



Detecting Prefix Hijackings in the Internet with Argus

Xingang Shi **Yang Xiang** Zhiliang Wang
Xia Yin Jianping Wu

Tsinghua University

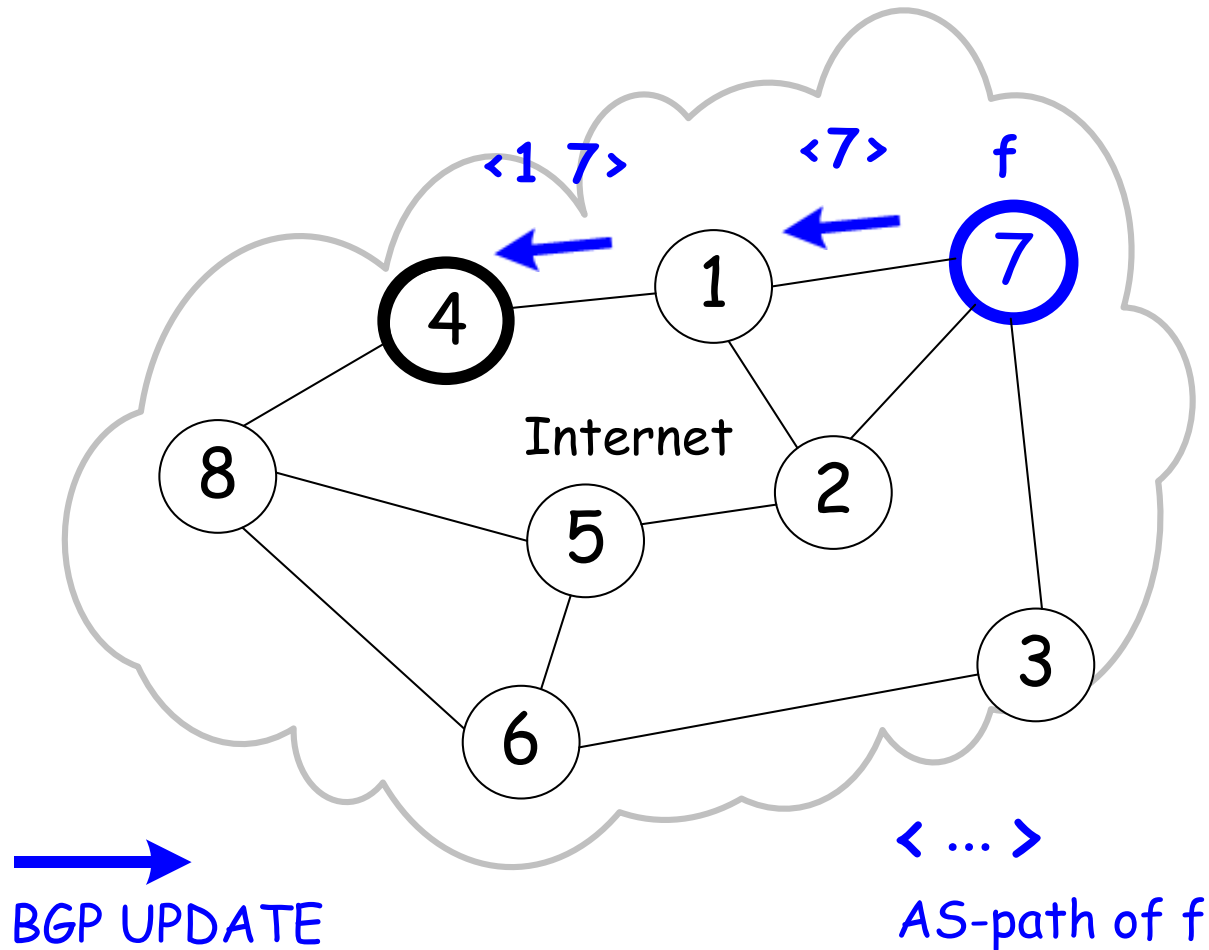
Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

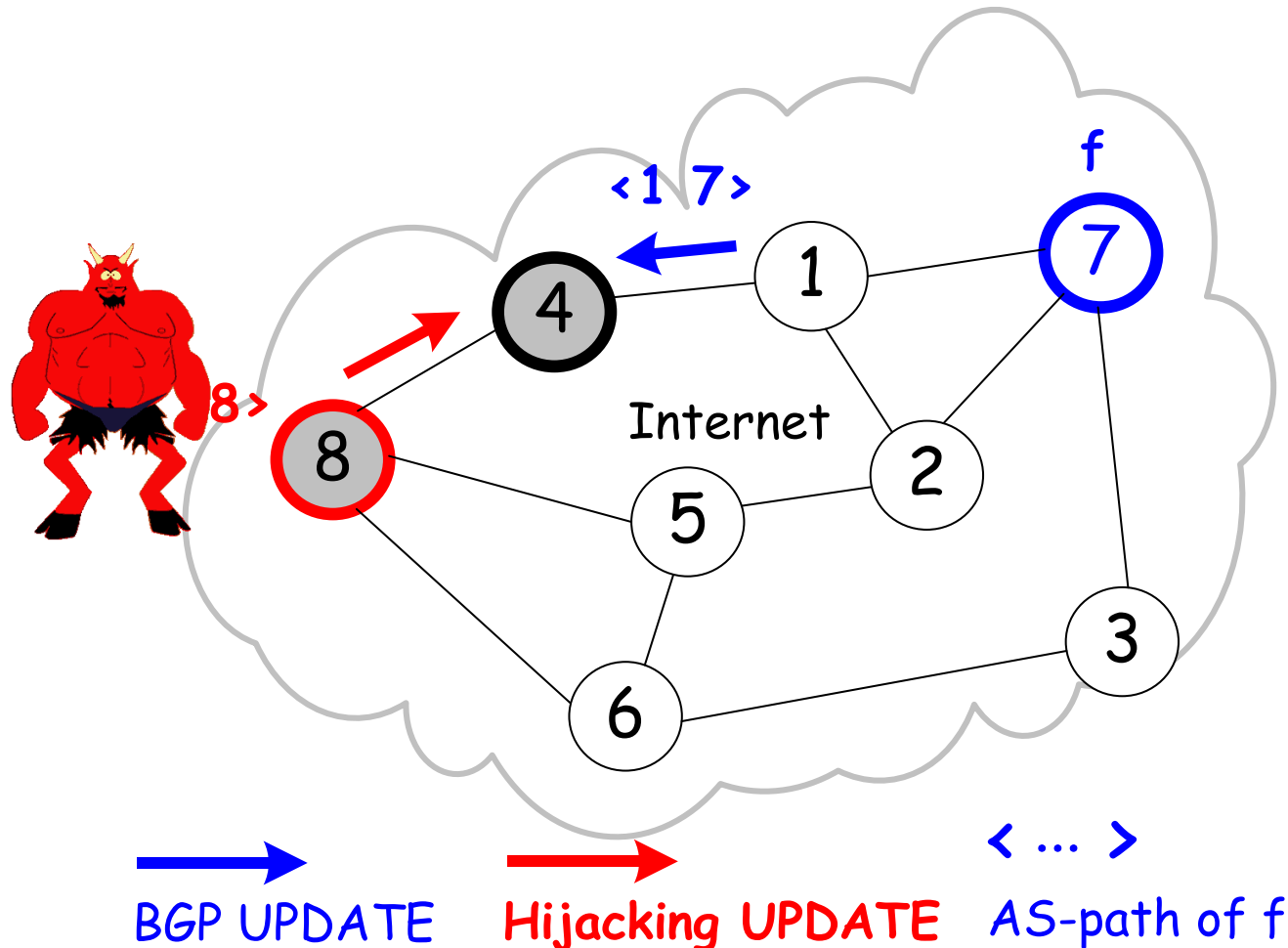
Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

Inter-domain Routing



Prefix Hijacking



Black-holing Hijackings

- Packets dropped by the attacker
- Also cased by **unintentional mis-configurations**
 - 2010, China Tele. hijacked **15%** of Internet
 - 2008, Pakistan Tele. hijacked Youtube for **2 hours**
- Other types such as imposture/interception
 - Harder to detect
 - E2E mechanisms, i.e., IPsec, HTTPS

Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

Challenges of Hijacking Detection

Hijacking can pollute a large number of ASes in several seconds!

