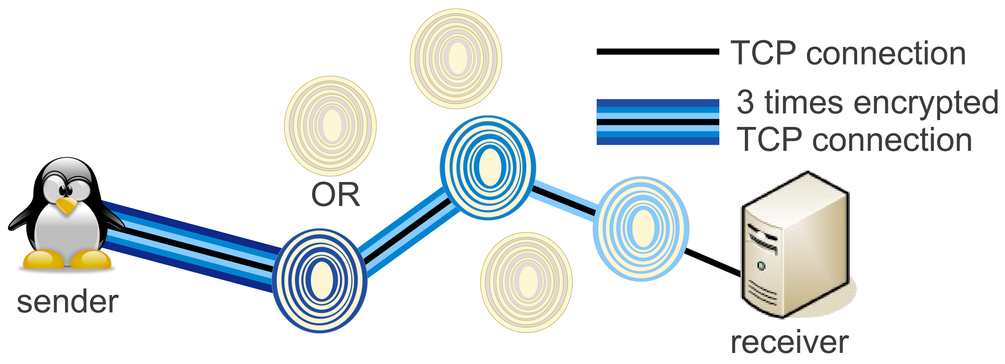
Splitting the Tor Network
Potential Challenges Considering the Gold Star Scheme

Benedikt Westermann, Pern Hui Chia

Tor – The Onion Router

The Onion Router network, better known as Tor, is the most popular and by far the biggest anonymity network in the world. **More than 2000 servers**, so-called **Onion Router (OR)**, build the core Tor network and help to anonymize the traffic of **hundreds of thousands of users**. With Tor, only the user knows which website he visits. All other parties know, either the sender only, the receiver only, or neither of them. This is achieved in Tor by **routing the user traffic over various ORs** and by **making the users as indistinguishable as possible.**



The routing process works as follows. The first OR in a path through the network knows the sender, but it cannot read the address of the receiver as the message has **several layers of encryption**. The first layer of encryption is removed by the first OR before forwarding the message to the second OR. The second OR removes another layer of encryption and continues the forwarding. Eventually, when the last OR in the path receives the message, it removes the last layer of encryption, reads the address of the ultimate receiver, and forwards the plain message to the receiver. The last OR knows about the receiver but it is not aware of the sender.

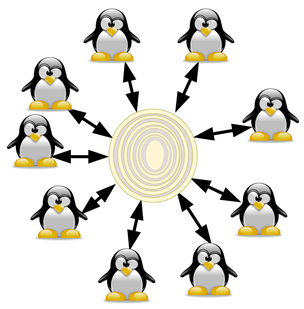
Major Challenges

Finding Volunteers

All ORs are operated by volunteers who do not get any benefit in doing so. On the contrary, they have to pay for the traffic and the server. Moreover, some operators have been approached by law enforcement agencies as some users misused Tor for illegal activities. Naturally, **it is hard to find volunteers**.

Scalability of the Tor Network

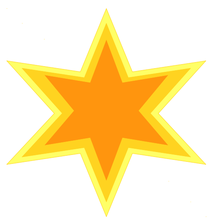
Tor is an **overlay network**. Users need to know the addresses of the ORs. To make the users as indistinguishable as possible, it is wise to provide all users with the **full view** of the Tor network. In general, the highest anonymity is achieved when all users know about all ORs and can use any subset of them for routing. Yet, this **does not scale.** On the other hand, providing the users with a **partial view** only, **can harm the anonymity** of the users [2].



Two Proposed Solutions

Gold Star – Building Incentives into Tor

To motivate users to provide an OR, Ngan et.al. [1] propose the **Gold Star** scheme which gives a Gold Star to the best performing ORs. A Gold Star entitles the operator to build a path through the network with higher bandwidth and lower response times. They argue that the scheme can appeal to Tor users to operate an OR.

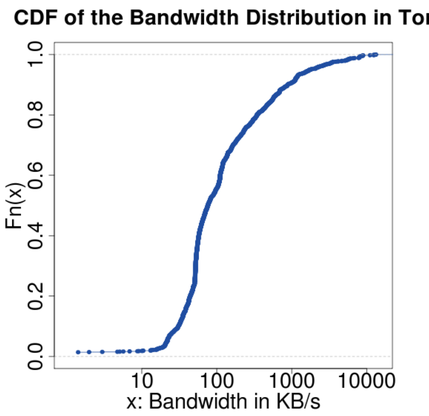


Splitting Up the Tor Network

In [2], the authors demonstrate that providing users with a partial view of the Tor network makes them vulnerable to several attacks. They concluded that **simply splitting an anonymity network into two** is most often **the best trade off between anonymity, performance and distribution costs**.

