Circuit Fingerprinting Attack: Passive Deanonymization of Tor Hidden Services

Albert Kwon[1] Mashael Saad Al-Sabah[123] David Lazar[1]
Marc Dacier[2] Srinivas Devadas[1]

[1]CSAIL/MIT

[2]Qatar Computing Research Institute

[3]Qatar University

August 25, 2015

Outline

1. Backgound
2. Observations
3. Circuit Fingerprinting Attack
4. Website Fingerprinting Hidden Services
5. Conclusion

Outline

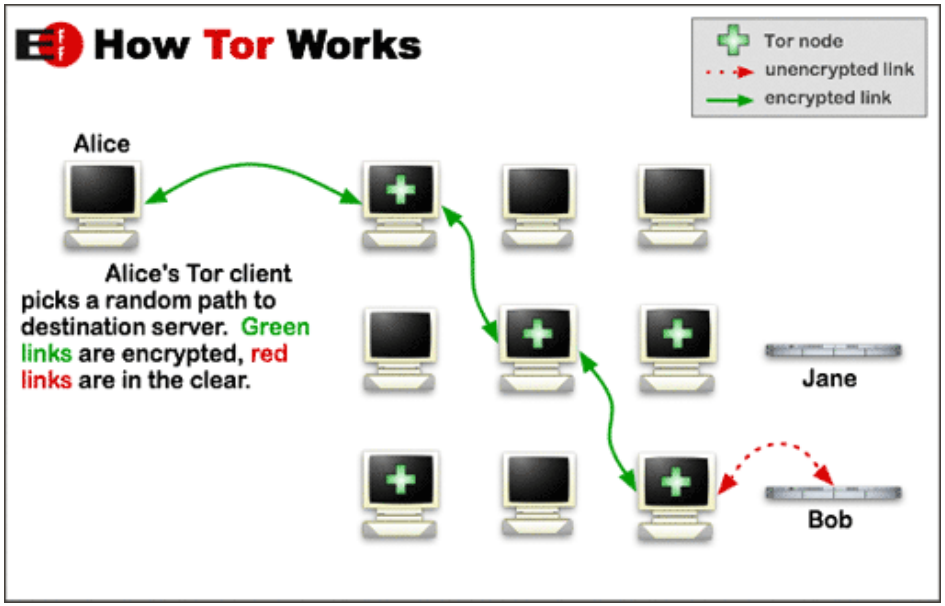
1. Backgound
2. Observations
3. Circuit Fingerprinting Attack
4. Website Fingerprinting Hidden Services
5. Conclusion

Tor: The Onion Router

- Conceal users' identities and activities

Tor: The Onion Router

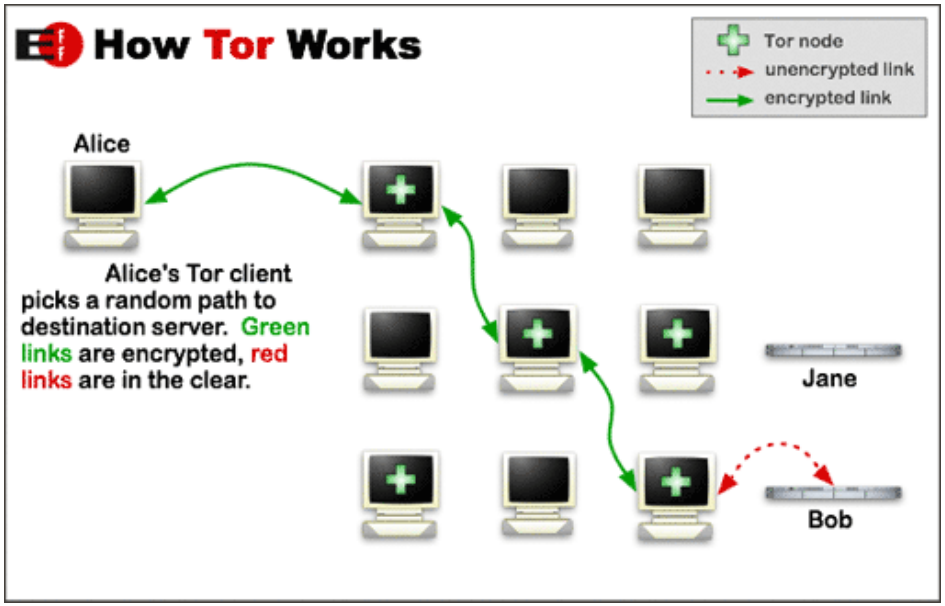
- Conceal users' identities and activities
- User picks 3 onion routers (*OR*),
  - Entry guard, middle, exit (*circuit*)



https://torproject.org

Tor: The Onion Router

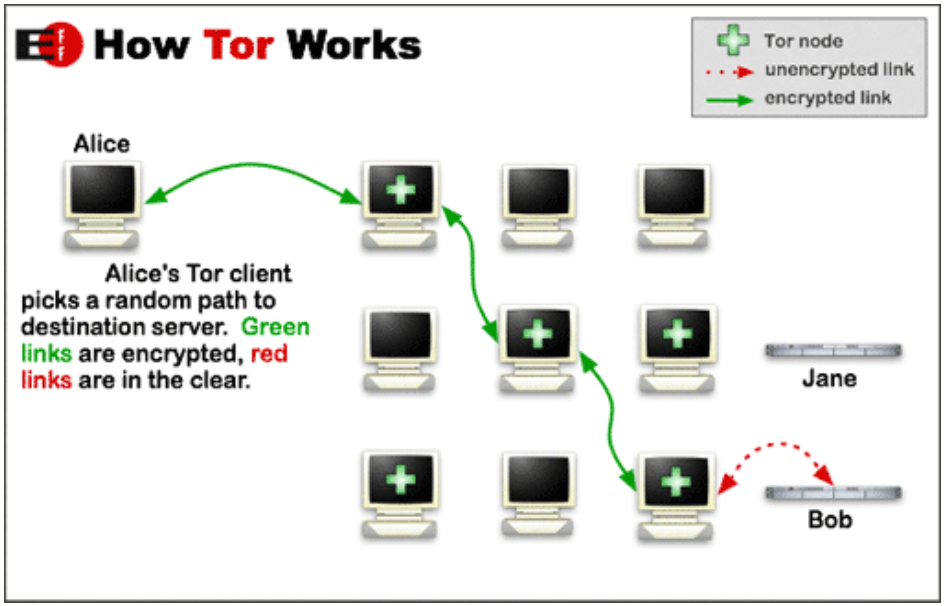
- Conceal users' identities and activities
- User picks 3 onion routers (*OR*),
  - Entry guard, middle, exit (*circuit*)
- Onion encrypts the message for the circuit



https://torproject.org

Tor: The Onion Router

- Conceal users' identities and activities
- User picks 3 onion routers (*OR*),
  - Entry guard, middle, exit (*circuit*)
- Onion encrypts the message for the circuit
- Protect client (user) anonymity



https://torproject.org

Tor Hidden Services (HS)

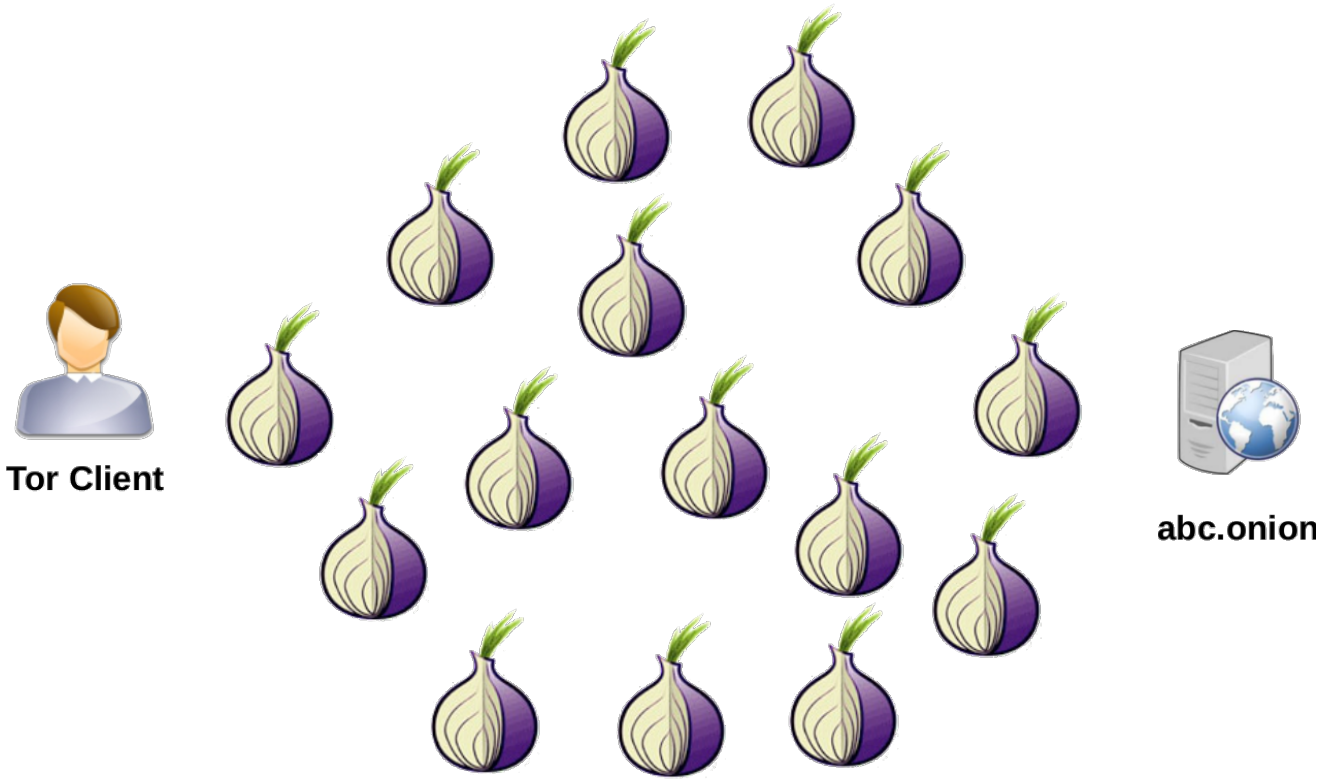
- Mechanism for protecting server anonymity

Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information

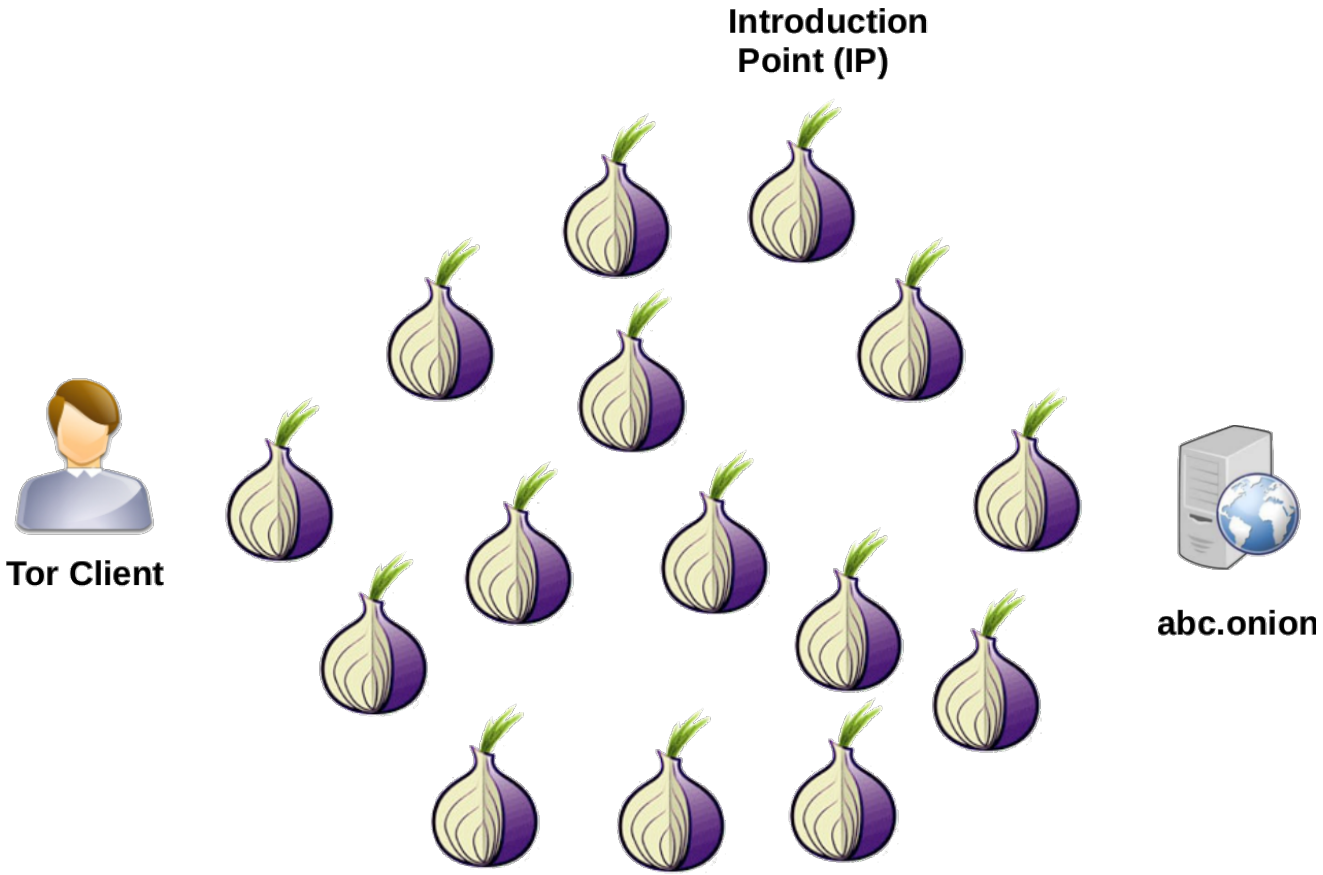
Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information



