Beauty And The Burst

Remote Identification of Encrypted Video Streams

Presented by: Aviel Zecharia & Eli Cohen

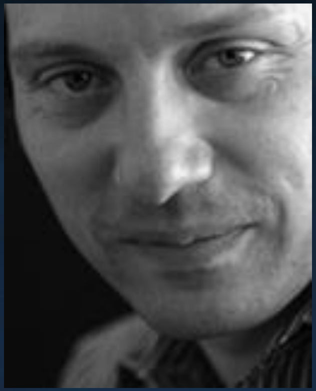
Agenda

- Background
- MPEG-DASH Standard
- Attack Overview
- Deep Neural Networks
- Adversarial Models
  - On-Path Attack
  - Off-Path Attack

Authors

Roei Schuster

- Tel Aviv University
- Cornell Tech



Vitaly Shmatikov

- Cornell Tech

Eran Tromer

- Tel Aviv University
- Columbia University

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

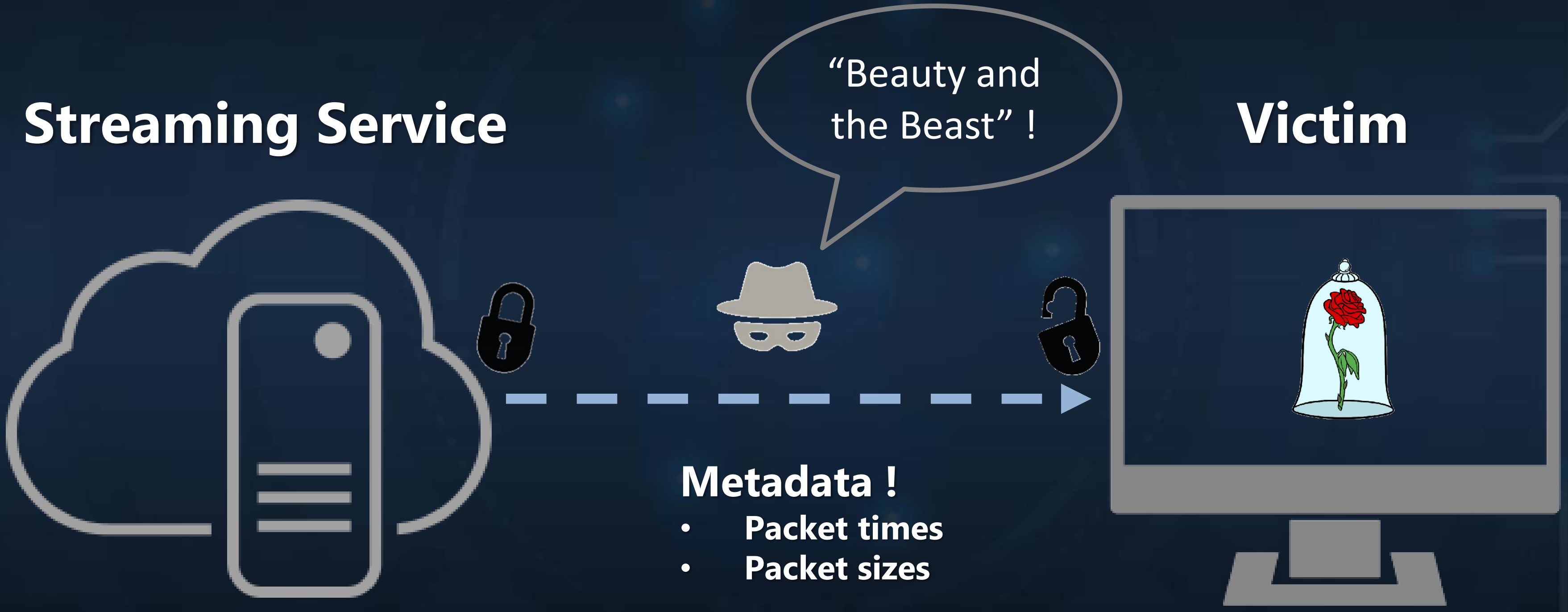
CORNELL TECH

Why video traffic is so interesting ?

Background

- Targeted marketing purposes
- Market characterization efforts
- Not everybody wants to volunteer this information about their habits
  - Video traffic is encrypted
  - HTTPS has been in wide deployment

What still can be learned ?



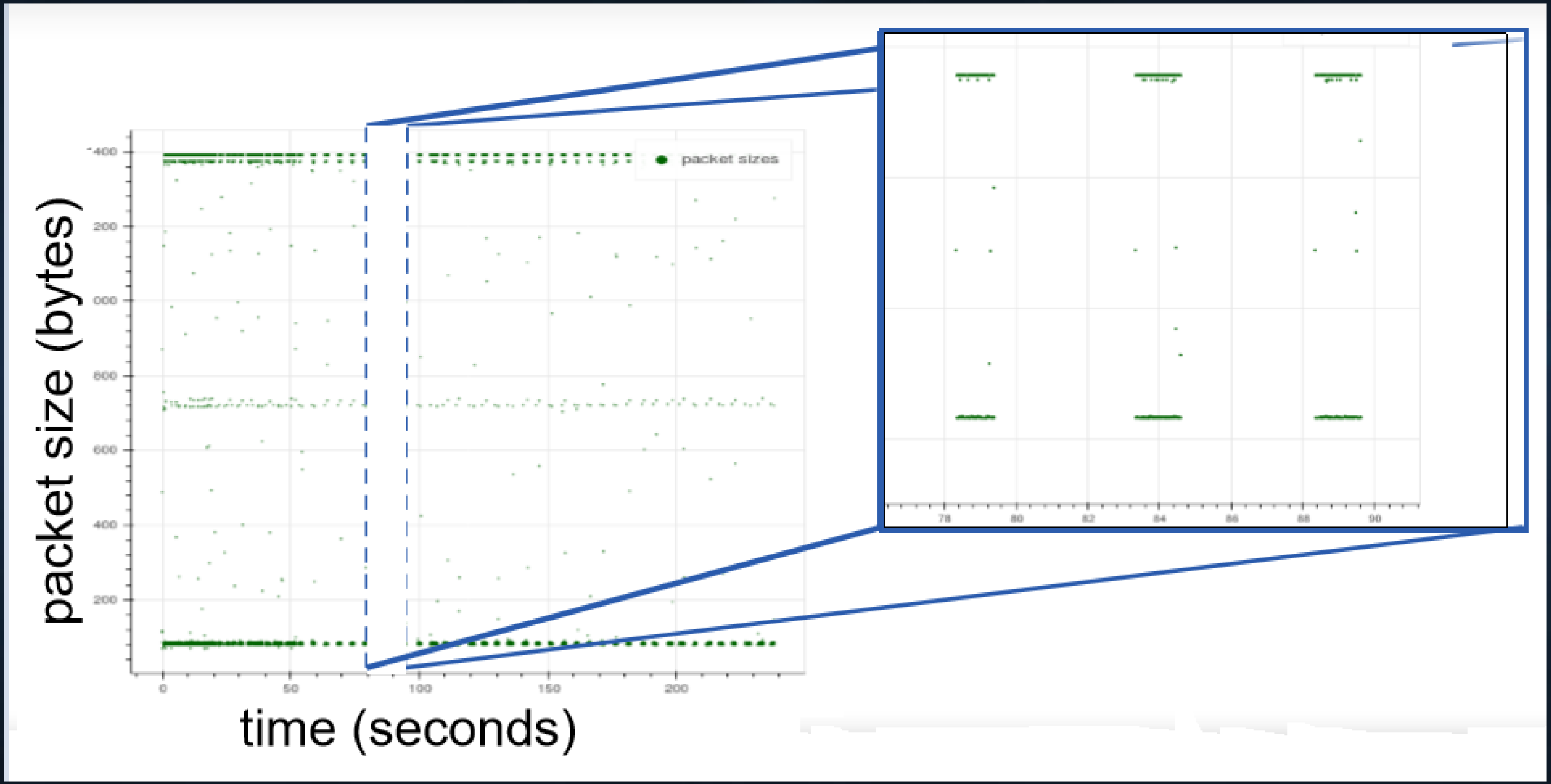
Streaming Service

Victim

Metadata !

