A Technique for Network Topology Deception

Samuel Trassare, Robert Beverly, David Alderson

Naval Postgraduate School
{sttrassa,rbeverly,dladers}@nps.edu
June 18, 2013

NPS Topology Meeting

Outline

traceroute

Active Network Topology Measurement

- `traceroute` and its variants source active TTL-limited probes to infer (remote) network connectivity and structure.
- `traceroute` reports hops along a forward path based on the source IP address of received ICMP TTL time exceeded packets.
- Useful diagnostic tool, invaluable to network topology researchers.
- Recall: `traceroute` is a happy hack (thanks Van Jacobson!). Internet never intended to be mapped.

`traceroute` in Practice

Real-world `traceroute`:

- For security, policy, and economic reasons, many providers actively prevent `traceroute` measurement
- Many routers do not respond with ICMP when TTL expires
- Many routers block ICMP
- In real-world traces, only $\leq$ 15% of random traces complete.

`traceroute` in Practice

Real-world `traceroute`:

- Long history of bad topology inferences by researchers
- e.g. false links, missing links, etc.
  - "*What are our standards for validation of measurement-based networking research?*" (Krishnamurthy, Willinger)
  - "*Mathematics and the Internet: A source of enormous confusion and great potential*" (Willinger, Alderson, Doyle)
- Implication: criticism of active `traceroute`-based topology measurement with respect to accuracy of inferred network(s).

Network Topology Deception

Fooling Traceroute

- Our insight: the inherent measurement weaknesses of `traceroute` provide an **opportunity**
- The same measurement weaknesses imply that it is easy (trivial) to fool a remote `traceroute`
- There is *value* to fooling `traceroute`
- We introduce a new sub-field: ***Network Topology Deception***

Defending a Network

Other ways `traceroute` is used:

- Of course, network probing is not limited to innocuous measurement researchers
- Networks are frequently and regularly probed for vulnerabilities
- Mapping potentially reveals critical details of a network's connectivity
- `traceroute` used as a reconnaissance tool to understand which links/routers to target for attack to partition network

Military Deception

Deception in Cyberspace

- Leverage concept of military deception for cyberspace: Manipulate network traffic to deceive adversary and influence his/her decision making.
- Cause adversary to attack false targets, dilute attack, etc.
- May be preferable to outright blocking (“that must be an interesting target...”)
- Analogy with deceptive radar returns in meatspace.

Outline

Topology Deception

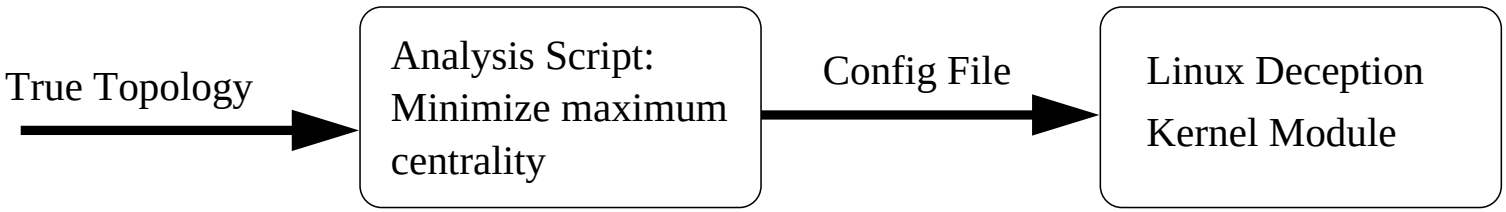
Sardine: Topology Deception

- Rather than block topology probes, return modified responses that cause adversary to infer a false topology:
  - Continuum: random vs. crafted responses
  - Graph theory: make weakest portion of topology appear to be most robust
- Keep adversary in collection rather than operational phase.
- Confuse adversary into believing least resilient portion of network is most robust.

