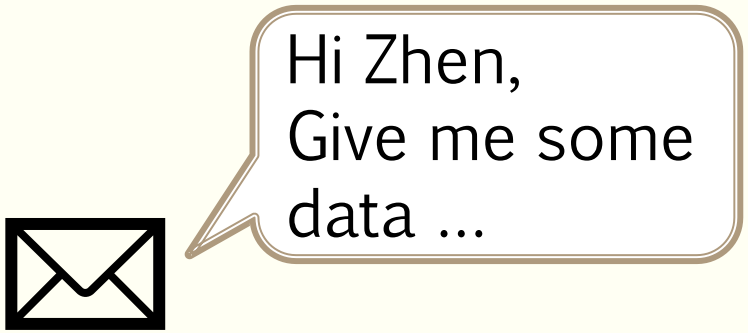
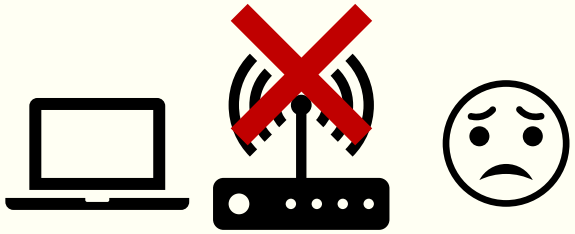
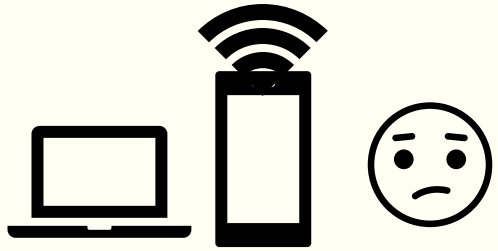
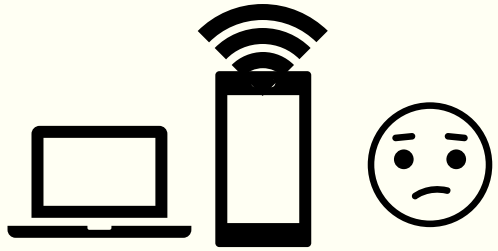
TOWARDS A SECURE ZERO-RATING FRAMEWORK WITH THREE PARTIES

Authors: Zhiheng Liu, **Zhen Zhang**, Yinzhi Cao†, Zhaohan Xi, Shihao Jing and Humberto La Roche ‡
Lehigh University, †Johns Hopkins University/Lehigh University, ‡Cisco System

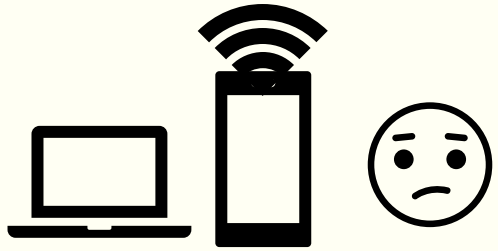

Hi Zhen,
Give me some
data ...



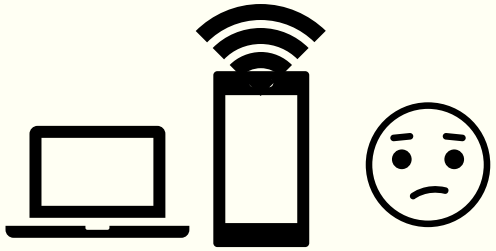


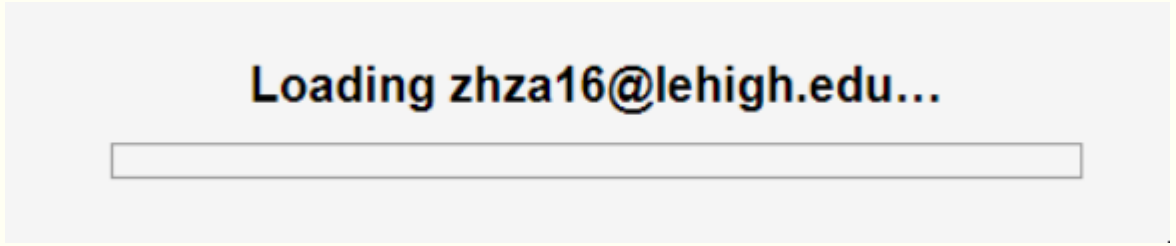


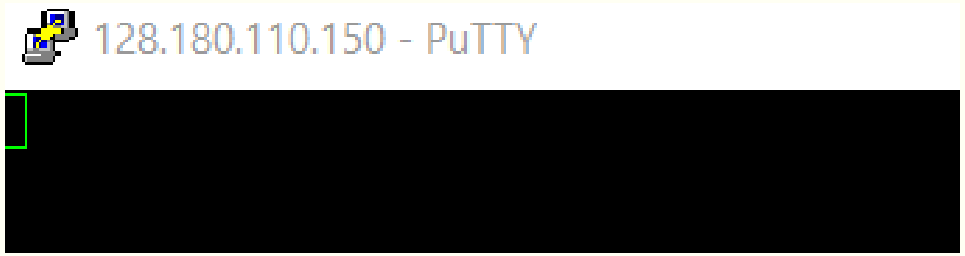

2G...



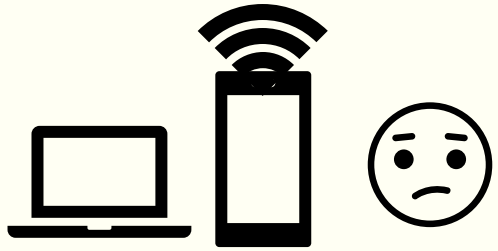
Loading zhza16@lehigh.edu…

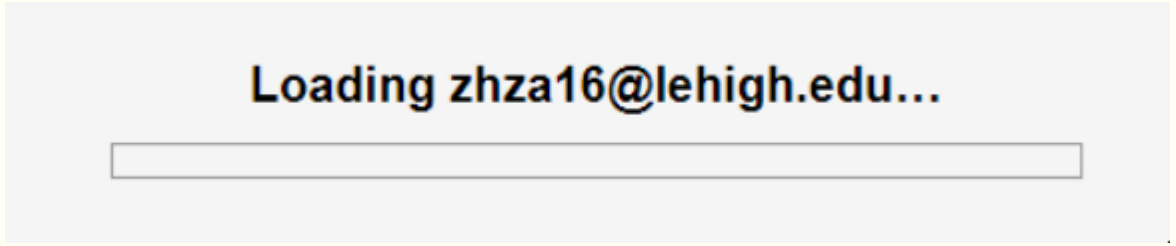


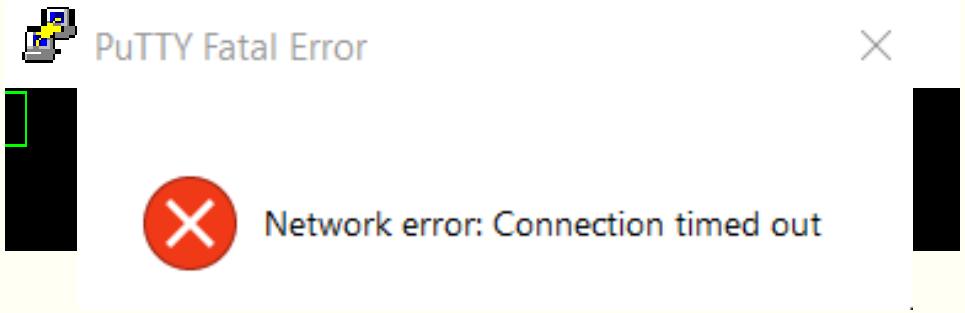

Loading zhza16@lehigh.edu...


128.180.110.150 - PuTTY

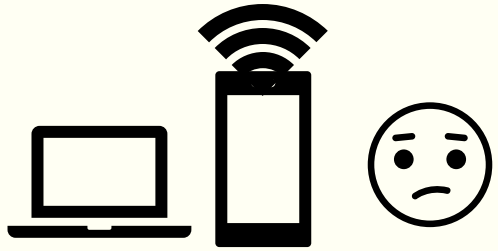

2G...



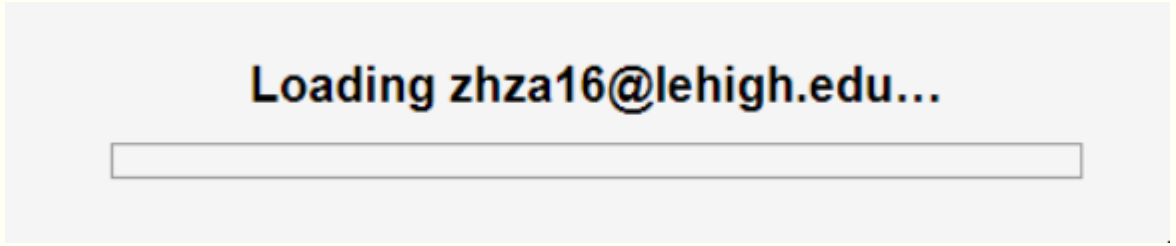

Loading zhza16@lehigh.edu...

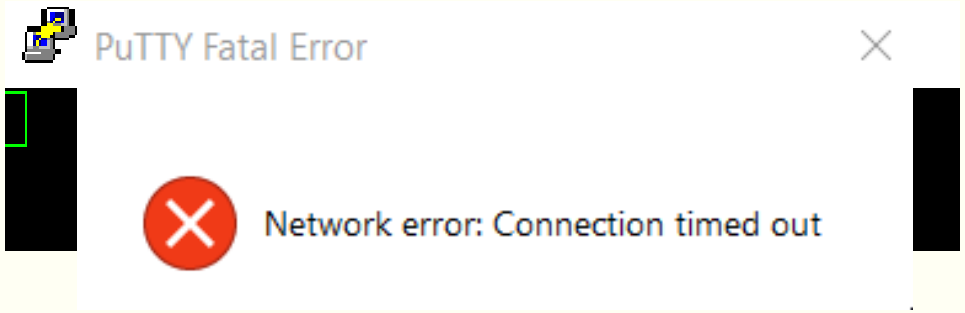

PuTTY Fatal Error
Network error: Connection timed out

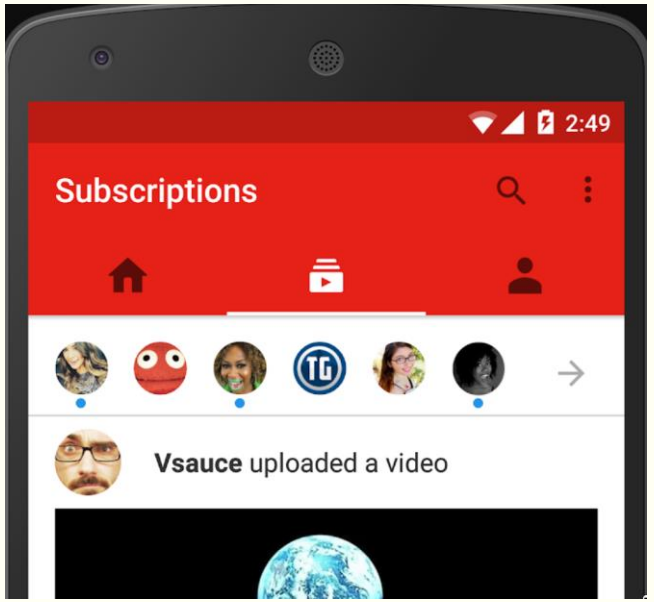

2G...

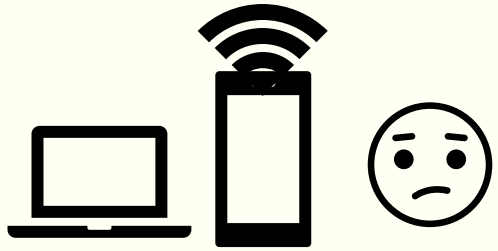


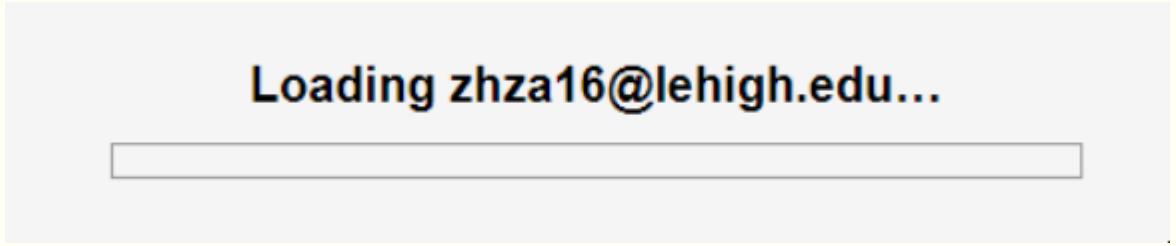

2G...

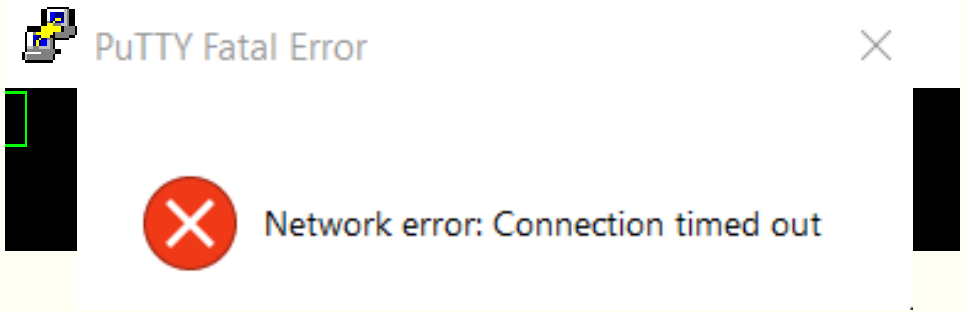

Loading zhza16@lehigh.edu...