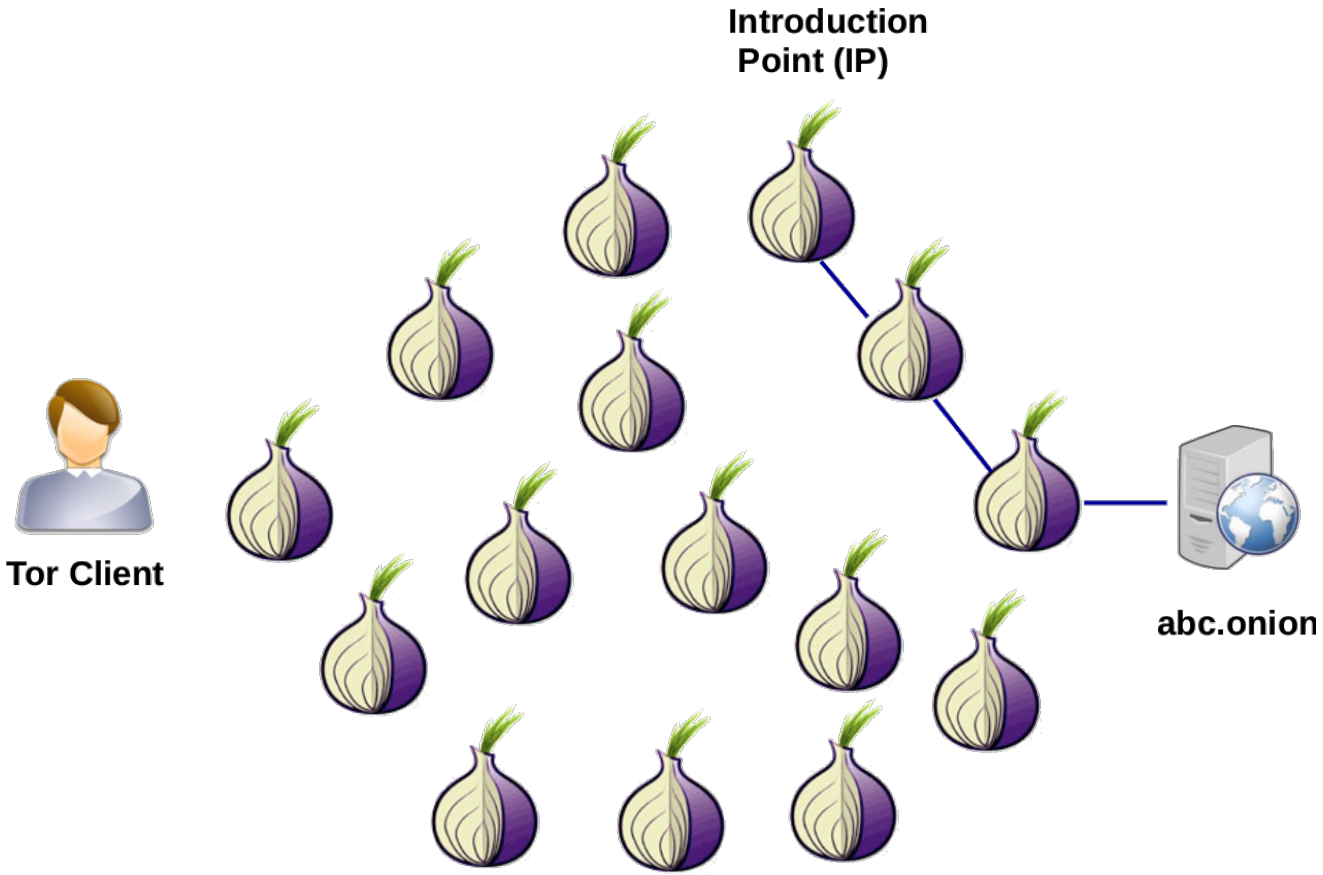
Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information



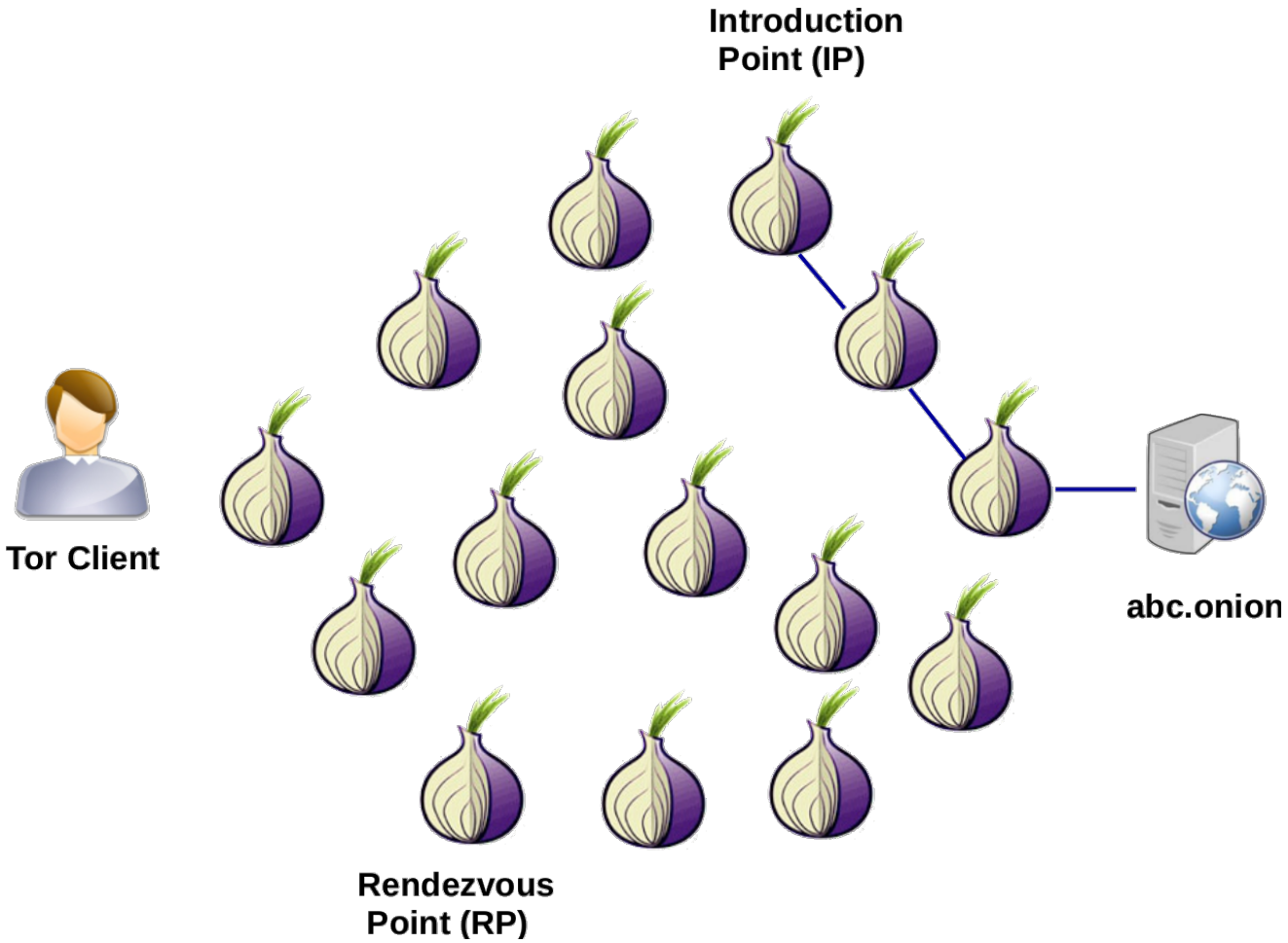
Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information



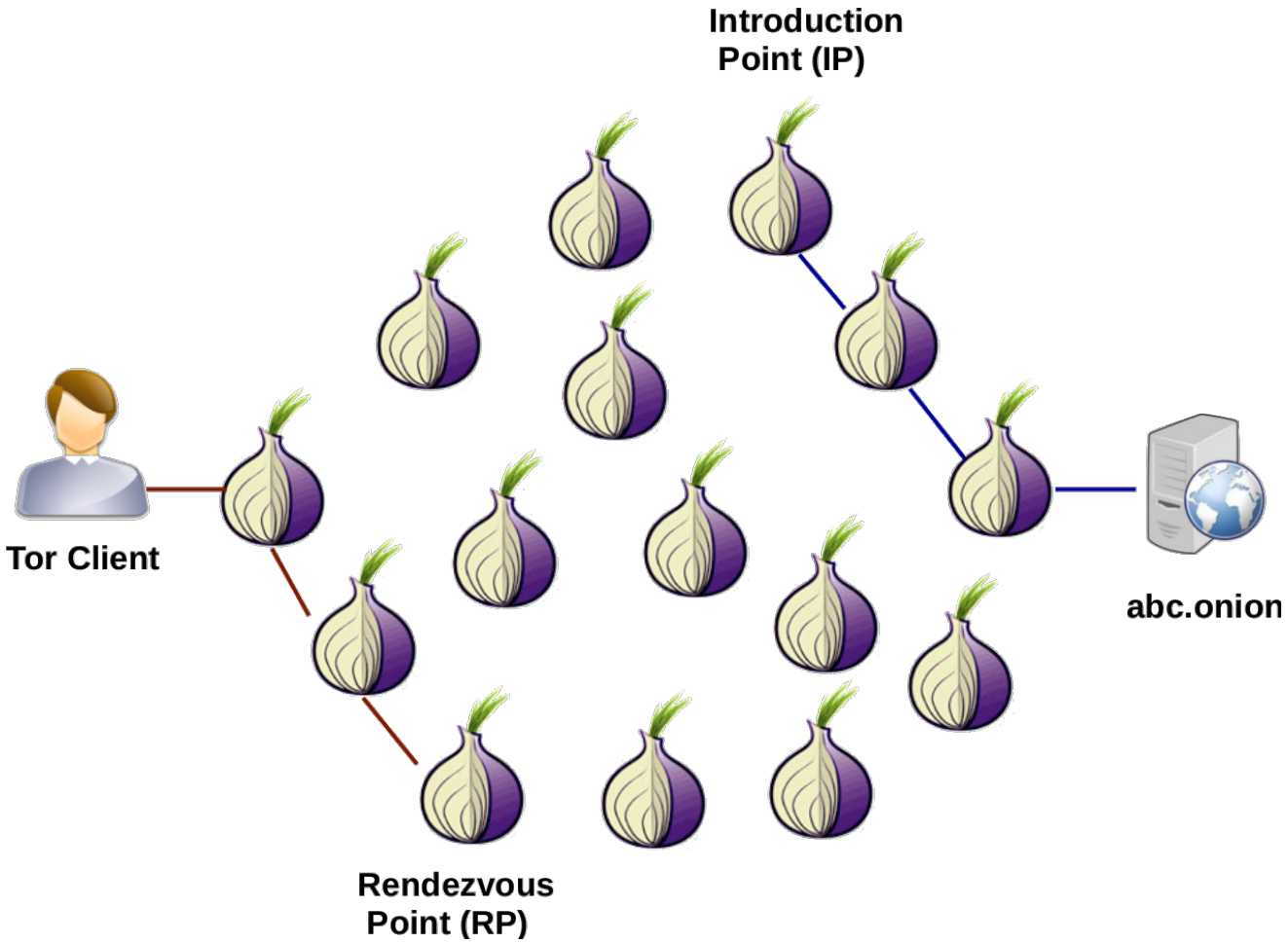
Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information