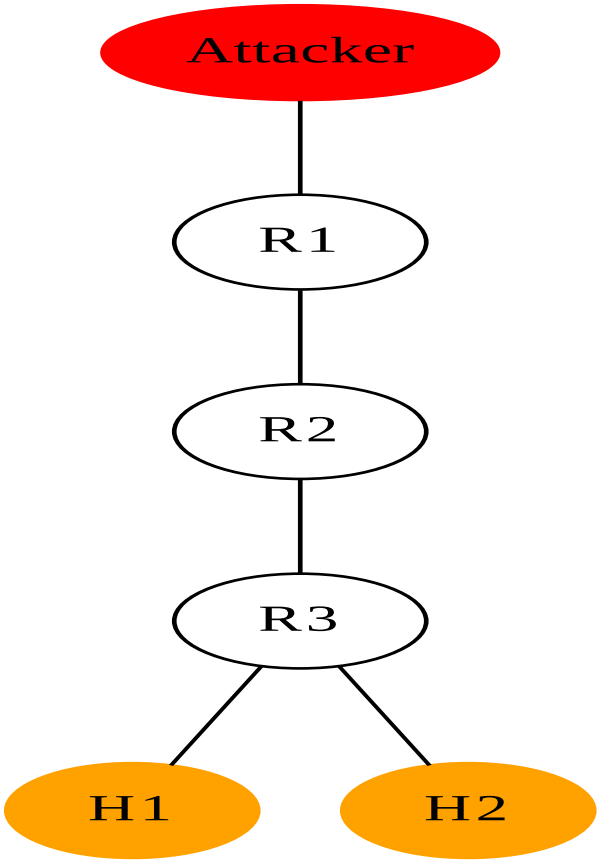
Topology Deception

Sardine: Topology Deception

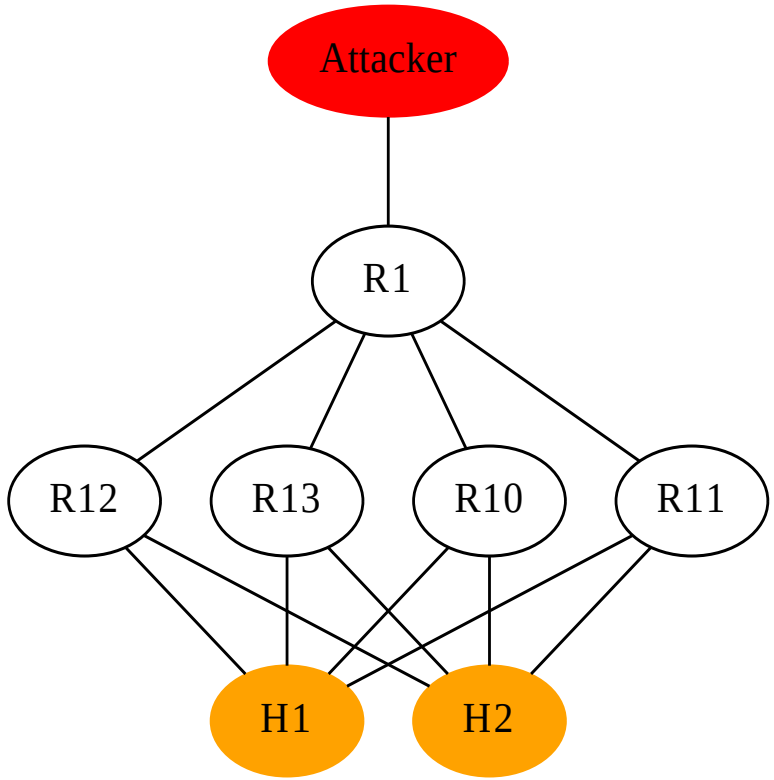
- Deception may be arbitrary
- We choose one exemplar utility function, minimizing the maximum betweenness centrality



