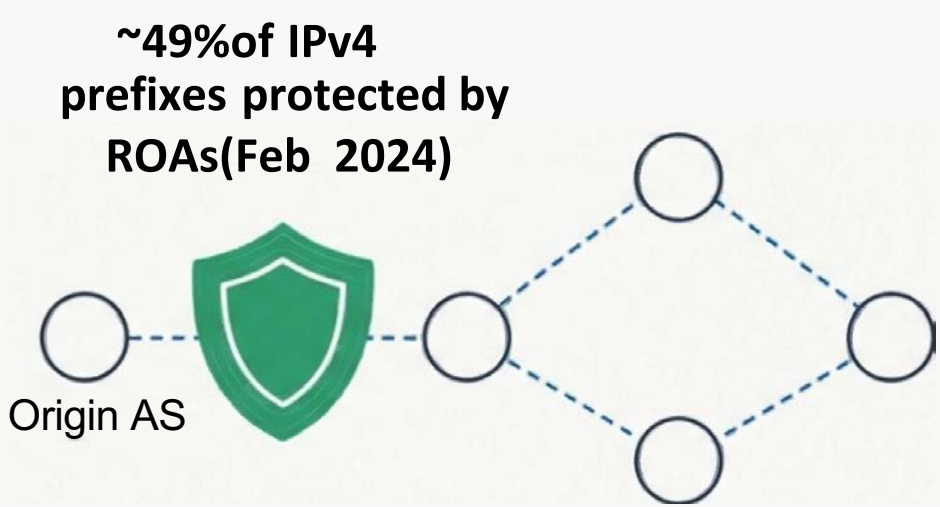
Minimal-Exposure AS-Path Verification against BGP Post-ROV Attacks

ZHAN JIANGOU, Tsinghua University

RPKI Has Hardened Origin Authentication, But Path Security Remains a Gap

- The Resource Public Key Infrastructure (RPKI) is a significant success in mitigating prefix/subprefix hijacking.
- Current deployment is substantial and growing:
  - ~49%of IPv4 prefixes are protected by Route Origin Authorizations(ROAs).
  - ~37% of Autonomous Systems(ASes) have deployed Route Origin Validation (ROV).
- **The Next Frontier:** Securing the AS-Path itself against 'Post-ROV' attacks.

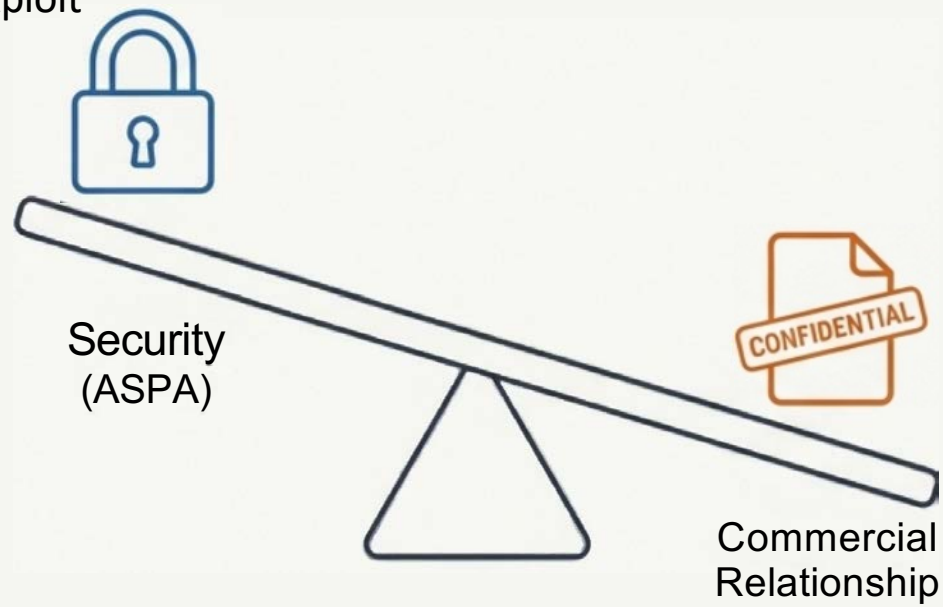


The Adoption Dilemma: Path Security vs. Commercial Confidentiality

Problem: Post-ROV attacks exploit unauthenticated AS-Paths.

