Privacy Preserving Detection of Path Bias Attacks in The Onion Router

A tour in Tor

Lauren Watson Anupam Mediratta Tariq Elahi Rik Sarkar

November 26, 2021

Table of Contents

- Introduction
- TOR Components
- How TOR Works?
- Hidden Server
- Path Bias Attacks and their Detection
- Conclusion
- References

Introduction

THE TOR NETWORK

- Open Source Network run by Volunteers

Introduction

THE TOR NETWORK

- Open Source Network run by Volunteers
- Designed for Anonymity and Privacy(Surveillance threats)

Introduction

THE TOR NETWORK

- Open Source Network run by Volunteers
- Designed for Anonymity and Privacy(Surveillance threats)
- Low-latency

Introduction

THE TOR NETWORK

- Open Source Network run by Volunteers
- Designed for Anonymity and Privacy(Surveillance threats)
- Low-latency
- Layered Encryption

Introduction

THE TOR NETWORK

- Open Source Network run by Volunteers
- Designed for Anonymity and Privacy(Surveillance threats)
- Low-latency
- Layered Encryption
- Anonymous Web hosting-Conceal Ip address of host server

Introduction

THE TOR NETWORK

- Open Source Network run by Volunteers
- Designed for Anonymity and Privacy(Surveillance threats)
- Low-latency
- Layered Encryption
- Anonymous Web hosting-Conceal Ip address of host server
- Mitigates Dos attacks

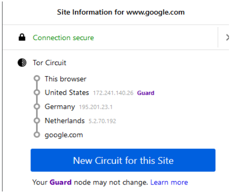
Introduction

THE TOR NETWORK

- Open Source Network run by Volunteers
- Designed for Anonymity and Privacy(Surveillance threats)
- Low-latency
- Layered Encryption
- Anonymous Web hosting-Conceal Ip address of host server
- Mitigates Dos attacks
- Uses stream ciphers

Components of TOR

- Guard Node aka Entry Relay/Bridge
- Middle Node
- Exit Relay
- Directory Server
- Hidden Server
- Rendezvous Point



Site Information for www.google.com

Connection secure

Tor Circuit

This browser

United States 172.241.140.26 Guard

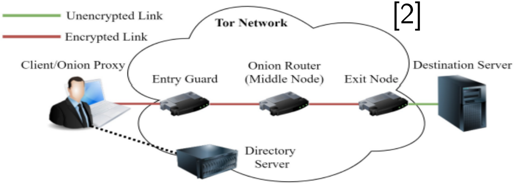
Germany 195.201.23.1

Netherlands 5.2.70.192

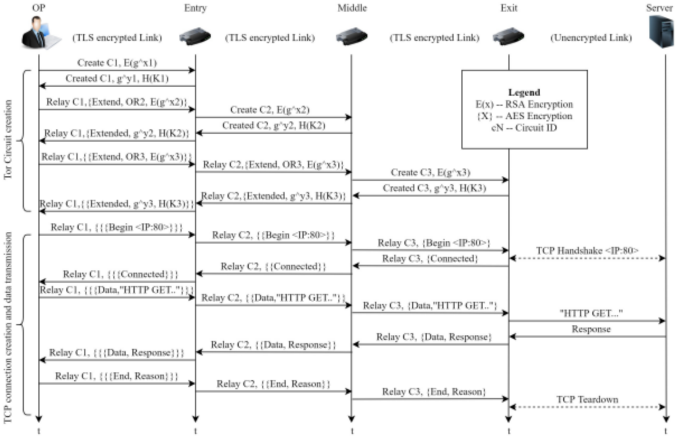
google.com

Your Guard node may not change. Learn more

[2]