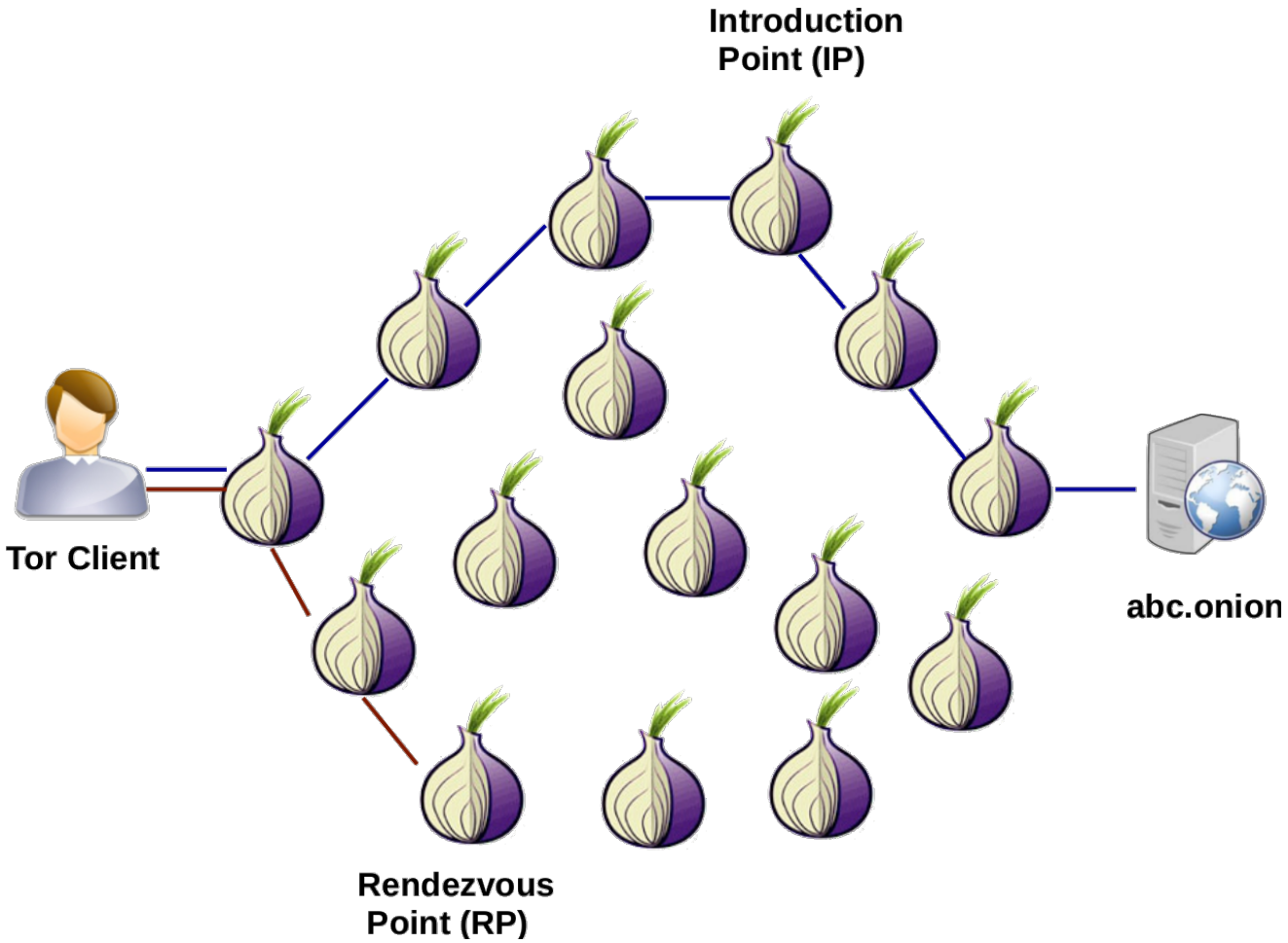
Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information



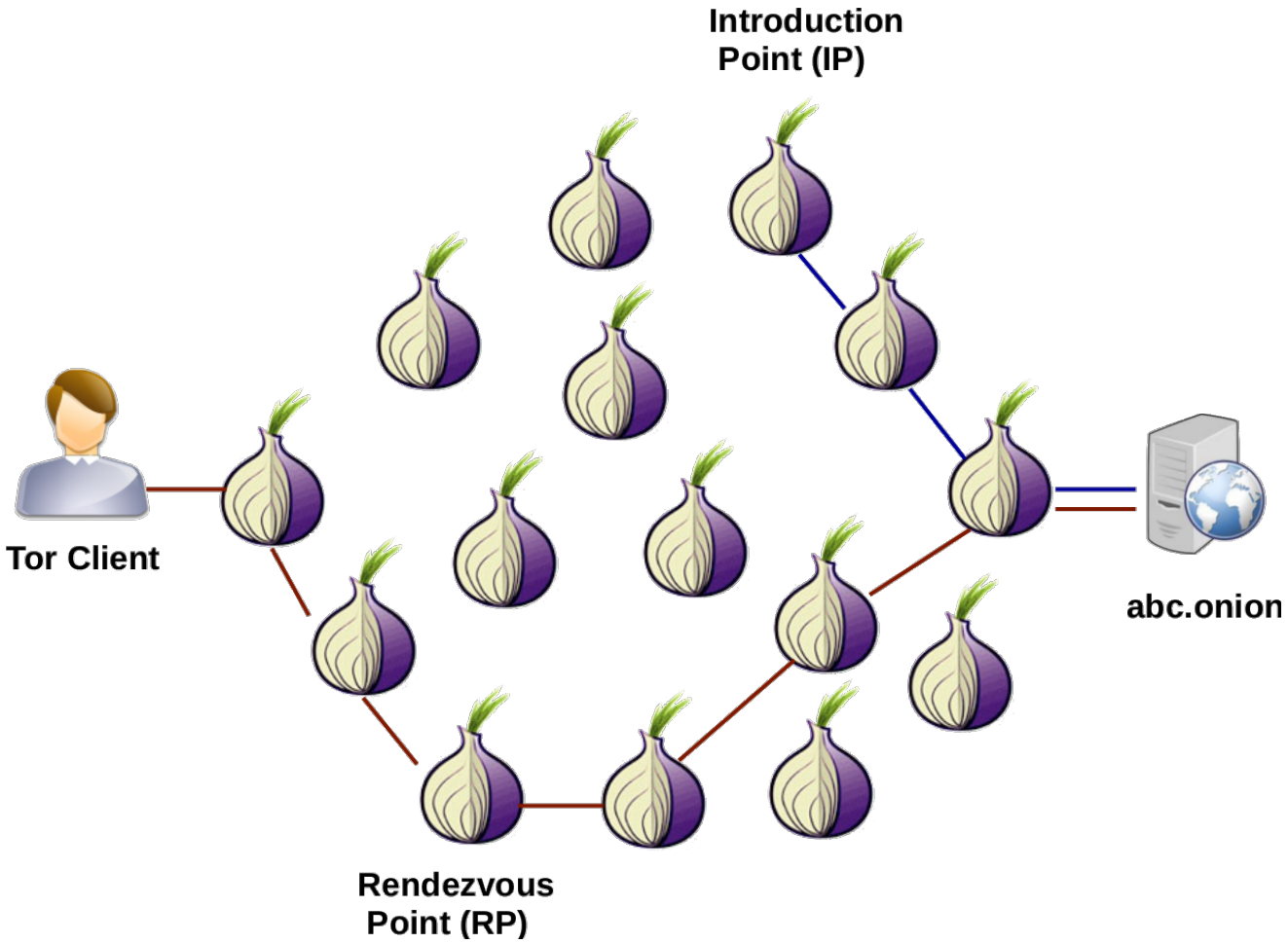
Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information



Tor Hidden Services (HS)

- Mechanism for protecting server anonymity
- Useful for servers hosting sensitive information



Threat Model

- Provide anonymity unless both ends of a circuit are compromised

Threat Model

- Provide anonymity unless both ends of a circuit are compromised
  - For HS, need to compromise two entry guards

Threat Model

- Provide anonymity unless both ends of a circuit are compromised
  - For HS, need to compromise two entry guards
- HS users/servers should look the same as regular clients

Threat Model

- Provide anonymity unless both ends of a circuit are compromised
  - For HS, need to compromise two entry guards
- HS users/servers should look the same as regular clients
- Our goal: break HS anonymity as a local adversary

Threat Model

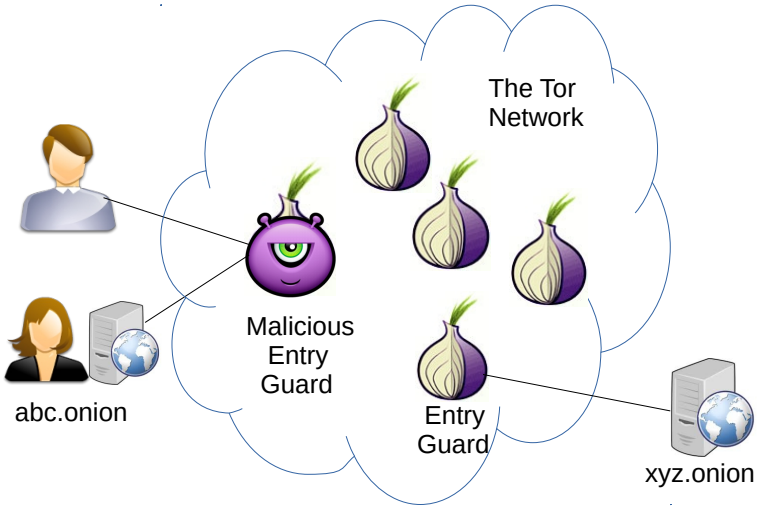
- Provide anonymity unless both ends of a circuit are compromised
  - For HS, need to compromise two entry guards
- HS users/servers should look the same as regular clients
- Our goal: break HS anonymity as a local adversary
  - Can get accurate packet information

Threat Model

- Provide anonymity unless both ends of a circuit are compromised
  - For HS, need to compromise two entry guards
- HS users/servers should look the same as regular clients
- Our goal: break HS anonymity as a local adversary
  - Can get accurate packet information
  - Has circuit level visibility

Threat Model

- Provide anonymity unless both ends of a circuit are compromised
  - For HS, need to compromise two entry guards
- HS users/servers should look the same as regular clients
- Our goal: break HS anonymity as a local adversary
  - Can get accurate packet information
  - Has circuit level visibility
    - Malicious entry guard



Approach and Experiments

- Experiments on live Tor network

Approach and Experiments

- Experiments on live Tor network
- Client side experiment
  - Visiting multiple websites and hidden services

Approach and Experiments

- Experiments on live Tor network
- Client side experiment
  - Visiting multiple websites and hidden services
- Server side experiment
  - Our own HS that serves cached versions of other HS

Approach and Experiments

- Experiments on live Tor network
- Client side experiment
  - Visiting multiple websites and hidden services
- Server side experiment
  - Our own HS that serves cached versions of other HS
- Identify HS circuits using their unique features

Approach and Experiments

- Experiments on live Tor network
- Client side experiment
  - Visiting multiple websites and hidden services
- Server side experiment
  - Our own HS that serves cached versions of other HS
- Identify HS circuits using their unique features
- Classify HS once the circuits are isolated

