Tor vs Yggdrasil: A Comparative Study

Kushal Kothari
University of Mumbai
Department of Computer Engineering
Mumbai,India
kushalkothari285@gmail.com

Tejal Palwankar
University of Mumbai
Department of Computer Engineering
Mumbai,India
tejal30palwankar@gmail.com

Ayush Dubey
University of Mumbai
Department of Computer Engineering
Mumbai,India
dubeyayush1687@gmail.com

Priya Parate
University of Mumbai
Department of Computer Engineering
Mumbai,India
priya.parate@mctrgit.ac.in

***Abstract*— The Internet is one of the main sources of communication in today's world but the identities of senders and receivers are not completely hidden. The most suitable choice if someone wants to hide his/her identity is to use anonymous communication. Anonymous communication provides anonymity and privacy. In this paper, we analyze and compare most widely used communication system i.e. Tor alongside Yggdrasil Network which is the most advanced and decentralized communication system. Tor is the most used anonymous communication system worldwide while Yggdrasil is created to be a future-proof decentralized anonymous alternative routing system.**

***Keywords* — Anonymity, encryption, Tor Network, Yggdrasil Network.**

I. Introduction

Anonymity means the identity of the user of the message must be hidden. Anonymity is carried out with the purpose to make the sender and receiver of the message hidden. On the internet, the IP address and host name are logged. Temporary IP numbers are allotted for every single use of the Internet; however, such numbers are logged through service providers of the internet. A service provider can be used in disclosing the identities of senders and receivers [1]. Anonymous Systems such as Tor, I2P etc are designed to protect anonymity and internet privacy. They hide the identities of the sender and receiver. Different encryption techniques are used to mask the identification of the individual from the system itself.[2-4].

Tor is a low latency and circuit-based overlay of a network that lays out privacy. Tor is the most used anonymous system for communication all over the world [5]. Yggdrasil is constructed as an overlay of networks, in which nodes are connected with virtual peers over networks of the local area or the Internet. In this paper, we analyzed and compared both the systems . The structure of the paper is as follows; In section 2, related works on comparison of different anonymous systems are discussed. In section 3, Tor is elaborated In section 4, Yggdrasil is discussed in detail. In section 5, we discussed the experimental setup when comparing both networks. In section 6, we discussed the results of our analysis, and lastly, in section 7, the conclusion is given.

II. RELATED WORKS

We reviewed some previous studies related to anonymous communication systems and what different methods are used to evaluate their anonymity.

Ramadhani, E. [6] The work in this paper focuses on the comparison of VPN and Tor in terms of security. The comparison between this anonymous system in this manuscript main, divided into three categories: confidentiality, integrity, and availability. The method used in this paper is by reviewing previous research papers that focus on Tor and VPN. The limitation of this manuscript is there is no practical implementation performed when comparing these two networks.

R. A. Haraty and B. Zantout. [7] The work in this paper mainly focuses on a complete overview of Tor. This manuscript also takes a deep dive into the features of Tot and what makes it so attractive compared to other anonymous systems. Some of these features are Open Design, Free Participation, Protection against Strong and Weak Attacks, etc. The added advantage of Tor like the more the Tor Nodes the More anonymity is added, Building Anonymous Paths for the Client Based on a List of Bridge Nodes, Protecting against Strong and Weak Attackers, etc. However, the manuscript also discusses several disadvantages such as 9001 TCP Can Not Only Be Blocked But Also Detected, Slow Performance, etc. The research gap in this manuscript was that a Bandwidth-choking approach was required when focusing on security features.

Negi, Neelam. [8] The work in this paper focuses on the comparison of three Anonymous networks, which are Tor, I2P, and Freenet. This paper mainly focuses on advancements in recent technology and the growing threat to online privacy. This manuscript observed various aspects such as anonymity, speed, popularity, usage, etc. However, this manuscript lacks in differentiating which one is best suited for use in different scenarios.

