RUB

RUHR-UNIVERSITÄT BOCHUM

DIGESTOR

Comparing Passive Traffic Analysis Attacks on Tor

Katharina Kohls
Ruhr-University Bochum

Christina Pöpper
NYU Abu Dhabi

NYU

hgi
Horst Görtz Institut
für IT-Sicherheit

Phileas Fogg:
Bet he could travel the world in 80 days

Detective Fix:
Assumes Fogg robbed a bank
and tries to catch him

The Fogg-Dilemma

Book a balloon flight via Internet.

Don't reveal any details to Detective Fix!

Phileas Fogg

Onion Routing
around the world in 80 days

Outline

Context: Traffic Analysis Attacks on Tor

Motivation: Diversity in Related Work

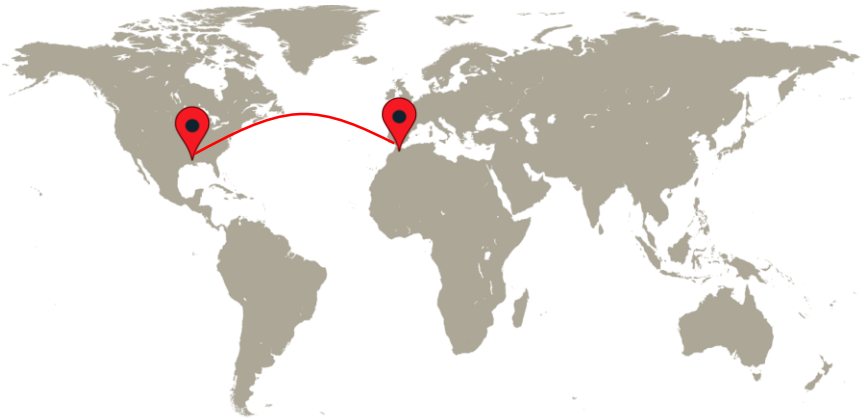
DigesTor: Achieving Comparability

Traffic Analysis Attacks on Tor

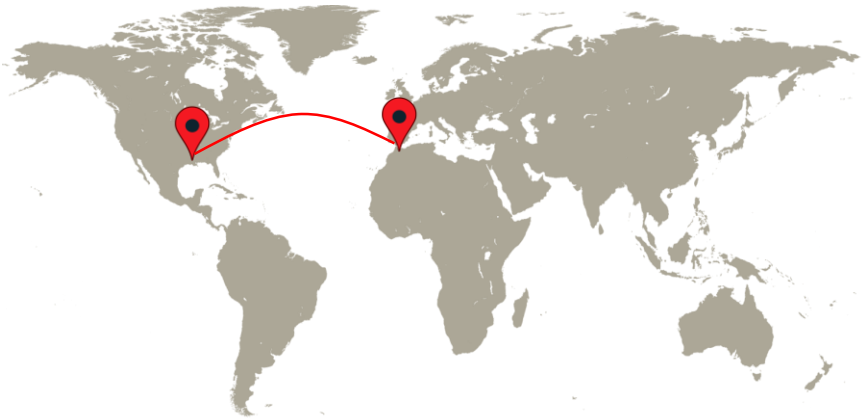
De-Anonymizing users from encrypted traffic

