On the Current Feasibility, Incentives, and Social Implications of Tor Monetization

Rob Jansen[1], Miles Richardson[2], Mainak Ghosh[2], and Bryan Ford[2]

[1] U.S. Naval Research Laboratory, Washington, DC
{rob.g.jansen}@nrl.navy.mil
[2] Yale University, New Haven, CT
{miles.richardson, mainak.ghosh, bryan.ford}@yale.edu

Abstract. The scalability of the Tor Anonymity Network suffers from the lack of an incentive to volunteer bandwidth resources, which are required for the system to operate effectively. This paper identifies the challenges and issues involved in producing such incentives, and proposes an architectural design with acceptable trade-offs that can be realized with mostly existing technologies.

1 Introduction

Tor is the most popular deployed anonymous communication system, currently transferring over 8 GiB/s in aggregate [1]. The bandwidth that Tor requires to function is donated by altruistic volunteers at a cost without any direct return on their investment. As a result, Tor has primarily grown through the use social and political means. It is a commonly held belief in the Tor community that utilizing volunteer resources without providing an incentive to contribute is not a viable long-term strategy for growing the network. How to recruit new bandwidth providers to the Tor network while maintaining anonymity is a well studied problem [2–8]. However, none of this work has led to any of a number of practical changes in Tor that would be required to move to an incentive-based resource model for a variety of reasons.

This paper has two major goals:

1. to identify the requirements, challenges, and trade-offs in designing an incentive scheme for the popular operational Tor Network; and
2. to propose an incentive-based Tor Network architecture with acceptable trade-offs while presenting an approach to realizing it with mostly existing technologies and some additional development.

We hope to illuminate the challenges and research problems in a way that will provoke useful discussion in the community while creating a useful base for future research in this area.

We begin in Section 2 by identifying the requirements and challenges involved in designing an incentive scheme for Tor while discussing the potential impacts that various design decisions may have on the existing network and its operators. We then propose a technical architecture based on existing technologies

in Section 3, discuss related work in Section 5, and present several remaining research problems while concluding in Section 6.

2 Requirements

A Tor incentive system that rewards volunteers for providing useful network services presents numerous requirements and challenges, both technical and social. In this section we briefly identify the major technical problems that we believe such a system should solve, while noting that all of the solutions should happen "offline" so as to minimize the interference with Tor's low-latency communication design. Please see Section 4 for a discussion of the social challenges involved in deploying a Tor incentive system.

Proofs of Useful Service A system that rewards users for serving the network should be able to prove that those services were in fact rendered. Ideally, the proofs of service would be publicly verifiable so that any member of the distributed network could validate the utility provided by any other member.

Rewards for Providing Service Members that contribute to the system should be rewarded for their contributions in proportion to the amount that was contributed. Ideally, the reward should have internal value in that a member can use it to achieve a desirable system service or attribute.

Accountability The system should provide a way to account for the rewards obtained by each member, and provide facilities to exchange rewards for desirable services. Double spending of rewards should be prevented or detected and handled. Ideally, the process of accounting for rewards should be publicly verifiable in order to eliminate reliance on centralized entities.

Preserve Anonymity The system should not introduce new attacks on the anonymity Tor offers to its users. As such, the solution to providing accountability and exchange of rewards should not link users to their past network usage activities.

Deployability The system should integrate well with the existing Tor network in order to maximize the utility provided to existing users and leverage the existing infrastructure and community. Ideally, the system components will be modular to allow them to be incrementally deployed with the existing Tor network.

3 Proposed Architecture

We now discuss the main components necessary to realize a practical Tor incentive system while identifying some open research and development problems.

3.1 Overview

We propose a system that measures bandwidth contributed to the Tor network to produce incentivise the addition of nodes to the Tor network. The system measures the bandwidth contributed by each relay in the Tor network and rewards them with a 'TOrCoin'. A Torcoin is an AltCoin that uses a bandwidth-intensive protocol as its proof-of-work. Thus, to produce a TorCoin, a relay must

have transmitted a certain amount of Tor traffic. To reduce the system's vulnerability to attackers and possible reduction of anonymity, we also utilize a system of 'Ephemeral Paths' to randomly assign relays to clients. These TorCoins can then be traded at an exchange for other AltCoins or other goods. This forms the basis of our incentivization scheme. This is different from systems that propose differentiated service [9, 10], since we do not propose to make the clients pay for access to the network. The coins are a byproduct of the usage of the system.

