Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Improving System Protection and Performance in The Tor System End-To-End Tunable Path Selection

[1]R. VITHISHKUMAR,
[1,2]Asst.professors,
Dept.of.Computer science,
Meenakshi Chandrasekaran
College of Arts & Science
Pattukkottai-614 626. Thanjavur.

[2]G. AMBIKA,
[1,2]Asst.professors,
Dept.of.Computer science,
Meenakshi Chandrasekaran
College of Arts & Science
Pattukkottai-614 626. Thanjavur.

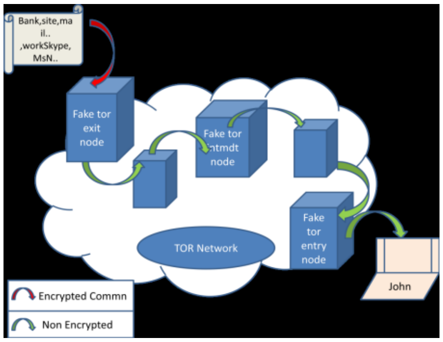
[3]A. ANITHA.
[3]Asst.professors,
Dept.of.Computer science,
Bonsecors college of Arts
& Science
Thanjavur.

***Abstract** - Tor, a circuit-based low-latency anonymous communication service, is a protocol that is both ore secure and performs better, both in terms of observed performance and in terms of achievable anonymityand provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. This paper proposes improvements to the existing Tor router bandwidth evaluationand routerselection algorithms. Additionally, by allowing the user to selecttheir preferred balance of performance and anonymity, these improvements increases the usability, and therefore the potential user base and security of the Tor network.It is proposed to increase the fidelity of the packet-level simulation in the Tor network by including such effects as variable file sizes, variable intervals between requests, and TCP slow-start behavior. This paper also proposes to examine the other aspects (such as latency, apart from bandwidth) of the tradeoff between performance and anonymity in anonymous networks of varying types. This paper explains an opportunistic bandwidth measurement and tunable performance extensions and examined their performance both throughsimulation and in the real Tor network. Additionally, this paper focuses on observing a number of interesting characteristics of the Tor network which could provide insight into the observed behavior of the Tor network.*

***Index Terms**:-Anonymous communication, bandwidth estimation, path selection.*

I. INTRODUCTION

This second-generation Onion Routing system addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points. Tor works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable tradeoff between anonymity, usability, and efficiency. It is proposed to replace the Tor mechanism with an opportunistic bandwidth measurement mechanism. Tor routers are registered with a directory service. Each router reports its IP address, public key, and policies about what traffic it will accept, and a bandwidth value that is determined by monitoring the peak bandwidth achieved by the router over a period of time. The directory service also maintains statistics about the uptime of each router. The Tor path construction algorithm, executed by the Tor client, will first select all routers that have an acceptable forwarding policy (e.g., many routers are unwilling to serve as exit routers) and then choose a random router out of the list, with the selection weighted by the reported bandwidth. This way, traffic is roughly balanced across Tor nodes in proportion to the bandwidth they have available



Tor Network Architecture

II. Related Works

Onion Routing is an infrastructure for private communication over a public network. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. Onion routing's anonymous connections are bidirectional and near real-time, re a socket connection can be used. Any identifying information must be in the data stream carried over an anonymous connection. An onion is a data structure that is treated as the destination address by onion routers; thus, it is used to establish an anonymous connection. Onions themselves appear differently to each onion router as well as to network observers. The same goes for data carried over the connections they establish. Proxy aware applications, such as web browsing and e-mail, require no modification to use onion routing, and do so through a series of proxies. Tor advertises itself as a means for people and groups to improve their privacy. And when used properly, the distributed, anonymous network does just that. But a Swedish security consultant has used the very same system to gain access to login credentials for a thousand or so individual email addresses, including those of at least 100 accounts belonging to foreign embassies. The Tor servers try to make it harder to trace the originator of traffic in much the same way an agent under surveillance might quickly drive in and out of a parking garage to throw off pursuers. Tor has taken pains to warn its users that people running so-called exit nodes which are the last Tor servers to touch a packet before sending it on its way.