Sardine Example



True Topology, Vulnerable Links



Faked Topology, False Links, Missing Links

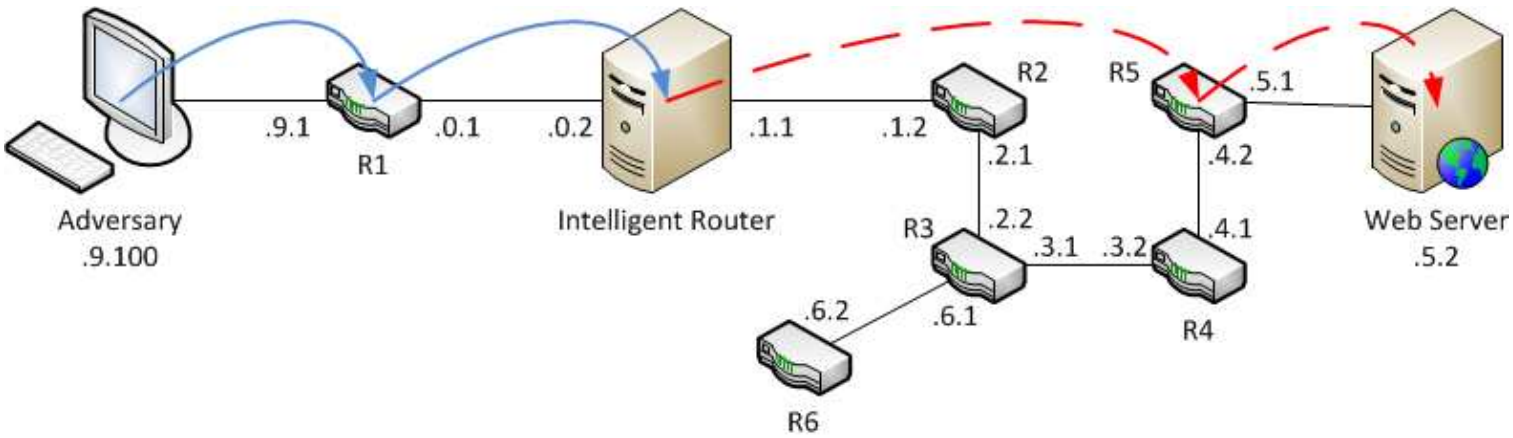
Development

Prototype:

- Linux-based router using `libnetfilter_queue`
- Runs as a kernel module
- Configurable per-TTL hops
- Configurable ICMP port unreachable (path length)
- Deterministic delay component
- Fake packets we originate sourced with a TTL corresponding to incoming TTL

