Abstract

The Tor network suffers from slow speeds due to oversubscription. Server-client parity is suboptimal because ”hosts” have little incentive to provide bandwidth to ”clients,” since bandwidth is expensive and hosts are volunteers. We propose a system for deploying a secondary Tor network that incentivizes bandwidth contribution using the Bitcoin protocol for both payment and bandwidth monitoring verification. We also introduce the concept of ”batching” of clients into ”batches” that use distributed consensus algorithms for anonymously assigning relay paths to clients, which significantly increases resistance to Sybil attacks.

TorCoin
Yale CPSC 490 Proposal

Richardson, Miles
miles.richardson@yale.edu

Ghosh, Mainak
mainak.ghosh@yale.edu

February 6, 2014

1 Team Members and Background

1.1 Miles Richardson, CS, 2014

- Project-Relevant Language Experience: Python, C, C++
- Project-Relevant Domain Experience: Running VPN, Proxy Business

1.2 Mainak Ghosh, EECS, 2014

- Project-relevant Language Experience: Ruby, C

2 Background Information

2.1 The Internet Empowers Citizens

The past decade has seen unprecedented empowerment of global citizens. Never before has it been so easy to share, communicate, and collaborate. Less than a century ago, sending a simple photo from China to the United States took weeks or months. Now, with the press of a button on a mobile phone, a single person in China can distribute a video to millions across the globe in a matter of seconds.

Such ability arms citizens with unprecedented political and social power, and forces accountability onto authoritarian governments. The Arab Spring exemplified the effect of social media on citizen empowerment, as crowds of millions in Egypt, Tunisia, Libya, and other Arab world countries took to the streets in mass protests of authoritarian regimes.

Unfortunately many governments, including China, Cuba, and some Middle Eastern regimes, have understandable resistance to such online social empowerment. So they employ complex censorship systems to quell any kind of power.

China, for example, uses deep packet inspection and address filtering in order to stop the spread of certain keywords.

2.2 Provide Anonymity, Resist Censorship

Tor, specifically the Tor network, is free software that uses a special “onion routing” protocol for routing Internet traffic while protecting anonymity and resisting censorship. It routes requests through thousands of volunteer nodes such that no node or outside observer can de-anonymize the request.

In the words of the NSA, Tor is “the king of high secure, low latency internet anonymity,” and “no contenders for the throne in waiting.” Any improvement to Tor creates more obstacles for the NSA, which serves as a nice symbol for adversaries of anonymity.

3 Problem Statement

Tor is slow. The slow speeds on the Tor network are a result of oversubscription to the network. As more users join the network without exit relay parity, bandwidth costs increase over the same number of machines, so speeds slow. As the network grows, it requires faster exit nodes. But exit nodes and bandwidth are expensive, the the Tor network is comprised of volunteers who are not compensated for providing bandwidth and computing resources.

4 Proposed Solution

We will build a system that enables deployment of a secondary, monetized Tor network. Independent communities can launch a private or public network that routes traffic over Tor, but “clients” (bandwidth consumers) pay “hosts” (bandwidth providers) per bit of bandwidth. TorCoin will anonymize payments such that no host knows which client is paying him. Theoretically, this secondary network would have faster speeds than the main Tor network.

5 Major Obstacles

5.1 Verifiable Bandwidth Monitoring and Consensus

One of the major obstacles to implementing a reliable incentive system has been the problem of verifiably monitoring bandwidth in a scalable and anonymous manner. Since relays cannot be trusted to self-report their bandwidth contributions, we will build upon the research of Eigenspeed to determine each relay’s contribution. Our novel contribution of using the Bitcoin protocol for exchanging bandwidth and money will solve many of the decentralization problems presented by Eigenspeed.

5.2 Coin Distribution

In general, this is a major obstacle for us, but we can solve it by either:

1. Using every nth packet as a 'token'. These tokens are then verified using a consensus algorithm by all the neighbours of the relay in question. Thus, the more bandwidth the relay serves, the more coins they will get.
2. Using Eigenspeed as a central trusted authority. The Eigenspeed authority will distribute the coins based on its estimate of the relays in the network.

We intend to use the decentralized token distribution method as it corresponds to the Bitcoin mining model. This also reduces the need for a trusted central authority in our Tor network.

