A Software-Defined Networking approach to enhance BGP security

Regivaldo Costa
Prof. Fernando Ramos (Advisor)

LaSIGE, Faculdade de Ciências
Universidade de Lisboa, Portugal

NavTalk, June/2017

Outline

Objective & Goals

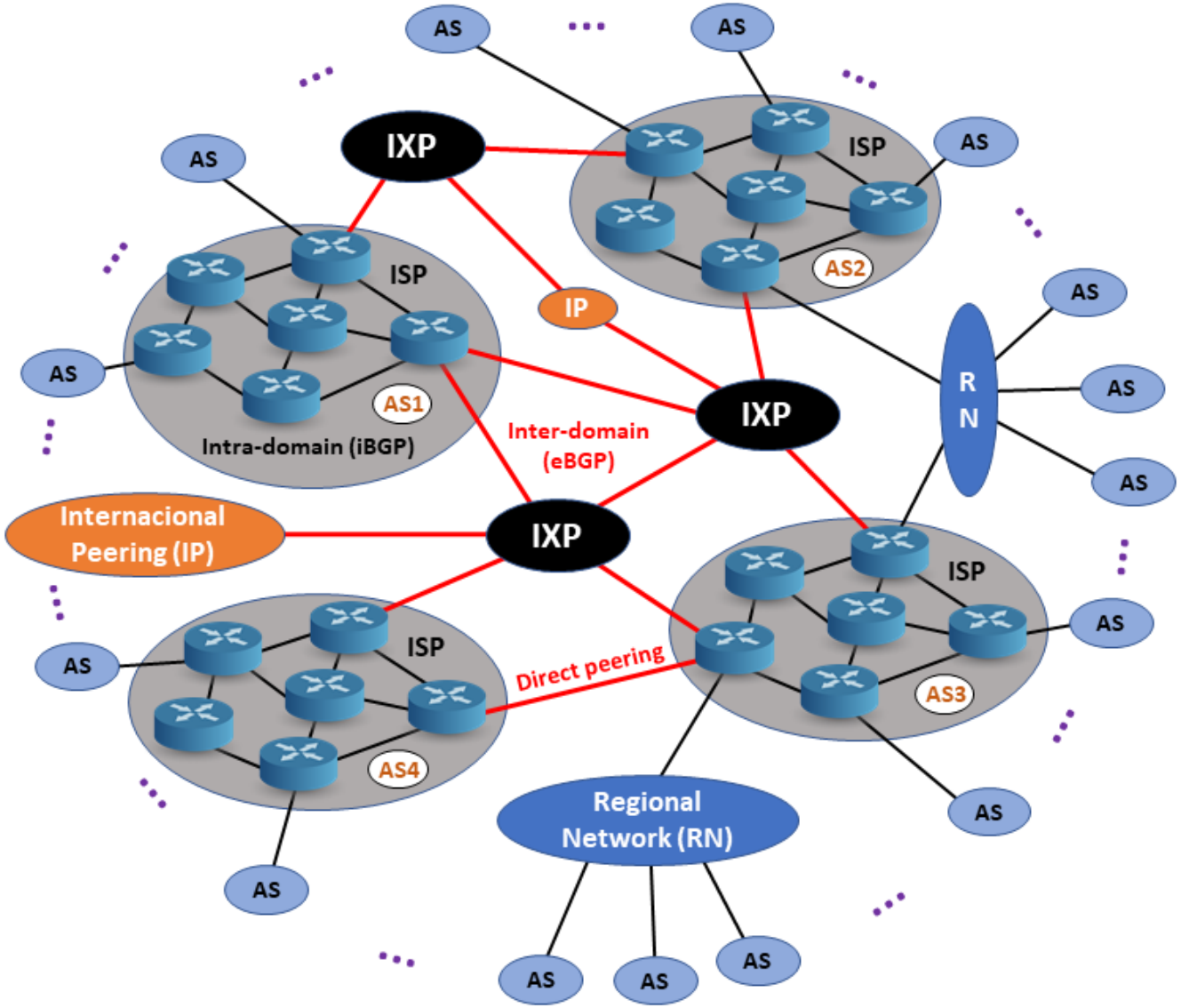
- Objective of this work: design, implementation and evaluation of an SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security.
- Our goals:
  - Provide Origin Authentication and Path Validation to avoid prefix hijacks and other fake BGP announcements.
  - Promote deployment.

Motivation (BGP Security)

- Some solutions to improve BGP security having been proposed in the past two decades [ProcIEEE'10], but the most effective security solutions have not seen widespread deployment [SIGCOMM'14]:
  - Proposed solutions require changes to BGP.
  - Proposed solutions represent a high computational burden to routers.
  - Network operators are not given the right incentives to migrate to a secure solution, and have concerns about the disclosure of business relationships considered private.

Background - Internet infrastructure/routing

Internet interconnection



Background (Internet infrastructure/routing)

IXPs around the world: **545 in May/2017** (source: peeringdb.com)

Continental Region	# IXPs	Continental Region	# IXPs
Europe	186	Africa	38
North Americ	131	Australia/New Zealand	27
Asia Pacific	92	Middle East	9
Central/South America	62		

Background (Internet infrastructure/routing)

IXPs around the world: **545 in May/2017** (source: peeringdb.com)

Continental Region	# IXPs	Continental Region	# IXPs
Europe	186	Africa	38
North Americ	131	Australia/New Zealand	27
Asia Pacific	92	Middle East	9
Central/South America	62		

Some IXPs are very large

Background (Internet infrastructure/routing)

IXPs around the world: **545 in May/2017** (source: peeringdb.com)

Continental Region	# IXPs	Continental Region	# IXPs
Europe	186	Africa	38
North Americ	131	Australia/New Zealand	27
Asia Pacific	92	Middle East	9
Central/South America	62		

Some IXPs are very large

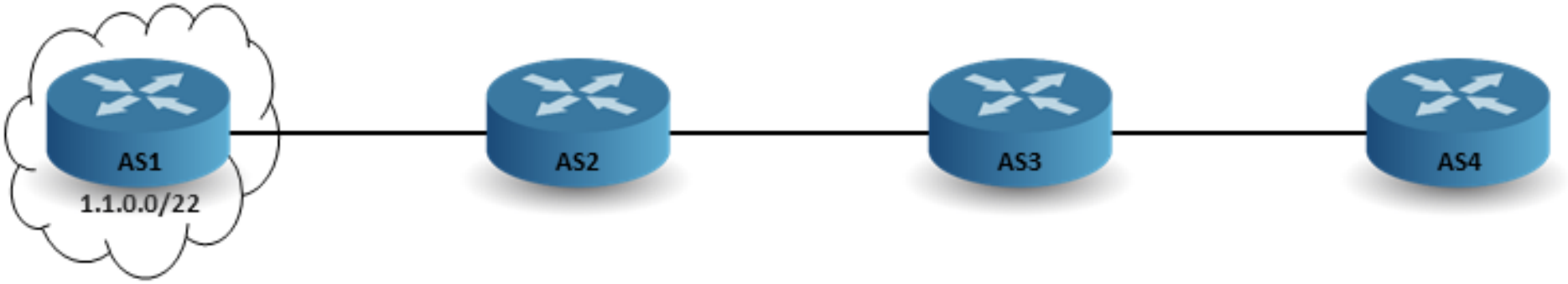
- DE-CIX has more than 600 connected networks.
- AMS-IX has more than 700 connected networks.
- CIX and AMS has each one a network traffic around 5 terabits/s.

Background (Internet infrastructure/routing))

IXPs visual distribution around the world (source: telegeography.com)

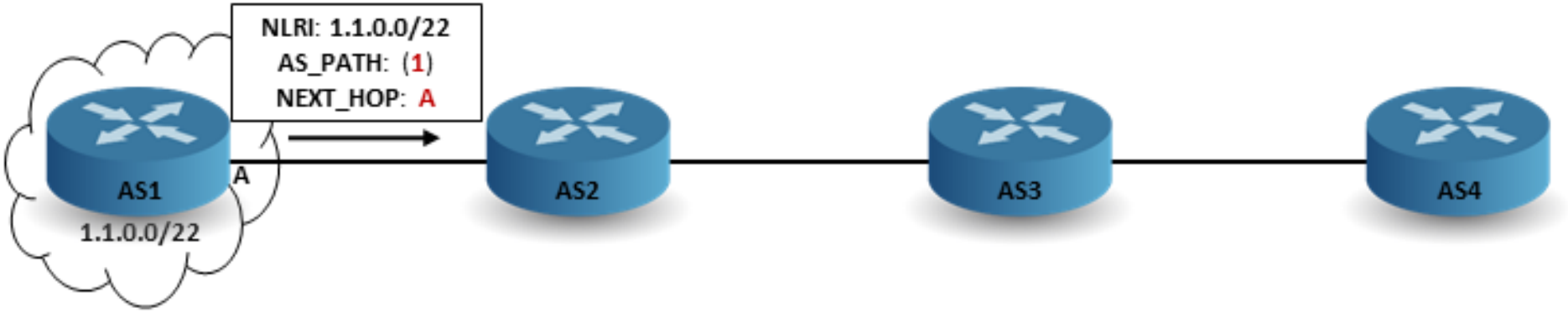
Background (BGP route announcement)

Route propagation along the path (**UPDATE** message)



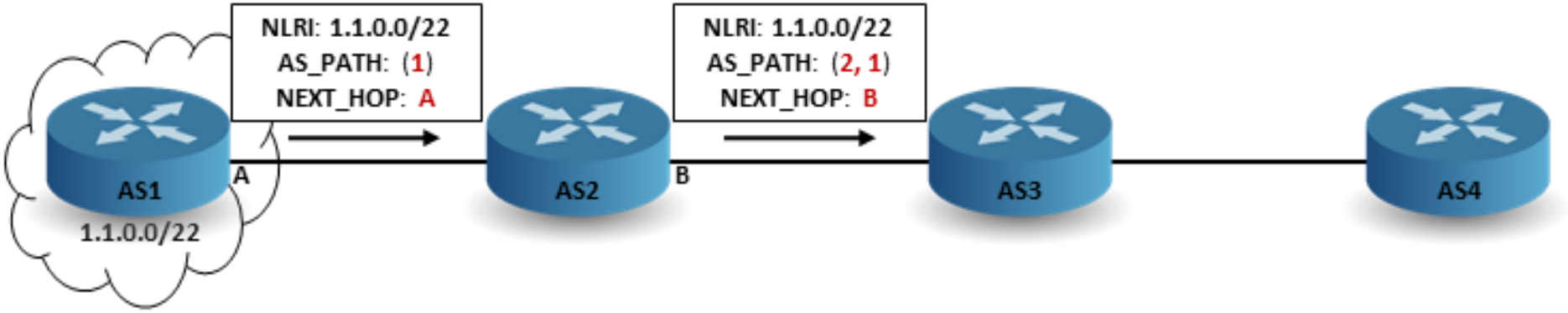
Background (BGP route announcement)

Route propagation along the path (**UPDATE** message)

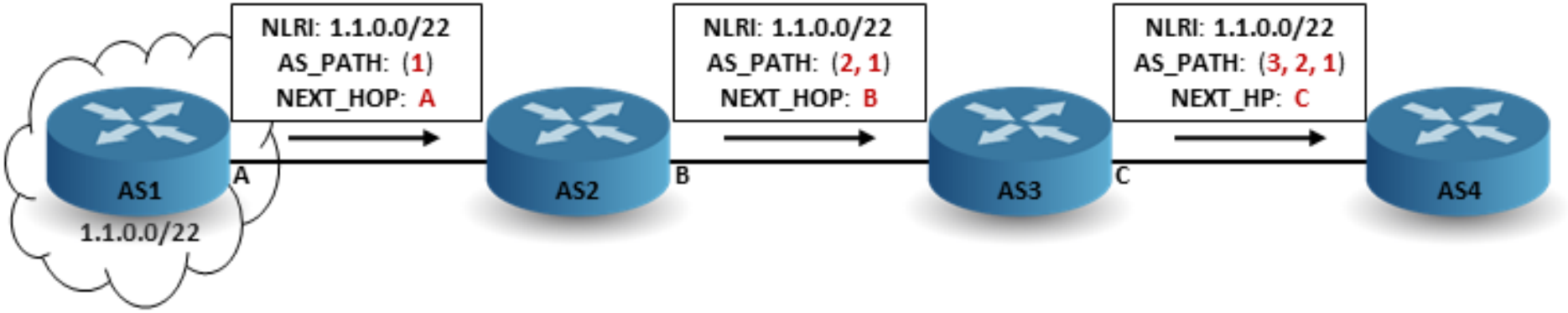


Background (BGP route announcement)

