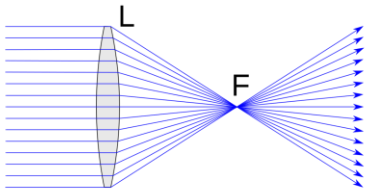
Temporal CDN-Convex Lens
A CDN-Assisted Practical Pulsing DDoS Attack

Run Guo, Jianjun Chen, **Yihang Wang**, Keran Mu, Baojun Liu, Xiang Li
Chao Zhang, Haixin Duan, Jianping Wu



清華大學 Tsinghua University

奇安信 新一代网络安全领军者

中关村实验室 ZGC Lab

Outlines

- **Background**
- Attacks
- Mitigations
- Conclusion

A warm-up wargame

Limited Attack Capability

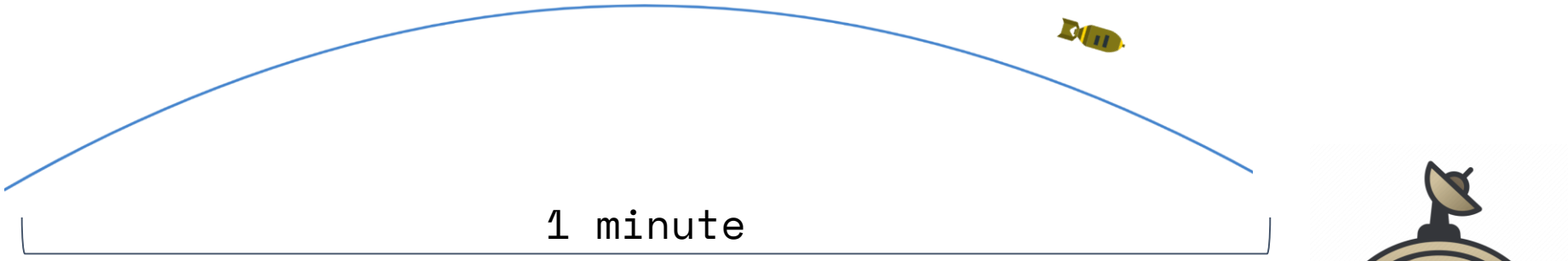
- 1 artilleries
- 1 shell per minute per unit

Defense Capability

- **Blast Resistance**
  - < 5 shells within 1 minute

1 shells “at max” within 1 minute

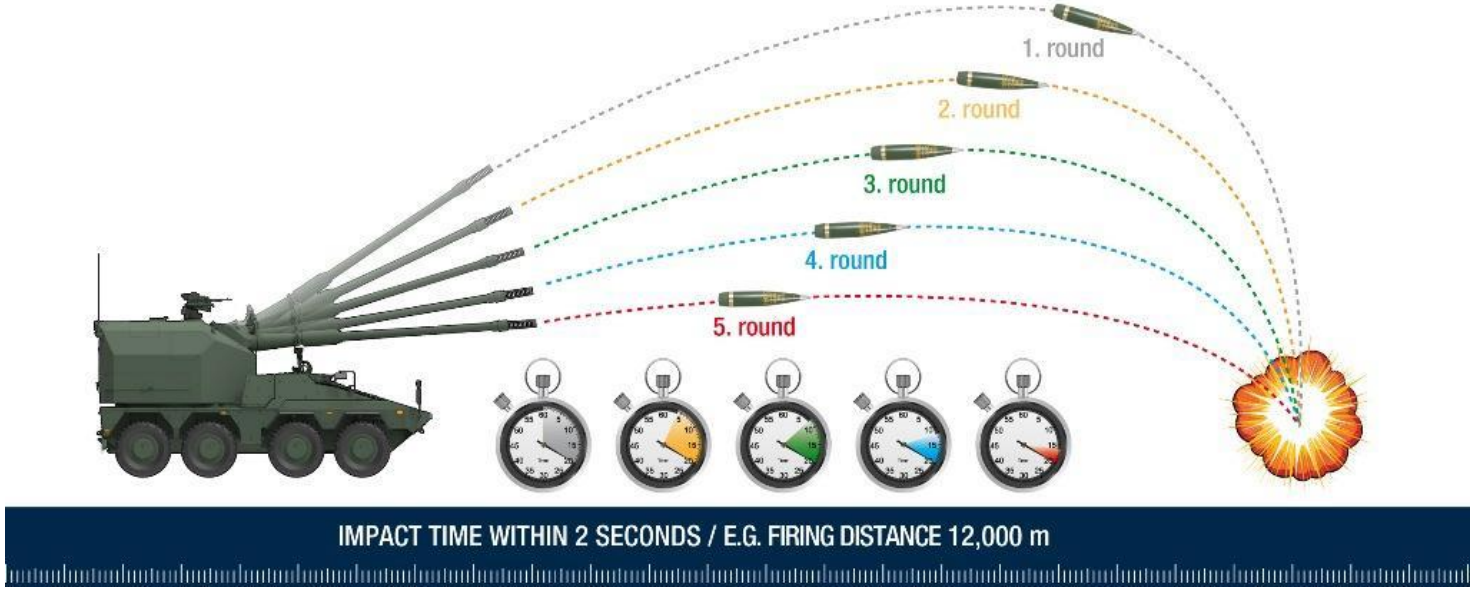
if **all** artilleries fire at the same time

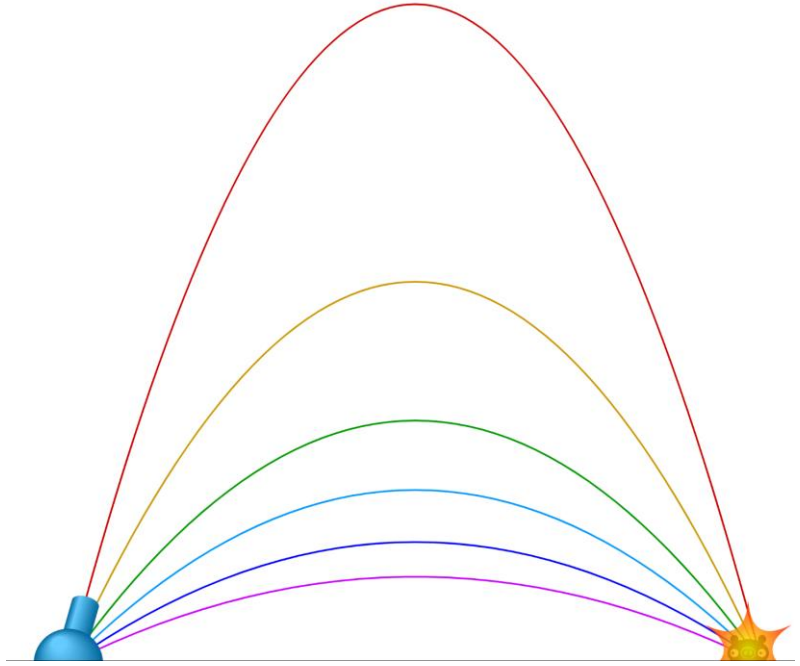


Mission Impossible ?

