Collaborative Network Security

Targeting Wide-area Routing and Edge-network Attacks

Rahul Hiran
Linköping University, Sweden
Supervisors: Nahid Shahmehri, Niklas Carlsson

LINKÖPING UNIVERSITY


Gmail
inbox.com
Windows Live
Aol.
ABN·AMRO
People's United Bank
Standard Chartered
BB&T
First National Bank
Commonwealth Bank
square 1 bank
KeyBank
TD Bank
JPMorganChase
OneWest Bank
RBC
QNB
Comerica Bank
WSFS bank
Bank of America
EverBank
BBVA Compass
BNP PARIBAS
Mechanics Bank
BridgeBank
COMMERZBANK
Santander
RBS
The Royal Bank of Scotland
Bradesco
City National Bank
EMBASSY BANK
Associated Bank
SBERBANK
STERLING BANK
Rabobank
Westpac
ROCKLAND TRUST
1-STBANK
HSBC
Danske Bank
First Interstate Bank
Cambridge Trust Company
ncb
CapitalOne
usbank
SVB
Investec
LLOYDS BANK
PNC
BROWN BROTHERS HARRIMAN
Alfa-Bank
ANZ
BBVA
SierraVista
ZIONS BANK
M&T Bank
citibank
CIBC
CNN
THE WALL STREET JOURNAL.
WSJ
MSNBC
New York Times
YAHOO!
THE HUFFINGTON POST
DRUDGE REPORT
ZDNet
TIME
Los Angeles Times
Slate
Aol News.
NBC Sports
Mashable
Bloomberg
digg
NYDailyNews.com
DAILY NEWS
San Francisco Chronicle
NewsMax.com
The Philadelphia Inquirer
FOX SPORTS
The Atlantic
MEDIAite
NATIONAL REVIEW
ajc The Atlanta Journal-Constitution
TVNEWSER
All Facebook
cnet
AFP
Consumer Reports
SportingNews


9:41


Gmail
inbox.com
Windows Live
Aol.


ABN·AMRO
People's United Bank
Standard Chartered
BB&T
First National Bank
KeyBank
TD Bank
RBC
JPMorganChase
OneWest Bank
EverBank
BBVA Compass
Comerica Bank
BNP PARIBAS
Mechanics Bank
BridgeBank
COMMERZBANK
Santander
RBS
Bradesco
CITY NATIONAL BANK
EMBASSY BANK
Associated Bank
SBERBANK
STERLING BANK
Rabobank
Westpac
ROCKLAND TRUST
HSBC
Danske Bank
First Interstate Bank
Cambridge Trust Company
CapitalOne
ncb
usbank
SVB
Investec
LLOYDS BANK
PNC
BROWN BROTHERS HARRIMAN
ANZ
BBVA
SierraVista
ZIONS BANK
M&T Bank
citibank
CIBC

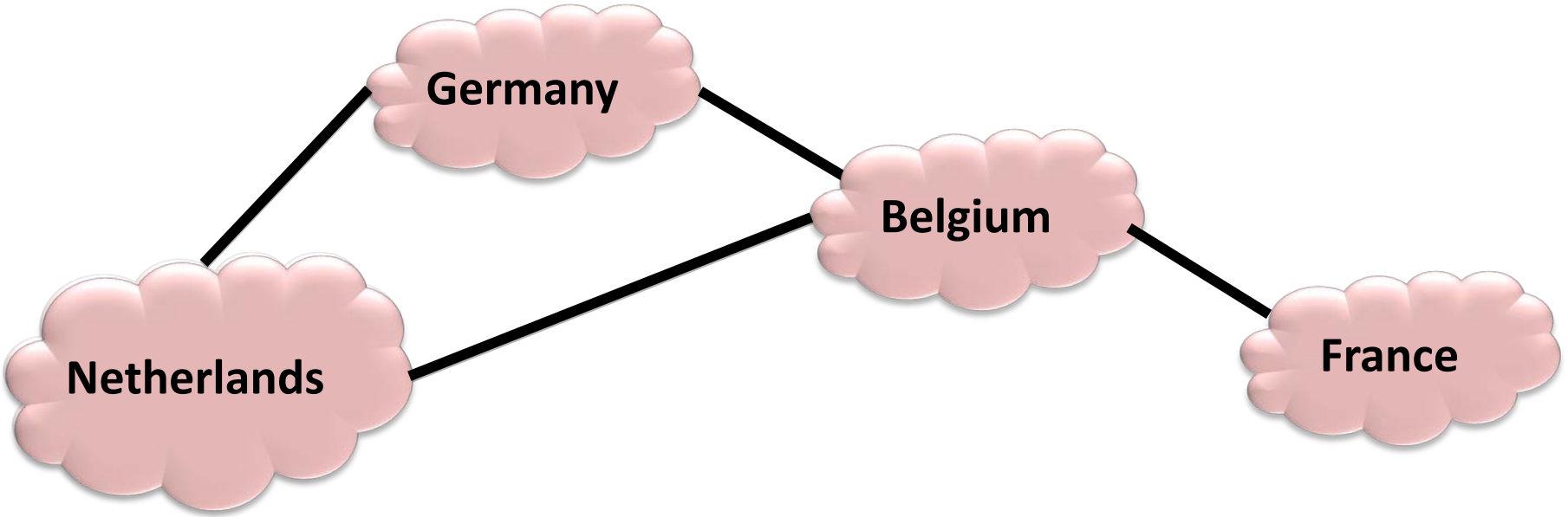

CNN
THE WALL STREET JOURNAL.
WSJ
MSNBC
New York Times
YAHOO!
THE HUFFINGTON POST
DRUDGE REPORT
ZDNet
TIME
Los Angeles Times
Mashable
Bloomberg
San Francisco Chronicle
NewsMax.com
NATIONAL REVIEW
The Atlanta Journal-Constitution
TVNEWSER
All Facebook
cnet
AFP

Slate
Aol News.
NBC Sports
NYDailyNews.com
DAILY NEWS
digg
The Philadelphia Inquirer
FOX SPORTS
The Atlantic
MEDIAite
Consumer Reports
SportingNews