Outline

1 Backgound

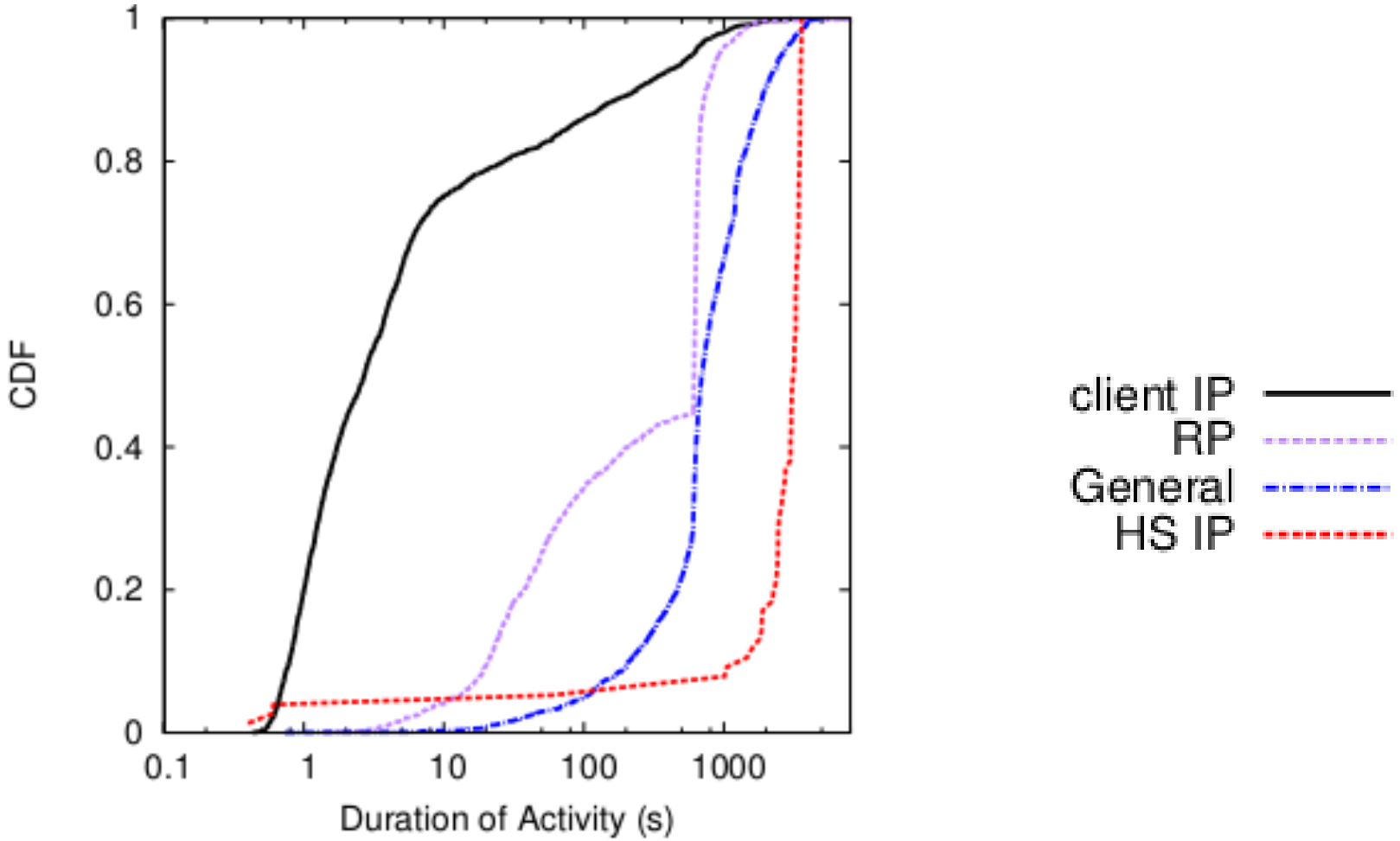
2 Observations

3 Circuit Fingerprinting Attack

4 Website Fingerprinting Hidden Services

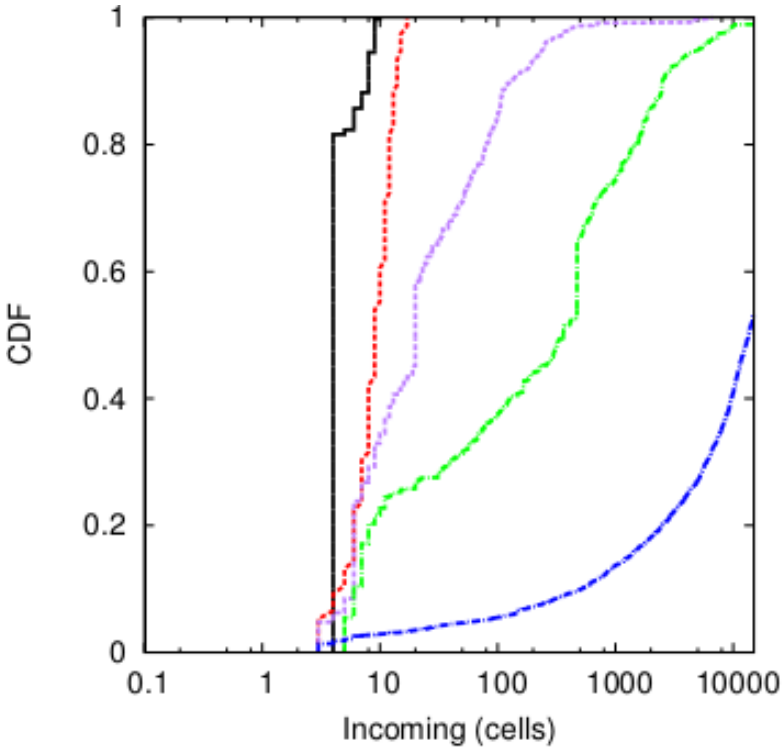
5 Conclusion

Characteristics: Cumulative Distribution Function

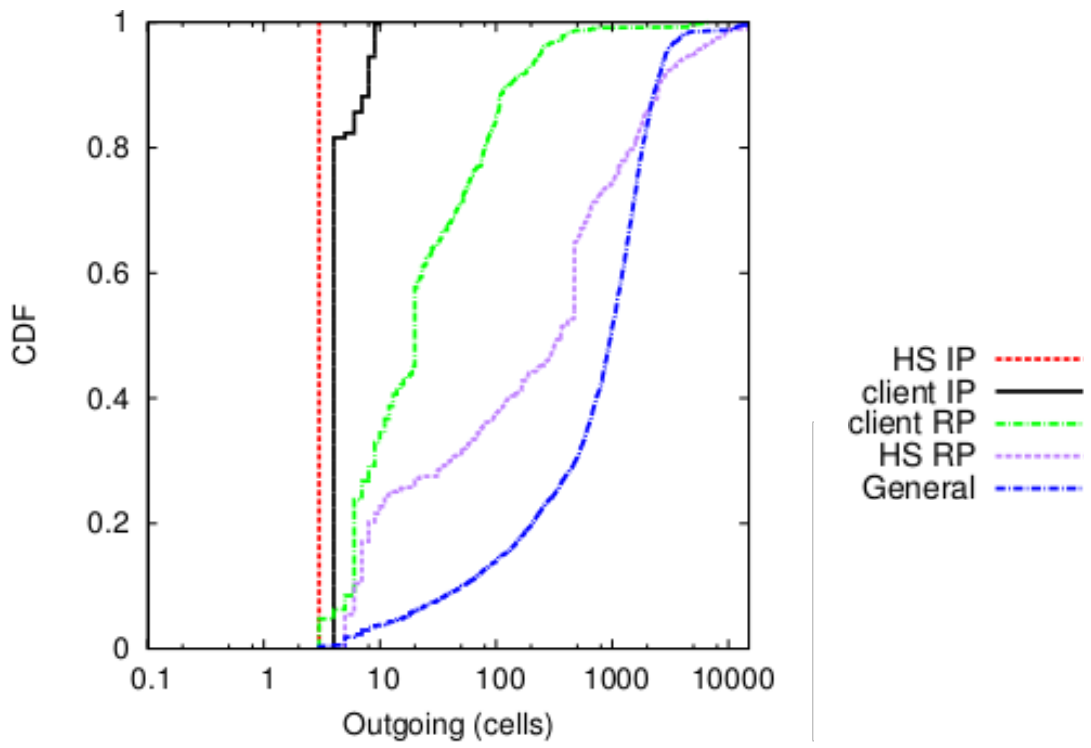


The duration of activity

Characteristics: Cumulative Distribution Function



The number of incoming cells



The number of outgoing cells

Observations

- IP circuits have unique characteristics
  - HS-IP's are long-lived and Client-IP's are short-lived
  - IP's have have little incoming and outgoing cells

Observations

- IP circuits have unique characteristics
  - HS-IP's are long-lived and Client-IP's are short-lived
  - IP's have have little incoming and outgoing cells
- HS-RP circuits have more outgoing than incoming

Observations

- IP circuits have unique characteristics
  - HS-IP's are long-lived and Client-IP's are short-lived
  - IP's have have little incoming and outgoing cells
- HS-RP circuits have more outgoing than incoming
- Streams for different `.onion` domains are not multiplexed

Observations

- IP circuits have unique characteristics
  - HS-IP's are long-lived and Client-IP's are short-lived
  - IP's have have little incoming and outgoing cells
- HS-RP circuits have more outgoing than incoming
- Streams for different `.onion` domains are not multiplexed
- IP and RP circuits are disjoint from general circuits

Observations

- IP circuits have unique characteristics
  - HS-IP's are long-lived and Client-IP's are short-lived
  - IP's have have little incoming and outgoing cells
- HS-RP circuits have more outgoing than incoming
- Streams for different `.onion` domains are not multiplexed
- IP and RP circuits are disjoint from general circuits
- Special circuits have particular starting cell sequences

Outline

1 Backgound

2 Observations

3 Circuit Fingerprinting Attack

4 Website Fingerprinting Hidden Services

5 Conclusion

Circuit Classification Attack

- Use the characteristics to classify circuits
  - HS-IP, Client-IP, HS-RP, Client-RP, and General

Circuit Classification Attack

- Use the characteristics to classify circuits
  - HS-IP, Client-IP, HS-RP, Client-RP, and General
- Features of the circuits
  - Duration of activity
  - The number of incoming and outgoing cells
  - Sequence of the first 10 cells

Circuit Classification Attack

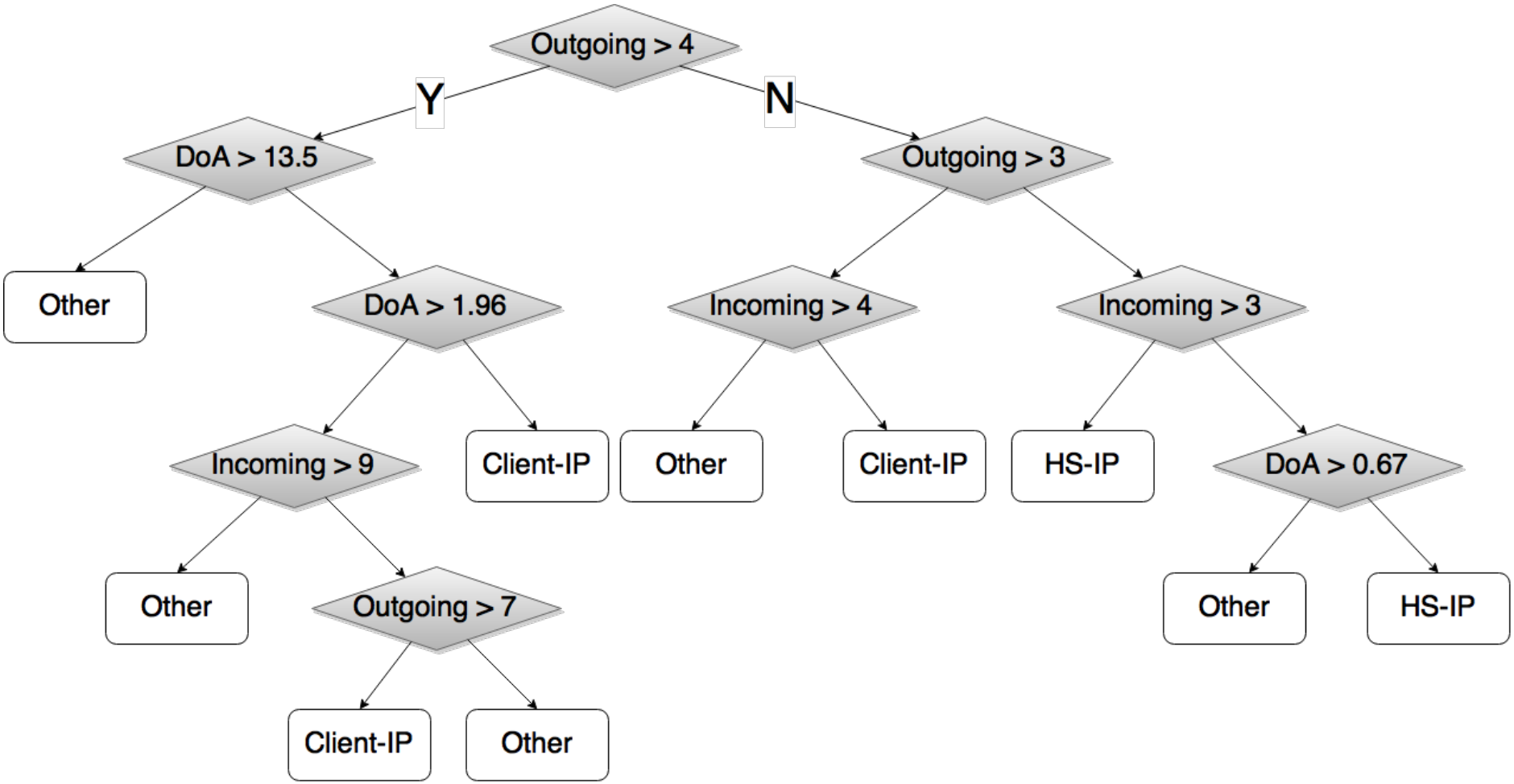
- Use the characteristics to classify circuits
  - HS-IP, Client-IP, HS-RP, Client-RP, and General
- Features of the circuits
  - Duration of activity
  - The number of incoming and outgoing cells
  - Sequence of the first 10 cells
- Tree-based and k-NN for classifier

