How Small Groups Can Secure Interdomain Routing

Martin Suchara

in collaboration with
I. Avramopoulos and J. Rexford

Interdomain Routing (BGP) is not Secure

- BGP is vulnerable to:
  - Deliberate attacks
  - Misconfigurations

- Yet, users demand:
  - Confidentiality
  - Integrity
  - Availability

Securing Interdomain Routing

- **Users demand:**
  - **Confidentiality**
  - **Integrity**
  - **Availability**
- **Existing crypto solutions**
- **Focus of this work**

Overview

I. **The routing system and its vulnerabilities**

II. **Why should small groups secure BGP**

III. **Securing BGP in small groups – effectiveness of techniques**

IV. **Our approach**

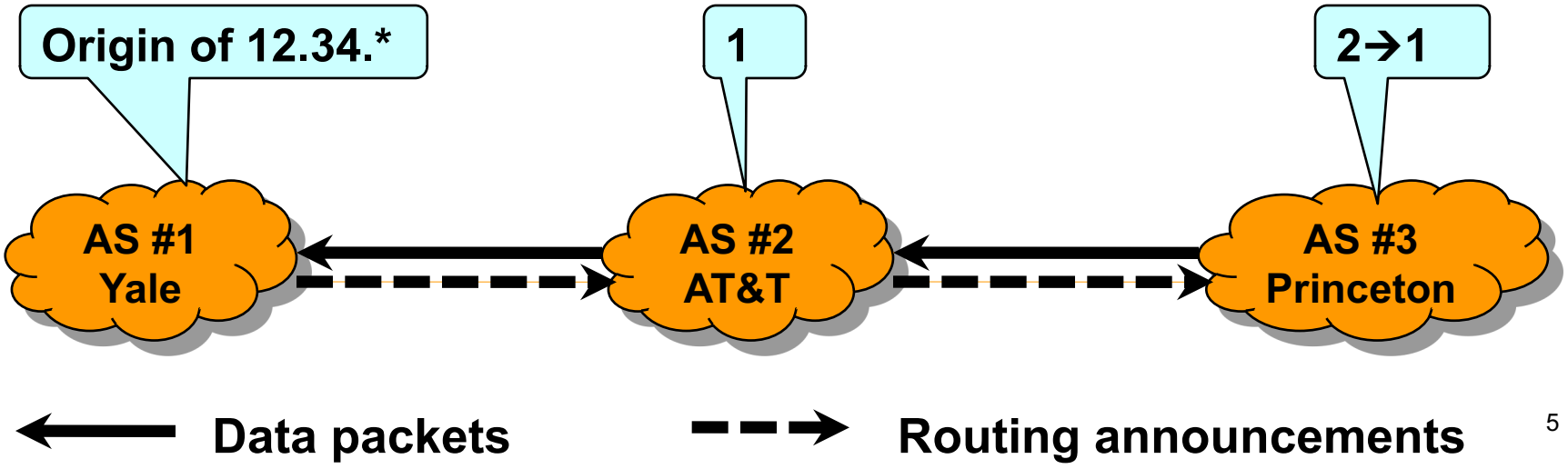
   a) **SBone – secure overlay routing**

   b) **Shout – hijacking the hijacker**

V. **Conclusion**

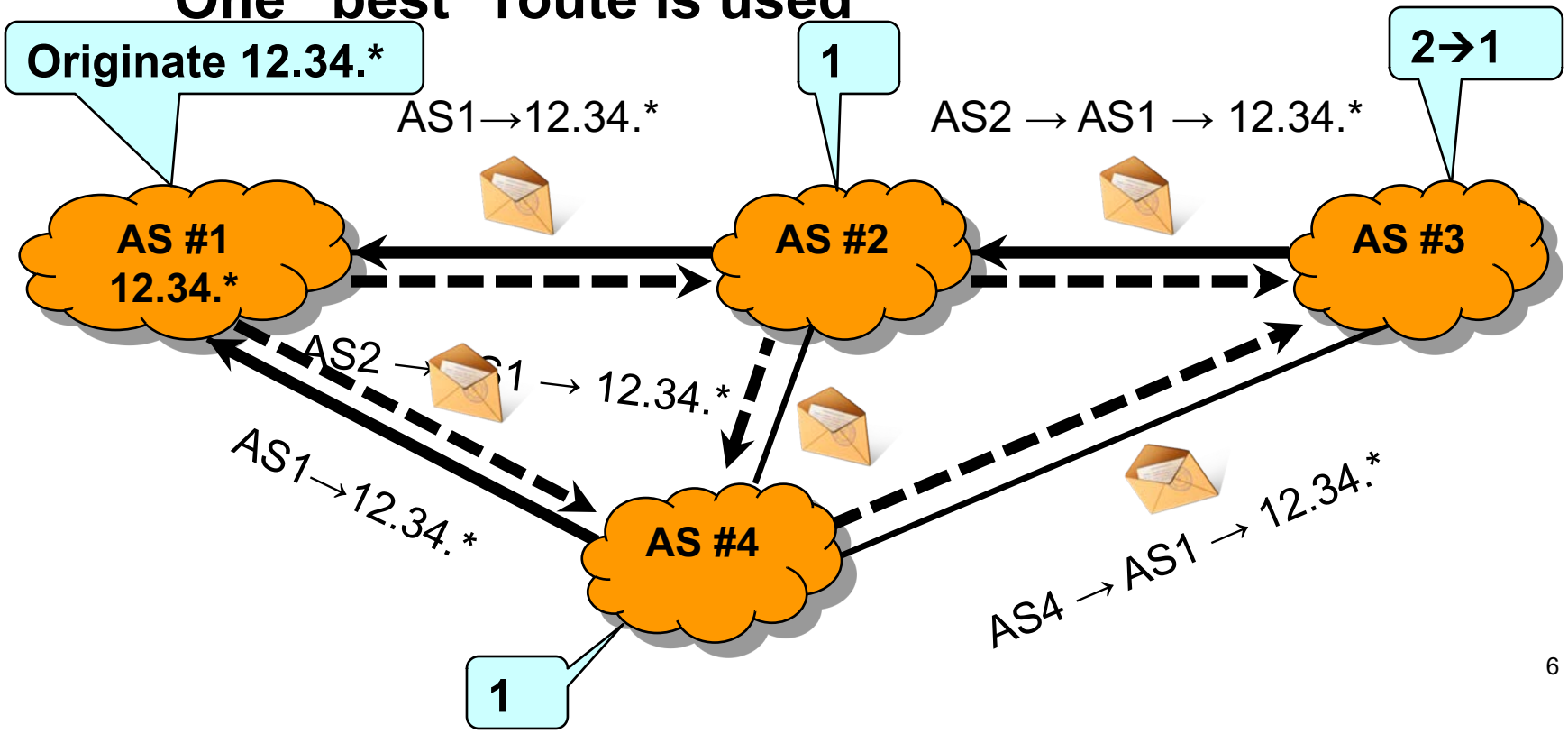
Interdomain Routing – Terminology

- **Autonomous Systems (ASes) = independently administered networks in a loose federation**
- **Prefix = set of IP addresses**
- **Origin = genuine owner of an address prefix**
- **Route = AS-level path to the origin**



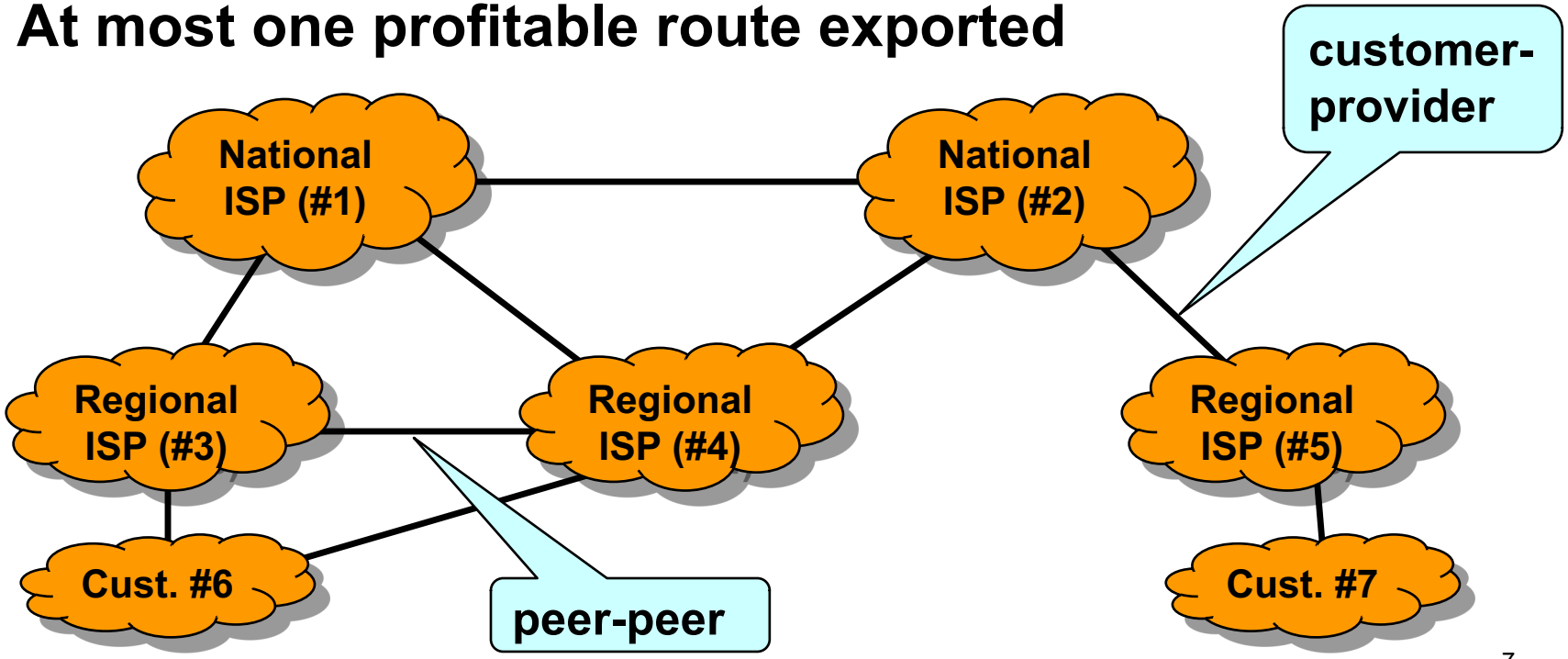
Interdomain Routing – Protocol Based on Trust

- **BGP is prefix-based path-vector protocol**
  - **Each AS maintains a set of routes to all prefixes**
  - **One "best" route is used**