Flight Plan

Mondays and Thursdays: Departure at **sunrise**

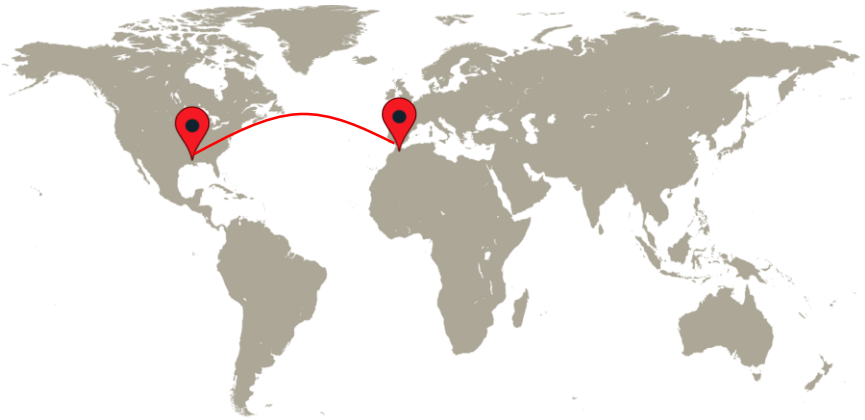


Fix knows:
Fogg will leave next Monday

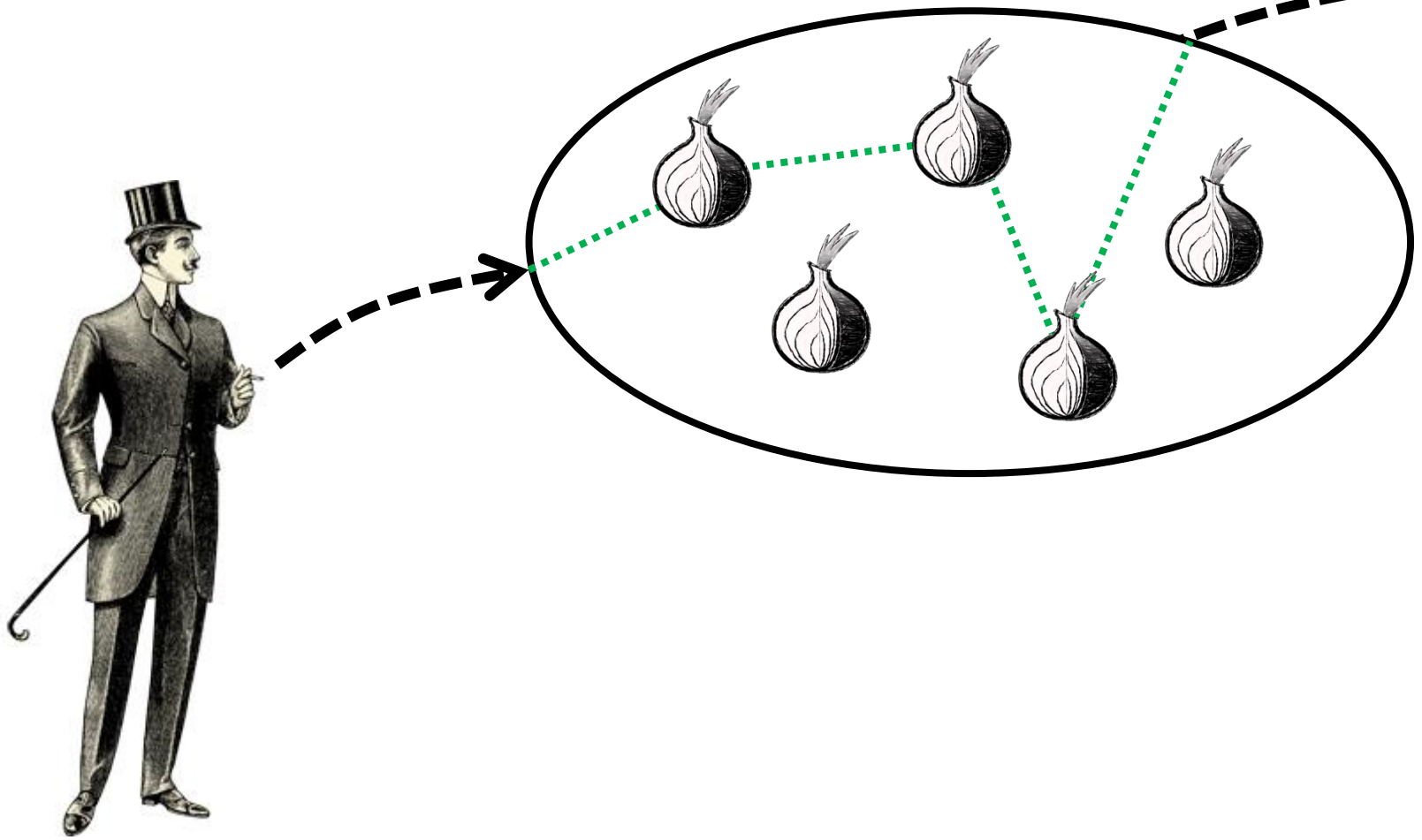


Anonymity

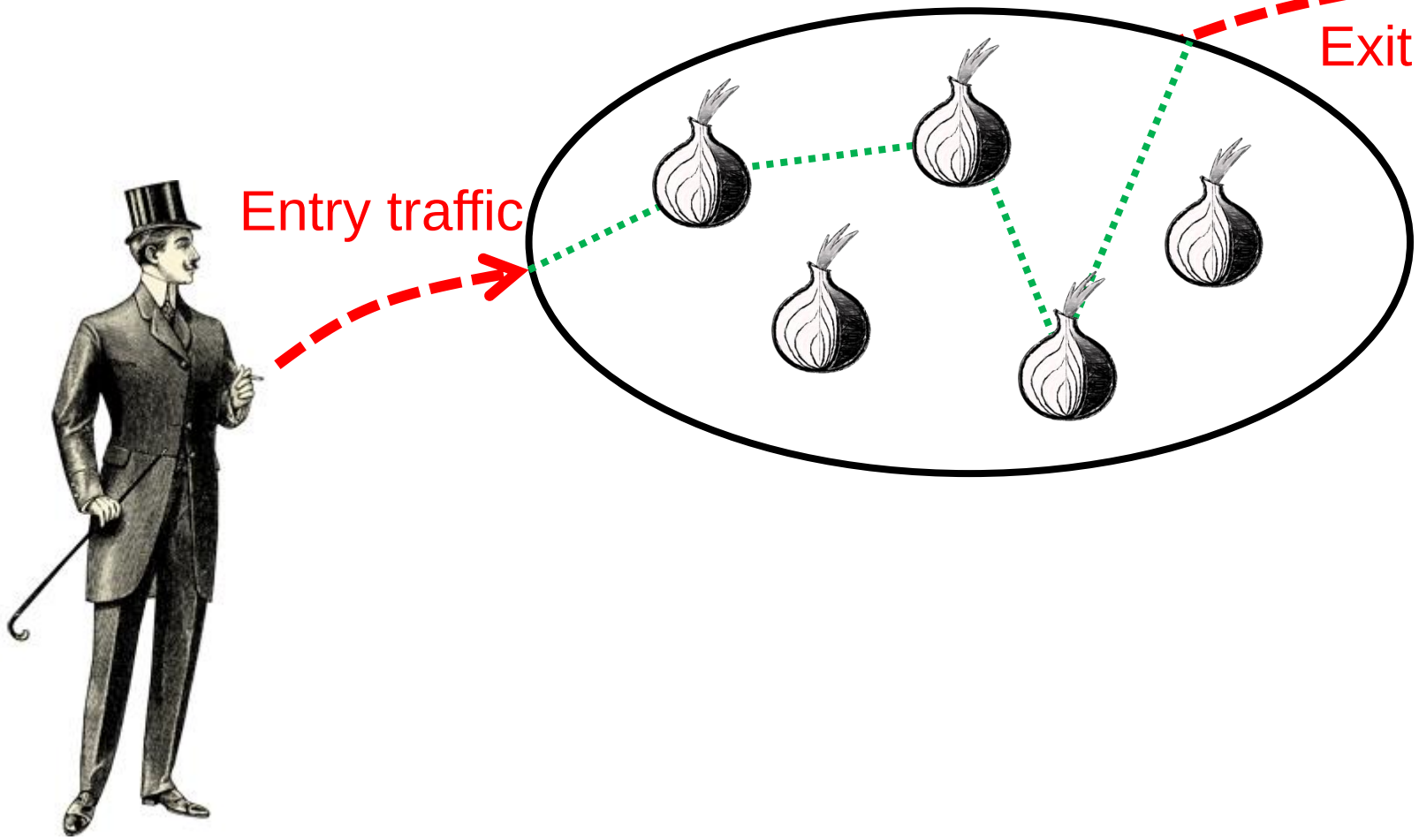
Separate **identity** from **content**



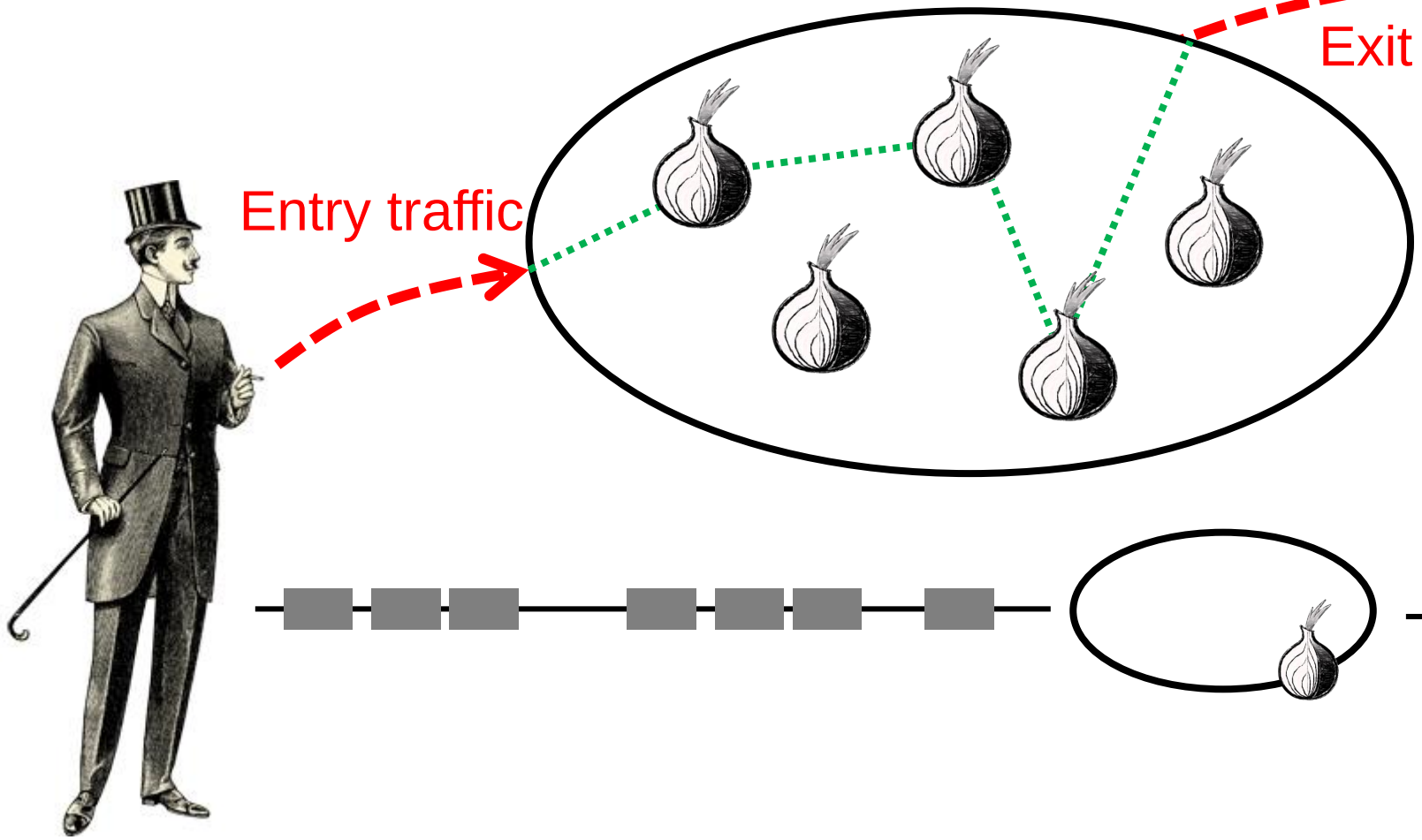
Tor: Anonymous Connections



Traffic Analysis



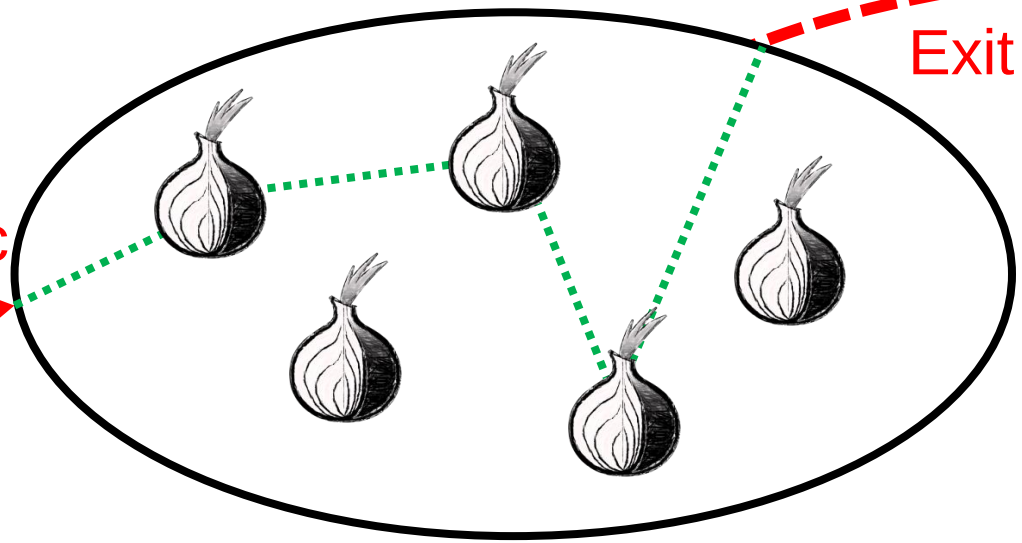
End-to-End Confirmation



Attack: Correlation

Entry traffic

Exit traffic



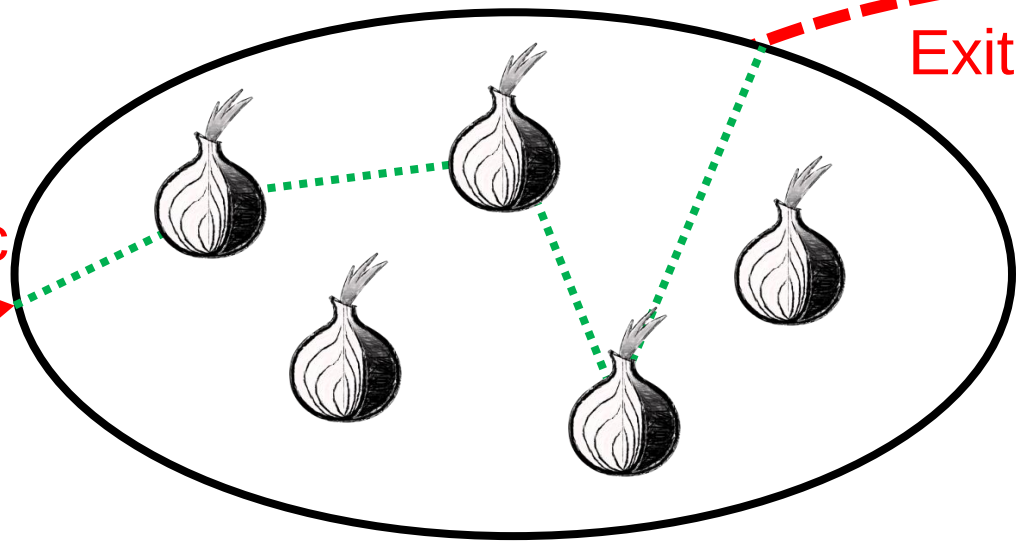
Entry traffic

Exit traffic

Countermeasure: Obfuscation

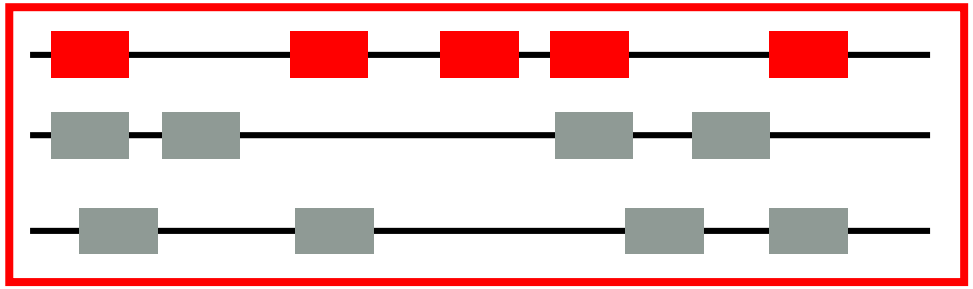
Entry traffic

Exit traffic



Entry traffic

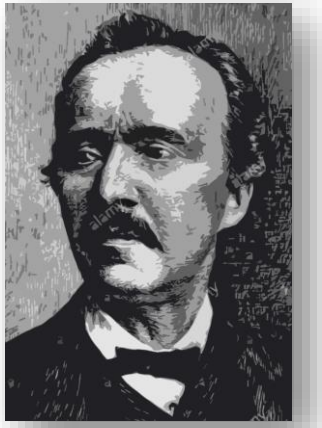
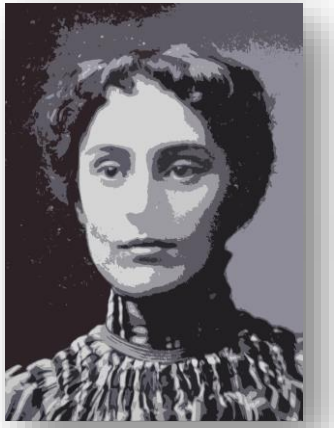
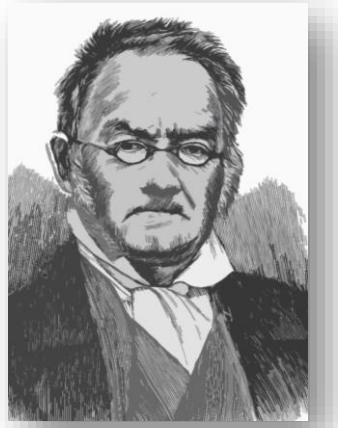
Exit traffic



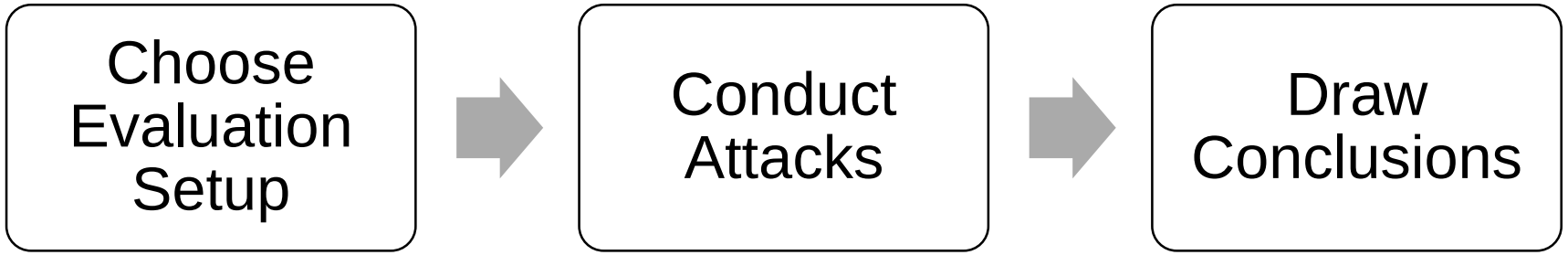
Diversity in Evaluation Techniques

Comparing Apples and Oranges

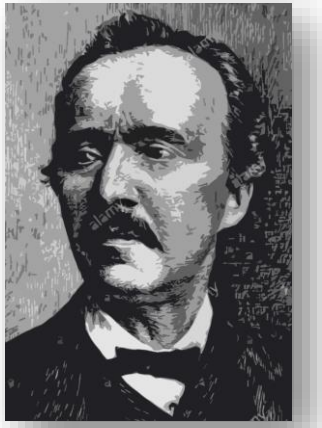
Evaluation Procedure

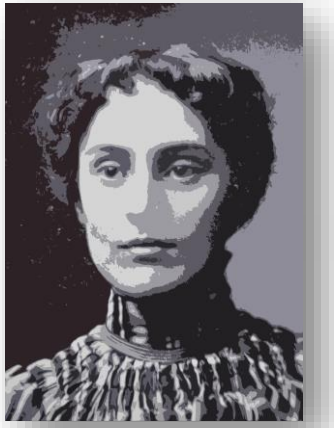
Research on Traffic Analysis Attacks



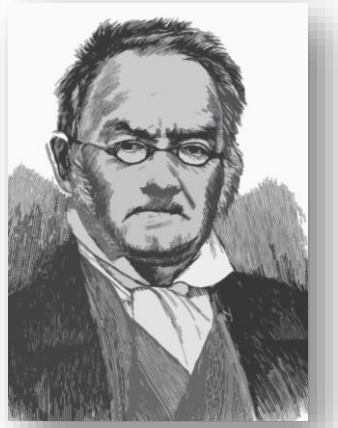
Example: Different Setups



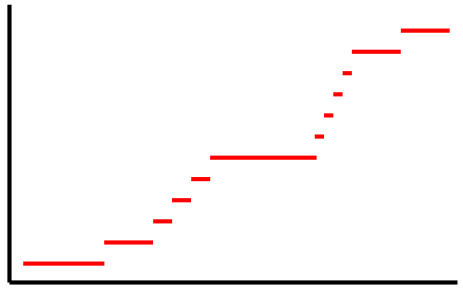
Statistical Model

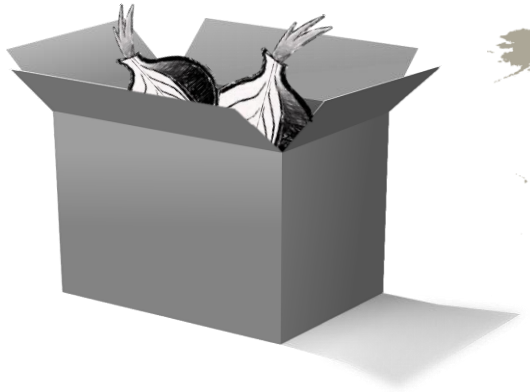


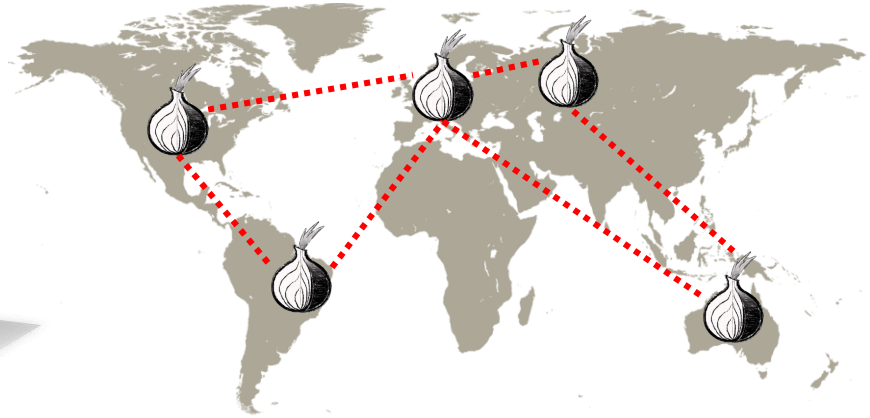
Simulation Model



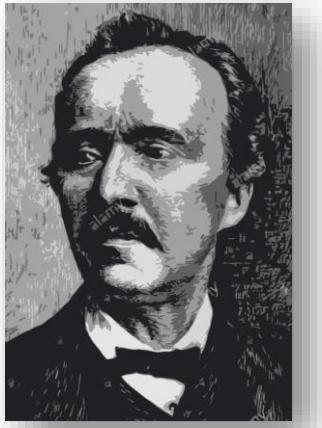
Live Network



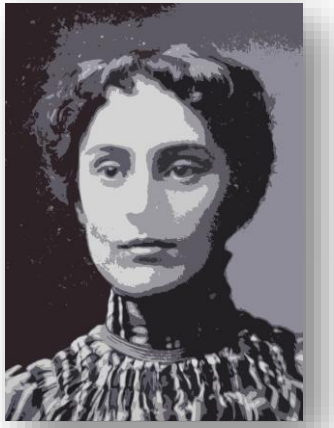




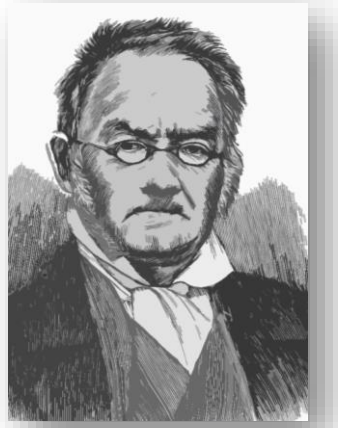
Example: Different Setups



Statistical Model



Simulation Model

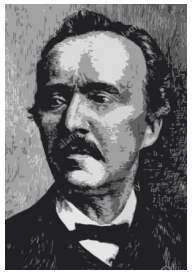


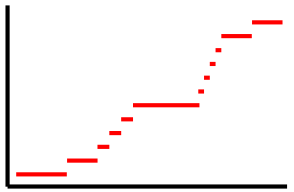
Live Network

Related Work Comparison

Attack	Ref.	A/P	Adv.	Setup	Noise	App.	Feature	Metric
Flow Comp.	[1,2]	○	●	◑	◑	○	iat	Corr.
	[3,4]	○	●	◑	◑	○	iat	MI
IXP	[5]	○	◑	●	●	●	iat	Stat.
Disclosure	[6-9]	○	●	○	○	○	-	Stat.
WM	[10-13]	●	◑	●	●	●	iat	Corr.
Coding	[14-17]	●	◑	●	●	○	-	Enc.
Protocol	[18,19]	●	◑	●	●	○	-	Cell
n-1	[20-22]	●	●	○	○	○	-	Blend

Statistical Models





Attack	Ref.	A/P	Adv.	Setup	Noise	App.	Feature	Metric
Flow Comp.	[1,2]	○	●	◐	◐	○	iat	Corr.
	[3,4]	○	●	◐	◐	○	iat	MI
IXP	[5]	○	◐	●	●	●	iat	Stat.
Disclosure	[6-9]	○	●	○	○	○	-	Stat.
WM	[10-13]	●	◐	●	●	●	iat	Corr.
Coding	[14-17]	●	◐	●	●	○	-	Enc.
Protocol	[18,19]	●	◐	●	●	○	-	Cell
n-1	[20-22]	●	●	○	○	○	-	Blend

