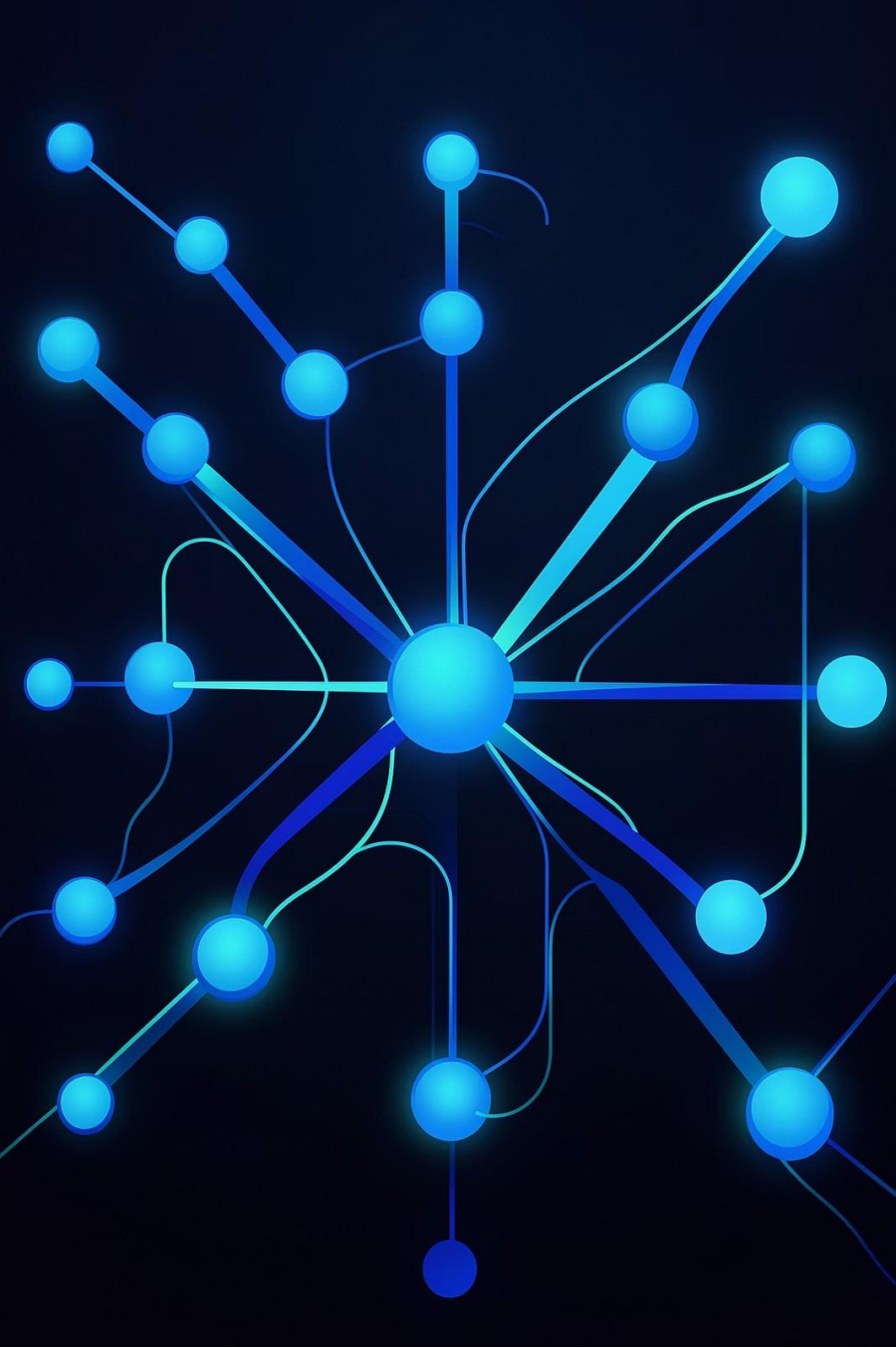




NETWORK SECURITY RESEARCH · NAYMUL HASNAT · ID: 2432483

Security Analysis of Vulnerabilities in Common Routing Protocols

RIP, OSPF, and BGP

The Insecure Foundations of Internet Routing



Routing protocols were designed for **trusted environments** not today's adversarial Internet. RIP and OSPF operate within administrative domains; BGP exchanges routes between autonomous systems globally.