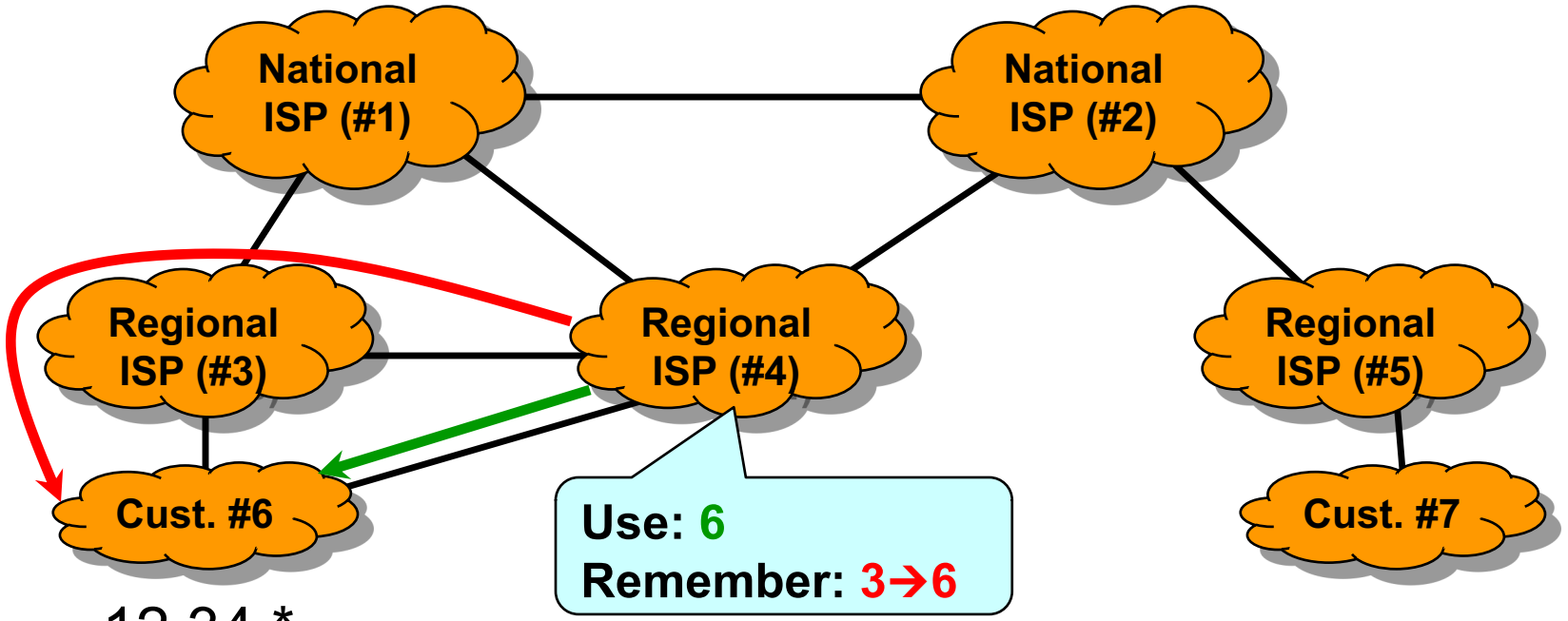
Interdomain Routing – Export & Policies

- **Customer-provider and peer-peer relationships**
- **Selecting a route: by assumption the most profitable, shortest route preferred**
- **At most one profitable route exported**



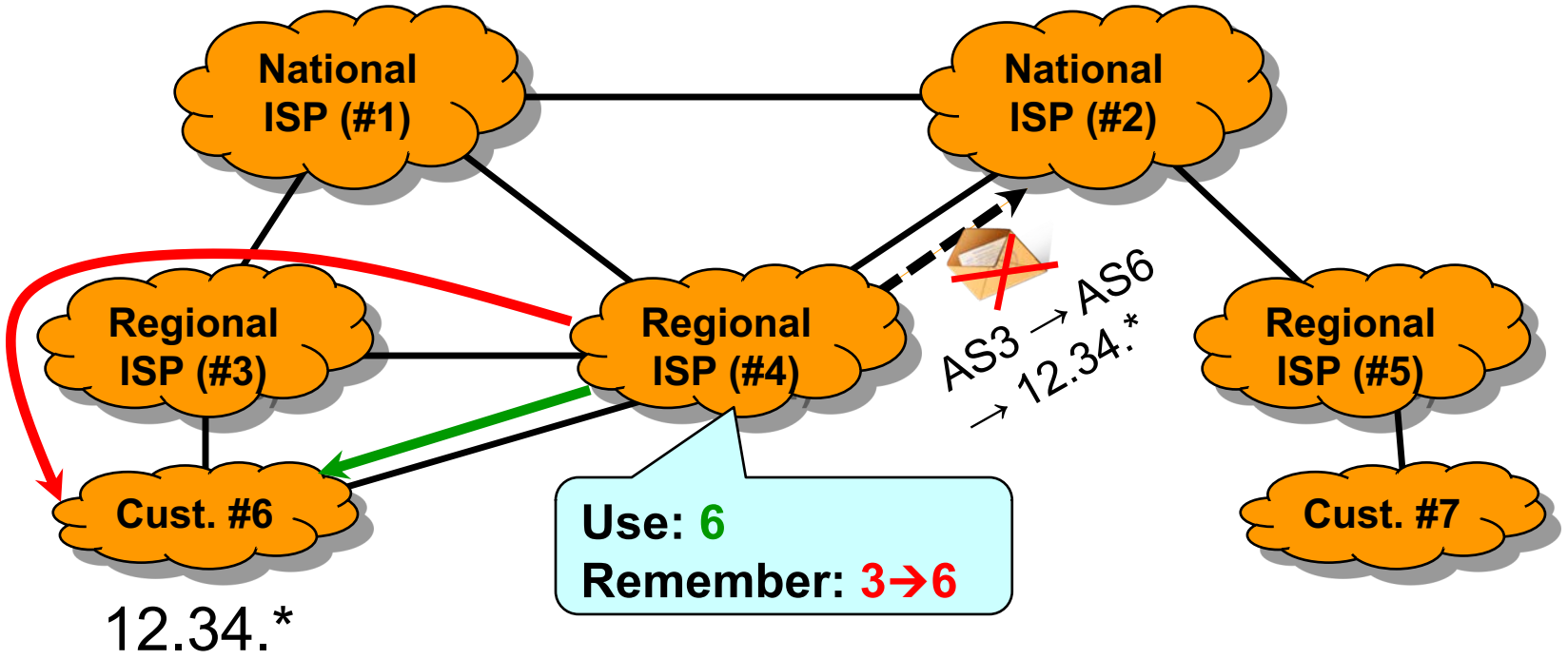
Interdomain Routing – Export & Policies

- **Customer-provider and peer-peer relationships**
- **Selecting a route: by assumption the most profitable, shortest route preferred**
- **At most one profitable route exported**



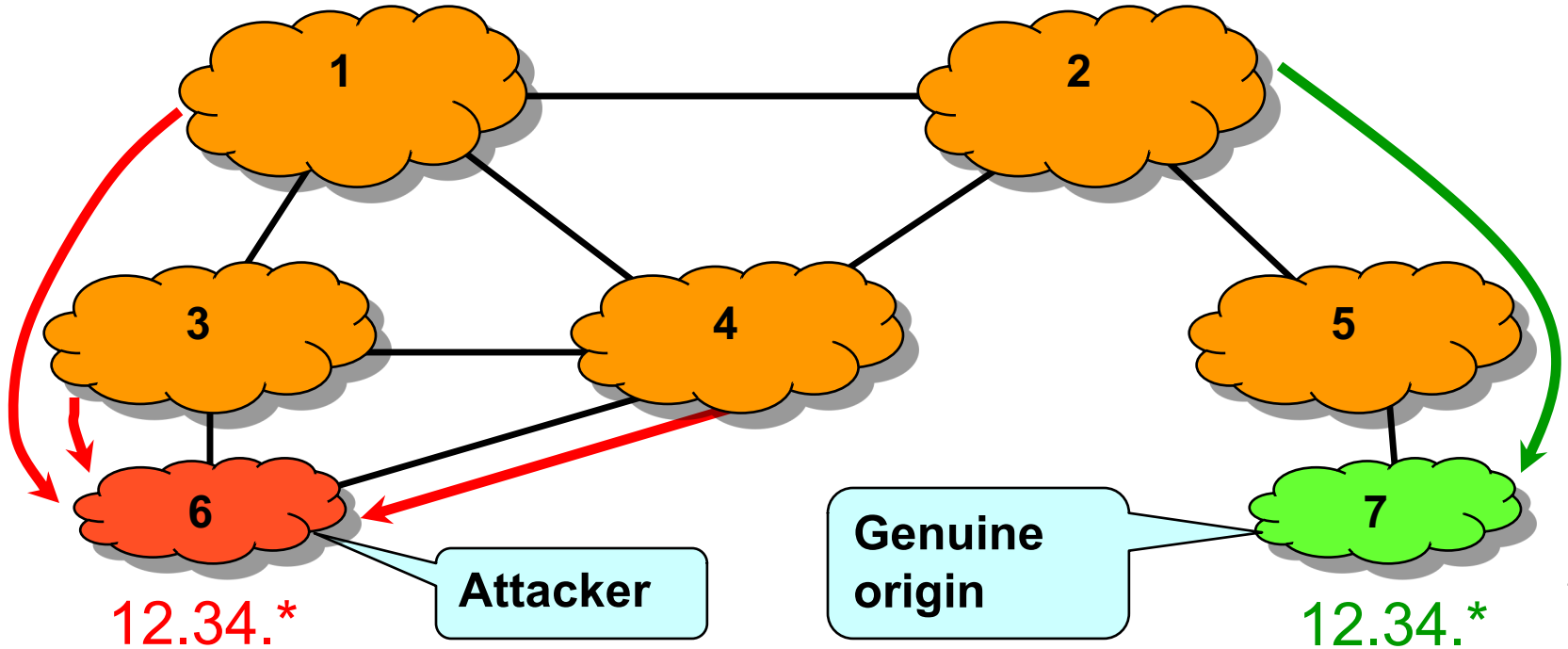
Interdomain Routing – One Cannot Learn Many Routes

- **Customer-provider and peer-peer relationships**
- **Selecting a route: by assumption the most profitable, shortest route preferred**
- **At most one profitable route exported**



