INTENDER: Fuzzing Intent-Based Networking with Intent-State Transition Guidance

Jiwon Kim[1], Benjamin E. Ujcich[2], and Dave (Jing) Tian[1]

[1]Purdue University [2]Georgetown University

USENIX Security 2023

MANUAL

wttw

NEWS

BUSINESS

Facebook Blames Outage on Error During Routine Maintenance

Associated Press | October 6, 2021 11:05 am

BLEEPINGCOMPUTER

Search Site LOGIN SIGN UP

NEWS DOWNLOADS VPNS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

South Korean telco KT suffers nationwide outage after routing error

October 25, 2021 12:20 PM 0

BBC Home News Sport Reel Worklife Travel Future

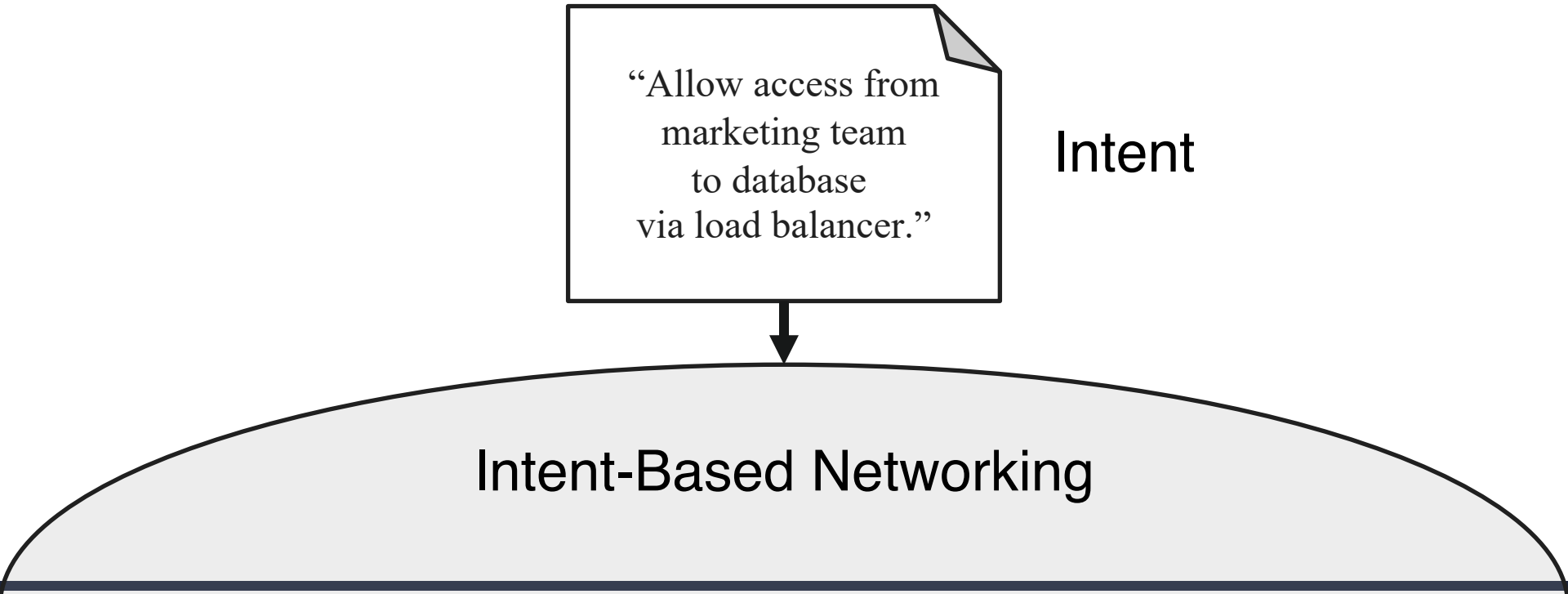
NEWS

Home | War in Ukraine | Climate | Video | World | US & Canada | UK | Business | Tech | Science | More

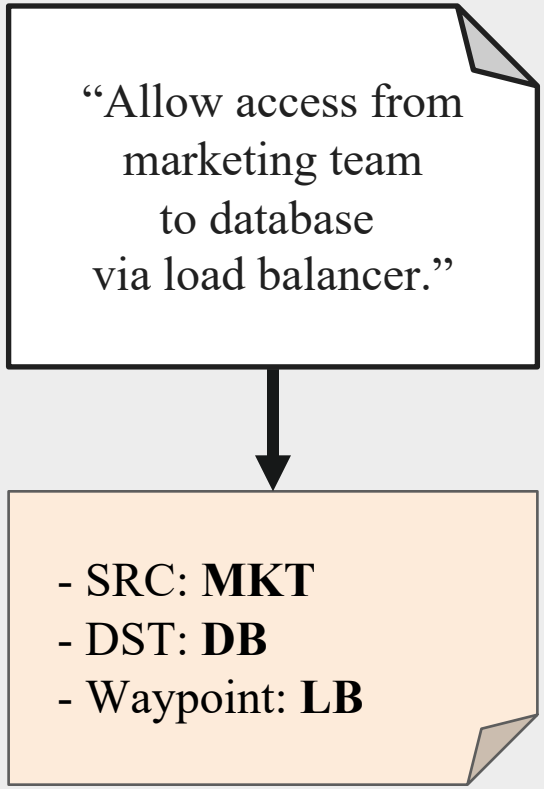
Europe | Guernsey

Human error behind network outage, Sure confirms

3 February


“Allow access from
marketing team
to database
via load balancer.”
Intent
Intent-Based Networking

Translation



Compilation

Network-level Intent(s)

- SRC: **MKT**
- DST: **DB**
- Waypoint: **LB**

```
config {
  service: db.aa.com
  vip: DB
  port: 3306
  backends: [DB1, 2, 3]
}
```

IN	SRC	DST	OUT
1	MKT1	DB	LB
2	MKT2	DB	LB

Network Object(s)

Activation

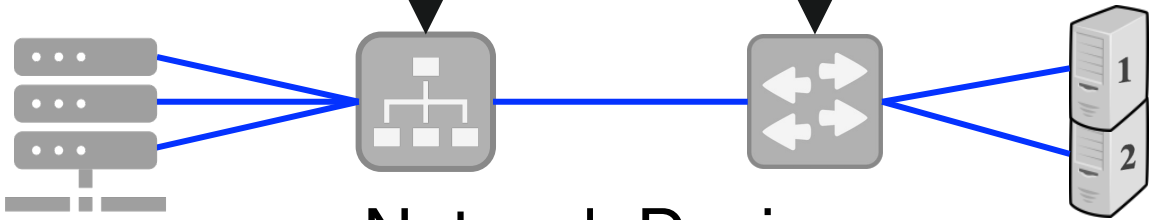
```
config {
  service: db.aa.com
  vip: DB
  port: 3306
  backends: [DB1, 2, 3]
}
```

IN	SRC	DST	OUT
1	MKT1	DB	LB
2	MKT2	DB	LB

Network Object(s)

Control Plane

Data Plane



Network Devices

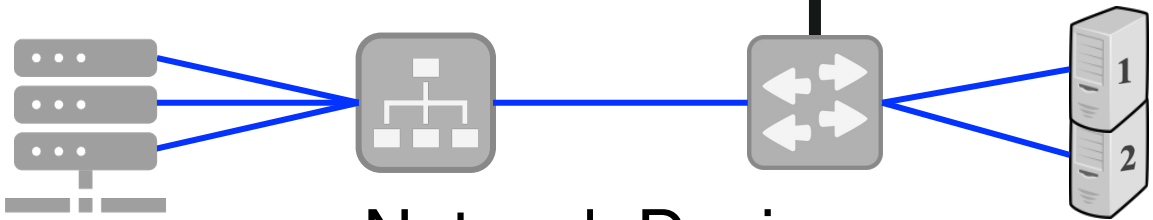
Monitoring

Telemetry Data

```
[S1] RX/TX
MKT1:   20mbps/20kbps
MKT2:  980mbps/20kbps
LB:     40kbps/ 1gbps
```

