

On the Feasibility of Rerouting-based DDoS Defenses

Muoi Tran, Min Suk Kang, Hsu-Chun Hsiao,
Wei-Hsuan Chiang, Shu-Po Tung, Yu-Su Wang
May 2019 | San Francisco, CA

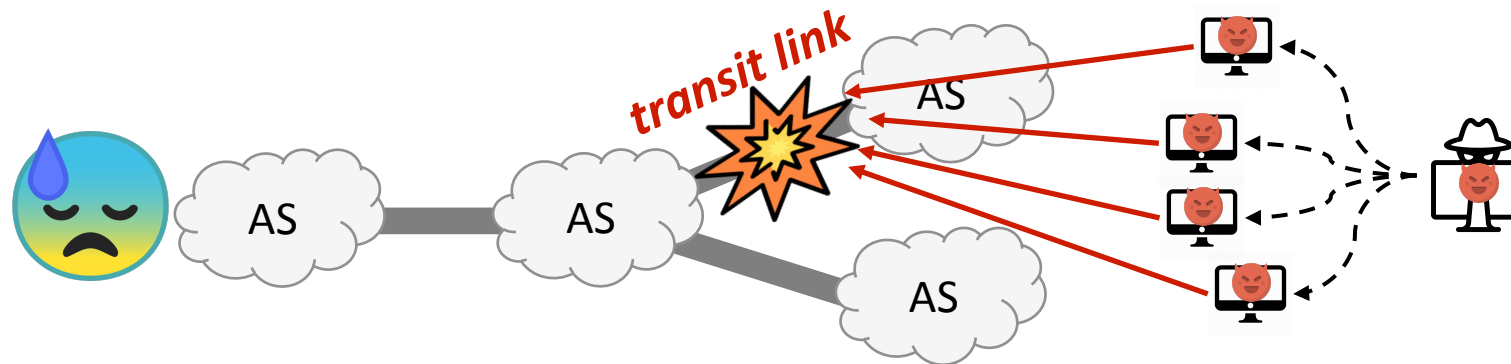


Transit-link DDoS attack: a powerful type of volumetric DDoS attack

(distributed denial of service)

Traditional: volumetric attack traffic targeting *end servers*

Non-traditional: volumetric attack traffic targeting *transit links*



Academic studies:

Coremelt attack
(ESORICS '09)

Crossfire attack
(S&P '13)

Real incidents:

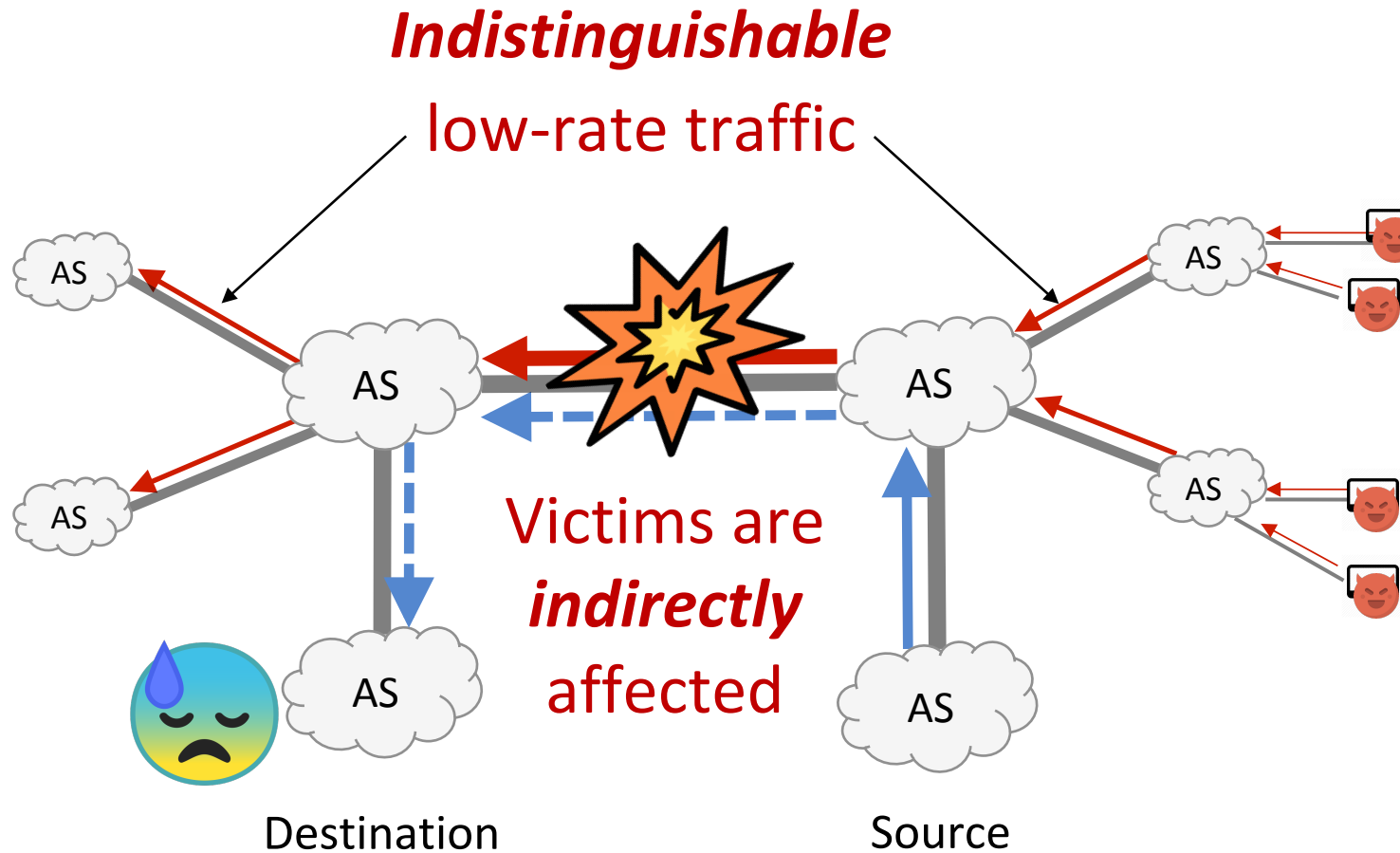
2013



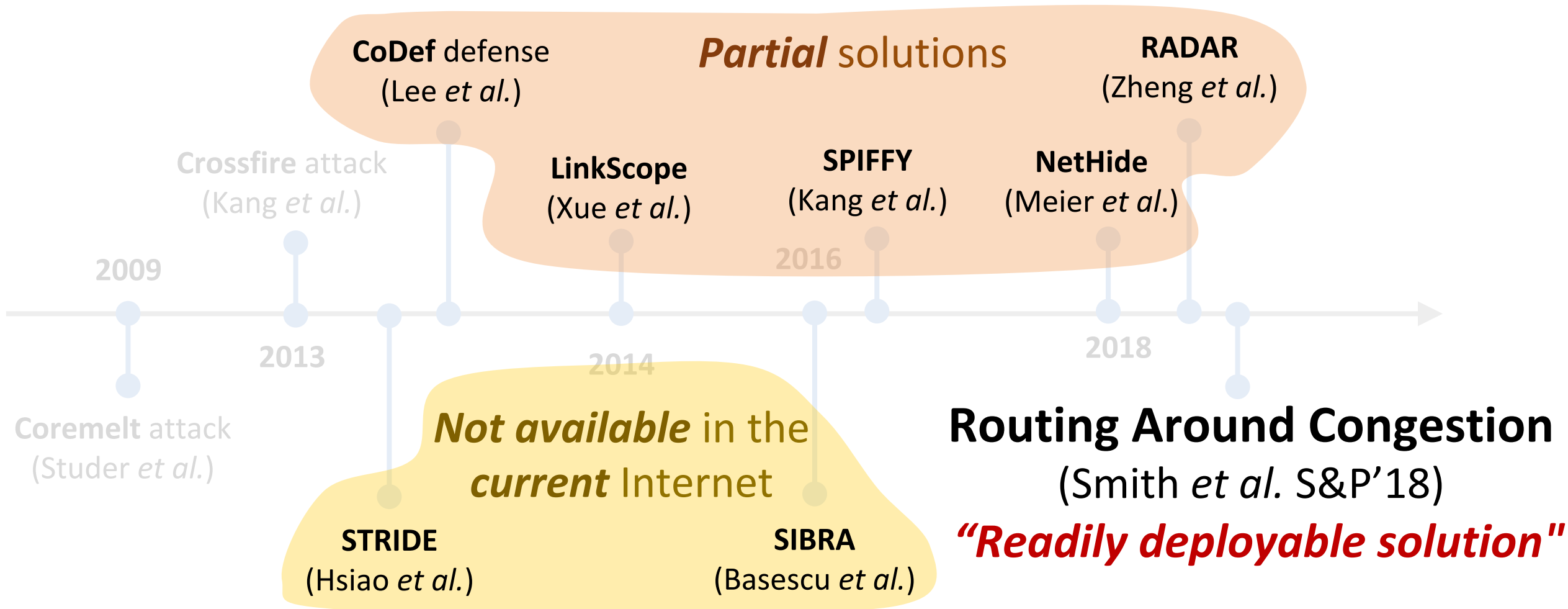
2015



Handling transit-link DDoS attack is *challenging*

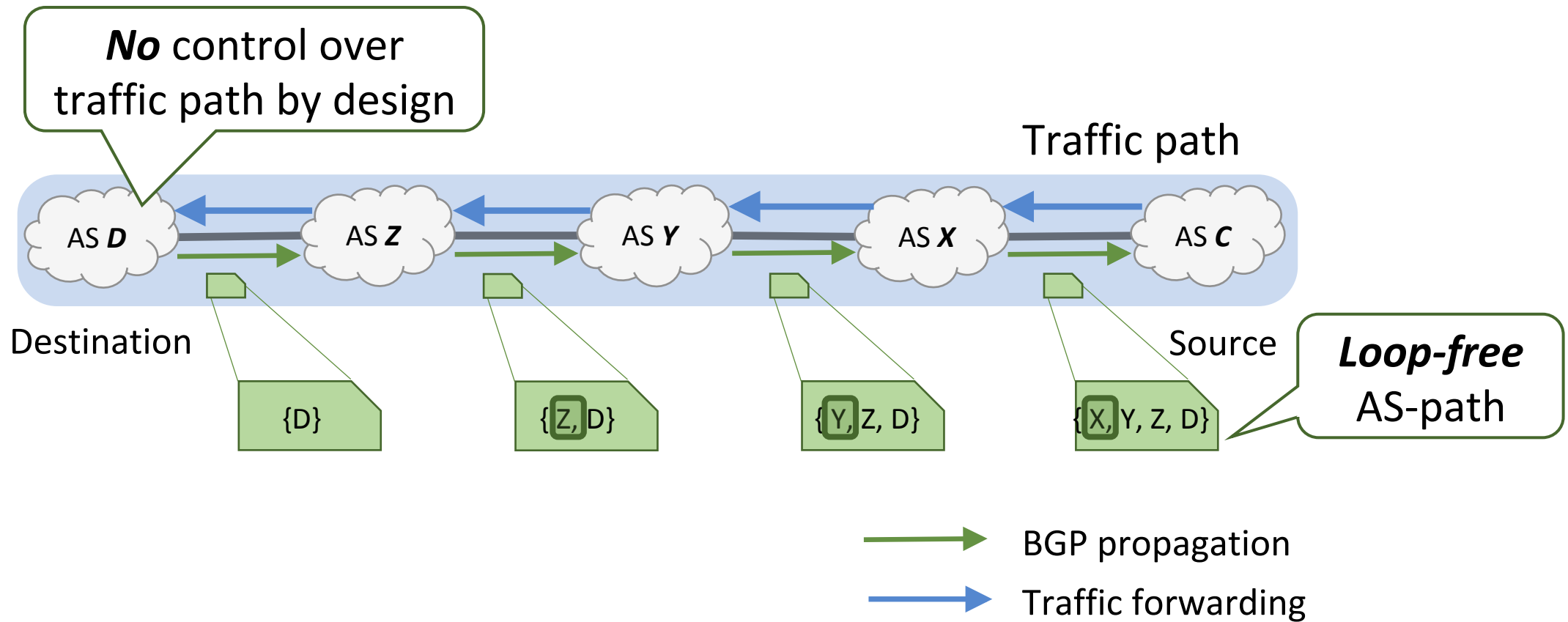


