A Distributed Framework To Enhance Inter-Domain Routing Security

A Localised Overlay Management Plane for BGP Byzantine Robustness

Author: Binita Makanji (22010350) | BSc Cyber Security
First Supervisor: Dr Vahid Heydari Fami Tafreshi
Second Supervisor: Dr Maryam Shahpasand

University of Staffordshire London

This project proposes and experimentally evaluates the use of an incrementally deployable integrated management plane framework that enables distributed route validation independently of the BGP control plane, while maintaining scalable and manageable operational overhead across increasing network topology sizes.

1 Background & Motivation

The Border Gateway Protocol (BGP) enables inter-domain routing between autonomous systems (ASes).

A lack of built-in security allows false route advertisements.

Prefix hijacking can cause traffic interception and widespread outages.

BGP remains fundamentally trust-based.

2 Project Objectives

- Analyse prefix hijacking behaviour.
- Evaluate AS connectivity and collusion impact on hijack success rates.
- Design an overlay management plane prototype in GNS3.
- Evaluate scalability and operational overhead.

3 Literature Review Key Findings

1. Cryptographic Overhead

- S-BGP introduces high convergence overhead [1].

2. Need for Global Adoption

- RPKI adoption remains limited across RIRs [2].

3. Internet-Scale Challenges

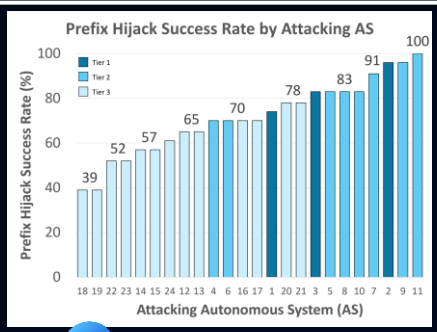
- Technical and financial costs limit deployment [3].

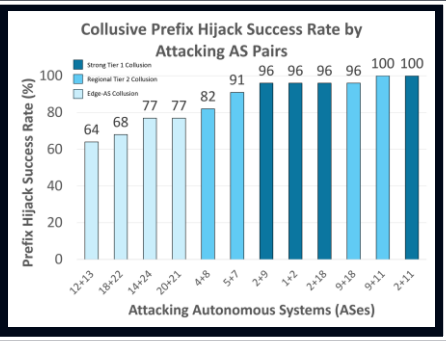
4. Deployment Complexity

- RPKI deployment remains costly and time-consuming [4].

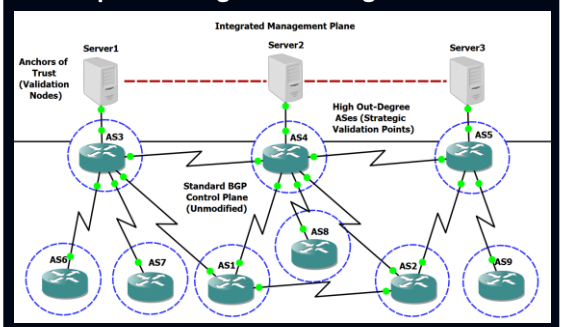
4 Prefix Hijacking & Collusion Simulations

- Higher tier and centrally connected ASes achieved the highest hijack success rates.
- Coordinated collusion attacks produced greater propagation impact than many single-attacker scenarios.
- Topological proximity to the victim AS significantly increased hijack success rates.





5 Proposed Integrated Management Plane

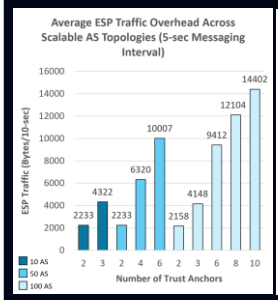


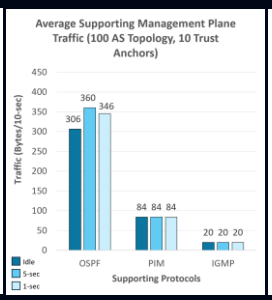
Framework Contributions:

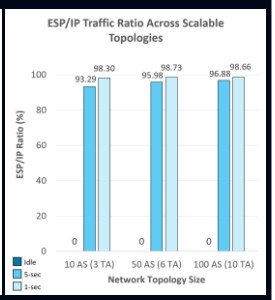
- Independent overlay validation plane separate from the standard BGP control plane.
- Incrementally deployable with no BGP modifications.
- High out-degree trust anchors for route visibility.
- Lightweight ESP/IP-based secure management plane communication.
- Scalable multicast distribution using PIM-SM and IGMP.

6 Scalability Evaluation Results

Assessing overhead across 10 AS, 50 AS & 100 AS topologies.







- Idle overlay operation introduced minimal traffic overhead.
- ESP overhead scaled predictably with increasing topology size.
- Supporting protocol traffic remained stable across varying topology sizes.

7 Conclusion & Future Work

BGP remains vulnerable to prefix hijacking attacks. The proposed overlay management plane enhances distributed route validation without modifying the standard BGP control plane. Experimental evaluation demonstrated predictable management overhead as the topology size increased, supporting scalable and incrementally deployable inter-domain routing security. Future work will implement the automated validation logic and investigate federated learning for collaborative anomaly detection.

[1] G. He, W. Su, S. Gao, J. Yue and S. K. Das, "ROAchain: Securing Route Origin Authorization With Blockchain for Inter-Domain Routing," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1690–1705, Jun. 2021.
[2] J. Li, J. Cao, Z. Meng, R. Xie, Q. Li, Y. Yang and M. Xu, "RoLL+: Real-Time and Accurate Route Leak Locating With AS Triplet Features at Scale," IEEE/ACM Transactions on Networking, vol. 32, no. 6, pp. 5263–5278, Dec. 2024.
[3] H. Lu, Y. Tang and Y. Sun, "DRRS-BC: Decentralized Routing Registration System Based on Blockchain," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1868–1876, Dec. 2021.
[4] Z. Wu, Y. Li, X. Wang, Z. Diao, W. Fan, F. Xiao and G. Xie, "GraphBGP: BGP Anomaly Detection Based on Dynamic Graph Learning," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 9864–9877, 2025.

University of Staffordshire London

A Distributed Framework To Enhance Inter-Domain Routing Security

Binita Makanji (22010350)

Level 6 Cyber Security

First Supervisor: Dr Vahid Heydari Fami Tafreshi
Second Supervisor: Dr Maryam Shahpasand

University of Staffordshire London

Presentation Overview

1. Background and Motivation
2. Research Objectives and Deliverables
3. Literature Review Key Findings
4. Prefix Hijacking Experimentation
5. Proposed Integrated Management Plane Design
6. Prototype Implementation
7. Scalability Evaluations
8. Conclusions and Future Work

University of Staffordshire London

Background: The Border Gateway Protocol

BGP is the core protocol used for inter-domain routing across the Internet.