Route propagation along the path (**UPDATE** message)

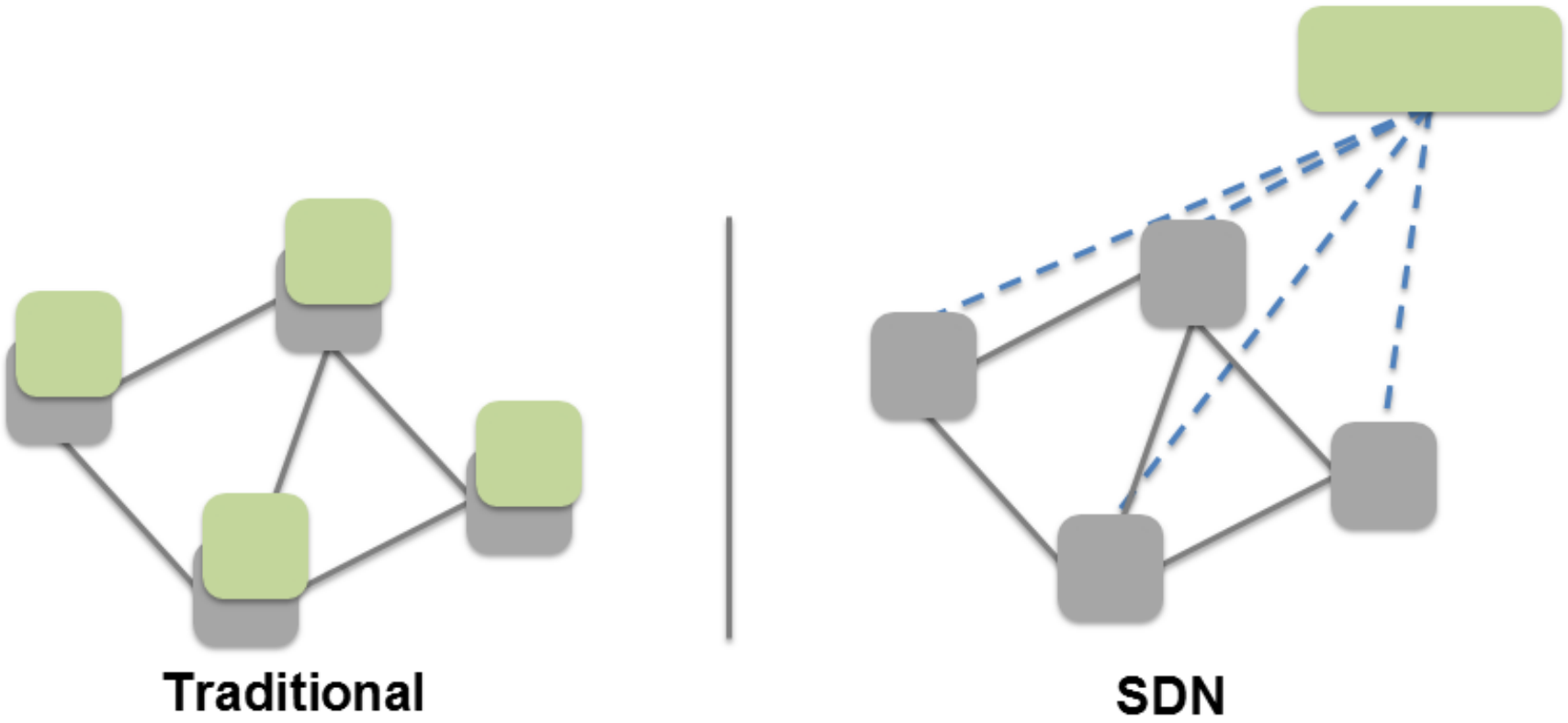


Route propagation along the path (**UPDATE** message)

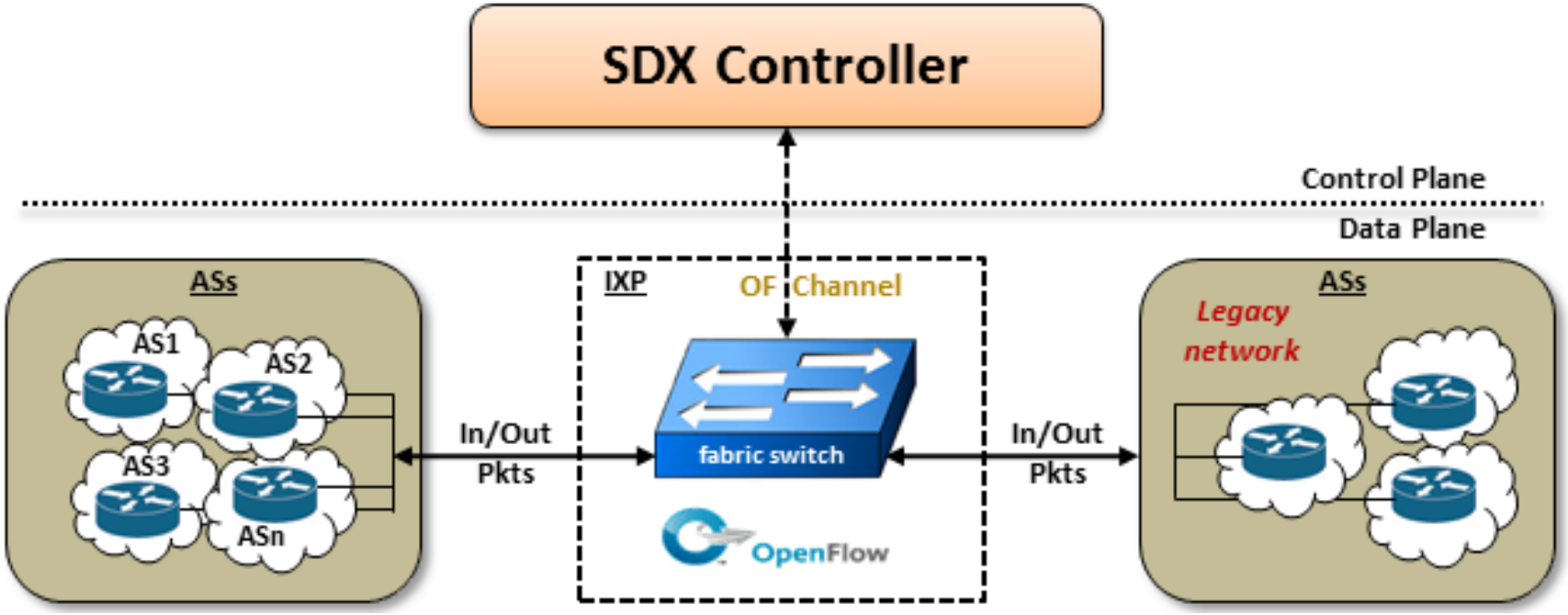


Background - Software-Defined Networking

Traditional and SDN network architecture

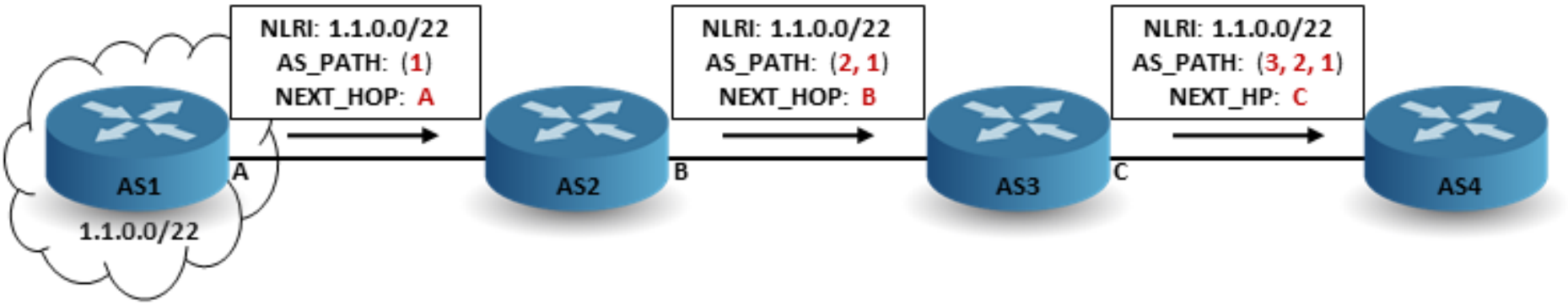


Software-Defined Exchange [SIGCOMM'14][NSDI'16]