Multiple Round Simultaneous Impact (MRSI)

- MRSI is when a single gun fires multiple shells so all arrive at the same target **simultaneously**
- A variation of military tactic "Time on Target (TOT)" in World War I





Advantages of MRSI

Efficiency

- Attacker
  - just fire the shells slowly
- Victim
  - receive all shells instantly

Stealth

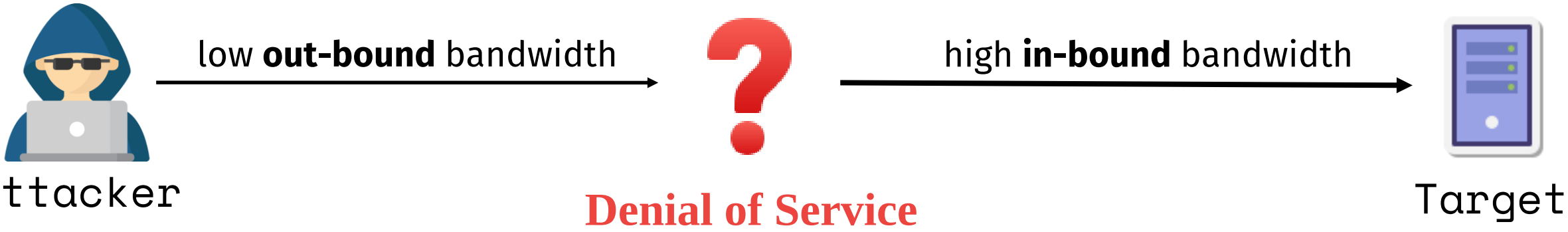
- Observe one of the attacker's artilleries alone, the rate of fire is pretty **low**
- The alarm won't be triggered

Prime Target

"Moments to go down, hours to recover"

When World War I meets the Internet

DoS a target with a **limited** bandwidth?



Previous Attack: Abusing **DNS** Infrastructure [1]

Properties	Value
Trajectories	≥ **Thousands** of Open DNS
Flight time of payload	≤ 700 milliseconds
Bandwidth Concentration Ratio	≈ **14**

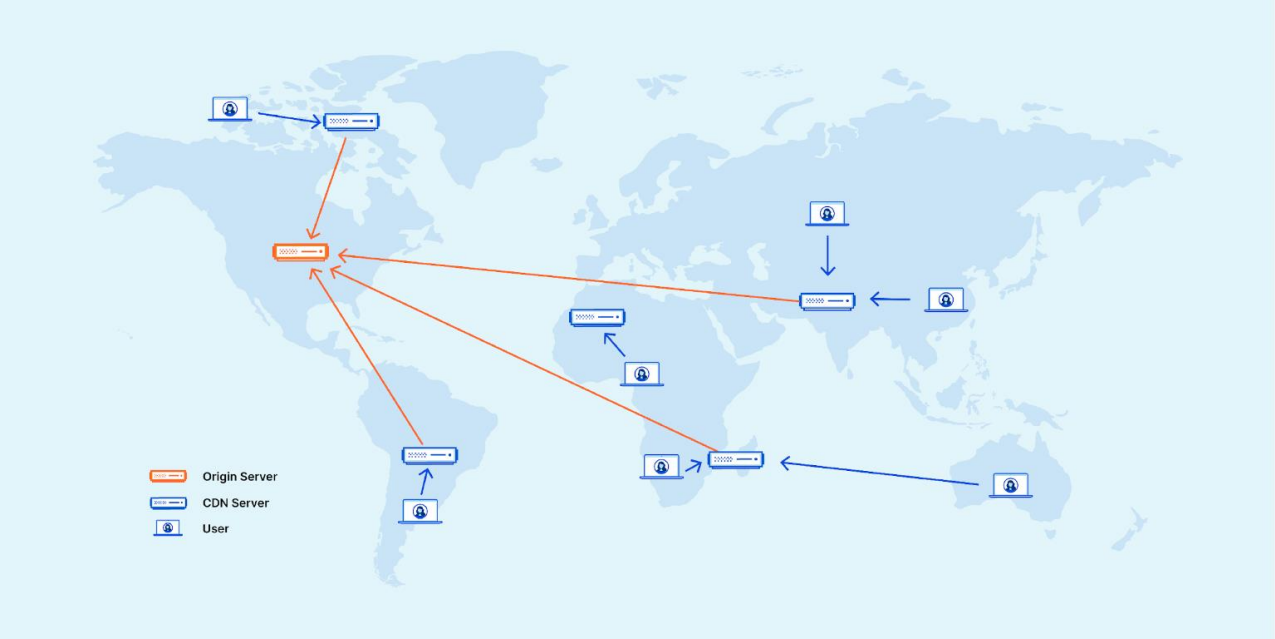
[1] R. Rasti, M. Murthy, N. Weaver, and V. Paxson, “Temporal Lensing and Its Application in Pulsing Denial-of-Service Attacks,” in 2015 IEEE Symposium on Security and Privacy, May 2015, pp. 187–198. doi: 10.1109/SP.2015.19.

Our Work: CDN-Convex Lens Attack

Properties	Value
Trajectories	≥ **Millions** of CDN edge servers
Flight time of payload	≥ **5,400,000** milliseconds
Bandwidth Concentration Ratio	≥ **1000**

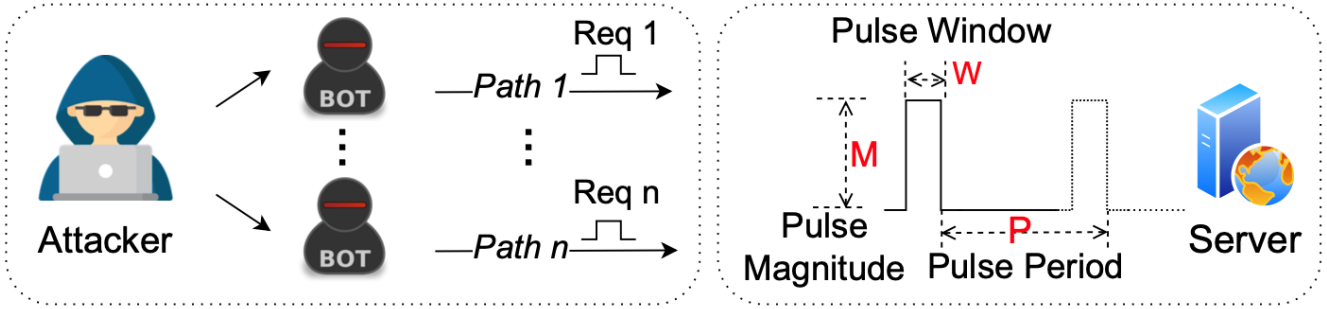
What is a Content Delivery Network (CDN)?

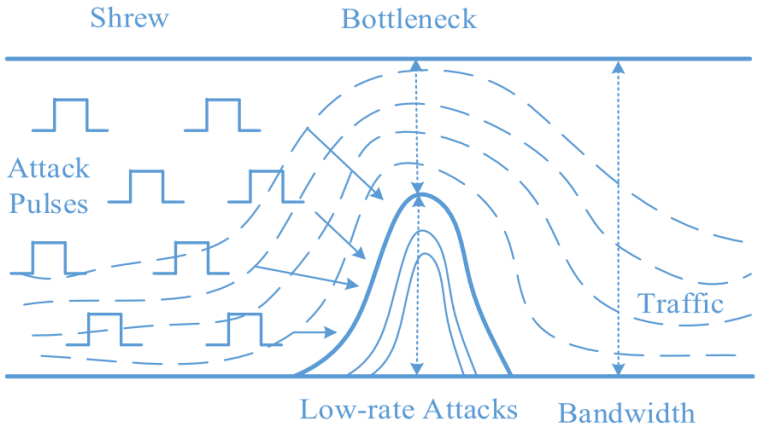
- **Globally Distributed:** **a large volume of servers** on Internet backbone
- **Cache then Forward:** act as the **Reverse Proxy** to the website
- **Proxy Service:** redirect the user's request to the **nearest** server
- **DDoS Protection:** **off-load traffic** from botnet-based DDoS attack



What is a Pulse Wave DDoS attack?