Exchanges reachability information between Autonomous Systems (ASes).

BGP routing decisions rely on implicit trust between neighbouring ASes.

No built-in verification of prefix ownership or AS-path authenticity.

Vulnerable to attacks such as prefix hijacking and sub-prefix hijacking.

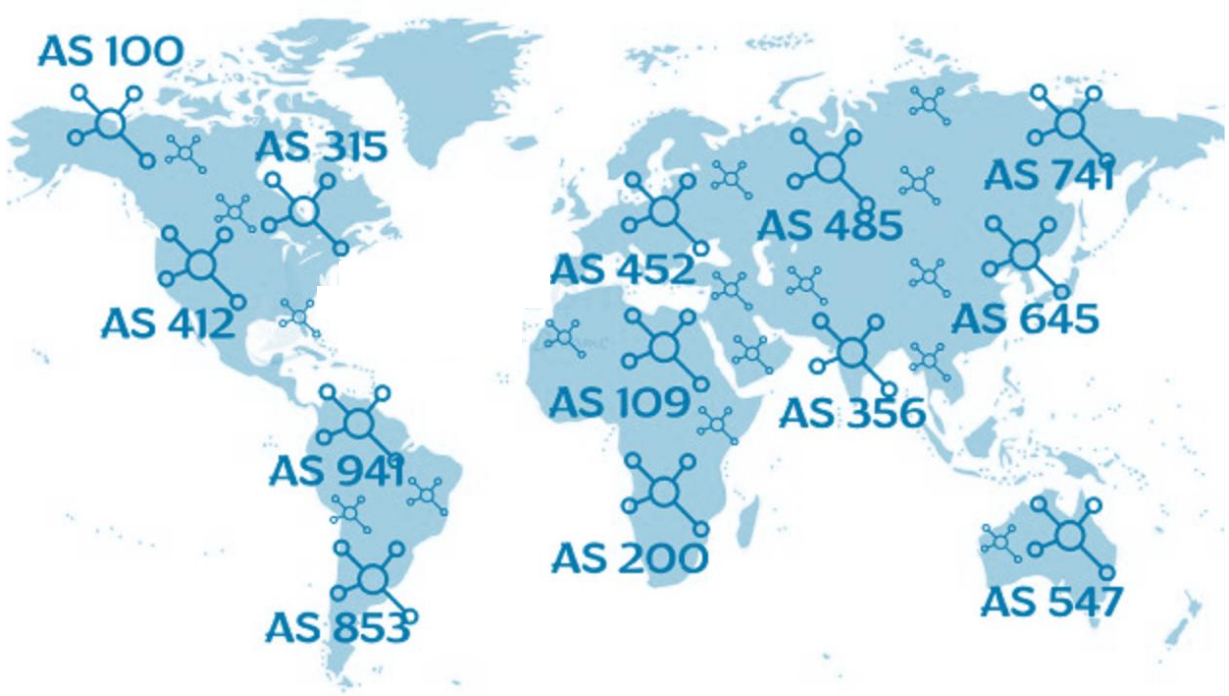


Fig 1: Global inter-domain routing between autonomous systems.

University of Staffordshire London

Research Problem & Gap

- BGP prefix hijacking accounts for approximately 96.48% of all BGP anomalies *(Wu et al., 2026).*
- Existing BGP security mechanisms improve validation, although they introduce practical deployment challenges.
- Many proposals struggle with:
  - Scalability
  - Requirement for protocol modification
  - Computational overhead
  - Reliance on centralised trust

S-BGP & BGPsec *(Kent et al., 2000)*	• High cryptographic overheads
RPKI *(Rodday et al., 2024)*	• Limited to origin validation • Restricted adoption
ML-Based Detection *(Cheng et al., 2021), (Shapira and Shavitt, 2022)*	• Reactive rather than preventative
Blockchain Approaches *(He et al., 2021), (Lu et al., 2021)*	• Scalability and consensus overhead

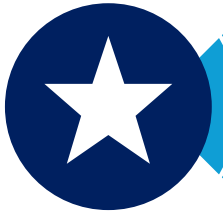
No existing approach simultaneously achieves strong routing validation, scalability, deployability, and low operational overhead.

University of Staffordshire London

Research Question & Project Aim

Can lightweight management plane validation improve BGP security scalability and deployability without modifying the control plane?

- Analyse prefix hijacking behaviour
- Evaluate management plane operational overhead
- Investigate scalability and incremental deployability



- Lightweight management plane overlay independent from BGP
- Incrementally deployable containment-focused architecture
- Experimental evaluation of scalability and operational overhead

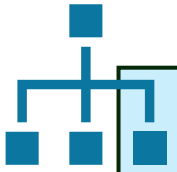
University of Staffordshire London

Project Objectives

Objective	Evaluation Method
1. Analyse prefix hijacking propagation behaviour	Controlled BGP hijacking experiments
2. Evaluate topology influence on attack success	Hijack success rate and AS connectivity analysis
3. Assess management plane scalability	10, 50, and 100 AS scalability testing
4. Measure operational overhead and evaluate deployment feasibility	Packet-level protocol and traffic analysis

University of Staffordshire London

Project Deliverables

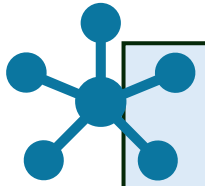


Deliverable 1: Simulated Inter-Domain Routing Environment

- Scalable 10, 50, and 100 AS topologies
- Tiered BGP architecture in GNS3

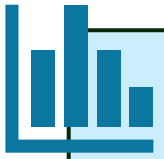
Deliverable 2: Prefix Hijacking Experimentation

- Controlled routing experiments
- Attack propagation analysis



Deliverable 3: Lightweight Management Plane Prototype

- Overlay validation architecture
- Independent from the BGP control plane



Deliverable 4: Scalability and Operational Overhead Evaluation

- Wireshark packet analysis
- ESP/IP traffic measurements across scalable AS topologies

University of Staffordshire London

Research Methods

1. Research Approach

Quantitative Experimental Methodology

- Simulation-driven evaluation
- Controlled routing experimentation

2. Experimental Environment

Simulated Inter-Domain Routing Environment

- 10, 50, and 100 AS topologies
- Controlled hijacking scenarios

3. Data Collection

Packet-Level Monitoring & Observation

- Wireshark traffic captures
- Inter-domain routing behaviour

4. Evaluation & Analysis

Experimental Performance Assessment

- Hijack success rate analysis
- Scalability testing
- Operational overhead evaluation