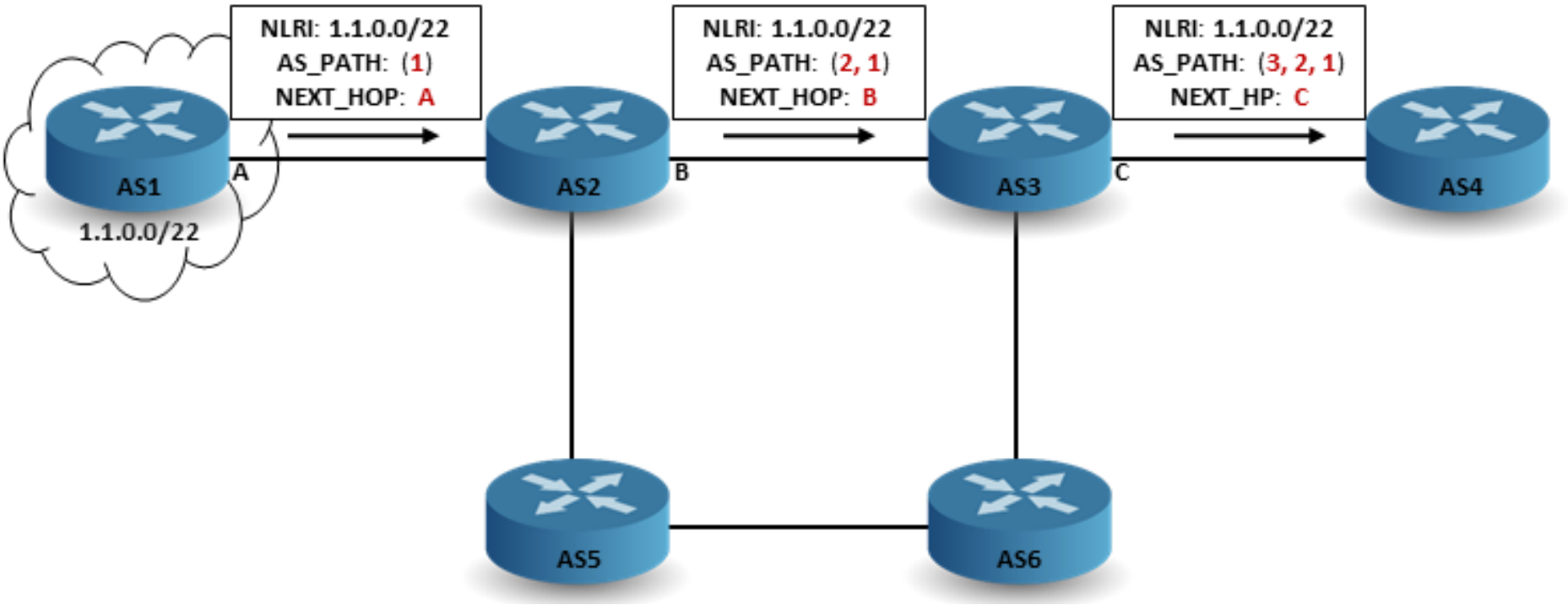


BGP Security Problems - Prefix Hijacking

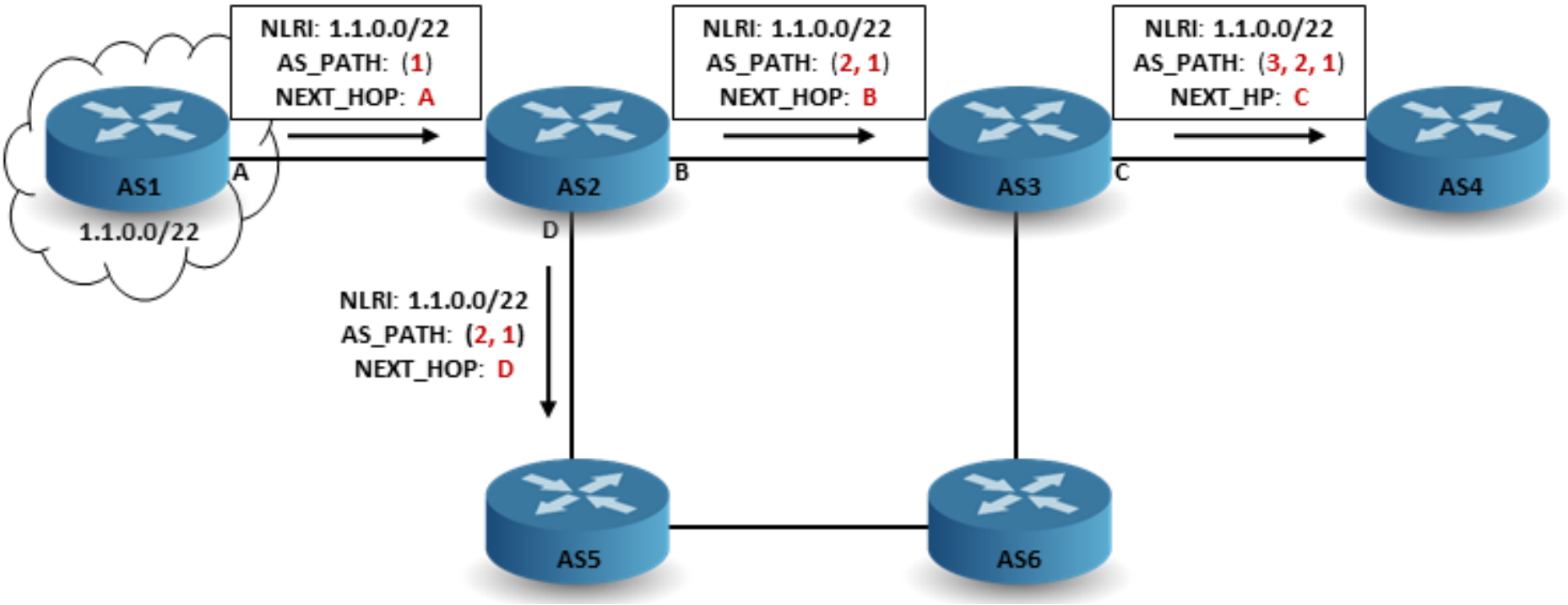
Prefix/Sub Prefix Hijacking



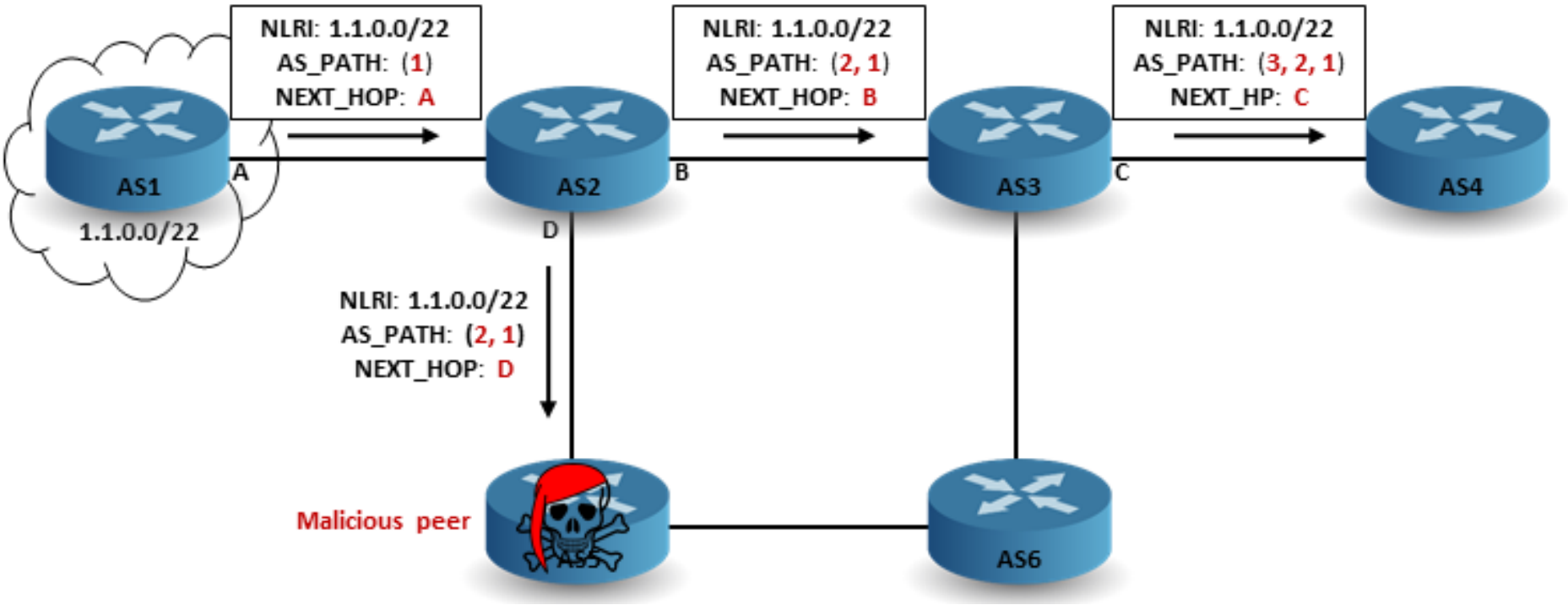
Prefix/Sub Prefix Hijacking



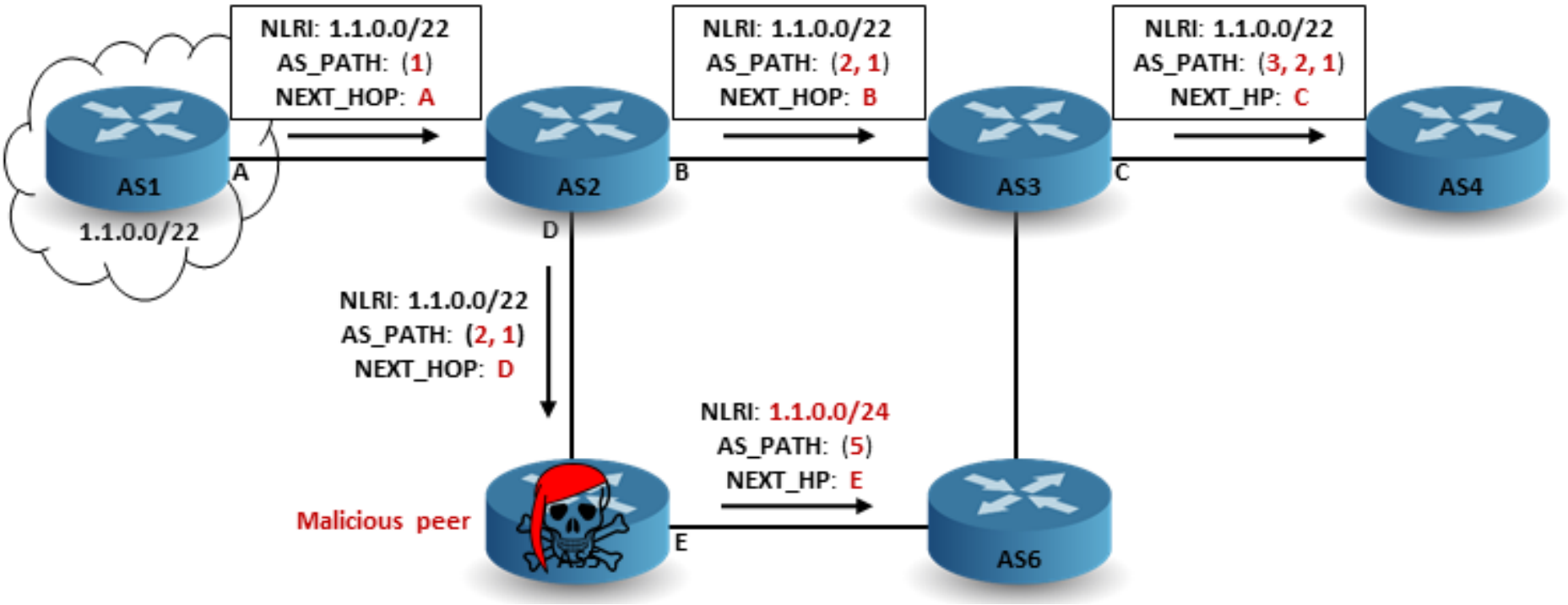
Prefix/Sub Prefix Hijacking



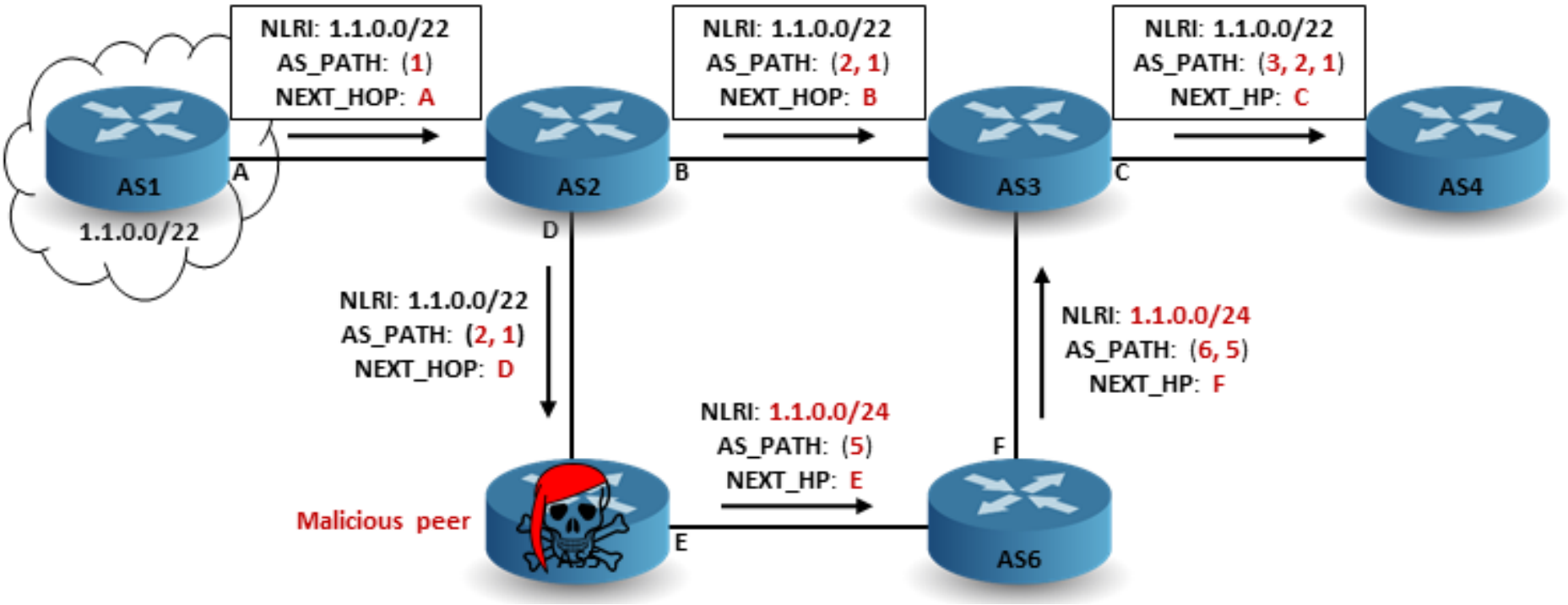
Prefix/Sub Prefix Hijacking



Prefix/Sub Prefix Hijacking

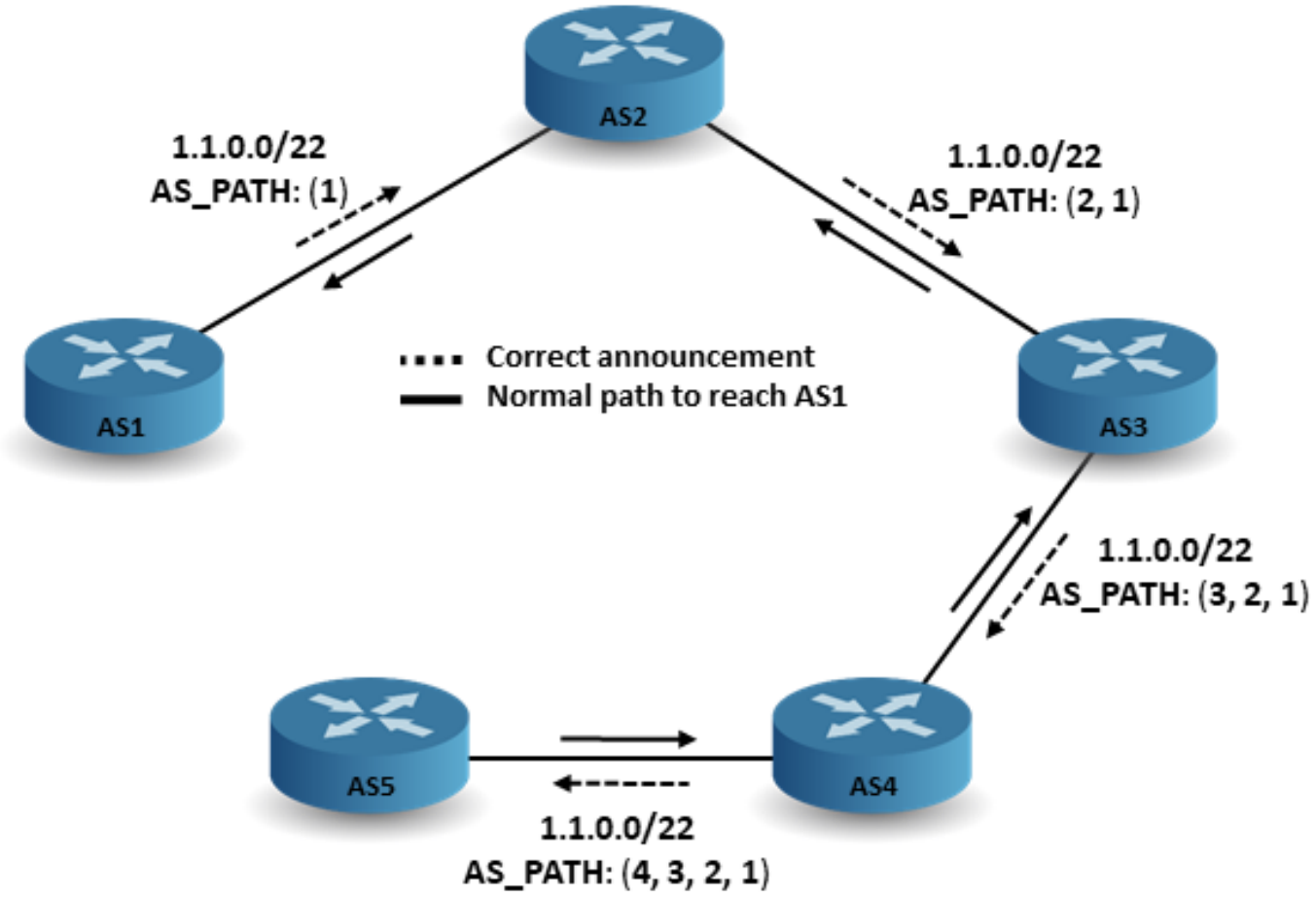