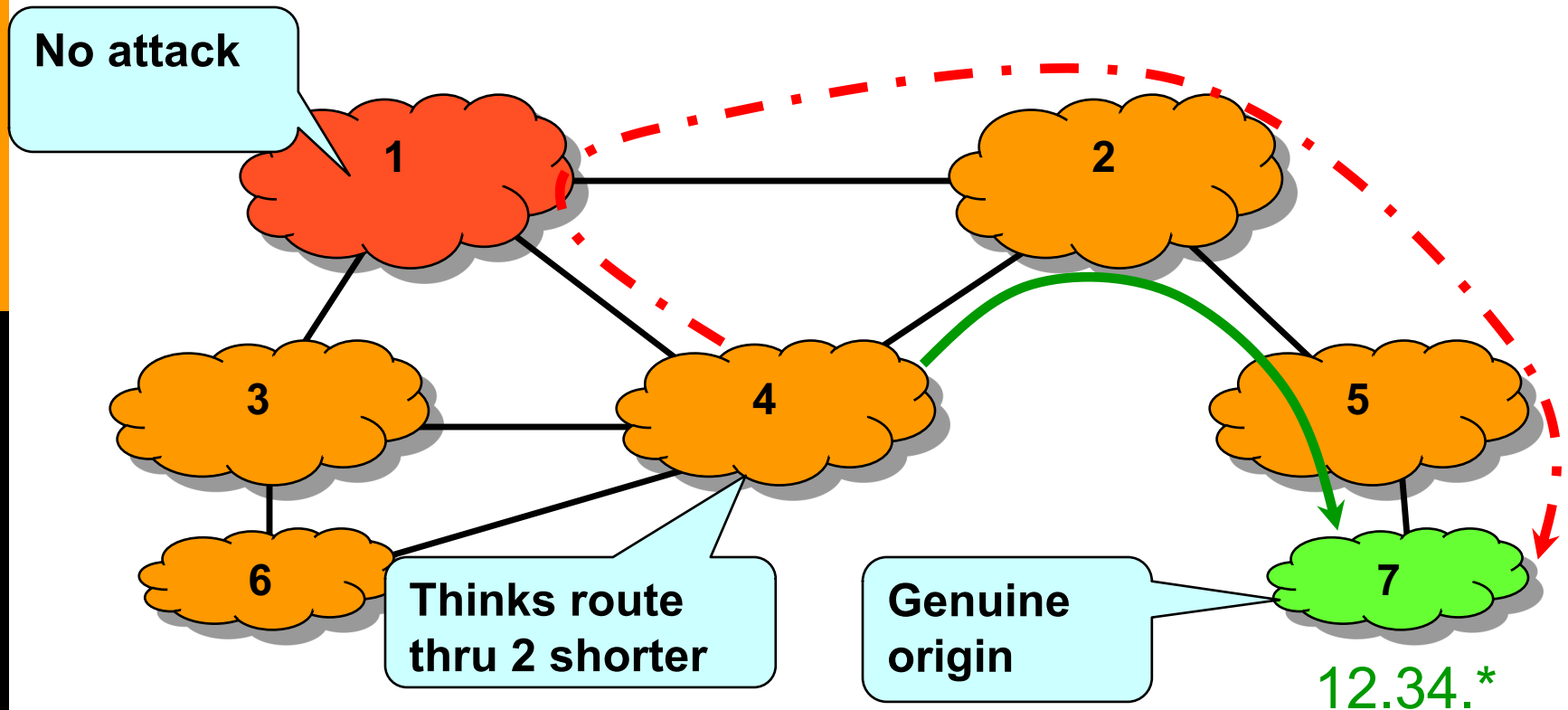
Vulnerabilities – Example 1

- **Invalid origin attack**
  - **Nodes 1, 3 and 4 route to the adversary**
  - **The true destination is blackholed**



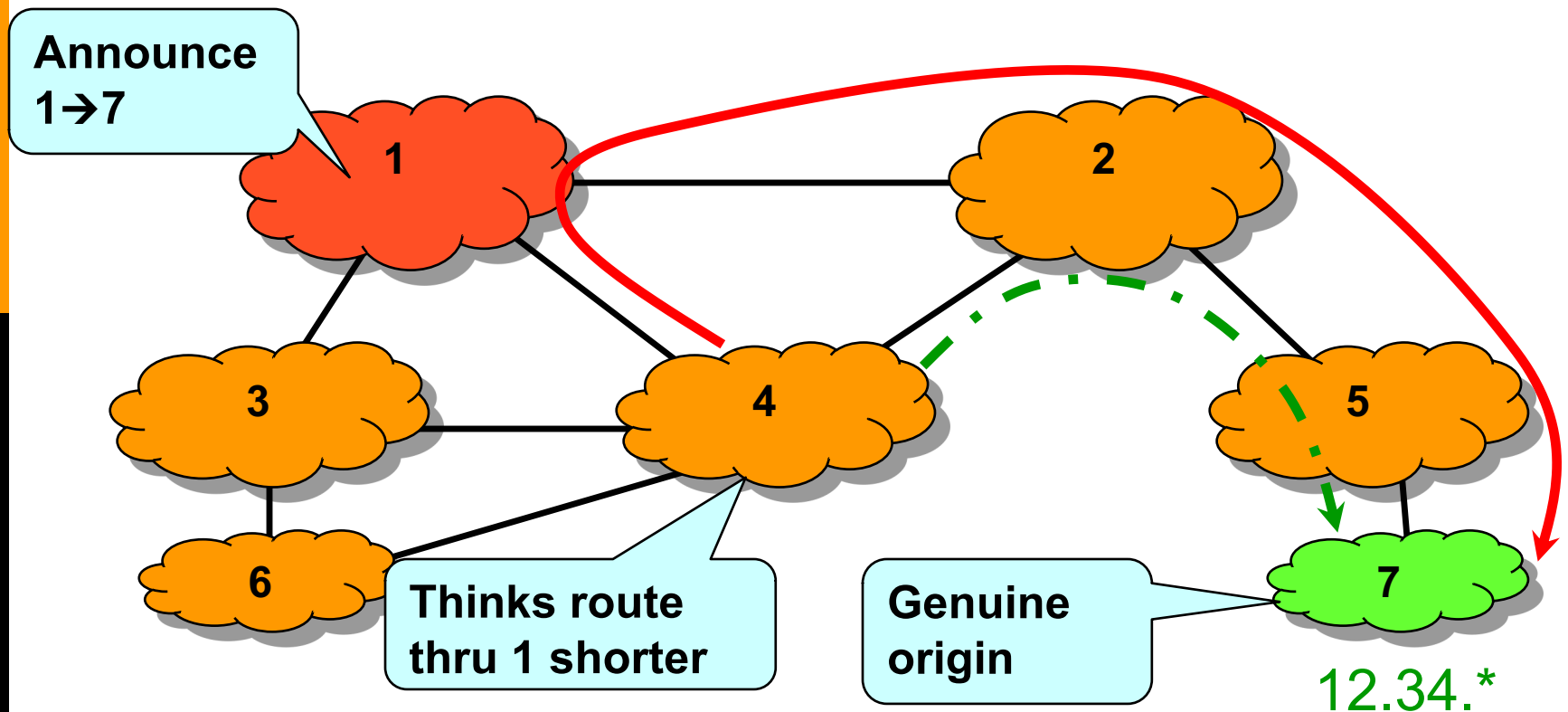
Vulnerabilities – Example 2

- Adversary spoofs a shorter path
  - Node 4 routes through 1 instead of 2
  - The traffic may be blackholed or intercepted



Vulnerabilities – Example 2

- **Adversary spoofs a shorter path**
  - **Node 4 routes through 1 instead of 2**
  - **The traffic may be blackholed or intercepted**



Overview

I. The routing system and its vulnerabilities

II. Why should small groups secure BGP

III. Securing BGP in small groups – effectiveness of techniques

IV. Our approach
   a) SBone – secure overlay routing
   b) Shout – hijacking the hijacker

V. Conclusion

State of the Art – S-BGP and soBGP

- **Mechanism: identify which routes are invalid and filter them**
- **S-BGP**
  - **Certificates to verify origin AS**
  - **Cryptographic attestations added to routing announcements at each hop**
- **soBGP**
  - **Build a (partial) AS level topology database**

Limitations of the Secure Protocols

- **Previous solutions**
  - **Benefits only for large deployments (~10,000s)**
  - **No incentive for early adopters**
  - **No deployment for over a decade**
- **Our goal: Provide incentives to early adopters!**

Our Approach

- Secure routing within a small group
  - 10-20 cooperating nodes
  - All participants' routes are secured
- Challenges
  - Non-participants outnumber participants
  - Participants rely on non-participants
  - Each AS exports only one route
- Focus on raising the bar for the adversary rather than residual vulnerabilities

Overview

I. The routing system and its vulnerabilities

II. Why should small groups secure BGP

III. **Securing BGP in small groups – effectiveness of techniques**

IV. **Our approach**

   a) **Sbone – secure overlay routing**

   b) **Shout – hijacking the hijacker**

V. **Conclusion**

Experimental Evaluations

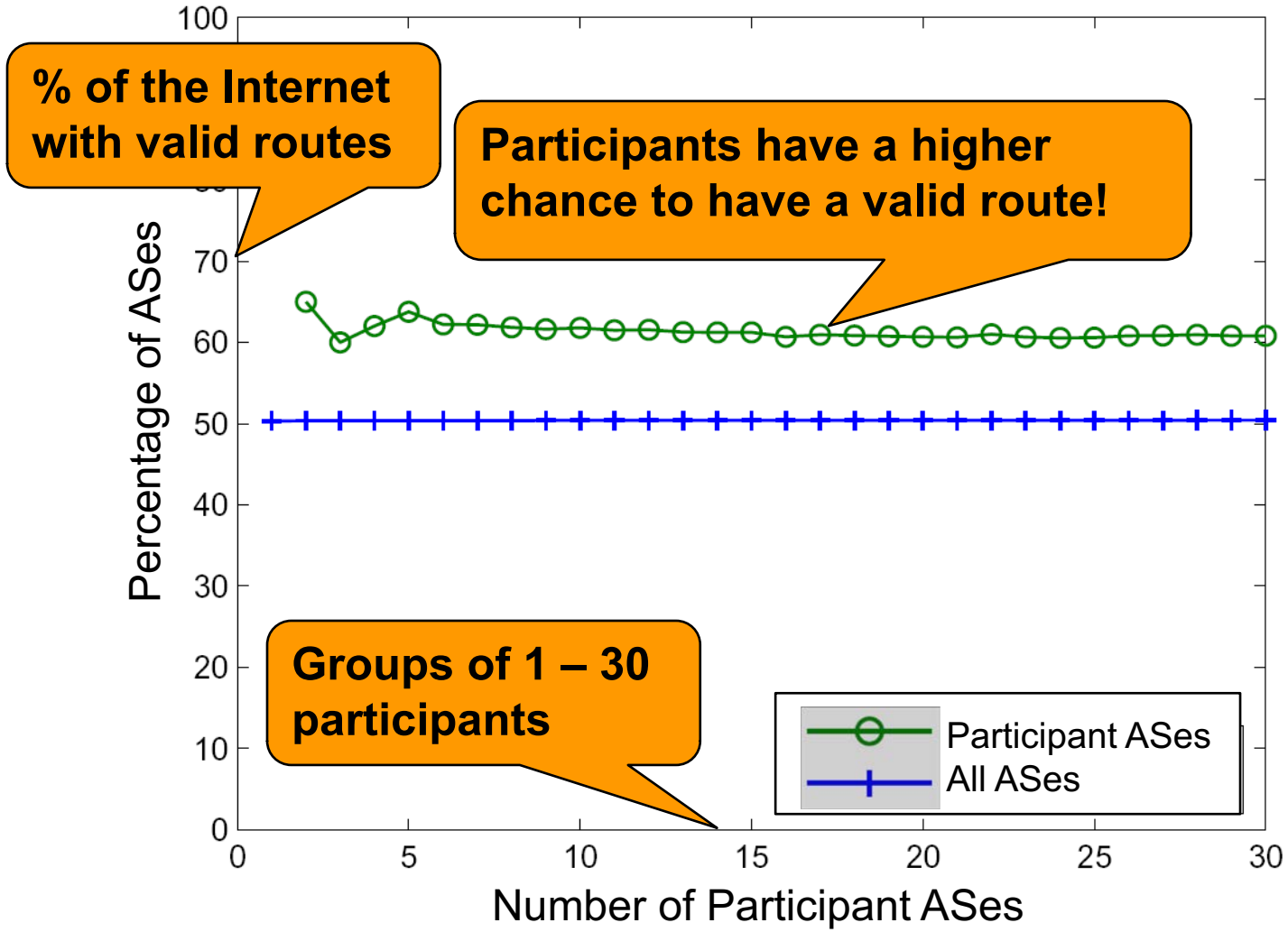
- **Performance of existing techniques**
  - **They work well in large scale deployments**
  - **How do they do in small groups?**