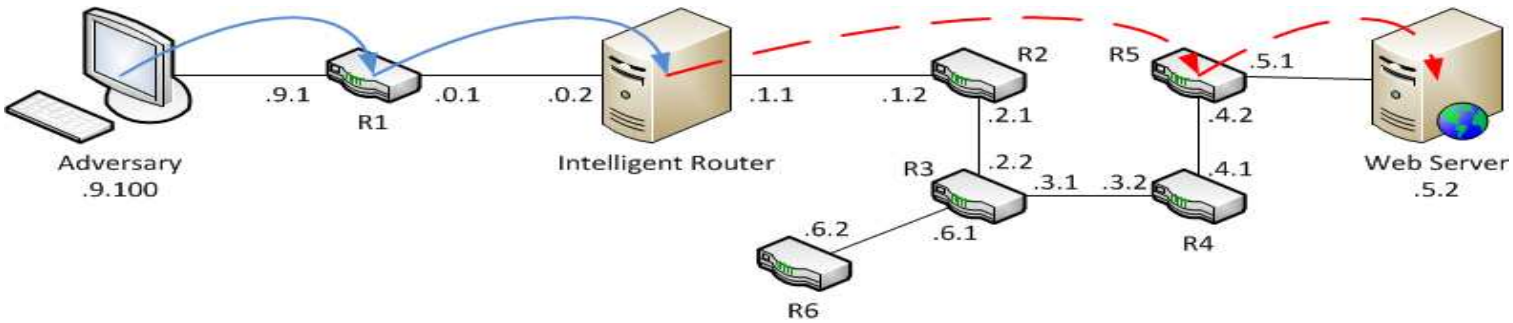
Outline

Topology Deception



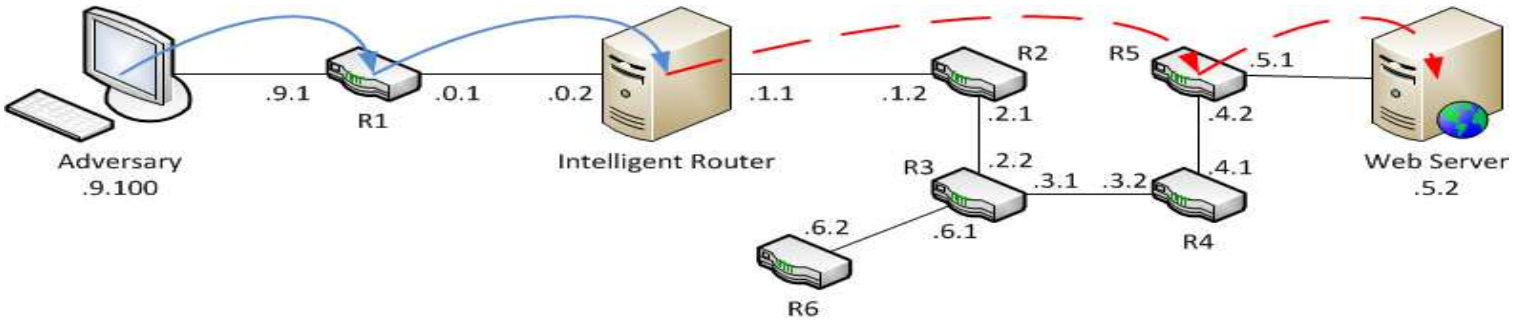
Candidate test topology in our lab (using GNS3)

True Topology



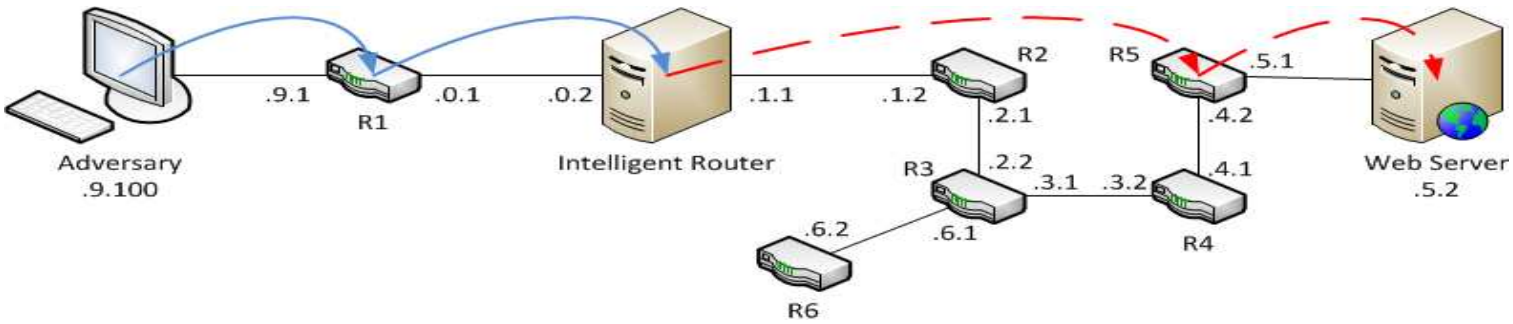

```
traceroute to 192.168.5.2 (192.168.5.2), 30 hops
 1  192.168.9.1  1.280  ms (R1)
 2  192.168.0.2  3.966  ms (Intelligent Router)
 3  192.168.1.2  5.997  ms (R2)
 4  192.168.2.2  10.097 ms (R3)
 5  192.168.3.2  12.135 ms (R4)
 6  192.168.4.2  14.330 ms (R5)
 7  192.168.5.2  16.109 ms (Web Server)
```

