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*—Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.**

***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, characterised 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. Aim and 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 anonymisation 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 utilised 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?

D. Delimitations of the Study

TODO

II. Literature Review

A. Overview of Tor and I2P Networks

Understanding the fundamentals of TOR and I2P networks is crucial for evaluating their performance, privacy, and security. This section provides a comprehensive overview of these networks, discussing their architectures, functionalities, and core principles.

1) The TOR Network: TOR (The Onion Router) is an anonymity network designed to protect users' privacy and freedom online by routing their internet traffic through a series of volunteer-operated servers. This multi-layered approach ensures that no single point can compromise user anonymity. TOR uses a technique called onion routing, where data is encrypted in multiple layers and sent through a circuit of randomly selected TOR relays. Each relay decrypts one layer before passing the data to the next relay. This method helps in concealing the user's IP address and the destination of the data [10]. TOR aims to provide online anonymity and resist traffic analysis. TOR has a larger user base and more relays compared to I2P, which helps in distributing traffic load more effectively and providing better performance under high demand. The larger network also contributes to stronger anonymity due to the increased difficulty of performing traffic analysis on a larger number of users. It supports various applications that use the TCP protocol, including web browsing, instant messaging, and secure shell (SSH) connections [10].

2) The I2P Network: I2P (Invisible Internet Project) is another anonymity network designed to facilitate secure and anonymous communication. Unlike TOR, which is optimised for accessing the regular internet anonymously, I2P is designed primarily for internal anonymous services. I2P uses a peer-to-peer model and builds a decentralised, self-organising network. It employs garlic routing, a variant of onion routing, where multiple messages are bundled together to improve efficiency and reduce the risk of correlation attacks. I2P's smaller and more community-driven network emphasises decentralisation and resilience against central points of failure, which enhances its security but can affect its scalability and overall performance under heavy load [3]. I2P provides various applications for anonymous browsing, chatting, and file sharing. It supports both TCP and UDP protocols and includes tools like I2P-Bote for anonymous email, and I2P torrents for anonymous file sharing [11].

B. Comparative Metrics for Anonymity Networks

1) Privacy Metrics: TODO @Fernando

2) Security Metrics: TODO @Gustav

3) Performance Metrics: Performance is a critical aspect of evaluating anonymity networks, as it directly impacts user experience and the practicality of the network for various applications. Two fundamental metrics used to measure the performance of anonymity networks are latency and throughput.

Latency, often referred to as delay, is defined as the time interval between the initiation of a request and the reception of the corresponding response [12]. In the context of anonymity networks like TOR and I2P, latency is influenced by several factors including the number of nodes in the network path, the processing time at each node, and the overall network congestion. High latency can significantly

degrade the user experience, making real-time applications such as voice or video communication difficult to use. According to Dingledine et al., the latency in TOR is affected by the need to route traffic through multiple relays, which introduces additional processing and transmission delays at each hop [10]. Similarly, I2P's latency is influenced by its routing mechanism, which also involves multiple hops to maintain anonymity [3]. Understanding latency is crucial for evaluating the efficiency of anonymity networks, as it directly impacts the usability of services running over these networks.

Throughput is the rate at which data is successfully transmitted from one point to another in a given time period. In anonymity networks, throughput is affected by the bandwidth limitations of individual nodes, the encryption and decryption processes, and the overall network traffic load. High throughput is essential for applications that require large amounts of data to be transferred quickly, such as file sharing or streaming services. Studies have shown that TOR's throughput can be limited by the bandwidth of the volunteer-operated relays and the need for encryption at each hop [10]. I2P, on the other hand, faces similar challenges due to its peer-to-peer architecture, which relies on the bandwidth and availability of participating nodes [3]. High throughput is indicative of a network's ability to handle large volumes of traffic efficiently, which is essential for assessing the scalability and performance of anonymity networks.

C. Existing Comparative Studies

Existing comparative studies on the performance, privacy, and security of anonymity networks like TOR and I2P provide valuable insights into their operational characteristics and effectiveness. This section reviews significant comparative studies to highlight the methodologies and findings relevant to understanding these networks while highlighting the need for more comparative studies like this paper.

