Even Rockets Cannot Make Pigs Fly Sustainably

Can BGP be Secured with BGPsec

Qi Li, ETH Zurich

Yih-Chun Hu, UIUC

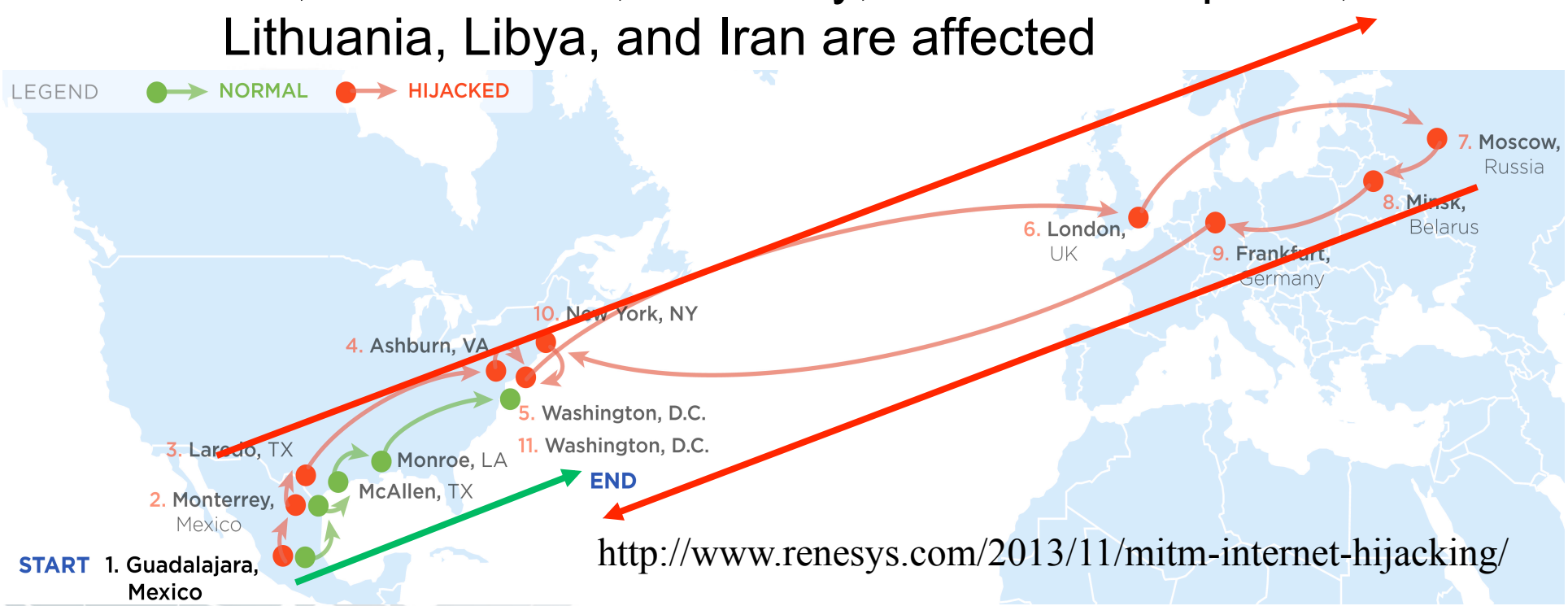
Xinwen Zhang, Huawei Research

BGP Is Not Secure

- The Border Gateway Protocol (BGP) is the de-facto protocol to ensure the inter-AS connectivity of the Internet
- BGP does not have built-in mechanisms to verify if a route is genuine, it suffers from severe security vulnerabilities
- To prevent false routing updates, a wide array of secure BGP schemes has been proposed
- This study will investigate the vulnerabilities of these schemes