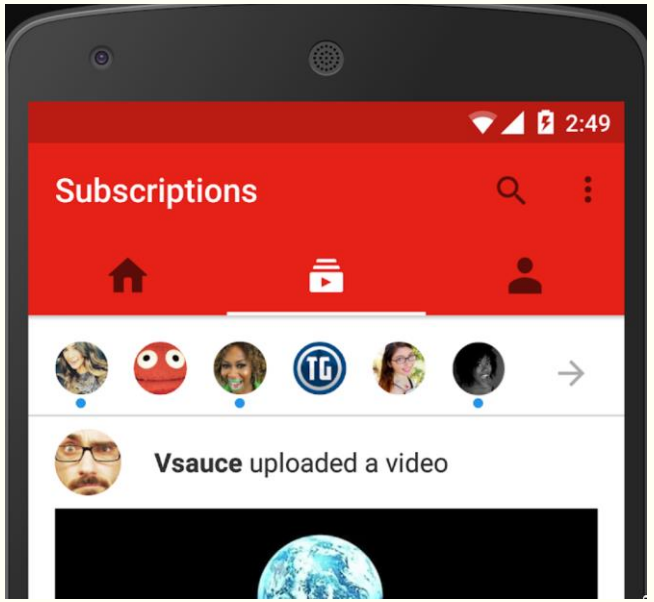

PuTTY Fatal Error
Network error: Connection timed out


2:49
Subscriptions
Vsauce uploaded a video

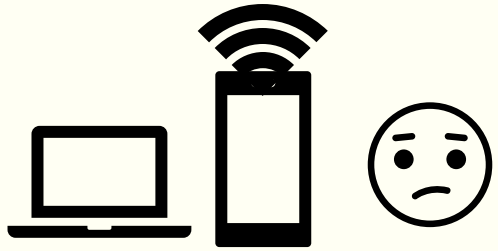


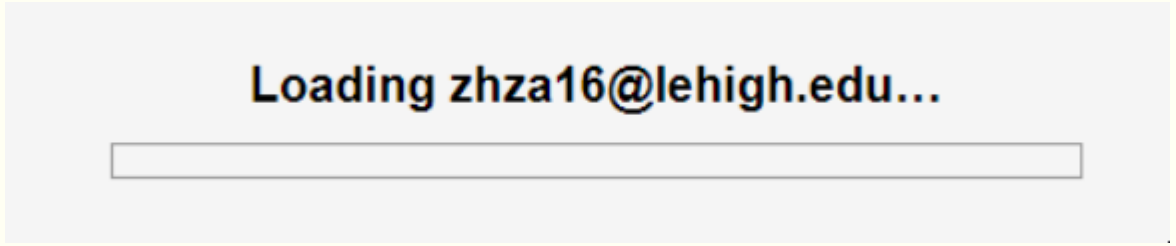


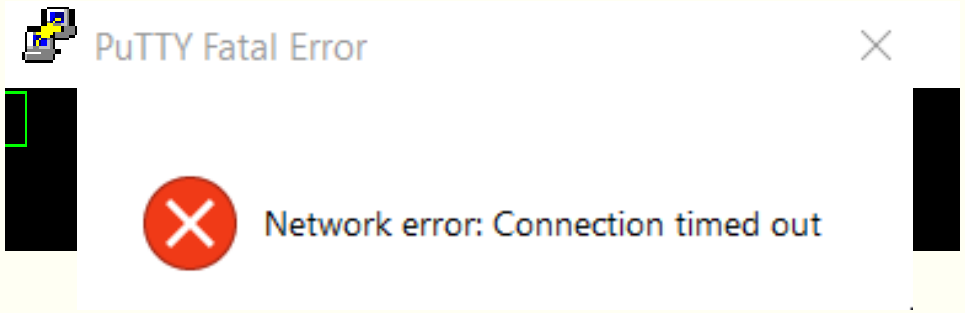


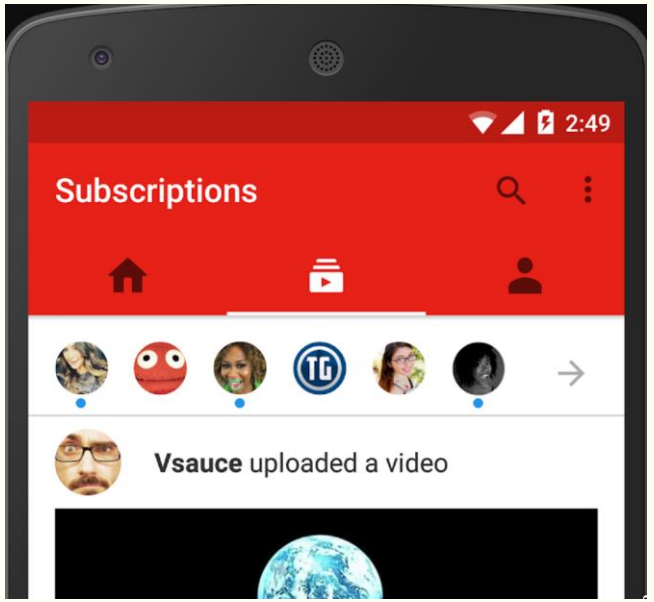


Zero-rating Services

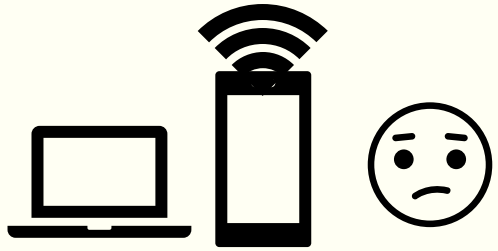


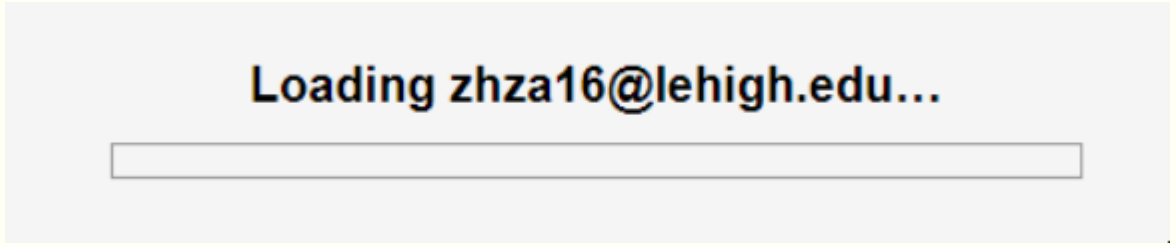


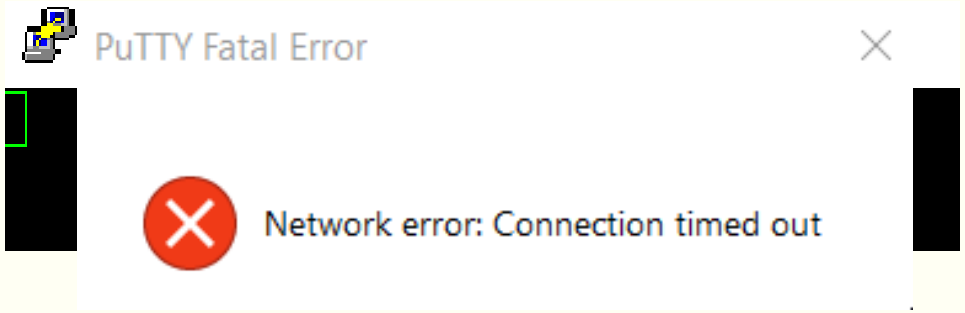


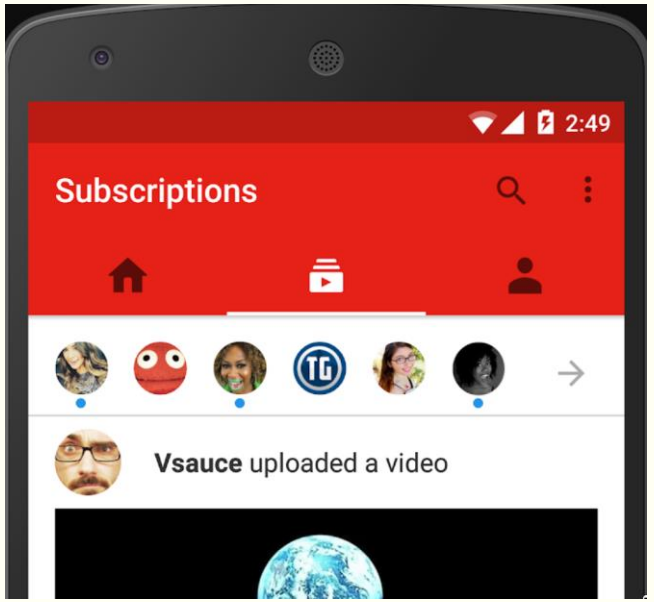


Zero-rating Services

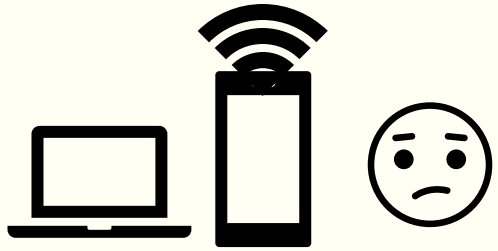


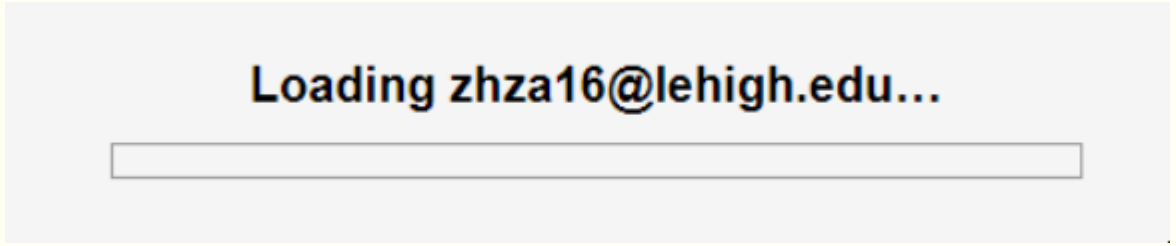


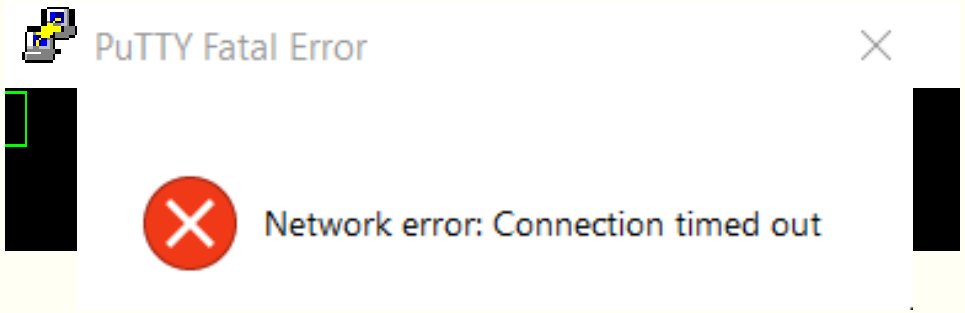


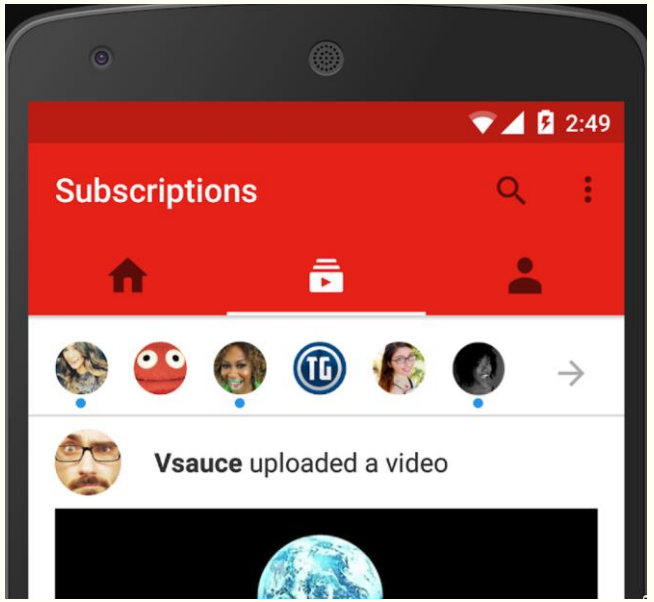


Zero-rating Services





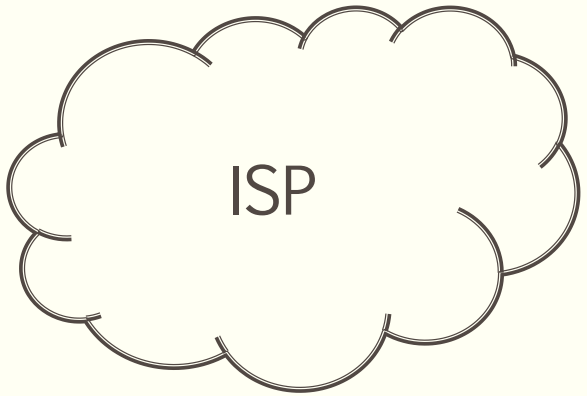




Zero-rating Services

Threat Model of Free-riding Attacks

Clients

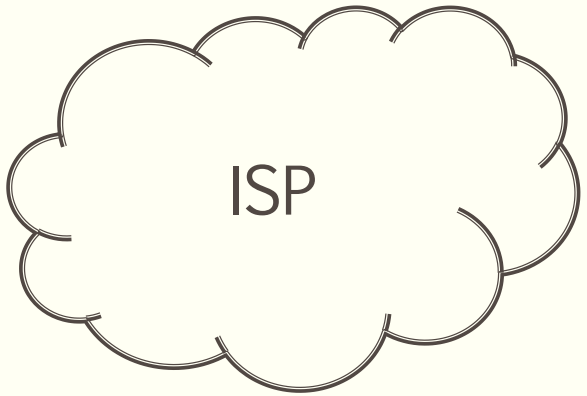


Content Providers

Threat Model of Free-riding Attacks

Clients

malicious

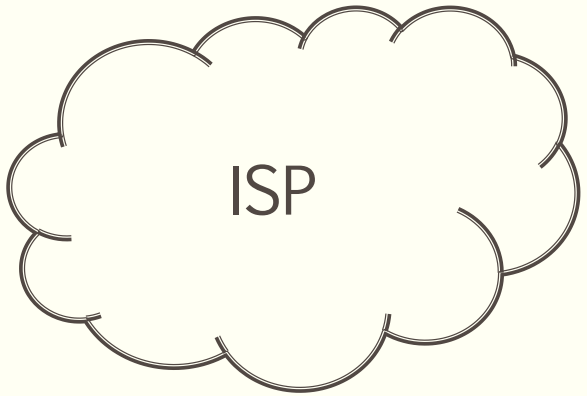


Content Providers

Threat Model of Free-riding Attacks

Clients

malicious



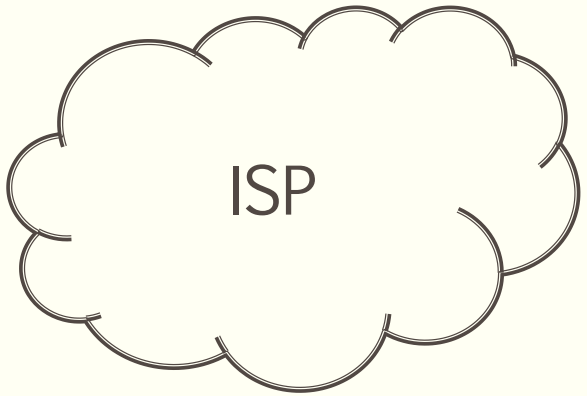
ISP is benign/victim

Content Providers

Threat Model of Free-riding Attacks

Clients

malicious



ISP is benign/victim

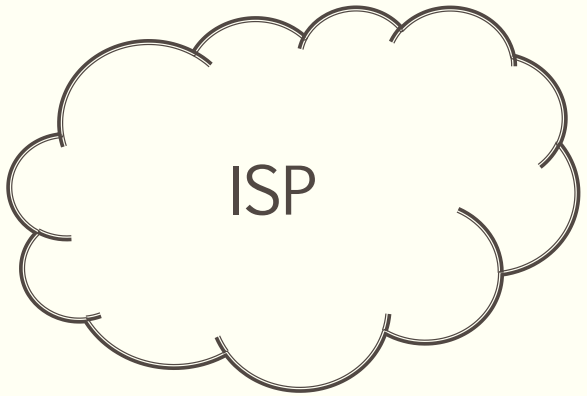
Content Providers

Zero-rated CPs are benign/victim

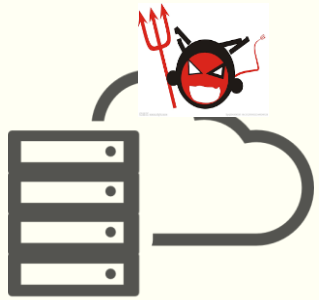
Threat Model of Free-riding Attacks

Clients

malicious



ISP is benign/victim



Attacker can masquerade zero-rating CP

Content Providers

Zero-rated CPs are benign/victim

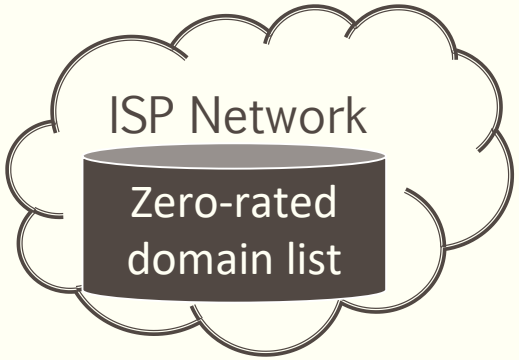
Outline

- Introduction
- **Free-riding Attacks**
- System Design
- Formal Security Analysis
- Implementation
- Evaluation
- Conclusion

Request Masquerade Attack on Industry System

- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field

Client

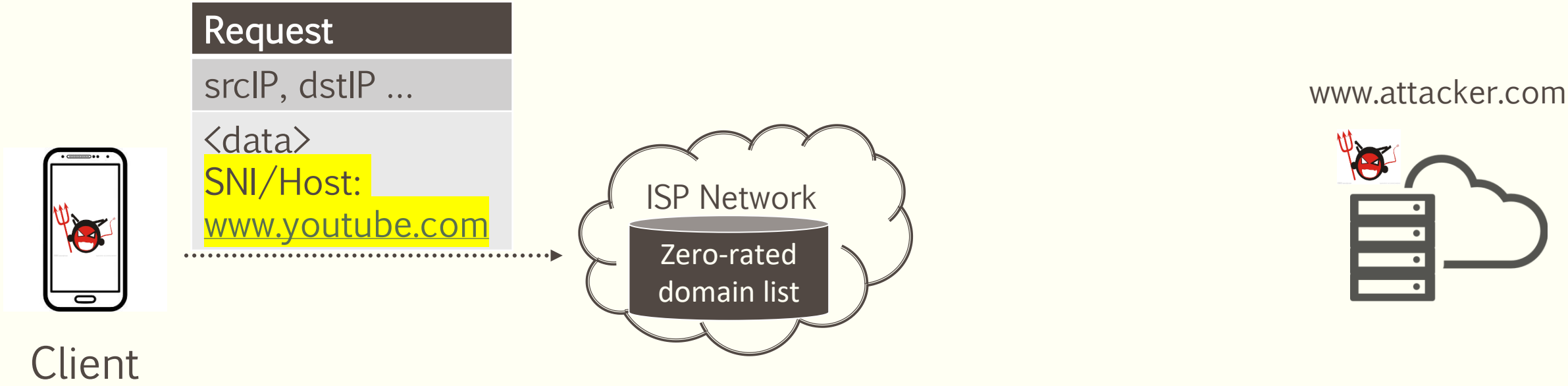


www.attacker.com

[1] Kakhki, Arash Molavi, et al. "Bingeon under the microscope: Understanding T-Mobiles zero-rating implementation." *Proceedings of the 2016 workshop on QoE-based Analysis and Management of Data Communication Networks*. ACM, 2016.