3.2 Ephemeral Paths

We propose the novel idea of ephemeral Tor networks, where a *group* of n clients at any given time form a consensus on an assignment of n routes to n clients, such that each route is publicly verifiable but privately addressable. We adhere to the following constraints:

- No client in the group can generate its own route.
- Every resulting route has a unique public key.
- No client in the group can know the route assigned to another client in the group.
- Any client can verify that a given public key represents a route assigned to a client in the current group.

The Tor directory servers will create the groups using the temporal locality of the clients connecting to them, but also ensure that their is geographical and other diversity in a group. This is to ensure that adversaries cannot deterministically place themselves in a single group by connecting at the same time. The Tor directory server will then initiate the setup protocol amongst the clients in each group. Each group will then perform a series of Neff Shuffles to produce a random combination of routes for each client in the group. This will be combined with El Gamal encryption to preserve anonymity within the group.

Decentralized Neff Shuffle for Consensus Tor Route Assignment to n Clients We perform a series of Neff shuffles so that each client in the group is assigned one *route* consisting of an entry, middle and exit relay. The route also has a publicly verifiable shared secret. That is, a route can collectively sign a TorCoin (explained later) such that any client in the group can verify that the signature came from a route assigned to another client in the group.

Implementation of Neff Shuffle THIS SECTION NEEDS TO BE MADE CLEARER / DIAGRAM

The clients are numbered 1 through N

Entry relays 1 to Me;

Middle relays: 1 through Mm;

Exit relays: 1 through Mx.

1. Each list of relays and clients goes through an independent Neff shuffle. The shuffled lists are concatenated, producing a shuffled 4xN matrix. Each client will have one row assigned to it, which only that client can verifiably associate with. This row represents the route for that client.

2. Each client can use their own private key to find out their own row and assigned relays after the shuffle, but no one else can.

3. The directory server generates a public and private key for all members of the row. This functions as the shared secret for the route.

It may be possible to use cryptographic accumulators along with the Neff shuffle. In that case, it will not be necessary to keep all the public keys generated in (4). Instead, the keys may be used to generate a cryptographic accumulator and this accumulator can be used to provide a zero-knowledge verification of group-membership.

We can then generate a publicly verifiable shared secret amongst the relays in any given route (a row in the 4XN matrix). That is, a route can collectively sign a TorCoin such that any client in the consensus group can verify that the signature came from a route assigned to another client in the consensus group.

Proof of Bandwidth Once the routes are setup, we can prove bandwidth transfer through the following protocol: Every n Tor packets, the client sends an extra packet (the Torcoin packet) containing an hash attempt likely to generate a TorCoin. Relay A gets it, generates a temporary private key Ka (generated using the route shared key) and hashes the received packet and this key. It then forwards it to B, which does the same thing, with its own private temporary key Kb. Similarly on to C. C can now add its own Kc, and if it generates a hash with a given number of zeros, it can claim to have found a TorCoin.

```
Client sends to A: T0 (its hash attempt)
A sends to B     : Hash(T0 + K1) = Ta # K1 is A's temporary private key.
B sends to C     : Hash(Ta + K2) = Tb # K2 is Bs temporary private key.
C computes       : Hash(Tb + K3) = Tc # K3 is Cs temporary private key.
C sends to B     : (Tc, K3) to verify.
B sends to A     : (Tc, K3, Tb, K2) to verify.
A sends to client: (Tc, K3, Tb, K2, Ta, K1) to verify.
Once the client has verified the hash, we can confirm that the data has made a
round trip through the route. This completes the proof of bandwidth.
```

TorCoin We can also implement an AltCoin based on the proof-of-work concept in the following manner:

```
If (Tc = '000...')
  If the client succesfully verifies the hash
    It adds the coin to the blockchain with the following information:
    1. Clients public key
    2. Route Shared key (Lets any other group member verify that the route is
       genuine. See accumulator/Neffs key.)
    3. TorCoin Hash
    It then gives 1/3rd of the coin to each of the relays in the route. (If the
    client is rogue, can we identify and kick the client off?)
```

3.3 Robustness to attack

The entire reason for constructing the elaborate ephemeral routes algorithm is to make the Torcoin system robust to attackers. Due to the random group selection system, it is hard for attackers to deterministically place themselves in a group. In addition, because the attacker needs to control all four components fo a route to mint a TorCoin fraudulently, even 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. In practice, gaining control of half of the entire Tor client and relay network is practically impossible. A separate rate-limiting mechanism can 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.

