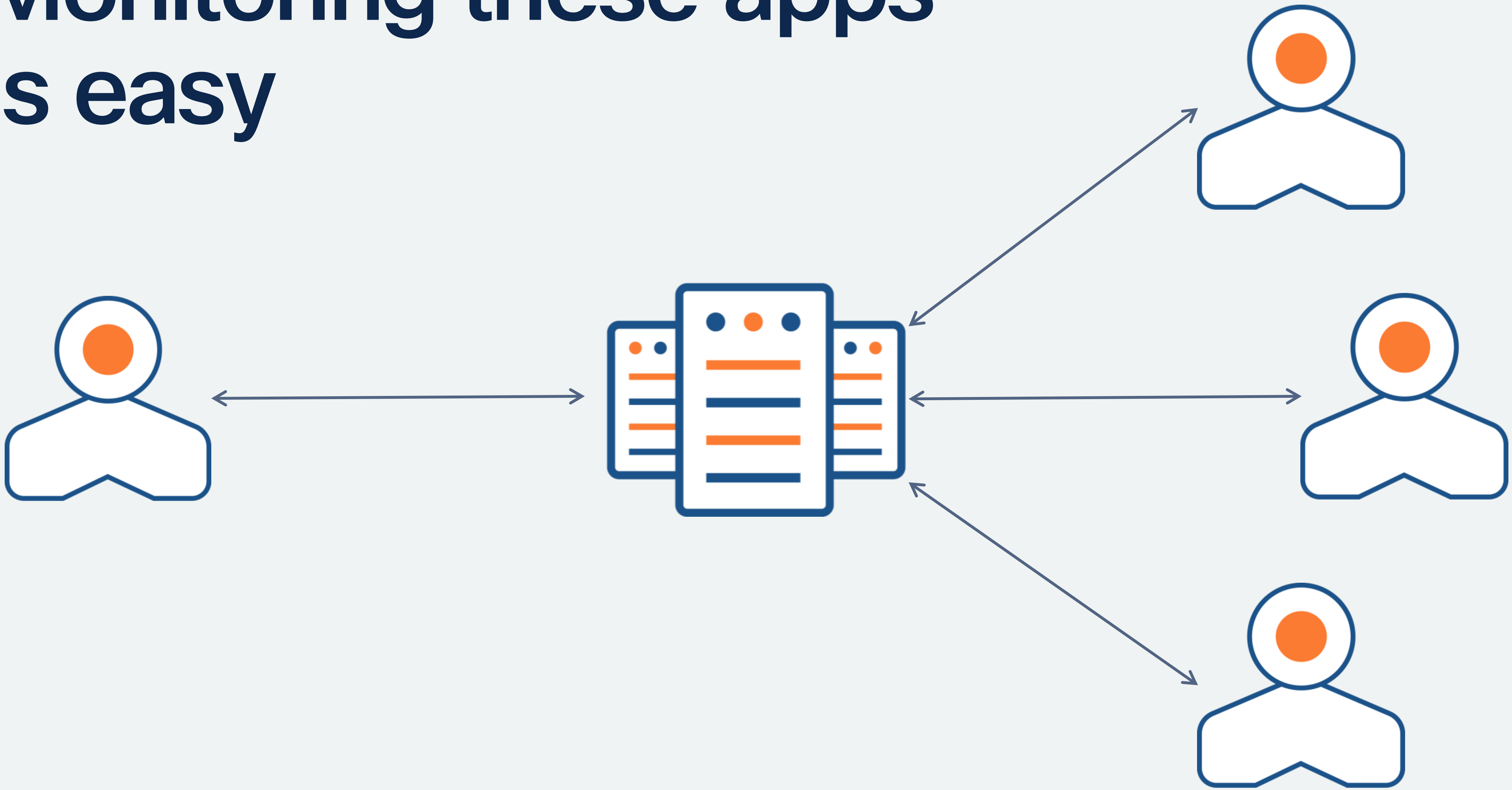
Lost in encryption: monitoring media flows without payload in video conferencing apps