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 analyse 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. Jansen et al. conducted a comprehensive performance analysis of the TOR network, focusing on metrics such as latency and throughput. They found that TOR generally provides higher latency compared to conventional networks due to its multiple relay nodes but still offers acceptable performance for non-interactive applications [13]. Johnson et al. compared the security vulnerabilities of TOR and I2P, focusing on their susceptibility to traffic analysis attacks. The study concluded that TOR's design is more robust against traffic correlation attacks due to its larger and more diverse network, but I2P's decentralised approach offers significant resilience against single-point failures [14]. Overlier and Syverson (2006) present a comprehensive comparison of TOR and I2P, evaluating both performance and security aspects. They highlighted the trade-offs between performance and security, noting that while TOR offers better performance metrics, I2P's architecture provides certain security advantages due to its decentralisation [15].

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 and structured comparative analysis based on the three factors Privacy, Security and Performance of these essential privacy technologies.

III. Methodology

A. Research Design

B. Data Collection Method

1) Data Collection for Privacy:

2) Data Collection for Security:

3) Data Collection for Performance: To compare the performance of the TOR network and the I2P network in terms of latency and throughput, we designed experiments aimed at gathering quantitative data. This chapter details the methodology employed to collect sufficient and reliable data, ensuring consistency and minimising external variations. The primary objective of these experiments was to measure and compare the latency and throughput of the TOR and I2P networks. Latency is defined as the time taken for a data packet to travel from the source to the destination, while throughput refers to the rate at which data is successfully transferred from one point to another within a network.

a) Experimental Setup: To ensure consistency in our measurements, we utilised identical hardware (Kali VM) for running both TOR and I2P. Both networks were configured to run their latest stable versions to reflect current performance accurately. The experiments were conducted under similar network conditions, such as the time of day and general network traffic, to minimise external variations that could impact the results.

b) Measurement: The measurements were conducted using a Python script designed to access 50 commonly used hidden services (.i2p for I2P and .onion for TOR) to reflect browsing behaviour. Each website was accessed 10 times, resulting in a total of 500 requests per network.

To measure latency, the Python script sent HTTP GET requests to each of the 50 websites. The script recorded the time taken for each website to respond to the request. Specifically, the latency was defined as the duration between the initiation of the request and the receipt of the first byte of the response. This approach provides an accurate measure of the network's responsiveness.

Throughput was measured based on the time required to fully load the website and the size of the content delivered to the client. For each HTTP GET request, the Python script tracked the total amount of data received and the time taken to complete the data transfer. Throughput was then calculated using the formula:

$$\text{Throughput (KB/s)} = \frac{\text{Total Data Received (KB)}}{\text{Total Time Taken (s)}}$$

This calculation provided a clear indication of the network's data transfer capabilities under typical usage conditions. The latency and throughput data for each request were stored in a structured format (CSV) for subsequent analysis.

C. Data Analysis Method

1) Data Analysis for Privacy:

2) Data Analysis for Security:

3) Data Analysis for Performance: The objective of the data analysis is to identify and quantify differences in latency and throughput between the two networks, using various statistical measures and visual representation techniques.

a) Data Preprocessing: Before analysis, the raw data collected from the latency and throughput experiments is cleaned and organised. This involves removing data from incomplete requests that could skew results, ensuring consistency in the data format for both networks.

b) Statistical Measures: To comprehensively compare the performance of TOR and I2P, several key metrics are calculated:

1) Successful requests (*succ.*) to indicate how many of the 500 requests were successful and thus show how many valid data points the evaluation is based on for each network.
2) Average/Mean (*mean*) to provide a central value that represents typical performance, facilitating straightforward comparisons.
3) Minimum (*min*) and Maximum (*max*) to help identify the range of performance and the best and worst-case scenarios for each network.
4) Standard Deviation (*std_dev*) to indicate the consistency of network performance; a lower standard deviation signifies more stable performance.
5) 90th Percentile (*perc_90*) to understand the performance distribution and identifying how often high latencies or low throughputs occur.

To calculate these metrics, Python and pandas dataframes were used.

c) Interpretation and Contextualisation: The final step in the data analysis method involves interpreting the results and placing them in context. First we identify key differences by highlighting significant differences in the performance metrics of TOR and I2P and discussing potential reasons for these differences based on network architecture, usage patterns, and technological advancements. And finally we discuss the practical implications of the findings for users of TOR and I2P and provide recommendations based on the comparative analysis, such as which network may be more suitable for specific use cases.