Path Manipulation:
Forging paths to hijack traffic.

Route Leaks:
Propagating routes in violation of policy.



Existing Solutions &Their Trade-off:

- Mechanisms like BGPsec face high computational overhead.
- ASPA requires global publication of customer-provider relationships, exposing sensitive interconnection policies.

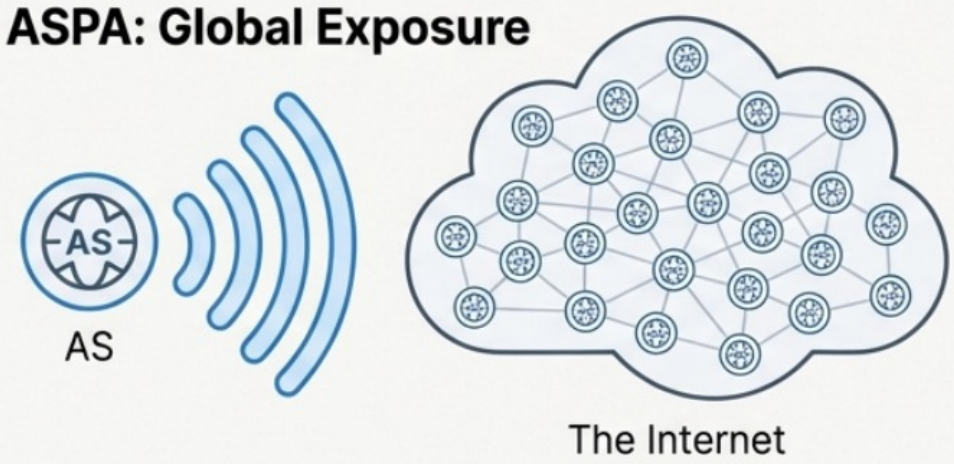
Core Conflict:Mandatory transparency creates a major barrier to widespread adoption.

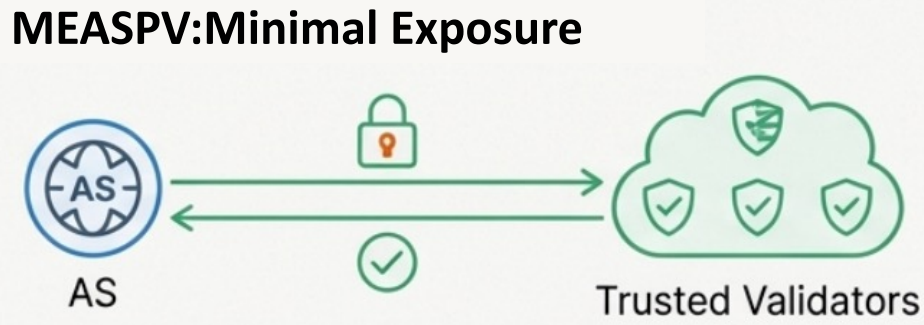
Our Approach: MEASPV Decouples Validation from Disclosure

Core Principle: Enable robust AS-Path verification while confining visibility of relationship attestations strictly to relevant entities.