6 Prior Research

Two papers address major obstacles we will face, which we address in the "major obstacles" section. These two papers seem the most relevant to our research. Links are in the references section.

6.1 LIRA: Lightweight Incentivized Routing for Anonymity

Lira is a lightweight system providing "performance incentives for users to contribute bandwidth to the Tor network." It uses coins, similar to "in game currency," to distribute payment. Lira uses coins with tunable probability of being right, and clients can guess lottery tickets with probability, p of being right.

Lira provides a nice base of prior research for us to build upon. We will adopt some of the work, and also improve upon it by introducing the Bitcoin protocol into the system, enabling us to gain from its advantages.

6.2 Eigenspeed: Secure Peer-to-peer Bandwidth Evaluation

Eigenspeed is a peer-to-peer consensus building algorithm for monitoring bandwidth over a network, specifically implemented for Tor. Unfortunately it requires a central authority for computing Principal Component Analysis operations. While we believe these operations could be decentralized, we are not interested in extending Eigenspeed. Instead, we will exploit properties of the Bitcoin protocol to allow for bandwidth monitoring that is sufficient to generate payment tickets.

7 Novel Contribution

We have two novel contributions: we exploit the bitcoin protocol for use as a bandwidth accounting mechanism, and we introduce a concept of client batching based on partially contributed randomness for resistance against Sybil attacks.

7.1 Batching of Clients

We modify the directory server to randomly group clients wishing to use the TorCoin network into batches of size n. These batches then use a consensus algorithm to derive a common relay list. For each client, the "batch" chooses a list of three relays using a decentralized random algorithm that is seeded by each client in the batch.

- The batch then communicates to each relay the list of clients it is supposed to connect to.
- The relays only communicate with these clients, and no other clients.
- Each client now has an ordered triple of the relays it can connect to. It now proceeds to communicate using the existing Tor protocol.

This scheme requires small modifications to the tor directory server code (grouping clients into batches), client code (path selection algorithm), and relay servers (to accept/deny connections from certain clients). We will also need to build a separate, localized layer on top of the relay and client code for the purposes of accounting.

7.2 Bitcoin for Bandwidth Accounting

We propose a modification of the 'proof of work' used in the Bitcoin protocol. Instead of cracking hashes of a given number of ciphers as proof of work to produce a coin, we will use the bandwidth transmitted by a relay. We hope to implement the monetization procedure by a direct translation of the Bitcoin protocol so that every nth packet generated by a client is a special token. When it is received by a relay, it can be converted into a coin and is added to the TorCoin blockchain, with the relay as the owner.

8 Security Considerations

Robustness under attack: The initial decentralized relay selection mechanism is robust to groups of adversaries colluding to attack the network. If the adversaries control up to half the network, there is a probability of only 1/16 that an adversary client gets a path of three colluding relays.

A separate rate-limiting mechanism can then be deployed to detect dishonest relays and assign them a lower weightage in the path selection procedure. An independent verification authority, such as one based on Eigenspeed, could be used to detect these discrepancies.

9 Deliverables

- Modified Tor client. We will wrap the existing Tor client with a layer that generates and injects a token into the client's packet stream at a given frequency. These tokens form the basis of the proof-of-work concept for the TorCoin protocol.

- Modified Tor relays: We will also wrap the existing Tor relays with the packet inspection layer that can generate TorCoins in proportion to the bandwidth served by the relay.
- TorCoin protocol: The Bitcoin protocol must be modified to accept our revised proof-of-work concept.

10 Division of Work

We are allocating a few blocks of hours per week when we will meet and pair-program most of the major modifications we need to make. This will give each of us a holistic understanding of the entire codebase, ensure accountability to each other, and increase productivity. We will have distinct areas of focus. Miles will focus on Tor client modifications and implementing the TorCoin protocol with the novel proof-of-work, while Mainak will focus on implementing the Tor relay selection protocol and consensus-based authorization of clients.

11 References

- http://cs.gmu.edu/~astavrou/research/Par_PET_2008.pdf
- http://www.ohmygodel.com/publications/lira-ndss13.pdf
- https://bitcointalk.org/index.php?topic=62107.20
- http://www.reddit.com/r/Bitcoin/comments/1f97um/what_about_a_torcoin_that_would_help_secure_and/
- https://www.usenix.org/legacy/event/iptps09/tech/full_papers/snader/snader.pdf
- http://www.bitcloudproject.org/