short delay

high accuracy

Multi-homing, TE, BGP anycast, Backup links, Route failure, Policy change

Real system or service

easy to deploy

high scalability

Monitoring the whole Internet

Robust channel to notify the attacker

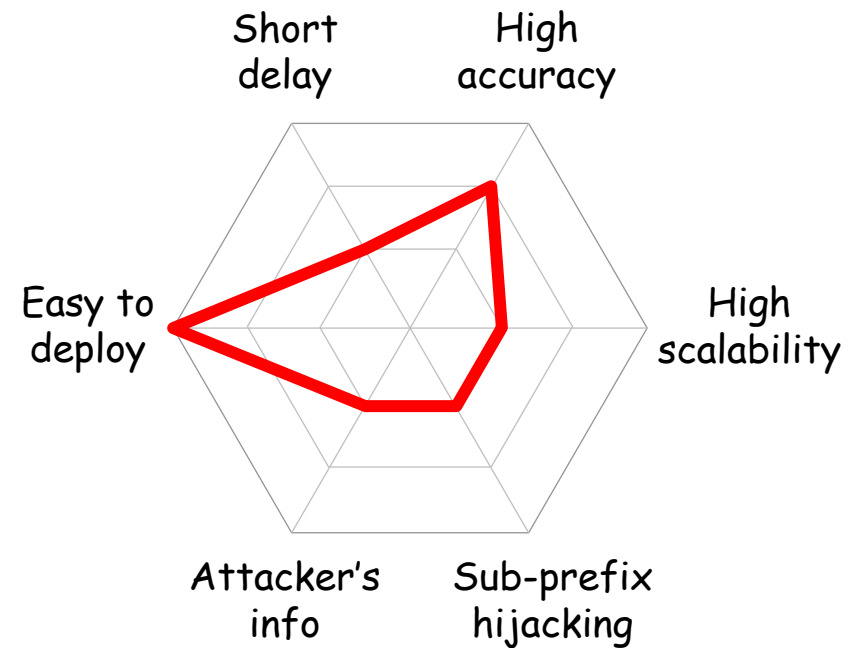
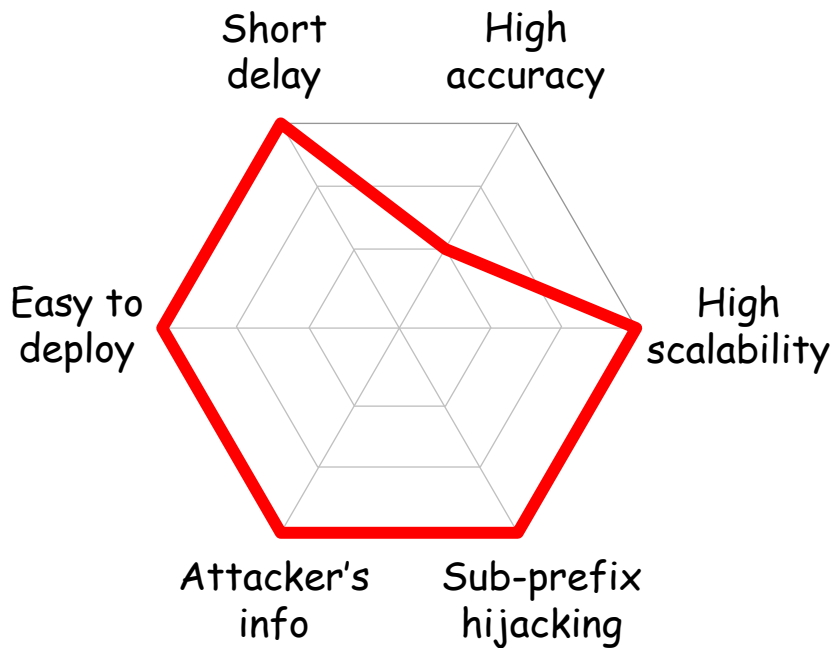
attacker's info

sub-prefix hijacking

Sub-prefix hijacking is more aggressive

Existing Control or Data Plane Methods

- Complementary advantages



- Control-plane monitoring

- BGPmon.net
- PHAS, Cyclops
- MyASN

- Data-plane probing

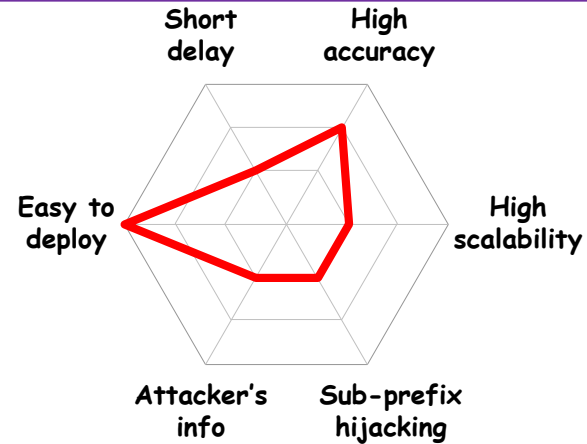
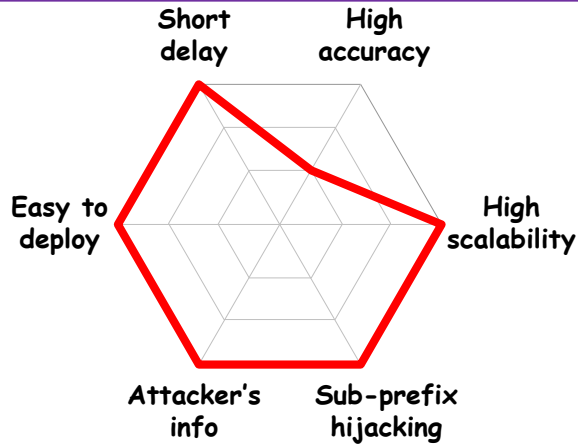
- iSPY [SIGCOMM '08]
- Reference Point [SIGCOMM '07]

Hybrid: control & data plane

- Hybrid solution [S&P '07]
 - Control-plane driven: monitoring anomalous route
 - Data-plane verification: whether it is a hijacking
- Cons.
 - **Minutes** of detection delay
 - Traceroute, nmap, IP/TCP timestamp, reflect scan, ...
 - **Hard to deploy**
 - Planetlab
 - BGP anycast
- Lack of **correlation** between control and data plane status

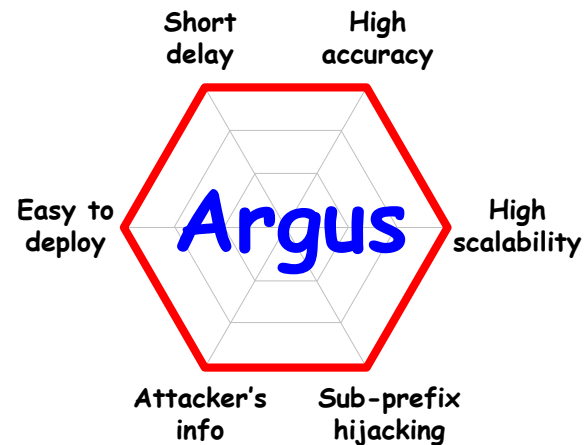
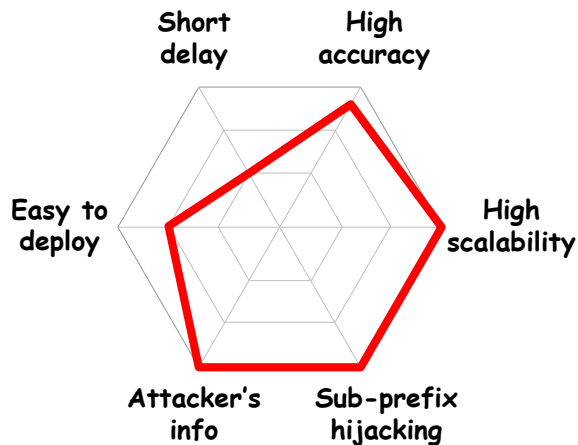
Our Approach