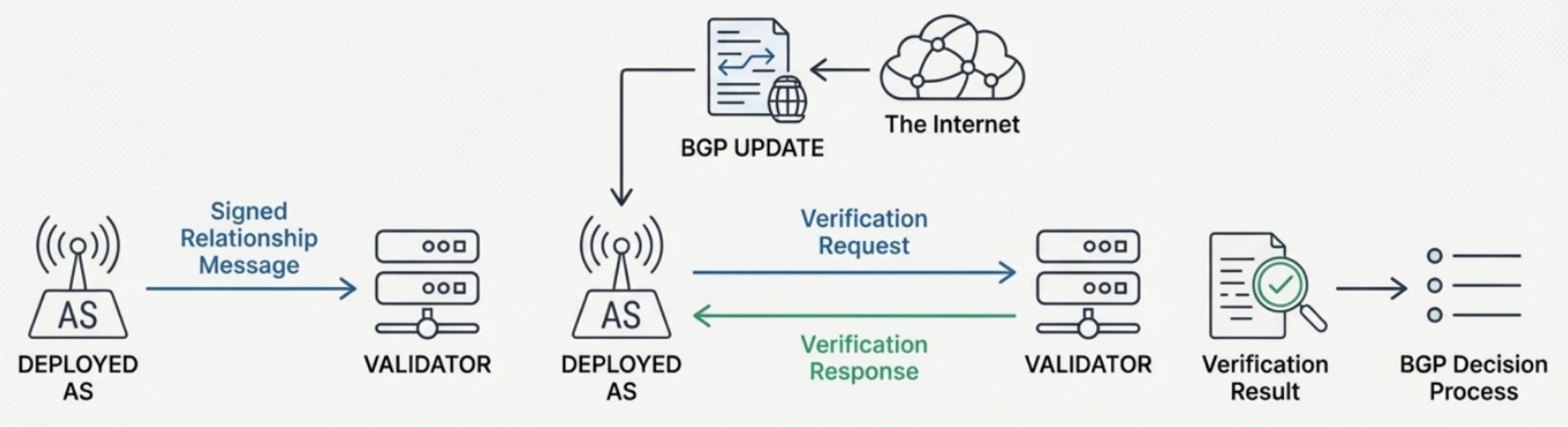
Design Goals:

- **Security**: Effective defense against path manipulation and route leaks.
- **Minimal Information Exposure**: Avoid global publication of AS topology.
- **Incremental Deployability**: Provide benefits even under partial adoption.
- **Low Overhead**: Negligible costs; no modifications to BGP-4 formats.





MEASPV Employs a Validator-Assisted Architecture in Three Phases



Phase 1:Trust Establishment

High-tier ASes can register as **Validators.** Deploying ASes establish secure channels with chosen Validators and share encrypted, authenticated neighbor relationship data.

Phase 2:Path Verification

An AS receives a BGP UPDATE,sends a Verification Request to its Validators,and receives a Verification Response.

Phase 3:Secure Route Selection

The AS aggregates responses into a **Security Score.** This score is used as a new tie-breaker in the BGP decision process.

Validation Logic Is Based on a Hierarchy of Trust

Validator Information Sources:

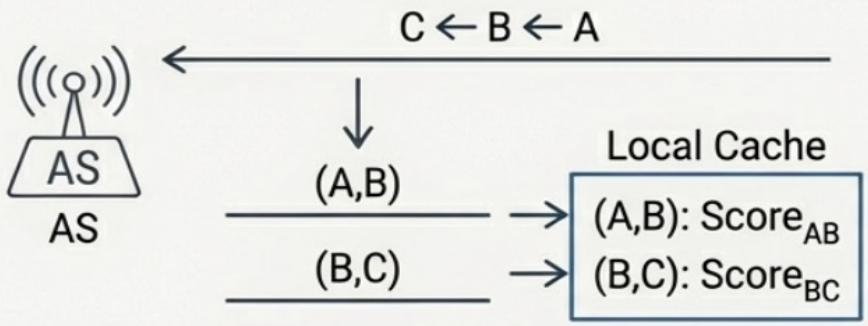
- **Type-I(High Trust):** Direct, authenticated neighbor reports received from deploying ASes over secure channels.
- **Type-II (Lower Trust):** Publicly available data (e.g.,CAIDA, RouteViews) used to supplement Type-I information.

