A Comparative Analysis of Privacy, Security and Performance in the TOR and I2P Network

Fernando Manuel Sanfeliz
Dept. of Computer and Systems Sci.
Stockholm University
Stockholm, Sweden
fesa6676@student.su.se

Gustav Mönefors
Dept. of Computer and Systems Sci.
Stockholm University
Stockholm, Sweden
gumo9296@student.su.se

Silas Pohl
Dept. of Computer and Systems Sci.
Stockholm University
Stockholm, Sweden
sipo6151@student.su.se

***Abstract*—Work in Progress**

***Index Terms*—Darknet, Anonymity Networks, The Onion Router, Tor, Invisible Internet Project, I2P, Onion Routing, Garlic Routing, Latency, Throughput, Network Performance Evaluation**

I. Introduction

A. Background

In today's digital age, characterized by an ever-expanding online presence and the ubiquity of digital communication, concerns over privacy and security have taken center stage. The pervasive collection and exploitation of personal data by governments, corporations, and malicious actors have raised profound questions about individual autonomy, freedom of expression, and the right to privacy. In response to these growing threats, anonymity networks have emerged as crucial mechanisms for protecting digital identities and activities [1].

Anonymity networks, such as The Onion Router (TOR) [2] and the Invisible Internet Project (I2P) [3], offer users the means to navigate the digital realm without fear of surveillance, tracking, or censorship [4]. These networks achieve anonymity through sophisticated routing mechanisms that obscure the origin and destination of internet traffic, as well as robust encryption protocols that safeguard the confidentiality and integrity of data [1].

B. Research Problem

Previous studies about anonymity networks have often focused on individual enhancements to the respective network [5] or have uncovered concerns about security and privacy issues [6] [7]. The focus has mostly been on a specific network, making a direct comparison of different networks difficult. Some studies touched on this by comparing anonymity networks such as TOR and I2P, but a comprehensive understanding of the respective advantages and disadvantages in the context of specific use cases remains unclear. Existing research often lacks insights into the specific use cases where one network may outperform the other [8] [1] or compares specific factors of the networks like performance and scalability [9] [4]. However, a systematic comparative analysis across multiple dimensions, including privacy, security, and performance, that elucidates the nuanced differences between TOR and I2P across various use cases and operational contexts is still lacking.

C. Research Question

In order to make a contribution to closing the aforementioned research problem, the paper will attempt to provide an answer to the following research question:

- How do the TOR and I2P network compare in terms of privacy, security, and performance?

Based on the formulated research question, we have derived two closely related sub-research question for each factor to be investigated in order to examine the individual factors (Privacy, Security and Performance) in a methodologically sound manner and finally to combine and evaluate the results to answer the main research question:

1) Privacy:

- How do the anonymization techniques employed by TOR and I2P differ?
- What are the vulnerabilities associated with each network in preserving user anonymity?

2) Security:

- What encryption algorithms and protocols are utilized by TOR and I2P?
- How do they compare in terms of robustness against common attacks?

3) Performance:

- How do TOR and I2P compare in terms of latency of network activities?
- How do TOR and I2P compare in terms of throughput of network activities?

II. Scientific Base

A. TOR and I2P's underlying protocols

1) Onion Protocol: Similar to the layers of an onion, this protocol involves encapsulating messages within many encryption layers and are then "peeled" away as they pass through randomly selected nodes. Utilized by Tor, it is the cornerstone of anonymous communication over the internet [2].

2) Garlic Protocol: Employed by the Invisible Internet Project (I2P), this protocol is an extension to the Onion protocol. The main difference is, that Garlic bundles multiple messages together, enhancing efficiency and potentially offering stronger resistance against traffic analysis [3].

B. Discussion of Previous Research

Ranging from Ali et al.'s "TOR vs I2P: A Comparative Study" [8] to Hosseini Shirvani, M., & Akbarifar, A.'s "A Comparative Study on Anonymizing Networks: TOR, I2P, and Riffle Networks Comparison" [1], both these studies provide in-depth research on the Onion and Garlic protocols and analyze these systems' methods, vulnerabilities, and efficiencies alongside critical differences shared. Furthermore, "A Survey on Tor and I2P" by Conrad and Shirazi [4] showcases how each protocol adapts to different applications with specification into node selection, performance, and scalability.