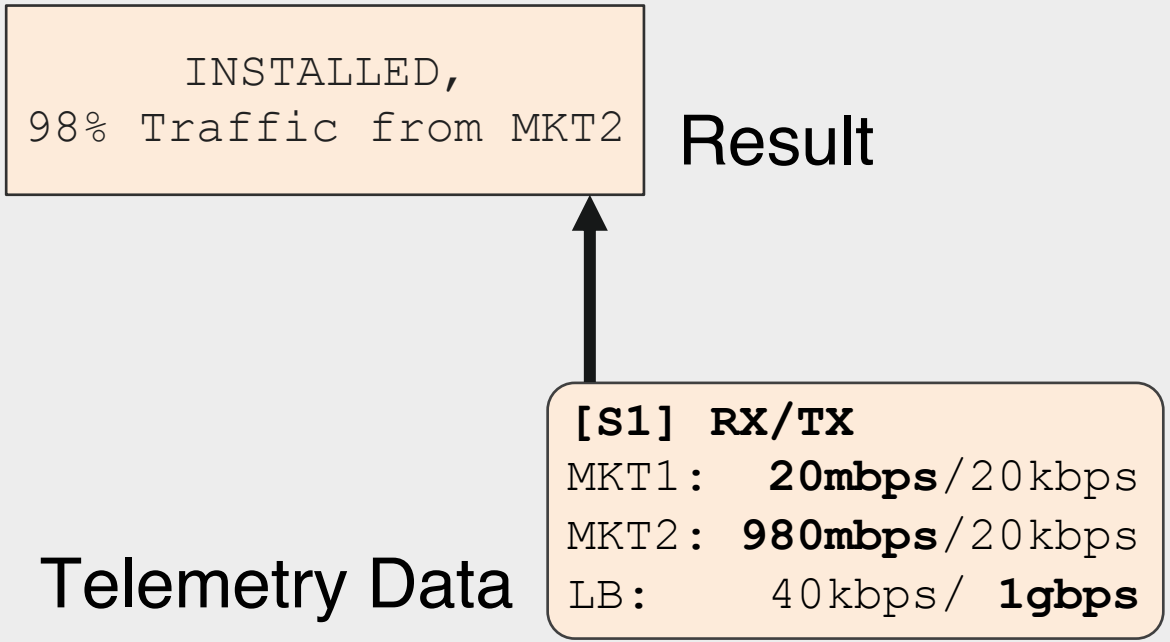
Control Plane

Data Plane

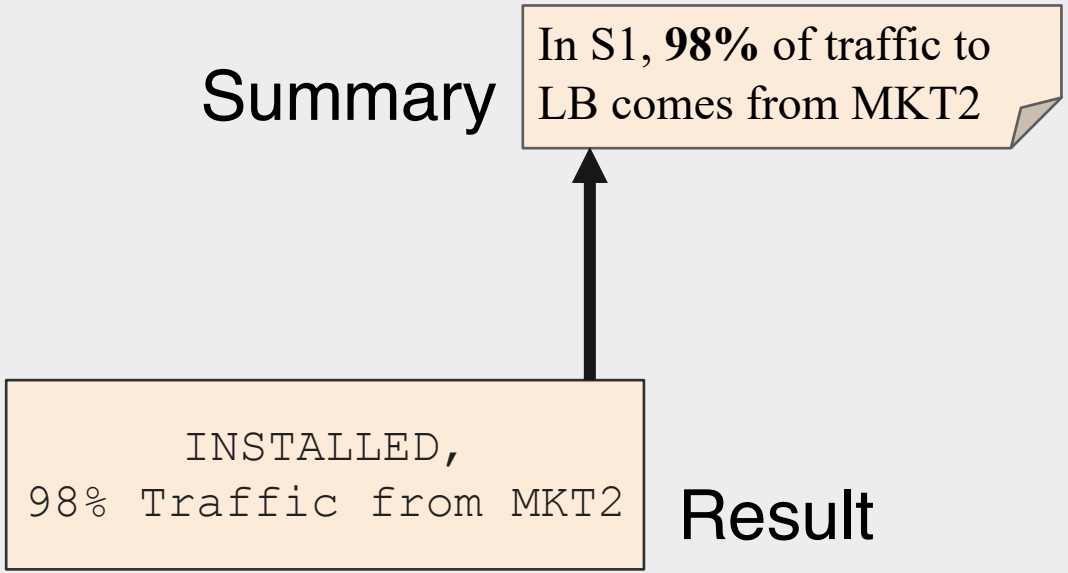


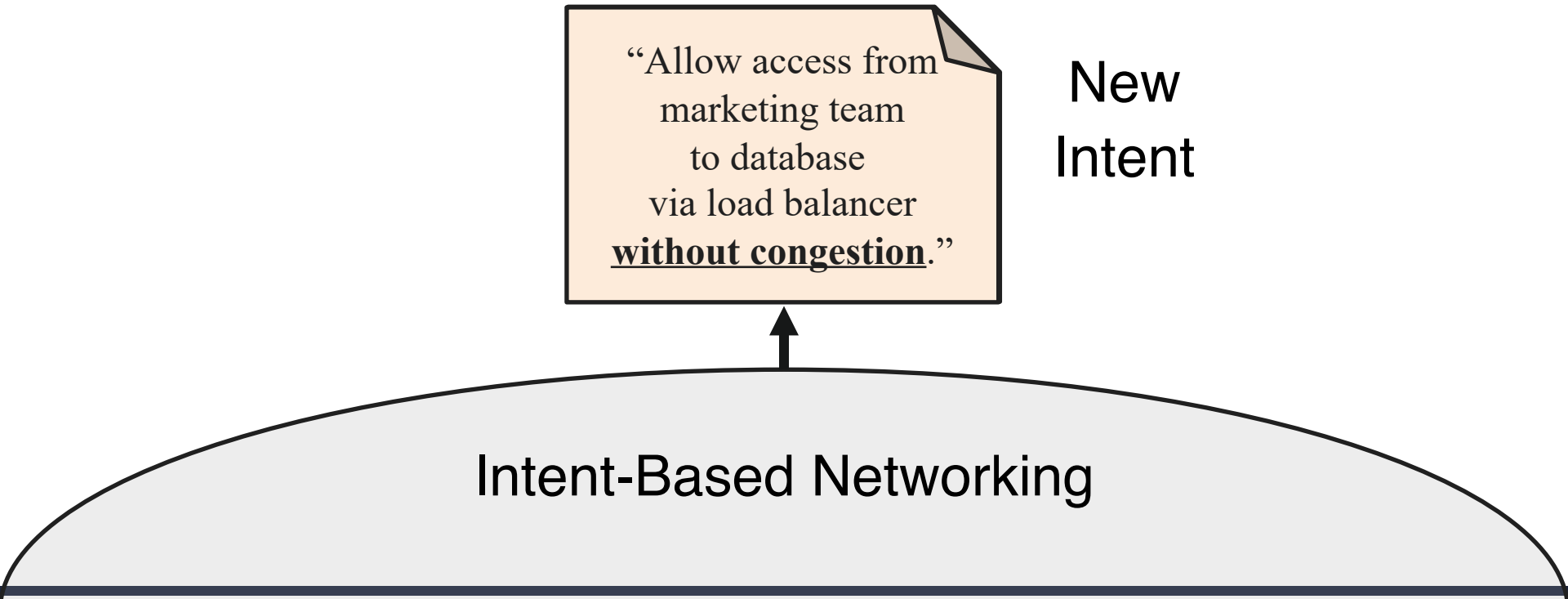
Network Devices

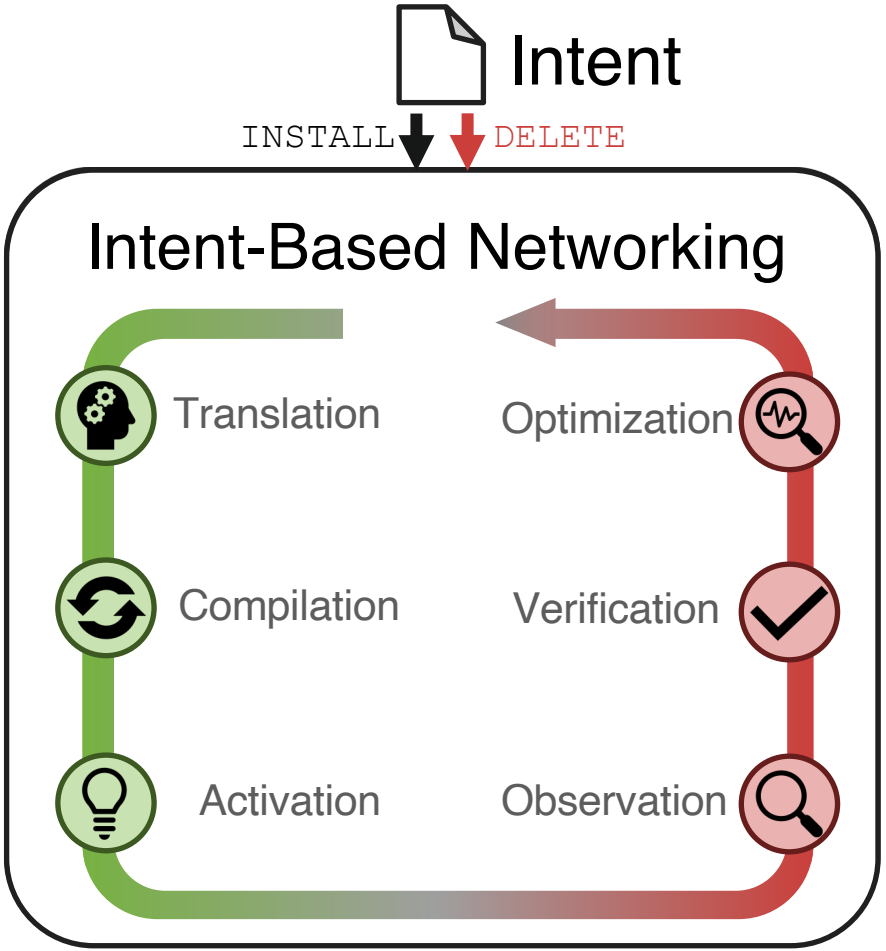
Verification



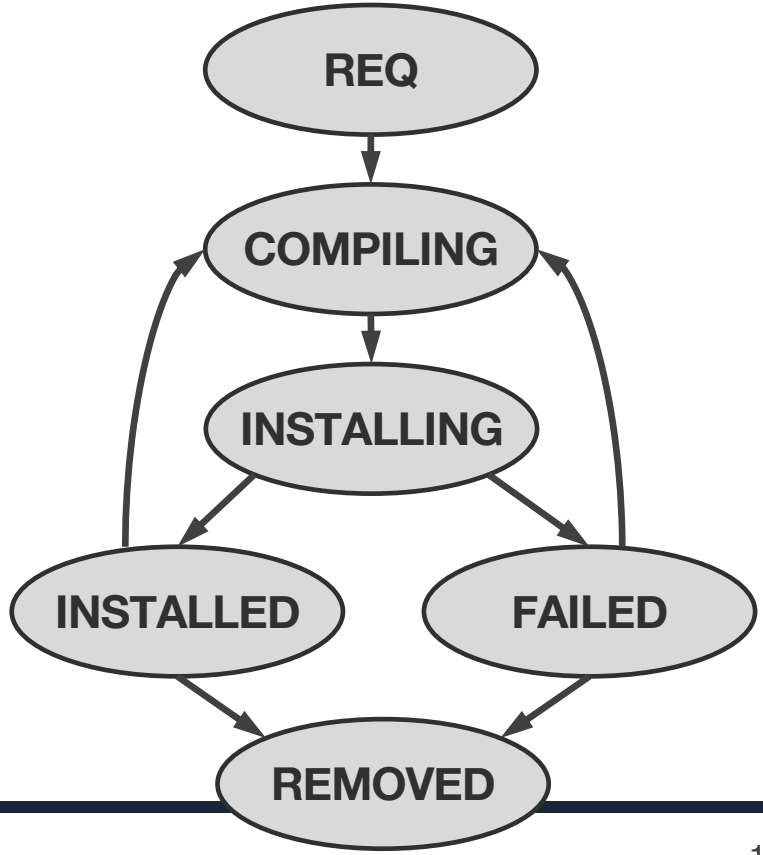
Optimization



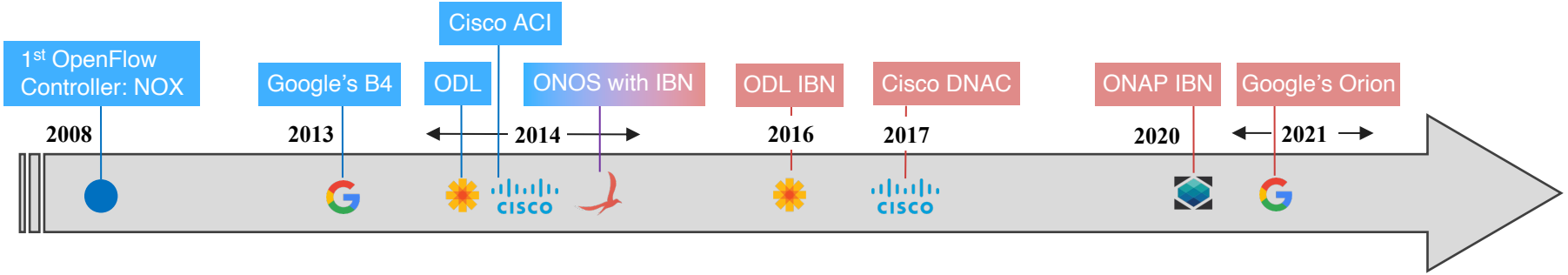

"Allow access from
marketing team
to database
via load balancer
without congestion."
New
Intent
Intent-Based Networking

