RUHR-UNIVERSITÄT BOCHUM

DIGESTOR

Comparing Passive Traffic Analysis Attacks on Tor

Katharina Kohls
Ruhr-University Bochum

Christina Pöpper
NYU Abu Dhabi

RUHR-UNIVERSITÄT BOCHUM

DIGESTOR

Comparing Passive Traffic Analysis Attacks on Tor

Katharina Kohls
Ruhr-University Bochum

Christina Pöpper
NYU Abu Dhabi
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!
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
Cyrrus Smith
Balloon Inc.

Flight Plan
Mondays and Thursdays:
Departure at sunrise
Cyrrus Smith
Balloon Inc.

Flight Plan
Mondays and
Thursdays:
Departure at
sunrise

Fix knows:
Fogg will leave next Monday
Cyrrus Smith Balloon Inc.

Flight Plan
Mondays and Thursdays: Departure at sunrise

Anonymity
Separate identity from content
Tor: Anonymous Connections

Cyrrus Smith Balloon Inc.

Flight Plan
Mondays and Thursdays:
Departure at sunrise
Traffic Analysis

Cyrrus Smith Balloon Inc.

**Flight Plan**
Mondays and Thursdays: Departure at sunrise
End-to-End Confirmation

Flight Plan
Mondays and Thursdays:
Departure at sunrise

Entry traffic
Exit traffic

Cyrrus Smith Balloon Inc.
Attack: Correlation

Cyrrus Smith
Balloon Inc.

Flight Plan
Mondays and Thursdays:
Departure at sunrise
Countermeasure: Obfuscation

Flight Plan
Mondays and Thursdays:
Departure at sunrise

Entry traffic

Exit traffic
Diversity in Evaluation Techniques
Comparing Apples and Oranges
Evaluation Procedure

Research on Traffic Analysis Attacks

Choose Evaluation Setup ➔ Conduct Attacks ➔ Draw Conclusions
Example: Different Setups

Statistical Model

Simulation Model

Live Network
Example: Different Setups

Statistical Model

Simulation Model

Live Network
## Related Work Comparison

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Comp.</td>
<td>[1,2]</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>iat</td>
<td>Corr.</td>
</tr>
<tr>
<td></td>
<td>[3,4]</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>iat</td>
<td>MI</td>
</tr>
<tr>
<td>Coding</td>
<td>[14-17]</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>-</td>
<td>Enc.</td>
</tr>
<tr>
<td>Protocol</td>
<td>[18,19]</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>-</td>
<td>Cell</td>
</tr>
<tr>
<td>n-1</td>
<td>[20-22]</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>-</td>
<td>Blend</td>
</tr>
</tbody>
</table>
### Statistical Models

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Comp.</td>
<td>[1,2]</td>
<td></td>
<td>●</td>
<td>□</td>
<td>□</td>
<td>●</td>
<td>iat</td>
<td>Corr.</td>
</tr>
<tr>
<td></td>
<td>[3,4]</td>
<td></td>
<td>●</td>
<td>□</td>
<td>□</td>
<td>●</td>
<td>iat</td>
<td>MI</td>
</tr>
<tr>
<td>Coding</td>
<td>[14-17]</td>
<td></td>
<td>●</td>
<td>□</td>
<td>□</td>
<td>●</td>
<td>-</td>
<td>Enc.</td>
</tr>
<tr>
<td>Protocol</td>
<td>[18,19]</td>
<td></td>
<td>●</td>
<td>□</td>
<td>□</td>
<td>●</td>
<td>-</td>
<td>Cell</td>
</tr>
<tr>
<td>n-1</td>
<td>[20-22]</td>
<td></td>
<td>●</td>
<td>□</td>
<td>□</td>
<td>●</td>
<td>-</td>
<td>Blend</td>
</tr>
</tbody>
</table>
Simulation Models

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Comp.</td>
<td>[1,2]</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>iat</td>
<td>Corr.</td>
</tr>
<tr>
<td></td>
<td>[3,4]</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>iat</td>
<td>MI</td>
</tr>
<tr>
<td>Coding</td>
<td>[14-17]</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>-</td>
<td>Enc.</td>
</tr>
<tr>
<td>Protocol</td>
<td>[18,19]</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>-</td>
<td>Cell</td>
</tr>
<tr>
<td>n-1</td>
<td>[20-22]</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>-</td>
<td>Blend</td>
</tr>
</tbody>
</table>
# Comparison Framework

