Abstract

Nada Mostafa Abdeaziem

Aggregating Local Metrics for Global Trust Calculations in the TOR Network

This paper discusses the design and implementation of a distributed trust calculation mechanism that allows users in the peer-to-peer TOR anonymity network to determine whether not the nodes that comprise the TOR network are malicious. This is done through a cooperative algorithm that allows individual nodes to measure the trust of the TOR nodes they communicate with. The paper measures the performance of this algorithm and shows that the algorithm can accurately identify several kinds of malicious nodes in the TOR network. This paper will focus on the following security issues: the problem of self reported bandwidth and uptime that can lead to low resource attack, geographical location and Denial of service (DoS) attack and how to aggregate all these criteria in one value that indicate whether not the onion router is malicious. The aggregation is performed using two different techniques, each of which uses the exact same aggregation methods except for geographical location. The first method, which excludes entire geographical locations, produced slightly worse results than the second method, which assigned a scale between 0 and 0.99 for each geographical location to signify its trust