How TOR Works


OP
Entry
Middle
Exit
Server
(TLS encrypted Link)
(TLS encrypted Link)
(TLS encrypted Link)
(Unencrypted Link)
Tor Circuit creation
TCP connection creation and data transmission
Create C1, E(g^x1)
Created C1, g^y1, H(K1)
Relay C1,{Extend, OR2, E(g^x2)}
Create C2, E(g^x2)
Created C2, g^y2, H(K2)
Relay C1,{Extended, g^y2, H(K2)}
Relay C1,{{Extend, OR3, E(g^x3)}}
Relay C2,{Extend, OR3, E(g^x3)}
Create C3, E(g^x3)
Created C3, g^y3, H(K3)
Relay C2,{Extended, g^y3, H(K3)}
Relay C1,{{Extended, g^y3, H(K3)}}
Legend
E(x) -- RSA Encryption
{X} -- AES Encryption
cN -- Circuit ID
Relay C1, {{{Begin <IP:80>}}}
Relay C2, {{Begin <IP:80>}}
Relay C3, {Begin <IP:80>}
TCP Handshake <IP:80>
Relay C3, {Connected}
Relay C2, {{Connected}}
Relay C1, {{{Connected}}}
Relay C1, {{{Data,"HTTP GET.."}}}
Relay C2, {{Data,"HTTP GET.."}}
Relay C3, {Data,"HTTP GET.."}
"HTTP GET..."
Response
Relay C3, {Data, Response}
Relay C2, {{Data, Response}}
Relay C1, {{{Data, Response}}}
Relay C1, {{{End, Reason}}}
Relay C2, {{End, Reason}}
Relay C3, {End, Reason}
TCP Teardown
t
t
t
t
t

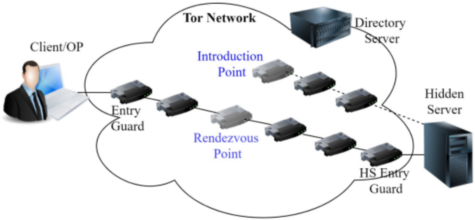
[2]

Client → $Entry : E_{PK_{Entry}}(g^x)$

Entry → $Client : g^y, H(K = g^{xy})$

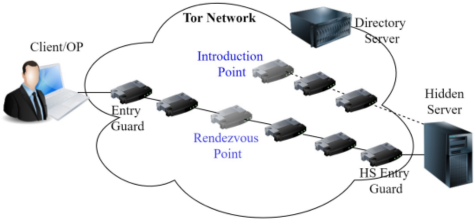
$E_{K_{Entry}}(E_{K_{Middle}}(E_{K_{Exit}}(M)))$

Hidden Server(.onion)



[2]

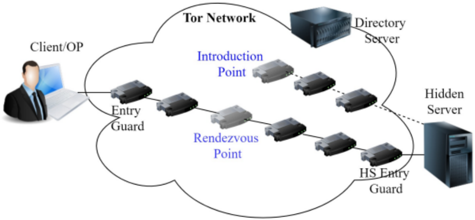
Hidden Server(.onion)



[2]

- Web Server picks random Introduction points

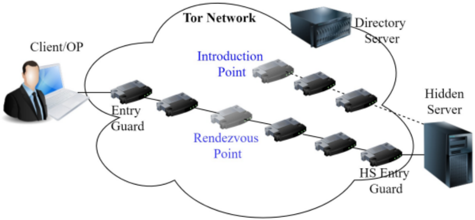
Hidden Server(.onion)



[2]

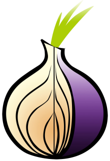
- Web Server picks random Introduction points
- Advertises Introduction points in HSDir

Hidden Server(.onion)

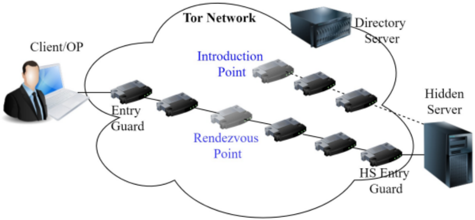


[2]

- Web Server picks random Introduction points
- Advertises Introduction points in HSDir
- Client Connects to Rendezvous point



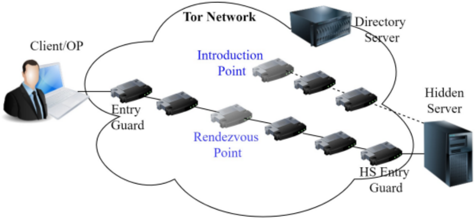
Hidden Server(.onion)



[2]

- Web Server picks random Introduction points
- Advertises Introduction points in HSDir
- Client Connects to Rendezvous point
- Client sends RP cookie to server introduction point