- **Evaluate performance of state-of-the art: soBGP**
  - **Evaluate partial deployment**
  - **If two ASes participate, a valid link connecting them must be in the registry**

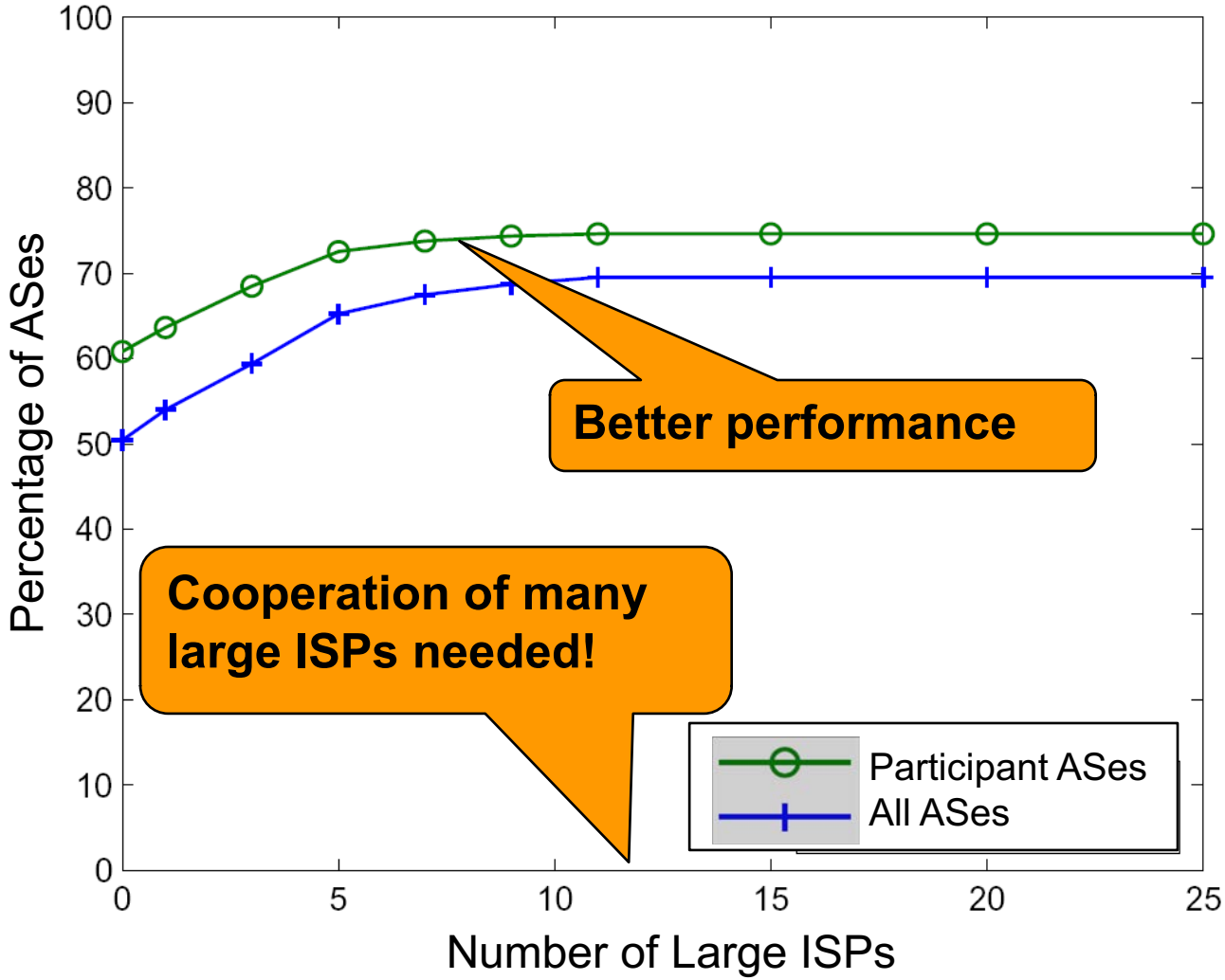
Experimental Setup – All Experiments

- **Method – simulation of BGP announcements on the AS-level Internet topology**
  - **Topology information from RouteViews**
  - **Adversary and origin chosen at random**
  - **Participants implement secure protocol**
  - **1 or 5 adversaries**
- **Performance metric – fraction of the Internet ASes with valid routes**
  - **Average of 100 runs**

soBGP – Random Participation, 1 adversary



soBGP – Deployment by 30 Random + Some Largest ISPs

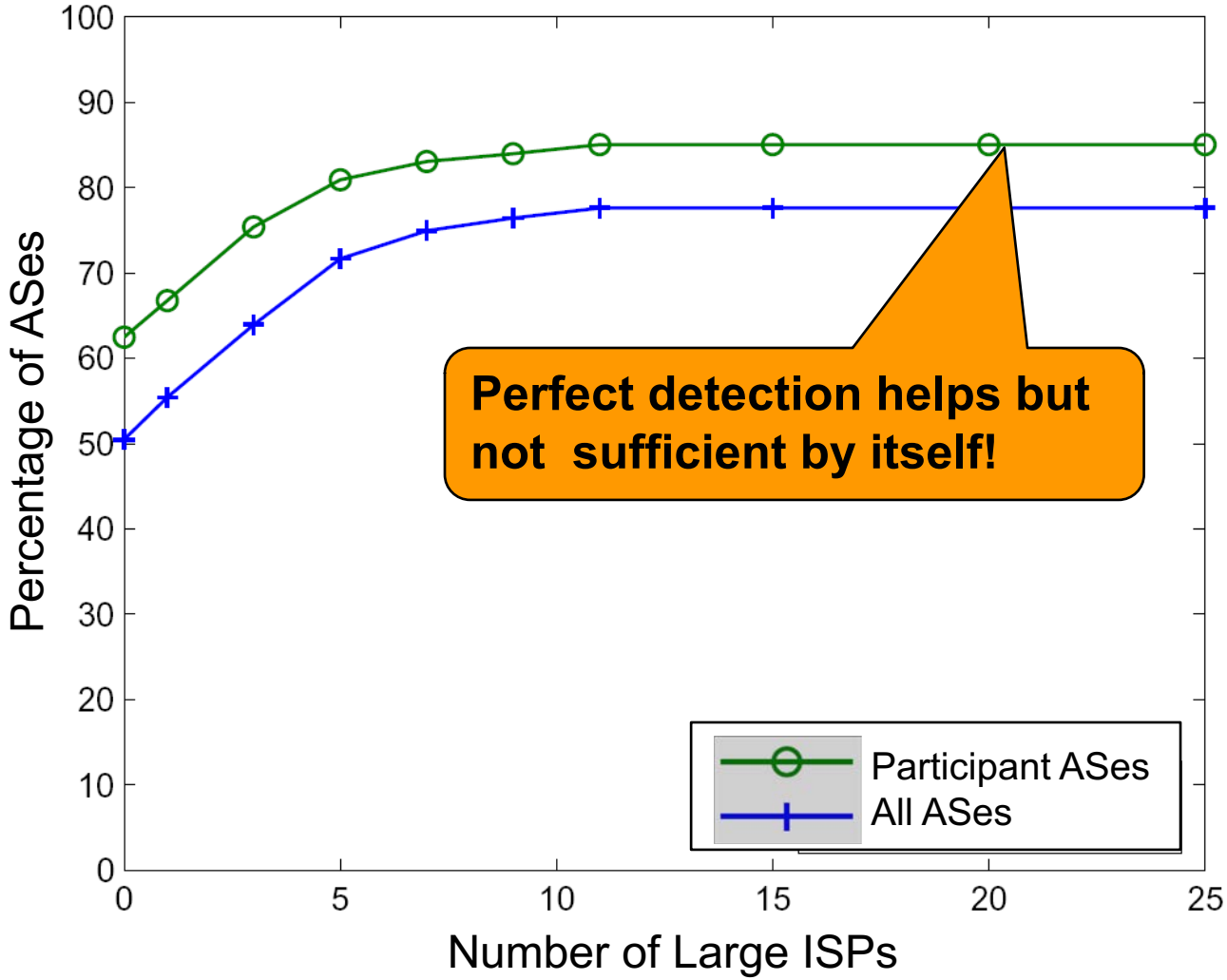


Perfect Detection

- **Simulations:** give ability to detect routes that don't work
  - Is this sufficient to secure routing?
  - How useful is it to have perfect detection?