What If We Combine the Two?

While "s*plitting the Tor network"* and the "*Gold Star"* schemes are sound when considered separately, the results may change when the two are combined. The situation is tricky given that a small set of top performing ORs currently determines the overall performance of the Tor network. **18% from the 2140 active ORs actually provide 82% of the total available bandwidth (~904 MB/s).**



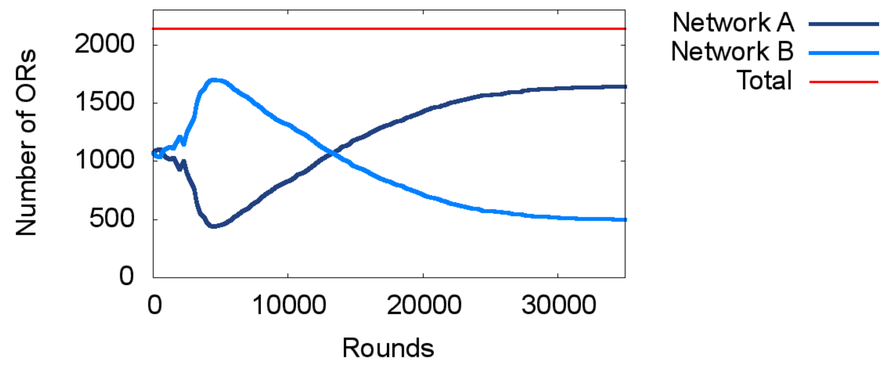
Our Intuition

ORs without a GS in one network might get a GS in the other network. A rational OR operator would switch in this case to the other network in order to obtain a higher bandwidth. We hypothesize that, without a good policy, splitting the Tor network while using the GS scheme can lead to an **undesired competition between the sub-networks** resulting in an imbalanced distribution of network size and bandwidth. The advantage of splitting the Tor network diminishes.

Simulation

We downloaded the directory information of the Tor network (e.g., the name of each OR together with the bandwidth that was observed at the corresponding OR) to setup a simple model that mimics the real life scenario in Tor. We ran a simulation with the following rules:

- The top 87.5% performing ORs in each sub-network receive a GS.
- Having a GS is always better than having no GS.
- With a GS, the operator enjoys a bandwidth equal to the median of the bandwidth of all GS-ORs.
- An OR operator switches to another network if he gets a GS that results in a higher bandwidth using that network.
- The bandwidth enjoyed by ORs without a GS is the same in both sub-networks assuming that the normal Tor users (i.e., non-OR operators) will distribute their traffic such that the bandwidth experienced in both sub-networks is roughly the same without a GS.



The simulation model stabilizes with **one sub-network having 84.4% of the total bandwidth** (i.e., 763 MB/s). This imbalanced split has adverse effects on the distribution costs and the provided anonymity.

The Next Steps

We aim to analyze the conditions under which both sub-networks can balance themselves with similar properties in equilibrium. **Game theory** can be a suitable tool for further investigations. To verify the results of the analytical analysis, it is also important to extend the simulation model and to find better estimators for the bandwidth experienced by the ORs with and without a Gold Star.

Our simple model here demonstrates that problems can arise when both solutions are combined without any intervention. This underlines the importance of a thorough analysis before the Tor network is split into two to cope with the increasing distribution costs.

References

1. Ngan, T.W., Dingledine, R., Wallach, D.S.: Building incentives into Tor. In Sion, R., ed.: Financial Cryptography. Volume 6052 of Lecture Notes in Computer Science., Springer (2010), 238 - 255
2. Danezis, G., Syverson, P.F.: Bridging and fingerprinting: Epistemic attacks on route selection. In Borisov, N., Goldberg, I., eds.: Privacy Enhancing Technologies. Volume 5134 of Lecture Notes in Computer Science., Springer (2008) 151–166

NTNU
Norwegian University of Science and Technology

http://www.q2s.ntnu.no
westermann@q2s.ntnu.no
chia@q2s.ntnu.no

Center for Quantifiable Quality of Service in Communication Systems
Center of Excellence
Norwegian University of Science and Technology