- **Packet times**
- **Packet sizes**

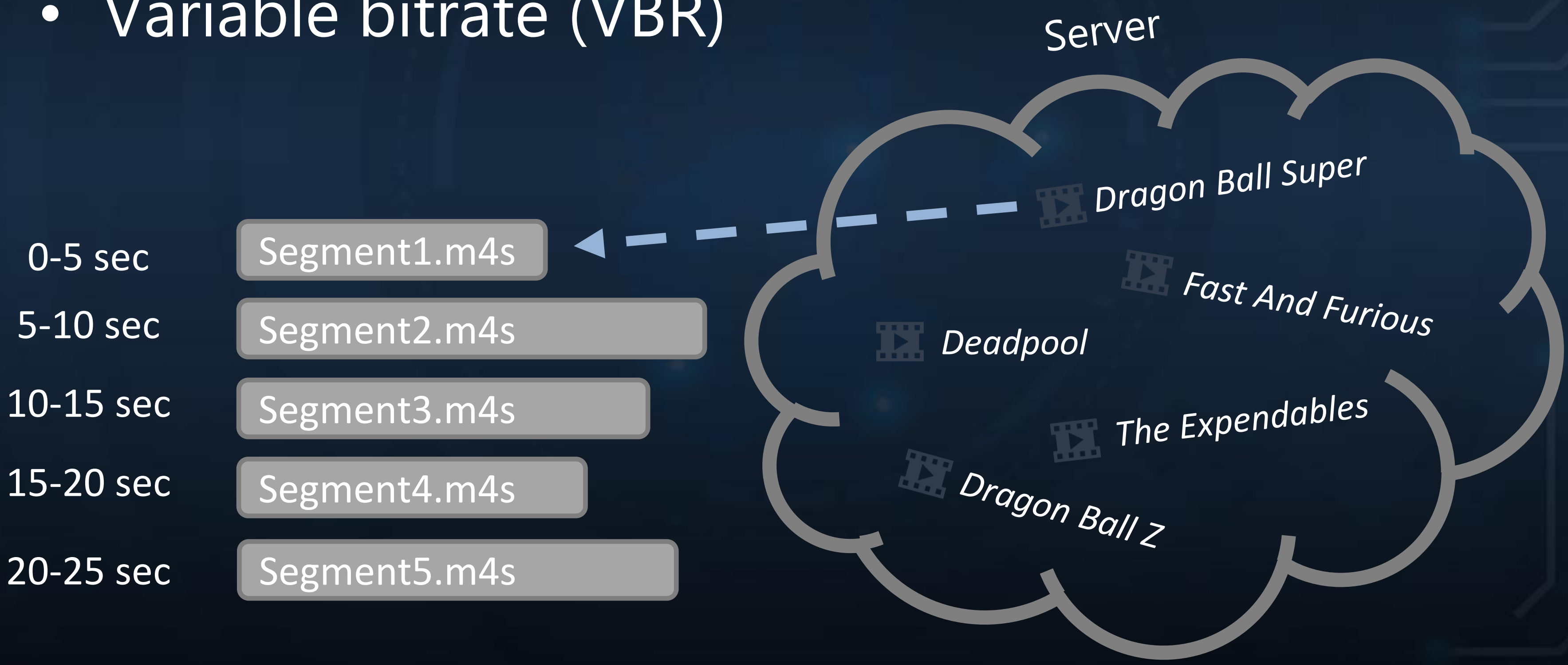
Initial buffering & on/off bursts



Where the bursts come from ?

MPEG-DASH standard

- Widely adopted by major streaming providers
  - Netflix, YouTube etc.
- Variable bitrate (VBR)