The selection of studies for this thesis was driven by their in-depth analyses and relevance to the network's underlying core functionalities and protocols. The thesis utilises theories of foundational concepts for the onion and garlic protocol in regard to cryptographic privacy and network security. These include concepts of symmetric and asymmetric encryption, both of which are integral to fully comprehend how Tor and I2P maintain anonymity and data integrity. This scientific base lays the groundwork for a detailed exploration of the TOR and I2P networks, aiming to contribute significantly to the field of computer and systems sciences by providing a deeper comparative analysis of these essential privacy technologies.

III. Methodology

This study will have a comparative analytical approach to examine the privacy, security, and performance characteristics of TOR and I2P networks. The research will be based on mixed-methods combining both qualitative and quantitative data.

Firstly, privacy aspects will be analyzed by comparing the anonymization techniques of both networks. This will involve a review of secondary data from existing studies, complemented by experiments to identify vulnerabilities that could compromise user anonymity.

Secondly for the security analysis, the encryption algorithms and protocols used by each network will be cataloged from academic articles and technical documentation. Their effectiveness will be assessed through simulated attacks to measure their robustness.

Thirdly, the performance metrics latency and throughput, will be measured using controlled experiments where data packets are transmitted through both networks under similar conditions to ensure comparability. These experiments will be conducted in a controlled lab environment, using network simulation tools to mimic realistic internet traffic scenarios. Data analysis will involve statistical testing to compare the networks' performance, and thematic analysis for qualitative data regarding security and privacy. This methodological approach aims to gather how TOR and I2P operate under various scenarios and therefore assist in answering the research questions.

References

[1] A. Akbarifar and M. H. Shirvani, "A Comparative Study on Anonymizing Networks: TOR, I2P, and Riffle Networks Comparison," *Journal of Electrical and Computer Engineering*, p. 15, 11 2021. [Online]. Available: https://jecei.sru.ac.ir/article_1630_86a21780622d23f325605053a067414a.pdf

[2] "The Tor Project," accessed 17.04.2024. [Online]. Available: https://www.torproject.org/

[3] “The Invisible Internet Project,” accessed 17.04.2024. [Online]. Available: https://geti2p.net/en/

[4] B. Conrad and F. Shirazi, “A Survey on Tor and I2P,” *ICIMP 2014 : The Ninth International Conference on Internet Monitoring and Protection*, 2014. [Online]. Available: http://www.i2project.net/_static/pdf/icimp_2014_1_40_30015.pdf

[5] M. S., G. Thangavel, and S. Basheer, “A Review on Garlic Routing and Artificial Intelligence Applications in Public Network,” in *2023 International Conference on Computer Science and Emerging Technologies (CSET)*, 2023, pp. 1–6.

[6] M. Simioni, P. Gladyshev, B. Habibnia, and P. R. Nunes de Souza, “Monitoring an anonymity network: Toward the deanonymization of hidden services,” *Forensic Science International: Digital Investigation*, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281721000330

[7] M. Mehdi, “Convenient Detection Method for Anonymous Networks ”I2P vs Tor”,” 11 2023. [Online]. Available: https://www.researchgate.net/publication/375182370_Convenient_Detection_Method_for_Anonymous_Networks_I2P_vs_Tor

[8] A. Ali, M. Khan, M. Saddique, U. Pirzada, M. Zohaib, I. Ahmad, and N. Debnath, “TOR vs I2P: A comparative study,” in *2016 IEEE International Conference on Industrial Technology (ICIT)*, 2016, pp. 1748–1751.

[9] M. Ehlert, “I2P Usability vs. Tor Usability: A Bandwidth and Latency Comparison,” 2011. [Online]. Available: https://www.freehaven.net/anonbib/cache/ehlert2011:usability-comparison-i2p-tor.pdf