On Multi-Point, In-Network Filtering of Distributed Denial-of-Service Traffic

Mingwei Zhang, Lumin Shi, Devkishen Sisodia, Jun Li (UOregon),
Peter Reiher (UCLA)
IM 2019
April 10th, 2019

UNIVERSITY
OF OREGON

UCLA

Outline

- Background on DDoS attacks and defense
- Modeling the in-network defense algorithms
  - Types of algorithms
  - Cost of defense
  - Performance metrics
- Performance Evaluation of defense algorithms
- Conclusion

Distributed Denial-of-Service (DDoS) Attacks

TECHNOLOGY

Mirai offshoot offers 'greater firepow
for DDoS attacks, researchers warn

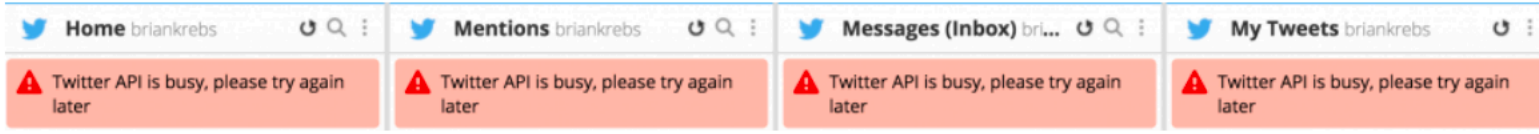
ABTV

Arbor Networks: 1.7Tbit/s DDoS Attack Sets Record

ts Twitter, Spotify, Reddit

d Dyn, a company that provides core Interne
Reddit and a host of other sites, causing outage

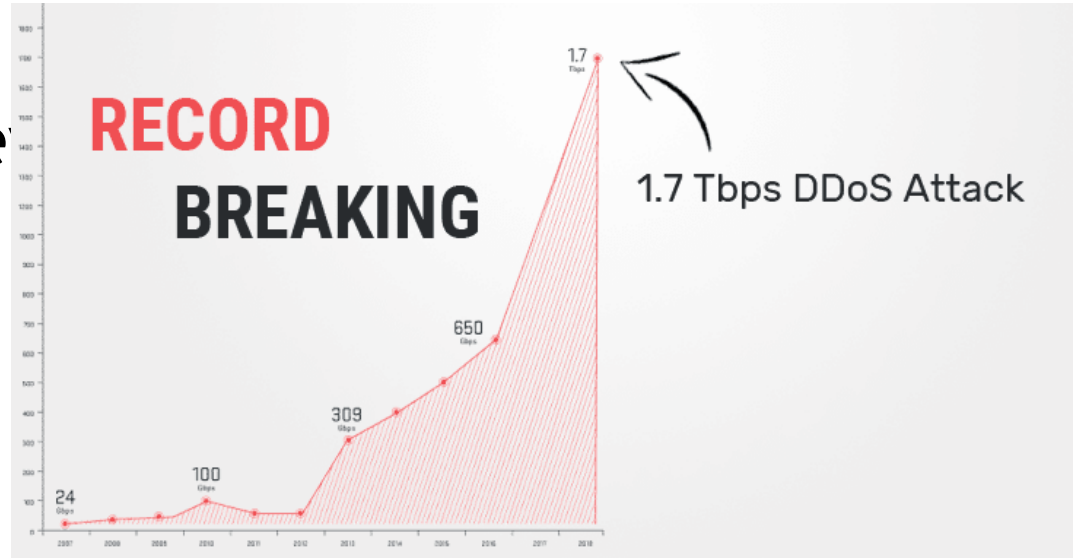
and slowness for many of Dyn's customers.



