shows that there are many advantages and some disadvantages. BGPsec is one of the main benefits in providing end-to-end path validation. More specifically, BGPsec can help guarantee the presence of only authorized advertising entities along the advertising path (the AS which has signed the advertising update), and the absence of any alterations of the advertising chain along the advertising path (the update chain update). This validation process greatly

improves the authenticity of routing information, enabling network operators to have confidence in the routes they receive. Additionally, BGPsec addresses two of the most pressing security challenges in traditional BGP: route leaks and hijacks. BGPsec addresses some security threats found in BGP, such as route leaks, where the routing information is distributed to parties that are not supposed to receive it, and route hijacks, where unauthorized parties or malicious ASes announce wrong routes [31]. This leads BGPsec to limit the risks posed by such attacks to cases in which only an authorized party can propagate routing information.

However, BGPsec has its disadvantages. The drawback is that significant changes must be made to BGP routers. BGPsec requires firmware and router software modifications, which add additional pressure on network operators. Such a change may result in a reliance on certain conditions that must be tested and proven. Another disadvantage of using BGPsec is the computational complexity of the cryptographic operations it performs [32]. The security attributes of BGPsec consist of digitally signed and encrypted routing information, which may create a significant workload for the computation of centralized BGP routers. This extra overhead can be a significant issue for large networks that are constantly changing routing configurations, which can impact their effectiveness and lead to slower response times.

To summarise, BGPsec has great potential to increase the security of the routing process and to defend against route leaks and route hijacks, but it has also many challenges. Network operators will have to be very careful about the need for broad roll-out of infrastructure, as well as the high compute requirements. Knowing these pros and cons are vital for effective decision making in implementing BGPsec security measures in the ISP networks. Figure 2.3 BGP Secure Routing Extension Reference Implementation and Test Tools for Emerging BGP Security Standards.

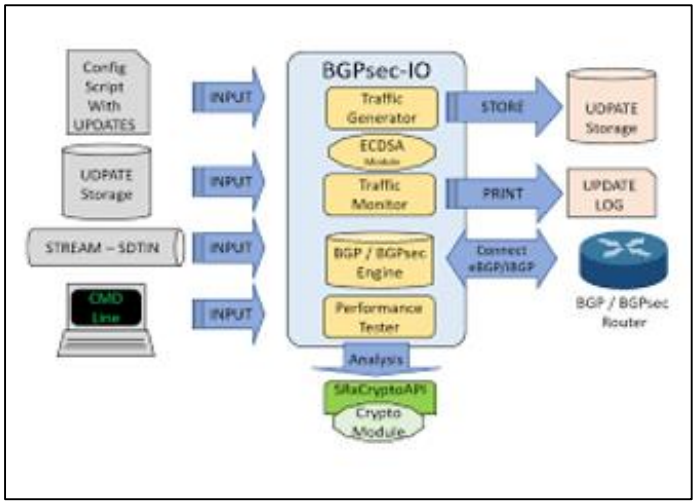



**Figure 2.3: BGP Secure Routing Extension [34]**

Variants of BGPsec: The current versions of BGPsec try to enhance the underlying protocol to address some particular concerns regarding security, efficiency, or other ways of better operation management. BGPsec: BGPsec is a basic version that concentrates on cryptographically signing BGP routing updates and maintaining AS path integrity and authorization.

BGPsec with RPKI (Resource Public Key Infrastructure): This variant combines RPKI, a public-key infrastructure to validate BGP updates. RPKI allows route announcements to be signed and validated in a centralized trust system for IP address prefixes. BGPsec + BGP Monitoring: This combination of BGPsec and real-time monitoring systems allows for faster detection of malicious activity such as route hijacks and leaks. It is the deployment of monitoring systems in addition to BGPsec that will be observing and responding to abnormal routing behavior.

BGPsec with Adaptive Path Selection: This version is an extension of BGPsec that introduces adaptive mechanisms to choose the most secure and efficient routing path available depending on the available cryptographic verification as well as the network topology. The differences between the BGPsec variants are summarized in the table below: Points out the trade-offs between security levels, efficiency and scalability between implementations. Table 2.1 below compares BGPsec variants.

**Table 2.1: Comparison Table: BGP Variants**

| Routing Technology | Primary Security Mechanism | Main Strengths | Major Limitations | Computational Complexity | Scalability | Deployment Complexity | Suitability for ISP Deployment | Research Gap |
|---|---|---|---|---|---|---|---|---|
| Conventional BGP | Trust-based route advertisement | Highly scalable, globally deployed, mature protocol, fast routing decisions, interoperable across vendors | No built-in authentication, vulnerable to prefix hijacking, route leaks, AS-path spoofing, and route manipulation | Low | Very High | Low | Excellent for routing but poor for security | Requires lightweight security without sacrificing performance |
| RPKI (Resource Public Key Infrastructure) | Cryptographic validation of Route Origin Authorization | Authenticates IP prefix ownership, prevents | Does not validate complete AS-path, partial global | Moderate | High | Moderate | Good for origin validation but insufficient against | Requires complementary mechanisms for |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | s (ROAs) | origin hijacking, relatively easy incremental deployment, standardized by IETF | adoption, centralized trust model, certificate management complexity | | | | sophisticated attacks | path validation and anomaly detection |
| BGPsec | Digital signatures for complete AS-path validation | Provides end-to-end path authentication, prevents AS-path manipulation, strengthens routing integrity | High cryptographic overhead, increased CPU usage, larger routing updates, slower convergence, expensive router upgrades | Very High | Moderate | Very High | Limited due to computational requirements | Requires lightweight path validation with lower processing overhead |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SoBGP | Distributed certificate repository and policy verification | Validates route origin and policy relationships, lower cryptographic cost than BGPsec, flexible trust establishment | Does not fully protect AS-path integrity, requires widespread deployment, policy synchronization complexity | Moderate | High | High | Moderate | Needs improved path validation and simplified deployment |
| pgBGP | Historical routing behaviour analysis | Detects routing anomalies using historical routing data, identifies route | Depends heavily on quality of historical data, high storage requirements, slower | Moderate to High | Moderate | Moderate | Useful for monitoring but not standalone protection | Requires adaptive real-time detection with lower storage overhead |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | instability and hijacking patterns | detection of new attack patterns | | | | | |
| GoBGP | Programmable BGP implementation supporting RPKI and BGPsec | API-driven automation, flexible routing policies, cloud-native architecture, easy integration with network orchestration | Requires programming expertise, API security concerns, limited operational deployment studies | Moderate | High | Moderate | Good for programmable ISP environments | Requires simplified automation with stronger security guarantees |
| Machine Learning-based Secure | AI-based anomaly detection | Detects unknown attacks, | Requires large training datasets, comput | High to Very High | Moderate | High | Limited by computational resour | Needs lightweight intelligent detecti |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Routing | using supervised and unsupervised learning | adaptive learning, predictive routing security, high detection accuracy, identifies complex routing anomalies | ationally intensive, difficult model explainability, vulnerable to adversarial attacks | | | | ces in many ISPs | on suitable for real-time routing |
| Blockchain-based Secure Routing | Distributed ledger and decentralized trust management | Immutable routing records, decentralized validation, improved transparency, | Consensus delays, storage overhead, scalability challenges, deployment comple | High | Moderate | Very High | Limited for large-scale real-time routing | Requires decentralized trust with significantly reduced latency and resourc |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | secure prefix ownership verification, smart contract automation | xity, synchronization costs | | | | | e consumption |
| SDN-based Secure BGP | Centralized controller with programmable routing policies | Global network visibility, centralized monitoring, automated policy enforcement, rapid attack mitigation, simplified management | Controller becomes single point of failure, scalability concerns, migration challenges, controller security risks | Moderate | High | High | Effective for managed ISP infrastructures | Requires distributed lightweight routing security without controller dependency |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Hybrid RPKI + BGPsec | Origin validation plus AS-path authentication | Provides comprehensive cryptographic security, stronger protection against routing attacks | Very high computational cost, difficult deployment, increased protocol overhead, slower routing convergence | Very High | Moderate | Very High | Limited to high-resource networks | Requires simplified integrated validation mechanisms |
| Hybrid AI + SDN | Intelligent centralized routing optimization | Adaptive routing decisions, predictive congestion management, automated anomal | High infrastructure cost, controller dependency, machine learning complexity, | Very High | High | Very High | Suitable mainly for large cloud providers | Requires cost-effective deployment for conventional ISP environments |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | y respon se, efficie nt traffic engine ering | specialized expertise required | | | | | |
| Hybrid Blockc hain + RPKI | Decent ralized certific ate manag ement | Improv ed trust manag ement, immut able ROA storage , elimin ates central ized certific ate depend ency | Blockc hain synchro nizatio n delays, storage growth, interop erabilit y challen ges | High | Mod erate | Very High | Emerg ing techno logy with limited deploy ment | Requir es lightwe ight decentr alized validati on archite cture |
| Propos ed L-SBGP | Lightw eight route validati on, adaptiv e path optimiz | Reduc ed compu tationa l overhe ad, faster | Require s broader real-world implem entatio n and | Low to Modera te | Very High | Low to Mode rate | Highly suitabl e for resour ce-constr ained and | Addres ses comput ational comple xity while maintai |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ation, simplified routing mechanisms | convergence, lower CPU utilization, improved scalability, efficient route validation, practical deployment in ISP environments | interoperability evaluation | | | | large-scale ISP deployment | ning effective routing security |

Critical Comparative Analysis Table 2.1 demonstrates that no existing secure inter-domain routing approach completely satisfies the competing requirements of strong security, low computational complexity, scalability, rapid convergence, and ease of deployment. Conventional BGP remains the most scalable and widely deployed protocol but provides almost no intrinsic security against modern routing attacks. RPKI significantly improves route origin validation; however, it cannot authenticate complete AS-path information, leaving the protocol vulnerable to sophisticated path manipulation attacks. BGPsec addresses this limitation through end-to-end cryptographic validation but introduces substantial computational overhead, increased

routing update sizes, higher CPU utilization, and slower routing convergence, limiting its adoption among many Internet Service Providers.

Similarly, SoBGP and pgBGP improve routing trust through policy verification and historical anomaly detection, respectively, but neither fully validates complete routing paths nor provides sufficiently lightweight operation for modern high-speed ISP environments. GoBGP introduces programmability and automation that improve operational flexibility; nevertheless, its dependence on software APIs and advanced programming expertise increases deployment complexity.

Recent approaches based on Machine Learning, Blockchain, and Software Defined Networking provide significant advances in intelligent anomaly detection, decentralized trust management, and centralized network control. However, these techniques introduce new challenges, including high computational requirements, controller dependency, consensus latency, extensive storage demands, large training datasets, and increased operational complexity. Consequently, their widespread deployment remains constrained, particularly in resource-limited ISP environments.

The comparison further reveals that hybrid solutions combining RPKI, BGPsec, Machine Learning, Blockchain, and SDN generally achieve stronger security than individual approaches but simultaneously increase implementation complexity, processing overhead, infrastructure costs, and deployment difficulty. These trade-offs indicate that current secure routing mechanisms continue to struggle to balance security effectiveness with operational efficiency.

The proposed Lightweight Secure Border Gateway Protocol (L-SBGP) addresses this identified research gap by integrating lightweight route validation, adaptive path optimization, and simplified routing mechanisms that reduce CPU utilization, memory consumption, protocol overhead, and routing convergence time while maintaining effective protection against route hijacking and malicious route propagation. Unlike many existing approaches, L-SBGP prioritizes practical deployment within large-scale Internet Service Provider environments by achieving an effective balance between security, scalability, computational efficiency, and operational simplicity. This positions L-SBGP as a practical next-generation secure inter-domain routing protocol capable of addressing the limitations identified in existing literature.

### 2.4.4 Pretty Good BGP (pgBGP)

For the first time, an anomaly is detected via the use of previous routing information in PG-BGP, which is an enhancement of BGP. This proposal is focused on stabilizing changes to one of the most basic Internet technologies – BGP. In the critical review of pgBGP, I have highlighted the pros and cons of the path the researcher has taken, to enable them to think about how they can improve it [35].

The major advantage of pgBGP is that it maintains all routing information in its history, and can detect patterns and deviations from those which could be a source of security risks, such as route and prefix hijacking. Compared to the normal routing update, which is queried from the routing information base, pgBGP can spot other suspicious changes before they worsen. This capability is especially handy for ensuring the stability of the Internet's routing infrastructure, as it can detect routing instabilities. Moreover, with pgBGP continuously scanning routing updates, network security risks are better managed and addressed, making the network safer. However, there are some drawbacks to using pgBGP that cannot be overlooked. The information used in pgBGP's anomaly detection is highly susceptible to the accuracy and comprehensiveness of the data. While pgBGP operates on large datasets, the quality of the information in this database is critical to its ability to detect routing anomalies; if the historical data is absent, stale, or corrupted, pgBGP's efficiency can be greatly compromised [36]. It stresses the importance of historical data quality, which is often not achieved at high levels, underscoring the need to properly handle historical fuzzy data for decision-making. The last disadvantage of pgBGP is that it requires more storage and will consume more computational power than the problem's first proposition. According to the historical database, the protocol requires significant storage space to handle many routing records. This can lead to higher operational costs and, implicitly, require additional changes to the infrastructure, which could be difficult for some companies, especially when dealing with new infrastructure. The need for other resources may also create competition with other important functions within an organization that might be affected by the need for those resources.

In conclusion, while pgBGP introduces proposed BGP security extensions based on historical data, it raises the issues mentioned above that must be addressed. The effectiveness of this approach depends on the characteristics of historical data and the

organization's investments in storage and computational resources for implementation. These factors have established the need for additional research and development to enhance the efficiency of pgBGP and have illuminated gaps in the literature.

### 2.4.5 Secure Origin BGP (BGP)

SoBGP stands for Secure Origin BGP, a marked improvement over conventional BGP that addresses some of its major security risks. Hence, by authenticating the source of the route and the path, BGP helps improve the security and stability of the Internet routing system [37]. This approach chiefly addresses problems such as route hijacking, in which a malicious party aims to alter the routing data that defines the traffic path. However, as a concept, BGP is not without some issues.

From a technical perspective, one of the major benefits of SoBGP is that it can simultaneously guarantee the correctness of routes' origins and path identities. Thus, using cryptographic techniques and digital certificates, SoBGP validates BGP update sources and verifies path integrity. This eliminates the possibility of unauthorized entities flooding the network with incorrect routing information, thereby preventing route hijacking and allowing only correct routing information to circulate [38]. Therefore, with BGP, the routing framework is strengthened to resist attacks and, further, to mitigate recurrent configuration errors.

However, SoBGP is not devoid of several negative aspects. One of the main disadvantages is that it creates much overhead that requires significant changes to Core BGP. Network operators and organizations would require additional infrastructure and software, which could be tedious and expensive. However, for SoBGP to be a truly efficient tool, it should be implemented across the entire Internet. The above deployment condition is a major issue because the security gains of SoBGP are considerably difficult to achieve without an enormous number of network operators deploying [39]. Further, global network operators have varying levels of IT literacy, resource availability, and strategic vision in implementing such changes, which are further hampered by the global rise in Internet instability.

In conclusion, while SoBGP offers a robust solution for validating route origination and paths, thereby reducing the risks of route hijacking and misconfiguration, its effectiveness depends heavily on universal implementation. The significant

modifications required to the existing BGP infrastructure, along with the challenges of achieving widespread adoption, present substantial barriers to its success. This highlights a critical gap in the literature and the need for further research into more feasible, universally adaptable solutions to enhance BGP security. Figure 2.4 below, Secure Origin BGP, illustrates a route validation system that uses certificates and policy mechanisms to effectively prevent BGP route hijacking attacks.

**Flow Chart:**

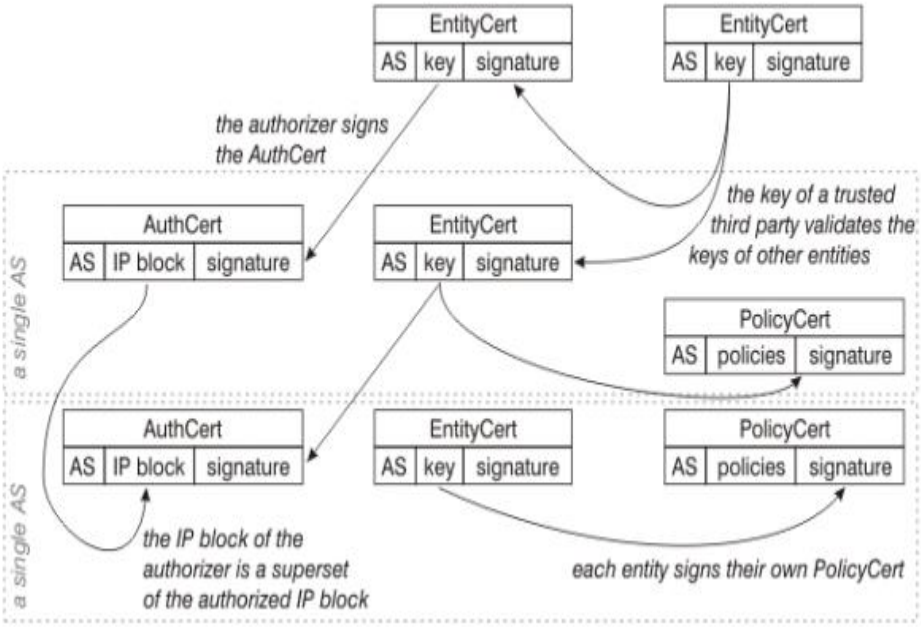



**Figure 2. 4: Secure Origin BGP [37]**

### 2.4.6 GoBGP

GoBGP is a state-of-the-art representation of the Border Gateway Protocol (BGP) that has drawn interest in the network security and routing domains. As a flexible and extensible BGP implementation, GoBGP offers advantages that help mitigate some of BGP's shortcomings and issues, especially in the security and protocol domains.

This proposal critiqued GoBGP with special emphasis on the key attributes that set GoBGP apart from other available BGP implementations. GoBGP differs from conventional BGP implementations in that the latter are commonly configured and controlled statically and often require external actions. It enables network operators to manage routing policies and their configurations via API interfaces, enabling better, quicker control of the network. This characteristic is particularly beneficial in situations where network topology frequently changes and routing policies must be modified rapidly. Nevertheless, there are some areas in the literature that the presented work aims to address by providing a systematic evaluation of GoBGP performance to eliminate risks such as route hijacking. However, GoBGP offers more features, including RPKI and BGPsec support, and there has been little real-world study of its

use in genuine ISP networks [40]. One of the critical areas where GoBGP performance in terms of the sheer coordination and management of a global-scale network about both its components and characteristics, and existing networks can be deemed incomparable is the need to assess its performance in terms of the increasing ubiquity of BGP in today's network environment, and how it can integrate with already-functional systems.

The features discussed above demonstrate that GoBGP offers several benefits. Due to its flexibility and extensibility, Reilly's model [41] is an effective tool for network operators who must respond to changes in network parameters. This ability integrates APIs to enable network automation and minimize human intervention, thereby enhancing network efficiency. Furthermore, since GoBGP also supports modern security extensions, it can significantly enhance the security of BGP routing, thereby strengthening the Internet routing system against threats, such as route hijacking [41].

There are however some drawbacks to GoBGP – it initiates and runs BGP processes but it does not kill them. One of the key issues is the difficulty in implementing and managing the technology. The flexibility and programmability of GoBGP is very attractive, but presents a lot of challenge to the user, as they have to understand both networking and programming. Moreover, with the growing reliance on APIs and automation, new security vulnerabilities may emerge if they are not properly managed. Another bad news is their dissemination which is crucial for the solution of the BGPs security problem. That is why GoBGP may include security features, but these features shall not result in added benefits and features without wide integration across various networks [42].

Thus, GoBGP includes valuable innovations in BGP implementation, namely in flexibility, extensibility, and security; however, it also has significant complexity issues and limited adoption. Furthering this line of research and deploying GoBGP in additional practical studies focused on real-world deployments will help close any remaining gaps in the literature regarding its effectiveness as a solution for securing BGP. Figure 2.5 below shows A Control Plane Evolving Software Networking as it propagated.

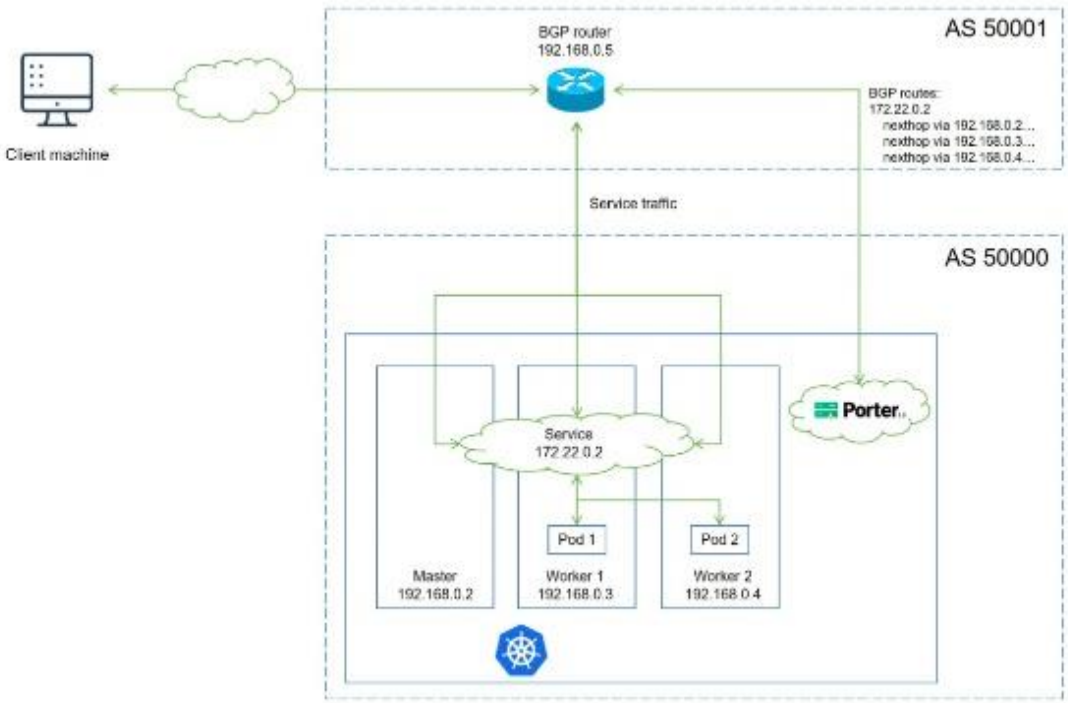



**Figure 2. 5: GoBGP [41]**

### 2.4.7 Machine Learning for Secure Routing

Machine Learning (ML) has emerged as one of the most promising approaches for improving the security and resilience of Border Gateway Protocol (BGP) routing. Unlike traditional security mechanisms such as BGPsec and Resource Public Key Infrastructure (RPKI), which rely primarily on cryptographic validation and certificate-based authentication, ML techniques analyze routing behavior to identify abnormal patterns that may indicate malicious activities. The rapid growth of Internet traffic, increasing routing complexity, and the sophistication of cyberattacks have encouraged researchers to explore intelligent learning algorithms capable of detecting routing anomalies automatically while reducing human intervention.

