MirageFlow:

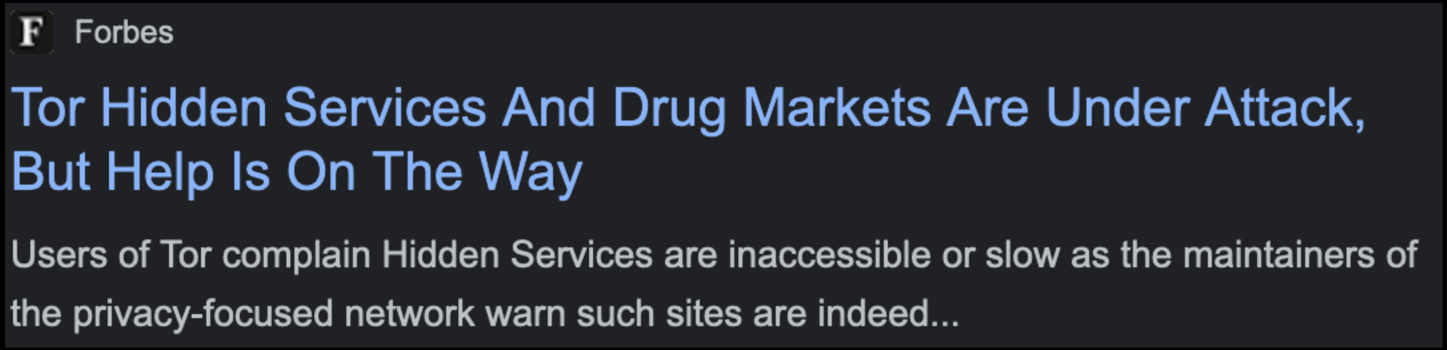
A New Bandwidth Inflation Attack on Tor

Christoph Sendner[1], Jasper Stang[1], Alexandra Dmitrienko[1], Raveen Wijewickrama[2], Murtuza Jadliwala[2]

[1]University of Würzburg, [2]University of Texas at San Antonio

NDSS
SYMPOSIUM/2024

Tor in the News

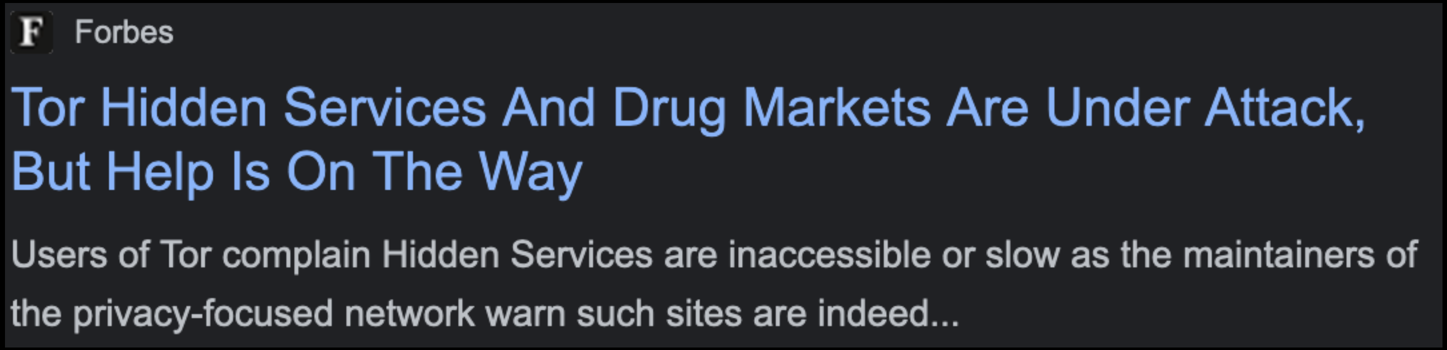


Forbes

Tor Hidden Services And Drug Markets Are Under Attack, But Help Is On The Way

Users of Tor complain Hidden Services are inaccessible or slow as the maintainers of the privacy-focused network warn such sites are indeed...

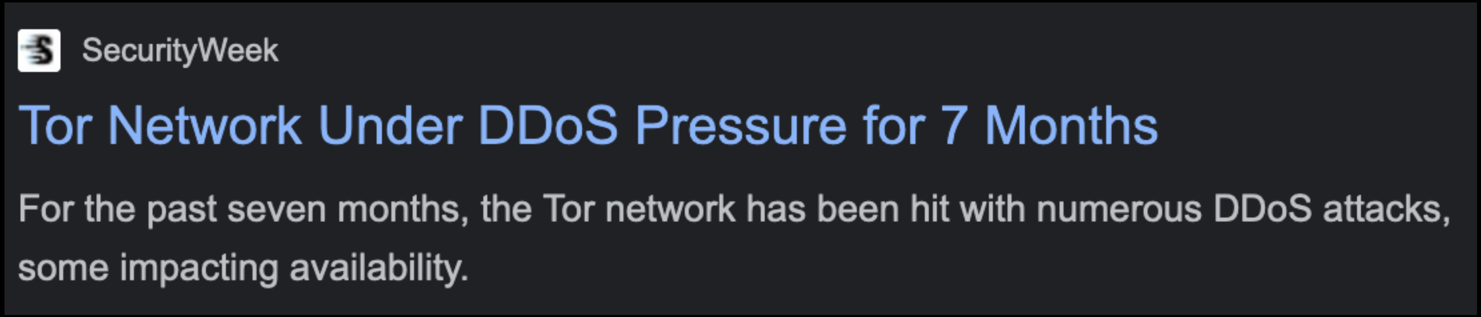
Tor in the News



Forbes

Tor Hidden Services And Drug Markets Are Under Attack, But Help Is On The Way

Users of Tor complain Hidden Services are inaccessible or slow as the maintainers of the privacy-focused network warn such sites are indeed...

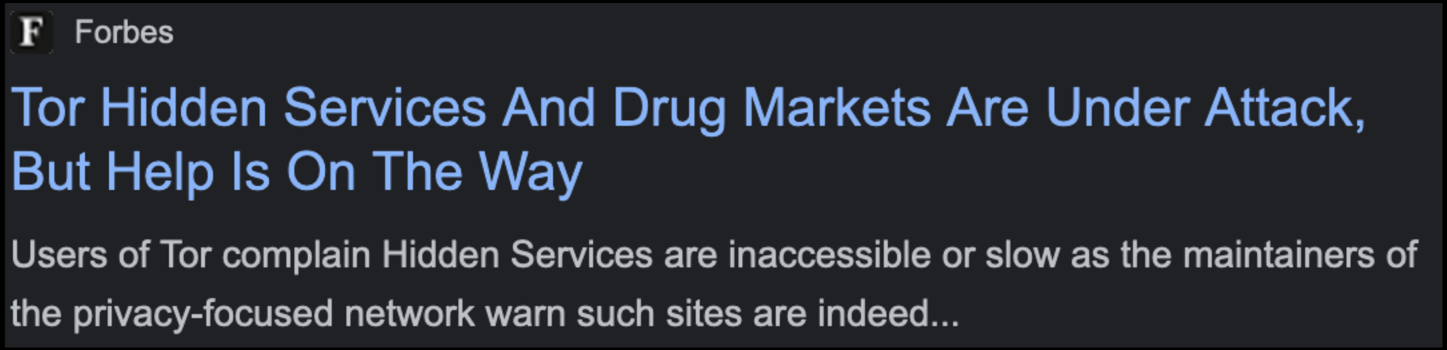


SecurityWeek

Tor Network Under DDoS Pressure for 7 Months

For the past seven months, the Tor network has been hit with numerous DDoS attacks, some impacting availability.

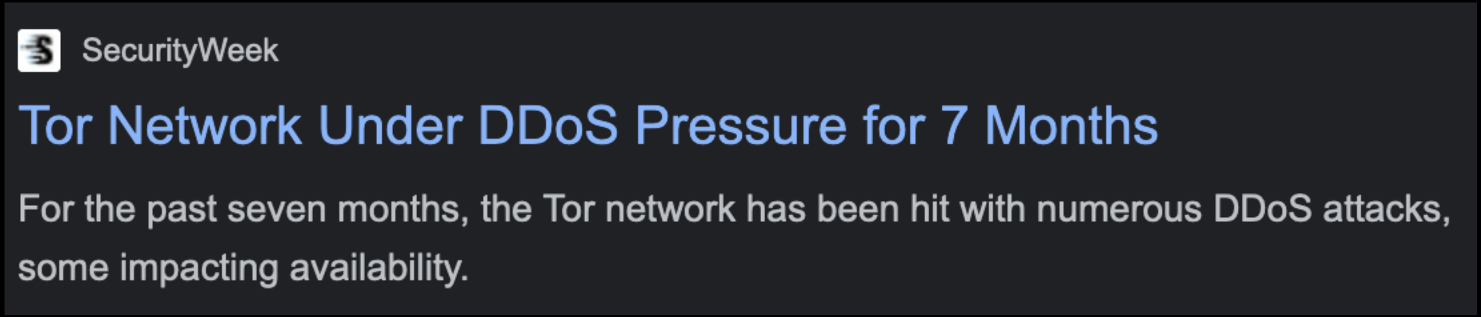
Tor in the News



Forbes

Tor Hidden Services And Drug Markets Are Under Attack, But Help Is On The Way

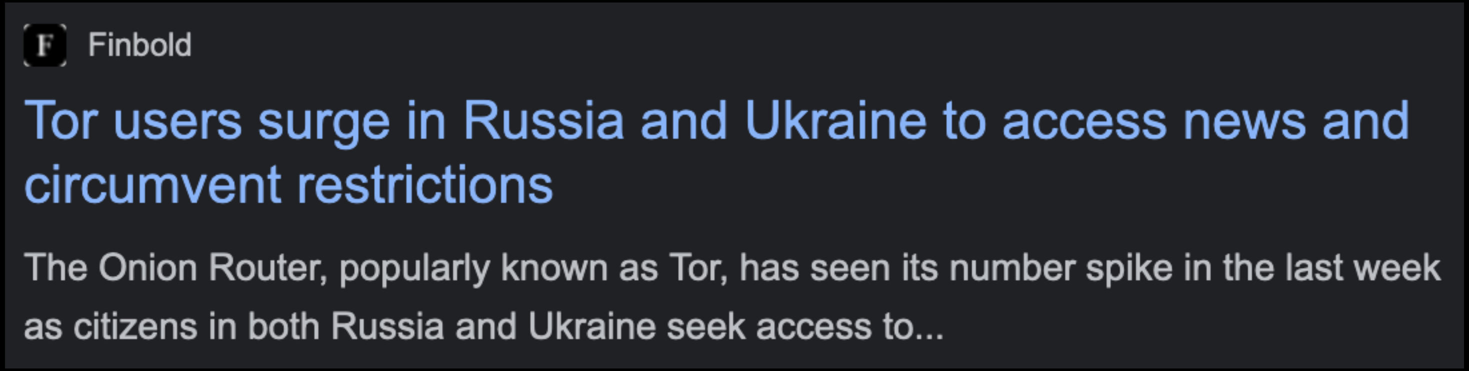
Users of Tor complain Hidden Services are inaccessible or slow as the maintainers of the privacy-focused network warn such sites are indeed...



SecurityWeek

Tor Network Under DDoS Pressure for 7 Months

For the past seven months, the Tor network has been hit with numerous DDoS attacks, some impacting availability.



Finbold

Tor users surge in Russia and Ukraine to access news and circumvent restrictions

The Onion Router, popularly known as Tor, has seen its number spike in the last week as citizens in both Russia and Ukraine seek access to...

