NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

ENHANCING TOR'S EFFICACY: CUSTOM CIRCUITS AS A KEY TOOL AGAINST CENSORSHIP AND FOR ONLINE PRIVACY PROTECTION

Mr. Smeet Sabalpara

School of Cyber Security & Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India
smeetsabalpara@gmail.com

Mr. Vishwajeet Yelkar

School of Cyber Security & Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India
vyelhekar@gmail.com

Mr. Ramya Shah

School of Cyber Security & Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India
ramyashah4@gmail.com

Mr. Sarang Rajvansh

School of Cyber Security & Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India
sarang.rajvansh@nfsu.ac.in

Dr. Digvijaysinh Rathod

School of Cyber Security & Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India
digvijay.rathod@nfsu.ac.in

Abstract:
The use of the TOR network [5] has become increasingly important as a tool for protecting online privacy and bypassing censorship. However, the use of custom circuits[3] within the TOR network[5] can further enhance the ability of users to avoid detection and access blocked content. This research paper explores the need for custom circuits[3] in TOR, particularly in regards to censorship. Through analysis of case studies and existing literature, we demonstrate the effectiveness of custom circuits in bypassing censorship[8][9] and the ways in which they can be used to improve the overall security and anonymity[7][11] of the TOR network. Additionally, we discuss the challenges and limitations of implementing custom circuits and provide recommendations for future research in this area. Overall, our findings suggest that the incorporation of custom circuits is essential for ensuring the continued effectiveness of TOR as a tool for overcoming censorship and protecting online privacy.

INTRODUCTION

The Deep Web

The surface grid represents the searchable part of the Internet, while the deep grid includes all other parts that cannot or do not want to be indexed. Its size exceeds what many people think because the deep wingspan is far wider than expected. It is important to understand that the Internet is not the same as the Surface Web; The latter is a purely accessible resource available through the Internet system. As a result, a substantial proportion of deep networks reside on the Internet as well, including networks or systems that require a login credential.

Need for TOR

The TOR (The Onion Router[4]) network[5] is a free, open-source software that enables anonymous communication[1] over the internet.

It was originally developed by the U.S. Navy as a way to protect government communications, but it is now used by millions of people around the world to protect their privacy and security online. There are many situations where people may need to use TOR to protect their online activity.
For example, journalists, activists, and human rights workers may use TOR to communicate with sources or report on sensitive issues without fear of reprisal. TOR can also be used by individuals living in countries with internet censorship [8][9] to access blocked websites and content. TOR is particularly useful for people who are concerned about being monitored by governments, employers, or other third parties. By routing internet traffic [6] through multiple layers of encryption and multiple servers, TOR makes it nearly impossible for anyone to track a user's online activity or identify their location. Overall, TOR is an important tool for anyone who values their privacy and security online.

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

Whether you are a journalist, an activist, or simply someone who wants to protect their personal information, TOR can help you stay safe and secure while using the internet.

BACKGROUND STUDY

The TOR browser builds on the Mozilla Firefox web browser as its base. Using a technique called "onion routing", this browser encrypts user data [2] through multiple layers, reminiscent of the concentric onion layer and later in the process, the data is encrypted through the relays in TOR networks [5].

TOR relay

A TOR relay is a type of computer network that allows users to browse the internet anonymously and securely. It is part of the larger TOR network, which is a decentralized network of servers that helps to obscure the location and identity of its users. When a user connects to the internet through a TOR relay, their internet activity is routed through a series of randomly selected servers before reaching its destination. This makes it difficult for anyone to track the user's activity or identify their location.

In addition to providing anonymity [7][11], TOR relays also help to improve the overall security of the internet by acting as a sort of "middleman" between users and the websites they visit. By routing traffic through a series of servers, TOR relays can help to protect users from malicious actors who may be trying to intercept their data or compromise their devices.

TOR relays are operated by volunteers who donate their bandwidth and resources to the network. This allows the network to remain decentralized and independent, as there is no central authority or organization controlling it. As a result, the TOR network is often used by journalists, activists, and other individuals who may be targeted by governments or other organizations for their online activities.

Overall, TOR relays play a crucial role in helping to protect the privacy and security of internet users around the world. By routing traffic through a series of servers and obscuring the location and identity of its users, TOR relays allow users to browse the internet freely and securely, without fear of being monitored or tracked.