Prefix/Sub Prefix Hijacking

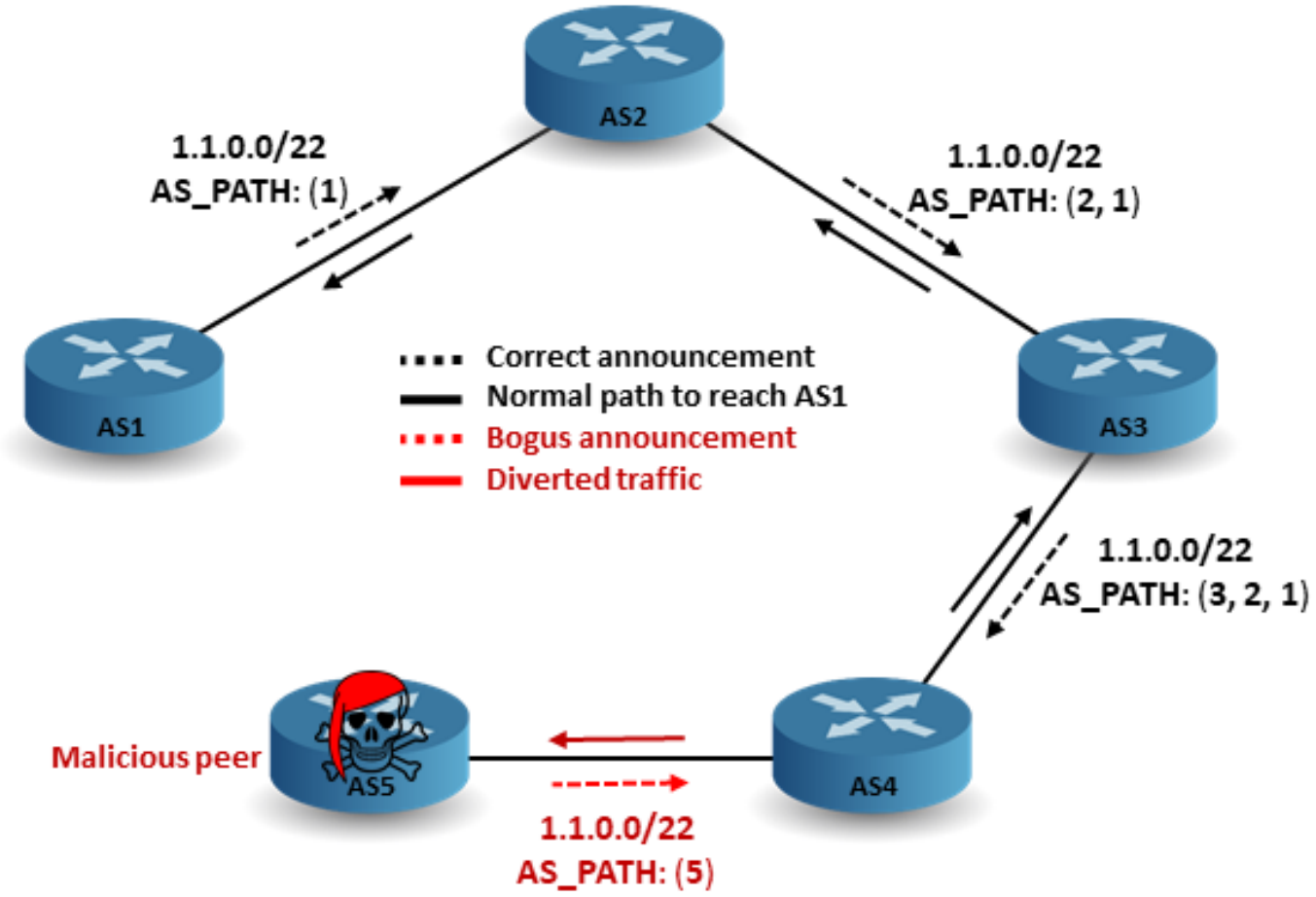


BGP Securiy Problemas - Path manipulation

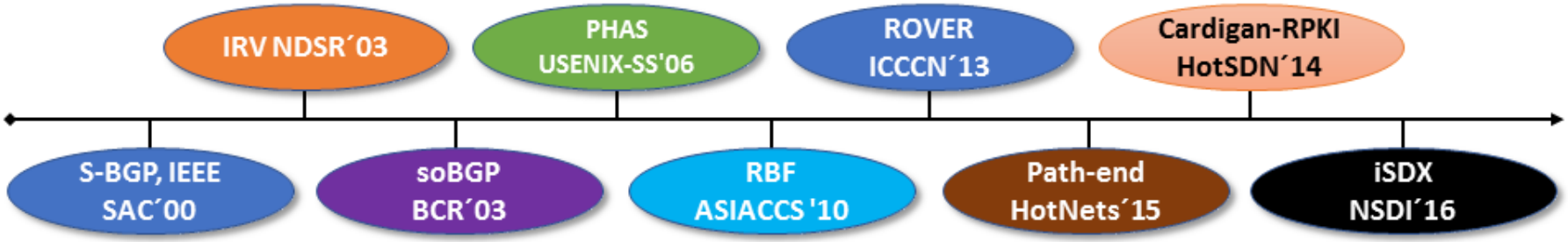
Path manipulation (path-shortening)



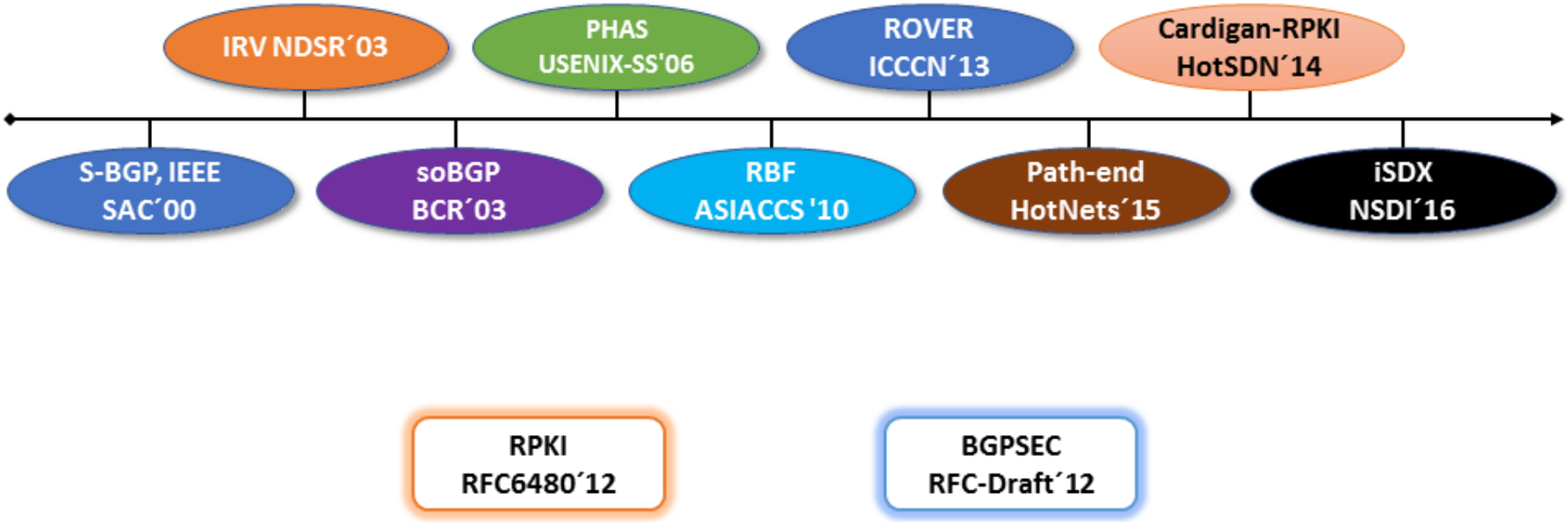
Path manipulation (path-shortening)



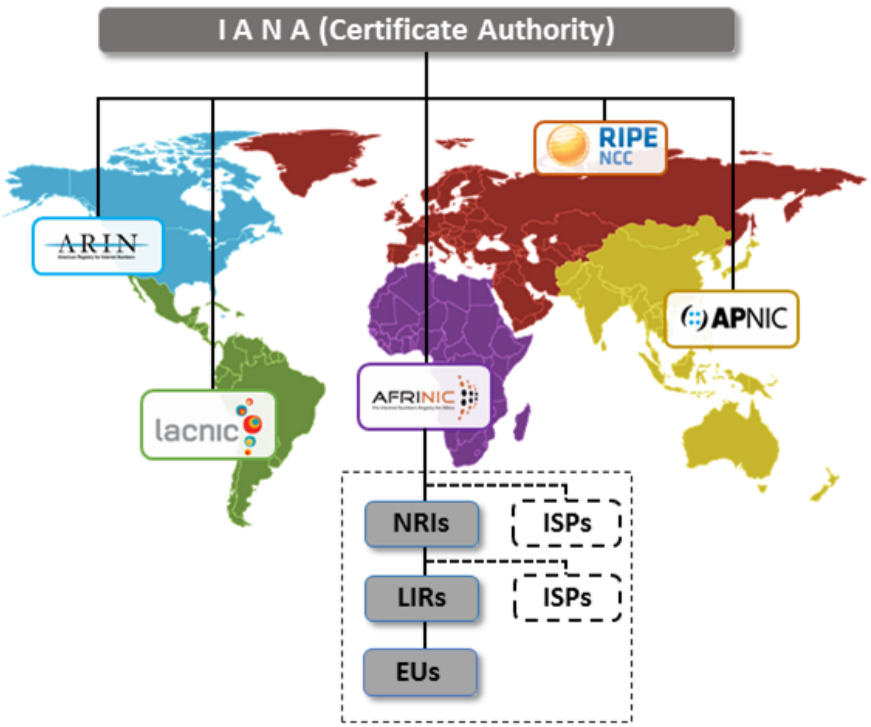
Related work

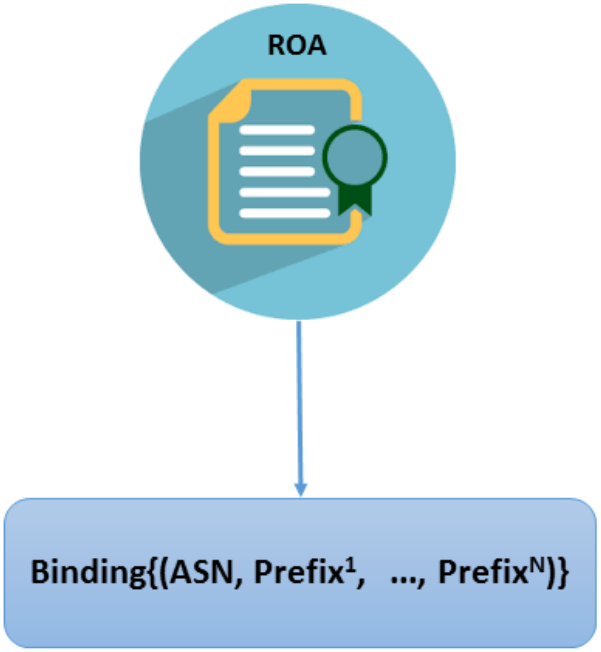


Related work



Related work: Origin Authentication (RPKI) [RFC6480]