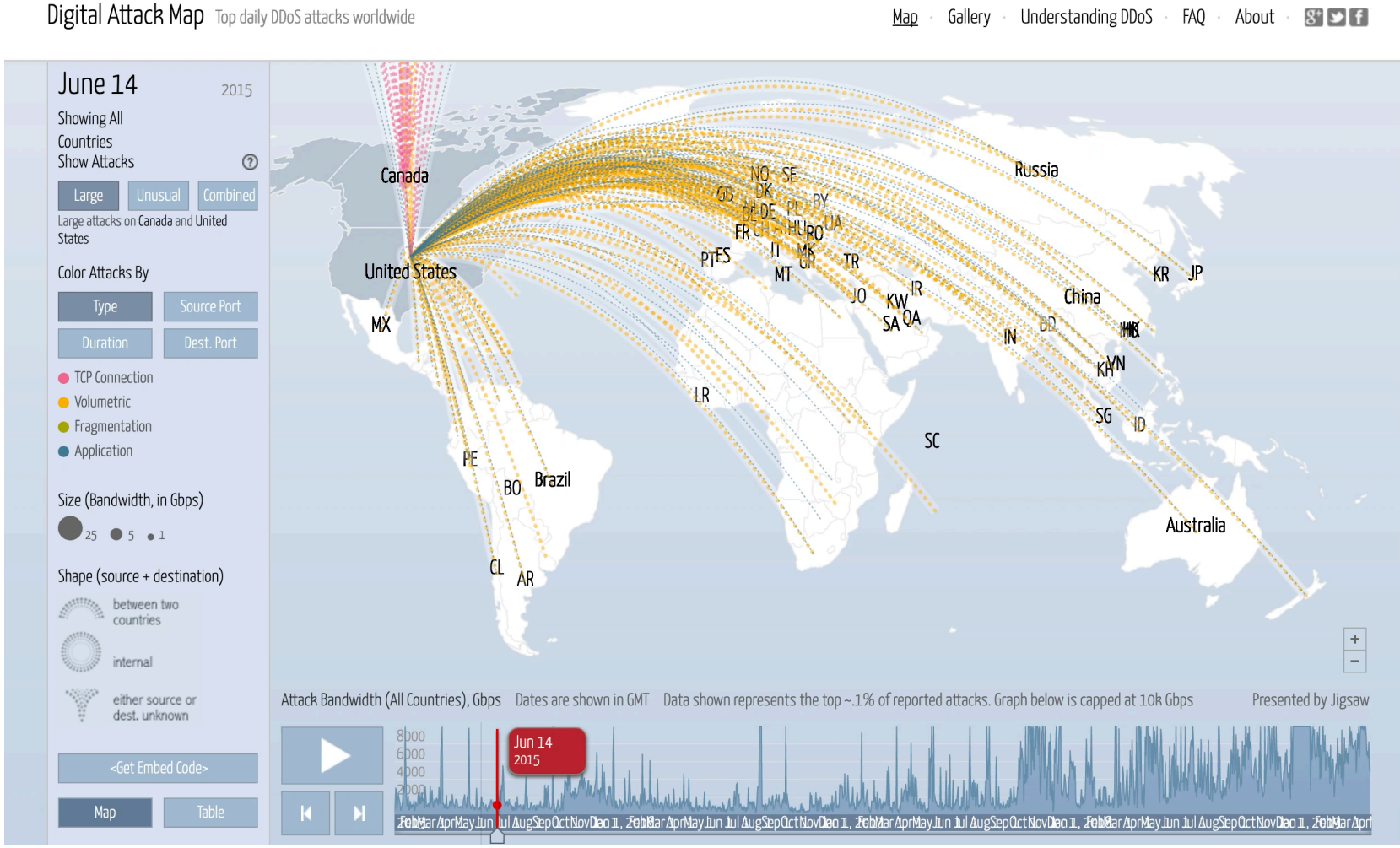
Twitter is experiencing problems, as seen through the social media platform Hootsuite.

Distributed Denial-of-Service (DDoS) Attacks

- Utilizing large number of compromised to hosts to send junk traffic
  - Traditional Botnet
  - IoT Botnets
- Use reflectors to amplify volume of traffic
  - DNS
  - NTP
- Volume reaches Terabits-per-second le
  - 2016, Dyn DNS (Mirai Botnet): 1.2 Tbps
  - 2018, GitHub: 1.3 Tbps
  - 2018, Arbor: 1.7 Tbps
- **It's getting worse**