- **Efficiency**: Periodical Saturation of Bottleneck Resources
- **Stealthy**: High-rate, short-lived bursts
- **Unusual on Internet**
  - Require a botnet
  - Botnet is preferably used to launch simple flooding attack

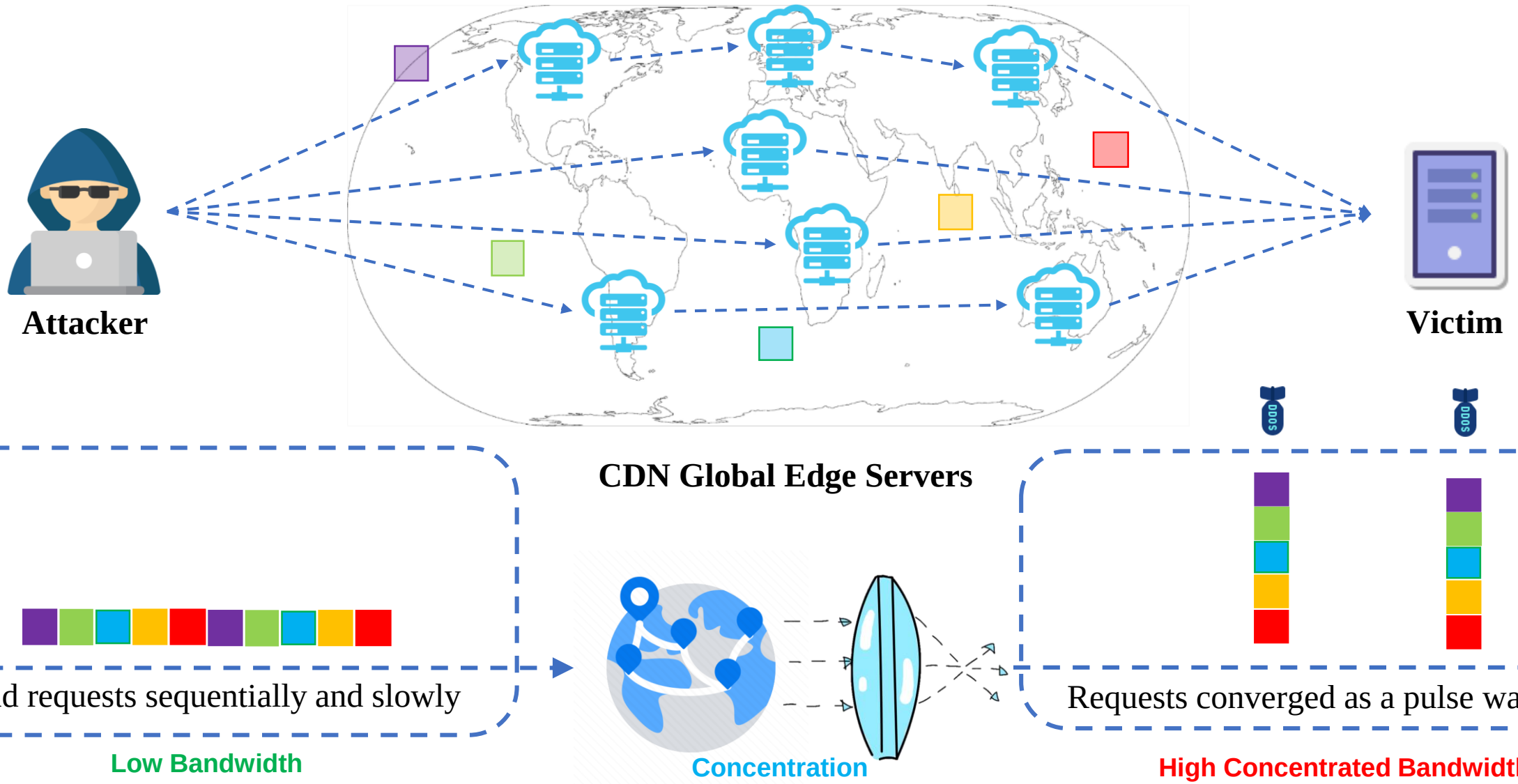




Outlines

- Background
- **Attacks**
- Mitigations
- Conclusion

Concept of CDN-Convex Lens Attack

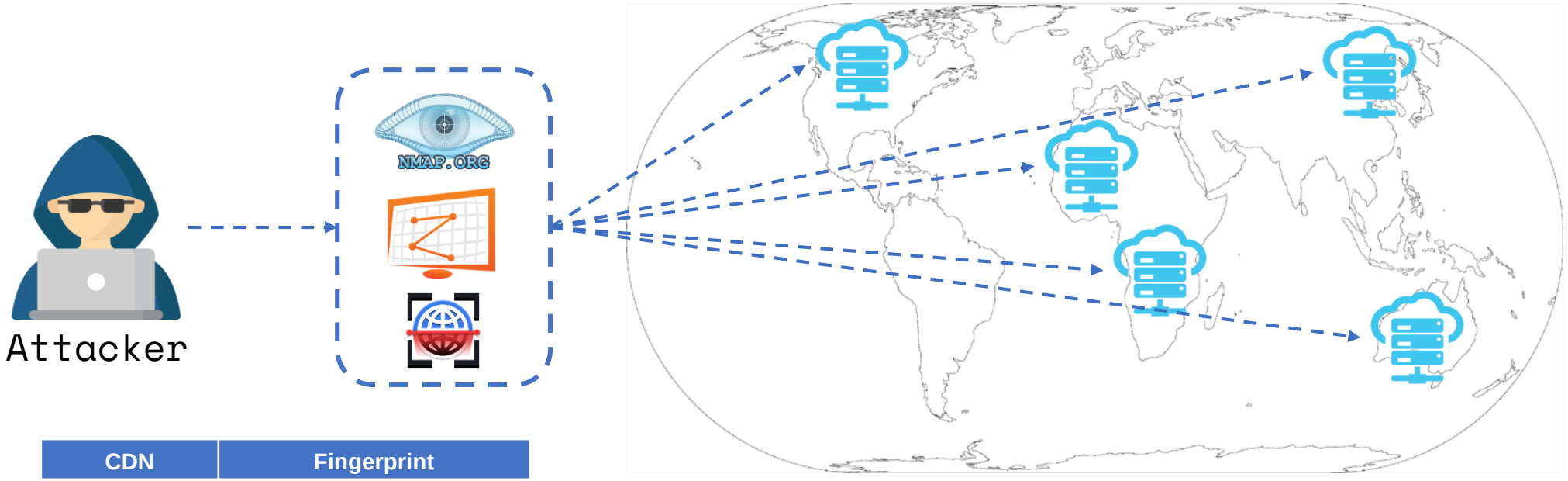


Attack Steps

- **Step I**: CDN Node Harvest
- **Step II**: Configure CDN to Point to the Victim
- **Step III**: Measure the flight time (latency)
- **Step IV**: Bypass the cache mechanism
- **Step V**: Send the requests on time

Step I: CDN Node Harvest

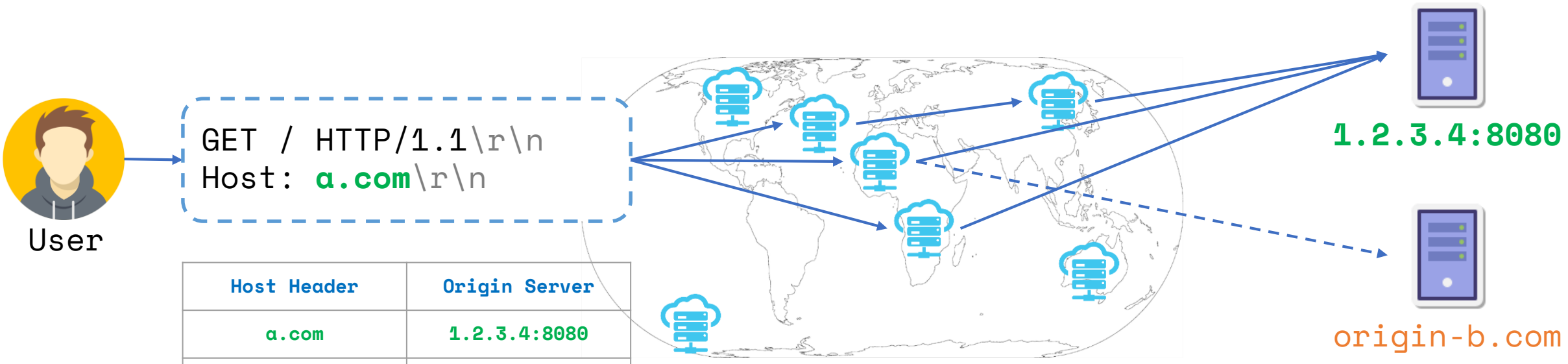
- collect IP addresses of global CDN edge servers by
  - Internet-wide **scanning** / **fingerprinting**