Outcome	Basis of Evidence	Score
Strong-Valid	Entire path confirmed by Type-I	+2
Weak-Valid	Entire path legal (Mix I & II)	+1
Unknown	Insufficient information	0
Weak-Suspect	Contradicted by Type-II	-1
Strong-Suspect	Contradicted by Type-I	-2

The final scores are mapped from the aggregated outcomes.

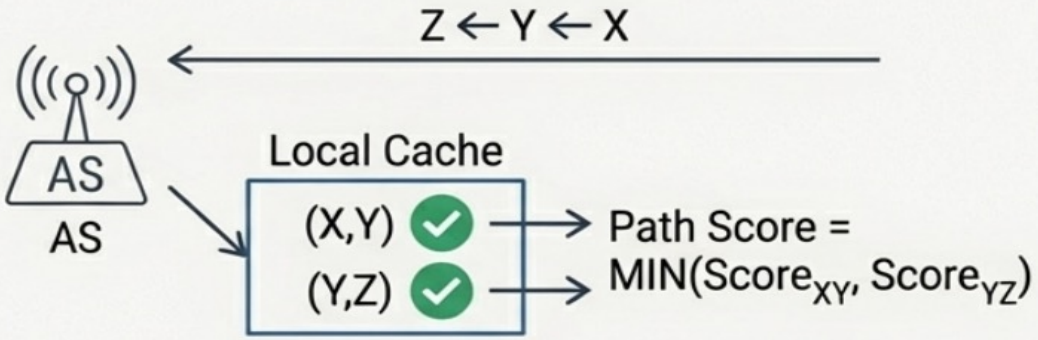
Caching Optimization Minimizes Latency and Control Traffic

Phase 1: Populating the Cache



After receiving a validation result for a full path, the AS decomposes it into individual edges and caches their scores.