The Onion Routing

The Onion Routing

📍 7k+ Relays

The Onion Routing

2M/Day

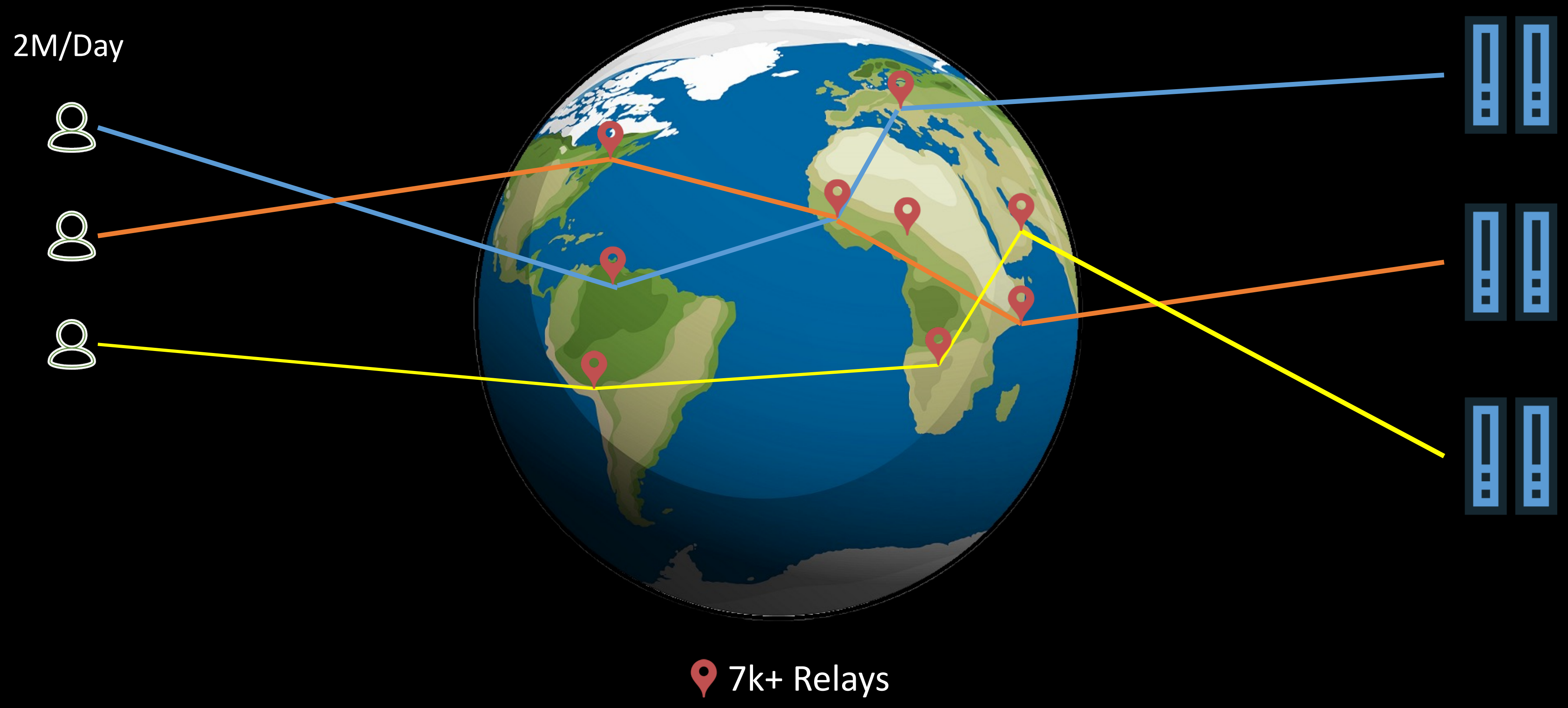
📍 7k+ Relays

The Onion Routing

2M/Day

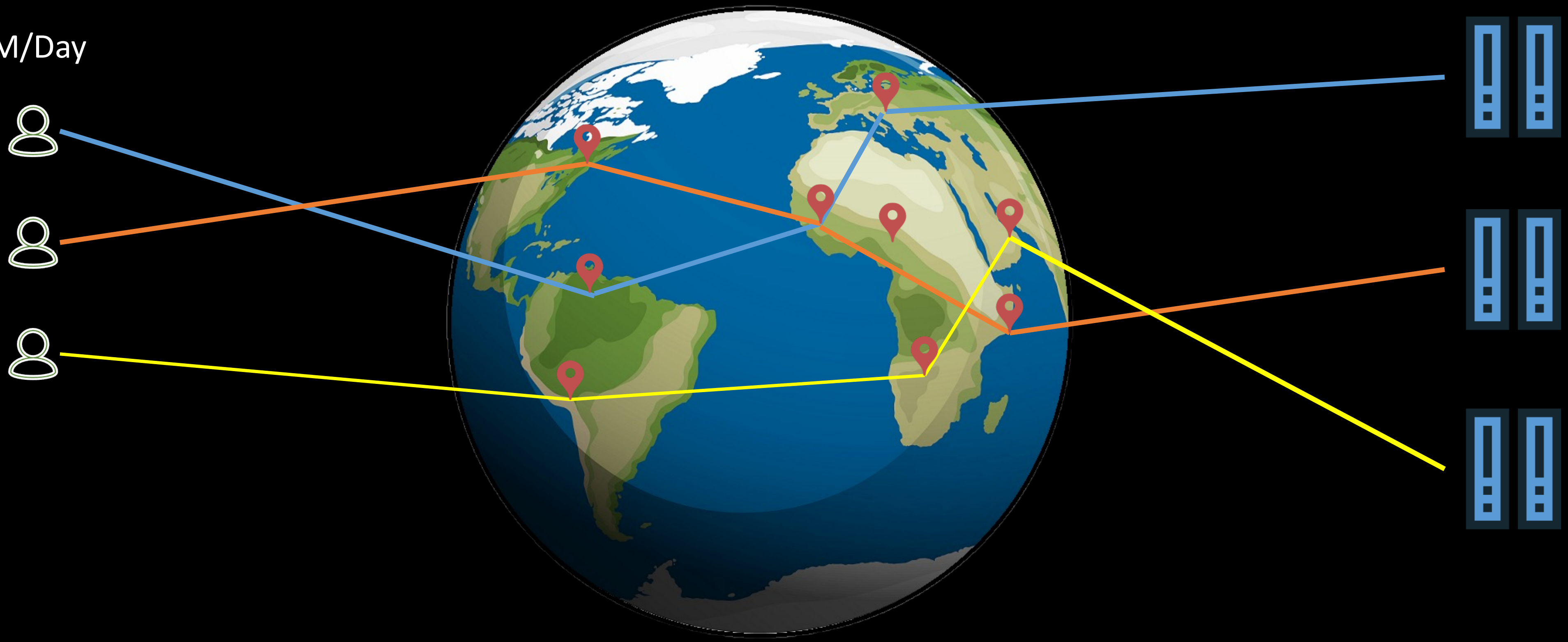
7k+ Relays

The Onion Routing



The Onion Routing

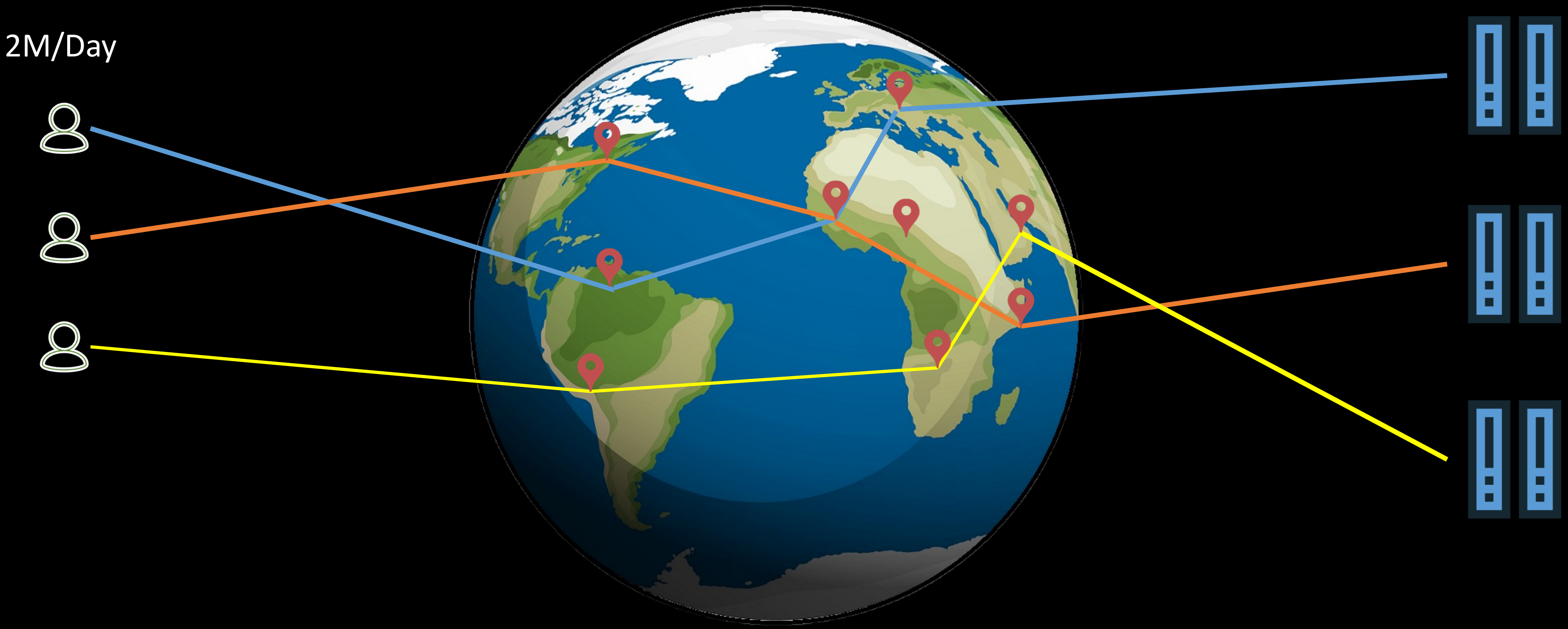
2M/Day



📍 7k+ Relays

300 Gbit/s user traffic

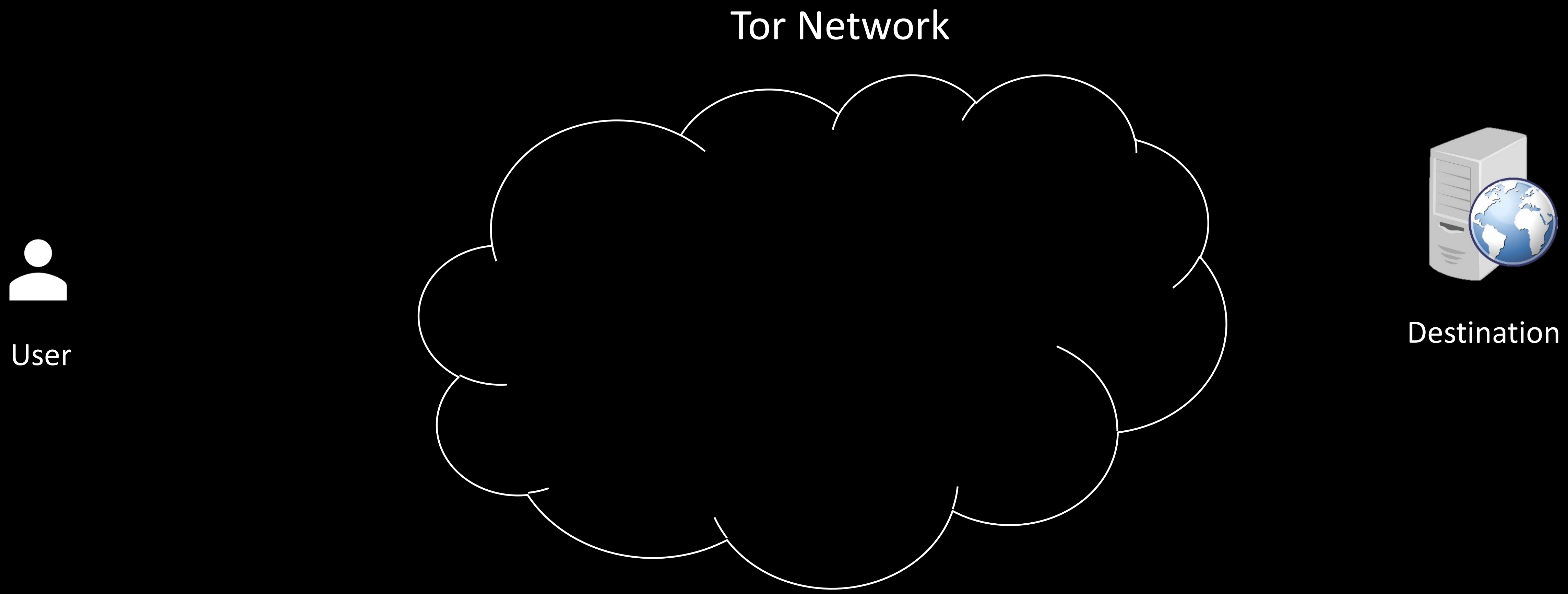
The Onion Routing



📍 7k+ Relays

300 Gbit/s user traffic
750 Gbit/s advertised

Tor Network

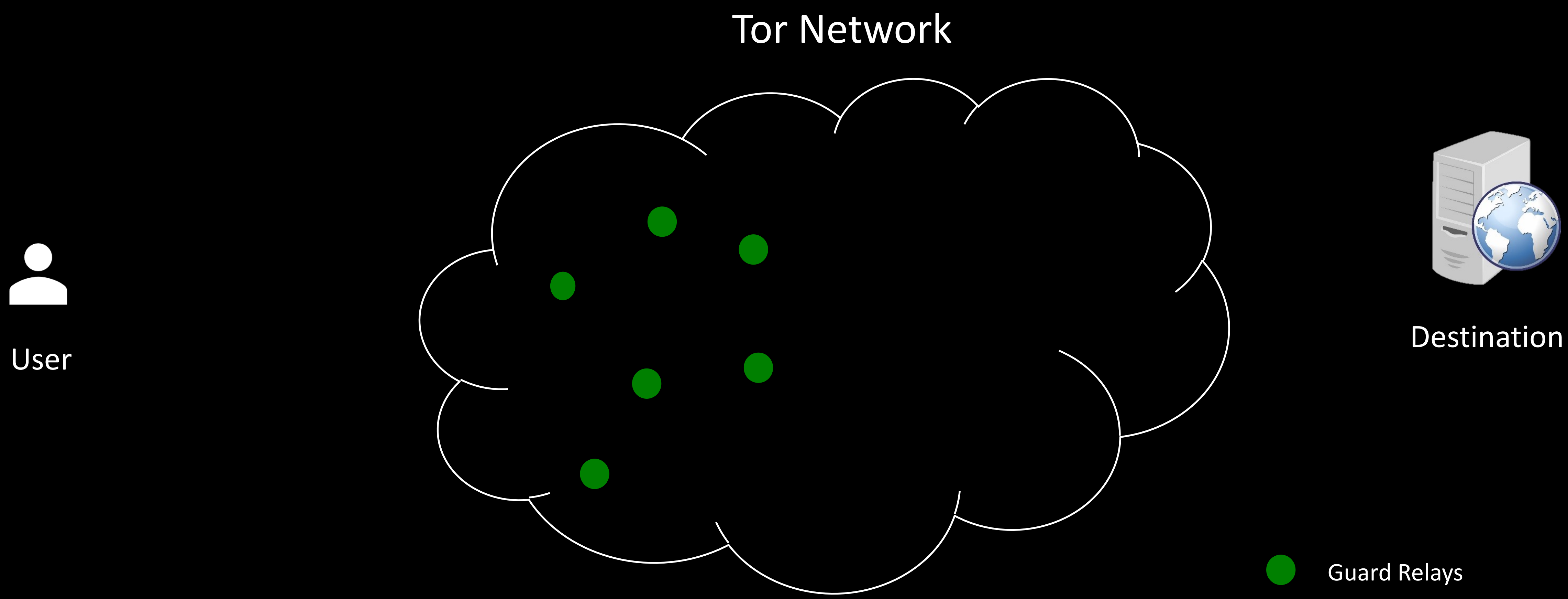


Tor Network

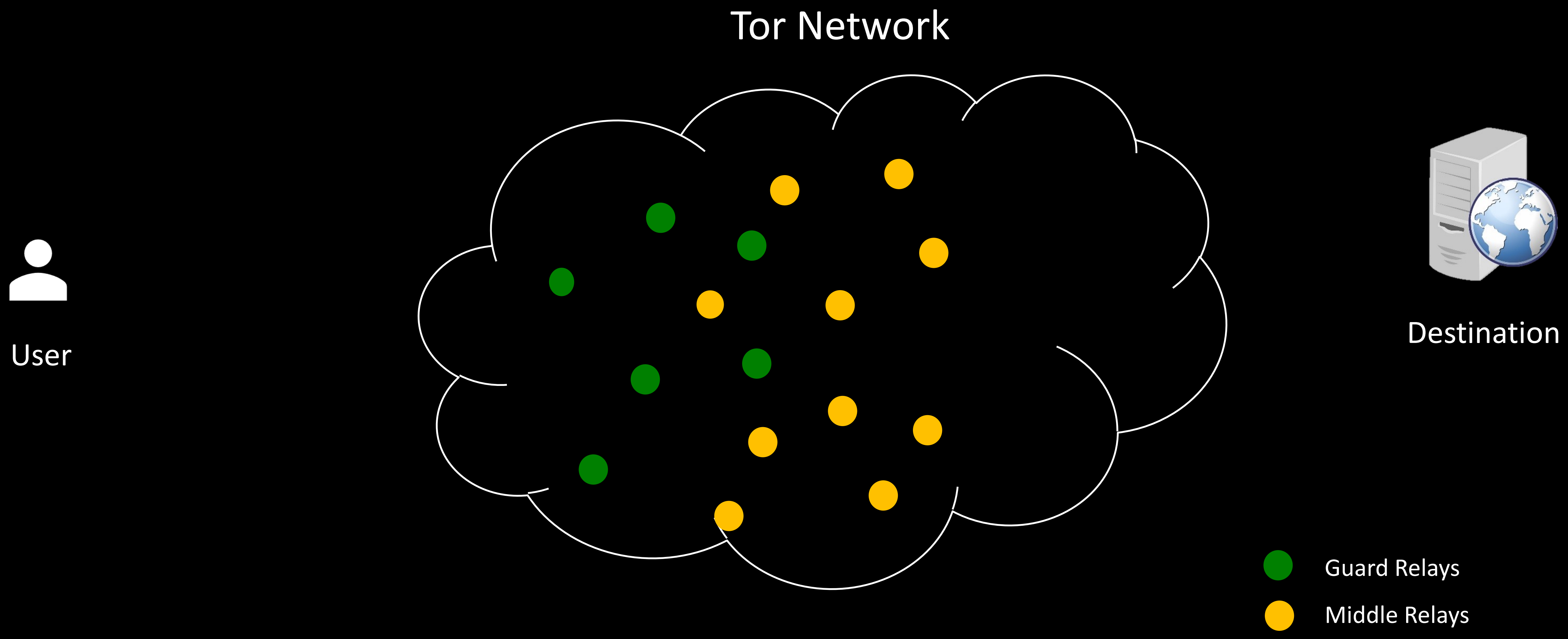
User

Destination

Tor Network



Tor Network



Tor Network

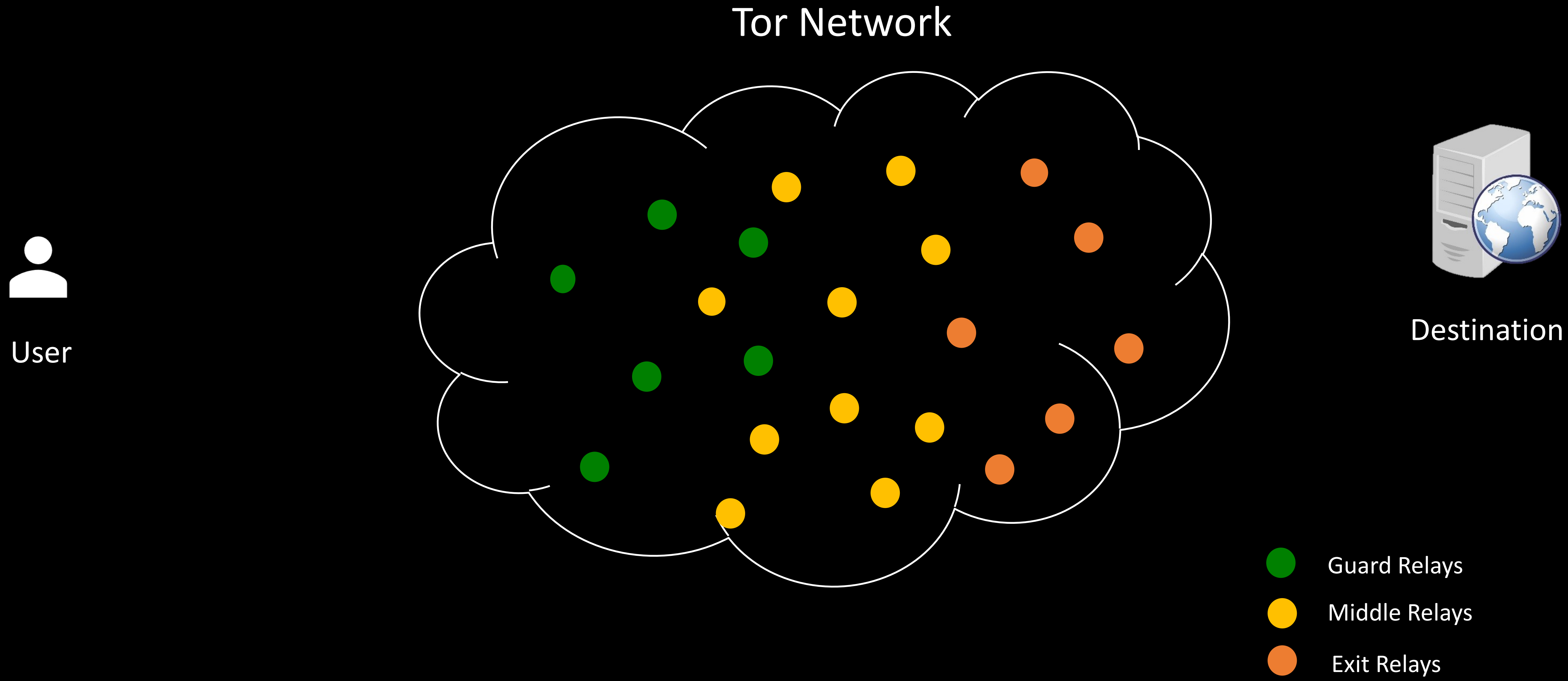
User

Destination

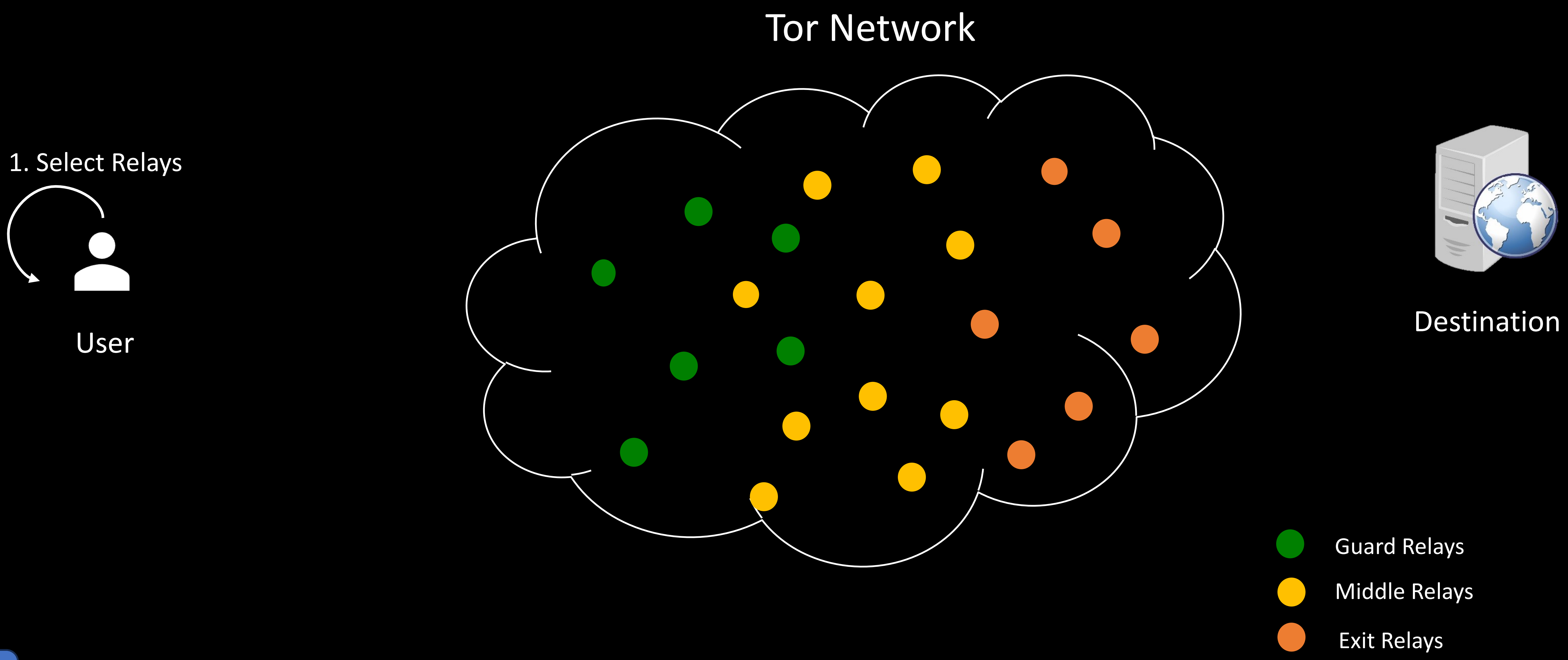
🟢 Guard Relays

🟡 Middle Relays

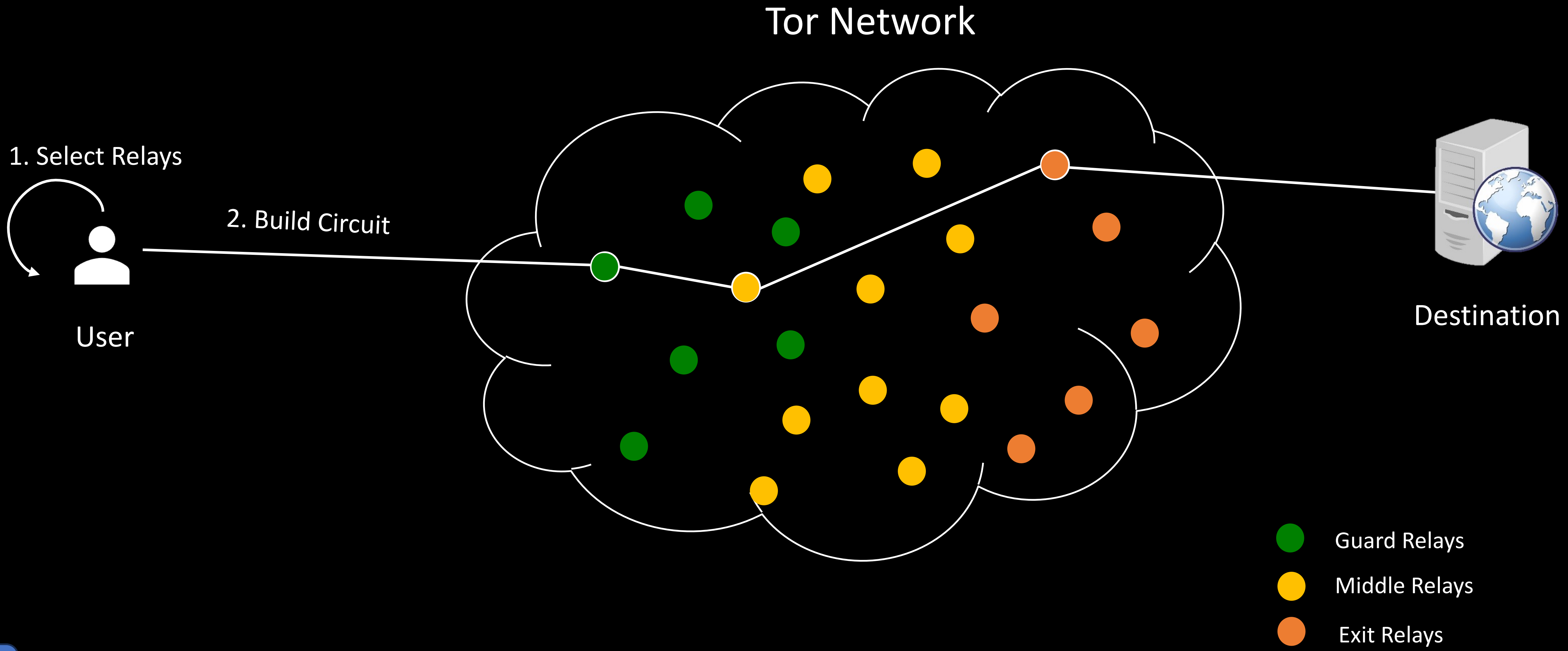
Tor Network


Tor Network
User
Destination
Guard Relays
Middle Relays
Exit Relays

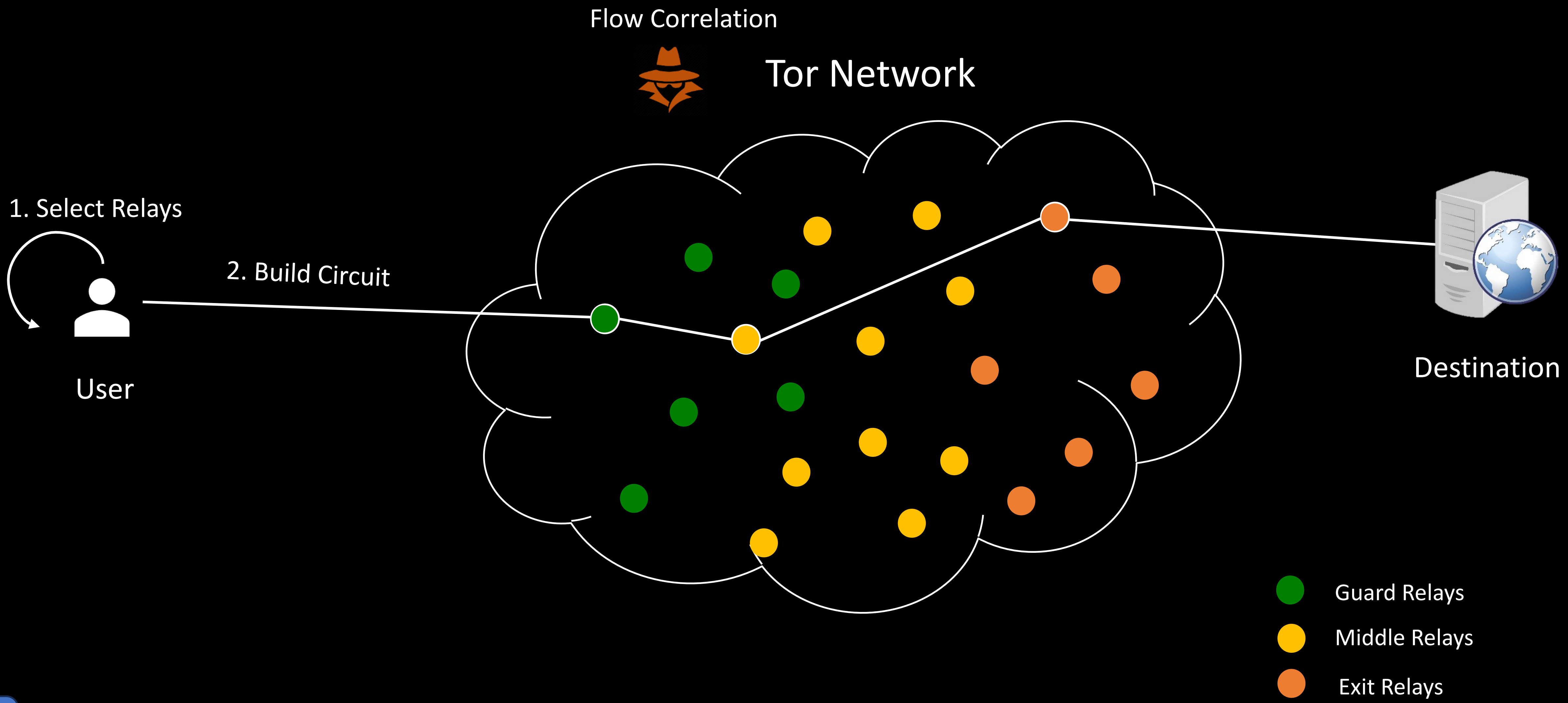
Tor Network


Tor Network
1. Select Relays
User
Destination
Guard Relays
Middle Relays
Exit Relays

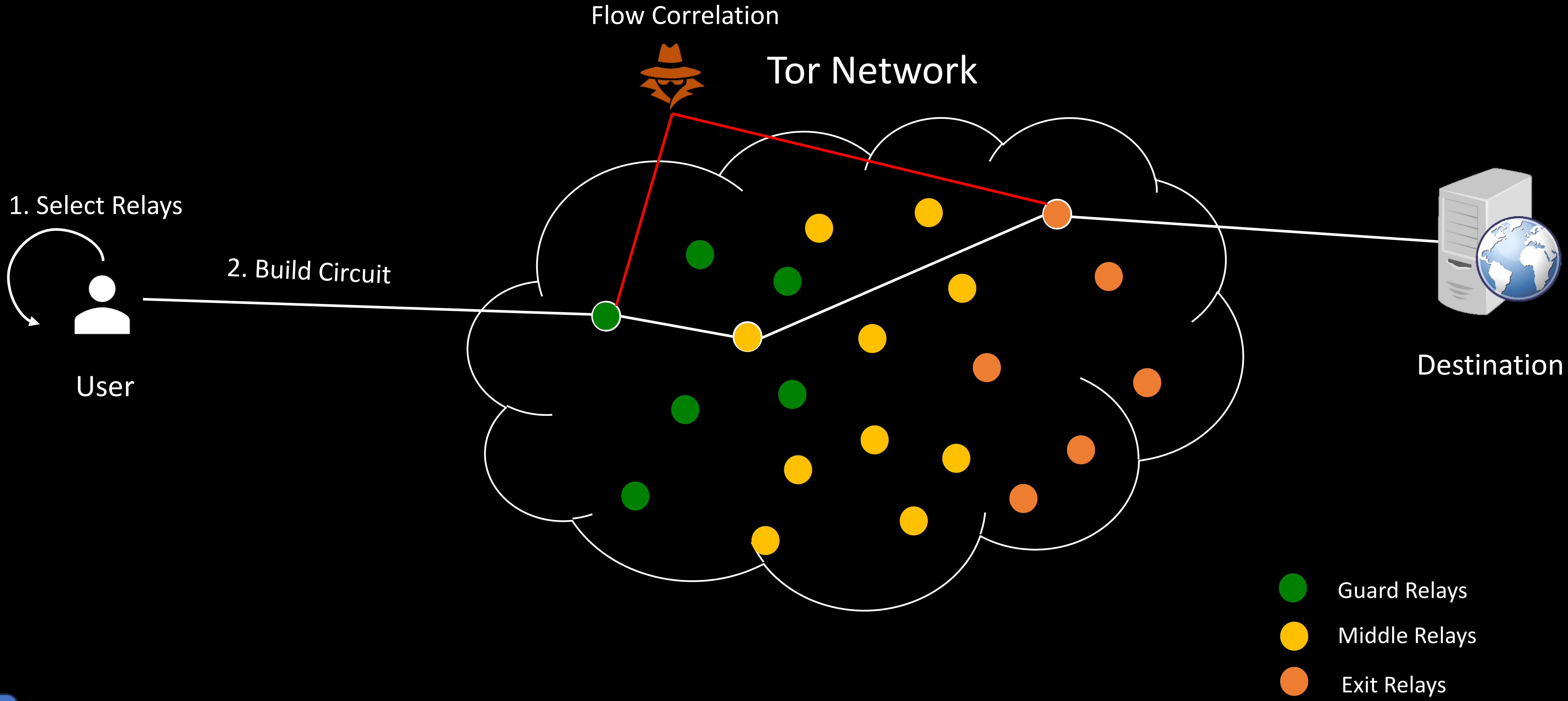
Tor Network


Tor Network
1. Select Relays
2. Build Circuit
User
Destination
● Guard Relays
● Middle Relays
● Exit Relays