Control plane



Data plane

Hybrid



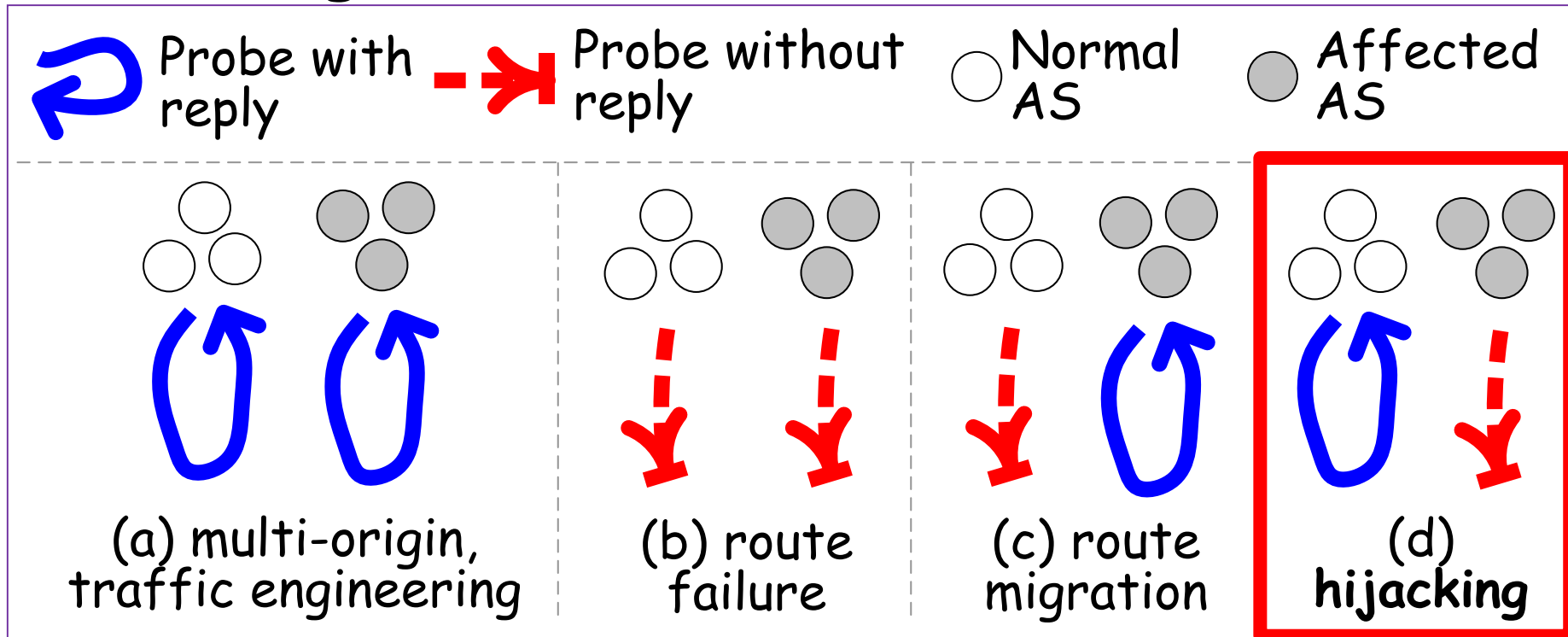
Correlation

Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

Key Observations: Relationship between Control and Data Plane

- Only part of the Internet is polluted
- Distinguishable from other route events



Status Matching

- **Eyes of Argus**: public route-servers, looking-glasses
 - Simple & fast commands: show ip bgp, ping
- Eye_j at time t
 - Control plane $C_{t,j}$: not affected by the anomalous route?
 - Data plane $D_{t,j}$: live IP in the corresponding prefix can be reached?

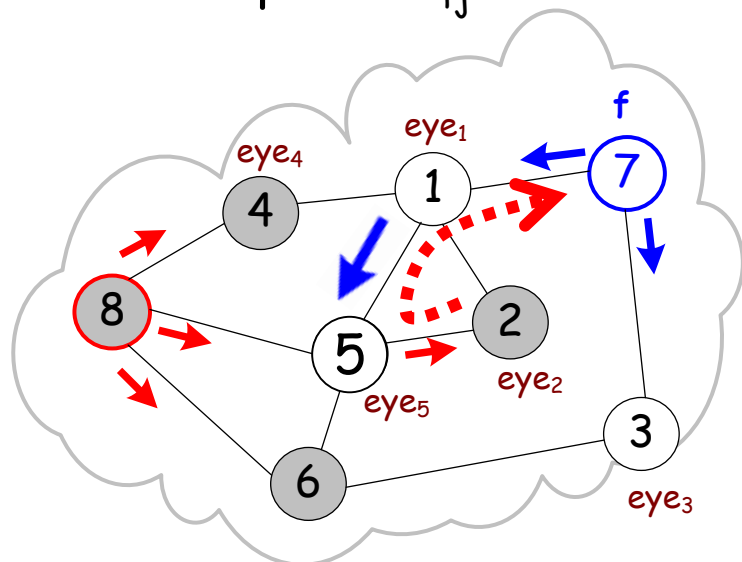
$$C_t = \{C_{t,j}\} = [1, 0, 1, 0, 0]$$

$$D_t = \{D_{t,j}\} = [1, 1, 1, 0, 0]$$

	$C_{t,j}$	$D_{t,j}$
eye ₁	1	1
eye ₂	0	1
eye ₃	1	1
eye ₄	0	0
eye ₅	0	0

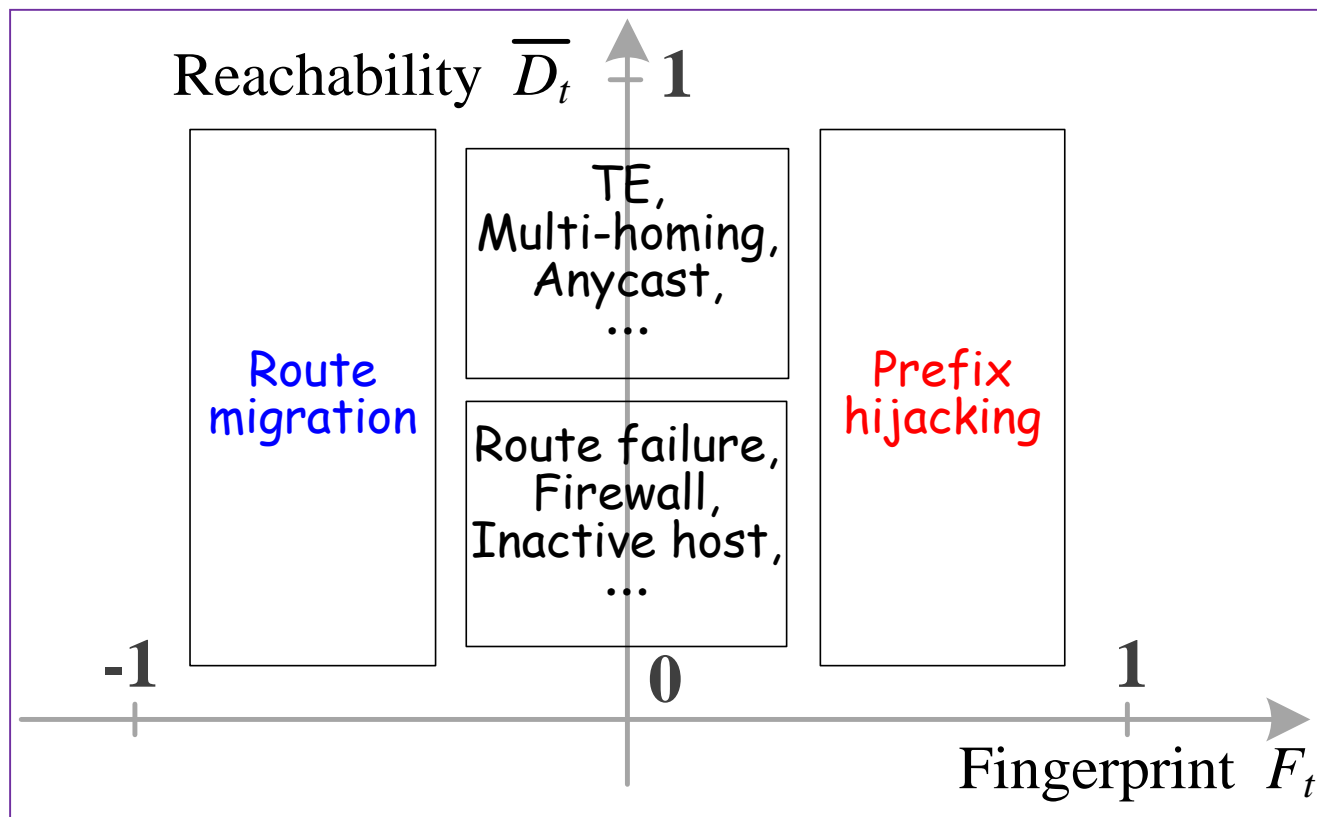
Fingerprint:

$$F_t = \frac{\sum_{j=1}^N [(C_{t,j} - \bar{C}_t)(D_{t,j} - \bar{D}_t)]}{\sqrt{\sum_{j=1}^N (C_{t,j} - \bar{C}_t)^2 \times \sum_{j=1}^N (D_{t,j} - \bar{D}_t)^2}}$$



