

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

Can you think of a misuse of routing algorithms?



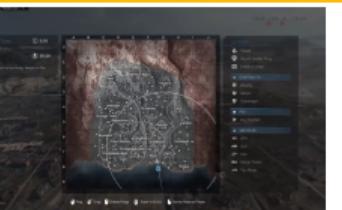
China rerouted mobile traffic from several European networks
(Getty Images/iStockphoto)

Computer Networks

2022-02-21

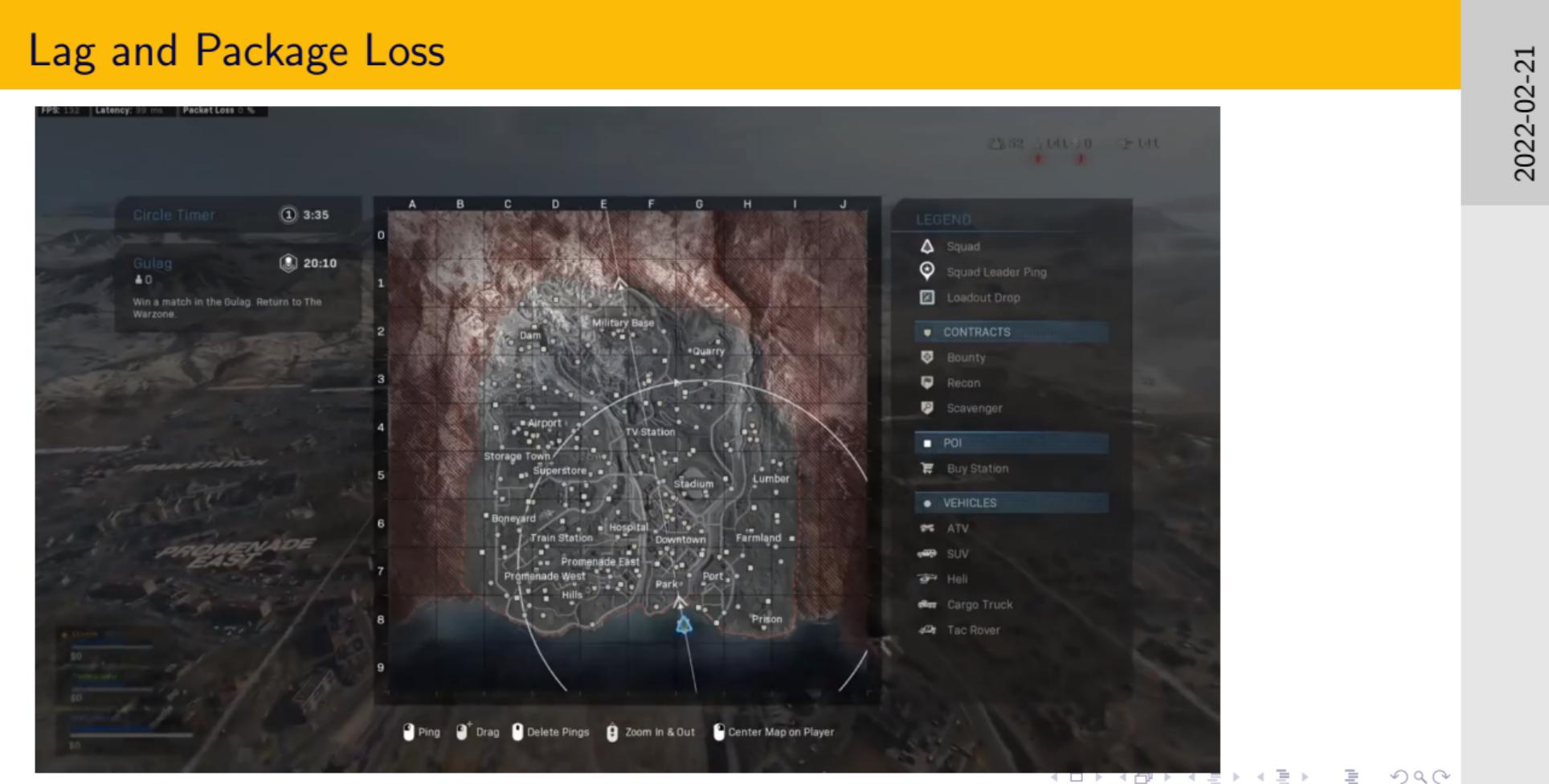
In June 2019, European internet traffic was routed through China (also in 2010). This can allow interception of data, or MITM attacks. Similar attacks happened in the past as well. They rely on manipulating BGP.