CDN	Fingerprint
Cloudfront	X-Amz-Cf-Id
Cloudflare	Cf-Cache-Status
FrontDoor	X-Azure-Ref
…	…

CDN Edge Servers can be abused by the Attacker

- Tons of edge servers **can be abused** by the attacker
  - CDN edge servers are allowed to forward HTTP requests with a **valid host header**

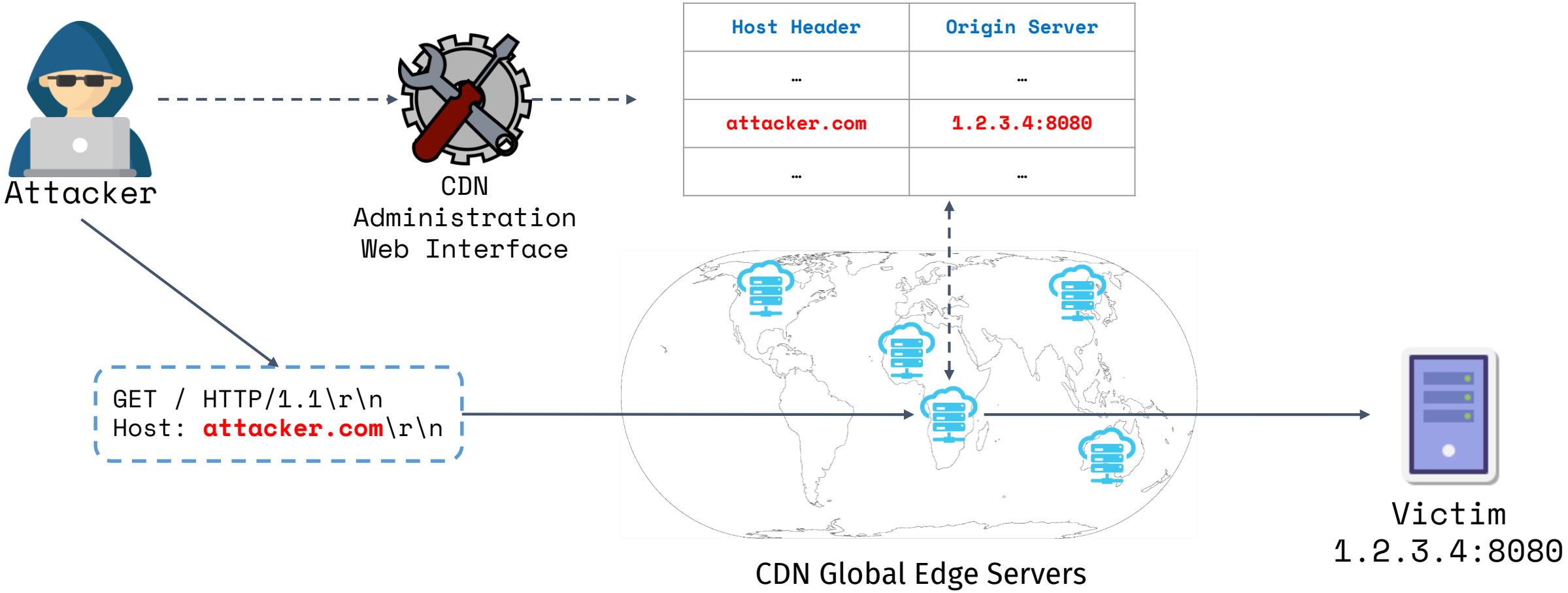


Host Header	Origin Server
a.com	1.2.3.4:8080
b.com	origin-b.com
…	…

CDN Internal Forwarding Tables

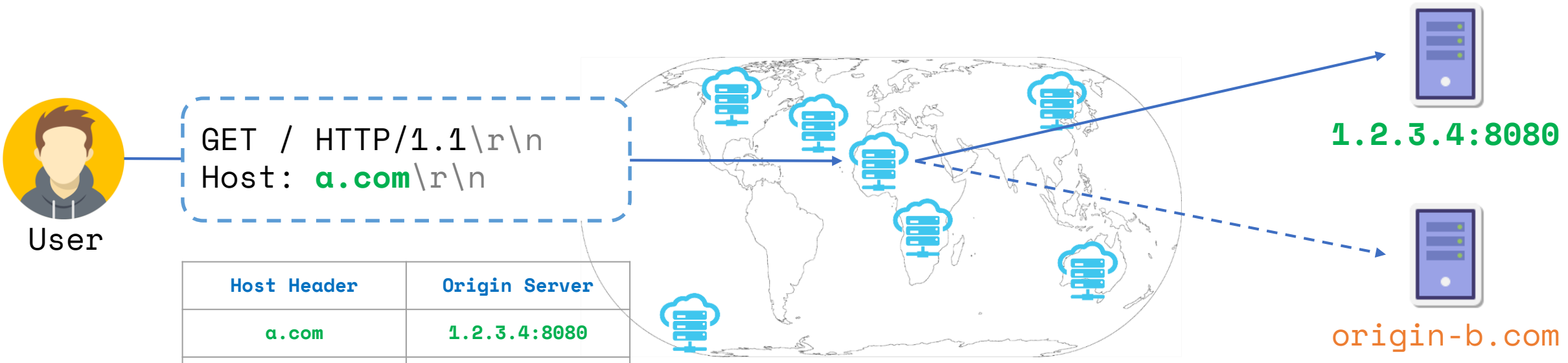
Step II: Configure CDN to Point to the Victim

- **Register** CDN services, then **config** the victim website as a origin server



CDN Lacks of Origin Ownership Verification

- CDN **lacks of ownership verification** for the Origin Server
  - CDN can be configured to fetch resource from any IP and any port

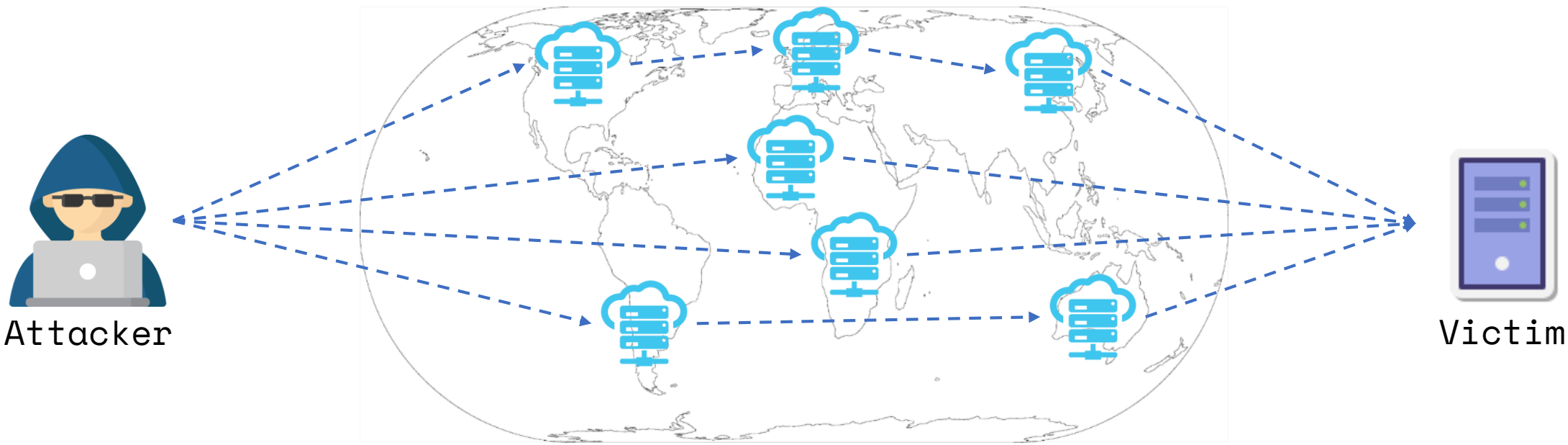


Host Header	Origin Server
a.com	1.2.3.4:8080
b.com	origin-b.com
…	…

CDN Internal Forwarding Tables

Step III: Measure the flight time (latency)