University of Staffordshire London

Literature Review Key Findings

1. Computationally Expensive Cryptographic Validation

- S-BGP introduces significant computational and convergence overhead *(Lu et al., 2021).*
- Complex validation increases processing and memory overhead *(Ye et al., 2026).*
- Global BGP updates can exceed 10^6 updates/sec, challenging scalability *(Wu et al., 2025).*

2. Dependence on Widespread or Global Adoption

- RPKI deployment across RIRs ranged between 1.38% to 15.11% *(He et al., 2021).*
- Universal deployment across 70,000+ ASes is impractical *(Jin et al., 2026).*
- Security effectiveness often depends on widespread inter-AS adoption *(He et al., 2021).*

3. Protocol Modifications Increase Implementation Complexity

- RPKI and ASPA deployment can be costly and time-consuming *(Wu et al., 2025).*
- Existing solutions introduce certificate management complexities *(He et al., 2021).*
- Legal and operational constraints continue to hinder adoption *(Tang et al., 2025).*

4. Large-Scale Deployment Challenges

- Internet-scale deployment remains difficult in practice *(Jin et al., 2026).*
- Technical and financial deployment costs limit adoption *(Shapira and Shavitt, 2022).*
- AS operators are hesitant to share sensitive routing information *(Li et al., 2024).*

University of Staffordshire London

Experimental Topology Design

- Topology design derived from existing BGP security experimentation research using a modified private IP addressing scheme *(Zeb and Farooq, 2011)*.
- Tiered AS hierarchy reflecting realistic inter-domain routing structure.
- Standard BGP configurations applied, with no specific local routing policies enforced.
- The foundation for controlled prefix hijacking experimentation.

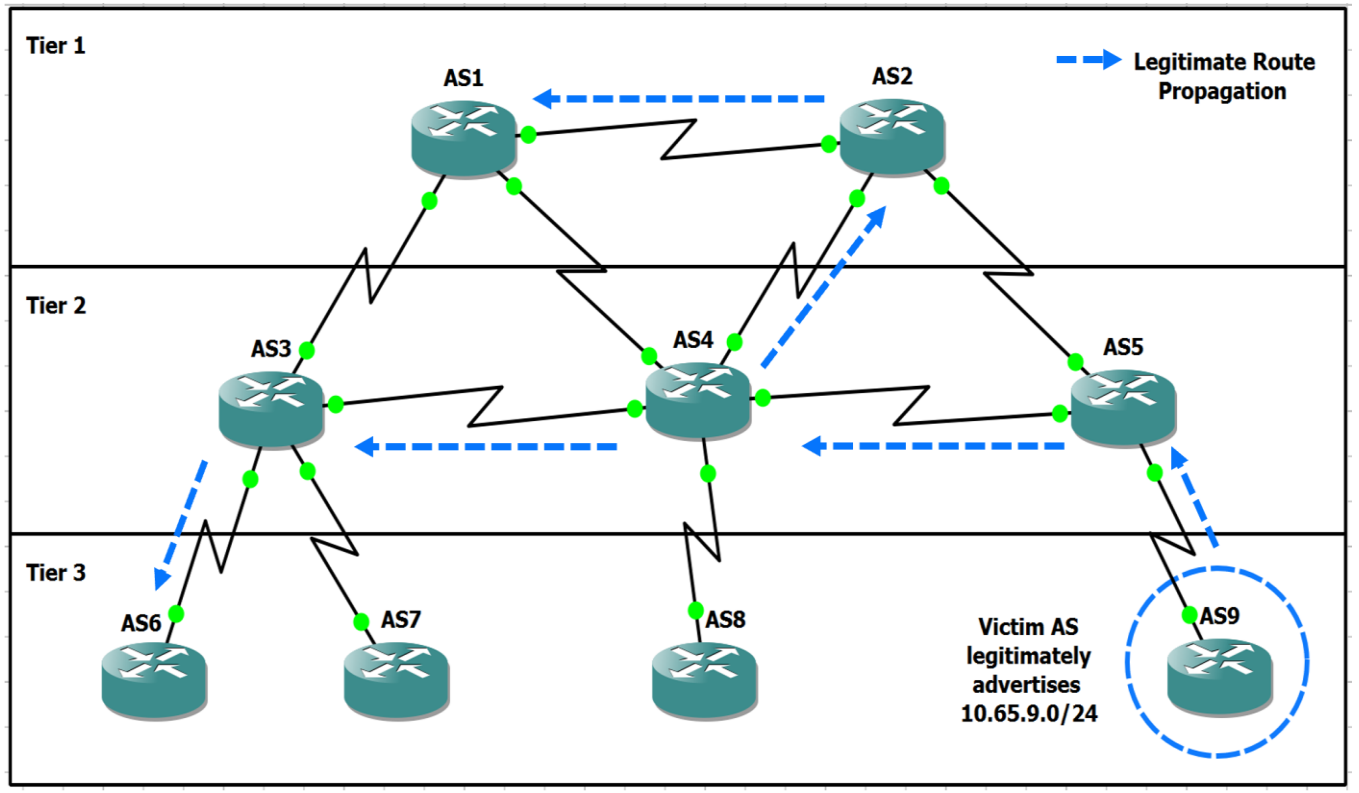


Fig 2: Three-tier 9 AS experimental topology that illustrates legitimate BGP route propagation from AS9 prior to prefix hijacking experimentation.

University of Staffordshire London

Prefix Hijacking Experimentation

- Victim: AS9 that legitimately advertises 10.65.9.0/24.
- Each AS, in turn, exhibits Byzantine routing behaviour, advertising the same IP prefix as AS9.
- Hijack success evaluated against topology position and AS connectivity.
- Controlled experimentation facilitates repeatable observation of hijack propagation patterns.