- **Weak authentication:** plaintext passwords, optional MD5, or no validation at all
- **BGP:** no native origin verification thousands of prefix hijacks occur annually
- **2019 Cloudflare outage:** caused by an accidental BGP route leak, demonstrating real-world impact

What This Research Addresses

Fragmented Knowledge

Existing studies focus on individual protocols or specific attacks. No unified comparative framework evaluates RIP, OSPF, and BGP under consistent criteria.

Uneven Deployment

Authentication is often disabled in practice. RPKI adoption for BGP remains partial, leaving many networks exposed to hijacks and route leaks.

Core Research Question

How do design-level weaknesses in RIP, OSPF, and BGP enable specific attacks, and what mitigations are most effective under realistic deployment conditions?

Five Objectives Driving This Study

01

Literature Synthesis

Review academic and industry sources (2020–2026) on routing protocol vulnerabilities and attack vectors.

02

Threat Characterization

Categorize attack types per protocol route injection, prefix hijacking, LSA spoofing, DoS.

03

Framework Development

Design a comparative evaluation framework assessing authentication, integrity, and attack resilience.

04

Empirical Analysis

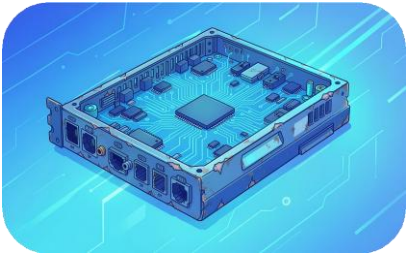
Simulate attacks on RIP, OSPF, and BGP in controlled testbeds; evaluate countermeasures.

05

Recommendations

Propose best practices: RPKI deployment, OSPF HMAC–SHA, secure protocol variants.

Vulnerability Profiles Across Three Protocols



RIP 4 Distance-Vector

Route poisoning, impersonation, and arbitrary injection. RIPv1 has no authentication; RIPv2's MD5 is vulnerable if a router is compromised.



OSPF 4 Link-State

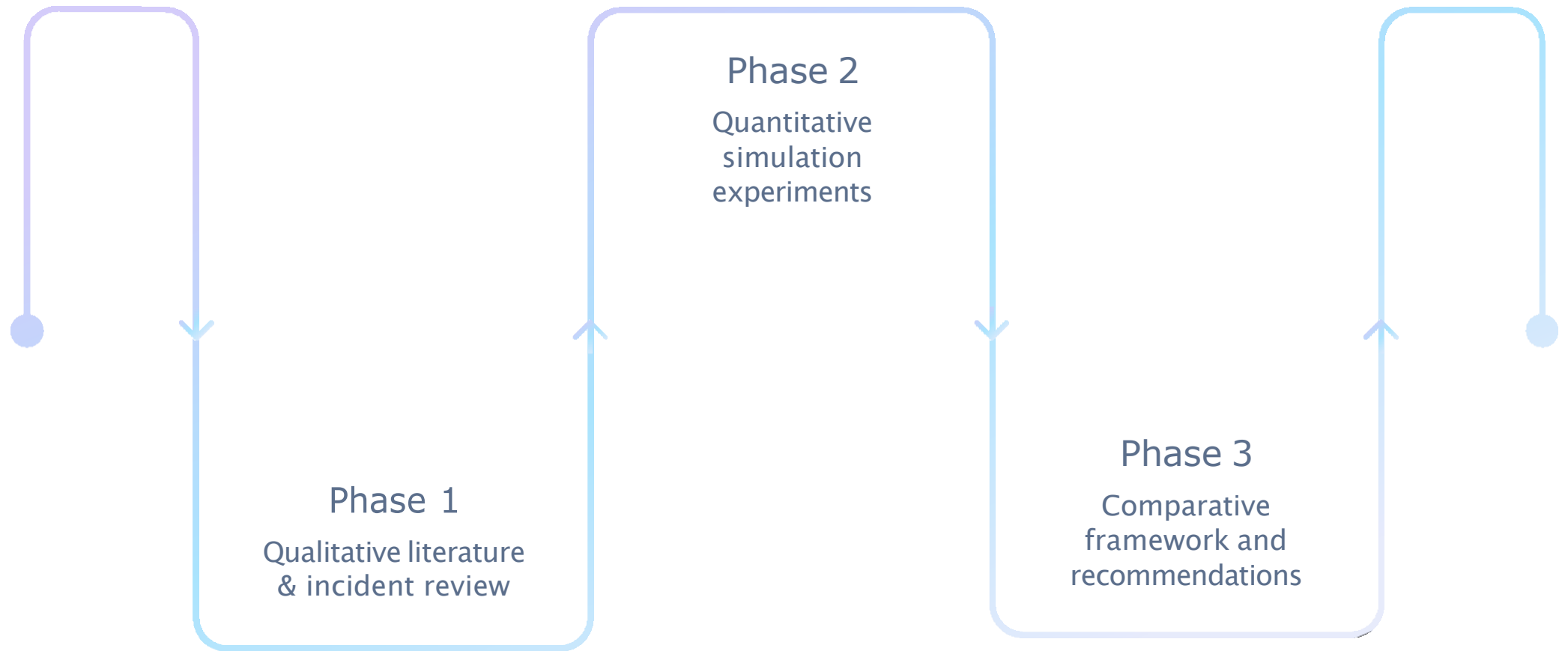
Forged LSAs can corrupt the link-state database. Cisco advisory confirms unauthenticated attackers can take full control of OSPF routing tables.