III ANALYSIS ON TOR

The Tor network is a low latency network which provides anonymity. It is the most used anonymous system around the globe. Its users include military, intelligence agencies, journalists, etc., and in more than 78 countries with 6018 relays is in hundreds of thousands to provide online anonymity. The technique behind Tor is "onion routing". David Goldschlag, Paul Syverson, and Michael Reed developed it around the year 1990-1991. U.S. Naval Research Laboratory funds Tor. Anonymity over the computer/internet is

provided by Onion Routing for communicating anonymously. Messages are encrypted and sent to known nodes. No nodes have the information of where the message is sent or received [9].

A Traffic Encryption in Tor

Tor encrypts a user's traffic and routes the traffic at three Tor nodes so that the user's request and IP address during transit is masked from observers. Tor exits through its exit node once the request reaches its intended destination.

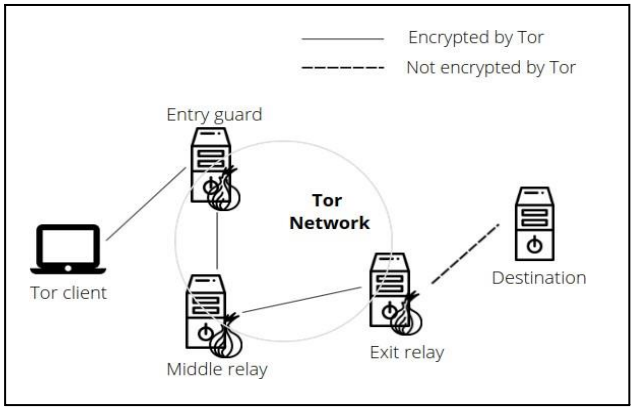

Fig 1. Network traffic encryption in Tor

B Anonymity in Tor

Tor offers anonymity but anyone who wants to be anonymous or hide their identity online should follow best practices when using this technology. Though Tor can anonymize the network and internet address one has to be careful when visiting illicit websites and not reveal his true identity or location, nationality, or any information which can reveal itself. Any small clue can be used for people to find out who you are. Even more, law enforcement will use every detail about an online person to find a wanted suspect.[10]

IV. YGGDRASIL NETWORK

Yggdrasil, a globally agreed spanning tree formed between interconnected nodes, chooses another approach when distributing information of routing. Yggdrasil constructs a topology that is a single network and global whereas traditional systems assign address ranges as paths. This connected graph provides synchronization allowing it to distribute a set of tree mesh. These are particularly used in interchanging messages. Nodes set up paths throughout the network to their keyspace neighbors ordered by public keys, effectively arranging the network into a virtual line. Intermediate nodes populate the routing tables with these paths.

Yggdrasil implements Crypto-Key Routing. The main reason behind Crypto Key Routing is that it defines routes stating that specific subnets should be routed to a given node on the network, identified by their public encryption key. The traffic is fully encrypted, and sent to the specified node which effectively gives the ability to roll VPNs over the Yggdrasil network without the need for any additional software.

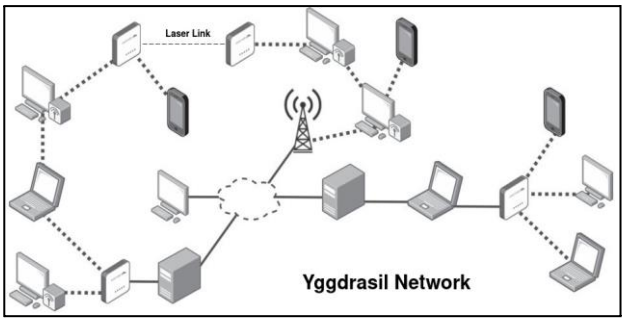

Fig 2. Yggdrasil Network

A Traffic encryption in Yggdrasil

All the traffic in Yggdrasil is encrypted at all times to ensure that traffic is private when routed across other network nodes. Even applications like plain-text are encrypted, ensuring that intermediate nodes cannot decrypt traffic when it is forwarded onto the network. Traffic between nodes is very much encrypted , so even if the site in the Yggdrasil network does not contain an SSL certificate i.e. address starting with http:// not https://, we can still be sure that the connection is protected from any kind of interception.