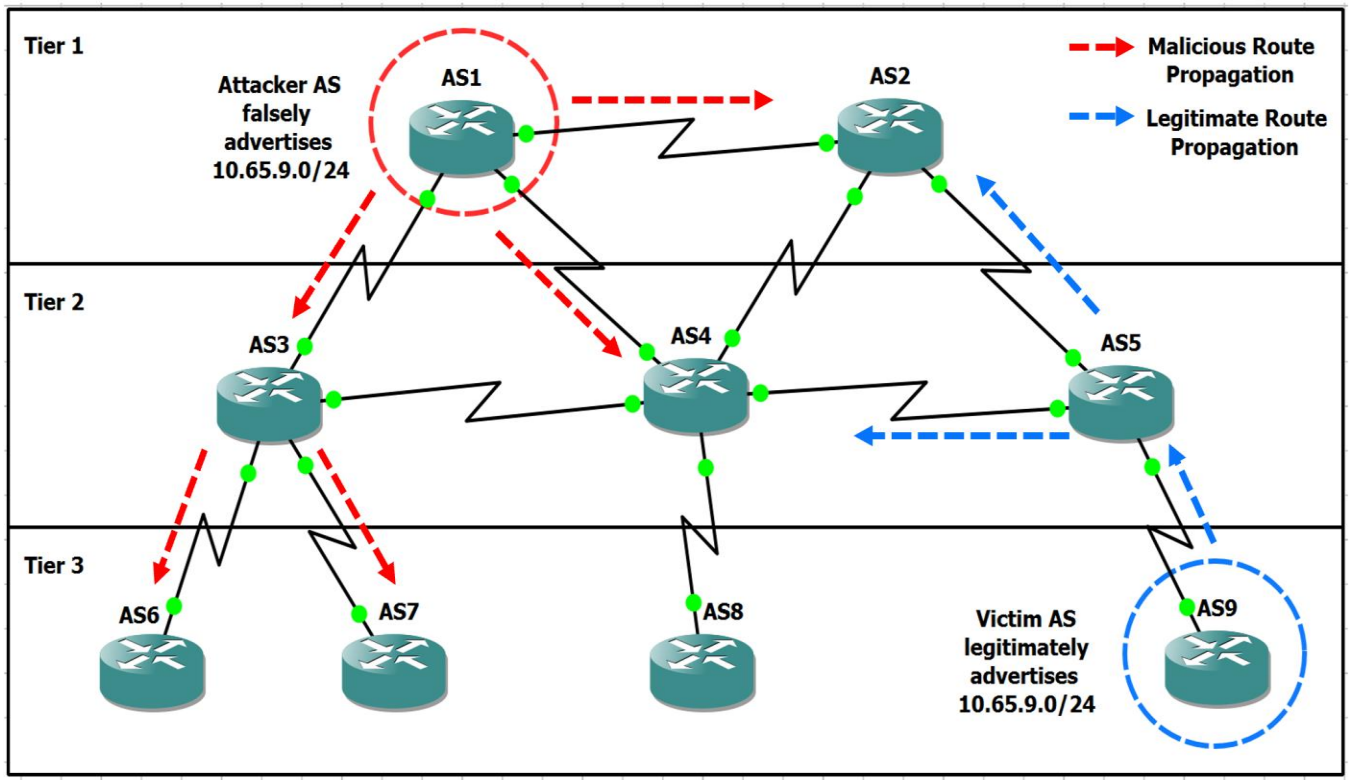
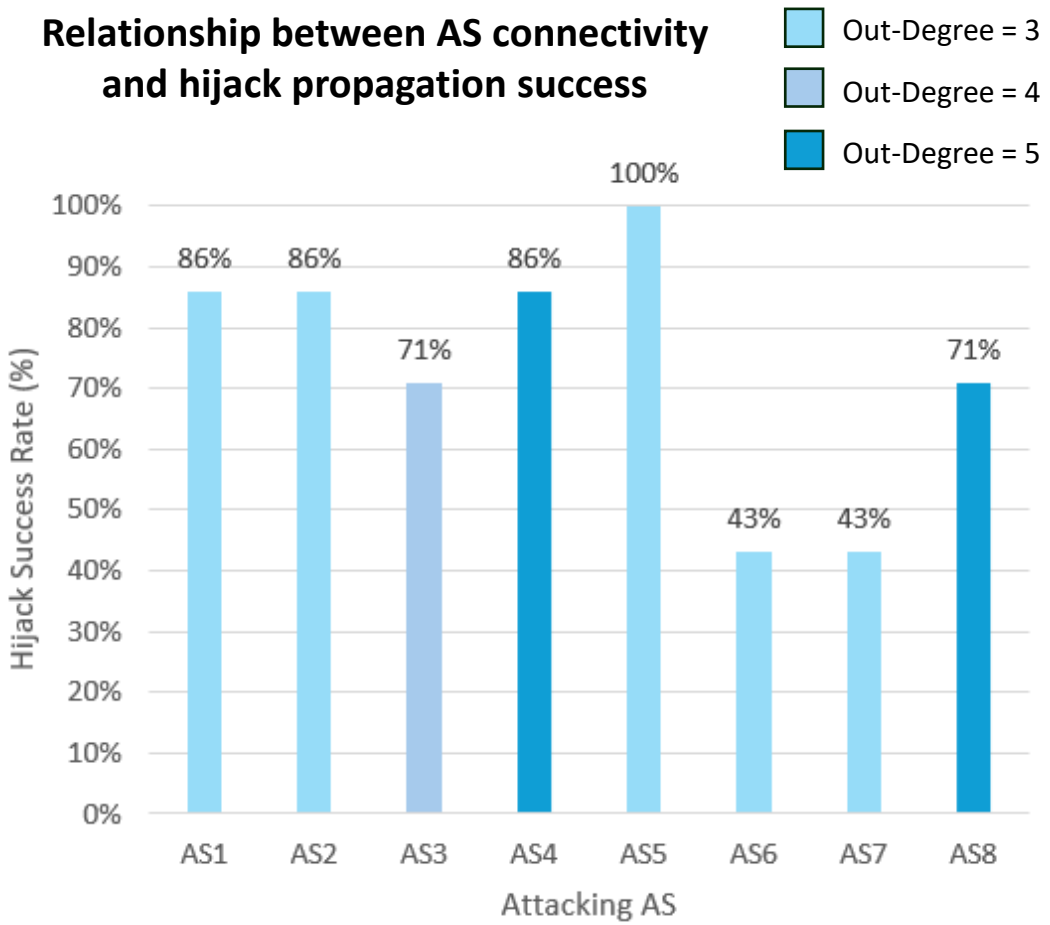


Fig 3: Prefix hijacking illustration showing malicious route propagation from AS1 competing with the legitimate advertisement from victim AS9.

University of Staffordshire London

Prefix Hijacking Results



Key Findings:

- Higher AS connectivity increased hijack propagation success.
- Topological proximity significantly influenced routing adoption behaviour.
- Tier 1 and 2 ASes exhibited greater propagation influence than edge ASes.
- Reflects how baseline BGP trust relationships enable widespread malicious route acceptance.

University of Staffordshire London

Proposed Management Plane Architecture

Architectural Contributions:

- Independent validation overlay.
- Strategic high out-degree trust anchors.
- Lightweight ESP/IP-based secure management communication.
- Incrementally deployable without BGP modification.
- Leverages existing networking and security protocols.