- **Can be done in practice:**
  - Data-plane probing verifies validity of route by using it

Perfect Detection at 30 Random + Some Largest ISPs



Lessons Learned

Observation	Justification
Participation of large ISPs is important	They learn many routes some of which are valid
Perfect detection of bad routes is desirable	Better (but not ideal) performance
The non-participants are worse off than the participants	The participants reject implicated routes while non-participants accept all
Need to increase path diversity	Perfect detection not enough

Overview

I. The routing system and its vulnerabilities

II. Why should small groups secure BGP

III. Securing BGP in small groups – effectiveness of techniques

IV. **Our approach**

   a) **Sbone – secure overlay routing**

   b) **Shout – hijacking the hijacker**

V. **Conclusion**

Our Approach – Key Ideas

- **Circumvent the adversary with secure overlay routing**
- **Hijack the hijacker: all participants announce the protected prefix**
- **Hire a few large ISPs to help**
- **Detect invalid routes accurately with data plane detectors**

Our Approach – Key Ideas

- **Circumvent the adversary with secure overlay routing**
- **Hijack the hijacker: all participants announce the protected prefix**
- **Hire a few large ISPs to help**
- **Detect invalid routes accurately with data plane detectors**

Our Approach – Key Ideas

- **Circumvent the adversary with secure overlay routing**
- **Hijack the hijacker: all participants announce the protected prefix**
- **Hire a few large ISPs to help**
- **Detect invalid routes accurately with data plane detectors**

Our Approach – Key Ideas

- **Circumvent the adversary with secure overlay routing**
- **Hijack the hijacker: all participants announce the protected prefix**
- **Hire a few large ISPs to help**
- **Detect invalid routes accurately with data plane detectors**

Overview

I. The routing system and its vulnerabilities

II. Why should small groups secure BGP

III. Securing BGP in small groups – effectiveness of techniques

IV. Our approach

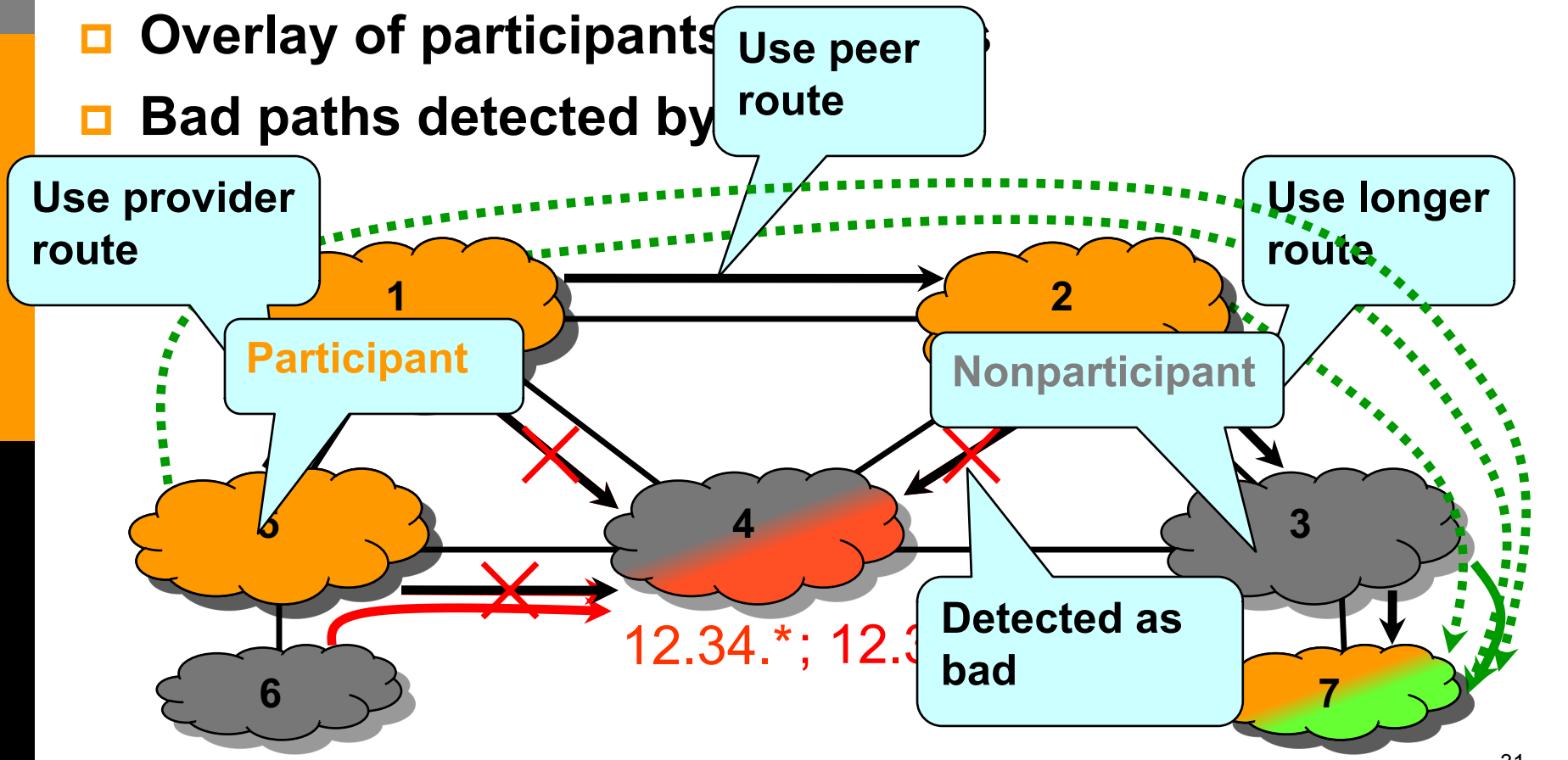
   a) SBone – secure overlay routing

   b) Shout – hijacking the hijacker

V. Conclusion

Secure Overlay Routing (SBone)

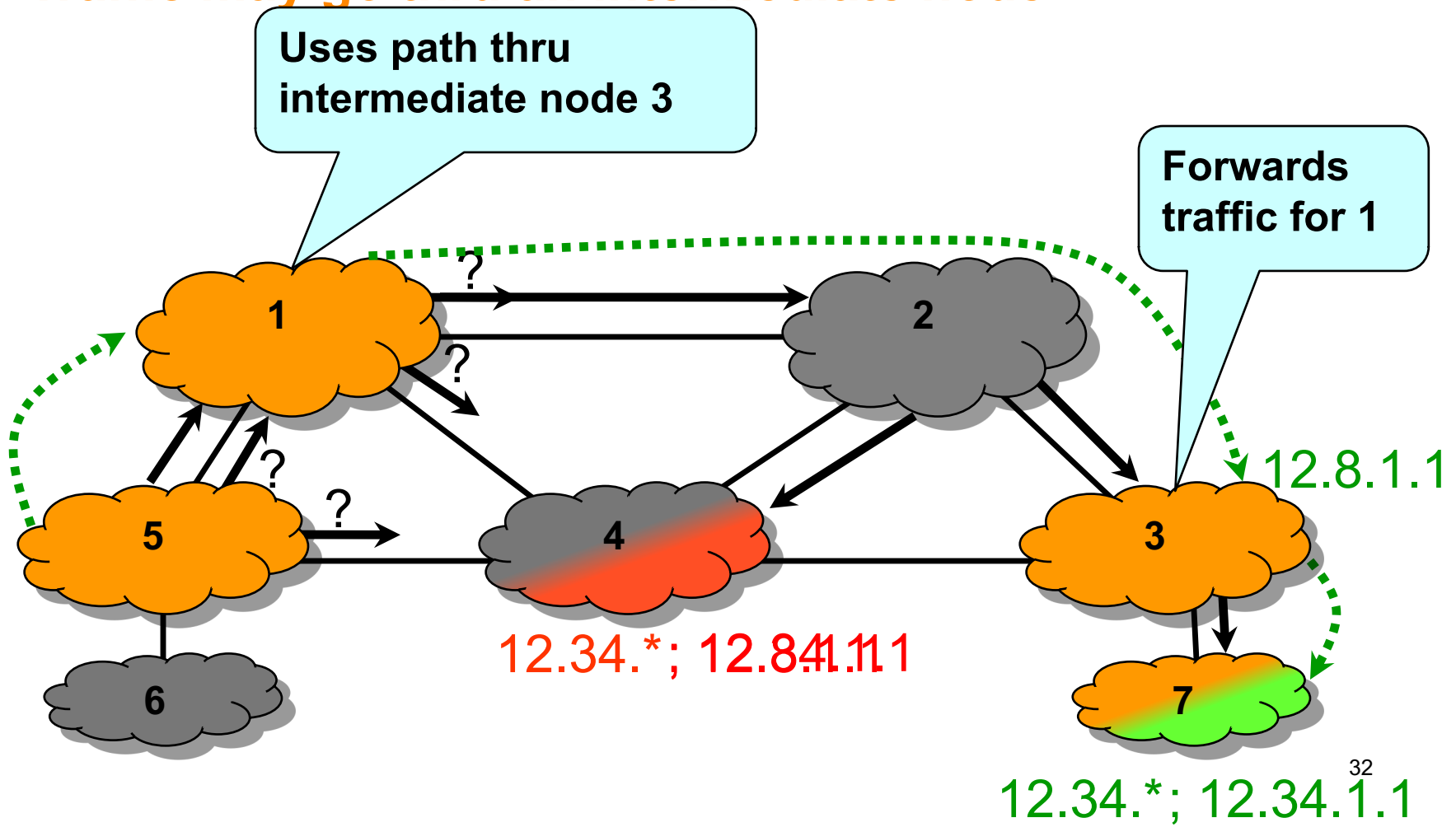
- Protects intra-group traffic
- Overlay of participants
- Bad paths detected by