IP-Decision Tree

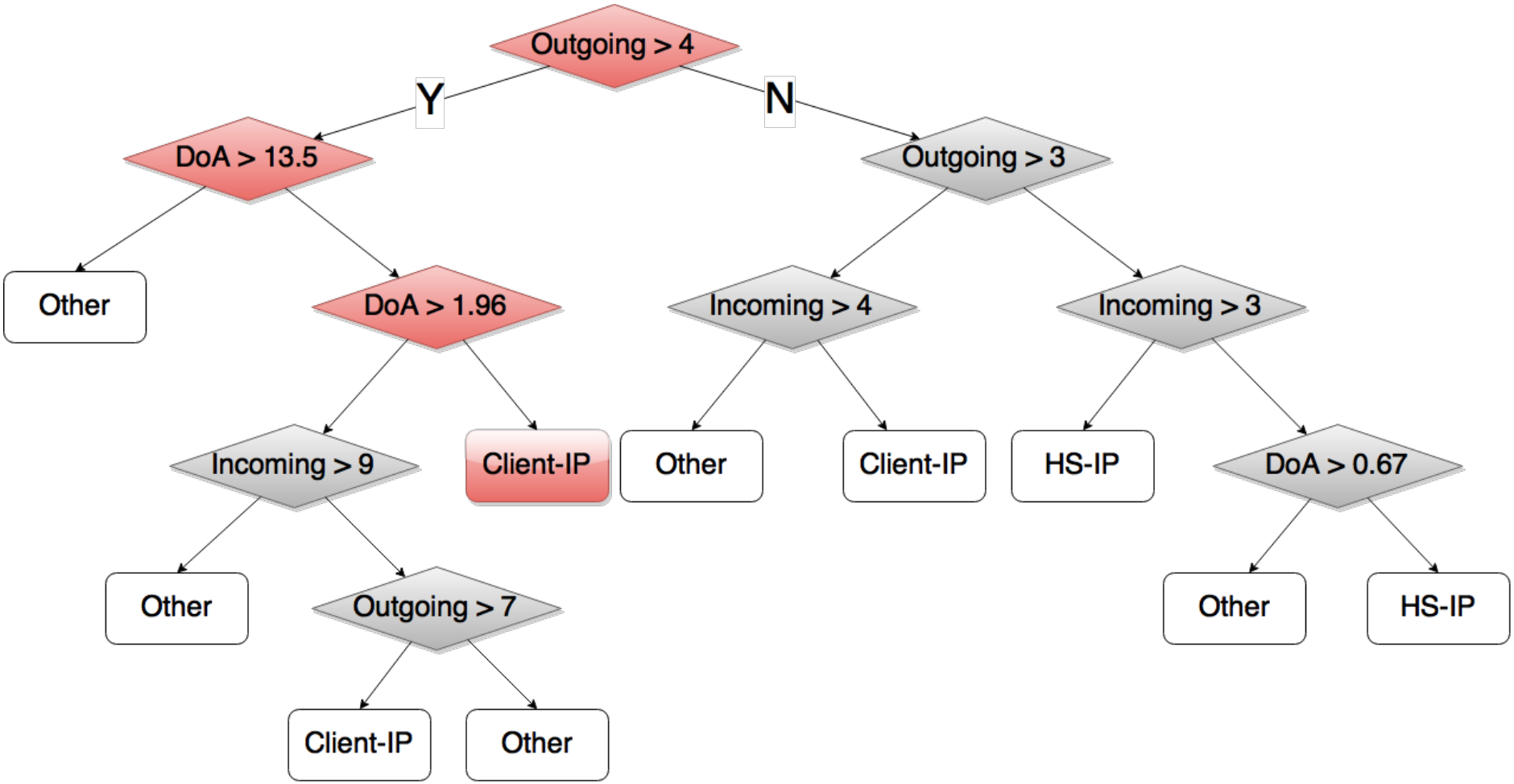
```
outgoing <= 4
|   outgoing <= 3
|   |   incoming <= 3
|   |   |   DoA <= 0.66873: HS-IP (3.0)
|   |   |   DoA > 0.66873: noise (16.0/1.0)
|   |   incoming > 3: HS-IP (72.0)
|   outgoing > 3
|   |   incoming <= 4: Client-IP (199.0/12.0)
|   |   incoming > 4: noise (39.0)
outgoing > 4
|   DoA <= 13.507868
|   |   DoA <= 1.962158: Client-IP (5.0)
|   |   DoA > 1.962158
|   |   |   incoming <= 9
|   |   |   |   outgoing <= 7: noise (42.0)
|   |   |   |   outgoing > 7: Client-IP (7.0)
|   |   |   incoming > 9: noise (84.0)
|   DoA > 13.507868: noise (6402.0/1.0)
```