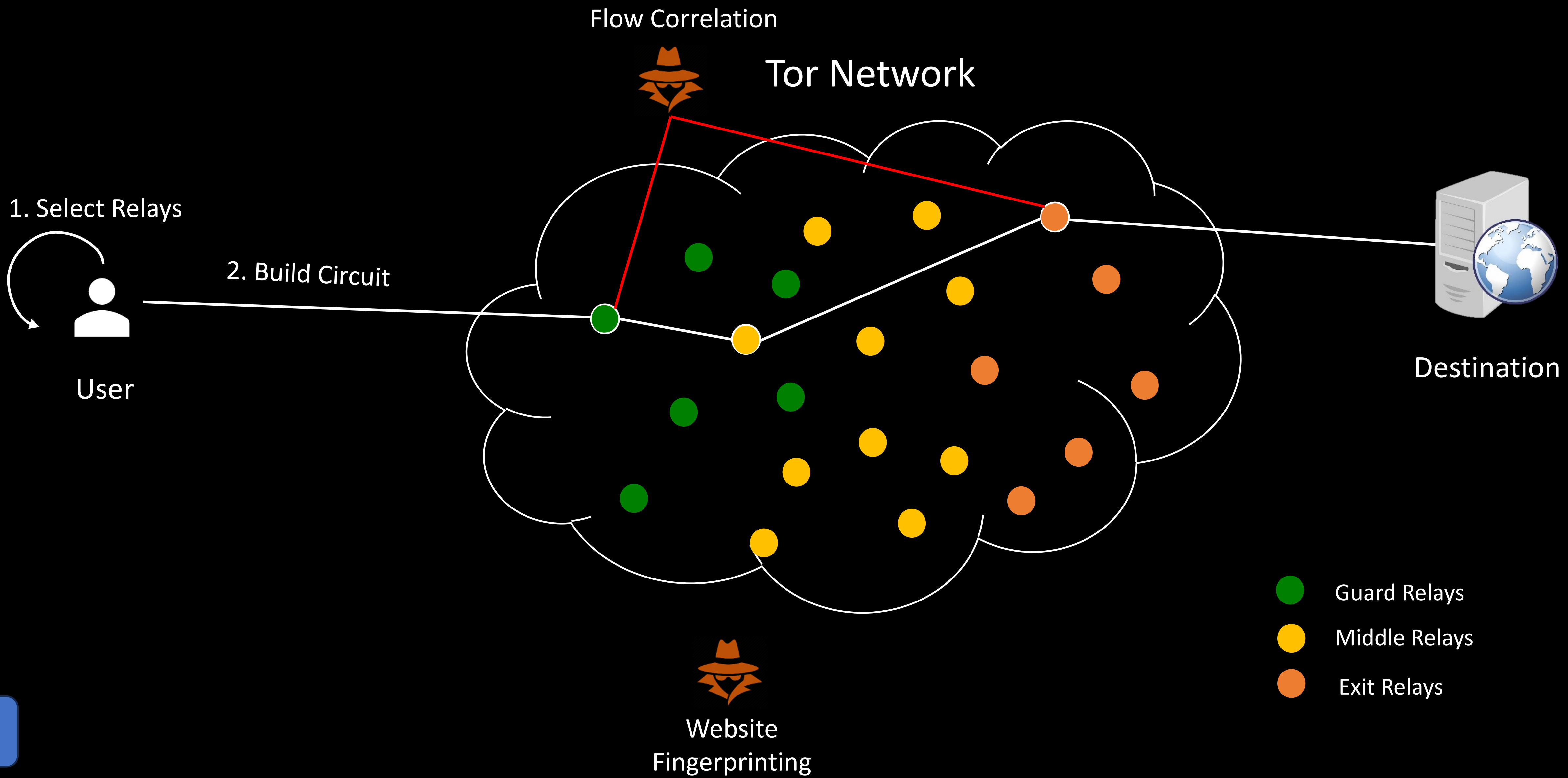
Tor Network


Flow Correlation
Tor Network
1. Select Relays
2. Build Circuit
User
Destination
Guard Relays
Middle Relays
Exit Relays

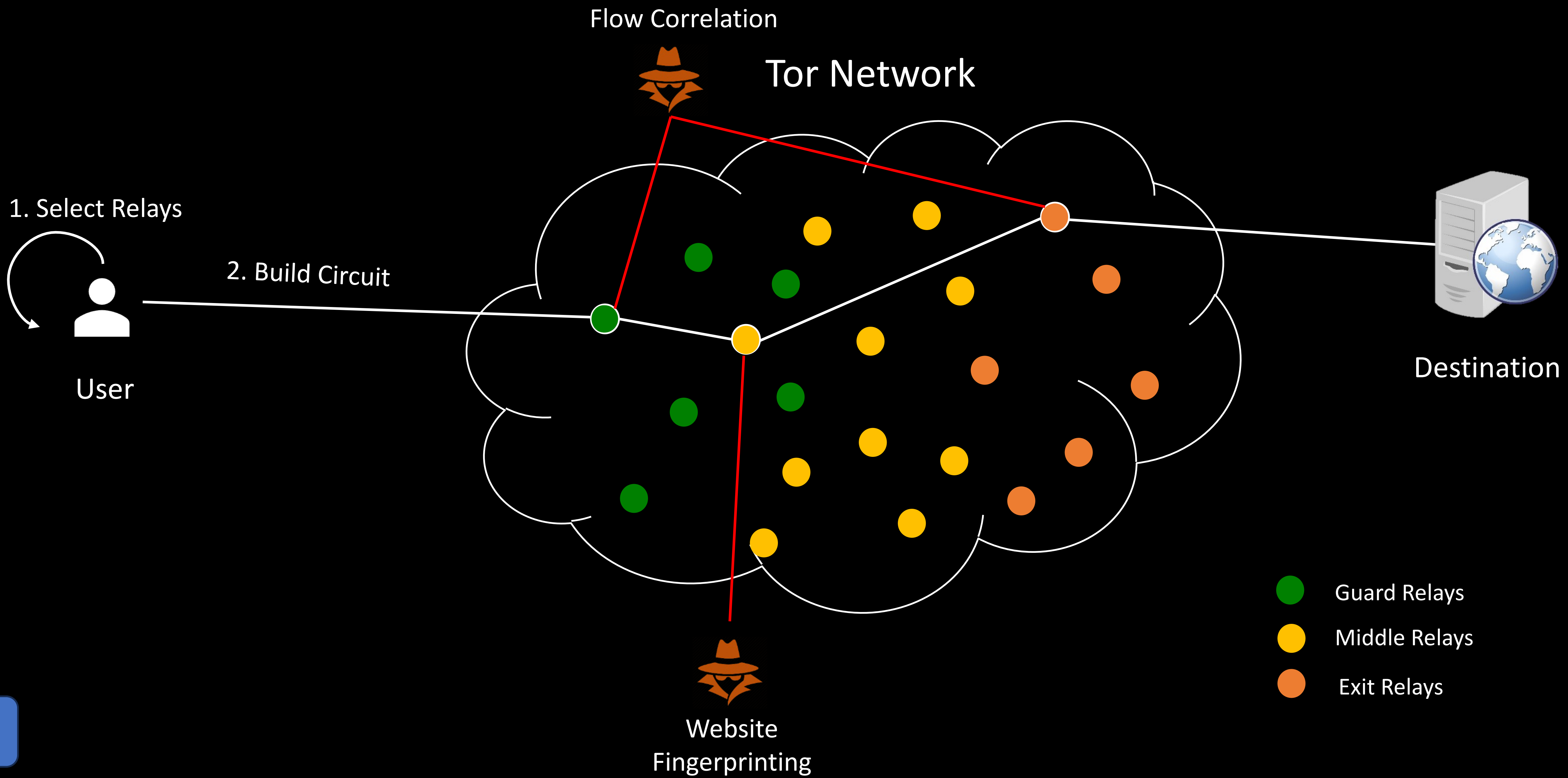
Tor Network


Flow Correlation
Tor Network
1. Select Relays
2. Build Circuit
User
Destination
🟢 Guard Relays
🟡 Middle Relays
🟠 Exit Relays

Tor Network

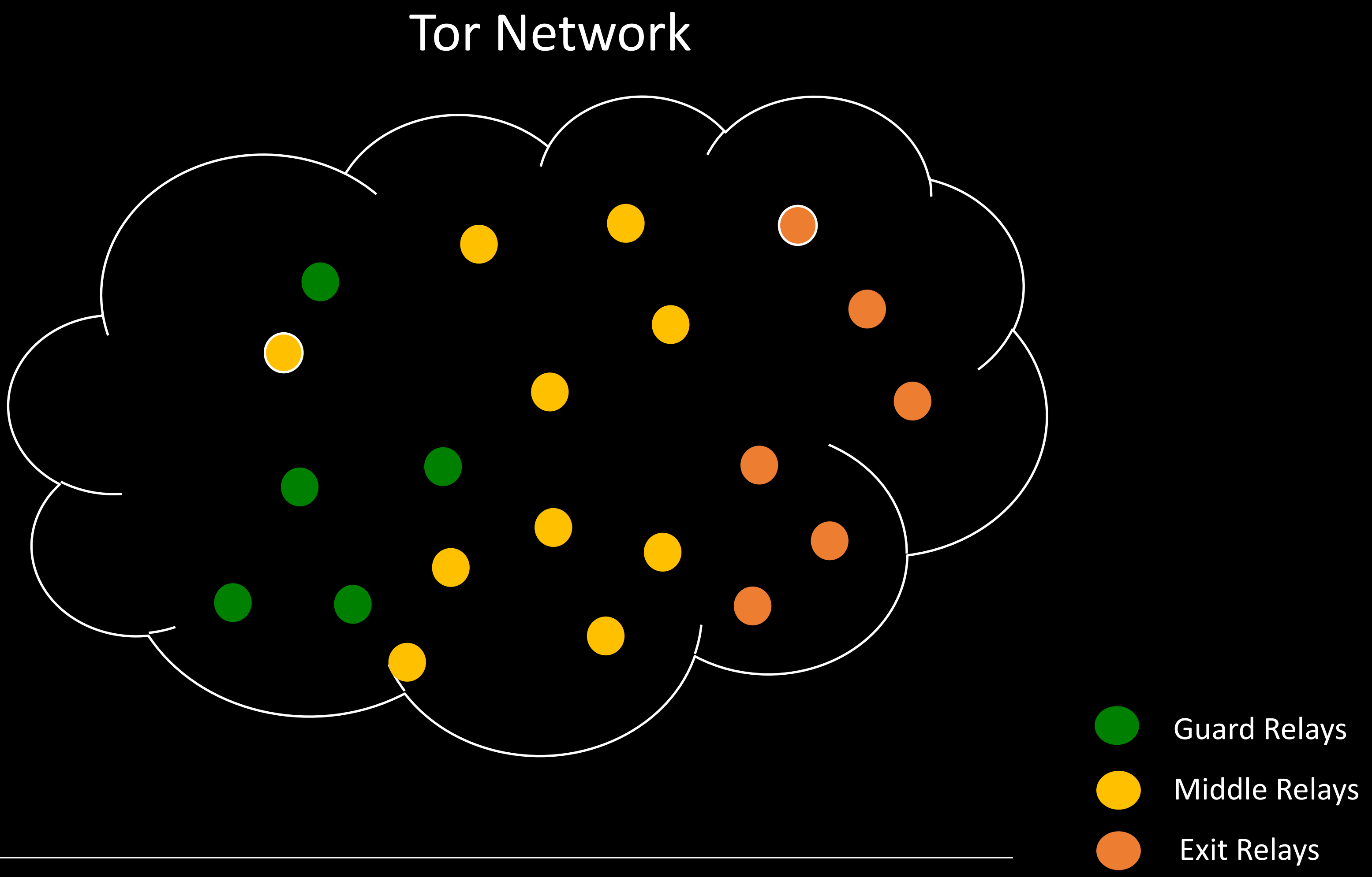

Flow Correlation
Tor Network
1. Select Relays
2. Build Circuit
User
Destination
Website Fingerprinting
🟢 Guard Relays
🟡 Middle Relays
🟠 Exit Relays

Tor Network


Flow Correlation
Tor Network
1. Select Relays
2. Build Circuit
User
Destination
Website Fingerprinting
Guard Relays
Middle Relays
Exit Relays

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]

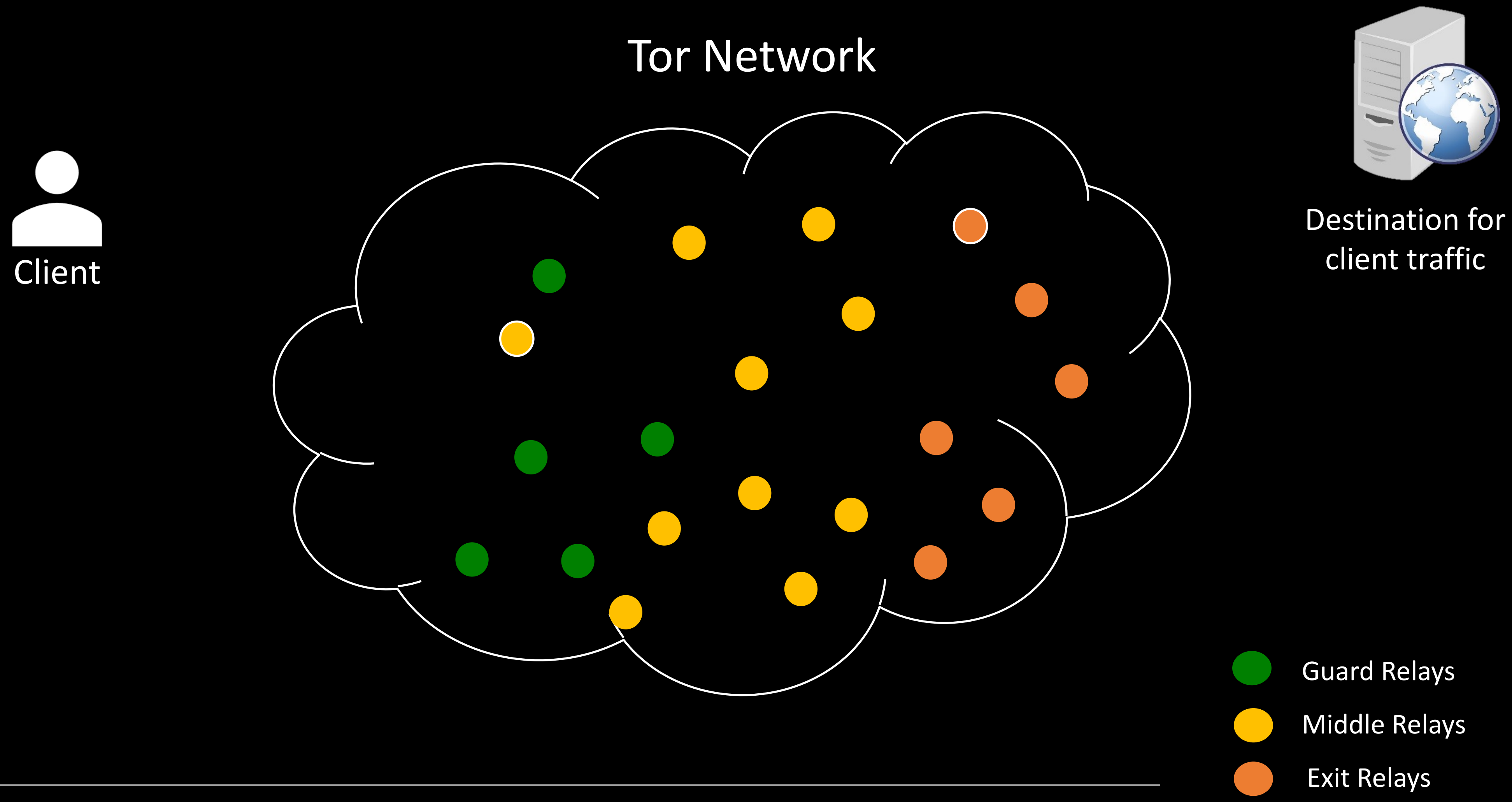


[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]

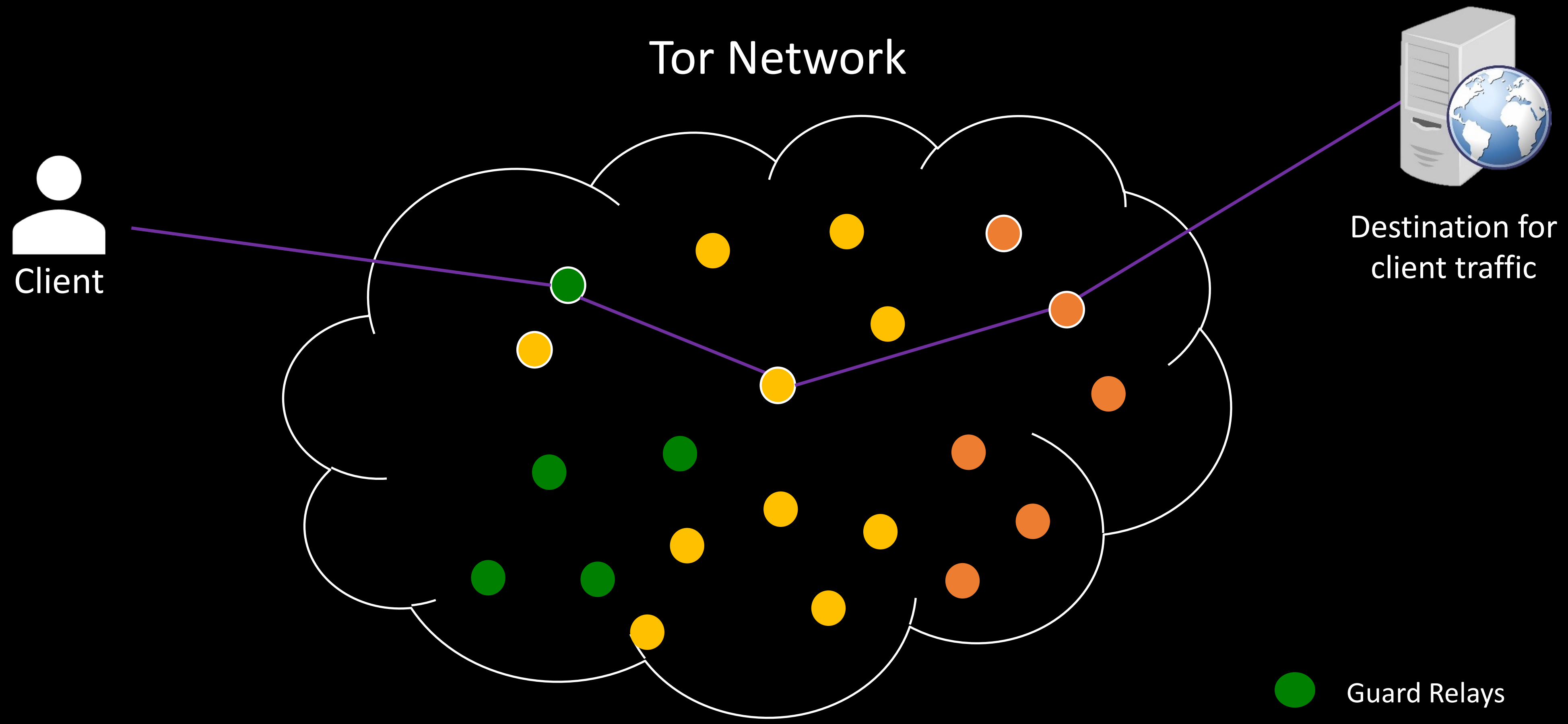


[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]



🟢 Guard Relays

🟡 Middle Relays

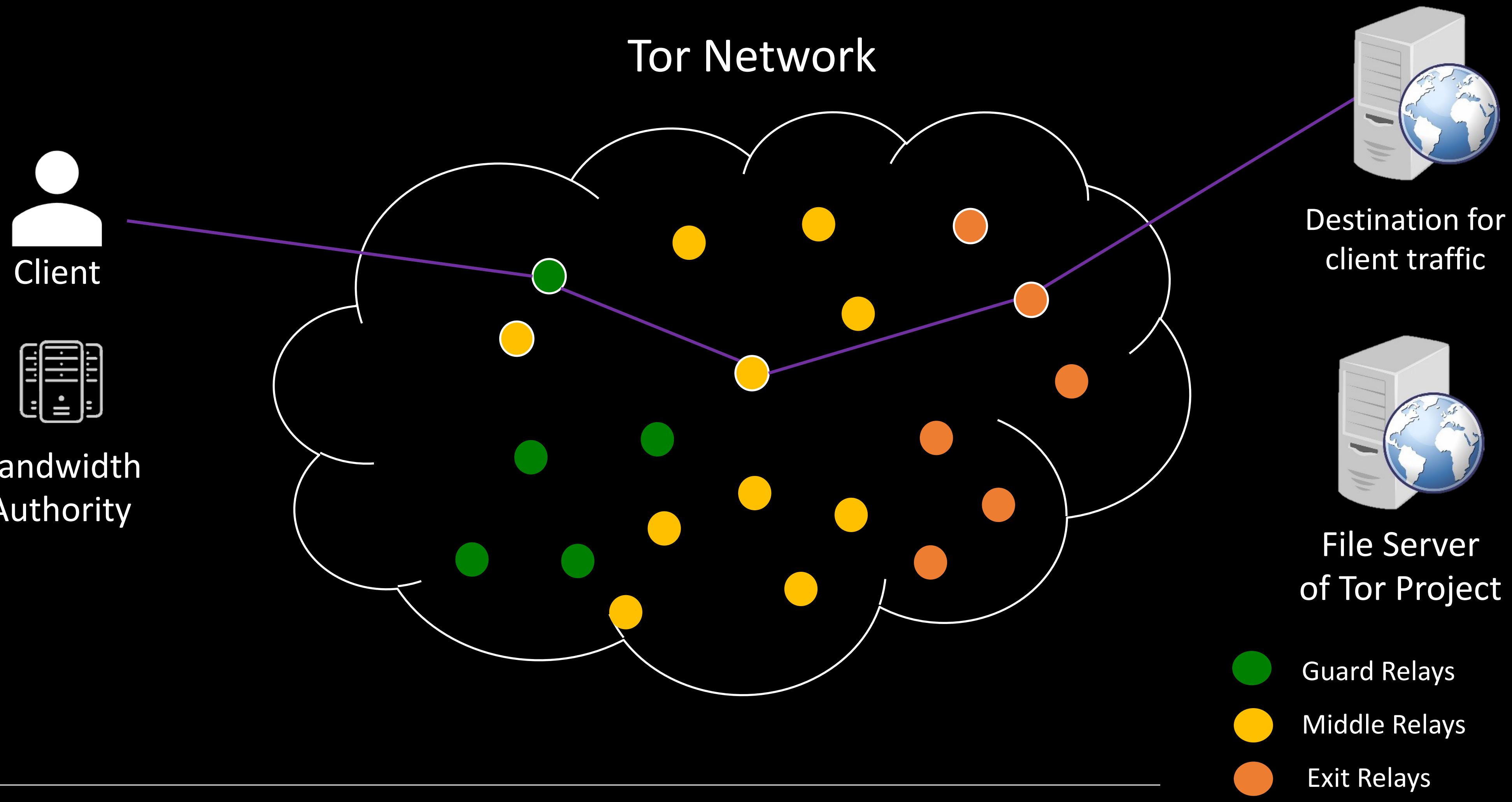
🟠 Exit Relays

[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]