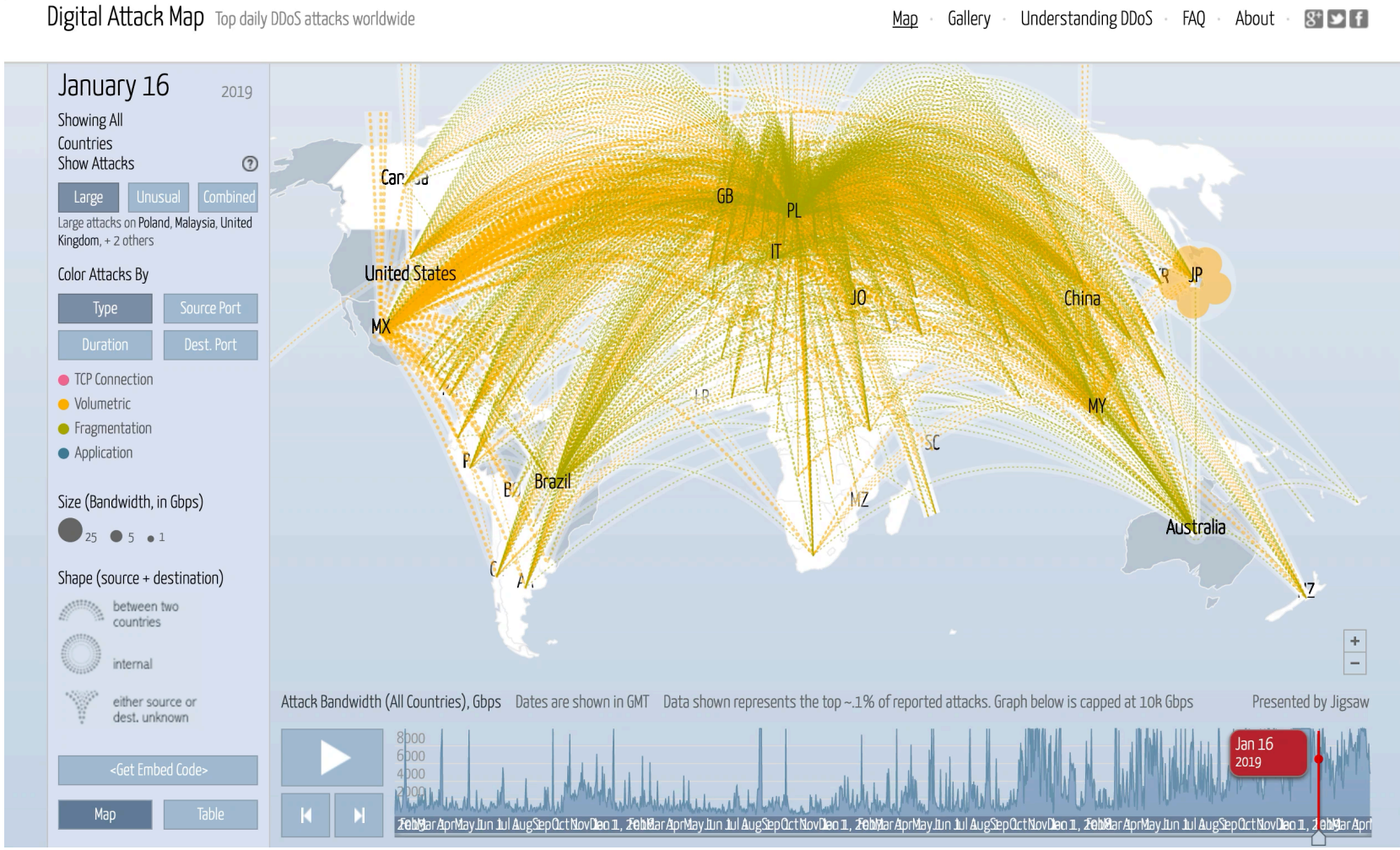


Attacks in 2015

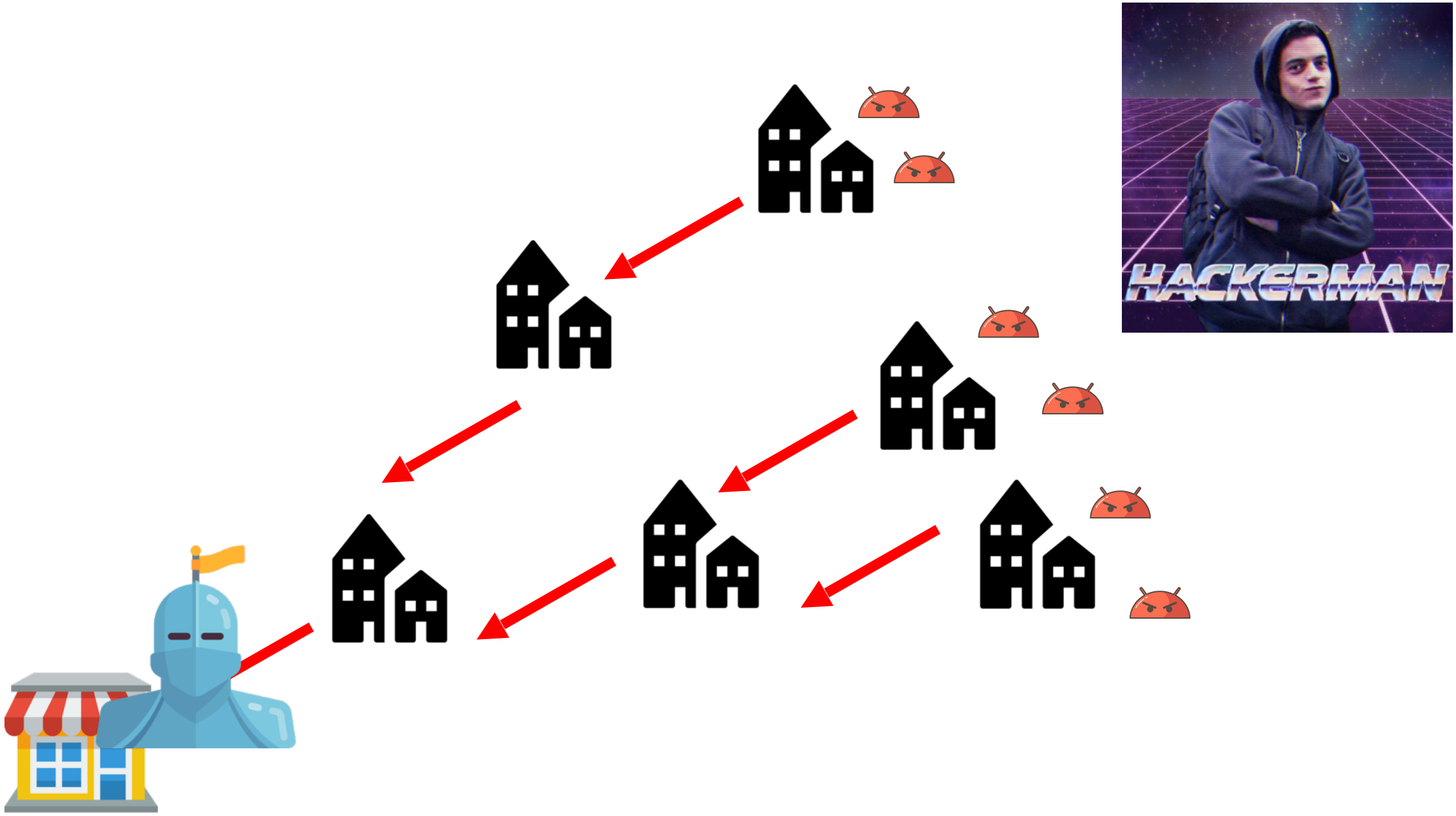


http://www.digitalattackmap.com/

Attacks in 2019



http://www.digitalattackmap.com/


HACKERMAN

DDoS Defense in Tbps DDoS Era

- Arms' race between DDoS Protection Services and Attackers
  - Larger attacks -> bigger pipes
  - Bigger pipes -> larger attacks
- Problem 1: capacity hard to catchup
  - CloudFlare has 30 Tbps of capacity[1]
  - But that's shared across all of it's customers
- Problem 2: congestion before reaching defense points
  - Overwhelming traffic aggregates before reaching the point of filtering
- Solution: defend on **multiple points** and **earlier**