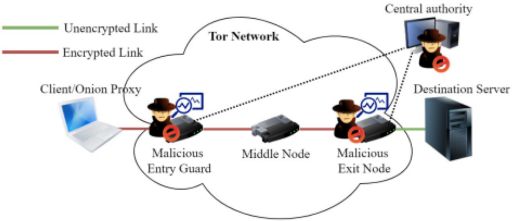
Hidden Server(.onion)



[2]

- Web Server picks random Introduction points
- Advertises Introduction points in HSDir
- Client Connects to Rendezvous point
- Client sends RP cookie to server introduction point
- Server connects to RP of client

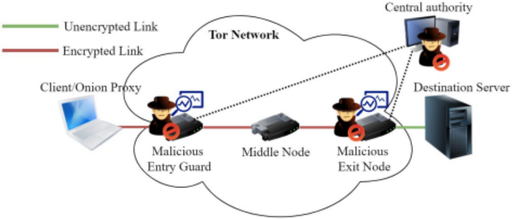
Path Bias Attacks



[2]

- Adversary to have access to both entry and exit ORs

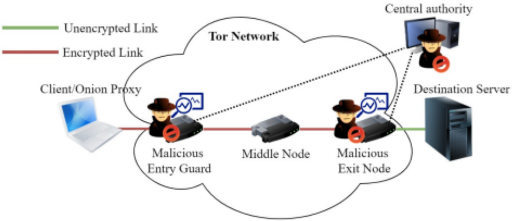
Path Bias Attacks



[2]

- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes

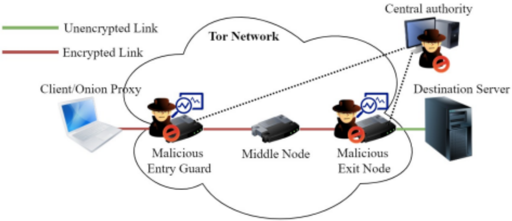
Path Bias Attacks



[2]

- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR

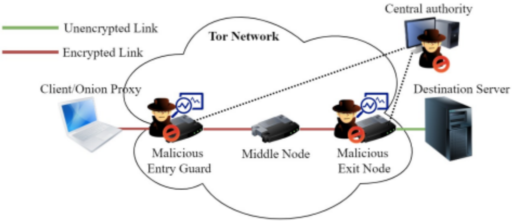
Path Bias Attacks



[2]

- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR
- Active Attacks

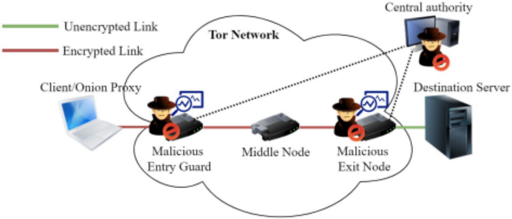
Path Bias Attacks



[2]

- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR
- Active Attacks
  Attacker denies service to circuits that cannot compromise

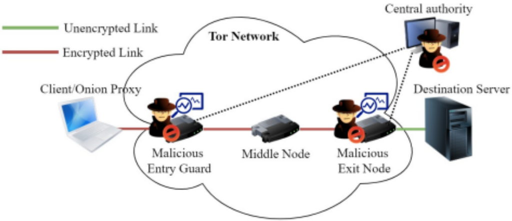
Path Bias Attacks



[2]

- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR
- Active Attacks
  Attacker denies service to circuits that cannot compromise
  Traffic Co-Relation

Path Bias Attacks



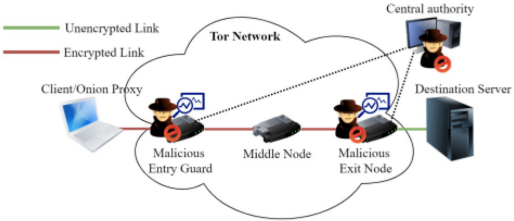
[2]

- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR
- Active Attacks

  Attacker denies service to circuits that cannot compromise

  Traffic Co-Relation
- Passive Attacks

Path Bias Attacks



[2]

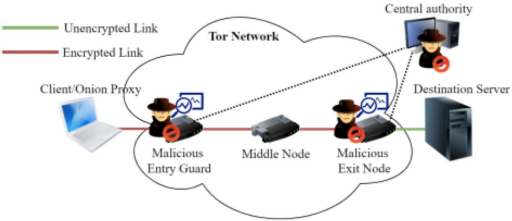
- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR
- Active Attacks