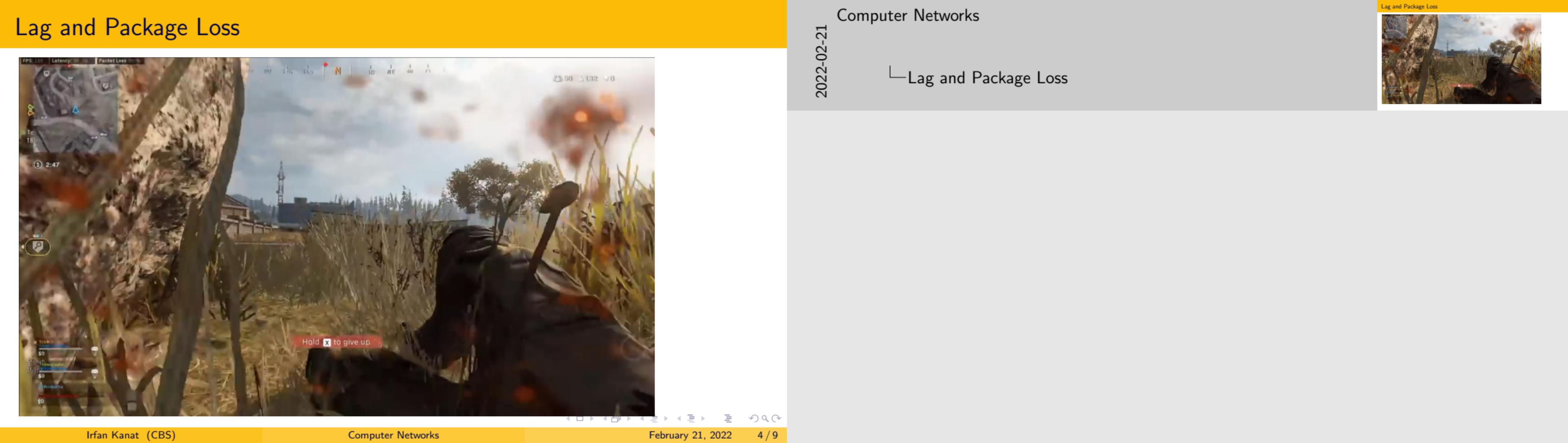
EUROPEAN MOBILE TRAFFIC MYSTERIOUSLY ROUTED THROUGH CHINA FOR TWO



2022-02-21

Lag and Package Loss



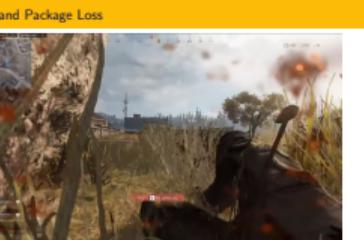


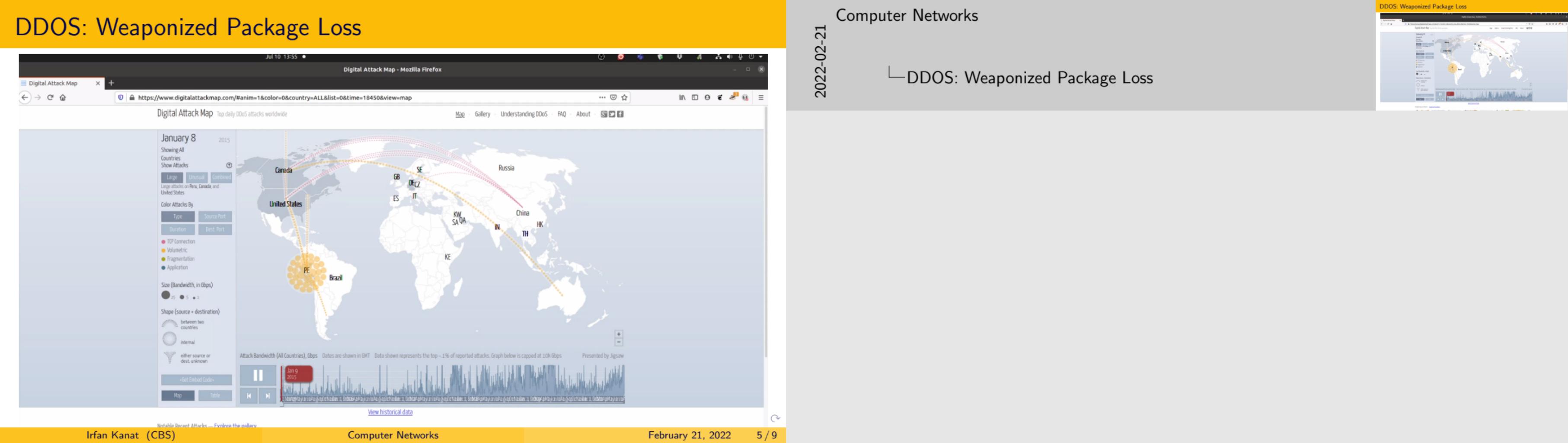
Lag and Package Loss

Computer Networks

2022-02-21

└ Lag and Package Loss





Networking and Security: Segmentation

2022-02-21

Computer Networks

- Networking and Security: Segmentation

Segmentation: it kept coming up in cases we read (target esp.)
The idea is, you can have multiple virtual networks on the same hardware. So you put your customer facing machines on one network, and your back office operations in another, and perhaps mission critical systems on yet another network. What this means is they all get their own IP prefix and treat each other as nodes in different networks.

Networking and Security: Segmentation

Zero Trust Architecture

```
graph TD; A((VERIFY THE USER)) --> B((VALIDATE THE DEVICE)); B --> C((LIMIT ACCESS & PRIVILEGE)); C --> A; D[LEARN & ADAPT]
```

The diagram illustrates the Zero Trust Architecture as a continuous, circular process. It begins with 'VERIFY THE USER' (represented by a user icon with a smartphone and a fingerprint), moves to 'VALIDATE THE DEVICE' (represented by a device icon with a magnifying glass), and finally reaches 'LIMIT ACCESS & PRIVILEGE' (represented by a user icon with a server and database icon). A large gear icon labeled 'LEARN & ADAPT' is positioned at the top right, indicating the ongoing monitoring and adjustment of the trust levels.

Computer Networks

2022-02-21

Zero Trust Architecture

This is a more recent trend.

No trust is granted based on network location.

All devices and users authenticated

Data released on a need to know basis

Focus is on protecting resources and not network segments.

This is in contrast to prior approaches that focused on network segments.

