

# An approach to enhance the privacy in TOR network

Subhajit Saha<sup>1</sup>, Mohammed Ameenulla<sup>2</sup>

<sup>1</sup>Jain School of CS & IT

<sup>2</sup>Asst. Professor Jain School of CS & IT

**Abstract-** The tor is the software that makes the user surf the internet anonymously. The network keeps data communication hidden from any third party snooping. Tor creates multiple layers of encryption circuit between communicating parties to make user anonymous over the internet. It sends the user's request through many tor relays(nodes) around the globe before it reaches to the desired destination. The request goes through three nodes *entry, middle and exit nodes*. If the entry and exit nodes exist in same country or same geographical location sniffing or selling of data can take place. Hence, propose a simple mechanism to manually put the nodes into two political opposition countries so that chances of selling data is minimal.

**Keywords-** encryption, snooping, relays, nodes, sniffing, algorithms, traffic fingerprinting, eavesdropping, packets, metadata.

## I. INTRODUCTION

When it comes to digital privacy everyone is concern about it, but there is no basic mechanism to browse Internet privately. Most of them are expensive, untrusted, complex or not available. Hence we propose a mechanism which will help users to give a certain level of privacy. Tor or The Onion Router is a network that enables a user to stay anonymous on the Internet and get rid of any possible surveillance while using the Internet. Tor works on the concept of 'onion routing' method in which the user data is first encrypted and then transferred through different relays (nodes) present in the Tor network[1], thus creating a multi-layered encryption (layers like an onion), thereby keeping the identity of the user safe. One encryption layer is decrypted at each successive Tor relay, and the remaining data is forwarded to any random relay until it reaches its destination server. For the destination server, the last Tor node/exit relay appears as the origin of the data. It is thus tough to trace the identity of the user or the server by any surveillance system acting in the mid-way. So we have to secure our first node/entry node and the last node/exit node, What if these nodes are basically based in the same country? The probability of selling data or sniffing is high.

Not only selling of data, A person can do packet injection and manipulate the flow of data. In 2015, MIT researchers used machine learning algorithms to monitor that data and count the packets. Using only this metric, the system can determine with 99% accuracy what kind of resource the user is accessing (i.e. the open web, a hidden service, and so on) but the algorithms can do a lot more with the traffic data. Traffic fingerprinting can be used to determine which hidden services a user is accessing with 88% accuracy based solely on the pattern of packets sent. Also in 2018, Turmoil vulnerability buzzed all

over the Internet[7]. The bug owes its origins to Firefox, the browser on which Tor is built. The developers at Tor have found a way to help plug the leak of IP addresses, but that was only a temporary solution. The Tor browser may revisit its security levels in the coming days to institute long-term fixes to any more flaws.

## II. IMPLEMENTATION

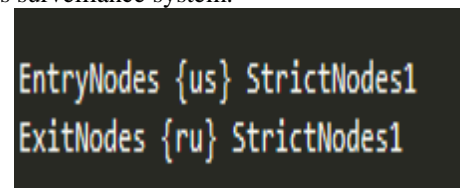
We visualise if the entry and exit nodes come under a country, the selling of data or the eavesdropping by an organization is possibly high. So, what if we divide the entry and exit nodes into two opposite countries or the countries that we can trust over for not selling the information directly or not dealing with normal users data by its privacy laws or their political perspective.

If the nodes are in the same country, anyone or any organization can retrieve the data easily. Also if a malicious guy is sniffing the two nodes can watch what all users are trying to do within the Tor network. Also if the two nodes are owned by a single person, he can sniff out the packets and possibly do whatever he wants with user's data.

By analyzing all these we propose to put the nodes into different locations by editing our torrc file which is one of the configuration files of a Tor network. If we are using Tor browser we can get the tor config file in

" *Desktop/tor/Browser/TorBrowser/Data/Tor/torrc* " and if we are using tor service in any Linux environment we can get the torrc file in

`"/etc/tor/torrc"` path. So adding "EntryNodes {US} StrictNodes1" "ExitNodes {RU} StrictNodes1" in torrc (as shown in fig 1.). Our traffic will route from the USA to Russia (as shown in fig.2). The keyword here "StrictNodes1" plays a crucial role which says that we don't want to change the nodes rather than our own choice of country nodes if there are no nodes available in that country better say "can't connect to the tor network" instead of changing into some other country's node. Now, there is a very less chance of selling of data and eavesdropping also by the country's surveillance system.



```
EntryNodes {us} StrictNodes1
ExitNodes {ru} StrictNodes1
```

fig.1:



fig.2:

We can find these country codes in many websites over the internet. Better use different pair of country codes in different Tor sessions or else tracking becomes easy with the metadata as we are using the same country nodes in every session.

### III. CONCLUSION

Keeping both the nodes (entry & exit) in the same location results into vulnerability of tor network, as it is easy to track. Splitting the nodes into two different geographical locations (different countries) would help us overcome this loophole, only if the genuine tor community members have the authority for setting up the nodes. The privacy hence can't be compromised as the two nodes are apart into two different countries. Considering our mechanism, the privacy can be restored & as the community grows the time latency problem with node's location would get solve.

### IV. REFERENCES

- [1]. Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker, "Shining Light in Dark

Places: Understanding the Tor Network," Department of Computer Science, University of Colorado, Boulder, USA 2008.

- [2]. Adrian Barberis, Danny Radosevich, Wyatt Emery and Mike Borowczak, "Portable Tor Router: Easy Enabling Web Privacy for Consumers"-2018.
- [3]. Timothy Girry kale, Satoshi Ohzahata, Celimuge Wu and Toshihiko Kato "Improving the Tor Traffic Distribution with Circuit Switching Method" -2016.
- [4]. N. Mathewson, "Def con 2007: Technical changes since the last tor talk" <https://www.freehaven.net/~nickm/slides/Defcon07/TorChanges.pdf>, 2007
- [5]. Murdoch, S.J., Danezis, G.: Low-cost traffic analysis of Tor. In Proceedings of the 2005 IEEE Symposium on Security and Privacy, IEEE CS (May 2005).
- [6]. "Safely Measuring Tor" Rob Jansen and Aaron Johnson, U.S. Naval Research Laboratory, Washington, D.C, 2016.
- [7]. <http://news.mit.edu/2015/tor-vulnerability-0729>
- [8]. Perry, M.: Torflow. <https://www.torproject.org/svn/torflow/README>
- [9]. Robin Snader and Nikita Borisov. 2008. A Tune-up for Tor: Improving Security and Performance in the Tor Network. San Diego, California, USA, 10th February- 13th February 2008, The Internet Society.
- [10]. Trawling for Tor Hidden Services: Detection, Measurement, De-anonymization, Alex Biryukov, Ivan Pustogarov, Ralf-Philipp Weinmann, University of Luxembourg, 2013.
- [11]. "Performance and Security Improvements for Tor: A Survey", Masha'el AlSabah, Qatar University and Qatar Computing Research Institute Ian Goldberg, University of Waterloo, 2015.