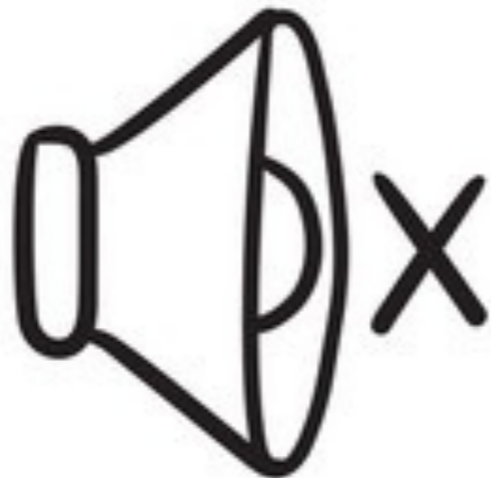


# 2020: Time to Shutdown DDoS?



Stefano Vissicchio

University College London

@ Cosener's

July 6th, 2018

# 2020: Time to Shutdown DDoS?



Stefano Vissicchio  
*NOT a security expert*



@ Cosener's  
July 6th, 2018

Isn't the problem old?

Isn't the problem **old**?

DDoS techniques from late 90s (Smurf)  
Noticeable attacks from 1999-2000

Isn't the problem old?

- **Still important**

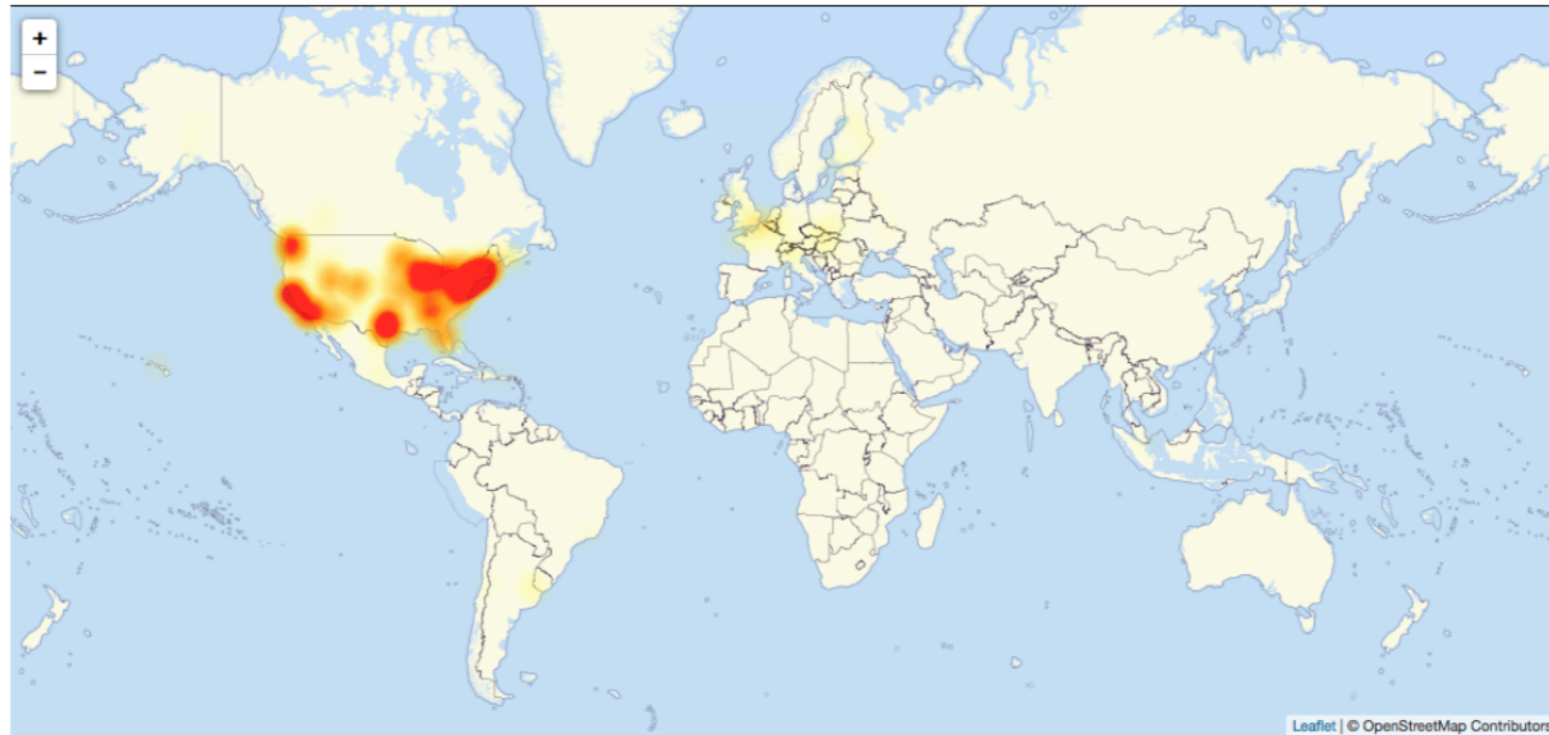
# Many DDoS attacks happen every day

- 2,000+ attacks per day, keep growing in number e.g., see reports from Arbor Networks
- > 1/3 of the used /24s were attacked in 2015-2017 as measured in Jonker et al., IMC'17
- 1/3 of all downtime incidents attributed to DDoS as reported by Verisign/Merril Research

... the big ones make the news, regularly

The New York Times

## *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*



A map of the areas experiencing problems, as of Friday afternoon, according to [downdetector.com](http://downdetector.com).

By **Nicole Perlroth**

Oct. 21, 2016



... the big ones make the news, regularly

The image shows a screenshot of the BBC News website. At the top, the BBC logo is on the left, and navigation links for 'Sign in', 'News', 'Sport', 'Weather', 'iPlayer', 'TV', and 'Radio' are on the right. Below this is a red banner with the word 'NEWS' in white. Underneath the banner is a secondary navigation bar with links for 'Home', 'UK', 'World', 'Business', 'Politics', 'Tech', 'Science', 'Health', and 'Family & Education'. The 'Tech' link is highlighted with a white underline.

The main content area features the article title 'Web attack knocks BBC websites offline' in large, bold black text. Below the title is the date '31 December 2015' and a row of social media sharing icons for Facebook, Messenger, Twitter, Email, and a 'Share' button.

The article content is mostly obscured by a large, semi-transparent 'Error 500 - Internal Error' message. The error message has a white background with a grey border and contains the following text:

**Error 500 - Internal Error**

**This might be because:**

- We are experiencing abnormal traffic to our network or
- the service or servers it is on is not currently available.

**Please try the following options instead:**

- Try again later once we have solved the problem.
- Use our [site index](#)

To the right of the text is a circular graphic featuring a cartoon character holding a sign that says '500'.

At the bottom of the error message, there is a map of the world. Below the map, the text 'according to' is partially visible. At the very bottom of the page, there is a black footer bar with the text: 'An error message greeted many visitors to the BBC news website on Thursday morning'. To the right of the footer bar are icons for Facebook, Twitter, Email, a share icon, and a bookmark icon.



... the big ones make the news, regularly

The image shows a screenshot of a news article from the website Wired. The article is titled "UK is second most targeted nation for DDoS attacks" and is categorized under "Hacking". The sub-headline reads: "Only the United States is hit by more distributed denial of service attacks". The author is identified as Matt Reynolds, with the byline "By MATT REYNOLDS" and the date "Wednesday 24 August 2016". The article features a portrait of the author and a background image of computer code. On the left side of the screenshot, there is a vertical sidebar with the BBC News logo and navigation links for Home, UK, and Technology. At the bottom left, a partial "Error 500" message is visible.