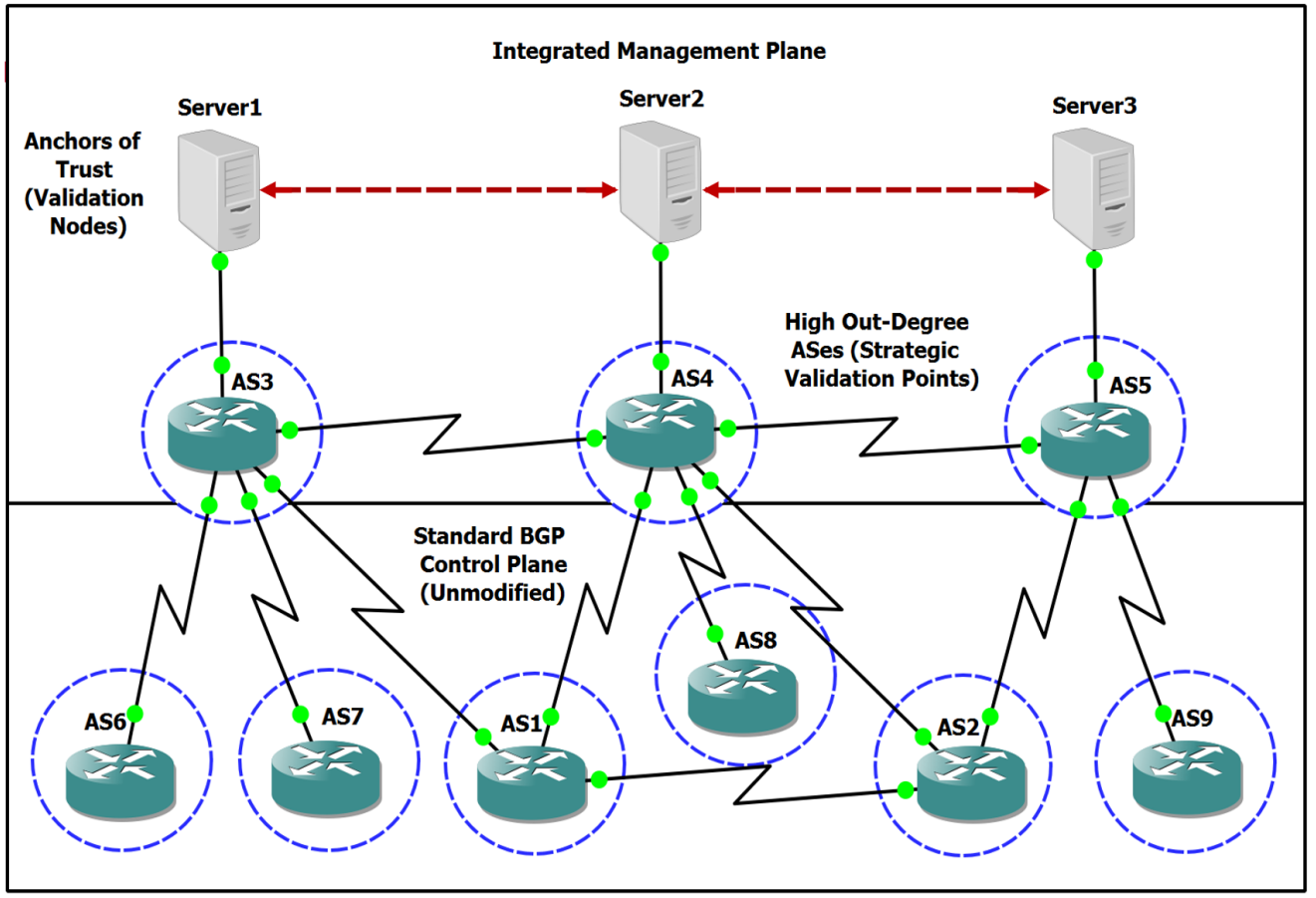


Fig 4: Design for proposed integrated management plane.

University of Staffordshire London

Validation Workflow

1. BGP UPDATE observed	New route advertisement received for a prefix.
2. Extract AS-to-IP prefix mapping	Check advertised origin AS and prefix ownership.
3. Compare with trusted ownership view	Use trusted IANA/RIR-style ownership data where available.
4. Consult trust anchors	Validation nodes confirm whether the prefix is associated with another origin.
5. Optional registry / history validation	Check authoritative registries, whois, or recent historical UPDATE records.
6. Decision made	**Valid advertisement:** allow normal propagation. **Invalid or suspicious advertisement:** lower preference, quarantine, or filter propagation.

University of Staffordshire London

Prototype Implementation

1. Routing Simulation

- GNS3-based environment
- 10, 50 and 100 AS topologies for scalability
- BGP configured across loopback-based sessions

2. Management Plane

- Trust-anchor servers connected to selected ASes
- ESP/IP-secured multicast communication overlay
- Python TCP sockets used for application-layer message exchange