- A trusted DB is used to guarantee that an **AS cannot falsely claim** to be the rightful owner for an IP prefix (Route Origin Authorization - **ROA**) [RFC6482].
- The RPKI provides a trusted mapping - a **whitelist** - from allocated prefixes to ASes by establishing a cryptographic hierarchy of authorities.

Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons**:

Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons**:
  - (**+**) Offline cryptography.

Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons**:
  - (**+**) Offline cryptography.
  - (**+**) Low computational burden to routers.

Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons**:
  - (**+**) Offline cryptography.
  - (**+**) Low computational burden to routers.
  - (**+**) No changes to BGP.

Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons**:
  - (**+**) Offline cryptography.
  - (**+**) Low computational burden to routers.
  - (**+**) No changes to BGP.
  - (**+**) Protects from BGP hijacks.

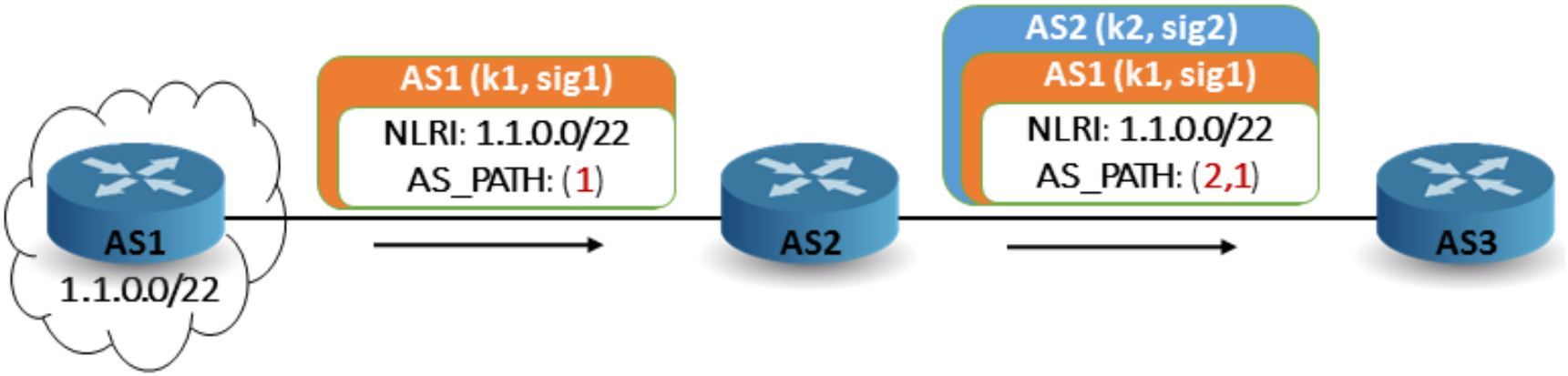
Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons**:
  - (+) Offline cryptography.
  - (+) Low computational burden to routers.
  - (+) No changes to BGP.
  - (+) Protects from BGP hijacks.
  - (-) Does not avoid path manipulation.

Related work: Origin Authentication (RPKI) [RFC6480]

- **Pros & Cons**:
  - (+) Offline cryptography.
  - (+) Low computational burden to routers.
  - (+) No changes to BGP.
  - (+) Protects from BGP hijacks.
  - (-) Does not avoid path manipulation.
  - (-) RPKI coverage is small.

Related work: BGP securicy extension (BGPSEC) [RFC-Draft]



- In addition to origin authentication, it uses cryptographically-signed routing announcements to **provide path verification**.
- It comprises a set of nested signature which need to be verified.

Related work: BGP securicy extension (BGPSEC) [RFC-Draft]

- **Pros & Cons**:

Related work: BGP securicy extension (BGPSEC) [RFC-Draft]

- **Pros & Cons**:
  - (**+**) Protects from BGP hijacks.

Related work: BGP securicy extension (BGPSEC) [RFC-Draft]

- **Pros & Cons**:
  - (**+**) Protects from BGP hijacks.
  - (**+**) Protects from path manipulation.

Related work: BGP securicy extension (BGPSEC) [RFC-Draft]

- **Pros & Cons**:
  - (**+**) Protects from BGP hijacks.
  - (**+**) Protects from path manipulation.
  - (**-**) High computational burden to routers.

Related work: BGP securicy extension (BGPSEC) [RFC-Draft]

- **Pros & Cons**:
  - (+) Protects from BGP hijacks.
  - (+) Protects from path manipulation.
  - (-) High computational burden to routers.
  - (-) Requires changes to BGP.

Related work: BGP securicy extension (BGPSEC) [RFC-Draft]

- **Pros & Cons**:
  - (+) Protects from BGP hijacks.
  - (+) Protects from path manipulation.
  - (-) High computational burden to routers.
  - (-) Requires changes to BGP.
  - (-) Benefits only with large deployment.

Proposal - Design requirements

Proposal - design requirements

We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.

Proposal - design requirements

We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.

Proposal - design requirements

We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.
- Don't require changes to BGP.

Proposal - design requirements

We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

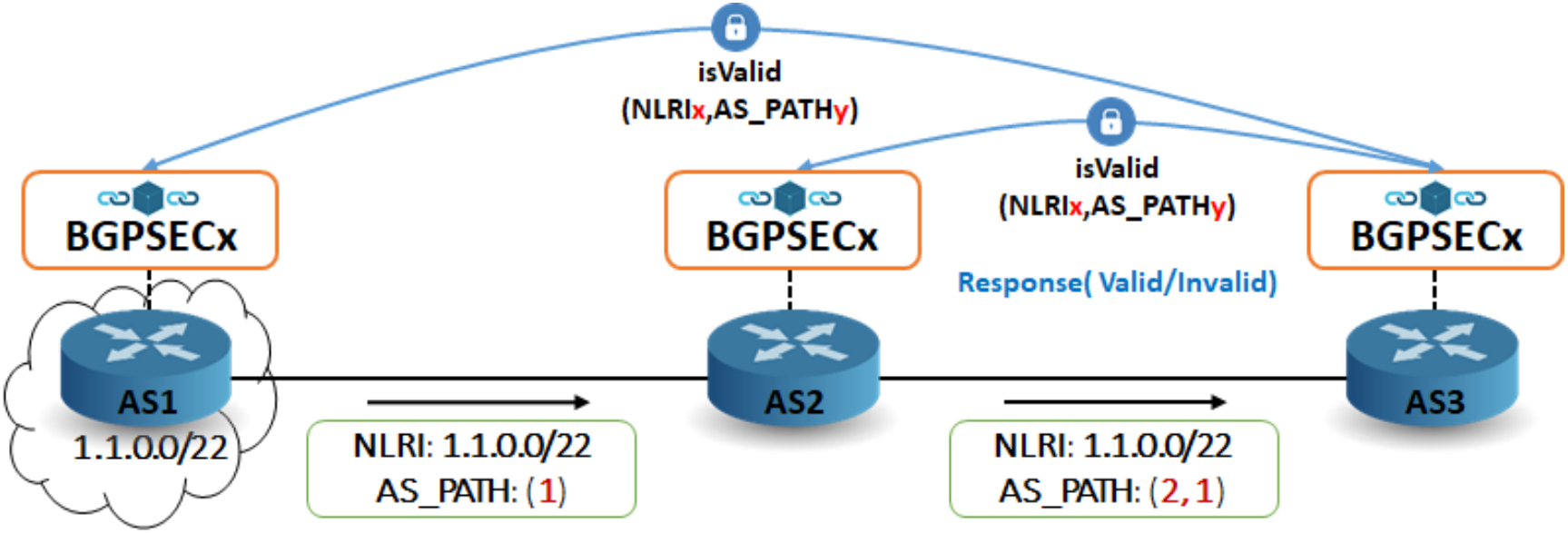
- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.
- Don't require changes to BGP.
- Remove computational burden from routers.

Proposal - design requirements

We proposed a SDN-based architecture targeting Internet Exchange Points (IXPs) to enhance BGP security (BGPSECx). Requirements:

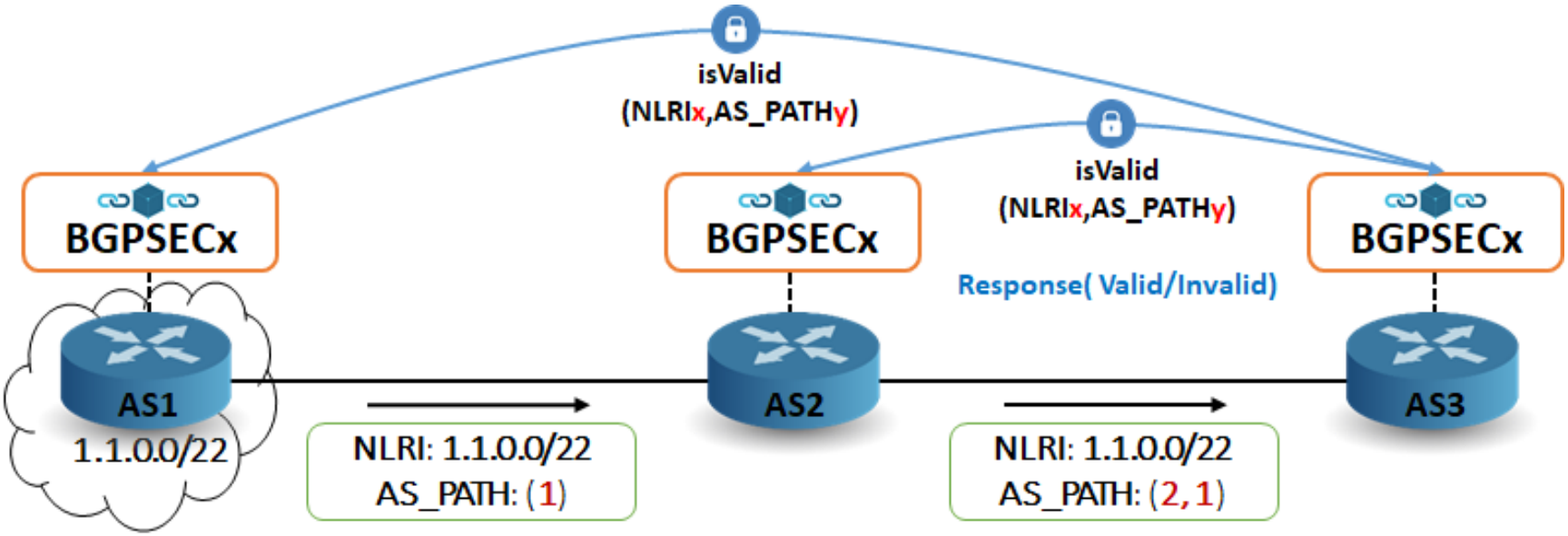
- Perform Origin Authentication and Path Validation.
- Enables incremental deployment.
- Don't require changes to BGP.
- Remove computational burden from routers.
- Creates incentives to ASes and removes disincentives.