BGP 4 Path-Vector

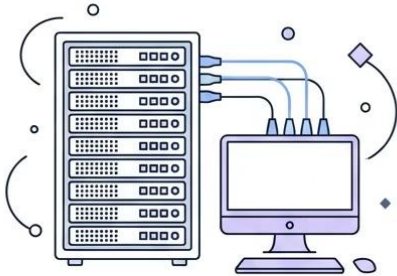
Prefix hijacking and route leaks propagate globally without origin validation. RPKI covers ~50% of prefixes but misconfigurations persist.

Mixed-Methods Research Design



Experiments toggle authentication (OSPF MD5/HMAC, BGP RPKI) to compare secure vs. insecure scenarios. Metrics include routes diverted, traffic rerouted, and convergence time.

Tools, Testbeds & Data Sources



SIMULATION TOOLS
GNS3, Cisco Packet Tracer, BIRD, FRRouting, Quagga



ANALYSIS TOOLS
Wireshark, Python scripting, Routinator RPKI validator



DATA SOURCES
CVE/NVD, BGPStream, RIPE RIS, RouteViews, operator mailing lists



HARDWARE
high-spec workstation, cloud VMs, optional physical lab devices

Experimental Architecture

A flexible emulation setup enables controlled attack injection:

- **RIP/OSPF:** GNS3 or Packet Tracer running IOS router images
- **BGP:** BIRD/FRRouting on Linux VMs with virtual interconnects
- **Validation:** Routinator RPKI validator for origin checks
- **Ethics:** All experiments confined to isolated lab networks

EXPECTED OUTCOMES & IMPACT

Anticipated Contributions

Threat Taxonomy

Structured classification of attacks per protocol 4 from RIP route poisoning to BGP sub-prefix hijacks and OSPF LSA spoofing.

Comparative Security Profile

OSPF with MD5/HMAC resists intra-domain attacks; BGP remains the weakest link without widespread RPKI adoption.

Actionable Guidance

Evidence-based recommendations: enable OSPF authentication, deploy RPKI, adopt MANRS guidelines, and filter suspicious BGP updates.

Scope Constraints & External Validity



Simulation Scale

Lab environments cannot replicate full Internet BGP topology or router resource constraints.

Data Availability

Public route collector data limits ability to simulate nation-scale incidents.

Rapid Evolution

Vulnerabilities may be patched faster than the research timeframe allows full analysis.

External Validity

Findings assume worst-case attacker proximity; real-world conditions may differ.

REFERENCES

Key Sources

[1] Siddiqui, A. (2022)

BGP Security in 2021. *MANRS Observatory Blog*.

[3] Mirdita, D. et al. (2024)

SoK: An Introspective Analysis of RPKI Security.
arXiv:2408.12359.

[5] Cisco Systems (2013)

OSPF LSA Manipulation Vulnerability. *Cisco Security Advisory*.

[2] Danquah, P. (2026)

Evaluation of Secured and Unsecured OSPF Routing Protocols. *East African J. of Info. Tech.*, 9(1), 104–120.

[4] Kranakis, S. & Ravel, K. B. (2024)

S-RIP: A Secure Distance Vector Routing Protocol. *ACNS 2004*, pp. 43–59.

[6] Scott, B. A. et al. (2024)

A Survey of Advanced BGP Attack Detection Techniques. *Sensors*, 24(19), 6414.



Thank You!