ProTO: Proactive Topology Obfuscation Against Adversarial Network Topology Inference

TAO HOU†, ZHE QU†, TAO WANG‡, ZHUO LU† AND YAO LIU†
†UNIVERSITY OF SOUTH FLORIDA ‡NEW MEXICO STATE UNIVERSITY
Network Topology

- P2P
- VPN
- CDN
- VOIP

Network diagnosis

Failure localization
Motivation

• Advancing attackers’ malicious objectives
  - DDoS attack
  - DNS poisoning
  - Internet censorship

• Disturbing network diagnosis

• Leaking commercial interests and private information
Motivation

• Advancing attackers’ malicious objectives
  - DDoS attack
  - It may not always be desirable or even prohibitive to disclose network topology
  - Leaking commercial interests and private information
There are mainly two types of topology inference techniques:

- Internally cooperative topology inference
  - Disable internal routers’ response to traceroute or ping
  - Advanced designs, such as NetHide

- External end-to-end topology inference
There are mainly two types of topology inference techniques:

- Internally cooperative topology inference:
  - Disable internal routers' response to traceroute or ping
  - Advanced designs, such as NetHide

- External end-to-end topology inference
External End-to-end Topology Inference

- Topology recovering example
Countermeasures

• Intuitive way: detect-then-disable
  o Attacker may notice and develop follow-on actions
  o False alarm

• Our Design: Proactive Topology Obfuscation (ProTO)
  o Detect-then-obfuscate
  o Proactively delay packet forwarding
  o Deliver a structurally accurate yet fake topology to the attacker
ProTO consists of two major modules: (i) identification and manipulation module and (ii) topology control module.
We develop a lightweight k-Nearest Neighbor (light-k-NN) approach to identify probe packets.

- A multi-round dynamic method to adaptively train the weights
- A voting-based lazy-learning update strategy

Light-k-NN is as easy as traditional k-NN to be used, but is more suitable for ProTO for real-time network devices.
Topography Obfuscation

- Routing matrix

![Routing matrix diagram]

- Inference formulation

\[ \mathbf{x} = \mathbf{A} \mathbf{\mu} \]

The measurement results \( \mathbf{x} \) are related to the link delays through the routing matrix \( \mathbf{A} \) and the vector \( \mathbf{\mu} \).
Topology Obfuscation

- Topology obfuscation

\[ Fx = FA\mu \]

The measurement results \( Fx \) equal to \( FA\mu \) Link delays

\[ FA = A_m \]

Fake topology

- Goal of topology obfuscation

Find the manipulation matrix \( F \), given the real topology \( A \) and the fake one \( A_m \)
System Implementation

• ProTO is implemented in P4 integrated with Python.
  - It is hardware independent and can be compiled to different realistic network devices. (Thanks to P4)

• Use real-world network topologies from Internet Topology Zoo

• Each node is created as a virtual machine that runs OpenWrt
Evaluation of Probe Packet Detection

- ProTO achieves a detection rate of 99.9% and a false alarm rate of around 3%
Evaluation of Topology Obfuscation

• Effectiveness Metric

\[ \text{similarity score} = 1 - \frac{\text{TED}_0}{\text{TED}_1 + \text{TED}_2} \]

**TED** = Tree Edit Distance

**TED\(_0\)** = distance between tree 1 and tree 2

**TED\(_1\)** = distance between tree 1 and zero-node tree

**TED\(_2\)** = distance between tree 2 and zero-node tree
Effectiveness of Topology Obfuscation

- **Similarity score between the inferred topology and the real topology without protection.**

- **Similarity score between the inferred topology and the real topology under protection.**

- **Similarity score between the inferred topology and the intended topology.**
Performance Cost of Topology Obfuscation

The performance cost of normal packets that are misidentified as probe packets and delayed by ProTO

<table>
<thead>
<tr>
<th></th>
<th>Low Utilization</th>
<th>High Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claranet</td>
<td>1.28%</td>
<td>1.93%</td>
</tr>
<tr>
<td>Switch</td>
<td>1.33%</td>
<td>1.95%</td>
</tr>
<tr>
<td>Cogent</td>
<td>1.35%</td>
<td>1.99%</td>
</tr>
</tbody>
</table>

The average performance cost of all normal packets
Conclusion

We develop a practical system ProTO that adopts a detect-then-obfuscate framework to combat adversarial network topology inference.

Evaluation results show that ProTO can effectively and efficiently defend against potential attacks.
Thank you!