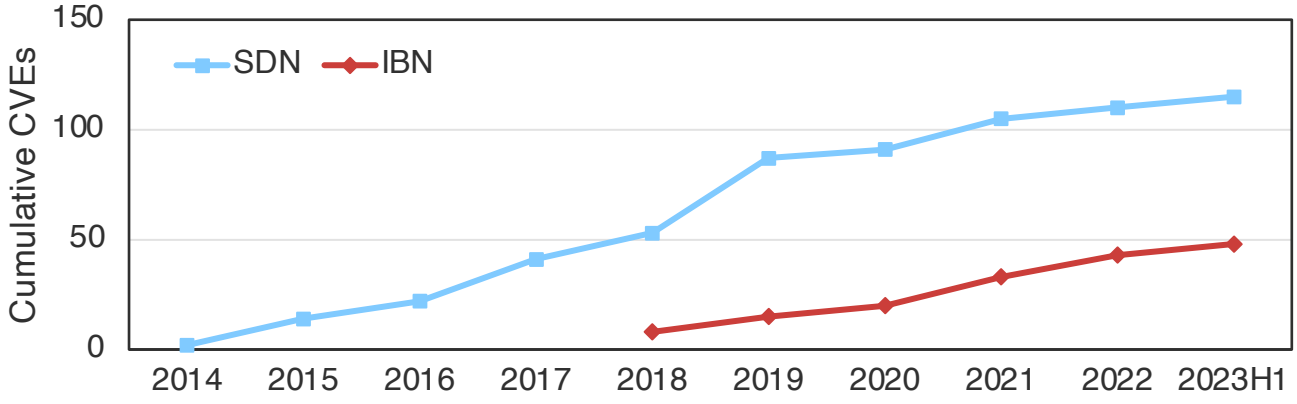


Intent State Machine

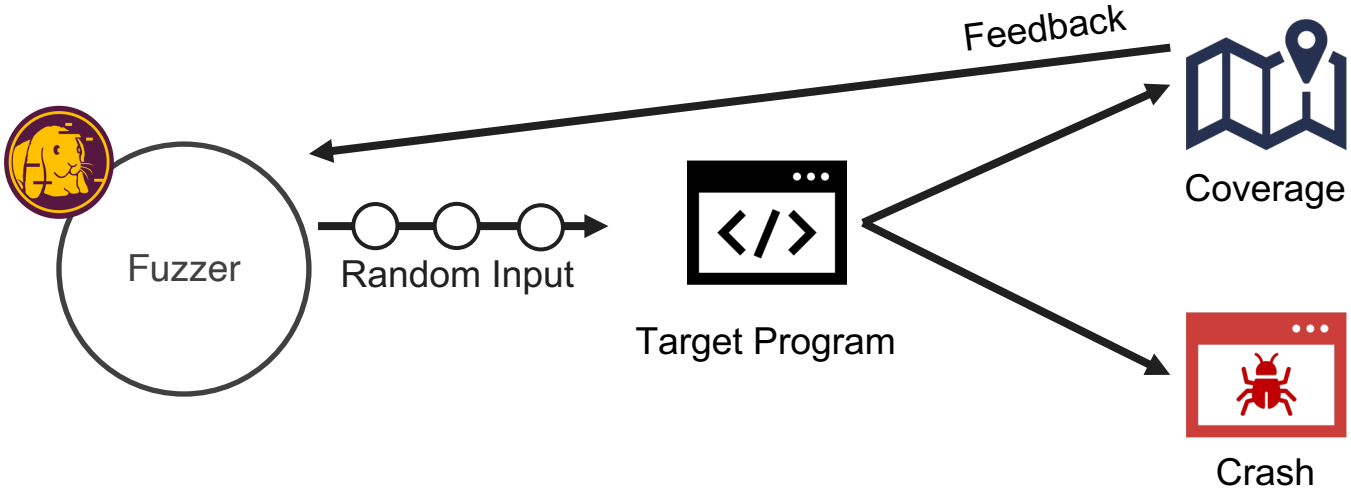


Vulnerabilities in SDN and IBN

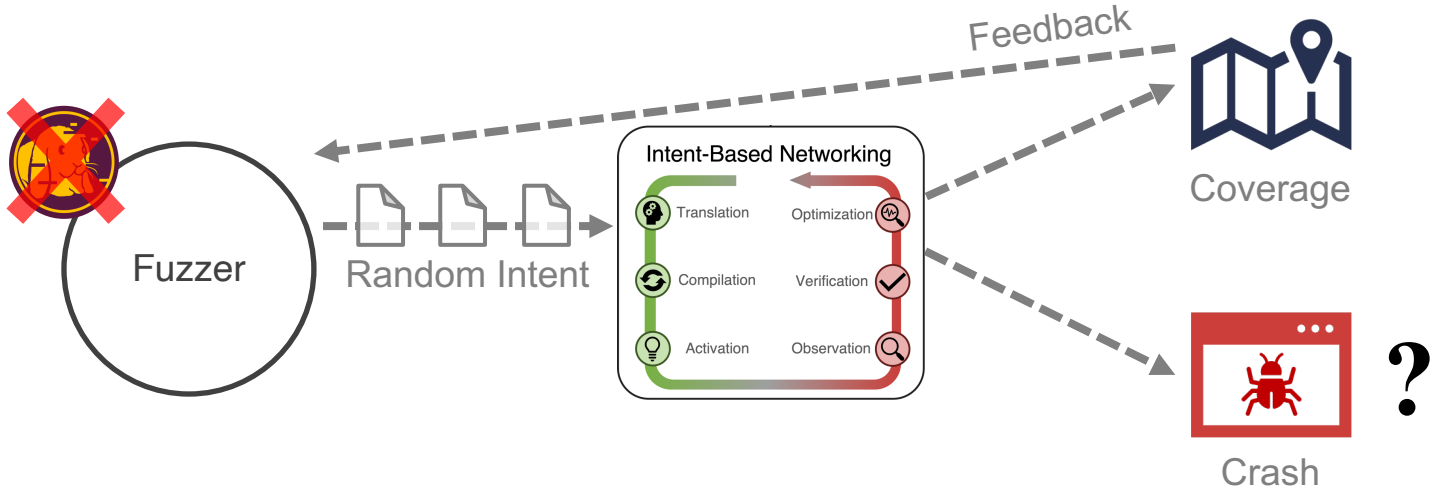




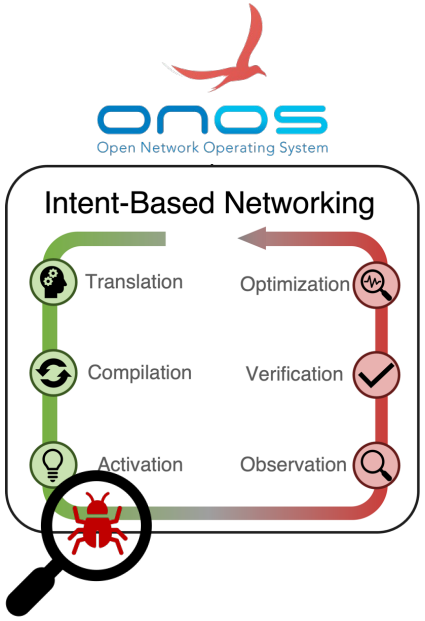
Fuzzing Programs

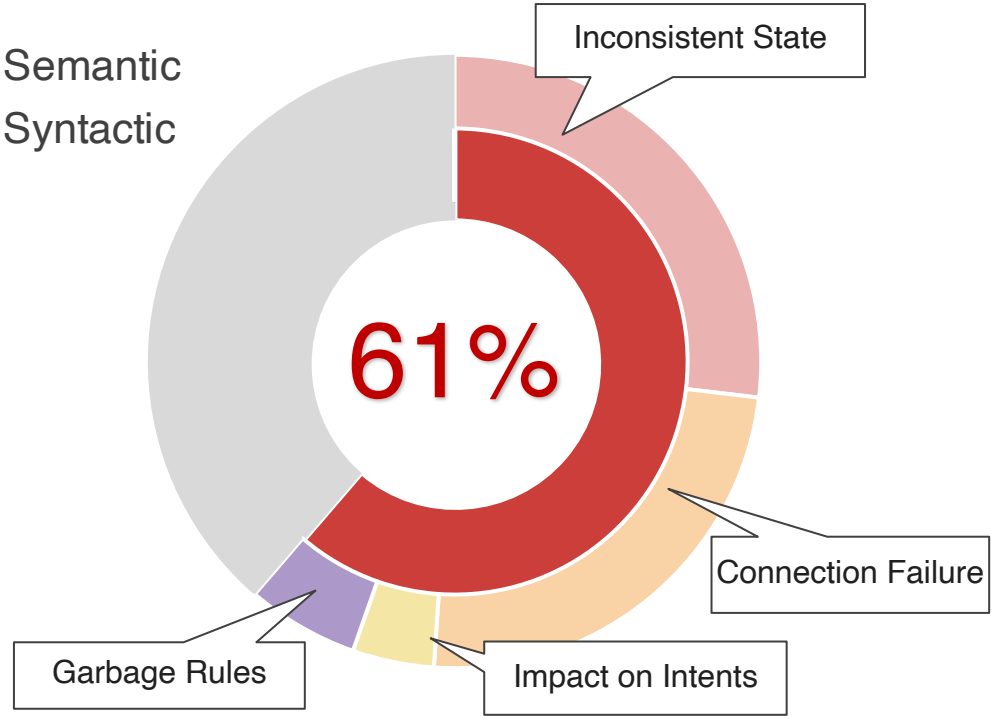


Fuzzing IBN [1/3]