**WIRED** Technology | Science | Culture | Gear | Business | Politics | More


Hacking

# UK is second most targeted nation for DDoS attacks

Only the United States is hit by more distributed denial of service attacks

—



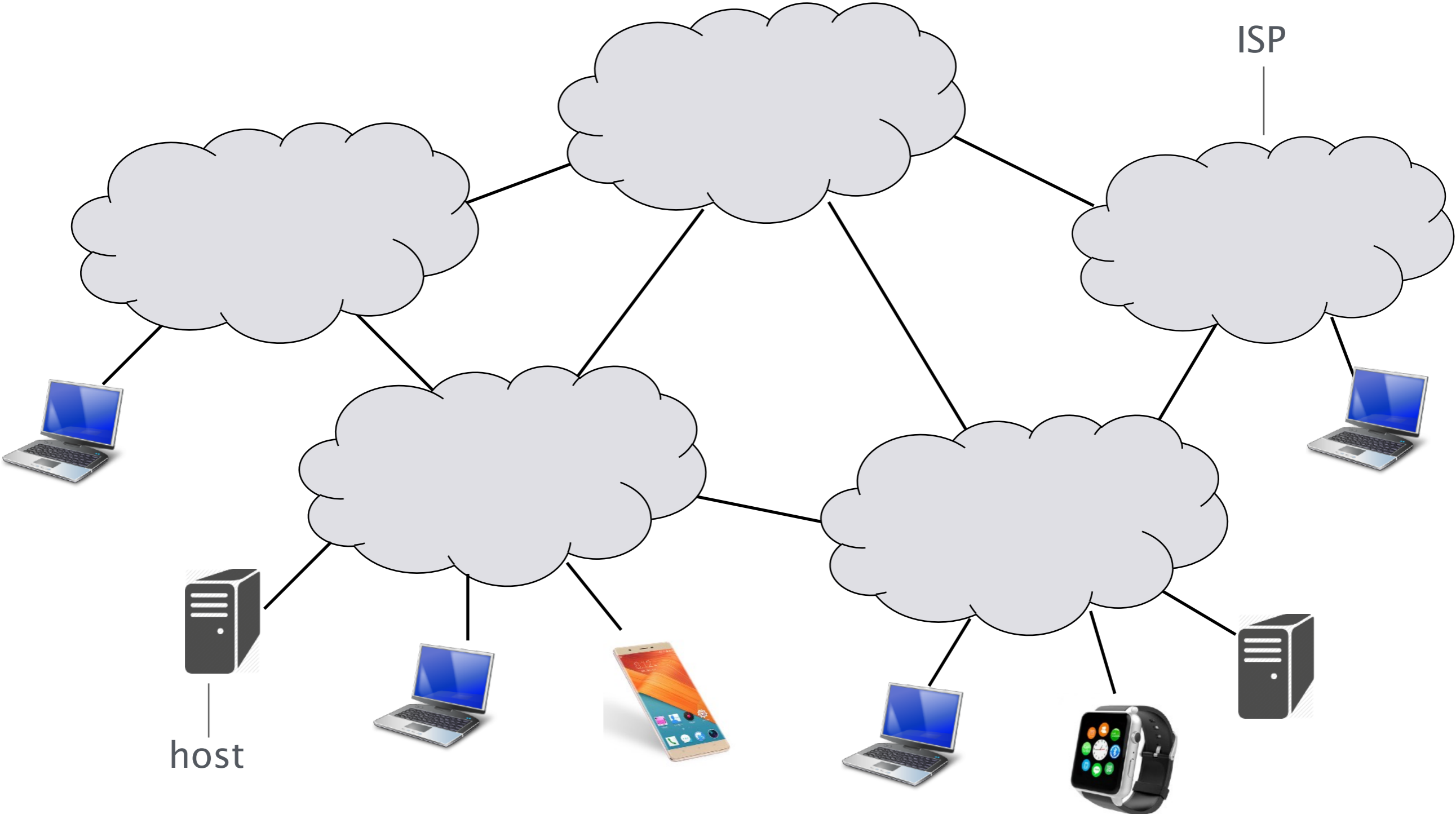
By **MATT REYNOLDS**

—

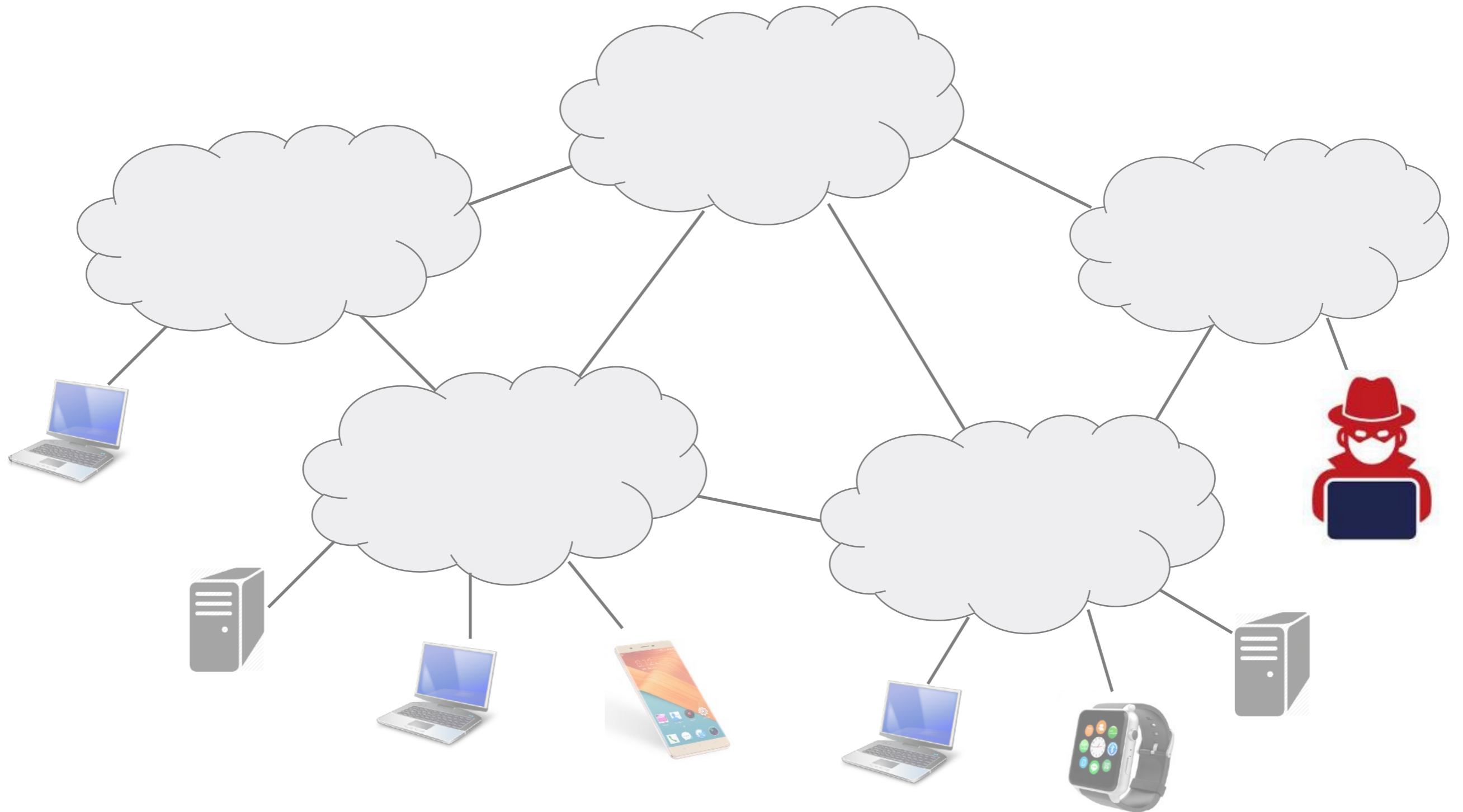
Wednesday 24 August 2016

An error mess

# DDoS thrives because attacks are easy and cheap



# Malicious users can easily connect to the Internet



# They can easily infect devices — e.g., think of IoT\*

\* G. Huston's great post [blog.apnic.net/2015/04/30/the-internet-of-stupid-things/](http://blog.apnic.net/2015/04/30/the-internet-of-stupid-things/)