Request Masquerade Attack on Industry System

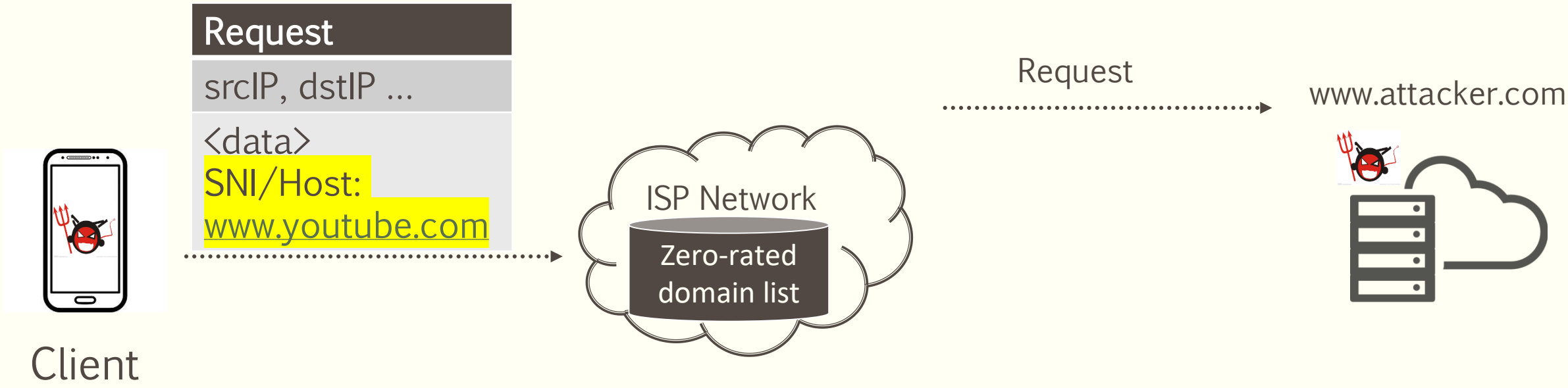
- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field



[1] Kakhki, Arash Molavi, et al. "Bingeon under the microscope: Understanding T-Mobiles zero-rating implementation." *Proceedings of the 2016 workshop on QoE-based Analysis and Management of Data Communication Networks*. ACM, 2016.

Request Masquerade Attack on Industry System

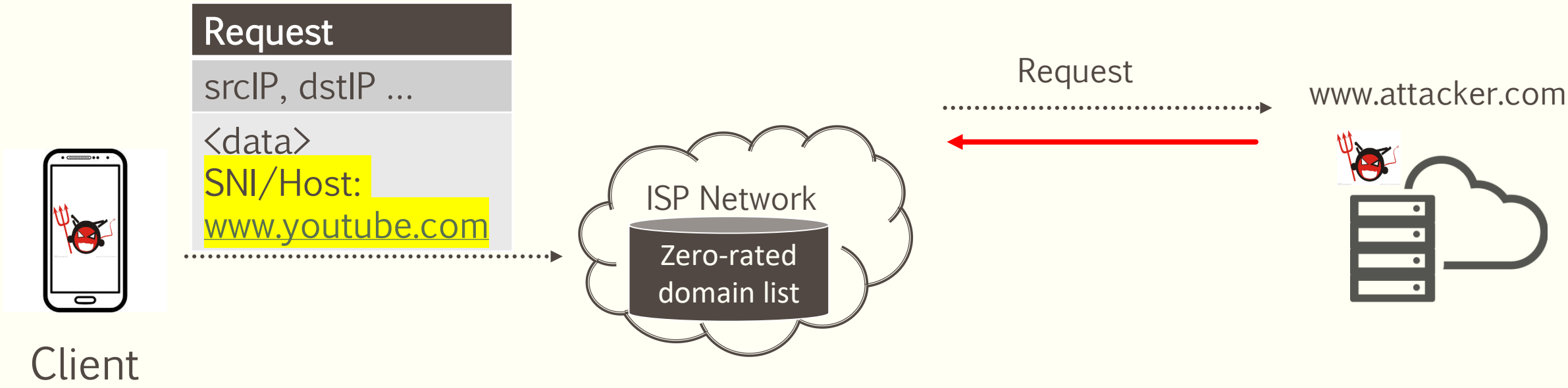
- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field



[1] Kakhki, Arash Molavi, et al. "Bingeon under the microscope: Understanding T-Mobiles zero-rating implementation." *Proceedings of the 2016 workshop on QoE-based Analysis and Management of Data Communication Networks*. ACM, 2016.

Request Masquerade Attack on Industry System

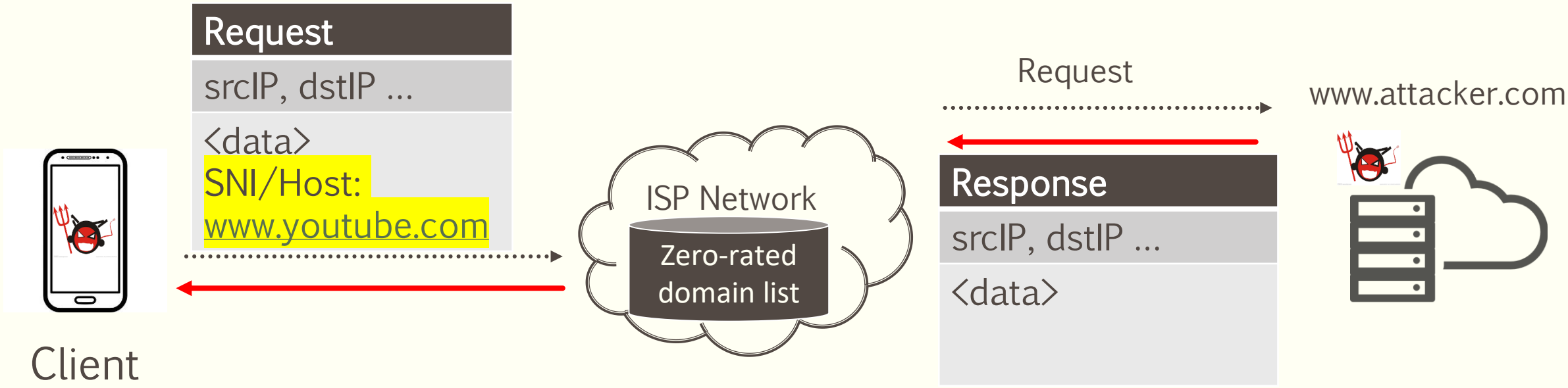
- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field



[1] Kakhki, Arash Molavi, et al. "Bingeon under the microscope: Understanding T-Mobiles zero-rating implementation." *Proceedings of the 2016 workshop on QoE-based Analysis and Management of Data Communication Networks*. ACM, 2016.

Request Masquerade Attack on Industry System

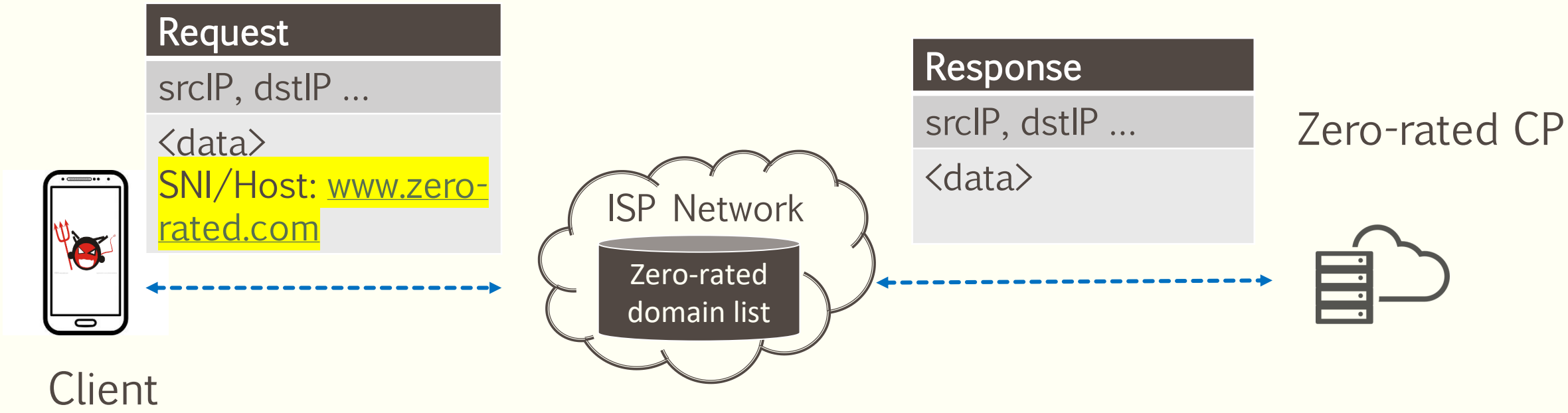
- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field



[1] Kakhki, Arash Molavi, et al. "Bingeon under the microscope: Understanding T-Mobiles zero-rating implementation." *Proceedings of the 2016 workshop on QoE-based Analysis and Management of Data Communication Networks*. ACM, 2016.

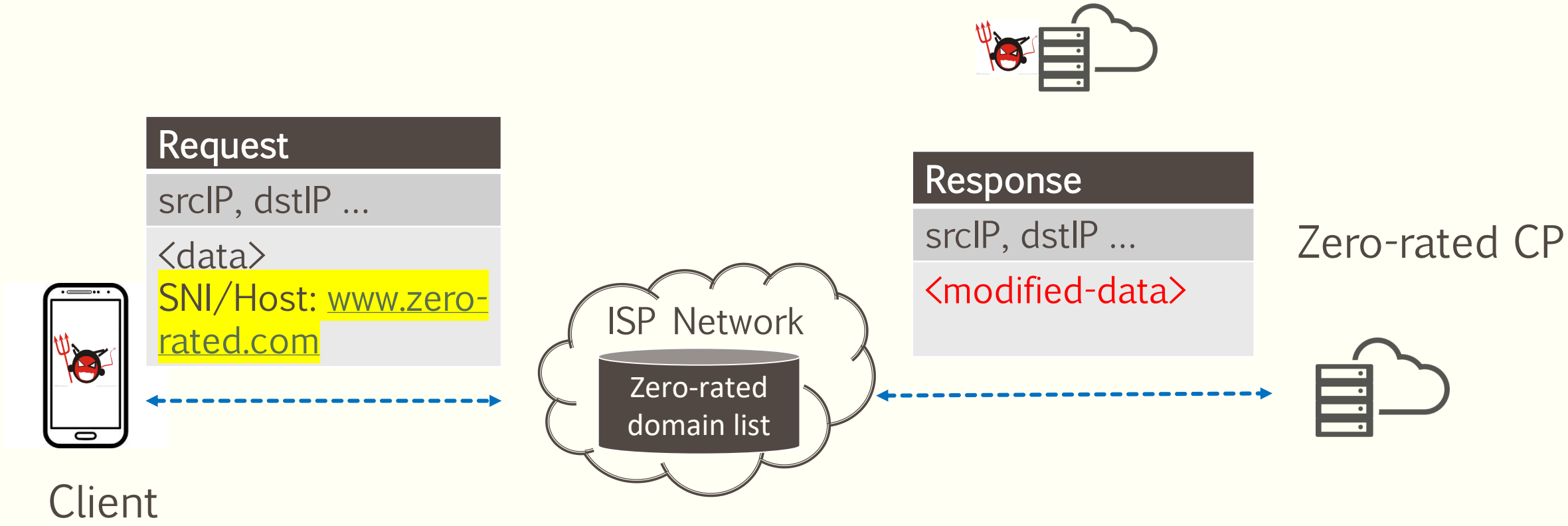
Response Modification Attack on Industry System

- Inject non-zero-rated content



Response Modification Attack on Industry System

- Inject non-zero-rated content



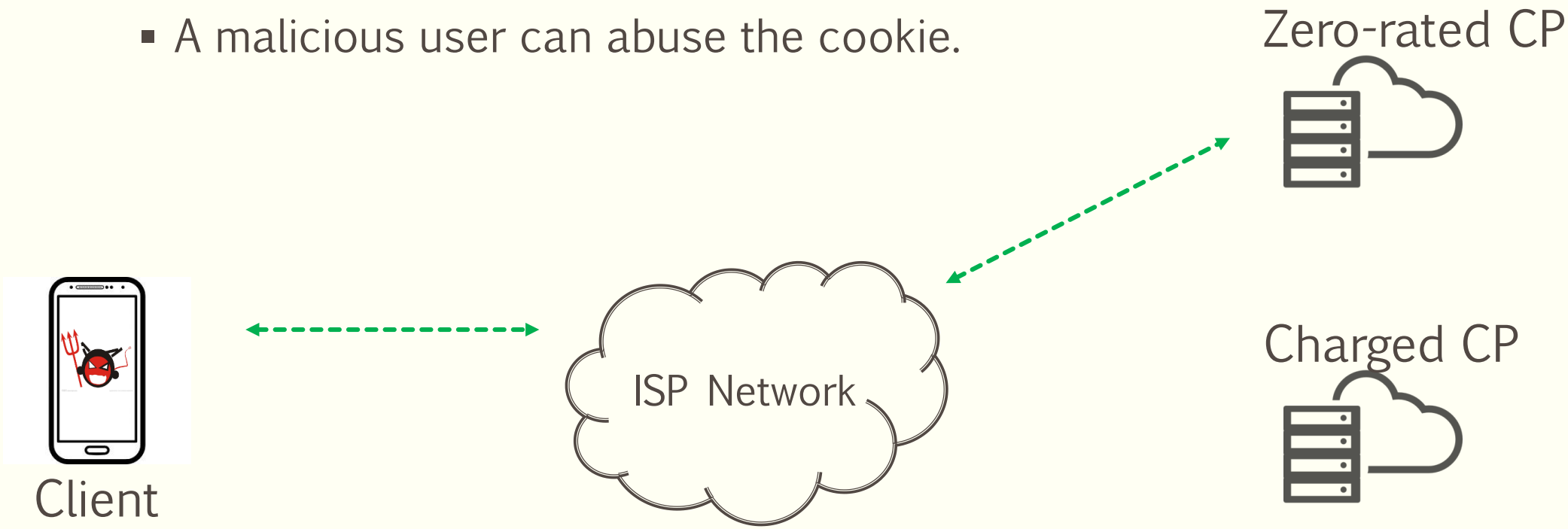
Prototype Zero-Rating Systems

- Network Cookies [1]
  - A malicious user can abuse the cookie.
- IP Whitelist-based Method [2]
  - An attacker at the server side can abuse source IP address.

[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on Network Cookies

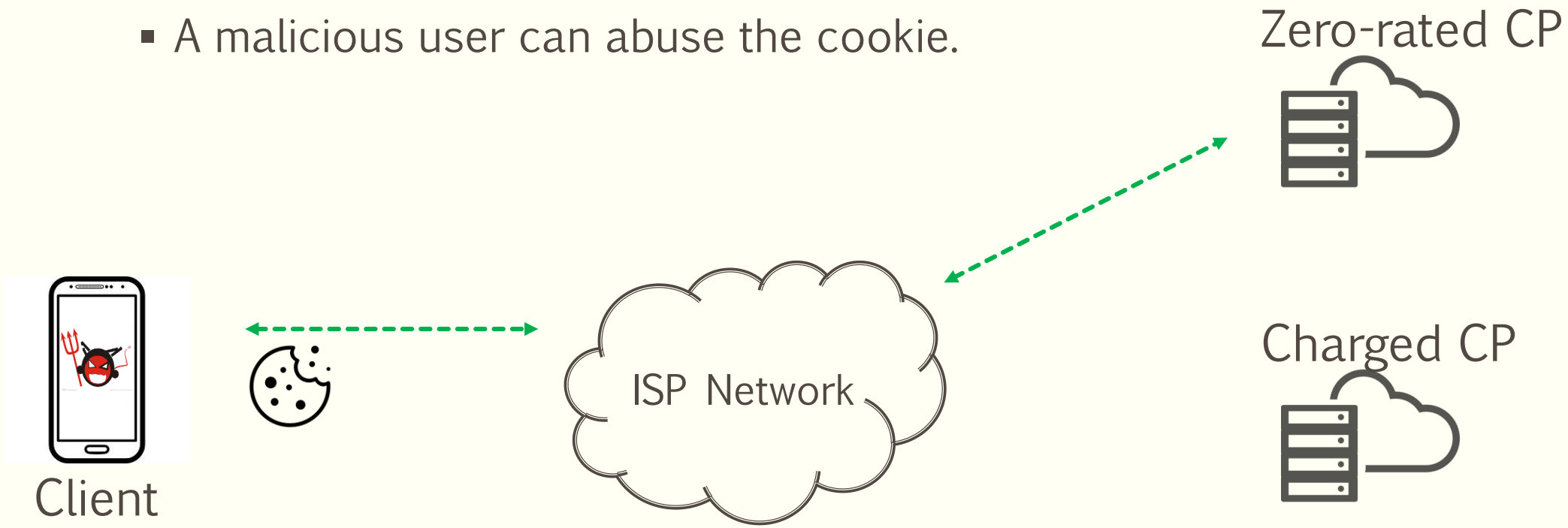
- Network Cookies [1]
  - A malicious user can abuse the cookie.