19 nodes and 10 leaves

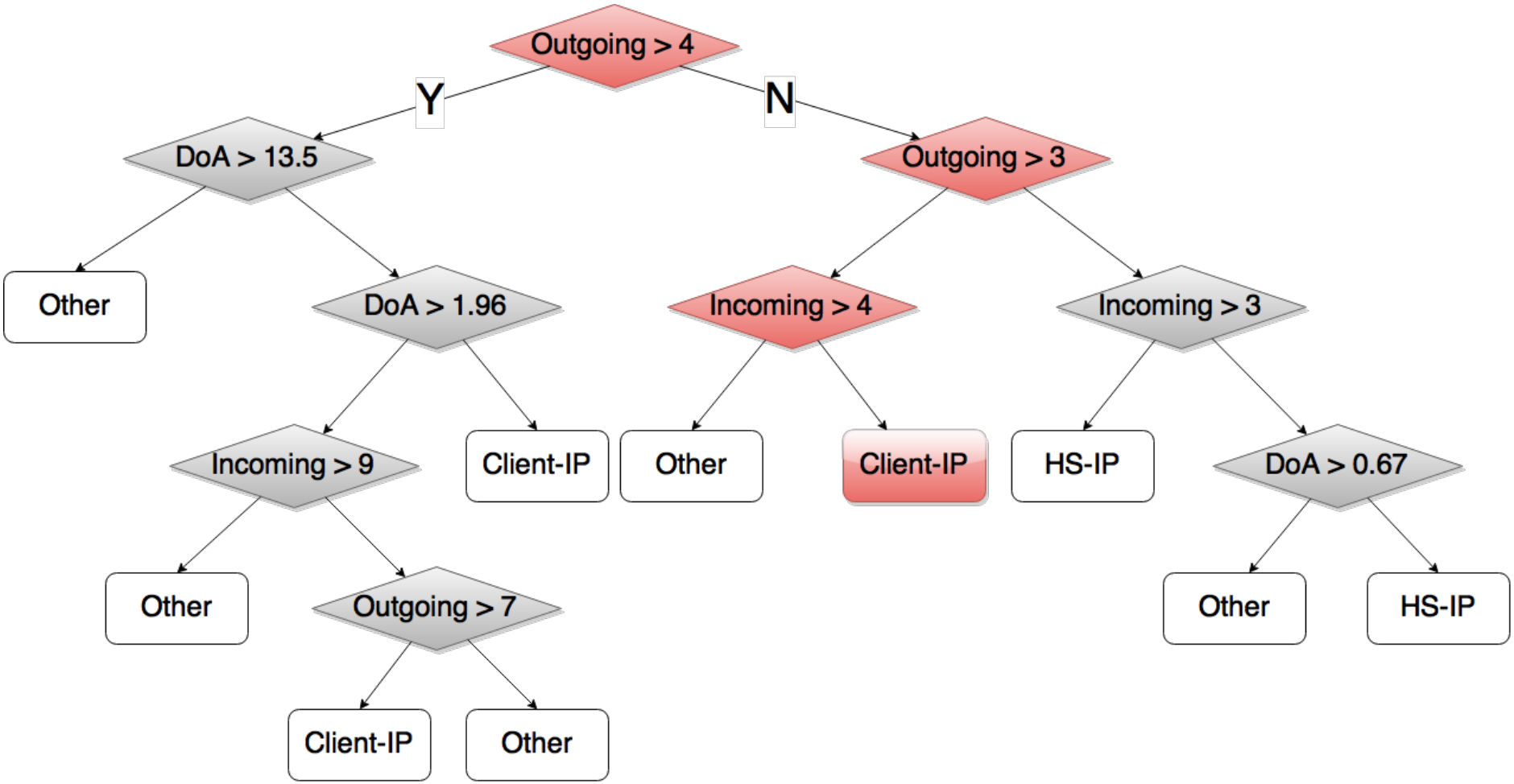
IP-Decision Tree



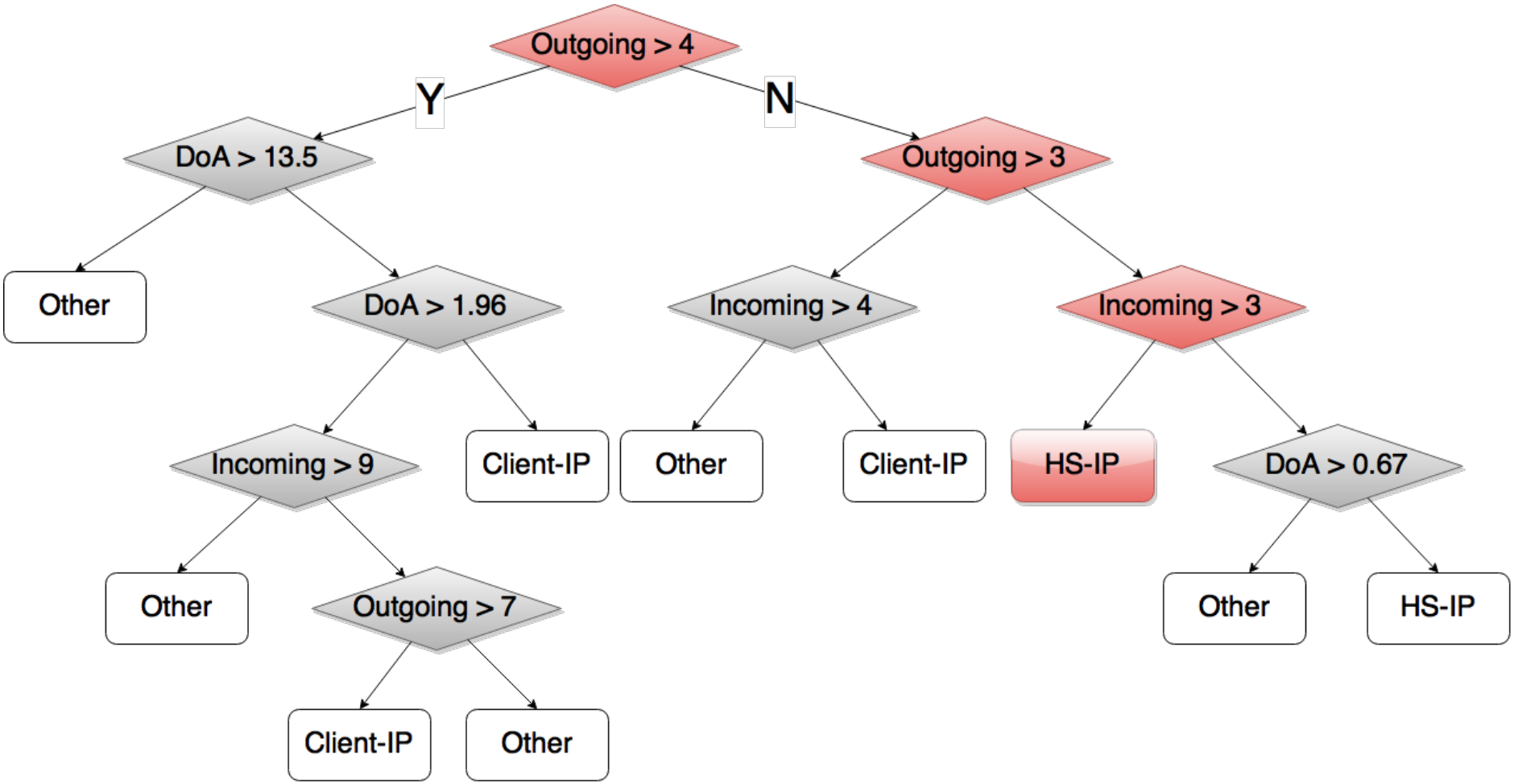
IP-Decision Tree



IP-Decision Tree



IP-Decision Tree

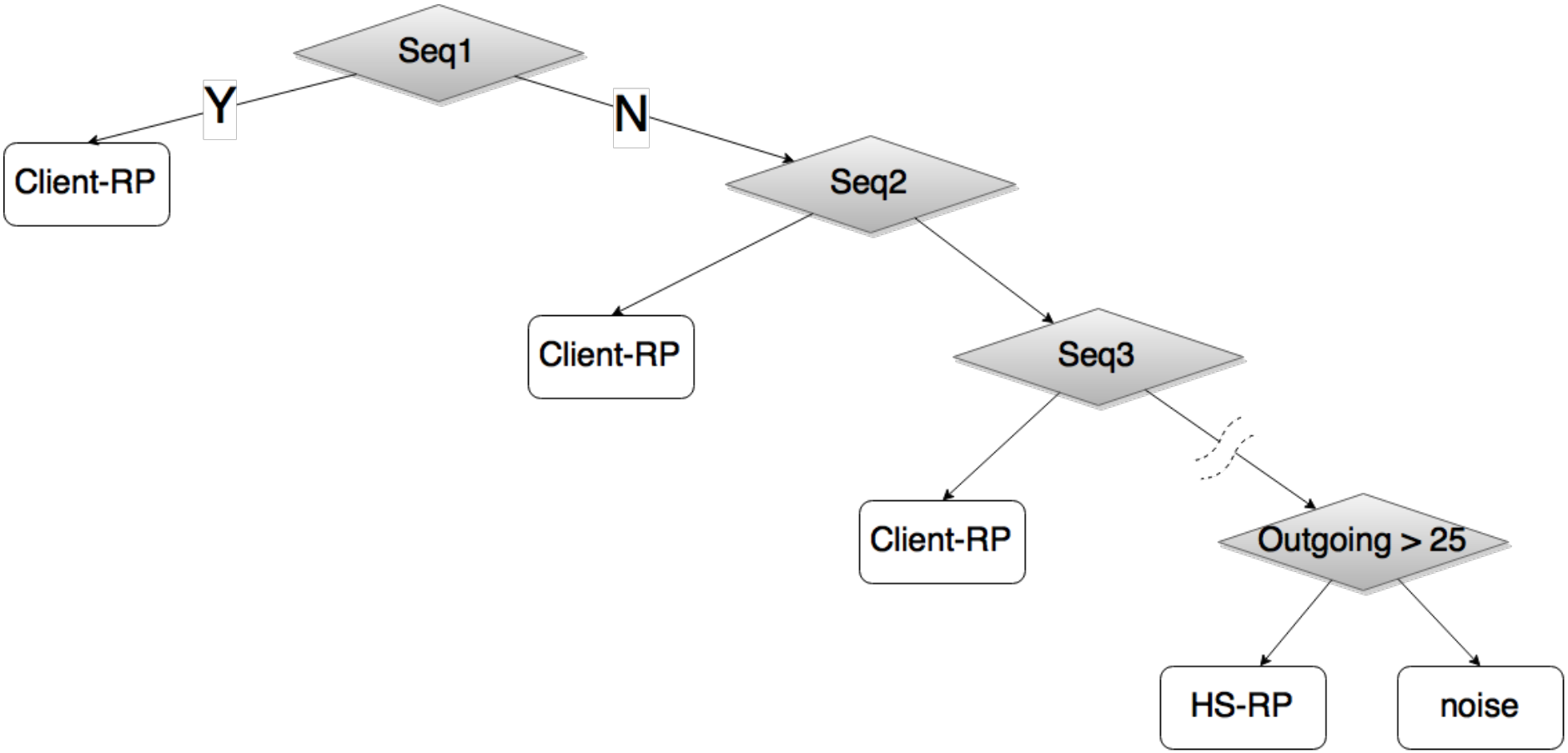


RP-Decision Tree

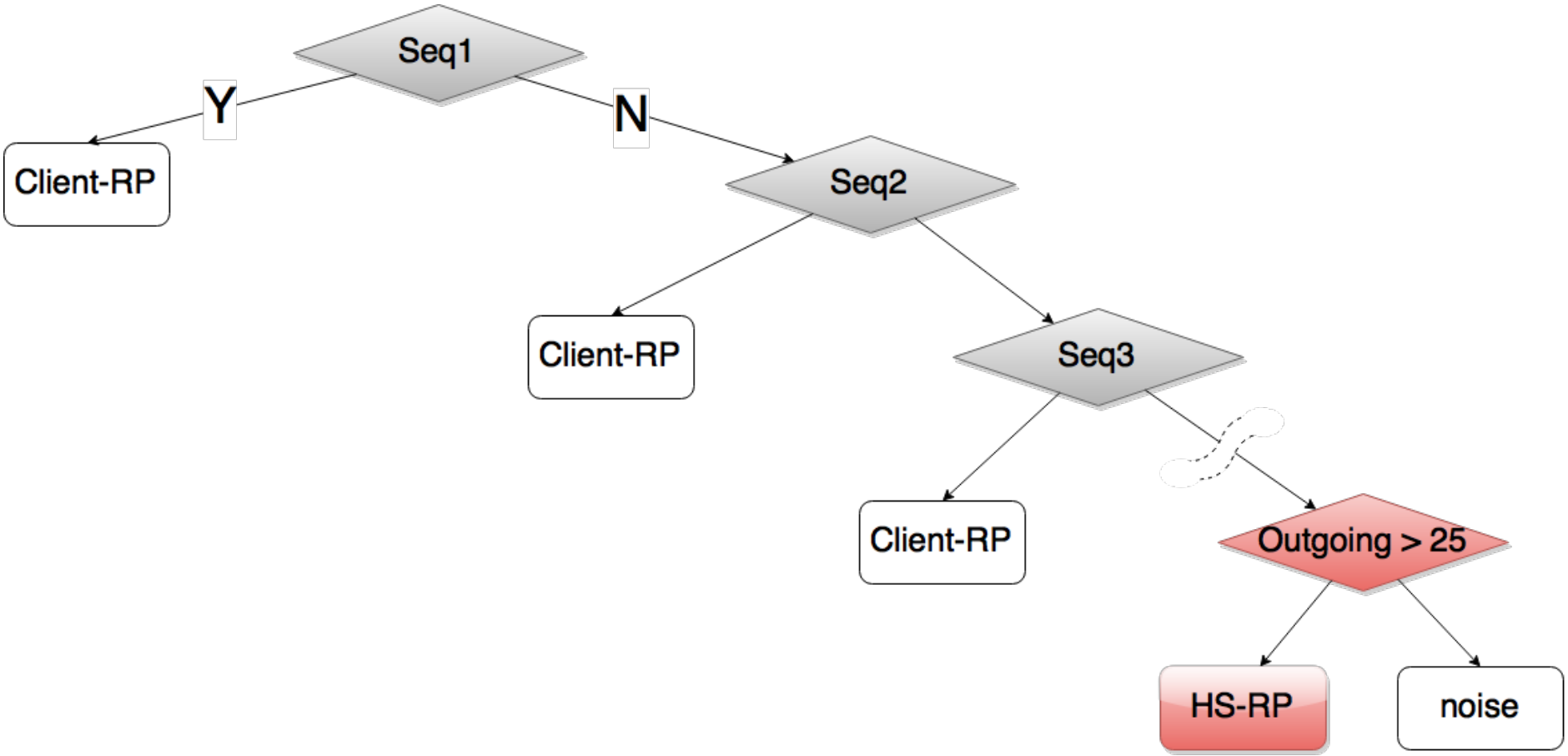
```
-1+1-1+1-1+1+1-1+1-1 <= 0
|    -1+1-1+1-1+1+1-1+1 <= 0
|    |    -1+1-1+1-1+1+1-1+1+1 <= 0
|    |    |    inc_50 <= 25
|    |    |    |    -1+1-1+1-1+1-1 <= 0
|    |    |    |    |    -1+1-1+1-1+1-1+1 <= 0
|    |    |    |    |    |    -1+1-1+1-1+1-1+1-1+1 <= 0: noise (136.0)
|    |    |    |    |    |    -1+1-1+1-1+1-1+1-1+1 > 0
|    |    |    |    |    |    |    out_50 <= 25: noise (69.0/8.0)
|    |    |    |    |    |    |    out_50 > 25: HS-RP (931.0/5.0)
|    |    |    |    |    -1+1-1+1-1+1-1+1 > 0: HS-RP (13.0/5.0)
|    |    |    |    -1+1-1+1-1+1-1 > 0: HS-RP (12.0)
|    |    |    inc_50 > 25: noise (3657.0)
|    |    -1+1-1+1-1+1+1-1+1+1 > 0: Client-RP (38.0)
|    -1+1-1+1-1+1+1-1+1 > 0: Client-RP (40.0)
-1+1-1+1-1+1+1-1+1-1 > 0: Client-RP (4436.0)
```