[1] (Date of access: April 10, 2019) https://www.cloudflare.com/ddos/

In-network DDoS Defense

- In-network defense:
  - Happens inside the Internet
  - Multiple ASes collaborating for defense
  - Filters traffic before reaching the victim
- Benefits
  - Scalable: no single-entity should handle the whole defense burden
  - Effective: defense happen early on, less traffic to cause congestion
- Requirement: collaboration
  - Remotely Triggered Black Hole (RTBH): RFC5635, RFC7999
  - BGP FlowSpec
- Why don’t people use them already?
  1. Many types of in-network defense
  2. No guidelines for what to use which types defense
  3. No cost/performance comparison among types of defenses

In this study

- Summarize the in-network defense algorithms from the current literature
  - Propose improved algorithm
- Performance evaluation quantitatively across defense algorithms
  - Cost of the defense
  - Performance of the defense
- Based on evaluation results, provide usable guidelines on when to use what types of collaborative defense

Modeling and Quantitative Comparison of the In-network DDoS Defense Algorithms

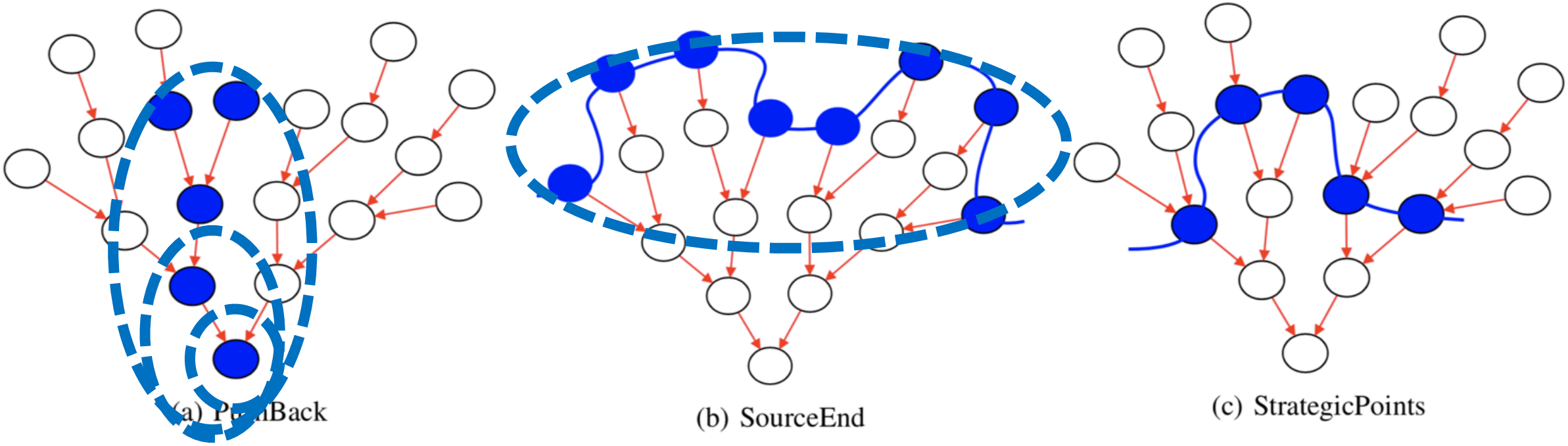
In-network Defense

- Assuming infrastructure in place, where should we place the filters?
- Two basic types of in-network defense algorithms in the literature
  - PushBack: push defense from the victim to the source if pressure mounts
  - SourceEnd: place filters at the sources
- Ot
  mu

Work	Single-AS	Multi-AS		
		PushBack	SourceEnd	Other
RADAR[11], Sahay et al.[12], SPIFFY[13], Bohatei[14]	✓			
ScoreForCore[15], Yau et al.[16], Mahajan et al.[9]		✓		
FireCol[17], DefCOM[8], AITF[18], COSSACK[19], StopIt[20], D-WARD[21], Argyraki et al.[22], Huici et al.[23]			✓	
MiddlePolice[10], Keromytis et al.[24], Andersen et al.[25]				✓

TABLE I: DDoS defense solution categorizations

In-network DDoS Defense Algorithms



(a) PushBack

(b) SourceEnd

(c) StrategicPoints

What algorithm should we use?