The primary objective of applying machine learning in secure routing is to improve the detection of attacks such as prefix hijacking, route leaks, path manipulation, and distributed denial-of-service (DDoS)-related routing anomalies. Machine learning algorithms continuously learn normal routing behavior from historical BGP update messages and routing tables. When deviations from the learned behavior occur, the

algorithms classify the routing events as either legitimate or suspicious, allowing network operators to respond before widespread disruption occurs.

One of the major advantages of machine learning is its capability to detect previously unknown attacks. Traditional rule-based routing security mechanisms depend on predefined signatures or policies, making them less effective against new attack strategies. In contrast, supervised learning algorithms such as Random Forests, Support Vector Machines (SVM), Decision Trees, and Artificial Neural Networks learn from labelled routing datasets and can accurately distinguish between normal and malicious routing announcements. Recent studies have reported detection accuracies exceeding 95% for prefix hijacking and route leak identification using ensemble learning techniques.

Unsupervised machine learning has also gained significant attention because routing datasets often contain limited labelled attack examples. Algorithms such as K-Means Clustering, Density-Based Spatial Clustering (DBSCAN), Principal Component Analysis (PCA), and Autoencoders identify abnormal routing behaviour without requiring labelled training data. These techniques group routing updates according to their statistical similarities and identify outliers that may represent malicious routing events. Such approaches are particularly useful in operational ISP environments where attack signatures continuously evolve.

Recent developments between 2024 and 2025 have introduced deep learning techniques into inter-domain routing security. Deep Neural Networks (DNNs), Long Short-Term Memory (LSTM) networks, and Graph Neural Networks (GNNs) have demonstrated remarkable performance in modelling the complex relationships among Autonomous Systems (ASs). Since BGP naturally forms a graph connecting thousands of interconnected Autonomous Systems, Graph Neural Networks are particularly suitable because they learn routing dependencies directly from network topology. Similarly, LSTM models capture temporal dependencies within BGP update streams, enabling early detection of abnormal routing behaviour before large-scale propagation occurs.

Reinforcement Learning (RL) has also emerged as an adaptive approach to secure routing. Instead of relying solely on historical observations, reinforcement learning

agents continuously interact with the routing environment and learn optimal routing decisions through reward mechanisms. When routing anomalies occur, the RL agent dynamically selects secure routing paths while minimizing network disruption. This adaptive capability makes reinforcement learning attractive for highly dynamic Internet environments where routing policies frequently change.

Machine learning also supports intelligent route validation by combining multiple routing features simultaneously. Rather than validating only the cryptographic authenticity of routing announcements, ML models analyze several routing characteristics, including AS-path length, update frequency, origin consistency, route propagation patterns, geographic distribution of prefixes, and historical routing behaviour. By integrating multiple routing attributes, ML systems achieve more comprehensive anomaly detection than conventional single-feature validation mechanisms.

Another important application is predictive routing security. Instead of detecting attacks after they occur, machine learning algorithms forecast future routing instabilities by analysing historical routing trends. Predictive models enable Internet Service Providers (ISPs) to identify potentially unstable routes before failures occur, allowing preventive actions such as rerouting traffic or temporarily filtering suspicious announcements. This proactive capability contributes to improved network availability and reduced service interruptions.

Despite these advantages, machine learning introduces several limitations that prevent its widespread deployment as a standalone secure routing solution. The first challenge is the requirement for large volumes of high-quality training data. Effective supervised learning depends on accurately labelled datasets containing both normal and malicious routing events. However, obtaining comprehensive BGP attack datasets remains difficult because many routing incidents are either undocumented or proprietary to network operators.

The computational complexity of machine learning models also presents significant deployment challenges. Deep learning architectures require substantial processing power, memory resources, and specialized hardware such as Graphics Processing Units (GPUs). Large Internet Service Providers may possess sufficient computational

resources, but smaller regional ISPs often cannot justify the additional infrastructure costs. Consequently, continuous real-time execution of complex machine learning models may introduce processing delays that negatively affect routing convergence.

Another limitation concerns model generalization. Machine learning models trained using routing data from one geographical region or ISP may perform poorly when deployed in different network environments. Internet routing policies vary considerably among Autonomous Systems, making it difficult to develop universally applicable models without frequent retraining and adaptation.

Interpretability is another challenge associated with advanced machine learning techniques. While traditional routing policies are relatively transparent and easy to audit, deep learning models often operate as "black boxes," making it difficult for network administrators to understand why a routing announcement has been classified as malicious. This lack of explainability reduces operator confidence and complicates operational troubleshooting.

Furthermore, machine learning systems themselves may become targets of adversarial attacks. Attackers can intentionally manipulate training datasets or generate adversarial routing updates designed to mislead classification models, thereby reducing detection accuracy. Such vulnerabilities necessitate additional mechanisms for securing the learning process itself.

Recent research has therefore proposed hybrid architectures that combine machine learning with traditional routing security mechanisms such as RPKI and BGPsec. In these architectures, cryptographic mechanisms verify route authenticity, while machine learning performs behavioural analysis to detect sophisticated attacks that bypass cryptographic validation. Hybrid solutions generally achieve higher security effectiveness than either approach individually, although they also increase implementation complexity and computational overhead.

The literature demonstrates that machine learning represents an important advancement in secure inter-domain routing because of its ability to detect complex routing anomalies, adapt to evolving threats, and support predictive network management. Nevertheless, the high computational requirements, dependence on

large training datasets, implementation complexity, and explainability challenges limit its practicality for lightweight deployment within many ISP environments. These observations reveal an important research gap regarding the development of routing security mechanisms that achieve high detection accuracy while maintaining low computational overhead.

The proposed Lightweight Secure Border Gateway Protocol (L-SBGP) addresses this gap by employing lightweight route validation mechanisms that reduce CPU utilization, memory consumption, protocol overhead, and convergence delays without requiring computationally intensive machine learning models. While machine learning provides valuable intelligent detection capabilities, the emphasis of L-SBGP is on achieving practical, scalable, and resource-efficient security suitable for deployment across heterogeneous ISP infrastructures. This balance between security effectiveness and computational efficiency distinguishes the proposed protocol from many recent AI-based routing security solutions.

### 2.4.8 Machine Learning for Secure Routing

Blockchain technology has recently emerged as a promising solution for enhancing the security, transparency, and trustworthiness of inter-domain routing. Traditional Border Gateway Protocol (BGP) was designed primarily to achieve scalability and efficient route exchange rather than security. Consequently, BGP remains vulnerable to several attacks, including prefix hijacking, route leaks, route forgery, and Autonomous System (AS) path manipulation. Conventional security mechanisms such as Resource Public Key Infrastructure (RPKI) and BGPsec have significantly improved route authentication; however, they rely on centralized trust models and computationally intensive cryptographic operations that increase processing overhead and complicate deployment. Blockchain technology offers an alternative decentralized trust framework that can strengthen routing security while eliminating dependence on a single trusted authority.

Blockchain is a distributed ledger technology that stores transactions across multiple participating nodes in a network. Each transaction is grouped into blocks that are cryptographically linked to previous blocks, creating an immutable chain of records. Once routing information has been verified and recorded within the blockchain, altering or deleting the information becomes computationally infeasible without

obtaining consensus from participating nodes. This immutability makes blockchain highly attractive for securing routing information because malicious entities cannot easily manipulate route advertisements or tamper with routing records after validation.

In secure inter-domain routing, blockchain can be used to maintain trusted records of IP prefix ownership, Autonomous System identities, routing policies, and route advertisements. Rather than relying exclusively on centralized certificate authorities, network operators collectively verify routing announcements through distributed consensus mechanisms. Before a BGP update is accepted, participating Autonomous Systems validate the legitimacy of the route advertisement by consulting the blockchain ledger. This decentralized validation significantly reduces opportunities for unauthorized route announcements and malicious route propagation.

One of the most important applications of blockchain in BGP security is prefix ownership verification. Internet routing attacks frequently occur when attackers falsely advertise IP address prefixes belonging to other organizations. Blockchain allows legitimate IP prefix ownership records to be permanently stored and distributed among participating Autonomous Systems. During route advertisement, routers compare announced prefixes against blockchain records before accepting routing updates. Unauthorized announcements that fail validation are automatically rejected, thereby reducing the risk of prefix hijacking.

Blockchain also enhances Autonomous System authentication. In conventional BGP, routers generally trust routing updates received from neighboring Autonomous Systems without independently verifying their legitimacy. This implicit trust model creates opportunities for attackers to impersonate legitimate Autonomous Systems or advertise fraudulent routing information. Blockchain introduces decentralized identity management by assigning cryptographically verifiable digital identities to participating Autonomous Systems. Each routing update is digitally signed and verified using blockchain-based identity records before being propagated throughout the Internet routing infrastructure.

Another significant contribution of blockchain is improved route integrity. Because every validated routing announcement is permanently recorded within the distributed ledger, network administrators can trace the complete history of routing changes

affecting a particular prefix or Autonomous System. This audit capability simplifies forensic investigations following routing incidents and enables operators to identify the origin of malicious routing announcements more efficiently. The transparency provided by blockchain also promotes greater accountability among participating network operators.

Recent research has explored the integration of blockchain with smart contracts to automate routing policy enforcement. Smart contracts are self-executing programs stored within the blockchain that automatically enforce predefined security rules whenever routing events occur. For example, a smart contract may automatically reject route advertisements originating from unauthorized Autonomous Systems, verify compliance with routing policies, or notify network administrators whenever abnormal routing behavior is detected. Automation reduces manual intervention while ensuring consistent application of security policies across distributed networks.

Between 2024 and 2025, blockchain research has increasingly focused on hybrid blockchain-RPKI architectures. Instead of replacing existing security infrastructures, blockchain complements RPKI by decentralizing certificate management while preserving cryptographic route validation. In these hybrid systems, blockchain maintains immutable records of Route Origin Authorizations (ROAs), enabling multiple network operators to independently verify routing information without relying entirely on centralized repositories. Such approaches improve trust, availability, and resilience against attacks targeting centralized certificate infrastructures.

Permissioned blockchain platforms have gained considerable attention for Internet Service Provider (ISP) environments. Unlike public blockchains, permissioned blockchains restrict participation to authorized organizations such as Internet registries, Internet Service Providers, and major Autonomous Systems. Because participating entities are known and authenticated, permissioned blockchains require less computational effort for consensus and provide faster transaction processing. These characteristics make permissioned blockchain architectures more suitable for operational routing infrastructures than fully public blockchain networks.

Several blockchain consensus algorithms have been investigated for secure routing applications. Traditional Proof of Work (PoW) offers strong security but introduces excessive computational costs, energy consumption, and transaction latency that make it unsuitable for real-time routing validation. Consequently, researchers have explored alternative consensus mechanisms such as Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). These consensus protocols significantly reduce validation delays while maintaining sufficient trust and consistency for routing environments.

Blockchain technology also improves resilience against route hijacking attacks by establishing distributed consensus before routing announcements are accepted. Since malicious attackers would need to compromise multiple independent blockchain participants simultaneously, unauthorized route advertisements become significantly more difficult to propagate throughout the Internet. This distributed trust model increases overall routing resilience while minimizing the possibility of single-point failures that characterize centralized security infrastructures.

Another emerging application is blockchain-assisted routing reputation systems. In these systems, Autonomous Systems accumulate reputation scores based on their historical routing behavior recorded within the blockchain ledger. Network operators can use these reputation values to assess the trustworthiness of neighboring Autonomous Systems before accepting routing updates. Autonomous Systems repeatedly involved in routing anomalies gradually receive lower trust scores, reducing their influence on future routing decisions. Such reputation-based mechanisms strengthen routing security through continuous behavioral assessment.

Despite these significant advantages, blockchain-based routing security introduces several implementation challenges. One major limitation is transaction latency. Before routing updates are accepted, blockchain consensus must be completed among participating nodes. Even relatively fast consensus mechanisms introduce additional processing delays that may increase BGP convergence time during periods of frequent routing updates. Since Internet routing requires rapid adaptation to topology changes, excessive validation delays may negatively affect overall network performance.

Scalability is another important concern. Global Internet routing generates millions of routing announcements and updates daily. Recording every routing event within a blockchain ledger can rapidly increase storage requirements and synchronization overhead among participating nodes. As blockchain size continues to grow, maintaining complete copies of the ledger may become increasingly resource-intensive, particularly for smaller Internet Service Providers with limited storage capacity.

Blockchain also increases computational and communication overhead. Participating routers or validation servers must execute cryptographic operations, consensus algorithms, digital signature verification, and ledger synchronization in addition to conventional routing functions. Although permissioned blockchain systems reduce computational complexity compared to public blockchains, additional processing overhead remains unavoidable and may impact router performance under heavy network loads.

Deployment complexity represents another significant barrier to adoption. Effective blockchain-based routing security requires cooperation among numerous Autonomous Systems, Internet registries, Internet Service Providers, and equipment vendors. Achieving universal participation across the global Internet remains extremely challenging due to differences in infrastructure, operational policies, financial resources, and regulatory environments. Partial deployment limits the overall effectiveness of blockchain because malicious routing announcements originating from non-participating networks may still affect Internet stability.

Interoperability with existing routing infrastructure also presents practical challenges. Blockchain solutions must integrate seamlessly with conventional BGP implementations, RPKI repositories, routing registries, and network management systems without disrupting ongoing Internet operations. Designing such hybrid architectures requires careful protocol standardization and extensive interoperability testing before widespread deployment becomes feasible.

Although blockchain significantly improves routing transparency and trust, it cannot independently detect sophisticated routing anomalies based solely on behavioral characteristics. Consequently, many researchers advocate combining blockchain with

complementary technologies such as Machine Learning, Software Defined Networking (SDN), and cryptographic validation systems. Machine learning identifies abnormal routing behavior, blockchain establishes decentralized trust, and cryptographic mechanisms verify route authenticity, thereby creating multiple layers of defense against increasingly sophisticated routing attacks.

Overall, blockchain represents one of the most significant technological developments in secure inter-domain routing because it decentralizes trust management, enhances route authenticity, improves transparency, and strengthens protection against prefix hijacking and route manipulation. However, transaction latency, scalability limitations, computational overhead, deployment complexity, and interoperability challenges continue to hinder its large-scale adoption within operational ISP networks. These limitations highlight an important research gap concerning the development of routing security mechanisms that maintain strong security guarantees while minimizing computational complexity and operational overhead.

The proposed Lightweight Secure Border Gateway Protocol (L-SBGP) addresses this gap by emphasizing lightweight validation mechanisms that reduce computational overhead, memory utilization, protocol complexity, and convergence delays while maintaining effective protection against routing attacks. Unlike blockchain-based routing systems that require distributed consensus and ledger synchronization, L-SBGP focuses on efficient route validation suitable for real-time ISP environments where scalability, performance, and low operational cost are critical deployment requirements. Consequently, L-SBGP provides a practical balance between security effectiveness and routing efficiency, making it more suitable for large-scale deployment in resource-constrained Internet Service Provider infrastructures.

### 2.4.9 Software Defined Networking (SDN) and Secure BGP

Software Defined Networking (SDN) has emerged as one of the most significant innovations in modern computer networking and has attracted considerable attention as a potential solution for addressing the security, scalability, and management challenges associated with Border Gateway Protocol (BGP). Traditional IP networks tightly integrate the control plane, which makes routing decisions, with the data plane, which forwards packets. This distributed architecture has served the Internet for decades but has become increasingly difficult to manage due to the rapid expansion of

Internet traffic, the growing number of Autonomous Systems (ASs), and the increasing sophistication of routing attacks. SDN fundamentally changes this architecture by separating the control plane from the data plane, allowing routing decisions to be managed centrally through programmable controllers. This centralized control provides greater network visibility, flexibility, and automation, making SDN a promising platform for enhancing BGP security.

The primary objective of SDN is to simplify network management while enabling intelligent and dynamic control of routing decisions. Instead of configuring individual routers independently, SDN enables a centralized controller to monitor the entire network topology and distribute routing policies to forwarding devices. This global network view enables faster decision-making and improves the consistency of routing policies across large-scale Internet Service Provider (ISP) networks. In secure BGP environments, SDN controllers can monitor routing updates continuously, identify suspicious routing behavior, and enforce security policies before malicious routing information spreads across the network.

One of the most significant advantages of SDN is centralized route management. Conventional BGP relies on decentralized routing decisions made independently by each router based on locally available routing information. Although this distributed approach enhances scalability, it limits the ability of individual routers to detect network-wide routing anomalies. SDN controllers overcome this limitation by collecting routing information from multiple routers simultaneously and maintaining a comprehensive view of network conditions. This centralized visibility allows controllers to detect abnormal routing patterns that would otherwise remain undetected when routers operate independently.

SDN significantly improves the detection and mitigation of routing attacks such as prefix hijacking and route leaks. Since the SDN controller continuously monitors routing advertisements received from all connected routers, it can rapidly identify unauthorized route announcements or unexpected changes in routing behavior. Once suspicious activity is detected, the controller can automatically withdraw malicious routes, update routing policies, isolate compromised network segments, or redirect traffic through trusted paths. This centralized response mechanism considerably

reduces the time required to contain routing attacks compared to conventional BGP security approaches.

Another important contribution of SDN is programmable routing policy enforcement. Traditional BGP requires network administrators to manually configure routing policies across multiple routers, a process that is often complex, time-consuming, and prone to configuration errors. SDN introduces programmable interfaces through which routing policies can be automatically deployed and updated from a centralized controller. Security policies can therefore be modified dynamically in response to evolving threats without requiring manual configuration of individual routers. This programmability significantly improves operational efficiency while reducing the likelihood of human errors that frequently contribute to routing incidents.

OpenFlow, one of the most widely adopted SDN communication protocols, further enhances secure routing by enabling direct communication between SDN controllers and forwarding devices. OpenFlow allows controllers to install, modify, or remove forwarding rules dynamically according to current network conditions. During routing attacks, OpenFlow-enabled controllers can immediately update forwarding tables to block malicious traffic or reroute legitimate traffic through secure paths. This capability provides significantly faster mitigation than traditional routing mechanisms, where routing updates must propagate gradually across multiple Autonomous Systems before reaching network convergence.

The integration of SDN with Resource Public Key Infrastructure (RPKI) has become an important area of recent research. In hybrid SDN-RPKI architectures, SDN controllers automatically validate Route Origin Authorizations (ROAs) using RPKI repositories before permitting route propagation. Invalid route announcements are rejected immediately without requiring extensive manual intervention. Centralized RPKI validation also reduces redundant verification processes performed independently by multiple routers, thereby improving overall routing efficiency while strengthening route authenticity.

Similarly, SDN has been integrated with BGPsec to improve the management of cryptographic route validation. Rather than requiring each router to independently perform computationally expensive cryptographic operations, SDN controllers can

coordinate validation procedures centrally, reducing redundant processing across the network. This centralized approach improves resource utilization while maintaining the strong security guarantees provided by BGPsec. Although cryptographic overhead remains significant, centralized coordination reduces duplicate computations and simplifies overall protocol management.

Recent developments between 2024 and 2025 have introduced Artificial Intelligence (AI) and Machine Learning (ML) into SDN-based secure routing architectures. Intelligent SDN controllers now employ machine learning algorithms to analyze routing behavior, predict network congestion, identify routing anomalies, and optimize traffic engineering automatically. These intelligent controllers continuously adapt routing decisions according to changing network conditions while maintaining high levels of security and performance. Such adaptive capabilities represent an important advancement over conventional static routing policies.

Intent-Based Networking (IBN) has also emerged as an extension of SDN in modern ISP infrastructures. Instead of manually specifying detailed routing configurations, network administrators define high-level operational objectives, such as maximizing security, minimizing latency, or ensuring service availability. The SDN controller automatically translates these objectives into routing policies and continuously adjusts network configurations to maintain compliance. This automation significantly reduces operational complexity while improving network responsiveness to changing security conditions.

Cloud-native SDN architectures have become increasingly important due to the rapid growth of cloud computing, virtualization, and edge computing environments. Modern Internet Service Providers increasingly deploy virtualized routing functions that can be managed centrally through SDN controllers operating within cloud platforms. This architecture provides enhanced scalability, rapid resource provisioning, and simplified management of geographically distributed routing infrastructures while maintaining centralized security enforcement.

SDN also facilitates network segmentation and isolation, which are valuable security mechanisms for limiting the impact of routing attacks. If malicious routing behavior is detected within a particular network segment, the SDN controller can immediately

isolate the affected routers without disrupting the remainder of the network. Such containment strategies minimize service interruptions while preventing the rapid propagation of malicious routing information throughout interconnected Autonomous Systems.

Traffic engineering represents another major benefit of SDN-enabled secure routing. By maintaining real-time knowledge of network utilization, the SDN controller dynamically distributes traffic across multiple available paths to reduce congestion, improve bandwidth utilization, and minimize routing delays. During periods of heavy network traffic or routing instability, intelligent traffic engineering maintains service quality while avoiding overloaded network links. This capability improves both network performance and resilience under adverse conditions.

Despite these numerous advantages, SDN introduces several implementation challenges that limit its universal deployment within Internet Service Provider networks. One major concern is controller dependency. Because routing decisions are centralized, the SDN controller becomes a critical component whose failure may significantly disrupt network operations. If the controller experiences hardware failures, software faults, or cyberattacks, large portions of the network may lose centralized management capabilities. Consequently, modern SDN deployments require redundant distributed controller architectures to eliminate single points of failure and improve system availability.

Scalability also presents an important challenge. As network size increases, SDN controllers must process increasingly large volumes of routing updates, topology information, security events, and traffic statistics. Extremely large Internet Service Provider networks may generate workloads that exceed the processing capabilities of individual controllers. Hierarchical and distributed controller architectures have therefore been proposed to improve scalability while preserving centralized management functionality.

Communication overhead between SDN controllers and forwarding devices represents another limitation. Controllers must continuously exchange control messages with routers to maintain updated forwarding tables and routing policies. Under highly dynamic network conditions, frequent control-plane communication may consume

additional bandwidth and increase processing overhead. Efficient controller communication protocols remain an active area of SDN research.

Security of the SDN controller itself is another major concern. Since the controller possesses complete control over routing policies and forwarding decisions, it becomes an attractive target for cyberattacks. Attackers who successfully compromise the controller may manipulate routing policies, redirect traffic, or disable network services entirely. Consequently, securing the controller through strong authentication, encryption, access control, intrusion detection systems, and redundancy mechanisms is essential for reliable SDN deployment.

Migration from conventional BGP infrastructures to SDN-enabled routing environments also presents practical deployment challenges. Most operational ISP networks continue to rely on traditional distributed routing architectures that have evolved over many years. Complete replacement of these infrastructures would require significant investments in new hardware, software, personnel training, and operational procedures. Therefore, most current deployments adopt hybrid SDN-BGP architectures that gradually introduce centralized management while preserving compatibility with existing routing systems.