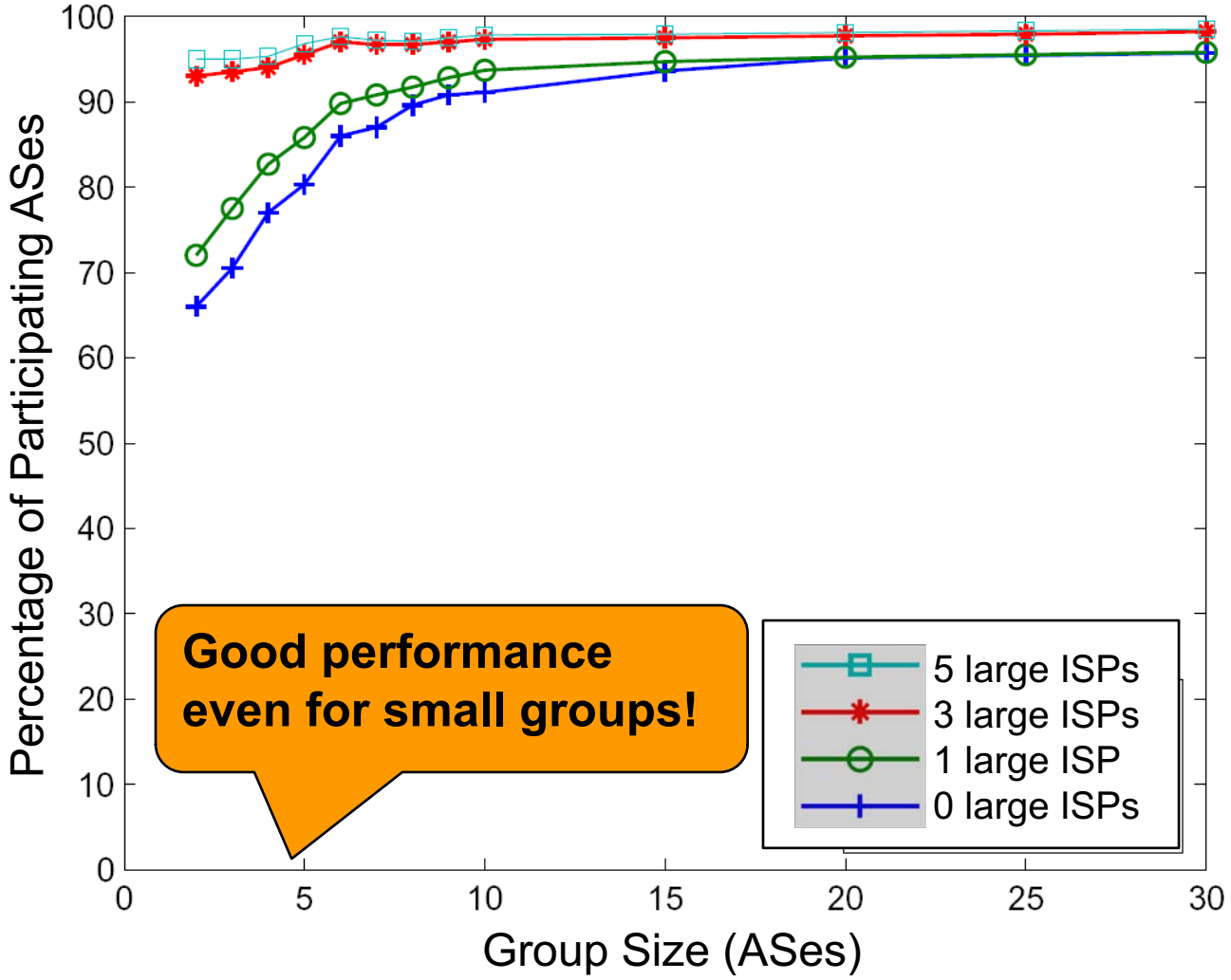
12.34.*; 12.34.1.1

Secure Overlay Routing (SBone)

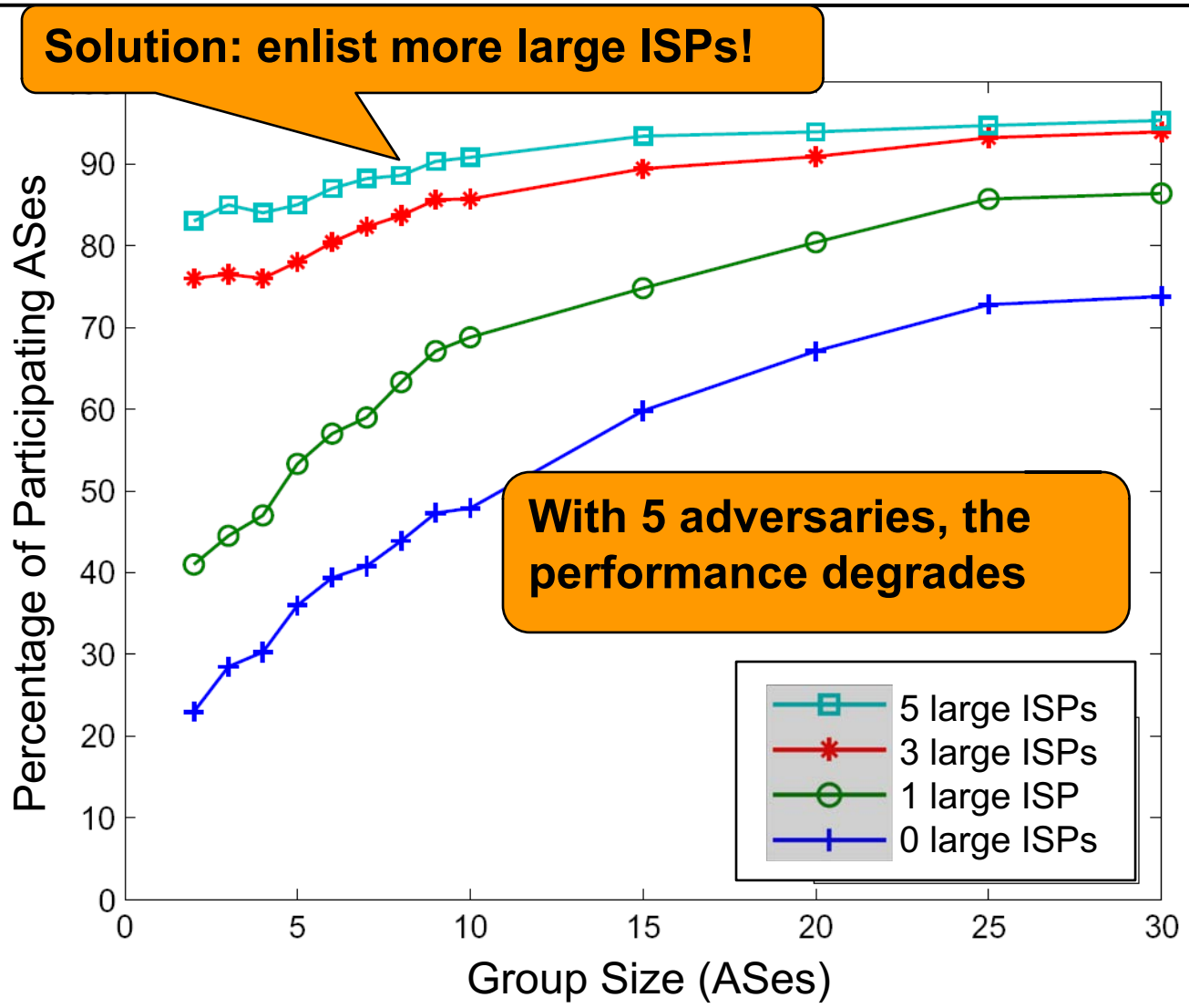
- Traffic may go thru an intermediate node



SBone – 30 Random + Help of Some Large ISPs



SBone – Multiple Adversaries



SBone - Summary

Observation	Justification
SBone offers good availability even for very small groups	It better exposes path diversity
Non-participants are not secure yet	They lack the ability to tunnel around problems