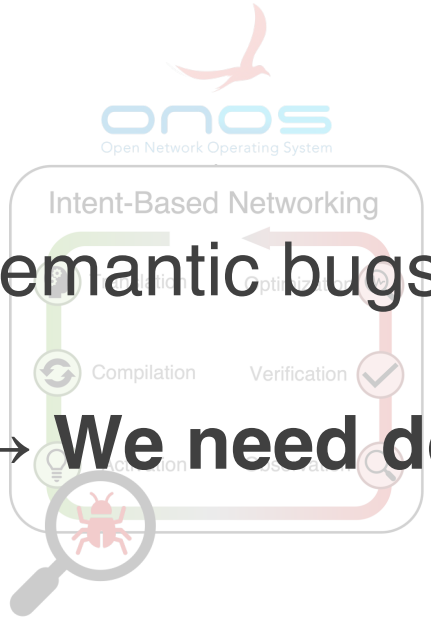


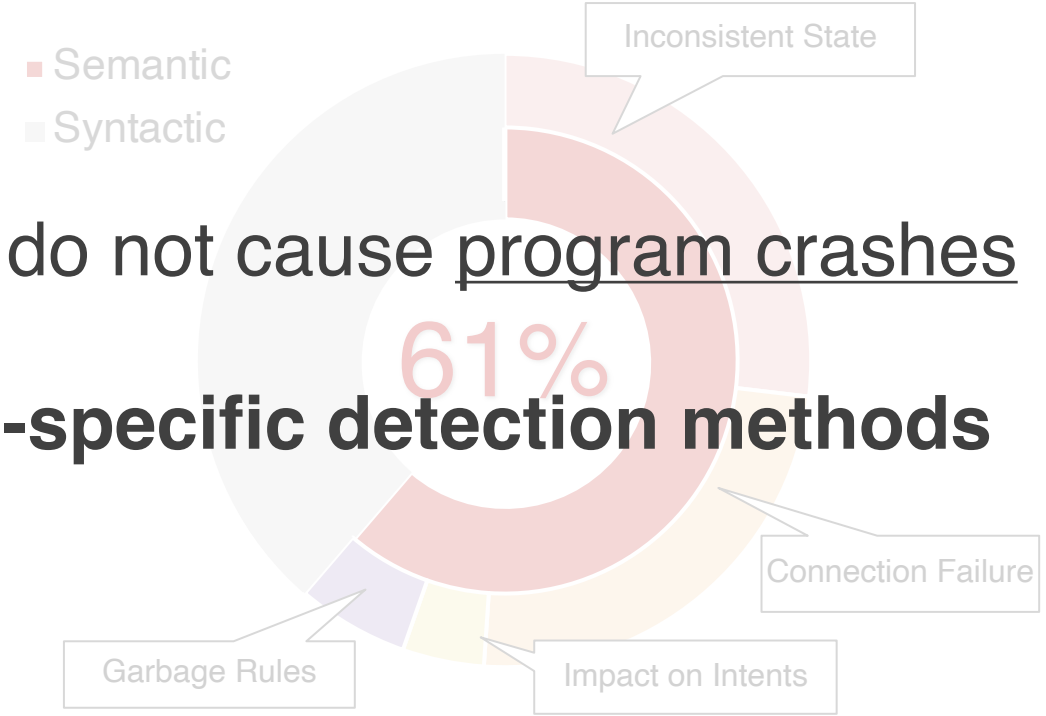
I. Bug Study in ONOS IBN





I. Bug Study in ONOS IBN

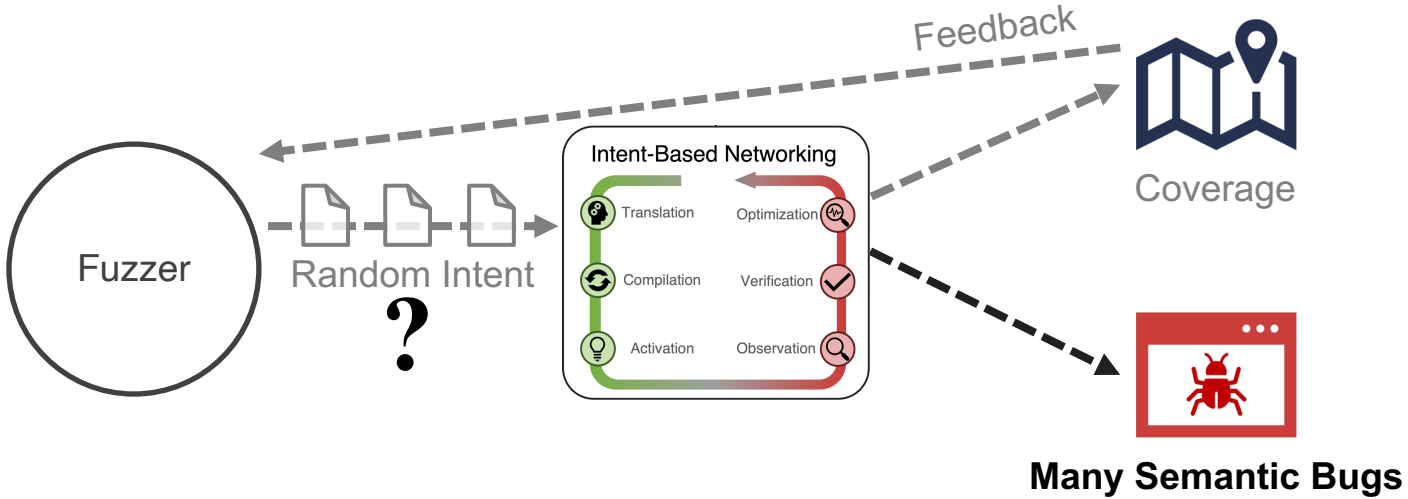




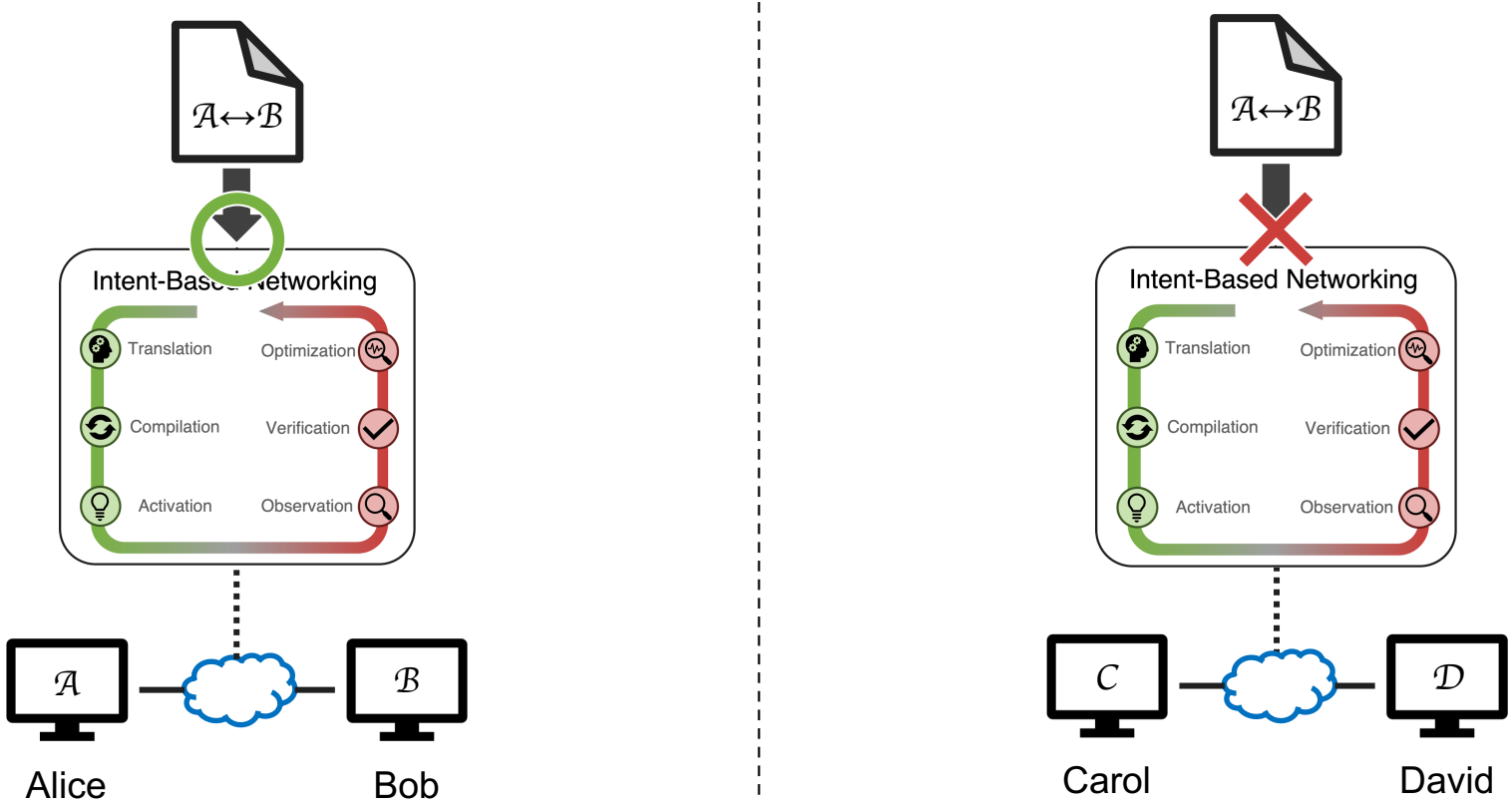
Semantic bugs often do not cause program crashes