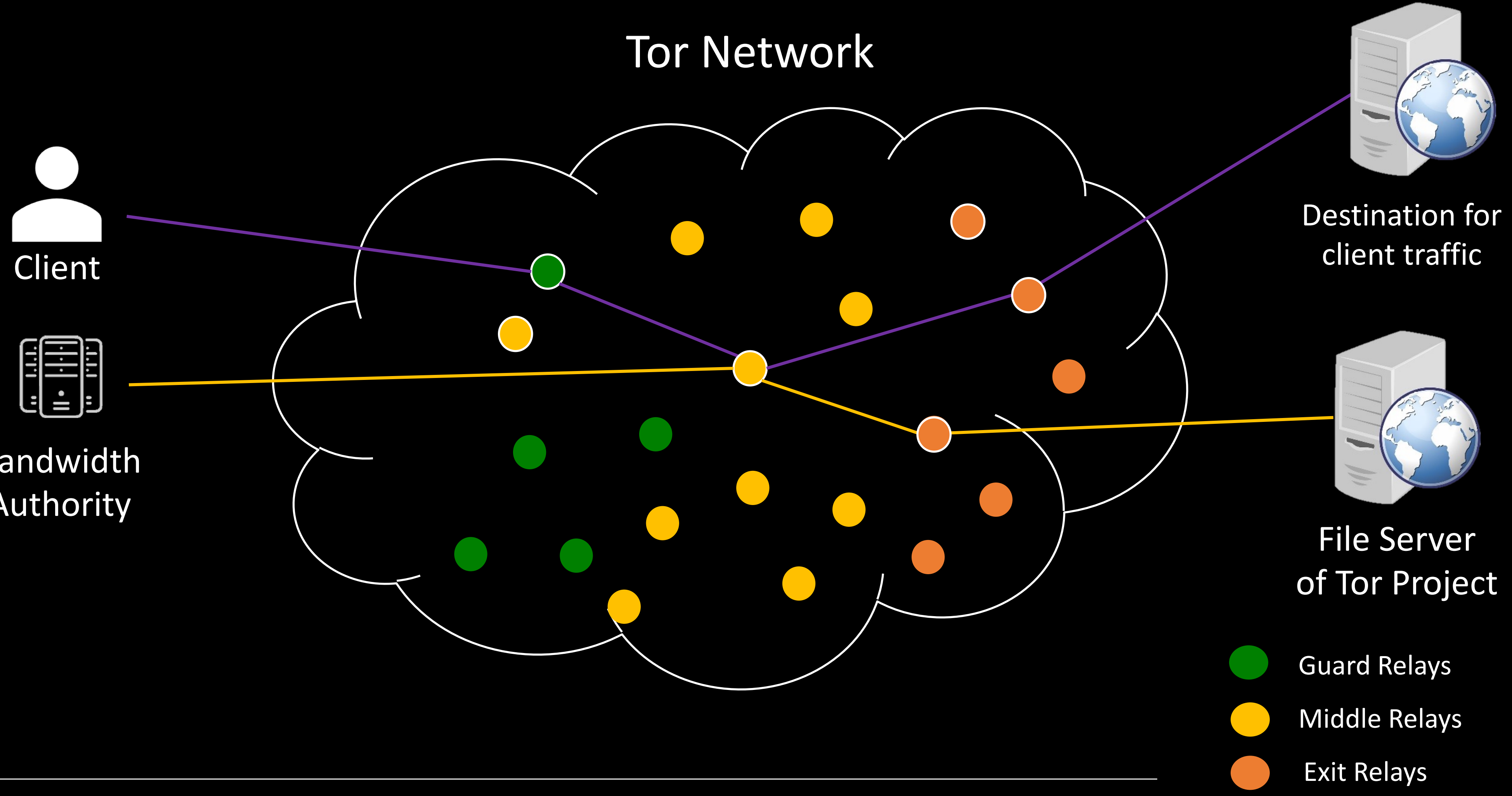


[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]

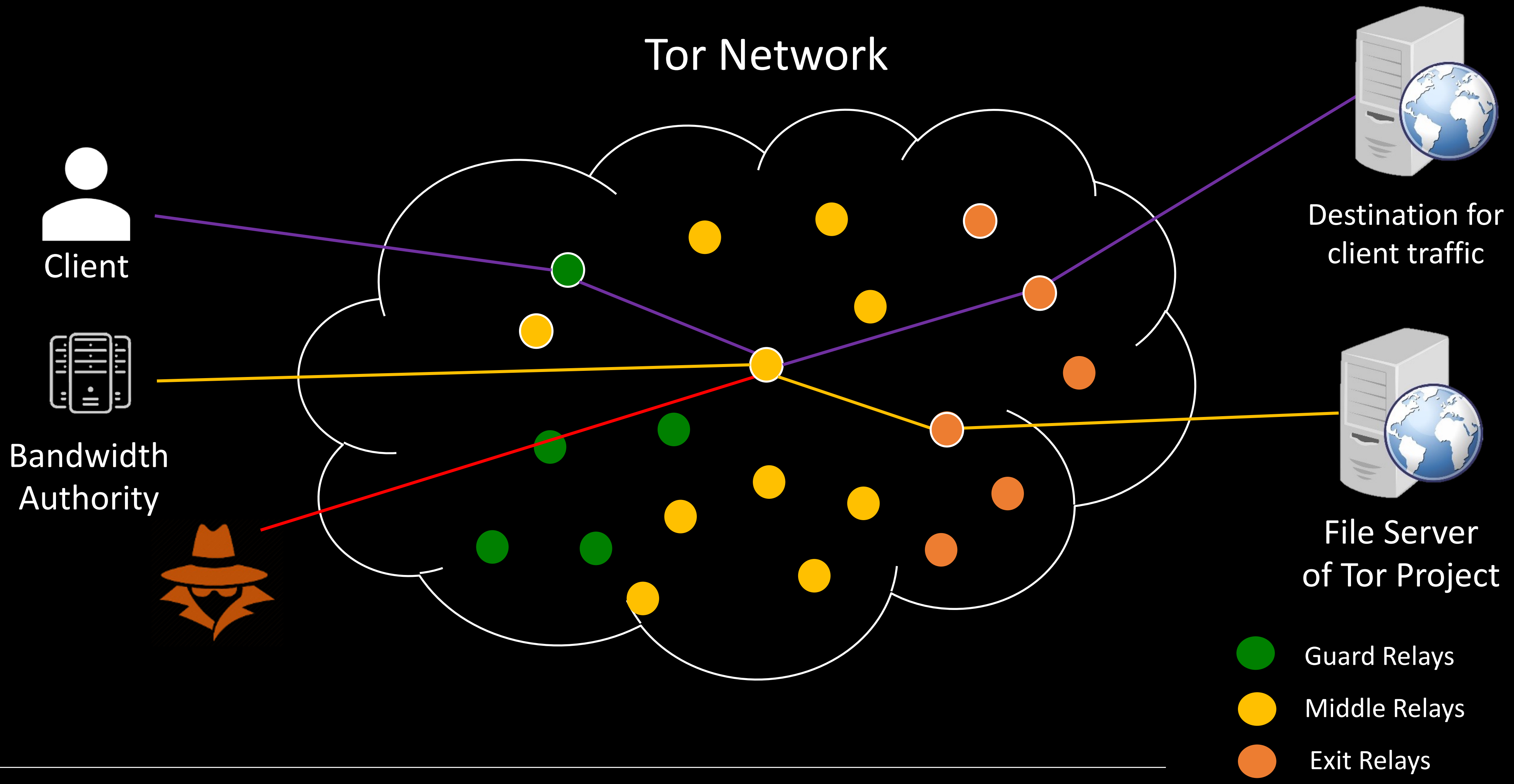


[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]

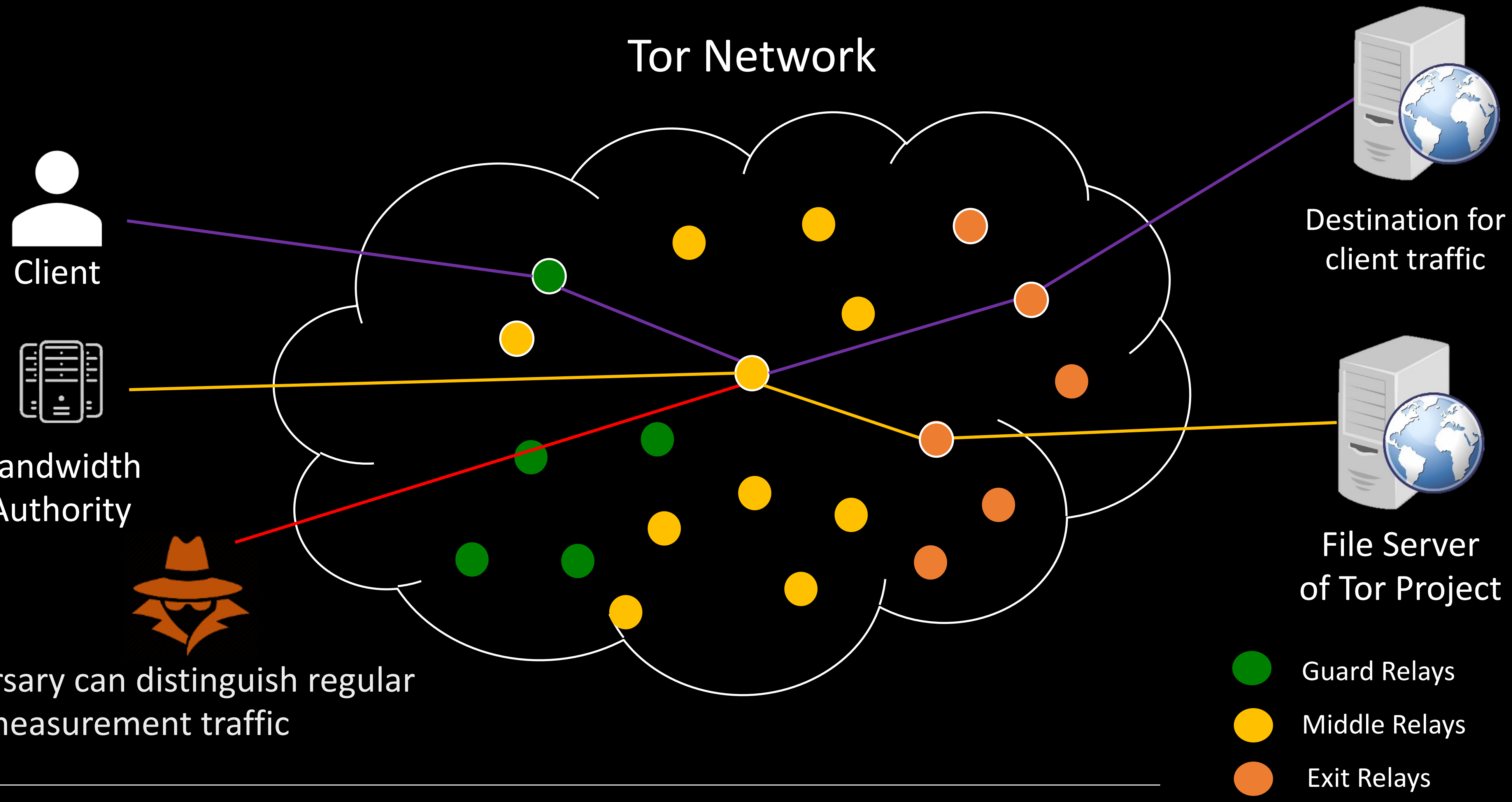


[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]



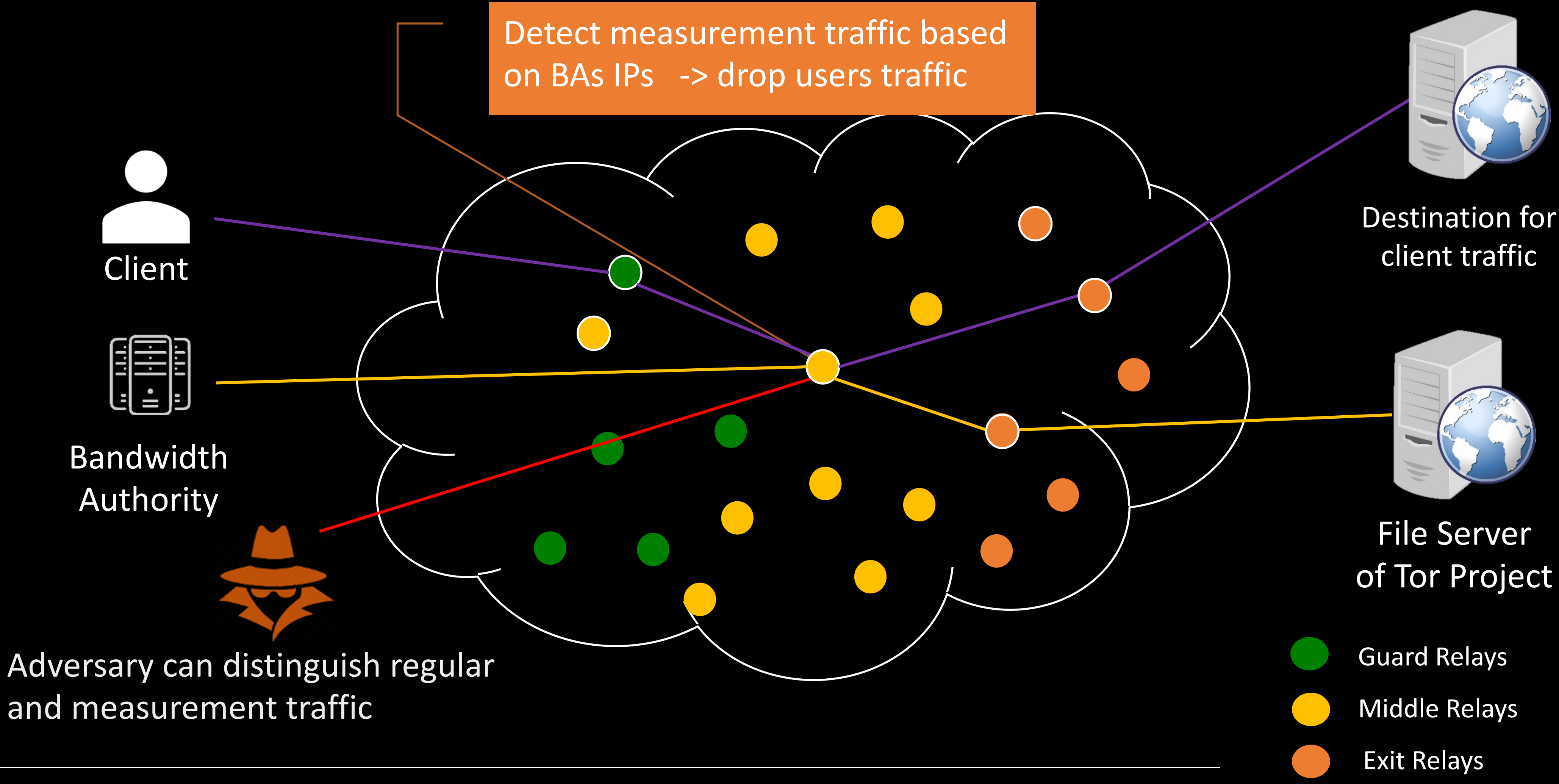
Adversary can distinguish regular and measurement traffic

[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]


Detect measurement traffic based on BAs IPs -> drop users traffic
Client
Bandwidth Authority
Destination for client traffic
File Server of Tor Project
Guard Relays
Middle Relays
Exit Relays

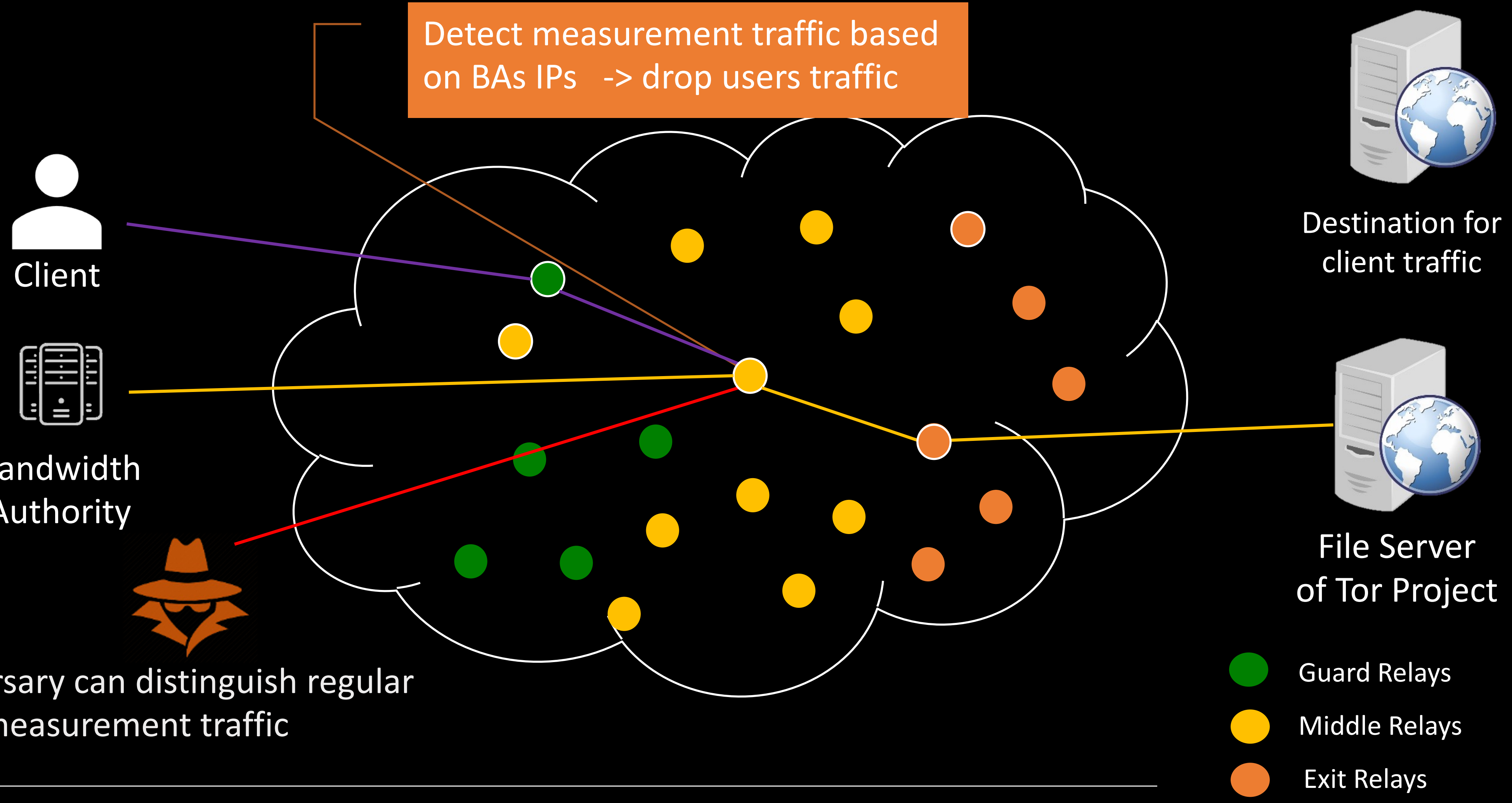
Adversary can distinguish regular and measurement traffic

[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]



Detect measurement traffic based on BAs IPs -> drop users traffic

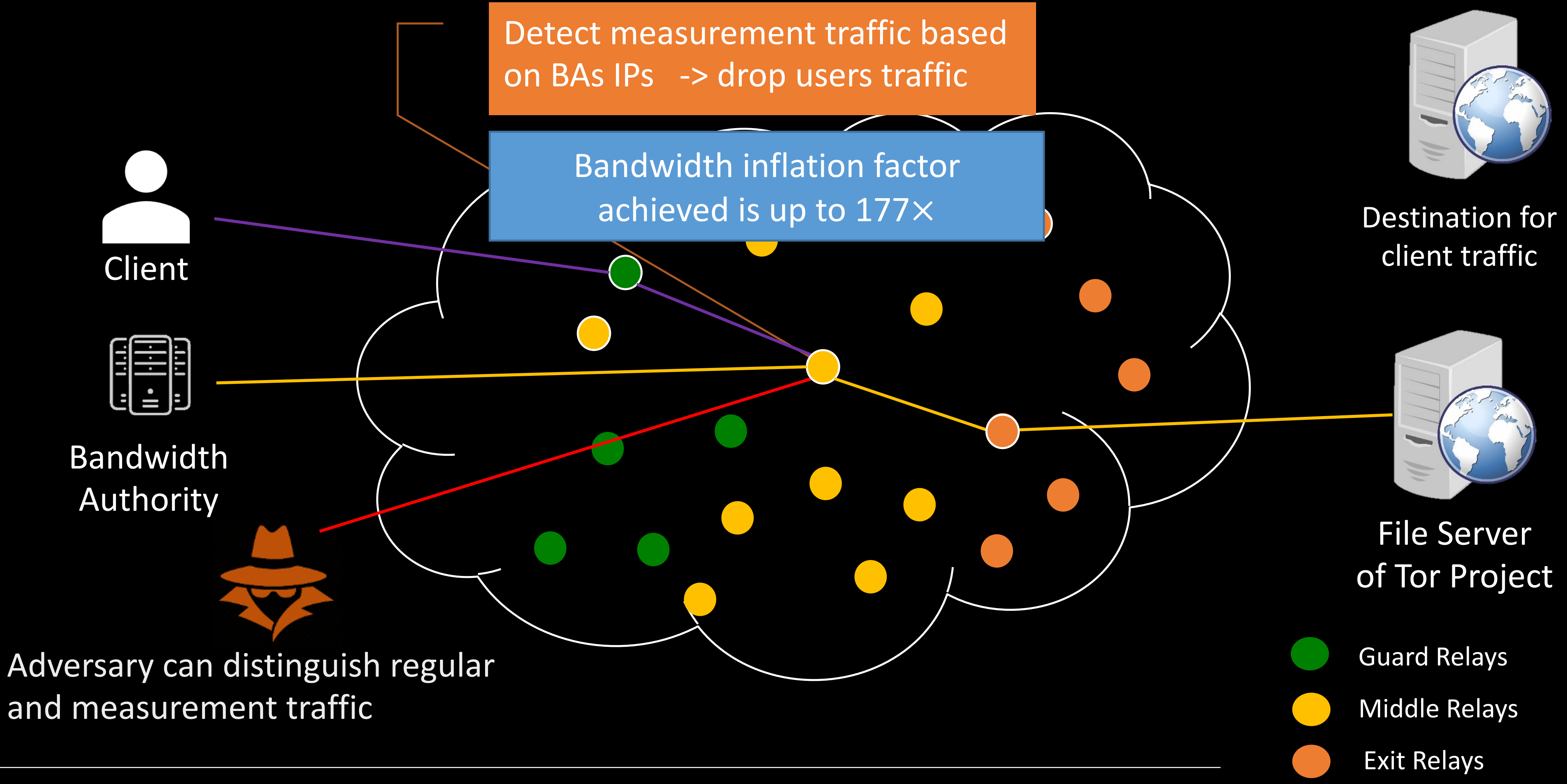
Adversary can distinguish regular and measurement traffic

[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

Bandwidth Inflation Attacks Known so Far

Biryukov et al. [1] & Johnson et al. [2]



Detect measurement traffic based on BAs IPs -> drop users traffic

Bandwidth inflation factor achieved is up to 177×

Adversary can distinguish regular and measurement traffic

[1] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, “Trawling for tor hidden services: Detection, measurement, deanonymization,” in 2013 IEEE Symposium on Security and Privacy, pp. 80–94, 2013

[2] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson, “Peerflow: Secure load balancing in tor.,” PoPETs, vol. 2017, no. 2, pp. 74–94, 2017.