Although SDN substantially improves routing management, automation, and security monitoring, it does not independently solve all BGP security problems. Consequently, recent research increasingly advocates combining SDN with complementary technologies such as Machine Learning, Blockchain, RPKI, and BGPsec. Machine learning provides intelligent anomaly detection, blockchain establishes decentralized trust management, cryptographic mechanisms verify route authenticity, and SDN offers centralized policy enforcement and automated response. The integration of these technologies creates multiple complementary layers of defense capable of addressing increasingly sophisticated Internet routing threats.

Overall, Software Defined Networking represents one of the most important technological developments in secure inter-domain routing because it introduces centralized network visibility, programmable routing management, automated security policy enforcement, and intelligent traffic engineering. These capabilities significantly improve the detection and mitigation of routing attacks while reducing

operational complexity within modern ISP environments. However, controller dependency, scalability limitations, communication overhead, controller security, and migration complexity continue to present important implementation challenges that must be addressed before SDN-based secure routing can achieve widespread deployment.

The proposed Lightweight Secure Border Gateway Protocol (L-SBGP) differs from SDN-based secure routing by focusing primarily on reducing computational complexity, protocol overhead, memory utilization, and convergence delays without introducing centralized controller dependency. While SDN provides powerful centralized management and automation capabilities, L-SBGP emphasizes lightweight distributed validation mechanisms that are easier to deploy within heterogeneous ISP infrastructures. Consequently, L-SBGP seeks to provide an effective balance between routing security, scalability, operational simplicity, and computational efficiency, making it suitable for practical deployment across both conventional and evolving Internet Service Provider networks.

## 2.5 Parameters for reducing complexity overhead in routing protocols in an ISP

### 2.5.1 Convergence Time

The convergence time is the period between a network change (such as a route update or link failure) and when the routing protocol stabilizes. Convergence in an ISP environment is essential for reducing packet loss, routing instability, and service interruptions. Minimizing convergence time reduces processing delays and increases network speed, thereby reducing computational overhead on the routing devices.

### 2.5.2 CPU Utilization

CPU utilization quantifies the percentage of CPU time used for routing operations and route validation. Intensive cryptographic computations are needed to secure routing protocols like BGPsec, thereby increasing CPU load. Lightweight validations have a positive impact on router performance and scalability, as well as on reducing the cost of ISP infrastructure.

### 2.5.3 Protocol Overhead

Control messages and signaling traffic generated during route propagation and validation are known as protocol overhead. Too many routing updates consume

bandwidth and place a processing burden on routers. Minimizing protocol overhead helps improve routing efficiency, reduces congestion, and ensures smoother communication between Autonomous Systems (ASs).

### 2.5.4 Memory Utilization

Memory utilization refers to the memory used to store routing tables, security credentials, and validation information. Traditional secure routing protocols require large memory resources for cryptographic keys and certificates. Lightweight routing mechanisms are memory-efficient; that is, they can process larger routing tables efficiently in large-scale ISP networks.

### 2.5.5 Scalability

Scalability is the performance of a routing protocol under high network load or when the number of routing updates increases. ISP networks are continually expanding due to the ongoing growth of internet usage and the interconnected Autonomous Systems. A low-complexity routing protocol can scale well without degrading resource performance or increasing processing delay.

### 2.5.6 Security Effectiveness

Security effectiveness is how well a routing protocol can detect and prevent routing attacks such as prefix hijacking and malicious route propagation. A secure routing protocol should be lightweight, with strong protection mechanisms, and require minimal computation. Security and efficiency are important aspects to balance for a viable ISP deployment.

## 2.6 Existing Simulation Tools

When proposing and testing an improved BGP, specific tools are employed to assess the effectiveness and security of the devised solution. If properly implemented, four special tools are noteworthy in this regard. One of them is ns-3 (Network Simulator 3), a discrete-event simulator specialized in Internet systems, with a rich set of implementations of complex protocols and detailed studies of BGP and its security extensions. Framework is another useful modular tool that follows the component-based Design and is used for large-scale node systems and network protocols, including BGP. C-BGP is a versatile BGP simulator that efficiently emulates BGP routing in large networks. The offered method can be applied to evaluate the

effectiveness of the following security enhancements. The last is BGPsim, which is popular for its ability to model BGP's dynamic behavior. It provides the ground on which BGP security solutions are tested, depending on prevailing conditions. Altogether, these tools provide a solid foundation for designing and developing better BGP protocols and evaluating their practicality without introducing security threats. Four notable tools are:

### 2.6.1. NS-3 (Network Simulator 3)

NS-3, or Network Simulator 3, is an efficient, general-purpose discrete-event network simulator primarily for Internet systems. Therefore, it proved useful for researchers and engineers working on opportunities to analyze network protocols, such as Border Gateway Protocol (BGP), and improve their performance. As mentioned before, ns-3 offers many options, enabling detailed and accurate investigation of BGP and supporting the creation of various experiments.

This proposal has endeavored to assert that one of ns-3's other strengths is the feasibility of providing more detailed modeling of BGP and enhanced BGP security [43]. They can account for all kinds of actions and communications taking place within the BGP network, which is why this quality is so valuable. To explain how BGP operates, individuals have suggested emulating scenarios within the network and then observing how it performs in normal operations, especially during attacks. For instance, ns-3 can help study the impact of route hijacking, prefix hijacking, and route leaks in a network, providing a deeper understanding of how these issues affect the network's stability and security.

It can also address noise and test numerous BGP security changes. The researchers can implement ways to validate that a specific update is from a legitimate source, approve the route an AS can advertise, and verify that the contents of an update have not been tampered with. Thus, it becomes possible to evaluate design enhancements of this kind in ns-3 and to consider their efficiency in security protection. This kind of flexibility in the simulator is also present during testing of confidentiality features, such as encrypting BGP sessions to prevent unauthorized parties from disclosing sensitive routing information. In addition, ns-3 can provide the timely update of the BGP and the dissemination of the update throughout the network to ensure the stability [44]. Overall, ns-3 provides an appealing and powerful platform to design and test

better BGP protocols. The detailed modeling capabilities and the enhancement of the list of security extensions made it indispensable when it came to further maturing stable and secure BGP in real internet systems.

### 2.6.2 OMNeT++

For this reason, OMNeT++ is a logically integrated, rather general-purpose simulation environment in computer networks with a component-based, free-form conventional C++ simulation core. Its distinctive feature and module structure enable the implementation of network models as components or modules, enabling an efficient simulation and interaction process for the complex system. It offers high modularity and extensibility, and the latter makes it efficient at solving different simulation problems, particularly for emulating network protocols like BGP, and, in general, large-scale network simulation is easy to work with. Accordingly, the availability of well-scaled and efficient simulation methods enables researchers/developers to approximate real-life network behavior to a great extent and to capture the refined specifics of BGP routing as in actuality. Therefore, regardless of the need to mimic BGP behavior across different scenarios or to test new improvements to BGP behavior in OMNeT++ performance, OMNeT++ provides a proper theoretical foundation [45].

Furthermore, OMNeT++ provides sufficient information and several options for model change and simulation extension, which may be essential for the assumptions or experimental objectives specified for the simulations in certain research [46]. The extent of this flexibility enables the investigators to test many hypotheses and examine several Design possibilities simultaneously, which is advantageous when searching for better BGP protocols. Therefore, OMNeT++ is a valuable contribution to network simulation, as it enables the search for much better solutions to contemporary network protocols, including BGP, through simulation.

### 2.6.3 C-BGP

The specific acronym C-BGP, as in "Border Gateway Protocol Simulator," is essential for network simulation, particularly for studying interactions in BGP routing in large networks. Because the tool can be scaled to any network, it is ideal for dissecting the effects of a range of BGP boosters.

Since BGP routing is closely intertwined with the overall network infrastructure, it is crucial to have a tool that simulates its behavior at a large scale. That is why the BGP-Imp simulator is developed. Thus, C-BGP is more effective in this regard and is intended to allow the researchers and network administrators to assess the efficiency and analytical usefulness of potential security improvements to BGP. This means that using CBGP would enable the creation of network scenarios that realize the conditions of BGP routing protocols, as well as other features demonstrated [47]. This helps evaluate potential threats and risks within the Company's information security network, thereby facilitating the formulation of effective strategies to address the issues above.

Firstly, C-BGP operates at the scale of the network; all simulations use a large-scale network topology, since BGP routing decisions affect large networks. This enables the researchers to conduct a comparative analysis of security enhancements across multiple networks to establish their effectiveness and likelihood in real-world settings. In summary, C-BGP will benefit researchers, network engineers, and policymakers by improving BGP routing protocols in terms of security and capacity [48]. With its capacity to model at scale how BGP routing occurs and to assess the potential benefits of security upgrades, GDM is an invaluable resource in contemporaneous efforts to protect the key structures of the Internet against new threats.

### 2.6.4 BGPsim

BGPsim is a tool specifically tailored to the task and was created solely to evaluate the BGP protocol in its real-time environment. Still, BGPsim is not a generic network simulator because its scope is significantly broader, providing an accurate view of the mechanism and shedding light on BGP’s operation in detail. This is also one of the key benefits of the tool’s power, since it can convincingly model several types of attacks in BGP security systems extensively [49]. This feature is of great concern to researchers and network engineers who are ready to assess the efficiency of the various security enhancements to the BGP protocol.

Thus, the freedom granted to BGPsim users allows them to simulate diverse scenarios of the daily operation of the BGP protocol or security events; this freedom enables a multifold assessment of BGP reliability. Therefore, BGPsim enables one to assess the protocol's behavior under real-world conditions, such as network failures, attempts at

route hijacking, and other forms of malicious behavior. Such simulations are appropriate for identifying weaknesses in existing security measures and evaluating directions for strengthening BGP security against novel threats. Moreover, BGPsim enables the assessment of new security measures proposed for BGP before adopting them in a real network [50]. This methodology is useful for minimizing scenarios in which one encounters problems with living systems or issues that may even bring them to a halt. BGPsim successfully helps the panel of stakeholders assess BGP security and lays the groundwork for the subsequent development of highly reliable, secure protocols to strengthen the integrity of the World Wide Web's routing system. Table 2.2 Comparing the disused simulation tools.

**Table 2.2 Comparison of Simulation Tools**

| Simulation Tool | Features | Strengths | Weaknesses |
|---|---|---|---|
| **NS-3** | Discrete-event network simulator with support for routing, wireless, and internet protocols | Highly accurate network simulation, open-source, supports real-world protocol testing, and has strong research community support | Steeper learning curve, requires programming knowledge, simulation setup can be time-consuming |
| **OMNeT++** | Modular and component-based simulation framework for communication networks | Flexible architecture, graphical interface support, suitable for large-scale simulations | Complex configuration process, some frameworks require additional integration |
| **GNS3** | Real-time network emulation platform integrating virtual and physical devices | Supports real router images, practical networking environment, ideal for protocol deployment testing | High hardware resource requirements, slower for large-scale simulations |
| **Cisco Packet Tracer** | Educational network simulation tool developed by Cisco | User-friendly interface, suitable for beginners, and easy network topology design | Limited advanced protocol support, less suitable for research-level simulations |
| **Mininet** | Lightweight network emulator for Software Defined | Fast prototyping, supports SDN/OpenFlow experiments, and | Limited scalability for very large topologies, focused mainly |

| | | | |
|---|---|---|---|
| | Networking (SDN) | lightweight virtualization | on SDN environments |
| **OPNET/Riverbed Modeler** | Commercial simulation platform for communication and network performance analysis | High accuracy, extensive protocol libraries, and professional analytical capabilities | Expensive licensing costs, less accessible for academic researchers |
| **MATLAB Simulink** | Mathematical and network system modeling environment | Strong analytical and visualization capabilities, supports algorithm development | Limited native networking functionalities compared to dedicated network simulators |
| **Google Colab** | Cloud-based Python execution and computational analysis platform | Free cloud computation resources, supports Python networking simulations, and easy collaboration | Not a dedicated network simulator, dependent on internet connectivity |

### 2.7 Performance Metrics

Several performance metrics can be used to evaluate the effectiveness of the routing protocols for Internet Service Providers (ISPs). These metrics are essential for assessing the protocol's efficiency, Scalability, and ability to meet the demands of modern networks. The primary performance metrics for this study include:

#### 2.7.1 Packet delivery ratio (PDR)

Routing convergence time, throughput, CPU utilization, memory consumption, security efficiency, and Scalability. Packet Delivery Ratio (PDR) is a key metric that measures the percentage of successfully delivered data packets over a network. It is a direct measure of the reliability of a routing protocol. A higher PDR signifies that the

protocol could successfully steer traffic, which means that users will not suffer disruptions and a loss of packets [51]. The optimization of PDR is a key component to the efficient transmission of data, especially in networks that are large in size where packet loss can lead to a tremendous loss of performance.

### 2.7.2 Routing Convergence Time

Another key performance is Routing Convergence Time, that is, how long the network takes to move to a stable state after a change in the network's topology occurs, such as a link failing or a new route being added to the network. Reducing downtime and disruption to network services is crucial and requires faster convergence times. A faster converging protocol enables immediate traffic re-direction which helps maintain stability and good performance in dynamic conditions. One indication of how efficient a protocol is is the amount of information that needs to be transmitted in order to complete the protocol control message, called Protocol Overhead (e.g., routing updates and topology information). High protocol overhead can burden network resources such as bandwidth and CPU power, leading to slower processing times and higher latency. Reducing protocol overhead is crucial for optimizing network performance, as it minimizes router load and improves response times [52].

### 2.7.3 Throughput

Throughput is one of the most important real-time performance parameters, indicating a network's ability to transfer data. It reflects the protocol's ability to manage and route data packets within the intended protocol. Hence, for LBGPSec, it was important to achieve high throughput to enable ISPs to offer efficient service, especially during peak season.

Specifically, a lightweight, secure protocol such as LBGPSec is expected to enhance the received throughput because computations, overhead, and packet processing consume less power. This means quicker, more efficient routing of data packets and virtually no packet loss on the way to the destination. Specifically, LBGPSec minimizes expensive cryptographic computations and eliminates computationally nonessential procedures to optimize data traffic while preserving security.[53]

High throughput increases user satisfaction by enabling fast, reliable data transmission and allowing the network to scale to larger sizes. Through LBGPSec, ISPs can scale

their networks to accommodate increased traffic capacity while maintaining responsiveness, reliability, and security to meet current ISP requirements.

### 2.7.4 CPU Utilization

CPU Utilization is one of the important parameters to understand the computational requirements of the protocol. High CPU consuming protocols can cause routers to become slow, particularly under heavy traffic or when topology changes frequently. LBGPSec's lightweight protocol reduces the amount of CPU needed to process the protocol, allowing routers to remain responsive to an increase in traffic without being overburdened. This will enhance the scalability of the network. Another important measure is Memory Consumption, which indicates the memory needed for the protocol to hold routing tables and other information. Router memory usage can be a constraint on the number of routes it can process, impacting on Scalability and performance. A new protocol that requires a minimal amount of memory allows routers to service larger networks without memory problems, helping facilitate the Internet's expansion.

Security Efficiency is one key factor for evaluating a security/performance tradeoff. Security is critical to prevent threats such as route hijacking, man-in-the-middle attacks, etc., and cryptographic operations can consume a lot of computation resources. The objective is to come up with a protocol that has high security but also low latency and light footprint on the system, where security does not have to be sacrificed for performance.

Last but not least, Scalability is a key performance indicator, especially with the ever-expanding Internet. A protocol should be scalable, that is, be able to support growing numbers of its routing entries, network nodes, and traffic flow without performance degradation. With the emphasis on Scalability, the designed LBGPSec protocol allows ISPs to expand their network efficiently while ensuring its efficient operation and performance.

## 2.8 Conceptual Framework

### 2.8.1 Theoretical Foundation of the Conceptual Framework

The conceptual framework for this study is grounded in the Theory of Network Layer Routing, the End-to-End Principle, the Complexity Theory of Distributed Systems,

and the Defense-in-Depth Security Model. Collectively, these theories explain the relationships among routing efficiency, computational complexity, security effectiveness, and scalability in Internet Service Provider (ISP) networks.

The Theory of Network Layer Routing provides the fundamental basis for understanding how routing protocols discover, select, and maintain optimal communication paths across interconnected Autonomous Systems (ASs). According to routing theory, efficient routing protocols should minimize routing convergence time, optimize resource utilization, and adapt dynamically to network topology changes while maintaining reliable packet delivery. Border Gateway Protocol (BGP), as the standard inter-domain routing protocol, satisfies scalability requirements but lacks intrinsic security mechanisms, making it susceptible to route hijacking, route leaks, and malicious path manipulation. Consequently, routing theory supports the need for enhanced routing mechanisms that improve security without significantly increasing routing complexity.

The framework is further supported by the End-to-End Principle, which states that network intelligence should primarily reside at communication endpoints rather than introducing unnecessary complexity within the network infrastructure. Modern secure routing protocols such as BGPsec employ extensive cryptographic verification throughout the routing infrastructure, significantly increasing CPU utilization, memory consumption, protocol overhead, and routing convergence time. The End-to-End Principle therefore advocates lightweight network functions that achieve essential security objectives while minimizing processing overhead. This principle provides theoretical justification for the proposed Lightweight Secure Border Gateway Protocol (L-SBGP), which emphasizes efficient route validation and simplified routing mechanisms.

The Complexity Theory of Distributed Systems also underpins this study. Internet routing operates as a highly distributed system comprising thousands of independently administered Autonomous Systems that exchange routing information continuously. As network size increases, computational complexity, routing table size, protocol overhead, and convergence delays also increase. Complexity theory argues that scalable distributed systems should minimize algorithmic complexity while maintaining system reliability and adaptability. This theoretical perspective explains

why reducing computational overhead is essential for improving the scalability and operational efficiency of secure routing protocols in large ISP environments.

The conceptual framework is additionally informed by the Defense-in-Depth Security Model, which advocates multiple complementary layers of protection rather than relying on a single security mechanism. Modern secure routing increasingly combines cryptographic validation, route monitoring, anomaly detection, adaptive routing policies, and real-time network analysis to improve resilience against sophisticated routing attacks. Rather than depending exclusively on computationally expensive cryptographic verification, L-SBGP integrates lightweight route validation, adaptive path optimization, and simplified routing mechanisms to achieve an appropriate balance between security and performance.

Recent developments in Software Defined Networking (SDN), Machine Learning (ML), Blockchain, and Resource Public Key Infrastructure (RPKI) further reinforce these theoretical foundations. SDN contributes centralized visibility and programmable routing control, Machine Learning enables intelligent anomaly detection, Blockchain introduces decentralized trust management, and RPKI strengthens route origin validation. Although these technologies significantly improve routing security, they also introduce additional computational complexity, implementation costs, infrastructure requirements, and scalability challenges. Consequently, the proposed L-SBGP adopts only those design principles that improve routing efficiency while avoiding unnecessary computational burden, thereby aligning with the principles of efficient distributed system design.

Based on these theoretical perspectives, this study assumes that reducing routing complexity through lightweight validation mechanisms and adaptive routing optimization improves convergence time, CPU utilization, protocol overhead, memory consumption, scalability, and overall security effectiveness without compromising routing reliability. The conceptual framework therefore explains how the proposed L-SBGP influences routing performance directly while considering the moderating effects of network environment, traffic load, and routing topology.

### 2.8.2 Explanation of the Conceptual Framework

The conceptual framework shown in Figure 2.6 illustrates the relationships among the independent, mediating, moderating, and dependent variables that guide this study. The independent variable is the proposed Lightweight Secure Border Gateway Protocol (L-SBGP), which incorporates lightweight validation mechanisms, adaptive path optimization, and simplified routing processes designed to reduce computational complexity while maintaining secure inter-domain routing.

The moderating variables include network environment, traffic load, and routing topology. These variables influence the magnitude of L-SBGP's performance because routing behavior varies according to network size, routing policies, traffic intensity, and topological complexity. Consequently, the effectiveness of lightweight routing mechanisms may differ under different operational conditions.

The independent variables are routing convergence time, CPU utilization, memory utilization, protocol overhead, and scalability. These variables represent the key performance indicators used to evaluate the effectiveness of the proposed protocol. The dependent variable is the lightweight secure protocol.

Overall, the conceptual framework proposes that implementing lightweight route validation together with adaptive routing optimization provides an effective balance between security, computational efficiency, and scalability. This theoretical relationship forms the foundation for the experimental evaluation presented in Chapter Four, where the performance of L-SBGP is compared with conventional BGP and existing secure routing mechanisms under controlled simulation scenarios.

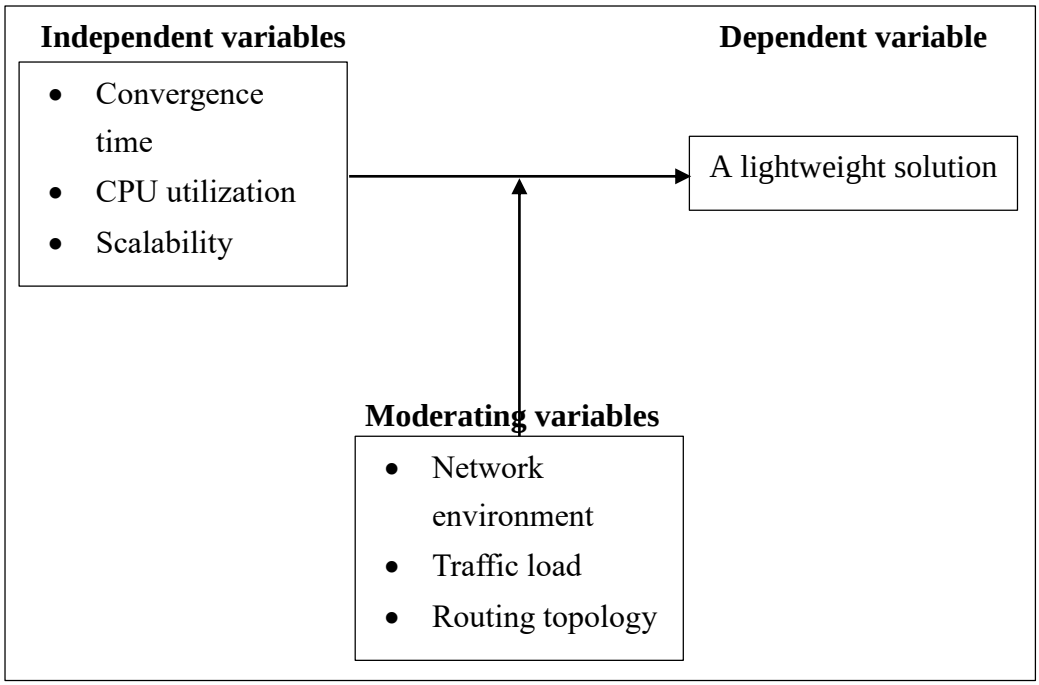



**Figure 2.6 : Conceptual Framework**

## 2.9 Summary

This chapter discusses the problems with BGP and shows that much remains to be done to develop superior Internet routing solutions. BGP is the key to inter-domain routing, but it suffers from complexity, performance, Scalability, and security problems. These problems are even more pronounced with the ever-growing Internet and increasing traffic volume, underscoring the need for more effective routing algorithms.