→ **We need domain-specific detection methods**

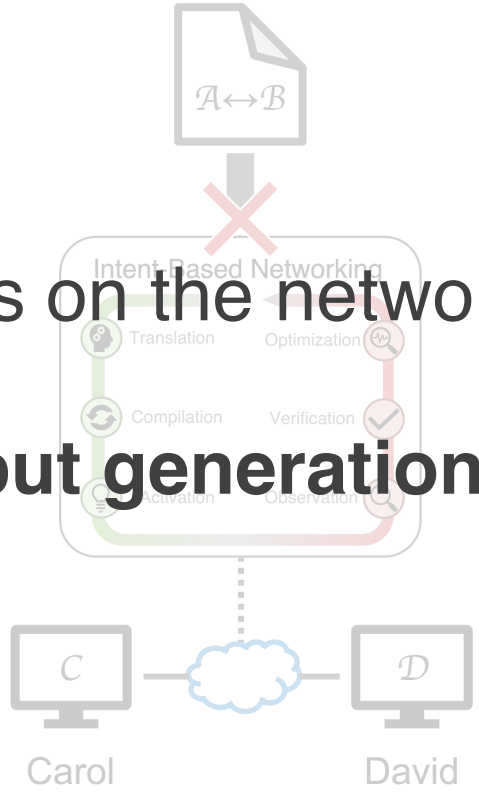
Fuzzing IBN [2/3]



II. Limitation in Input Generation



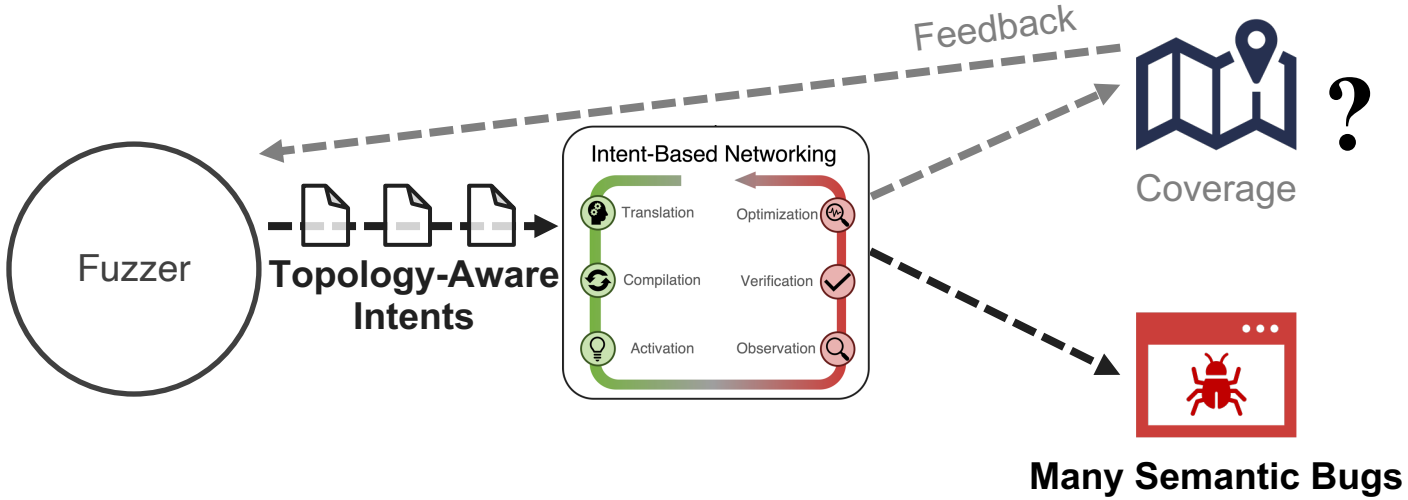
II. Limitation in Input Generation



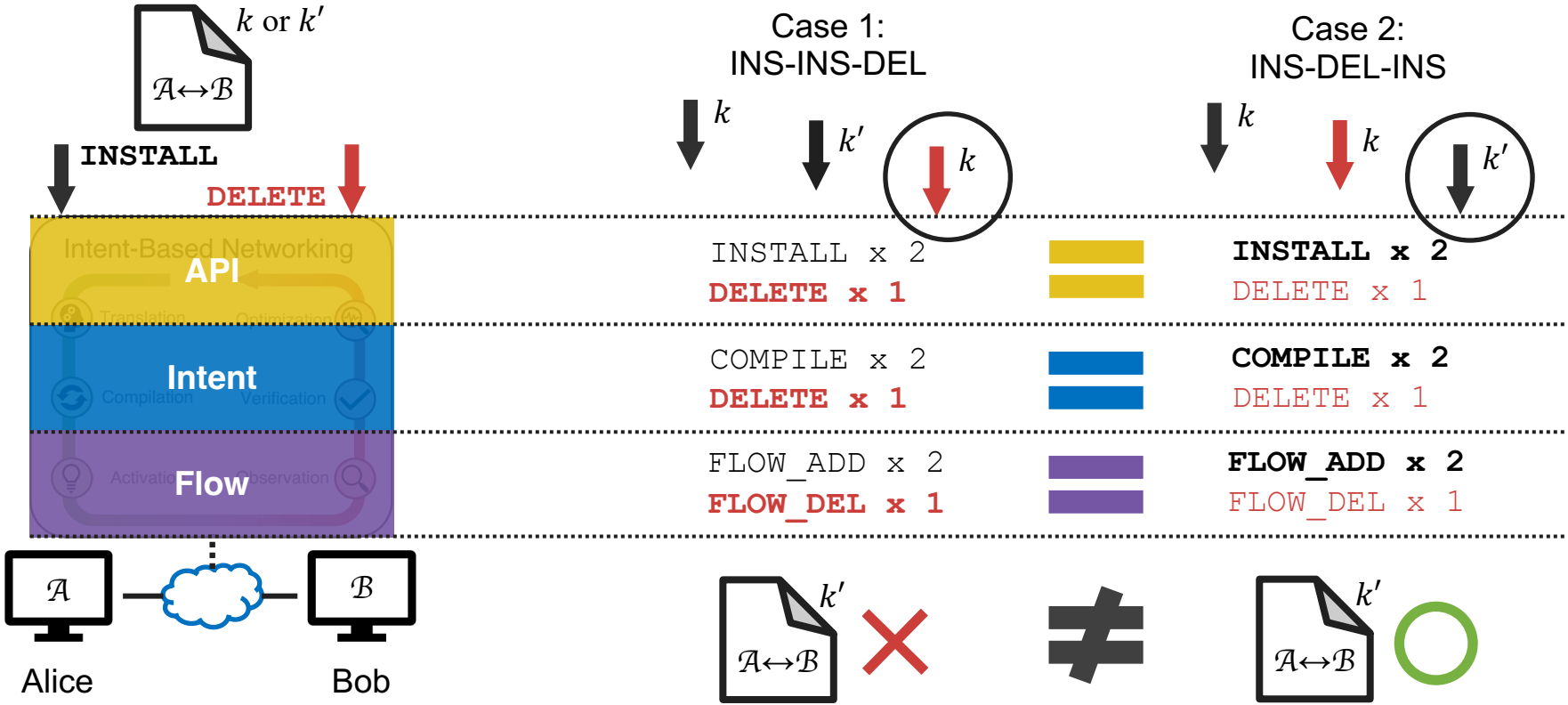
The success of an intent depends on the network