Server

Dragon Ball Super

Fast And Furious

Deadpool

The Expendables

Dragon Ball Z

0-5 sec Segment1.m4s

5-10 sec Segment2.m4s

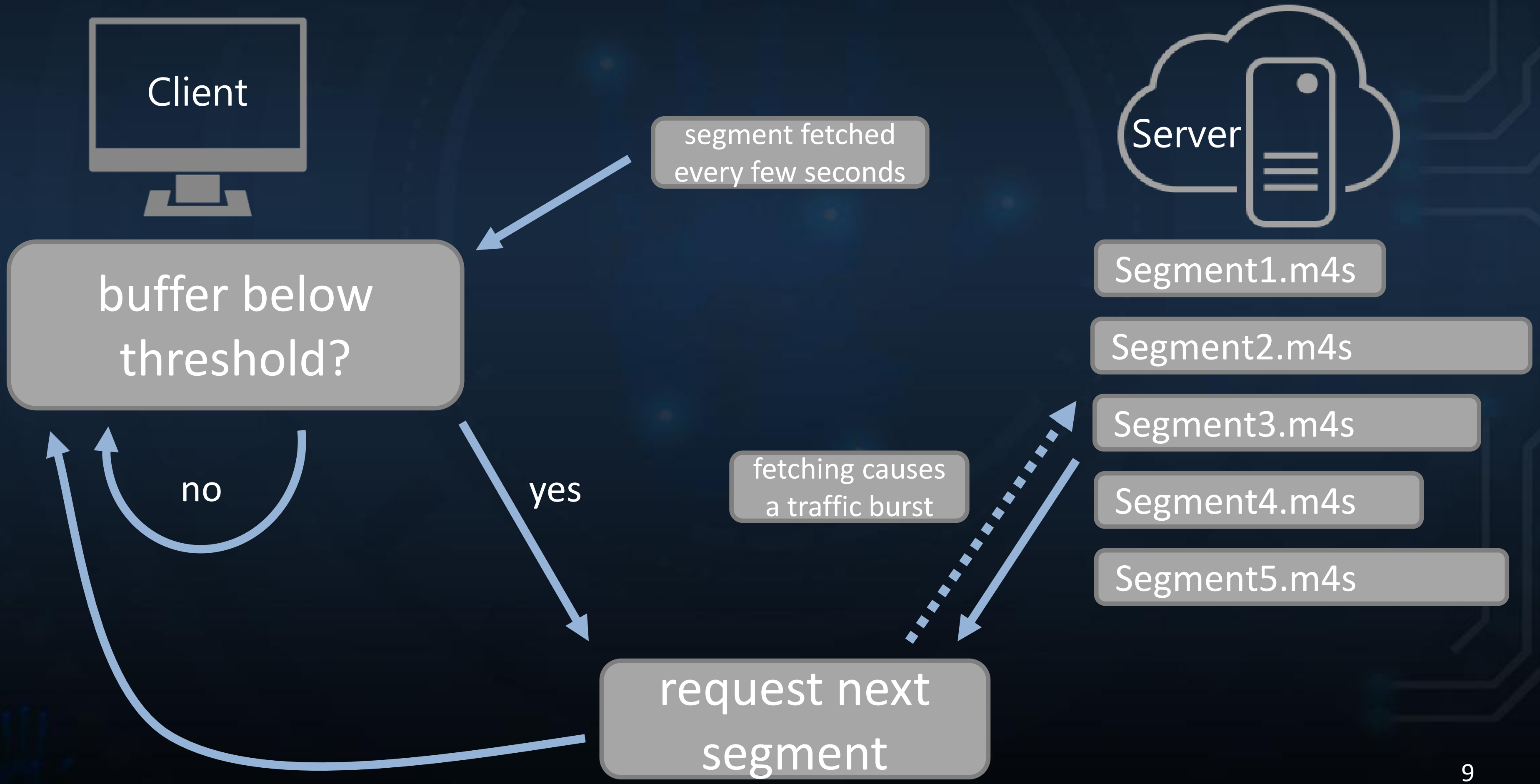
10-15 sec Segment3.m4s

15-20 sec Segment4.m4s

20-25 sec Segment5.m4s

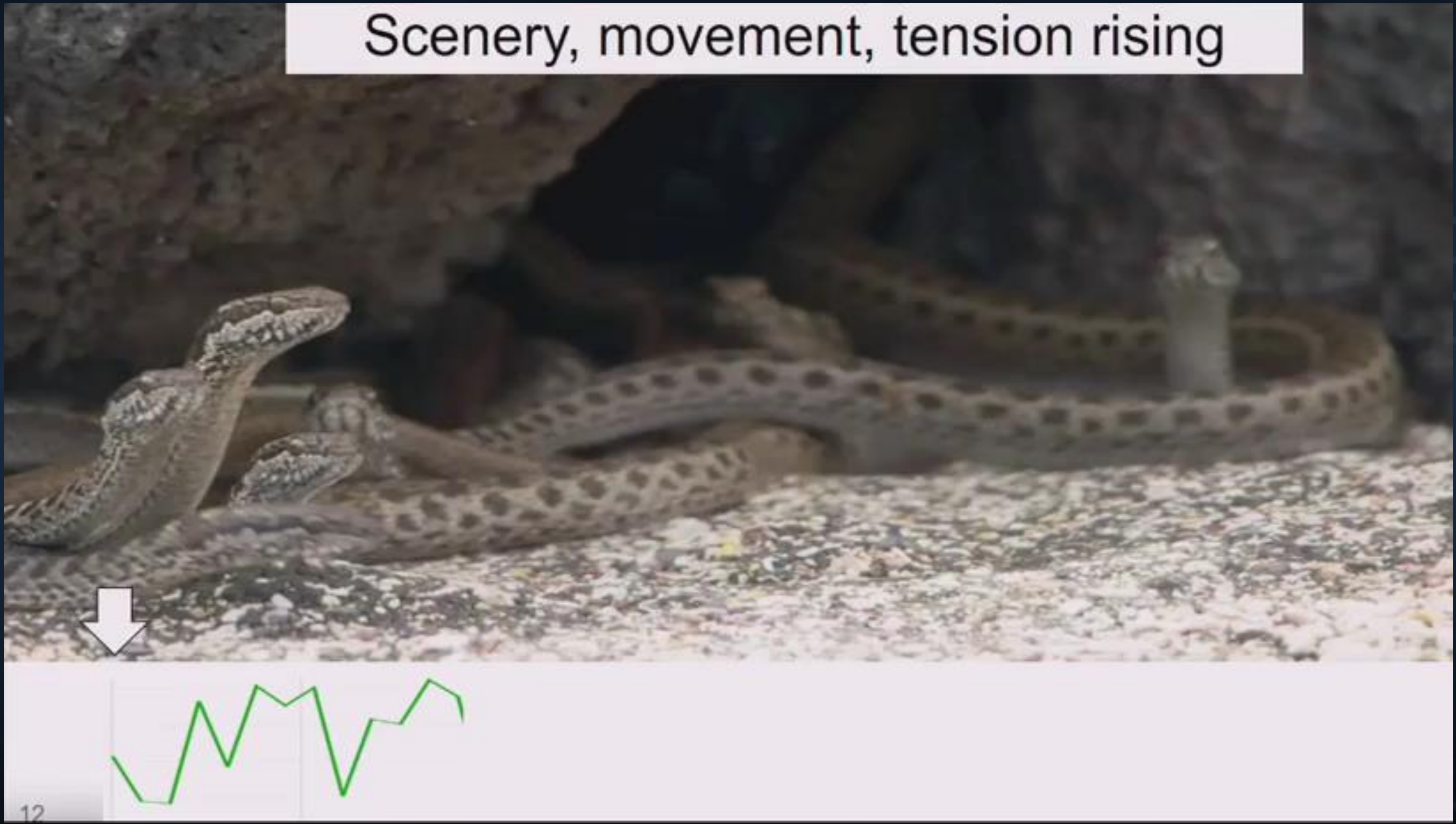
MPEG-DASH standard

- Adaptive bitrate streaming over HTTP



VBR Demo

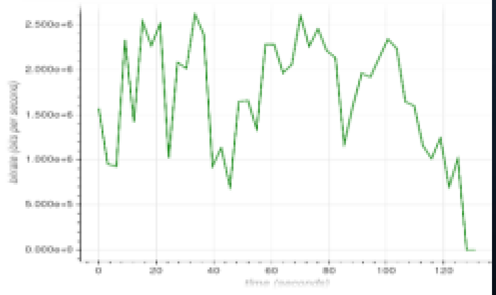
Iguana vs. Snakes



MPEG-DASH leak

Content

VBR pattern



Segments

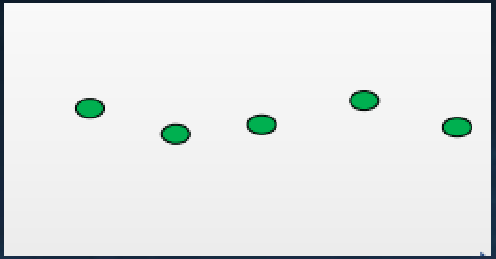
Segment1.m4s

Segment2.m4s

Segment3.m4s

• • •

Burst sizes



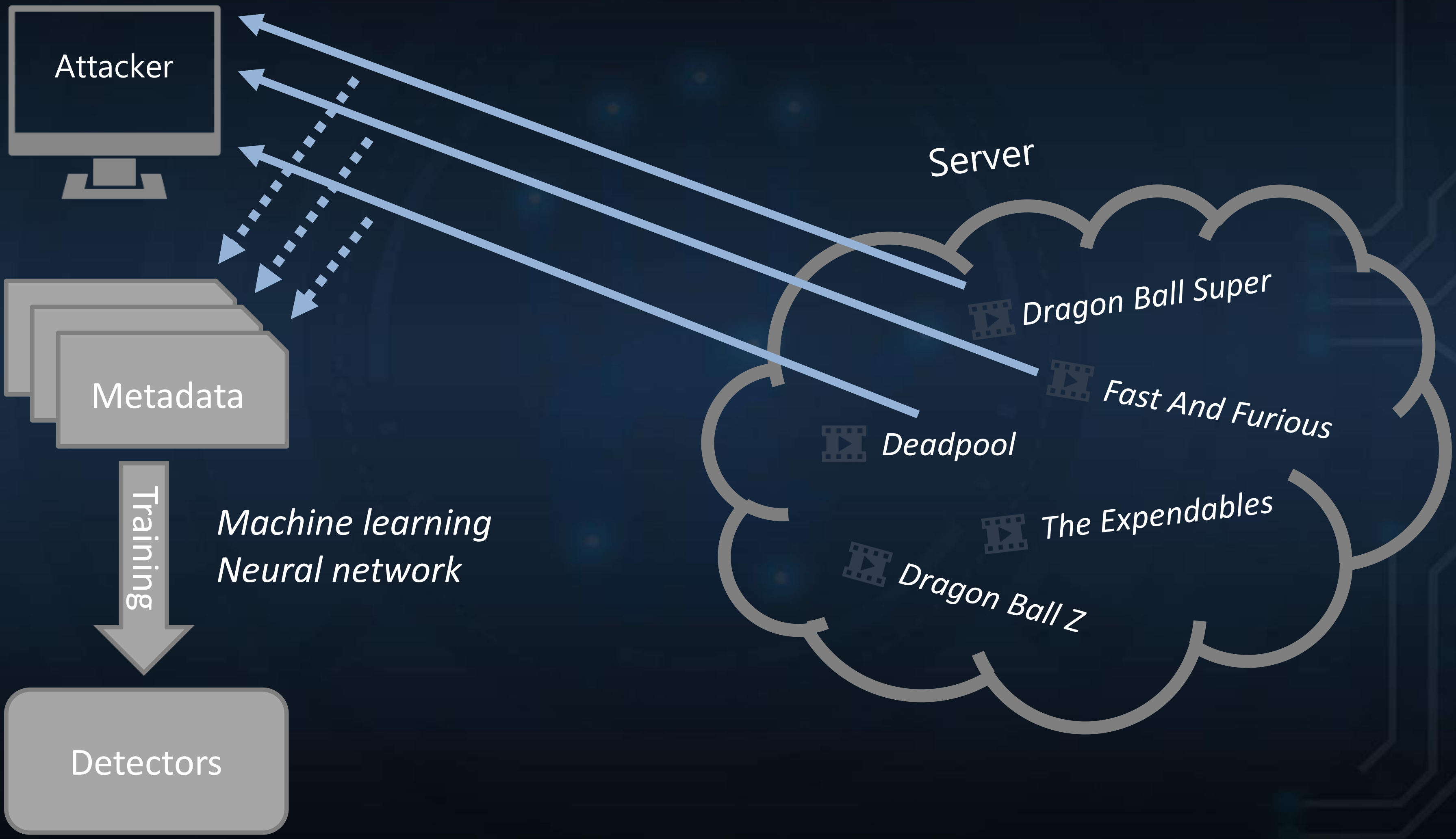
From a leak to a fingerprint