Overview

I. The routing system and its vulnerabilities

II. Why should small groups secure BGP

III. Securing BGP in small groups – effectiveness of techniques

IV. Our approach

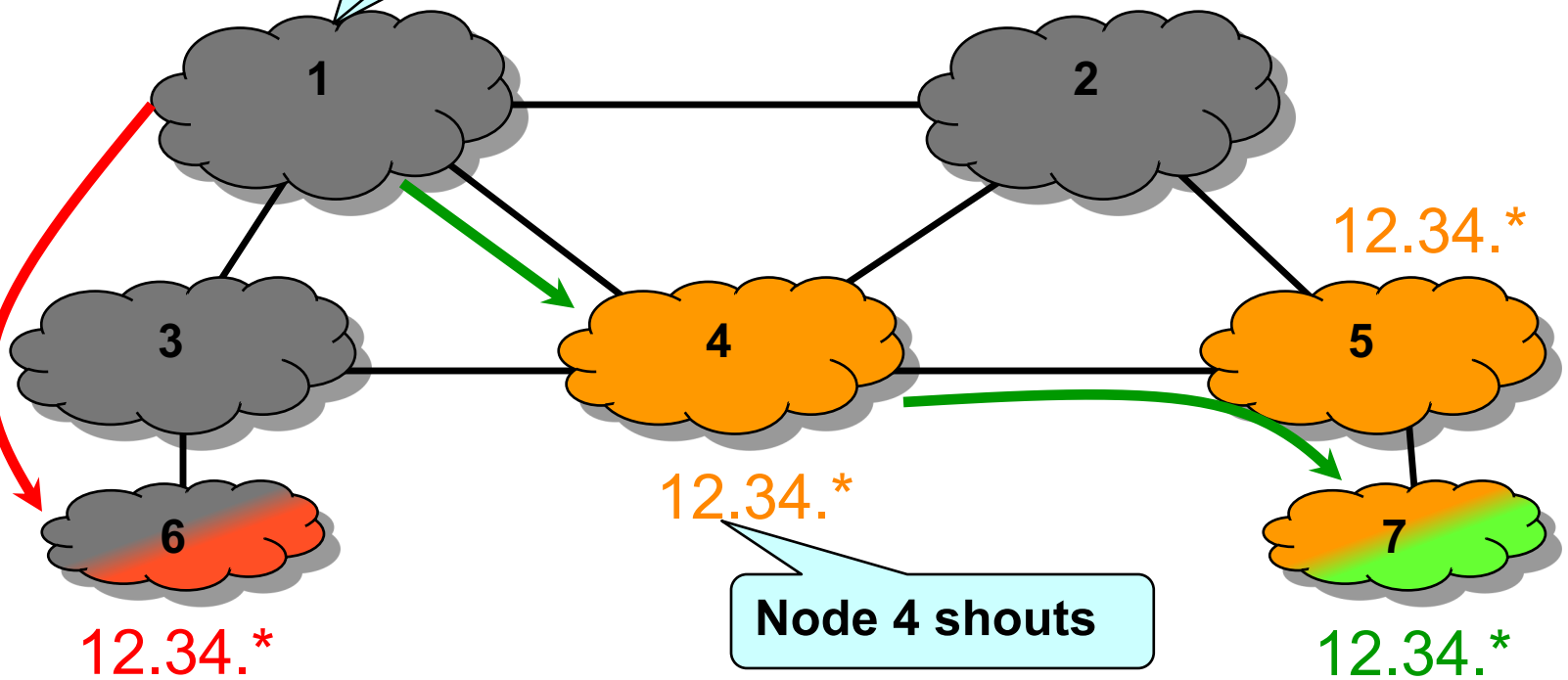
   a) SBone – secure overlay routing

   b) Shout – hijacking the hijacker

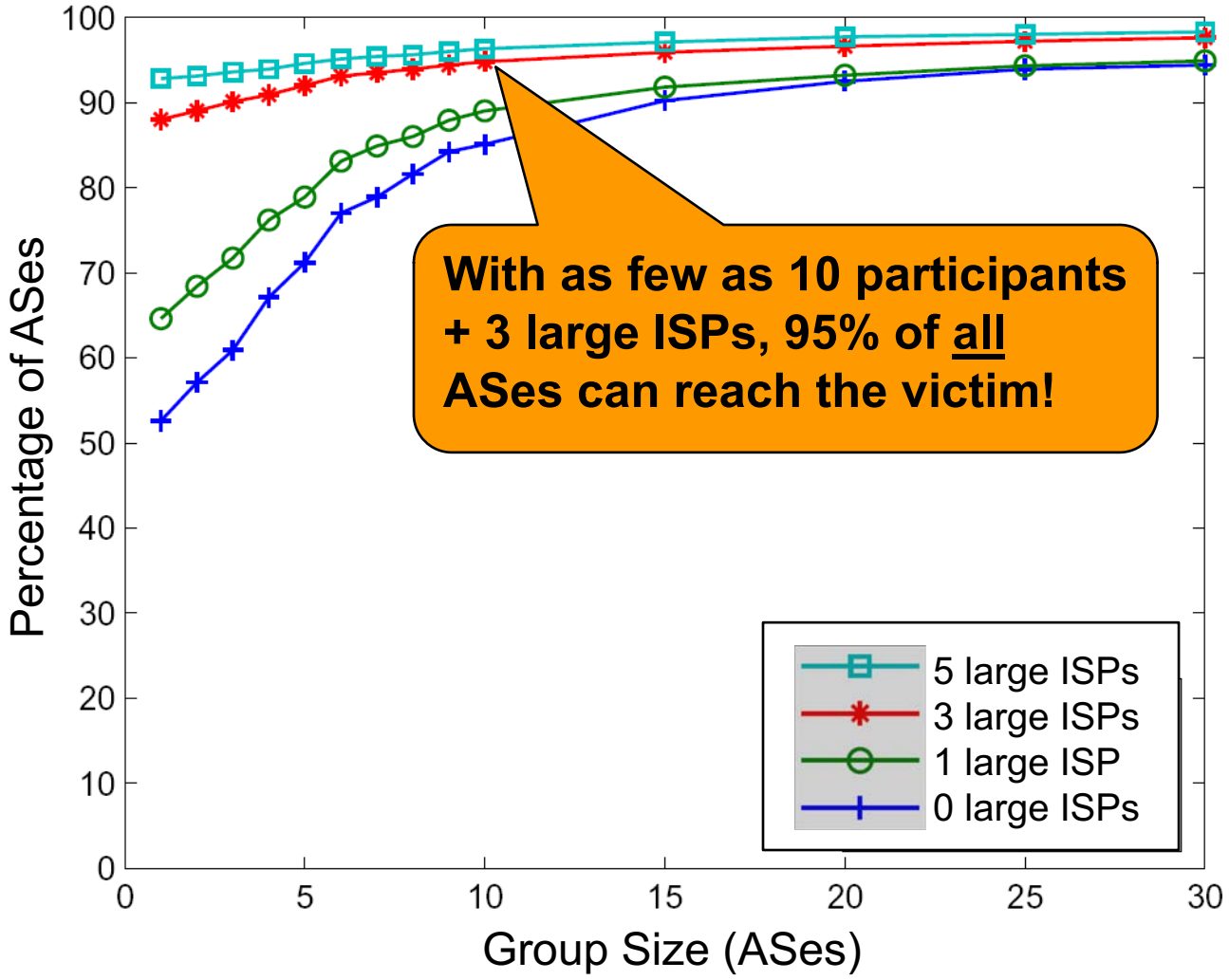
V. Conclusion

Hijacking the Hijacker – Shout

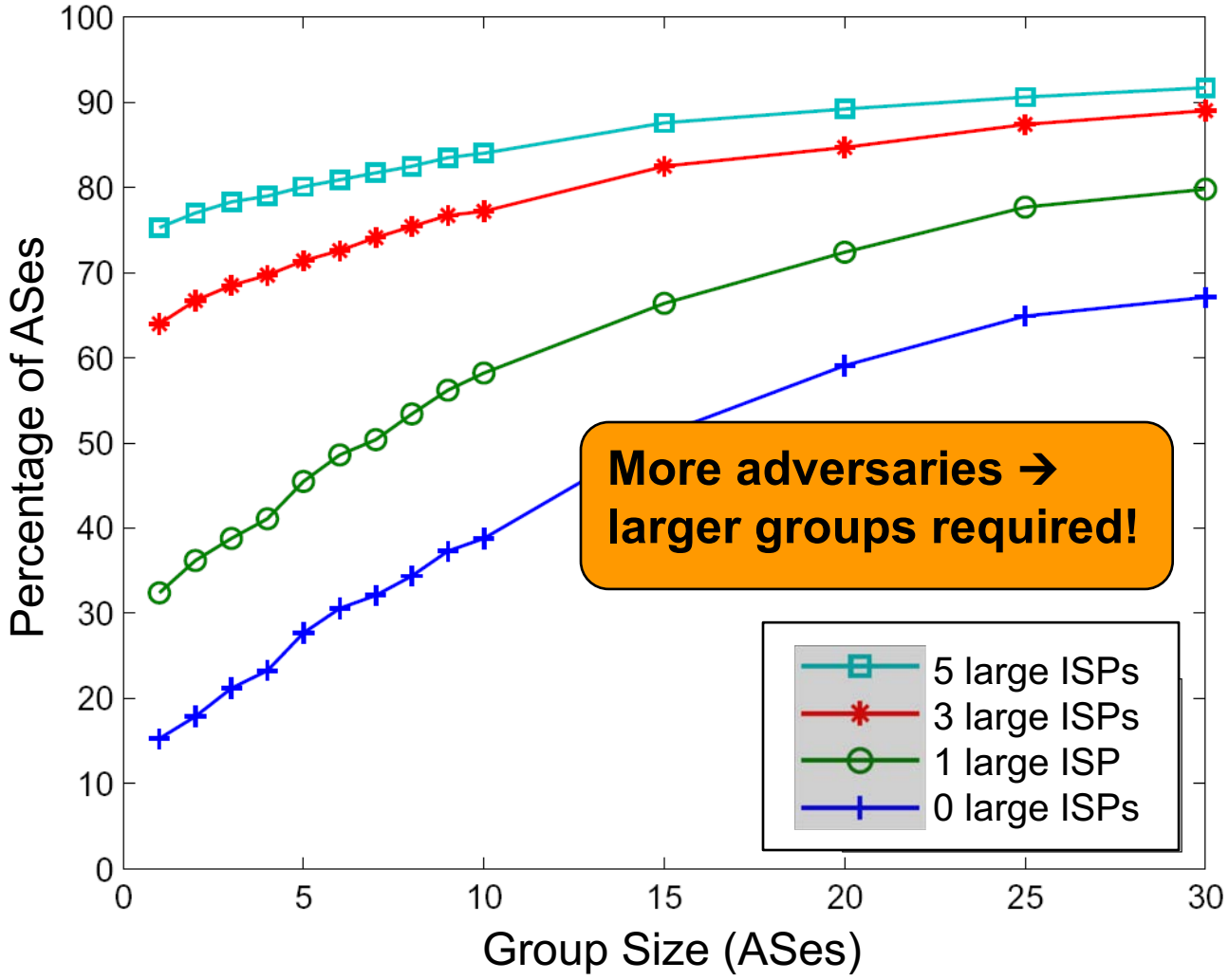
- Secure traffic from non-participants
- All partic… …ner's …tected prefix
- Once the… …, it is securely forwarded t… …e true prefix owner



Shout + SBone – 1 Adversary



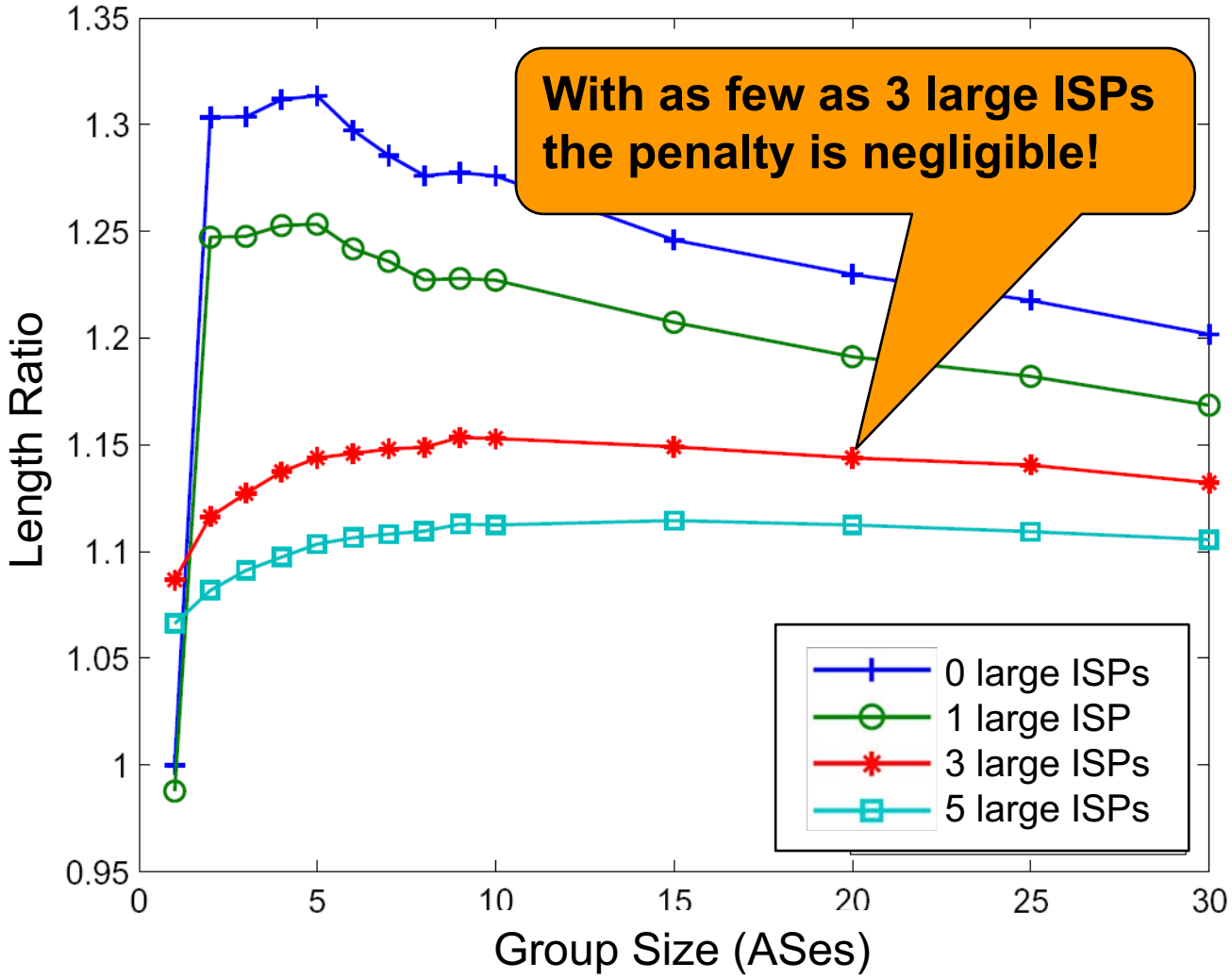
Shout + SBone – 5 Adversaries



Performance and Scalability of Shout

- Shout can be used reactively
  - Only shout if an attack is detected
- Changes in routing table sizes negligible
  - Alternate routes must be saved in routing tables
  - The average table size increased by less than 5%
- After shouting path lengths increase modestly
  - Paths less than 1.35 times longer
  - Detailed results next