An Attack Example

- In February 2013, global traffic was redirected to Belarusian ISP
  - US, South Korea, Germany, the Czech Republic, Lithuania, Libya, and Iran are affected



http://www.renesys.com/2013/11/mitm-internet-hijacking/

Background

- BGPsec is recently proposed by IETF
  - Leverage Resource Public Key Infrastructure (RPKI) to authenticate prefix origins
  - Insert correct AS number with the AS link signature into routing paths
- Insufficient security of BGP security schemes
  - Manipulation attacks: good routes are damped (Song et al. 2013)
  - Cheating attacks: traffic forwarding paths are deviated from the announced paths (Goldberg et al. 2008)

Y. Song, A. Venkataramani and L. Gao. "Identifying and Addressing Protocol Manipulation Attacks in ``Secure" BGP", ICDCS 2013

S. Goldberg, S. Halevi, A. D. Jaggard, V. Ramachandran, and R. N. Wright, “Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP,” Proceedings of SIGCOMM 2008

Contribution of This Paper

- Investigate a set of security properties of BGP
  - Routing availability, Path predictability, Blackhole-resistant routing, and Loop-free routing
- Show that BGPsec is unable to achieve the security properties
- Identify two new vulnerabilities of BGPsec and use real data to measure the impacts of the vulnerabilities

Desirable Security Properties (1)

- Routing availability
  - Ensure convergence in the presence of different network events, e.g., routing attacks
  - Throttle the manipulation attacks and data plane attacks
- Path predictability
  - Senders know the path that traffic will traverse before sending out the traffic
  - Ensure that forwarding table is consistent with routing updates

Desirable Security Properties (2)

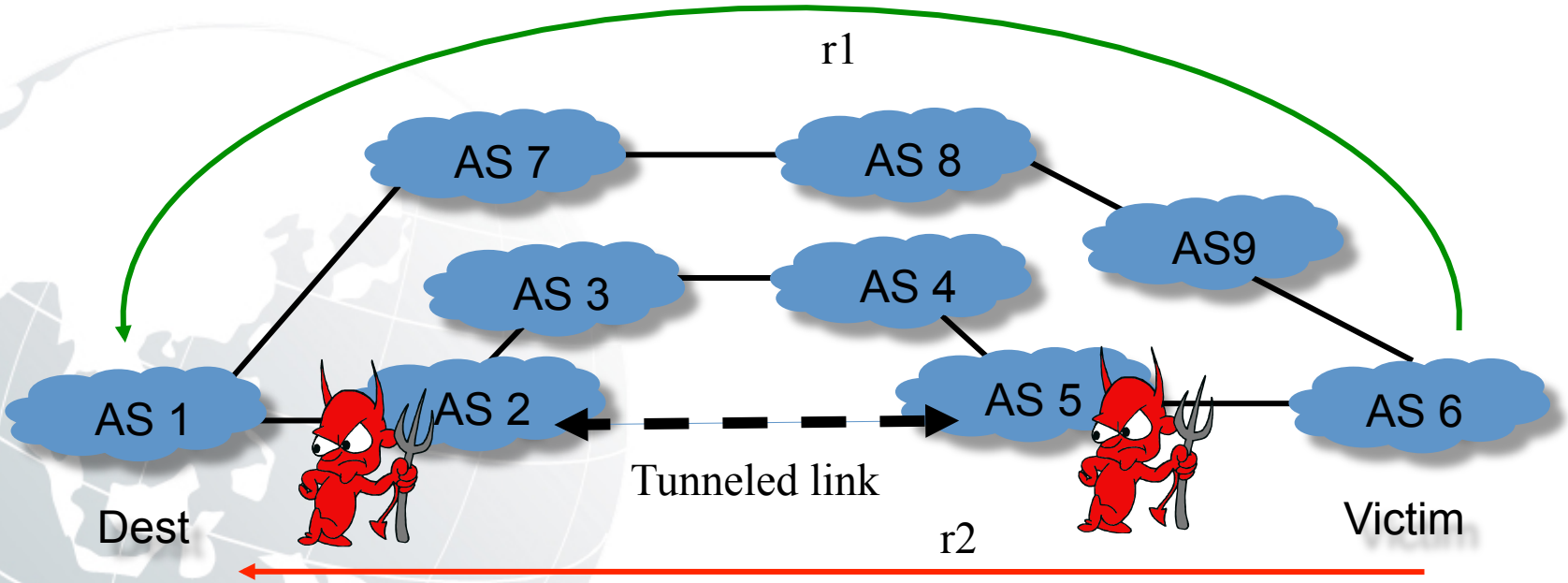
- Blackhole-resistant routing
  - A blackhole is used to hijack traffic to an AS that would not traverse that AS.
  - Prevent malicious AS from traffic hijacking to blackholes
- Loop-free routing
  - No traffic will enter a forwarding loop even under attacks
  - Network links will not be overloaded by such forwarding loops