- Does the pattern of burst (segment) sizes uniquely characterize a title?
- Empirically for the 3500 downloaded from YouTube 20% of them have a uniquely identifying pattern
- Can we learn a title’s identifying pattern?
- We can learn a title’s identifying pattern because of the pattern consistency

⇓

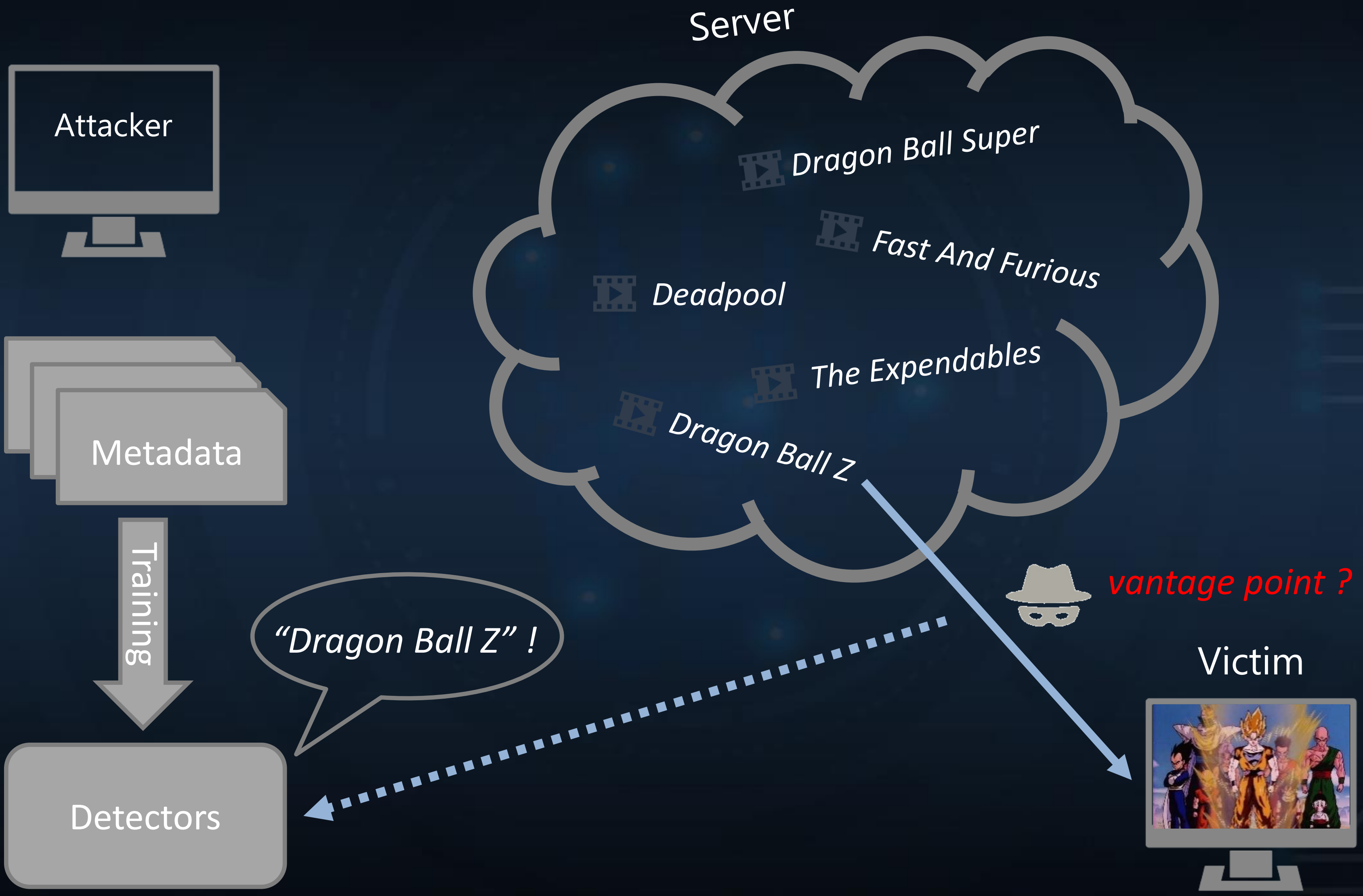
~20% of YouTube titles have fingerprints

Attack overview



Machine learning
Neural network

Attack overview


Server

Dragon Ball Super

Fast And Furious

Deadpool

The Expendables

Dragon Ball Z

Attacker

Metadata

Training

Detectors

"Dragon Ball Z" !

vantage point ?