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on Network Cookies

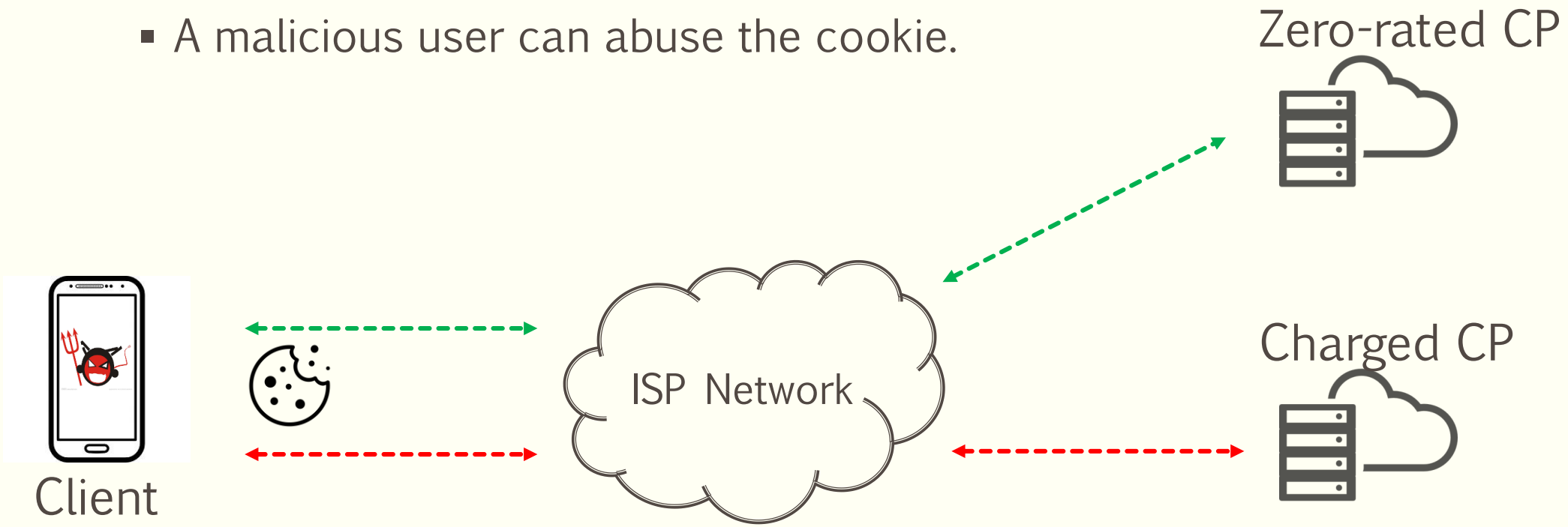
- Network Cookies [1]
  - A malicious user can abuse the cookie.



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on Network Cookies

- Network Cookies [1]
  - A malicious user can abuse the cookie.



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

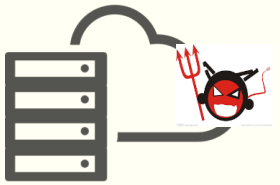
Attacks on IP whitelist based system

- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.

Client

Zero-rated CP

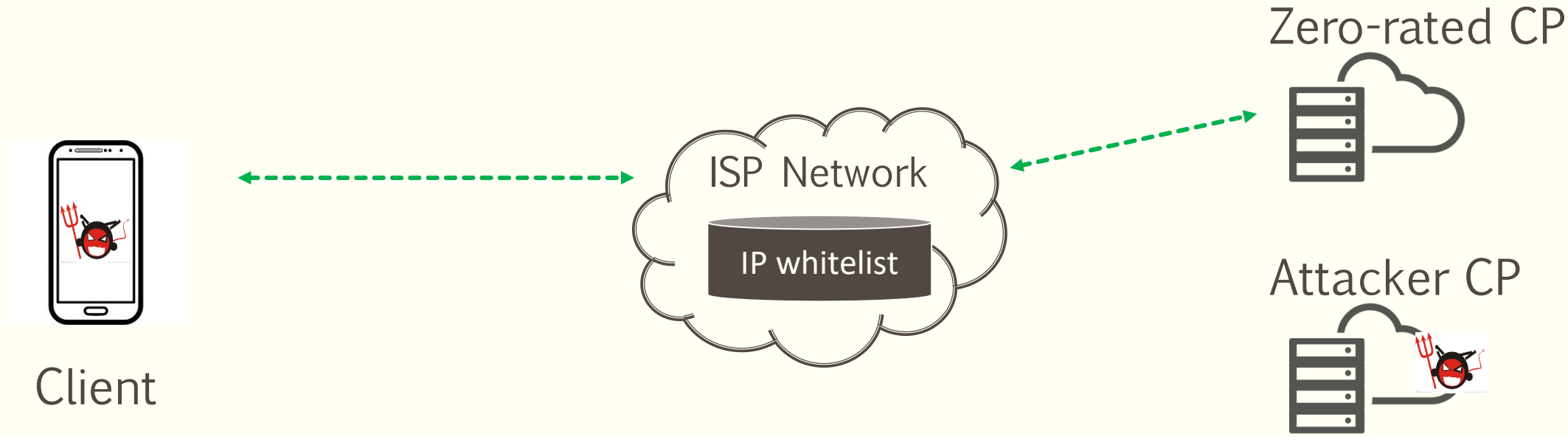
Attacker CP



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on IP whitelist based system

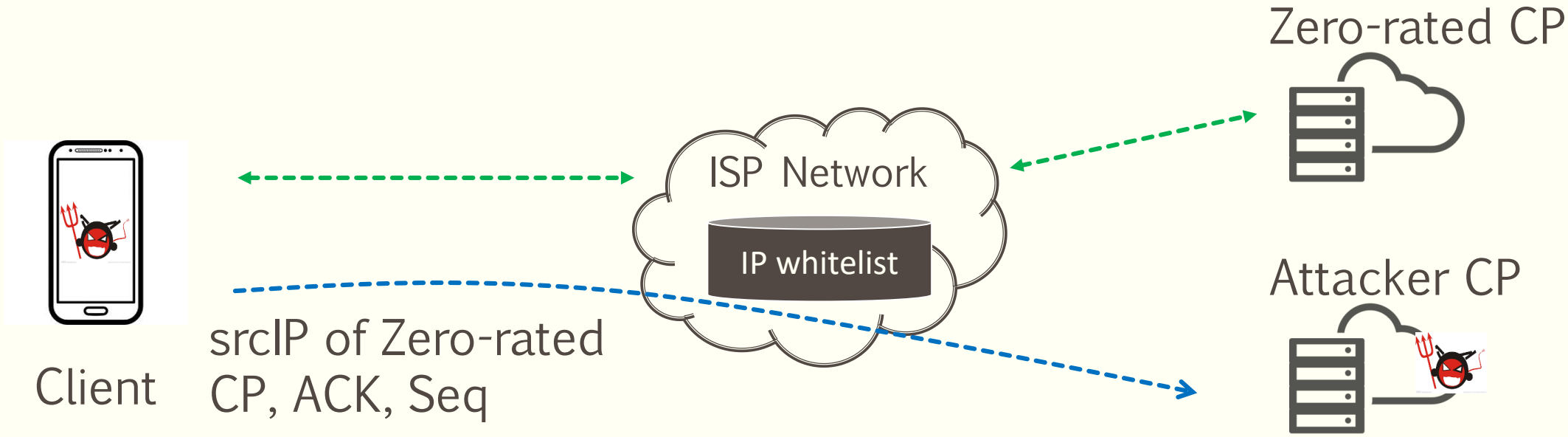
- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on IP whitelist based system

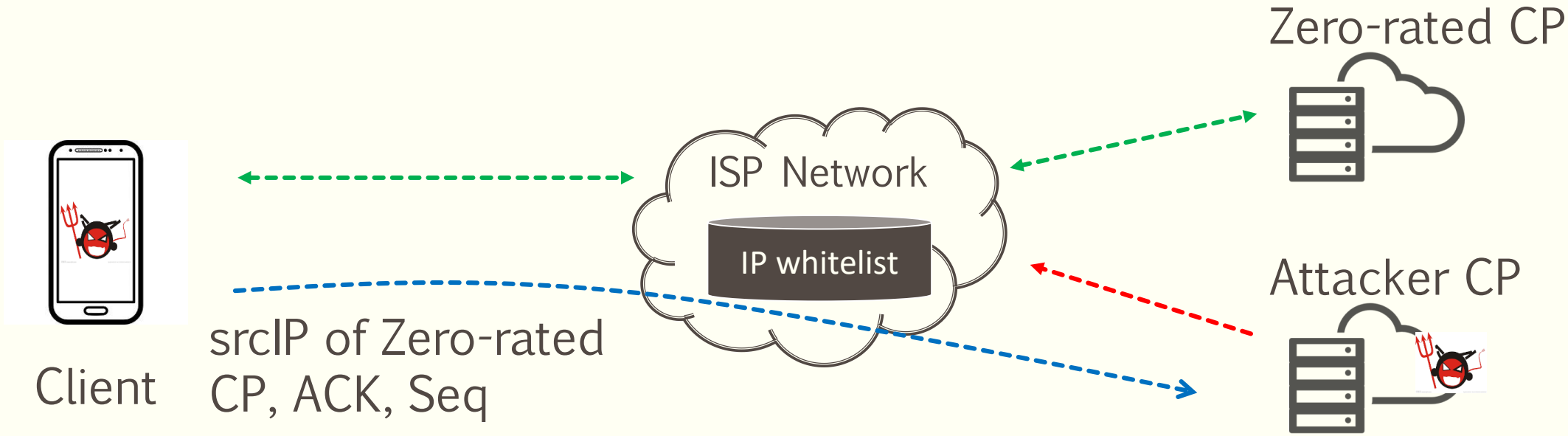
- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on IP whitelist based system

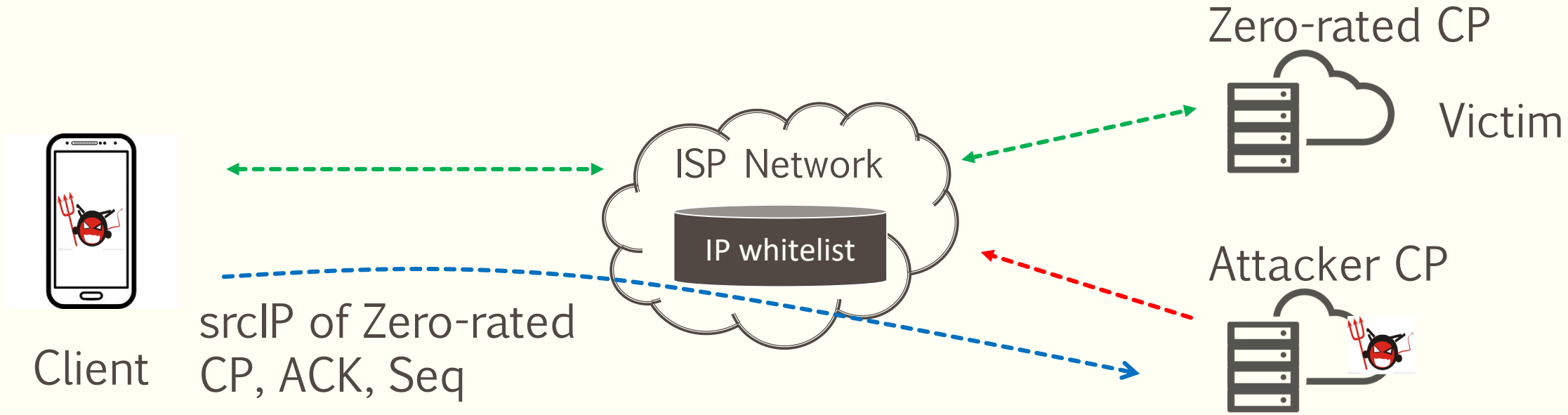
- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on IP whitelist based system

- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.



[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.
[2] (2014, Dec.) Delivering zero-rated traffic. https://connect.limelight.com/blogs/limelight/2014/12/08/delivering-zero-rated-traffic

Attacks on Zero-Rating Systems

		T-Mobile	China Mobile	China Unicom	United WiFi	ORD WiFi	Network Cookies [1]	IP Whitelist
🔓	Req-Mas	×	×	N/A	×	×	×	×
	Res-Mod	×	×	N/A	×	×	×	×
🔒	Req-Mas	×	N/A	×	N/A	×	×	×
	Res-Mod	×	N/A	×	N/A	×	×	×

🔓 : Unencrypted Traffic; 🔒 : Encrypted Traffic;

Req-Mas: Request Masquerade; Res-Mod: Response Modification

[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.

Impacts of free-riding attacks

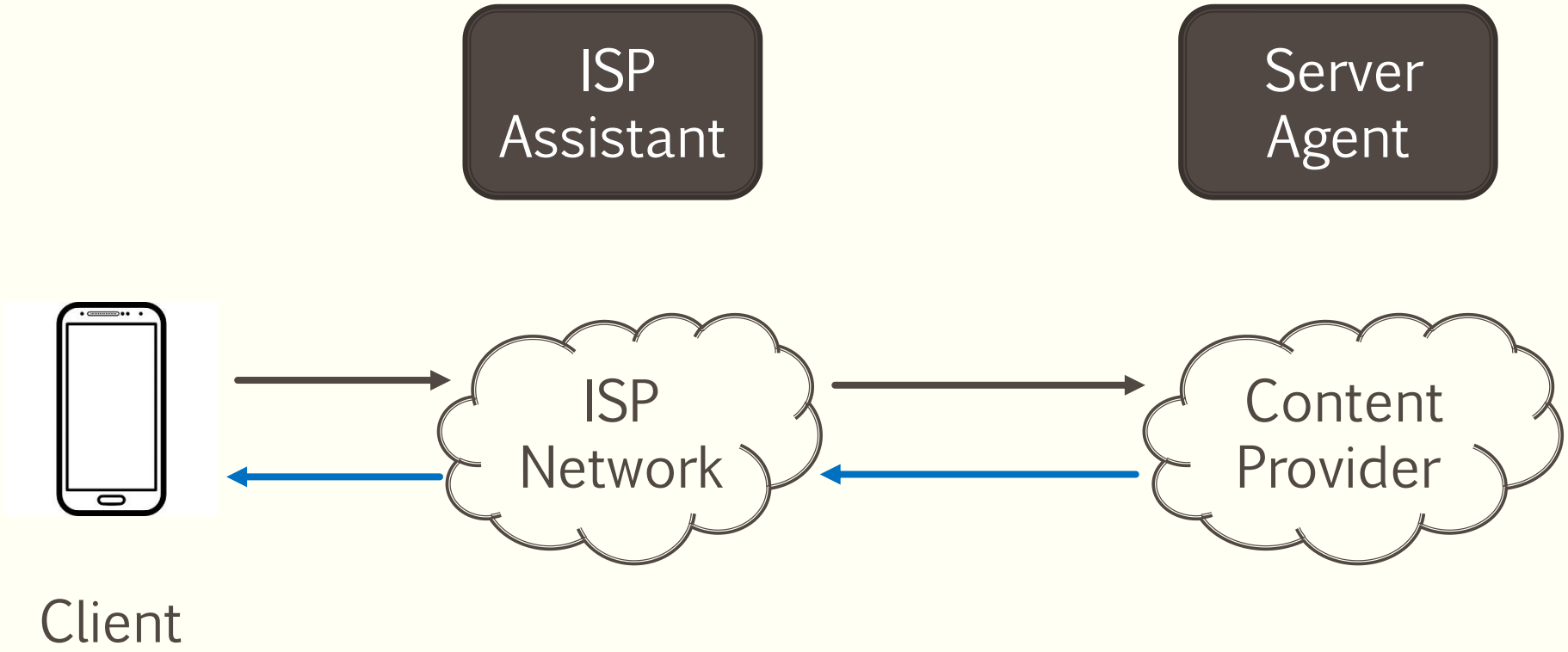
- A major U.S. network carrier lost over 7 millions in a month [1]
- China Mobile lost over 0.5 million/month in one province.
  - Filtering abnormal users , i.e., those consuming over 3 GB per month zero rating traffic
  - Inspecting unencrypted data manually
  - Results: found 71TB free-riding traffic