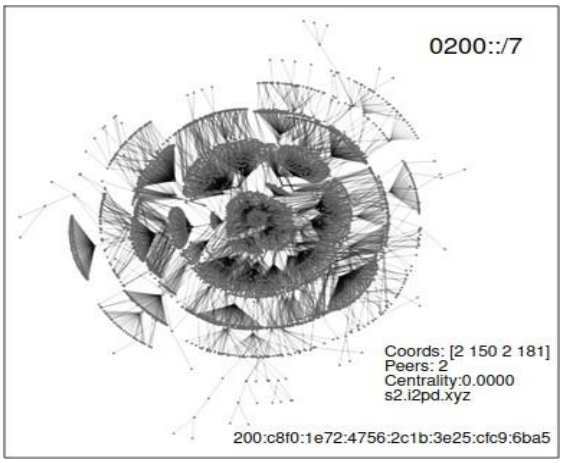

Fig 3. Map of the spanning tree subset of the network.

The above figure includes the minimum subset of links needed to construct the spanning tree. The tree coordinates, as well as known nodes, are taken from Yakamo's API [11]. One can configure the names of the nodes by setting a "name" field in NodeInfo, or from Yakamo's node list as a fallback.

B Anonymity in Yggdrasil

Traffic in Yggdrasil nodes is fully encrypted. Within the network, the device receives a unique "white" IPv6 address. Connecting to the network is the installation of the Yggdrasil-go program, which runs the TCP / IP abstraction on top of the connection already existing in the system, creating a virtual network adapter. This application connects via Wi-Fi, optical cable, Ethernet, or other means to another device or network, and then can be used to organize the Yggdrasil network. The Yggdrasil network can be used by devices that are not connected to the net: it only requires a connection to another device which has the internet connected to Yggdrasil.

V. EXPERIMENTAL SETUP

We first take a look at our tools and then outline our method with the help of these tools

Tracing Links. We are using oneprobe as it is a TCP-based tracing method. We used HTTP GET requests in the data probes of TCP to generate HTTP response messages. Each probe measures the performance of forwarding links using customized back-to-back packets. The performance of the reverse link is measured when probes arrive at the remote end and send two back-to-back packets. The values of the forward and reverse links are evaluated for further calculation. The parameters set are as follows:

Parameters	z (bytes)	M (bytes)	m (bytes)	e (seconds)	r (pkt/s)
Values	65535	750	750	300	2

Table 1. Parameters of Tools Setup

In Table 1, Parameter z stands for the size of the packets. M stands for the size of the packets, and m stands for the response packets size. e stands for controlling how long the probe will take place. Parameter r stands for the rate at which packets are sent. We are sending 2 packets/sec.

(1) Obtaining web links: For better accuracy of our method, we took the entity of each web address to be over 10 Kbytes so that we can generate enough packets when analyzing such kinds of web links. We considered over one million websites as a dataset and obtained desirable results in the form of web links. We also considered IPv6 to evaluate both Tor and Yggdrasil networks.

(2) Categorizing web links: We split the web links into five regions of Web Registers and evaluate the address of our web links and match with these Web Registers. Today, there are five RIRs – APNIC, ARIN, RIPE NCC, LACNIC, and AFRINIC.[12]

(3) Probe: We choose less than 14 web links each time so that we do not face impact caused by large numbers of packets. We chose this URL from different sites For each RIR, we designated 50 mins as one cycle because while analyzing we assigned 300 seconds to IPv4 and 300 seconds to IPv6, and therefore it cost 3000 seconds i.e. fifty mins for all the 5RIRs to complete its one cycle.

VI. RESULTS

We analyzed and compared both Tor and Yggdrasil networks based on four factors. Seven days of data were collected and used according to the method described in the previous section. One week of observation was carried out with one sixty-eight polling cycles.

A) Interruption Rate:

Different possible points are available which can create an interruption in a network like security-policy control, adoption in routing, non-performing link, and non-performance of the node.

$$\textit{Interrupt rate} = \textit{interrupts} / (\textit{no of polling cycles} * \textit{no of web links}).$$

Regions	APNIC	ARIN	RIPENCC	AFRINIC	LACNIC
Interrupt	20	136	272	228	20
Interrupt Rate	0.4%	2.7%	5.4%	6.2%	0.54%

Table 2. Interrupt Rate of Yggdrasil.