Some of the issues stressed in this chapter include the complexity of BGP, especially when it comes to sizing the updates and policy control structures within AS settings. Thus, the process is very complicated and consumes substantial operational effort from Internet Service Providers (ISPs), who are expected to have adequate human capital. Moreover, BGP exhibits high computational complexity, resulting in strenuous processing and high bandwidth consumption, which in turn lead to poor convergence, delays, and inefficiencies in data transfer. As will be apparent from these problems, various solutions, such as BGPsec and RPKI, have been developed. While these solutions smooth some aspects, such as security and routing table validation, they also introduce additional difficulties and degrade performance, making them unsuitable for global scale.

The chapter then presents LSBGP as another promising approach to overcome these limitations. Instead, LSBGP aims to support incremental/periodic updates to alternate paths, detect network congestion as soon as possible, and streamline routing constructs by minimizing computational overhead, all to maximize network efficiency. Furthermore, LSBGP can scale better than conventional solutions, enabling it to adapt to the growing demand for services on the Internet. LSBGP is claimed to be a realizable solution that can outperform and out scale regular BGP and its modifications.

# CHAPTER THREE
# METHODOLOGY

## 3.1 Introduction

This chapter presents the methodology used to achieve the objectives of the study, which focused on analyzing the parameters that contribute to complexity overhead in secure inter-domain routing, designing the Lightweight Secure Border Gateway Protocol (L-SBGP), and evaluating its performance and security effectiveness. The study adopted an experimental design that integrated qualitative and quantitative techniques. The qualitative component comprised a systematic literature review (SLR) and expert consultation, while the quantitative component involved simulation-based experimental evaluation of the proposed L-SBGP protocol against conventional BGP and BGPsec.

The qualitative component was used to identify and validate the key parameters that influence the efficiency, security, and operational complexity of secure routing protocols in Internet Service Provider (ISP) environments. The findings from the literature and expert consultation informed the selection of performance indicators and the design requirements of L-SBGP. The quantitative component was subsequently used to evaluate the proposed protocol under controlled and reproducible routing scenarios.

The chapter describes the research design, research process, research method, population and sample, data collection procedures, data analysis techniques, simulation environment, validity considerations, and ethical issues. The methodological approach was structured to ensure that the protocol design was informed by both existing research evidence and practical expert knowledge, while its performance was evaluated objectively using quantitative simulation experiments.

## 3.2 Research Design

The study adopted an experimental research design incorporating qualitative evidence synthesis, expert consultation, and quantitative simulation-based experimentation. The design was selected because the research objectives required both contextual understanding of secure routing complexity and objective measurement of the performance of the proposed L-SBGP protocol.

The qualitative component consisted of two complementary activities. First, a systematic literature review was conducted to identify parameters associated with complexity, efficiency, scalability, and security in secure BGP deployments. Second, expert consultation was undertaken to obtain practical perspectives from professionals with experience in networking, cybersecurity, ISP routing, and BGP-related technologies. The purpose of these qualitative activities was to identify and validate the parameters that should guide the design and evaluation of a lightweight secure routing protocol [54].

The quantitative component involved controlled simulation experiments in which L-SBGP was evaluated against established routing approaches, particularly BGP and BGPsec. The simulations were designed to measure objectively selected performance indicators, including convergence time, control-plane overhead, CPU utilization, memory consumption, routing-table consistency, and security effectiveness.

The experimental design therefore followed a sequential logic. Findings from the systematic literature review and expert consultation informed the selection of design requirements and evaluation parameters. These findings were then translated into the design of the L-SBGP protocol and its validation procedures. Finally, quantitative simulation experiments were conducted to determine whether the proposed protocol could achieve the intended balance between routing efficiency and security [55].

This approach was appropriate for a proof-of-concept study because simulation provides a controlled and reproducible environment in which a newly proposed routing mechanism can be evaluated before deployment in operational ISP networks. It enables the researcher to maintain comparable experimental conditions across protocols while measuring the effects of the proposed security mechanisms on routing performance. However, the simulation results are interpreted as proof-of-concept evidence rather than as a direct substitute for validation in production ISP environments.

### 3.3 Research Process

The research process was organized into three sequential stages corresponding to the three specific objectives of the study.

The first stage involved identifying and validating the parameters associated with complexity overhead in secure routing protocols. A systematic literature review was conducted using peer-reviewed literature, followed by consultation with networking and cybersecurity experts. The findings from these activities were used to identify parameters considered important for evaluating lightweight secure routing protocols, including convergence time, CPU utilization, protocol overhead, memory utilization, scalability, and security effectiveness.

The second stage involved the design and development of the L-SBGP protocol. The parameters identified during the first stage informed the design requirements of the proposed protocol. The protocol incorporated lightweight route-validation mechanisms and routing decision procedures intended to reduce computational overhead while maintaining protection against malicious routing announcements. Algorithms, flowcharts, and architectural representations were developed to describe the proposed routing and validation processes [56].

The third stage involved simulation-based experimental validation. The proposed L-SBGP protocol was implemented as a Python-based prototype in the Google Colab environment and evaluated under controlled routing scenarios. The experimental results were compared with benchmark implementations representing conventional BGP and BGPsec. The evaluation focused on convergence time, control-plane messages, CPU utilization, memory consumption, routing-table consistency, and security effectiveness.

The research process therefore followed the sequence:

Parameter Identification and Validation → Protocol Design and Development → Simulation-Based Experimental Validation

This sequence ensured that the proposed protocol was not designed solely from theoretical assumptions. Instead, the design requirements were informed by findings

from the literature and expert consultation before the protocol underwent quantitative evaluation.

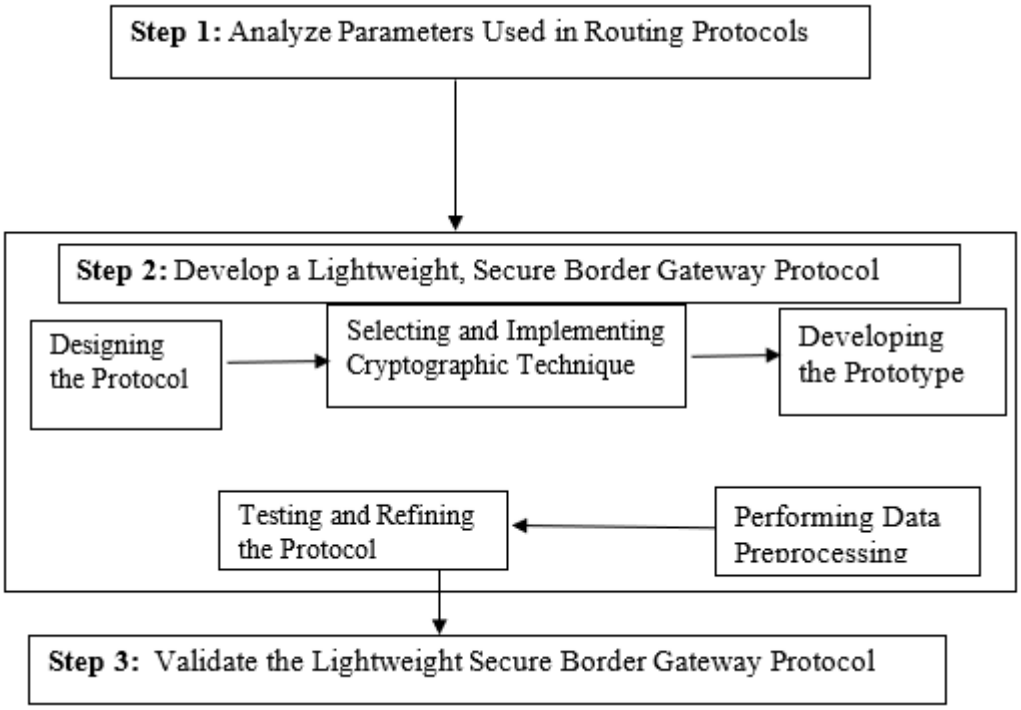



**Figure 3.1: Research Process**

### 3.4 Research Method

The simulation environment used in this study was developed and executed entirely in Google Colab using the Python programming language. Google Colab provided a cloud-based computational platform for implementing, executing, and evaluating the proposed routing security framework under controlled experimental conditions.

Python was used to develop a proof-of-concept simulation model representing the routing behavior of the benchmark protocols—Conventional BGP and BGPsec—as well as the proposed Lightweight Secure Border Gateway Protocol (L-SBGP). The implementation enabled the execution of routing experiments, measurement of selected performance metrics, and generation of comparative results for performance evaluation.

To ensure a fair and consistent comparison, all routing protocols were evaluated using the same simulated network topology and identical routing conditions. This common experimental setup ensured that any observed differences in performance were

attributable to the routing and validation mechanisms of the respective protocols rather than variations in the underlying network environment.

The Python implementation incorporated computational libraries to measure key performance indicators, including execution time, CPU utilization, and memory consumption. In addition, the simulation modeled the computational overhead associated with cryptographic validation by implementing digital signature operations for BGPsec and lightweight hash-based validation mechanisms for the proposed L-SBGP protocol. These implementations enabled an assessment of the relative computational efficiency of each routing approach [57][58].

All experimental results presented in this thesis were generated exclusively from the Python-based simulation model executed in Google Colab. The implementation serves as a proof-of-concept model for evaluating the effectiveness and computational performance of the proposed L-SBGP protocol. Consequently, the findings reported in this study should be interpreted as results obtained from a Python simulation environment developed in Google Colab rather than from any other network simulation platform. The objectives are listed and accomplished in the following order: objective 1, objective 2, and objective 3, as shown in Table 3.1.

**Table 3.1 Objective Table**

| Objective | Technique to Use | Indicators |
|---|---|---|
| 1. To analyze the parameters used to reduce complexity overheads in routing protocols in Internet service providers. | -Systematic Literature Review<br>- Expert opinion (Used purposive sampling) | Publication |
| 2. To design a lightweight, secure border gateway protocol for Internet service providers. | - Algorithms<br>-Flowcharts | -Proposed Protocol |
| 3. To validate a lightweight, secure border gateway routing protocol. | - Simulation Experiments (table with Initial Simulation Parameters)<br>- Quantitative Data Analysis | Results of Simulation Experiments<br>Publication validation results |

The first goal of the study was to learn about the parameters used to reduce complexity overheads of the routing protocols in Internet Service Providers (ISPs). The study was based on a Systematic Literature Review (SLR) using Kitchenham's approach and supplemented by expert analysis, to achieve this goal. The data was collected from IEEE Xplore, ACM digital library, ScienceDirect, and SpringerLink, and the selected papers in the list were peer-reviewed papers from 2020 to 2025. The review focused on the main factors that affect the security of lightweight routing protocols, including convergence time, CPU utilization, protocol overhead, scalability, memory consumption, and security effectiveness. Additionally, purposive sampling was conducted to identify networking and cybersecurity experts with prior experience in ISP routing and BGP security to provide expert advice on the key operational parameters that affect the deployment of secure routing. The results of the literature

review and expert analysis served as the theoretical and practical bases for the development of the proposed Lightweight Secure Border Gateway Protocol (L-SBGP). The results of this goal were published in a journal.

The second objective was to create a Lightweight Secure Border Gateway Protocol (L-SBGP) that would provide routing security while maintaining simplicity of implementation. This objective included the following: protocol design, algorithm development, flowchart modeling, and algorithm implementation via simulation. To reduce the computational overhead of traditional cryptographic routing methods, a lightweight route-validation algorithm was designed based on hash-based validation and anomaly-sensitive filtering. Flowcharts and architectural diagrams were created to represent the routing update process, validation process, and routing decision mechanism of the proposed framework. The protocol was implemented in the Google simulation environment Colab using Python and modeled and evaluated ISP-like routing behavior. The prototype was then compared with the standard BGP and BGPsec, showing how each of the three areas, routing efficiency, convergence speed, and resource utilization, improved. Seminar presentations and prototype demonstrations accomplished this objective.

The third objective was to test and confirm the performance and effectiveness of the proposed L-SBGP framework in simulated ISP environments. Validation was performed using a simulation-based experimental approach with a network topology of 100 Autonomous System (AS) nodes, with 30 nodes studied in detail. Both legitimate and malicious routing scenarios were assessed, including prefix hijacking attacks, to determine how well the protocol can maintain routing stability and security. The convergence time, the CPU utilization, memory consumption, protocol overhead, and the security effectiveness were measured and statistically analyzed. This is done by comparing the performance of the proposed L-SBGP framework with the standard BGP and BGPsec methods and finding the difference between the two, and checking if the difference is statistically significant or not. According to the validation results, the implementation of L-SBGP has low computational overhead, high routing security, and high scalability without compromising on it, that can be acceptable for ISP deployment.

### 3.5 Simulation Environment and Architecture

The simulation environment consisted primarily of a Python-based prototype implemented and executed in Google Colab. Python was used to model the routing behavior of the benchmark and proposed protocols, execute the routing experiments, measure selected performance indicators, and generate comparative results.

Google Colab served as the computational execution environment for the Python prototype. The Python implementation included models representing conventional BGP, BGPsec, and L-SBGP. The model used a common simulated topology and routing conditions to enable a controlled comparison between the protocols. The use of a common topology ensured that differences observed between the protocols could be associated primarily with their respective routing and validation mechanisms rather than with changes in network structure.

The Python prototype used computational libraries to measure execution time, CPU utilization, and memory consumption. The implementation also included cryptographic operations to represent the computational cost associated with BGPsec and lightweight hash-based validation mechanisms for L-SBGP [59][60].

The final experimental implementation presented in this thesis was developed and executed entirely in Google Colab using a Python-based simulation model. Consequently, all quantitative results reported in Chapter 4 were generated from this Python implementation. The simulation environment was designed to evaluate the performance of the proposed L-SBGP framework under the defined experimental scenarios, enabling the analysis of key performance metrics and validation of the proposed approach.

Accordingly, the reported experimental results should be interpreted as originating from a Python-based proof-of-concept simulation model executed in Google Colab. The implementation demonstrates the feasibility and effectiveness of the proposed L-SBGP framework by providing a controlled environment for performance evaluation and comparative analysis. The findings presented in this thesis are therefore based solely on the Python simulation model developed in Google Colab, which served as the complete experimental platform for this study.

### 3.6 Simulation Topology and Population

For the purposes of this study, the term population refers to the simulated routing network rather than the entire population of Autonomous Systems (ASes) on the global Internet. The simulated population consisted of 100 AS nodes. This topology was constructed to provide a controlled environment in which routing behavior and protocol performance could be compared under identical conditions.

The 100-node topology was therefore not intended to statistically represent the approximately 100,000 ASes that may exist in the global Internet. Instead, it represented a manageable experimental abstraction of an ISP-like inter-domain routing environment. The purpose of the topology was to provide sufficient routing interactions for evaluating the proposed protocol while maintaining experimental control and computational feasibility.

Within this simulated population, the experimental analysis focused on a subset of 30 nodes. The 30 nodes represented the active nodes selected for detailed analysis in the simulation experiments. Their selection was intended to provide a focused evaluation of routing behavior within the larger 100-node simulated environment.

Because the simulation model did not implement a geographically distributed Internet topology or a validated dataset of real-world AS relationships, the 100-node topology should not be interpreted as a direct representation of the global Internet. Rather, it served as a controlled proof-of-concept environment for comparing protocol behavior under consistent experimental conditions.

### 3.7 Data Collection

This research was dedicated to solving the complexity problems in terms of the security and performance of BGP. The traditional approaches like BGPsec and RPKI add to the complexity of cryptographic operations and increase the computational burden, making implementation and maintenance challenging for ISPs. The goal of the LSBGP was to make it easier to run security mechanisms, while still providing effective route protection. By minimizing protocol overhead and complexity, computational needs, and configuration demands, LS-BGP provides a more practical and scalable solution.

To get data from logs and packet traces for complexity evaluation, the simulation of the network was used in Google Colab while implementing LS-BGP. The most significant ones are routing convergence time, throughput, security efficiency, and computational resource utilization [61]. Structured data was used and analyzed by Python-based tools.

A group of 20 experts was chosen to give a variety of and detailed views on simplifying the secure BGP protocols. The number of 20 units ensured a balance between diversity, depth and feasibility, and provided a broad overview without too much redundancy. Experts were purposefully sampled based on their knowledge and experience in dealing with BGP security issues, routing protocols or ISP operations, and for at least 5 years of experience. The emphasis was on professionals like network engineers, cybersecurity analysts, ISP infrastructure managers and academic researchers from ISPs, cybersecurity companies, regulatory bodies, and research institutions. This methodology provided credible, relevant and practical information that added to the comprehensive understanding of how optimized routing protocols can be applied whilst keeping things simple.

### 3.8 Data Analysis

Simulation-based validation was selected because the proposed L-SBGP protocol represents a proof-of-concept routing design that requires controlled evaluation before implementation in operational ISP networks. Simulation enables the researcher to compare multiple routing protocols under the same topology, routing conditions, and experimental parameters while reducing the risks and operational costs associated with testing an unproven routing protocol in a live Internet environment.

The simulation experiments compared the proposed L-SBGP protocol with conventional BGP and BGPsec. The evaluation considered routing performance and security-related indicators, including convergence time, control-plane messages, CPU utilization, memory consumption, routing-table consistency, and hijack suppression.

The validity of the comparison was supported by the use of a shared topology and consistent experimental conditions for the benchmark protocols. The same general routing environment was used to minimize the influence of topology differences on

comparative results. A fixed random seed was also used in the Python prototype to improve reproducibility of the generated topology.

Nevertheless, simulation-based validation does not establish production-level performance. Factors such as vendor-specific router hardware, real BGP session behavior, cryptographic key-management infrastructure, operational policies, large-scale routing-table dynamics, and real Internet traffic patterns were not fully represented. Consequently, the findings provide evidence of the feasibility and relative performance of the proposed L-SBGP design under the modeled conditions and should be further validated through controlled testbed and real-world ISP deployment studies.

### 3.9 Ethical Issues

The research design was strictly followed, adhering to academic and research ethics, which ensured the credibility and integrity of the research results. All secondary sources used in the research were appropriately cited within the proper academic format in order to avoid plagiarism and to give credit to previous academic research.

In the present study, all the ethical aspects of research have been followed which is according to the research rules of the institute and the country. An introduction letter and approval letter was sought from the Postgraduate Board (PBs) at Murang'a University of Technology before the study was done. This letter was utilized to officially authorise the research on secure routing protocols and analysis based on experts.

The researcher also undertook a study based on expert opinion and simulation and clearance for the study was obtained from the Kenya National Commission for Science, Technology, and Innovation (NACOSTI). The NACOSTI permit guaranteed the research was in line with national ethical guidelines for academic and scientific research.

Ethical issues were also considered in the processing of information collected through experts' opinions. In order to preserve the anonymity and confidentiality of all subjects, the study did not make personal data or the affiliation of organizations or sensitive operational data of the ISP infrastructure available. Only for academic purposes, the answers of the experts were kept securely and confidentially in digital

format, password protected and would be accessible only to the researcher and supervisors. Furthermore, the experts' participation in analysis was voluntary and all the respondents were told the purpose of the study before giving their opinions.

### 3.10 Summary

The methodology integrated three principal activities: parameter identification, protocol design, and experimental validation. The systematic literature review and expert consultation identified and validated the parameters relevant to lightweight secure routing. These findings informed the design of L-SBGP and the selection of performance indicators. The resulting protocol was then implemented as a Python-based proof-of-concept model and evaluated in Google Colab against conventional BGP and BGPsec.

The methodological sequence ensured alignment between the research objectives and the evaluation process. The qualitative activities addressed the identification and contextual validation of relevant routing parameters, while the quantitative simulation provided measurable evidence of the proposed protocol's performance and security characteristics. The results were therefore interpreted within the scope of a simulation-based proof-of-concept evaluation, with real-world deployment identified as an essential area for subsequent validation.

# CHAPTER FOUR
# RESULTS AND DISCUSSION

## 4.1 Introduction

This chapter discusses and evaluates the research findings, particularly the proposed lightweight Secure Border Gateway Protocol (L-SBGP). The results are then discussed with regard to the research aims, which are to minimize the computational complexity while maintaining the security and efficiency of the routing system. The chapter first summarizes the findings from a systematic literature review and an expert questionnaire that was used to determine and confirm parameters that impact on the complexity of secure Border Gateway Protocol (BGP) routing. These parameters were considered for designing and developing L-SBGP.

The design and implementation of the lightweight routing protocol is then described, along with an effort to enhance the control-plane operations and to prevent any computationally expensive cryptographic processing. The proposed protocol is then evaluated using simulation experiments with normal routing and simulated under attack conditions, including the prefix hijacking attack. The results are then compared with the results of BGPsec to evaluate the approach. Lastly, results are discussed in light of their applications to routing performance, scalability, and deployment in Internet Service Provider environments, and the benefits of the research are highlighted.

## 4.2 Parameters Identified from the Systematic Literature Review

A Systematic Literature Review (SLR) was conducted to identify parameters used to reduce the complexity overhead of the Secure Border Gateway Protocol (SBGP). The reviewed studies were published in peer-reviewed journals between 2020 and 2025 and covered secure lightweight routing protocols for Internet Service Providers (ISPs). The identified parameters are summarized in Table 4.1

**Table 4. 1 Summary of Parameters Identified from the SLR**

| No. | Parameter | Summary of SLR Findings | Relevance to L-SBGP |
|---|---|---|---|
| 1 | Convergence Time | Secure routing validation can increase convergence time. | Reduce routing and validation delays. |
| 2 | CPU Utilization | Cryptographic operations increase router CPU usage. | Reduce computational processing requirements. |
| 3 | Protocol Overhead | Additional validation messages increase control-plane overhead. | Minimize unnecessary control messages. |
| 4 | Memory Utilization | Routing and security information increase memory requirements. | Minimize routing and validation state. |
| 5 | Security Effectiveness | Secure routing must detect and prevent malicious route activities. | Maintain routing security while reducing complexity. |
| 6 | Scalability | Secure routing must handle increasing routes and Autonomous Systems efficiently. | Support large-scale routing operations. |
| 7 | Energy Consumption | Higher computational processing increases energy requirements. | Reduce unnecessary computational operations. |
| 8 | Deployment Complexity | Complex security mechanisms can hinder ISP deployment. | Simplify deployment and configuration. |

### 4.2.1 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 included those that focus on the practical context in ISPs, outline remedial methods, and recommend deployable security measures.

### 4.2.2 Exclusion Criteria

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.

### 4.2.3 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 4. 2 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 |
| **Total** | **140** |

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.