3. Protocols & Technologies

- BGP, OSPF
- GDOI, ESP/IPsec
- PIM Sparse Mode

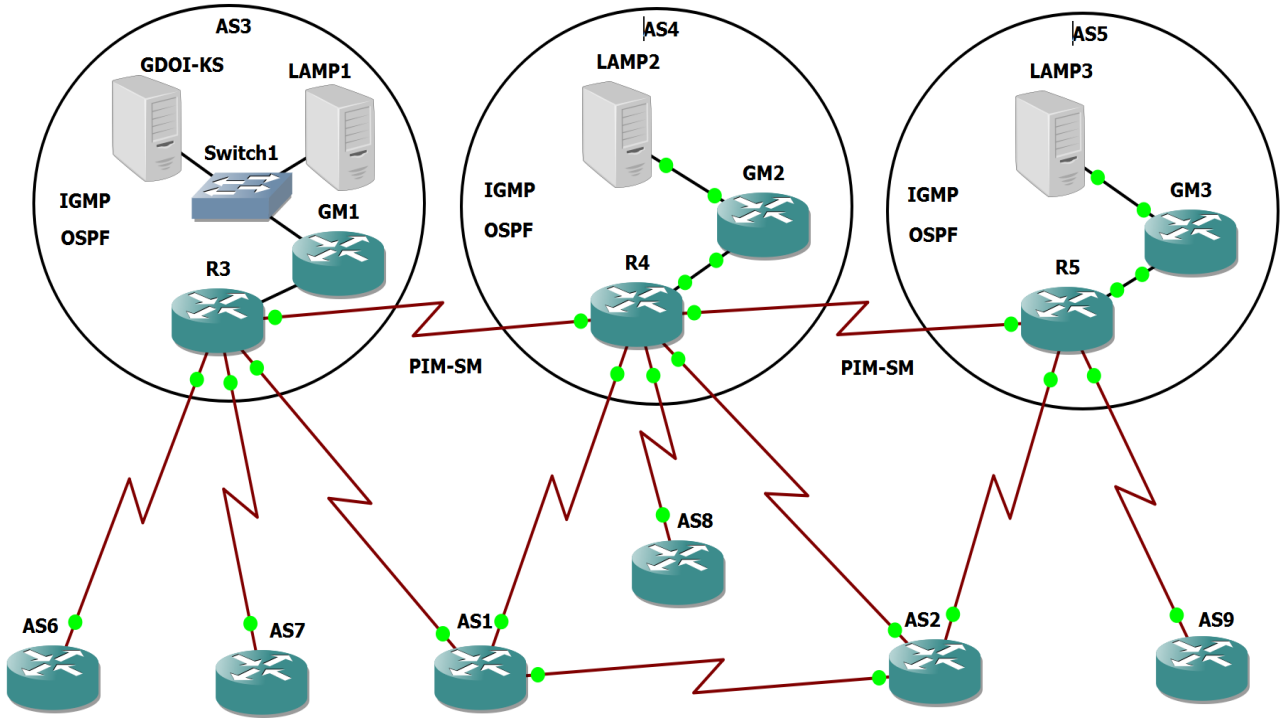


Fig 5: Prototype implemented in GNS3 showing trust anchor deployment, multicast management plane communication and secure inter-AS connectivity.

University of Staffordshire London

Prototype Validation

```
GM1#show crypto gdoi group LAMP
    Group Name               : LAMP
    Group Identity           : 1
    Rekeys received          : 0
    IPSec SA Direction       : Both
    Active Group Server      : 192.168.10.254
    Group Server list        : 192.168.10.254

    GM Reregisters in        : 231 secs
    Rekey Received           : never
    Rekeys received
         Cumulative          : 0
         After registration  : 0

 ACL Downloaded From KS 192.168.10.254:
   access-list  permit ip 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255
   access-list  permit ip 192.168.10.0 0.0.0.255 192.168.12.0 0.0.0.255
   access-list  permit ip 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255
   access-list  permit ip 192.168.11.0 0.0.0.255 192.168.12.0 0.0.0.255
   access-list  permit ip 192.168.12.0 0.0.0.255 192.168.10.0 0.0.0.255
   access-list  permit ip 192.168.12.0 0.0.0.255 192.168.11.0 0.0.0.255
   access-list  permit ip 192.168.0.0 0.0.255.255 host 239.1.2.3

TEK POLICY for the current KS-Policy ACEs Downloaded:
  GigabitEthernet1/0:
    IPsec SA:
        spi: 0xCC58E6D6(3428378326)
        transform: esp-256-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (395)
        Anti-Replay :  Disabled
```

Fig 6: GDOI group configuration and TEK policy distribution.

```
GM1#show crypto ipsec sa | include encaps|decaps
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
    #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
    #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
```

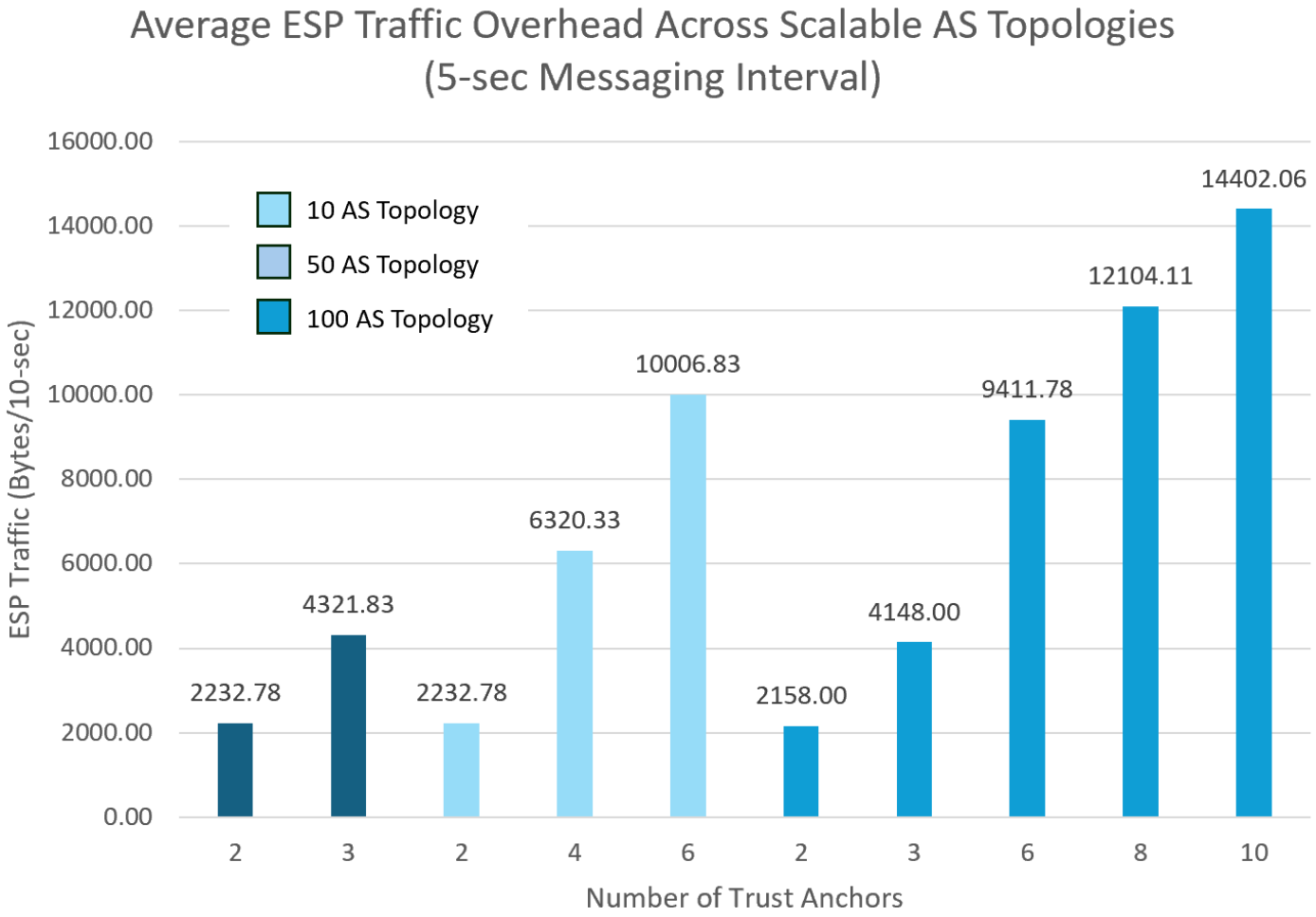
Fig 7: ESP/IPsec encapsulation and decryption packet counters.

```
ubuntu@ubuntu-Standard-PC-i440FX-PIIX-1996:~$ ./run_client.sh
Sending at Fri  1 May 09:08:47 BST 2026
Sent to 192.168.129.11:5000 -> Hello from Server1 at 2026-05-01 09:08:47.268626
Received from 192.168.129.11:5000 -> ACK from Server2 at 2026-05-01 09:08:47.538
211

Sent to 192.168.130.11:5000 -> Hello from Server1 at 2026-05-01 09:08:47.466028
Received from 192.168.130.11:5000 -> ACK from Server3 at 2026-05-01 09:08:49.075
835

Sending at Fri  1 May 09:08:57 BST 2026
Sent to 192.168.129.11:5000 -> Hello from Server1 at 2026-05-01 09:08:57.756417
Received from 192.168.129.11:5000 -> ACK from Server2 at 2026-05-01 09:08:58.001
422
```

Fig 8: TCP message exchange between trust anchors.