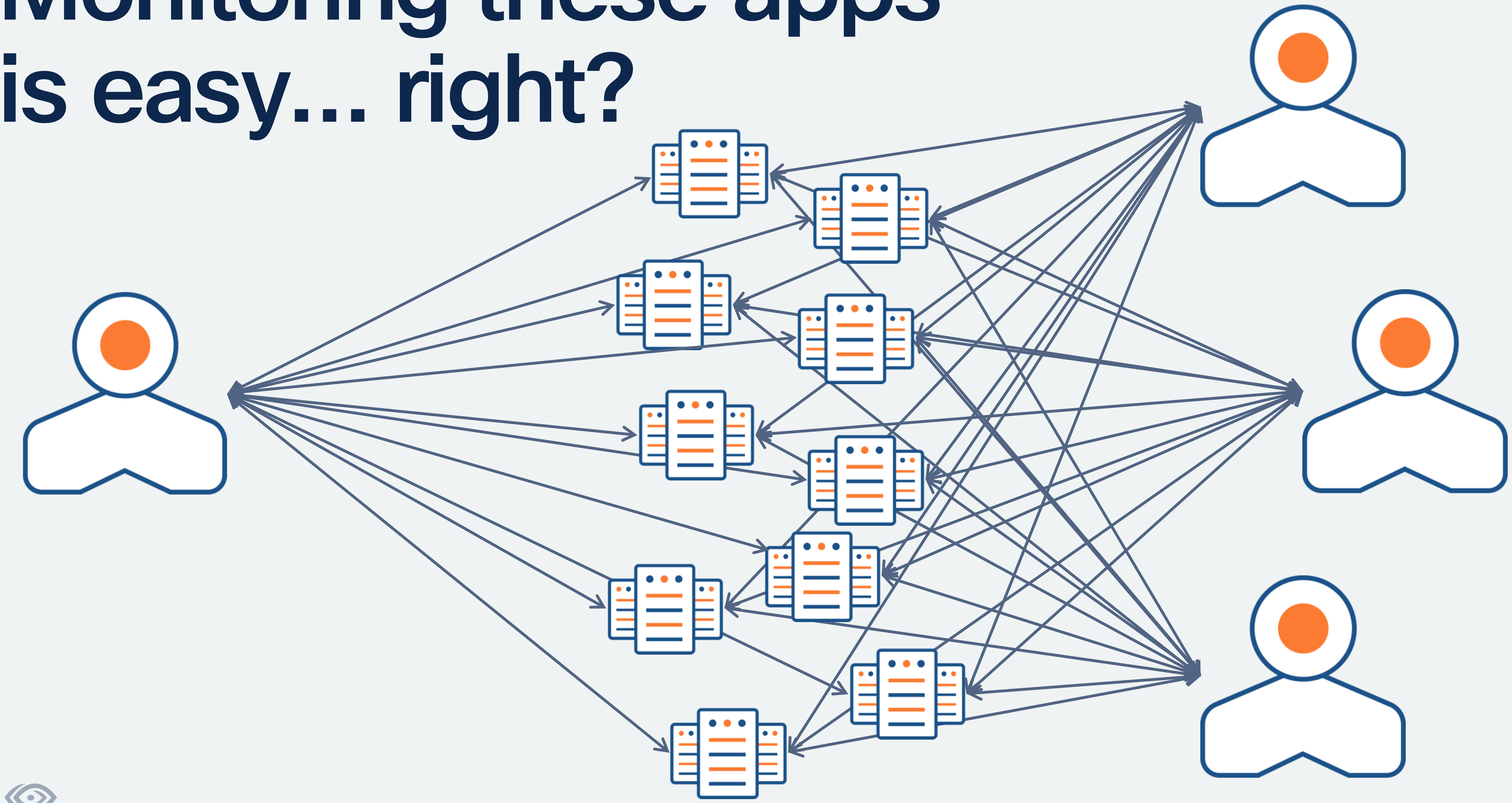
Julien Gamba | Cisco ThousandEyes

Video conferencing apps are everywhere

Monitoring these apps is easy



Monitoring these apps is easy… right?