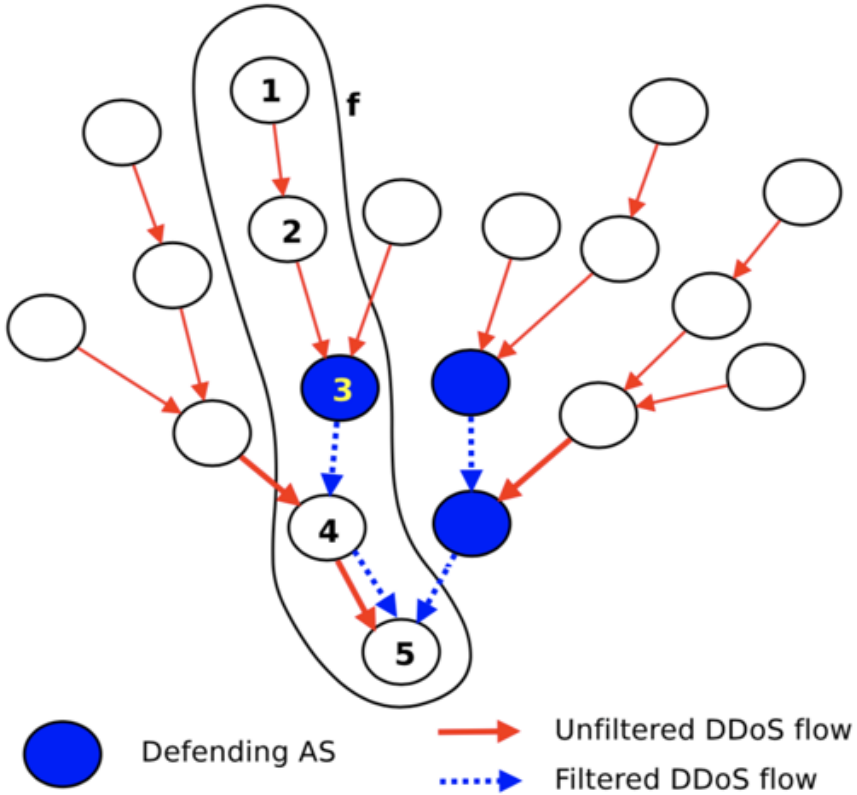
- Plenty of weapons in hand, what are the most effective?
  - Cost
  - Performance
- In-network defense doesn’t come without cost
  - ASes involved in defenses
  - Filtering rules needed for defenses
- Performance metrics
  - Traffic reached to the victim
  - Traffic running on the Internet before reaching the victim

Cost of In-network DDoS Defense

- Cost of collaborative defense is not negligible
- Dmax: **Number of ASes** participating in defense
- Rmax: **Number of filtering rules**

DDoS Traffic Leakage and Pollution

- Metrics for evaluating a DDoS defense solution:
  - Leakage: how much traffic leaked through the defense line?
  - Pollution: how much traffic running across the Internet before filtered?
- Why do we care about pollution?
  - Less pollution, less congestion



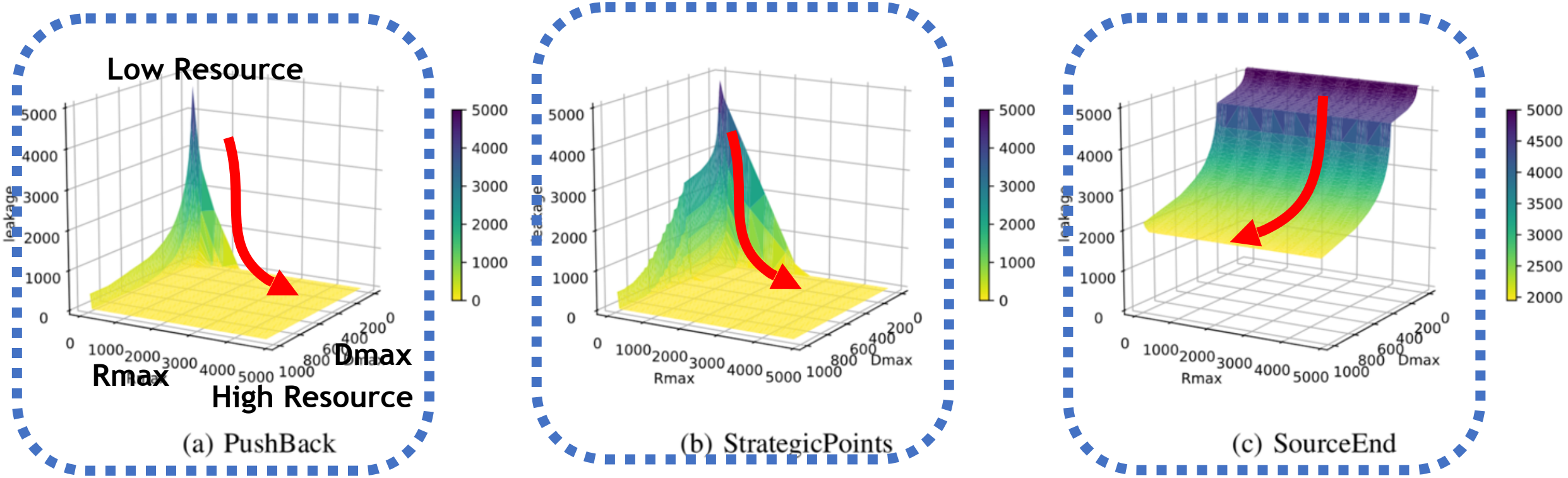
Simulation-based Evaluation

- Build topology route data from all collectors of RouteViews and RIPE RIS
- Simulate DDoS attacks using real-world attack traces
  - Attack collected by CAIDA/UCSD in 2007
  - Attack on RADB service collected by Merit in 2016

Trace name	# of sources	# of source ASes
CAIDA-2007 [29]	∼4,700	∼1,400
Merit-2016 [30]	∼2,300	∼1,300