Shout + SBone – Increase in Path Length



Shout - Summary

Observation	Justification
Can secure communication from non-participants	It suffices if non-participant reaches any participant
Routing table sizes do not increase	Increases < 5%
Shout does not inflate path lengths significantly	Path lengths increase by <15% with 3 large ISPs

Overview

I. The routing system and its vulnerabilities

II. Why should small groups secure BGP

III. Securing BGP in small groups – effectiveness of techniques

IV. Our approach
   a) SBone – secure overlay routing
   b) Shout – hijacking the hijacker

V. Conclusion

Conclusion

- **BGP should be secured by small groups**

- **To be effective, the group members should**

(i) Detect and filter compromised routes accurately
(ii) Cooperate to expose path diversity
(iii) Coax non-participants to pick valid routes
(iv) Enlist a few large ISPs

Conclusion

- **SBone and Shout are novel mechanisms that achieve these goals**
- **The proposed solution**

(i)	Secures address space of a small group of participants
(ii)	Allows both participants and non-participants pick valid routes
(iii)	Provides incentives to the adopters

Future Work

- Deployment in larger groups where participants don't trust each other
  - Secure routing protocol on the overlay?
- Analytic models of the deployment
  - Predict which additional ASes to enlist to boost performance?
  - Effects of the structure of the graph on the outcomes?

Thank you for your attention!

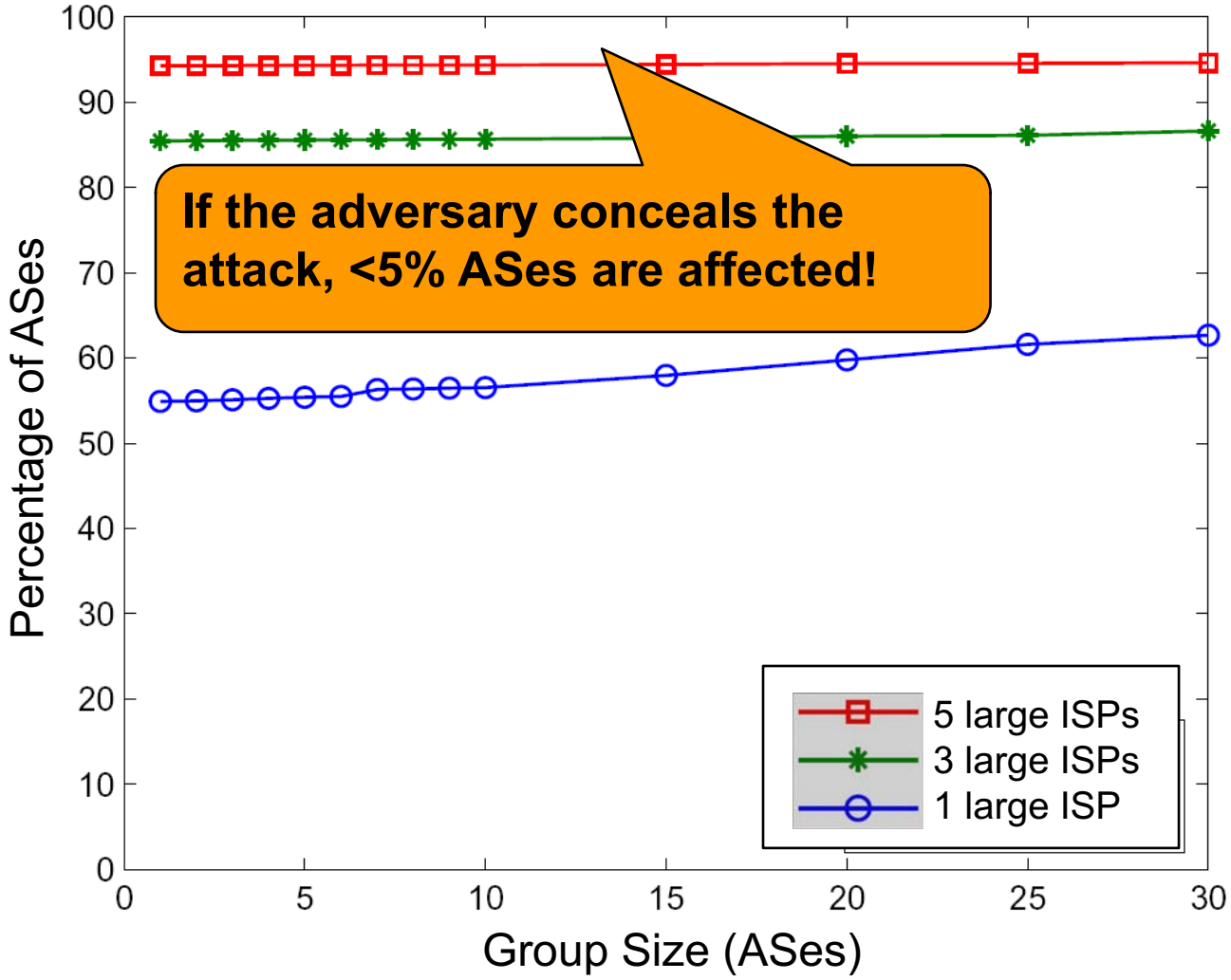
Discussion

1. **Effects of subprefix hijacking**
2. **What if participants not willing to choose less profitable routes?**
3. **What if N large ISPs are used instead of N largest ones?**
4. **Average results and error bars**

1. Subprefix Hijacking

- **Threat: adversary deaggregates the victim's prefix, all traffic is directed to the adversary**
- **Key security mechanisms**
  - **Deaggregate the prefix and use shout to announce it**
  - **Tunnel endpoints already secure if announced with /24 prefixes**
- **Only deaggregate when attack detected**
- **Attack detected if at least one participant sees an unauthorized subprefix**

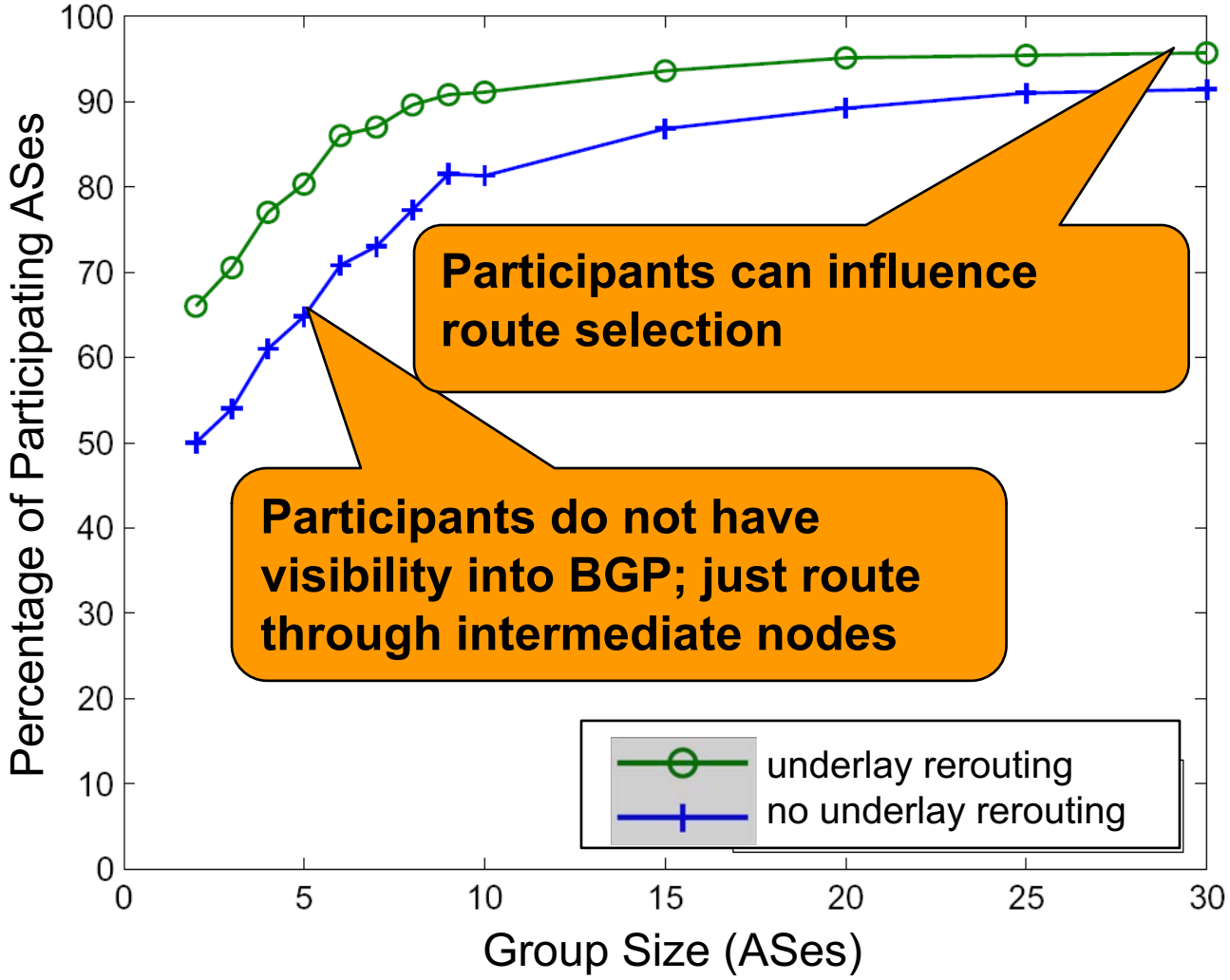
1. Subprefix Hijacking – Avoiding Detection



1. Subprefix Hijacking - Summary

Observation	Justification
Can secure against subprefix hijacking	Deaggregation in addition to shout
Low overhead	Reactive scheme used only if attack detected
Detection is accurate	Large ISPs have good connectivity and learn the offending sub-prefix easily

2. SBone – Preserve Business Relationships?



3. Effect of Choosing the Largest ISPs

- **The largest ISPs are similar in terms of connectivity and size**
- **Which one of these we enlist among the participants does not matter much**

SBone vs. Perfect Detection Alone