Victim

Deep Neural Networks

- Very good at learning high-level concepts that human can easily agree on but find it hard to formally express
- Can operate on noisy and coarse measurements
- Agnostic to protocol-specific attributes
- Can learn features other than burst patterns, e.g. arrival patterns of individual packets
- Can use multiple session representations, train on all at once

Deep Neural Networks

NETFLIX

100 titles
98.5% accuracy

YouTube

18 titles + 3500 sessions
of different other titles
99.5% accuracy

amazon instant video

10 titles
92.5% accuracy

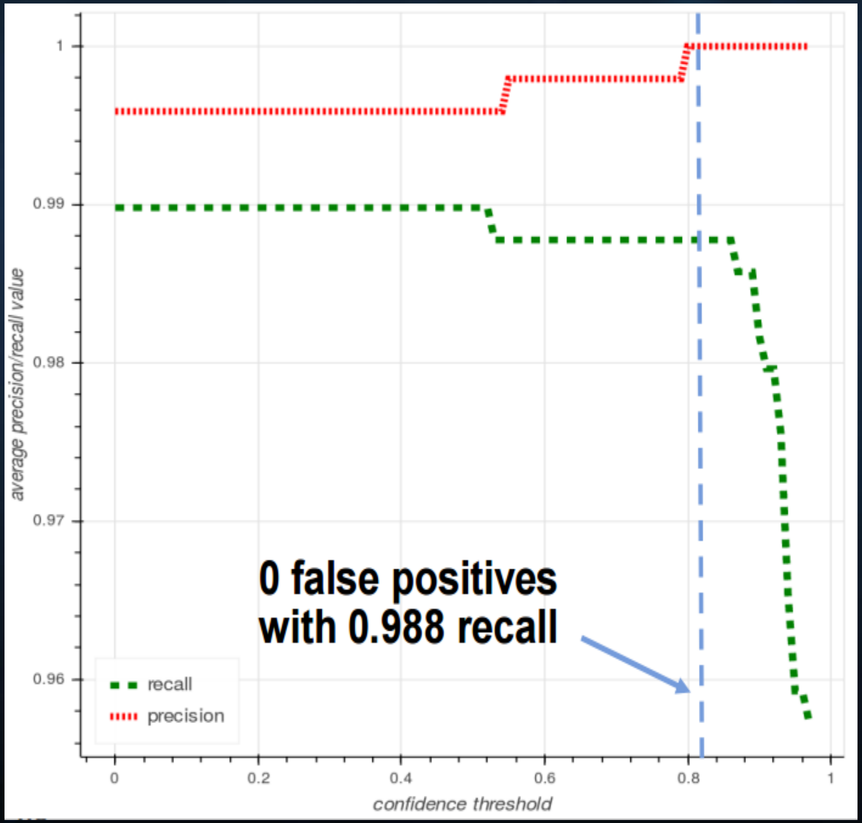
vimeo

10 titles
98.6% accuracy

Tuning for precision

YouTube

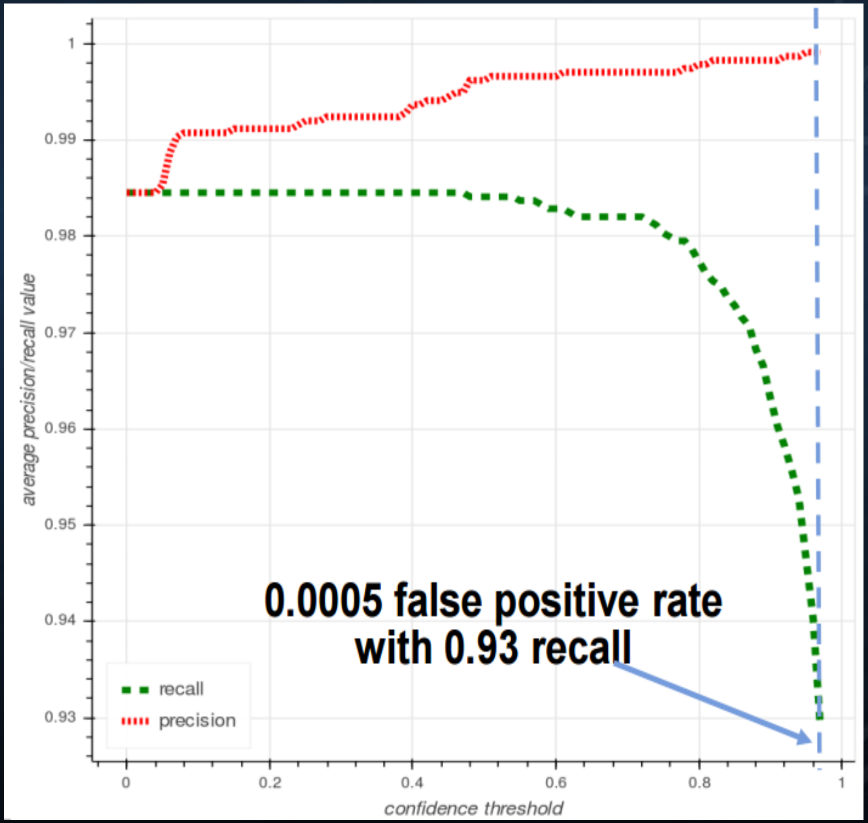
feature: total burst size



0 false positives with 0.988 recall

Netflix

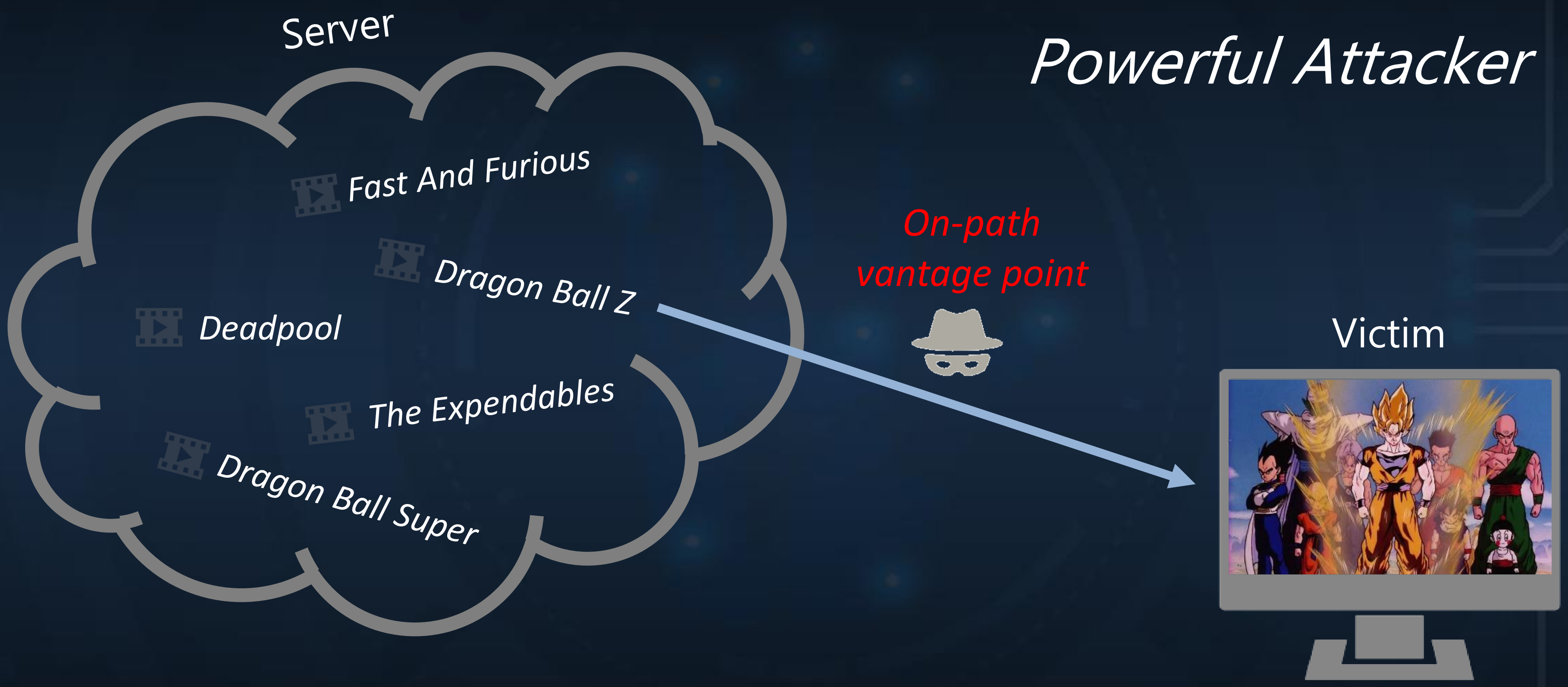
feature: total burst size



0.0005 false positive rate with 0.93 recall

So what is the vantage point ?