Types of relays

In the TOR network, there are three types of relays: entry, middle, and exit[10].

1. The entry relay is the first relay in the network that receives a user's internet traffic. It is responsible for encrypting the traffic and forwarding it to the middle relay. The entry relay does not know the user's true location or identity, nor does it know the final destination of the traffic.
2. The middle relay is the second relay in the network. It receives the encrypted traffic from the entry relay and decrypts it before forwarding it to the exit relay. Like the entry relay, the middle relay does not know the user's true location or identity, nor does it know the final destination of the traffic.
3. The exit relay is the final relay in the network. It receives the decrypted traffic from the middle relay and sends it on to its final destination. The exit relay is the only relay that is able to see the user's true IP address and the final destination of the traffic. However, it is not able to trace the traffic back to the user's location or identity because it was encrypted by the entry relay.

In summary, the entry, middle, and exit relays work together to create a secure and anonymous connection for internet users. The entry and middle relays protect the user's identity by encrypting and routing the traffic, while the exit relay allows the traffic to reach its final destination without revealing the user's true location or identity.

What are circuits

In the TOR network, a circuit is a path that internet traffic takes through a series of servers before reaching its destination. These circuits are created by the TOR software on a user's device and are designed to obscure the user's location and identity. To create a circuit, the TOR software first establishes a connection with a directory server, which maintains a list of all the servers (known as relays) that are currently available in the network.

The software then selects three randomly chosen relays from this list and establishes connections with them. These three relays form the first circuit, and the traffic from the user's device is routed through them before reaching its destination. The process of creating a circuit is known as building a circuit. This occurs every time a user connects to the internet through the TOR network, and a new circuit is created for each new connection. This helps to ensure that the user's location and identity remain anonymous [14], as the traffic is constantly being routed through different relays.

In addition to building circuits, the TOR software also maintains a pool of "idle" circuits that are ready to be used when a user initiates a new connection. This helps to speed up the process of building circuits and allows users to connect to the internet more quickly.

Overall, circuits play a crucial role in the TOR network, as they help to obscure the location and identity of users and protect their online privacy and security. By routing traffic through a series of randomly chosen relays, circuits allow users to browse the internet anonymously and securely, without fear of being tracked or monitored.

Socks proxy

When a user wants to access a website or other Internet resource, their request is encrypted and passed through several nodes, each of which decrypts a layer of encryption to reveal the next node in the path. This process helps to conceal the user's identity and location. A SOCKS proxy can be used to route traffic through a specific node in the TOR network, allowing the user to communicate with the Internet anonymously. This is useful for protecting the user's privacy and security online, as it prevents their IP address from being exposed and makes it more difficult for their online activity to be tracked.

Number of relays throughout the countries

Countries	*Number of relays(Approx.)*
Germany	1400
United States	1500
Sweden	143
India	500
France	1700

Table. 1.0 The table shows some of the countries and their approximate number of relays.

Daily TOR users in 2022

Country	**Mean daily users**
United States	543367 (21.56 %)
Germany	293350 (11.64 %)
Finland	121578 (4.82 %)
Russia	116190 (4.61 %)
India	101693 (4.03 %)
France	85604 (3.40 %)
Indonesia	84773 (3.36 %)
Netherlands	82178 (3.26 %)
United Kingdom	62943 (2.50 %)
Brazil	45714 (1.81 %)

This table shows the top-10 countries by estimated number of directly-connecting clients. These numbers are derived from directory requests counted on directory authorities and mirrors.

IMPLEMENTATION / WORK DONE

Need for this project

Censorship [8] is a major concern for many individuals who use the TOR network. This is especially true for those who live in countries with strict internet censorship laws. In these countries, the government may block certain websites or restrict access to certain types of content. This can make it difficult for individuals to access information or communicate freely online. One way to bypass these restrictions is by creating a custom circuit on TOR. This involves selecting specific countries as entry and exit nodes for your internet connection. By choosing countries with more lenient censorship laws, you can potentially access more content and communicate more freely.

However, there are a few considerations to keep in mind when creating a custom circuit on TOR. First, it is important to choose countries that are not known for their own censorship practices. For example, you may want to avoid selecting countries that have a history of blocking certain websites or monitoring internet activity.