III. Proposed Methodology

3.1. TOR NETWORK CREATION

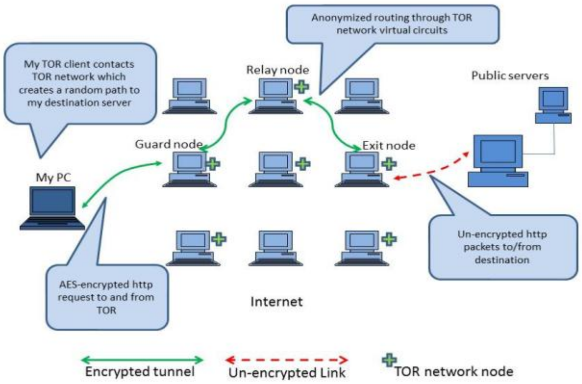
Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.

3.2. USER REQUEST-RESPONSE:

Client-Server interaction is maintained in this module. Java file as input and the corresponding output will be given as response to the client to do the task of routing packets between networks. Because real by connecting to the server IP, client will access services available at particular port numbers. Routing path will be specified by route configuration. Server will cache the route and the path will be traced for routing the data through that path.

IV.Softwarerouterconfiguration

Tor network uses software routers for routing data. Software router is a term denoting a computer or a PC designatedhardware routers are costly (in most cases costlier than an average PC), this technique of modifying the PC and using it as a router is desired. Routeconfiguration information will be provided to the router. Since Overlay topology is used in Tor network which is an unstructured topology(peer knows information about the adjacent peers only)

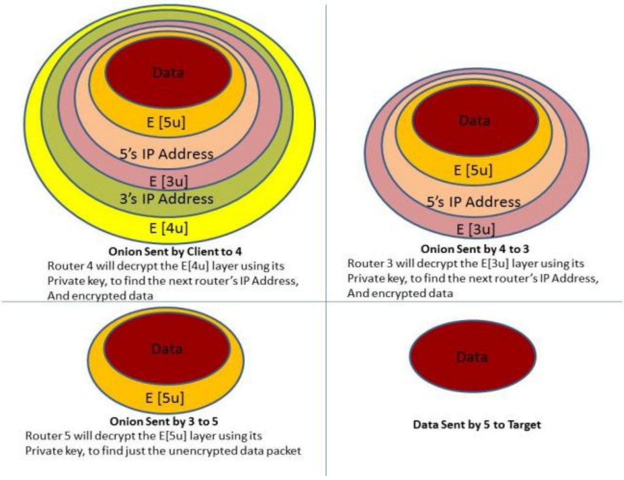

Anonymized routing through TOR network virtual circuits
My TOR client contacts TOR network which creates a random path to my destination server
Relay node
Public servers
Guard node
Exit node
My PC
Un-encrypted http packets to/from destination
AES-encrypted http request to and from TOR
Internet
Encrypted tunnel
Un-encrypted Link
TOR network node

Tor Anonymity

The router used will be static, i.e., the path through the network -a tunnel- is constructed so that each router knows only the previous and the next router inthe path. In particular, the first (entry) router knows the source of the tunnel, but not its destination, and the last (exit) router knows the destination but not the source.

V. Encryption

Encryption in the Tor network is performed using AES algorithm.AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware. Unlike itspredecessor, DES,in Tor routing path of the network, encryption in Tor network is performed based on the number of routers in Tor routing path of the network. Encryption is based on the fact that how many routers are there in routing path, that much times AES encryption will be performed before routing and at each router the layers of encryption will be removed. Ultimately the original data will be given to the destination node. AES has fixed blocks of size 128 bits and a key size of 128,192, or 256 bits. AES operates 4×4 column-major order matrix of bytes, termed the state. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of the cipher text. Each round consists of several processing steps, including one that depends on encryption key.



Onion Sent by Client to 4
Router 4 will decrypt the E[4u] layer using its Private key, to find the next router's IP Address, And encrypted data

Onion Sent by 4 to 3
Router 3 will decrypt the E[3u] layer using its Private key, to find the next router's IP Address, And encrypted data

Onion Sent by 3 to 5
Router 5 will decrypt the E[5u] layer using its Private key, to find just the unencrypted data packet

Data Sent by 5 to Target

Encryption in Tor Network

traffic it will accept, and a bandwidth value that is determined by monitoring the peak bandwidth achieved by the router over a period of time. The directory service also maintains statistics about the uptime of each router.