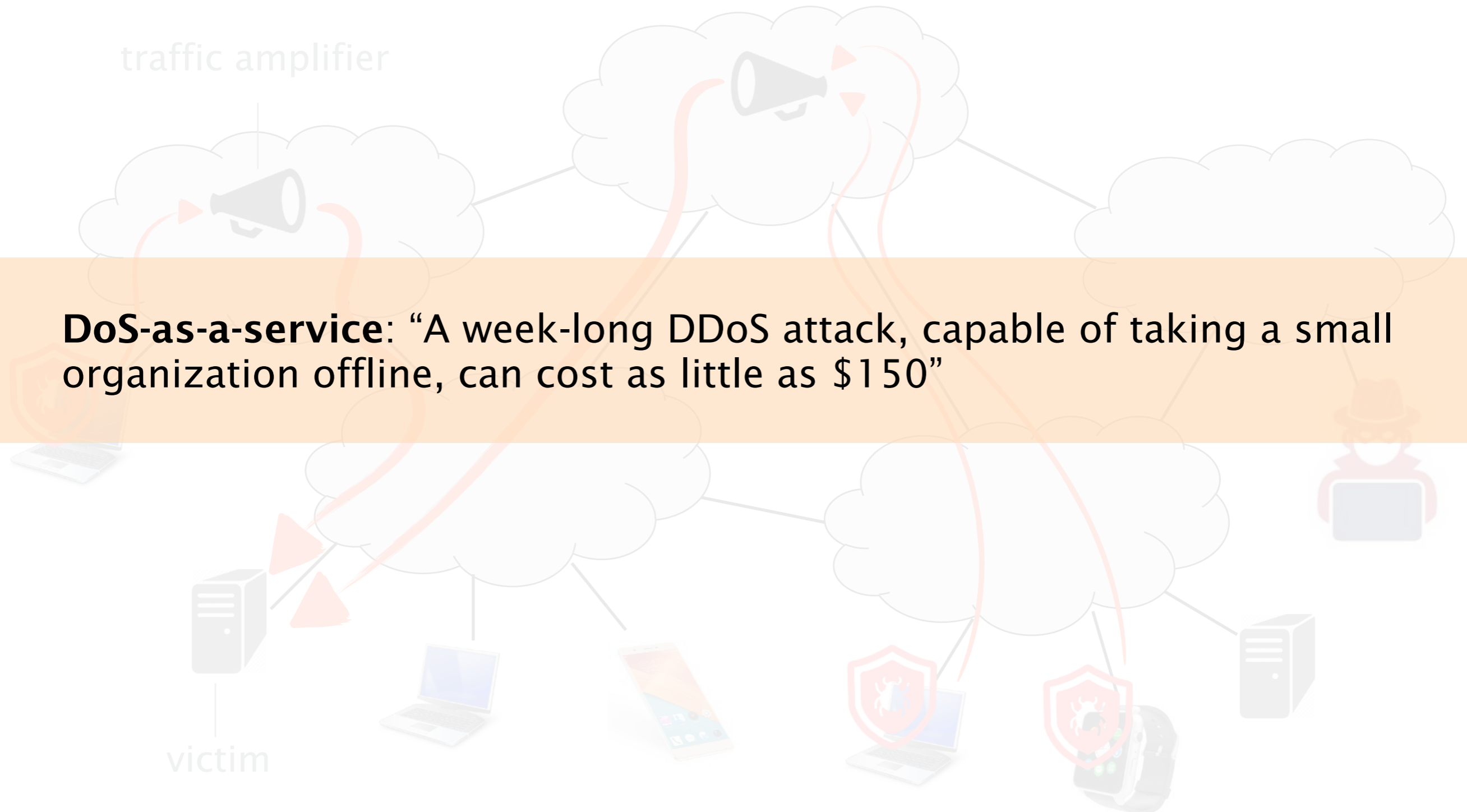


# The infected devices are a botnet, ready to attack



# Renting a botnet is cheaper than a train to Newcastle\*

\* “Man flies from Newcastle to London via Spain because it’s cheaper than the train” in Metro, Jun 2017




**DoS-as-a-service:** “A week-long DDoS attack, capable of taking a small organization offline, can cost as little as \$150”

Isn't the problem old?

- Still important
- **Still unsolved**

DDoS mitigation also makes the “news”

