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 uses both performance and market mechanisms to produce incentives to contribute bandwidth to Tor. We propose that relays support a new circuit scheduler based on Proportionally Differentiated Services [9, 10] that is capable of proportionally prioritizing traffic belonging to different service classes. To receive scheduling priority, clients first purchase anonymous electronic

cash (æcash) from a federated bank that is run by the existing Tor directory authorities and backed by a fully decentralized ledger. Clients then identify the desired service class to the Tor relays by sending æcash payments during circuit usage, and the relays prioritize traffic accordingly. Relays will be measured and those that are providing useful service to Tor will be awarded æcash in return, allowing them to either receive traffic priority when using Tor as a client or exchange their æcash for other goods and services on the open market. For experimental purposes, we propose that the incentive system be deployed as a secondary network that remains linked to the existing network.

3.2 Proof of Useful Service

In order to create incentives for users to contribute to Tor, we will need a system that is capable of verifying that useful service was actually provided by system participants. While useful service is certainly not limited to bandwidth, we focus on it here as it is currently the most demanded resource.

Bandwidth The current Tor bandwidth measurement scheme has been shown to be easily manipulable [11]. An alternative, and the state-of-the-art in Tor bandwidth measurement, is called EigenSpeed [12, 13].

In EigenSpeed, relays opportunistically measure their interactions with other relays and send the observation vectors to the authorities. The authorities combine the measurements from all relays using principal component analysis (PCA), and produce a set of authoritative weights that can be distributed via the Tor consensus file. **TODO!–in progress**

- Discuss Eigenspeed.
- Needs to work for all circuit positions.
- A solution will need to account for bandwidth in both directions through a circuit, and work for all circuit positions

Open Problems -does not handle asymmetric bandwidth (which is why it 'works' in Tor)
-how to measure the fastest relays
-how to prevent sybil attacks by malicious collectives
-how to measure nodes in various positions in the circuit
-evaluation and security analysis

3.3 Rewards for Providing Service

In our incentive proposal, the above scheduler would replace Tor's existing circuit scheduler. Any number of classes can be configured as well as the prices and proportions between them. We suggest three service classes: basic (free), standard, and premium. Clients can select their priority class by supplying the correct number of æcash independently to each relay in their circuit, and each æcash token can provide the selected priority for a configurable amount of data.

TODO!–How to handle verification that the desired service was provided?

We acknowledge that traffic priority will fundamentally allow users that are categorized into different service classes to be distinguished from one another,

which may result in a partitioning of Tor's anonymity set. However, as Johnson *et al.* argue [8], users with lower security requirements may in fact be willing to trade off reduced security for improved flexibility and performance. Further, a faster network that is more flexible (clients may specify their desired performance level) may attract a significant number of new users and result in a net increase of both the "payer" and "non-payer" anonymity sets. We note that it is important to make clear to users the risks and trade-offs they assume by participating in such a network.

3.4 Accountability

The "bank" provides the transaction processing services necessary for the tokens to function as a currency. The functions are enumerated below:

- Currency creation: The bank will issue new currency as a reward for computing some useful service. In the context of Tor, this means printing new currency in exchange for showing publicly verifiable evidence of providing bandwidth to the network. It would also be reasonable, for example, for new currency to be created by trusted administrators, for the purpose of providing currency tokens to new users.
- Currency redemption: Users can redeem currency for preferential service in the Tor network.
- Checking account functionality: The bank will maintain a ledger of balances associated with public keys. Signed messages can be used to transfer quantities from one account to another. These are immediately publicly verifiable. Checking accounts are not truly private.
- Cash exchanges in and out of accounts. In order to regain unlinkability, money can be transferred from a checking account to a cash pool and back out again.

Conceptually other schemes are possible; in particular, we could do away with the "checking account" functionality, and require that currency creation, transfers, and redemption use only the cash layer. However we think that having checking accounts available as an intermediate layer is usefulI guess it's hard to articulate why..., and better reflects the architecture of existing systems like Bitcoin, Zerocoin, and OpenTransactions.

One key design goal for the bank implementation is *accountability*. We typically envision that the bank will be run by (a quorum) of semi-trusted servers, such as the directory servers which are currently part of Tors reliance set. On the other hand, despite admitting that we intend to allow some reliance on these servers, we will still seek to minimize reliance on them as much as possible. There are at least two good reasons for this:

1. The less trust is required, generally the less expensive it is to secure and maintain the servers.
2. We would like to optionally be able to replace the semi-trusted transaction-processing server with a large-scale public distributed process, in the same fashion as Bitcoin mining. It is conceptually simpler to begin with a scheme using a third party.