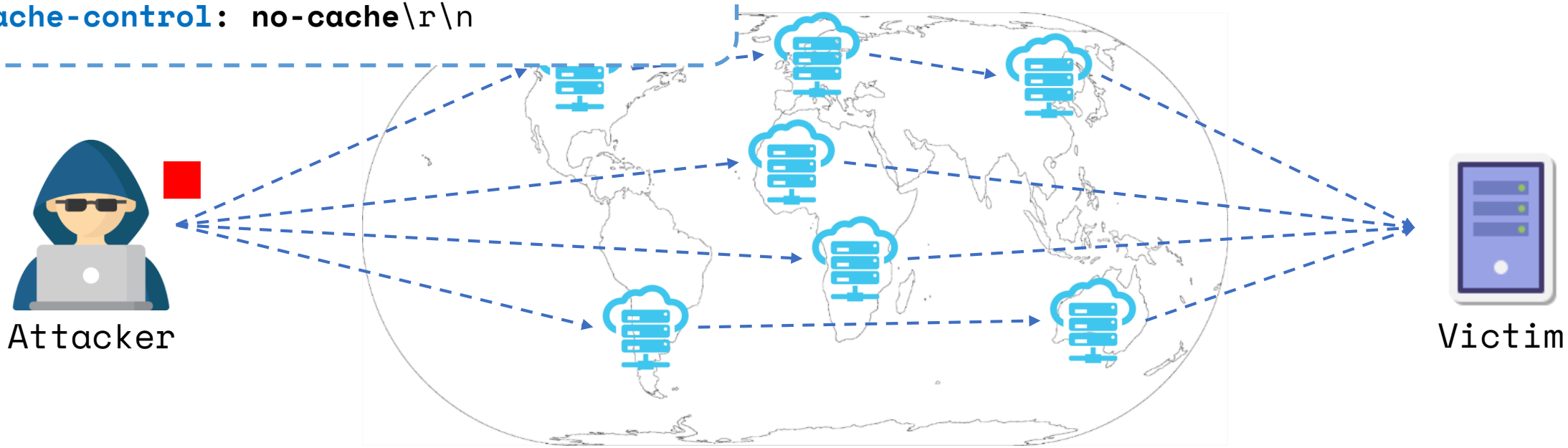
- **Measure latencies** of CDN forwarding paths and filter stable ones



Step IV: Bypass CDN cache mechanism

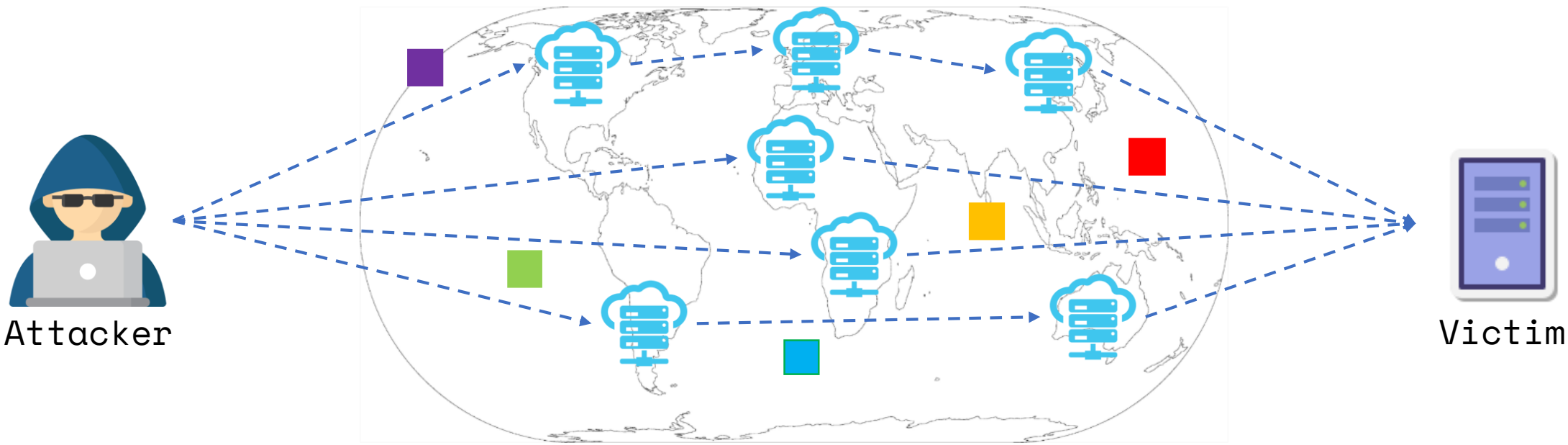
- Craft request to **bypass CDN cache** and saturate the bottleneck resources

```
POST /bottleneck.php?nonce HTTP/1.1\r\n
Host: victim.com\r\n
Cache-control: no-cache\r\n
```



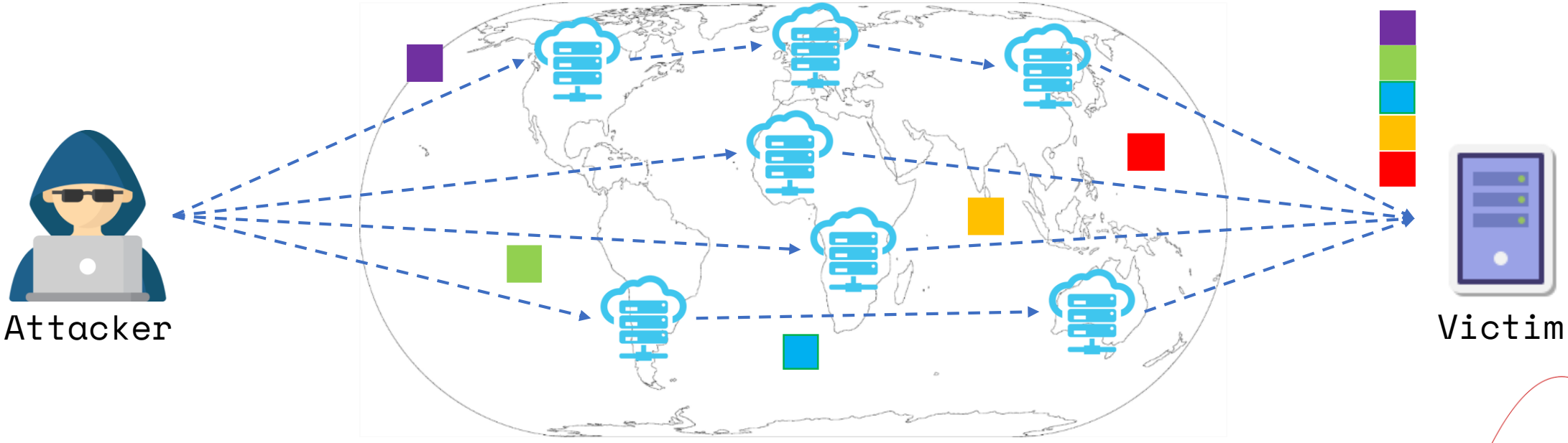
Step V: Send the requests on time

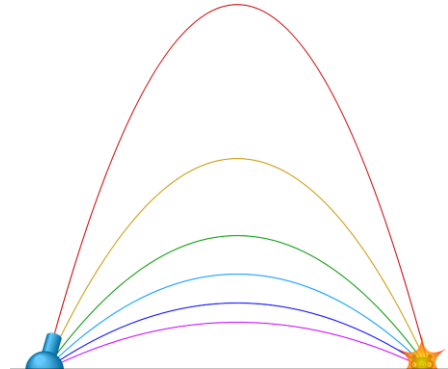
- **Send low rate of the HTTP requests** in accord with path latencies



The Pulsing-Wave is Coming!