 **WIRED** GitHub Survived the Biggest DDoS Attack Ever Recorded


---

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM


# GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

**SHARE**


---

 **SHARE**  
14009


---

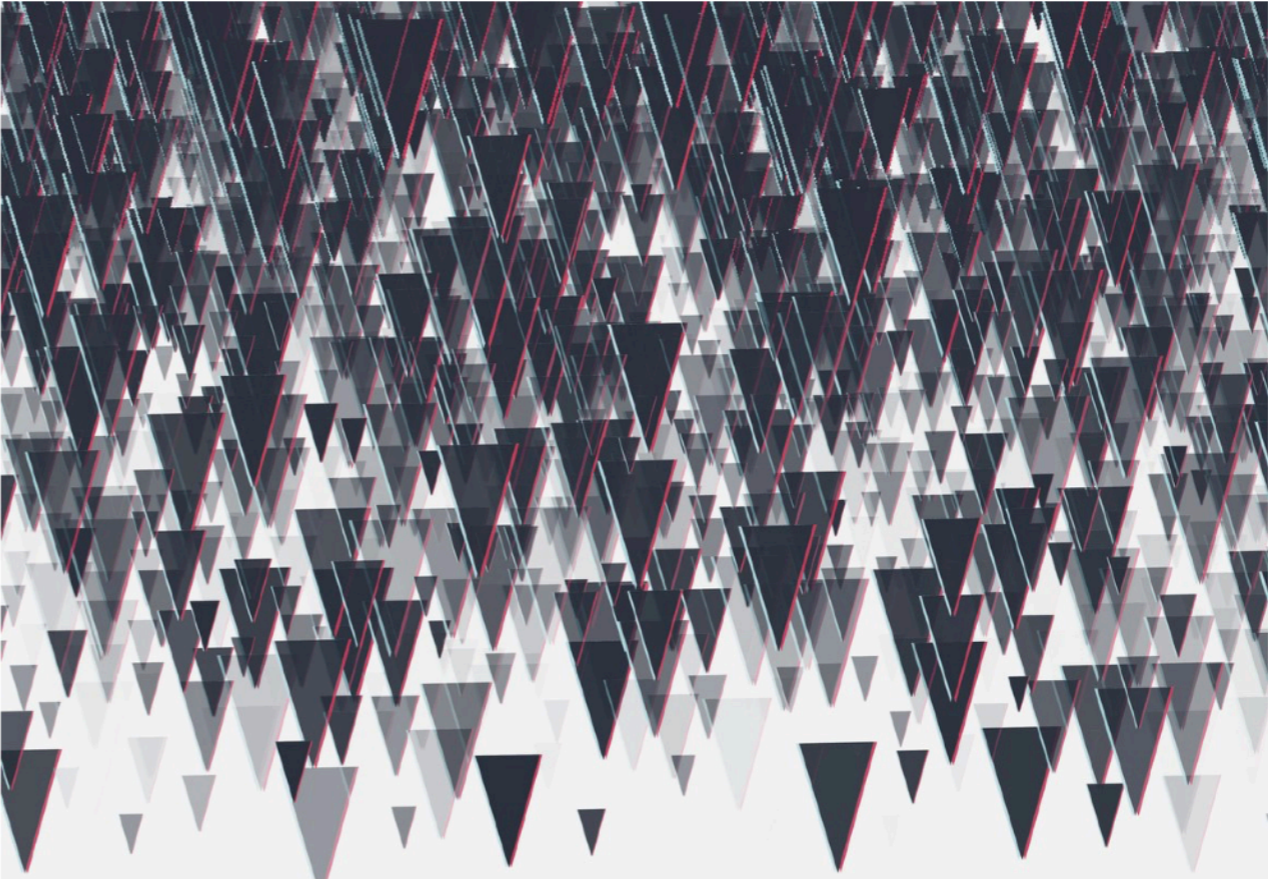
 **TWEET**

---

 **COMMENT**

---

 **EMAIL**

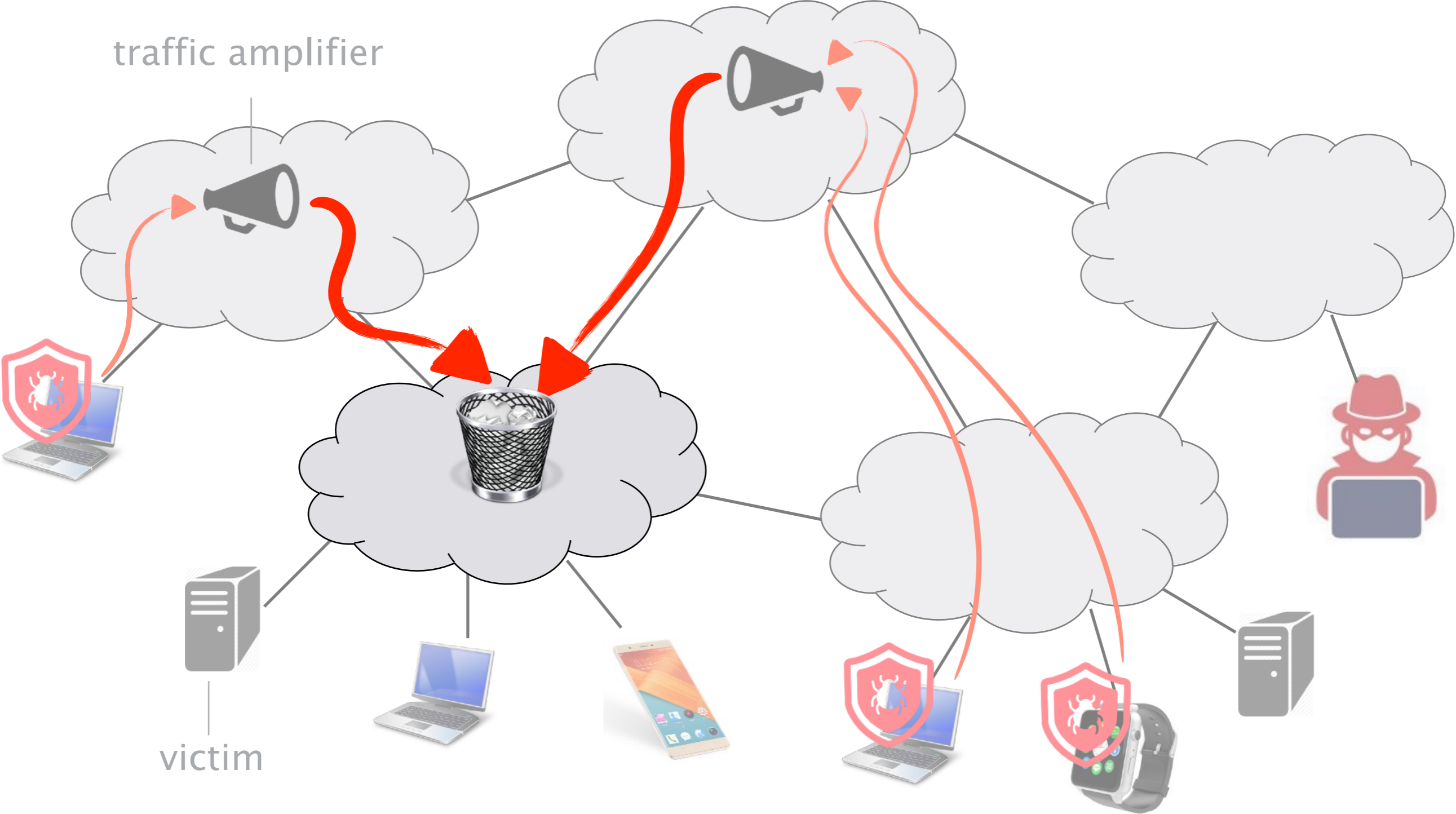




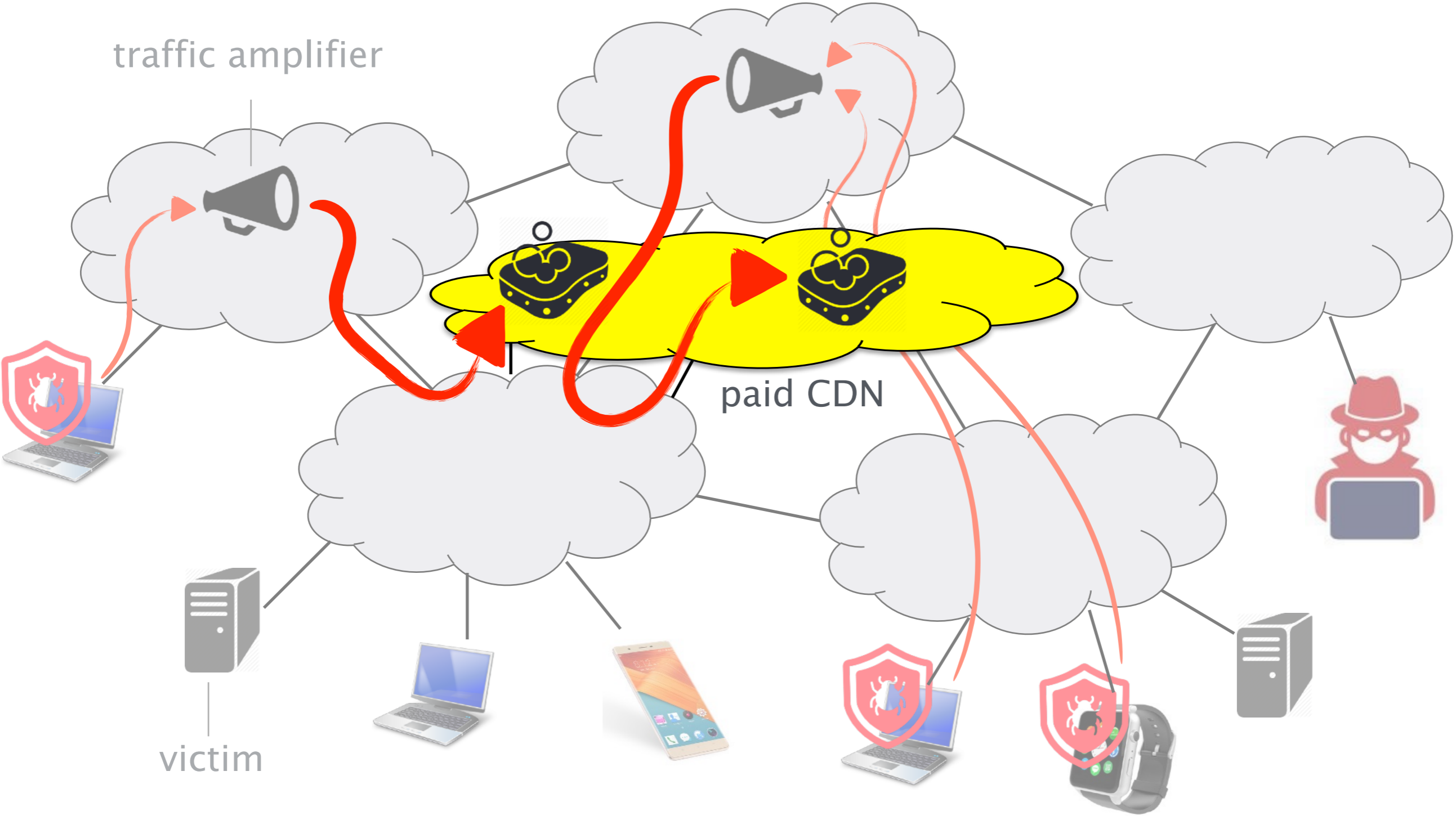
# Let's take back our DDoS example



# Mitigation 1: Ask ISPs to drop all traffic



# Mitigation 2: Pay reverse-proxy providers to scrub traffic



# Current solutions may not be a great deal for victims

- Customers **pay fees**, plus **extras** for surge protection\*  
protection may be more expensive than ransoms
- Dropping or scrubbing can **block legitimate** traffic  
DDoS can still affect service availability and reputation

\* except Google's Project Shield and the very recent Cloudflare's Unmetered Mitigation

## ... and also have technical limitations

- **slow**: 3-5 hours *at least* to even detect attacks according to the Neustar 2017 survey
- Current solutions may not **scale** indefinitely  
attackers may potentially generate HUGE traffic volumes
- Current solutions are **not universal**  