Simulation Models

Attack	Ref.	A/P	Adv.	Setup	Noise	App.	Feature	Metric
Flow Comp.	[1,2]	○	●	◑	◑	○	iat	Corr.
	[3,4]	○	●	◑	◑	○	iat	MI
IXP	[5]	○	◑	●	●	●	iat	Stat.
Disclosure	[6-9]	○	●	○	○	○	-	Stat.
WM	[10-13]	●	◑	●	●	●	iat	Corr.
Coding	[14-17]	●	◑	●	●	○	-	Enc.
Protocol	[18,19]	●	◑	●	●	○	-	Cell
n-1	[20-22]	●	●	○	○	○	-	Blend

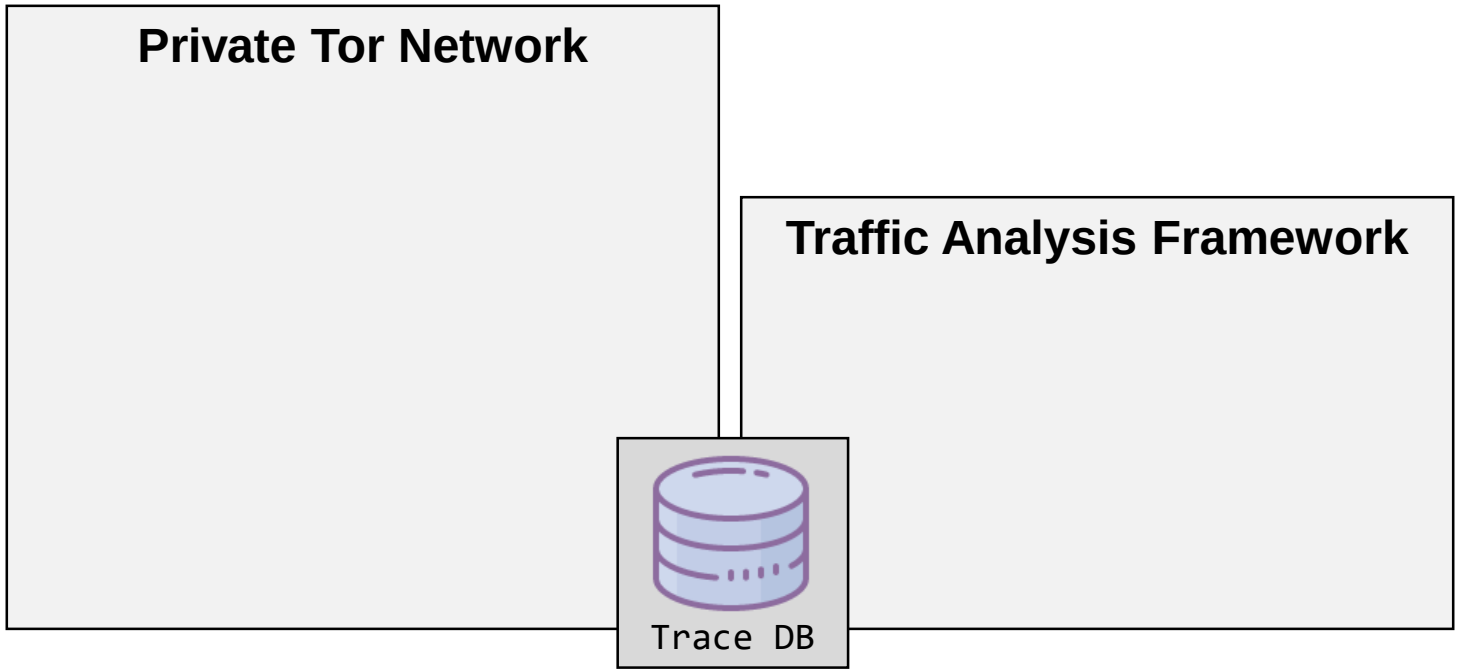
Comparison Framework

Attack	Ref.	A/P	Adv.	Setup	Noise	App.	Feature	Metric
Flow Comp.	[1,2]	○	●	◐	◐	○	iat	Corr.
	[3,4]	○	●	◐	◐	○	iat	MI
IXP	[5]	○	◐	●	●	●	iat	Stat.
Disclosure	[6-9]	○	●	○	○	○	-	Stat.
WM	[10-13]	●	◐	●	●	●	iat	Corr.
Coding	[14-17]	●	◐	●	●	○	-	Enc.
Protocol	[18,19]	●	◐	●	●	○	-	Cell
n-1	[20-22]	●	●	○	○	○	-	Blend
DigesTor	**[1-9]**	○	●	◐	●	●	**5 Feat.**	**5 Metrics**

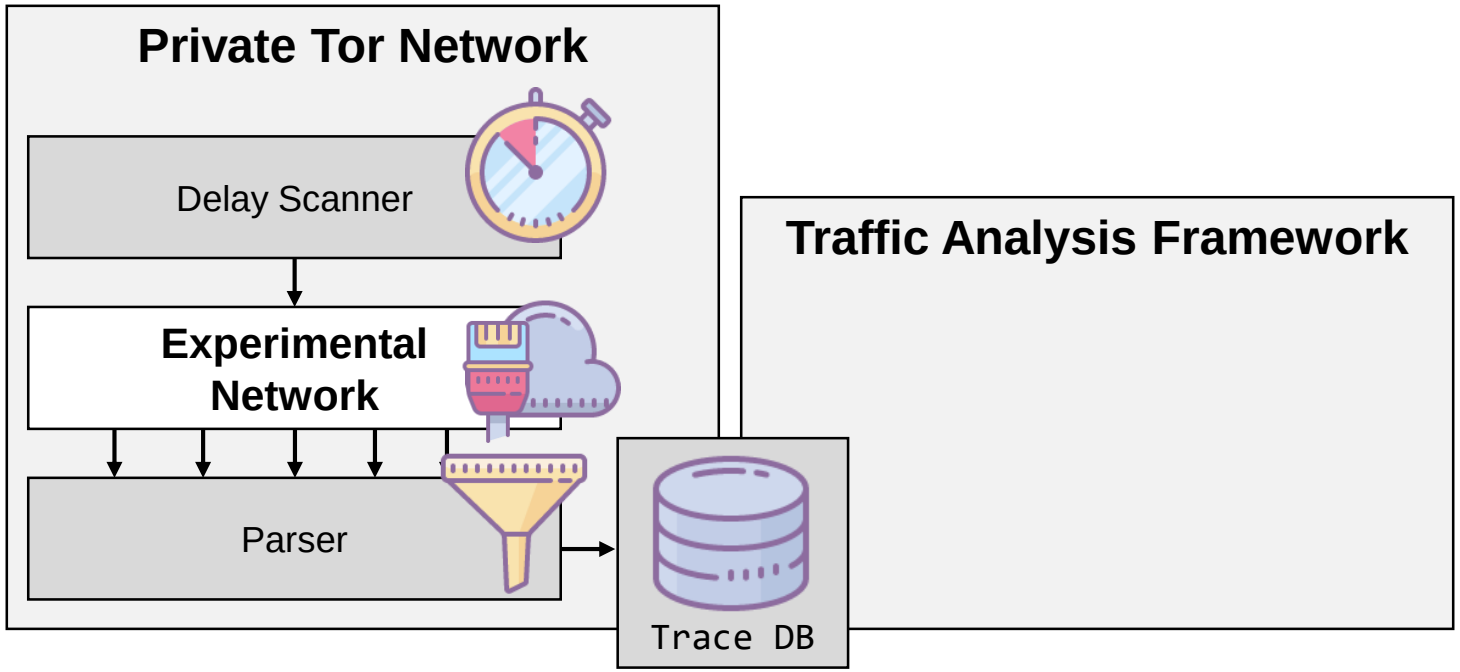
Comparing Passive Traffic Analysis Attacks on Tor