BGPSECx design - (OA/PV on BGPSECx using Inter-IXP queries)



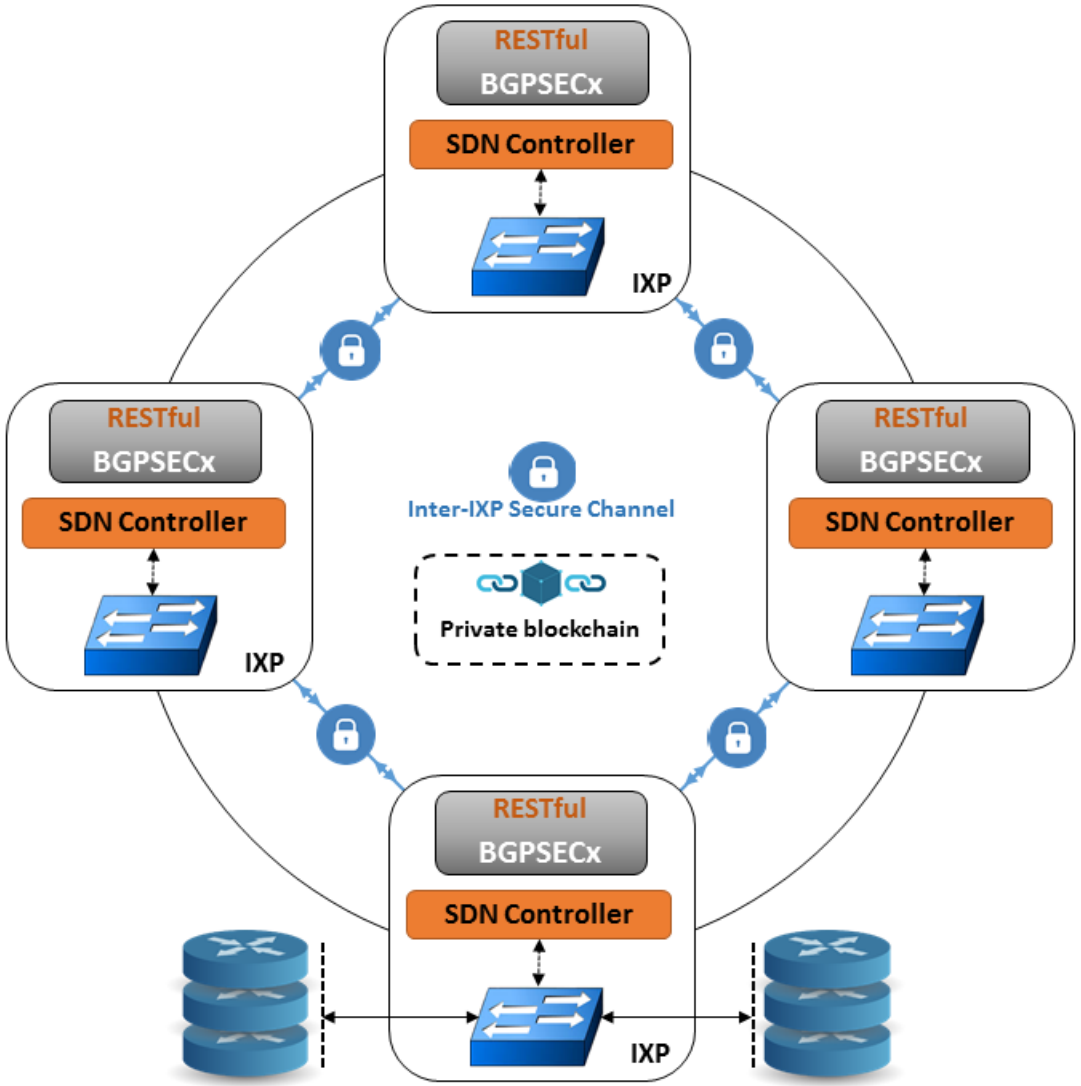
- Peer which receives the advertisement makes queries on each AS of the path to validate the announcement.
- In the queries, for a legitimate advertisement is returned VALID, otherwise INVALID.
- Queries uses RESTful over HTTPS.
- Queries in blockchain uses JSON-RPC (based in key/value).

BGPSECx design - (OA/PV on BGPSECx using blochchain)

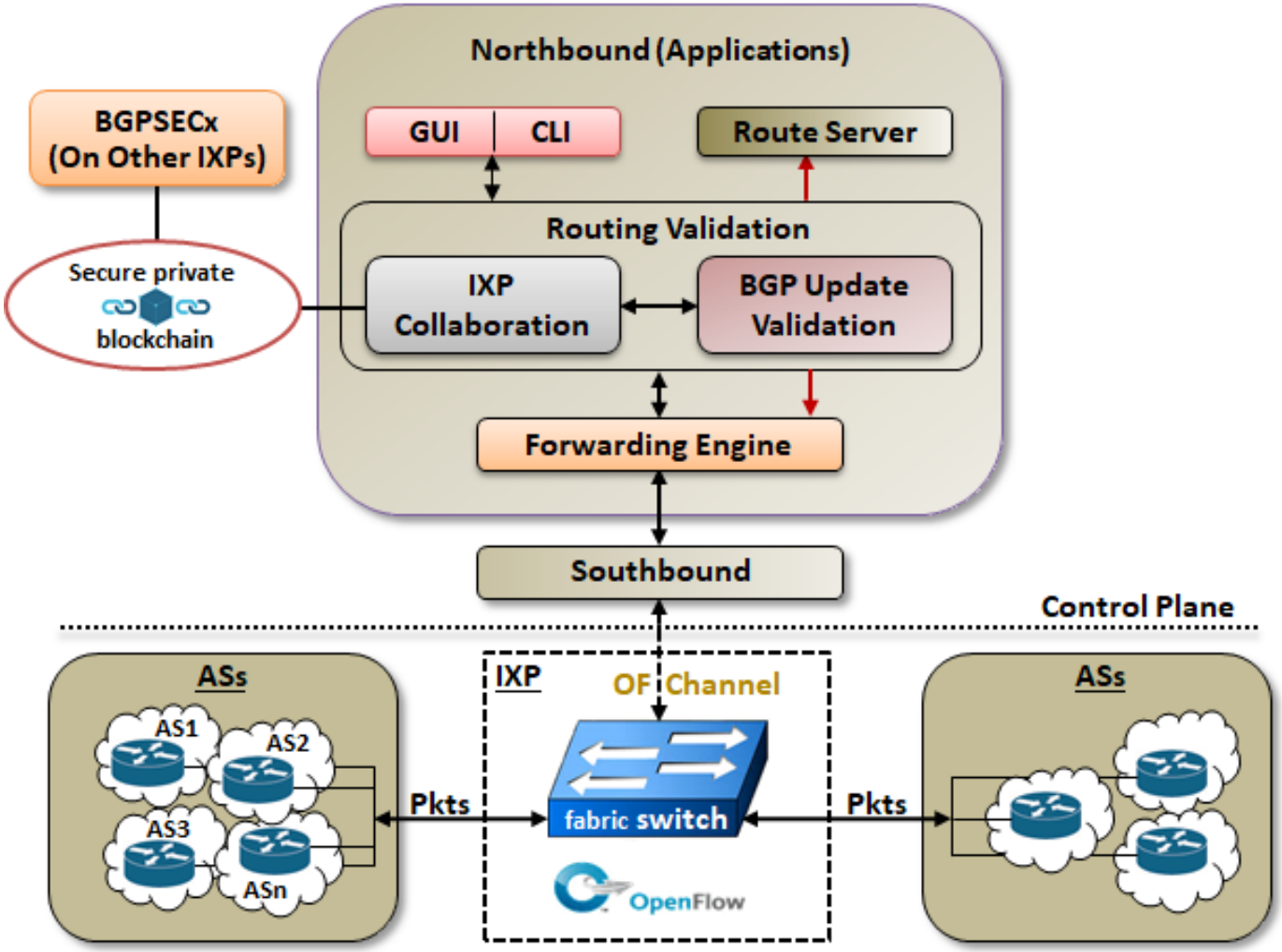


- Each peer have its blockchain and are synchronized with each other. No proof-of-work is required to include transactions. To avoid malicious peer is used a permission policy.
- To validate OA/PV, the AS makes queries in its own blockchain.
- To avoid synchronization problems, queries may be performed on the remote peer using JSON-RPC (HTTPS or SSL/TCP-Socket).

BGPSECx design (Inter-IXP queries)



Secure BGP for Internet Exchange Points - **BGPSECx**



Proposal - Implementation

Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).

Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.

Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.

Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.

Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.
- With CLI and graphics interface tools to facilitate the management and mitigate misconfiguration issues.

Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.
- With CLI and graphics interface tools to facilitate the management and mitigate misconfiguration issues.
- HTTPS/RESTful to provide IXP collaboration.

Implementation

We have implemented BGPSECx:

- Java based to keep portability (Unix-like, Windows e Mac).
- Application on top of ONOS Controller.
- SDNIP to manage data planes SDN-based.
- Quagga software router as route server.
- With CLI and graphics interface tools to facilitate the management and mitigate misconfiguration issues.
- HTTPS/RESTful to provide IXP collaboration.
- Multichain approach to support blockchain.

Empirical analysis: methodology

- Data-driven simulations using empical data: public BGP routing information and IXP datasets.

Empirical analysis: methodology

- Data-driven simulations using empical data: public BGP routing information and IXP datasets.
- We simulate the process of validating each BGP update:
  - **(a)** Validating origin using RPKI
  - **(b)** Validating origin using BGPSECx
  - **(c)** Validating the full path using BGPSECx

Empirical analysis: methodology

- Data-driven simulations using empical data: public BGP routing information and IXP datasets.
- We simulate the process of validating each BGP update:
  - **(a)** Validating origin using RPKI
  - **(b)** Validating origin using BGPSECx
  - **(c)** Validating the full path using BGPSECx
- For BGPSECx we assume that:
  - Only the 10% largest IXPs use BGPSECx (it represents IXPs with more than 50 ASes, totalizing 4147).
  - Only a random set of X% of peers connected to each IXP uses BGPSECx: X = [1, **10**, 25, **50**, 75, **100**].
- Running each experiment 10 times.

Evaluation: routing dataset

Routing collector points and data volume (1/2)

IXP/Locality	# Updates	# Prefixes
RIPE (Amsterdam/NL)*	1176888	5886175
LINX (London/UK)	642095	3219512
AMS-IX (Amsterdam/NL)	802181	4021230
CIXP/CERN (Geneva/CH)	610684	2711758
VIX (Vienna/AT)	463082	2133931
JPIX (Otemachi/JP)*	141904	590750
NETNOD (Stockholm/SE)	918238	3350961
MIX (Milan/IT)	762713	3288810
NYIIX (New Yourk/US)*	897104	4344049