Regions	APNIC	ARIN	RIPENCC	AFRINIC	LACNIC
Interrupt	287	18	24	8	100
Interrupt Rate	5.7%	0.36%	0.48%	0.2%	2.1%

Table 3. Interrupt Rate of Tor.

The interrupt rate of Yggdrasil and Tor are given above in table. In general, the tor has better interrupt rate than Yggdrasil.

B) Packet Round Trip(RTT).

Round trip time can be termed as the total time between initiation of a network request and receiving a response. As shown in figure 4 other than the Asia Pacific Network Information Centre, the RTT of Yggdrasil Network is almost the same as that of Tor as Yggdrasil Network and Tor are similar. We see, Yggdrasil Network RTT is bigger than Tor RTT in APNIC. This variation is due to connectivity between other countries in Tor being much better compared to the Yggdrasil network, which results in Yggdrasil RTT being bigger than Tor for most destined web links.

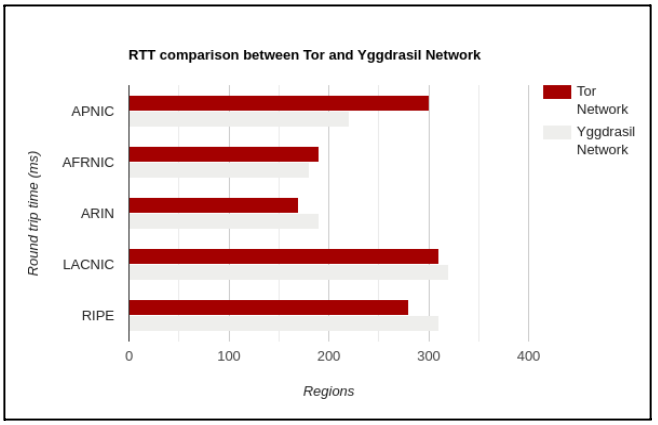

Fig 4. RTT Comparison between Tor and Yggdrasil Network

C) Packet loss Rate.

We differentiated Tor and Yggdrasil Network in terms of packet loss rate. As shown in Figure 5, the packet loss rate of the Yggdrasil Network is very much close to Tor in regions other than APNIC. This proves that the value of the packet loss rate is not affected by the delay. We then try to find the reason for the variation between the Yggdrasil and Tor packet loss rate in APNIC. We calculated the packet loss rate in APNIC for each URL in the destination. We found that packet loss rates in the same region are roughly the same for these web links, and the variations are mainly caused when web links are from different countries. Yggdrasil Network is encountered with a higher packet loss rate compared to Tor in distinguished regions. We also conducted a comparison and analyzed the Tor and Yggdrasil Network packet loss rate in the areas with no distinguished regions. The average rate of packet loss of Yggdrasil Network turns out to be 0.26%, and the average loss rate of Tor is 0.34%

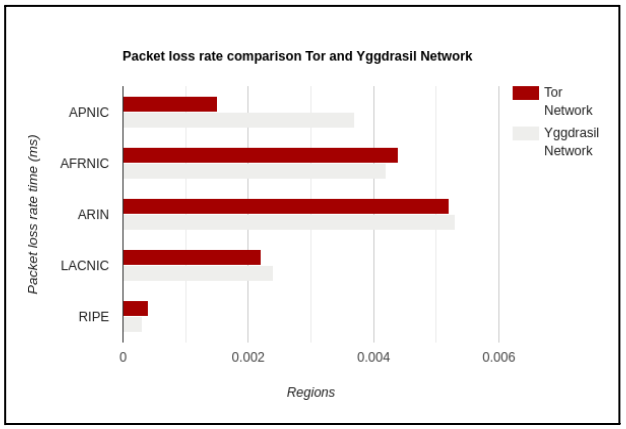

Fig 5. Packet Loss rate comparison of Tor and Yggdrasil

D) Packet Reordering.