  Attacker denies service to circuits that cannot compromise

  Traffic Co-Relation
- Passive Attacks

  Traffic Pattern Analysis

Path Bias Attacks



[2]

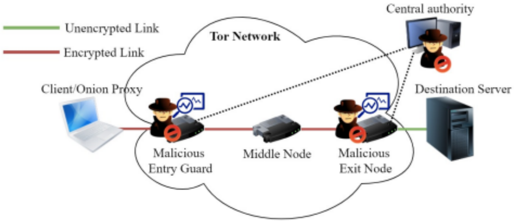
- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR
- Active Attacks

  Attacker denies service to circuits that cannot compromise

  Traffic Co-Relation
- Passive Attacks

  Traffic Pattern Analysis
  - Timing Attacks:Inter packet Arrival time,Packet rate,latency

Path Bias Attacks



[2]

- Adversary to have access to both entry and exit ORs
  - Compromising Existing Tor nodes
  - Introducing new Attacker controlled nodes into TOR
- Active Attacks

  Attacker denies service to circuits that cannot compromise

  Traffic Co-Relation
- Passive Attacks

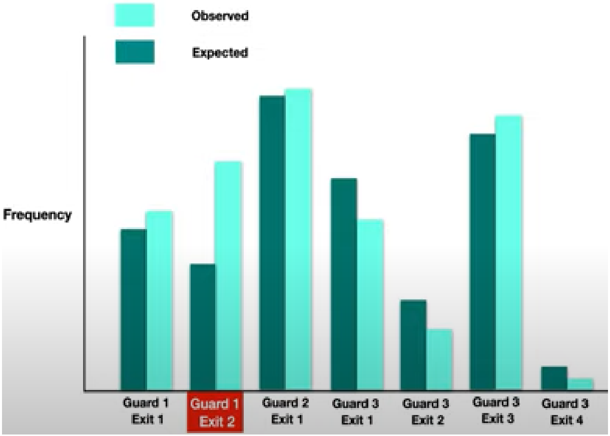
  Traffic Pattern Analysis
  - Timing Attacks:Inter packet Arrival time,Packet rate,latency
  - Water Marking attacks

Path Bias Detection scheme

- Adversary repeats rejection of circuits if nodes are not compromised

Path Bias Detection scheme

- Adversary repeats rejection of circuits if nodes are not compromised
- Mark a node as Malicious if $n_{gx} > E_{gx}$



[4]

Path Bias Detection scheme

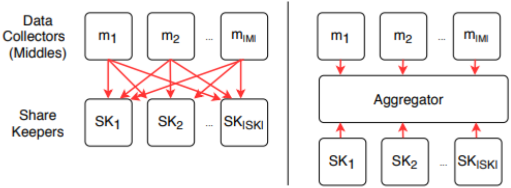
- Adversary repeats rejection of circuits if nodes are not compromised
- Mark a node as Malicious if $n_{gx} > E_{gx}$
- Bandwidth determines prob of a node, $E_{gx} = n(\frac{BW_g}{BW_G})(\frac{BW_x}{BW_X})$ [3]

Path Bias Detection scheme

- Adversary repeats rejection of circuits if nodes are not compromised
- Mark a node as Malicious if $n_{gx} > E_{gx}$
- Bandwidth determines prob of a node, $E_{gx} = n(\frac{BW_g}{BW_G})(\frac{BW_x}{BW_X})$ [3]
- Middle Relays to calculate n_{gx}=C

Path Bias Detection scheme

- Adversary repeats rejection of circuits if nodes are not compromised
- Mark a node as Malicious if $n_{gx} > E_{gx}$
- Bandwidth determines prob of a node, $E_{gx} = n(\frac{BW_g}{BW_G})(\frac{BW_x}{BW_X})$ [3]
- Middle Relays to calculate n_{gx}=C
- Uses additive secret sharing to intialize secret shares $x_1, x_2, \ldots ,x_k$
- Middle guard shares $C - (x_1 + x_2 + \ldots +x_k)$ to Aggregator