- Requests **converged** as a **high-rate**, **short-lived** pulse burst to saturate target



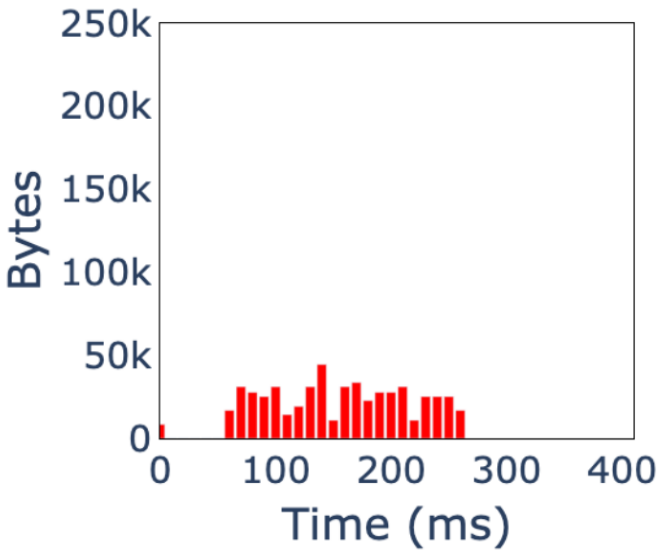


Result of the Basic CDN-Convex Attack

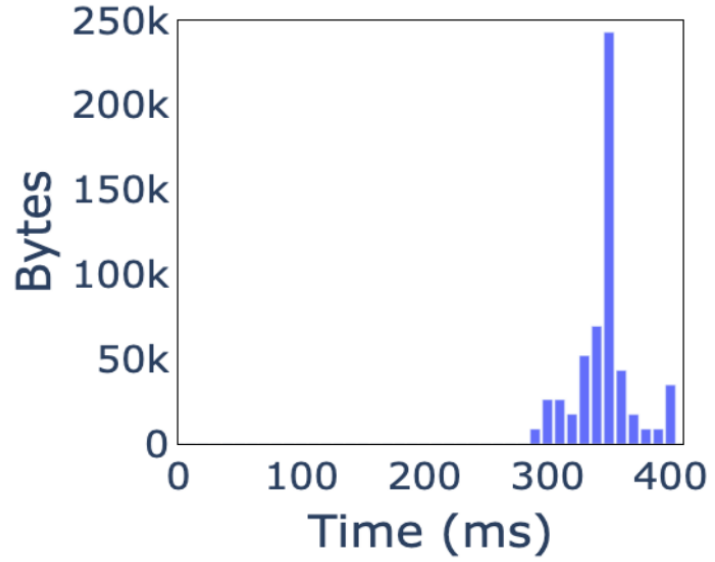
Core Concept
Use native path latency
to arrange all HTTP requests

Max Bandwidth Concentration Ratio
~ 6

Attack's **out-bound** bandwidth



Victim's **in-bound** bandwidth



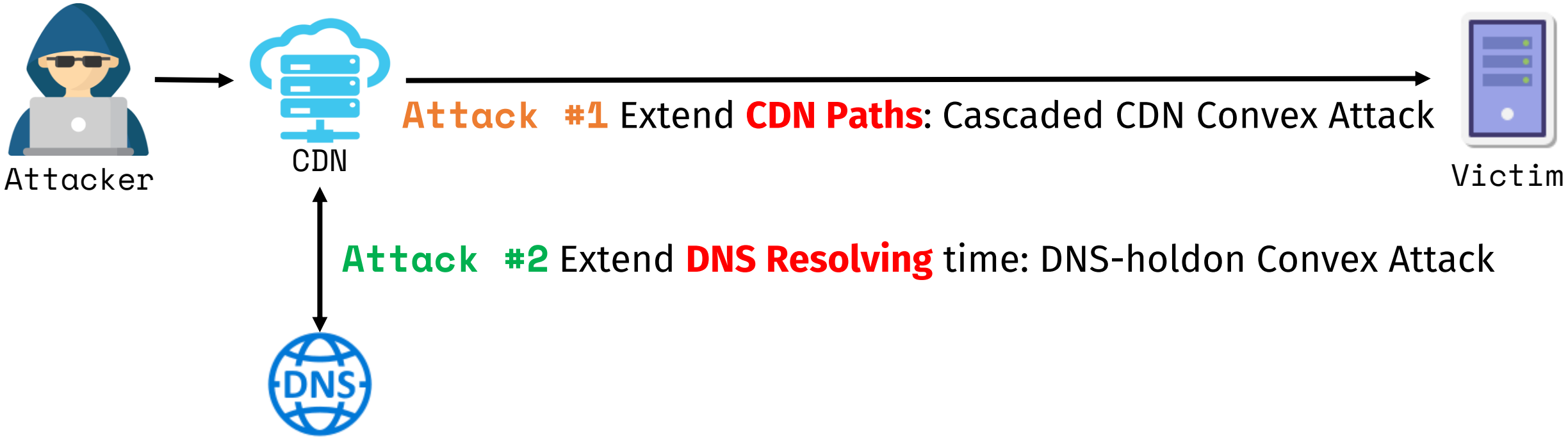
CDN	Akamai	Azure	**CloudFront**	Cloudflare	Fastly
Bandwidth Concentration Ratio	5.46	4.66	**6.42**	3.73	1.49

Why did we obtain a low concentration ratio?

- **Concentration ratio is limited by**
  - diversity of path latencies
  - the longest forwarding time (latency) of CDN global paths

- **Challenges**
  - How can we **Enlarge** / **Control** the forwarding time to allow more requests being buffered in CDN global paths?

Our Attacks: Exploit CDN Features to **Enlarge** / **Control** the forwarding time



Attack #1 Extend **CDN Paths**: Cascaded CDN Convex Attack

Attack #2 Extend **DNS Resolving** time: DNS-holdon Convex Attack

Incomplete packets being **buffered** at CDN servers for a period of time

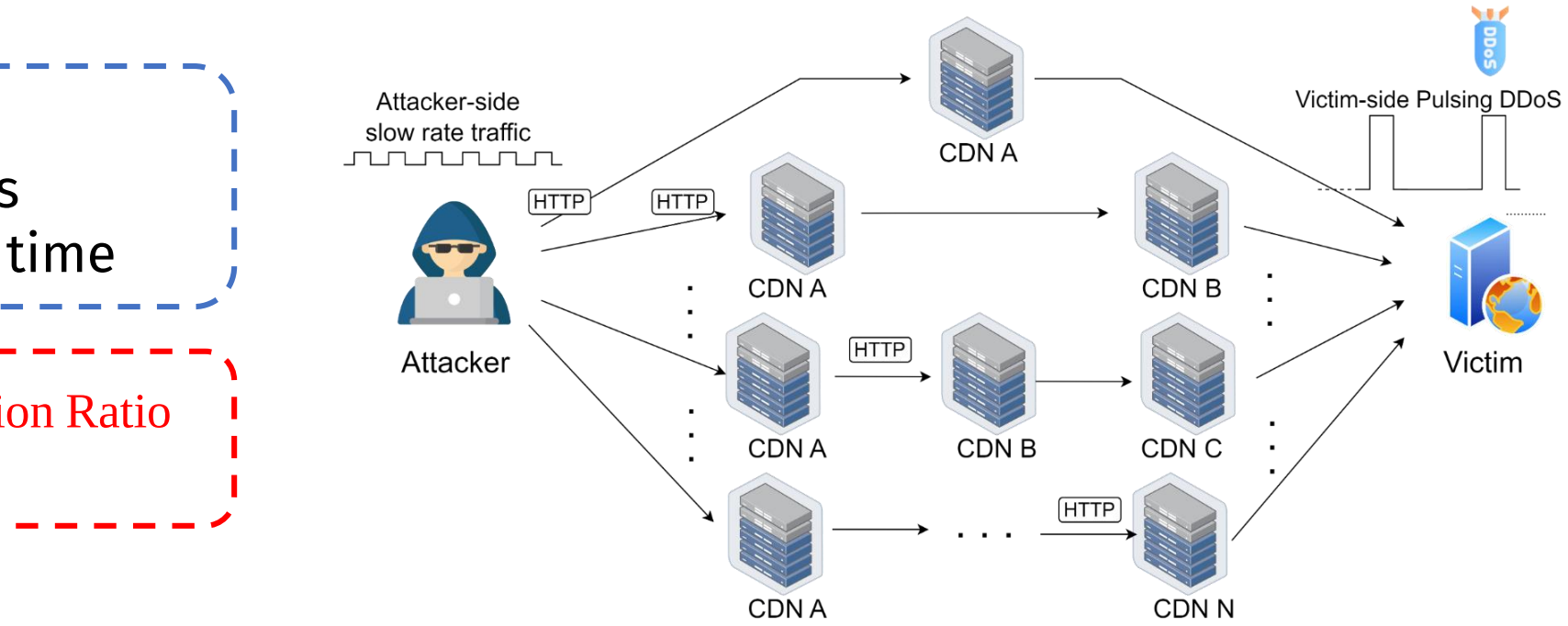
Attack #3 IP-Fragmentation Convex Attack