4 Discussion

TODO!–this section is currently merely an outline of topics for discussion

4.1 Path to Deployment

If it is run outside of Tor it may be better for experimental purposes, but longer term it would be nice not to partition the network.

How do these options this affect the anonymity sets? Will it always be possible to split the sets anyway due to the fundamental nature of diffserv scheduling?

Deploy in Existing Tor Network Write Tor proposals, get all the new features blessed by the Tor developers, integrate into existing network.

New and Separate Anonymity Network Fork Tor and add the new features. Create a separate network that does not interact with the existing network.

New Anonymity Network used with Tor Run a separate network that is 'attached' to the existing network. In other words, the new network interoperates with Tor by having two consensus files, etc. Then, when people wanting to use the coin mechanism use the new consensus to choose relays from the new network, and non-payers use the Tor consensus to choose circuits in the existing Tor network.

As it is important to minimize the loss in anonymity to the existing Tor users, we propose the deployment of a secondary experimental Tor network that will separate the incentive design and its risks from the existing network. Those participating in the incentive scheme will choose relays from a new consensus produced by a new set of directory servers, and those that do not with to participate will use the existing network as usual. This deployment strategy offers the flexibility of merging the incentive design back into Tor should it prove beneficial, while minimizing risk should it not.

4.2 Trust in Network Elements

The benefits of a system that is capable of moving to a decentralized trust model.

Federated

- runs on existing directory servers using something like opentransactions.org to provide ecash
- transactions are instantaneous
- relies on small trusted directory server set
- communication/performance overhead among bank members means it is not scalable, and it gets more complicated if you need several federated sets to handle different parts of the network

Completely decentralized

- use an AltCoin or something else as a distributed storage medium for the ledger
- more scalable
- decentralized trust may not be relevant in Tor's existing trust model, but will be when Tor moves away from federated directory server model
- transaction linkability issues leads to protocol complexities and questions about anonymity. does zerocoin work here?

4.3 Diversity

Location Diversity The market might prefer a single cheap ISP, which would not add additional location diversity to the network. Could we create a "diversity weight" and pay more for relays that increase the diversity weight?

Circuit Position Diversity Should we pay more for entry or exit position, or for exit policies that are more open by some definition? Or will the market smooth this out automatically?

Diversity in Capabilities Could we offer more reward for faster relays (i.e. a super-linear reward scale)? Or for relays that are running a certain version or support a certain feature (experimental or otherwise)? This could improve the community's ability to contribute to decisions about what to support instead of completely relying on the Tor developers (could be a good thing or a bad thing).

4.4 Community

If a new incentive scheme is incorporated into Tor, will existing volunteers stop caring become less altruistic and leave because they will view Tor as a commercial network? Will people lose interest in helping the broader Internet freedom cause?

Does a token that only provides a performance enhancement but has no intrisic value (cannot be traded with others) solve this problem? Or does the fact that you can trade the coins provide most of the incentives?

Would a smaller scale experiment outside of the existing Tor network to test the feasibility of an incentive approach be helpful, or would the conclusions simply be synthetic because users/relays in the experimental network would not have the same ideals and values as in existing network?

5 Related Work

PAR [2], XPay [3], Gold Star [4], BRAIDS [5], Tortoise [6], LIRA [7], onions for sale [8].

On the economics of anonymity [11], one-to-n scrip systems [12].