Second, you should be aware of the potential risks associated with using a custom circuit. While it may allow you to access more content, it can also make it more difficult for you to protect your privacy. This is because the more countries you pass through, the more opportunities there are for someone to intercept your internet traffic.

Finally, it is important to remember that censorship is a fluid issue. Even if you choose a country with relatively lenient censorship laws today, that could change in the future. This means that you may need to update your custom circuit periodically to ensure that you are still able to access the content you need.

Overall, censorship is a major concern for many individuals who use the TOR network. By creating a custom circuit from user-defined countries, you can potentially bypass censorship restrictions and access more content. However, it is important to be aware of the potential risks and to choose countries carefully to ensure that you are able to protect your privacy while still accessing the information you need.

Pseudocode

```
Flag_list: α
Fp_list: β
Ip_list: γ
Iso3_list: δ
listIndex: ϵ
rangFig:θ
Country: ρ
Circuit: ω
CustomCountriesFile: ψ
Flag:  ϕ
CustomCircuit: μ

for ω in range( ψ ):
ϕ ← True
Reader ← ψ iterator
Set α, β,  γ, δ
ϵ ← array[ ]
for i in range(0,sizeOf(α)):
ϵ[ ] ←  append i
while( ϕ ):
θ ← random( ϵ )
If α[θ] is “Both” or “Guard”:
ω ← append( α[θ] )
ϕ ← False
else if α[θ] is “Other”:
ω ← append( α[θ] )
ϕ ← False
else if α[θ] is “Both” or “Exit”:
ω ← append( α[θ] )
```

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

ϕ ← False

μ ← control.new_circuit(ω, await_build=True)

OUTCOMES/VISUALIZATION

1. Creating a custom TOR circuit.

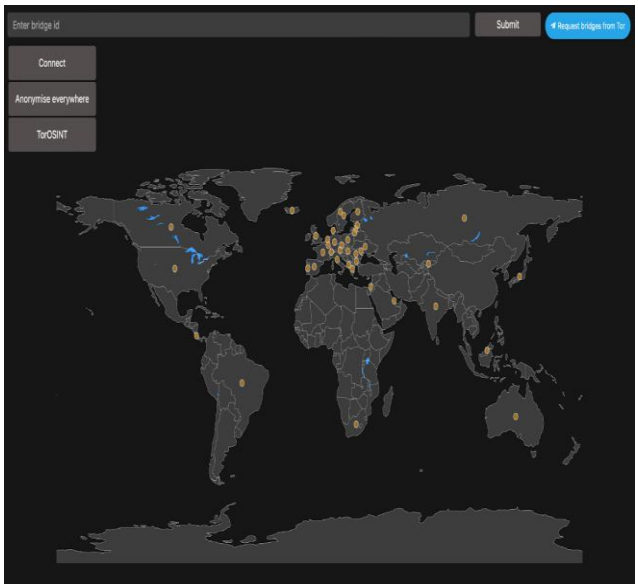

Figure 1. GUI of the Tool

The yellow plots on the countries allow the users to select the sequence in which their traffic should hop and create a custom circuit.

After selecting the country, the IP table will list all the available IPs with their bandwidth and consensus weight, this gives users multitudinous options.

Figure 2. Selecting 1st node i.e. “Guard Node” as Canada.

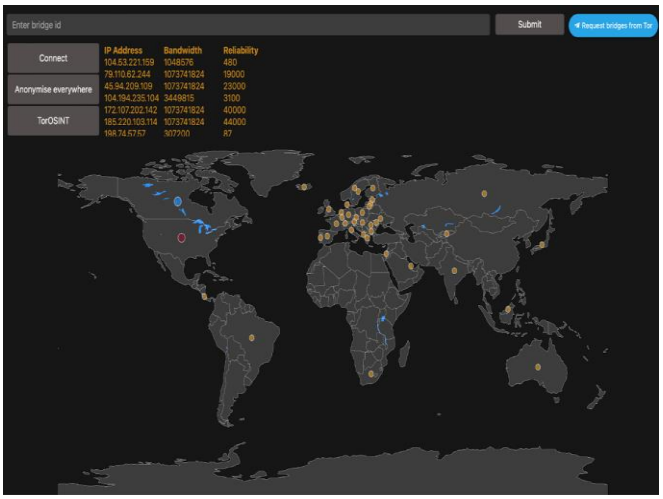

Figure 3: Selecting 2nd node i.e. “Middle Node” in the United States of America.