MirageFlow: General Idea

- Share resources between relays

MirageFlow: General Idea

- Share resources between relays
- Once a measurement is detected, reroute it to a powerful server or drop the user traffic

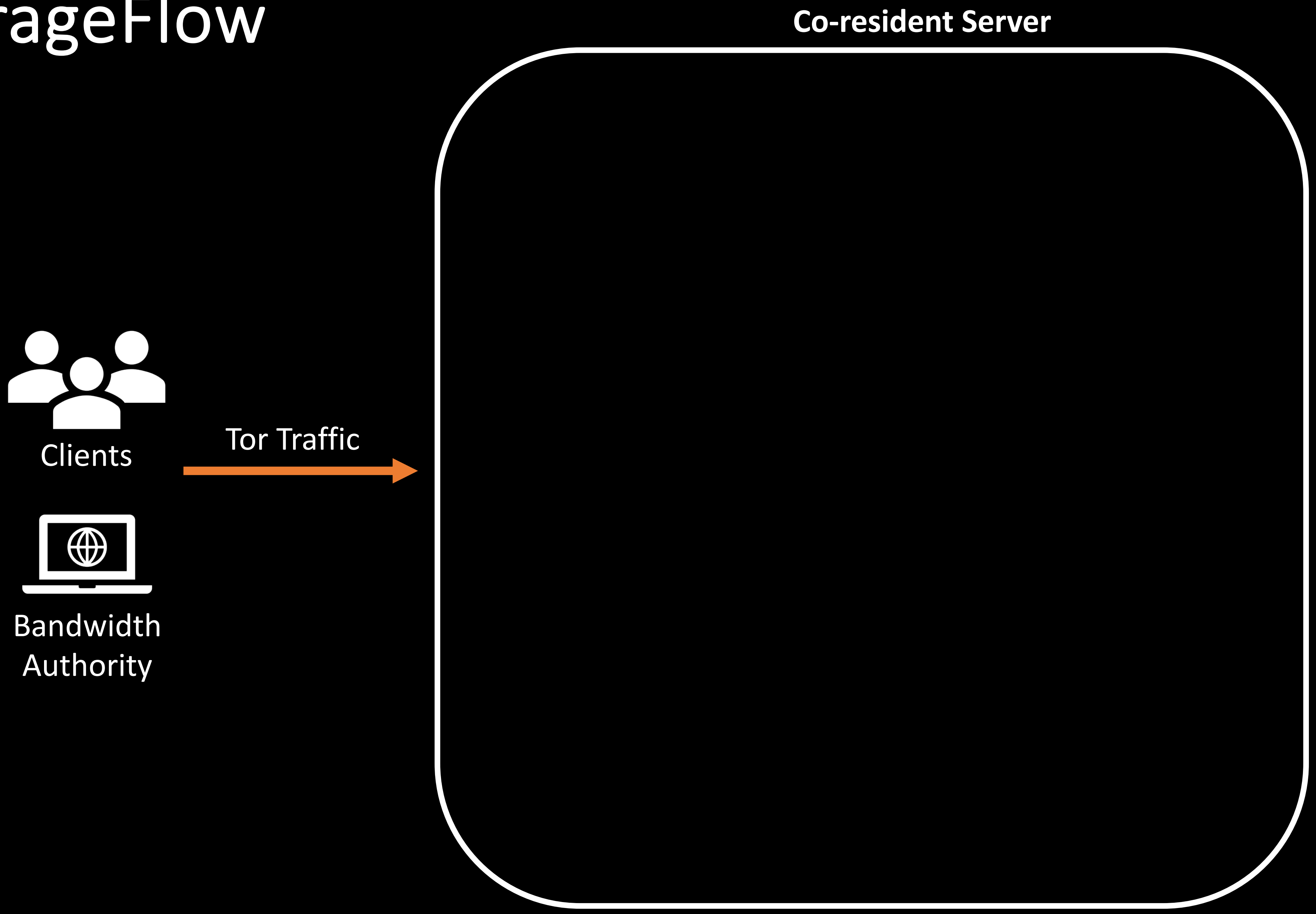
MirageFlow: General Idea

- Share resources between relays
- Once a measurement is detected, reroute it to a powerful server or drop the user traffic
- Two attack variants:
  - C-MirageFlow (Share one powerful server between relays)

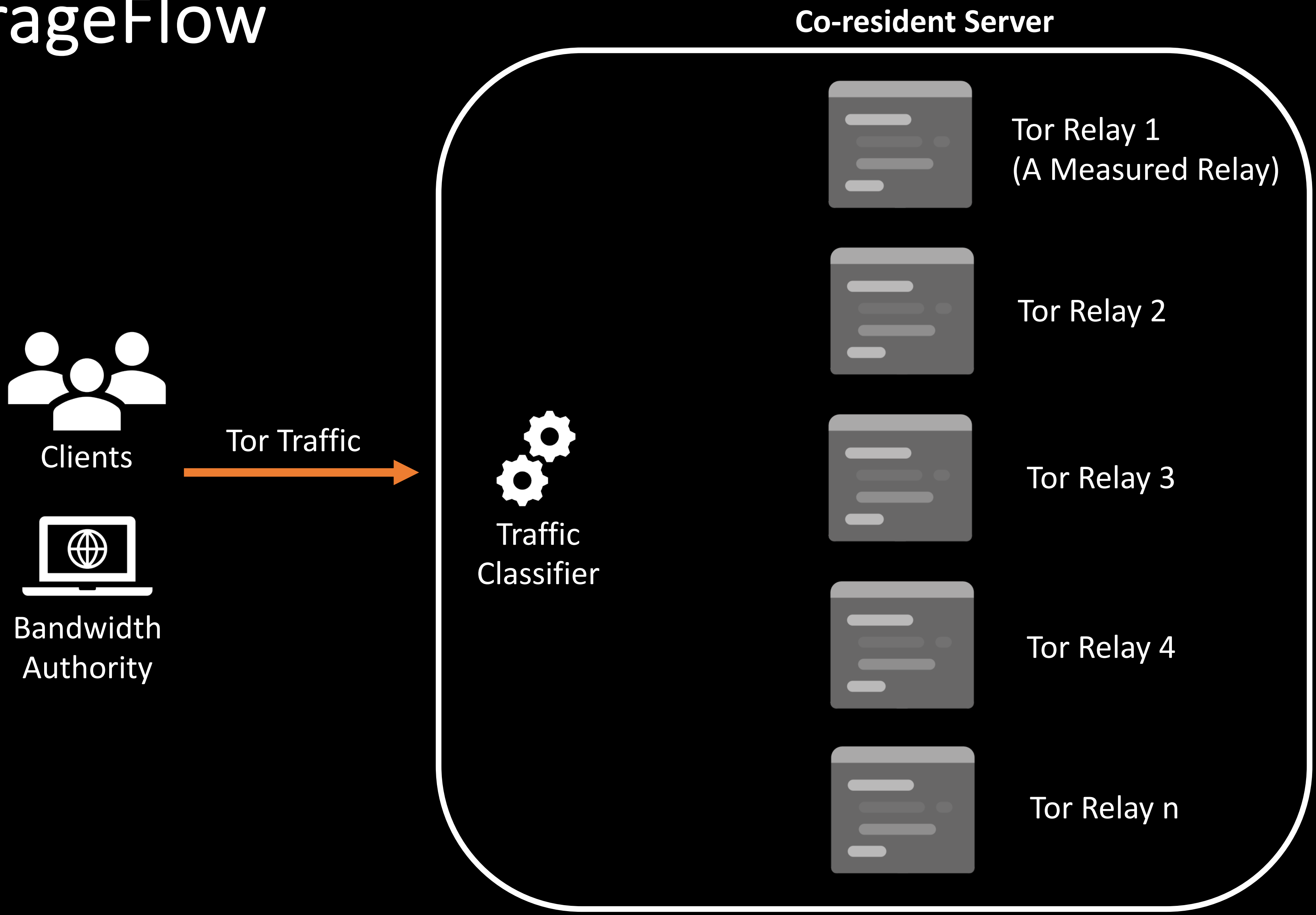
MirageFlow: General Idea

- Share resources between relays
- Once a measurement is detected, reroute it to a powerful server or drop the user traffic
- Two attack variants:
  - C-MirageFlow (Share one powerful server between relays)
  - D-MirageFlow (Use one powerful and many weak servers)