e.g., can't block attacks to the network infrastructure

# What if attackers are smarter and more tenacious? (e.g., think of country-level attackers)

- Can evolve the attack over time  
e.g., pause and resume the attack after mitigation
- Can follow moving targets  
e.g., attack the new IP of a Web site, when updated
- Can focus on hard-to-mitigate attacks  
e.g., those on the network infrastructure

## Isn't the problem old?

- Still important
- Still unsolved
- **We can do better**      *with programmable networks*

# We can extract information from traffic behaviour

- The control-plane can track unexpected patterns  
e.g., links impossible to offload, unusual mixes of traffic type, ...
- Example: reaction to traffic engineering (TE)  
provocation: maybe, this pile of TE work on minimising link utilisation is useful for security



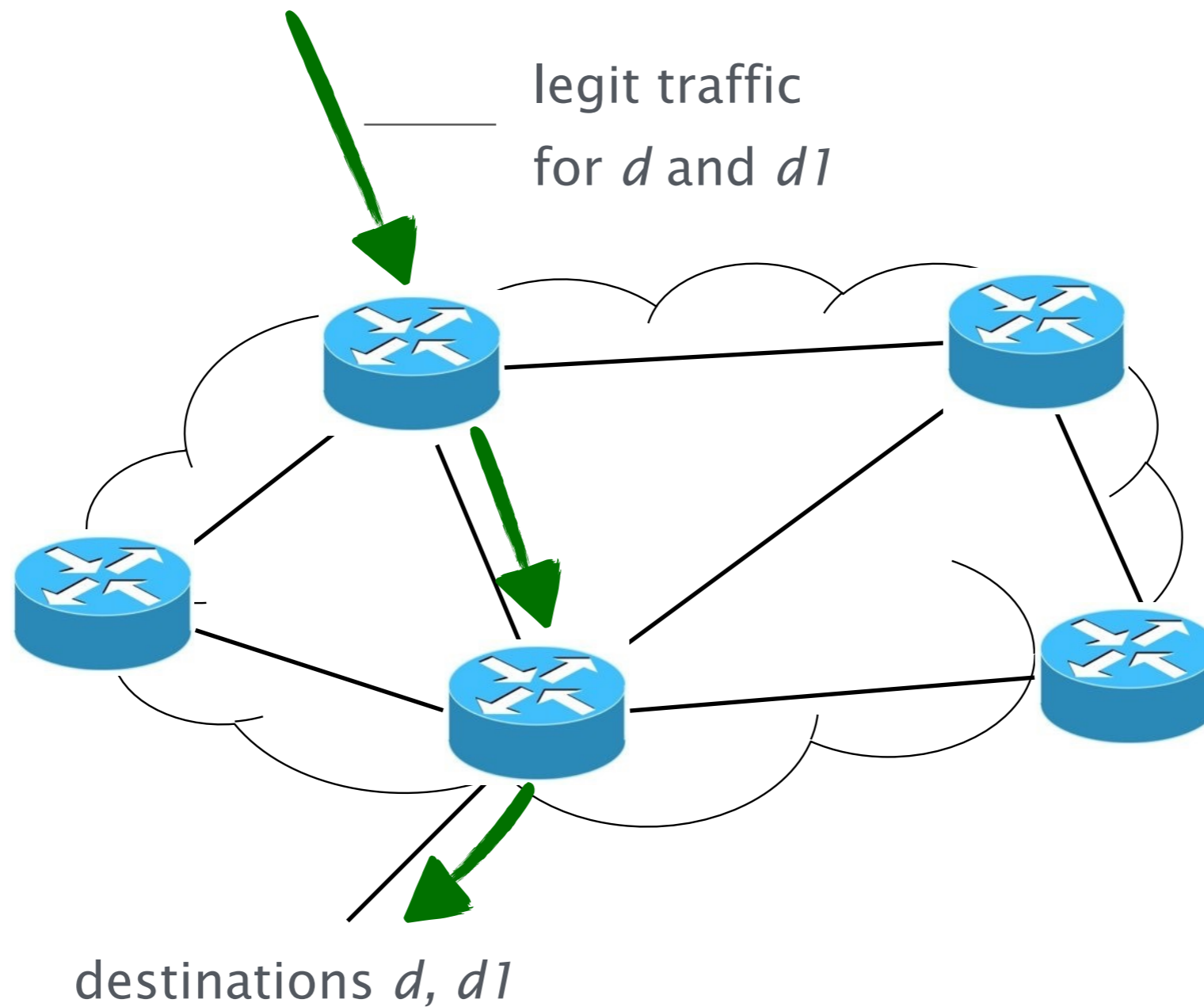
# We can extract information from traffic behaviour

For better resource utilisation with TE, you may be interested in “On low-latency-capable topologies, and their impact on the design of intra-domain routing”, to appear in SIGCOMM 2018

- Example: reaction to traffic engineering (TE)  
provocation: maybe, this pile of TE work on minimising link utilisation is useful for security