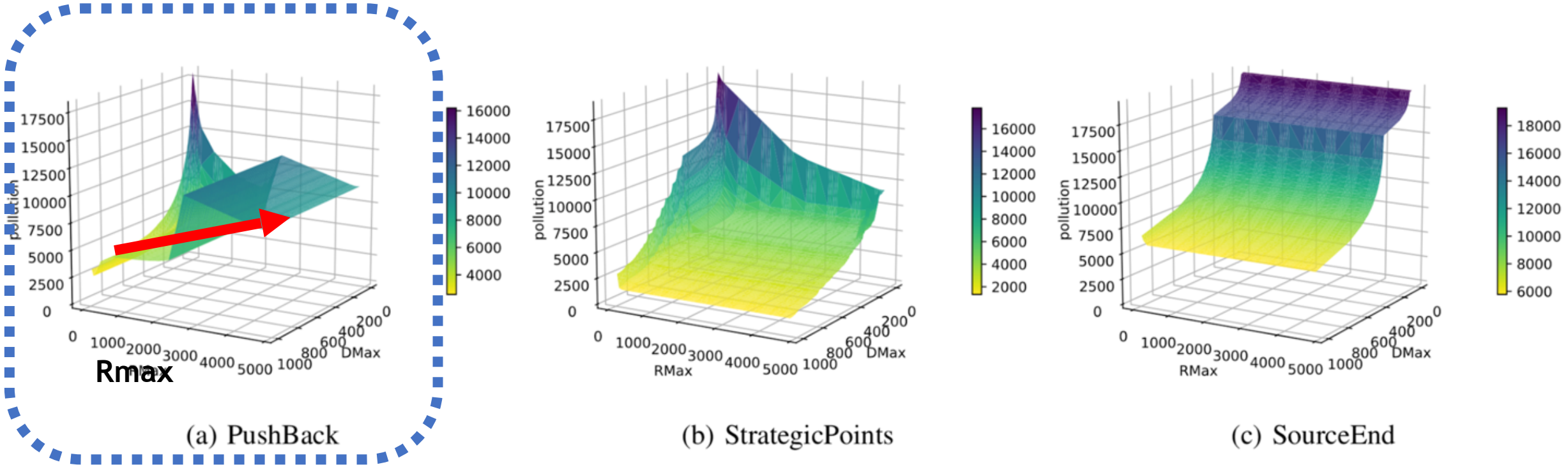
TABLE II: DDoS attack traces used in simulation.

DDoS Traffic Leakage



- Rmax (# of rules); Dmax (# of defenders)
- PushBack and StrategicPoints performances are similar
- SourceEnd requires a lot higher Dmax to perform well

DDoS Traffic Pollution



(a) PushBack (b) StrategicPoints (c) SourceEnd

- PushBack left high pollution when resource is abundant
- StrategicPoints performance remain stable
- SourceEnd’s pollution metric hammered by high leakage

Summary

algorithm	leakage	pollution	dynamic attack resiliency	key resource	when to use
PushBack	low	high	medium	Rmax	very low $Dmax$ or $Rmax$
SourceEnd	high	medium	low	Dmax	$Dmax$ close to total source ASes
StrategicPoints	**low**	**low**	**high**	**Dmax**	**all other cases**

- When to use PushBack?
  - Very low number of collaborative ASes, or low number of filtering rules
- When to use SourceEnd?
  - Very high number of collaborative ASes
- When to use StrategicPoints
  - All other cases

Takeaways

- Collaborative DDoS defense is the most effective way of dealing with DDoS attacks, both in terms of cost and performance
- Choosing

Conclusion

- In-network DDoS defense the effective way of dealing with DDoS attacks
- Choosing appropriate method to place filters are very important
- We summarized three types of defense algorithms
- Quantitatively evaluated the performance of algorithms
- Provided usage guidelines for algorithms under different scenarios

Effective collaboration is better than arms race

UNIVERSITY
OF OREGON

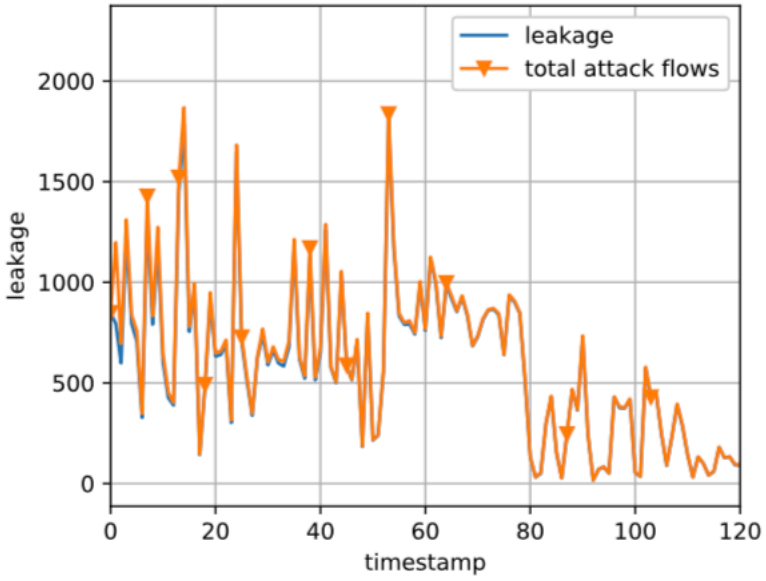
Contact:
Professor Jun Li
Center for Cyber Security and Privacy, University of Oregon
ccsp@uoregon.edu
https://ccsp.uoregon.edu/