[1] (2017 global internet phenomena) spotlight: Zero-rating fraud. https://www.sandvine.com/hubfs/downloads/archive/2017-global-internet-phenomena-spotlight-zero-rating-fraud.pdf

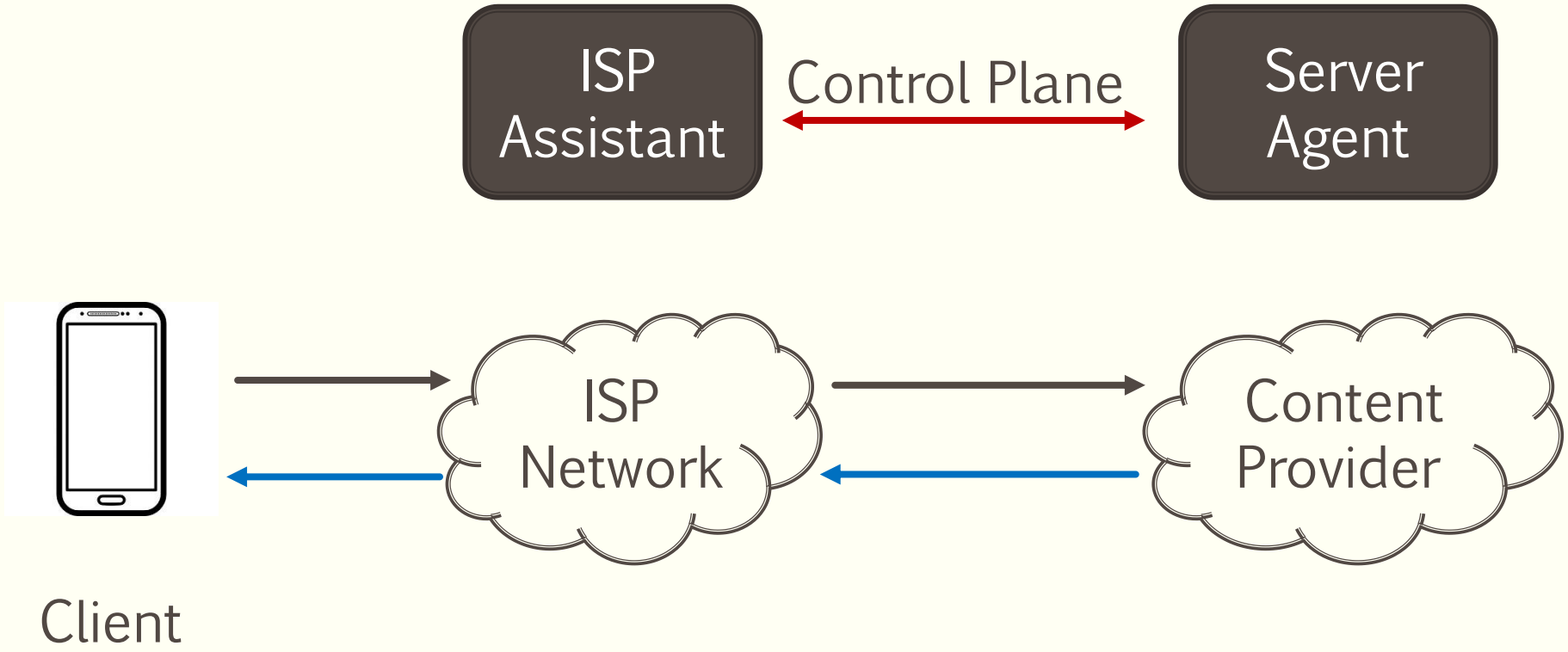
Outline

- Introduction
- Free-riding Attacks
- **System Design**
- Formal Security Analysis
- Implementation
- Evaluation
- Conclusion

