TOR Research Problem

Jesse Sheppard
Department of Computer Science
Montana State University
Bozeman, Mt 59717
Email: jesse.sheppard@cs.montana.edu

Mike Wittie
Department of Computer Science
Montana State University
Bozeman, Mt 59717
Email: mwittie@cs.montana.edu

***Abstract*—The abstract goes here.**

I. Introduction

The Tor network uses encryption and multiple relays to provide a level of anonymity to its users [1]. The developers of Tor acknowledge that Tor is a slow method to communicate messages from one point to another, and try to speed up the network without sacrificing the anonymity it promises. [2]. This year, nearly half of the tor user base stopped using tor, but this usage may have been through a subnetwork called the silk road, which was used for drug dealing, which was shut down [3]. Since Tor relies on a user base to supply bandwidth, Tor will not be as efficient as before the drop in user base.

When a message is sent from one client to another, the message is encrypted in layers. The message is to be decrypted layer by layer, in each relay, until it reaches its destination. These relays are supplied by other tor users. Supplying a relay is entirely voluntary, and not all users need to supply one. When supplying relays, users may determine how much bandwith they supply. If users do not supply much bandwidth, the tor network will have many messages to send, and not much space in which to send it. As a result, it would be beneficial to provide an incentive system in which users would be rewarded for supplying relays for other users [2].

Some basic incentive systems involve determining how much bandwidth a user may take up, based on how much the user supplies. Or, the user is awarded some kind of currency for supplying bandwidth, and may spend the currency for faster paths throught the TOR network [2].

Another issue that tor has is that it does not choose relays to use very efficiently. It only looks at bandwidth for choosing particular relays [2] [4]. If it could also factor in latency, it might significantly allow messages to travel along the network more efficiently [2]. A method to favor low-bandwidth relays may also provide security at the cost of time efficiency, and vice-versa; therefor, a method to determine whether a user prefers a fast message, or a secure message, and selecting the relevant relays may help users recieve what they want out of tor [4].

Tor may be used to download files, which may take up a lot of bandwidth. This will penalize users who might want to use tor for browsing the web. A potential solution to this may involve setting a limit on how fast messages may move through the network. Large messages, like downloaded files, may take longer in favor of the users who want to browse content on the web [5].

References

[1] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[2] R. Dingledine and S. J. Murdoch, "Performance improvements on Tor or, why Tor is slow and what we're going to do about it," 2009.

[3] E. Markowitz, "Tor usage has dropped nearly 50% in three months," 2014. [Online]. Available: www.vocativ.com/01-2014/tor-usage-dropped-neary-50-three-months/

[4] R. Snader and N. Borisov, "A tune-up for Tor: Improving security and performance in the Tor network," in *Proceedings of the Network and Distributed Security Symposium - NDSS '08*. Internet Society, February 2008.

[5] W. B. Moore, C. Wacek, and M. Sherr, "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.