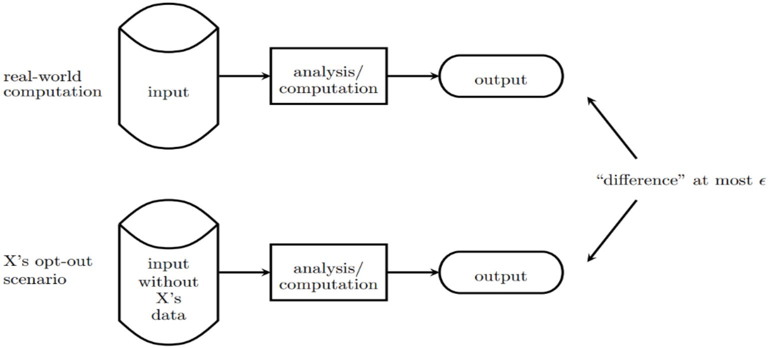


[3]

Differential Privacy

A Randomized algorithm K operating on the database satisfies ϵ-differential privacy if given any two neighbouring databases D and D' and a set of outputs S $\subseteq$ Range(K)

$$P[K(D) \in S] \leq e^{\epsilon}(P[K(D') \in S] \tag{1}$$



[5]

Differential Privacy

A Randomized algorithm K operating on the database satisfies ϵ-differential privacy if given any two neighbouring databases D and D' and a set of outputs S $\subseteq$ Range(K)

$$P[K(D) \in S] \leq e^{\epsilon}(P[K(D') \in S] \tag{1}$$

- Monitoring Anonymity networks is challenging

Differential Privacy

A Randomized algorithm K operating on the database satisfies ϵ-differential privacy if given any two neighbouring databases D and D' and a set of outputs S $\subseteq$ Range(K)

$$P[K(D) \in S] \leq e^{\epsilon}(P[K(D') \in S] \tag{1}$$

- Monitoring Anonymity networks is challenging
- Prevent data/statistics published by aggregtor by adding noise γ

Differential Privacy

A Randomized algorithm K operating on the database satisfies ϵ-differential privacy if given any two neighbouring databases D and D' and a set of outputs S $\subseteq$ Range(K)

$$P[K(D) \in S] \leq e^{\epsilon}(P[K(D') \in S] \tag{1}$$

- Monitoring Anonymity networks is challenging
- Prevent data/statistics published by aggregtor by adding noise γ

Laplace Mechanism

Differential Privacy

A Randomized algorithm K operating on the database satisfies ϵ-differential privacy if given any two neighbouring databases D and D' and a set of outputs S $\subseteq$ Range(K)

$$P[K(D) \in S] \leq e^{\epsilon}(P[K(D') \in S] \tag{1}$$

- Monitoring Anonymity networks is challenging
- Prevent data/statistics published by aggregtor by adding noise γ

Laplace Mechanism

Random number $\gamma \sim Lap(\frac{1}{\epsilon})$, mean 0,scale $\frac{1}{\epsilon}$

Differential Privacy

A Randomized algorithm K operating on the database satisfies ϵ-differential privacy if given any two neighbouring databases D and D' and a set of outputs S $\subseteq$ Range(K)

$$P[K(D) \in S] \leq e^{\epsilon}(P[K(D') \in S] \tag{1}$$

- Monitoring Anonymity networks is challenging
- Prevent data/statistics published by aggregtor by adding noise γ

Laplace Mechanism

Random number $\gamma \sim Lap(\frac{1}{\epsilon})$, mean 0,scale $\frac{1}{\epsilon}$

Count C(by middle relay) $\Rightarrow C + \gamma$

Enhanced Detection Algorithm

- Low probability exits will have very small count, $\gamma >> C$

Enhanced Detection Algorithm

- Low probability exits will have very small count,$\gamma >> C$
- Grouping multiple exit relays into bins

Enhanced Detection Algorithm

- Low probability exits will have very small count,$\gamma >> C$
- Grouping multiple exit relays into bins
- Binning achieved by processing exits in decreasing order of bandwidth

Enhanced Detection Algorithm

- Low probability exits will have very small count,$\gamma >> C$
- Grouping multiple exit relays into bins
- Binning achieved by processing exits in decreasing order of bandwidth
- Middle relays report count(C) for bins instead of individual exits

Enhanced Detection Algorithm

- Low probability exits will have very small count,$\gamma >> C$
- Grouping multiple exit relays into bins
- Binning achieved by processing exits in decreasing order of bandwidth
- Middle relays report count(C) for bins instead of individual exits
- Noise is added to a bin