UCLA

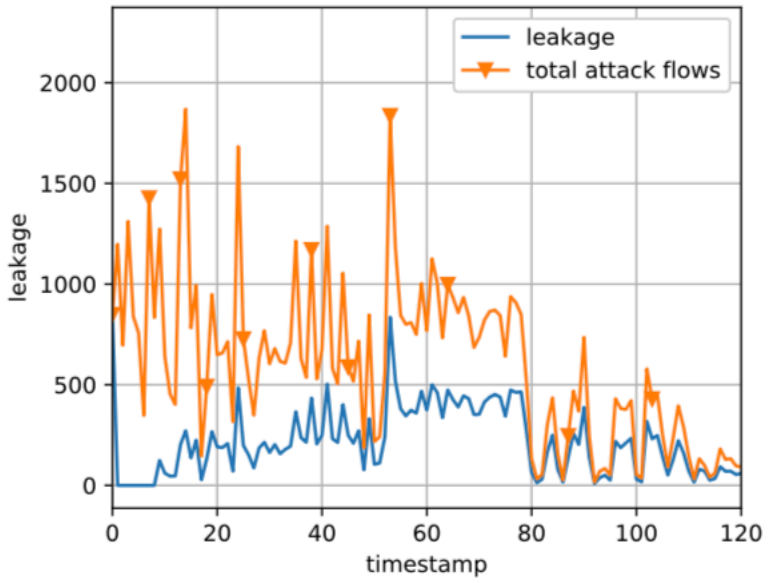
Backup Slides

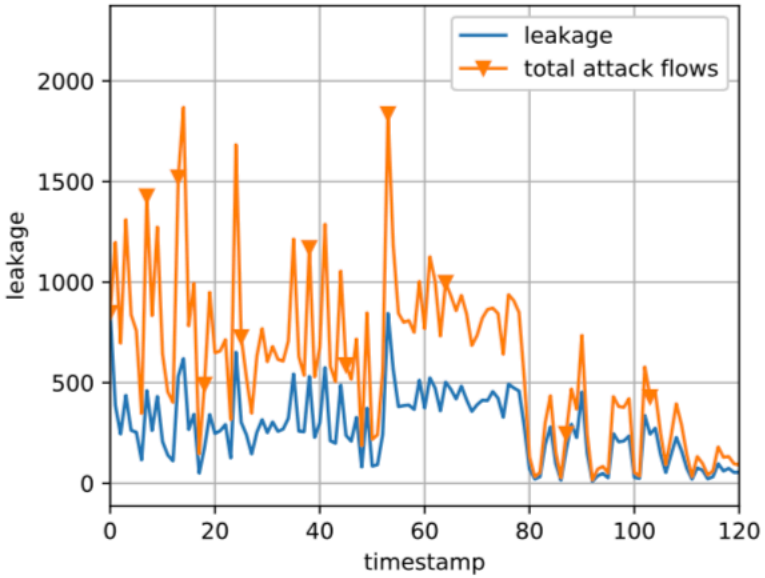
Resiliency Against Dynamic Attacks

- What happens when attack sources shifts?
- Use 15% attack sources for training to find defense locations
- PushBack is very ineffective due to lack of extra space for defense
- StrategicPoints and SourceEnd both perform better