Calling the bank (although this is a misnomer - a notary better captures, as it timestamps, signs, and checks basic validity conditions of transactions, but does not lend money or otherwise have economic stake in the transactions).

We will achieve accountability by adhering to the following guidelines:

- All messages sent from the bank should be publicly verifiable. Any incorrect action should be detectable, and publicly verifiable evidence should be obtained. This is essentially the covert security model**CITE NEEDED!** .
- The bank should maintain no secret information about clients. If an adversary is eavesdropping on the server, it should not be able to compromise. This implies it is safe to publish all interactions with the bank.
- Optionally, if a broadcast channel is available (such as the Bitcoin blockchain, arguably), then interactions with the bank may be conducted over this broadcast channel, thereby guaranteeing that the bank cannot selectively refuse service to clients. Otherwise, the server may simply refuse to process some requests and the client would not be able prove that the requests were actually sent.

Communication medium and Gossip Protocol The value of "public auditability" relies on the assumption that there is a public communication medium (generally called a "gossip network") such that sufficiently motivated members of the public will circulate all messages, and will process the messages looking for instances of misbehavior. There is a lot more to discuss here - does anyone have an incentive to check all this? It's possible to hire public auditors (at least they're not trusted with private information), but how do we know they're working correctly? It's possible to offer incentives/bounties to encourage members of the public to collect data and check it, but if misbehavior is rare, the incentives might not be effective. It may not be necessary to check every piece of data, instead random checking (in a distributed fashion) might suffice. These problems are not at all unique to our problem, but instead are all relevant to the recent trend in "certificate transparency."

Availability of Existing implementations

- OpenTransactions: based on the Lucre**CITE NEEDED!** implementation (by Ben Laurie) of Chaumian-style ecash tokens based on blind signatures. This protocol is not publicly verifiable I'm not totally sure - this means that either the server's secret key or the client's secret key is necessary to prove that a message is faulty. Additionally, the existing implementation is vulnerable to a privacy-compromising attack from a malicious server; possible countermeasures are described in documentation included with Lucre.
- Zerocoin: Zerocoin is a publicly verifiable (and public coin) cash system, intended as a modification (or alternative) to Bitcoin. Instead of asking the server to sign a blinded token, a client adds a commitment to a token into a cryptographic accumulator. To withdraw the coin, the client reveals its token and proves (in zero knowledge) that the token is a valid opening of *some* commitment in the accumulator.

Integration With Bitcoin this probably belongs in its own section? Although we have described the bank system as something to be run by one or more servers, by requiring that the protocol is publicly verifiable, it may also be possible to implement the bank as an "altcoin", i.e. a Bitcoin-like public network.

In order for this to work, an additional requirement to public verifiability is that the bank must be "public coin", meaning it does not need to generate any private keys. This is because the participants in the network (i.e. the miners) include anonymous members of the public, and hence includes adversaries. As mentioned, Zerocoin is public coin and therefore suitable for this purpose. Other publicly verifiable ecash protocols such as those of Lysanka and Camendisch**CITE NEEDED!** are publicly verifiable but not public coin.

There are a variety of ways of integrating with Bitcoin summarize these from Futurecoin:

- as a modification to Bitcoin
- as a separate system
- as an overlay system using Bitcoin just as a transaction log (i.e., Mastercoin or coloredcoins)

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 [14], one-to-n scrip systems [15].

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. Biryukov, A., Pustogarov, I., Weinmann, R.: Trawling for tor hidden services: Detection, measurement, deanonymization. In: Security and Privacy (SP), 2013 IEEE Symposium on, IEEE (2013) 80–94
12. Snader, R., Borisov, N.: Eigenspeed: secure peer-to-peer bandwidth evaluation. In: IPTPS. (2009) 9
13. Snader, R., Borisov, N.: Improving security and performance in the tor network through tunable path selection. Dependable and Secure Computing, IEEE Transactions on **8**(5) (2011) 728–741
14. Acquisti, A., Dingledine, R., Syverson, P.: On the economics of anonymity. In: Financial Cryptography. Springer-Verlag, LNCS 2742. (2003) 84–102
15. 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)

16. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An Architecture for Differentiated Services (1998)
17. 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 [16] can be used to improve the control over traffic priority in Tor, as previously outlined by Jansen [17]. 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.