17 nodes and 9 leaves

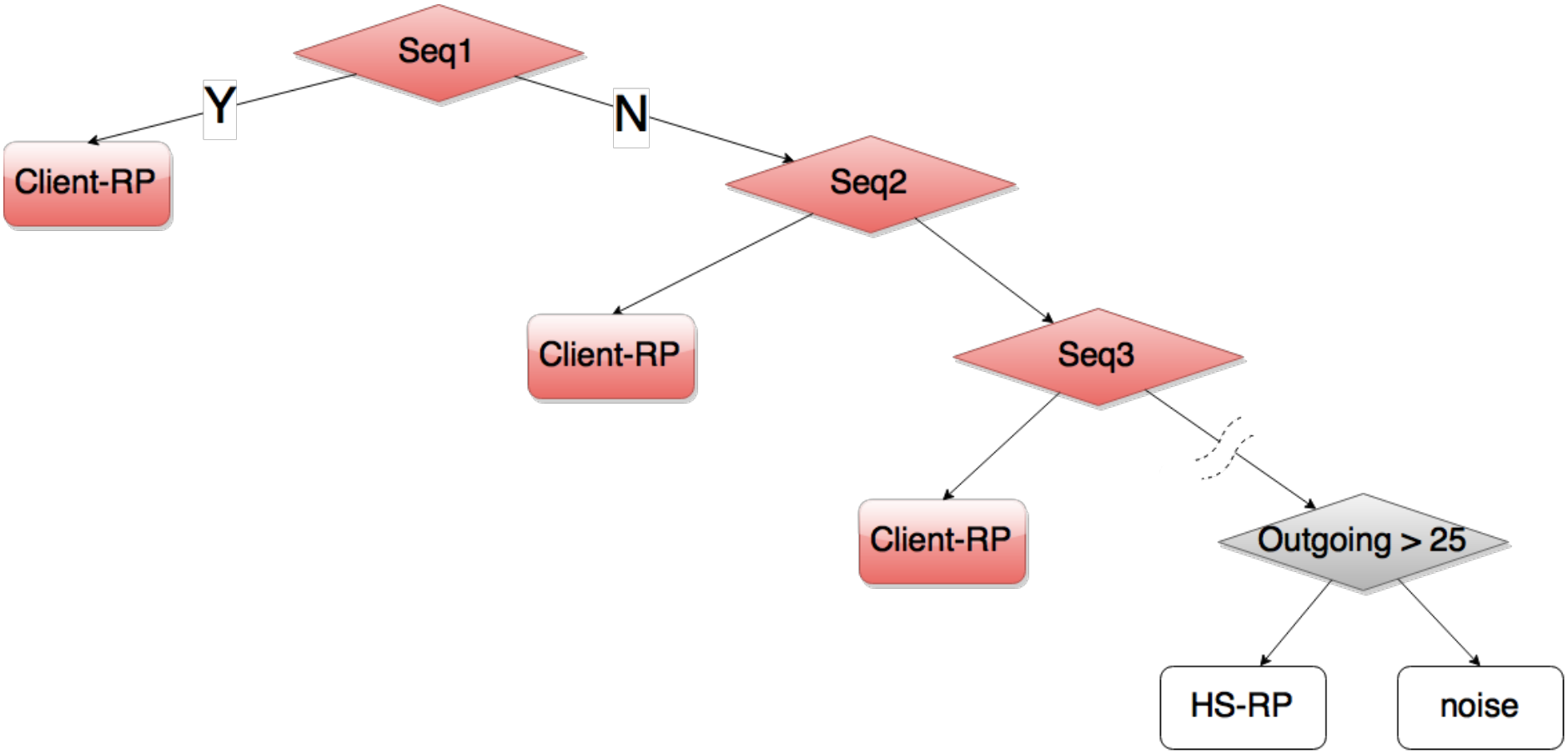
RP-Decision Tree



RP-Decision Tree



RP-Decision Tree

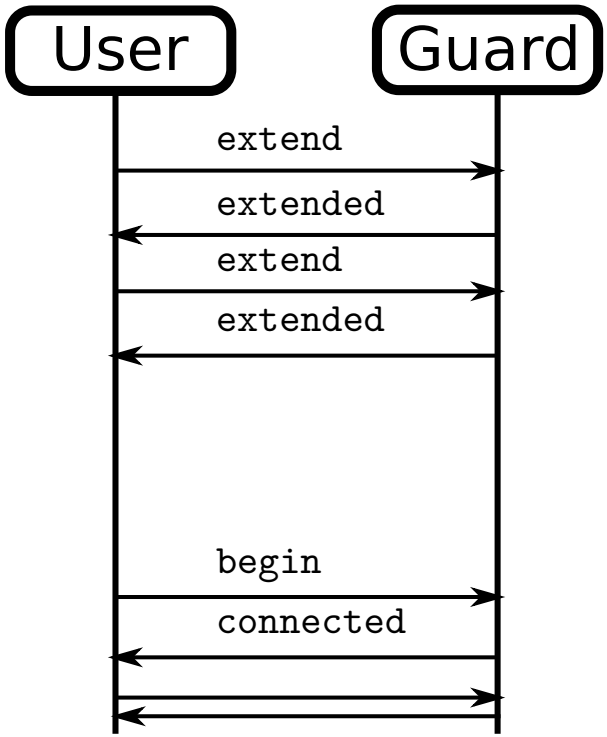


RP-Uniqueness

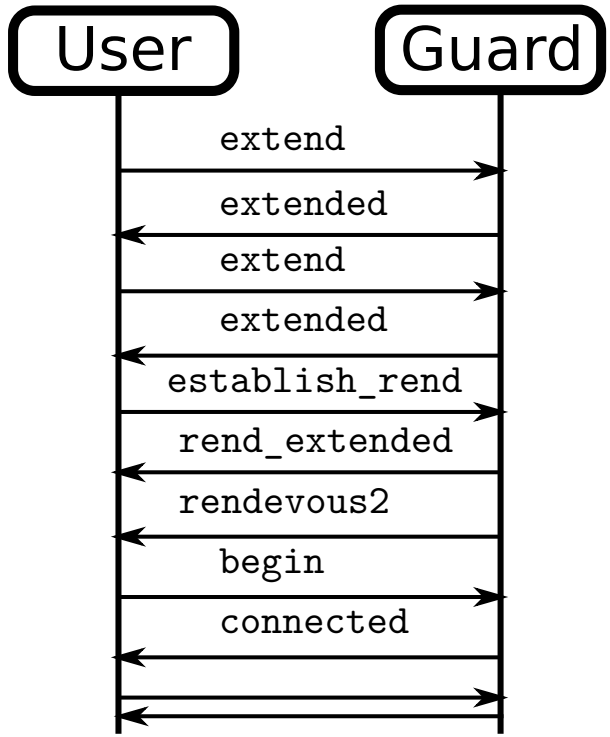
- Sequences:
  - O, I, O, I, O, I, I, O, I, O
  - O, I, O, I, O, I, I, O, I
  - O, I, O, I, O, I, I, O, I, I

RP-Uniqueness

- Sequences:
  - O, I, O, I, O, I, I, O, I, O
  - O, I, O, I, O, I, I, O, I
  - O, I, O, I, O, I, I, O, I, I



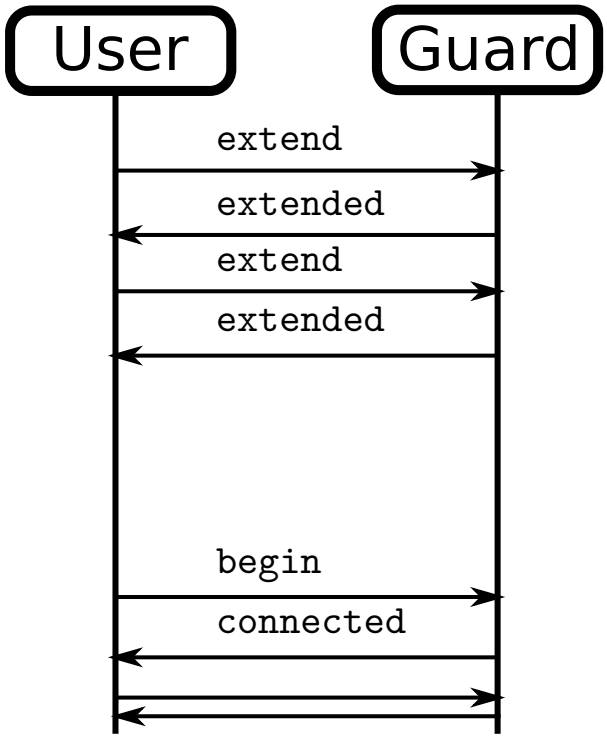
General circuit



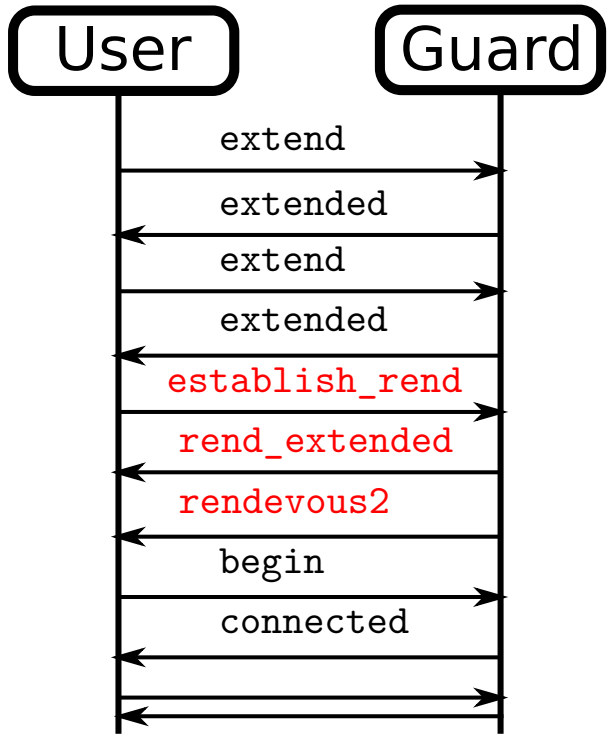
Client-RP circuit

RP-Uniqueness

- Sequences:
  - O, I, O, I, O, I, I, O, I, O
  - O, I, O, I, O, I, I, O, I
  - O, I, O, I, O, I, I, O, I, I



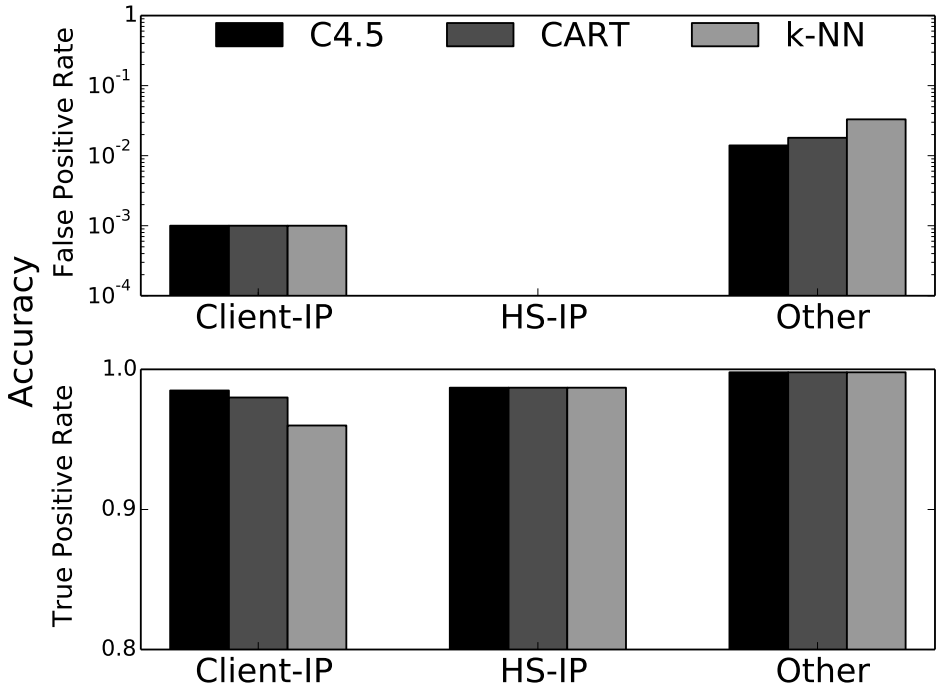
General circuit



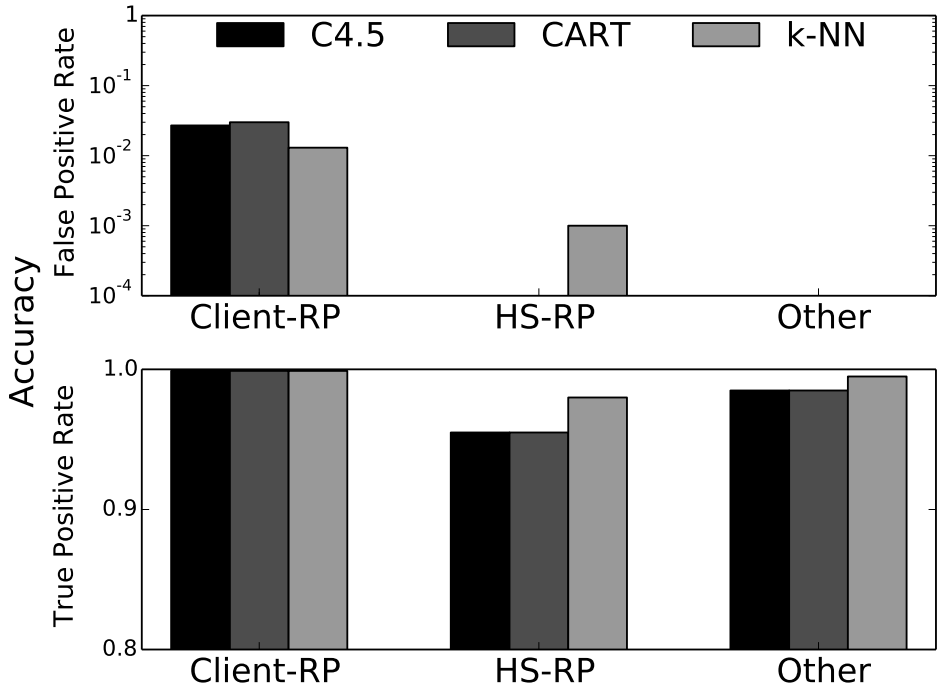
Client-RP circuit

Evaluation: Circuit Classification

- Dataset
  - 76 HS-IP, 200 Client-IP, and 6593 others
  - 954 HS-RP, 4514 Client-RP, and 3862 others



IP Classification Accuracy



RP Classification Accuracy

Outline

1 Backgound

2 Observations

3 Circuit Fingerprinting Attack

4 Website Fingerprinting Hidden Services

5 Conclusion

Website Fingerprinting (WF)

- Local adversary to deanonymize a user
- Classify websites using features of the communication
  - Duration of activity
  - Number of incoming/outgoing
  - Bursts of incoming/outgoing

WF Criticisms*

- Noisy streams of data
  - General circuits are multiplexed between multiple connections

*Juarez et al., A Critical Evaluation of Website Fingerprinting Attacks, CCS 2014.