Insufficiency of BGPsec

- Existing attacks show the first two properties do not hold in BGPsec
  - Routing availability: manipulation attacks
  - Path predictability: cheating attacks
- This talk will show that the last two security properties are not met by BGPsec
  - Blackhole-resistant routing: traffic hijacking by launching wormhole attacks
  - Loop-free routing: forwarding loops by launching mole attacks

Wormhole Attack

- Colluding Ases generate fake links with valid signatures
  - produced forged routing paths

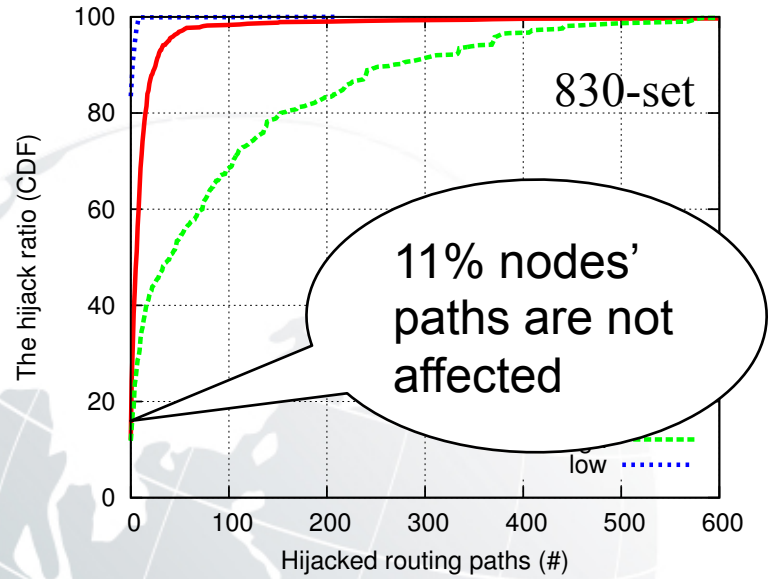


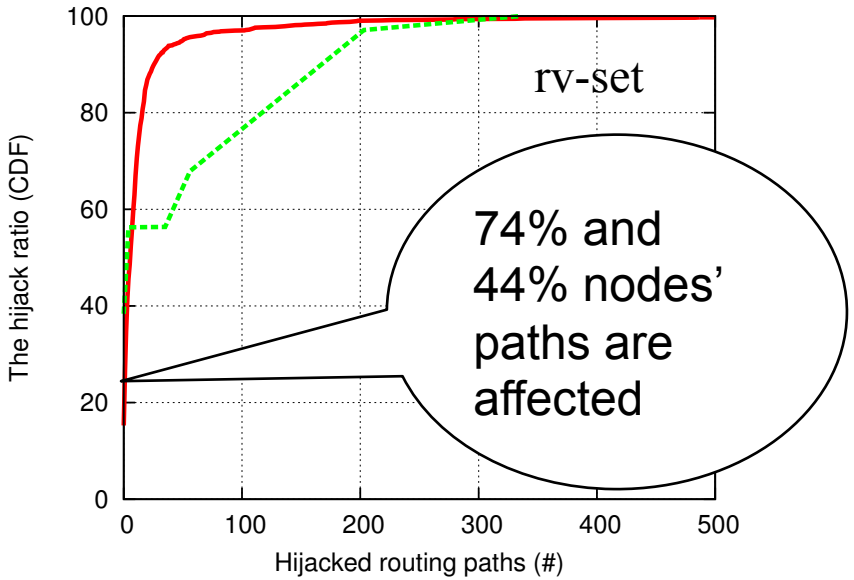
Evaluation

- Simulation based on two different measured Internet AS topology set
  - The 830-set and rv-set AS topologies
- Compute all end-to-end routing paths by simulating BGP routing according to Gao-Rexford conditions
- Measure routing paths with different attack scenarios by selecting 10 AS pairs with different degree as colluding Ases