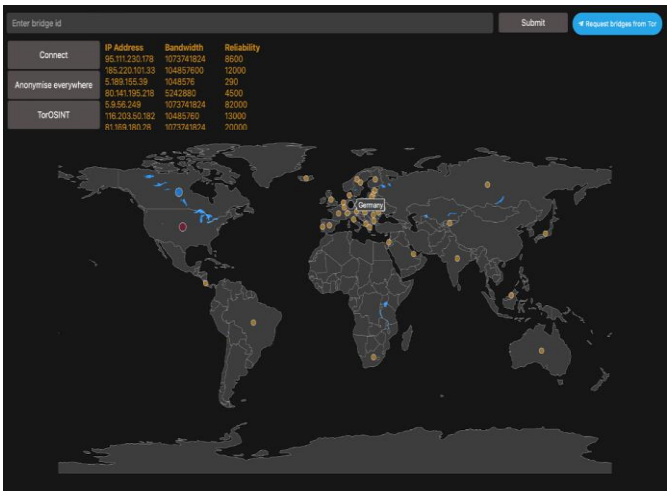

Figure 4: Selecting 3rd node i.e. “Exit Node” in Germany

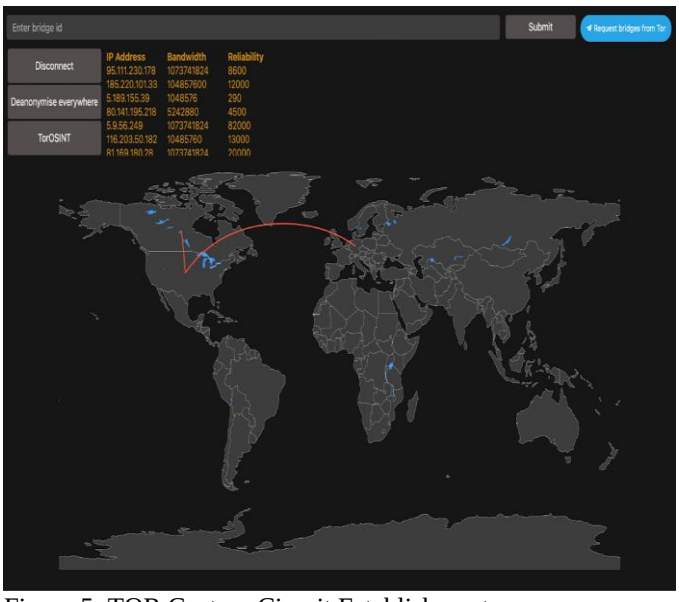

Figure 5: TOR Custom Circuit Establishment

2. Including custom bridge / available bridge in the TOR Circuit

The "Request bridges from TOR" button redirects the user to the official Telegram page of Tor where users can get the list of Bridges they can use.

Figure 6: Request Bridges from the TOR (Telegram Page of TOR – Redirection)

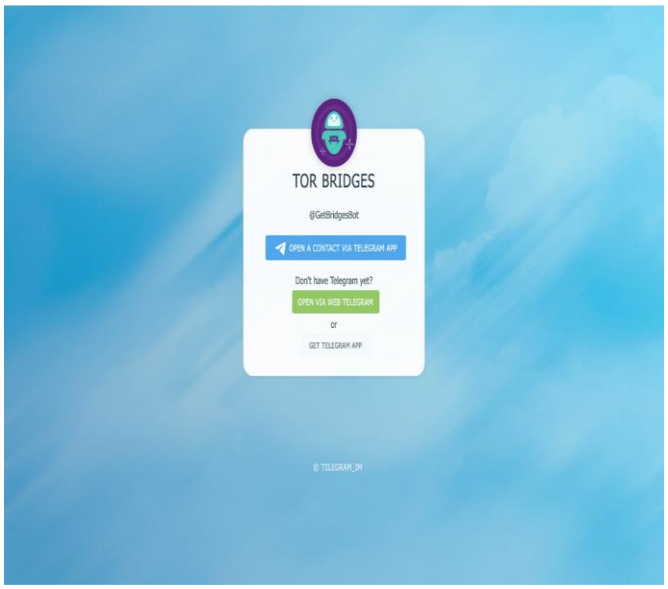

Figure 7: Telegram Page of TOR Bridges

Adding Bridge fingerprint in the text field and pressing "Submit" adds the bridge to the circuit.