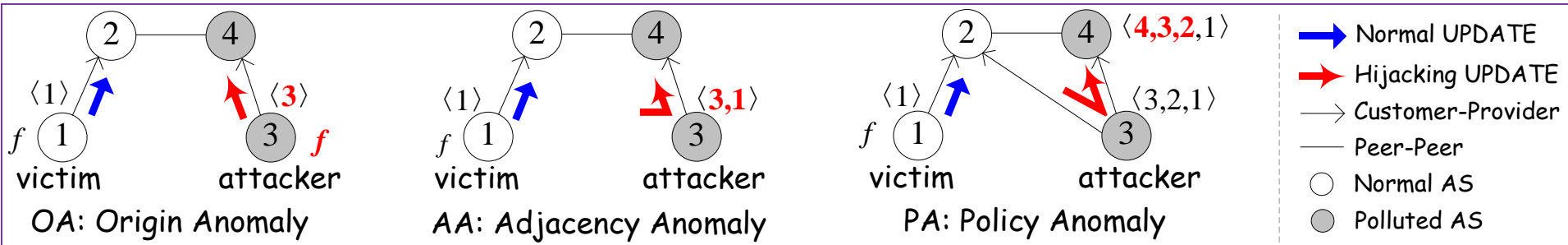
Identification of Prefix Hijacking

- Prefix hijacking: $F_t \rightarrow 1.0$, ($F_t \geq \text{threshold } \mu$)



Type of Anomalies

- AS-path $p = \langle a_n, \dots, a_{i+1}, a_i, a_{i-1}, \dots, a_0 \rangle$
 - OA: Origin Anomaly
 - Anomalous origin AS: $p_a = \langle a_0, f \rangle$
 - AA: Adjacency Anomaly
 - Anomalous AS pair in AS-path: $p_a = \langle a_j, a_{j-1} \rangle$
 - PA: Policy Anomaly
 - Anomalous AS triple in AS-path: $p_a = \langle a_{j+1}, a_j, a_{j-1} \rangle$



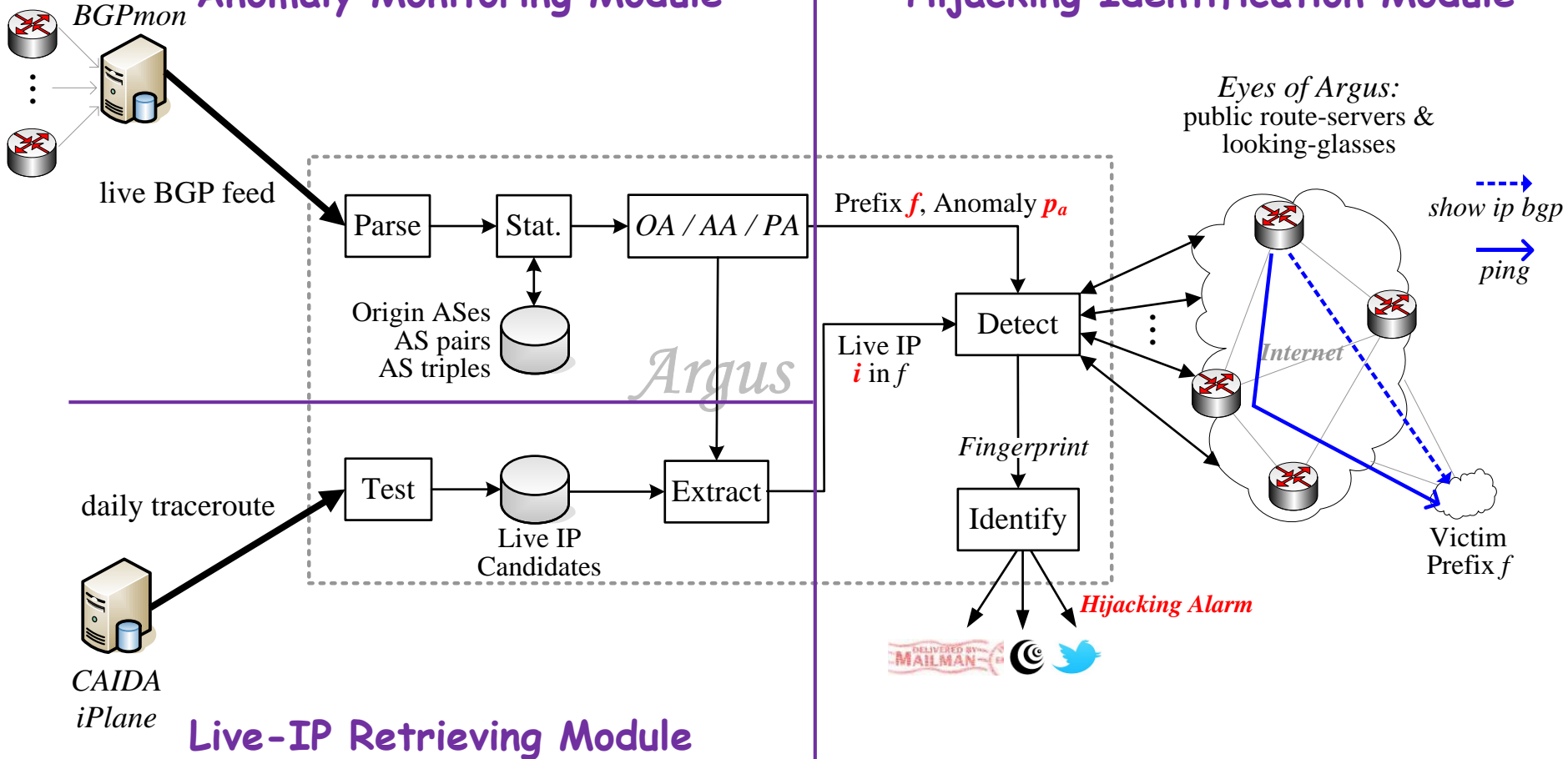
Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

Architecture of Argus

Anomaly Monitoring Module

Hijacking Identification Module



System Deployment

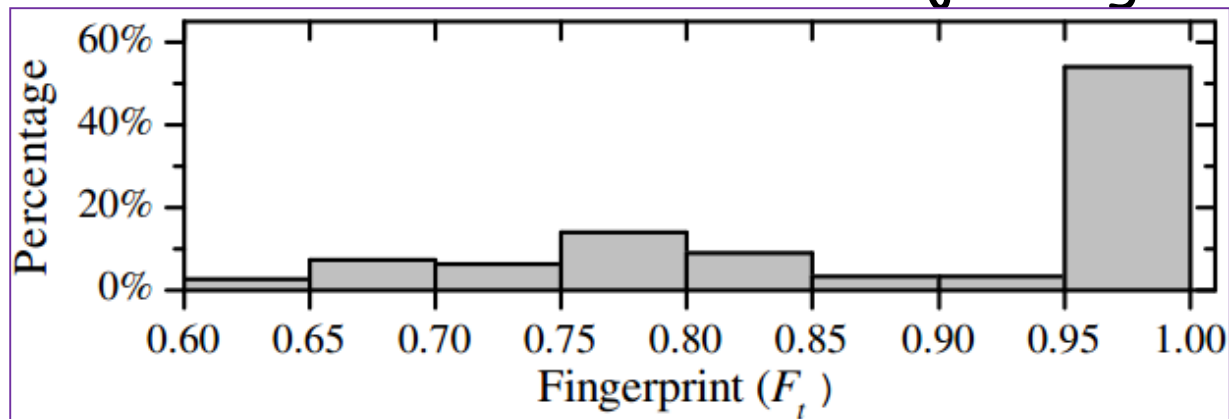
- From May 2011, launched >1 years
- Live BGP feed collected from ~130 peers
 - BGPmon: <http://bgpmon.netsec.colostate.edu/>
 - 10GB BGP UPDATE /day, 20Mbps peak
- 389 eyes, in 41 transit AS
- Online notification services
 - (AS-4847) Mailing list
 - (AS-13414, AS-35995) Twitter
 - (AS-4538) Website, web service APIs

Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

Argus is Online

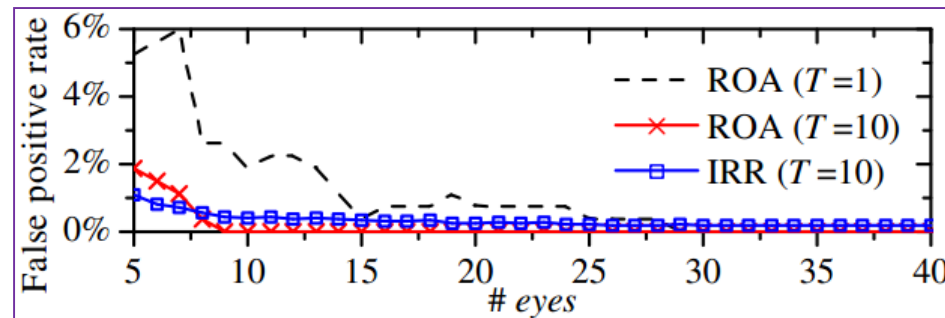
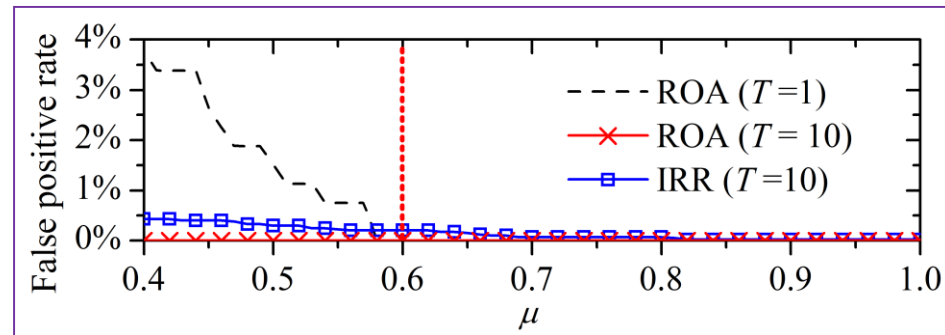
- 40k anomalous route events
- **220 stable hijackings**
 - Duration of $F_+ \geq \mu$ in more than T seconds
 - μ : fingerprint threshold of hijacking
 - T : duration threshold of stable hijacking



Fingerprint (F_+) distribution of all stable hijackings.

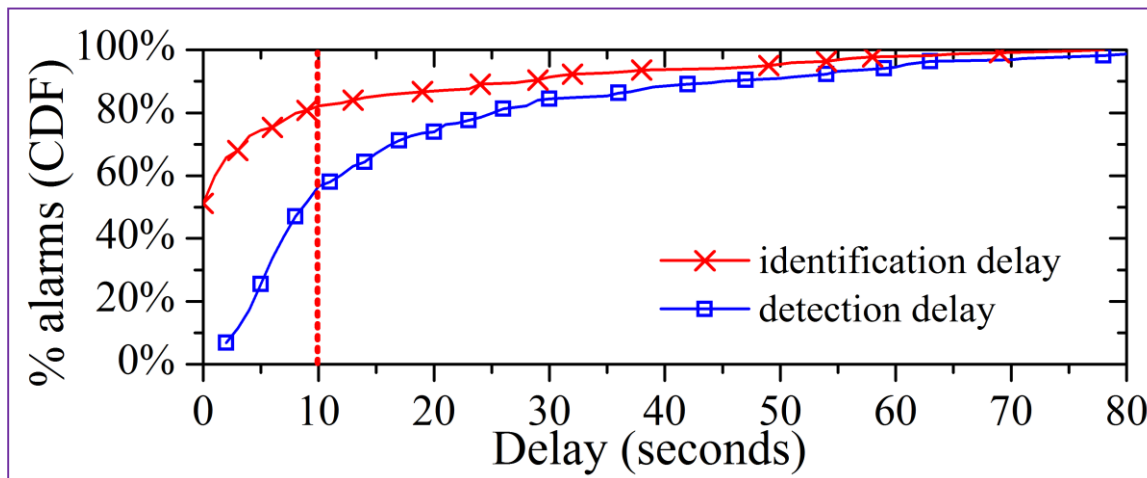
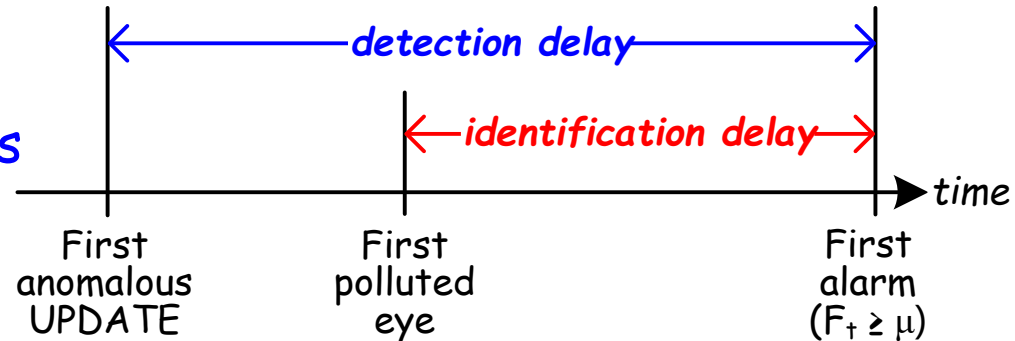
False Positive

- Directly contact network operators (March-April, 2012)
 - 10/31 confirmed our hijacking alarms
 - No objection
- ROA: Route Origin Authorization
 - 266 anomalies with ROA records
 - False positive 0%
($\mu=0.6$, $T=10$, $\#eyes=40$)
- IRR: Internet Routing Registry
 - 3988 anomalies with IRR records
 - False positive 0.2%
($\mu=0.6$, $T=10$, $\#eyes=40$)



Delay

- Detection delay
 - 60% less than 10 seconds
- Identification delay
 - 80% less than 10 seconds
 - 50% less than 1 second



Outline

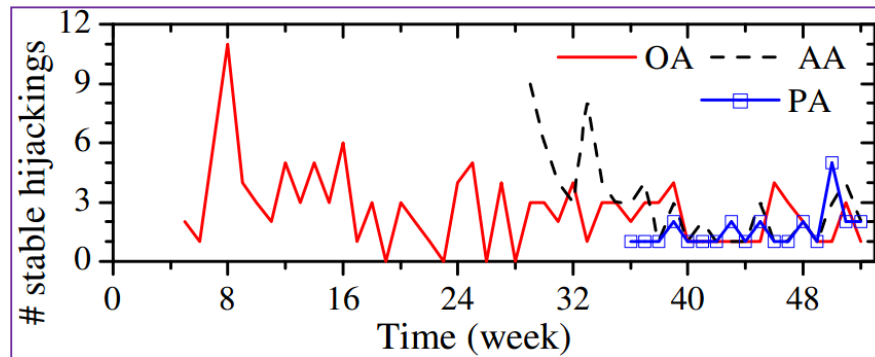
- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - **Statistics**
 - Case Studies
- Conclusion

Statistics - Overview

- Adjacency/Policy based hijacking do exists

	Total	OA (origin AS)	AA (Adjacency)	PA (Policy)
Anomalies	40k	20k	6.7k	13.3k
Hijackings	220	122	71	27

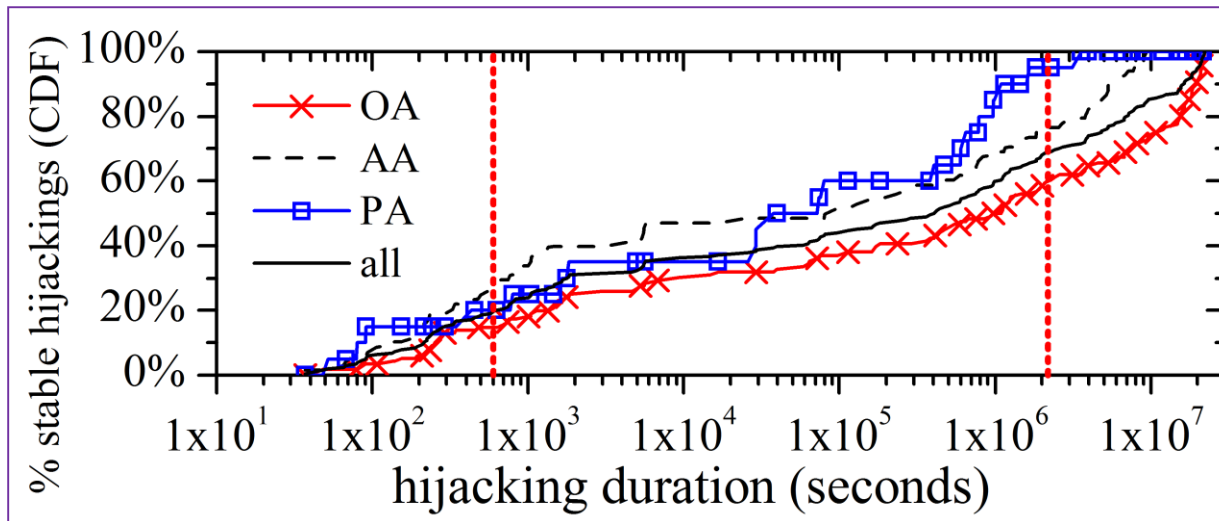
Total # of route anomalies and stable hijackings in one year.