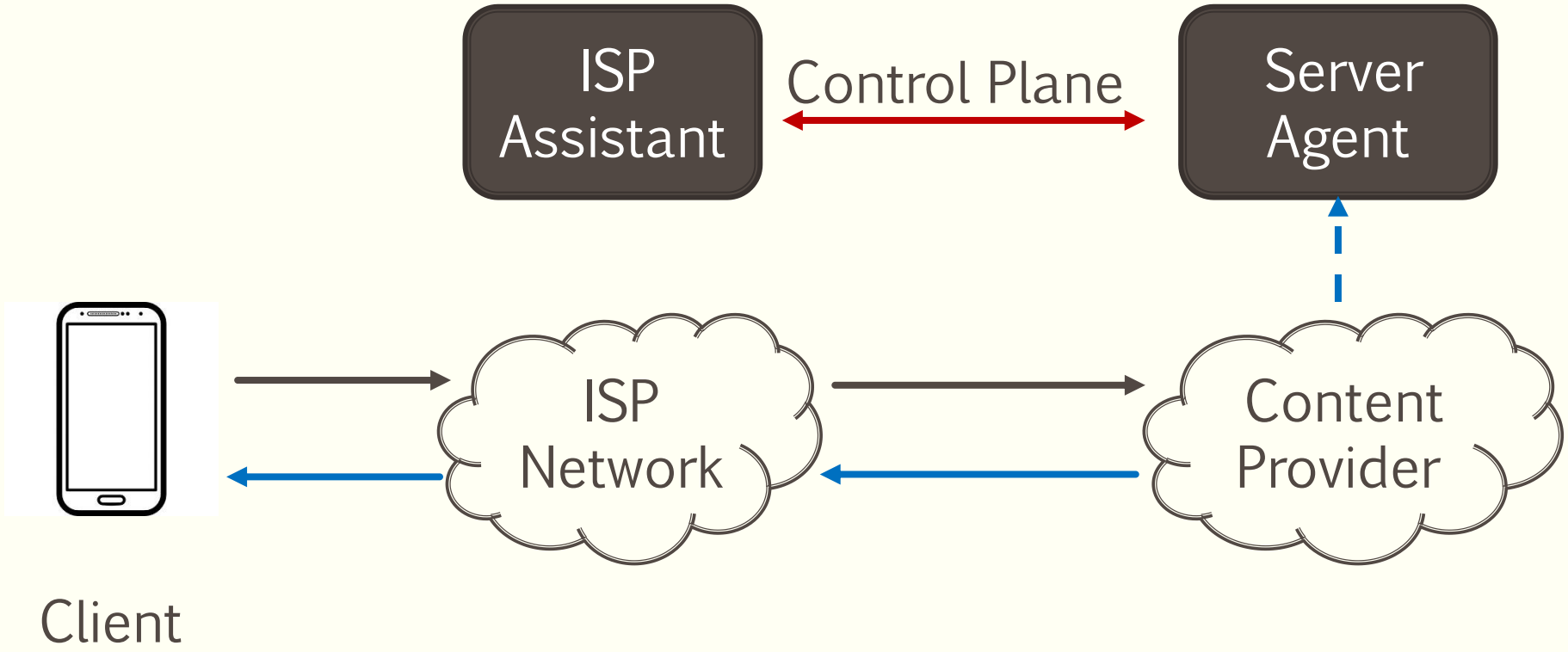
System Design: Overview



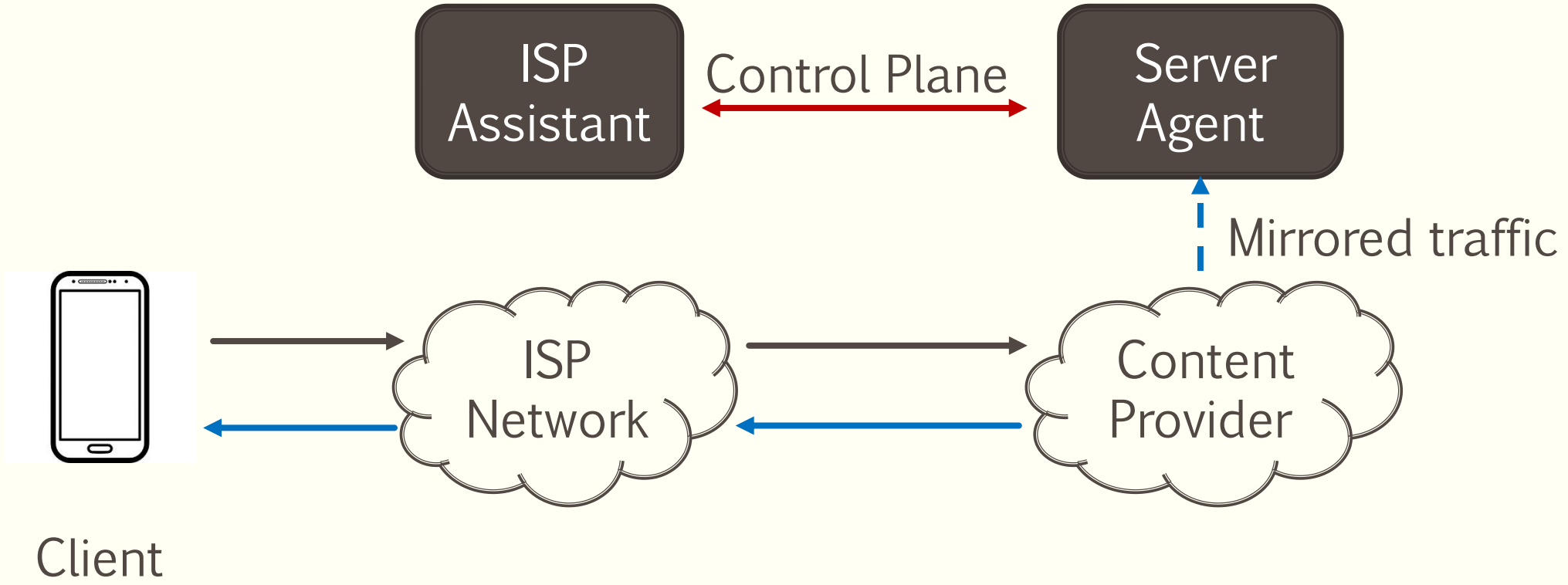
System Design: Overview



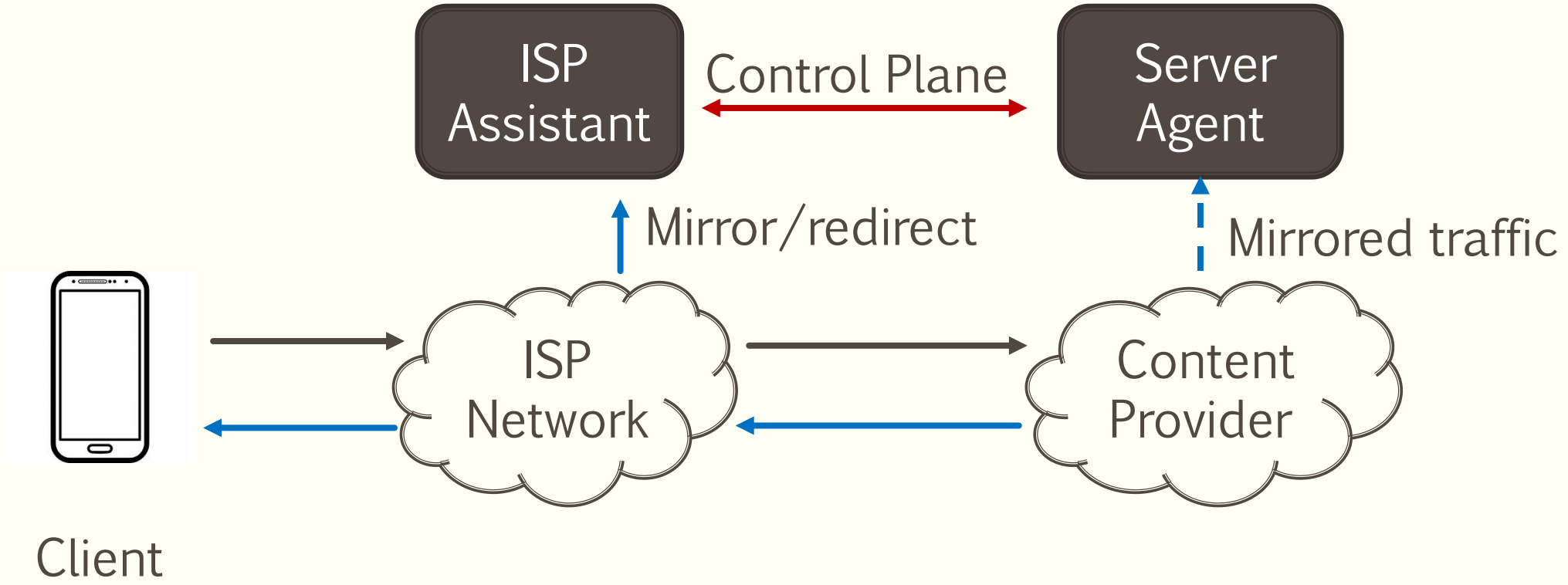
System Design: Overview



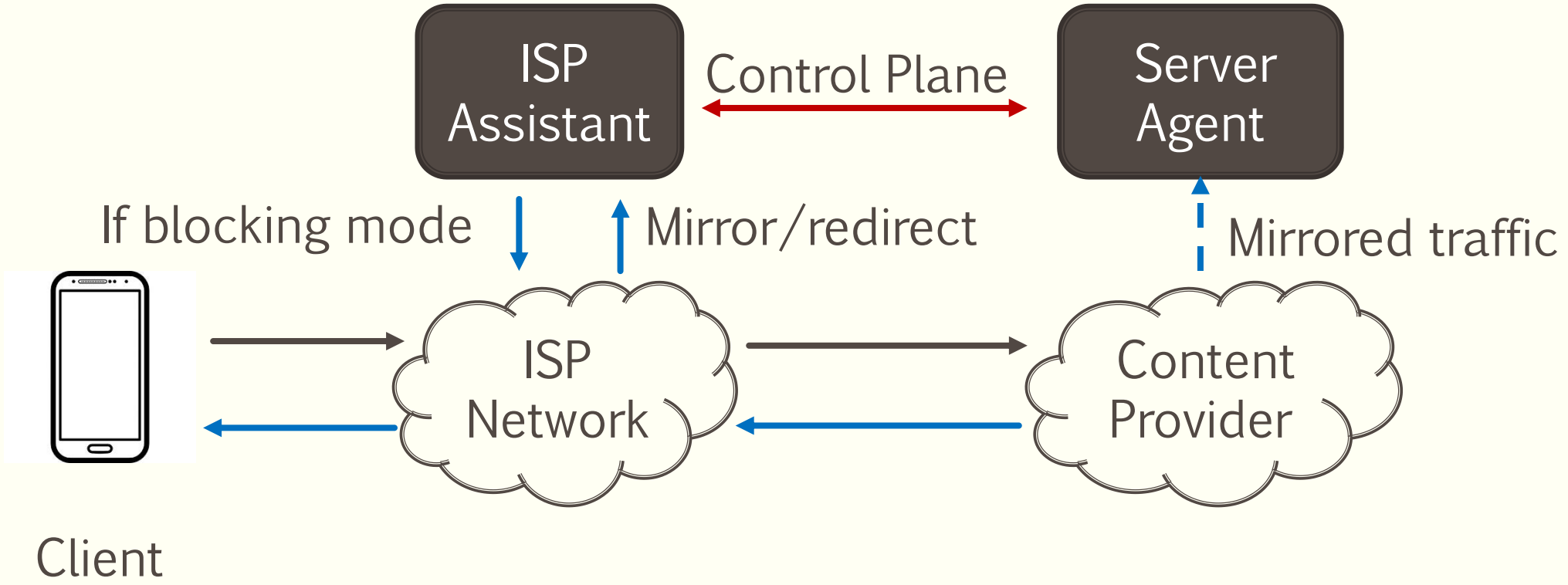
System Design: Overview



System Design: Overview

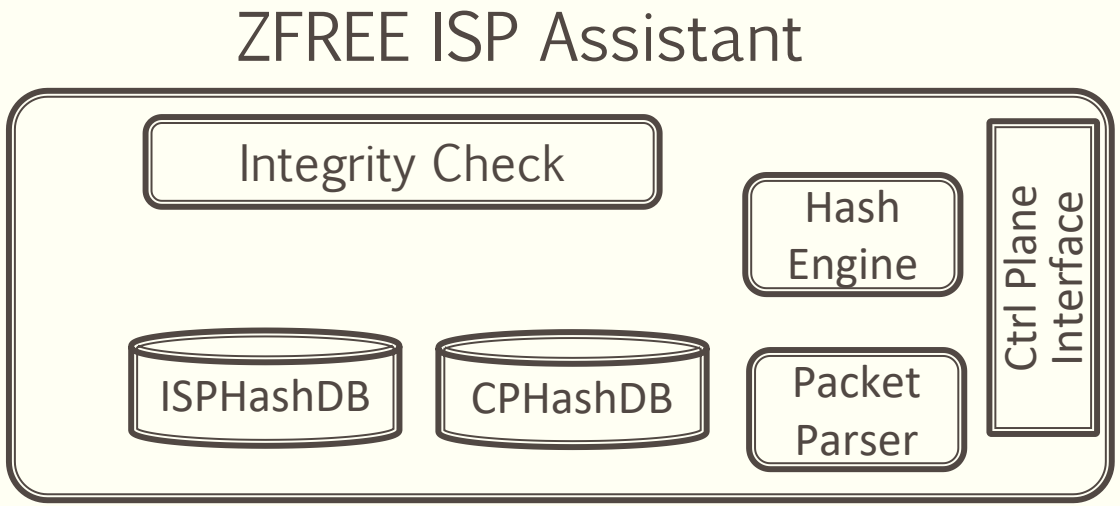


System Design: Overview



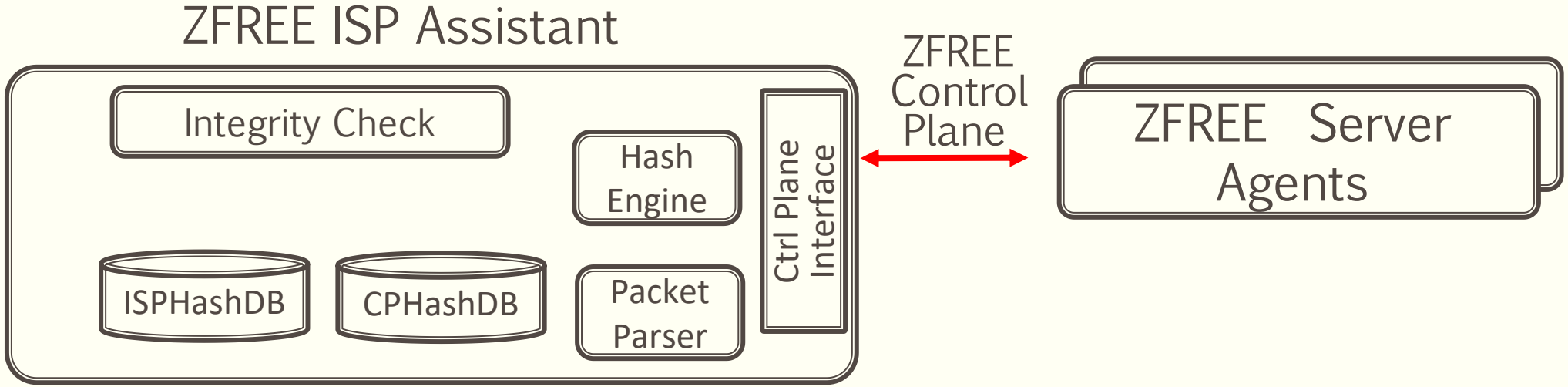
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match



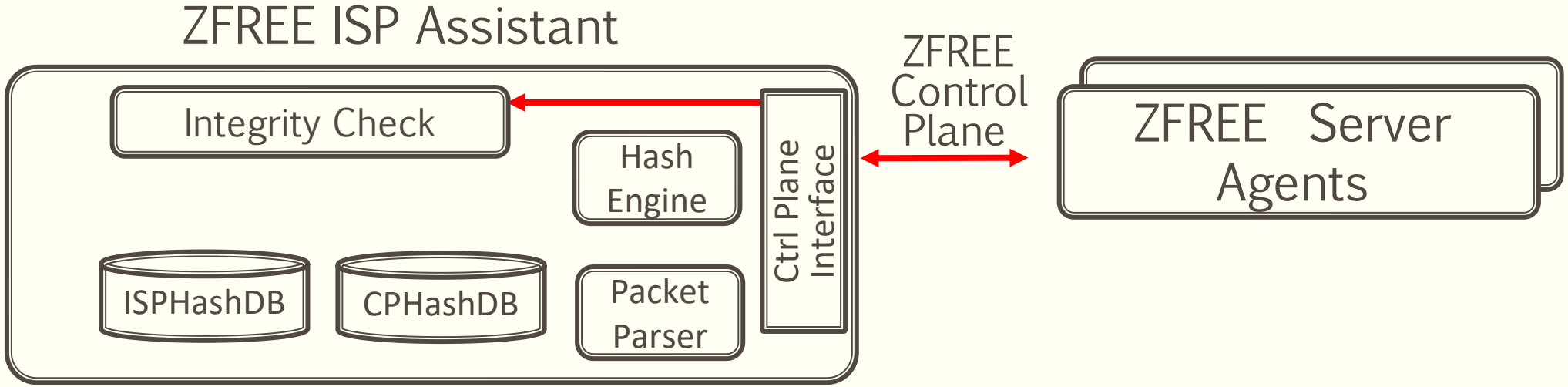
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match



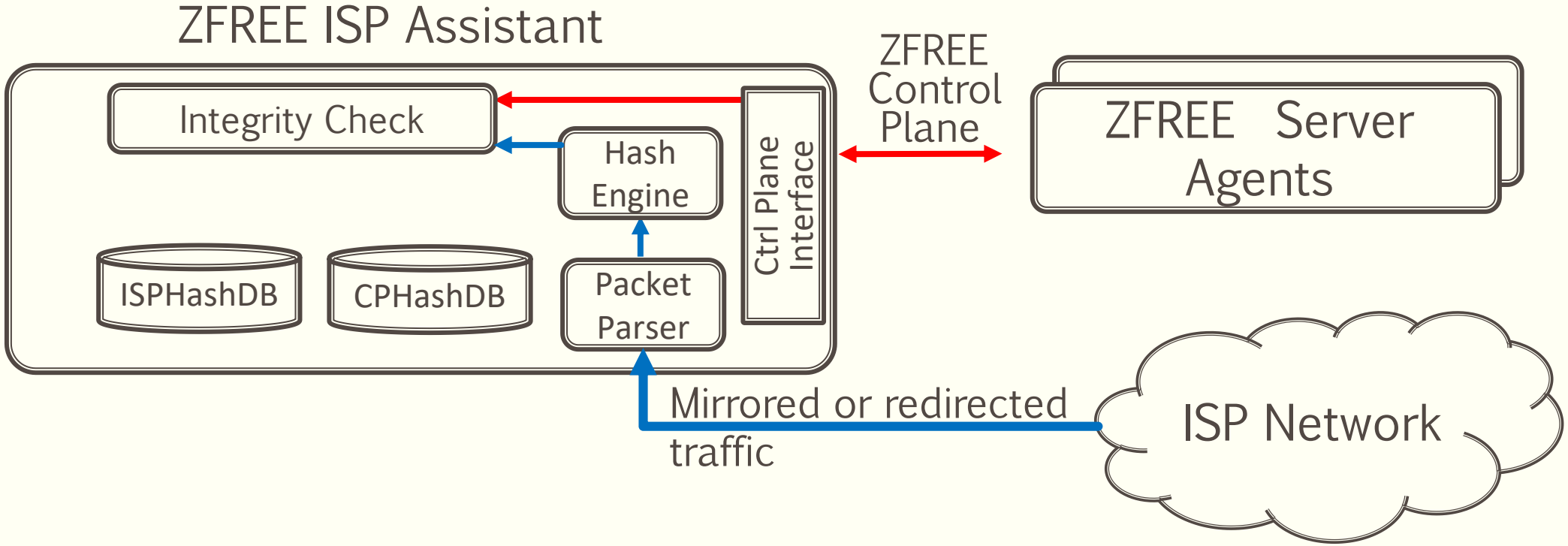
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match



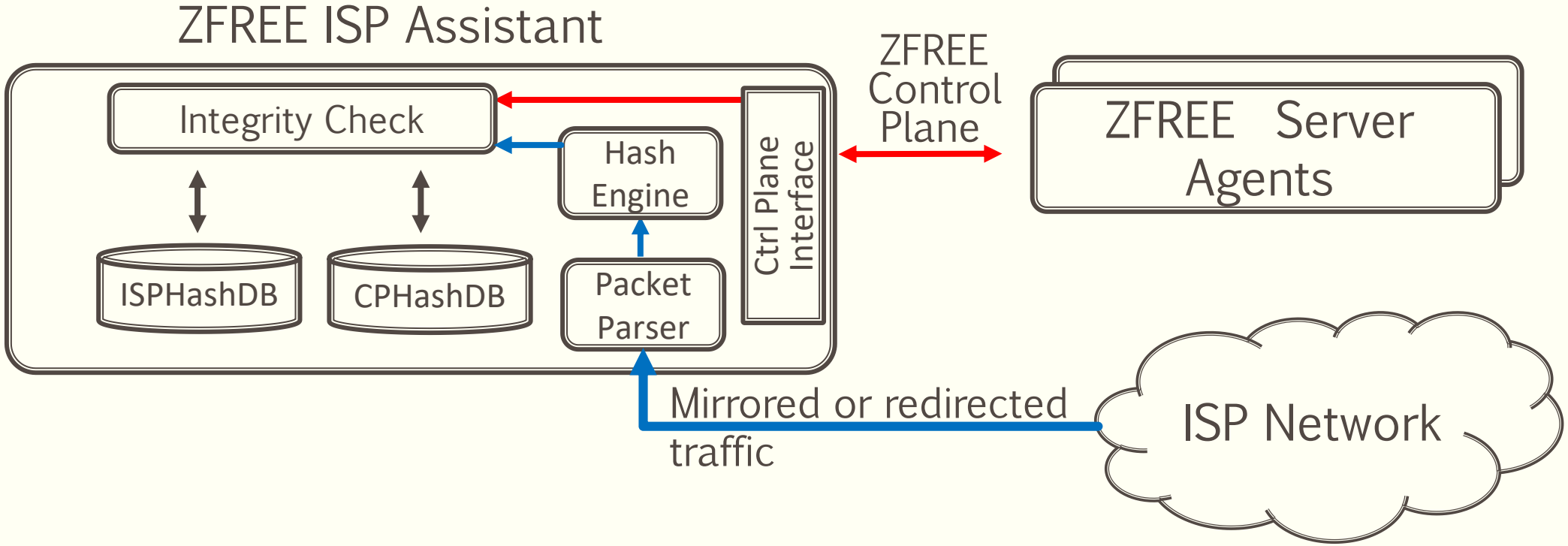
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match



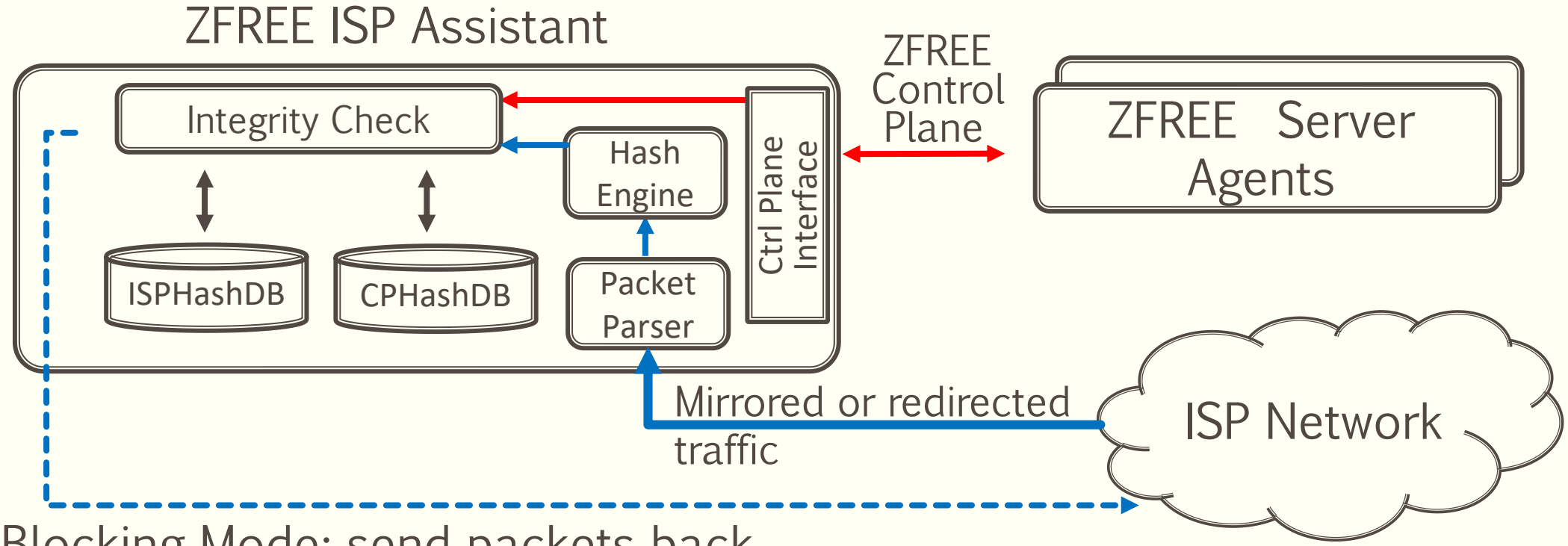
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match



System Design: ISP Assistant

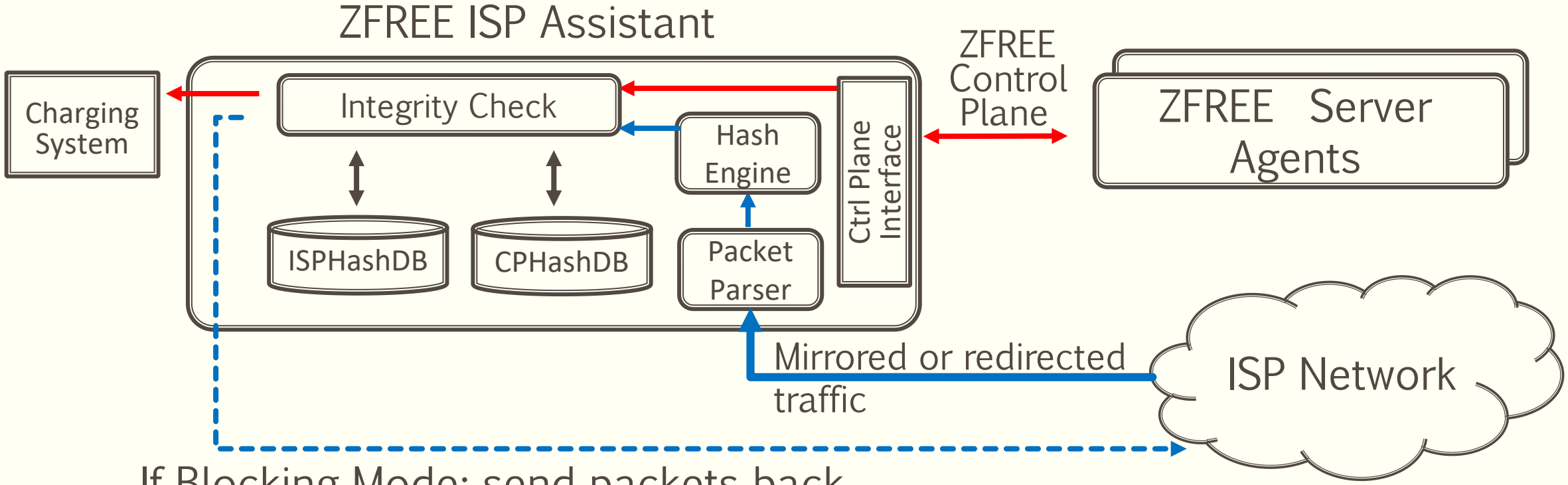
- Blocking/Non-Blocking Mode
- Accept hash values and match