→ **We need topology-aware input generation**

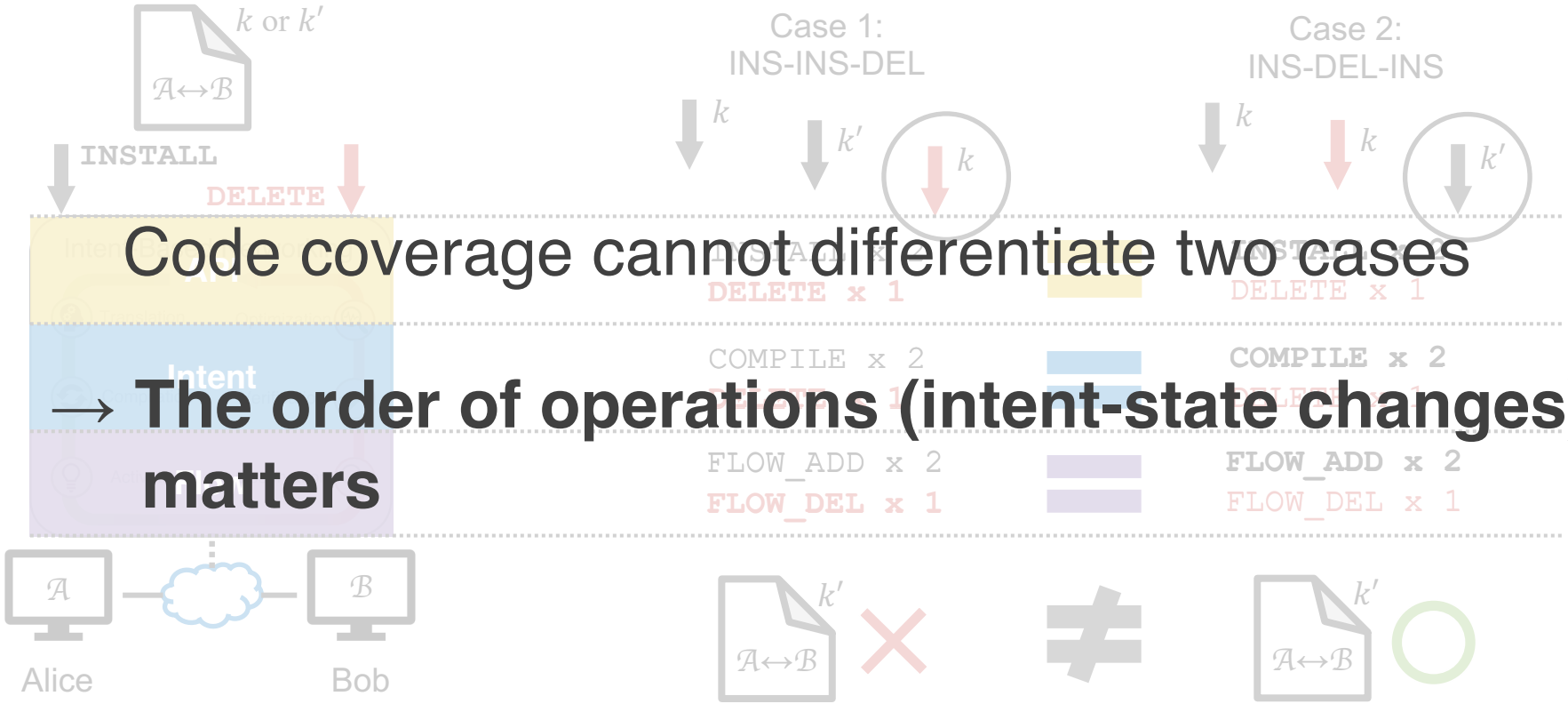
Fuzzing IBN [3/3]



III. Limitation in Code-Coverage Guidance



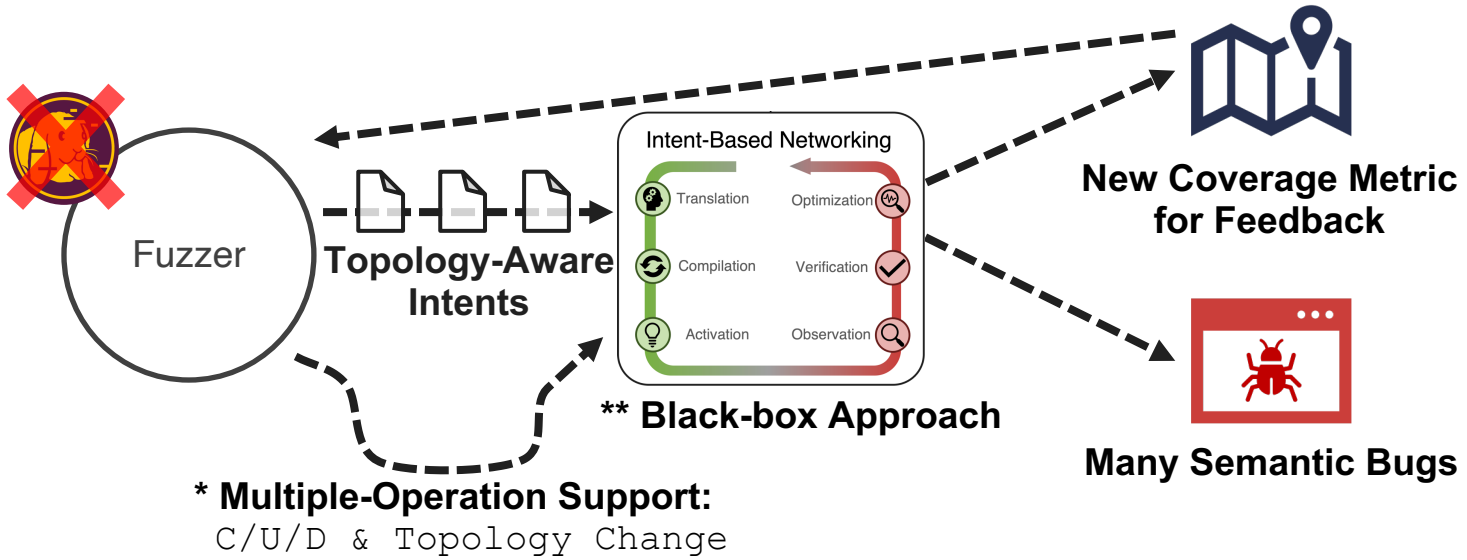
III. Limitation in Code-Coverage Guidance



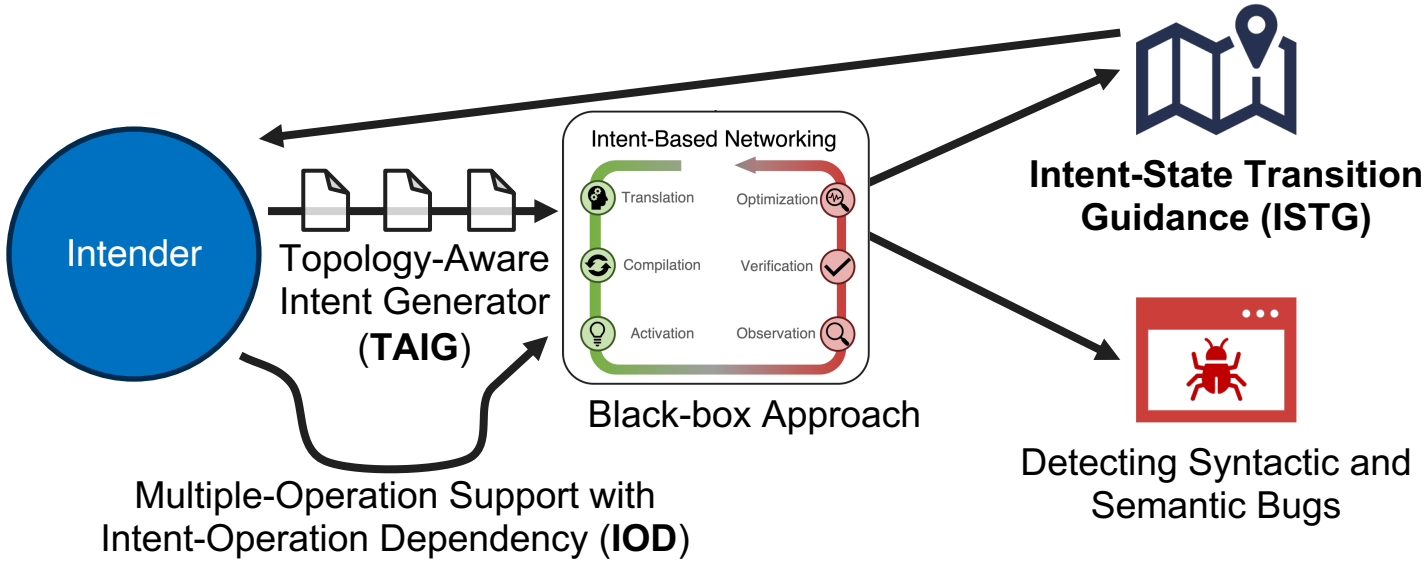
Code coverage cannot differentiate two cases

