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. Coming soon.

1 Introduction

2 Requirements, Challenges, and Discussion

There are several requirements and challenges, both technical and social, in any Tor incentive approach. Here we describe the issues.

2.1 Secure Bandwidth Measurement

Can existing proof of bandwidth solutions can be dropped in, or do we need to design a new one?

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

2.2 Account Management

We need some way to manage an account for relays to represent the ammount of bandwidth they have contributed. All interaction with the account management system should happen offline, that is, it should not be part of the circuit construction phase so that it does not cause blocking behavior in Tor.

Network Structure Central:

- run by a single entity
- not resilient to takedowns or malicious behavior
- potentially a severe performance bottleneck

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?

Trust Assumptions trusted, honest but curious, untrusted.

2.3 Incentives to Participate

We can use performance enhancements as an incentive, which may lead to monetary value if a generic 'coin' or other token is used that can be traded among clients. There may be designs where exchanging coins is not possible, and so the coin would have no value to others.

Differentated Services [1].

Guaranteed Quality of Service

Differentiated Service Differentated Services [1].

2.4 Integration with the Tor Network

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.

2.5 Anonymity

Transaction Unlinkablity Whatever mechanism used to pay relays (ecash, coin, or bank) should provide completely unlinkable transactions in order to maintain Tor's anonymity.

Partitioning Anonymity Sets The anonymity sets of payers vs non-payers should be considered. Is anonymity fundamental to diffserv or a similar approach that is needed to actually create the incentive? In other words, if we use performance differentiation as an incentive, then at some level that can also be used as a distinguisher of who is paying and not paying for service.

2.6 Diversity

Location Diversity The market might prefer a single cheap ISP, which would not add additional location diversity to the network. We could 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 We could 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).

2.7 Community Interaction

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?

3 Proposed Architecture

3.1 Proof of Bandwidth

Need to be able to measure and verify bandwidth in a secure way that is not gameable or easy to disrupt. Explain here in the high level what a proof of bandwidth system would provide to an incentive scheme, and point to the next section for technical details of how that would work.

3.2 Bank

Describe our model of the bank to handle the user and relay accounts.

3.3 Scheduling

Describe how Proportionally Differentated Services [2, 3] can be used to provide a performance enhancement.

3.4 Deployment

4 Proof of Bandwidth

Because the current Tor measurement scheme has been shown to be easily manipulable [4], we will need to use a different approach to bandwidth measurement or design a new one. This section discusses how the state-of-the-art in

distributed system bandwidth measurement may be applied to Tor, and offers an alternative scheme that may also be used for bandwidth accounting purposes.

EigenSpeed Discuss here how EigenSpeed [5] or something similar [6, 7] may be used in the context of Tor and how our incentive system may take advantage of it.

Ephemeral Paths

5 Related Work

PAR [8], XPay [9], Gold Star [10], BRAIDS [11], Tortoise [12], LIRA [13], onions for sale [14].

On the economics of anonymity [15], one-to-n scrip systems [16].

6 Future Work and Conclusions

References

1. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W.: An architecture for differentiated service (1998)
2. Dovrolis, C., Ramanathan, P.: A case for relative differentiated services and the proportional differentiation model. Network, IEEE **13**(5) (1999) 26–34
3. 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
4. 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
5. Snader, R., Borisov, N.: Eigenspeed: secure peer-to-peer bandwidth evaluation. In: IPTPS. (2009) 9
6. Snader, R., Borisov, N.: A tune-up for tor: Improving security and performance in the tor network. In: NDSS. Volume 8. (2008) 127
7. 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
8. 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
9. 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)
10. 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)
11. 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)
12. 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)

13. Jansen, R., Johnson, A., Syverson, P.: Lira: Lightweight incentivized routing for anonymity
14. Johnson, A., Jansen, R., Syverson, P.: Onions for sale: Putting privacy on the market. In: Financial Cryptography and Data Security. Springer (2013) 399–400
15. Acquisti, A., Dingledine, R., Syverson, P.: On the economics of anonymity. In: Financial Cryptography. Springer-Verlag, LNCS 2742. (2003) 84–102
16. 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)