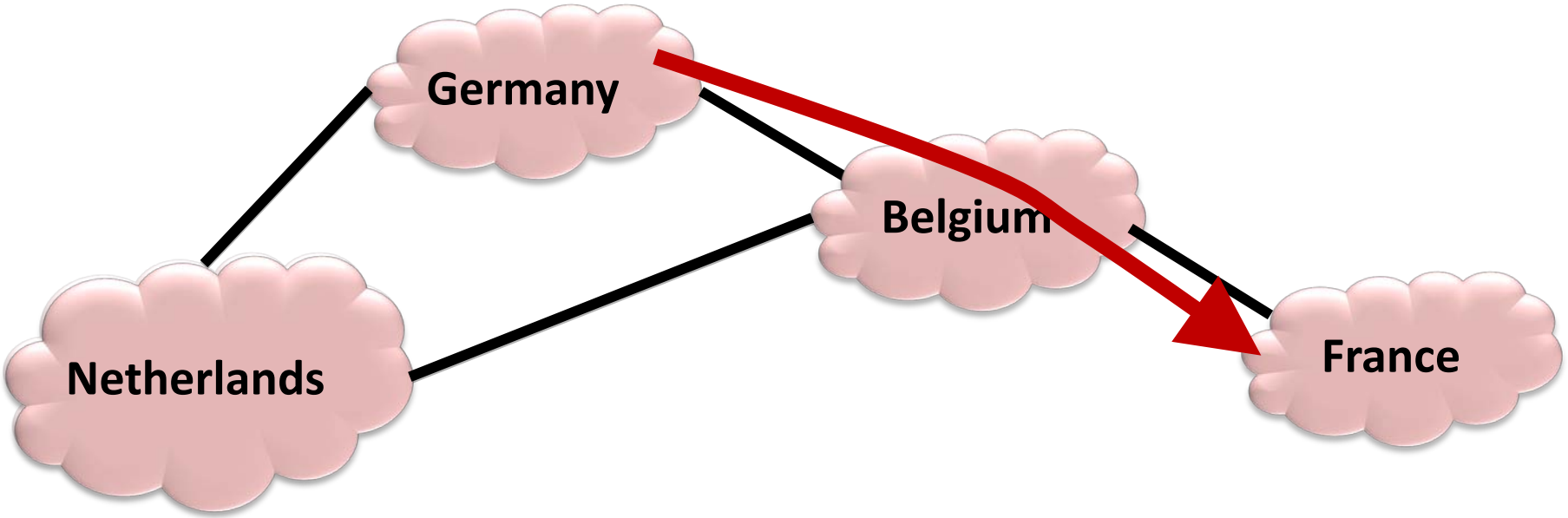

9:41

Background

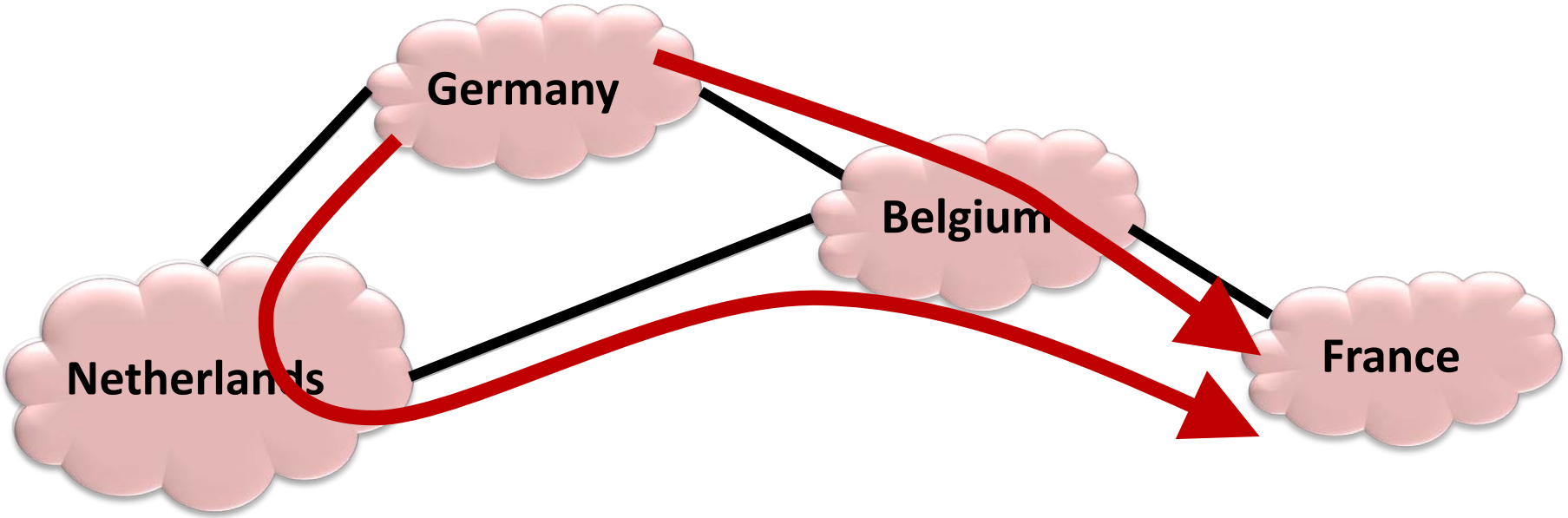
BGP refresher



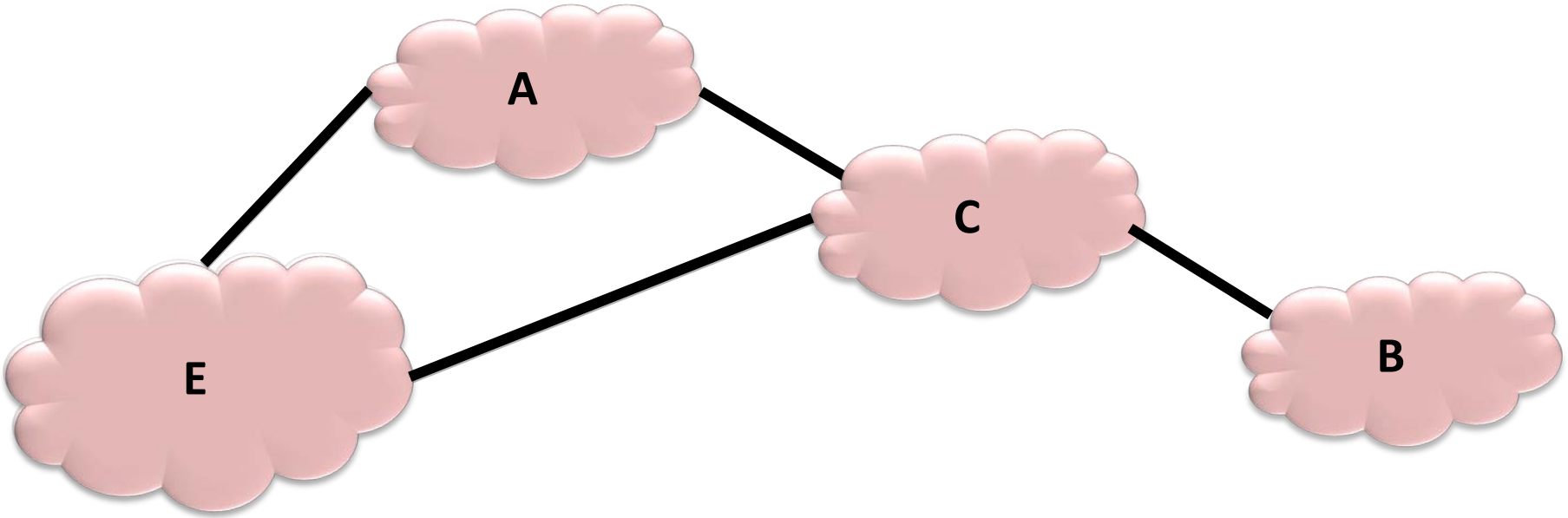
BGP refresher



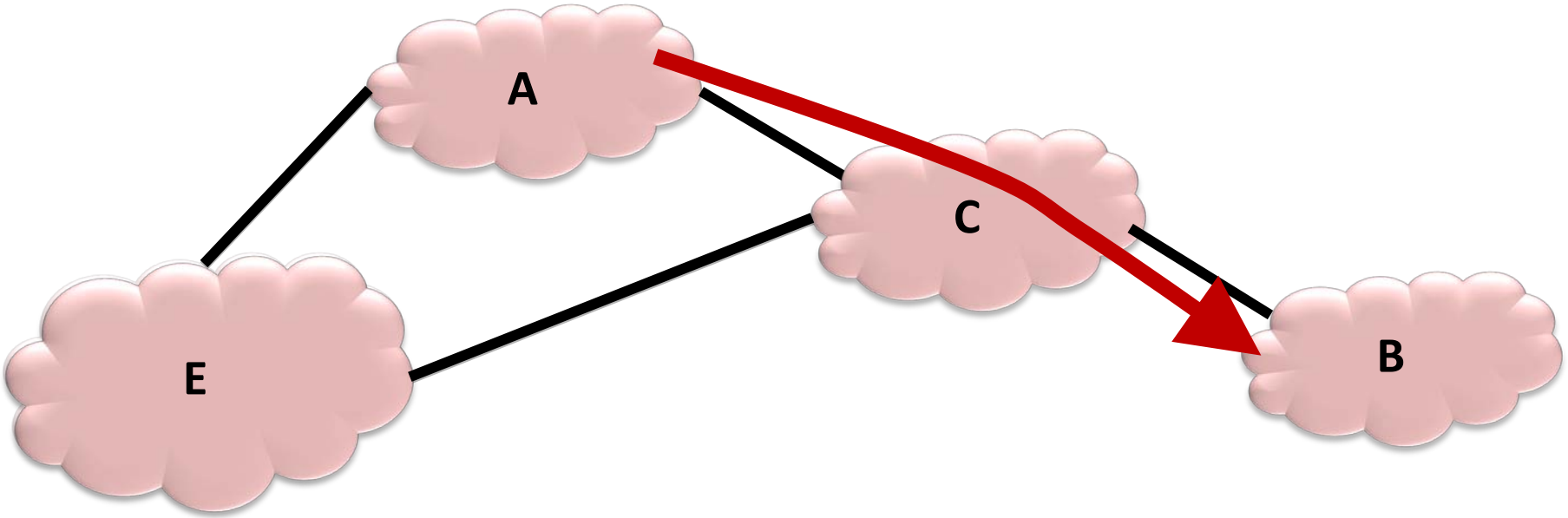
BGP refresher



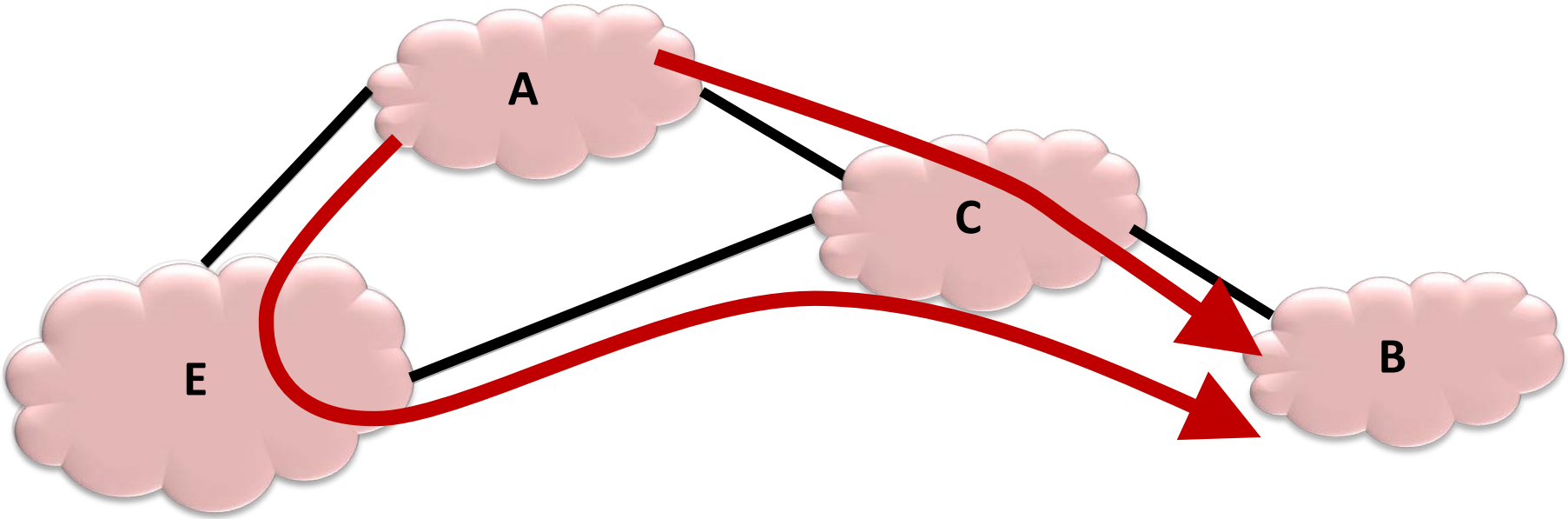
BGP refresher



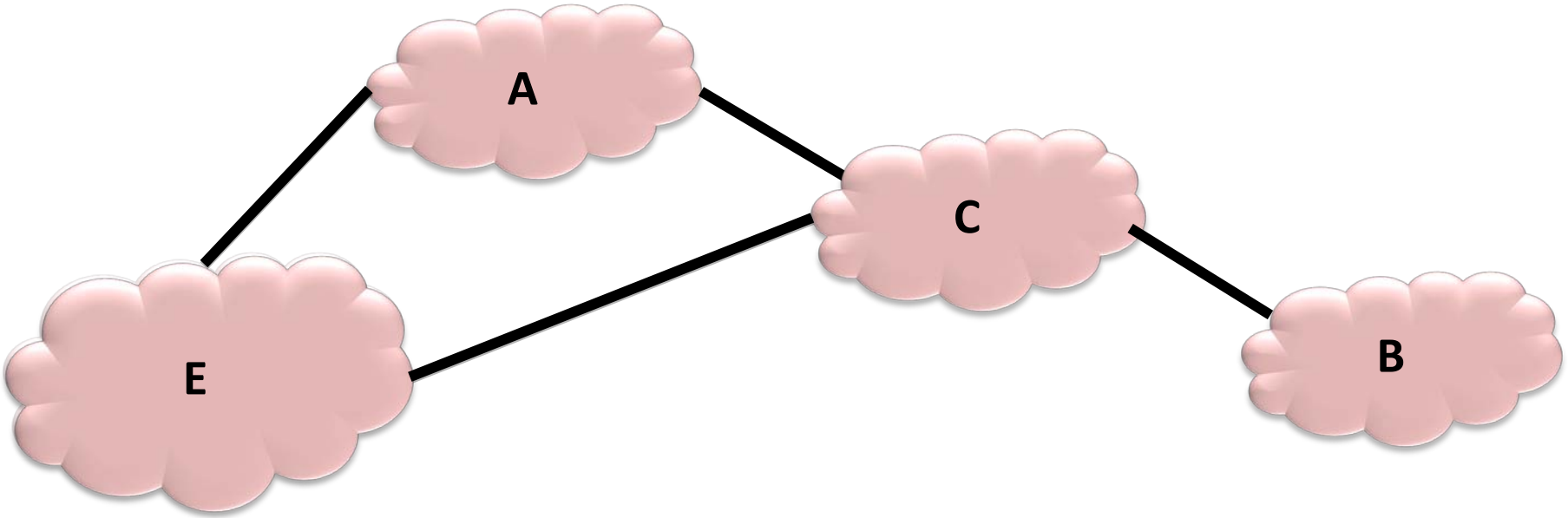
BGP refresher



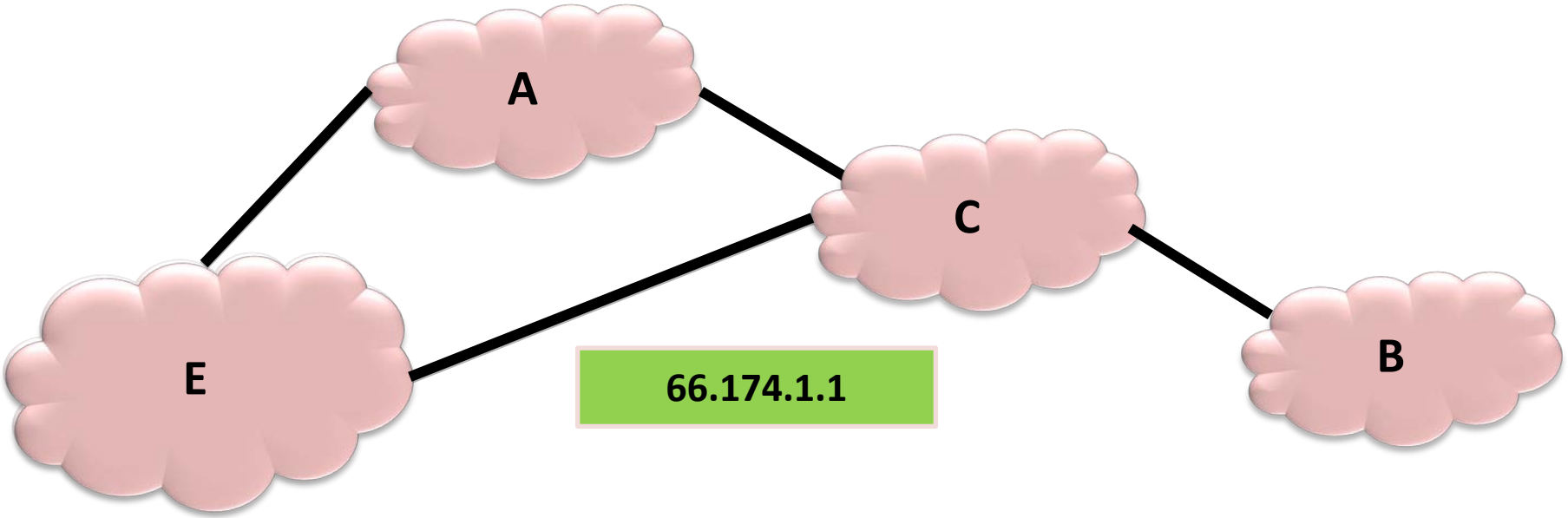
BGP refresher



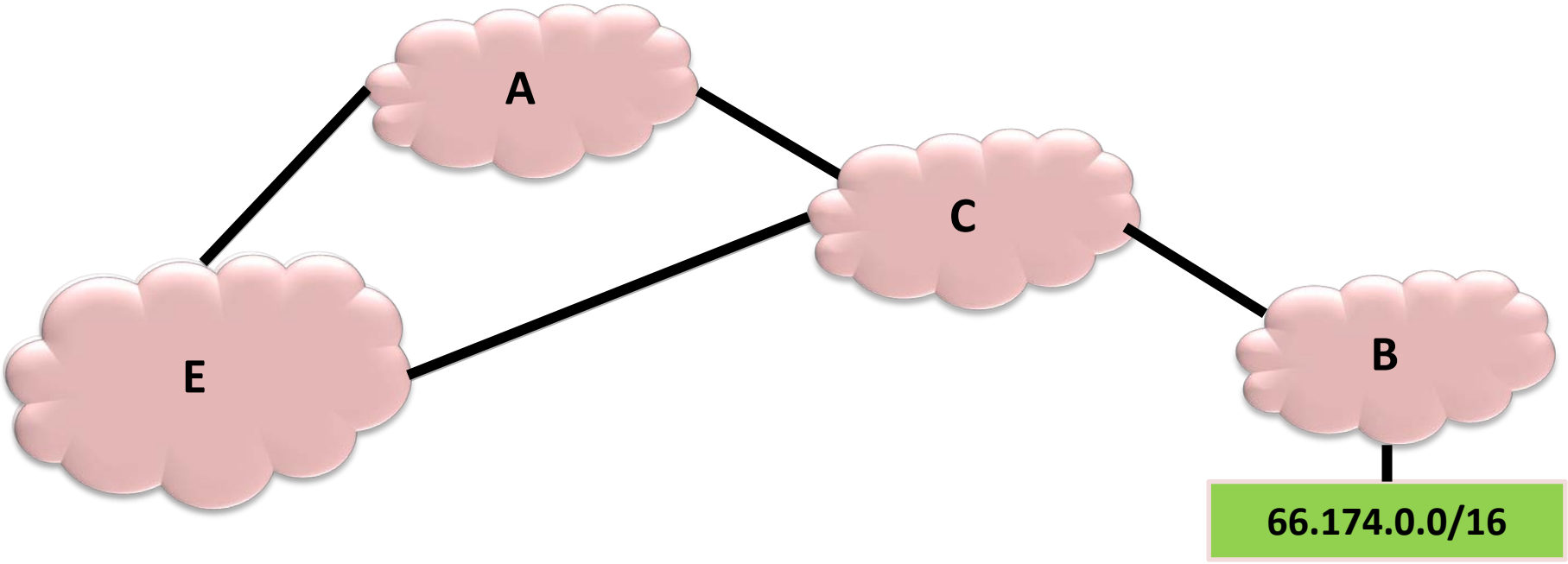
BGP refresher



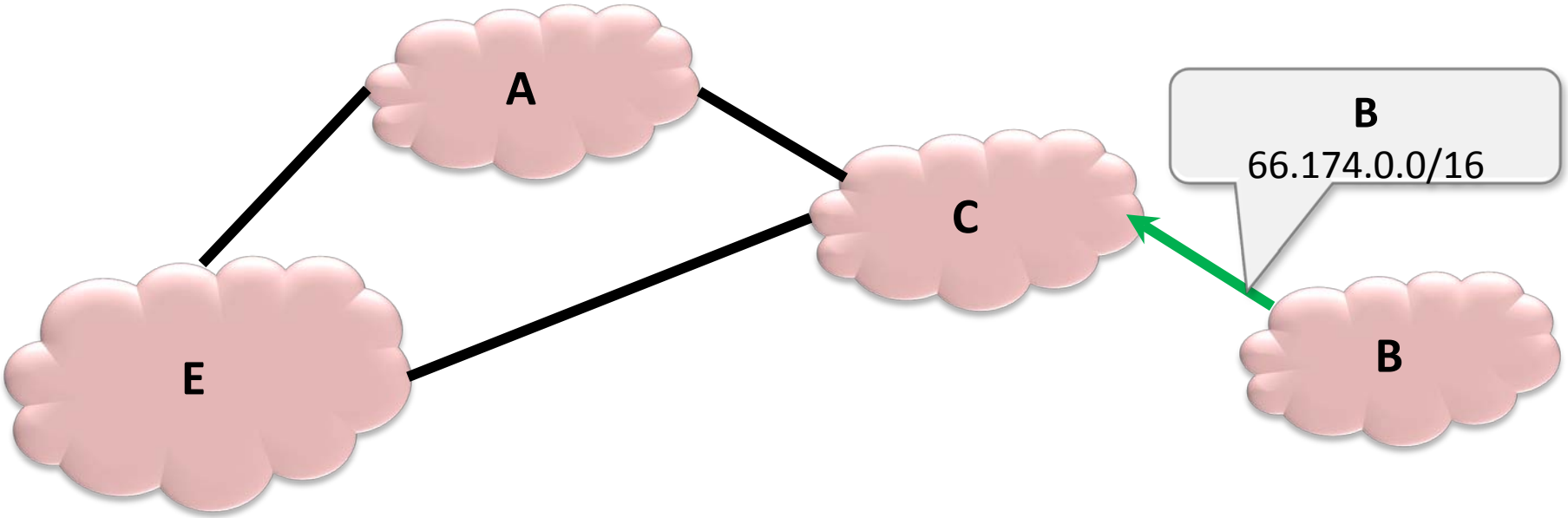
BGP refresher



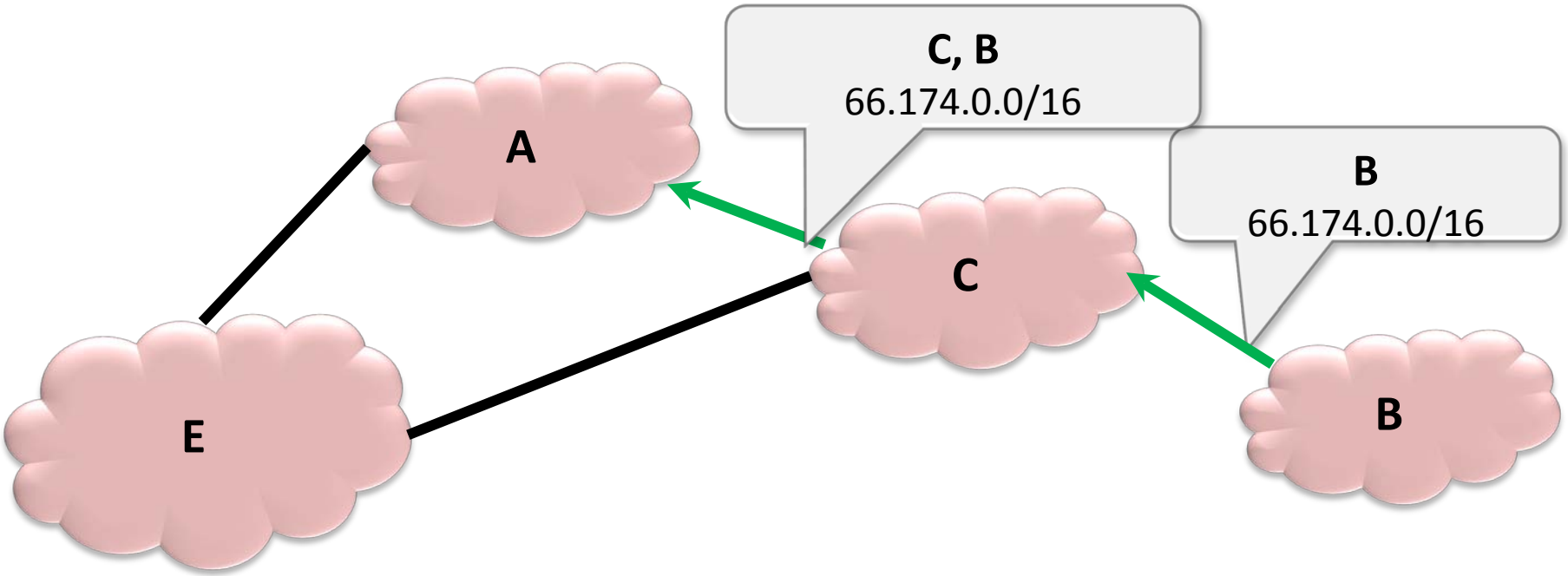
BGP refresher



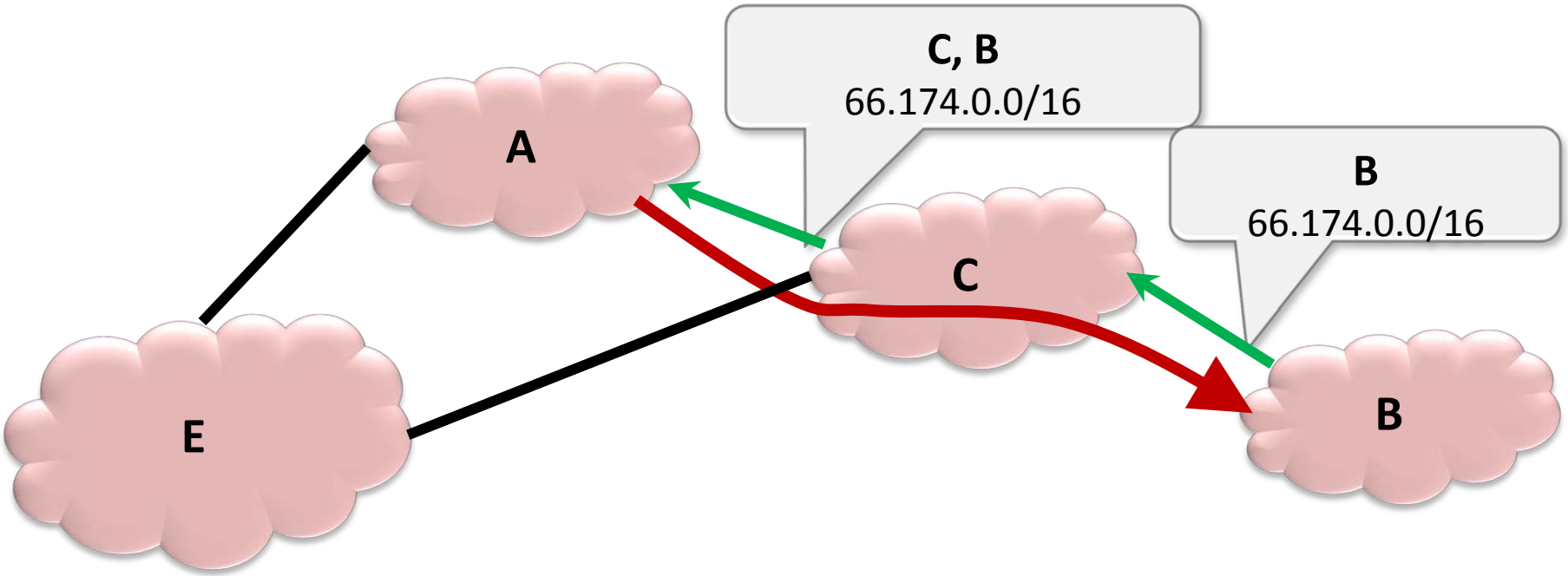
BGP refresher



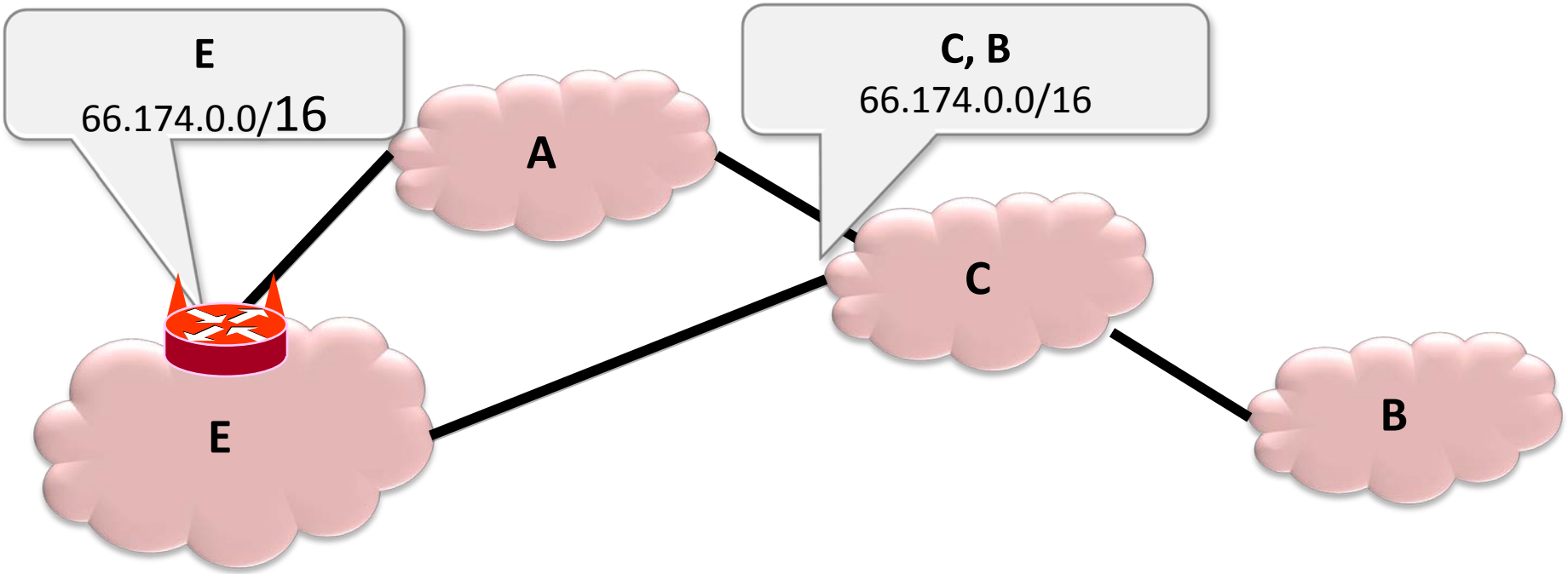
BGP refresher



BGP refresher

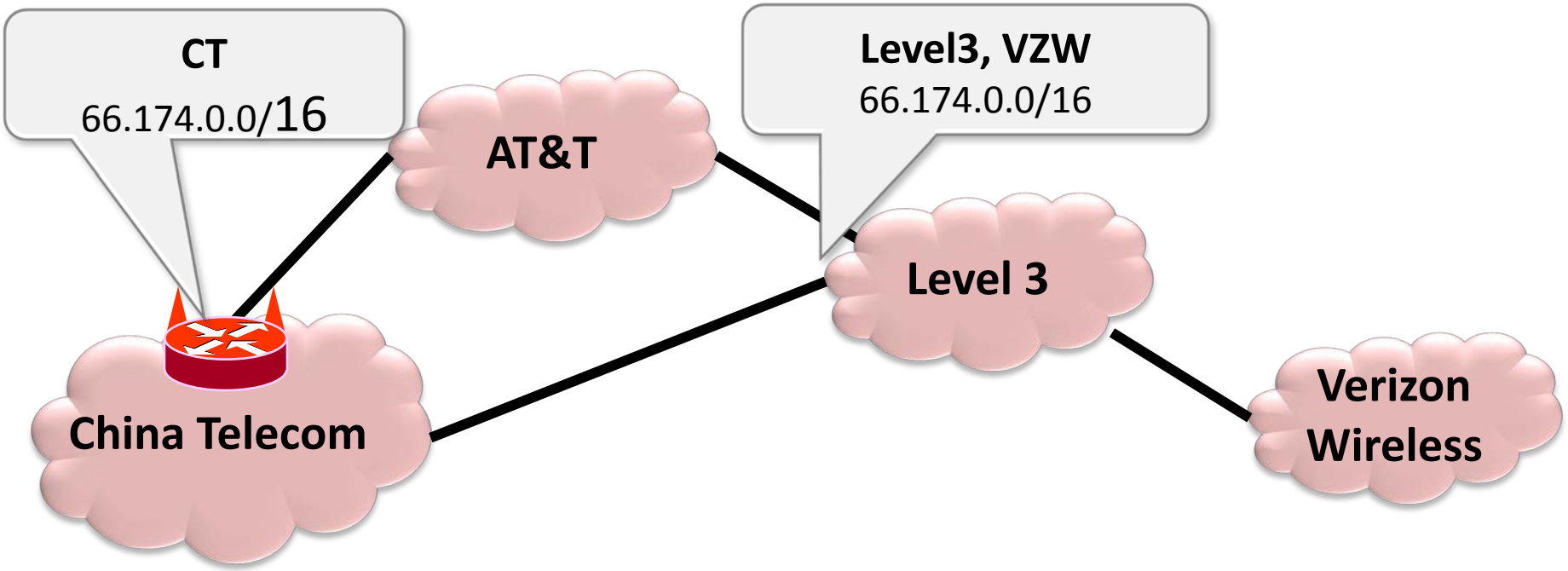


BGP refresher

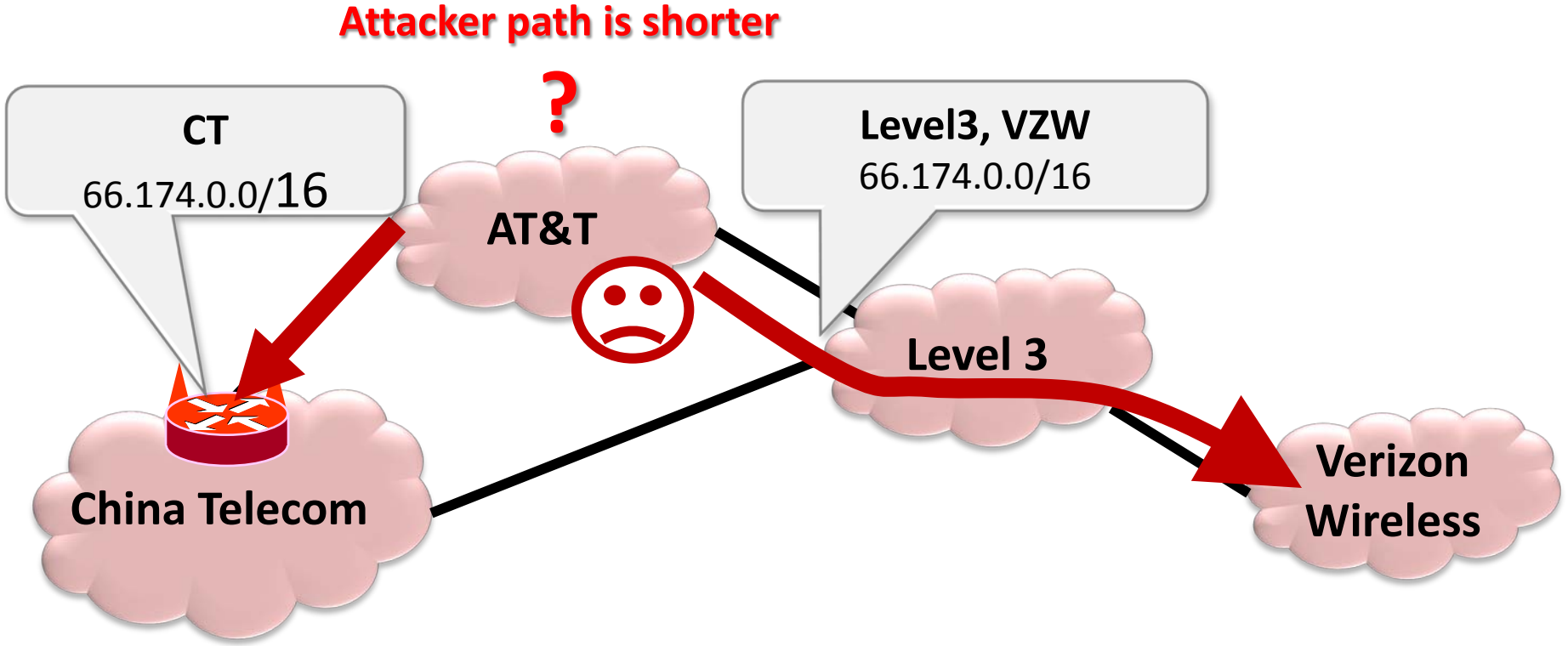


Difficult to check true ownership of prefixes

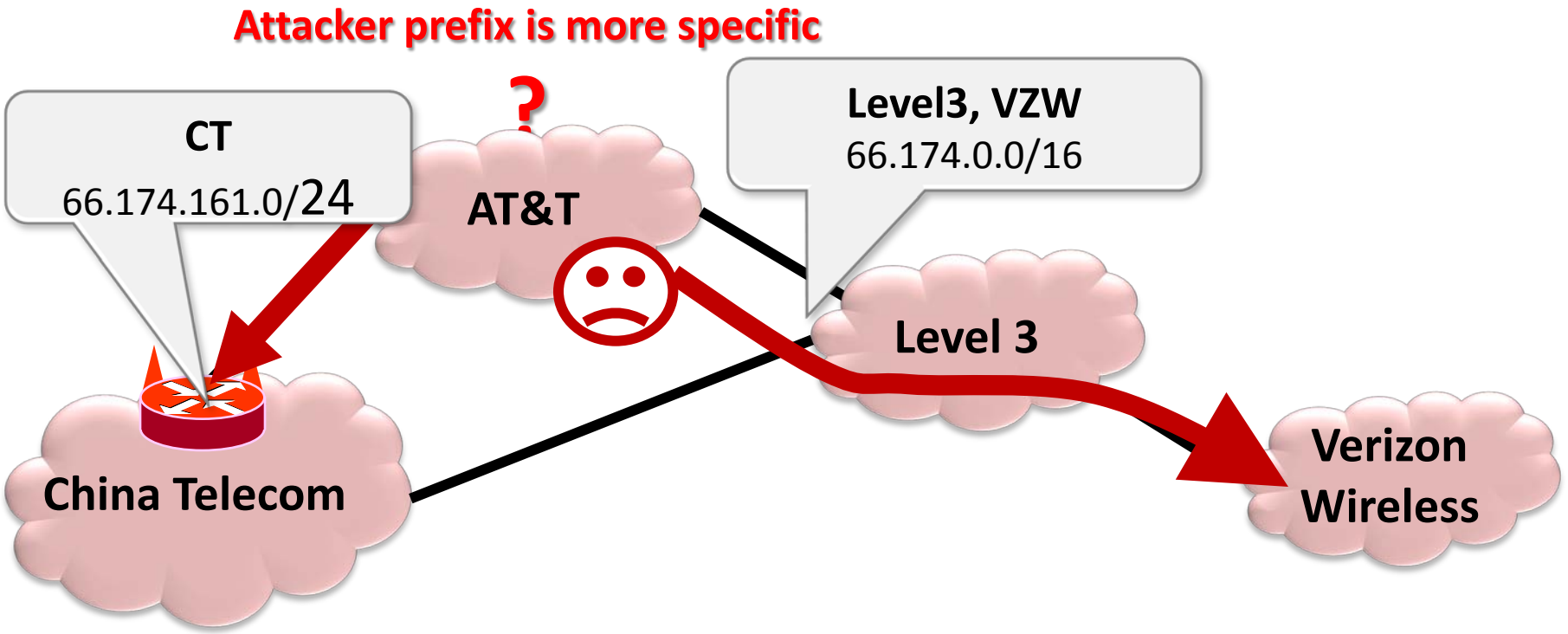
Prefix hijack attack



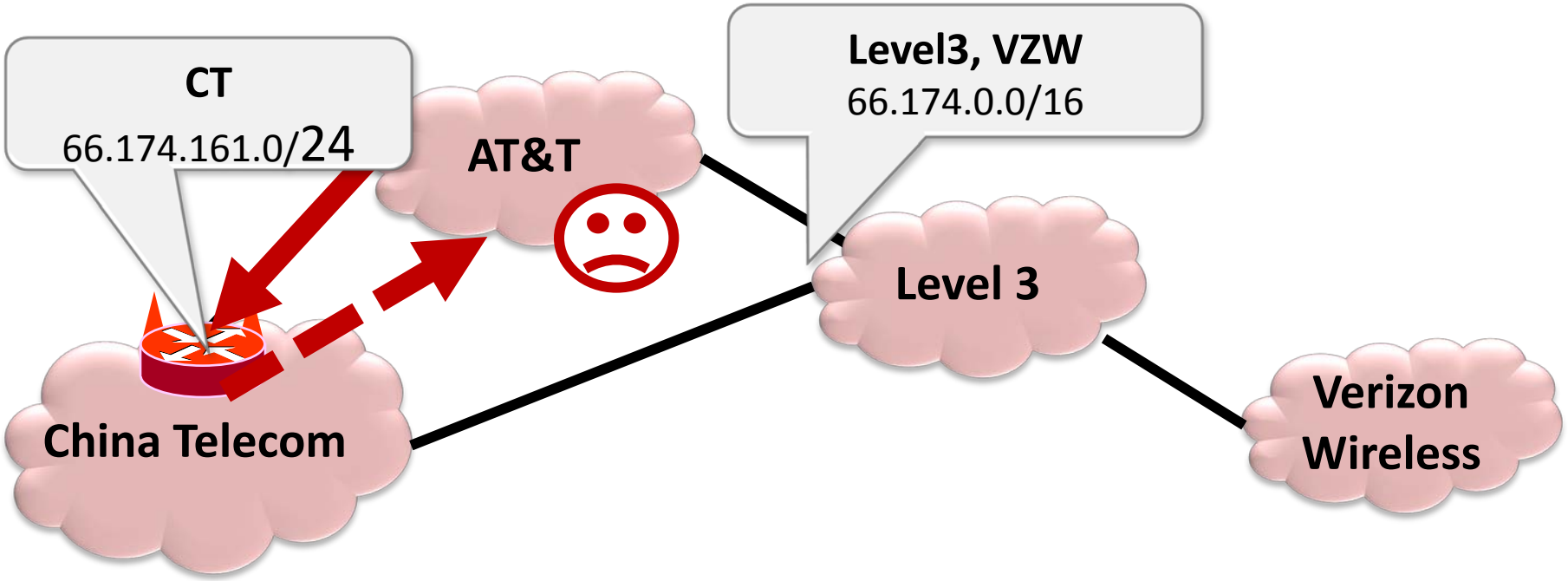
Prefix hijack attack



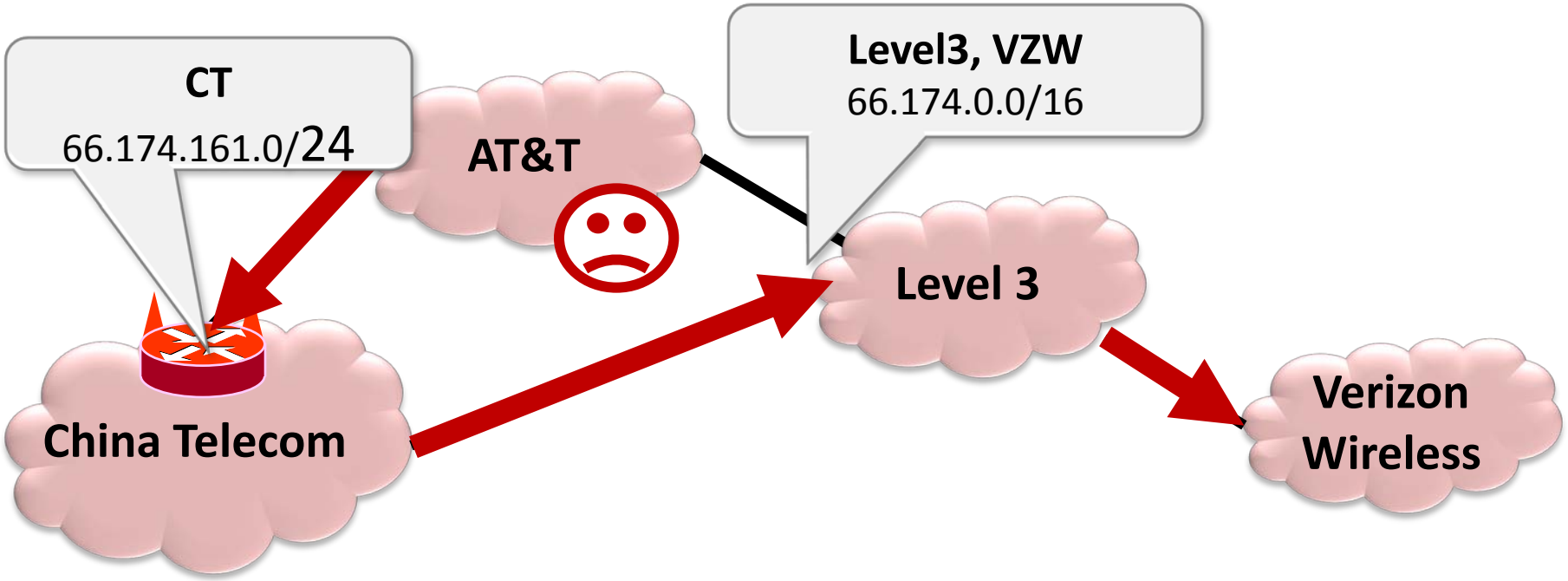
Subprefix hijack attack



Imposture attack



Interception attack



Research questions

Research questions