The Framework

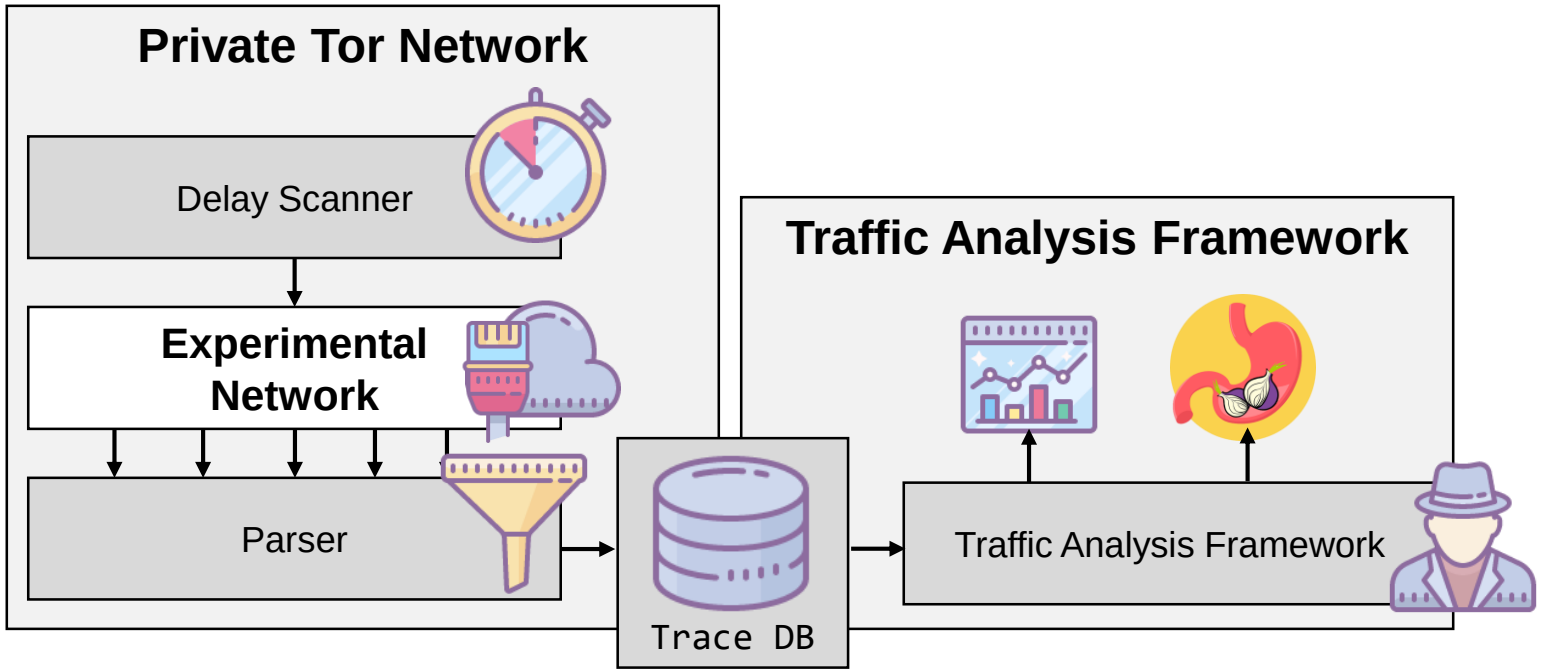
Private Tor Network and TA Framework



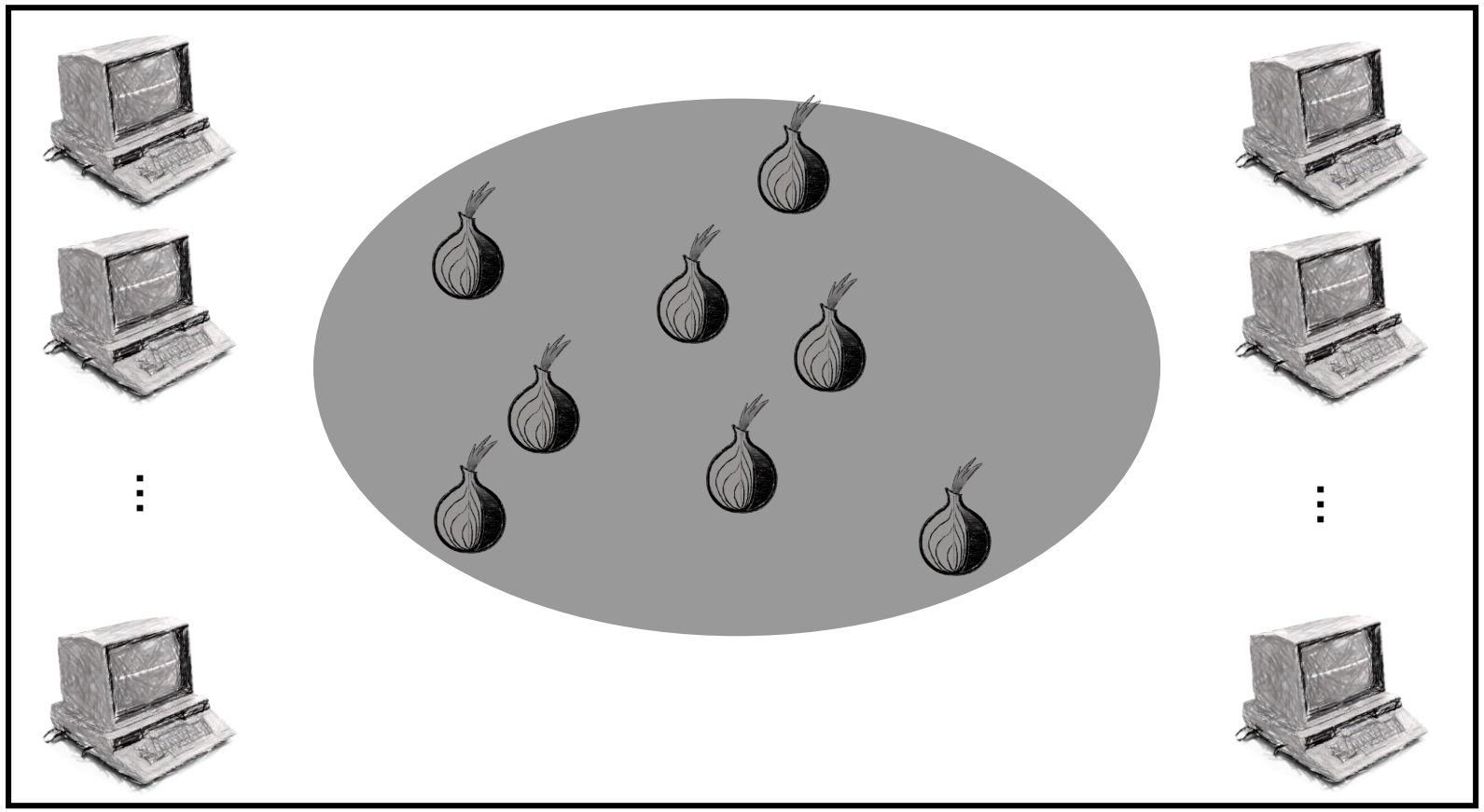
Empirical Parameters & Virtual Network



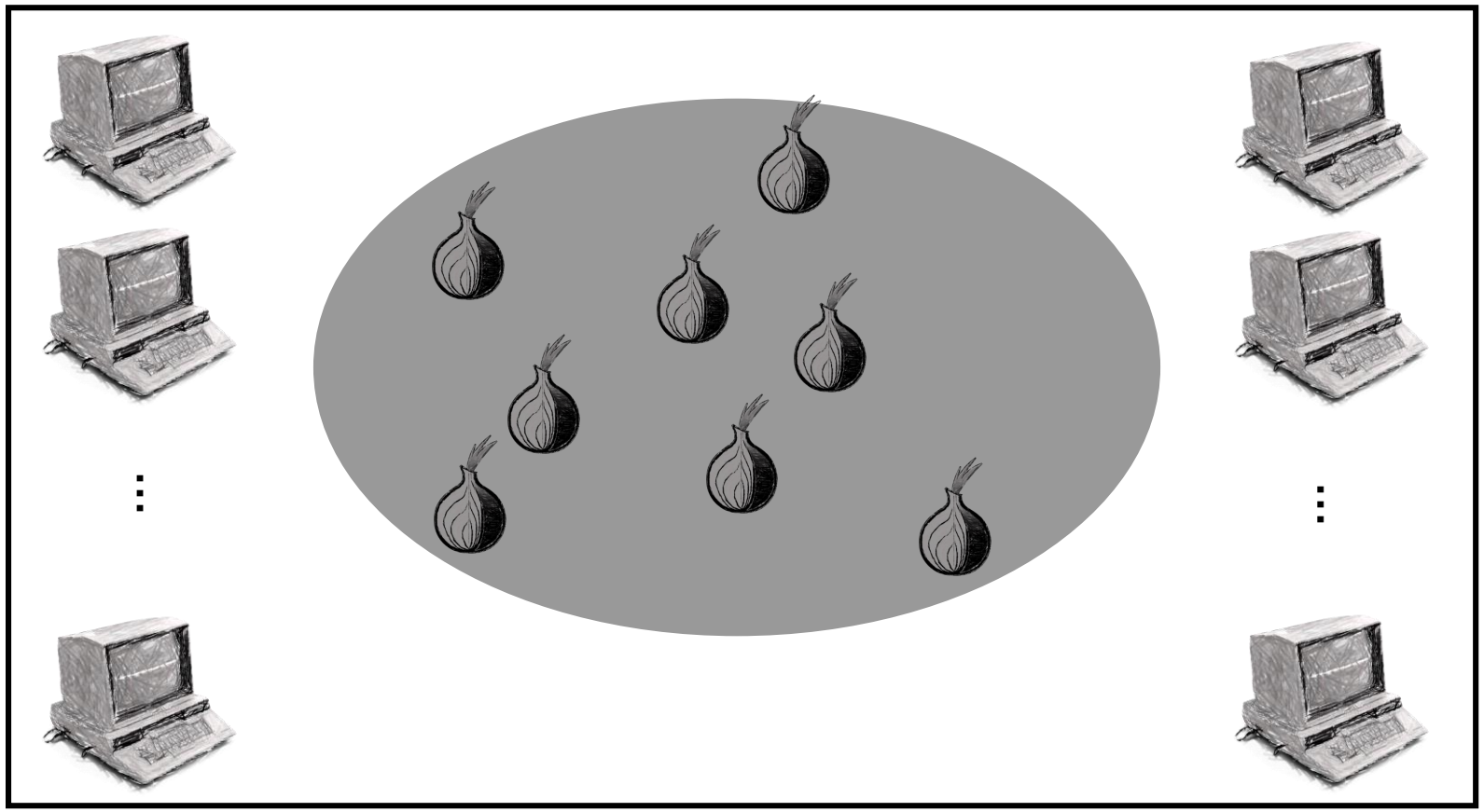
Traffic Analysis Attacks



Shadow Simulation Model



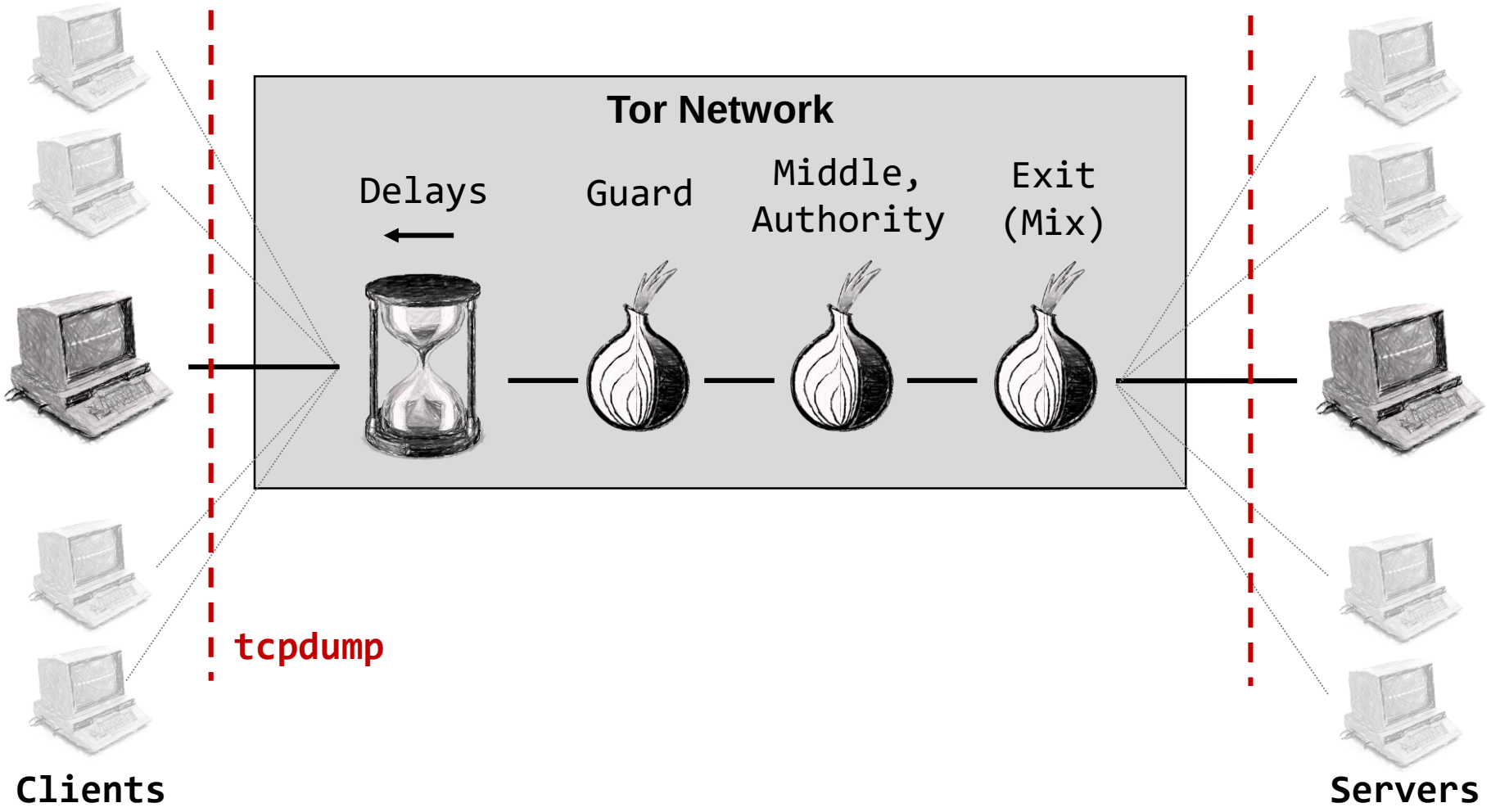
Limitations

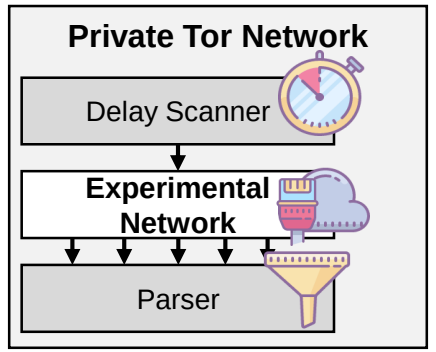


Pros
- Simulation Time
- Large-Scale Models
- Consensus
- …

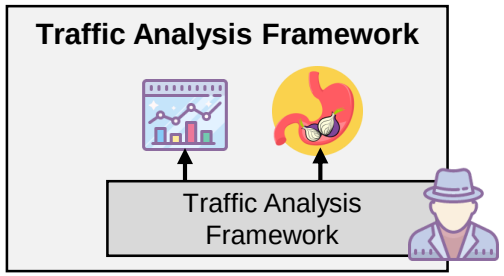
Cons
- No actual transmissions
- No **network stack**
- Traffic generation models
- …

Virtual Network Setup





TA Framework



- **Apply 5 comparison metrics**
  - Correlation between traces or
  - Error between traces
- **For 5 metadata features**

Metric/Feature	cnt	iat	len	ttl	wis
Scalar	X	X	X	X	X
PCA, Pearson	X	X	X	X	X
Pearson Correlation	X	X	X	X	X
RMSE	X	X	X	X	X
Mutual Information	X	X	X	X	X

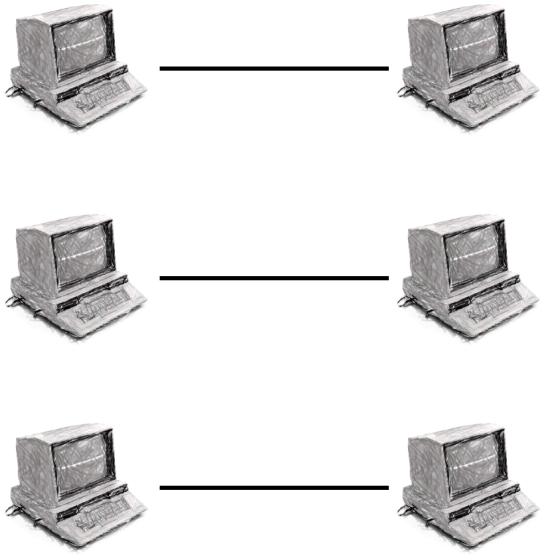
Experiments

Generate data, apply metrics, compare results

Scenarios: Network Topologies

Directed setup:

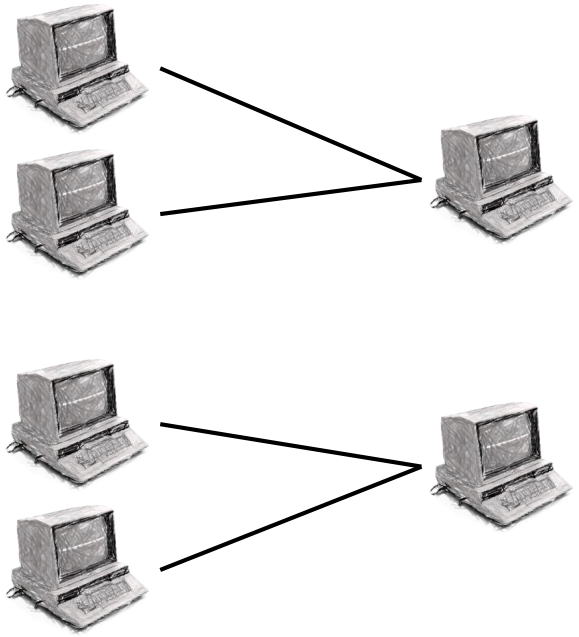
- $n = [2, \dots, 30]$ clients connect to
- $n = [2, \dots, 30]$ servers



Isolated Connections

Grouped setup:

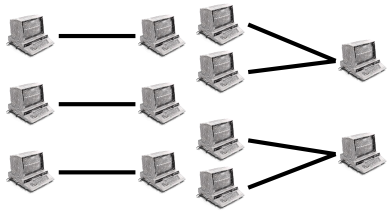
- $n = [2, \dots, 30]$ clients connect to
- 2 servers



Concurrent Connections

Scenarios: Applications

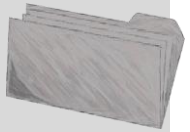
- **Network Topologies:** Directed, Grouped

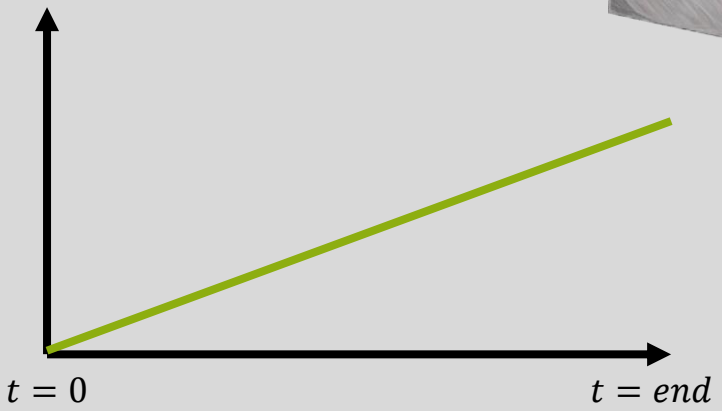


- **Applications**

Static

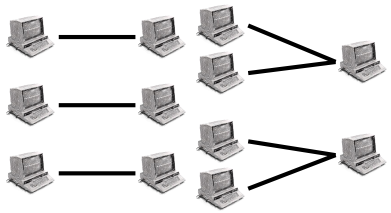
cURL request to server for constant download





Scenarios: Applications

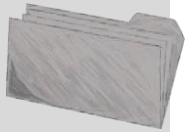
- **Network Topologies:** Directed, Grouped

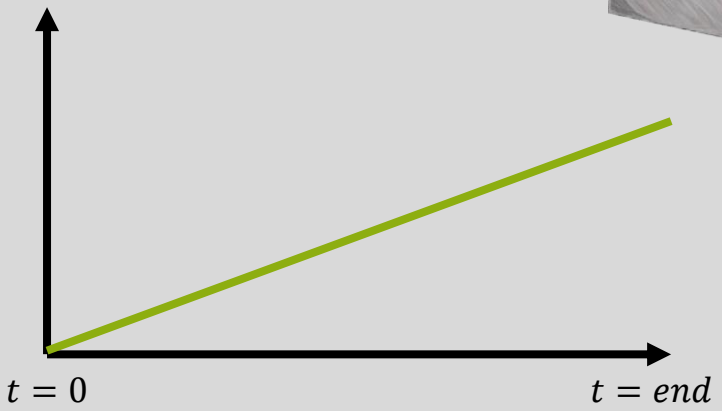


- **Applications**

Static

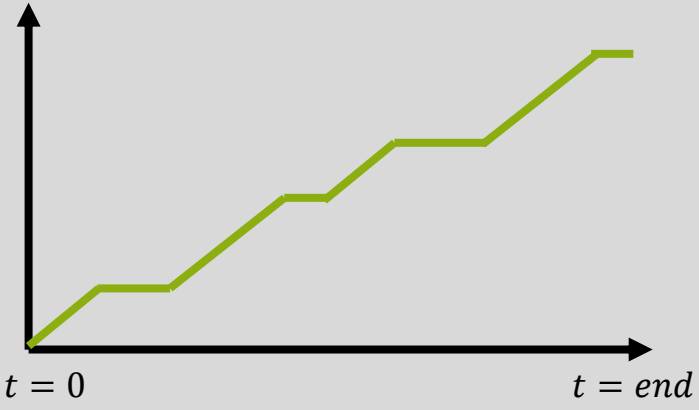
cURL request to server for constant download