Phase 2: Using the Cache Shortcut

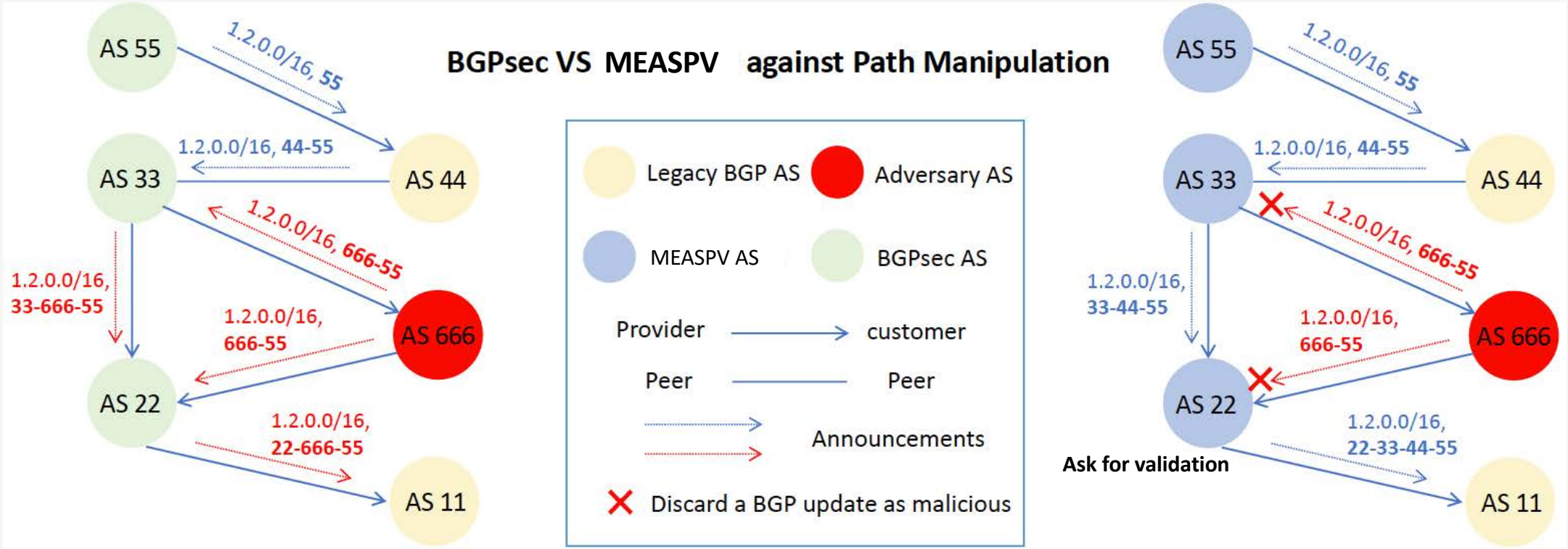


For a new path, if all edges are cached, the score is computed locally. No validator query is needed.

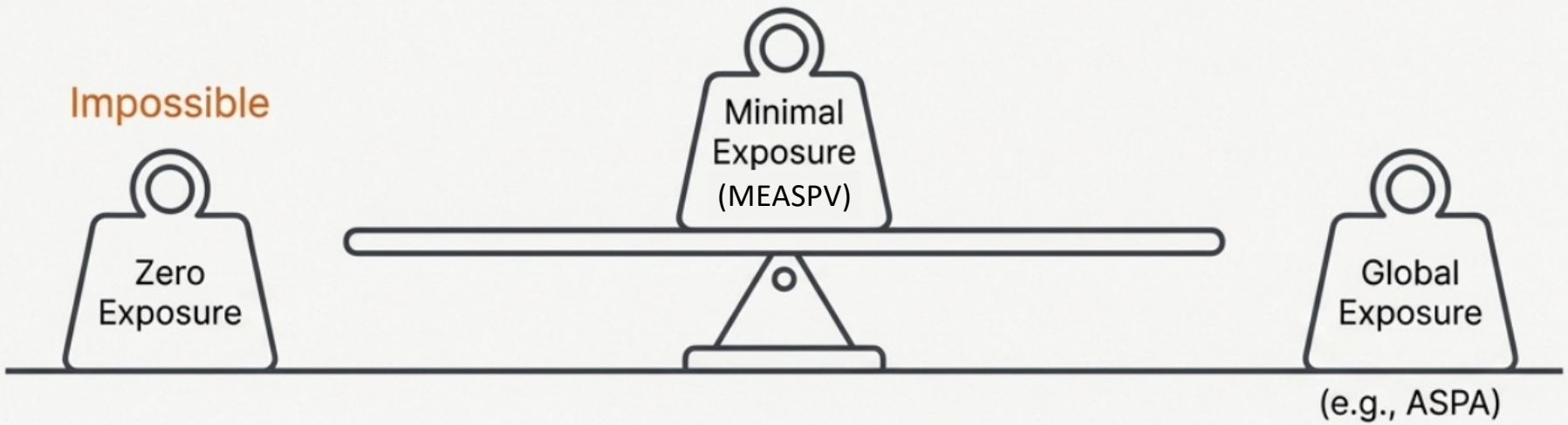
1-5 day cycle

Cache entries expire to ensure freshness.

MEASPV Defense against Path Manipulation Even in Partial Deployment



Achieved the Theoretical Lower Bound on Information Exposure



Constraint: Assumes no modification to BGP-4 message fields.