- What can we learn about large scale routing anomalies using publicly available datasets?
- How can we design scalable mechanisms to raise alerts for routing attacks and malicious edge-network-based activities?
- How are the gains from routing security mechanisms affected by scale, size, and locality aspects of the collaborating ASes?

Contributions

- Characterization of the China Telecom incident
- Decentralized collaborative mechanisms to detect attacks
  - PrefiSec
  - CrowdSec
  - TRAP
- Evaluation of different routing security mechanisms from scale, size, and locality perspective
  - Routepath updates
  - Origin information
  - Traffic properties such as RTT

Contributions

China Telecom incident

- Characterization of the China Telecom incident
- Decentralized collaborative mechanisms
  - PrefiSec
  - CrowdSec
  - TRAP

Collaborative mechanisms

- Evaluation of different routing security mechanisms from scale, size, and locality perspective
  - Routepath updates
  - Origin information
  - Traffic properties such as RTT

Effect of scale, size, locality

China Telecom incident

China Telecom incident

Forbes · New Posts +26 posts this hour · Most Popular Google's Driverless Car · Lists Business Of Basketball

overnment
ia Chinese

0 Share 0 Tweet 0 Share

Andy Greenberg, Forbes Staff
Covering the worlds of data security, privacy and hacker culture.
+ Follow (647)

SECURITY | 11/19/2010 @ 12:(

China Hija
Traffic? M

The Tel

HOME NEWS WORL
USA Asia China

theguardian

News Sport Comment Culture Business Money Life & style

News Technology Internet

China denies 'hijacking' internet traffic

US report claims Chinese telecoms company had access to 15% of global traffic, including military emails, for 18 minutes

HOME » NEWS » WORLD NEWS » ASIA » CHINA

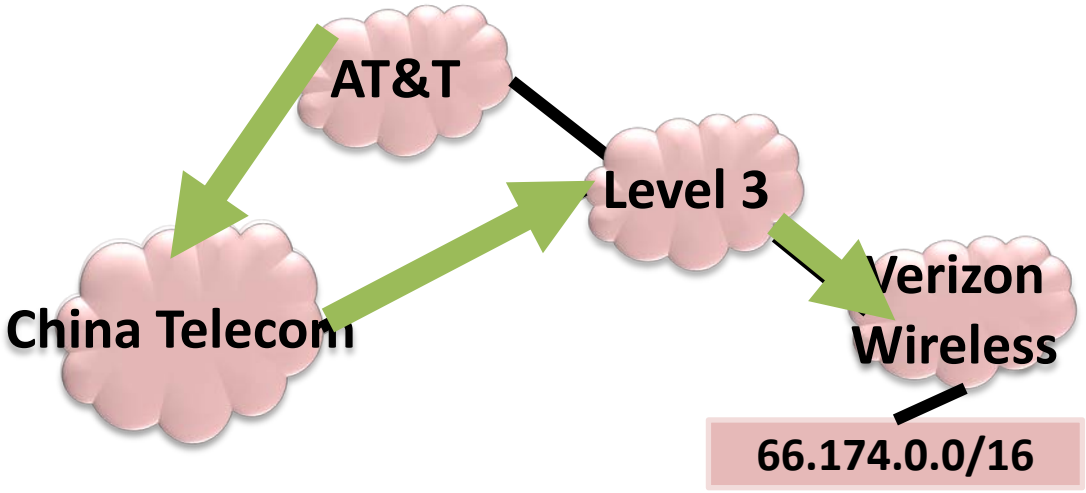
China 'hijacks' 15 per cent of world's internet traffic

China "hijacked" 15 per cent of the world's internet traffic for 18 minutes earlier this year, including highly sensitive email exchanges between senior US government and military figures, a report to the US Congress said.

How did interception occur?

Two routing decisions required for traffic interception:

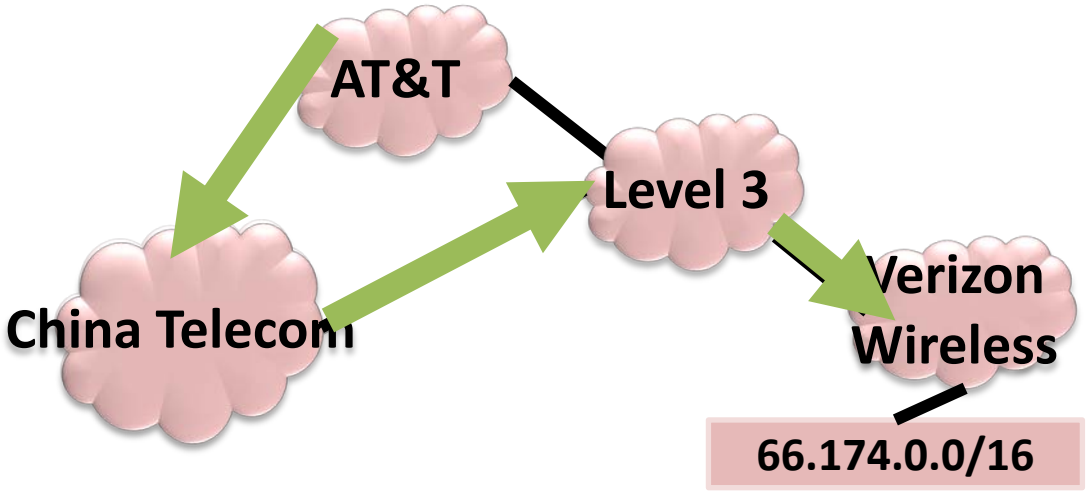
1. A neighbor routes to China Telecom for hijacked prefix
2. Another neighbor does not do so



How did interception occur?