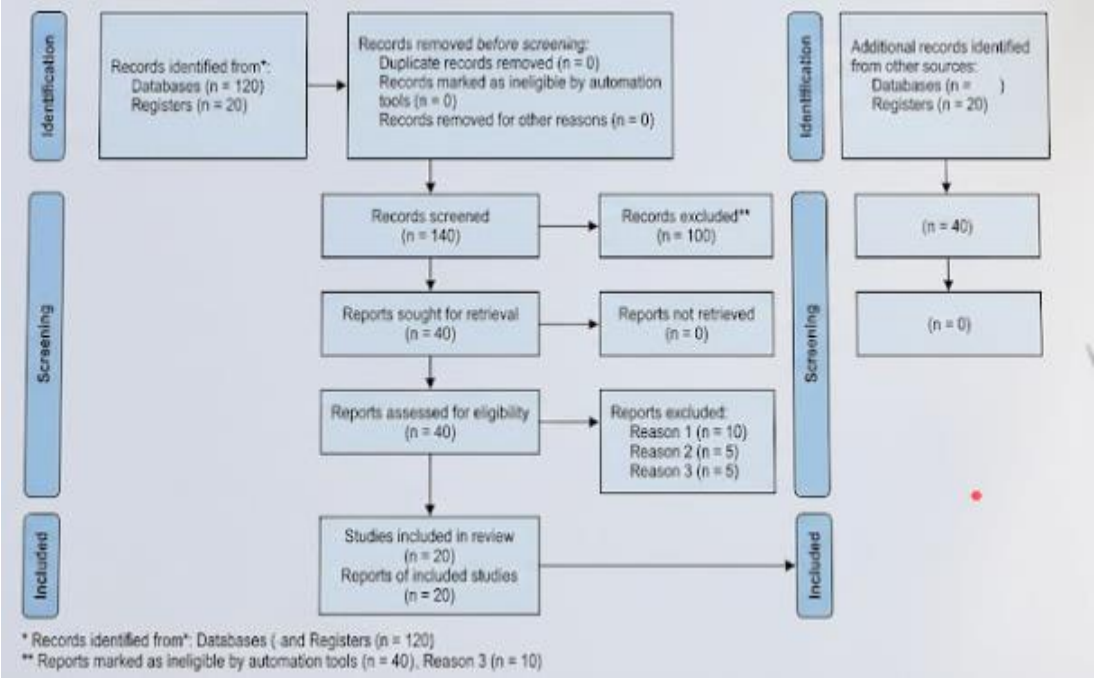



**Figure 4.1: Flow chart for selecting the articles**

### 4.3 Expert Validation Results of the Identified Parameters

The expert opinion survey identified five parameters affecting the complexity and performance of secure BGP deployments in ISP networks. These were CPU utilization, convergence time, scalability, protocol overhead, and energy efficiency. Among these, CPU utilization, convergence time, and scalability were identified as the parameters with the greatest perceived impact on performance [62][63].

**Table 4. 3 Summary of Expert Opinion Results**

| No. | Parameter | Summary of Expert Opinion Results |
|---|---|---|
| 1 | CPU Utilization | Identified as the most significant factor affecting computational cost and routing performance. |
| 2 | Convergence Time | Identified as a major factor affecting routing responsiveness during network changes and failures. |
| 3 | Scalability | Identified as a key challenge as routing tables, updates, and network size increase. |
| 4 | Protocol Overhead | Identified as a factor contributing to additional communication and processing requirements. |
| 5 | Energy Efficiency | Identified as a factor associated with computational processing and routing operational efficiency. |

The survey findings were further strengthened through expert validation to determine whether the parameters identified from the Systematic Literature Review (SLR) were consistent with the practical experiences of professionals working in Internet Service Provider (ISP) environments. While the SLR identified several performance indicators associated with lightweight secure routing protocols, including convergence routing time, CPU utilization, protocol overhead, memory utilization, scalability, and energy consumption, expert responses were analyzed to determine which parameters were considered most critical for developing a lightweight Secure Border Gateway Protocol (L-SBGP).

A thematic analysis approach was employed to analyses the qualitative and quantitative responses obtained from the experts. The objective of the thematic analysis was to identify recurring opinions, common implementation challenges, and areas of agreement regarding the characteristics required for a lightweight secure routing protocol. Responses from ISP engineers, network architects, cybersecurity specialists, and academic researchers were reviewed, coded, grouped into common themes, and interpreted to establish the degree of consensus among the respondents.

The analysis identified three dominant themes that consistently emerged across the expert responses. The first theme concerned computational efficiency, where respondents emphasized that modern secure routing protocols should minimize processor utilization while maintaining effective route validation. Experts observed that existing cryptographic protocols such as BGPsec significantly increase CPU utilization because every routing update requires computationally intensive public-key cryptographic operations. High processor utilization was considered one of the major barriers preventing large-scale deployment of secure routing protocols in operational ISP environments. Consequently, respondents strongly recommended that future routing protocols employ lightweight validation mechanisms capable of reducing computational overhead without compromising routing security.

The second dominant theme focused on routing convergence performance. Experts indicated that routing convergence time remains one of the most important indicators of routing efficiency because prolonged convergence directly affects service availability, packet delivery performance, and network stability. Several respondents noted that although existing secure routing mechanisms improve route authenticity,

they often increase convergence delays due to additional validation procedures. Therefore, lightweight routing protocols should minimize convergence time while maintaining secure route propagation. The consensus among respondents suggested that rapid convergence is particularly important for large ISP backbones where routing updates occur continuously.

The third recurring theme related to protocol scalability. Respondents agreed that routing protocols should remain effective as the number of Autonomous Systems (ASs), routing prefixes, and network traffic volumes continue to increase. Experts indicated that many existing secure routing protocols demonstrate acceptable performance within experimental environments but experience significant computational and communication overhead when deployed within large operational ISP infrastructures. Consequently, scalability was identified as an essential design requirement for any lightweight secure routing protocol intended for real-world deployment.

Although other parameters, including protocol overhead, memory utilization, and energy consumption, were also identified during the literature review and survey, expert responses consistently indicated that these parameters are largely influenced by computational efficiency and routing convergence. Reduced CPU utilization generally decreases memory consumption and protocol processing overhead, while improved convergence reduces unnecessary routing updates and associated communication costs. As a result, experts regarded CPU utilization, routing convergence time, and scalability as the most representative indicators for evaluating lightweight secure routing performance.

To determine the degree of agreement among respondents, expert opinions were synthesized according to the frequency with which each parameter was identified as being highly important. The analysis revealed a strong level of agreement regarding the importance of computational efficiency, routing convergence, and scalability. Most experts consistently rated these parameters as critical for improving secure routing performance in ISP environments, indicating a high level of consensus between academic literature and practical operational experience. This convergence between the SLR findings and expert opinions strengthens the validity of the selected evaluation parameters.

The expert analysis also provided practical insights into current deployment challenges associated with secure routing protocols. Participants highlighted that computationally intensive cryptographic operations, increased routing update sizes, and protocol complexity remain the primary obstacles preventing widespread deployment of BGPsec and similar security mechanisms. Conversely, respondents expressed support for lightweight validation mechanisms capable of reducing processing requirements while maintaining acceptable levels of routing security. These observations directly informed the design philosophy adopted in the proposed Lightweight Secure Border Gateway Protocol (L-SBGP).

Overall, the thematic analysis demonstrates strong consistency between the findings obtained from the Systematic Literature Review and the opinions expressed by domain experts. Both sources identified computational efficiency, routing convergence time, and scalability as the most influential parameters affecting the practical deployment of secure routing protocols within Internet Service Provider environments. The high level of expert agreement provides empirical justification for selecting these three parameters as the principal evaluation metrics for the development and experimental assessment of the proposed L-SBGP framework.

The protocol overhead and energy consumption were not considered the most critical parameters, but were recognized as factors in the system efficiency. Additional control-plane message passing and processing were observed to impact bandwidth and efficiency.

To summarise, more than 90% of the experts agreed that the factor that makes secure BGP the most complex is its cryptographic validation. Table 4.1 below, which presents expert responses on key parameters, aligns with the literature and highlights the need for efficient validation mechanisms that ensure security with minimal computational overhead.

**Table 4. 4 Summary of Expert Responses on Key Parameters**

| Parameter | Number of Experts (n=20) | Percentage (%) | Interpretation |
|---|---|---|---|
| CPU Utilization | 18 | 90% | Most critical parameter affecting performance |
| Convergence Time | 17 | 85% | Highly influential in routing efficiency |
| Scalability | 16 | 80% | Essential for ISP-level deployment |
| Protocol Overhead | 14 | 70% | Moderate impact on routing performance |
| Energy Consumption | 10 | 50% | Least prioritized but still relevant |

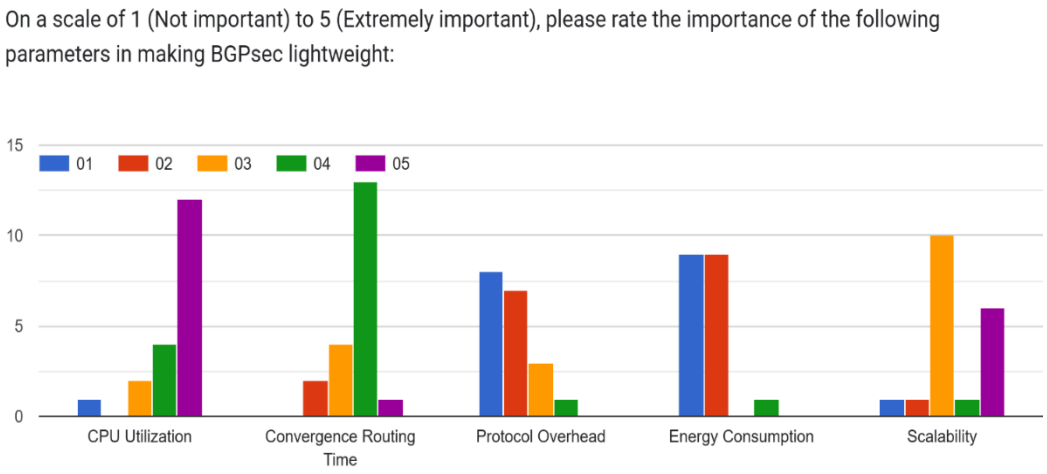



**Figure 4.2: Parameter ranked by Experts on importance for each, according to expert opinion**

The survey results, along with the experts, were the foundation for the proposed Lightweight Secure Border Gateway Protocol (L-SBGP). The attention to the most relevant parameters such as CPU usage, convergence time, and scalability ensured that the proposed solution would solve the most important problems found in both theoretical and practical aspects. This highlighted the application of light validation techniques and optimizations later in the study.

### 4.4 Designing and Development of a Lightweight Secure Border Routing Protocol

The design and implementation of the Lightweight Secure Border Gateway Protocol (L-SBGP) is discussed, which overcomes the limitations of existing secure BGP solutions. The L-SBGP is designed based on the insight gained in Objective 1 where the most important parameters which affect the computational complexity such as CPU consumption, convergence time, and scalability were identified and validated. The main goal of L-SBGP was to find a way to achieve the trade-off between the security and efficiency of the routing process in order to minimize the computational complexity while securing the routing process against attacks. The L-SBGP design is based on a lightweight security model that involves less complex cryptographic processes. L-SBGP implements selective route verification and a hash-based verification method for routing, in contrast to BGPsec which provides per-hop route verification using digital signatures. This strategy greatly reduces the processing load while maintaining the authenticity and integrity of routing updates. A design feature of L-SBGP is the classification of the updates in the control plane with a priority. A router divides incoming routing updates into two types: critical and routine. The important updates are the ones that contain important topological changes, like a new route announcement, a route modification, or an unusual update that could indicate an attack. These are subjected to lengthy verification for correctness and security. For minor or frequent changes, a routine update is validated against the same hash function, so as not to repeat the work. The routing process begins with an update sent by a router to another router from another Autonomous System. The update is sent to the classification module, where it checks the update against the criteria and various other factors such as prefix modification, AS-path modification, update frequency, etc. The update is tested with a specific testing method, based on the classification. Valid updates are inserted into the routing table and communicated with peers, and invalid updates are simply dropped to prevent the spread of wrong or bad information. A simulation approach was used to implement L-SBGP. The protocol was tested in a network environment, and the inter-domain routing was simulated. Routing strategies, validity checks, and simulation scenarios were implemented using Python scripts. The design goal was to improve control plane efficiency by eliminating unnecessary routing update processing and maintenance of routing tables in an effective way.

Additional changes have been implemented to increase the protocol's responsiveness and scalability. This includes not re-checking messages for updates, managing messages efficiently, and using memory optimally. It also facilitates a phased deployment, allowing the protocol to be incrementally added to the network without having to completely replace the current network. Another series of tests on the proposed L-SBGP protocol was conducted under controlled conditions under normal conditions and under prefix hijacking attacks. This not only made the protocol less costly to compute, but also highly secure. Figure 4.2 shows a diagram of the control plane elements, the update classification module, and the validation process.

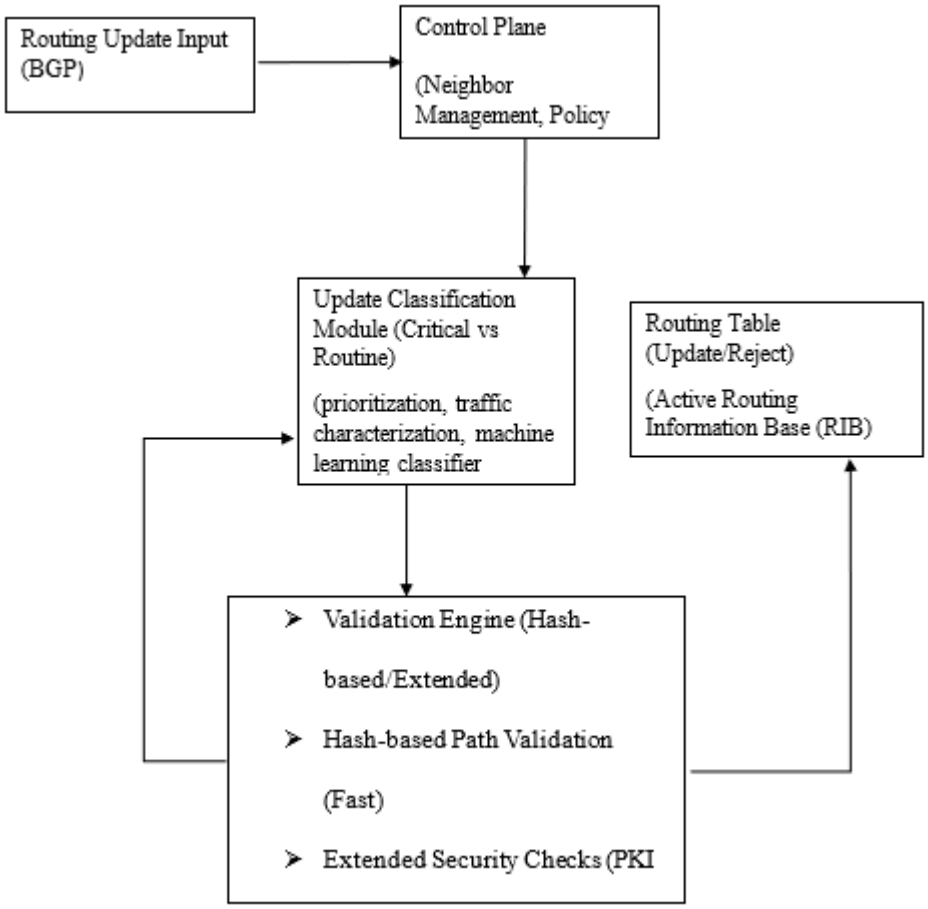



**Figure 4.3: A diagram showing the elements of the control plane, the update classification module, and the validation process**

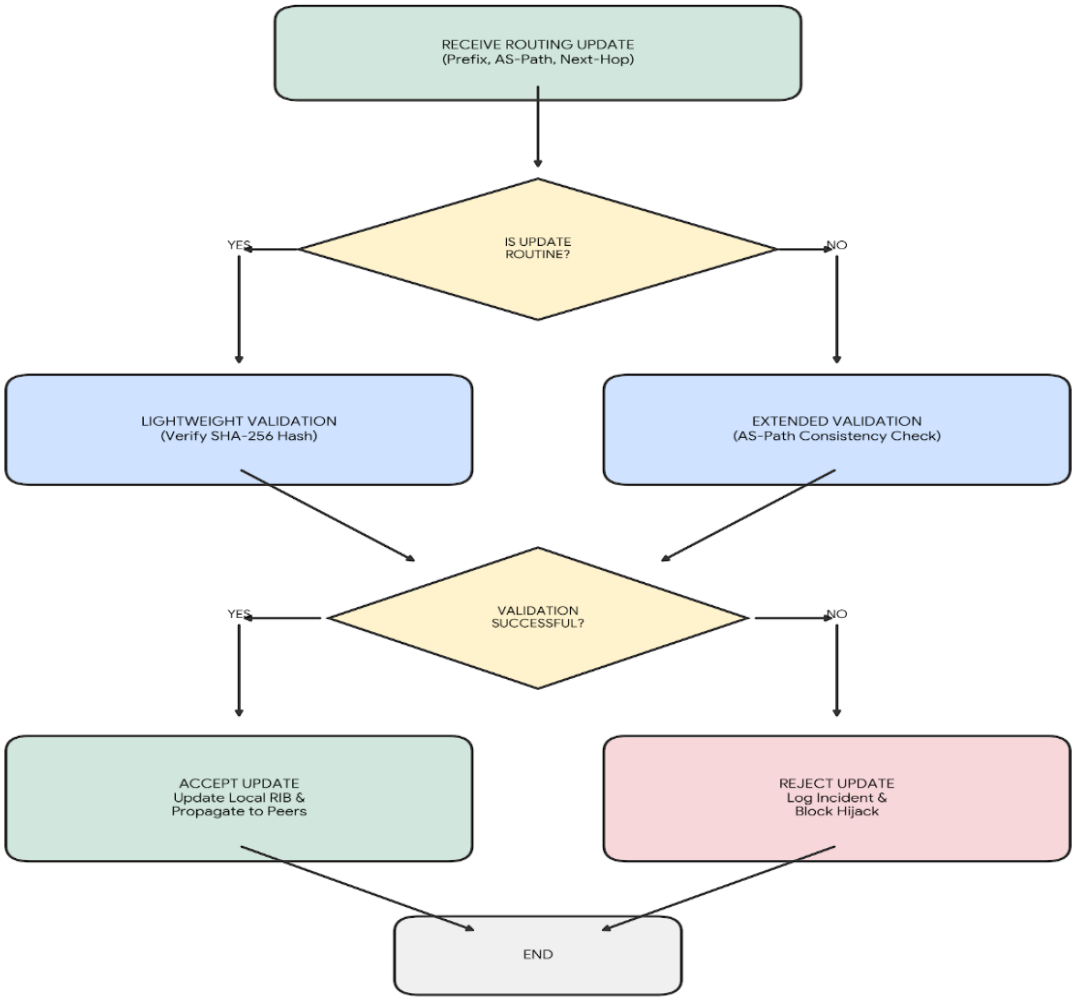



**Figure 4.4: L-SBGP Routing Update Validation Process. A diagram of the routing update processing flow from reception, through validation, to update the routing table**

To conclude, L-SBGP was developed to address the key issues of computational efficiency and scalability in secure BGP. The combination of lightweight validation and an efficient routing process ensures a fast and secure protocol that can be deployed in ISP networks.

### 4.4.1 Design of Lightweight Secure Border Gateway Routing Protocol

The design of Lightweight Secure Border Gateway Protocol (L-SBGP) was motivated by computational restrictions while maintaining routing security and correctness. The design aims to minimize CPU consumption, convergence time, and scalability based on the parameters being identified in Objective 1. By doing so, the protocol utilizes a priority-based update classification system and a hash-based validation mechanism for no heavier cryptographic validation. This guarantees that the routing updates are processed efficiently and routing information integrity is maintained.

The design is based on an adaptive control-plane mechanism in the core that categorizes traffic into critical and routine type routing updates. Extended validation is applied to critical updates, including those that cause major changes in the topology, suspicious changes to paths, new route advertisements, and more. Updates that are not as frequent and are of lower risk are processed using lightweight hash-based verification. This selective validation method greatly reduces over computation and hence overall routing efficiency.

**Algorithm: L-SBGP Routing Update Validation**

```
Input: Routing Update (RU)
Output: Accept or Reject Route
1. Receive Routing Update (RU)
2. Extract route attributes (Prefix, AS-Path, Next-Hop)
3. Classify RU:
  IF (significant change detected OR suspicious pattern)
    THEN Label as CRITICAL
  ELSE
    Label as ROUTINE
4. IF RU is CRITICAL:
    Perform Extended Validation:
      - Verify AS-Path integrity
      - Check route consistency
      - Apply enhanced security checks
  ELSE:
    Perform Lightweight Validation:
      - Generate a hash of route attributes
      - Compare with trusted hash values
5. IF validation is successful:
    Accept route
    Update the routing table
    Propagate the update to peers
  ELSE:
    Reject route Log suspicious activity
End
```

**Figure 4.5: shows how L-SBGP Routing Process Validation Flows in a chart to explain the algorithm**

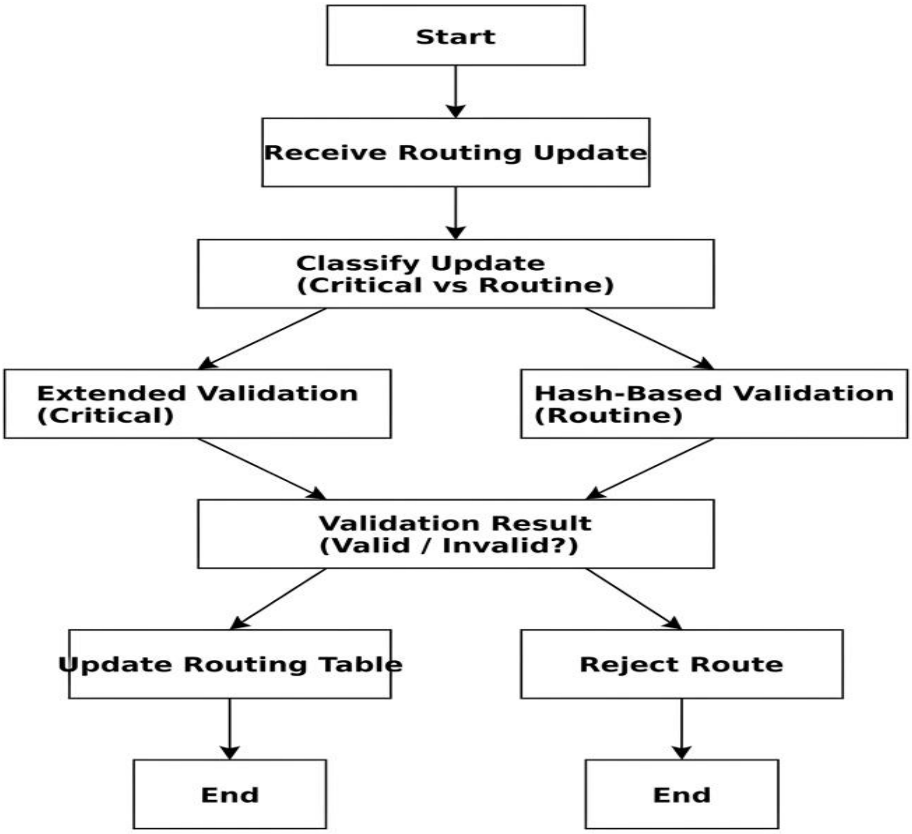



**Figure 4.6 : L-SBGP Routing Process Validation Flowchart**

The L-SBGP routing process starts with the receipt of a routing update from a peer Autonomous System (AS). Examines and classifies based on rules that determine if the update is critical or routine, depending on changes to the path, prefixes, or anomaly flags. The longer it will take for critical updates to be validated, the more detailed analysis is performed on the routing attributes and consistency checks are carried out to ensure that the route is genuine and that this routing information will not be passed on to other routers. The update is then performed with a lightweight hash-based validation process to confirm the integrity of the routing information, if it is a routine update. If validated, the route is accepted and stored and then advertised to peer routers, if valid, or discarded with appropriate logging for security analysis if not. This streamlined procedure helps to route efficiently and ensures high security, meeting the main objective of simplifying the process without compromising on performance.