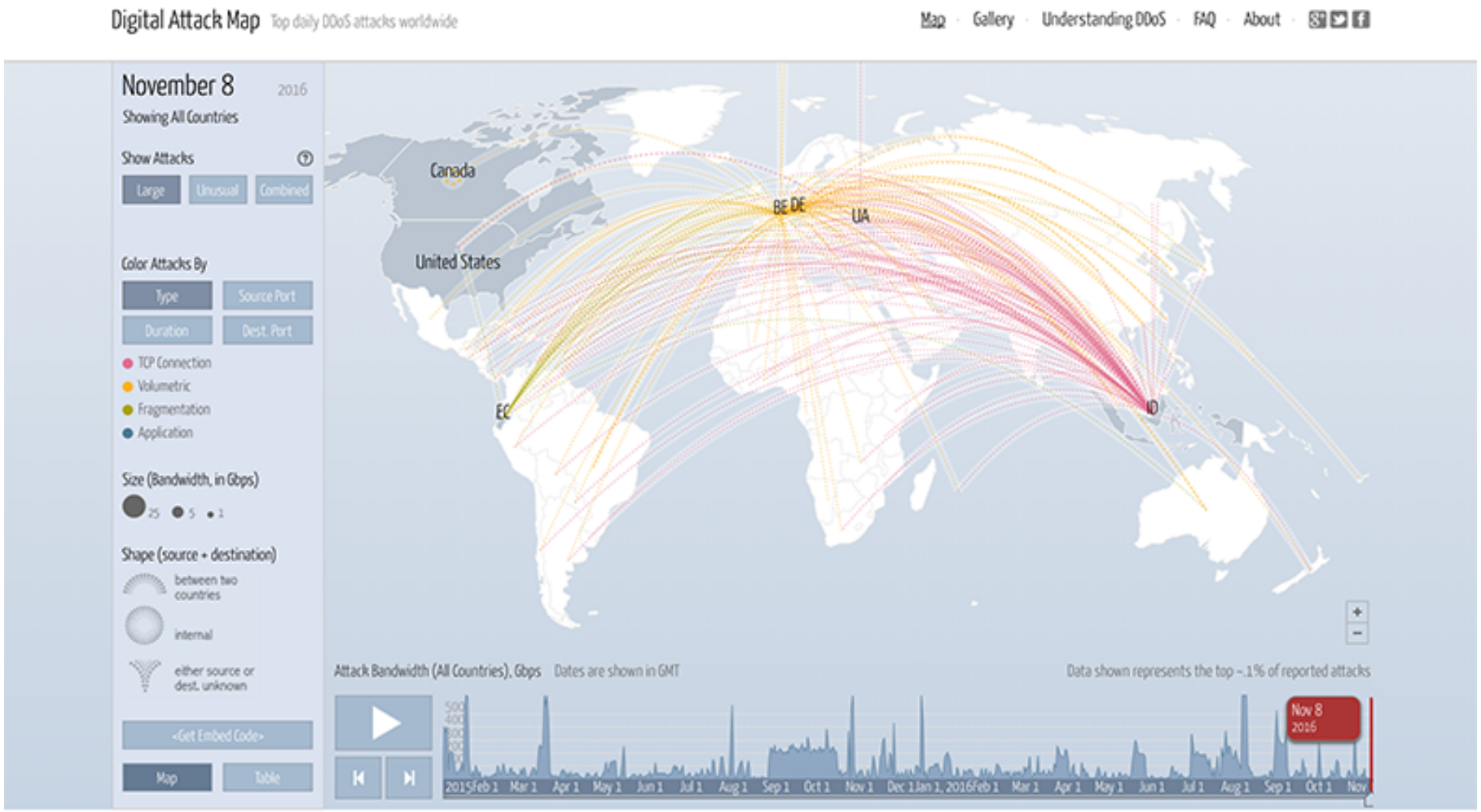


(a) PushBack

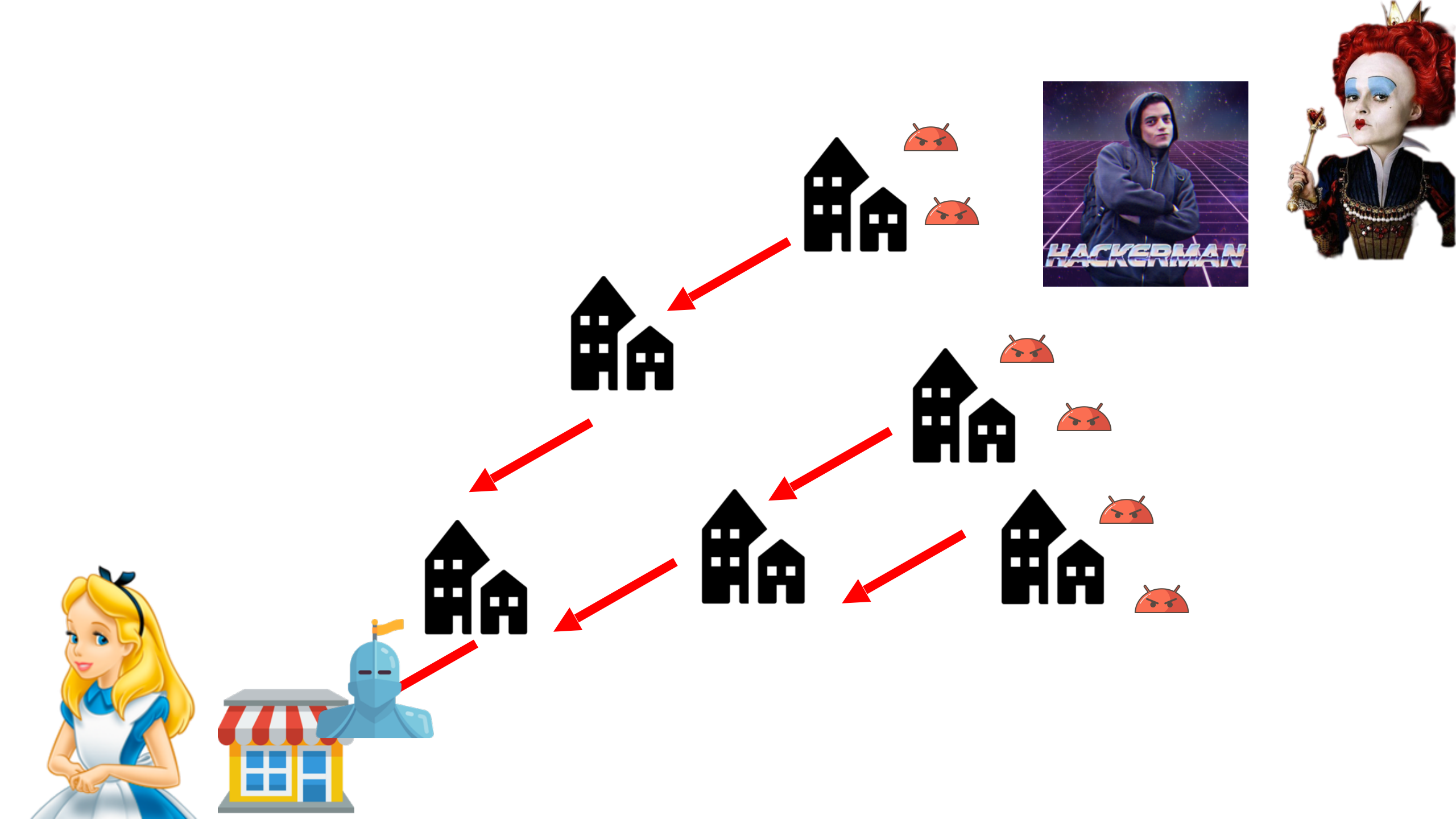




Distributed Denial-of-Service (DDoS) Attacks



http://www.digitalattackmap.com/


HACKERMAN