Two routing decisions required for traffic interception:

1. A neighbor routes to China Telecom for hijacked prefix
2. Another neighbor does not do so



Reasons for not routing to China Telecom

Reason	# of traceroutes	% of traceroutes
Had a customer path	139	39%
Had a shorter path	193	54%
Had an equally good path	18	5%
Other	7	2%

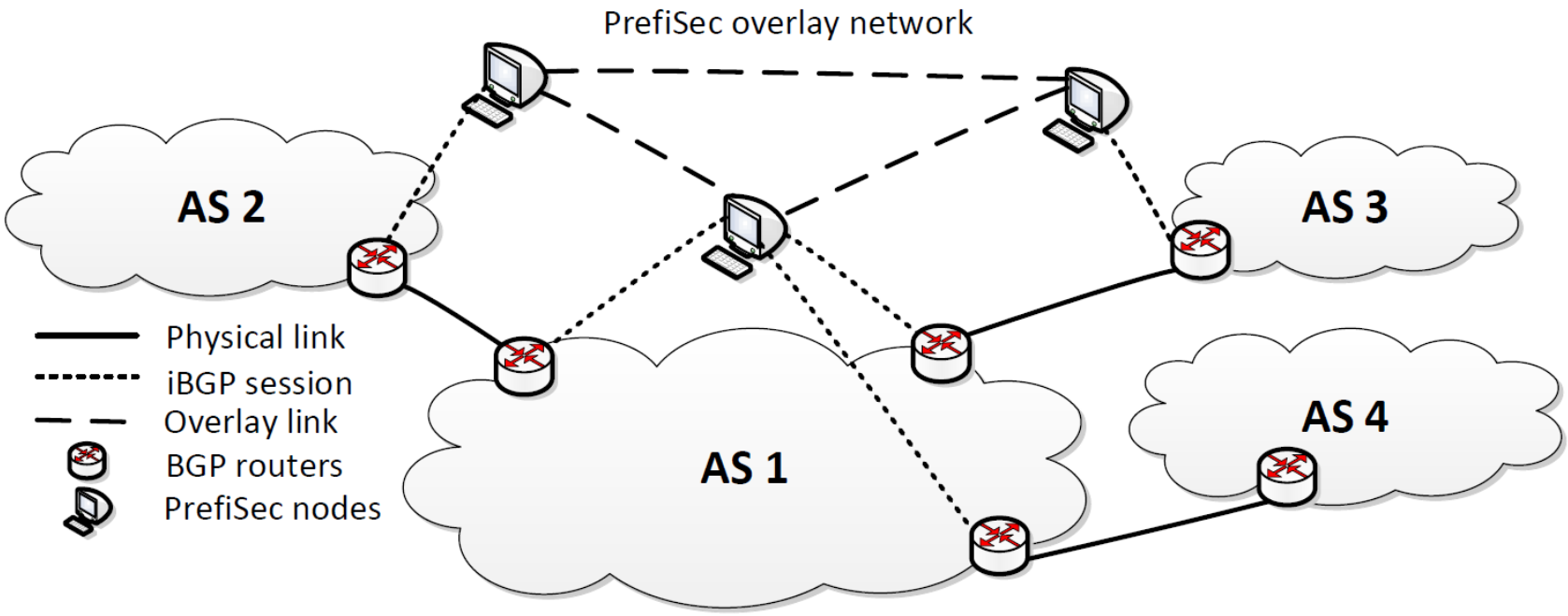
Reasons for not routing to China Telecom

Reason	# of traceroutes	% of traceroutes
Had a customer path	139	39%
Had a shorter path	193	54%
Had an equally good path	18	5%
Other	7	2%

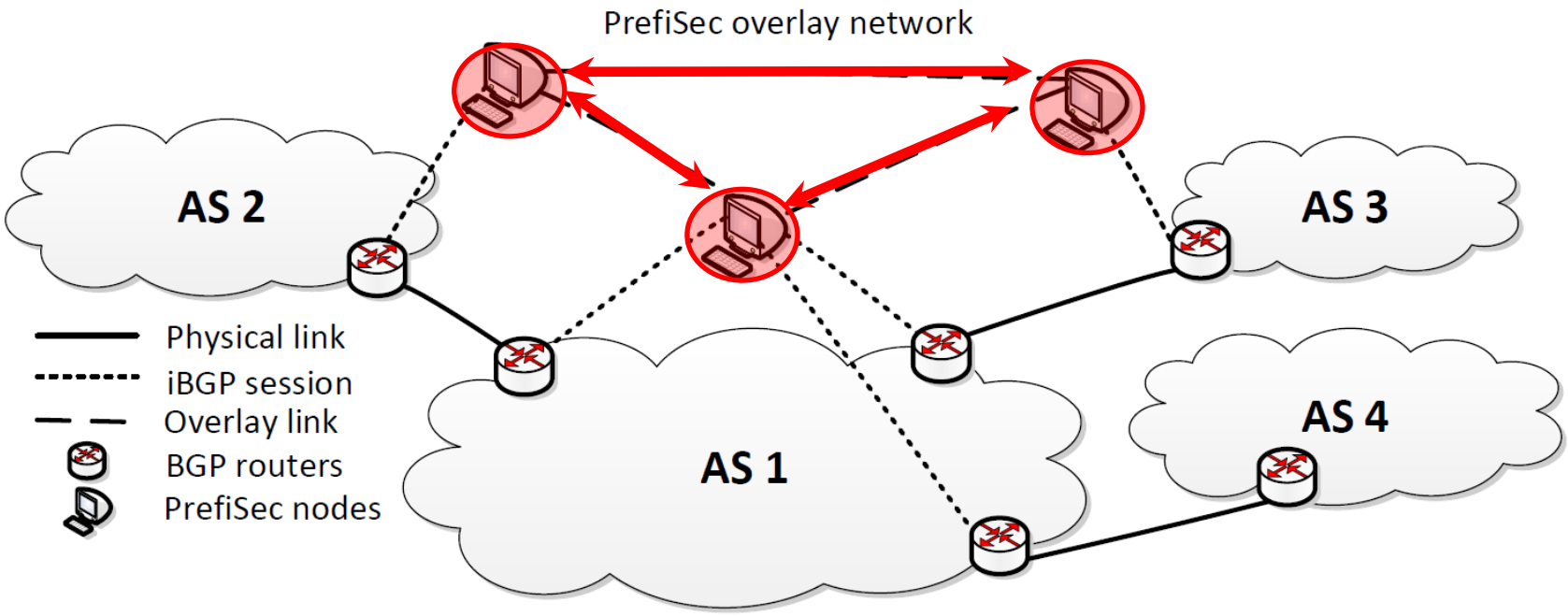
- Decisions made by ASes resulted in interception
- Collaboration important to detect such attacks