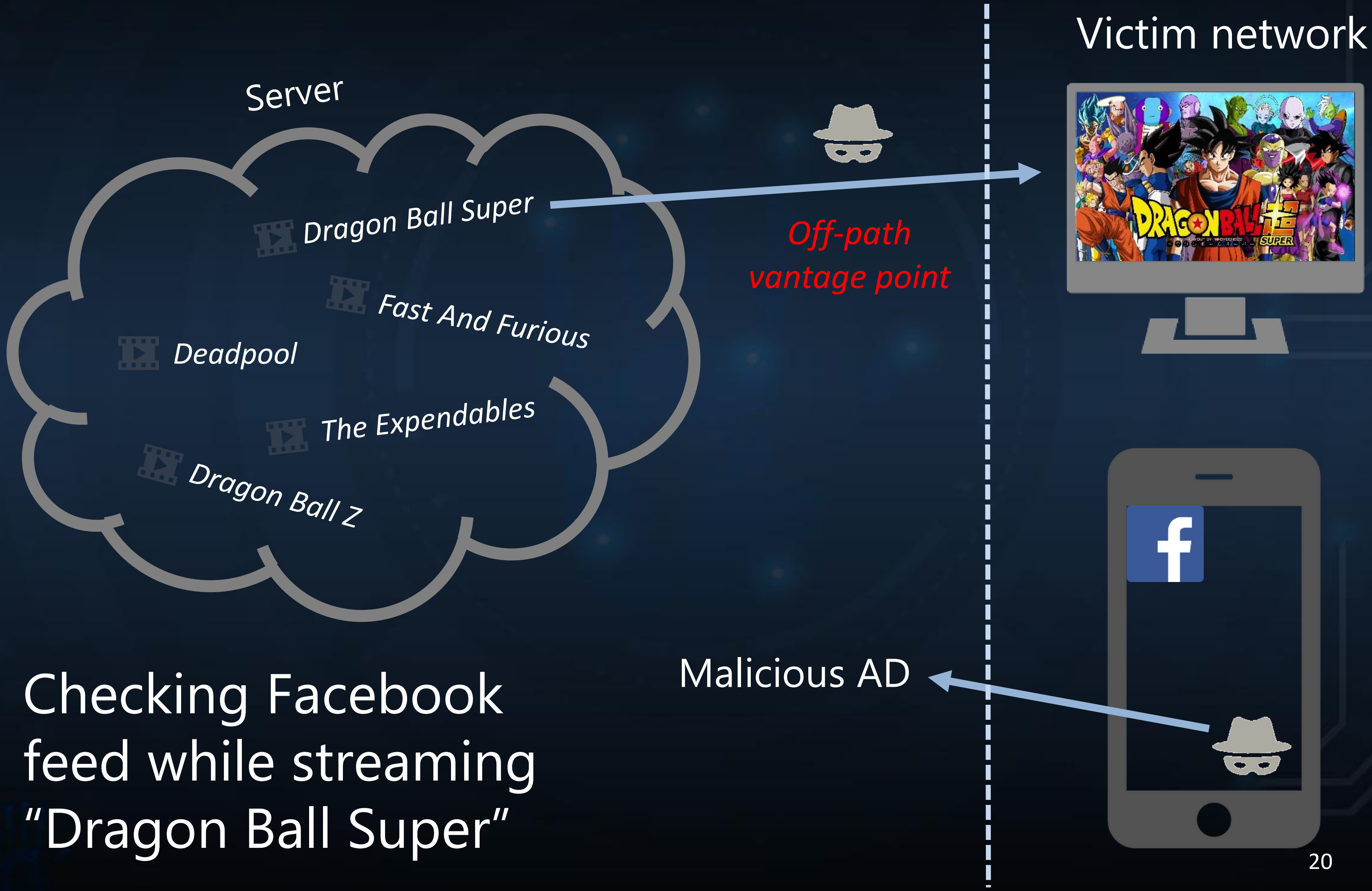
Scenario I: on-path attack



Powerful Attacker

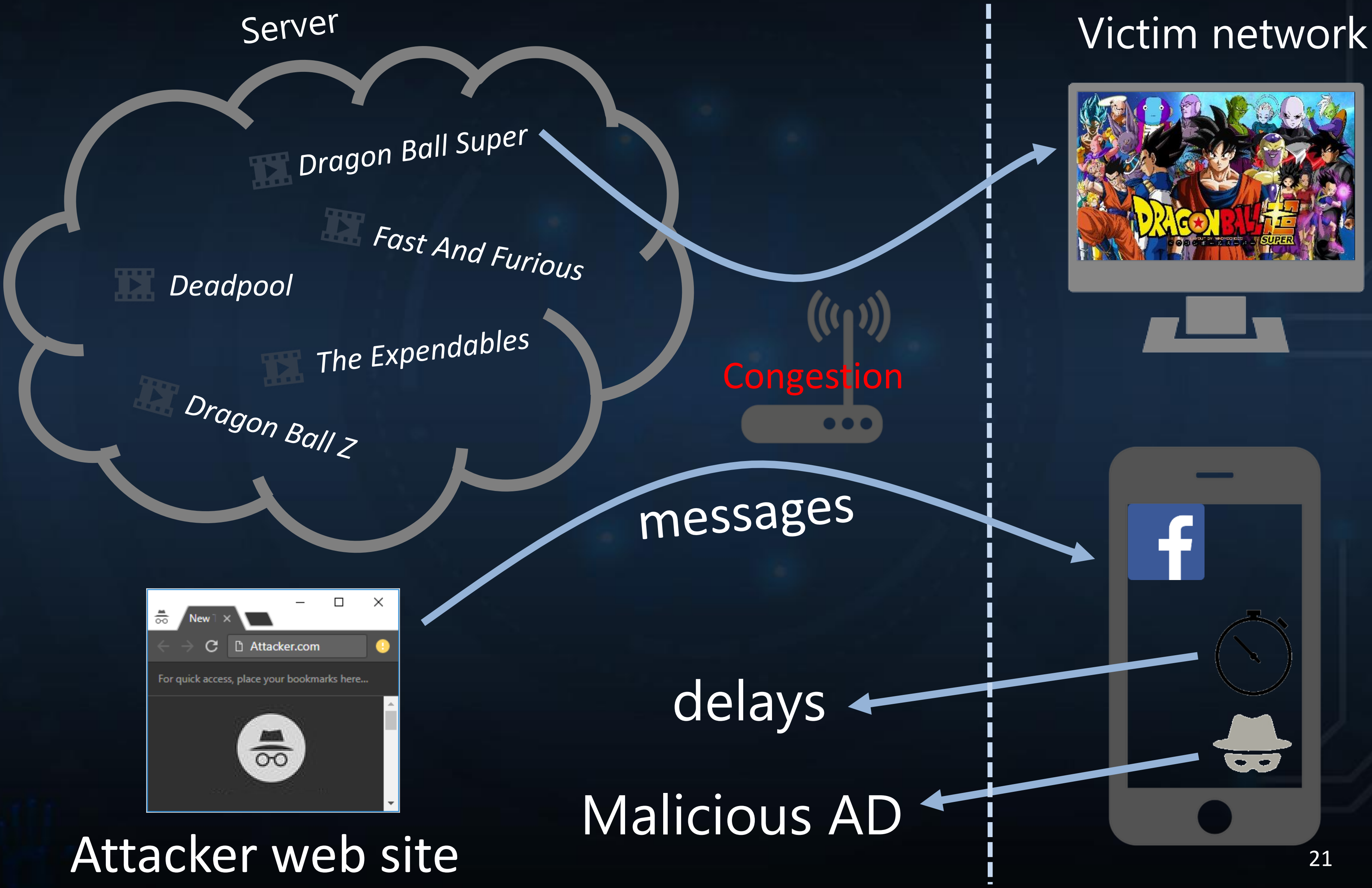
Wi-Fi access points, proxies, routers, enterprise or national network censors, ISPs

Scenario II: off-path attack



Checking Facebook feed while streaming "Dragon Ball Super"