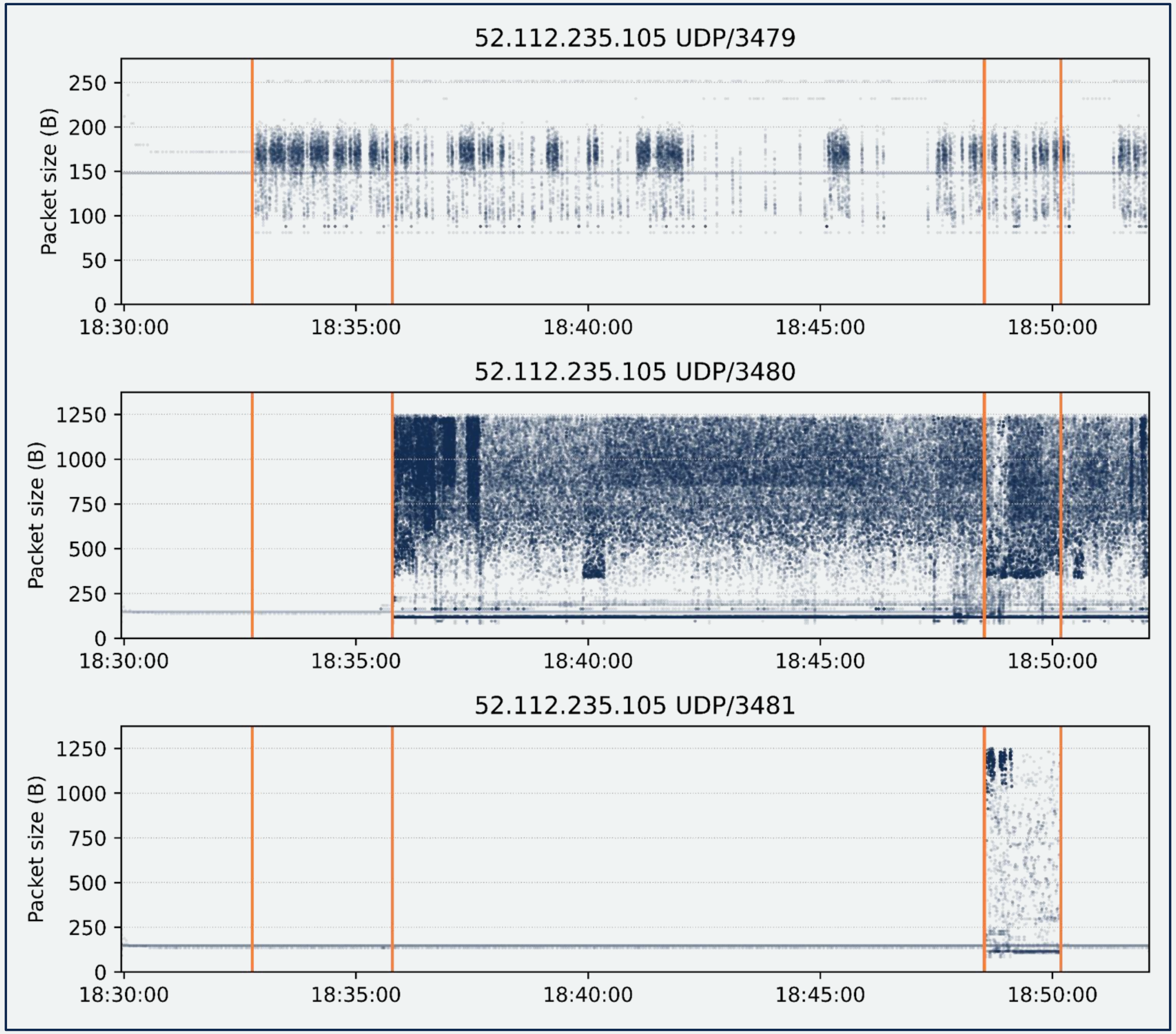


It gets worse

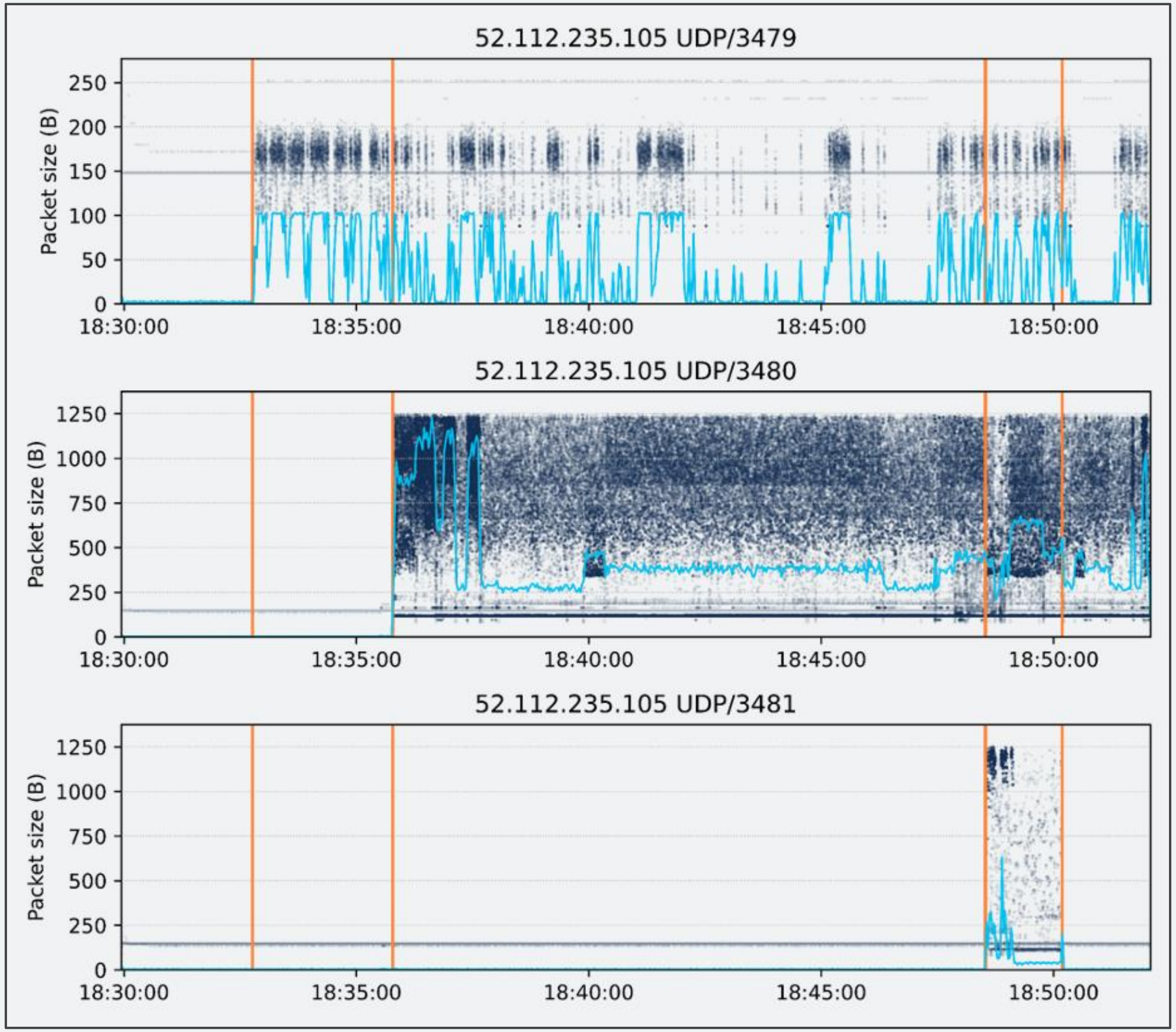
- We monitor from the client and have no access to RTP headers
- … or the full IP/UDP headers
- … we only have a 5-tuple and packets timing information