University of Staffordshire London

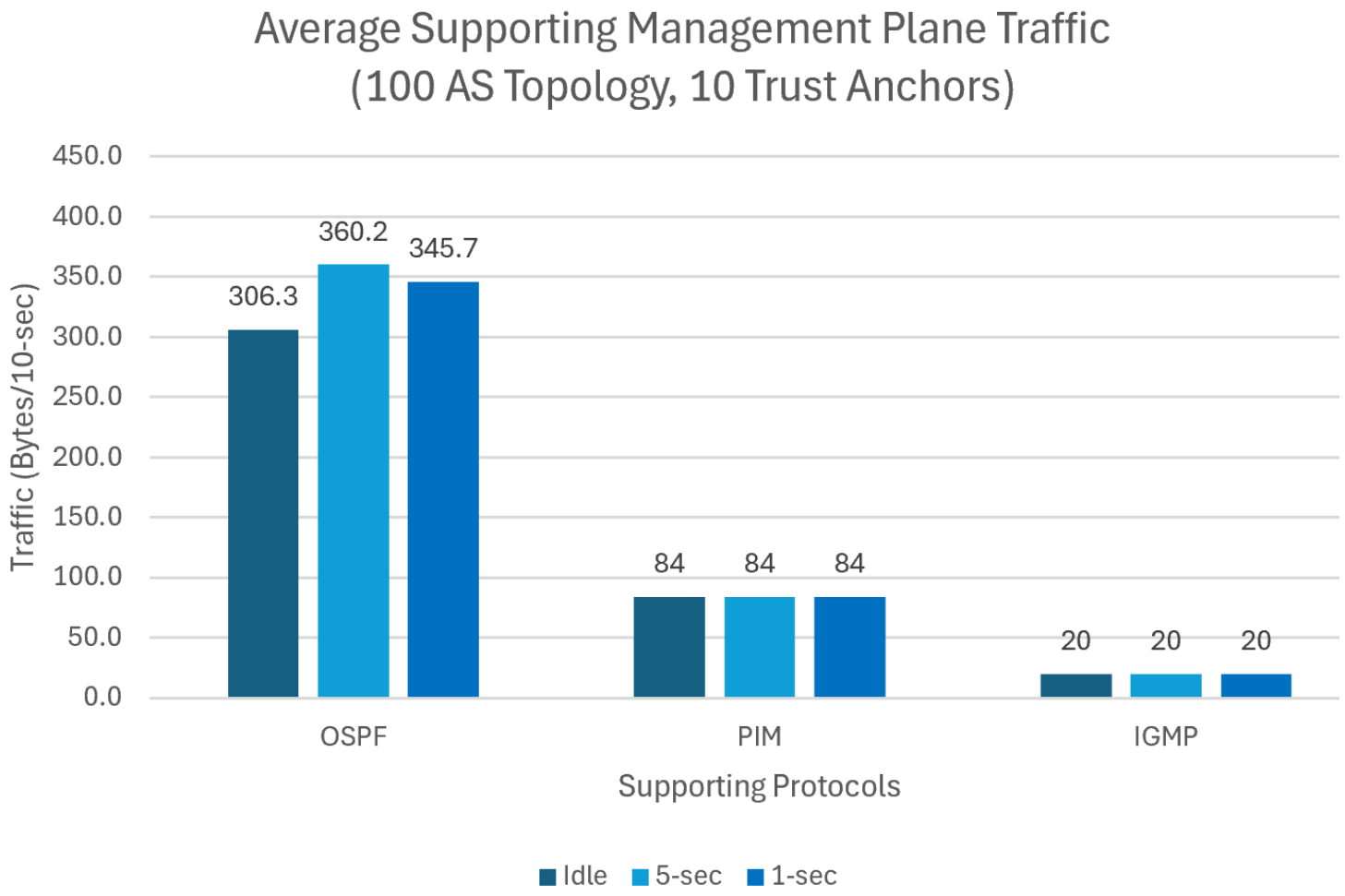
Scalability Evaluation: ESP Overhead



- ESP traffic increased with topology size and trust-anchor deployment.
- 100 AS topology exhibited the highest secure validation overhead.
- Overhead growth remained predictable across scalability scenarios.