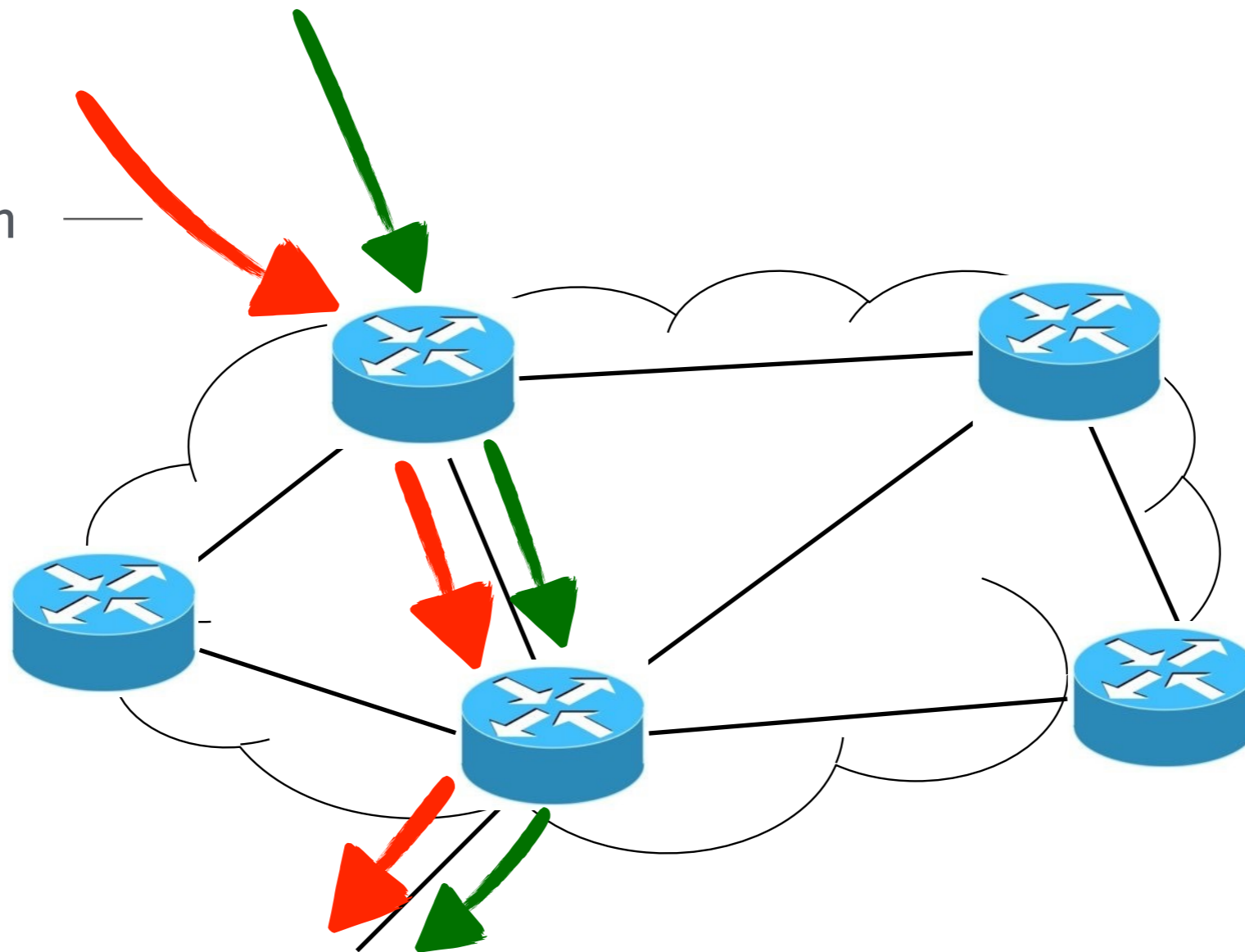
Programmable networks can do even better

# The control-plane decides traffic paths



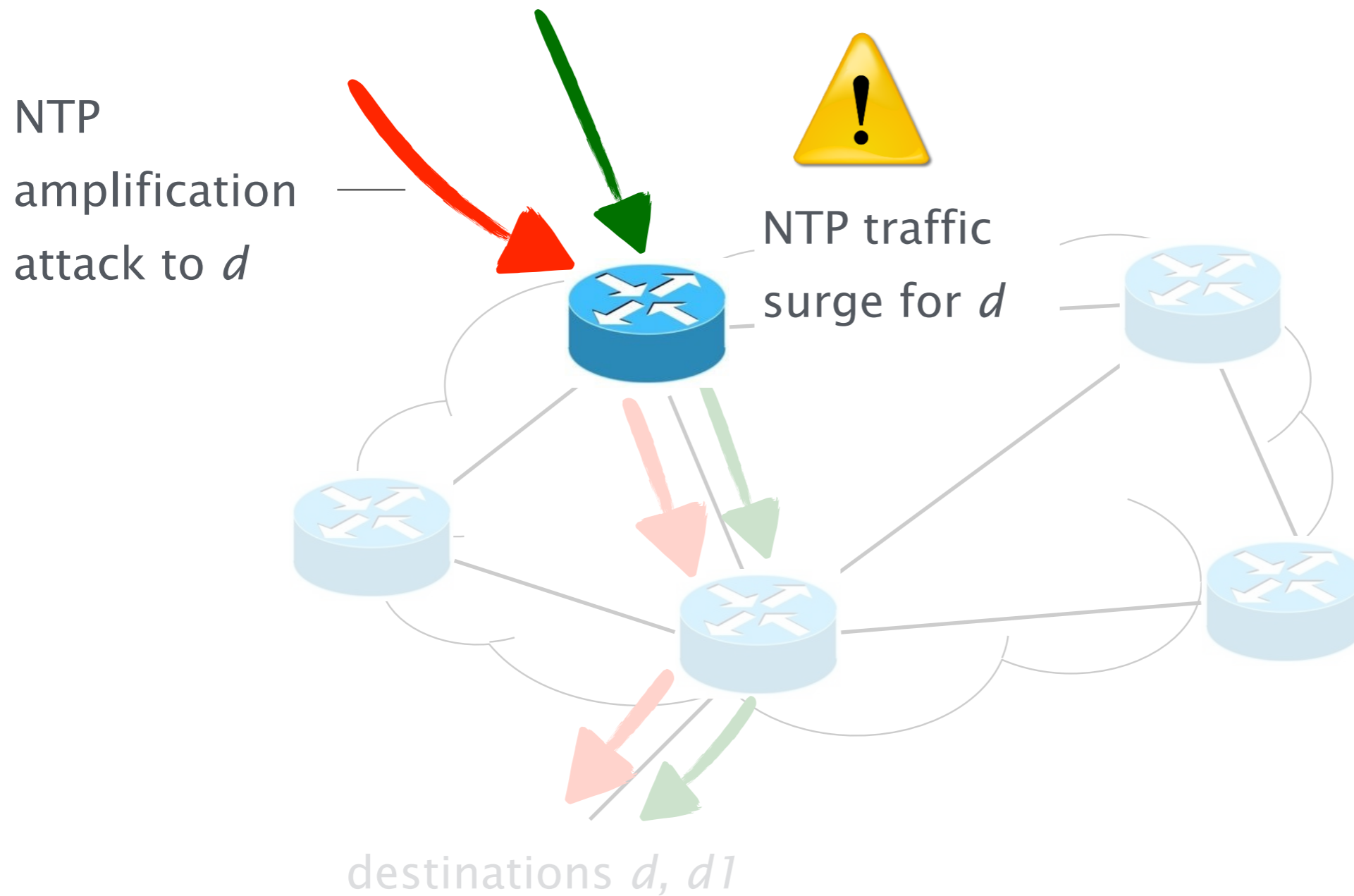
Currently, paths don't depend on traffic type