Attack #4 Request-Pending Convex Attack

Attack #1 Extend CDN Paths: Cascaded CDN Convex Attack

Core Concept
Chain more CDNs
to **enlarge** the flight time

Max Bandwidth Concentration Ratio
~ 9



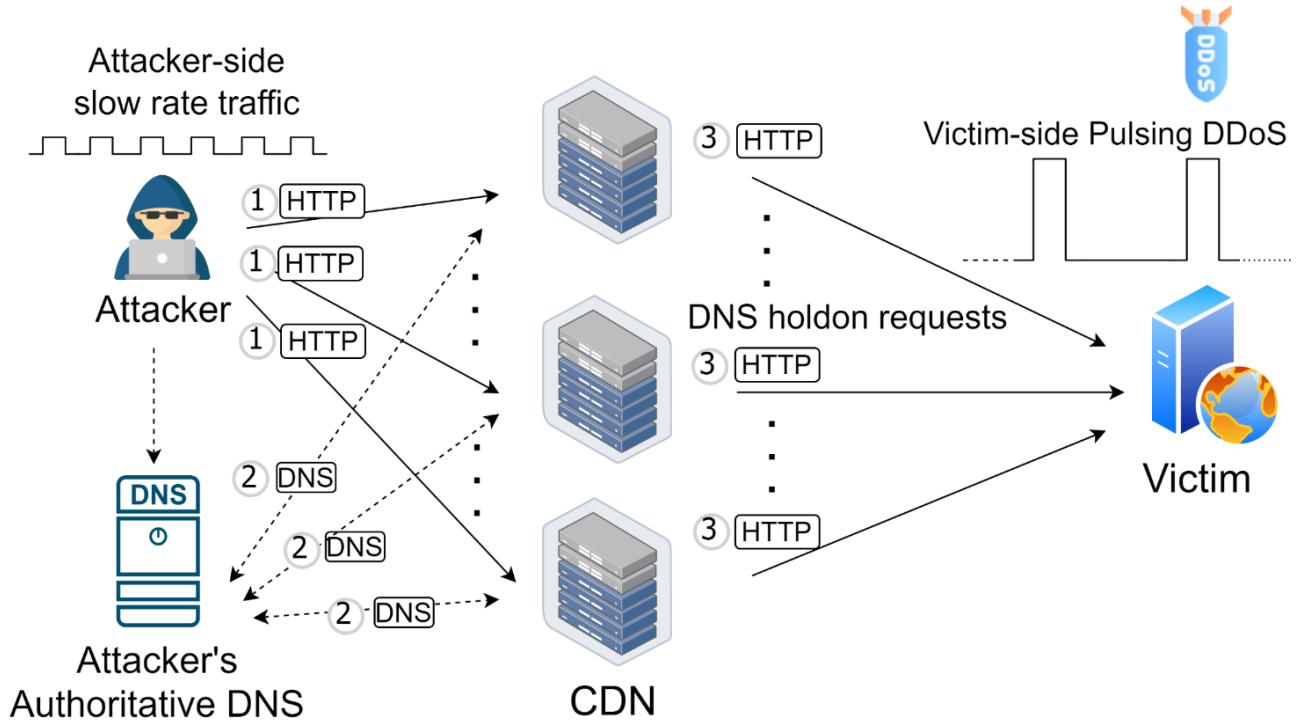
Attack #2 Extend DNS Resolving time: DNS-holdon Convex Attack

Core Concept

Use **DNS query** by edge servers to **control** flight time

Max Bandwidth Concentration Ratio

~ 17



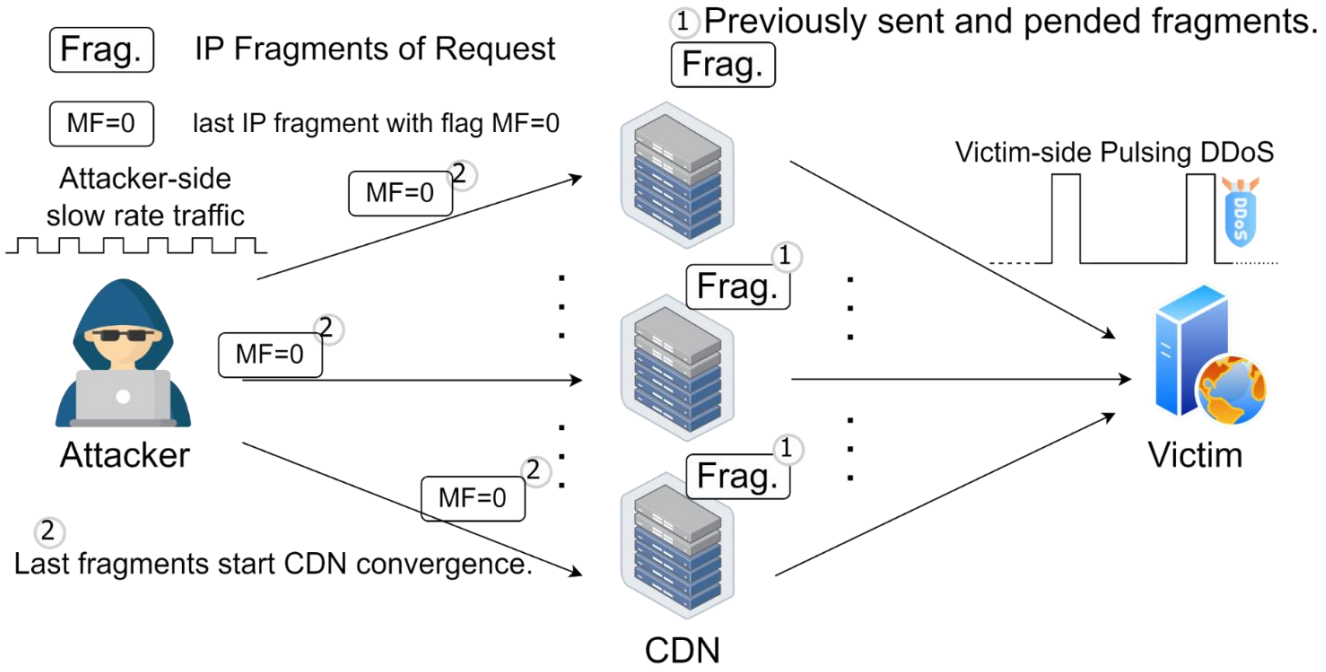
Attack #3 IP-Fragmentation Convex Attack