University of Staffordshire London

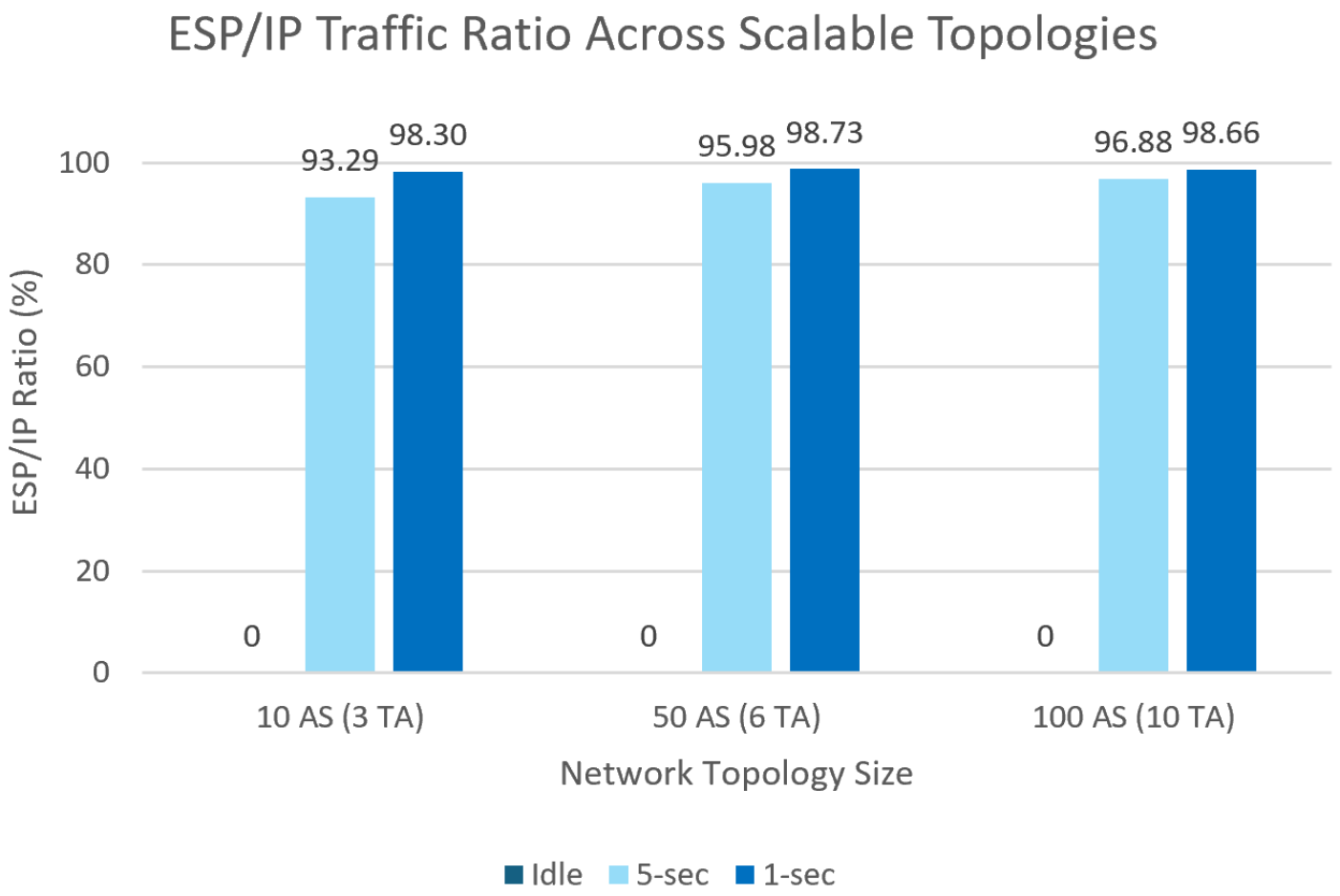
Scalability Evaluation: Supporting Protocol Traffic



- OSPF generated the highest supporting protocol traffic.
- PIM and IGMP introduced comparatively minimal overhead.
- Supporting protocol traffic remained stable across varying messaging intervals and topology sizes.

University of Staffordshire London

Scalability Evaluation: ESP/IP Traffic Ratio



- ESP traffic accounted for over 93-98% of management plane traffic.
- Higher messaging frequencies increased secure messaging dominance.
- Supporting protocols contributed only a small proportion of total traffic.

University of Staffordshire London

Conclusions & Future Work

- BGP remains vulnerable due to its trust-based design.
- Existing security approaches face deployment and scalability challenges.
- Proposed management plane enables secure validation without modifying BGP.
- Scalability evaluations demonstrated stable overlay operation and predictable encrypted communication overhead.
- Supporting protocols introduced minimal additional management plane traffic.

Future Work

- ➢ Implement complete automated route validation logic.
- ➢ Investigate dynamic trust-anchor selection mechanisms.
- ➢ Explore federated learning-based anomaly detection.

University of Staffordshire London

References

- Cheng, M., Li, Q., Lu, J., Liu, W. and Wang, J. (2021). Multi-Scale LSTM Model for BGP Anomaly Classification. IEEE Transactions on Services Computing, 14(3), pp.765–778.
- He, G., Su, W., Gao, S., Yue, J. and Das, S.K. (2021). ROAchain: Securing Route Origin Authorization With Blockchain for Inter-Domain Routing. IEEE Transactions on Network and Service Management, 18(2), pp.1690–1705.
- Jin, Z., Shi, X., Wang, Z., Zhao, K., Wang, Z. and Yin, X. (2026). VBGP: Flexible Multipath Selection for the Inter-Domain Routing Evolution. IEEE Transactions on Networking, 34, pp.1393–1407.
- Kent, S., Lynn, C. and Seo, K. (2000). Secure Border Gateway Protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 18(4), pp.582–592.
- Li, J., Cao, J., Meng, Z., Xie, R., Li, Q., Yang, Y. and Xu, M. (2024). RoLL+: Real-Time and Accurate Route Leak Locating With AS Triplet Features at Scale. IEEE/ACM Transactions on Networking, 32(6), pp.5263–5278.
- Lu, H., Tang, Y. and Sun, Y. (2021). DRRS-BC: Decentralized Routing Registration System Based on Blockchain. IEEE/CAA Journal of Automatica Sinica, 8(12), pp.1868–1876.
- Rodday, N., Cunha, Í., Bush, R., Katz-Bassett, E., Rodosek, G.D., Schmidt, T.C. and Wählisch, M. (2024). The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects. IEEE Transactions on Network and Service Management, 21(2), pp.2353–2373.
- Sermpezis, P., Kotronis, V., Gigis, P., Dimitropoulos, X., Cicalese, D., King, A. and Dainotti, A. (2018). ARTEMIS: Neutralizing BGP Hijacking Within a Minute. IEEE/ACM Transactions on Networking, 26(6), pp.2471–2486.
- Shapira, T. and Shavitt, Y. (2022). AP2Vec: an Unsupervised Approach for BGP Hijacking Detection. IEEE Transactions on Network and Service Management, pp.1–1.
- Tang, J., Sun, G., Chen, J., Zhang, G., Jiang, Q., Li, Y., Zhang, G., Liu, J., Wang, H. and Liang, R. (2024). Towards Enhancing Inter-Domain Routing Security with Visualization and Visual Analytics. IEEE Transactions on Big Data, pp.1–19.
- Wu, Z., Li, Y., Wang, X., Diao, Z., Fan, W., Xiao, F. and Xie, G. (2025). GraphBGP: BGP Anomaly Detection Based on Dynamic Graph Learning. IEEE Transactions on Information Forensics and Security, 20, pp.9864–9877.
- Wu, Z., Liu, S., Xie, R., Gao, M., Wu, Z., Han, L., Chen, X. and Xiao, F. (2026). CloudTrie: An Uncertainty-Quantified Anomaly Detection Framework for Prefix Hijacking With Multisource Fusion. IEEE Transactions on Instrumentation and Measurement, 75, pp.1–14.
- Ye, J., Mo, L., Fei, G., Zhou, Y., Xian, M., Zhai, X., Hu, G. and Liang, M. (2026). TopoKG: Infer Internet AS-Level Topology From Global Perspective. IEEE Transactions on Network and Service Management, 23, pp.2006–2023.
- Zeb, A. and Farooq, M. (2011) 'BGP Threats and Practical Security.' MSc dissertation. Sweden: Chalmers University of Technology.

University of Staffordshire London

Thank you for taking the time to read about my project!