NTP  
amplification  
attack to  $d$

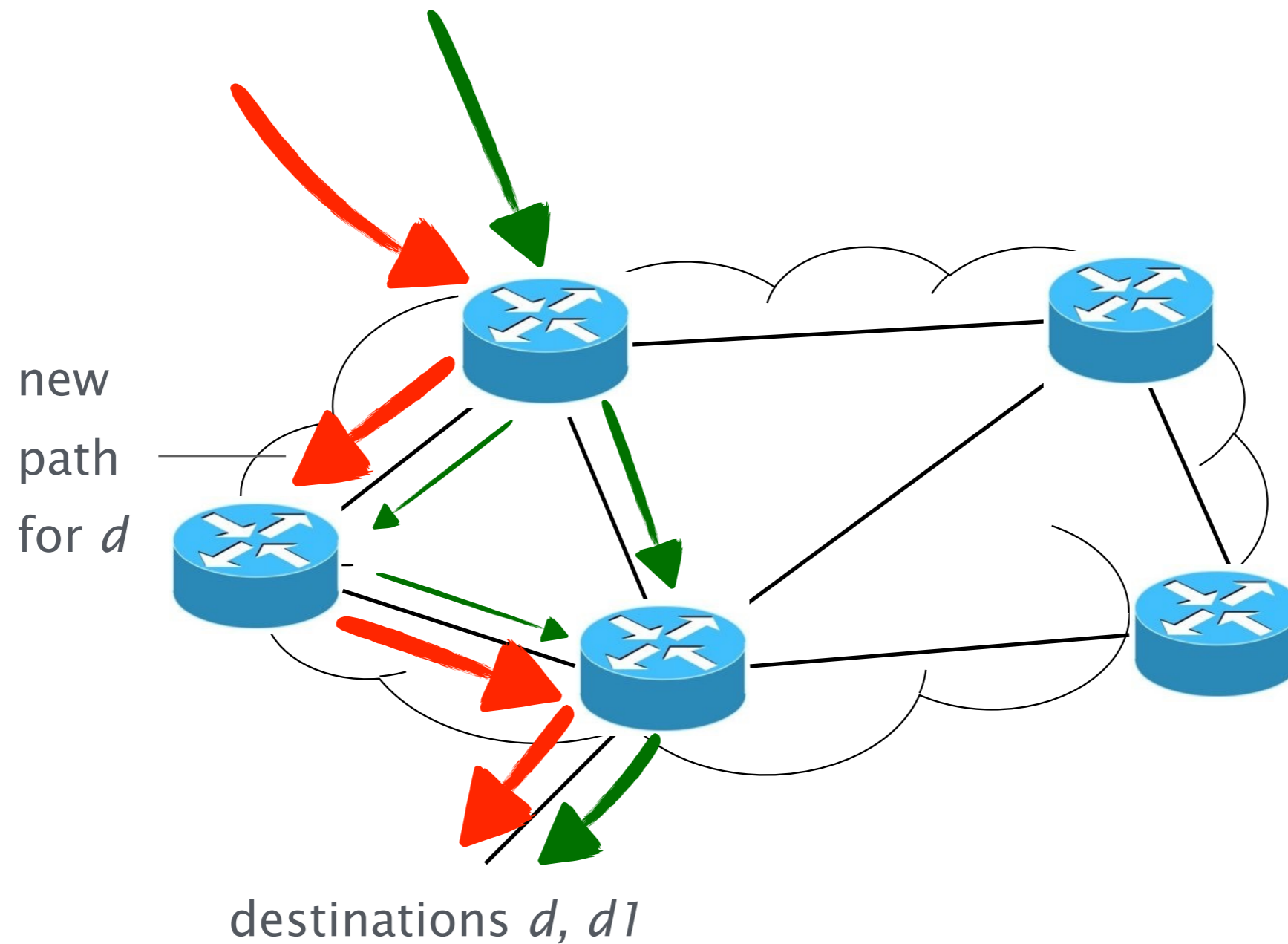


destinations  $d, d1$

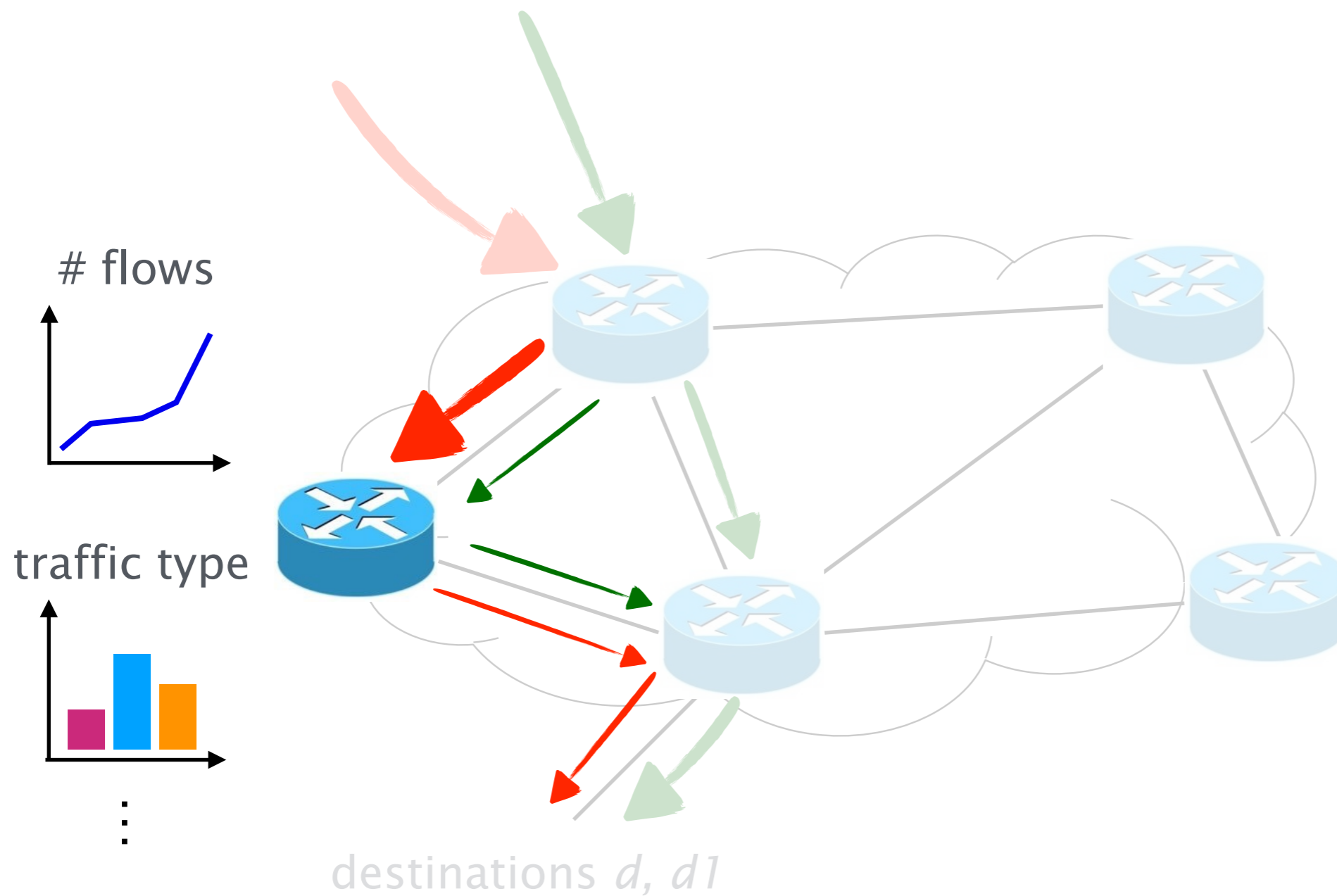
# Programmable data-plane can raise custom alerts