Core Concept

Use incomplete **fragmented IP packages** to **control** flight time

Max Bandwidth Concentration Ratio

~ 140



CDN	**Akamai**	Azure	CloudFront	Cloudflare	Fastly
IP Fragmentation Timeout	**~ 30s**	~ 30s	~ 30s	~ 15s	~ 10s
Bandwidth Concentration Ratio	**142.23**	118.35	72.62	48.66	21.63

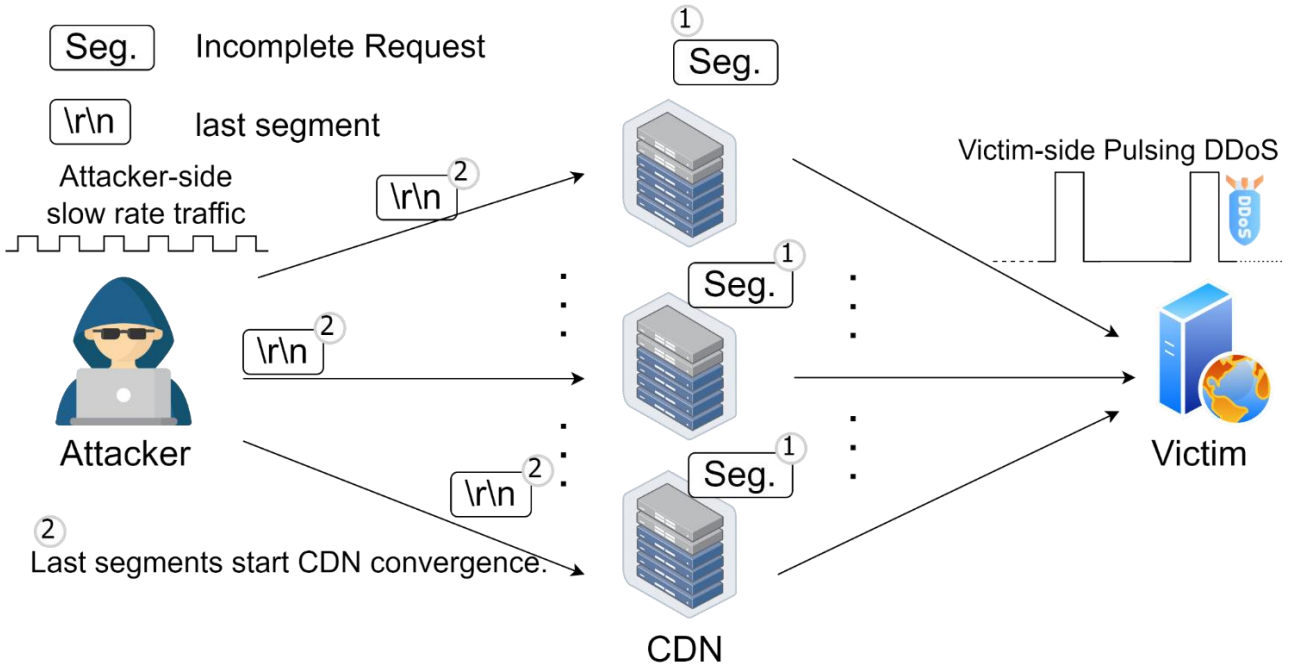
Attack #4 Request-Pending Convex Attack

Core Concept

Use **incomplete HTTP requests** to **control** flight time

Max Bandwidth Concentration Ratio

~ 4800



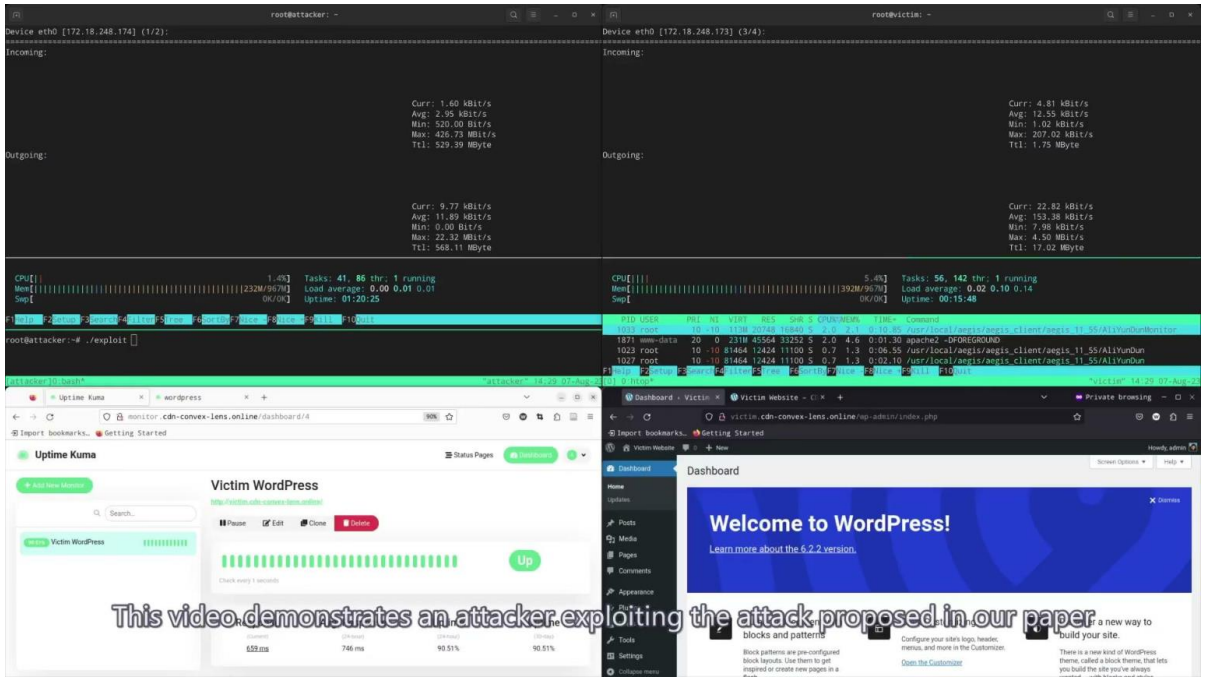
CDN	Akamai	**Azure**	CloudFront	Cloudflare	Fastly
HTTP Forwarding Timeout	~ 16s	**~ 1600s**	~ 12s	≥ 3600s	~ 16s
Bandwidth Concentration Ratio	1426.38	**4842.69**	31.3	1786.37	988.48

Real-World Demonstration Video

Experiment Setup

- **Only 32** edge servers were used
- **Only 16MB × 32 = 512MB** data were sent
- **No impact** on other websites
  - the victim website is under our control
- Attacker Outbound-Bandwidth: ~7Mbps
- Victim Inbound-Bandwidth: ~100Mbps
  - Limited by the cloud provider (100Mbps at max)

Demo



The targeted website server is directly **out of service**

"Out of memory: Killed process apache2"

Outlines

- Background
- Attacks
- **Mitigations**
- Conclusion

Mitigations

- **For CDN**
  - **Validate the ownership** of customer-supplied origin configuration
    - Stop CDN being abused to attack 3rd party targets
    - Can still attack websites hosted on CDN
  - **Fast forwarding** of requests (#enhancement 4)
    - Forward on each byte of received request
  - **Standardizing a unified head field** to expose client IP
    - Filter or limit attacking traffic based on client IP
- **For Victim**
  - **limit the request rate** from the same client IP

Outlines

- Background
- Attacks
- Mitigations
- **Conclusion**

Conclusion

- We present a novel **the CDN-Convex attack** which uses CDN-Introduced delay distribution to launch a pulsing DDoS attack against any 3rd party TCP service
- **4 novel enhancement** for the impact from 2 aspects
  - Increasing network pathways (Cascaded CDN)
  - Controlling network latency (DNS-Holdon, IP-Fragmentation, HTTP-Holdon)
- Bandwidth Concentration Ratio **≥ 1000**

Thank you for listening!
Q & A

Video

Paper

Lab

清華大學
Tsinghua University

奇安信
新一代网络安全领军者

中关村实验室
ZGC Lab