# Alibi Routing

Aniruddha Shukla
ags4602@cs.rit.edu

Manan Joshi
mj5784@cs.rit.edu

Aakshaye M Gaikar
ag5308@cs.rit.edu

***Abstract*— In the past, there have been mechanisms through which users can understand where the packets they sent have gone. However, these mechanisms cannot provide indisputable proof that their packets have not passed through a particular part of the world *en route* to the destination host. The authors of the paper present Alibi Routing, which introduces the problem of finding evidence that packets and its response has taken a path that avoids a user-specified forbidden geographic region. Alibi Routing uses a peer-to-peer overlay routing system for finding alibis very efficiently and securely. *Alibis* are relay nodes that are chosen with certain timing constraints which when maintained, make it impossible to traverse both the relay node and the forbidden region. Proving that something did not happen can quite often be intractable, but the authors demonstrate a proof structure with low overhead based on speed of light propagation delays and GPS coordinates provided by the user.**

## I. Introduction

Earlier approaches such as record-route IP, overlay routing systems such as Tor or source routing bring to light the path a user's packet took. But, they do not allow users to determine or influence with proof that their packets did *not* go to a region. The authors of the paper introduce a concept known as *provable avoidance routing* [1]. Provable avoidance routing aims at detection rather than prevention which means it cannot assure a user that the packets sent will *not* traverse a given geographical region. It does not require modifying the existing routing protocols or even the underlying hardware. The proofs of avoidance are provided for each packet and can be established only *after* the packet has been sent and reply for it received. This is needed to confirm that the round-trip communication avoided the forbidden region.

Even though provable avoidance routing does not provide prevention, detection itself can be powerful. Censorship, which is a great threat to the Internet has many forms which includes not only dropping packets or logging of traffic but also packet spoofing. Censorship can occur not necessarily at the source or destination but at the regions that the packets transits through as well. Alibi Routing provides a way of avoiding the censor altogether using an orthogonal approach.

The authors of the paper make 2 main technical contributions. The first being the proofs of avoidance, which is a means of proving that a packet avoided a forbidden region. Secondly, they have designed and implemented Alibi Routing, a peer-to-peer overlay routing system to find alibis safely and efficiently. Alibi routing is secure because when trying to find alibis to avoid forbidden region F, it itself avoids F. It is efficient because it requires a few states and few hops and more importantly is incrementally deployable since it does not require public key infrastructure or switching hardware. It also does not require synchronized clocks. Alibi routing derives its proofs from local measurements of round-trip times (RTTs) and an estimate of source and destination GPS coordinates.

## II. Goals and Non-Goals

This section states what provable avoidance routing aims to provide and what it does not.

### A. Goals

- Alibi routing aims to prove that a packet must have avoided a forbidden region F after it has in fact happened. It does not guarantee that a packet will not traverse F.

### B. Non-Goals

- It does *not* seek to provide confidentiality. Alibi routing cannot guarantee that an adversary would never see a copy of the packet. This is because even if a proof is obtained that an adversary is not on the packet's round-trip path, it does not stop nodes on the path from copying and delivering the packets to an adversary.
- The algorithm does not guarantee that the packet will not travel through the forbidden region (F). It can only verify whether the path taken by the packet went through the forbidden region or not, after the fact.

## III. Solution Approach

- The first step is to setup the network topology. We have used GENI to set up our topology.
- JSON is the format used for message being exchanged over the wire. JSON has some overhead compared to packed binary data, but having the data in string form makes it easier to understand and debug the messages being exchanged.
- Alibi routing uses a peer-to-peer network. Whenever a node comes online it communicates with bootstrap nodes to get neighbor information. So the next step is to configure the bootstrap nodes for each participating node.
- After bootstrapping, the nodes needs to find information about their neighbors. This process includes calculating the RTT to all neighbors, choosing the best neighbors based on latency and diversity criteria and starting exchange of messages with them.

- Each node in Alibi Routing keeps track of the neighbors of its neighbors (2 hop neighbors). So, next step is populating the 2 hop neighbors. Each neighbor is requested for its list of neighbors.

### A. Trust Assumptions

Alibi routing assumes that all participating peers outside of the forbidden region follow the protocol *correctly*. This is a critical trust assumption, without which it would not be possible to prove avoidance.

### B. Neighbor Maintenance

Every node in the peer-to-peer system has a fixed set of neighbors depending on the topology we created in our GENI deployment. The neighbors should be diverse in terms of latency and geography in order to increase the probability of finding peers that can route queries towards a target region and at the same time, stay away from the forbidden region. To make this possible, each node maintains two sets of peers: 1) a set of known active peers 2) a set of $n$ neighbors which $p$ uses when processing queries.