If Blocking Mode: send packets back

System Design: ISP Assistant

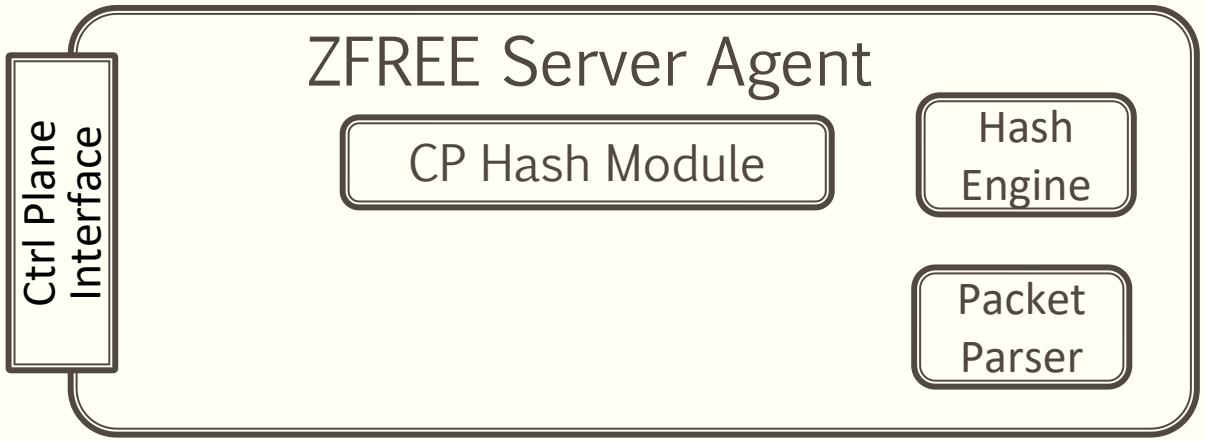
- Blocking/Non-Blocking Mode
- Accept hash values and match



If Blocking Mode: send packets back

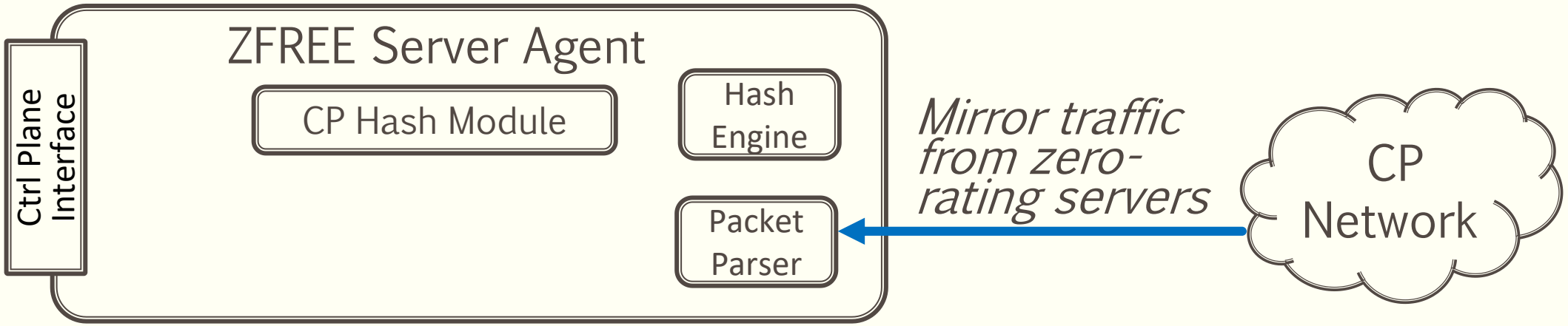
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report



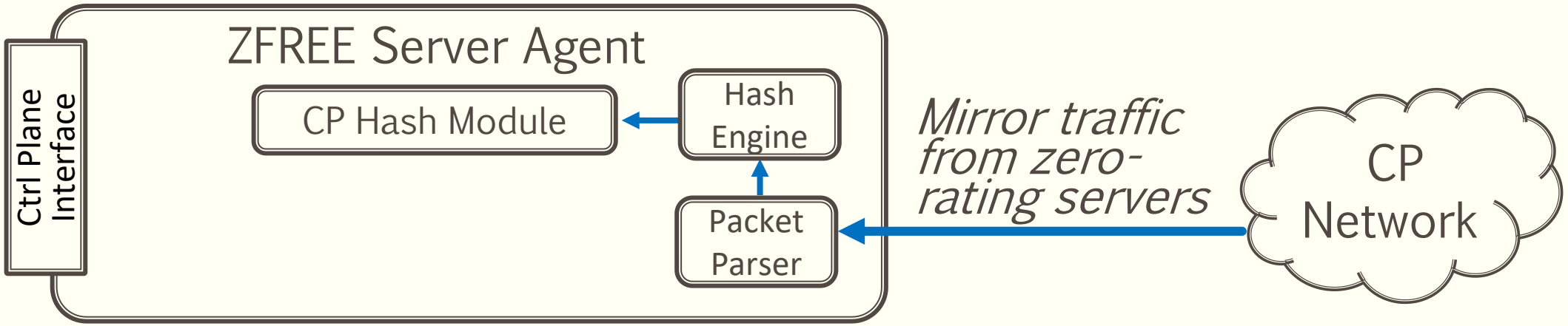
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report



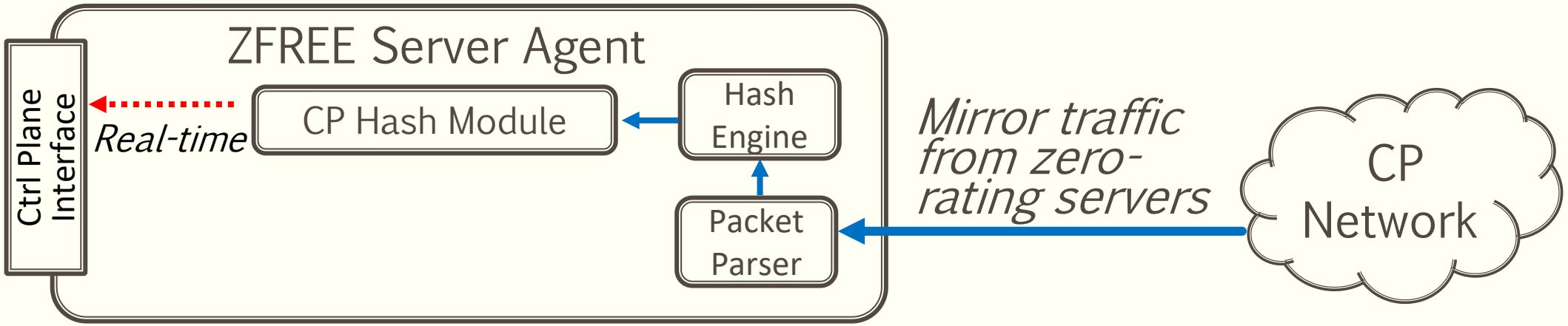
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report



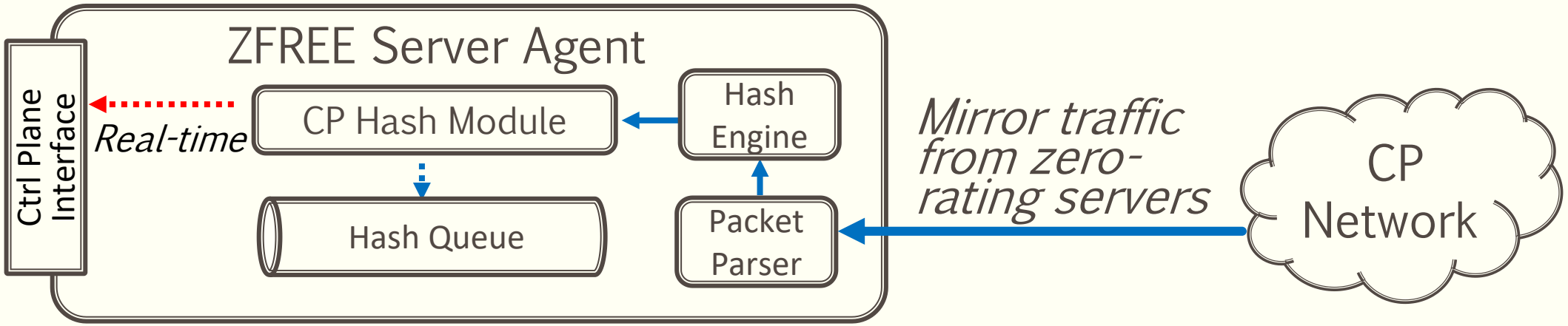
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report



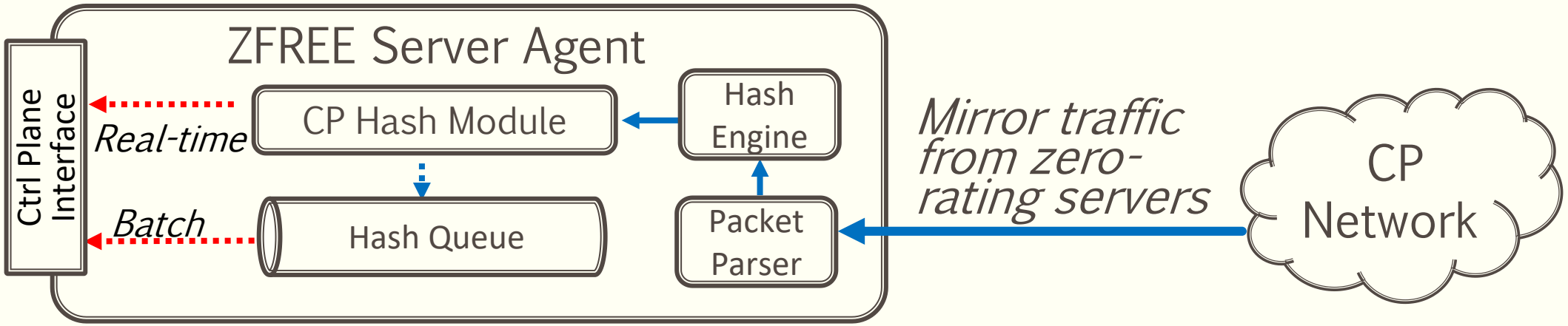
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report



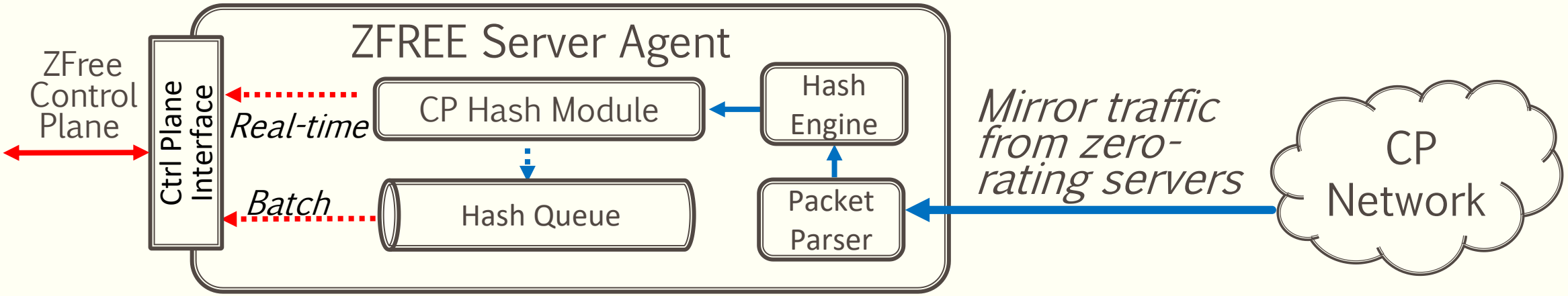
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report



System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report



Outline

- Introduction
- Free-riding Attacks
- System Design
- **Formal Security Analysis**
- Implementation
- Evaluation
- Conclusion

Formal Security Analysis

- Using ProVerif

Goals	Network Cookies[1]		IP Whitelist		ZFree	
	🔓	🔒	🔓	🔒	🔓	🔒
Packet Integrity	✗	✗	✗	✗	✓	✓
CP Authenticity	✗	✗	✗	✗	✓	✓
Data Secrecy	✗	✓	✗	✓	✗	✓

🔓 🔒/ : Unencrypted/Encrypted data plane communication

[1] Yiakoumis, Yiannis, Sachin Katti, and Nick McKeown. "Neutral net neutrality." *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016.

Outline

- Introduction
- Free-riding Attacks
- System Design
- Formal Security Analysis
- **Implementation**
- Evaluation
- Conclusion

Implementation

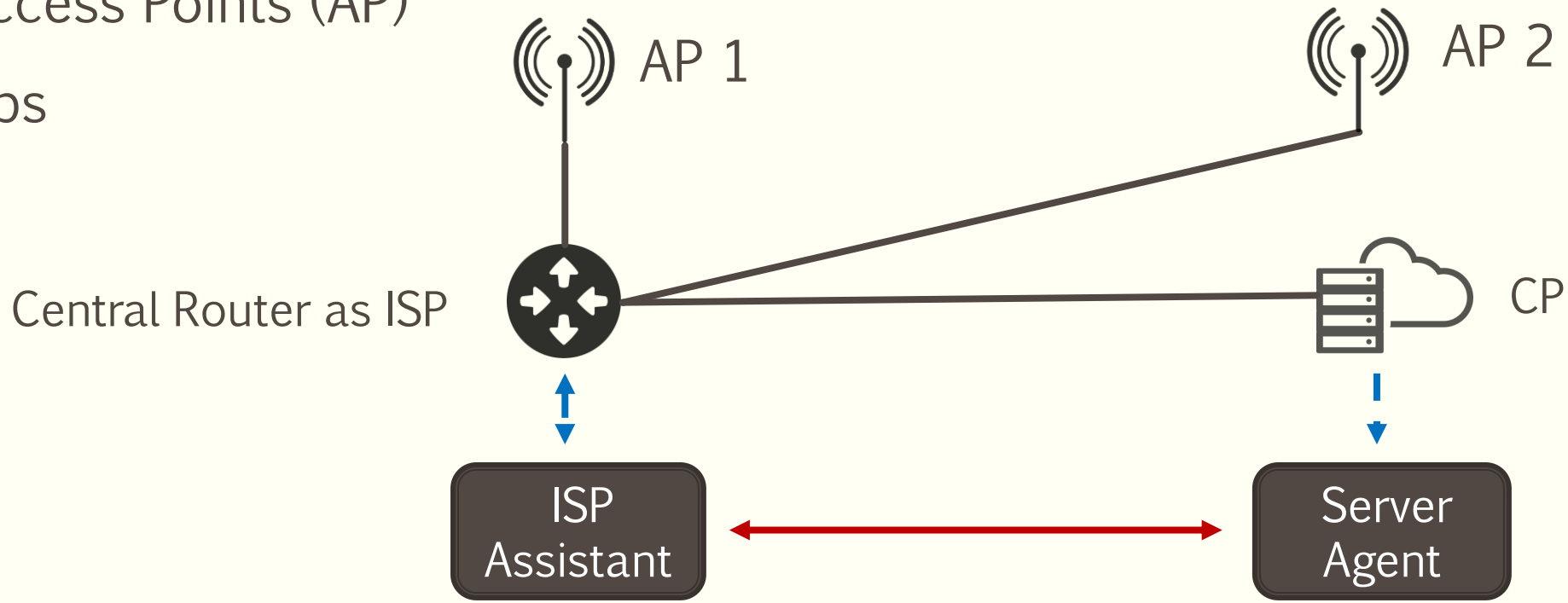
- ZFree Prototype: 1,890 Lines of Code (LoC):
  - 1,100 LoC for ISP assistant
  - 790 LoC for Server Agent
- LTE network (ns3)
- WiFi network (Mininet)
- Formal verification code: 1,680 LoC

Outline

- Introduction
- Free-riding Attacks
- System Design
- Formal Security Analysis
- Implementation
- **Evaluation**
- Conclusion