→ **The order of operations (intent-state changes) matters**

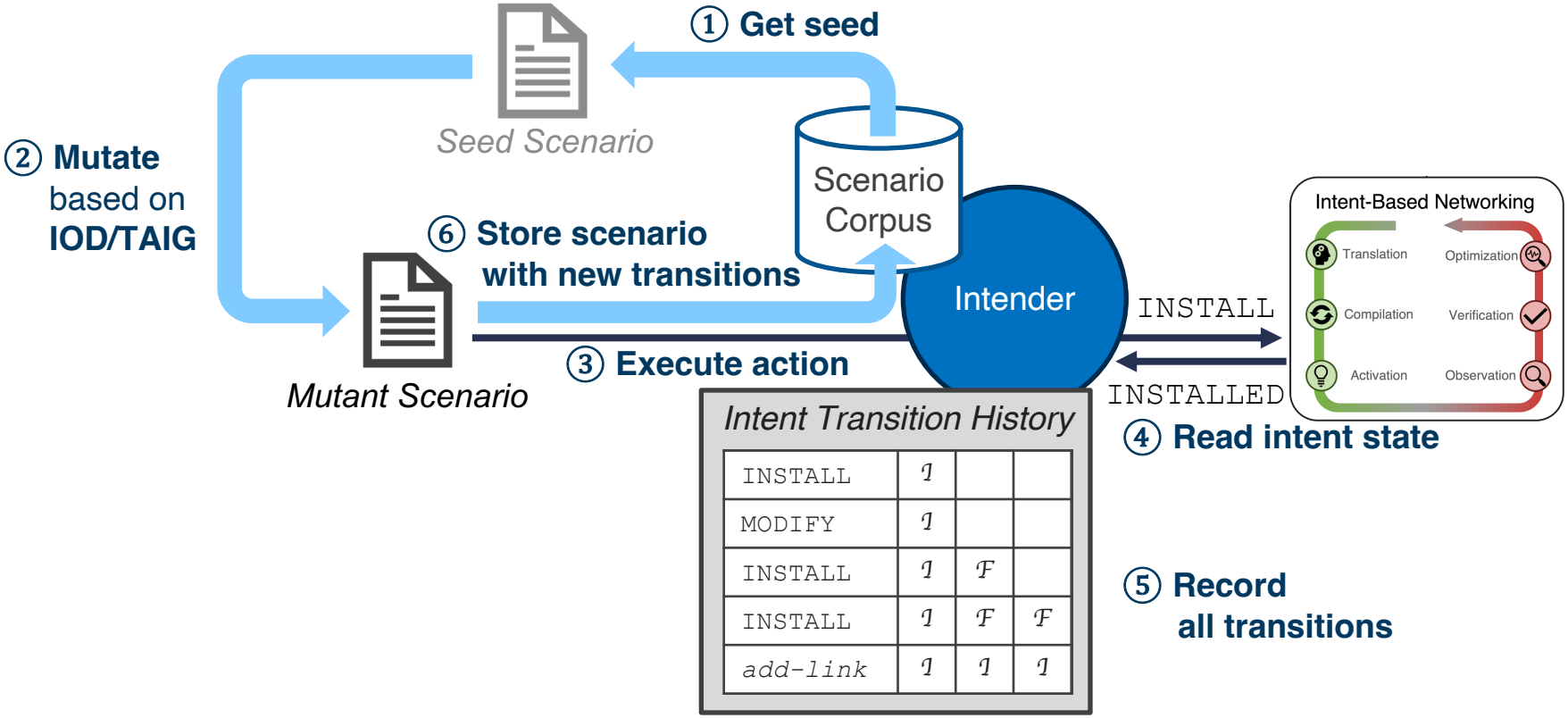
Limitations in Fuzzing IBN



Intender: Fuzzing IBN



Intent-State Transition Guidance (ISTG)



Evaluation (1/2)

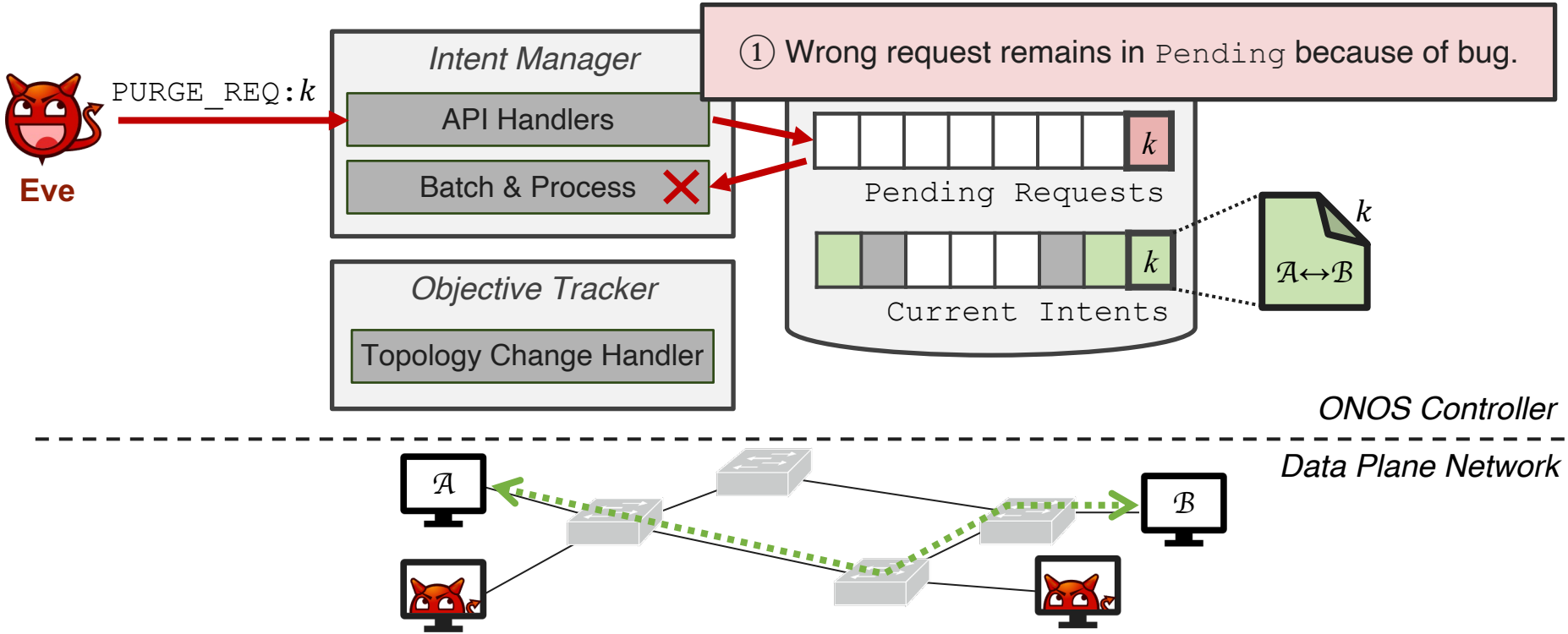
- Environment Setup
  - Google Cloud VM: 4 vCPU, 16GB MEM, 60GB SSD
  - ONOS v2.5.1
- Found **12 new bugs (11 security-critical CVEs)**
  - 9 semantic bugs
  - Security impacts: network-wide **denial of service** & **tampering**
- Compare 4 existing fuzzers (AFL, Jazzer, Zest, PAZZ)
  - Up to **2.2×** better in branch coverage
  - Up to **82.6×** more number of unique errors

Evaluation (2/2)

- Improve fuzzing performance compared to baselines
  - *Topology-Aware Input Generation* (TAIG) can produce **78.7×** more valid intents
  - *Intent-Operation Dependency* (IOD) can reduce **73.02%** of redundant operations
  - *Intent-State Transition Guidance* (ISTG) leads to **1.8×** more intent-state transitions than code coverage guidance (CCG)

