Alibi Routing

Levin, Lee, Valenta, Li, Lai, Lumezanu, Spring, Chatterjee

SIGCOMM '15

Presented by Will Roever
Provable Route Avoidance

- Traceroute and ping expose likely subsets of nodes traversed from source ⇒ destination ⇒ source
- But... What if we want to ensure our traffic did NOT traverse a node in some part of the world?
- Useful if:
  - We suspect some intermediate entity is tampering with packets
  - We want to securely exchange public keys (Diffie-Hellman key exchange)

We need a proof of avoidance (i.e. an alibi)
Proof of Avoidance
Amounts to an alibi demonstrating the impossibility that some region was traversed, based on reasonable assumptions about the laws of physics.

P2P Overlay Routing System
Describes a demonstrably secure and efficient implementation that enables one to secure alibis, where possible.

It is not always possible to obtain such proof.
A Word: Detection vs. Prevention

- Goal of alibi routing is **detection** (a posteriori)
- Prevention would be ideal, but not a goal here
- Higher-layer protocols must decide how to handle case where no alibi can be extracted
- Alibi routing not a panacea:
  - Can’t avoid countries we are in
  - **Does not guarantee a copy of some packet is not transmitted to the region**
Alibi Conditions
Math not as bad as it looks!

\[
R(s, r) + R(r, d) \ll R(s, r) + \min_{f \in F} \{R(r, f) + R(f, d)\} \\
R(s, r) \ll \min_{f \in F} \{R(s, f) + R(f, r)\}
\]

Where: \( x \ll y \rightarrow \exists (\delta \geq 0) : (1 + \delta)x < y \)

<table>
<thead>
<tr>
<th>s</th>
<th>source</th>
</tr>
</thead>
<tbody>
<tr>
<td>d</td>
<td>destination</td>
</tr>
<tr>
<td>r</td>
<td>relay node</td>
</tr>
<tr>
<td>F</td>
<td>“forbidden” geographic region we’d like to avoid</td>
</tr>
<tr>
<td>f</td>
<td>any node in F</td>
</tr>
<tr>
<td>( R(\cdot) )</td>
<td>round-trip time</td>
</tr>
</tbody>
</table>
If we can find a relay $r$ such that the RTT from $r$ to $d$ is less than the minimum possible sum of RTTs from $r$ to $f$ and $f$ to $d$, we have an alibi from $r$ to $d$!

$$R(s, r) + R(r, d) < R(s, r) + \min_{f \in F} \{R(r, f) + R(f, d)\}$$

Condition 1:

If a packet arrives at $d$ with a signature from a proof-yielding $r$, we can say the packet has an alibi.
Condition 2:

\[ R(s, r) \ll \min_{f \in F} \{ R(s, f) + R(f, r) \} \]

If we can find a relay \( r \) such that the RTT from \( s \) to \( r \) is less than the minimum possible sum of RTTs from \( s \) to \( f \) and \( f \) to \( r \), we have an alibi from \( s \) to \( r \)!
How do we demonstrate these conditions are satisfied?

Requires identifying node(s) $f$ in region $F$ which minimize:

1. $\text{RTT}(s,f) + \text{RTT}(f,r)$
2. $\text{RTT}(r,f) + \text{RTT}(f,d)$
RTT\((q,n)\) has a theoretical minimum, defined as the time it takes a particle traveling at the speed of light to travel the great circle distance between \(q\) and \(n\):

\[
\mathcal{L}_F(q) = \frac{1}{2c} \times \text{ShortestDistance}(q,F)
\]
Some Important Caveats

› Relay must be far from forbidden region to be an alibi
› Latencies are variable ⇒ a relay that is an alibi at one time may not always be a viable alibi
› $\delta$ represents a tradeoff between safety and efficiency:
  › Increases with distance of relay from $F$ (+safety, -efficiency)
› **User implicitly trusts all peers that are outside $F$**
Alibi Routing: Protocol Design

› Supports queries of the type:
  \[ \{s, d, F, T\} \]

› User specifies \( F \) by defining a set of polygons with (longitude, latitude) tuples

› \( T \) is a set of target regions (probable alibi locations) used to guide routing toward the destination

› A point \( g \) is in \( T \) if it satisfies:

\[
(1 + \delta) \cdot D(s, g) \leq \min_{f \in F} \{D(s, f) + D(f, g)\} \\
(1 + \delta) \cdot D(g, d) \leq \min_{f \in F} \{D(g, f) + D(f, d)\}
\]

Where \( D() \) denotes great-circle distance
Target Regions: Italy → Norway

$F = \text{Germany}$

- $g$ sampled at $2^\circ$ lat/lon intervals; $T$ constructed as the union of triangles of 3 contiguous points
- $T$ shown for $\delta = \{0, 0.05, 0.10, 0.15, 0.20\}$
Alibi Routing: Protocol Design

- Each node maintains a list of known-active peers
  - Records GPS coords, RTTs (updated via polling)
  - List is shared with peers
- Each also maintains a subset of 32 peers as **neighbors**
  - Maximal diversity in terms of latency/geography
- **Critical**: Nodes cannot lie by understating latencies

\[ L(q,n) < L(q,f) \Rightarrow n \text{ not in } F \]

**NOTE**: if the above does not hold, we can only say that \( n \text{ may be in } F \)
Safety vs. Efficiency

Two key challenges in a node identifying the next hop in a potential alibi path:

- **Safety**: Avoiding $F$
- **Efficiency**: ensuring next hop makes the most possible progress toward a target location

**Solution**: choose neighbor who minimizes:

$$I_T(n_i) - I_F(n_i)$$
How feasible is this really?

› Using latency data collected from 425 PlanetLab nodes, authors look at feasibility of Alibi Routing for various values of $\delta$

Figure 4: Feasibility of Alibi routing for different forbidden regions. (Simulated deployment on PlanetLab.)
Relays are abundant

- Simulated deployment on 20,000 nodes
- Based on MaxMind IP geolocation database ("Geolite")

**Remember**: nodes in target region $\not\Rightarrow$ an alibi exists
Looking closer...

- PlanetLab hosts classified as possible alibis for all (s,d) pairs in the simulated deployment

**Centrality** in the routing ecosystem is crucial w.r.t. avoidance
As expected, we see a strong correlation between the min. distance of a source or destination from \( F \) and the number of possible relays in \( T \).
The Verdict

- **Success rate**: ~84% of source, dest. pairs have alibis for high $\delta$ in the MaxMind simulated deployment
- **Overhead**: avg. search cost less than 40 nodes

Figure 8: Time taken to find a relay for all PlanetLab source-destination pairs. (Implementation on PlanetLab.)
Closing Thoughts

- This is a complicated business...
- Common target areas? Does centrality make certain areas strong candidates for alibi paths?
- Would be interesting to see more detailed data regarding added latency required for AR.
- What are the next steps as we approach the problem of avoidance with the stronger goal of prevention?
THANKS!