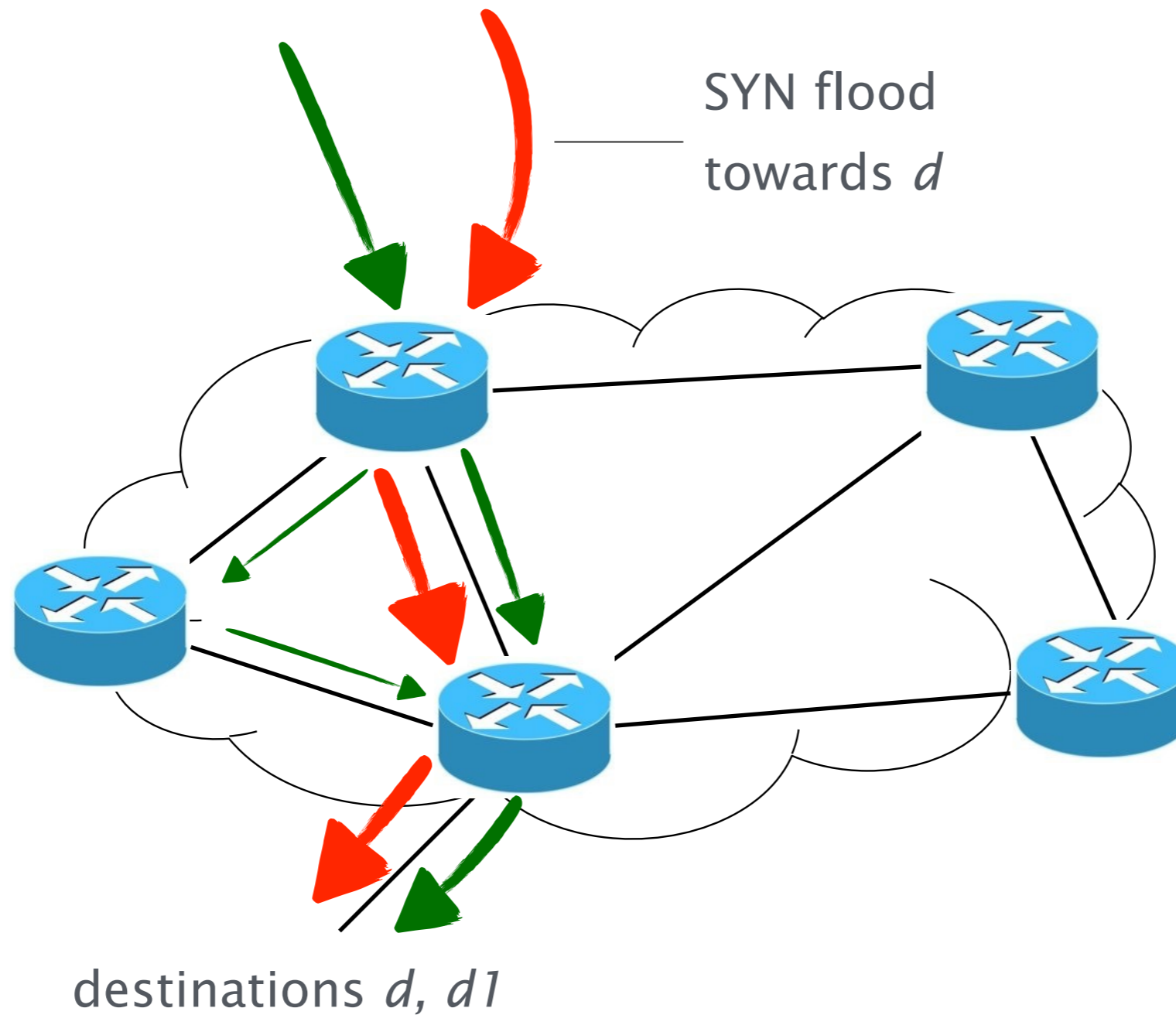
# New control-planes can install attack-exposing paths



... and program the data-plane to further zoom in  
(to detect, characterise, mitigate the attack)

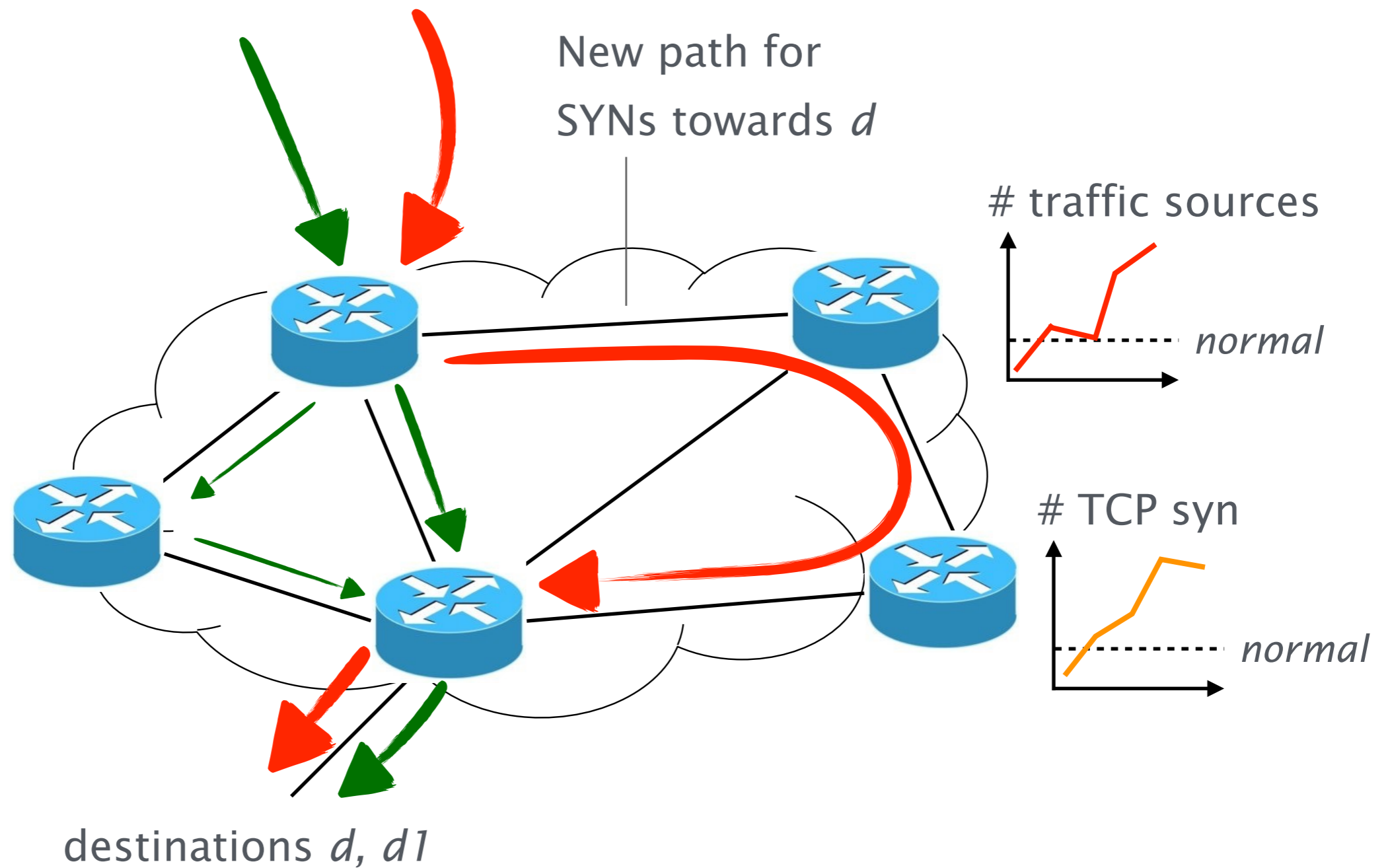


# The attack can evolve, reacting to mitigation





# Programmable networks can react again



# The interesting questions remain open

- Monitoring: Which stats to monitor? How, where, at which level of granularity? How to quickly and scalably zoom in/out on some traffic?
- Algorithms: How to select paths? Can the path selection avoid to affect non-DDoS traffic? How to avoid oscillations in path decisions?
- System: How fast can the system be? When to look for an attack, and when to declare an attack finished? Can the system itself be DDoS-ed?
- Approach: Which other possibilities are opened by programmability? For example, can a defender create disincentives for attackers during an attack?