Impact of Wormhole Attacks

- The number of hijacked routing paths affected by the attacks



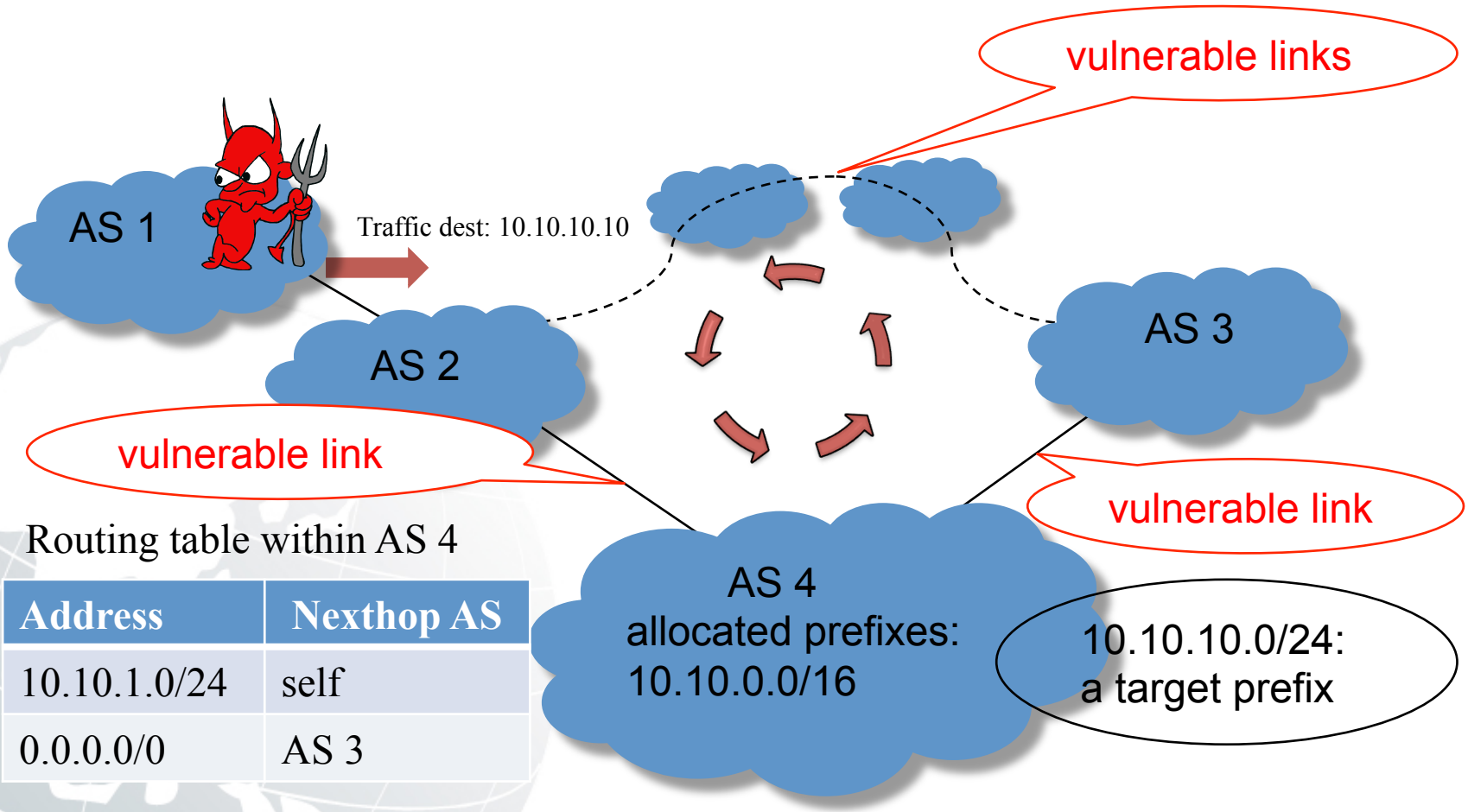


- BGPsec is unable to prevent hijacking attacks

Mole Attack

- An attacker can easily launch the mole attacks by generating traffic to the unused prefixes to overload the victim AS link
  - If a prefix is allocated to an AS and the AS does not fully consume it
  - If the Ases set a static default route to one of their providers
- To launch a mole attack and flood the target AS link, the attacker needs to locate a target prefix that will traverse the the vulnerable link

A Mole Attack Example



Routing table within AS 4

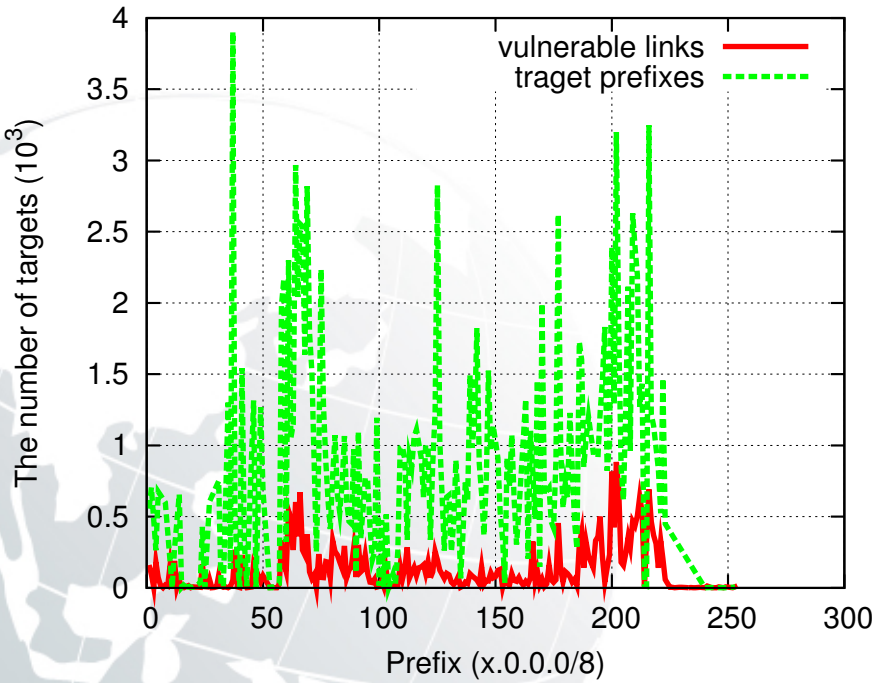
Address	Nexthop AS
10.10.1.0/24	self
0.0.0.0/0	AS 3

Evaluation

- Use traceroute to measure the routing paths to all /24 prefixes and use Routeview data to do prefix-to-AS mapping
- A target prefix is identified when the path to the prefix includes repeating AS links
- Measure the number of vulnerable links that can be the attack target and the number of target prefixes that can be used to attack the vulnerable links

Vulnerability to Mole Attacks

- The distribution of vulnerable links and target prefixes exhibit strong locality



- 170K /24 prefixes across the entire IPv4 address space can be used to flood the vulnerable links
- A vulnerable link can be flooded by using six /24 prefix blocks