VI. Result Analysis

The Tor load balancing algorithm provides a single, static compromise between performance and anonymity. Users who are highly anonymity sensitive (e.g., whistle blowers) might wish to distribute all of the tunnels uniformly across all routers, to prevent (purportedly) high-bandwidth routers from having a higher chance of compromising their traffic. Users who are less privacy-sensitive and are using the network for casual web browsing (e.g., users who want to hide their browsing activities from their neighbors) might value performance more and would be more willing to use high-bandwidth routers more often. By using the same path selection algorithm for both of these, the Tor router selection algorithm sacrifices the needs of both classes.

VII. Two Approaches For Quantifying

PERFORMANCE:

There are two general approaches for gathering performance data about overlay nodes. First, a source node can repeatedly perform end-to-end measurements on p paths. These repeated performance measurements expose the source node to new nodes in the system, increasing vulnerability to passive logging attacks, and is akin to building p different paths. The alternative is to ask nodes directly for their performance information. For example, Tor maintains node statistics on uptime and bandwidth in a central directory. While this is scalable and more robust, it makes the system vulnerable to malicious nodes who claim plentiful resources to bias flows to choose them as routers. This increases the probability of success of multiple attackers colluding together to break the anonymity of a flow. Despite systems to verify resource availability, attackers can always obtain resource-rich machines to bias path formation. Such an attack cannot be prevented as long as path selection is biased for resource availability.

VIII. Conclusion And Future Works

This paper proposes improvements to the existing Tor router bandwidth evaluation and router selection algorithms. Additionally, by allowing the user to select their preferred balance of performance and anonymity, these improvements increases the usability, and therefore the potential user base and security of the Tor network. It is proposed to increase the fidelity of the packet-level simulation in the Tor network by including such effects as variable file sizes, variable intervals between requests, and TCP slow-start behavior. This paper also proposes to examine the other aspects (such as latency, apart from bandwidth) of the tradeoff between performance and anonymity in anonymous networks of varying types. This paper explains an opportunistic bandwidth measurement and tunable performance extensions and examined their performance both through simulation and in the real Tor network. Additionally, this paper focuses on observing a number of interesting characteristics of the Tor network which could provide insight into the observed behavior of the Tor network. Evaluations of these changes show that they can result in increasing average throughput by a factor of almost three in exchange for a modest decrease in anonymity, or they can result in drastically improved anonymity while maintaining similar average throughput. It also shows that the improvement that is proposed can reduce or even eliminate the long tail of the transfer time distribution, greatly improving performance as perceived by the users of the network.

References

[1] P. Syverson, G. Tsudik, M. Reed, and C.Landwehr, “Towards an analysis ofonion routing security,” in *Proceedings of DesigningPrivacy Enhancing Technologies: Workshop on Design Issues inAnonymity and Unobservability*, H. Federrath, Ed. Springer- Verlag, LNCS 2009, Jul. 2000, pp. 96.114.

[2] A. Back, I. Goldberg, and A.Shostack, “Freedom systems 2.1 security issues and analysis,” Zero Knowledge Systems, Inc., White Paper, May 2001.

[3] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The second generation onion router,” in *Proceedings of the 13th USENIX SecuritySymposium (USENIX Security '04)*, Aug. 2004.

[4] “TorStatus - Tor network status,” http://torstatus.kgprog.com/. [5] K. Loesing, “Measuring the Tor network,” https://git.torproject.org/checkout/metrics/mast er/report/dirreq/directory-requests-2009-06-25.pdf.

[6] D. Goodin, “Tor at heart of embassy passwords leak,” *The Register*, Sep. 10, 2007.

[7] G. Goodell, S. Bradner, and M. Roussopoulos, “Building a coreless Internet without ripping out the core,” in *FourtWorkshopon HotTopicsinbNetworks*, College Park, MD, Nov. 2005.

[8] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, “Low-resource routing attacks against anonymous systems,” in *Proceedings of the 2007 Workshop on Privacy in the Electronic Society(WPES)*, Oct. 2007.

[9] R. Dingledine and N. Mathewson, “Anonymity loves company: Usability and the network effect,” in *Designing Security SystemsThat People Can Use*. O'Reilly Media, 2005.

[10] M. Wright, M. Adler, B. N. Levine, and C. Shields, “An analysis of the degradation of anonymous protocols,” in *Proceedings of theNetwork and Distributed SecuritySymposium*, Feb. 2002.