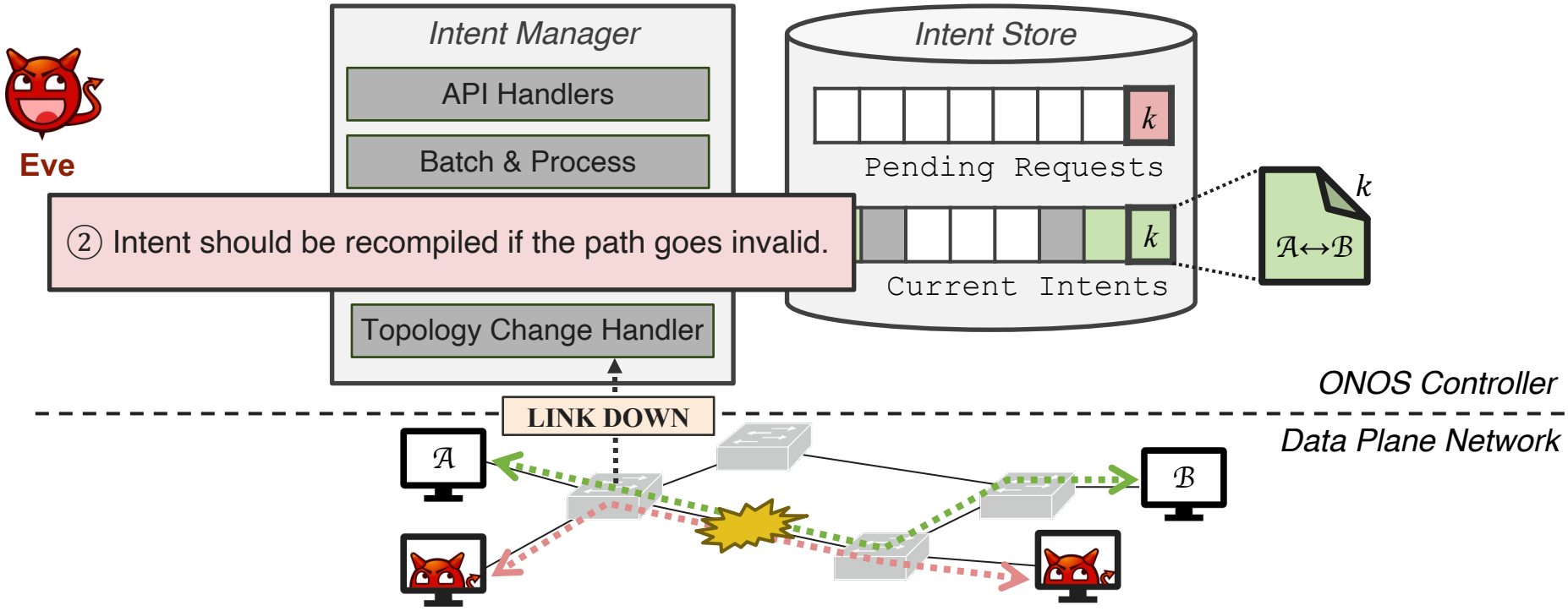
Case Study: CVE-2022-24035

(1) **Eve** requests `PURGE` on `INSTALLED` intent



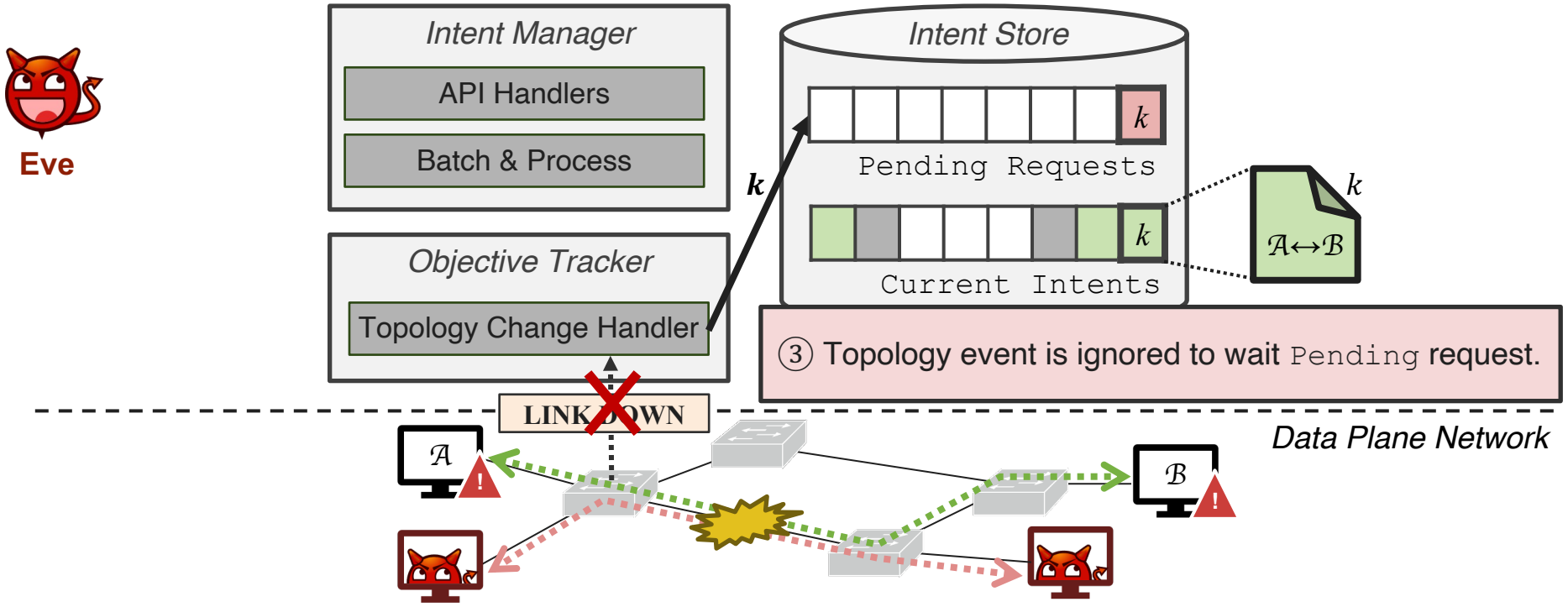
Case Study: CVE-2022-24035

(2) **Eve** exploits link-flooding attack



Case Study: CVE-2022-24035

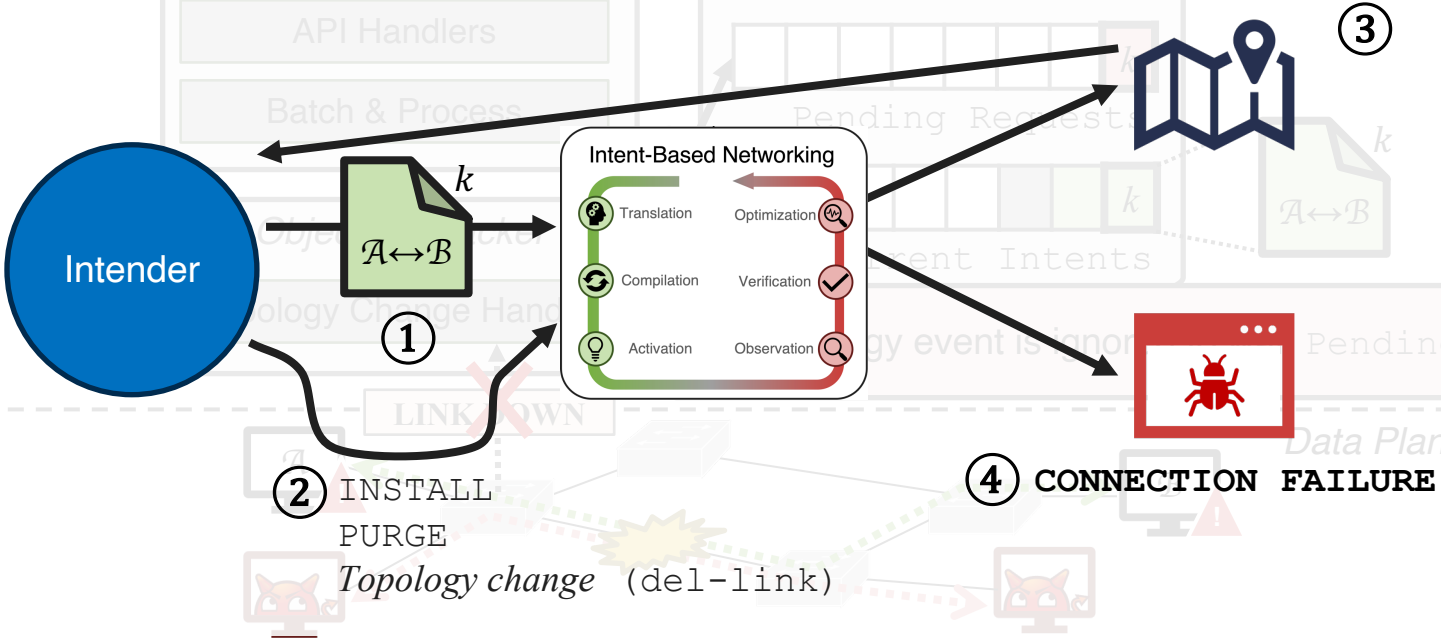
(3) Intent **DOES NOT** respond to topology event any more → **DoS**



Case Study: CVE-2022-24035

- *To discover this bug efficiently…*

Intent Transition History			
INSTALL	$\mathcal{I}$		
PURGE	$\mathcal{I}$		
del-link	$\mathcal{I}$		



Conclusions

- Analyzed **186 bugs** in ONOS IBN
- Designed **new fuzzing techniques for IBN**
  - *Topology-Aware Intent Generation* (**TAIG**)
  - *Intent-Operation Dependency* (**IOD**)
  - *Intent-State Transition Guidance* (**ISTG**)
- Developed **Intender architecture**
- Found **12 new bugs (11 CVEs)** in ONOS IBN

Thank you!

EMAIL

kim1685@purdue.edu

WEBSITE

https://kjw6855.github.io

CODE

https://bit.ly/44SF9nJ

PURDUE UNIVERSITY

CERIAS

PurSec Lab

GEORGETOWN UNIVERSITY

GEORGETOWN SECURITY LAB