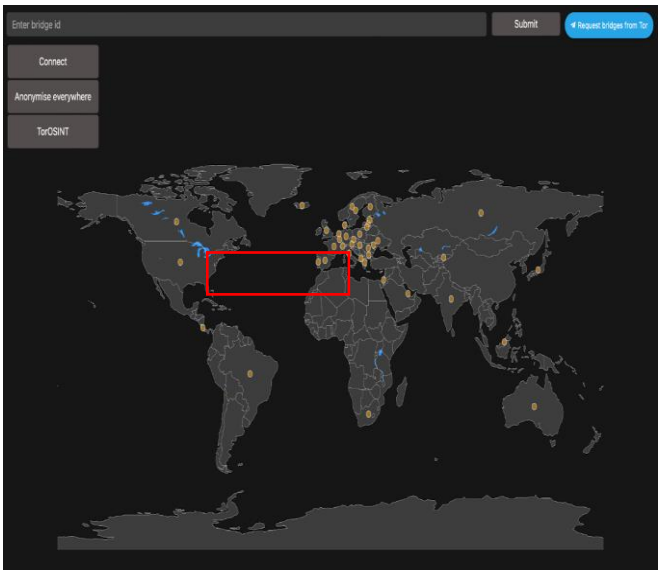

Figure 8: Bridge ID & Submission UI

3. Anonymise Everywhere

On pressing "Anonymise everywhere", the proxy settings of the device HTTP, HTTPS and SOCKS are changed.

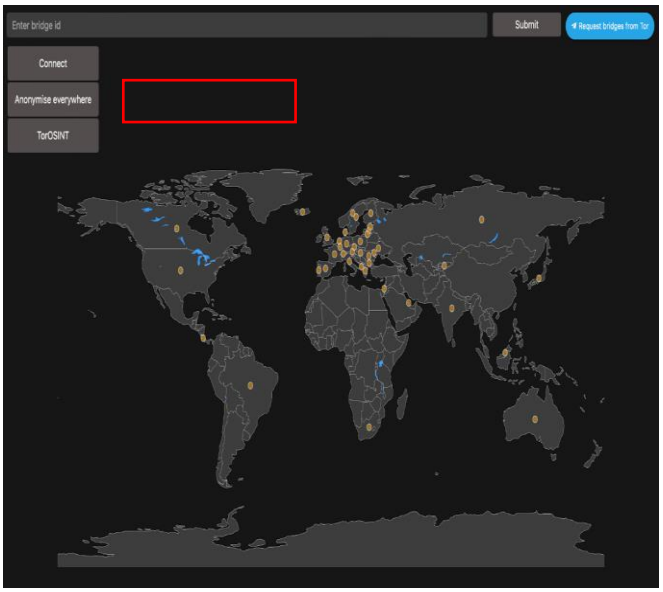

Figure 9: Anonymise Everywhere Option

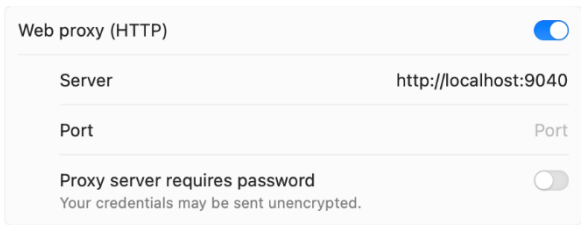

Figure 10: HTTP Connection Details Under Anonymise Everywhere Option

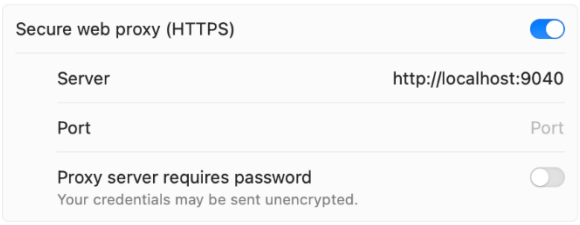

Figure 11: HTTPS Connection Details Under Anonymise Everywhere Option

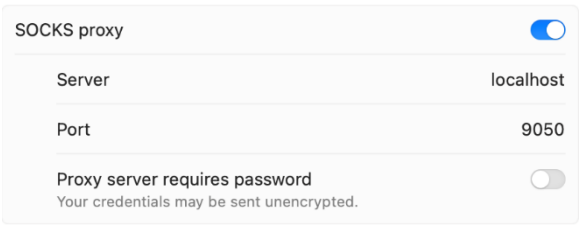

Figure 12: SOCKS Connection Details Under Anonymise Everywhere Option

4. Opensource Intelligence for TOR

"Tor OSINT" redirects the user to a new page where the table displays every detail of Tor relays.