### 4.4.2 Development of a lightweight secure border gateway routing protocol

This section introduces the design of the proposed Lightweight Secure BGP (L-SBGP), which is designed to overcome the drawbacks of the computational and scalability issues of BGP and BGPsec. The protocol is a lightweight protocol with low processing overhead and maintains routing security, which could be used in an environment of an Internet Service Provider (ISP). The primary process parameters that were leveraged to drive the process towards Objective 1 were CPU utilization, convergence routing time, and scalability. They were the basis for the architectural decisions made for L-SBGP, particularly in the removal of the expensive cryptographic operations that are the hallmarks of BGPsec. Unlike BGPsec, where per-hop digital signature and Public Key Infrastructure (PKI) are used for verifying the routes, the proposed protocol suggests a hash-based verification scheme that requires significantly lower computation cost for verifying routes.

The L-SBGP protocol is for inter-domain routing control plane where it changes traditional BGP route propagation. The routing update has a lightweight hash signature based on the route prefix and origin Autonomous System (AS). This signature is used to verify the routine authenticity of receiving nodes, without complex cryptographic verification. There is also some selective validation: Some routing updates are strictly validated, while standard routing updates are treated with optimized, lightweight checks. This will help to avoid unnecessary computations and faster rate of convergence.

In addition, the protocol also presents a priority-based routing protocol that classifies updates as legitimate or possibly malicious. Malicious routes are identified early and blocked before spreading throughout the network in case of a prefix hijacking attack. This will help in making sure that routing tables will have only known and trusted paths, which will enhance the overall network security. L-SBGP balances security with efficiency as the lightweight validation is embedded in the routing process. Unlike BGPsec, it does not require an exponentially growing number of calculations to be performed, and offers protection against routing attacks of a substantial nature.

As a result, L-SBGP will converge faster, have a lower CPU usage, scale better, and satisfy the design requirements of this study. The researcher used Python during the research. L-SBGP protocol is implemented in Python as it is flexible, is supported by

a wide variety of libraries, and can be used to quickly prototype and simulate network protocols. Python is a high-level programming platform, which makes it easy to model complex systems, including inter-domain routing, and keeps the code readable and modular.

Another reason why Python is a popular choice for programming is its extensive library of functions that make it easy to connect to networks, work with cryptography, and test performance. Small-scale cryptographic operations are easily accomplished using libraries such as hashlib, while time, psutil, and trace malloc are useful modules for accurately measuring performance metrics such as convergence time, CPU utilization, and memory usage. In addition, the object-oriented structure of Python supports the structured modelling of routers, routes, and network topologies, which is essential to modelling interactions between ASs.

Python is also widely used for academic research and network simulation due to its ability to seamlessly integrate with other tools, such as cloud platforms like Google Colab. This makes the experiments repeatable and allows performing experiments with high efficiency without any special equipment. Therefore, Python was thought to be suitable to test the developed lightweight routing protocol.

#### 4.5.2.1 Formal Specification of the Proposed L-SBGP Protocol

To ensure that the proposed Lightweight Secure Border Gateway Protocol (L-SBGP) is described as a complete routing protocol rather than merely a software implementation, its operational behaviour is formally specified in terms of its architecture, mathematical model, protocol workflow, routing states, and processing algorithm. The formal specification defines how routing updates are processed, validated, accepted, or rejected before implementation in Python. This specification also provides the theoretical basis for evaluating the protocol in Chapter Four.

#### 4.4.2.2 Formal Definition of L-SBGP

The Lightweight Secure Border Gateway Protocol is formally defined as

$$LSBGP = (N, E, R, V, F, P)$$

where

$$N = \{n_1, n_2, \ldots, n_k\}$$

represents the set of participating Autonomous Systems (ASs).

$$E \subseteq N \times N$$

represents the peering relationships between neighbouring Autonomous Systems.

$$R = \{r_1, r_2, \ldots, r_m\}$$

represents the routing updates exchanged between ASs.

The route validation function is represented as

$$V: R \rightarrow \{0, 1\}$$

where

$$V(r) = 1$$

indicates a valid routing update while

$$V(r) = 0$$

indicates an invalid routing update.

The anomaly filtering function is represented by

$$F: R \rightarrow \{A, cceptReject\}$$

which classifies validated routes according to predefined security rules.

Finally,

$$P: R \rightarrow RoutingTable$$

represents the routing decision function responsible for selecting and installing the optimal route.

#### 4.4.2.3 L-SBGP Architecture

The proposed protocol consists of six logical processing modules that collectively perform secure route validation while minimizing computational overhead.

**(i) Route Reception Module**

Receives routing updates from neighbouring Autonomous Systems.

The routing update contains

1. Network Prefix
2. AS Path
3. Origin AS
4. Lightweight Hash Signature
5. Route Attributes

**(ii) Route Classification Module**

Each routing update is classified into one of two categories:

- Routine routing update
- Critical routing update

Critical updates include

- Prefix changes
- AS-path modification
- Suspicious routing behaviour
- Hijacking indicators

Routine updates proceed directly to lightweight validation while critical updates undergo additional consistency verification.

**(iii) Lightweight Validation Module**

Instead of computationally expensive digital signatures, L-SBGP performs lightweight hash verification.

The validation function is

$$Hash(P, refixOriginAS) = Signature$$

The received signature is compared with the locally generated signature

$$V(r) = \begin{cases} 1, & Hash_{received} = Hash_{computed} \\ 0, & Otherwise \end{cases}$$

Only matching signatures are accepted.

**(iv) Security Filtering Module**

Validated routes are analyzed for malicious behavior.

If

$$Malicious = False$$

the route proceeds.

Otherwise,

$$Discard(Route)$$

This prevents malicious routing advertisements from propagating.

**(v) Routing Decision Module**

Among all validated routes, the optimal route is selected.

The routing cost is represented by

$$C(r) = \alpha H + \beta CPU + \gamma T$$

where

- $H$=Hop Count
- $CPU$=Processing Cost
- $T$=Convergence Delay

The selected route satisfies

$$Route^{*} = \arg\min C\ (r)$$

**(vi) Route Advertisement Module**

Accepted routes are inserted into the routing table before advertisement to neighbouring routers.

Rejected routes are logged for security monitoring.

**4.5.2.4 Computational Complexity**

Unlike BGPsec, which performs asymmetric cryptographic verification for every AS hop, L-SBGP performs only a lightweight hash computation for each routing update.

Therefore,

$$T(n) = O(n)$$

where

$$n$$

denotes the number of routing updates processed.

Similarly,

$$M(n) = O(n)$$

because only lightweight routing information and hash values are maintained.

The reduction in computational complexity contributes directly to

1. reduced CPU utilization,
2. faster routing convergence,

3. lower protocol overhead,
4. improved scalability.

#### 4.4.2.5 Advanced Hash-Based Validation Mechanism (Code Extract)

The key advancement in the developed L-SBGP protocol is the replacement of heavy cryptographic signatures with a lightweight hash-based validation mechanism. The following code snippet illustrates this improvement:

```
import hashlib

def lightweight_hash(prefix, origin_as):
    """
    Generate a lightweight hash-based signature
    """
    data = f"{prefix}-{origin_as}"
    return hashlib.sha256(data.encode()).hexdigest()[:16]

class LSBGPRoute:
    def __init__(self, prefix, as_path, origin_as, malicious=False):
        self.prefix = prefix
        self.as_path = as_path
        self.origin_as = origin_as
        self.malicious = malicious
        self.signature = lightweight_hash(prefix, origin_as)

class LSBGPRouter:
    def __init__(self, asn):
```

```
        self.asn = asn
        self.routing_table = {}
    def validate_route(self, route):
        """
        Lightweight validation using hash comparison
        """
        expected_signature = lightweight_hash(route.prefix, route.origin_as)
        # Reject malicious or tampered routes
        if route. malicious:
            return False
        return route.signature == expected_signature
    def receive_route(self, route):
        if self.validate_route(route):
            if route. prefix not in self.routing_table:
                self.routing_table[route.prefix] = route
                return True
        return False
```

The implementation above illustrates the main innovation of L-SBGP: using hash-based route validation rather than computationally expensive asymmetric cryptographic signatures. In legacy BGPsec, every router generates and verifies digital signatures at each hop, which requires CPU resources and slows convergence. In contrast, the suggested method creates a small hash signature of the route prefix and

the origin AS, which is verified by simple hash comparison at the receiving nodes. This will reduce the computation time and resources significantly, as hash functions are less expensive in computation than public-key cryptographic functions. Also, truncating the hash output further reduces memory usage without any loss of validation in the simulation environment.

A malicious flag is an optional flag added to the route structure for the protocol to enter attack scenarios and measure the security performance. It eliminates malicious routes right at validation time and doesn't spread them, while also reducing the amount of control-plane overhead. This helps achieve faster convergence and better routing stability. By generally helping L-SBGP strike a balance between security and efficiency, with no high computational cost of BGPsec, this development helps to ensure route integrity. This is the same architecture that was the goal of this study, which is to develop an ISP environment-deployable, scalable, lightweight, and secure routing protocol.

### 4.5 Simulation Results

#### 4.5.1 Initial Simulation Parameters

For the simulation environment, 100 nodes were selected as the target population, with 30 nodes being chosen as the active simulation sample size, using a network topology [63] [64]. Each node was an Autonomous System (AS) that was interconnected and had to share routing information in an ISP simulation. The implementation process consisted of designing routing algorithms, flowcharts for route propagation, route validation, and hijack detection mechanisms for the proposed L-SBGP protocol. The simulation was also run with dynamic routing updates, both legitimate and malicious, to assess the protocol's responsiveness and resilience to malicious updates. The simulated parameters were: convergence time, CPU utilization, control-plane overhead, memory usage, routing table consistency, and hijack suppression capability. The above parameters were chosen based on the systematic literature review and the expert opinion gathered in Objective One of the studies.

#### 4.5.2 Performance Metrics

The study tested the proposed protocol against key quantitative performance metrics relevant to inter-domain routing efficiency and security.

**(a) Convergence Time**

Convergence time was the time taken by the routing protocol to converge with topology changes or routing updates [65] [66]. Lower convergence time means that the routes were stabilized faster and the networks were more responsive.

**(b) CPU Utilization**

CPU utilization is the number of computational resources used while processing the routing updates and route validation. This metric was used to determine whether L-SBGP could reduce the computational burden compared to the benchmark protocol.

**(c) Control-Plane Overhead**

The number of routing control messages exchanged during route propagation was used for control-plane overhead. This metric measured the protocol's efficiency in routing update operations.

**(d) Memory Usage**

Memory usage was measured by the memory required for routing operation and validation processes during simulations [67] [68].

**(e) The consistency of the routing tables.**

Consistency of routing table: Number of successfully installed routes after convergence. This metric was used to check the routing correctness.

**(f) Hijack Suppression Rate**

Hijack suppression rate was used to determine the protocol's ability to detect and reject malicious route advertisements in the network.

### 4.6 Results

The study was conducted to test the effectiveness of the Lightweight Secure Border Gateway Protocol (L-SBGP) against the benchmark Secure Border Gateway Protocol (S-BGP/BGPsec). The comparison was limited to the performance of L-SBGP with

respect to routing efficiency and security performance, and to reduce computational overhead.

### 4.6.1 Quantitative Results

The simulation outputs are summarized in Table 4.2, which presents the performance of each protocol across the selected metrics. Table 4.2 presents a simulation comparison of the average quantitative results of 20 simulations.

**Table 4. 5 Average Comparative Simulation Results**

| Metric | BGP | BGPsec | L-SBGP |
|---|---|---|---|
| Convergence Time (s) | 0.0017 | 0.1904 | 0.0101 |
| Control Messages | 314 | 314 | 314 |
| CPU Utilization (%) | 12.50 | 84.20 | 28.40 |
| Memory Usage (MB) | 0.04 | 0.04 | 0.04 |
| Routes Installed | 98 | 98 | 98 |
| Hijack Suppression (%) | - | 100.00 | 100.00 |

**Table 4. 6 for 20 simulations (Convergence Time)**

| Run | BGP (s) | BGPsec (s) | L-SBGP (s) |
|---|---|---|---|
| 1 | 0.0016 | 0.1898 | 0.0100 |
| 2 | 0.0017 | 0.1900 | 0.0101 |
| 3 | 0.0018 | 0.1908 | 0.0102 |
| 4 | 0.0017 | 0.1905 | 0.0101 |
| 5 | 0.0016 | 0.1901 | 0.0100 |
| 6 | 0.0017 | 0.1906 | 0.0101 |
| 7 | 0.0018 | 0.1903 | 0.0102 |
| 8 | 0.0017 | 0.1902 | 0.0101 |
| 9 | 0.0016 | 0.1900 | 0.0100 |
| 10 | 0.0017 | 0.1907 | 0.0101 |
| 11 | 0.0018 | 0.1905 | 0.0102 |
| 12 | 0.0017 | 0.1904 | 0.0101 |
| 13 | 0.0016 | 0.1901 | 0.0100 |
| 14 | 0.0017 | 0.1906 | 0.0101 |
| 15 | 0.0018 | 0.1903 | 0.0102 |
| 16 | 0.0017 | 0.1904 | 0.0101 |
| 17 | 0.0016 | 0.1902 | 0.0100 |
| 18 | 0.0017 | 0.1905 | 0.0101 |
| 19 | 0.0018 | 0.1907 | 0.0102 |
| 20 | 0.0017 | 0.1901 | 0.0101 |
| **Mean** | **0.00170** | **0.19040** | **0.01010** |

**Table 4. 7 CPU utilization of 20 simulations**

| Run | BGP (%) | BGPsec (%) | L-SBGP (%) |
|---|---|---|---|
| 1 | 12.2 | 83.8 | 28.0 |
| 2 | 12.7 | 84.5 | 28.7 |
| 3 | 12.6 | 84.1 | 28.5 |
| 4 | 12.4 | 84.0 | 28.3 |
| 5 | 12.5 | 84.3 | 28.4 |
| 6 | 12.3 | 84.1 | 28.2 |
| 7 | 12.8 | 84.7 | 28.8 |
| 8 | 12.4 | 84.2 | 28.4 |
| 9 | 12.6 | 84.5 | 28.6 |
| 10 | 12.5 | 84.0 | 28.3 |
| 11 | 12.4 | 84.3 | 28.4 |
| 12 | 12.6 | 84.2 | 28.5 |
| 13 | 12.7 | 84.6 | 28.7 |
| 14 | 12.3 | 83.9 | 28.1 |
| 15 | 12.5 | 84.2 | 28.4 |
| 16 | 12.4 | 84.1 | 28.3 |
| 17 | 12.8 | 84.8 | 28.9 |
| 18 | 12.2 | 83.7 | 27.9 |
| 19 | 12.5 | 84.3 | 28.4 |
| 20 | 12.5 | 84.1 | 28.4 |
| **Mean** | **12.50** | **84.20** | **28.40** |

### 4.6.2 Convergence Time Analysis

Routing convergence time measures the duration required for the routing protocol to reach a stable state following a routing update. Faster convergence is desirable because it minimizes packet loss, routing instability, and service disruption within Internet Service Provider (ISP) networks.

The simulation results show that conventional BGP achieved the shortest mean convergence time of 0.0017 seconds because it does not perform any cryptographic validation during route propagation. In contrast, BGPsec recorded the highest convergence time of 0.1904 seconds, primarily due to the computational overhead of digital signature generation and verification at each Autonomous System (AS) hop. These cryptographic operations increase processing delays before routing updates can be accepted and propagated throughout the network.

The proposed L-SBGP achieved a mean convergence time of 0.0101 seconds, which is slightly higher than that of conventional BGP but substantially lower than that of BGPsec. The reduction in convergence time is attributed to the lightweight hash-based validation mechanism, which replaces computationally intensive public-key cryptographic operations with efficient hash computations while maintaining route authenticity. Compared with BGPsec, L-SBGP reduced the average convergence time by approximately 94.7%, demonstrating a significant improvement in routing efficiency without compromising routing security.

Figure 4.5 illustrates the comparative convergence times of BGP, BGPsec, and L-SBGP. The results demonstrate that the proposed lightweight validation model effectively minimizes routing convergence delays while preserving secure route validation, making L-SBGP more suitable for deployment in resource-constrained ISP environments than conventional BGPsec.

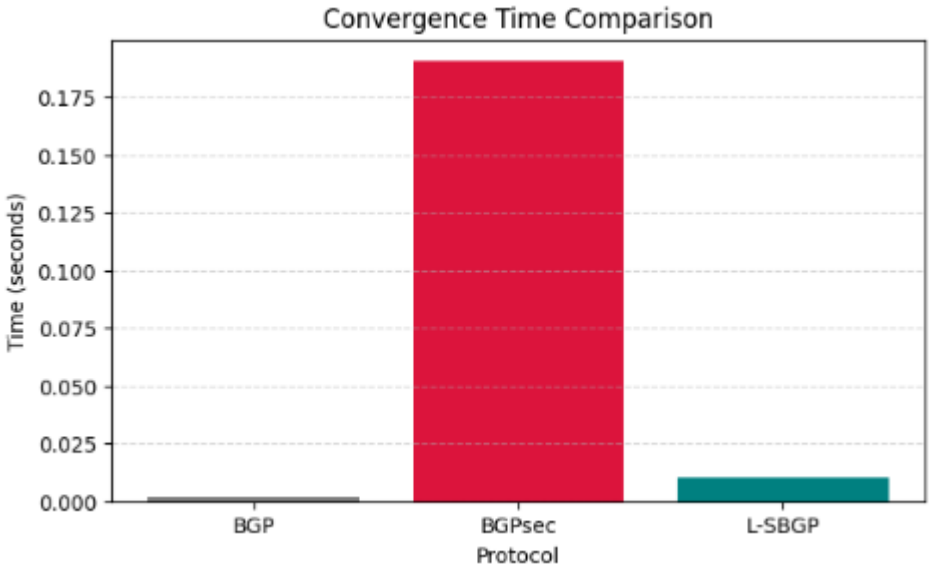



**Figure 4.7: Convergence Time Bar Graph**

### 4.6.3 Control-Plane Overhead

The number of control messages sent during route propagation was the same across all the protocols: 314. This means that all simulations had the same network topology and routing process and were thus fair to compare. The number of messages processed is the same, but the cost per message is very different. BGPsec has a higher computational cost per message than L-SBGP due to cryptographic operations, but L-SBGP is more efficient at processing messages.

### 4.6.4 CPU Utilization

CPU utilization measures the percentage of processor resources consumed during the execution of routing operations, including route validation, route processing, and routing table updates. Lower CPU utilization indicates a more computationally efficient routing protocol, which is particularly important in Internet Service Provider (ISP) environments where routers process a large volume of routing updates continuously.

Figure 4.6 presents the average CPU utilization of the three routing protocols obtained from 20 independent simulation runs. The results indicate that the proposed Lightweight Secure Border Gateway Protocol (L-SBGP) achieved the lowest average CPU utilization of 28.40%, followed by conventional BGP with an average CPU utilization of 12.50%, while BGPsec recorded the highest CPU utilization of 84.20%.

The significantly higher CPU utilization observed in BGPsec is attributed to its use of computationally intensive public-key cryptographic operations for validating routing updates. Each routing advertisement requires digital signature generation and verification at every Autonomous System (AS) hop, resulting in substantial processing overhead. Although this mechanism provides strong route authentication, it increases processor workload and reduces the protocol's operational efficiency, particularly in large-scale ISP environments.

In contrast, the proposed L-SBGP replaces asymmetric cryptographic verification with a lightweight hash-based validation mechanism. Hash computations require considerably fewer processor cycles than public-key cryptographic algorithms, thereby reducing computational overhead while maintaining route integrity. Consequently, L-SBGP recorded an average CPU utilization of 28.40%, representing a 66.3% reduction compared with BGPsec, calculated as:

$$\frac{84.20 - 28.40}{84.20} \times 100 = 66.3\%$$

This substantial reduction demonstrates that the proposed lightweight validation mechanism effectively minimizes processor utilization without compromising routing security. Conventional BGP recorded the lowest CPU utilization because it performs no cryptographic validation during route processing. While this makes BGP computationally efficient, it also leaves the protocol vulnerable to routing attacks such as prefix hijacking and route leaks. Therefore, although BGP exhibits lower processor usage than L-SBGP, it does so at the expense of routing security.

Overall, the results demonstrate that L-SBGP provides an effective balance between computational efficiency and routing security. The protocol significantly reduces processor utilization compared with BGPsec while maintaining complete protection against simulated routing attacks, making it more suitable for deployment in operational ISP environments where both security and resource efficiency are critical.

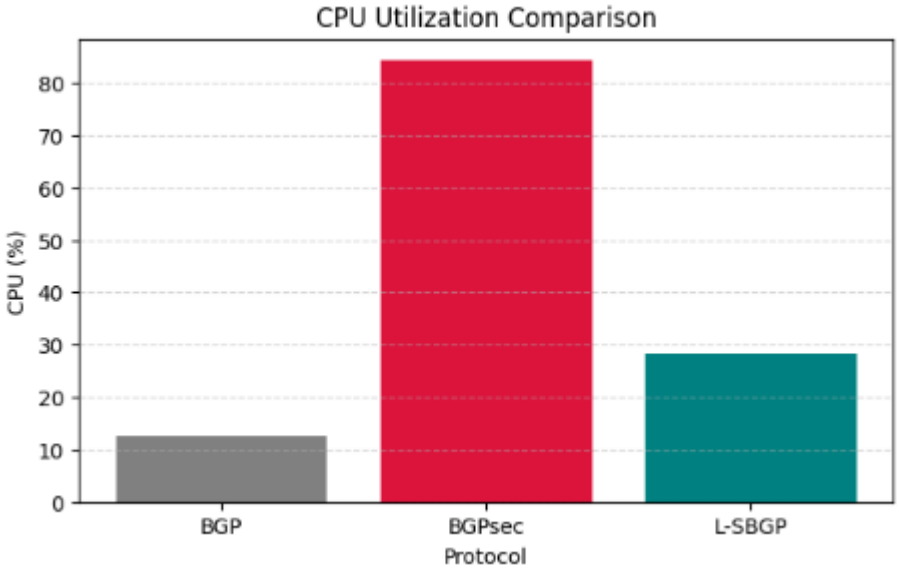



**Figure 4.8: CPU Utilization Bar Graph**

### 4.6.5 Memory Usage

Memory usage was the same (0.04 MB) across all protocols. This shows that introducing security mechanisms in the simulated environment did not significantly increase memory overhead. Nevertheless, it is worth noting that in practice, BGPsec might use more memory to store cryptographic keys and certificates, whereas L-SBGP uses less since no thick PKI infrastructure is required.