Collaborative mechanisms

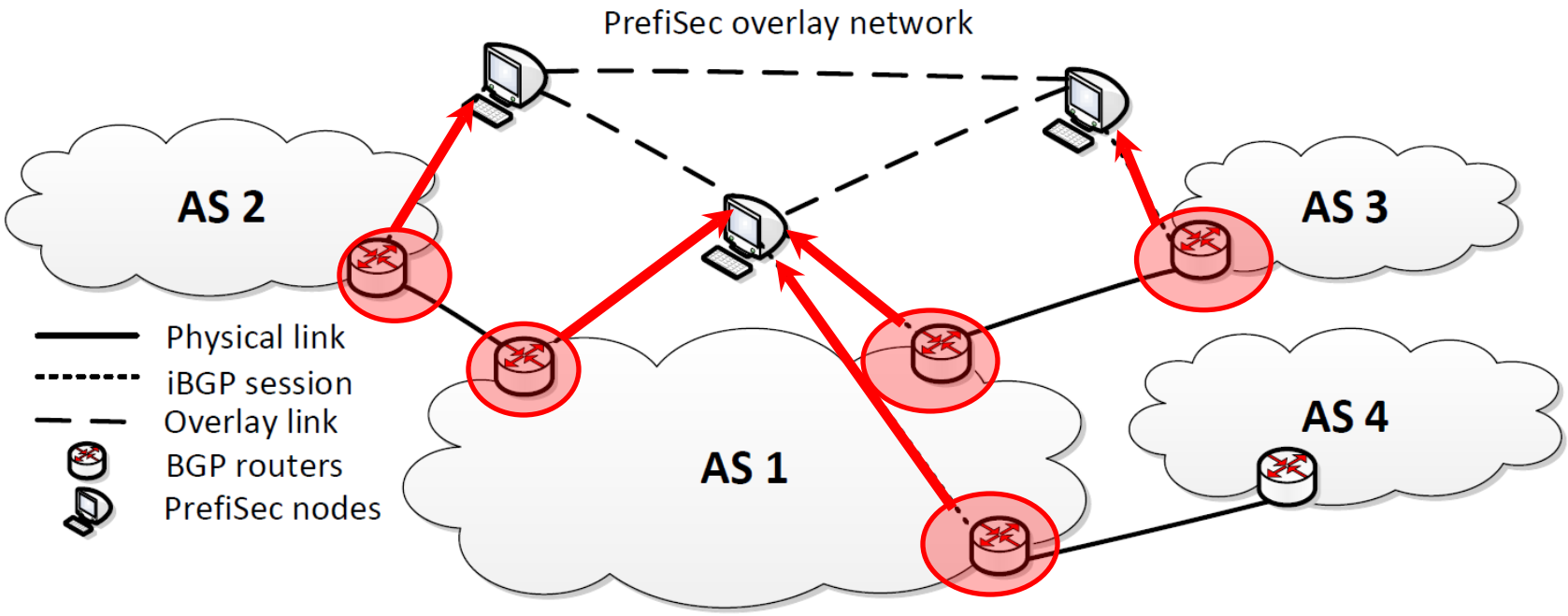
PrefiSec architecture



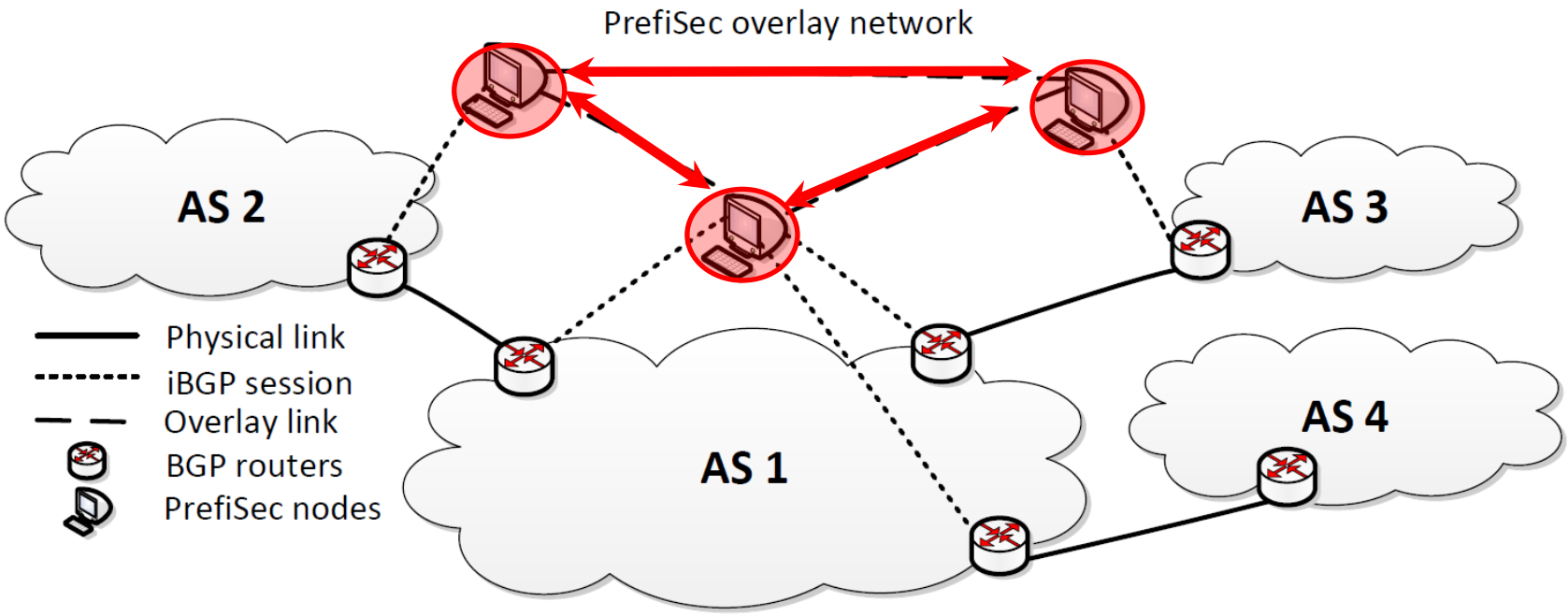
PrefiSec architecture



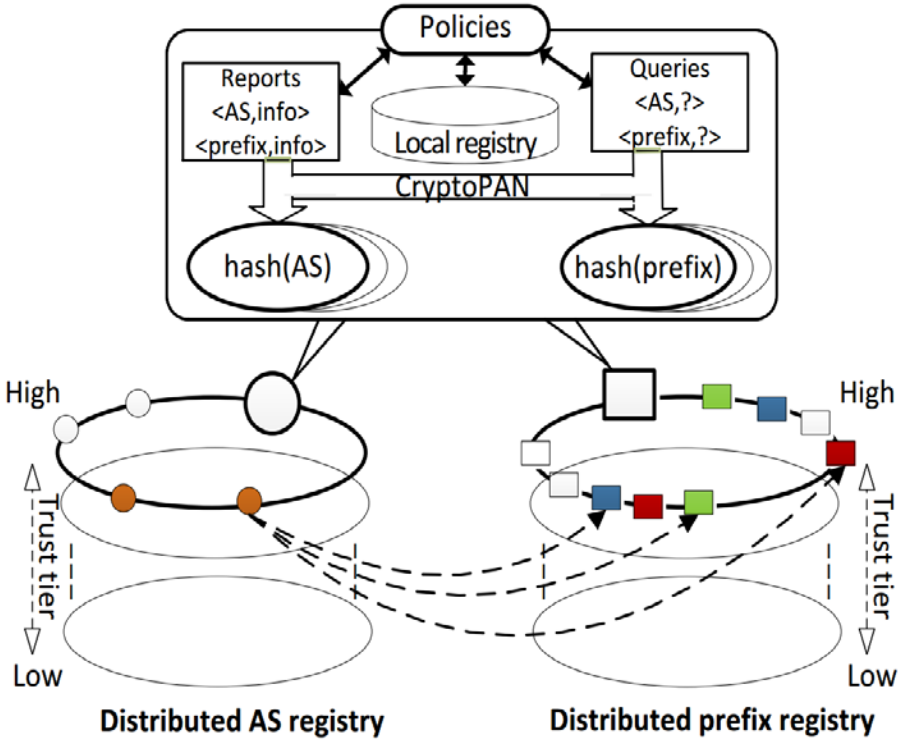
PrefiSec architecture



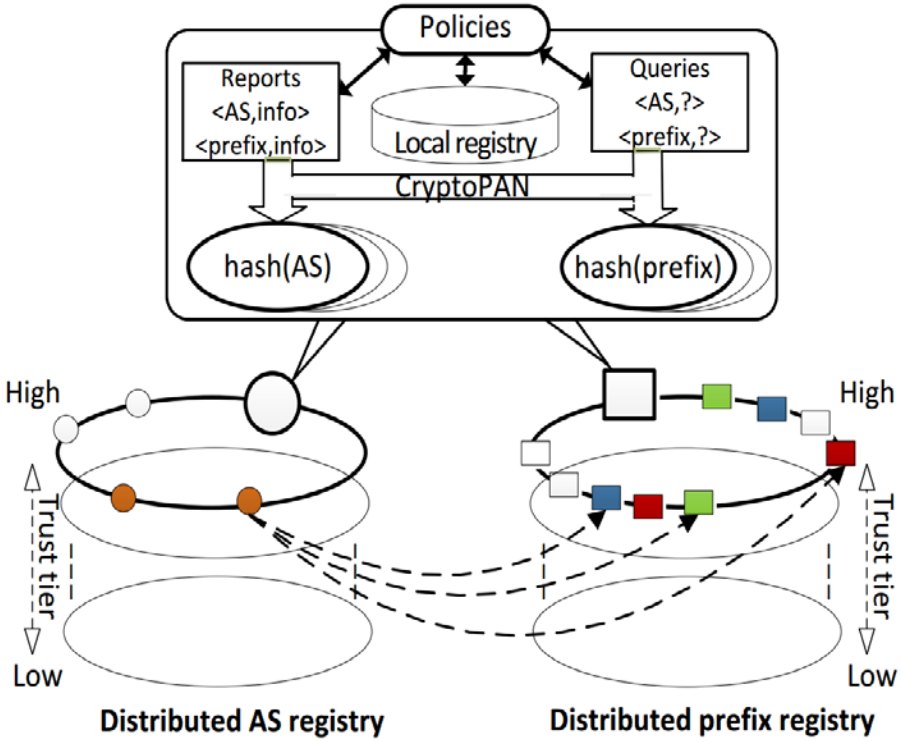
PrefiSec architecture



Components and structure

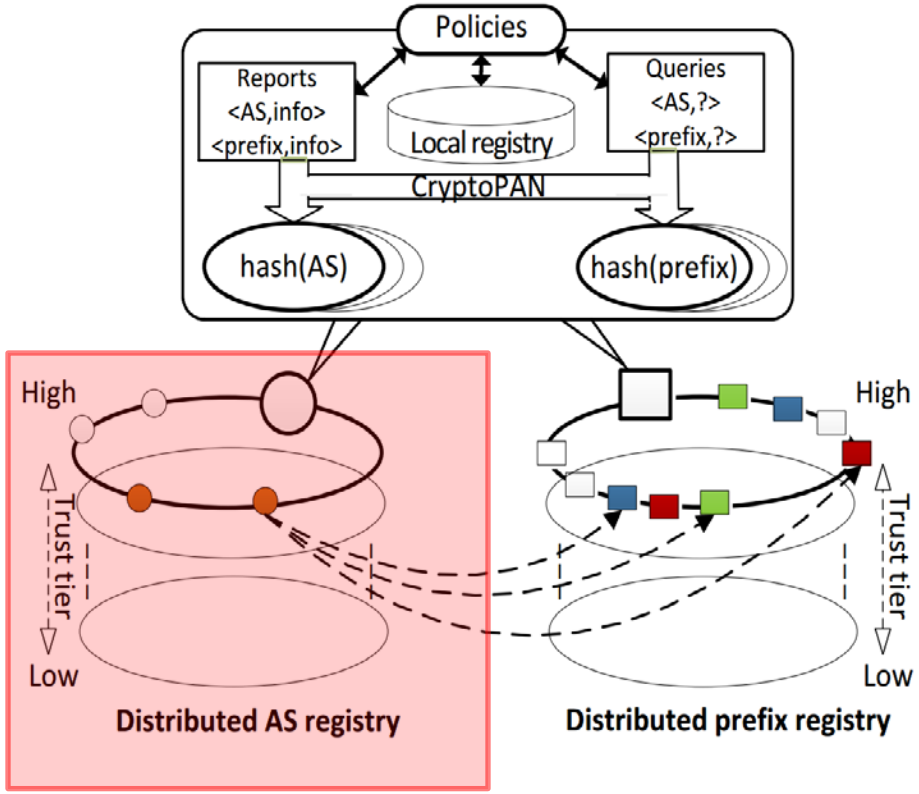


Components and structure



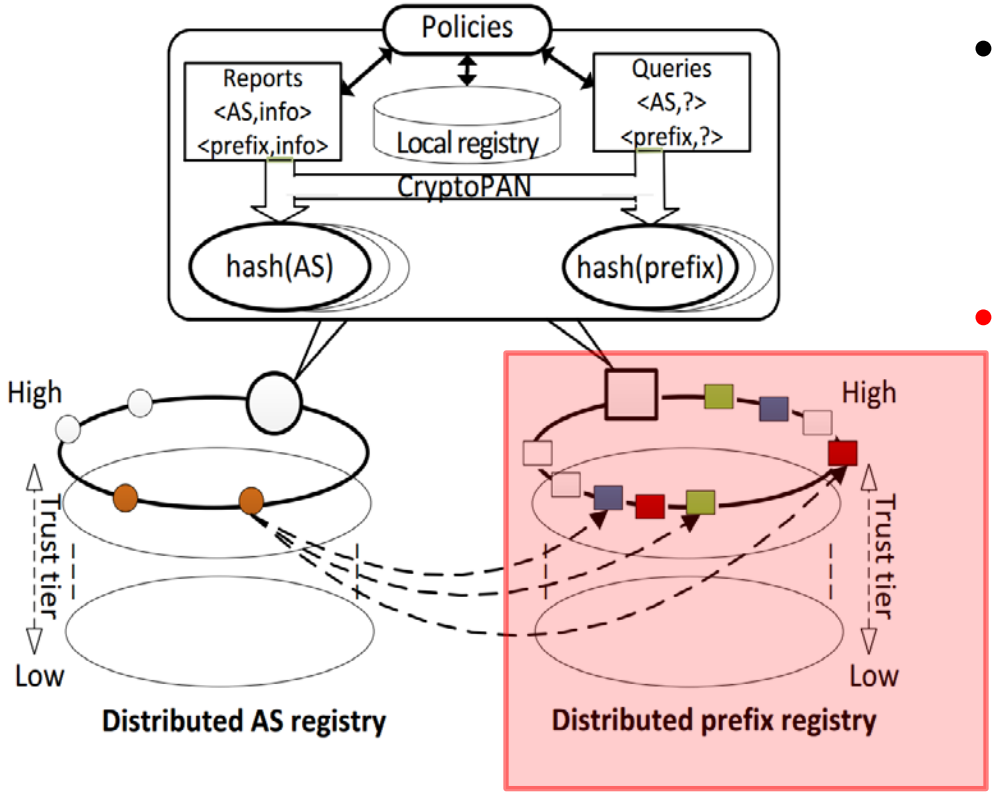
- AS registry
  -Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
  -Prefix origin information (prefix-to-AS mapping), and edge-network activities

Components and structure



- AS registry
  - -Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
  - -Prefix origin information (prefix-to-AS mapping), and edge-network activities

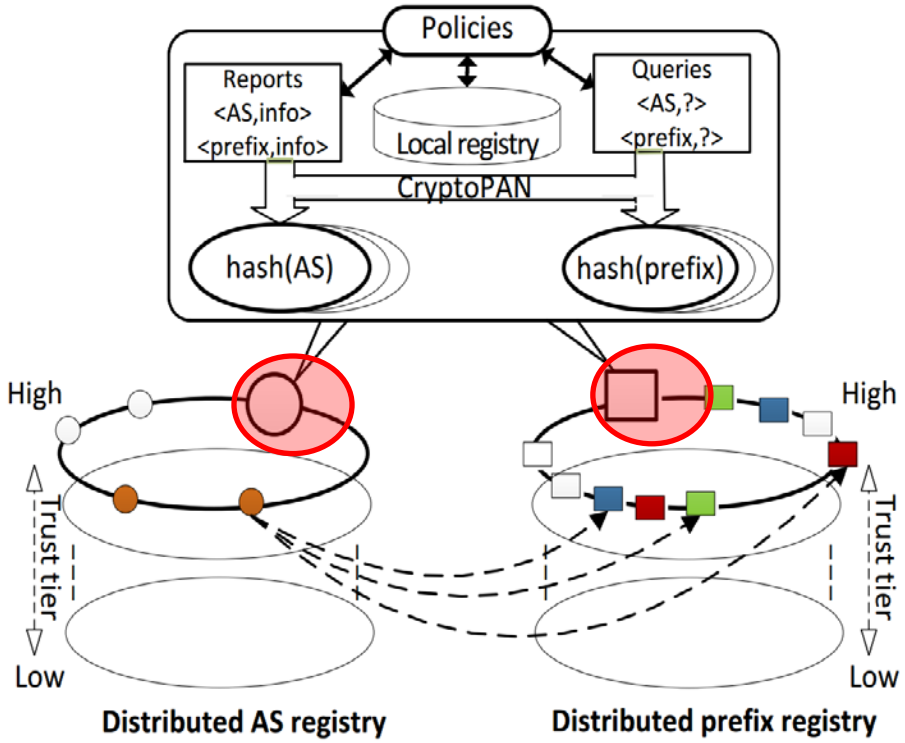
Components and structure



- AS registry
  - -Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
  - -Prefix origin information (prefix-to-AS mapping), and edge-network activities

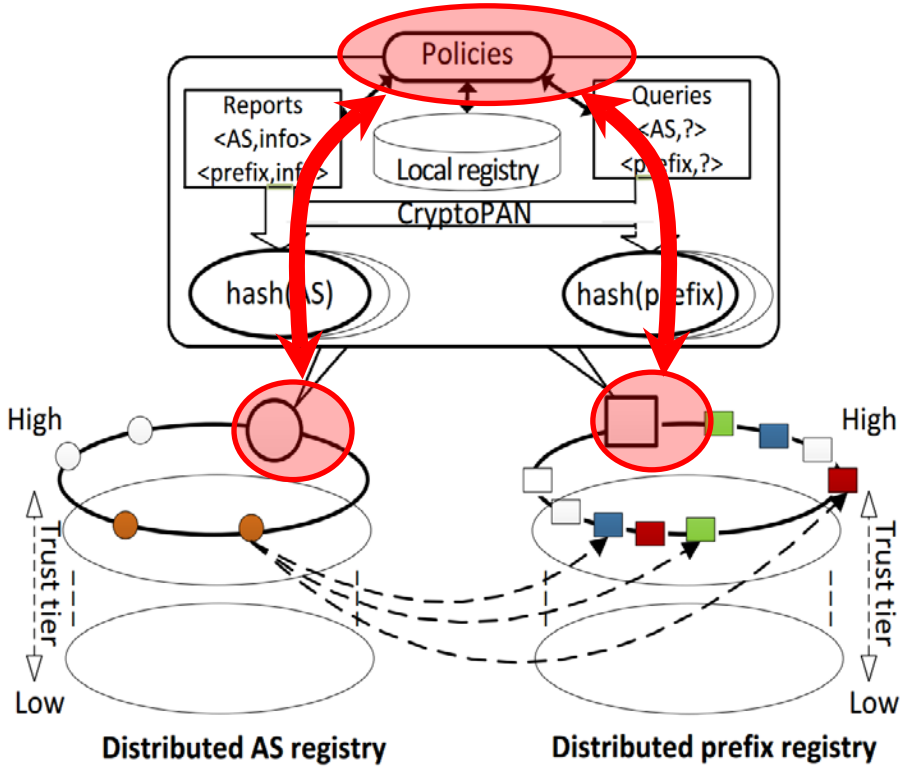
IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16

Components and structure



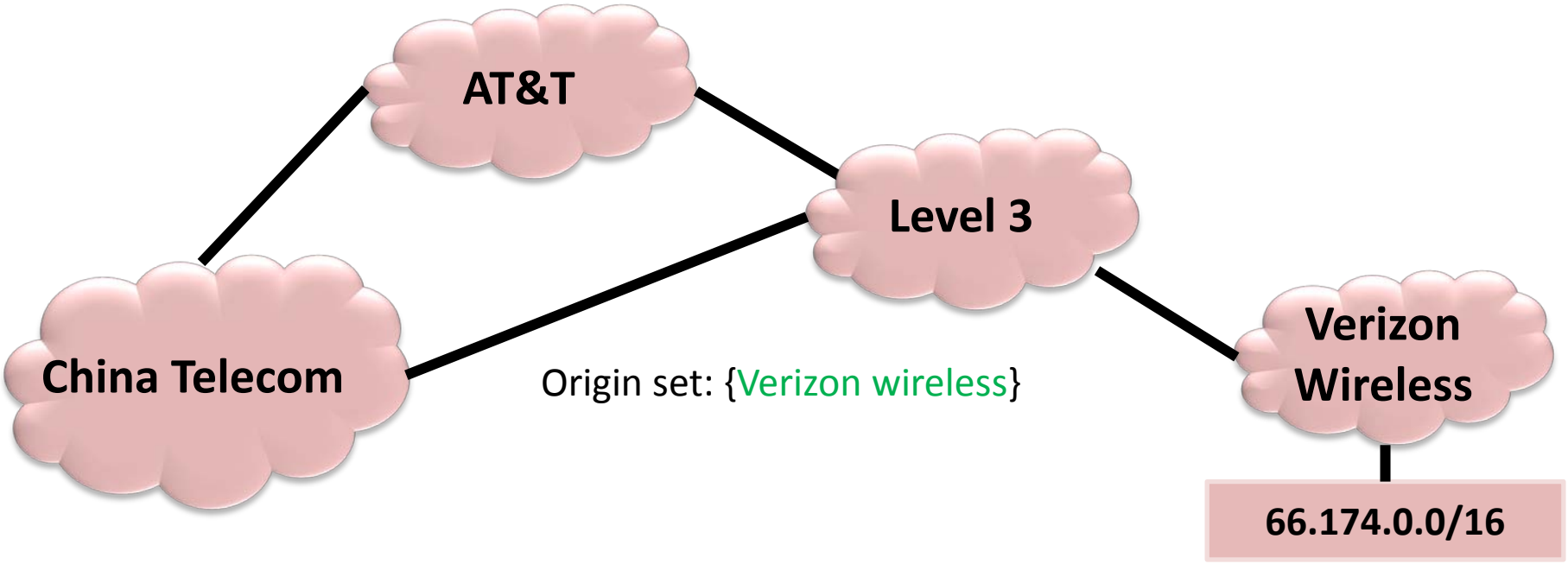
- AS registry
  - -Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
  - -Prefix origin information (prefix-to-AS mapping), and edge-network activities