Transit-link DDoS attacks still remain an *open problem*



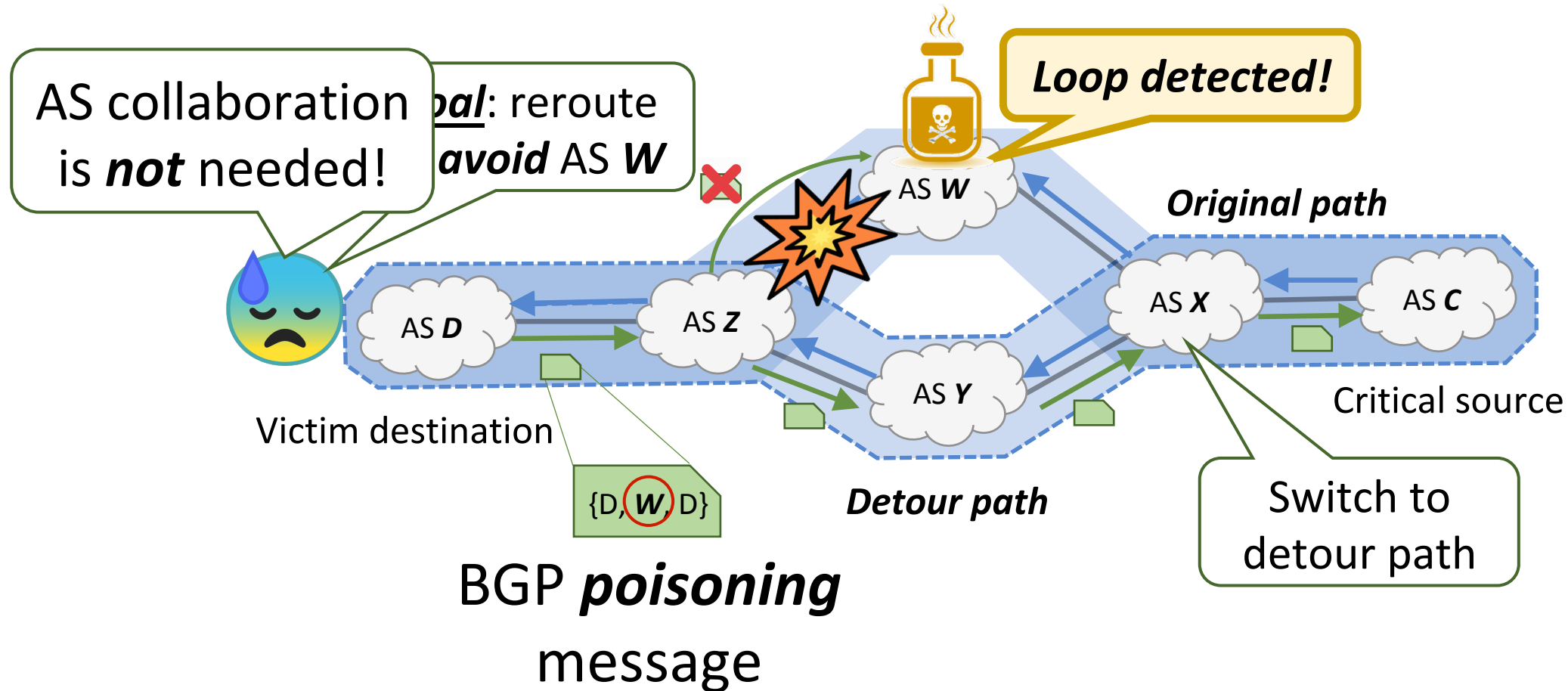
Background: How *BGP routing* works?

Border Gateway Protocol (BGP)



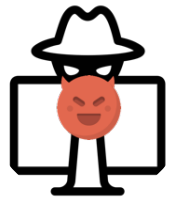
Routing Around Congestion (RAC):

Rerouting using BGP poisoning [Smith *et al.*, S&P '18]



Will ***RAC*** defense still work
against ***adaptive attackers***?