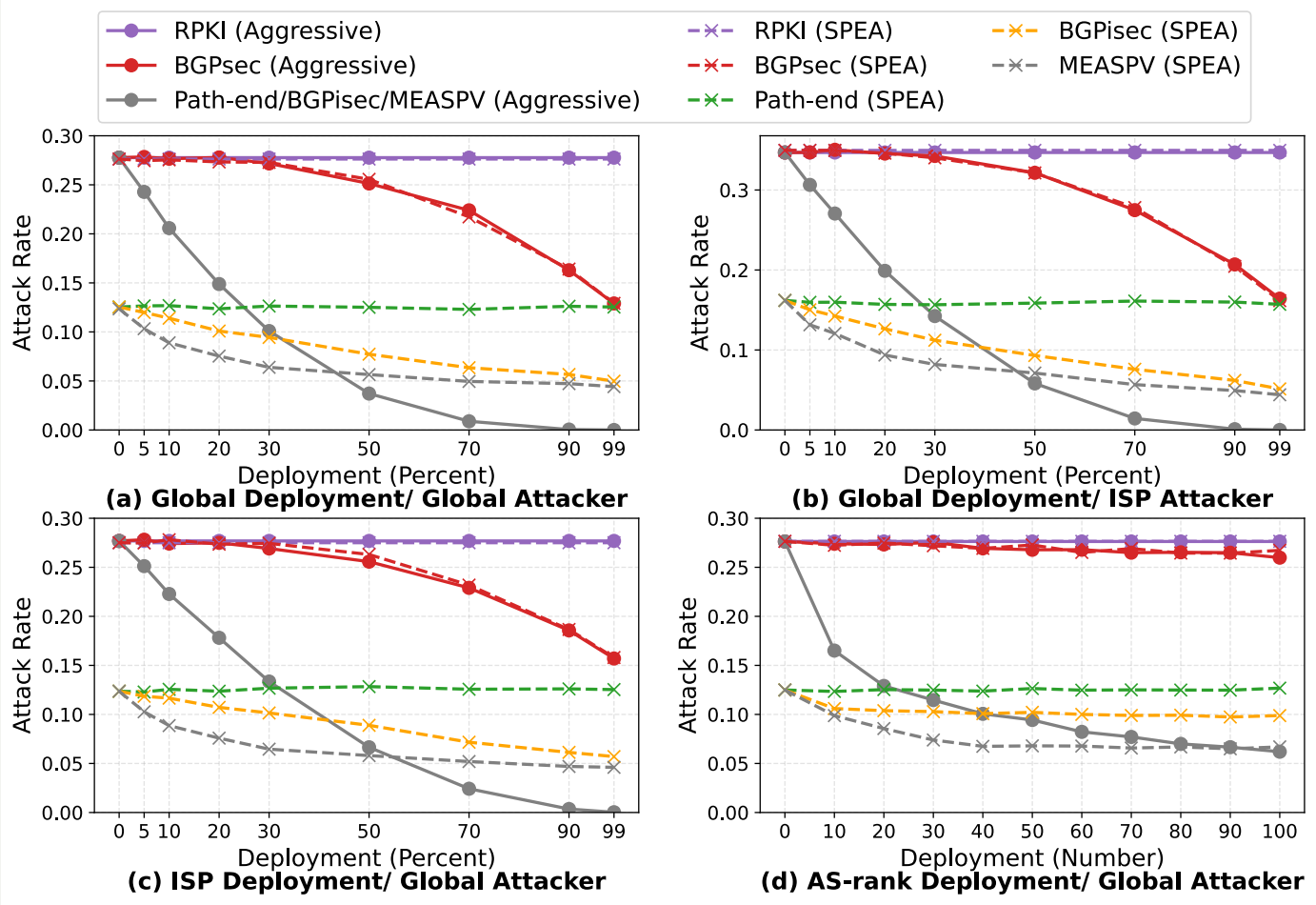
Lower Bound on Information Exposure: Any effective defense *must* expose business relationship information to at least one third-party verifier.

Implication: Zero information exposure is theoretically impossible. MEASPV adheres to this lower bound by confining the necessary exposure to trusted validators.