WF Criticisms*

- Noisy streams of data
  - General circuits are multiplexed between multiple connections
- Size of the world
  - Experiments only include $<$ 10,000 websites

* Juarez et al., A Critical Evaluation of Website Fingerprinting Attacks, CCS 2014.

WF Criticisms*

- Noisy streams of data
  - General circuits are multiplexed between multiple connections
- Size of the world
  - Experiments only include $<$ 10,000 websites
- Rapidly changing pages
  - Websites' contents (and thus traffic) are constantly changing

*Juarez et al., A Critical Evaluation of Website Fingerprinting Attacks, CCS 2014.

Website Fingerprinting HS

- HS circuits are not shared
  - Different `.onion` use different circuits
  - RP circuits and general circuits are disjoint

Website Fingerprinting HS

- HS circuits are not shared
  - Different `.onion` use different circuits
  - RP circuits and general circuits are disjoint
- Size of the world is significantly smaller
  - Only 30,000 unique `.onion` address
  - Even smaller number of popular HS

Website Fingerprinting HS

- HS circuits are not shared
  - Different `.onion` use different circuits
  - RP circuits and general circuits are disjoint
- Size of the world is significantly smaller
  - Only 30,000 unique `.onion` address
  - Even smaller number of popular HS
- HS pages are not rapidly changing

Similarity	1 week	2 weeks	3 weeks	8 weeks
Q1	1	0.997	0.994	0.980
Median	1	1	1	1
Q3	1	1	1	1
Mean	0.96	0.97	0.96	0.927

WF Experiments

- 50 “sensitive” and 950 “non-sensitive” hidden services

WF Experiments

- 50 “sensitive” and 950 “non-sensitive” hidden services
- Training set
  - 50 instances of 50 sensitive hidden services
  - 1 instance of 100 to 950 non-sensitive hidden services

WF Experiments

- 50 “sensitive” and 950 “non-sensitive” hidden services
- Training set
  - 50 instances of 50 sensitive hidden services
  - 1 instance of 100 to 950 non-sensitive hidden services
- Clients/servers visit/serve one of the 1000 pages
  - Classify into one of the sensitives or non-sensitive

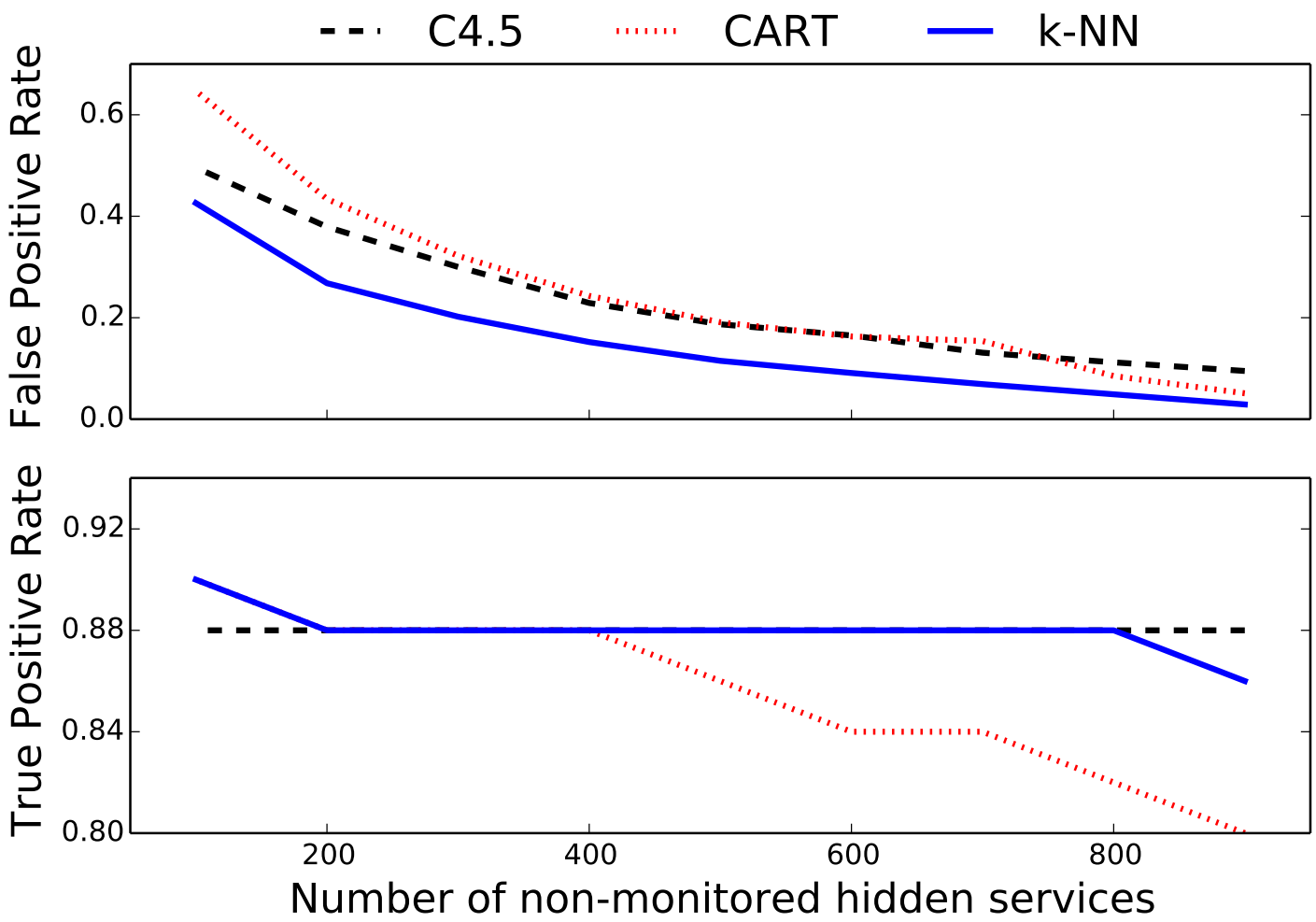
WF Experiments

- 50 “sensitive” and 950 “non-sensitive” hidden services
- Training set
  - 50 instances of 50 sensitive hidden services
  - 1 instance of 100 to 950 non-sensitive hidden services
- Clients/servers visit/serve one of the 1000 pages
  - Classify into one of the sensitives or non-sensitive
  - Our own HS serving cached pages

WF Experiments

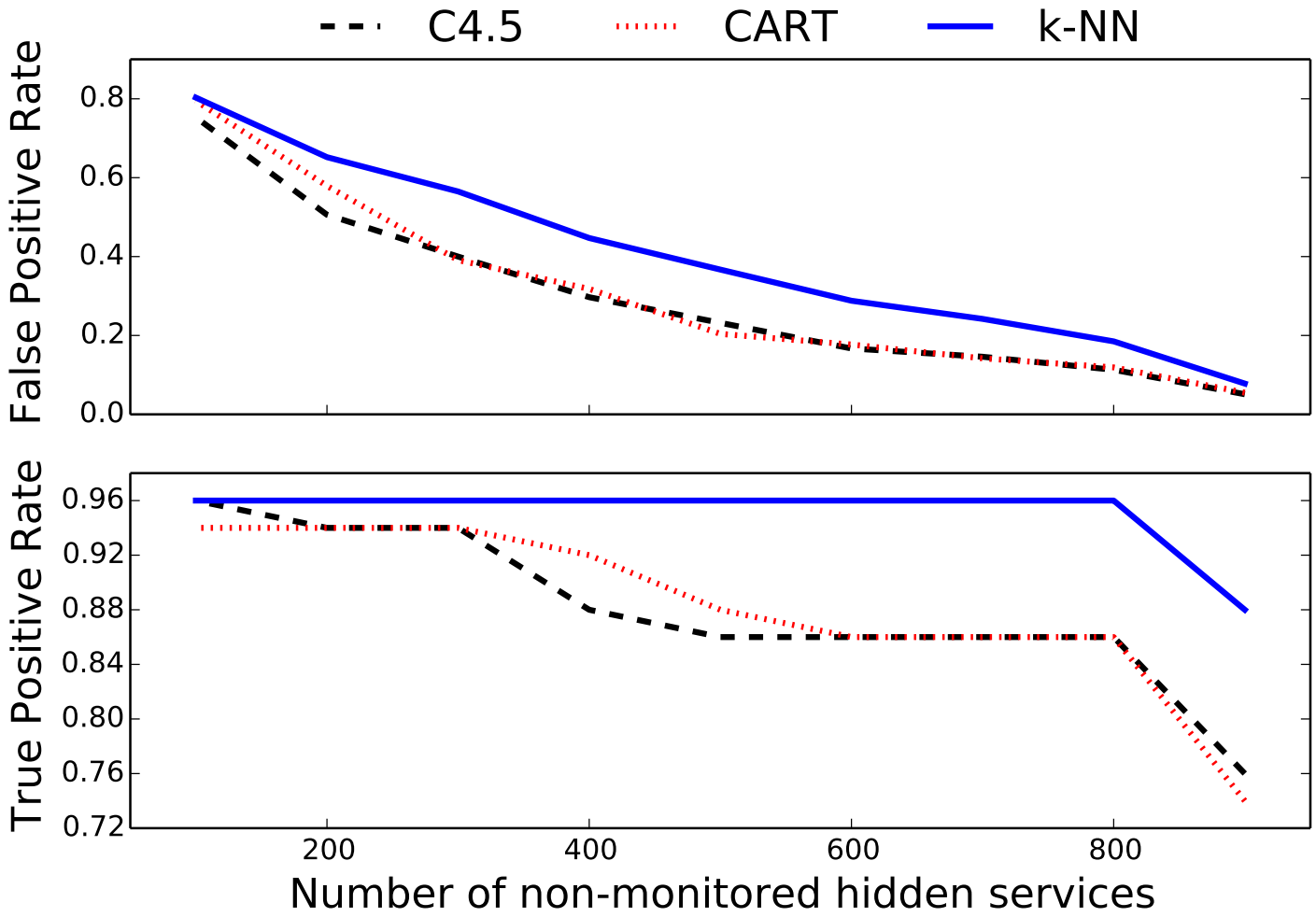
- 50 “sensitive” and 950 “non-sensitive” hidden services
- Training set
  - 50 instances of 50 sensitive hidden services
  - 1 instance of 100 to 950 non-sensitive hidden services
- Clients/servers visit/serve one of the 1000 pages
  - Classify into one of the sensitives or non-sensitive
  - Our own HS serving cached pages
- Tree-based and k-NN classifier

WF Accuracy



Client accuracy

WF Accuracy



Server accuracy

Outline

1 Backgound

2 Observations

3 Circuit Fingerprinting Attack

4 Website Fingerprinting Hidden Services

5 Conclusion

Potential Defenses

- Circuit classification defense
  - Obfuscate the features
- Website Fingerprinting
  - Multiplex the RP circuits
  - Previous work on defending WF attacks†

† Wang et al., Effective Attacks and Provable Defenses for Website Fingerprinting, USENIX Security 2014.

Conclusion

- Hidden service connections are fingerprintable
- Website fingerprinting is more realistic in the domain of HS
- Demonstrated effectiveness of the proposed attacks
- Data available at http://people.csail.mit.edu/kwonal/hswf.tar.gz

Thank you!