Our contributions



Adaptive detour-learning attack against rerouting solutions

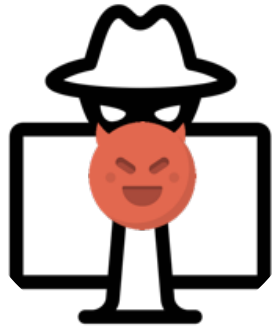


Practical challenge of mitigating adaptive detour-learning attack



Future directions for transit-link DDoS defenses

Adaptive detour-learning attack: Threat model



Goals:

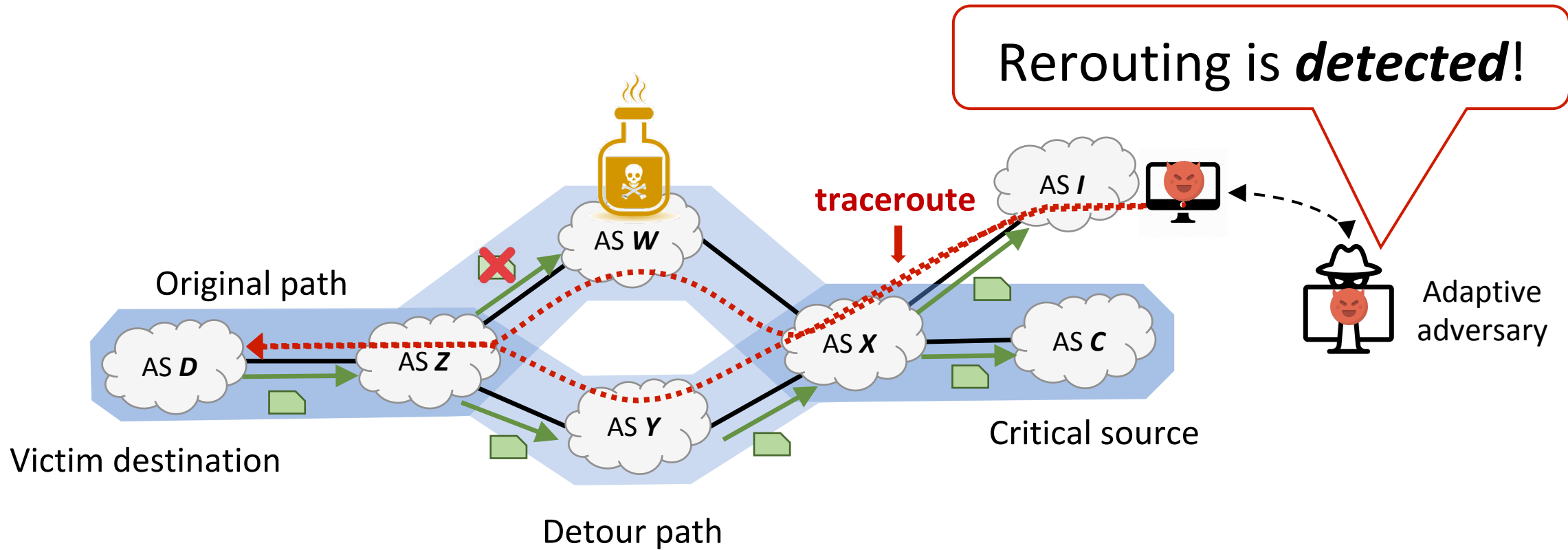
- (1) To detect rerouting in real-time
- (2) To learn new detour path accurately
- (3) To congest new detour path (see the paper)

Capabilities:

- Same botnets used in transit-link DDoS attack

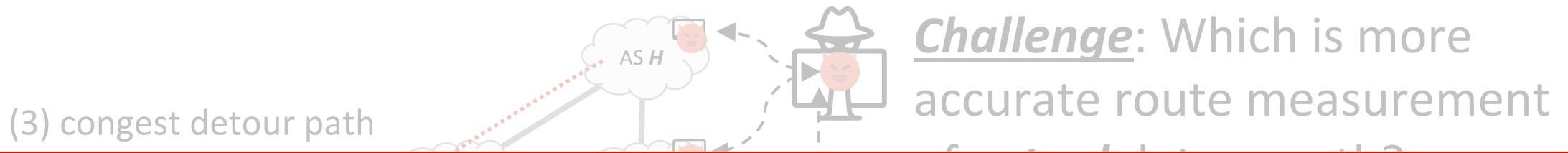
Adaptive detour-learning attack:

(1) how to ***detect*** rerouting in ***real-time***



Adaptive detour-learning attack:

(2) how to *learn* detour path *accurately*



Results: 94% of learned detour paths are correct



Our contributions



Adaptive detour-learning attack against rerouting solutions

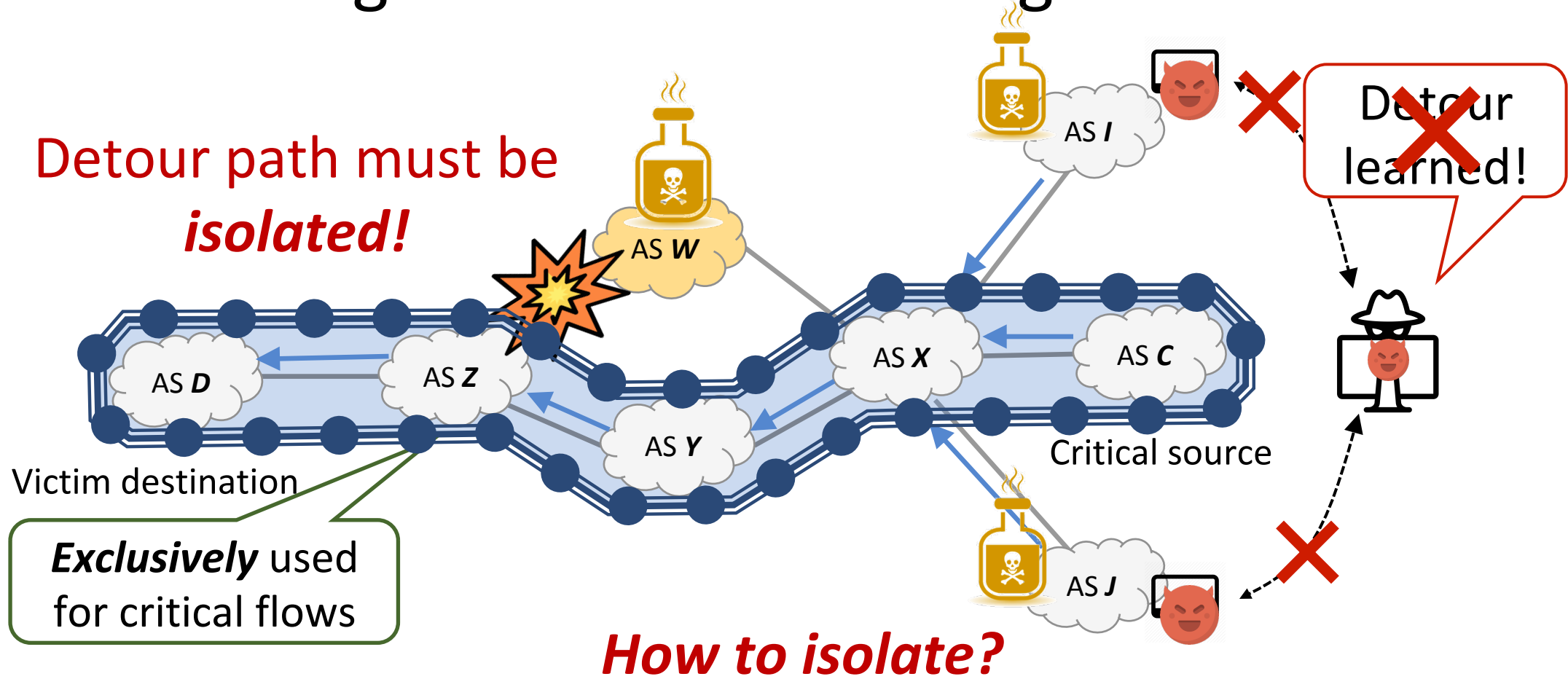


Practical challenge of mitigating adaptive detour-learning attack



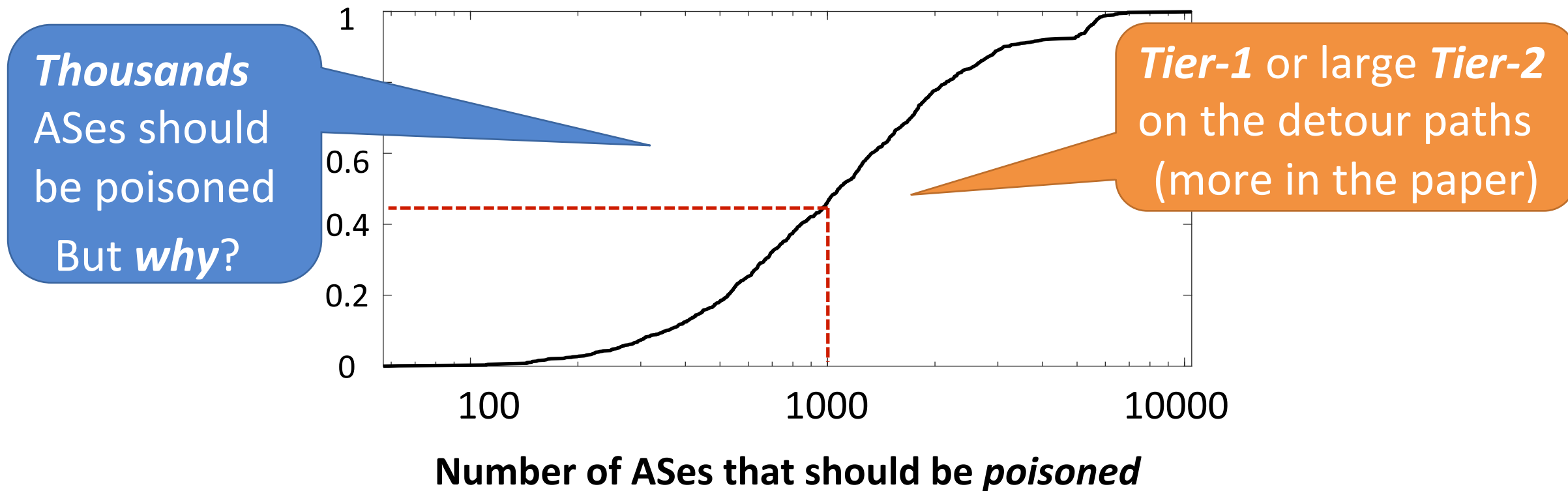
Future directions for transit-link DDoS defenses

How to defend against detour-learning attack?