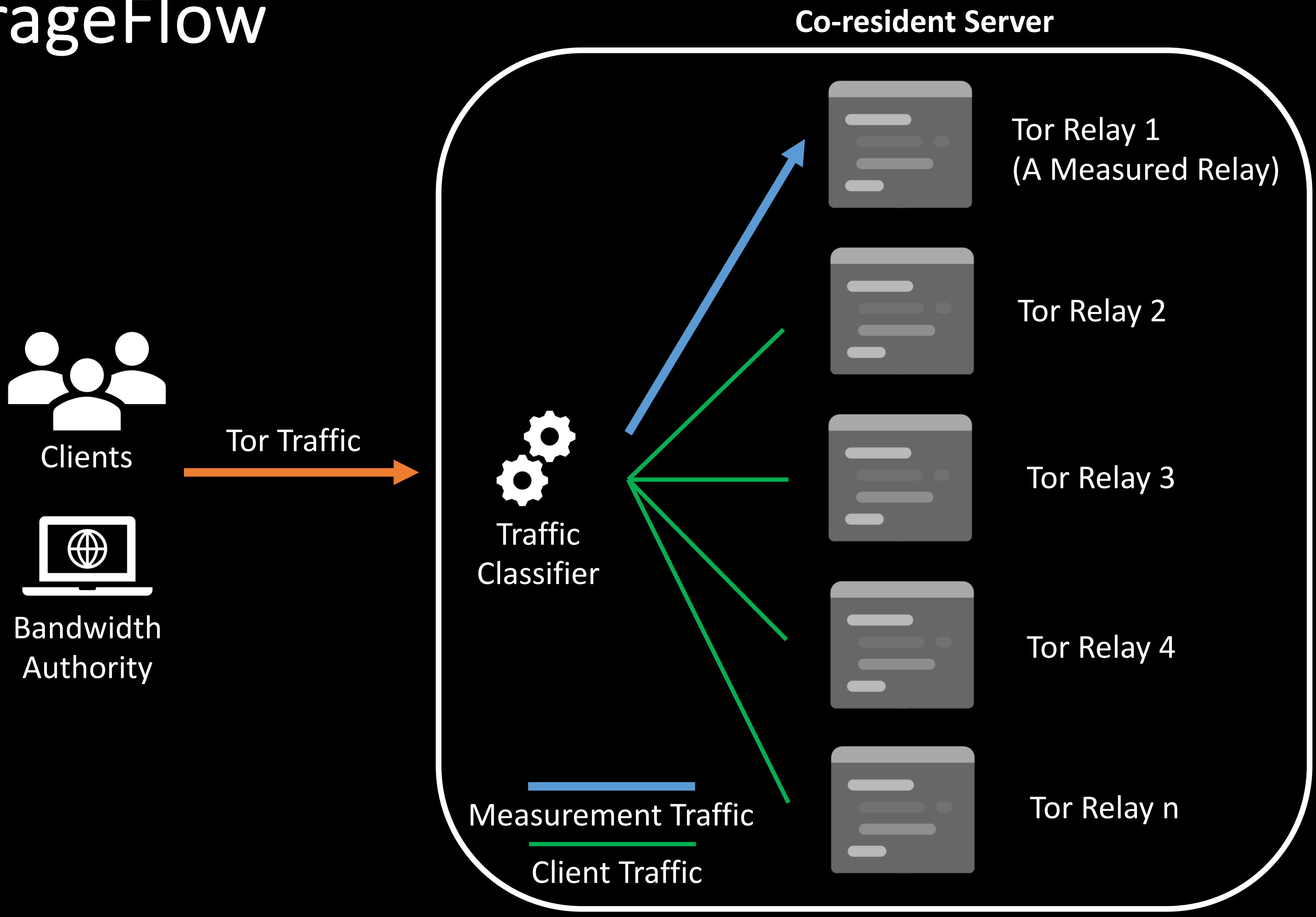
C-MirageFlow



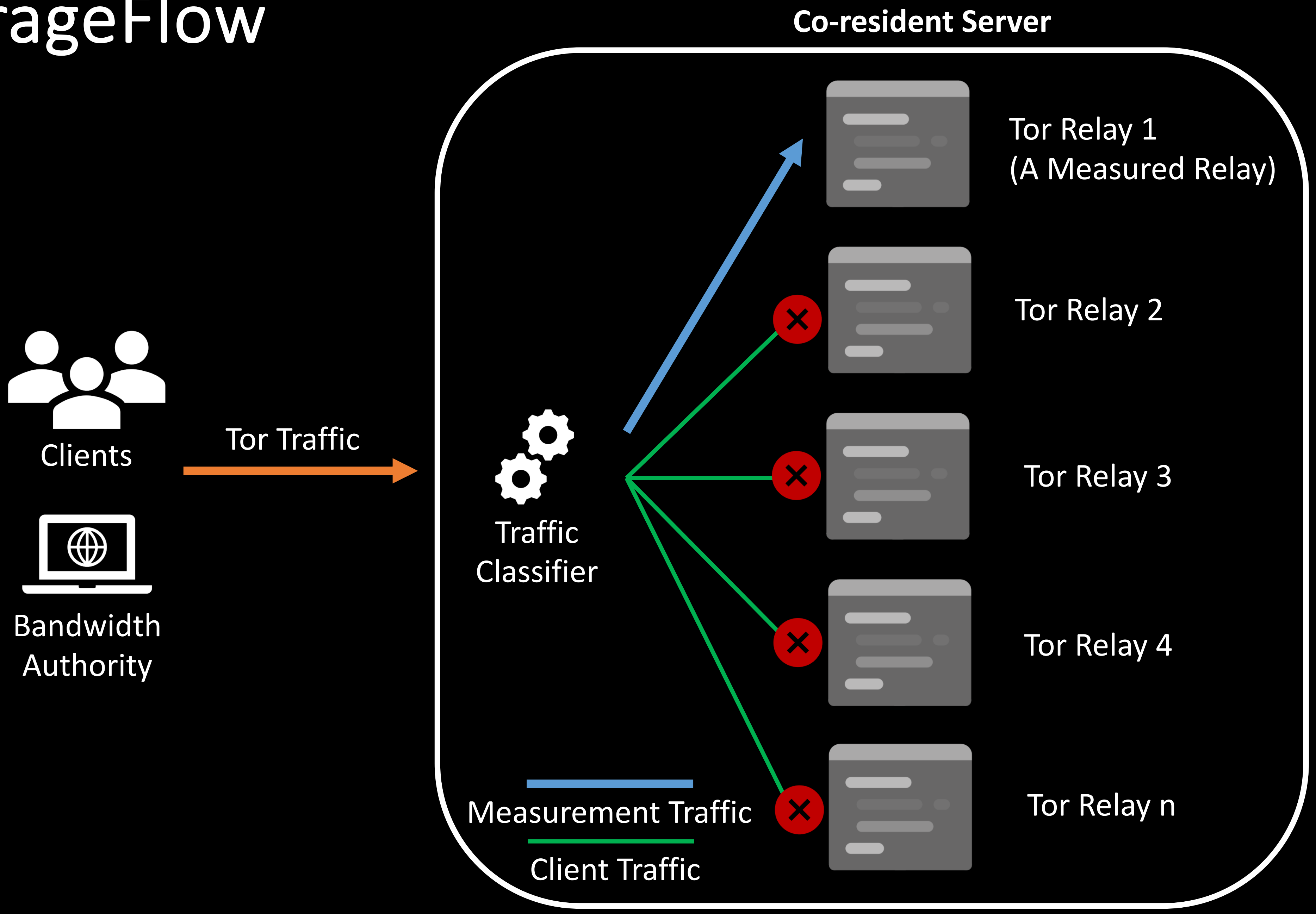
C-MirageFlow



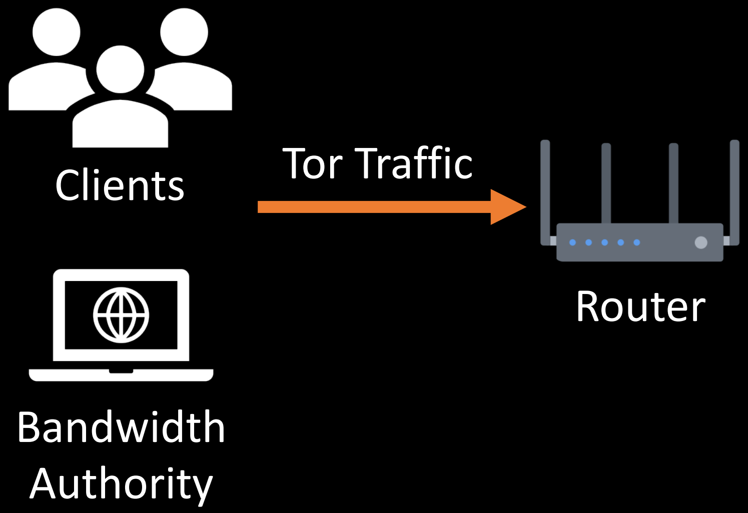
C-MirageFlow



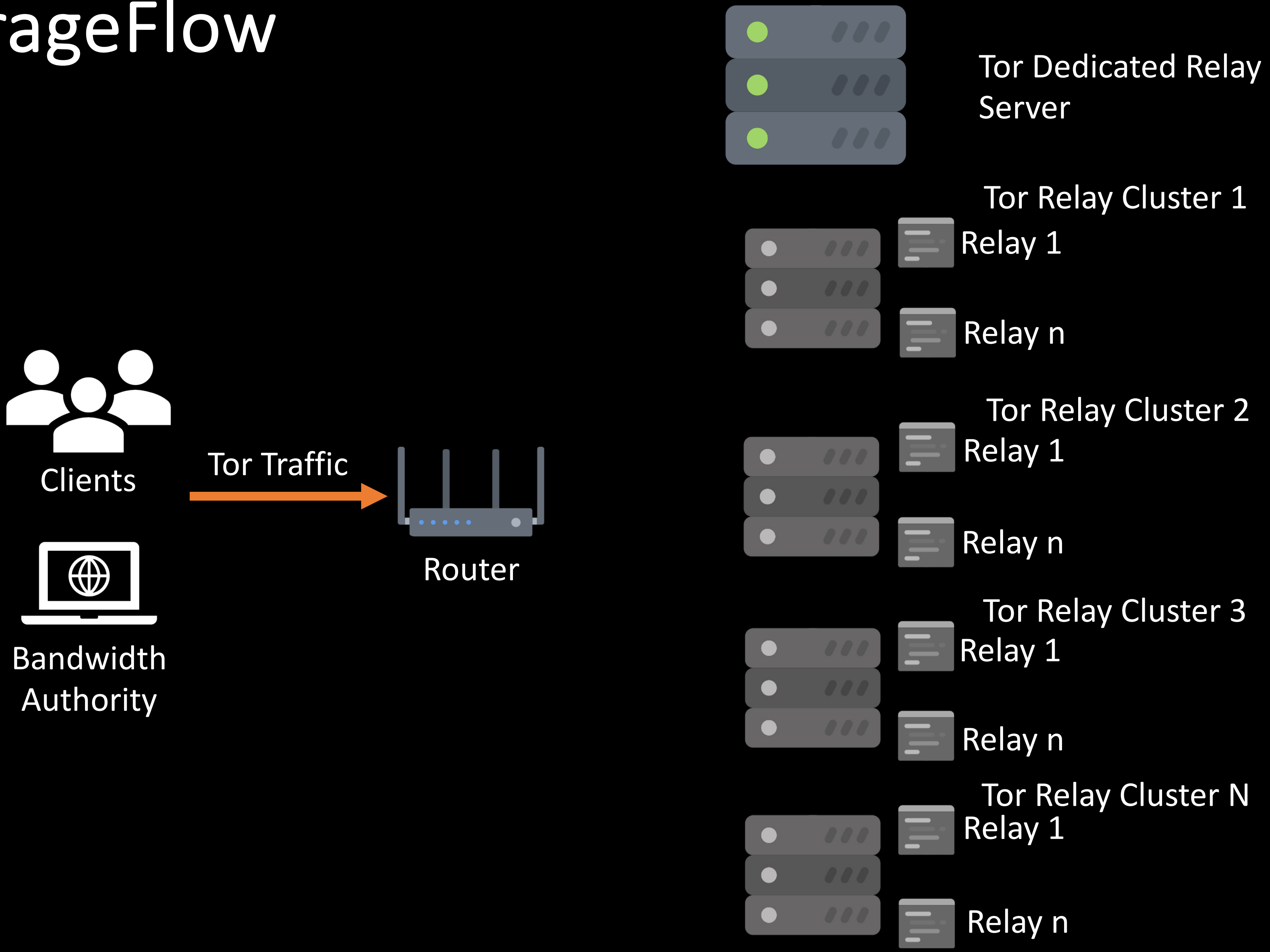
C-MirageFlow



D-MirageFlow



D-MirageFlow



Tor Dedicated Relay Server

Tor Relay Cluster 1

Relay 1

Relay n

Tor Relay Cluster 2

Relay 1

Relay n

Tor Relay Cluster 3

Relay 1

Relay n

Tor Relay Cluster N

Relay 1

Relay n

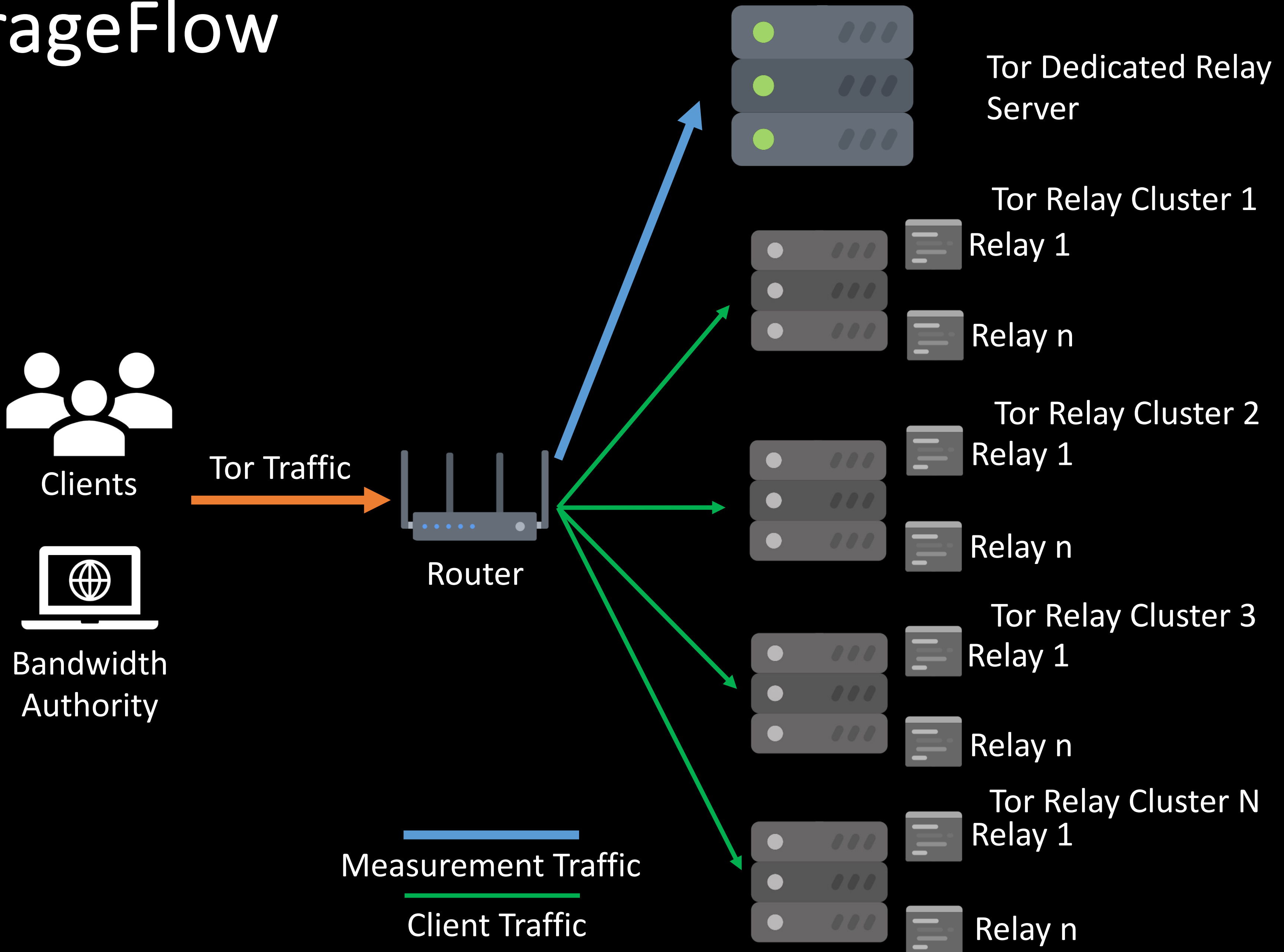
Clients

Tor Traffic

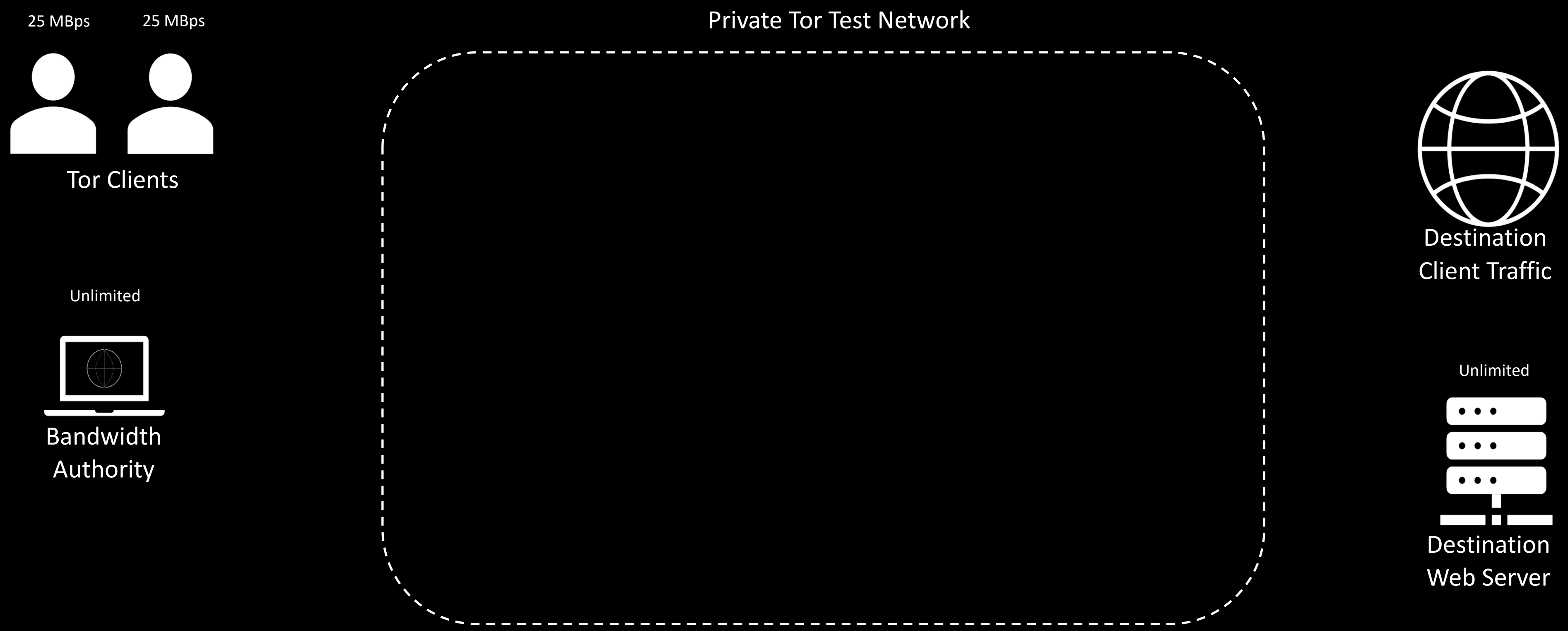
Router

Bandwidth Authority

D-MirageFlow



Evaluation Setup



25 MBps

25 MBps

Tor Clients

Unlimited

Bandwidth Authority

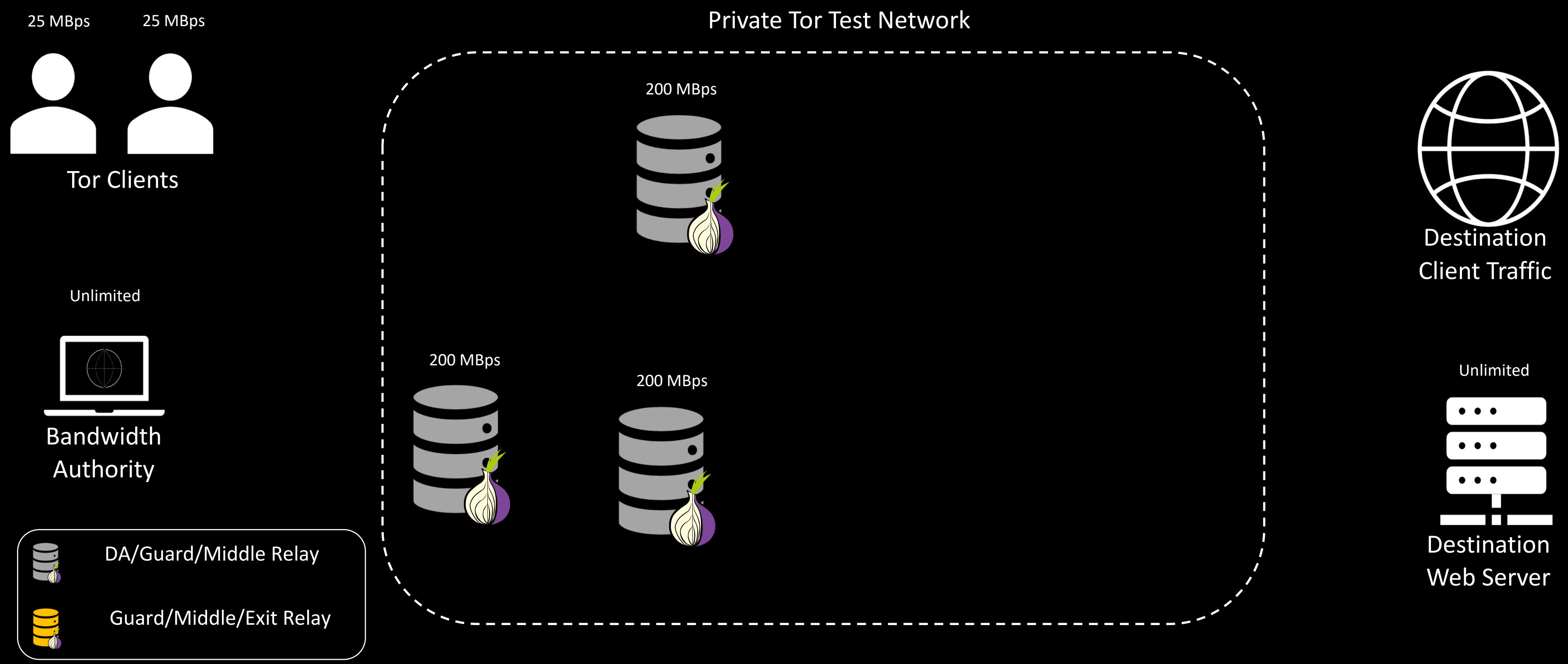
Private Tor Test Network

Destination Client Traffic

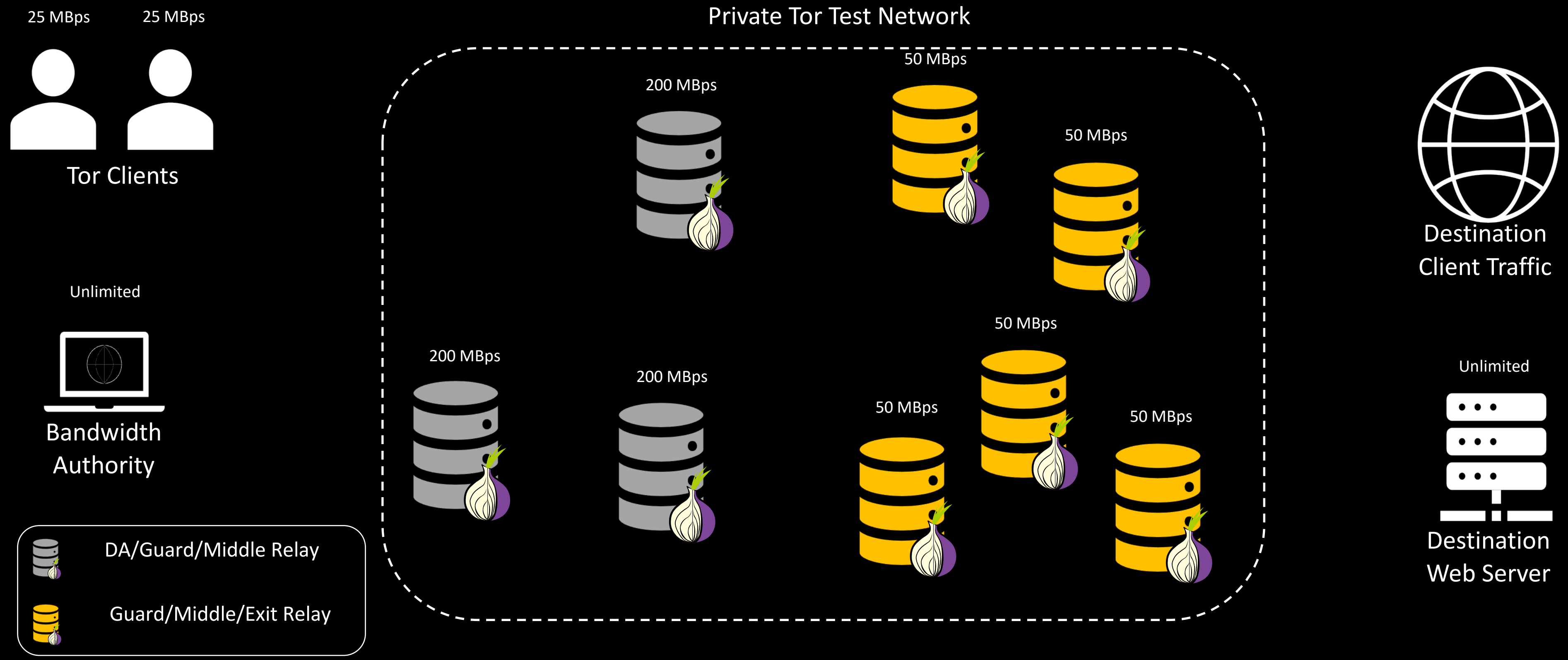
Unlimited

Destination Web Server

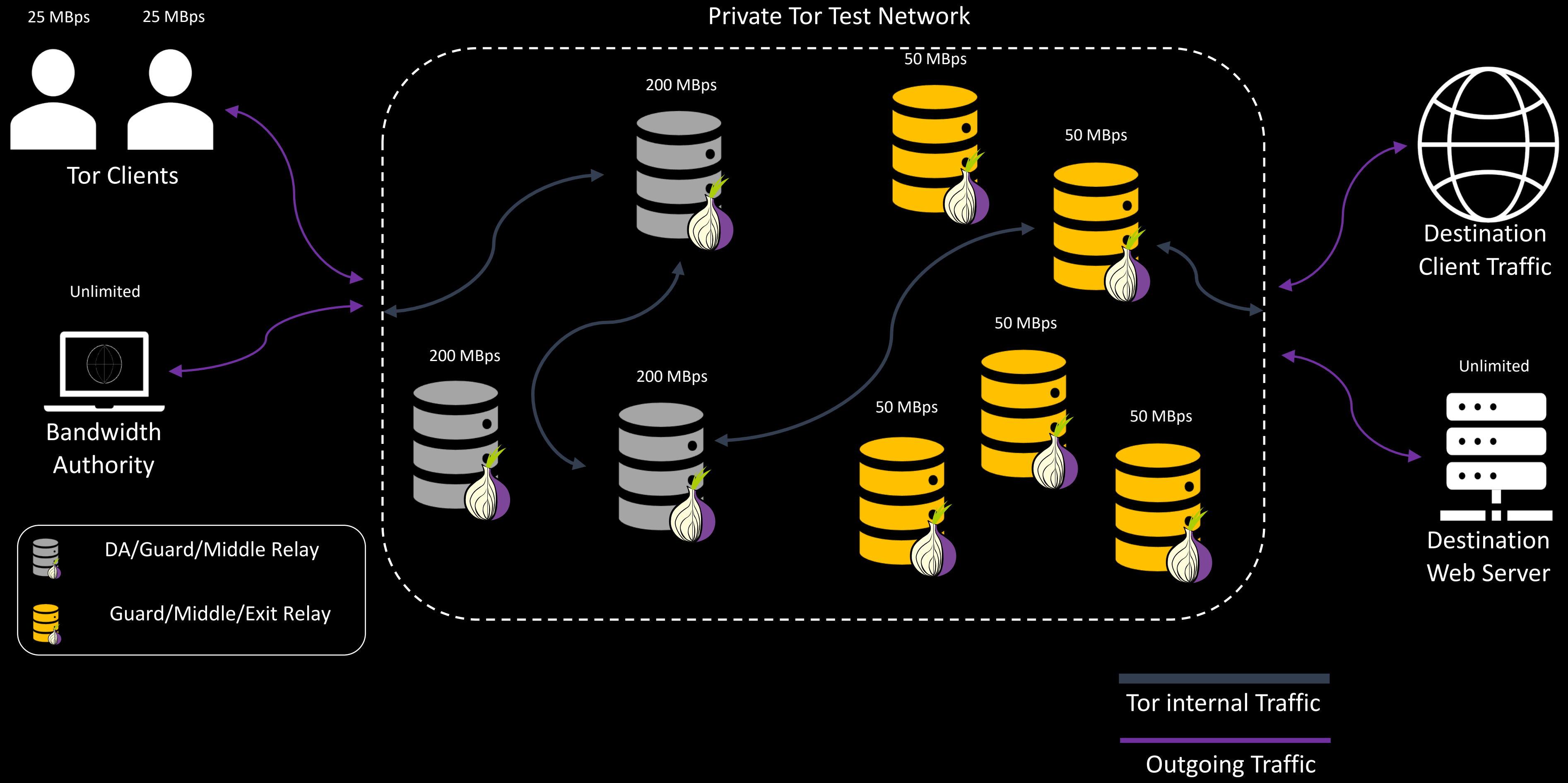
Evaluation Setup



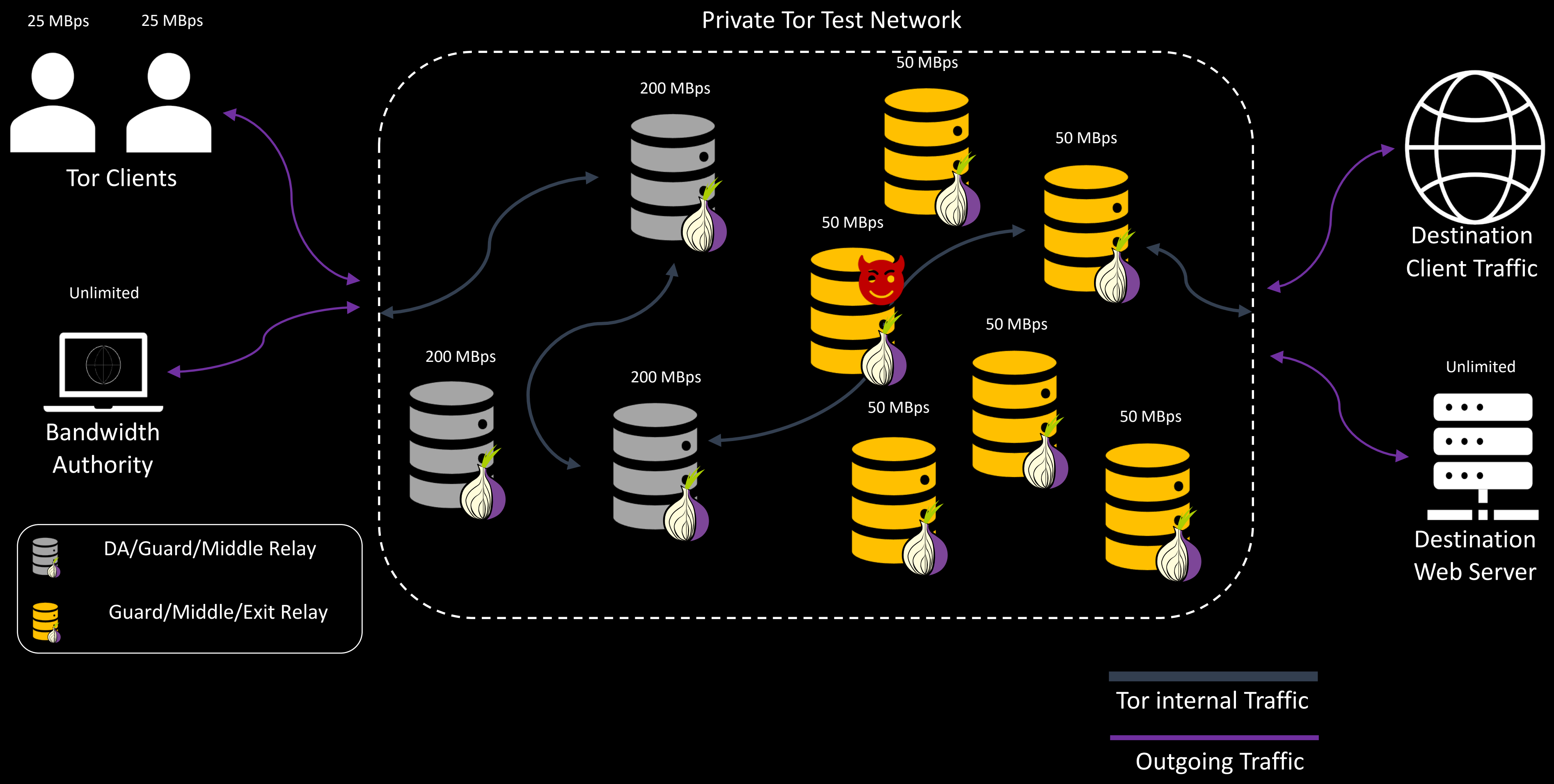
Evaluation Setup



Evaluation Setup



Evaluation Setup



Evaluation C-MirageFlow

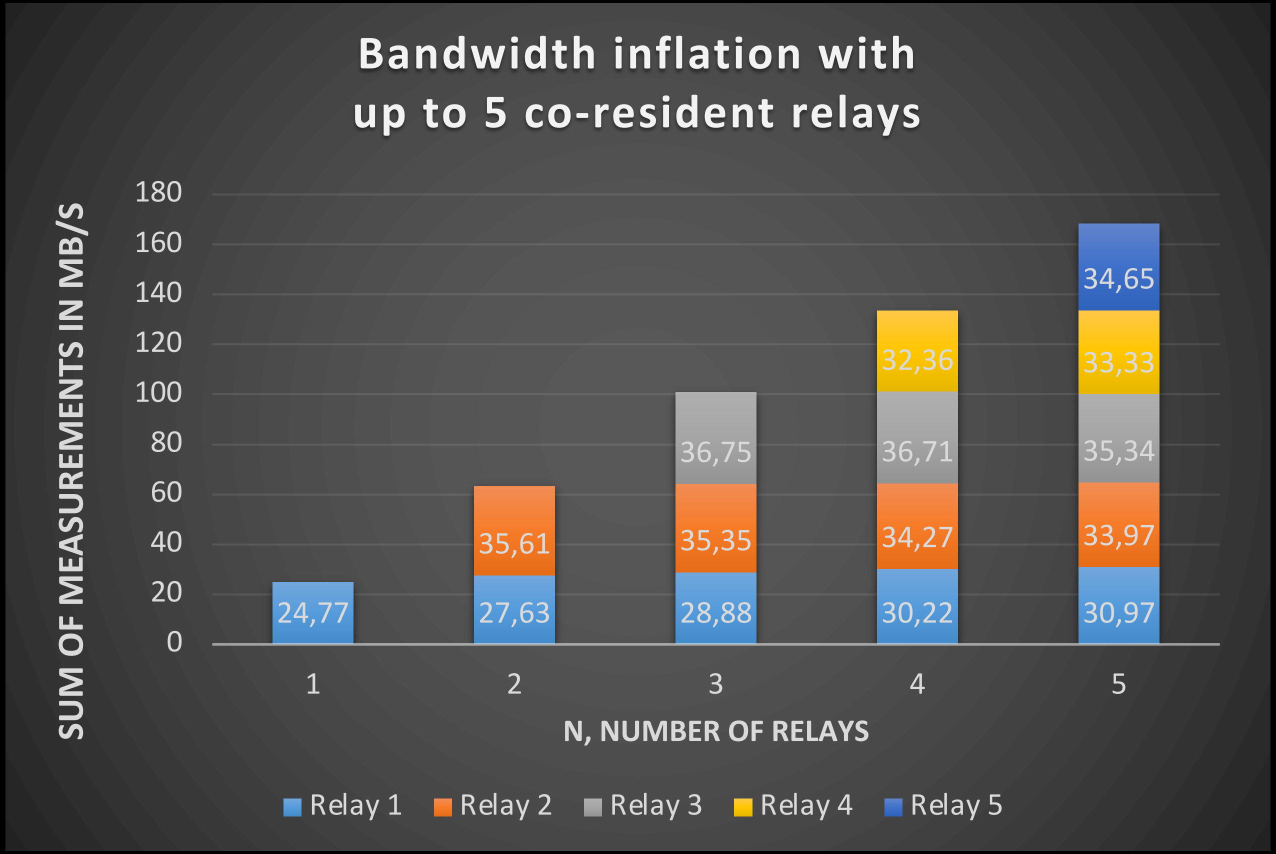
- The attack was conducted in a Tor test network (a limited number of relays)