Random Topology




```
traceroute to 192.168.5.2 (192.168.5.2), 30 hops
 1  192.168.9.1        1.039 ms
 2  132.65.218.87      3.996 ms
 3  240.184.140.169    3.935 ms
 4  247.10.122.16      4.178 ms
 5  153.55.189.76      3.956 ms
 6  255.253.22.13      4.126 ms
 7  112.52.193.63      3.942 ms
 8  213.218.8.151      2.829 ms
    ...
```

Deceptive Topology




```
traceroute to 192.168.5.2 (192.168.5.2), 30 hops
 1  192.168.9.1  2.478  ms (R1)
 2  192.168.0.2  15.078 ms (Intelligent Router)
 3  192.168.4.2  22.520 ms (R5)
 4  192.168.5.2  32.739 ms (Web Server)
```

Outline

Does Topology Deception Already Exist?

- Relatively simple to perform topology deception
- Current mapping systems could be influenced by fake topology
- Only prior work we are aware of used virtual forwarding tables (VRFs) on a single router to encode a message in DNS PTR records
- Fundamentally different – packets are actually being forwarded

Prior Art?

VRF-Based DNS Tricks

```
traceroute to 216.81.59.173 (216.81.59.173), 30 hops max, 60 byte packets
13  Episode.IV (206.214.251.1)  65.780 ms  67.914 ms  68.976 ms
14  A.NEW.HOPE (206.214.251.6)  66.577 ms  62.461 ms  65.629 ms
15  It.is.a.period.of.civil.war (206.214.251.9)  63.648 ms  64.774 ms  66.707 ms
16  Rebel.spaceships (206.214.251.14)  65.418 ms  62.541 ms  62.739 ms
17  striking.from.a.hidden.base (206.214.251.17)  63.203 ms  63.160 ms  62.312 ms
18  have.won.their.first.victory (206.214.251.22)  62.553 ms  63.069 ms  63.364 ms
19  against.the.evil.Galactic.Empire (206.214.251.25)  63.543 ms  63.404 ms  62.960 ms
20  During.the.battle (206.214.251.30)  62.878 ms  62.742 ms  63.378 ms
21  Rebel.spies.managed (206.214.251.33)  62.808 ms  62.351 ms  62.075 ms
22  to.steal.secret.plans (206.214.251.38)  62.829 ms  63.266 ms  63.256 ms
23  to.the.Empires.ultimate.weapon (206.214.251.41)  63.585 ms  63.652 ms  63.671 ms
24  the.DEATH.STAR (206.214.251.46)  63.002 ms  63.124 ms  63.120 ms
25  an.armored.space.station (206.214.251.49)  63.095 ms  62.905 ms  65.614 ms
26  with.enough.power.to (206.214.251.54)  65.654 ms  63.630 ms  64.248 ms
27  destroy.an.entire.planet (206.214.251.57)  66.392 ms  66.425 ms  63.759 ms
28  Pursued.by.the.Empires (206.214.251.62)  63.874 ms  65.473 ms  64.433 ms
29  sinister.agents (206.214.251.65)  63.987 ms  63.978 ms  64.188 ms
30  Princess.Leia.races.home (206.214.251.70)  64.206 ms  64.750 ms  64.826 ms
```

Current Status

Work in Progress:

- MILCOM paper in submission
- Change deception granularity to be configurable on a per source and destination prefix
- Exploring potential deployment in OpenFlow/SDN

Future Work

Future Work:

- Maintain consistency with multiple network ingresses
- Faking load-balancing
- Realistic latency distribution
- Supporting UDP and TCP-based `traceroute`
- Preventing detection of deception
- Applicability to DARPA's "moving target defense" strategy?

Thanks! Questions?