Identifying media flows

Let's look at the traffic

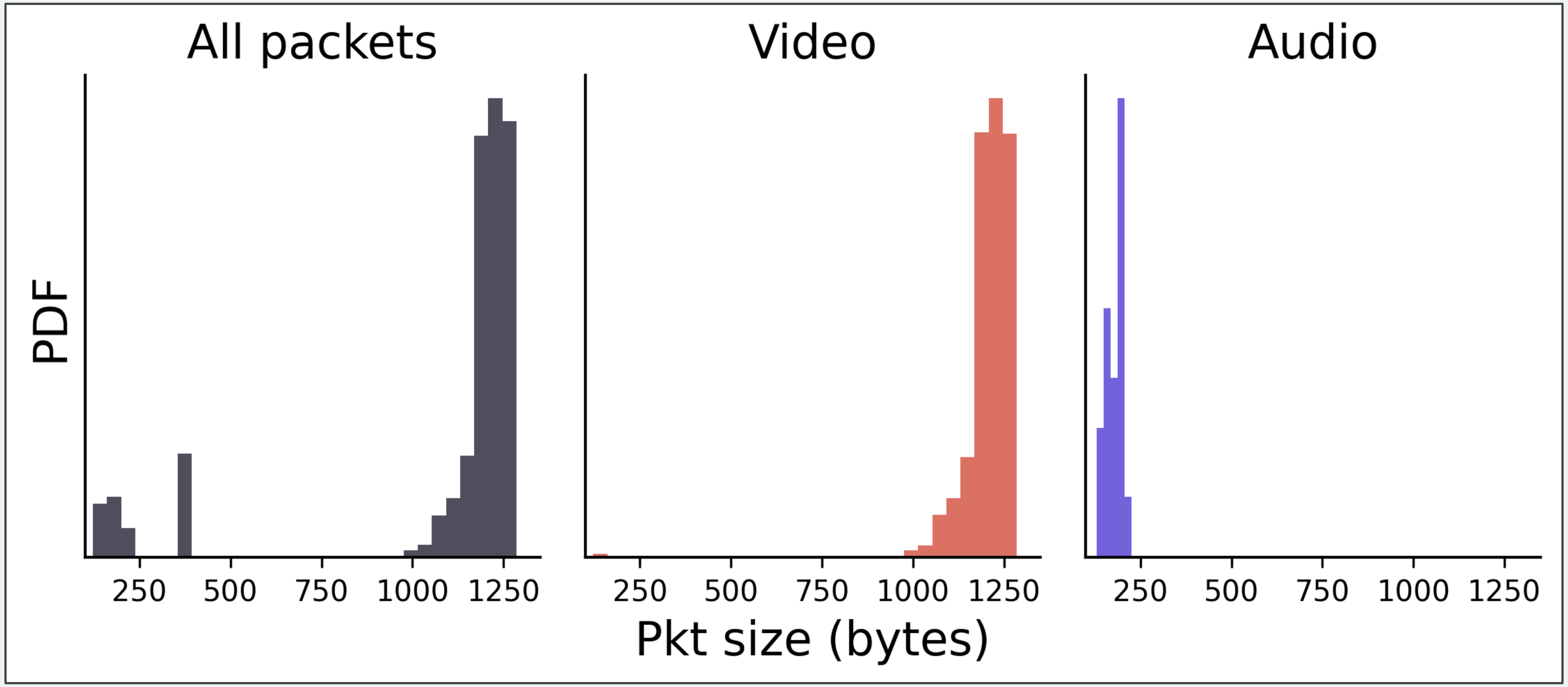


Let’s look at the traffic



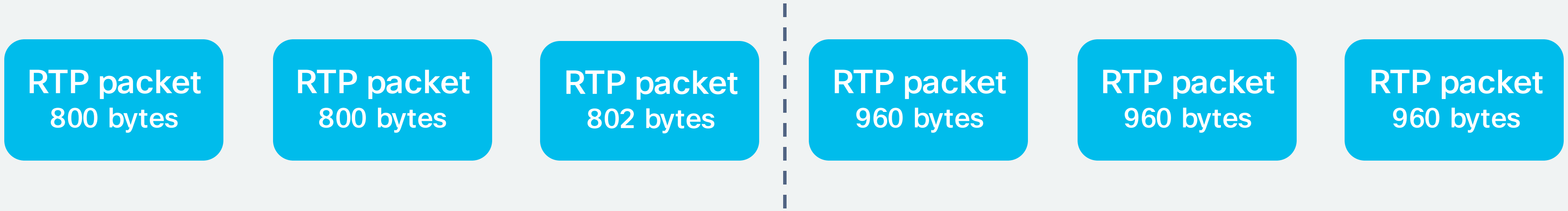
What else can we monitor this way?