Evaluation C-MirageFlow

- The attack was conducted in a Tor test network (a limited number of relays)
- The server has a bandwidth of 50 MB/s

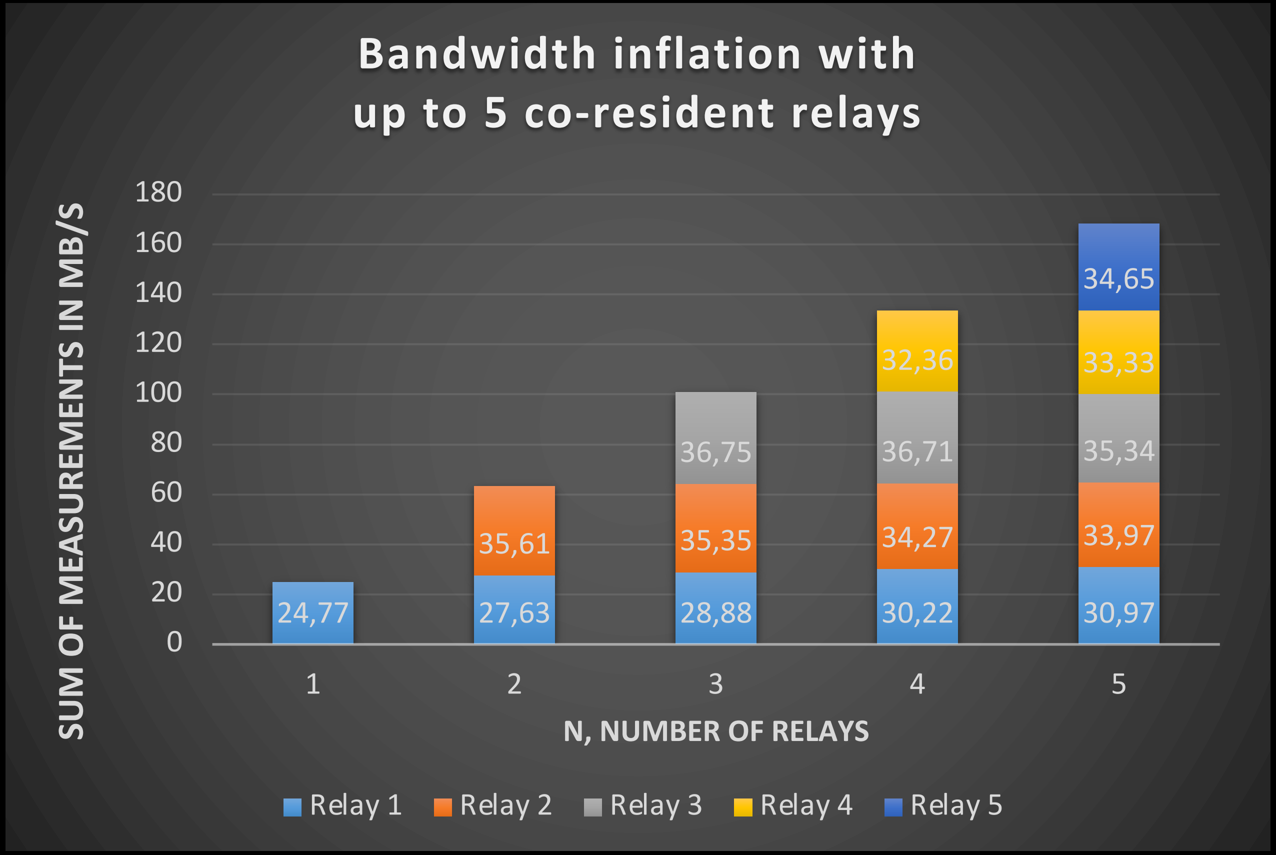
Evaluation C-MirageFlow

- The attack was conducted in a Tor test network (a limited number of relays)
- The server has a bandwidth of 50 MB/s



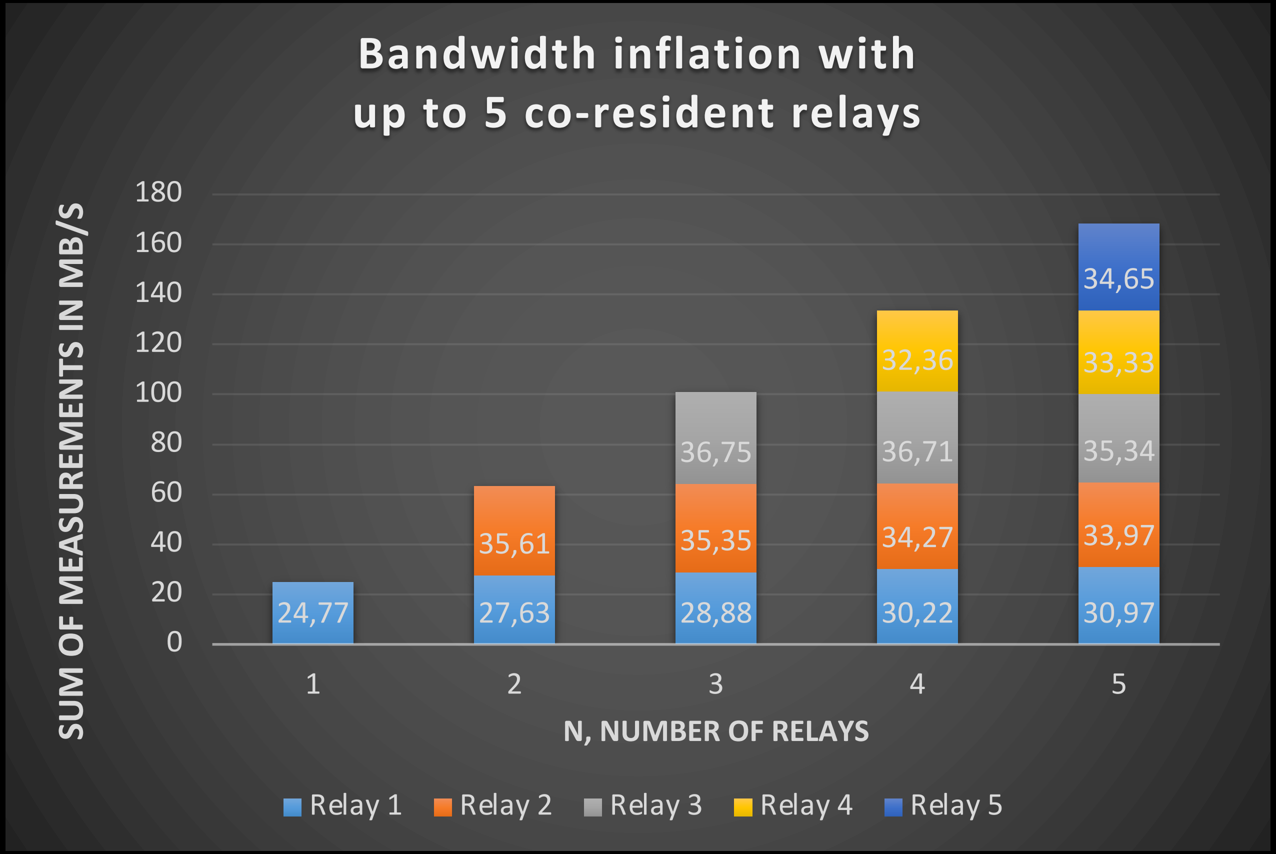
Evaluation C-MirageFlow

- The attack was conducted in a Tor test network (a limited number of relays)
- The server has a bandwidth of 50 MB/s
- Inflation of up to 336% (168 MB/s) for five relays can be achieved



Evaluation C-MirageFlow

- The attack was conducted in a Tor test network (a limited number of relays)
- The server has a bandwidth of 50 MB/s
- Inflation of up to 336% (168 MB/s) for five relays can be achieved
- Achieves an inflation factor close to N based on measurement of the first relay



Evaluation D-MirageFlow

- Three relay clusters (bandwidth of 25MB/s each) were instantiated as VMs, each hosting six Tor relays

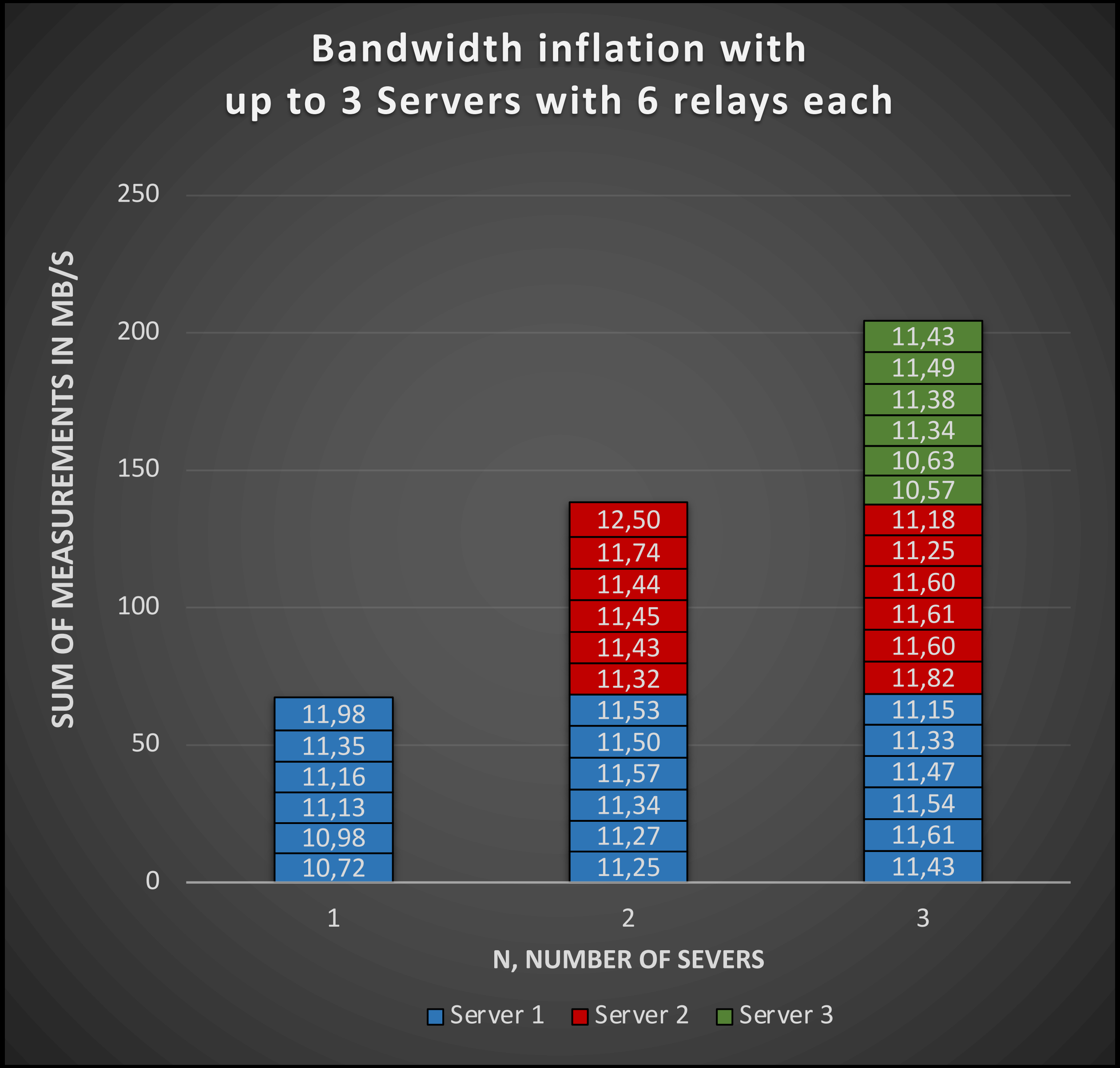
Evaluation D-MirageFlow

- Three relay clusters (bandwidth of 25MB/s each) were instantiated as VMs, each hosting six Tor relays

- A dedicated server and router with a bandwidth of 50MB/s each were utilized

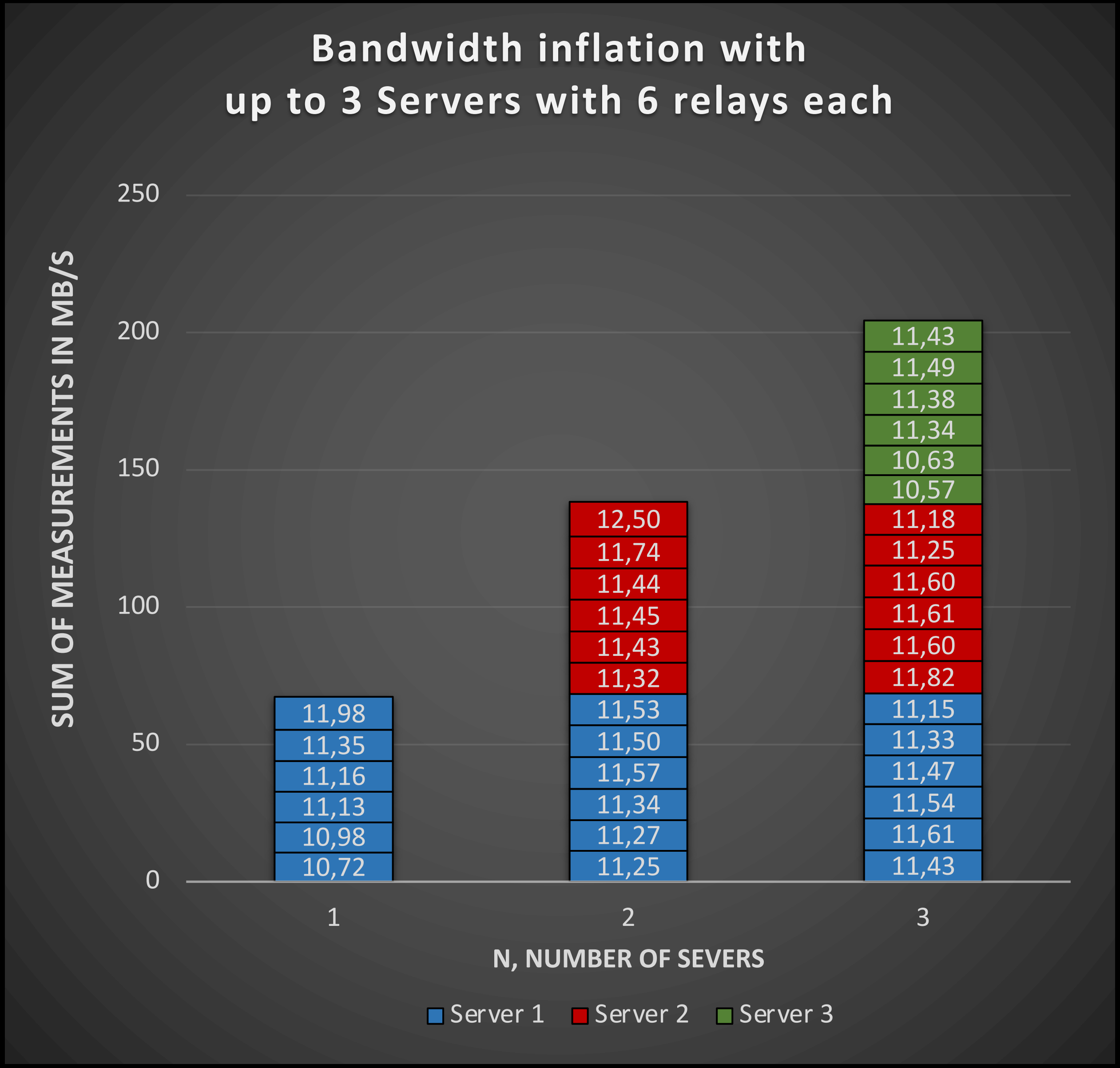
Evaluation D-MirageFlow

- Three relay clusters (bandwidth of 25MB/s each) were instantiated as VMs, each hosting six Tor relays
- A dedicated server and router with a bandwidth of 50MB/s each were utilized



Evaluation D-MirageFlow

- Three relay clusters (bandwidth of 25MB/s each) were instantiated as VMs, each hosting six Tor relays
- A dedicated server and router with a bandwidth of 50MB/s each were utilized
- The total measured bandwidth was inflated by 272% (204MB/s)



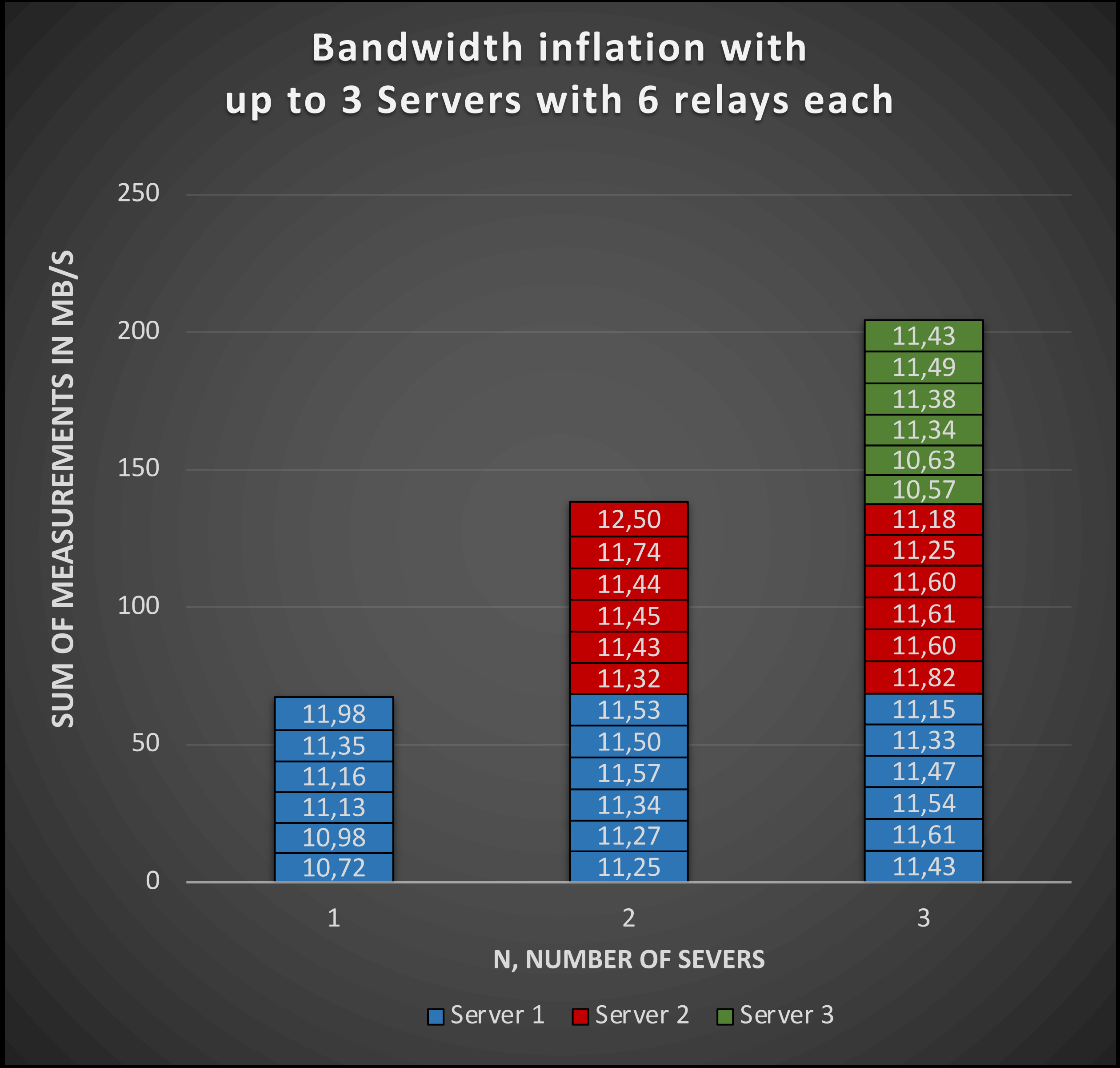
Evaluation D-MirageFlow

- Three relay clusters (bandwidth of 25MB/s each) were instantiated as VMs, each hosting six Tor relays

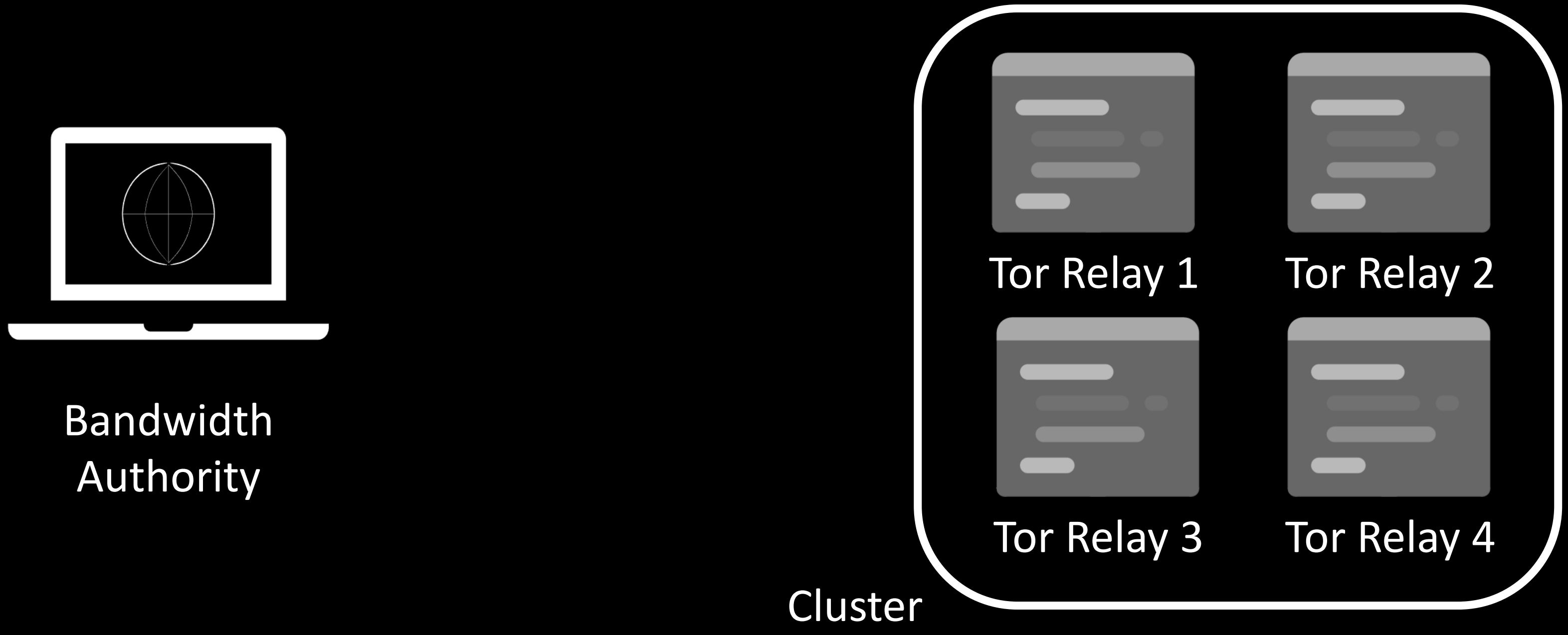
- A dedicated server and router with a bandwidth of 50MB/s each were utilized