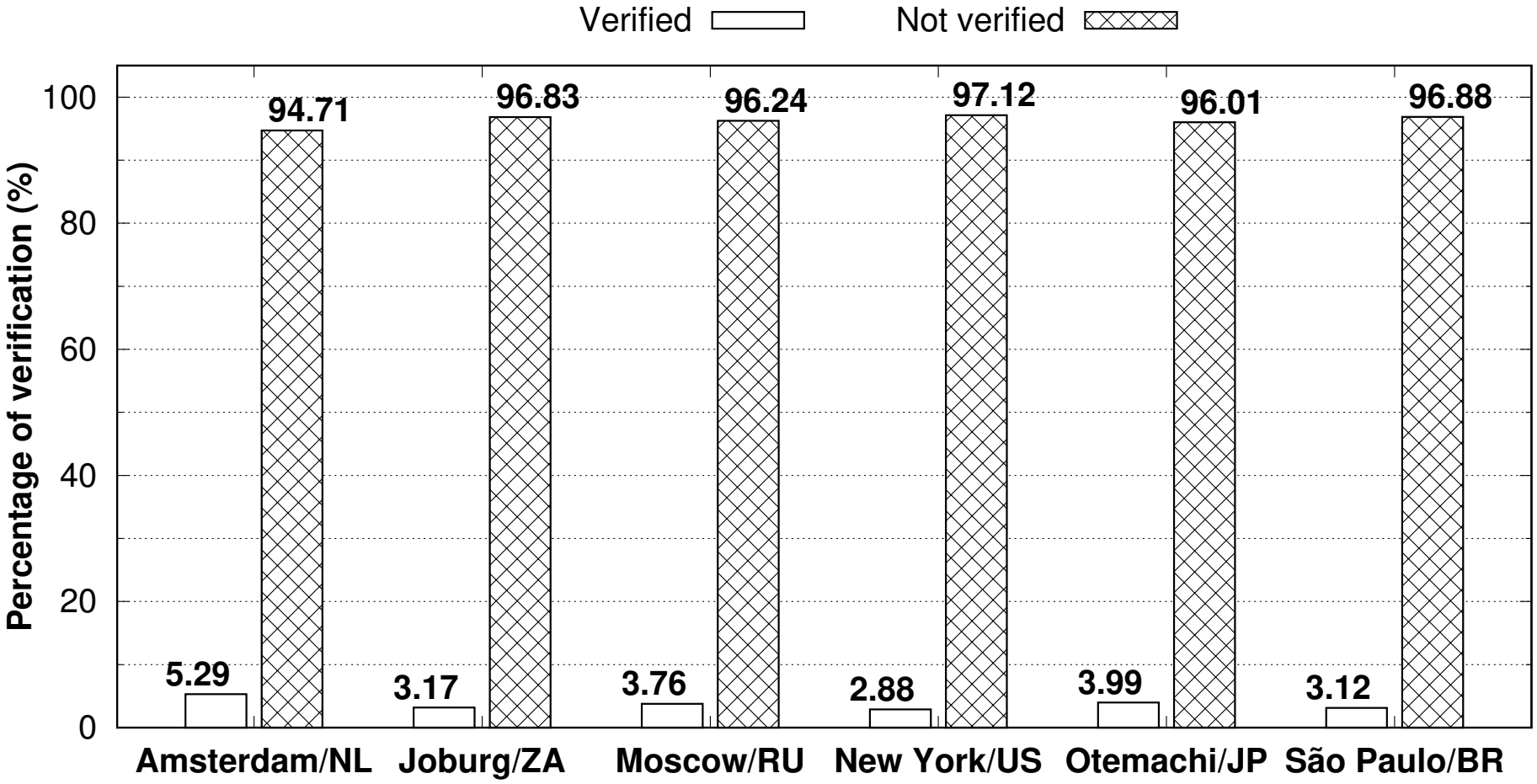
Evaluation: routing dataset

Routing collector points and data volume (2/2)

IXP/Locality	# Updates	# Prefixes
DE-CIX (Frankfurt/DE)	1524949	7004462
MSK/IX (Moscow/RU)*	1314165	4778407
PAIX (Palo Alto/US)	663323	3371273
PTTMetro (São Paulo/BR*	1896335	12324785
NOTA (Maiami/US)	259672	977813
CATNIX (Barcelona/ES)	**84222**	**278400**
NAP/JB (Johannesburg/ZA)*	437222	1820852
SwissIX (Zurich/CH)	**2015867**	**7900807**
FranceIX (Paris/FR)	1607568	7520597

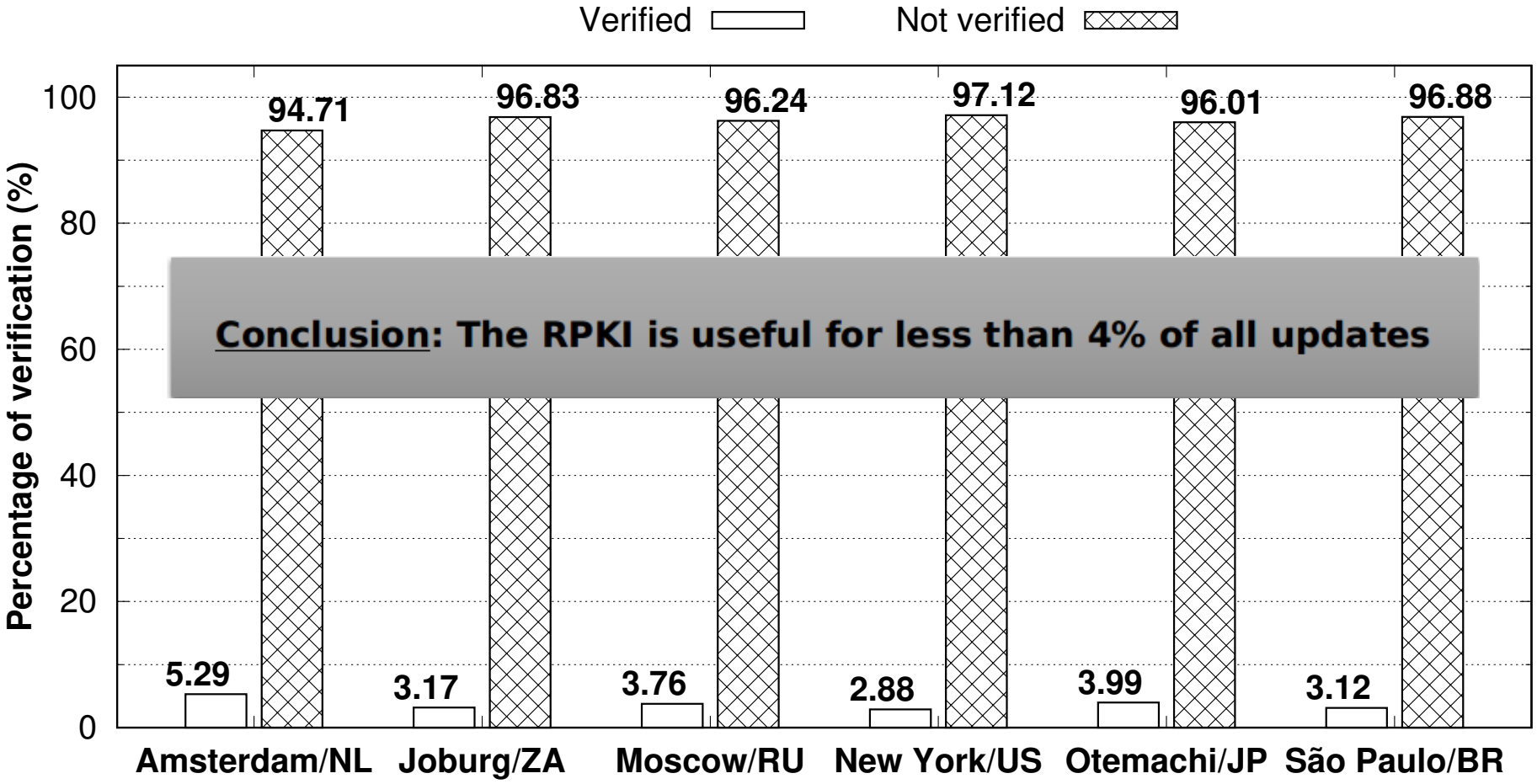
Empirical analysis: simulation results

Verification results of **OA/RPKI** from NL, ZA, RU, JP and BR



Empirical analysis: simulation results

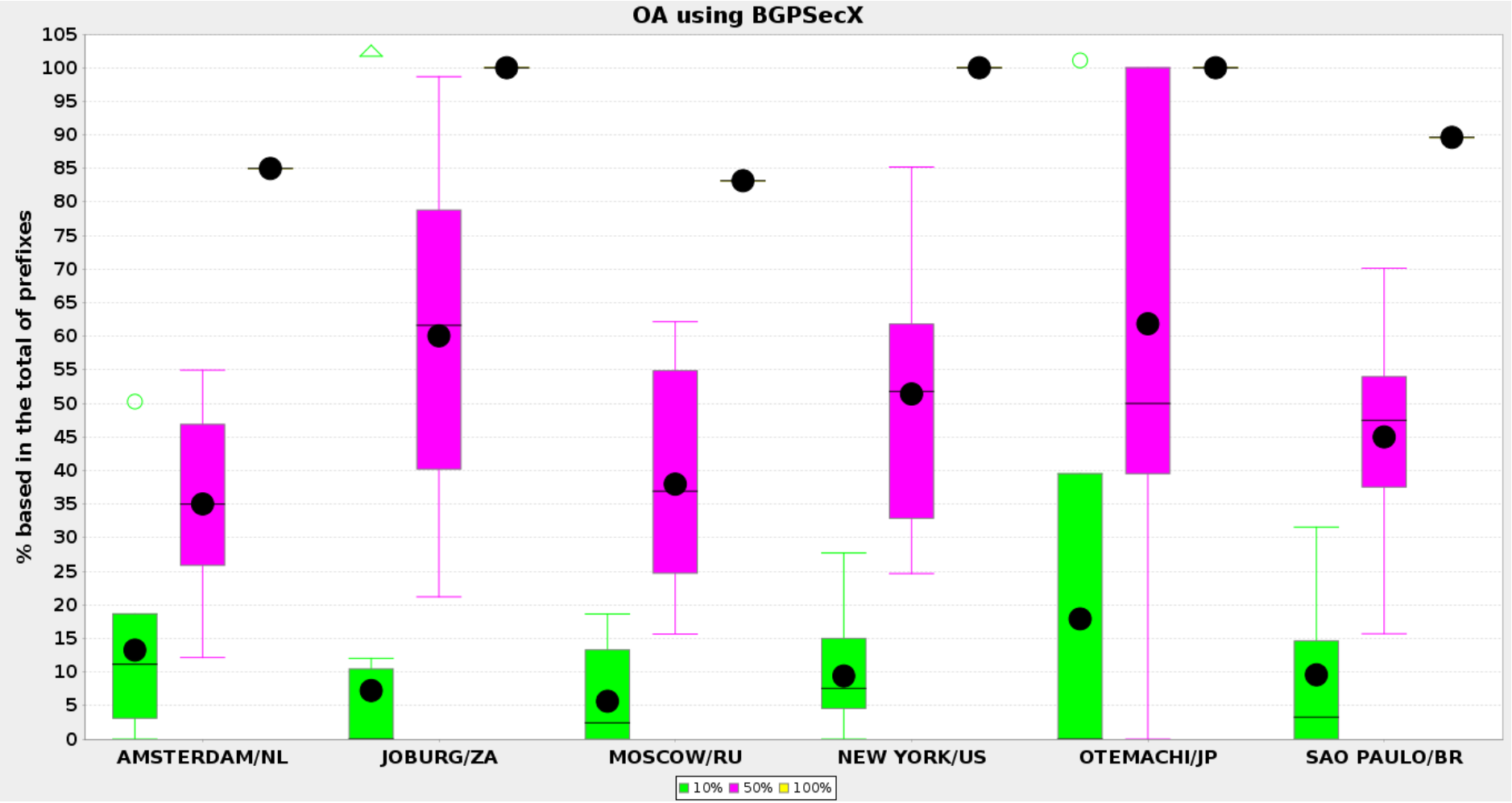
Verification results of **OA/RPKI** from NL, ZA, RU, JP and BR