Enhanced Detection Algorithm

- Low probability exits will have very small count,$\gamma >> C$
- Grouping multiple exit relays into bins
- Binning achieved by processing exits in decreasing order of bandwidth
- Middle relays report count(C) for bins instead of individual exits
- Noise is added to a bin
  $\forall x, y \in$ Bin B:

$$E_x \leq (1 + \gamma) E_y + \eta$$

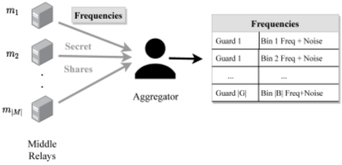
$$|B| \leq m$$

Enhanced Detection Algorithm

- Low probability exits will have very small count,$\gamma >> C$
- Grouping multiple exit relays into bins
- Binning achieved by processing exits in decreasing order of bandwidth
- Middle relays report count(C) for bins instead of individual exits
- Noise is added to a bin
  $\forall x, y \in$ Bin B:

$$E_x \leq (1+\gamma)E_y + \eta$$

$$|B| \leq m$$



Frequencies	
Guard 1	Bin 1 Freq + Noise
Guard 1	Bin 2 Freq + Noise
...	...
Guard |G|	Bin |B| Freq+Noise

[3]

Voting scheme

- If adversary compromises q middle relays??

Voting scheme

- If adversary compromises q middle relays??
  - Misreporting of guard-exit pairs

Voting scheme

- If adversary compromises q middle relays??
  - Misreporting of guard-exit pairs
- Run detection test on Middle relays and submit decision as vote

Voting scheme

- If adversary compromises q middle relays??
  - Misreporting of guard-exit pairs
- Run detection test on Middle relays and submit decision as vote
- Randomly selecting K Middle relays

Voting scheme

- If adversary compromises q middle relays??
    - Misreporting of guard-exit pairs
- Run detection test on Middle relays and submit decision as vote
- Randomly selecting K Middle relays
- Receive a binary vote for gx pair

Voting scheme

- If adversary compromises q middle relays??
  - Misreporting of guard-exit pairs
- Run detection test on Middle relays and submit decision as vote
- Randomly selecting K Middle relays
- Receive a binary vote for gx pair
- If total no of votes exceeds threshold , outlier pair

Voting scheme

- If adversary compromises q middle relays??
  - Misreporting of guard-exit pairs
- Run detection test on Middle relays and submit decision as vote
- Randomly selecting K Middle relays
- Receive a binary vote for gx pair
- If total no of votes exceeds threshold , outlier pair
- Reduce influence of misreporting relays

Voting scheme

- If adversary compromises q middle relays??
  - Misreporting of guard-exit pairs
- Run detection test on Middle relays and submit decision as vote
- Randomly selecting K Middle relays
- Receive a binary vote for gx pair
- If total no of votes exceeds threshold , outlier pair
- Reduce influence of misreporting relays
- High probability for detection of an outlier pair

Conclusion

Conclusion

- Working of TOR

Conclusion

- Working of TOR
- Path Bias attacks and Detection

Conclusion

- Working of TOR
- Path Bias attacks and Detection
- Differential privacy for individual user

Conclusion

- Working of TOR
- Path Bias attacks and Detection
- Differential privacy for individual user
- Enhanced Detection algorithm for low bandwidth

Conclusion

- Working of TOR
- Path Bias attacks and Detection
- Differential privacy for individual user
- Enhanced Detection algorithm for low bandwidth
- Voting scheme for misreporting

References

- Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith, *Calibrating noise to sensitivity in private data analysis*,2006.

- Ishan Karunanayake, Nadeem Ahmed, Robert Malaney, Rafiqul Islam and Sanjay Jha *Anonymity with Tor: A Survey on Tor Attacks*,2020.

- Lauren Watson*, Anupam Mediratta, Tariq Elahi, and Rik Sarkar *Privacy Preserving Detection of Path Bias Attacks in Tor* ,2020.

- Privacy Preserving Detection of Path Bias Attacks in Anonymity Networks. `https://www.youtube.com/watch?v=zfT16ZIMMMk`

- Kobbi Nissim, et al *Differential Privacy: A Primer for a Non-technical Audience.*, 2018.

Thank You!