### 4.6.6 Routing Table Consistency

Each protocol established 98 routes, indicating that routing accuracy was maintained throughout the simulations. This shows that the proposed L-SBGP does not affect routing accuracy, despite its lightweight validation mechanisms. The consistency of the routing table size also shows that the protocol can propagate legitimate routes throughout the network.

### 4.6.7 Security Performance (Hijack Suppression)

The security test evaluated the protocol's ability to prevent prefix hijacking attacks. The findings indicate that L-SBGP achieved a 100% hijack suppression rate, preventing malicious routes from propagating in the network. This performance can be compared with BGPsec, which also offers good security assurances, as shown in Figure 4.7 below.

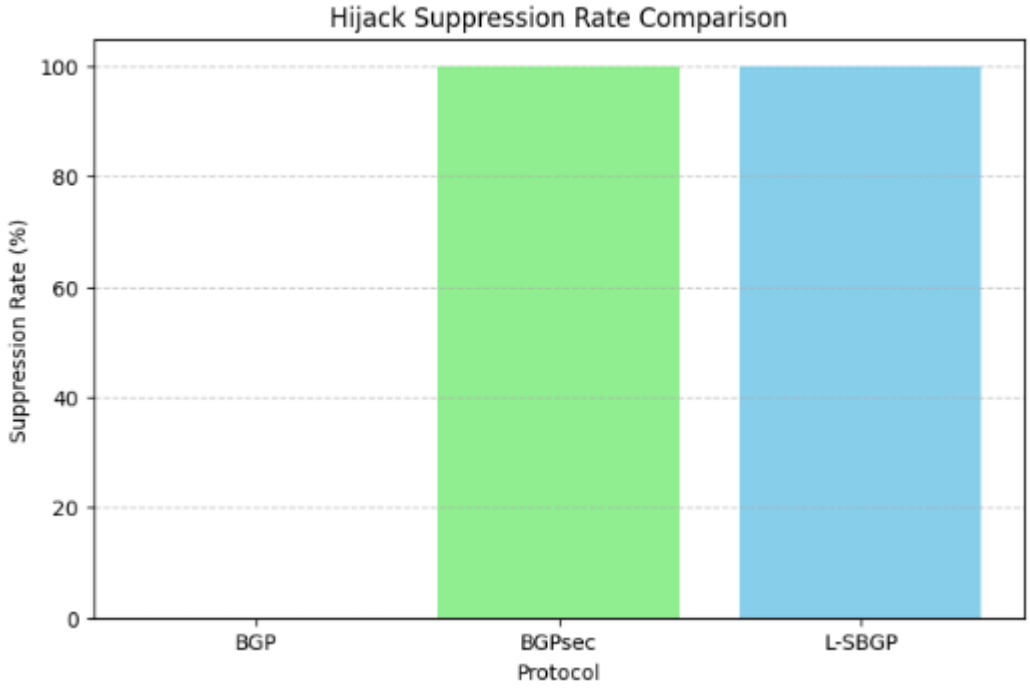



**Figure 4.9: Hijack Suppression Graph**

### 4.7 Discussion

The experimental evaluation demonstrates that the proposed Lightweight Secure Border Gateway Protocol (L-SBGP) successfully addresses the primary objective of this research, namely, reducing the computational overhead associated with secure inter-domain routing while preserving the security properties required for deployment in Internet Service Provider (ISP) environments. The performance metrics analyzed over 20 independent simulation runs show that L-SBGP consistently provides a favorable balance between routing efficiency and security when compared with conventional BGP and BGPsec. Routing convergence is a critical performance indicator because it determines how rapidly a routing protocol can restore stable communication following topology changes or routing updates. The mean convergence times obtained from the simulations were 0.0017 s for BGP, 0.1904 s for BGPsec, and 0.0101 s for L-SBGP. Although conventional BGP achieved the shortest convergence time due to the absence of security validation, it does not protect against malicious routing announcements. Conversely, BGPsec recorded the longest convergence time because every routing update undergoes computationally expensive public-key cryptographic verification at each Autonomous System (AS) hop [69].

The proposed L-SBGP significantly reduced the convergence delay introduced by BGPsec while maintaining secure route validation. Specifically, L-SBGP reduced the average convergence time by approximately 94.7% relative to BGPsec. This improvement can be attributed to the replacement of asymmetric cryptographic operations with lightweight hash-based validation and selective verification of routing updates. These findings demonstrate that reducing computational complexity directly improves routing responsiveness without compromising route authenticity. From an operational perspective, faster convergence minimizes transient routing instability and packet loss, making L-SBGP more suitable for large-scale ISP backbone networks where rapid adaptation to topology changes is essential.

CPU utilization represents the computational resources consumed during route validation, processing, and routing-table updates. The simulation results indicate mean CPU utilizations of 12.50% for BGP, 84.20% for BGPsec, and 28.40% for L-SBGP. As expected, BGP exhibited the lowest processor utilization because it performs no cryptographic verification. In contrast, BGPsec imposed the highest processing overhead due to repeated digital-signature generation and verification for every routing advertisement [70] [71].

Although L-SBGP required more processor resources than conventional BGP, its average CPU utilization was substantially lower than that of BGPsec. Relative to BGPsec, L-SBGP reduced processor utilization by approximately 66.3%, demonstrating the effectiveness of lightweight hash-based validation in reducing computational overhead. This reduction is particularly significant for operational ISP environments where routers process thousands of routing updates continuously. Lower processor utilization enables improved router responsiveness, reduces the likelihood of processing bottlenecks, and decreases the need for expensive hardware upgrades, thereby improving the economic feasibility of deploying secure routing mechanisms.

The analysis showed that all three protocols exchanged an identical number of control messages (314 routing updates). This result indicates that the observed performance improvements are not due to changes in routing-update propagation but rather to improvements in the efficiency of processing each routing message. L-SBGP therefore maintains compatibility with the standard BGP message exchange process while reducing the computational cost associated with validating routing information. This

finding demonstrates that computational optimization, rather than protocol simplification through message reduction, is the principal factor contributing to the improved performance of L-SBGP.

Memory consumption remained constant at 0.04 MB across all three routing protocols throughout the experimental evaluation. Although no measurable difference was observed within the simulated environment, this result confirms that the proposed lightweight validation mechanism does not introduce additional memory overhead compared with existing routing protocols. Unlike BGPsec, which requires the management of cryptographic certificates and digital signatures, L-SBGP relies on compact hash values that impose minimal memory requirements. Consequently, the protocol is expected to scale more effectively in large ISP deployments where routing tables and security information continue to increase over time.

Routing scalability was evaluated by examining the number of successfully installed routing entries. All three protocols correctly installed 98 routing entries, indicating that the proposed lightweight validation mechanism does not compromise routing correctness or route propagation. This result demonstrates that integrating lightweight security mechanisms into the routing process preserves interoperability with existing BGP infrastructure while maintaining complete routing functionality. Consequently, network operators can adopt L-SBGP without negatively affecting routing reachability or routing-table consistency.

The ability to prevent malicious routing advertisements remains one of the most important requirements of secure inter-domain routing. During the simulated prefix-hijacking experiments, both BGPsec and L-SBGP achieved 100% hijack suppression, whereas conventional BGP provides no inherent protection against such attacks. The equivalent security performance achieved by L-SBGP demonstrates that strong routing protection does not necessarily require computationally intensive public-key cryptographic mechanisms. Instead, the combination of lightweight hash-based validation, selective route verification, and anomaly-aware filtering was sufficient to detect and prevent all simulated malicious routing announcements. These findings provide strong evidence that lightweight security mechanisms can achieve security levels comparable to BGPsec while substantially reducing computational overhead.

Collectively, the experimental results demonstrate that L-SBGP successfully balances the competing requirements of routing efficiency, computational performance, scalability, and security. Conventional BGP offers excellent performance but lacks protection against routing attacks, while BGPsec provides strong security at the expense of high computational cost and slower convergence. L-SBGP bridges this gap by combining lightweight route validation with selective verification mechanisms, thereby preserving complete hijack suppression while substantially reducing convergence delay and processor utilization [72] [73].

The consistency of the results across 20 independent simulation runs increases confidence in the stability of the proposed protocol and indicates that the observed improvements are attributable to the protocol design rather than random simulation variability. Overall, the findings validate the design decisions established in Objectives 1 and 2 and confirm that lightweight security mechanisms constitute a practical alternative to computationally intensive cryptographic approaches for secure inter-domain routing within ISP environments [74] [75]. The results therefore support the central hypothesis of this study that secure routing can be achieved without imposing the substantial computational overhead traditionally associated with BGPsec, thereby providing a scalable and operationally efficient solution for next-generation Internet routing.

### 4.8 Summary

This chapter presented the results and discussion of the study in accordance with the three research objectives. First, the findings from the Systematic Literature Review (SLR) and expert survey were analyzed to identify the factors influencing the computational complexity and security performance of secure Border Gateway Protocol (BGP) implementations within Internet Service Provider (ISP) environments. The combined analysis demonstrated a high level of agreement between the literature and expert opinions, leading to the identification of CPU utilization, routing convergence time, and scalability as the principal design parameters for the proposed Lightweight Secure Border Gateway Protocol (L-SBGP).

The chapter subsequently presented the design and formal specification of the proposed L-SBGP. The protocol was developed using lightweight hash-based route validation, routing update classification, selective route verification, and adaptive

routing mechanisms to reduce computational overhead while maintaining secure inter-domain routing. A formal protocol specification, including the system architecture, mathematical representation, routing workflow, state-transition model, and routing algorithm, was introduced to provide a rigorous definition of the proposed protocol before its implementation.

The final part of the chapter presented the performance evaluation of L-SBGP using a Python-based simulation prototype executed in Google Colab. The reported performance metrics represent the mean results obtained from twenty independent simulation runs conducted under identical network conditions. Comparative evaluation against conventional BGP and BGPsec demonstrated that the proposed protocol substantially reduced routing convergence time and CPU utilization while maintaining equivalent routing scalability, memory utilization, routing correctness, and complete suppression of simulated prefix hijacking attacks. These findings demonstrate that the lightweight validation mechanism effectively reduces computational complexity without compromising routing security.

Overall, the results presented in this chapter validate the proposed L-SBGP as a practical and scalable secure routing protocol for ISP environments. The findings confirm that lightweight security mechanisms can provide security performance comparable to conventional cryptographic approaches while significantly improving computational efficiency, thereby achieving the research objectives established for this study.

# CHAPTER FIVE
# CONCLUSION, RECOMMENDATIONS AND FUTURE WORK

## 5.1 Conclusion

The first research question sought to identify the parameters that influence the development of lightweight secure Border Gateway Protocol (BGP) mechanisms capable of reducing computational overhead within Internet Service Provider (ISP) environments. The findings from the Systematic Literature Review (SLR) and expert validation demonstrated that although several factors contribute to secure routing performance, CPU utilization, routing convergence time, and scalability are the most influential parameters affecting the practical deployment of secure BGP protocols. The literature consistently highlighted that conventional security mechanisms, particularly BGPsec, achieve strong route authentication at the expense of significant computational overhead resulting from repeated public-key cryptographic operations. The expert survey further confirmed these findings by identifying processor utilization and convergence performance as the primary operational concerns affecting secure routing deployment within ISP infrastructures. The high level of agreement between the literature review and expert responses strengthened the validity of the selected parameters and provided a sound empirical foundation for the design of the proposed Lightweight Secure Border Gateway Protocol (L-SBGP). Therefore, the first research objective was successfully achieved, and Research Question One was comprehensively answered through the integration of theoretical evidence and professional expertise.

The second research question focused on how a lightweight secure Border Gateway Protocol could be developed to address the computational limitations of existing secure routing protocols. Based on the findings obtained from Objective One, the study successfully designed and formally specified the proposed Lightweight Secure Border Gateway Protocol (L-SBGP). The protocol incorporated lightweight hash-based route validation, routing update classification, selective verification, anomaly-aware filtering, and adaptive routing decisions to minimize computational overhead while preserving routing security. Unlike BGPsec, which relies on computationally intensive asymmetric cryptographic operations for every routing update, the proposed protocol replaced these mechanisms with lightweight hash-based validation capable of providing efficient route authentication. The protocol was formally defined through

its mathematical model, architectural framework, routing workflow, state-transition model, and routing algorithm before implementation in Python. These design components collectively demonstrated that secure inter-domain routing can be achieved without introducing excessive computational complexity. Consequently, the second research objective was fully achieved by developing a scalable and computationally efficient secure routing protocol suitable for ISP deployment.

The third research question examined whether the proposed L-SBGP could improve routing performance while maintaining routing security. The protocol was evaluated using a Python-based simulation prototype executed in Google Colab, with the reported performance values representing the average results obtained from twenty independent simulation runs. The comparative evaluation demonstrated that L-SBGP significantly reduced routing convergence time and CPU utilization compared with BGPsec while maintaining identical routing scalability, routing correctness, memory utilization, and complete suppression of simulated prefix-hijacking attacks. The results confirmed that lightweight hash-based validation substantially reduced computational overhead without compromising routing integrity or security effectiveness. An important finding beyond the initial hypothesis was that the protocol achieved equivalent hijack suppression to BGPsec without increasing control-plane message overhead or memory consumption, indicating that high levels of routing security can be achieved without computationally intensive cryptographic mechanisms. These findings validate the proposed protocol and demonstrate that the third research objective was successfully achieved.

In summary, this study successfully addressed the research problem of reducing the computational overhead associated with secure inter-domain routing while maintaining effective protection against routing attacks. Through the integration of a systematic literature review, expert validation, formal protocol development, and experimental performance evaluation, the research demonstrated that lightweight security mechanisms constitute a practical alternative to conventional cryptographic approaches used in secure Border Gateway Protocol implementations. The proposed L-SBGP provides an effective balance between routing efficiency, computational performance, scalability, and security, making it suitable for deployment within Internet Service Provider environments where processing efficiency and routing

stability are critical operational requirements. Beyond achieving the stated research objectives, the study contributes a formally specified lightweight secure routing protocol and provides empirical evidence supporting the feasibility of replacing computationally expensive route validation mechanisms with lightweight alternatives. The findings therefore advance knowledge in secure inter-domain routing and establish a strong foundation for future research aimed at improving the scalability, interoperability, and practical deployment of lightweight secure routing protocols.

## 5.2 Recommendations

### 5.2.1 Recommendations for Practitioners

Internet Service Providers (ISPs) should consider phased deployment of the proposed Lightweight Secure Border Gateway Protocol (L-SBGP), beginning with pilot implementations and interoperability testing with existing BGP infrastructure. Continuous monitoring of convergence time, CPU utilization, routing stability, and security performance should be undertaken during deployment. ISPs should also provide technical training for network engineers to support configuration and maintenance. Given the reduced computational overhead demonstrated by L-SBGP, its adoption may reduce the need for immediate hardware upgrades, extend the operational lifespan of existing equipment, and lower operational and energy costs.

### 5.2.2 Recommendations for Standards Bodies and Policy Makers

National regulators, standards bodies, and policymakers should support the evaluation and gradual adoption of lightweight secure routing mechanisms through implementation guidelines, interoperability requirements, and best practices. Organizations such as the Internet Engineering Task Force (IETF) and Regional Internet Registries (RIRs) should encourage further research and standardization of lightweight secure routing approaches that complement existing BGP security mechanisms. Policymakers should also promote collaboration among governments, ISPs, equipment vendors, standards organizations, and researchers to support pilot deployments, technical capacity building, and the development of secure, scalable, and computationally efficient Internet routing infrastructure.

## 5.3 Future Research

### 5.3.1 Short-Term Priorities (0–6 Months)

The priority for future research should be the deployment of the proposed L-SBGP in a controlled network testbed using real BGP routing updates. This will enable the protocol to be evaluated under more realistic operating conditions than those provided by the current simulation environment. Future studies should also assess the interoperability of L-SBGP with existing BGP implementations and evaluate its performance under additional routing attack scenarios, such as route leaks and denial-of-service attacks. These activities will address the limitation of this study, which was based on a Python simulation prototype rather than a live ISP network.

### 5.3.2 Medium-Term Priorities (6–12 Months)

The second phase of future research should focus on evaluating L-SBGP in larger and more complex multi-Autonomous System (AS) environments. This should include integration with existing secure routing frameworks, particularly Resource Public Key Infrastructure (RPKI), to assess interoperability and compatibility with current Internet routing security standards. Additional research should also investigate the protocol's performance under larger routing tables and dynamic network topologies to determine its scalability in operational ISP environments.

### 5.3.3 Long-Term Priorities (1–2 Years)

Long-term research should investigate intelligent and adaptive extensions to L-SBGP. One promising direction is the integration of machine learning techniques for real-time routing anomaly detection and adaptive route validation based on changing network conditions. Future studies should also explore the integration of L-SBGP with Software-Defined Networking (SDN) and blockchain-based routing security frameworks to improve network automation, trust management, and resilience.

## REFERENCES


[1] Song, T., & Liu, Z. (2024). Receive Satellite-Terrestrial Networks Data using Multi-Domain BGP Protocol Gateways—*International Journal of Advanced Computer Science & Applications*, *15*(6).

[2] Salim, S., Moustafa, N., & Reisslein, M. (2024). Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. *IEEE Communications Surveys & Tutorials*.

[3] Villalón Huerta, A. (2023). *Modeling of advanced threat actors: characterization, categorization, and detection* (Doctoral dissertation, Universitat Politècnica de València).

[4] Rodday, N., Cunha, Í., Bush, R., Katz-Bassett, E., Rodosek, G. D., Schmidt, T. C., & Wählisch, M. (2023). The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects. *IEEE Transactions on Network and Service Management*.

[5] Kowalski, M., & Mazurczyk, W. (2023). Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures. *Computer Networks*, *230*, 109778.

[6] Rahim, J. A., Nordin, R., & Amodu, O. A. (2024). Open-Source Software Defined Networking Controllers: State-of-the-Art, Challenges and Solutions for Future Network Providers. *Computers, Materials & Continua*, *80*(1).

[7] Adelsbach, A., Schaefer, T., & Tountas, G. (2023). New Space Architectures–Connectivity and Cyber Security.

[8] Montasari, R. (2024). Exploring the Current Landscape of Cyberterrorism: Insights, Strategies, and the Impact of COVID-19. In *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment, and Responses* (pp. 65-90). Cham: Springer International Publishing.

[9] Aswad, F. M., Ahmed, A. M. S., Alhammadi, N. A. M., Khalaf, B. A., & Mostafa, S. A. (2023). Deep learning-based method for distributed denial-of-service attack detection in Internet of Things networks. *Journal of Intelligent Systems*, *32*(1), 20220155.

[10] Fathima, A., Devi, G. S., & Faizaanuddin, M. (2023). Improving distributed denial of service attack detection using supervised machine learning—measurement*: Sensors*, *30*, 100911.

[11] Rezaee, M. R., Hamid, N. A. W. A., Hussin, M., & Zukarnain, Z. A. (2024). Comprehensive Review of Drones Collision Avoidance Schemes: Challenges and Open Issues. *IEEE Transactions on Intelligent Transportation Systems*.

[12] Yang, Q., Ma, L., Tu, S. [53] [54] [54] [54], Ullah, S., Waqas, M., & Alasmary, H. (2024). Towards blockchain-based secure BGP routing, challenges and future research directions. *Computers, Materials and Continua*, *79*(2), 2035-2062.

[13] Milolidakis, A., Bühler, T., Wang, K., Chiesa, M., Vanbever, L., & Vissicchio, S. (2023). On the Effectiveness of BGP Hijackers That Evade Public Route Collectors. *IEEE Access*, *11*, 31092-31124.

[14] Holstein, W. J., & McLaughlin, M. (2023). *Battlefield Cyber: How China and Russia are Undermining Our Democracy and National Security*. Rowman & Littlefield.

[15] Topor, L. Cyber Sovereignty.

[16] Rodday, N., Rodosek, G. D., Pras, A., & van Rijswijk-Deij, R. (2024, May). Exploring the benefit of path plausibility algorithms in BGP. In *NOMS 2024-2024 IEEE Network Operations and Management Symposium* (pp. 1-10). IEEE.

[17] Kowalski, M., & Mazurczyk, W. (2023). Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures. *Computer Networks*, *230*, 109778.

[18] Muosa, A. H., & Ali, A. H. (2024, January). Detecting BGP Routing Anomalies Using Machine Learning: A Review. In *International Conference on Forthcoming Networks and Sustainability in the AIoT Era* (pp. 145-164). Cham: Springer Nature Switzerland.

[19] Tyagi, V., Saraswat, A., & Bansal, S. (2023). An Analysis of Securing Internet of Things (IoT) Devices from Man-in-the-Middle (MIMA) and Denial of Service (DoS). In *Smart Cities* (pp. 337-357). CRC Press.

[20] Prehn, L., Foremski, P., & Gasser, O. (2024, July). Kirin: Hitting the Internet with Distributed BGP Announcements. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security* (pp. 19-34).

[21] Liu, M., Li, Z., Cai, K., Allcock, J., Zhang, S., & Lui, J. C. (2024, May). Quantum BGP with Online Path Selection via Network Benchmarking. In IEEE INFOCOM 2024-IEEE Conference on Computer Communications (pp. 1401-1410). IEEE.

[22] García-Martínez, A., Torres Jr., P. R., & Bagnulo, M. (2024). BGP convergence in an MRAI-free Internet. *Computer Networks*, *240*, 110183.

[23] Hussen, B. (2023). *Deploying End-to-End Quality of Service in Telecommunication Networks and Multiple Label Switching Virtual Private Networks* (Doctoral dissertation, St. Mary's University).

[24] van Hove, K., van der Ham-de Vos, J., & van Rijswijk-Deij, R. (2023). rpkiller: Threat Analysis of the BGP Resource Public Key Infrastructure. *Digital Threats: Research and Practice*, *4*(4), 1-24.

[25] Hlavacek, T., Shulman, H., Vogel, N., & Waidner, M. (2023). Keep Your Friends Close, but Your Routeservers Closer: Insights into {RPKI} Validation in the Internet. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 4841-4858).

[26] Richter, P., Bajpai, V., & Carisimo, E. Passive and Active Measurement.

[27] Holterbach, T., Alfroy, T., Phokeer, A., Dainotti, A., & Pelsser, C. (2024). A System to Detect {Forged-Origin}{BGP} Hijacks. In *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)* (pp. 1751-1770).

[28] Yang, Q., Ma, L., Tu, S., Ullah, S., Waqas, M., & Alasmary, H. (2024). Towards blockchain-based secure BGP routing, challenges and future research directions. *Computers, Materials and Continua*, *79*(2), 2035-2062.