Conclusion

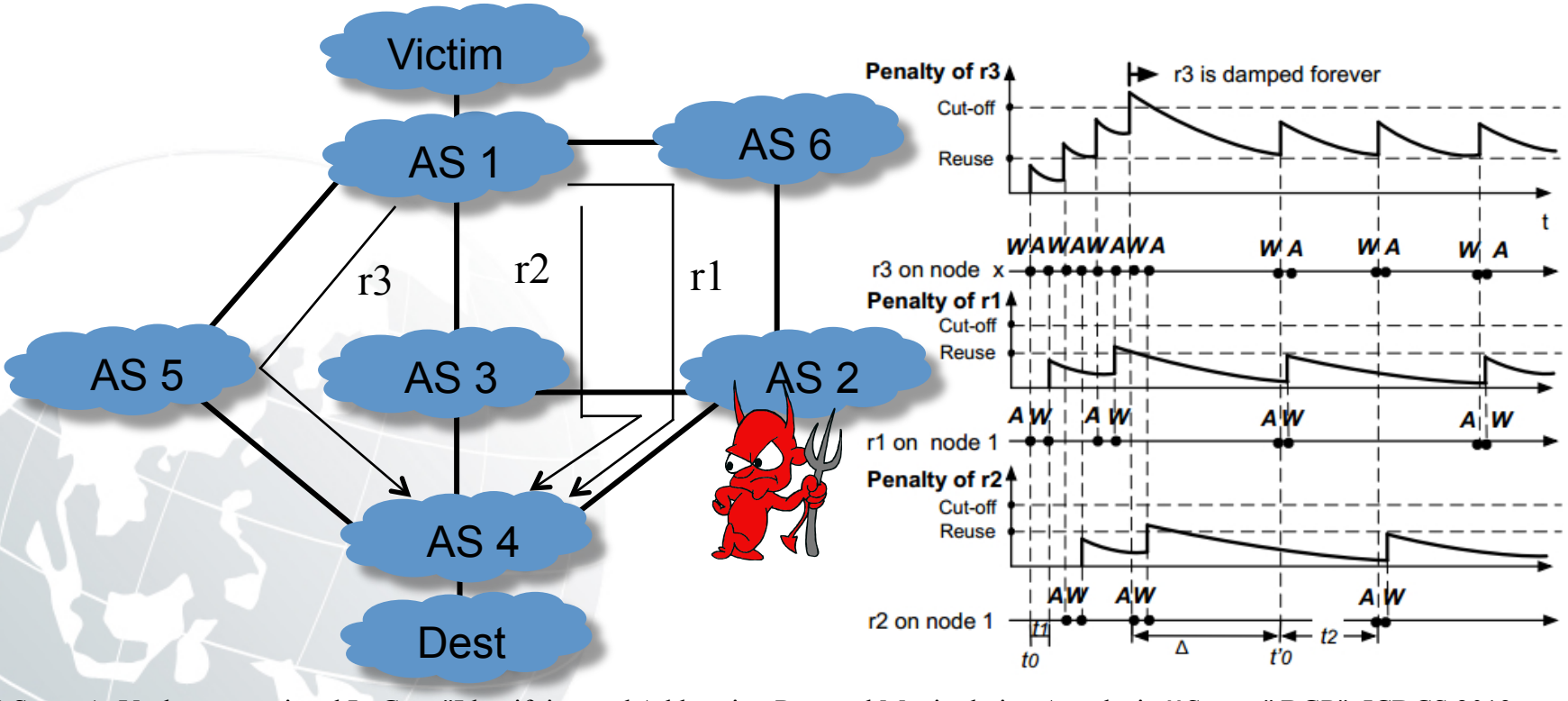
- We find that BGP armed with BGPsec cannot achieve any of the security properties due to their fundamental design principles
- We identify two new vulnerabilities of BGPsec
- We should rethink the fundamental tenets of BGP and BGPsec designs

Thank You!

Questions?