Components and structure

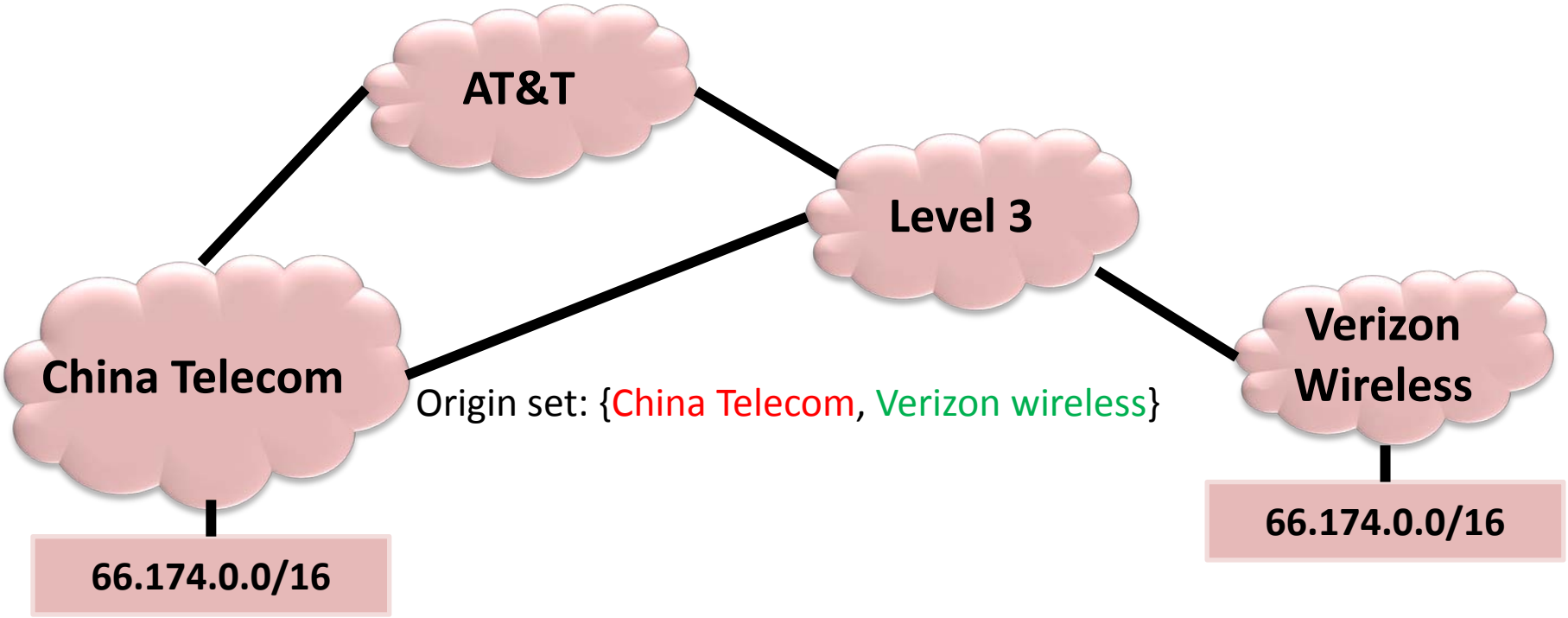


- AS registry
  - -Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
  - -Prefix origin information (prefix-to-AS mapping), and edge-network activities

Prefix hijack detection



Prefix hijack detection



Evaluation

- Performed data-driven analysis
- Used Routeviews data during the time when China Telecom incident occurred
- Simulate the proposed policy on each participating node

Example results

- Overhead small compared to centralized mechanisms
- Day before attack:
  - With all 6 routeviews servers collaborating, approximately 1,500 alerts raised
- Day of attack:
  - Would raise alerts for all 39,094 false announcement made by China Telecom
  - Same alert rate as centralized mechanism

Effect of scale, size, and locality

Mechanisms to secure BGP

- Prefix origin (hijack prevention): Route filtering, RPKI, ROVER
- Route path updates (hijack detection): PHAS, PrefiSec, PG-BGP
- Passive measurements: CrowdSec
- Active measurement: Zheng et al., PrefiSec

Mechanisms to secure BGP

- Prefix origin (hijack prevention): Route filtering, RPKI, ROVER
- Route path updates (hijack detection): PHAS, PrefiSec, PG-BGP
- Passive measurements: CrowdSec
- Active measurement: Zheng et al., PrefiSec

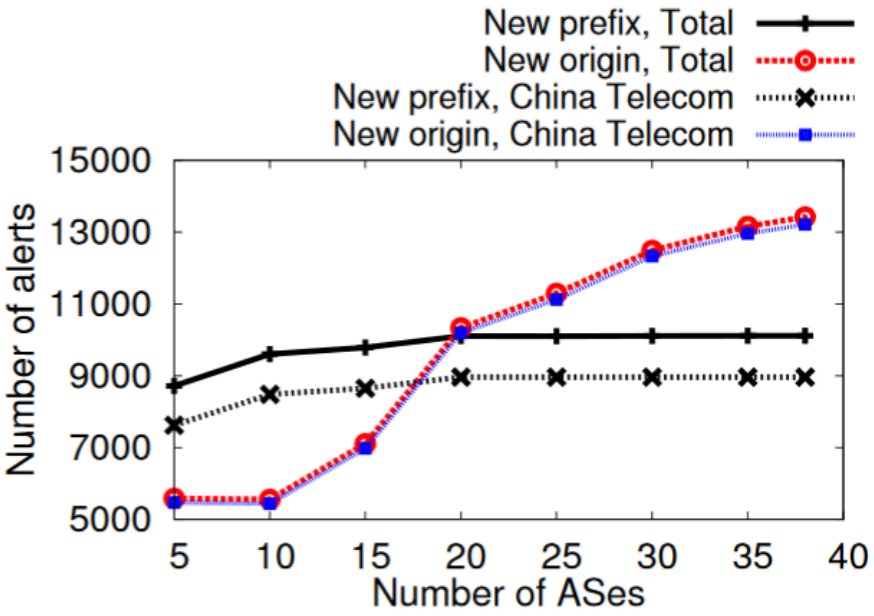
Evaluation aspects

- Locality
  - ASes in specific geographical area: European Union (EU), North America (NA), “rest of the world” and compare with global scenario
- Size
  - Size of an AS is based on the number of neighbors of that AS (termed as degree of AS)
- Scale
  - Number of collaborating ASes

Hijack detection mechanism

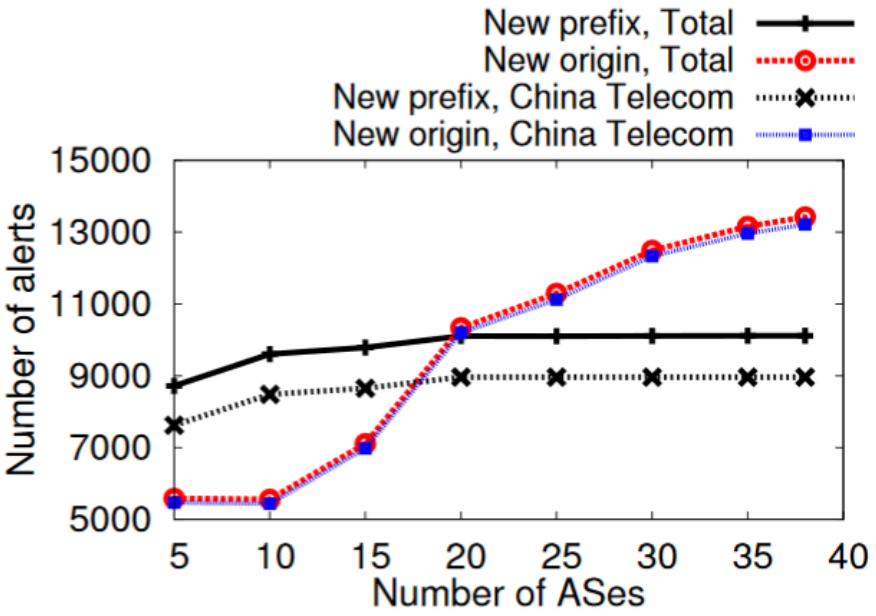
- Evaluation based on PrefiSec
- Instead of collaboration among routers in Routeviews data, we consider collaboration of ASes
- Data around time of the China Telecom incident

Scale and locality

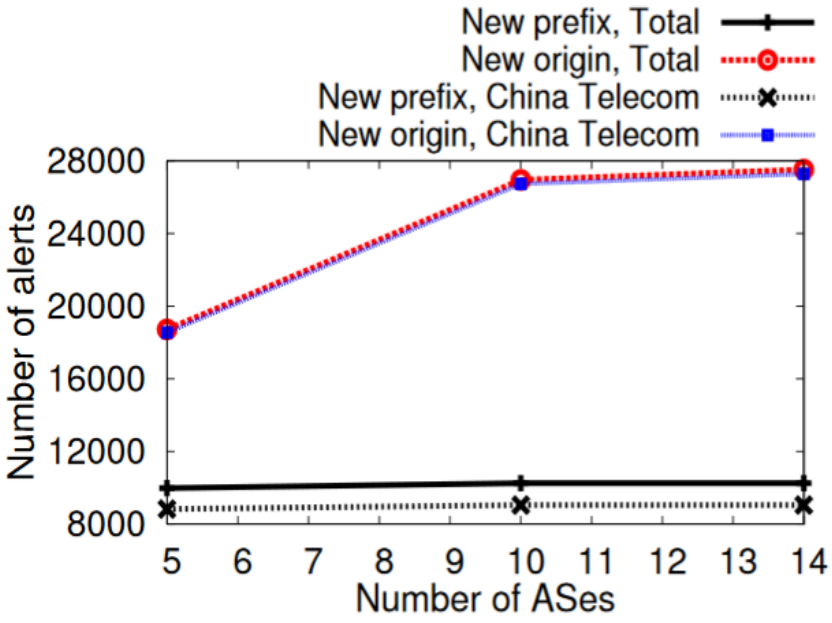


North America (NA)

Scale and locality



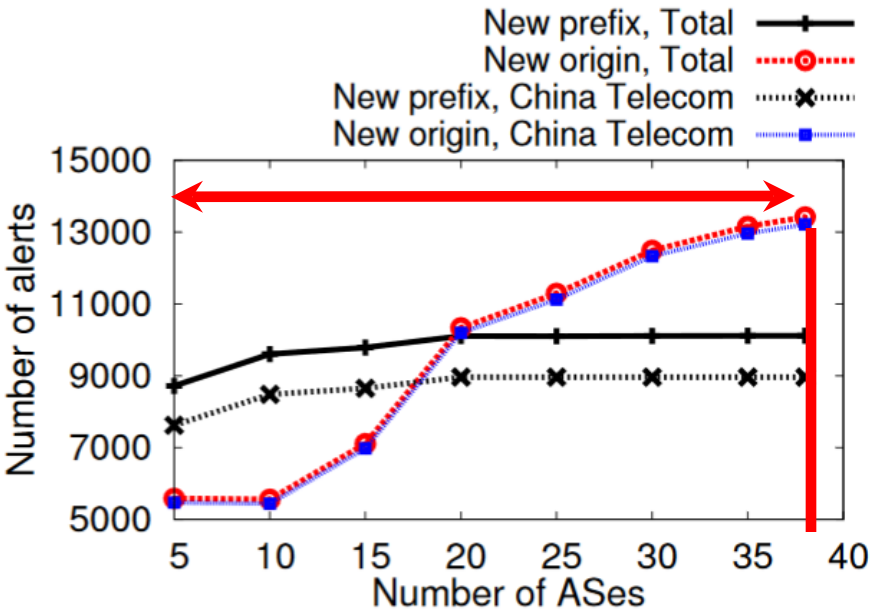
North America (NA)



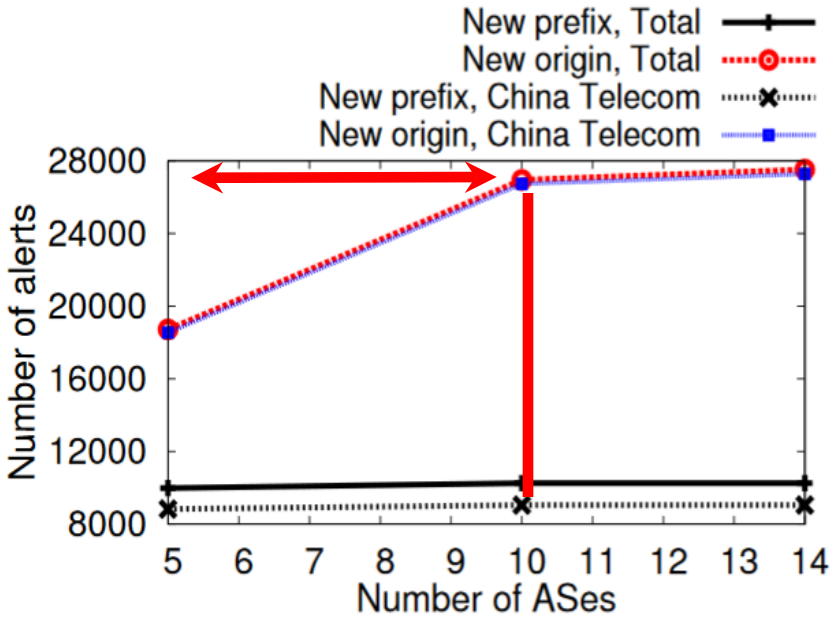
Rest of the world

- High detection rate in *rest of the world* despite fewer ASes
- Regional deployment along with ASes from other regions