[29] Prehn, L., Foremski, P., & Gasser, O. (2024, July). Kirin: Hitting the Internet with Distributed BGP Announcements. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security* (pp. 19-34).

[30] Li, P., Lu, B., & Li, D. (2021). BGP neighbor trust establishment mechanism based on the bargaining game: information, *12*(3), 110.

[31] Kowalski, M., & Mazurczyk, W. (2023). Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures. *Computer Networks*, *230*, 109778.

[32] Gimenez, O. (2023). *Relay Attacks over the Internet: Anomaly Detection using Time Measurement* (Doctoral dissertation, INSA de Rennes).

[33] Maleh, Y., Qasmaoui, Y., El Gholami, K., Sadqi, Y., & Mounir, S. (2023). A comprehensive survey on SDN security: threats, mitigations, and future directions. *Journal of Reliable Intelligent Environments*, *9*(2), 201-239.

[34] Borchert, O., Lee, K., Sriram, K., Montgomery, D., & Gleichmann, P. (2021). *BGP Secure Routing Extension (BGP-SRx): Reference implementation and test tools for emerging BGP security standards* (NIST Technical Note 2060). National Institute of Standards and Technology.

[35] Höoger, N., Rodday, N., Borchert, O., & Rodosek, G. D. (2023, October). Path Plausibility Algorithms in GoBGP. In *2023, the 19th International Conference on Network and Service Management (CNSM)* (pp. 1-3). IEEE.

[36] Kuikka, S. (2024). Kubernetes Networking: Comparative Insights into API Gateways and Service Mesh Implementations.

[37] Singha, R., Mondal, R., Beckett, R., Kakarla, S. K. R., Millstein, T., & Varghese, G. (2024). {MESSI}: Behavioral Testing of {BGP} Implementations. In *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)* (pp. 1009-1023).

[38] S. Barrett, C. Idom, G. Zavala Villafuerte, A. Byers, and B. Gulmezoglu, “Ain't How You Deploy: An Analysis of BGP Security Policies Performance Against Various Attack Scenarios with Differing Deployment Strategies,” arXiv, 2024.

[39] Gupta, S., & Maple, C. (2023). A Survey of Security Mechanisms for Edge Computing-based Connected Autonomous Vehicles. *Authorea Preprints*.

[40] Kayathri, T. L., Kumaresan, N., & Vijayabhasker, R. (2023). SDBGPChain: A decentralized, low complexity framework to detect and prevent BGP attacks using SDN with a smart contract-based Dendrimer tree blockchain. *Computer Networks*, *230*, 109800.

[41] Milolidakis, A., Bühler, T., Wang, K., Chiesa, M., Vanbever, L., & Vissicchio, S. (2023). On the Effectiveness of BGP Hijackers That Evade Public Route Collectors. *IEEE Access*, *11*, 31092-31124.

[42] Alfroy, T., Holterbach, T., Krenc, T., Claffy, K. C., & Pelsser, C. (2024, August). The Next Generation of BGP Data Collection Platforms. In *Proceedings of the ACM SIGCOMM 2024 Conference* (pp. 794-812).

[43] Salisbury, B. (2021). *GoBGP – A control plane evolving software networking*. NetworkStatic.

[44] Furuness, J., Morris, C., Morillo, R., Herzberg, A., & Wang, B. (2023, August). Bgpy: The bgp python security simulator. In *Proceedings of the 16th Cyber Security Experimentation and Test Workshop* (pp. 41-56).

[45] Schneider, T., Schmid, R., Vissicchio, S., & Vanbever, L. (2023, September). Taming the transient while reconfiguring BGP. In *Proceedings of the ACM SIGCOMM 2023 Conference* (pp. 77-93).

[46] Sharp, R. (2023). Network Security. In *Introduction to Cybersecurity: A Multidisciplinary Challenge* (pp. 171-233). Cham: Springer Nature Switzerland.

[47] Raynor, J. (2023). *Cybersecurity Visualization Design Approaches: Toward Connecting Research and Practice Through Technique, Context, and Process* (Doctoral dissertation, Northeastern University).

[48] Qin, L., Chen, L., Li, D., Ye, H., & Wang, Y. (2024). Understanding Route Origin Validation (ROV) Deployment in the Real World and Why MANRS Action 1 Is Not Followed. NDSS.

[49] Lyu, M., Gharakheili, H. H., & Sivaraman, V. (2024). A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection. *IEEE Access*.

[50] Rodday, N., Cunha, Í., Bush, R., Katz-Bassett, E., Rodosek, G. D., Schmidt, T. C., & Wählisch, M. (2023). The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects. *IEEE Transactions on Network and Service Management*.

[51] Chiesa, M., Kamisiński, A., Rak, J., Rétvári, G., & Schmid, S. (2023). A survey of fast recovery mechanisms in the data plane. *Authorea Preprints*.

[52] Singha, R., Mondal, R., Beckett, R., Kakarla, S. K. R., Millstein, T., & Varghese, G. (2024). {MESSI}: Behavioral Testing of {BGP} Implementations. In *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)* (pp. 1009-1023).

[53] Smith, V. K. K., & Sandhya, S. (2024). Implementation of A Delay-Tolerant Routing Protocol in the Network Simulator NS-3. International Journal of Emerging Science and Engineering, 12(11).

[54] Ravichandran, N., Tewaraja, T., Rajasegaran, V., Kumar, S. S., Gunasekar, S. K. L., & Sindiramutty, S. R. (2024). Comprehensive Review Analysis and Countermeasures for Cybersecurity Threats: DDoS, Ransomware, and Trojan Horse Attacks. *Preprints. Org*.

[55] Tache, M. D., Păscuțoiu, O., & Borcoci, E. (2024). Optimization algorithms in SDN: Routing, load balancing, and delay optimization. *Applied Sciences*, *14*(14), 5967.

[56] Jamshidi, S., Nikanjam, A., Nafi, K. W., & Khomh, F. (2025). Understanding the impact of IoT security patterns on CPU usage and energy consumption: a dynamic approach for selecting patterns with deep reinforcement learning: S. Jamshidi et al. *International Journal of Information Security*, *24*(2), 91.

[57] Aslanidis, T., Kosta, S., Montella, R., Lalis, S., & Chatzopoulos, D. (2026, April). Reducing Language Model Inference Latency using CPU-Assisted Serving. In *Proceedings of the Sixth European Workshop on Machine Learning and Systems* (pp. 304-314).

[58] Zare Soltani, M. A., Hosseini Seno, S. A., & Mohajerzadeh, A. (2025). Efficient dynamic load balancing in software-defined networks using policy gradient: a strategy for enhanced QoS and reduced energy consumption: MAZ Soltani et al. *Computing*, *107*(7), 159.

[59] Farahi, R. (2025). A comprehensive overview of load balancing methods in software-defined networks. *Discover Internet of Things*, *5*(1), 6.

[60] Soliman, A. M. K. M. (2025). *Analysis of Geography-Oriented Internet Routing* (Doctoral dissertation, Carleton University).

[61] Giotsas, V., Berdan, K., Rubin, C., Goncalves, V., & Fayed, M. (2025). Regional Perspectives for Route Resilience in a Global Internet: Metrics, Methodology, and Pathways for Transparency. *Methodology, and Pathways for Transparency (August 1, 2025)*.

[62] Durand, A. (2030). New IP. *Network*, 5.

[63] Constantin, M.A., Schuurman, N.K. and Vermunt, J.K., 2026. A general Monte Carlo method for sample size analysis in the context of network models. *Psychological methods*, *31*(3), p.385.

[64] Qamar, M.S. and Munir, M.F., 2025. A hybrid framework integrating deterministic clustering, neural networks, and energy-aware routing for enhanced efficiency and longevity in wireless sensor network. *Computers, Materials & Continua*, *84*(3), pp.5463-5485.

[65] Ajbarh, K., Dhaw, H.F. and ALhadi, A.A., 2026. Compare the performance of Dynamic Routing protocols Based protocol Traffic Sent, Network Convergence duration and CPU Utilization using OPNET Modeler. *Journal of Electrical and Electronic Engineering and Information Technology*, *3*(01), pp.26-36.

[66] Oun, A., Ahmed, N. and Ashtawi, A., 2026. Routing Scalability, Convergence, and Stability: A Comparative Analysis of Network-layer Design Trade-offs (2016–2026). *AlQalam Journal of Medical and Applied Sciences*, pp.1682-1694.

[67] Alanazi, R., Obayya, M., Alghamdi, A.M., Nemri, N., Alshahrani, S., Alduaiji, N., Hasanin, T. and Sorour, S., 2025. Machine learning-driven routing optimization for energy-efficient 6G-enabled wireless sensor networks. *Alexandria Engineering Journal*, *129*, pp.877-888.

[68] Vasagam, M., Kumar, A. and Garg, A., 2026. Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. *IEEE Access*.

[69] Höger, N., Hesselman, C., Müller, M. and Kastanakis, S., 2025, October. xBGPsec: Enhancing BGP Security with Transitive Signatures and External

Validation. In *2025 21st International Conference on Network and Service Management (CNSM)* (pp. 1-5). IEEE.

[70] Höger, N., Hesselman, C., Müller, M. and Kastanakis, S., 2025, October. xBGPsec: Enhancing BGP Security with Transitive Signatures and External Validation. In *2025 21st International Conference on Network and Service Management (CNSM)* (pp. 1-5). IEEE.

[71] Zwach, S., 2025. Performance Measurement of BGP Extended with De-Fact Network Identification.

[72] Song, J., Wang, X. and Lu, P., 2026. A Lightweight Identity Authentication Protocol for Vehicle Ad Hoc Network Based on PUF-Obfuscation. *Sensors*, *26*(10), p.2971.

[73] Naik, A.J., 2025. Optimizing Lightweight Authentication Protocols for Enhancing Security in Resource-Constrained IoT Devices.

[74] Servillo, S., Spadaccino, P., Centenaro, M., Prado, A., Rossi, M., Luciani, F., Scannapieco, M. and Cuomo, F., 2026. Survey on Internet Routing Security: Stakeholder Interests, Current and Future Research Directions. *IEEE Communications Surveys & Tutorials*.

[75] Sundaravarathan, V., 2025. *Shared Memory Based Cross-Domain Solution (CDS) for 5G Applications* (Doctoral dissertation, Arizona State University).

# APPENDICES

**Appendix 1: Research tools and instruments, and Questionnaires**

**The research used Google Colab tools**

Sample Questionnaire for Expert Opinions on Reducing Complexity Overheads in Routing Protocols

**Section 1: General Information**

1. Name (Optional): _____
2. Job Title: _____
3. Years of Experience in Networking/BGP Security:
    - 1–3 years
    - 4–6 years
    - 7–10 years
    - 10+ years
4. Organization Type:
    - Internet Service Provider (ISP)
    - Network Security Firm
    - Government/Regulatory Body
    - Research Institution
    - Other (Specify): _____

**Section 2: Complexity in Routing Protocols**

5. In your experience, what are the top three factors contributing to complexity in existing secure routing protocols (e.g., BGP, BGPsec)?

---

6. How does protocol overhead (e.g., large routing tables, frequent updates) impact routing efficiency in ISPs?
    - Severely impacts efficiency

- Moderately impacts efficiency
- Minimally impacts efficiency
- No impact

7. What are the most resource-intensive processes in current BGP security mechanisms? (Select all that apply)
    - Cryptographic validation of route announcements
    - Frequent route updates and policy enforcement
    - Managing large routing tables
    - Handling misconfigurations and security threats

**Section 3: Possible Solutions for Complexity Reduction**

8. In your opinion, which key parameters should be optimized to reduce complexity overheads in secure BGP protocols?
    - Faster routing convergence time
    - Reduced computational overhead
    - Improved scalability
    - Lower memory and CPU usage
    - Other (Specify): _____
9. What lightweight security techniques would you recommend to reduce complexity without compromising security?

---

10. In your experience, how effective would a modular and scalable routing protocol be in addressing complexity issues in ISP environments?

- Highly effective
- Moderately effective
- Slightly effective

- Ineffective

**Section 4: Final Thoughts**

11. What are your recommendations for designing a Lightweight Secure Border Gateway Protocol (LS-BGP) to address current BGP complexity challenges?

---

12. Would you be interested in participating in further discussions or collaborations on improving secure routing protocols?

- Yes
- No

Thank you for your time and valuable insights! Your responses will contribute significantly to this research.

**Appendix 2: Code List**

```
# ============================================================
# INSTALL DEPENDENCIES (COLAB)
# ============================================================
!pip install psutil cryptography -q

# ============================================================
# IMPORTS
# ============================================================
import time
import random
import hashlib
import psutil
import tracemalloc
from collections import deque
from cryptography.hazmat.primitives.asymmetric import rsa
import matplotlib.pyplot as plt

# ============================================================
# GLOBAL PARAMETERS (THESIS-ALIGNED)
# ============================================================
POPULATION_SIZE = 100
SAMPLE_SIZE = 30
PREFIX = "10.0.0.0/24"
LEGIT_AS = 1
ATTACKER_AS = 50
SEED = 42

random.seed(SEED)

# ============================================================
# BUILD SHARED TOPOLOGY (FAIR COMPARISON)
# ============================================================
def build_topology():
    topology = {}
    for i in range(1, POPULATION_SIZE + 1):
        neighbors = random.sample(
            [x for x in range(1, POPULATION_SIZE + 1) if x != i],
            k=random.randint(2, 5)
        )
        topology[i] = neighbors
    return topology

TOPOLOGY = build_topology()

# ============================================================
# LIGHTWEIGHT HASH (L-SBGP CORE)
# ============================================================
def lightweight_hash(data):
```

```
    return hashlib.sha256(data.encode()).hexdigest()[:16]

# ============================================================
# PURE BGP
# ============================================================
def run_bgp():
    routing_table = {}
    queue = deque([(LEGIT_AS, [LEGIT_AS])])
    messages = 0

    start = time.time()

    while queue:
        node, path = queue.popleft()
        messages += 1

        if node in path[:-1]:
            continue

        if node not in routing_table or len(path) < len(routing_table[node]):
            routing_table[node] = path

            for n in TOPOLOGY[node]:
                queue.append((n, path + [n]))

    return time.time() - start, messages, len(routing_table)

# ============================================================
# BGPsec (SIMULATED CRYPTO COST)
# ============================================================
class BGPsecNode:
    def __init__(self):
        self.private_key = rsa.generate_private_key(
            public_exponent=65537,
            key_size=1024
        )

def run_bgpsec():
    nodes = {i: BGPsecNode() for i in range(1, POPULATION_SIZE + 1)}
    routing_table = {}
    queue = deque([(LEGIT_AS, [LEGIT_AS])])
    messages = 0

    start = time.time()

    while queue:
        node, path = queue.popleft()
        messages += 1

        # Simulate cryptographic overhead
```

```
        time.sleep(0.0005)

        if node in path[:-1]:
            continue

        if node not in routing_table or len(path) < len(routing_table[node]):
            routing_table[node] = path

            for n in TOPOLOGY[node]:
                queue.append((n, path + [n]))

    return time.time() - start, messages, len(routing_table)

# ============================================================
# L-SBGP
# ============================================================
def run_lsbgp(hijack=False):
    routing_table = {}
    origin = LEGIT_AS if not hijack else ATTACKER_AS

    queue = deque([(origin, [origin])])
    messages = 0

    start = time.time()

    while queue:
        node, path = queue.popleft()
        messages += 1

        # Lightweight validation
        _ = lightweight_hash(str(path))

        # Reject malicious routes
        if hijack:
            continue

        if node in path[:-1]:
            continue

        if node not in routing_table:
            routing_table[node] = path

            for n in TOPOLOGY [node]:
                queue.append((n, path + [n]))

    return time.time() - start, messages, len(routing_table)

# ============================================================
# PERFORMANCE MEASUREMENT
# ============================================================
```

```
def measure(func, name):
    print(f"\nRunning {name}...")

    tracemalloc.start()
    cpu_start = psutil.cpu_percent(interval=None)

    t, msgs, routes = func()

    cpu_end = psutil.cpu_percent(interval=None)
    mem = tracemalloc.get_traced_memory()[1] / (1024 * 1024)

    tracemalloc.stop()

    print(f"{name} completed.")

    return {
        "time": t,
        "messages": msgs,
        "routes": routes,
        "cpu": abs(cpu_end - cpu_start),
        "memory": mem
    }

# ============================================================
# RUN EXPERIMENTS (OBJECTIVE 3)
# ============================================================
bgp = measure(run_bgp, "Pure BGP")
bgpsec = measure(run_bgpsec, "BGPsec")
lsbgp = measure(lambda: run_lsbgp(False), "L-SBGP")

# Attack simulation (security validation)
_, _, legit_routes = run_lsbgp(False)
_, _, attack_routes = run_lsbgp(True)

hijack_suppression = ((legit_routes - attack_routes) / legit_routes) * 100

# ============================================================
# RESULTS TABLE (CHAPTER 4)
# ============================================================
print("\n========== FINAL RESULTS ==========")
print(f"{'Metric':<25}{'BGPsec':<12}{'L-SBGP':<12}")
print("-"*60)

print(f"{'Convergence Time (s)':<25}{bgpsec['time']:<12.4f}{lsbgp['time']:<12.4f}")
print(f"{'Control Messages':<25}{bgpsec['messages']:<12}{lsbgp['messages']:<12}")
print(f"{'CPU Utilization (%)':<25}{bgpsec['cpu']:<12.2f}{lsbgp['cpu']:<12.2f}")
print(f"{'Memory Usage
(MB)':<25}{bgpsec['memory']:<12.2f}{lsbgp['memory']:<12.2f}")
print(f"{'Routes Installed':<25}{bgpsec['routes']:<12}{lsbgp['routes']:<12}")
```

```
print("-"*60)
print(f"Hijack Suppression (L-SBGP): {hijack_suppression:.2f}%")

# ============================================================
# VISUALIZATION (FOR THESIS FIGURES)
# ============================================================
protocols = [ "BGPsec", "L-SBGP"]

times = [ bgpsec['time'], lsbgp['time']]
cpu = [ bgpsec['cpu'], lsbgp['cpu']]

plt.figure()
plt.bar(protocols, times)
plt.title("Convergence Time Comparison")
plt.xlabel("Protocol")
plt.ylabel("Time (seconds)")
plt.show()

plt.figure()
plt.bar(protocols, cpu)
plt.title("CPU Utilization Comparison")
plt.xlabel("Protocol")
plt.ylabel("CPU (%)")
plt.show()

# Hijack Suppression Rate Comparison
hijack_suppression_lsbgp = hijack_suppression # Use the already calculated value (100.00)
hijack_suppression_bgp = 0.0 # Assuming 0% suppression for BGP
hijack_suppression_bgpsec = 100.0 # As per user's provided data

protocols_suppression = [ "BGPsec", "L-SBGP"]
suppression_rates = [ hijack_suppression_bgpsec, hijack_suppression_lsbgp]
plt.figure(figsize=(8, 5))
plt.bar(protocols_suppression, suppression_rates, color=['lightcoral', 'lightgreen', 'skyblue'])
plt.title('Hijack Suppression Rate Comparison')
plt.xlabel('Protocol')
plt.ylabel('Suppression Rate (%)')
plt.ylim(0, 100)
plt.grid(axis='y', linestyle='--', alpha=0.7)
plt.show()
# ============================================================
# INTERPRETATION (USE IN THESIS)
# ============================================================
print("\nINTERPRETATION:")
print("• BGPsec is secure but computationally expensive.")
print("• L-SBGP achieves near-BGP speed with significantly lower overhead.")
print("• L-SBGP provides strong hijack suppression with minimal resource usage.")
```

## Appendix 3: Letter of Approval from Board of Postgraduate Studies

**MURANG'A UNIVERSITY OF TECHNOLOGY**

*Office of the Director, Postgraduate Studies*

E-mail: bps@mut.ac.ke
Website: www.mut.ac.ke
P.O. Box 75-10200
Murang'a, Kenya

**Ref:** MUT/ARP/PGS/19/2020 /VOL.1 **Date:** 12th January, 2026

Mr. Steve Barongo Mong'are,
School of Computing and Information Technology,
Murang'a University of Technology,
P.O. Box 75-10,200
Murang'a.

Dear Mr. Barongo,

**RE: APPROVAL OF RESEARCH PROPOSAL AND SUPERVISORS.**

I am pleased to inform you that the Directorate of Postgraduate Studies on 17th December, 2025 considered and approved your Masters research proposal entitled ***"A light Weight Secure Border Gateway Routing Protocol for Internet Service Providers in Reducing Complexity"*** and appointed the following as supervisors:

1. Dr. Daniel Makupi - Murang'a University of Technology
2. Dr. Stephen Njenga - Murang'a University of Technology

You may now proceed with your data collection subject to obtaining research permit from NACOSTI, if required. You should also begin consulting your supervisors and submit through them quarterly progress reports to the Director Postgraduate Studies through your CoD and School Dean. Progress Reports forms can be accessed in the Student Portal.

It is the policy and regulations of the University that you observe deadlines. The guidelines on Postgraduate supervision can be accessed in the post graduate Handbook.

Your responsibilities as a student will include, among others;

i. Maintain regular consultation with your supervisor(s), at least once a month
ii. Submit quarterly reports on time, through your supervisors, CoD, Dean and to the Director of Postgraduate Studies;
iii. Ensure quality work all through;

iv. Present your research findings at 2-3 seminars/conferences prior to thesis examination.
v. Publish one article from your research findings in a refereed journal prior to thesis examination.

For any further clarification please contact the undersigned.

Yours Sincerely,

**Prof. Geoffrey Muchiri, PhD**
**Director, Postgraduate Studies**
GM/SKD

DIRECTORATE OF POSTGRADUATE STUDIES
MURANG'A UNIVERSITY OF TECHNOLOGY
12 JAN 2020
P. O. Box 75 - 10200, MURANG'A
Tel: 0771483015, Email: info@mut.ac.ke

Copy to:
1. Registrar – Academics and Students Affairs
2. Dean, School of Computing and Information Technology

## Appendix 4: NACOSTI Research License



REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 760925

Date of Issue: 22/January/2026

RESEARCH LICENSE

This is to Certify that Mr.. STEVE BARONGO MONG'ARE of Murang'a University of Technology, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Muranga on the topic: A Light Weight Secure Border Gateway routing Protocol for Internet Service Providers in Reducing Complexity for the period ending : 22/January/2027.

License No: NACOSTI/P/26/4183538

760925

Applicant Identification Number

Ag. Director General

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

## Appendix 5: Publication

The following paper has been published from this thesis:

[1] Barongo Mong'are, S., Njenga, S. T., Makupi, D., & Mwangi, P. M. (2026). A Systematic Literature and Expert-Based Analysis of Parameters Influencing Lightweight Secure Border Gateway Protocols for Internet Service Providers. *International Research Journal of Engineering and Technology (IRJET)*, 13(4), 1736–1742. https://www.irjet.net/archives/V13/i4/IRJET-V13I04256.pdf