Backup: Manipulation Attack

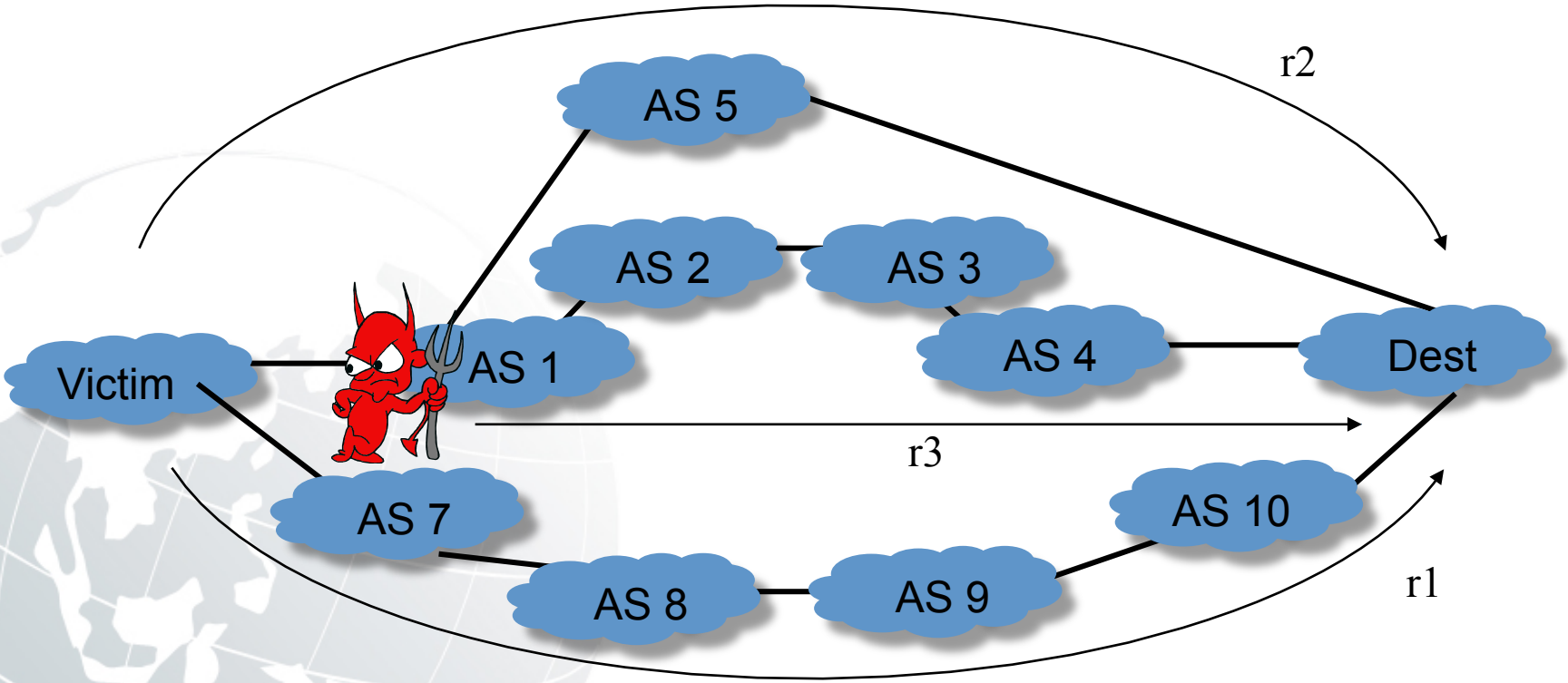
- Song et al. present protocol manipulation attacks to BGPsec, e.g., attacks to RFD and MARI



Y. Song, A. Venkataramani and L. Gao, "Identifying and Addressing Protocol Manipulation Attacks in ``Secure" BGP", ICDCS 2013

Backup: Cheating Attack

- Victim will adopt routing paths that they do not know (Goldberg et al. 2008)



S. Goldberg, S. Halevi, A. D. Jaggard, V. Ramachandran, and R. N. Wright, "Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP," Proceedings of SIGCOMM 2008.