It is necessary to maintain neighbors which are diverse in two aspects.

- Latency diversity: Each node obtains round-trip time (RTT) measurements in their known active set. This is done by pinging peers when they first find each other and in fixed intervals thereafter. The RTT measurements are recorded and stored. When a peer obtains a new RTT measurement, its set of known active peers is updated to store the least redundant node and its RTT. The neighbor with greatest redundancy is removed. The redundancy is calculated as the inverse of its relative difference to its neighboring values.
- Geographic diversity: We would like to have neighbors with diverse *bearing*, so that there aren't multiple neighbors that take us in the same direction. Neighbors are considered geographically redundant if they have the same, or very similar bearing.

The above diversity measures guide an Alibi Routing peer's decisions as to what neighbors to add or drop.

Joining: To join, a node *n* first contacts a peer it knows and obtains its know active-set. *n* then pings these nodes with random nonce and asks them for their GPS coordinates and adds them to his own known-active set. This is used to construct his own neighbor set. A neighbor set of a new node is likely to be different from the node that bootstrapped it with the exception the bootstrapped node is close to one another.

### C. Forwarding

The packets in Alibi Routing can only be forwarded if they meet a few standard conditions.

- The packet cannot go to the forbidden region and come back without noticeable increase in delay.
- RTT to the next hop should be significantly less than the RTT to the nearest point in the forbidden region.
- If the packet discovers a neighbor in the safe region it should choose that neighbor immediately.
- If the node is in viable distance the route should progress. This progress should be such that the route minimizes the distance to the target node while at the same time maximizing distance from the forbidden region.
- If while proceeding no more safe neighbors are found, the Alibi route fails.
- Having diverse neighbors helps in achieving the desired forwarding.

### D. Routing

- Every node will have a list of neighbors and its 2 hop neighbors along with the candidate neighbors and will also maintain all these lists.
- At regular interval each node will transmit gossip messages to its neighbors, so that it can periodically update all the neighbor lists that it maintains.
- Alibi route query will only be forwarded to a safe next hop.
- Upon receiving query a node will forward it to the next safe hop and will wait for a response.
- If an Alibi route is found, the response will take the same path back to the source.
- If at the end the source receives a response, it can be said that an Alibi route exits or else a timeout will result into failure and denote that there is indeed no Alibi route between the source and the destination.

## IV. RESULTS

The deployment topology is as given in Fig 1. The nodes are at

- Seattle (S)
- University of California, Los Angeles (U)
- University of Michigan (M)
- Rutgers University (R)
- University of Chicago, Illinois (I)

Figures 2 through 5 show the results of querying a route from a given source to destination, with the forbidden region set to Illinois.

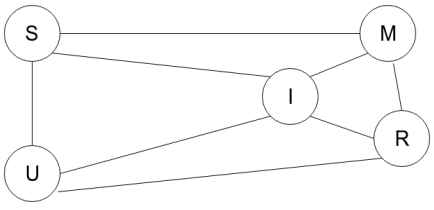


Fig. 1.


Fig. 2. Failed query result: Port forwarding issues on the node at Michigan


Fig. 3. Success query result: Able to detect a route from Rutgers to Washington


Fig. 4. Success query result: Able to detect a route from Michigan to Rutgers

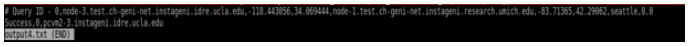


Fig. 5. Success query result: Able to detect a route from Los Angeles to Michigan

Our topology has its limitations. We are unable to exercise the test case of having a next hop that is not in the target relay zone. We attempted to construct a topology that would fulfill the criteria for this execution path, but faced errors during creation.

## V. Conclusion

This project tries to show that the concept of avoidance routing is achievable when given a destination and region to avoid and it provides proof after the fact that a packet and its response did not traverse the forbidden region. To demonstrate the feasibility of implementing this project, we have implemented Alibi Routing. Alibi Routing assumes that nodes outside the forbidden region are trustworthy in reporting their geographic locations and in vouching for neighbors that are too nearby to be in the forbidden region. It leverages this assumption to direct relay discovery queries toward a target region in which alibis might reside.

## References

[1] D. Levin, Y. Lee, L. Valenta, Z. Li, V. Lai, C. Lumezanu, N. Spring, and B. Bhattacharjee, "Alibi routing," in *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, (New York, NY, USA), pp. 611–624, ACM, 2015.