Classifying media types

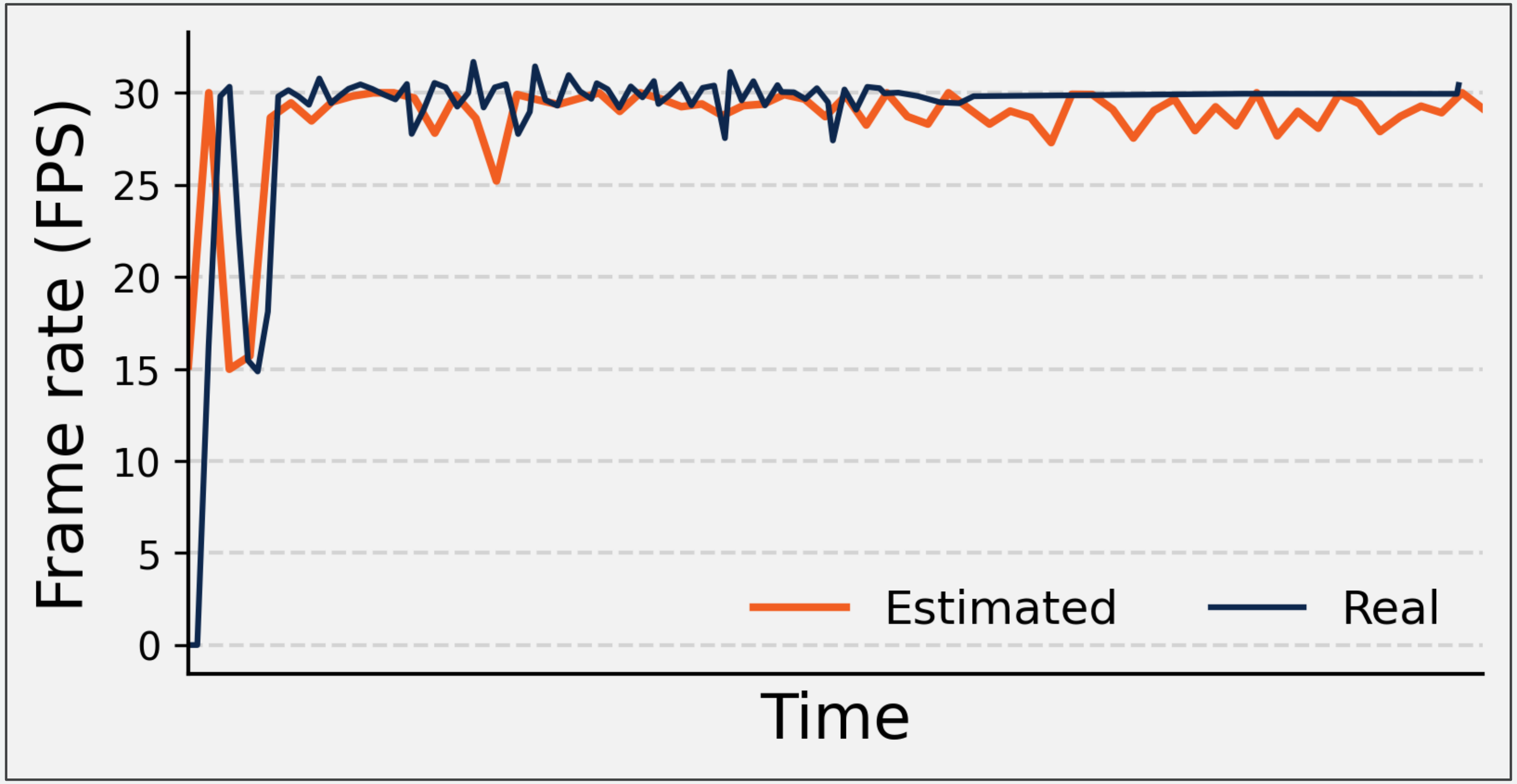


Passively identifying frames boundaries

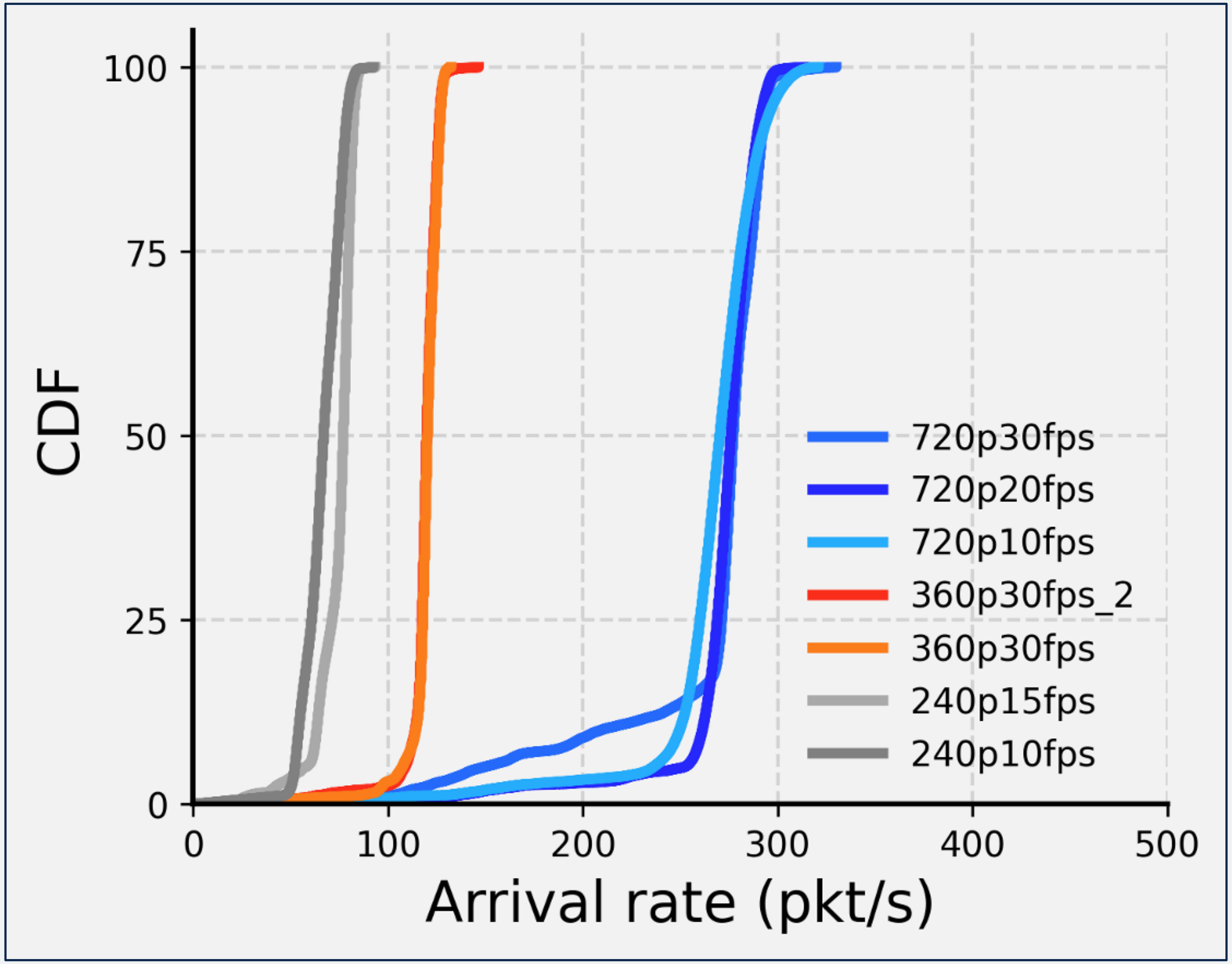
- Frames are usually too big to fit into one packet
- Packets of the same frame will have very similar sizes
- … but consecutive frames will not



Measuring the frame rate



Measuring video resolution



In summary

- We can detect media flows with only a 5-tuple and packet timing information

- We can monitor frame rate and video resolution completely passively

- Detection and monitoring happen completely on the client side with minimal impact on battery life