NIST draft 800-207

```
graph LR; A[VERIFY THE USER] --> B[VALIDATE THE DEVICE]; B --> C[LIMIT ACCESS & PRIVILEGE]; C --> A; D[LEARN & ADAPT]
```

A small diagram titled 'Zero Trust Architecture' located in the top right corner. It shows a linear process: 'VERIFY THE USER' leads to 'VALIDATE THE DEVICE', which leads to 'LIMIT ACCESS & PRIVILEGE'. Above this linear sequence is a circular arrow labeled 'LEARN & ADAPT', indicating an ongoing feedback loop.

Irfan Kanat (CBS)

Computer Networks

February 21, 2022

7 / 9

Intrusion Detection on Networks

- Unusual behavior on your network
- Heuristics
- Known signatures

Computer Networks

2022-02-21

Intrusion Detection on Networks

A few examples:
A client is rapidly sending packages to a large number of ip's and ports (probably nmap scan)
A server with minimal functionality generally does not initiate exchanges. Meaning TCP syn packets do not generally originate from servers. If you see your server reaching out.
Or generating traffic on ports it is not supposed to generate traffic on...
Then you know that there is something wrong.
Attacks often have certain characteristics. These attack specific characteristics are called signatures. These signatures are often shared through intel sharing schemes. If your network demonstrates behavior that matches the signature IDS will pick up.

Unusual behavior on your network
Heuristics
Known signatures

A set of small, light-gray navigation icons typically used in Beamer presentations for navigating between slides and sections.

Irfan Kanat (CBS)

Computer Networks

February 21, 2022

8 / 9

SNORT can be provided by appliances (like Watchguard), or by software solution (like SNORT). Appliances are used for larger networks where latency can be an issue.

Network based intrusion detection is often coupled with end point ids. That is not within scope today.