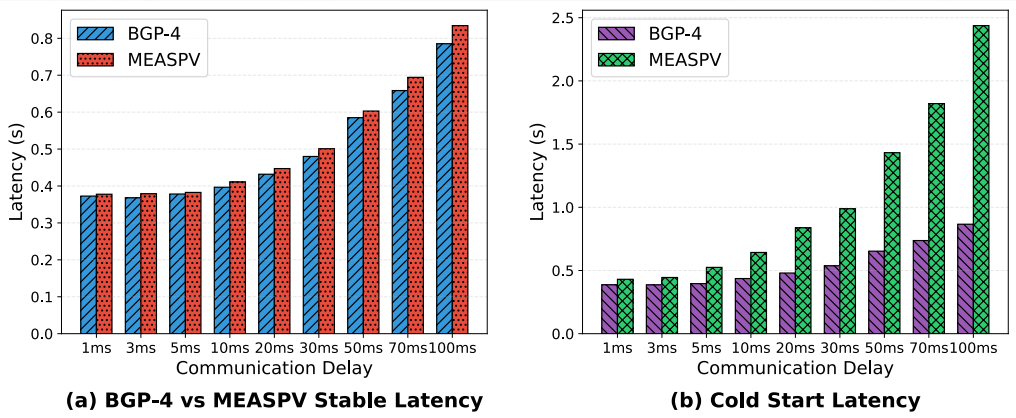
Evaluation: Path Manipulation

Metric: Attack Rate (% of legitimate ASes selecting a malicious path).

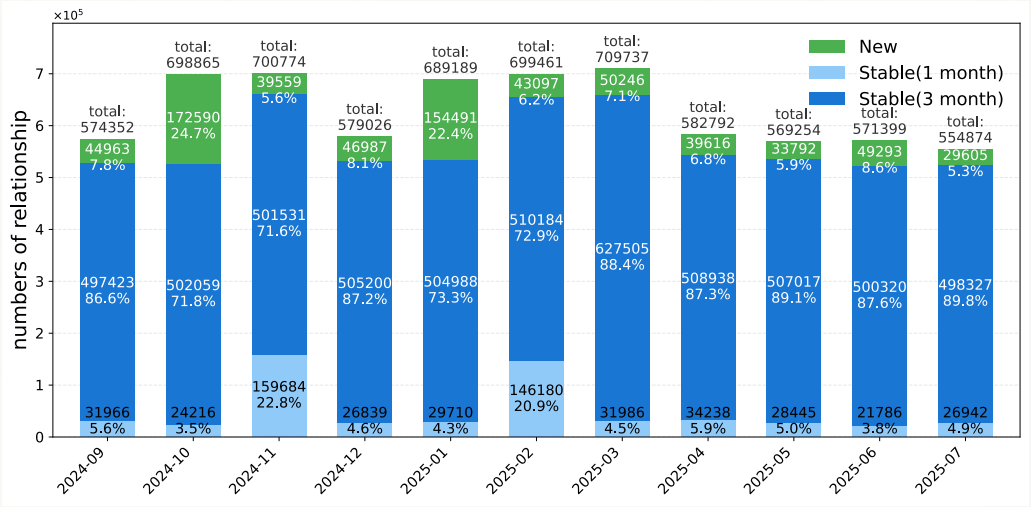
Key Result: MEASPV has achieved better defense effect in some deployment scenarios, especially in SPEA scenarios.



Performance: MEASPV Adds Negligible Latency Overhead



- **Stable State(Cache-hit):** Convergence latency is nearly identical to native BGP-4.
- **Cold Start (Cache-miss):** A rare, one-time cost as AS topology changes infrequently.



- The Monthly change of AS relationship
- The vast majority of AS relationships remain stable over long periods, with only a small fraction of new relationships emerging each month.

MEASPV is operationally feasible and avoids the high performance costs that hindered BGPsec

Conclusion: A Pragmatic Path to Incentive-Compatible Routing Security

The Problem Revisited

Global transparency is not a prerequisite for routing security. The need to protect commercial relationships is a fundamental adoption barrier.

MEASPV's Contribution

We resolve the tension between robust route verification and business confidentiality. By decoupling path validation from global disclosure, MEASPV provides security comparable to ASPA while minimal information exposure.

MEASPV offers a security, pragmatic, deployable, and less exposure path toward securing inter-domain routing.

THANK YOU !

Q&A