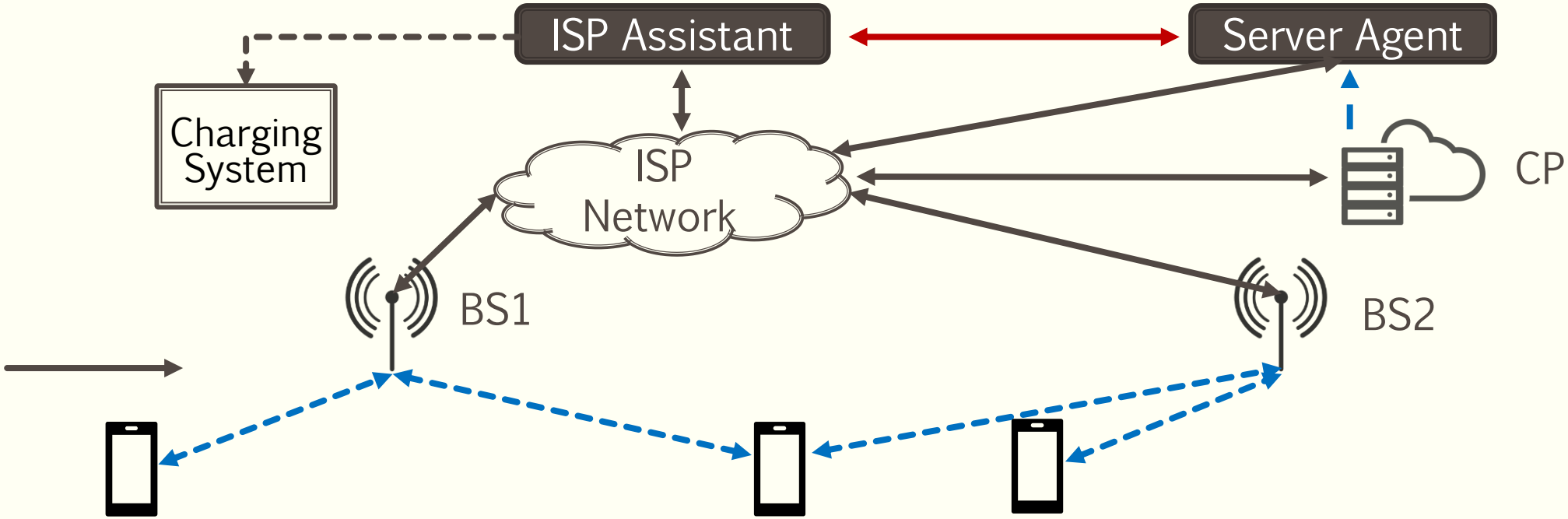
Evaluation: Environment Setup

- Airplane WiFi: Mininet-WiFi
- 120 User Equipments (UEs)
- Two Access Points (AP)
- 30 Mbps



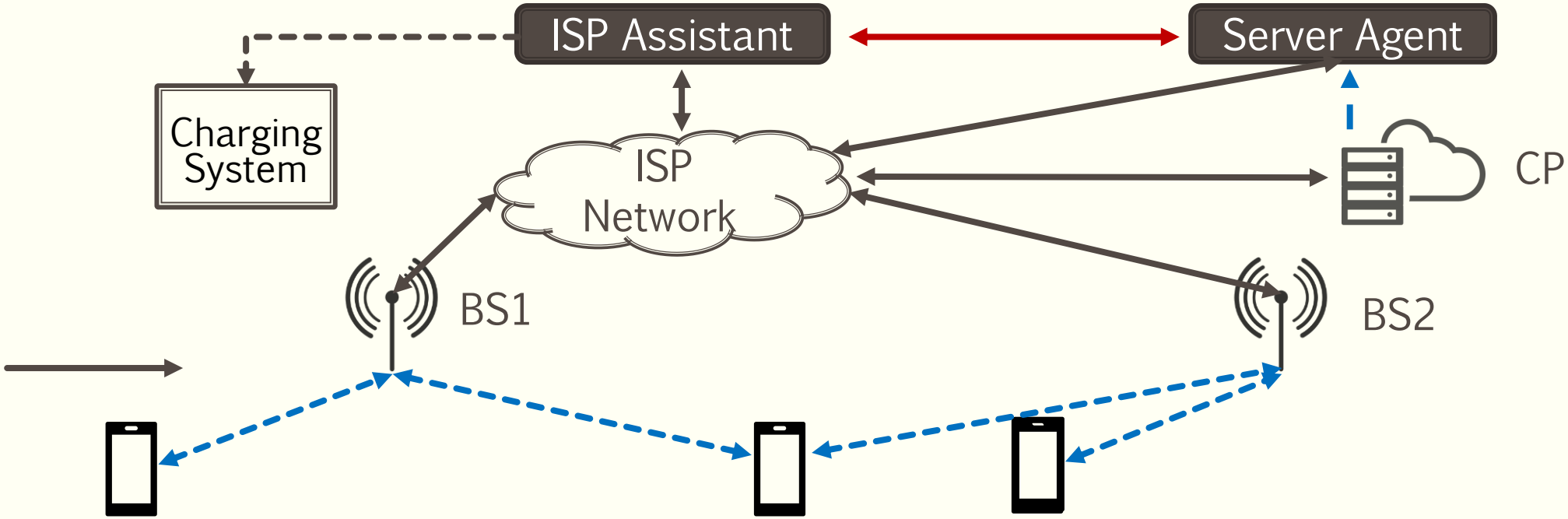
Evaluation: Environment Setup

- LTE network: ns3
- 1,200 UEs, two base stations (BSs)
- UE moving at speed 10-120km/h



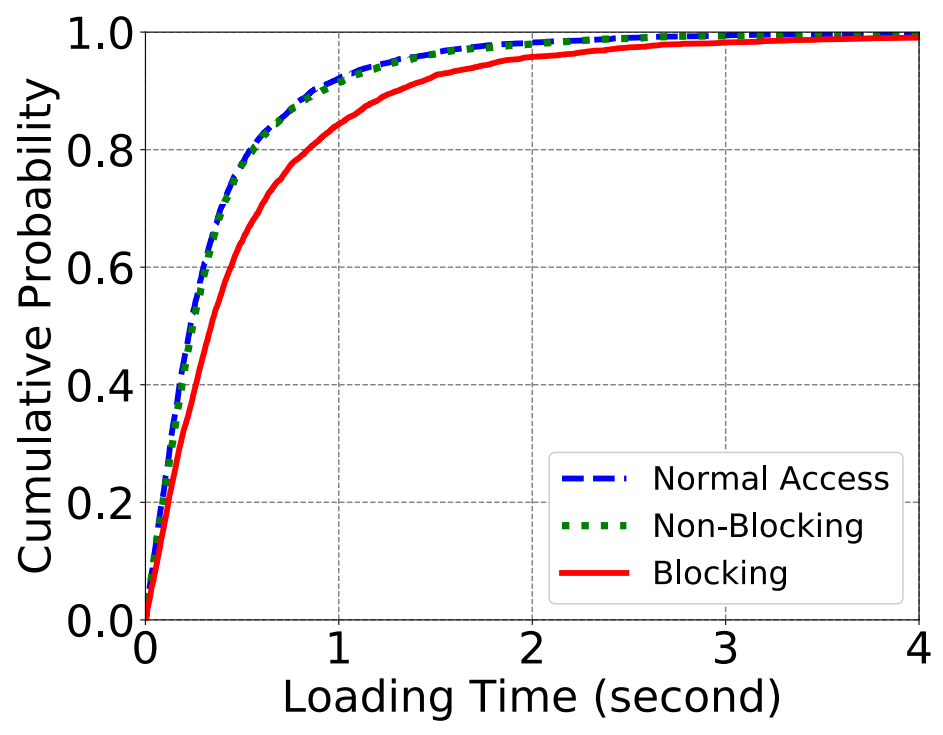
Evaluation: Environment Setup

- LTE network: ns3
- 1,200 UEs, two base stations (BSs)
- UE moving at speed 10-120km/h

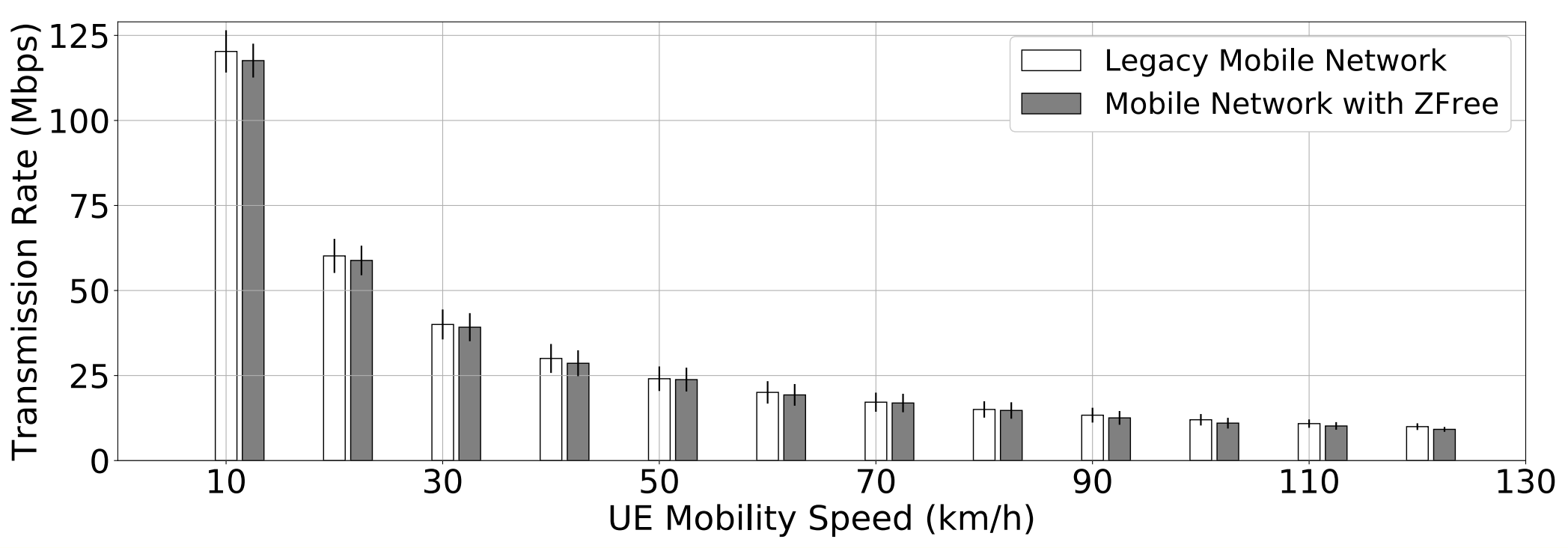


Evaluation: Page Loading Time Overhead is Ignorable

- Metric: Loading Time
- Content Provider as Network Proxy
- Top 500 Alexa websites

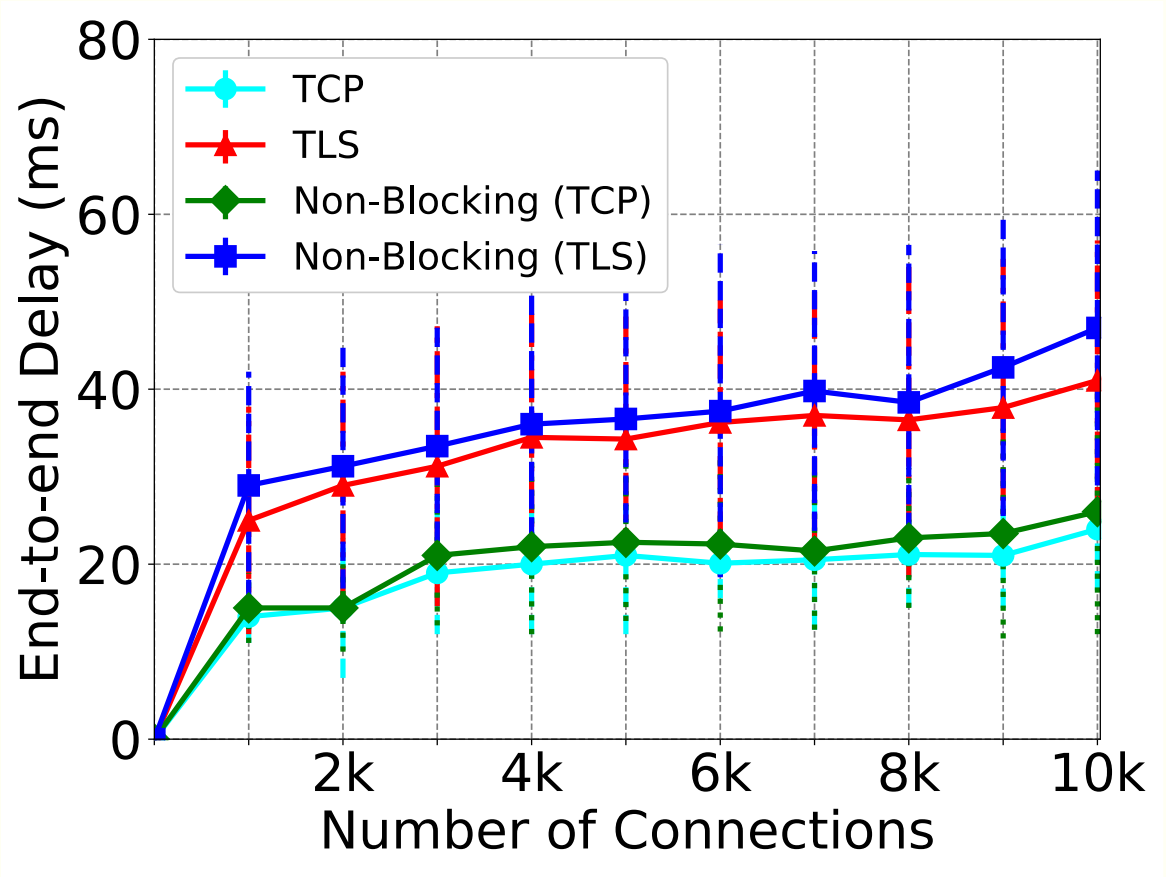


Evaluation: Transmission Overhead is Small

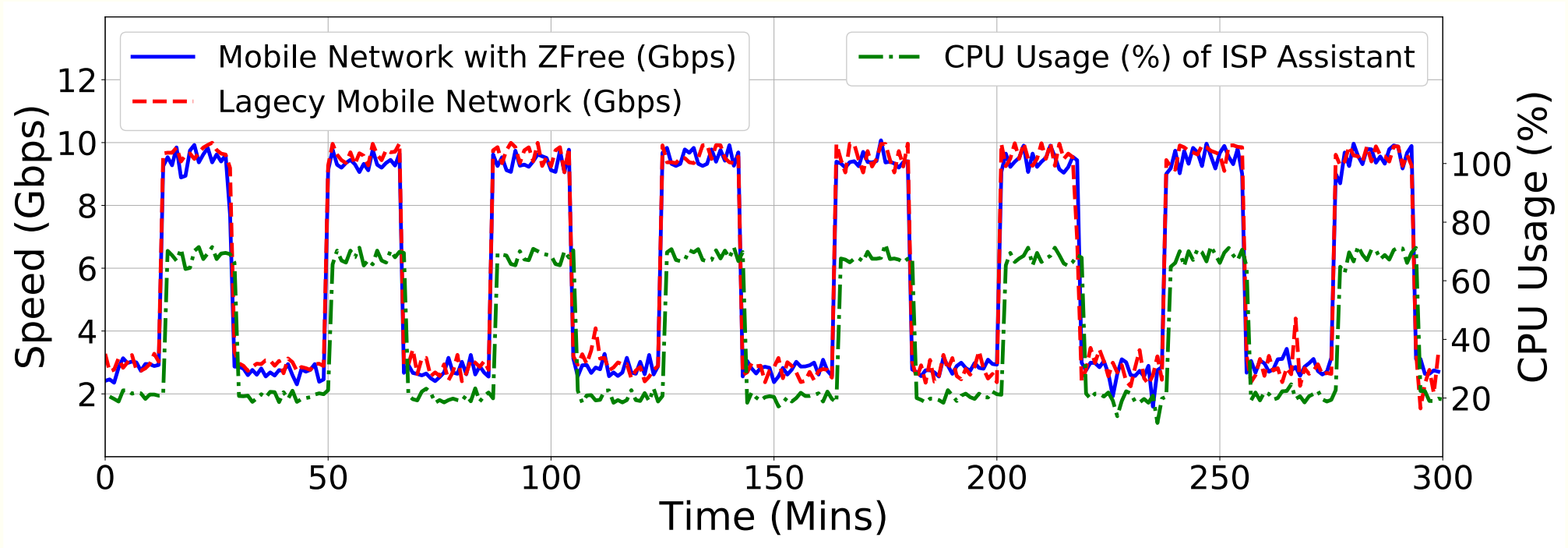


Evaluation: ZFree is Scalable

- Cellular Network: Bandwidth 150Mbps



Evaluation: ZFree is Durable



Evaluation: ZFree is Secure

- ZFree is robust against:
  - Request Masquerade attack
  - Response Modification attack
  - TCP retransmission-based attacks [1]

[1] Go, Younghwan, et al. "Gaining control of cellular traffic accounting by spurious TCP retransmission." *Network and Distributed System Security (NDSS) Symposium 2014*. Internet Society, 2014.

Outline

- Introduction
- Free-riding Attacks
- System Design
- Formal Security Analysis
- Implementation
- Evaluation
- **Conclusion**

Conclusion

- We launch free-riding attacks against real-world zero-rating services.
- We propose and implement ZFree, a secure, backward compatible, scalable zero-rating framework.
- We formally prove that ZFree is secure.
- Our evaluation results show that ZFree incurs ignorable overhead and is scalable.

Thank You! Questions?

- Source Code: https://github.com/zfree2018/ZFREE
- Online Demo: http://www.zfree.org