This means that packets sent may be received by the remote connection in a different order than the one they were sent. Network congestion, timeout retransmission, and multipath transmission are the three major reasons for packets that fail to be in order. We conducted thorough research on packet reordering of both Tor and Yggdrasil Network. As shown in Table 5, During the monitoring, there are no Yggdrasil packets in AFRINIC and RIPENCC which are out of order. Yggdrasil has some out-of-order packets in ARIN, LACNIC, and APNIC only in some polling cycles. We also observed that the Yggdrasil reordering rate is quite smaller than that of Tor Network. In Tor, packet reordering LACNIC is above 1%, while reordering rates are below 0.8% for the other RIRs. Yggdrasil PRR is $2.3 * 10 -6$, and of Tor is 0.79% due to the following two reasons: (1) Division of packets in the Yggdrasil network can only be performed by end hosts. Whereas, in the Tor network, both hosts and routers can carry out packet division,thus increasing the probability (2) Yggdrasil reduces the probability by simplifying its basic header which accelerates the processing of packets.

Type	APNIC	AFRINIC	ARIN	LACNIC	RIPENCC
Yggdrasil$(*10 -6)$	8.1329	0	0.1686	3.2457	0
Tor $(*10 -2)$	0.7243	0.7343	0.7857	1.3629	0.8186

Table 4. Out of order rate comparison between Yggdrasil and Tor.

VII. CONCLUSION AND FUTURE REMARKS

Providing anonymity to the user is the main goal of any anonymous system. However, most anonymous systems still work on old technologies to encrypt the data and provide anonymity for which hackers are now more capable with advanced technologies to decrypt, hack and steal or observe the data. In this paper, two advanced anonymous communication systems were first discussed and then tor, one of the most popular tools and Yggdrasil which is an IPv6-centric next-generation network are compared on the basis of interrupt rate, packet round trip etc. We collected seven days of data and analyzed crucial details for our comparison.

Throughout our research, we only considered data from a single source of location. However, establishing clients from multiple locations and gathering data in the future would provide a much better analysis when comparing these networks.

VIII. REFERENCES

1. Olivier Verscheure, Michail Vlachos, Aris Anagnostopoulos, Pascal Frossard, Eric Bouillet and Philip Yu, “Finding Who Is Talking to Whom” in VoIP Networks via Progressive Stream Clustering ”, in IBM Watson Research Center, pp. 1-11, 2004.
2. R. A. Haraty and B. Zantout, “A Collaborative-based approach to Avoiding Traffic Analysis and Assuring Data Integrity in Anonymous Systems”, Computers in Human Behavior Journal. Volume 51, Part B, October 2015, Pages 780–791.
3. B. Zantout and R. A. Haraty, “A Comparative Study between BitTorrent and NetCamo Data Communication Systems,” International Journal of Computational Intelligence and Information Security. March 2010. Volume 1, Number 2, 2010.
4. Badieh Trabousli and Ramzi A. Haraty. MANET with Q-RoutingProtocol. Proceedings of the Eleventh International Conference on Networks (ICN 2012). Reunion Island, France. February 2012.
5. Roger Dingledine, Nick Mathewson, and Paul Syverson, “Tor: the second- generation Onion Router”, in Proceedings of the 13 th conference on USENIX Security Symposium- Volume 13, pp. 21–21, 2004.
6. Ramadhani, E. "Anonymity communication VPN and Tor: a comparative study." Journal of Physics: Conference Series. Vol. 983. No. 1. IOP Publishing, 2018.
7. R. A. Haraty and B. Zantout, "The TOR data communication system: A survey," 2014 IEEE Symposium on Computers and Communications (ISCC), 2014, pp. 1-6, doi: 10.1109/ISCC.2014.6912635.
8. Negi, Neelam. "Comparison of anonymous communication networks-tor, I2P, Freenet." *International Research Journal of Engineering and Technology* 4, no. 07 (2017).
9. https://geti2p.net/en/docs/how/intro accessed on December 6, 2014.
10. https://portswigger.net/daily-swig/network-security
11. http://y.yakamo.org:3000/
12. https://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-regional-internet-registries/