6 Future Work and Conclusions

References

1. : Tor Network Metrics. https://metrics.torproject.org/network.html
2. Androulaki, E., Raykova, M., Srivatsan, S., Stavrou, A., Bellovin, S.M.: PAR: Payment for anonymous routing. In Borisov, N., Goldberg, I., eds.: Privacy Enhancing Technologies: 8th International Symposium, PETS 2008, Leuven, Belgium, Springer-Verlag, LNCS 5134 (July 2008) 219–236
3. Chen, Y., Sion, R., Carbunar, B.: XPay: Practical anonymous payments for Tor routing and other networked services. In: Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2009), ACM (November 2009)
4. Ngan, T.W.J., Dingledine, R., Wallach, D.S.: Building incentives into Tor. In Sion, R., ed.: Proceedings of Financial Cryptography (FC '10). (January 2010)
5. Jansen, R., Hopper, N., Kim, Y.: Recruiting new Tor relays with BRAIDS. In Keromytis, A.D., Shmatikov, V., eds.: Proceedings of the 2010 ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010, ACM (2010)
6. Moore, W.B., Wacek, C., Sherr, M.: Exploring the potential benefits of expanded rate limiting in tor: Slow and steady wins the race with tortoise. In: Proceedings of 2011 Annual Computer Security Applications Conference (ACSAC'11), Orlando, FL, USA. (December 2011)
7. Jansen, R., Johnson, A., Syverson, P.: LIRA: Lightweight Incentivized Routing for Anonymity. In: Proceedings of the Network and Distributed System Security Symposium - NDSS'13, Internet Society (February 2013)
8. Johnson, A., Jansen, R., Syverson, P.: Onions for sale: Putting privacy on the market. In: Financial Cryptography and Data Security. Springer (2013) 399–400
9. Dovrolis, C., Ramanathan, P.: A case for relative differentiated services and the proportional differentiation model. Network, IEEE **13**(5) (1999) 26–34
10. Dovrolis, C., Stiliadis, D., Ramanathan, P.: Proportional differentiated services: Delay differentiation and packet scheduling. IEEE/ACM Transactions on Networking (TON) **10**(1) (2002) 12–26
11. Acquisti, A., Dingledine, R., Syverson, P.: On the economics of anonymity. In: Financial Cryptography. Springer-Verlag, LNCS 2742. (2003) 84–102
12. Humbert, M., Manshaei, M., Hubaux, J.P.: One-to-n scrip systems for cooperative privacy-enhancing technologies. In: Proceedings of the 49th Annual Allerton Conference on Communication, Control, and Computing. (2011)
13. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An Architecture for Differentiated Services (1998)
14. Jansen, R.: Privacy Preserving Performance Enhancements for Anonymous Communication Systems. University of Minnesota PhD Thesis. (October 2012)

Appendices

A Performance Rewards with Differentiated Services

We now describe how the differentiated services architecture [13] can be used to improve the control over traffic priority in Tor, as previously outlined by Jansen [14]. More specifically, the proportional differentiation model [9] allows for predictable (i.e., consistent as load increases) and controllable (i.e., adjustable differentiation) performance between N traffic classes. The model allows for the configuration of a differentiation parameter p_i for each class i, and enforces the proportional priority of a traffic quality metric q between all pairs of classes i and j for measurement timescale σ as:

$$\forall i \in [N], \forall j \in [N] : \frac{q_i\left(t, t+\sigma\right)}{q_j\left(t, t+\sigma\right)} = \frac{p_i}{p_j} \tag{1}$$

where $p_1 < ... < p_N$ and p_i/p_j defines the quality proportion between classes i and j. The model is well defined when there is enough traffic in each class to allow a work-conserving scheduler to meet the desired proportions.

Dovrolis *et al.* design a scheduler under the proportional differentiation model using a queuing delay metric [10], which in our case corresponds to Tor cell waiting times. For class i, the quality metric q_i combines the queuing delay $D_i(t)$ of the longest waiting cell with the long-term average delay $\delta_i(t)$ of all previously scheduled cells at time t:

$$q_i(t) = D_i(t) \cdot f + \delta_i(t) \cdot (1 - f) \tag{2}$$

where f is an adjustable fraction that tunes the schedulers ability to react to short term spikes in delay. When a scheduling decision is to be made at time t, the longest waiting cell from the class with the maximum priority $P(t) = q(t)/p(t)$ is chosen and scheduled.