Weekly # of stable hijackings.

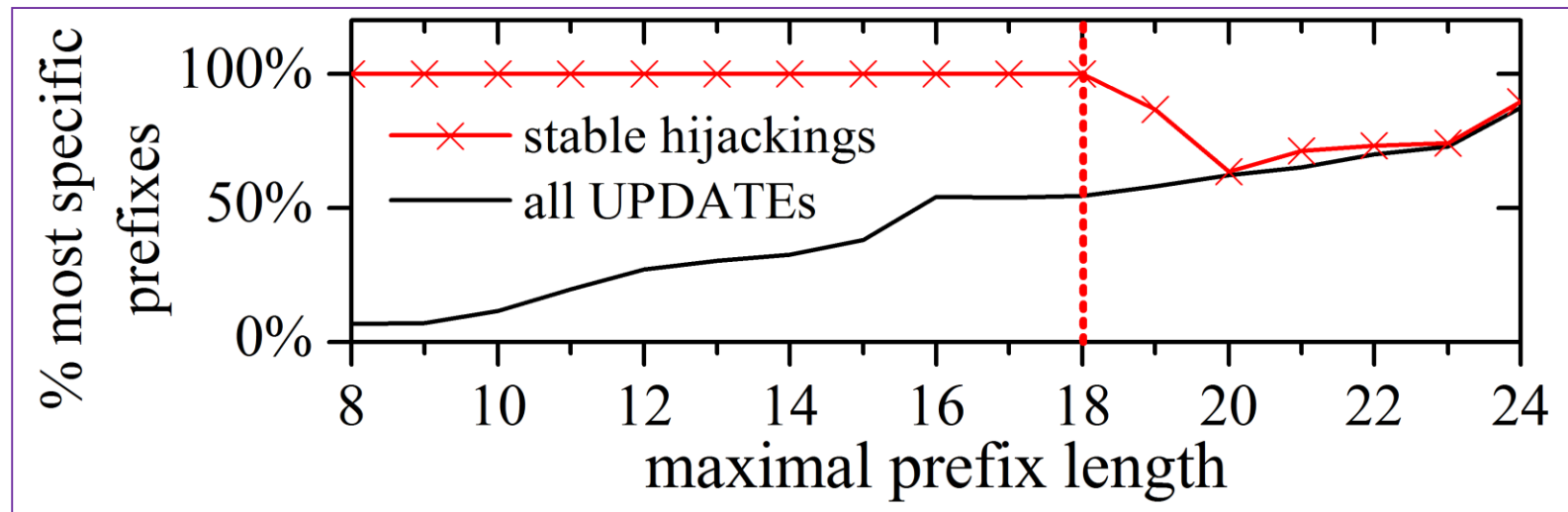
Statistics - Hijacking duration

- Stable hijacking duration: live time of anomalous route
 - 20+% hijackings last <10 minutes
 - Long hijackings also exist



Statistics - Prefix length

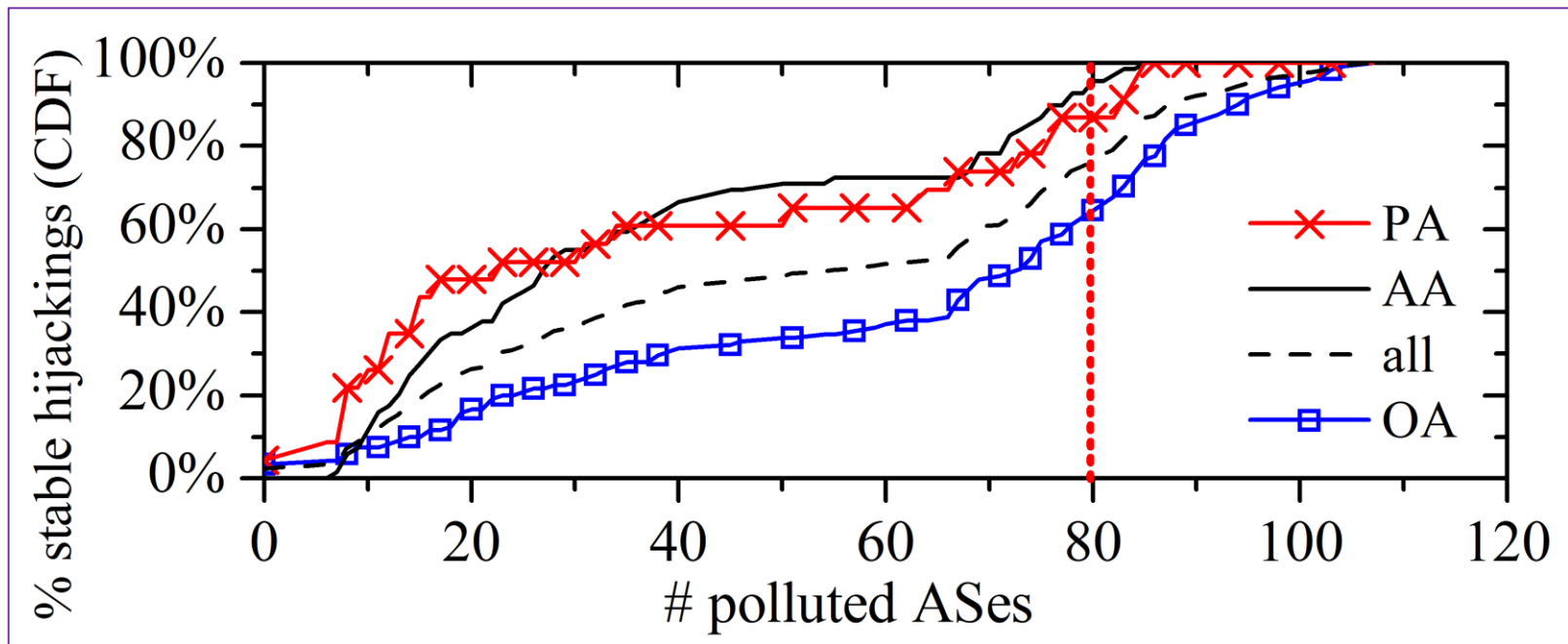
- Stable hijackings with most specific prefix
 - 91% hijacked prefixes are most specific
 - **100%** hijacked prefixes with length ≤ 18 are most specific



- **10%** stable hijackings are sub-prefix hijacking

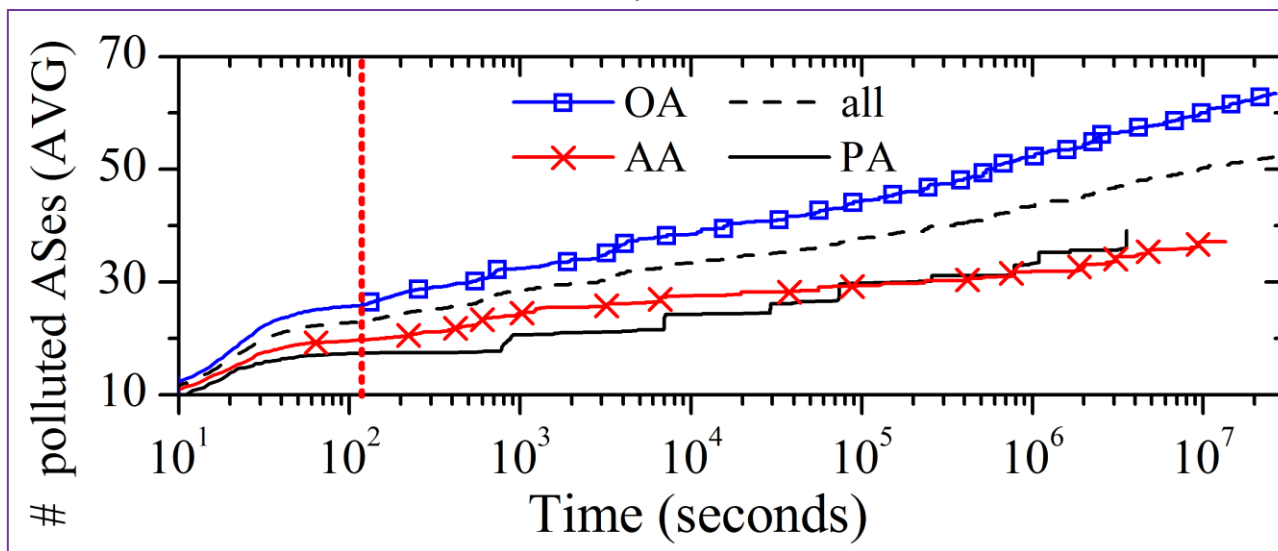
Statistics - Pollution scale

- 20% stable hijackings could pollute 80+ transit ASes



Statistics - Pollution speed

- 20+ transit ASes are polluted in 2 minutes



- For hijackings polluted 80+ transit ASes
 - 50% Internet are polluted within 20 seconds
 - 90% Internet are polluted within 2 minutes

Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

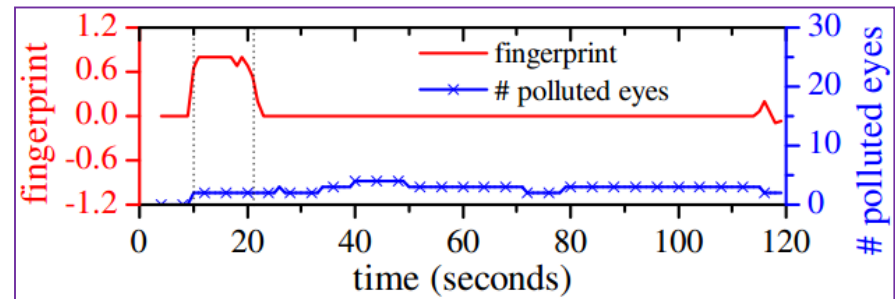
Case Studies

- OA hijackings (confirmed by email)
 - Missing route filters
 - Network maintenance misplay
 - Premature migration attempt
 - Sub-prefix hijacking
- AA hijackings (confirmed by email)
 - Mis-configuration in TE
 - AS-path poisoning experiment
- PA hijackings (verified in IRR)
 - Import policy violation
 - Export policy violation

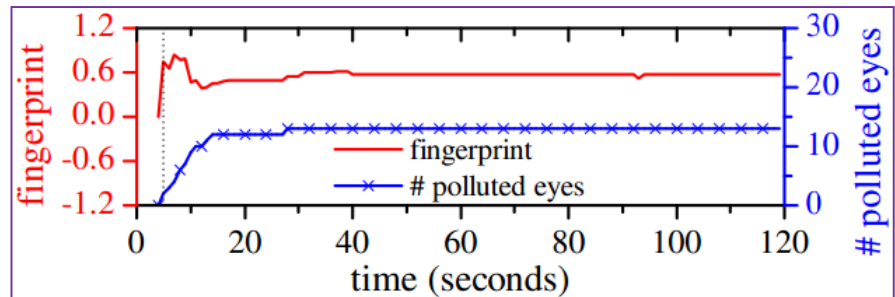
OA Hijackings

Time	Prefix	Normal Origin	Anomalous Origin	Duration	Delay
Nov. 27, 2011	166.111.32.0/24, ...	AS-4538 CERNET, CN	AS-23910 CERNET-2, CN	10+ sec	10 sec
Mar. 20, 2012	193.105.17.0/24	AS-50407 Douglas, DE	AS-15763 DOKOM, DE	12 min	5 sec

- Missing route filters



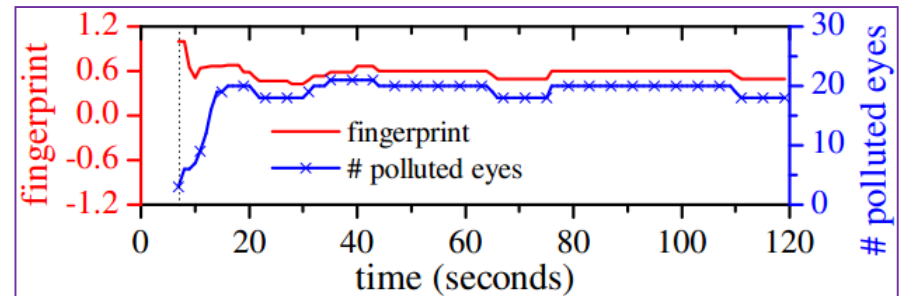
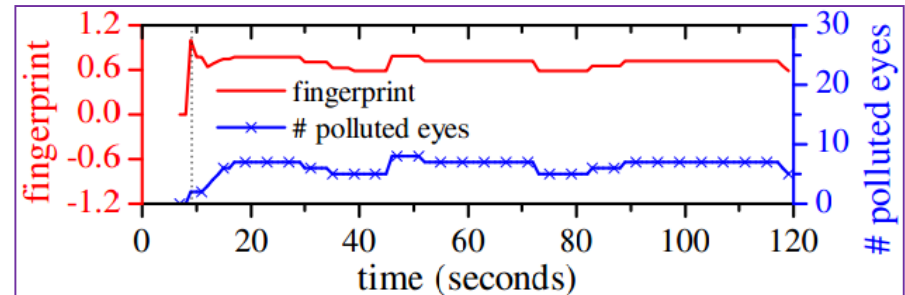
- Network maintenance misplay



OA Hijackings

Time	Prefix	Normal Origin	Anomalous Origin	Duration	Delay
Apr. 04, 2012	91.217.242.0/24	AS-197279 WizjaNet, PL	AS-48559 Infomex, PL	17 min	9
Mar. 22, 2012	12.231.155.0/24 (in 12.128.0.0/9)	AS-7018 AT&T, US	AS-13490 Buckeye, US	16 min	7

- Premature migration attempt
- Sub-prefix hijacking



AA Hijackings

Time	Prefix	AS-path	Delay
Apr. 12, 2012	210.1.38.0/24	<3043 174 38082 38794 24465>	12
Mar. 31, 2012	184.464.255.0/24	<4739 6939 2381 47065 19782 47065>	4

- Mis-configuration in TE
 - **AS-38794** (**BB-Broadband, TH**) is a new provider of AS-24465 (Kasikorn, TH)
- AS-path poisoning experiment [SIGCOMM '12]
 - BBN announces loop AS-paths **<47065, x, 47065>** for experimental purpose

PA Hijackings

Time	Prefix	AS-path	Delay
Apr. 19, 2012	77.223.240.0/22	<4739 24709 25388 21021 12741 47728 >	9
Apr. 16, 2012	195.10.205.0/24	<3043 174 20764 31484 3267 3216 35813>	5

- Import policy violation

IRR info. of

AS-21021

(**Multimedia, PL**):

```
import: from AS12741 action pref=150; accept AS12741
export: to AS12741 announce AS21021
```

- Export policy violation

IRR info. of

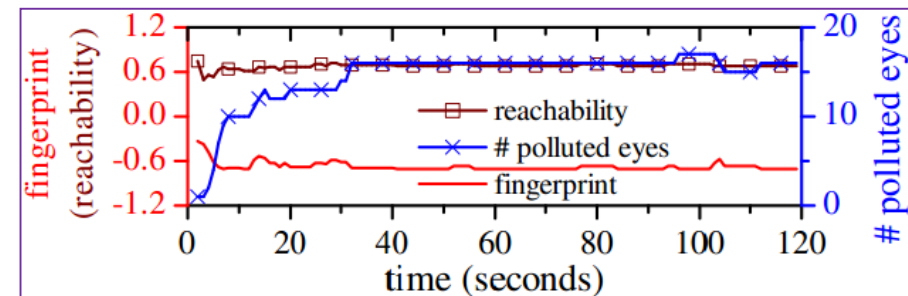
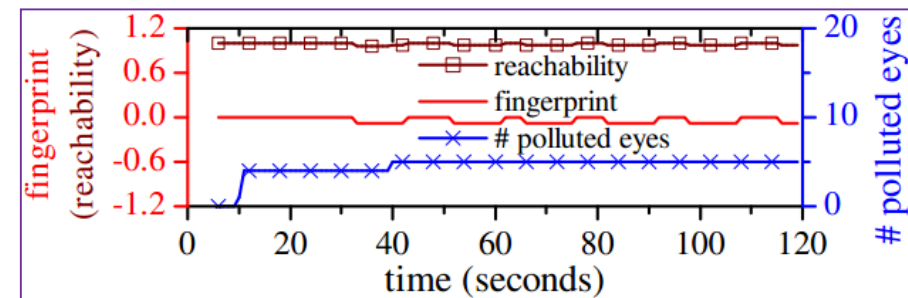
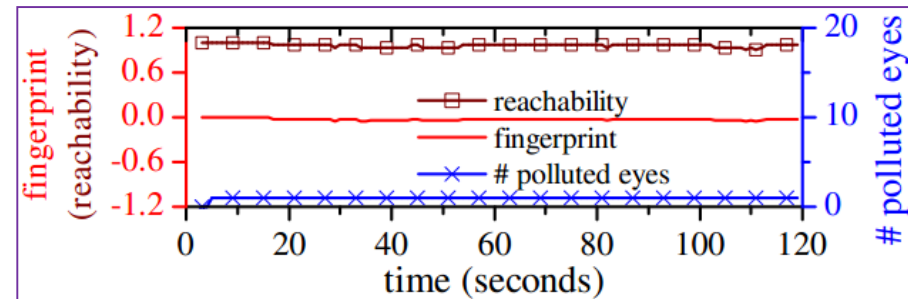
AS-31484