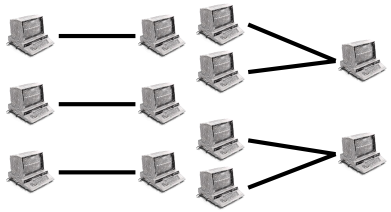
Random

cURL requests in random time patterns



Scenarios: Applications

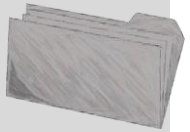
- **Network Topologies:** Directed, Grouped

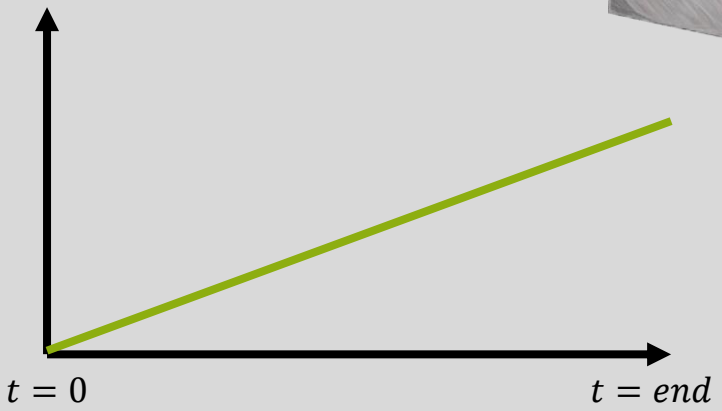


- **Applications**

Static

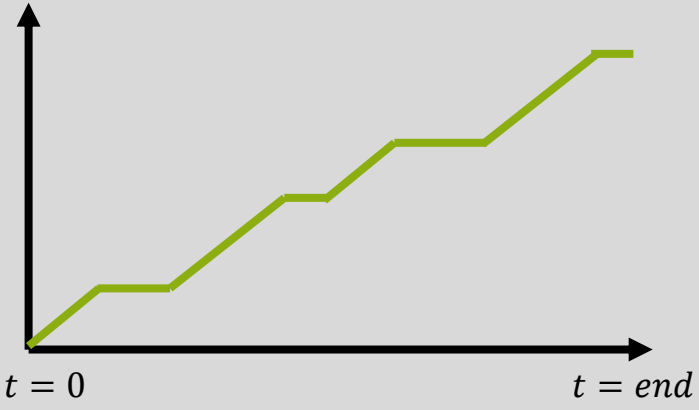
cURL request to server for constant download



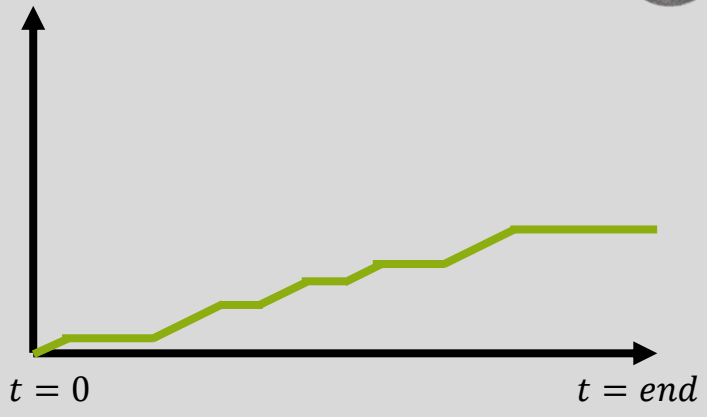


Random

cURL requests in random time patterns

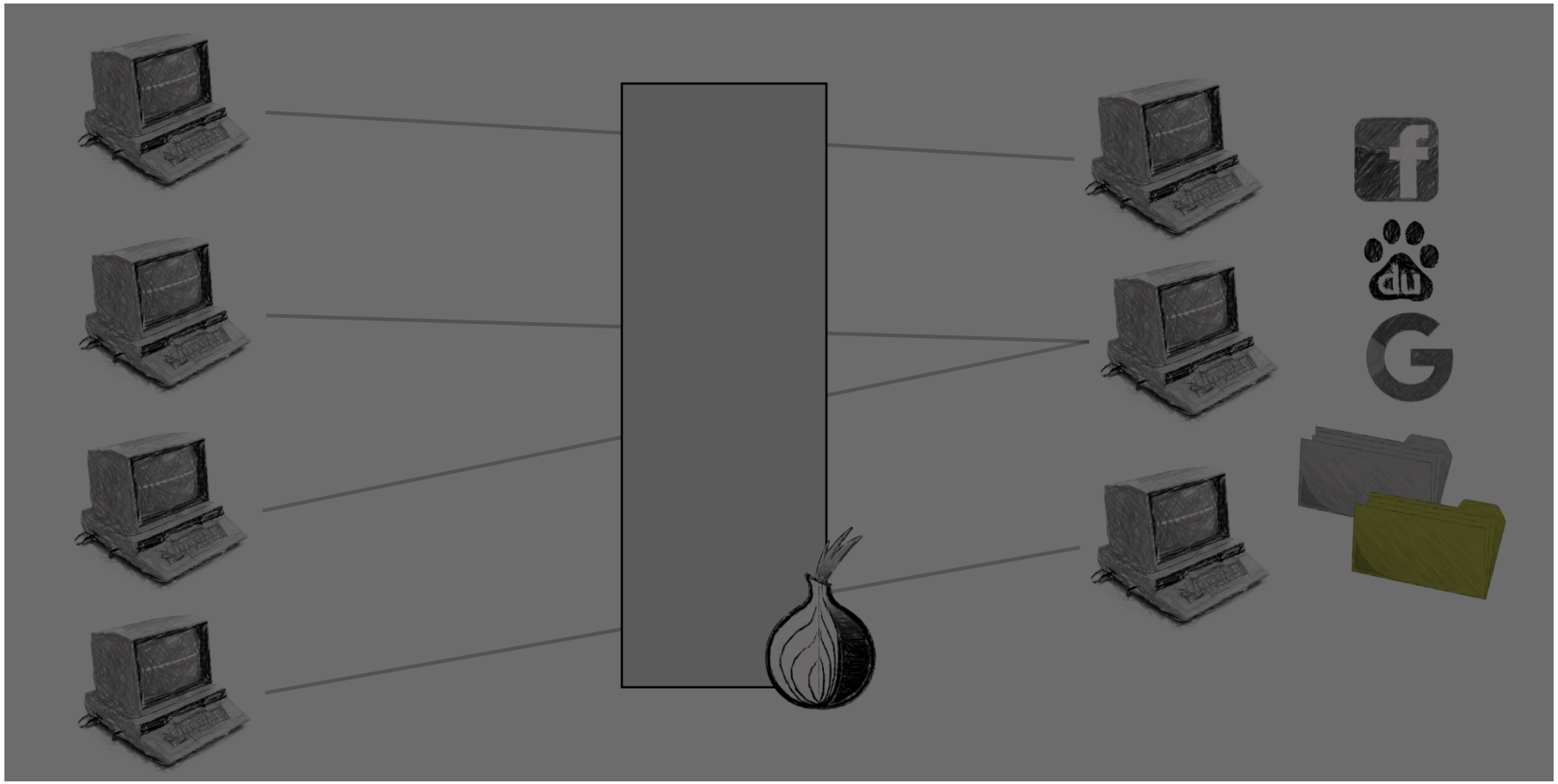


Browsing



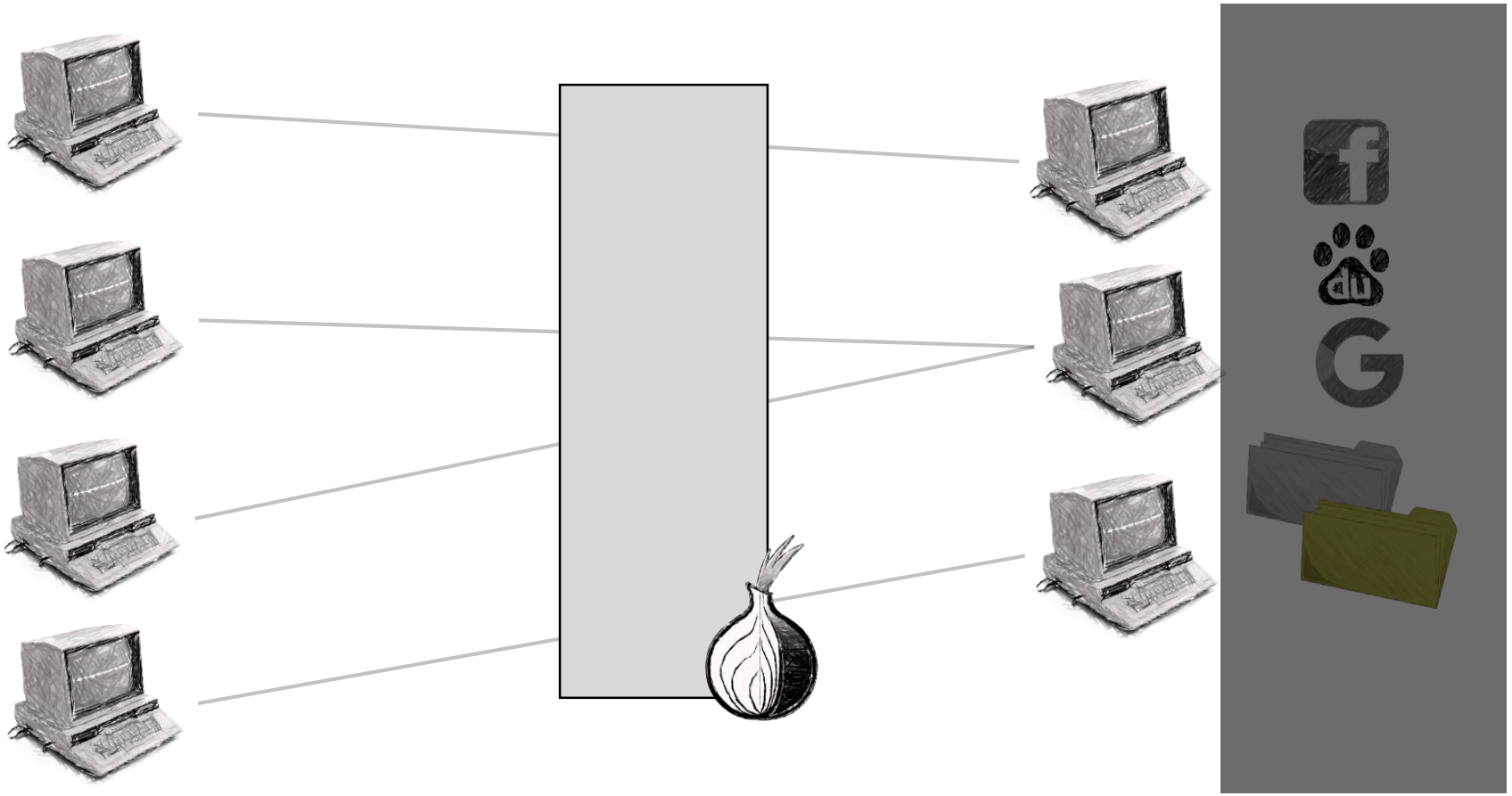
Evaluation Questions

Best Metric in a Generic Scenario?



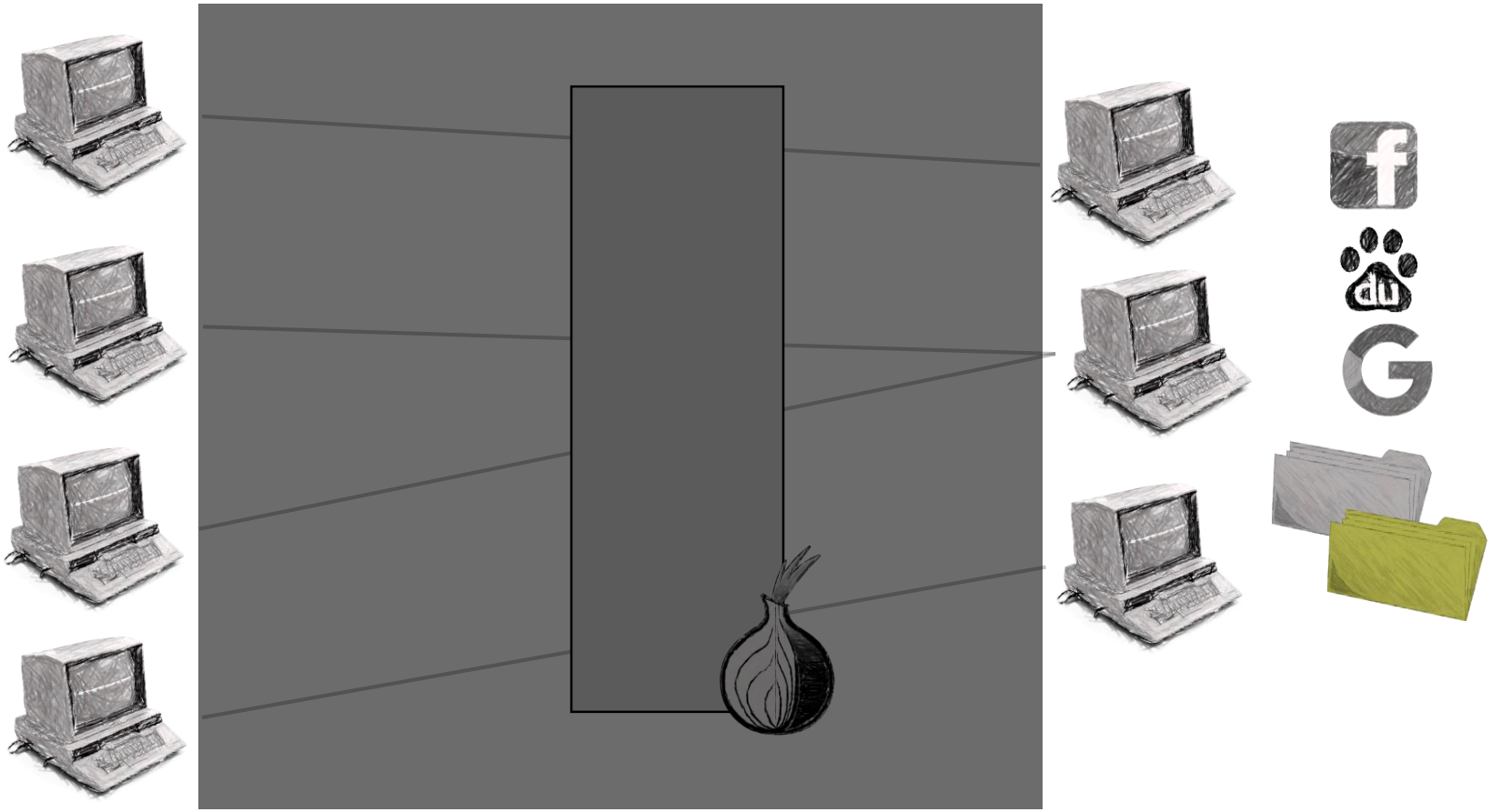
Evaluation Questions

Impact of Network Topologies?