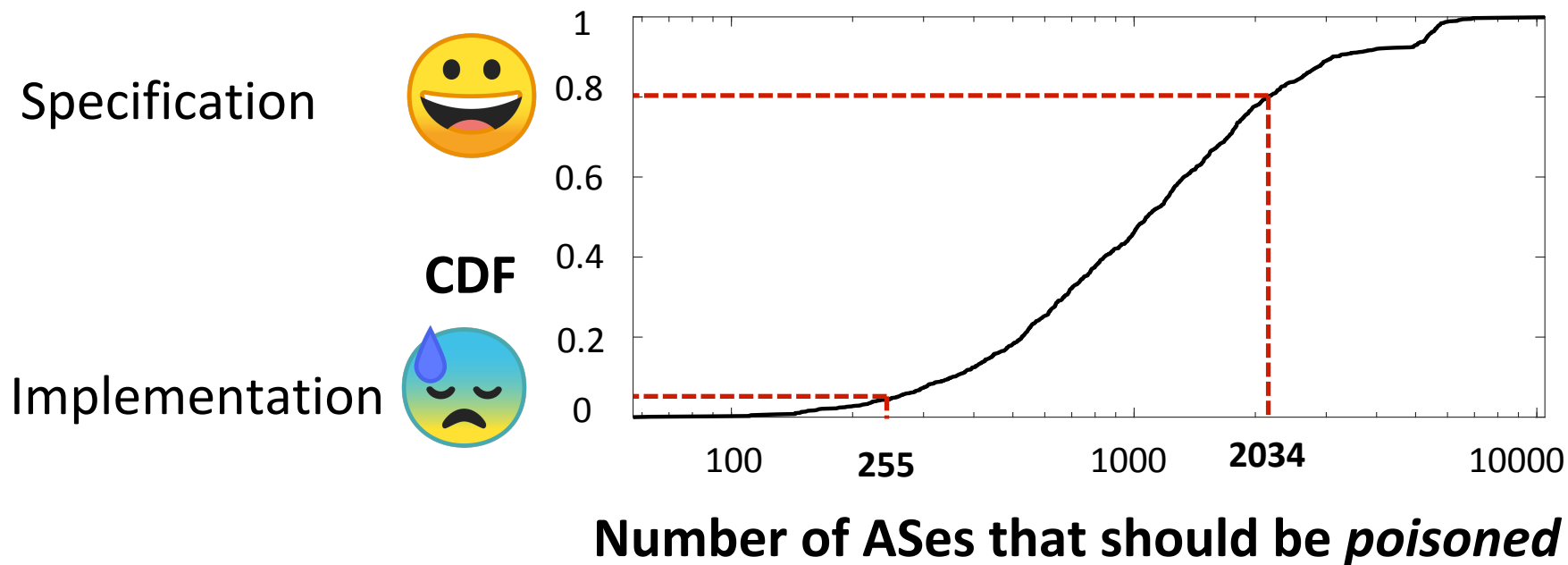


Poison all peers of ASes on detour path!

Detour path isolation => poisoning *too many* ASes



Can we poison that many ASes?



Specification



up to 2034

Implementation



up to 255

Configuration



up to 30-50

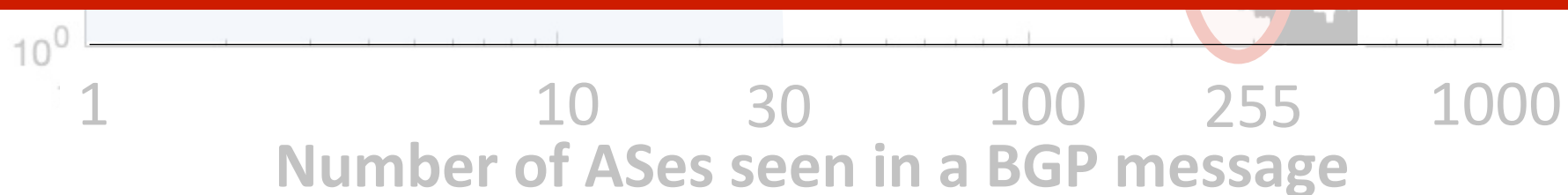
Confirmed: ISPs do not support poisoning > 255 ASes



Poisoning > 1,000 ASes is ***nearly impossible***

=> Detour path isolation is ***infeasible***

=> ***Detour-learning attack is almost always possible***



Our contributions



Adaptive detour-learning attack against rerouting solutions



Practical challenge of mitigating adaptive detour-learning attack



Future directions for transit-link DDoS defenses

Desired defense property: destination-controlled routing

Hacking BGP

e.g., Routing Around
Congestion

✗ Does not work

?

e.g., *explicit* BGP *rerouting*
for *critical* flows
under emergency

Clean-slate Internet
architecture

e.g., STRIDE, SIBRA

✗ Too costly to deploy

Two Lessons Learned

Lesson 1

Hacking the current Internet routing is a ***flawed*** idea!

- ✓ Adaptive attacks are possible
- ✓ Mitigation is hard
- ✓ Adaptive defense is slower than adaptive attacker (more in the paper)

Lesson 2

Analysis of protocol *specifications alone* is *insufficient!*

Specification



Implementation



Configuration



Conclusion

- ***Detour-learning attacks*** are ***effective*** and ***hard to mitigate***
 - ✓ Transit-link DDoS attacks still remain an open problem
- Suggestion on research direction
 - ✓ Balance ***destination-controlled routing*** and ***deployability***
- 2 lessons learned:
 - ✓ Hacking BGP for rerouting is a flawed idea
 - ✓ Analysis with specification only can be dangerous

Question?

Muoi Tran

muoitran@comp.nus.edu.sg