(**OOO Direct Tele., RU**):

```
remarks: --- Uplinks ---
import: from AS3267 action pref=85; accept ANY
export: to AS3267 announce AS31484 AND AS196931
import: from AS20764 action pref=85; accept ANY
export: to AS20764 announce AS31484 AND AS196931
```

Non-hijacking Anomalies

- TE using BGP anycast
 - 193.0.16.0/24 (DNS root-k) suddenly originated by AS-197000 (RIPE)
 - $F_+ \rightarrow 0, D_+ = 1$
- TE with backup links
 - AS-12476 (Aster, PL) announced prefix to a new provider AS-6453 (Tata, CA)
 - $F_+ \rightarrow 0, D_+ = 1$
- Route migration
 - Prefix owner changed from AS-12653 (KB Impuls, GR) to AS-7700 (Singapore Tele)
 - $F_+ \rightarrow -1$



Outline

- Introduction
 - Prefix Hijacking
 - Existing Detection Methods
- Argus
 - Key Observation & Algorithm
 - System Architecture & Implementation
- Internet Monitoring Practice
 - Evaluation
 - Statistics
 - Case Studies
- Conclusion

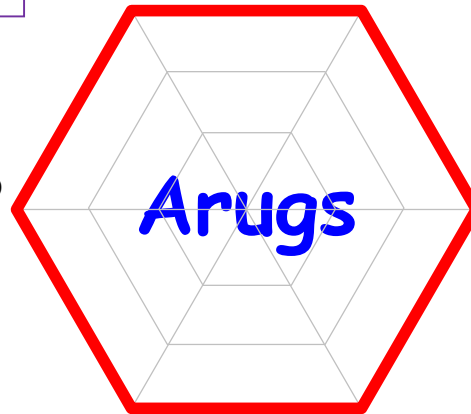
Conclusion of Our Contributions

- 80% delay <10 seconds
- 20% stable hijackings last <10 minutes, some can pollute 90% Internet in <2 minutes

- OA, AA, PA anomalies
- ROA, IRR, email confirmation

- show ip bgp, ping
- Public available external resources

Easy to deploy



High scalability

- Anomaly driven probing
- Monitoring the whole Internet

- Live BGP feed from BGPmon
- Victims can be noticed through several channels

Attacker's info

Sub-prefix hijacking

- 10% stable hijackings are sub-prefix hijacking

One year's Internet detection practice.



"Now Argus had a hundred eyes in his head, and never went to sleep with more than two at a time, so he kept watch of Io constantly."

-- Thomas Bulfinch, *The Age of Fable* (Philadelphia: Henry Altemus Company, 1897) 39

Thanks!

Q & A

- **Algorithm** for realtime & accurate hijacking detection
- **Online system** that monitoring the whole Internet
- **Online services** for network operators / researchers
- **One year** Internet wide hijacking detection practice
- **Root cause analysis** of hijackings and anomalies

tli.tl/argus

twitter.com/sharangxy



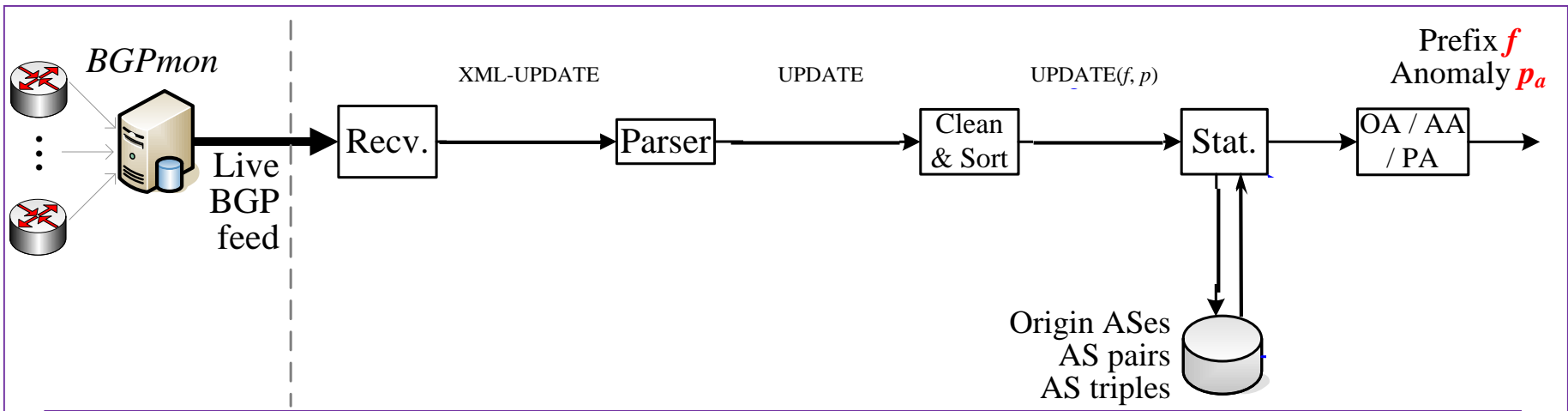
Backups

We focus on black-hole hijackings

- **Mis-configuration** typically cause black-holing
 - 2010, China Tele. hijacked **15%** of Internet
 - 2008, Pakistan Tele. hijacked Youtube for **two hours**
- ISP is trustworthy, malicious attack is relatively rare
- Perfect imposture/interception is difficult
 - Mimic all behaviors, forward all the traffic
- Detect interception is hard, any AS is a MITM
- E2E mechanism is more effective in preventing imposture/interception

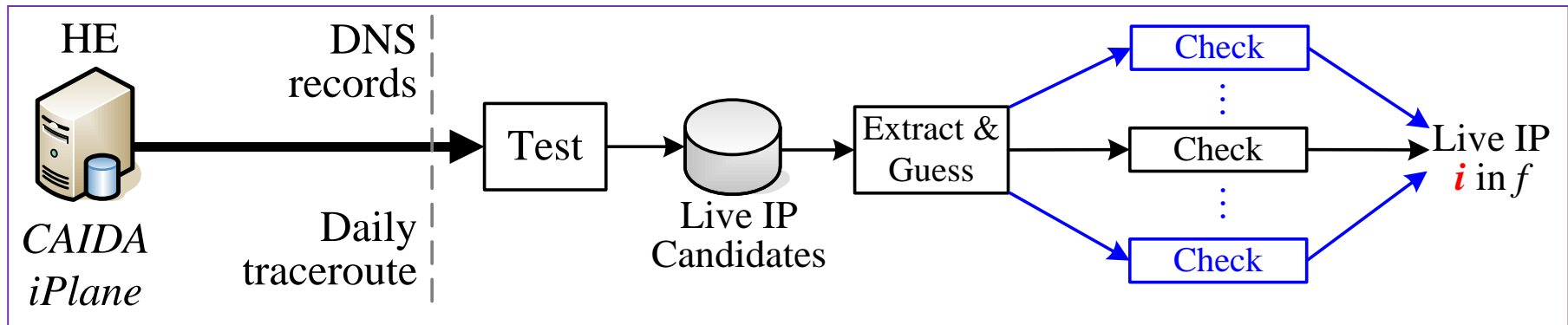
Anomaly Monitoring Module

- Live BGP feed, collected from ~130 peers
 - BGPmon: <http://bgpmon.netsec.colostate.edu/>
- 10GB BGP UPDATE /day, 20Mbps peak
 - 4-stage pipeline processing
 - Parallel UPDATE parser
 - Mem-cached DB read, batch write



Live-IP Retrieving Module

- Live-IP candidates in prefix f
 - Traceroute results, DNS records
 - Possible gateways
 - The first/last IP in every sub-prefix
- 512-parallel checking, find a live target in <1 second



Hijacking Identification Module

- Distinguish hijacking from other route events
 - Acquire C_+ and D_+
 - Calculate F_+
 - Last for $W=120$ seconds for every anomaly
- $N=389$ eyes, in 41 transit AS
- Online services
 - (AS-4847) Mailing list
 - (AS-13414, AS-35995) Twitter
 - (AS-4538) Website, web service APIs