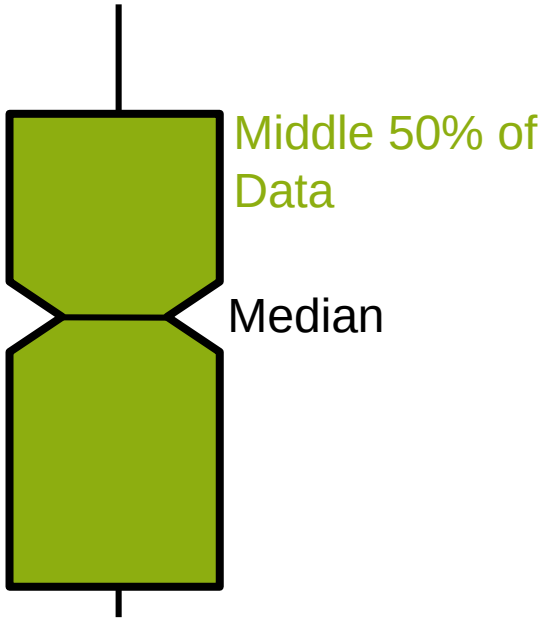
Evaluation Questions

Impact of Application Types?

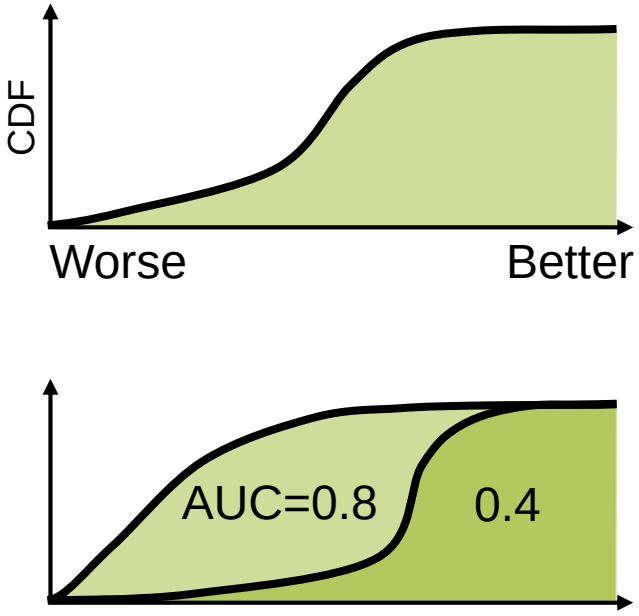


Analysis Metrics

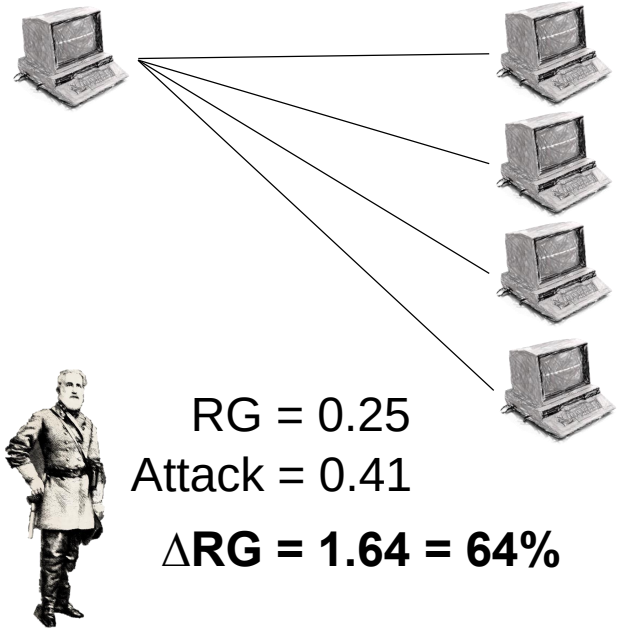
Boxplot
Summarizes Multiple Results



CDF & AUC
Distribution of Results

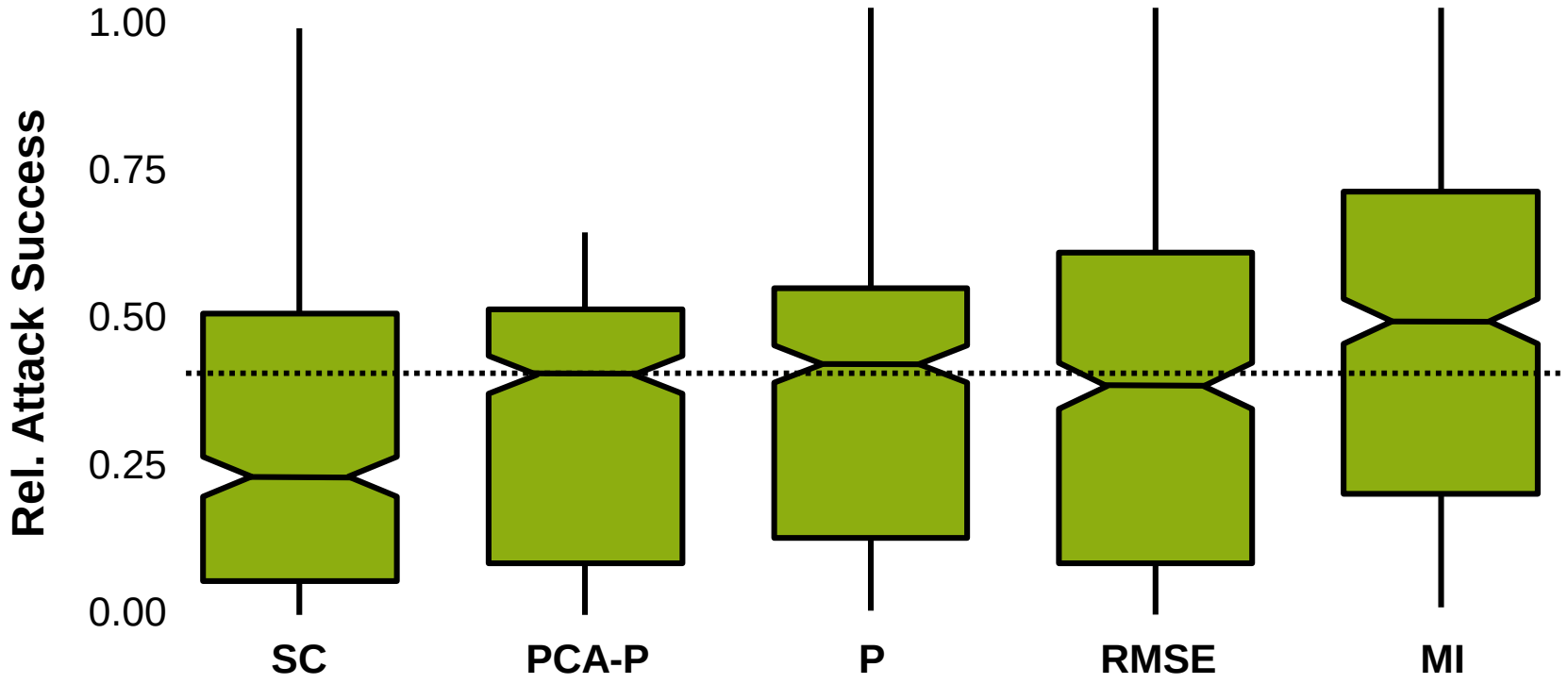


∆Random Guessing
Better than Uneducated Guess



RG = 0.25
Attack = 0.41
∆RG = 1.64 = 64%

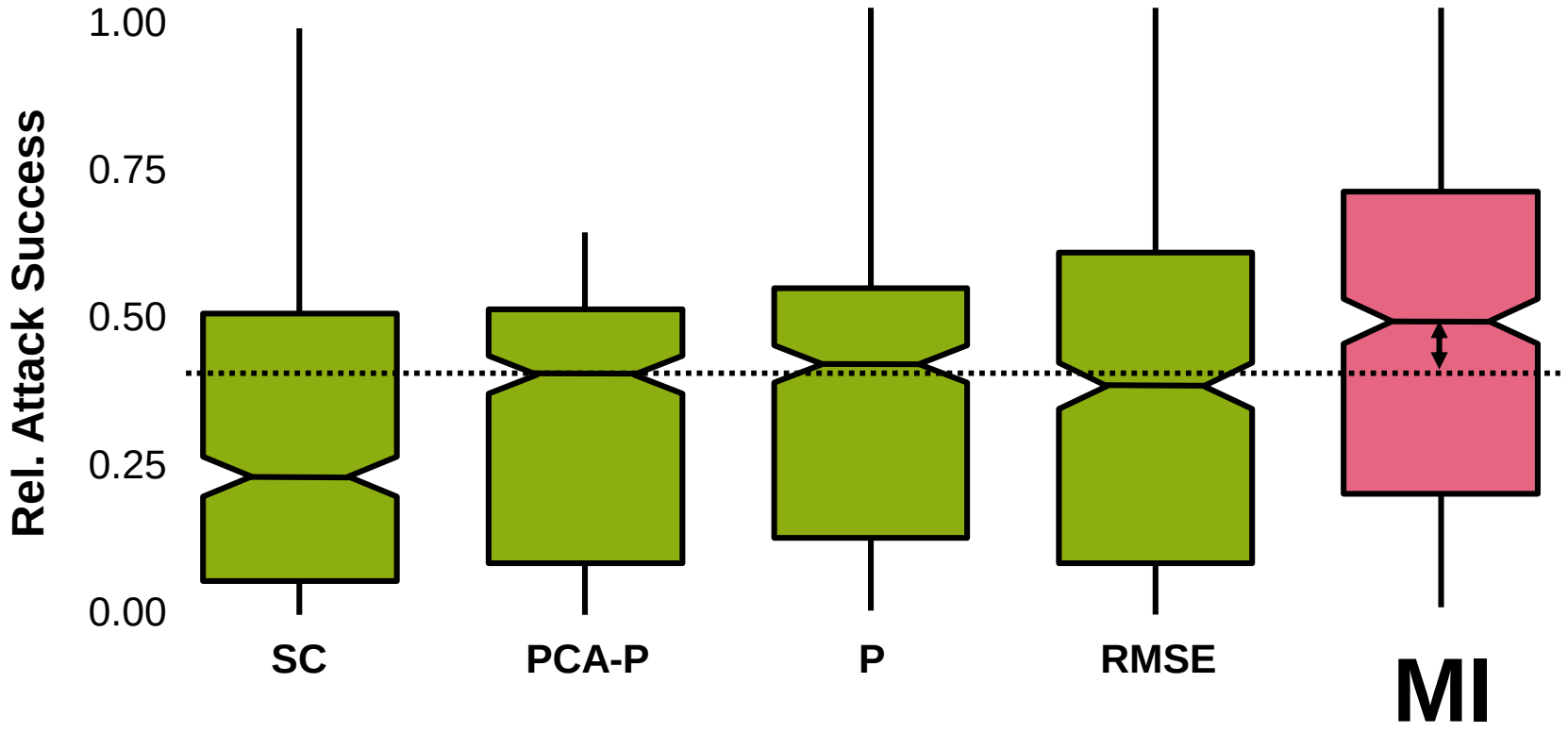
Best Metric?



Metrics

- **SC**: Scalar
- **PCA-P**: Principal Component Analysis & Pearson Correlation
- **P**: Pearson Correlation
- **RMSE**: Root-Mean-Square Error
- **MI**: Mutual Information