- The total measured bandwidth was inflated by 272% (204MB/s)

- Achieves an inflation factor close to n*N (n number of relays and N number of servers) based on measurement of the first relay


Bandwidth inflation with up to 3 Servers with 6 relays each

Limitation: Co-Measurement



Bandwidth Authority

Tor Relay 1

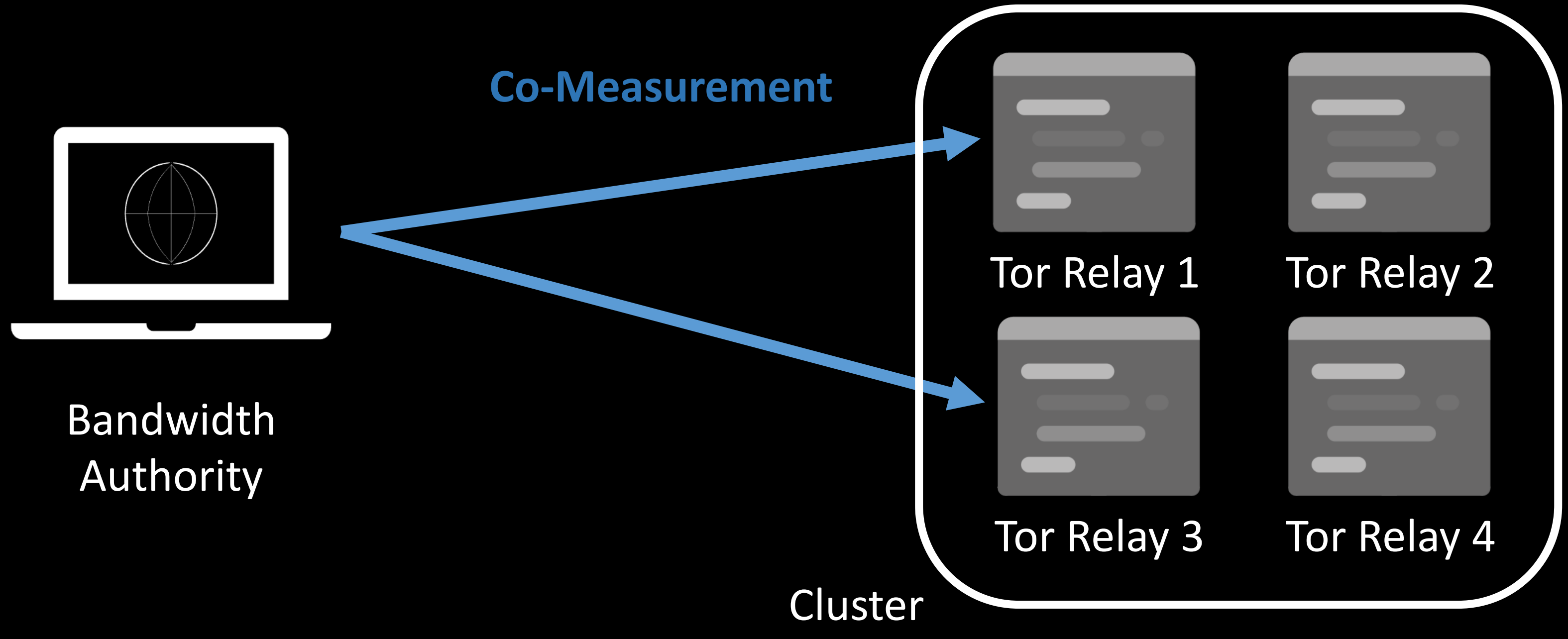
Tor Relay 2

Tor Relay 3

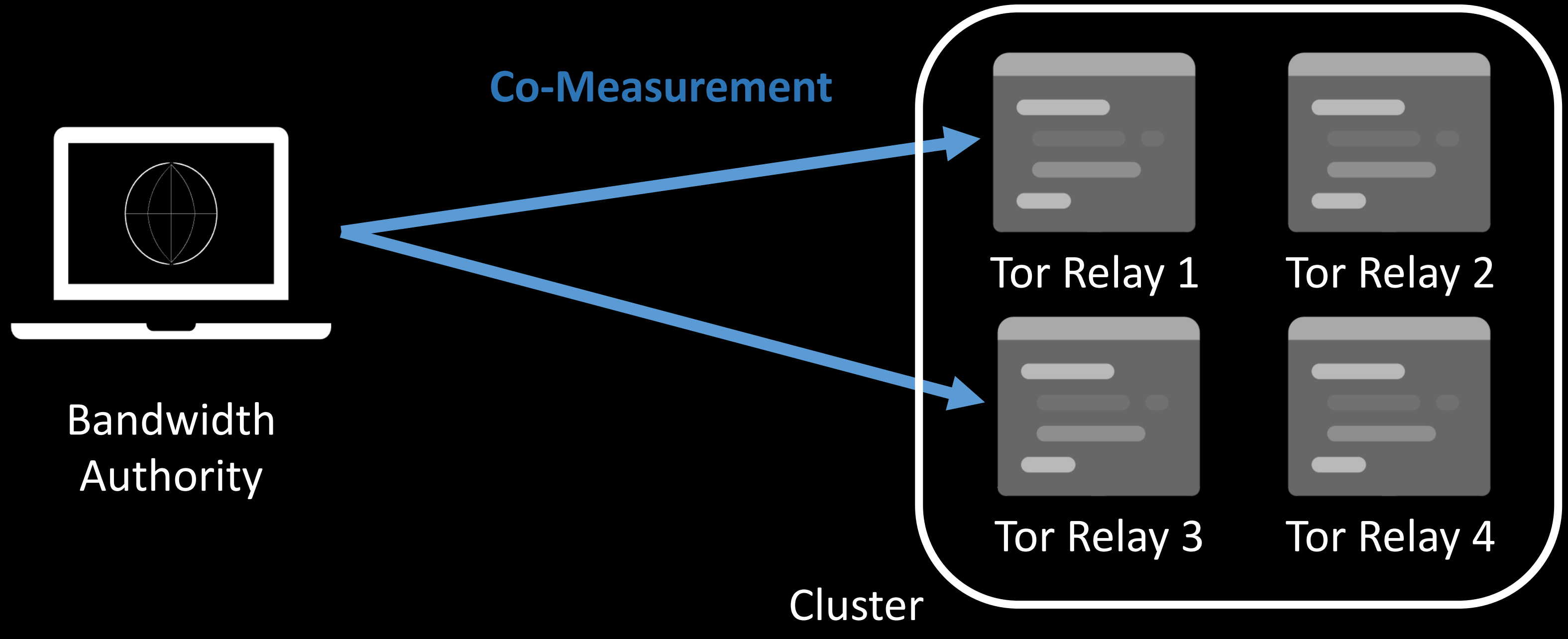
Tor Relay 4

Cluster

Limitation: Co-Measurement

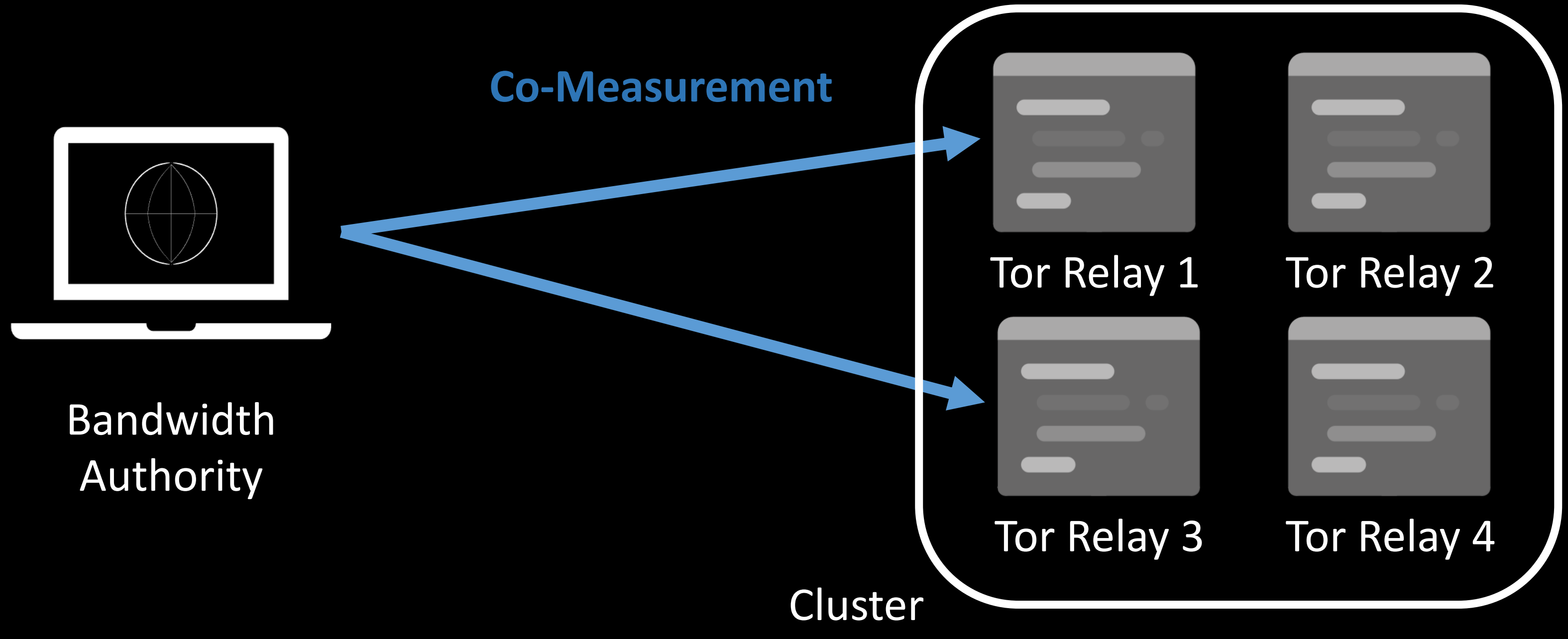


Limitation: Co-Measurement



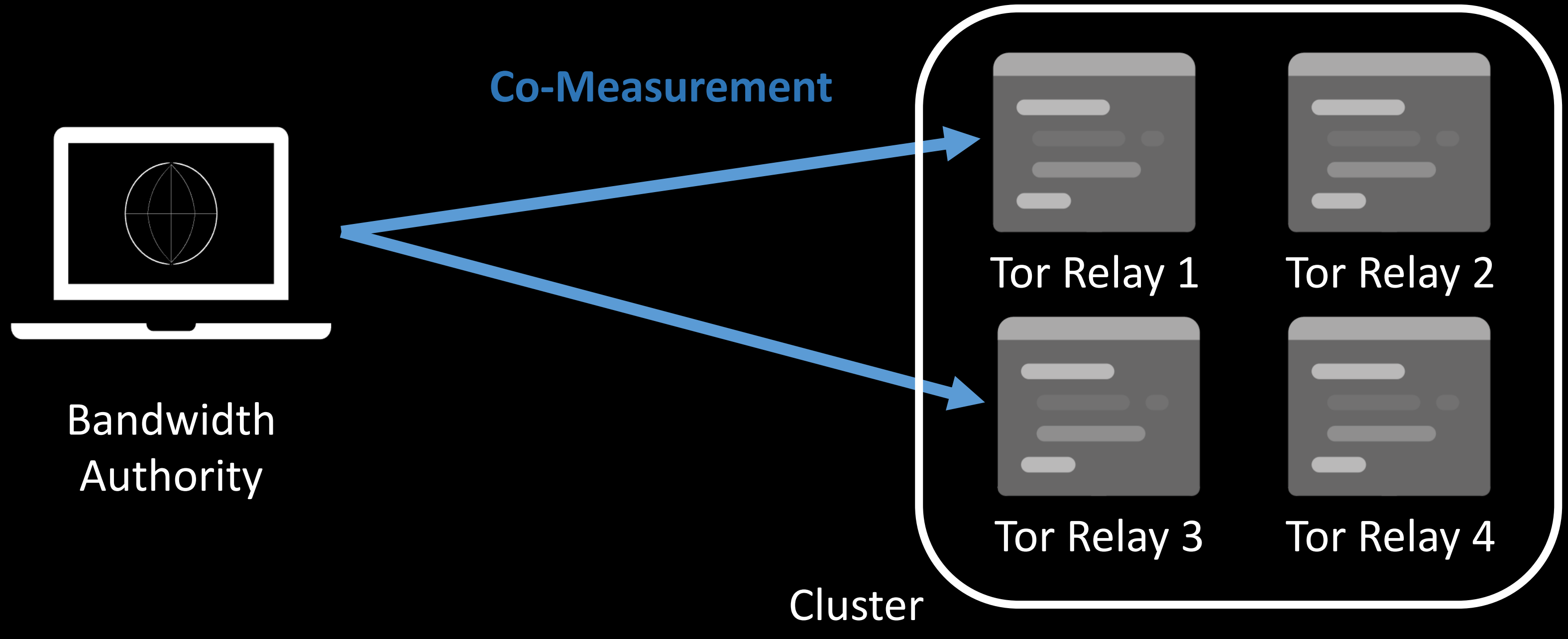
- Co-Measurements (two or more relays in the cluster are measured simultaneously) greatly limit the inflation factor of the attack

Limitation: Co-Measurement



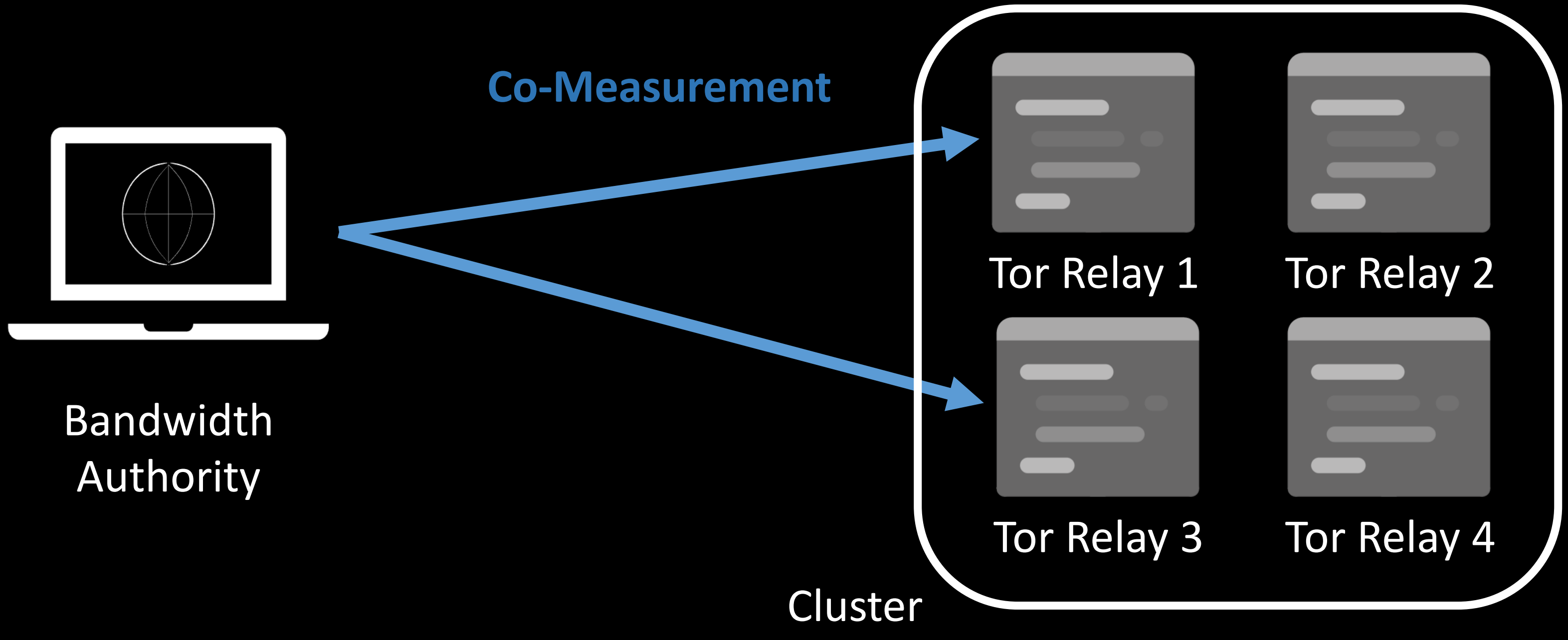
- Co-Measurements (two or more relays in the cluster are measured simultaneously) greatly limit the inflation factor of the attack
- Theoretical analysis was performed using historical bandwidth data from May to July 2022

Limitation: Co-Measurement



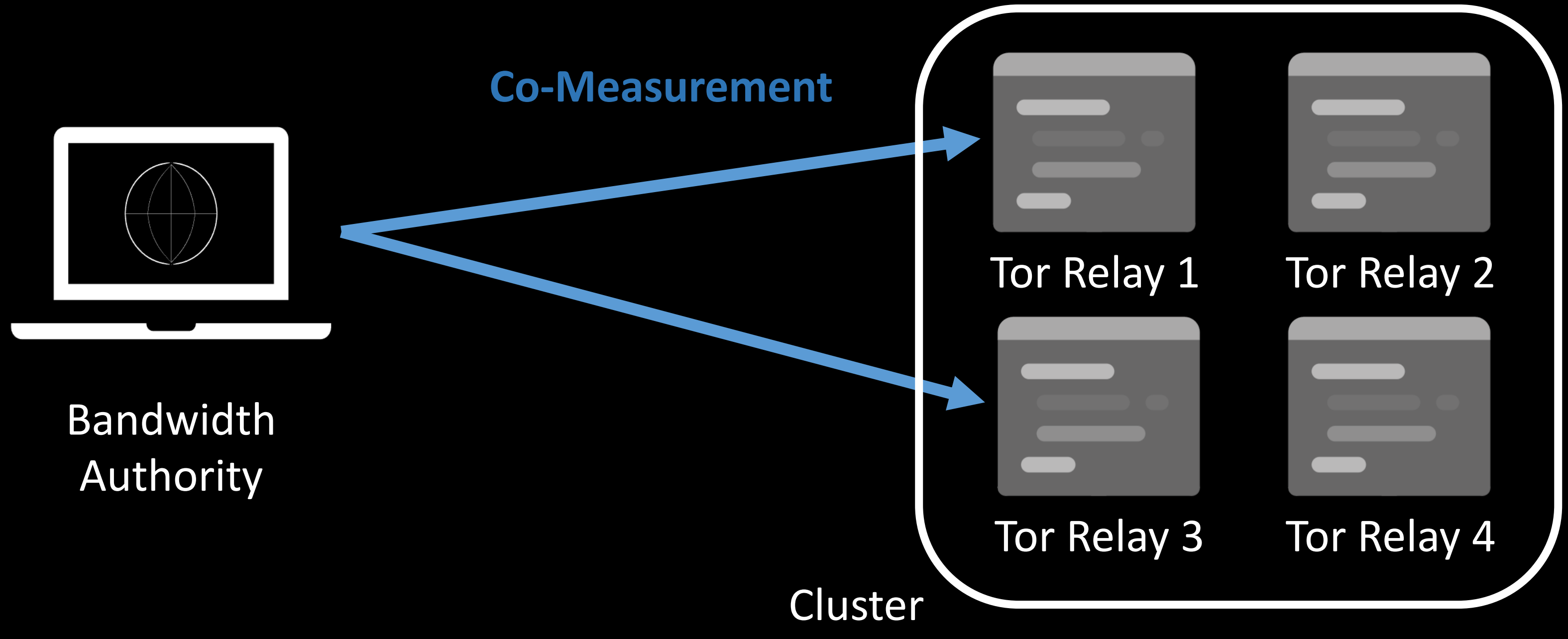
- Co-Measurements (two or more relays in the cluster are measured simultaneously) greatly limit the inflation factor of the attack
- Theoretical analysis was performed using historical bandwidth data from May to July 2022
- Co-measurements rarely occur for clusters of up to 120 relays

Limitation: Co-Measurement



- Co-Measurements (two or more relays in the cluster are measured simultaneously) greatly limit the inflation factor of the attack
- Theoretical analysis was performed using historical bandwidth data from May to July 2022
- Co-measurements rarely occur for clusters of up to 120 relays
- Inflation factor of up to 92 times with 120 relays is theoretically possible

Limitation: Co-Measurement



- Co-Measurements (two or more relays in the cluster are measured simultaneously) greatly limit the inflation factor of the attack
- Theoretical analysis was performed using historical bandwidth data from May to July 2022
- Co-measurements rarely occur for clusters of up to 120 relays
- Inflation factor of up to 92 times with 120 relays is theoretically possible
- With 10 dedicated servers (100MB/s and 109 relays each) running the MirageFlow attack 50% of Tor’s traffic can be controlled

Countermeasures

Detection based on historical data

Countermeasures

Detection based on historical data

Active detection by probing

Countermeasures

Detection based on historical data

Active detection by probing

Eliminating Explicit Measurement Traffic

Countermeasures

- Detection based on historical data
- Active detection by probing
- Eliminating Explicit Measurement Traffic
- Obscuring Measurement Traffic

Countermeasures

Detection based on historical data

Active detection by probing

Eliminating Explicit Measurement Traffic

Obscuring Measurement Traffic

Detection Based on Historical Data

If co-resident relays are co-measured, bandwidth measurement will drop

Detection Based on Historical Data

If co-resident relays are co-measured, bandwidth measurement will drop

Can be done by using historical BW files

Detection Based on Historical Data

If co-resident relays are co-measured, bandwidth measurement will drop

Can be done by using historical BW files

Detection Based on Historical Data

If co-resident relays are co-measured, bandwidth measurement will drop

Can be done by using historical BW files

- No deterministic timeline can be restored, as BW files only include the end of measurement

Detection Based on Historical Data

If co-resident relays are co-measured, bandwidth measurement will drop

Can be done by using historical BW files

- No deterministic timeline can be restored, as BW files only include the end of measurement
- Probabilistic timeline reveals possible relays applying MirageFlow

Detection Based on Historical Data

If co-resident relays are co-measured, bandwidth measurement will drop

Can be done by using historical BW files

- No deterministic timeline can be restored, as BW files only include the end of measurement
- Probabilistic timeline reveals possible relays applying MirageFlow
- BAs, however, have all the necessary information

Conclusion

We propose a new bandwidth inflation attack technique

Conclusion

We propose a new bandwidth inflation attack technique

Attack can be combined with previously known bandwidth inflation methods

Conclusion

- We propose a new bandwidth inflation attack technique
- Attack can be combined with previously known bandwidth inflation methods
- Some observations suggest that this attack technique might be in use in the wild

Conclusion

- We propose a new bandwidth inflation attack technique
- Attack can be combined with previously known bandwidth inflation methods
- Some observations suggest that this attack technique might be in use in the wild
- Countermeasures are either limited or not very practical

Conclusion

- We propose a new bandwidth inflation attack technique
- Attack can be combined with previously known bandwidth inflation methods
- Some observations suggest that this attack technique might be in use in the wild
- Countermeasures are either limited or not very practical
- There is a need for a more resilient measurement solution