Conclusion: The RPKI is useful for less than 4% of all updates

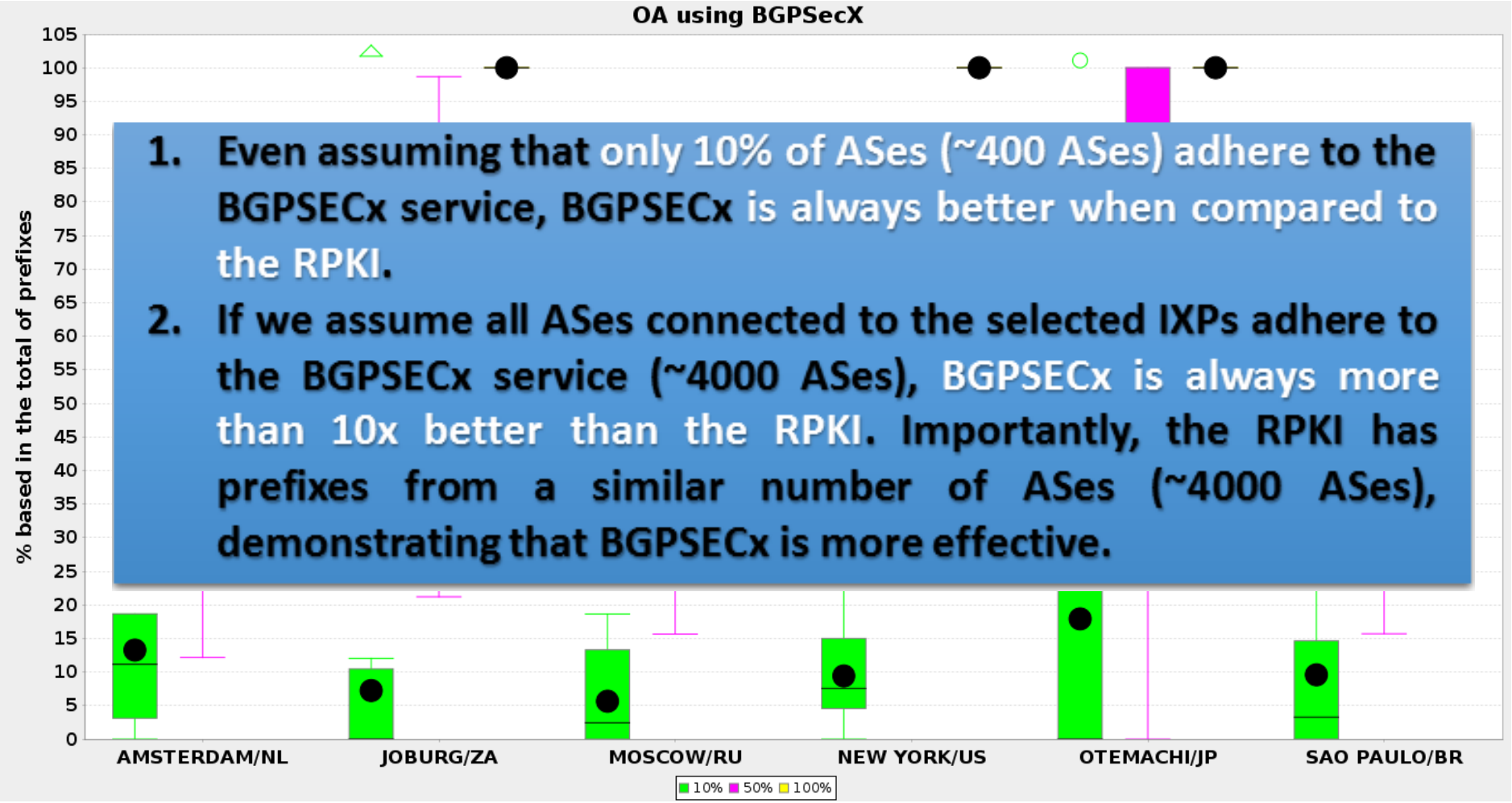
Empirical analysis: simulation results

Verification results of **OA/BGPSECx** from NL, ZA, RU, JP and BR



Empirical analysis: simulation results

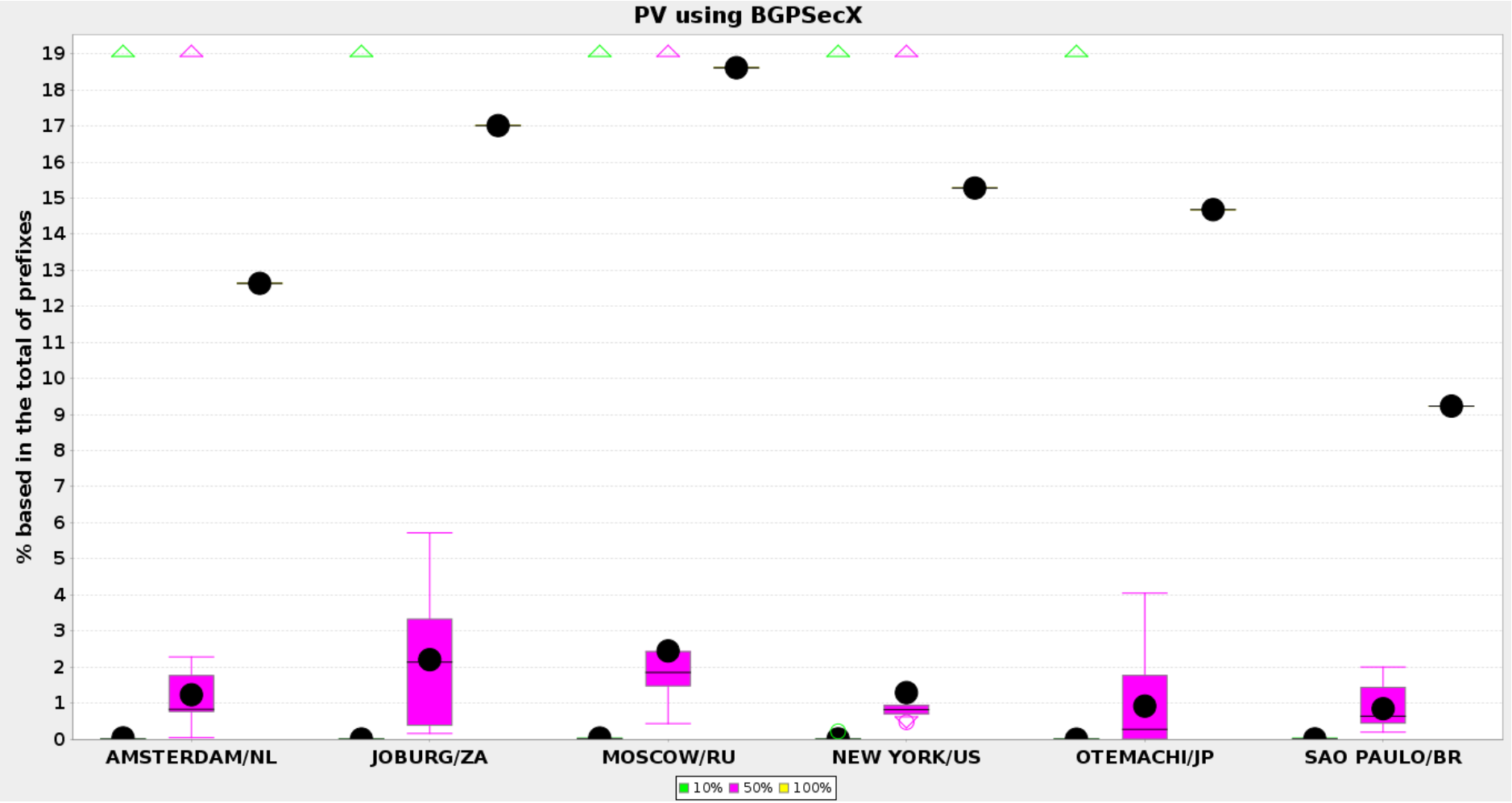
Verification results of **OA/BGPSECx** from NL, ZA, RU, JP and BR



1. Even assuming that only 10% of ASes (~400 ASes) adhere to the BGPSECx service, BGPSECx is always better when compared to the RPKI.
2. If we assume all ASes connected to the selected IXPs adhere to the BGPSECx service (~4000 ASes), BGPSECx is always more than 10x better than the RPKI. Importantly, the RPKI has prefixes from a similar number of ASes (~4000 ASes), demonstrating that BGPSECx is more effective.

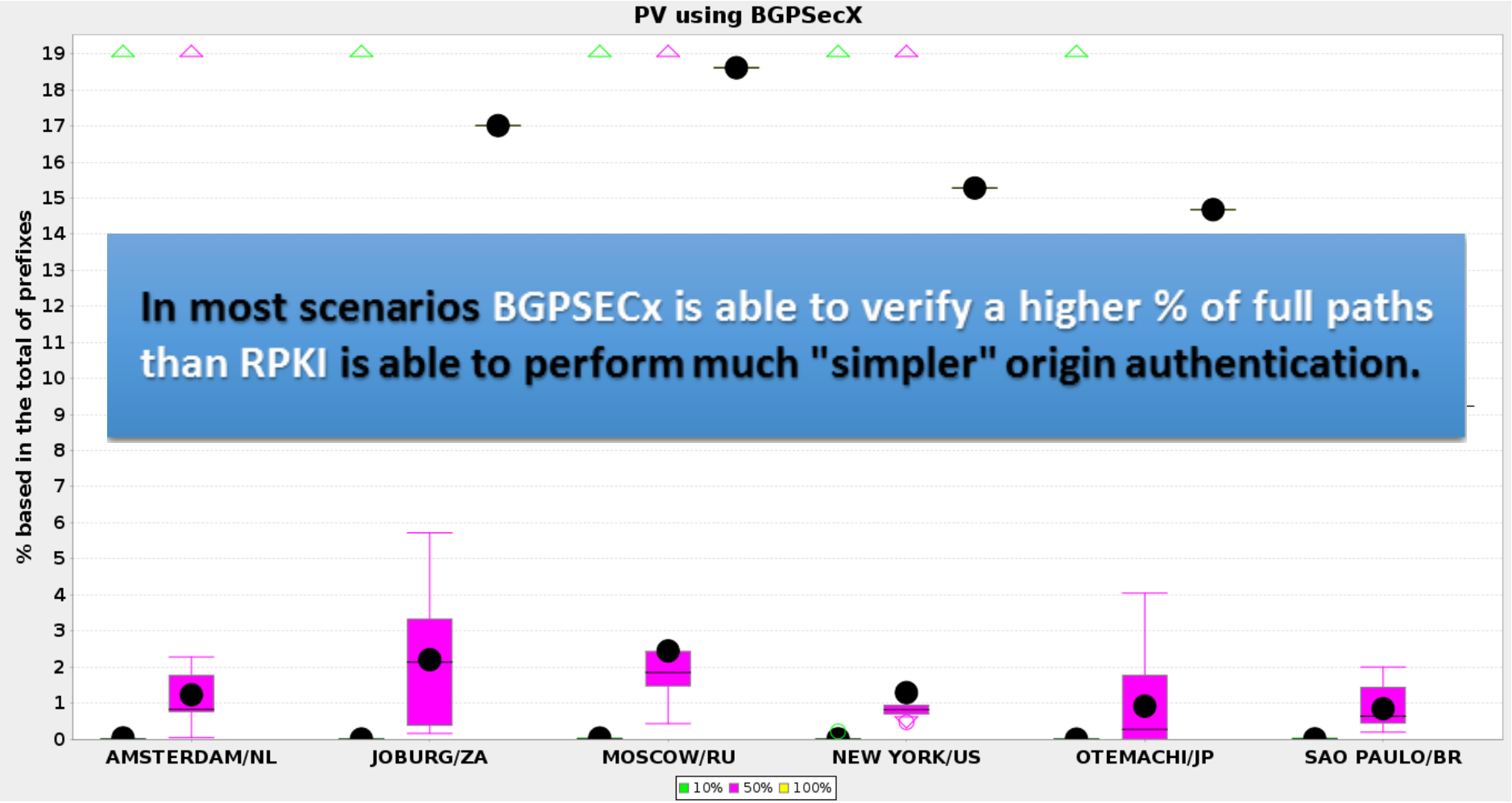
Empirical analysis: simulation results

Verification results of **PV/BGPSECx** from NL, ZA, RU, JP and BR



Empirical analysis: simulation results

Verification results of **PV/BGPSECx** from NL, ZA, RU, JP and BR



In most scenarios BGPSECx is able to verify a higher % of full paths than RPKI is able to perform much "simpler" origin authentication.

Conclusion

- BGP is insecure.

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;
  (3) They do not give operators **incentives** for deployment.

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;
  (3) They do not give operators **incentives** for deployment.
  (4) They create disincentives by disclosing business relationships.

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;
  (3) They do not give operators **incentives** for deployment.
  (4) They create disincentives by disclosing business relationships.
- Our proposal, BGPSECx, offers **equivalent security** to the most complete secure BGP solution while:

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;
  (3) They do not give operators **incentives** for deployment.
  (4) They create disincentives by disclosing business relationships.
- Our proposal, BGPSECx, offers **equivalent security** to the most complete secure BGP solution while:
  - Solving problems (1) and (2) by using an SDN-based approach.

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;
  (3) They do not give operators **incentives** for deployment.
  (4) They create disincentives by disclosing business relationships.
- Our proposal, BGPSECx, offers **equivalent security** to the most complete secure BGP solution while:
  - Solving problems (1) and (2) by using an SDN-based approach.
  - Solving problem (3) by targeting (clusters of collaborating) IXPs.

Conclusion

- BGP is insecure.
- Solutions for this problem remain **largely undeployed** for 4 fundamental reasons:
  (1) They require **changes to BGP**.
  (2) They are **computationally expensive** for routers, and/or;
  (3) They do not give operators **incentives** for deployment.
  (4) They create disincentives by disclosing business relationships.
- Our proposal, BGPSECx, offers **equivalent security** to the most complete secure BGP solution while:
  - Solving problems (1) and (2) by using an SDN-based approach.
  - Solving problem (3) by targeting (clusters of collaborating) IXPs.
  - Solving problem (4) by collaborating and of privacy-preserving smart contracts on top of a blockchain (next step to research).

Thank you!