Cross-device attack



Server

Dragon Ball Super

Fast And Furious

Deadpool

The Expendables

Dragon Ball Z

Congestion

Victim network

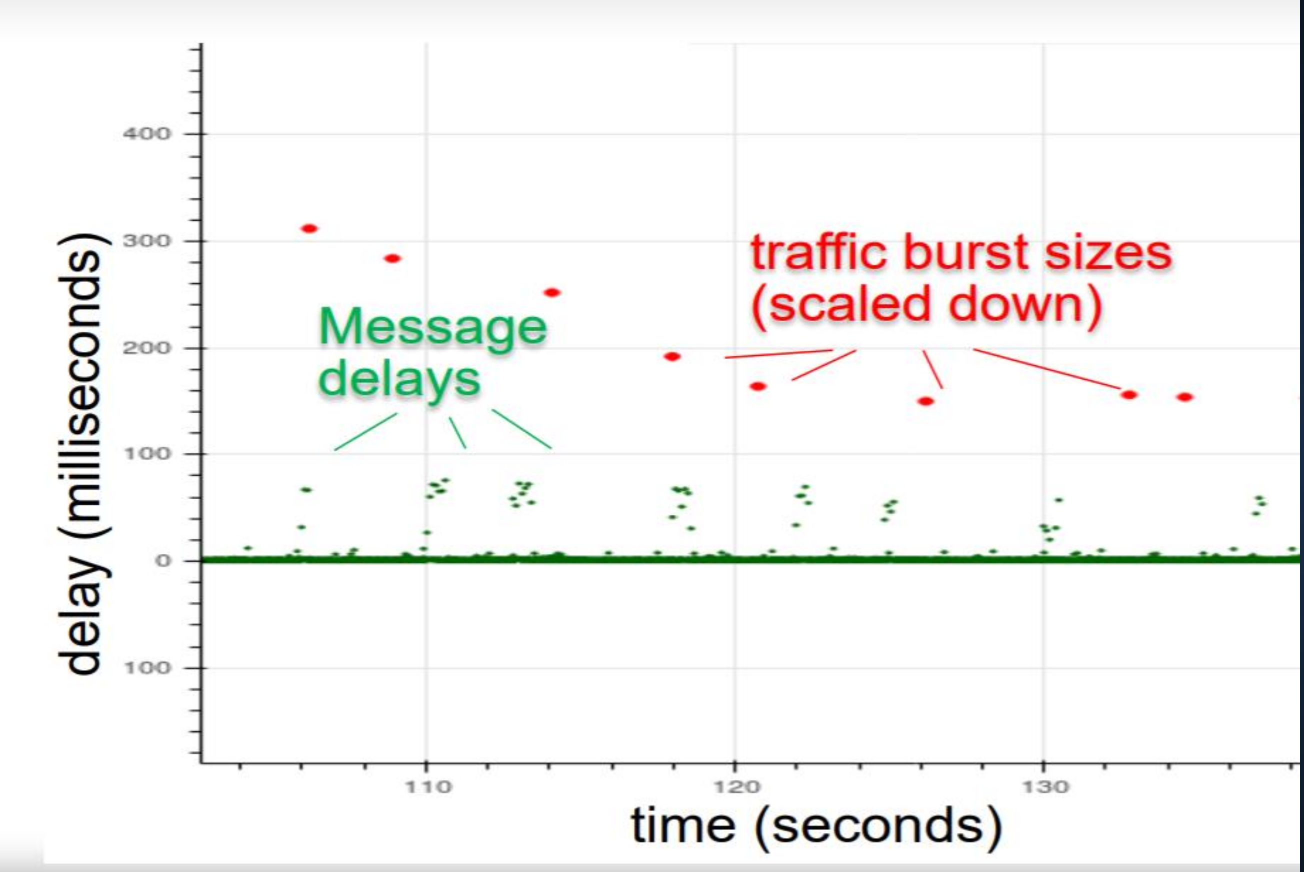
messages

delays

Malicious AD

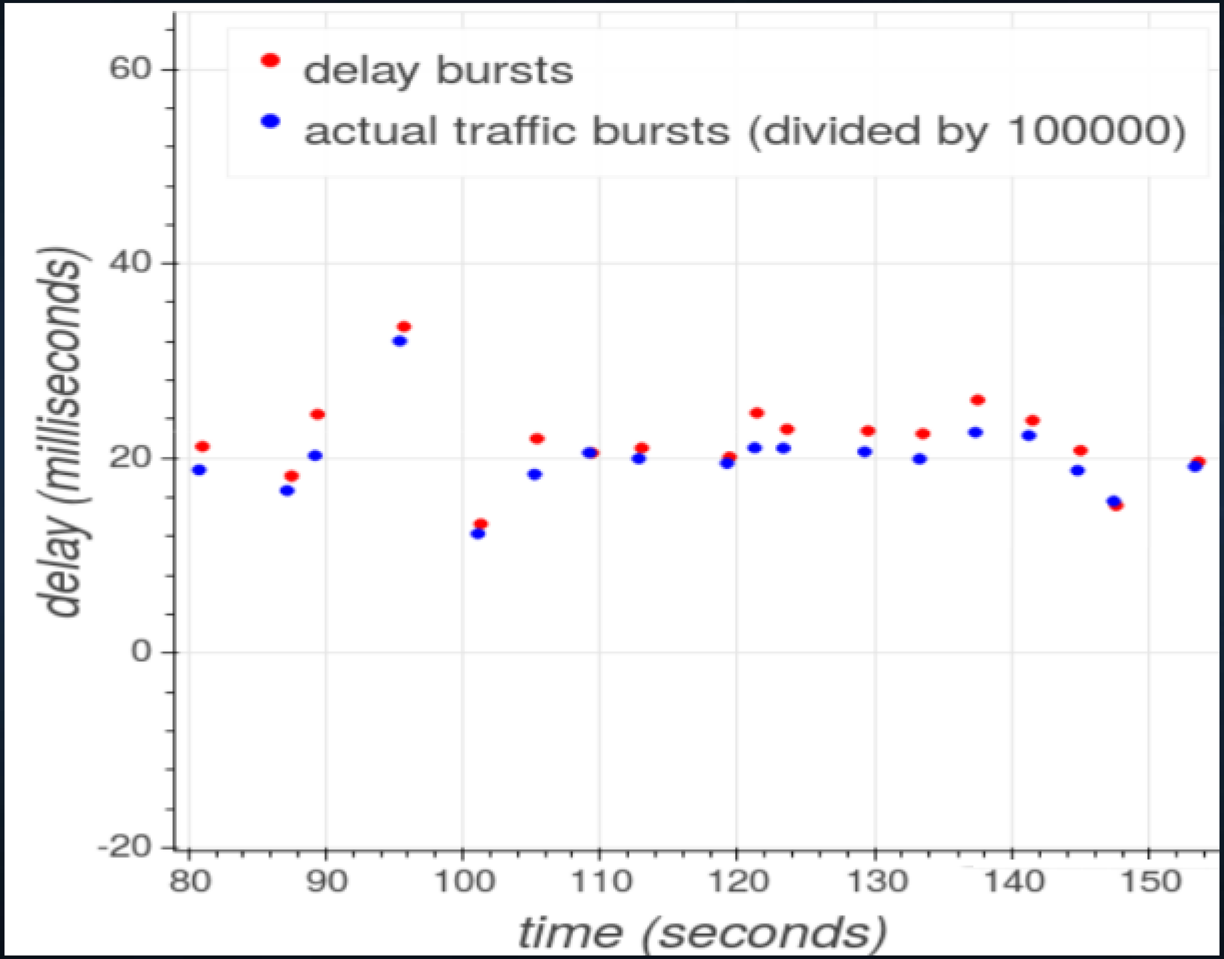
Attacker web site

Delay-bursts



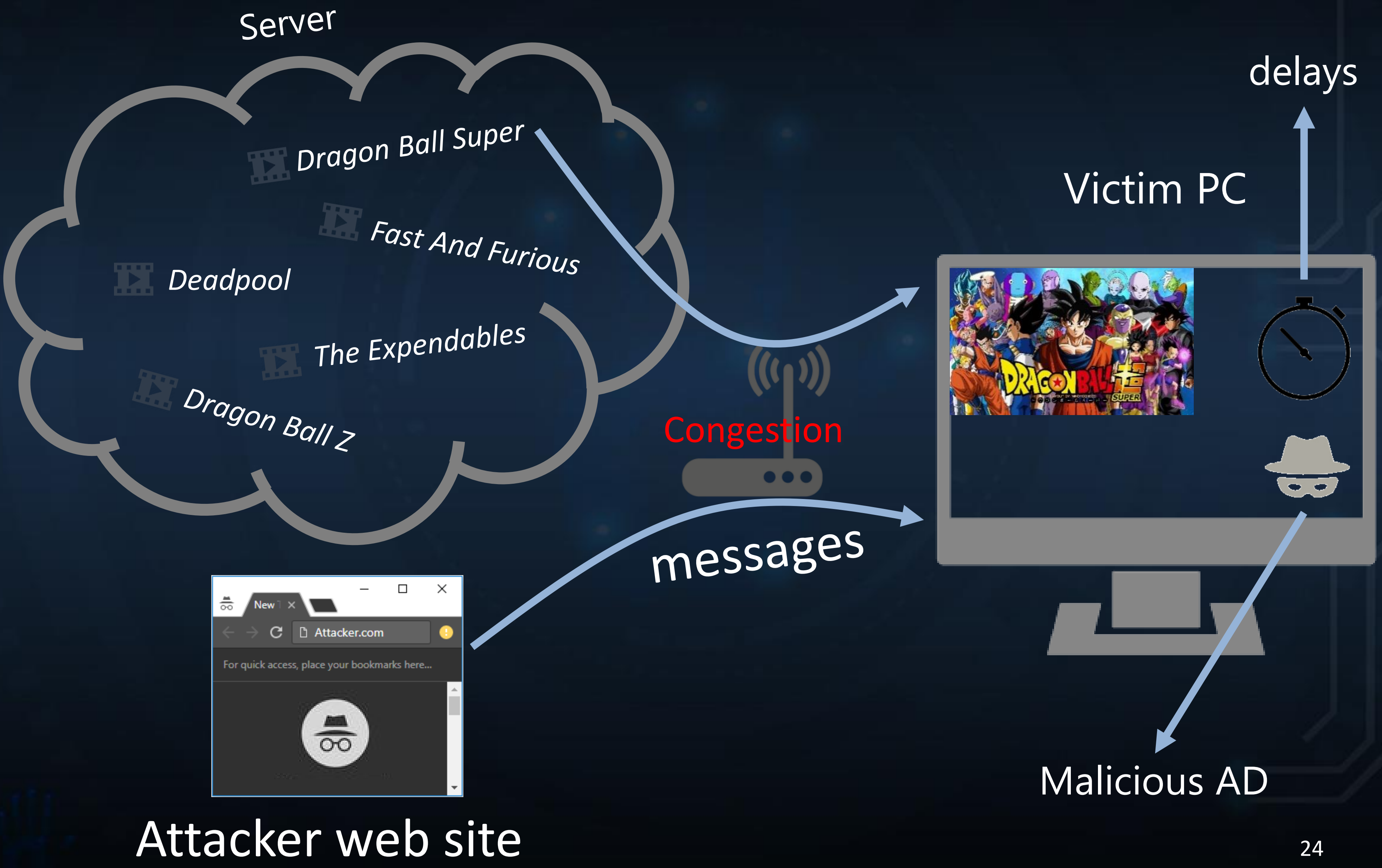
For each traffic burst, compute aggregate delay induced
Use resulting time-series as input to neural network

Delay-bursts VS. Traffic-bursts



Delay-bursts time series: the delays induced by traffic bursts

Cross-site attack



Mitigating the MPEG-DASH leak

- Modern streaming traffic characteristics
  - Title bitrate pattern unique when sampled at few-seconds granularity
  - Fetching at segment granularity (every few seconds)
- Maximizes quality of experience (QoE), server load, and network bandwidth utilization
- However, information leakage is intrinsic…

Conclusions

- Leakage of information about video content via network traffic patterns is prevalent in modern streaming protocols and popular services
- Detectors are tuned for high accuracy and effective in an "open-world" setting
- It can be used by on-path adversaries such as ISPs to spy on their users
- It can be used by off-path adversary who merely serves a Web page to identify videos being streamed by the user

Thank You !

- Further information and the paper: https://beautyburst.github.io/

“Everything has a fingerprint,
and so do encrypted streams”

Any Questions?