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Comp.</td>
<td>[1,2]</td>
<td></td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td></td>
<td>iat</td>
<td>Corr.</td>
</tr>
<tr>
<td></td>
<td>[3,4]</td>
<td></td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td></td>
<td>iat</td>
<td>MI</td>
</tr>
<tr>
<td>Coding</td>
<td>[14-17]</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td></td>
<td>-</td>
<td>Enc.</td>
</tr>
<tr>
<td>Protocol</td>
<td>[18,19]</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td></td>
<td>-</td>
<td>Cell</td>
</tr>
<tr>
<td>n-1</td>
<td>[20-22]</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td></td>
<td></td>
<td>-</td>
<td>Blend</td>
</tr>
</tbody>
</table>

| DigesTor     | [1-9]     |     | ⬤    | ⬤     | ⬤     | ⬤   | 5 Feat. | 5 Metrics |
Comparing Passive Traffic Analysis Attacks on Tor

The Framework
Private Tor Network and TA Framework

Private Tor Network

Traffic Analysis Framework

Trace DB
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

Tor Network

- Delays
- Guard
- Middle, Authority
- Exit (Mix)

Clients

tcpdump

Servers
TA Framework

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

<table>
<thead>
<tr>
<th>Metric/Feature</th>
<th>cnt</th>
<th>iat</th>
<th>len</th>
<th>ttl</th>
<th>wis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalar</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>PCA, Pearson</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Pearson Correlation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RMSE</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mutual Information</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Experiments
Generate data, apply metrics, compare results
Scenarios: Network Topologies

**Directed** setup:
- $n = [2, \ldots, 30]$ clients connect to
- $n = [2, \ldots, 30]$ servers

**Grouped** setup:
- $n = [2, \ldots, 30]$ clients connect to
- 2 servers

Isolated Connections

Concurrent Connections
Scenarios: Applications

- **Network Topologies**: Directed, Grouped

- **Applications**

  **Static**

cURL request to server for constant download

\[ t = 0 \quad t = \text{end} \]
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**
  cURL requests in random time patterns
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

- Middle 50% of Data
- Median

**CDF & AUC**
Distribution of Results

- CDF
- Worse
- Better

- AUC = 0.8
- 0.4

**ΔRandom Guessing**
Better than Uneducated Guess

- RG = 0.25
- Attack = 0.41
- ΔRG = 1.64 = 64%
Best Metric?

- **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

CDF

Avg. Relative Success

Directed

Grouped
Comparison of Setups

- Directed
  - Pearson Correlation, ttl: 35%
- Grouped
  - Mutual Information, iat: 22%
Comparison of Applications

![Comparison of Applications Graph](image-url)
Comparison of Applications

Im keynote über:

Start > Absatz >

Listenebene

Comparison of Applications

CDF

Avg. Relative Success

Random

Static

Browsing

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
Delay on Purpose

Entry traffic

Exit traffic

Delayed Transmission
Obfuscate Traffic

Entry traffic → Entry traffic

Exit traffic → Exit traffic

Delayed Transmission

Cyrrus Smith
Balloon Inc.
Protection at a Price

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
Traffic Analysis Attacks

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

Create Comparability

DigesTor

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

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

Create Comparability

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

Assess Attacks

Demonstrating the Framework

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

Evaluate Countermeasures
Experimental Diversity

Traffic Analysis Attacks
• Related work provides several different attacks
• Evaluation concepts differ
• Comparing results means comparing apples and oranges

Create Comparability

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

Assess Attacks

Demonstrating the Framework

Mixing
• Delay transmissions on purpose
• Obfuscate traffic patterns
• Hinder correlation

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

Connection-Individual Delay

End-to-End Delays
## Individual Results

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Metric</th>
<th>Feature</th>
<th>RG</th>
<th>AUC</th>
<th>AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed</td>
<td>P</td>
<td>ttl</td>
<td>35%</td>
<td>0.72</td>
<td>0.49</td>
</tr>
<tr>
<td>Grouped</td>
<td>MI</td>
<td>iat</td>
<td>22%</td>
<td>0.50</td>
<td>0.55</td>
</tr>
<tr>
<td>Random</td>
<td>RMSE</td>
<td>cnt</td>
<td>52%</td>
<td>0.48</td>
<td>0.80</td>
</tr>
<tr>
<td>Static</td>
<td>MI</td>
<td>iat</td>
<td>16%</td>
<td>0.65</td>
<td>0.46</td>
</tr>
<tr>
<td>Browsing</td>
<td>SC</td>
<td>iat</td>
<td>7.4%</td>
<td>0.70</td>
<td>0.34</td>
</tr>
<tr>
<td>Global</td>
<td>MI</td>
<td>iat</td>
<td>23%</td>
<td>0.61</td>
<td>0.52</td>
</tr>
</tbody>
</table>
Mixing: Performance Impairments

![Graph showing frequency vs. delay with different mixing levels: No Mixing, 0.1ms, 1ms, 10ms.](image-url)