Scale and locality



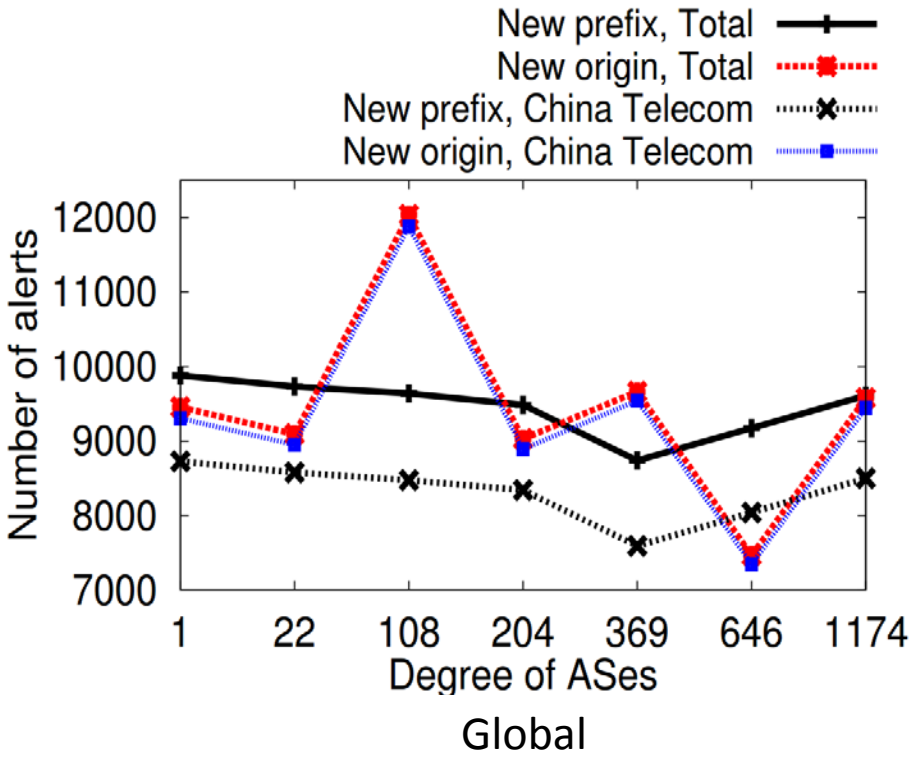
North America (NA)



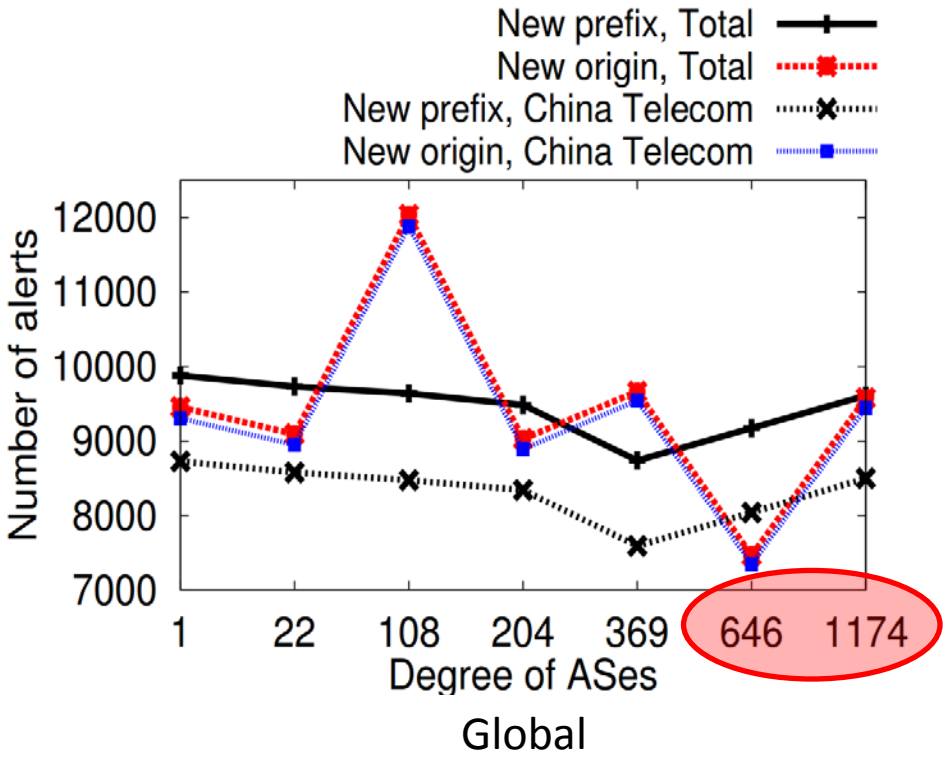
Rest of the world

- High detection rate in *rest of the world* despite fewer ASes
- Regional deployment along with ASes from other regions

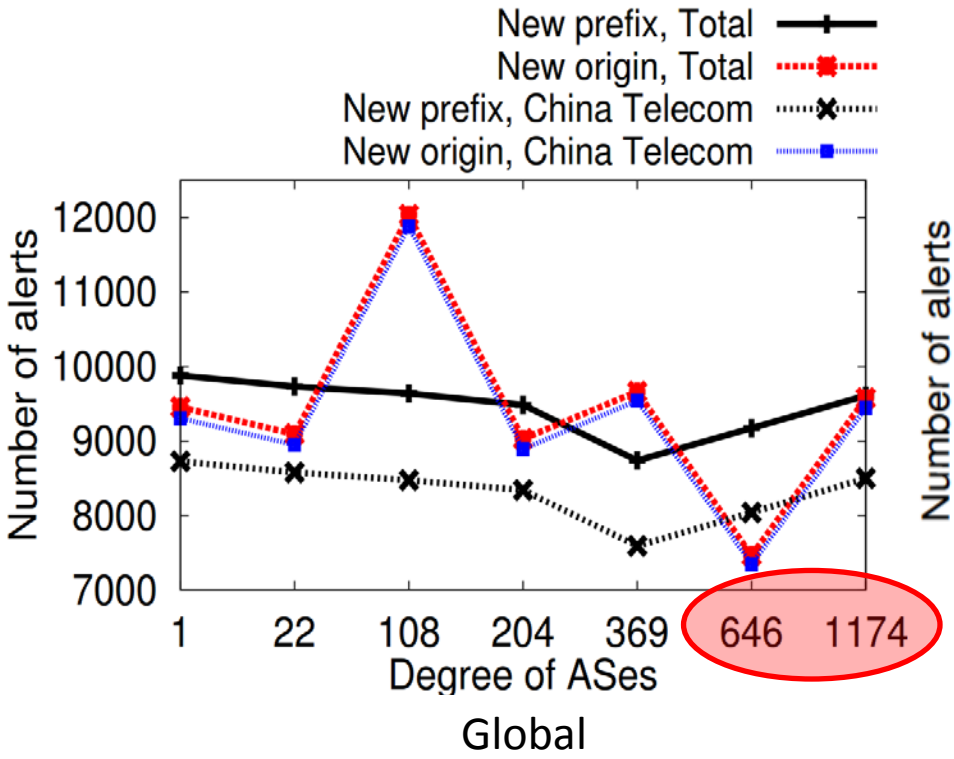
Size and locality



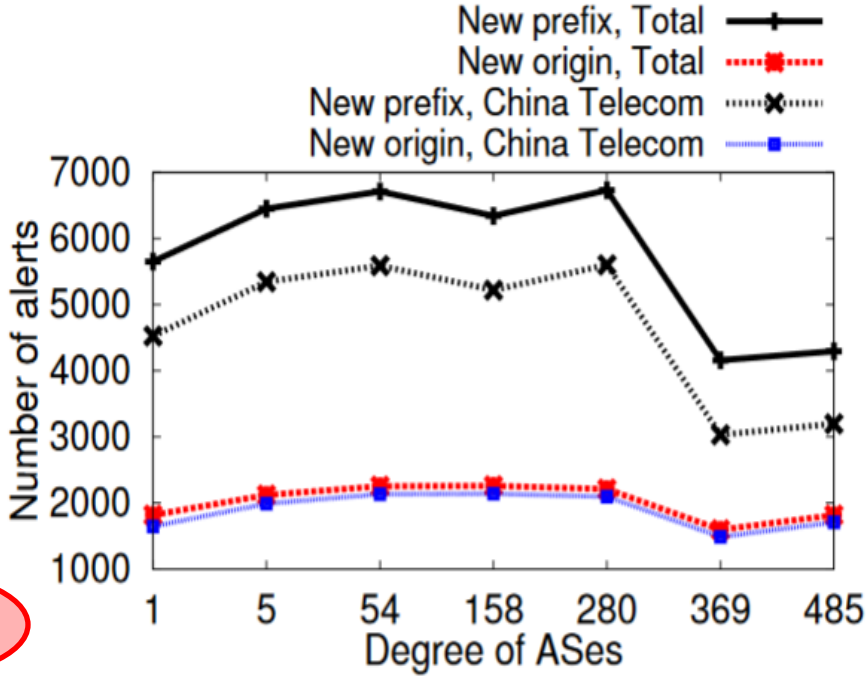
Size and locality



Size and locality

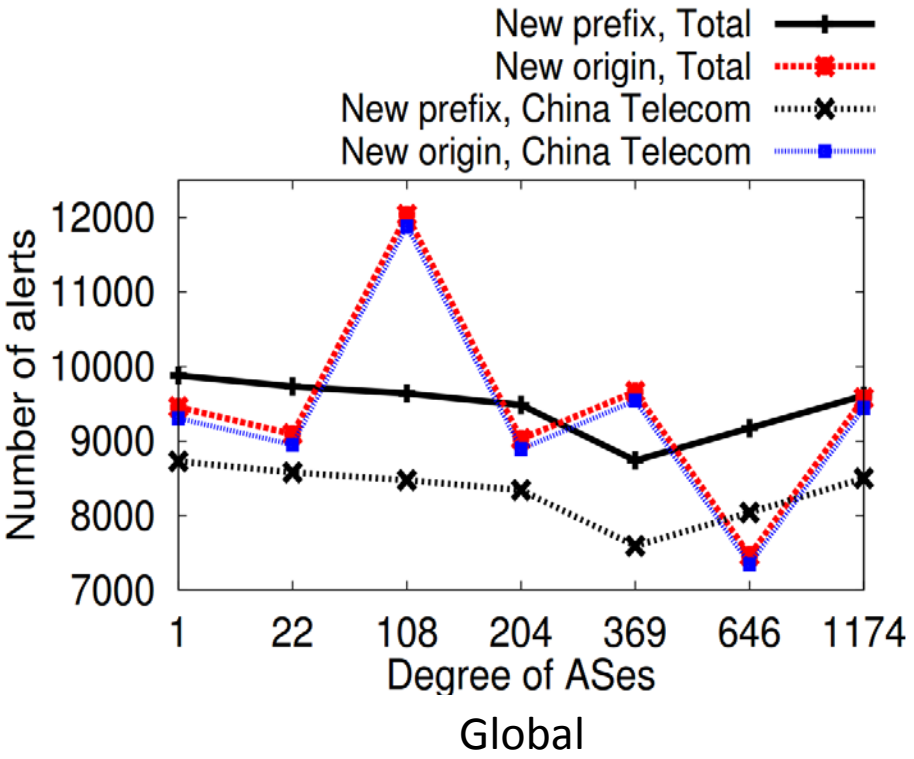


Global

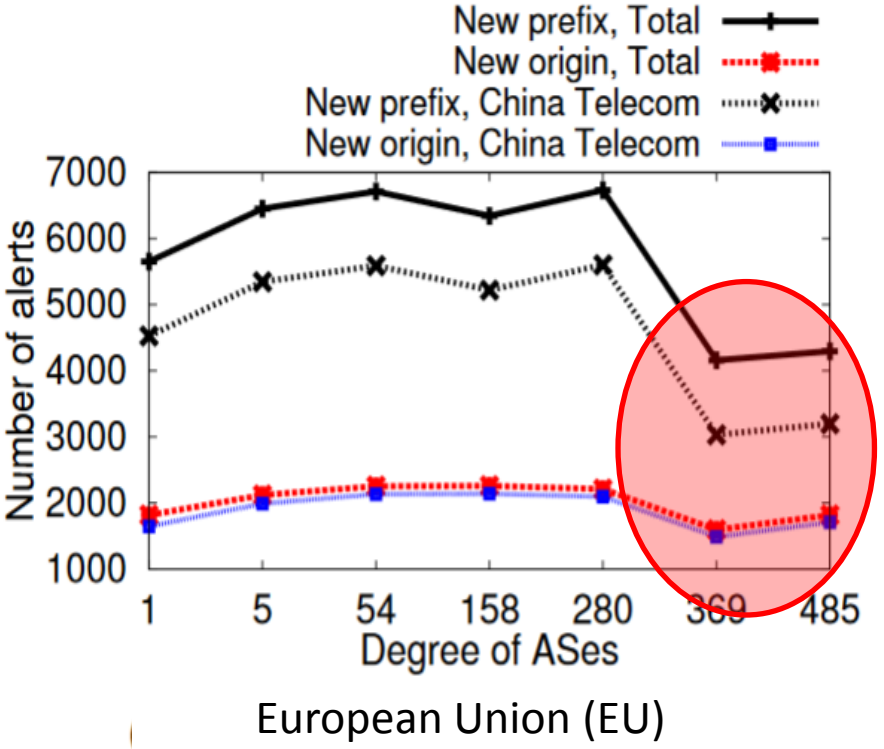


European Union (EU)

Size and locality



Global



European Union (EU)

Summary and contributions

- China Telecom incident characterization
  - Pointers to route leakage but difficult to rule out malicious intent
- On collaboration
  - Design collaborative mechanisms with decentralized operation
  - Targeting different attacks
- On scale, size, and locality
  - Evaluate security gains for a plausible approach to drive the deployment of these mechanisms
  - Smaller networks have important role to play

Collaborative Network Security

Rahul Hiran

- **Does Scale, Size, and Locality Matter? Evaluation of Collaborative BGP Security Mechanisms**, *Proc. IFIP Networking,* 2016
- **Crowd-based Detection of Routing Anomalies on the Internet**, Proc. *IEEE CNS*, 2015
- **PrefiSec: A Distributed Alliance Framework for Collaborative BGP Monitoring and Prefix-based Security** , Proc. *ACM WISCS @CCS* Scottsdale, AZ, 2014
- **Characterizing Large-scale Routing Anomalies: A Case Study of the China Telecom Incident**, Proc. *PAM,* 2013
- **TRAP: Open Decentralized Distributed Spam Filtering**, Proc. TrustBus, 2011

LINKÖPING UNIVERSITY

CUGS National Graduate School of Computer Science