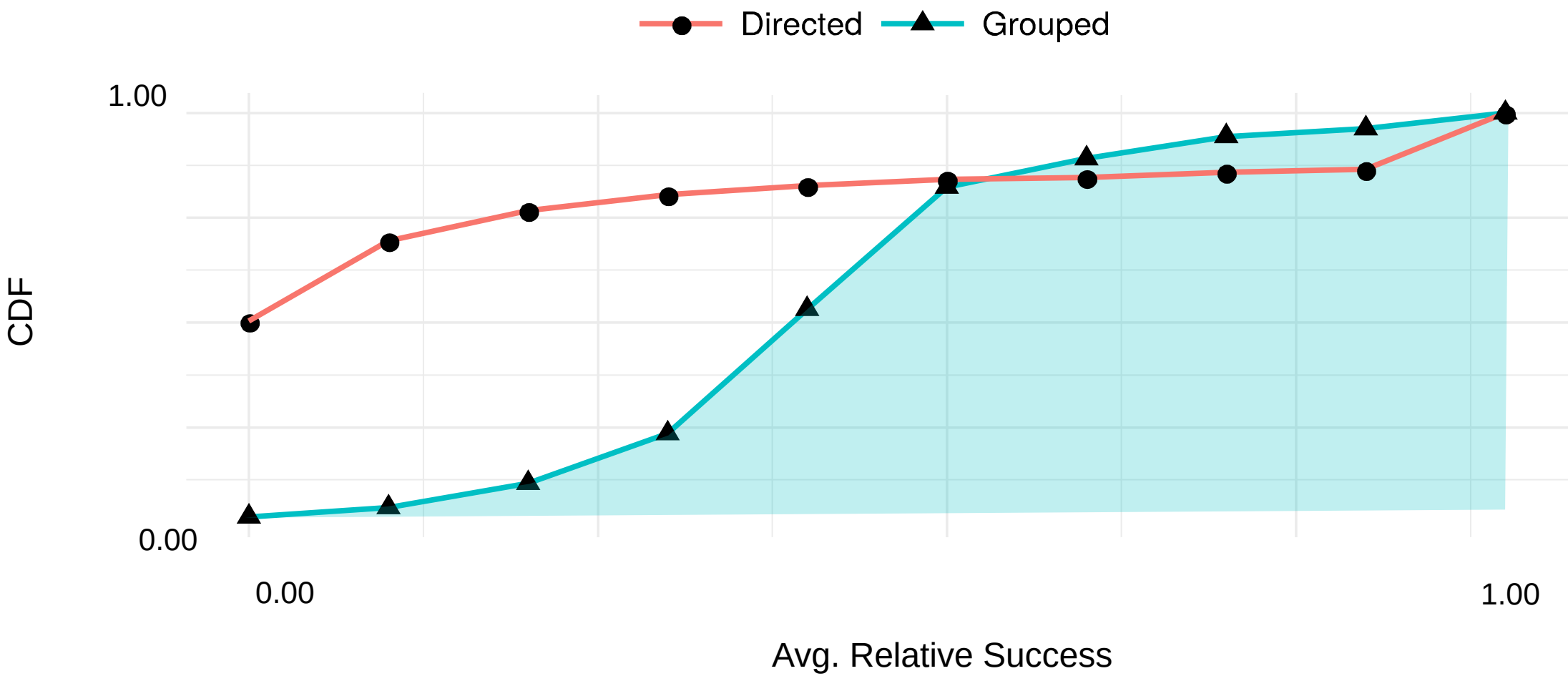
Mutual Information



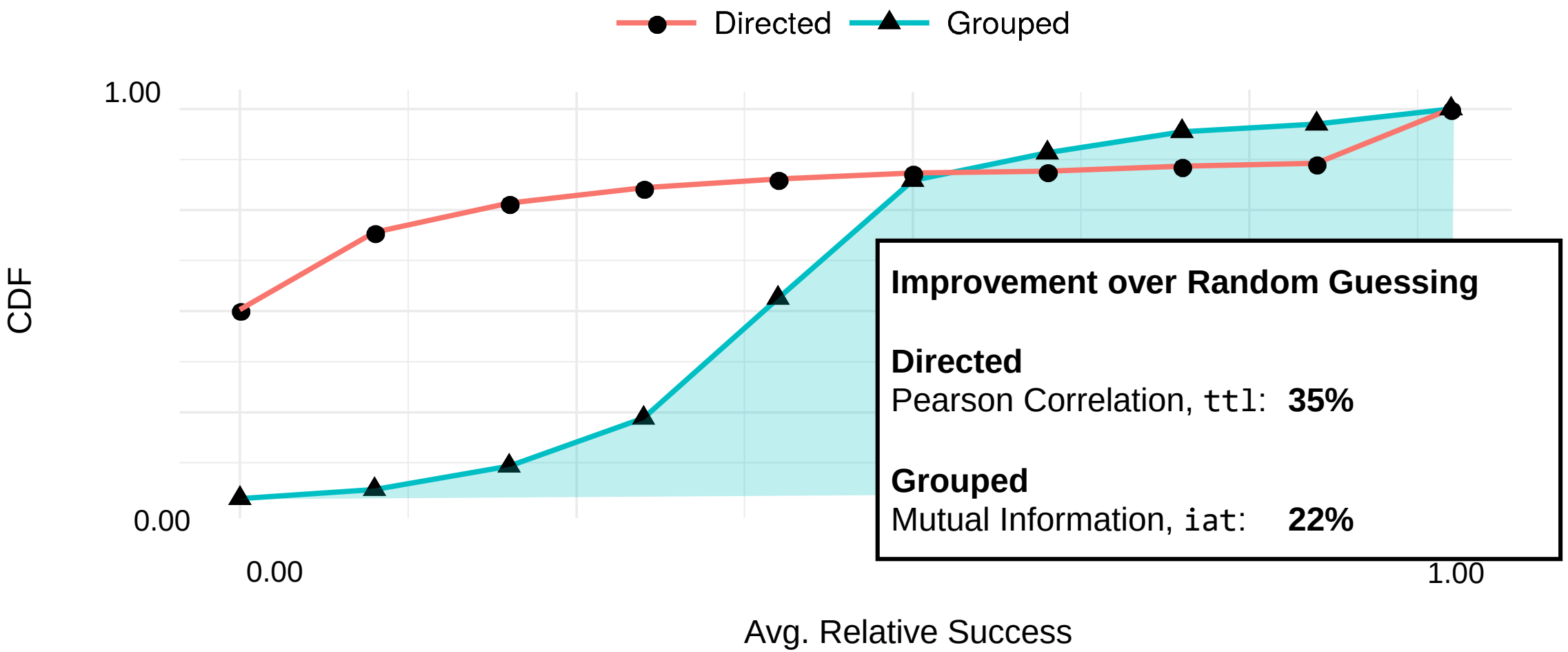
Metrics

- **SC**: Scalar
- **PCA-P**: Principal Component Analysis & Pearson Correlation
- **P**: Pearson Correlation
- **RMSE**: Root-Mean-Square Error
- **MI**: Mutual Information

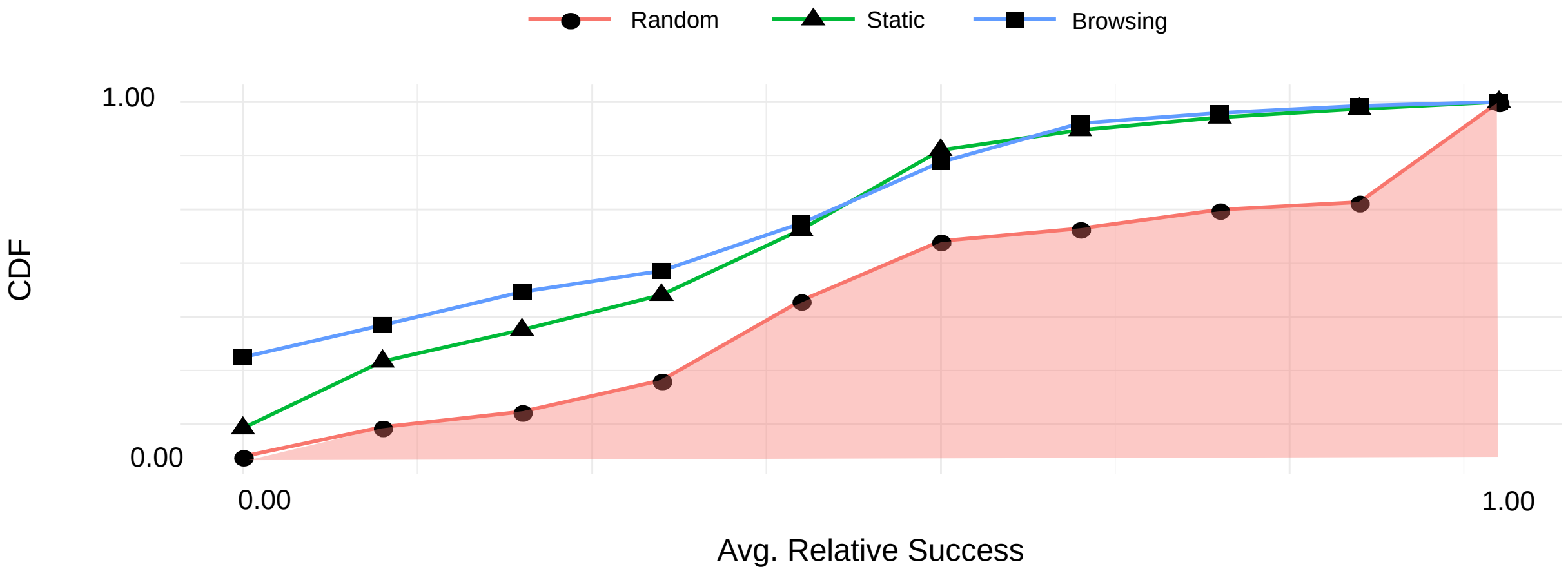
Comparison of Setups



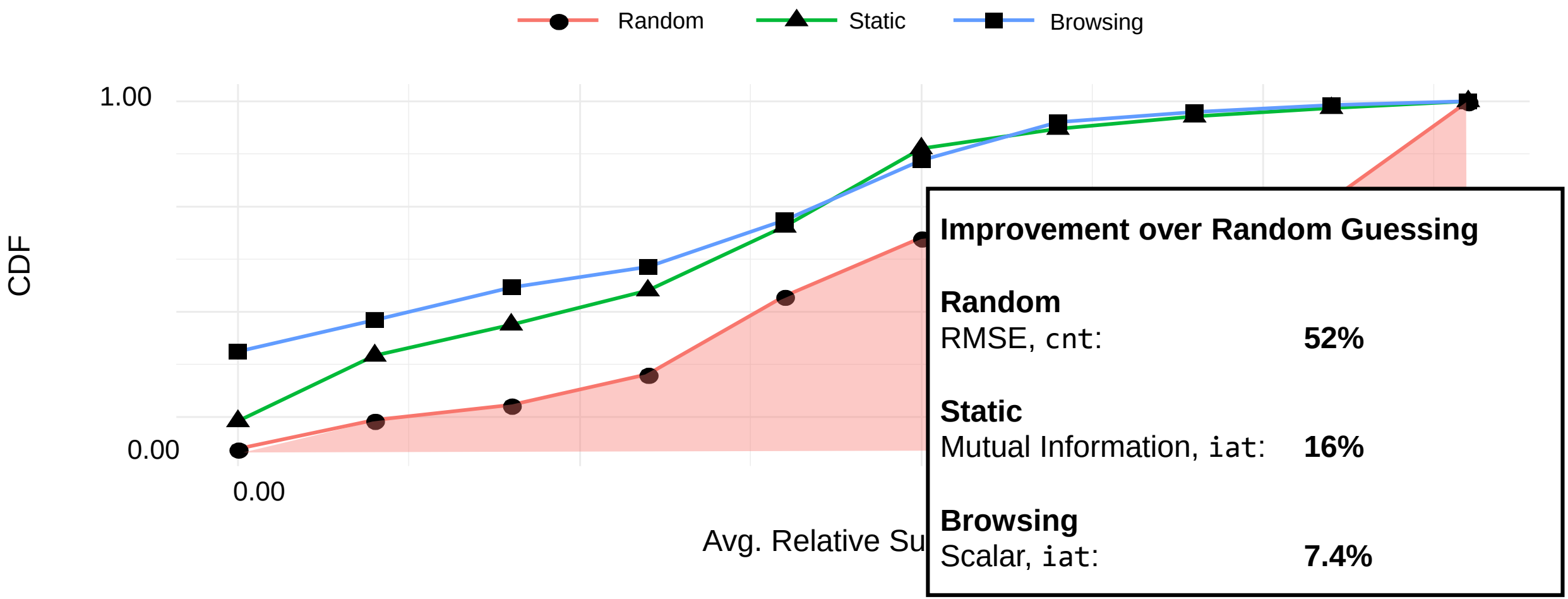
Comparison of Setups



Comparison of Applications



Comparison of Applications



Improvement over Random Guessing

Random
RMSE, `cnt`: **52%**

Static
Mutual Information, `iat`: **16%**

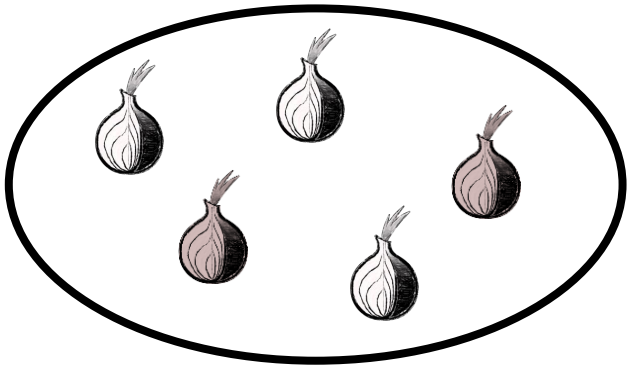
Browsing
Scalar, `iat`: **7.4%**

Demonstration of DigesTor

Mixing as Countermeasure

Countermeasure: Mixing

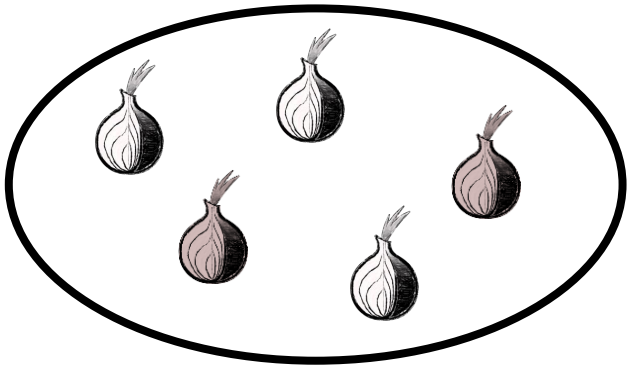
Entry traffic



Exit traffic

Delay on Purpose

Entry traffic

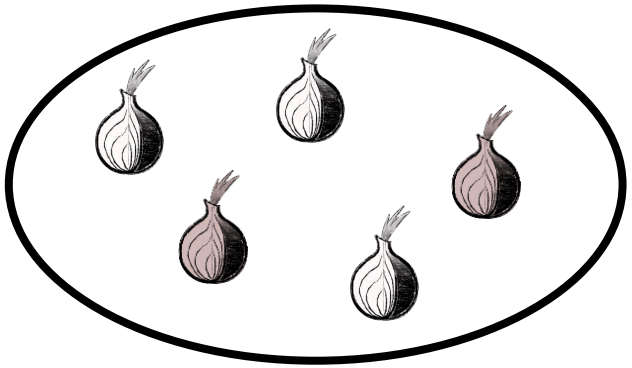


Exit traffic

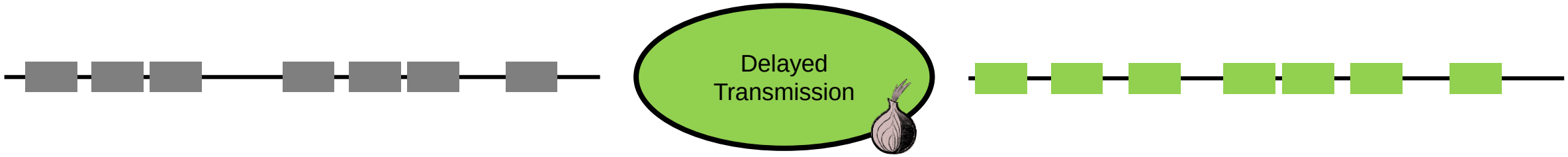
Delayed
Transmission

Obfuscate Traffic

Entry traffic

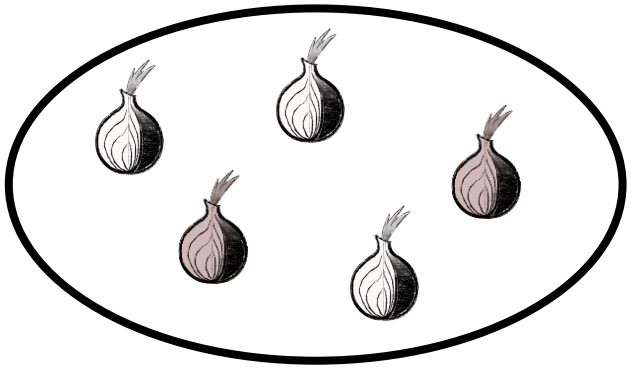


Exit traffic

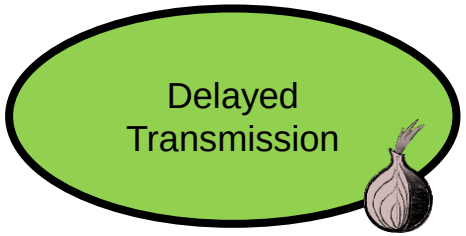


Protection at a Price

Entry traffic



Exit traffic



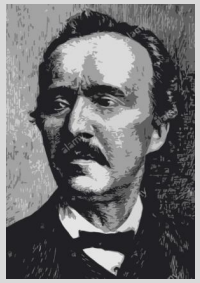
Mix Parameters
- 20% of TLS Records
- 0.1ms to 10ms

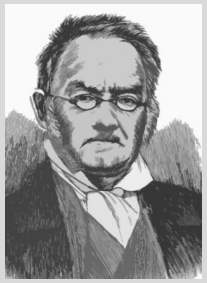
Result
- AUC from 0.72 to 0.9
- **20% Improvement**

Conclusion

What did we achieve?

