NOVA SCHOOL OF
SCIENCE & TECHNOLOGY

Reliable Distributed Systems

Trust-Aware Tor Path Selection (TAPS)

(Ivo Farias, 70621)

Introduction

Tor is a widely used low-latency anonymity network, vulnerable to "first-last" correlation attacks by adversaries able to observe both the entry and exit segments of a user's path. To address this, the Trust-Aware Path Selection (TAPS) algorithm was proposed, allowing users to make trust-based decisions in selecting relays. This project implements a simplified version of TAPS using the "TrustAll" model and the "Countries" adversary policy.

The core objective is to calculate relay trust scores based on the user's perception of each country's surveillance threat and avoid selecting circuits that could be compromised by collaborating countries. The system processes relay metadata (tor_consensus.json) and configuration input (client_input.json), and returns a bandwidth-weighted guard-middle-exit Tor circuit.

Key Decisions

1. Simplified Threat Model
Countries are assumed to observe all traffic originating within their borders and can form alliances with shared observation capabilities. This abstraction makes trust evaluation tractable and straightforward.

2. Alliance Expansion Logic
We developed a recursive function to resolve indirect alliances between countries. This ensures that countries indirectly connected via multiple alliance hops are properly accounted for.

3. Trust Weighting
Security is computed as the proportion of trust not compromised. If a country appears on both path segments and is distrusted, it reduces the trust score significantly. Relay selection prefers relays not associated with such compromised paths.

4. Bandwidth-Weighted Selection
To maintain network performance, even among safe and acceptable relays, selection is made probabilistically in proportion to bandwidth, balancing anonymity and throughput.

5. Trust Scores

For each country we stored the maximum trust value across all alliances where it appears.

6. Guard Relay Selection Logic

In the absence of explicit guard flags in the consensus data, the implementation classifies all non-exit relays as potential guards.

Trade-Offs and Challenges

Security vs Availability

In scenarios with high distrust (e.g., where most relays are in distrusted countries), the number of secure paths can become extremely limited or nonexistent. To mitigate this, we fall back to “acceptable” relays if “safe” ones cannot meet the required bandwidth fraction.

Middle Relay Randomization

Unlike guards and exits, middle relays are selected randomly, assuming they do not affect correlation risk (they’re not the guard or exit relays or part of their families).

GeoIP Reliability

The trust logic heavily depends on correct IP-to-country mapping.

Results

The system successfully outputs guard-middle-exit paths that avoid adversarial countries according to user-defined trust. Path selection succeeds unless all candidates are deemed insecure.