1 Keywords

anonymity random topology restricted topology random paths lookup peer-to-peer

2 ShadowWalker: peer-to-peer anonymous communication using redundant structured topologies

Prateek Mittal, Nikita Borisov

This article presents a low-latency, P2P anonymous communication system based on a random walk over a redundant structured topology.

The sell is that current anonymous communication networks like Tor are centralized and are strained by current demand levels. By providing a P2P alternative, we can improve the performance while maintaining anonymity.

The relevance to our paper is that if botnets were able to communicate anonymously, this would greatly reduce the risk of remediation or removal.

2.1 Solution Highlights

The properties of their solution are as follows:

- the system relies on so called shadow nodes. Shadow nodes redundnatly verify the correctness of a given nodes' routing table and certify it as correct. Such certificates can then be used to check the steps of a random walk through the network. By using certificates rather than online checks, information leak attacks can be avoided.
- they claim that the design is effectively able to prevent route capture attacks by employing a small number of shadows per node.
- an extension to this system was developed that defends against selective denial of service attacks and improves performance, at the expense of some anonmity protection.

2.2 Background

Anonymous communication systems can be either low- or high-latency systems. High latency systems are secure even against a powerful global passive adversary, but typically takes hours to transmit messages, or in other words they are impractical.

Tor is an example of a low latency system. users download a list of servers from a central directory and build anonymous paths using onion routing. The weak points of Tor's architecture are how it requires users to have a global view of all servers and for its centralized directory structure.

Peer to Peer designs have include:

1. Random Paths Using Lookup (Salsa): a circuit is built by selecting 3 random nodes and connecting them. A secure lookup operation is used to locate forwarder nodes; the lookups use checks to limit the bias of the lookup operation but make Salsa vulnerable to information leaks. This results in a tradeoff between robustness to active and passive attacks, and as a result, Salsa does not provide an adequate level of anonymity.

2. Random Walks on Restricted Topologies:

   - (Tarzan): relays are connected into a restricted (non-clique) topology. In Tarzan, each node has a small set of mimics and all circuits are created on links between mimics. The use of a restricted topology has the advantage that the local view at each hop is sufficient to extend the circuit, and covers traffic to be sent along all links in the topology. However, each node requires a global view of the system in order to verify that paths are constructed correctly. This is done using agossip protocol, which puts an upper cap on the number of nodes that the network can tolerate (around 10000).
   - In MorphMix, such scaling concerns are resolved using a randomized, unstructured overlay between relays, with circuits built on paths along the overlay. However, it needed to be able to trust nodes to correctly specify its neighbours when extending hte circuit. Thisct is done using witness nodes and collusion detection mechanisms. However, the issue here is that colluding adversaries share internal states and thereby bypass the detection mechanism.