Experimental Diversity



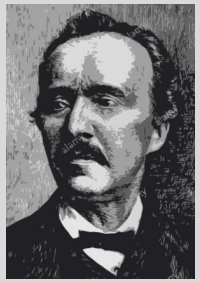


Traffic Analysis Attacks

- Related work provides several different attacks
- Evaluation concepts differ
- Comparing results means comparing apples and oranges

Create Comparability

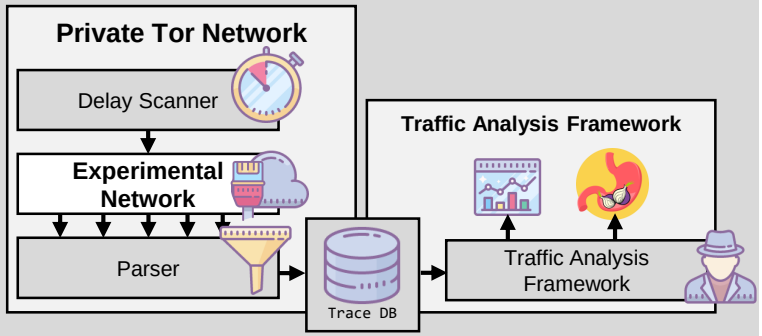
Experimental Diversity



Traffic Analysis Attacks

- Related work provides several different attacks
- Evaluation concepts differ
- Comparing results means comparing apples and oranges

Creating Comparability



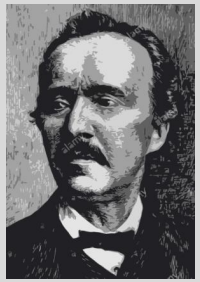
DigesTor

- Generate traces in controlled environment
- Share data in Trace DB
- Apply TA framework

Create Comparability

Assess Attacks

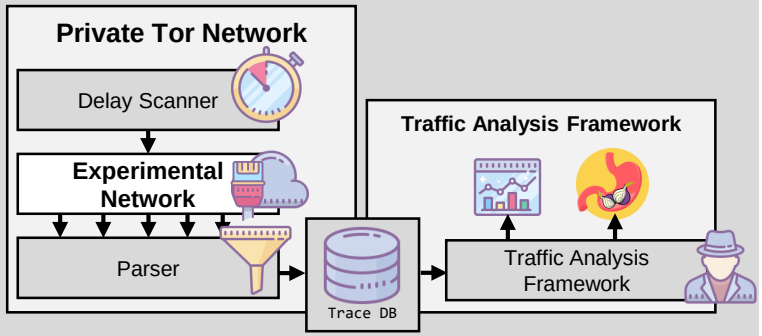
Experimental Diversity



Traffic Analysis Attacks

- Related work provides several different attacks
- Evaluation concepts differ
- Comparing results means comparing apples and oranges

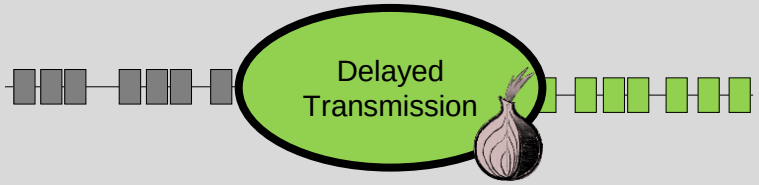
Creating Comparability



DigesTor

- Generate traces in controlled environment
- Share data in Trace DB
- Apply TA framework

Demonstrating the Framework



Mixing

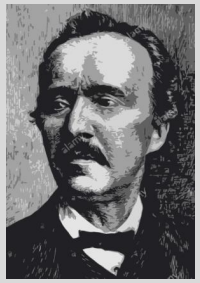
- Delay transmissions on purpose
- Obfuscate traffic patterns
- Hinder correlation

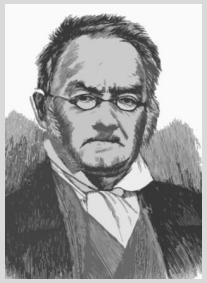
Create Comparability

Assess Attacks

Evaluate Countermeasures

Experimental Diversity

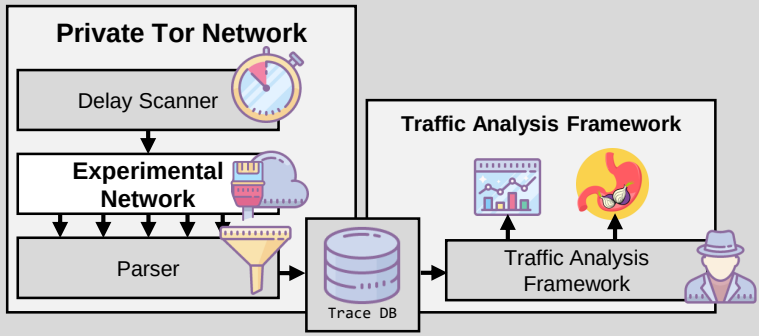




Traffic Analysis Attacks

- Related work provides several different attacks
- Evaluation concepts differ
- Comparing results means comparing apples and oranges

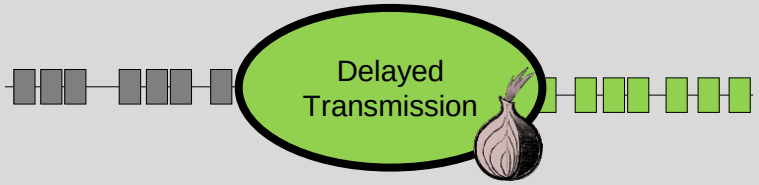
Creating Comparability



DigesTor

- Generate traces in controlled environment
- Share data in Trace DB
- Apply TA framework

Demonstrating the Framework



Mixing

- Delay transmissions on purpose
- Obfuscate traffic patterns
- Hinder correlation

Create Comparability

Assess Attacks

Evaluate Countermeasures

Thank You! Questions?

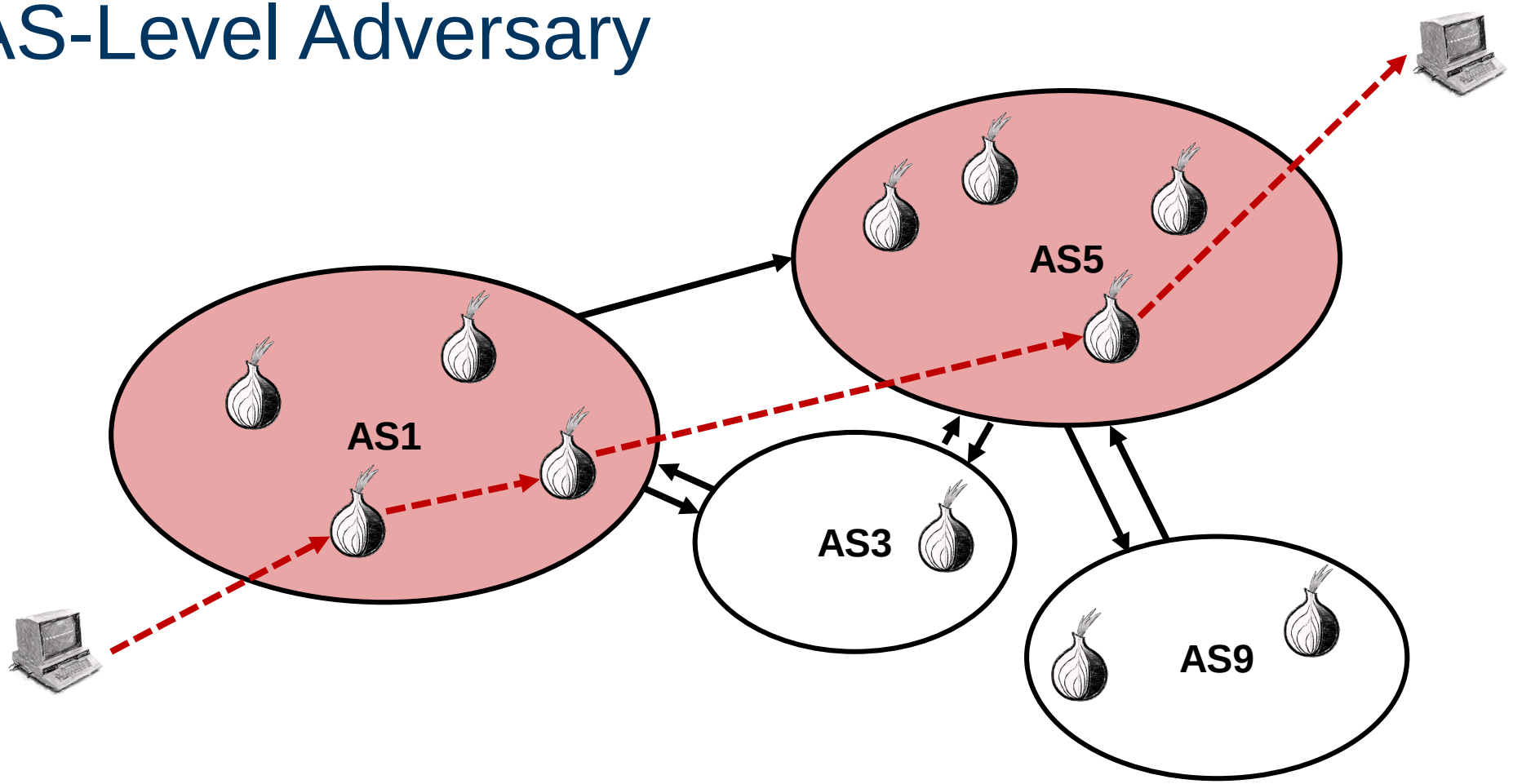
Appendix

Everything you asked for

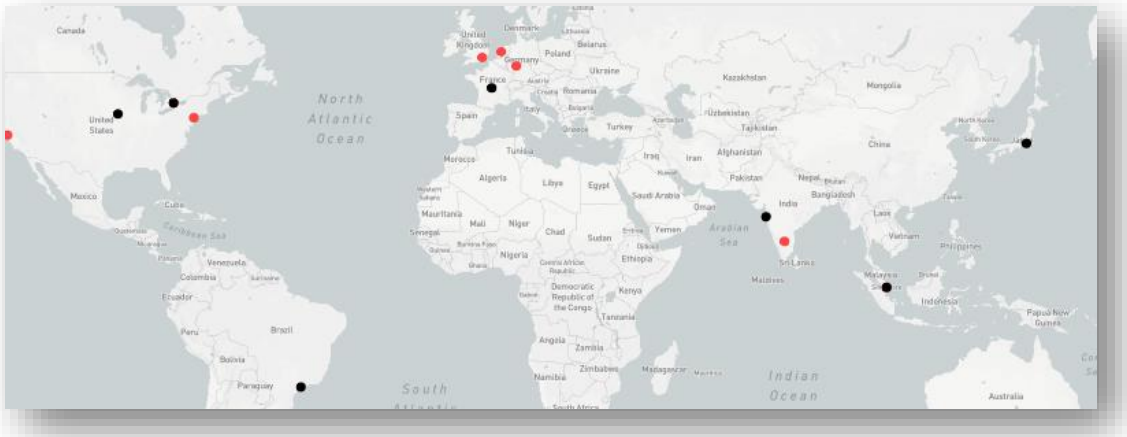
References: Passive Attacks

1. Timing Attacks in Low-Latency Mix Systems; Levine, Brian N and Reiter, Michael K and Wang, Chenxi and Wright, Matthew; International Conference on Financial Cryptography 2004
2. Timing Analysis in Low-Latency Mix Networks: Attacks and Defenses; Shmatikov, Vitaly and Wang, Ming-Hsiu; European Symposium on Research in Computer Security 2006
3. Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services; Kwon, Albert and AlSabah, Mashael and Lazar, David and Dacier, Marc and Devadas, Srinivas; USENIX Security Symposium 2015
4. On Flow Correlation Attacks and Countermeasures in Mix Networks; Zhu, Ye and Fu, Xinwen and Graham, Bryan and Bettati, Riccardo and Zhao, Wei; Privacy Enhancing Technologies Symposium 2005
5. Sampled Traffic Analysis by Internet-Exchange-Level Adversaries; Murdoch, Steven J and Zielinski, Piotr; Workshop on Privacy Enhancing Technologies 2007
6. Statistical Disclosure Attacks; Danezis, George; Security and Privacy in the Age of Uncertainty 2003
7. Two-Sided Statistical Disclosure Attack; Danezis, George and Diaz, Claudia and Troncoso, Carmela; Workshop on Privacy Enhancing Technologies 2007
8. Limits of Anonymity in Open Environments; Kesdogan, Dogan and Agrawal, Dakshi and Penz, Stefan; Workshop on Information Hiding 2002
9. Practical Traffic Analysis: Extending and Resisting Statistical Disclosure; Mathewson, Nick and Dingledine, Roger; Workshop on Privacy Enhancing Technologies 2004

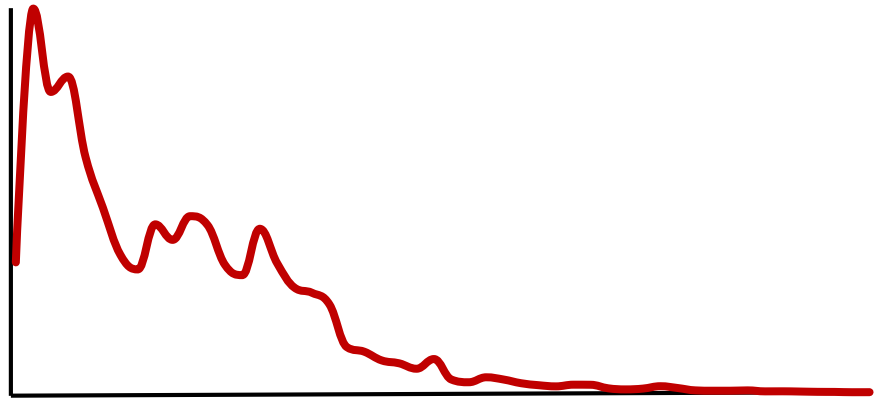
AS-Level Adversary



Empirical Delays

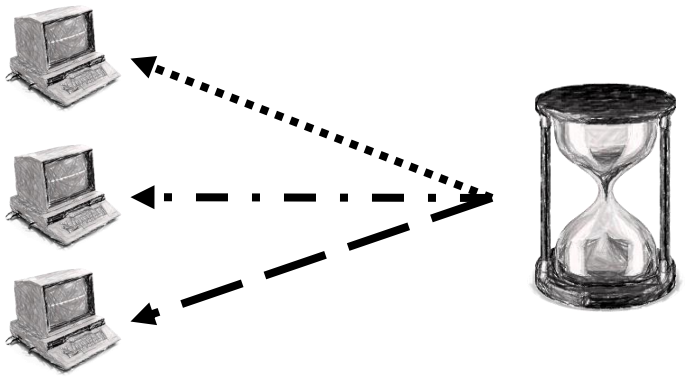


Worldwide Remote Servers



End-to-End Delays

Connection-Individual Delay



Individual Results

Scenario	Metric	Feature	RG	AUC	AS
Directed	P	`ttl`	35%	0.72	0.49
Grouped	MI	`iat`	22%	0.50	0.55
Random	RMSE	`cnt`	52%	0.48	0.80
Static	MI	`iat`	16%	0.65	0.46
Browsing	SC	`iat`	7.4%	0.70	0.34
Global	MI	`iat`	23%	0.61	0.52

Mixing: Performance Impairments