Figure 13: TOR Relay Details

CONCLUSION

In conclusion, this research paper underscores the critical role that custom circuits play in enhancing the effectiveness of the Tor network, particularly in the context of overcoming censorship and safeguarding online privacy. Through the analysis of case studies and existing literature, we have stated that very limited sources are available helping in creating a custom TOR circuit and making a connection more secure and powerful.

This paper demonstrated the creation of custom TOR circuits using self-developed approach which provides users a powerful means to avoid detection, access blocked content, and enhance their overall security and anonymity while using Tor. However, we acknowledge that there are challenges and limitations in implementing custom circuits, such as potential performance trade-offs, increased complexity and challenges in investigation. Nevertheless, the benefits they offer in terms of circumventing censorship and preserving privacy far outweigh these challenges.

The future outcomes based on this paper will be considered in terms of investigating such custom TOR circuits and identifying bridges being used during creation of such circuits.

REFERENCES

[1] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, "Anonymous Connections and Onion Routing," in 1997 IEEE Symposium on Security and Privacy, May 4-7, 1997, Oakland, CA, USA.

[2] R. Learmonth and K. Loesing, "Metrics Data Collection, Aggregation, and Presentation," Tor Tech Report 2019-03-001.

[3] X. Liu and N. Wang, "An Improved Tor Circuit-Building Protocol," in 2009 International Joint Conference on Artificial Intelligence, 07 July 2009, Hainan, China.

[4] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," June 2004.

[5] Monk, J. Mitchell, R. Frank, and G. Davies, "Uncovering Tor: An Examination of the Network Structure," Security and Communication Networks, vol. 2018, no. 3, pp. 1-12, May 2018.

[6] Lashkari, G. D. Gil, M. Mamun, and A. A. Ghorbani, "Characterization of Tor Traffic using Time-based Features," in 3rd International Conference on Information Systems Security and Privacy, January 2017.

[7] L. Basyoni, N. Fetais, A. Erbad, and A. Mohamed, "Traffic Analysis Attacks on Tor: A Survey," in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), February 2020.

[8] F. Naikoo, K. Ahmad, and K. A. B. Ahmad, "Anonymity-Enabled Communication Channels: Attacks and Defense Methods," in 2022 3rd International Conference for Emerging Technology (INCET), May 2022.

[9] Y. Song, M. Yang, Q. Chen, X. Gu, and Y. Yao, "Evaluating the Distinguishability of Tor Traffic over Censorship Circumvention Tools," IEEE, 22 June 2023.

[10] J. A. Vilalonga, J. S. Resende, and H. Domingos, "TorKameleon: Improving Tor's Censorship Resistance With K-anonymization and Media-based Covert Channels," March 2023.

[11] R. A. Haraty and B. Zantout, "The TOR data communication system: A survey," Journal of Communications and Networks, vol. 16, no. 4, pp. 415-420, August 2014.

[12] Engelmann and A. Jukan, "Defying Censorship with Multi-Circuit Tor and Linear Network Coding," IEEE, 20 January 2020.

[13] M. Khan, M. Saddique, U. Pirzada, M. Zohaib, A. Ali, B. Wadud, and I. Ahmad, "The effect of malicious nodes on Tor security," IEEE, 30 November 2015, Beiriut, Lebanon.
[14] L. Hellebrandt, I. Homoliak, K. Malinka, and P. Hanáček, "Increasing Trust in Tor Node List Using Blockchain," IEEE, 01 July 2019, Seoul, Korea (South).
[15] Döpmann, S. Rust, and F. Tschorsch, "Exploring Deployment Strategies for the Tor Network," IEEE, 10 February 2019, Chicago, IL, USA.
[16] Tor Nodes List [Online]. Available: https://www.dan.me.uk/tornodes. Last accessed on 09/01/2024.