D. Research Ethics

IV. Results

A. Privacy

1) Utilised Anonymization Techniques:

2) Associated Vulnerabilities:

B. Security

1) Utilised Encryption Algorithms & Protocols:

2) Robustness Against Common Attacks:

C. Performance

1) Latency Results: The latency experiments involved sending HTTP GET requests to 50 commonly used hidden services on each network, with each website being requested 10 times, totalling 500 requests per network. The table below summarises the key latency metrics in seconds for both networks:

	succ.	**mean**	**min**	**max**	**std_dev**	**perc_90**
I2P	479/500	0.73	0.40	60.49	2.08	0.71
TOR	361/500	6.02	0.59	29.96	5.81	13.36

The success rate indicates the number of successful HTTP GET requests out of the total 500 attempts. I2P had a higher success rate with 479 successful requests compared to TOR's 361 successful requests. This suggests that I2P is more reliable in terms of successfully retrieving web content from hidden services. This may be due to the selection of hidden services in the respective network (i.e. the selection of the 50 frequently used sites in the Tor network included more websites that are already offline)

The mean latency for I2P was significantly lower at 0.73 seconds compared to TOR's 6.02 seconds. This substantial difference highlights I2P's faster average response time, making it more efficient for accessing web content with lower latency.

The minimum latency recorded for I2P was 0.40 seconds, while TOR's minimum latency was slightly higher at 0.59 seconds. Although both networks showed relatively low minimum latency values, I2P still demonstrated a slight edge in the best-case scenario.

I2P exhibited a much higher maximum latency of 60.49 seconds, indicating occasional extreme delays. In contrast, TOR's maximum latency was 29.96 seconds, which, while still significant, was lower than I2P's maximum. These extreme values

highlight potential instability or outlier conditions within the I2P network.

The standard deviation of latency provides insight into the variability of response times. I2P had a standard deviation of 2.08 seconds, whereas TOR's standard deviation was significantly higher at 5.81 seconds. This indicates that TOR's latency is more variable and less consistent compared to I2P.

The 90th percentile latency, which indicates the latency below which 90% of the HTTP GET requests fall, was 0.71 seconds for I2P and 13.36 seconds for TOR. This further illustrates I2P's superior performance, as the vast majority of its requests experienced low latency, whereas TOR's latency was much higher for a significant portion of requests.

2) Throughput Results: The throughput experiments involved sending HTTP GET requests to 50 commonly used hidden services on each network, with each website being requested 10 times, totalling 500 requests per network. The table below summarises the key throughput metrics in kB/s for both networks:

	succ.	**mean**	**min**	**max**	**std_dev**	**perc_90**
I2P	479/500	9.24	0.02	436.04	34.92	4.28
TOR	361/500	23.31	0.02	333.35	48.90	66.60

The mean throughput for TOR was significantly higher at 23.31 KB/s compared to I2P's 9.24 KB/s. This indicates that, on average, TOR is capable of achieving higher data transfer rates than I2P, making it potentially more suitable for applications requiring higher throughput.

Both I2P and TOR exhibited a minimum throughput of 0.02 KB/s. This indicates that in the worst-case scenarios, both networks can experience extremely low data transfer rates, highlighting occasional performance bottlenecks or network congestion.

I2P exhibited a higher maximum throughput of 436.04 KB/s, while TOR's maximum throughput was 333.35 KB/s. These values indicate that I2P is capable of achieving higher peak data transfer rates under optimal conditions compared to TOR.

The standard deviation of throughput provides insight into the variability of data transfer rates. TOR had a higher standard deviation of 48.90 KB/s compared to I2P's 34.92 KB/s. This suggests that TOR's throughput is more variable and less consistent than I2P's.

The 90th percentile throughput, which indicates the throughput below which 90% of the HTTP GET requests fall, was 4.28 KB/s for I2P and 66.60 KB/s for TOR. This further illustrates TOR's superior performance in terms of higher throughput for the majority of requests, while I2P's throughput tends to be lower.

V. Discussion

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

[10] M. N. S. P. Dingledine, R., "Tor: The second-generation onion router," in *USENIX Security Symposium*, vol. 13, 2004, pp. 303–320.

[11] B. Zantout and R. Haraty, "I2p data communication system," 04 2002.

[12] W. Stallings, *Data and Computer Communications*, 7th ed. Pearson Prentice Hall, 2004.

[13] R. Jansen, A. Johnson, and P. Syverson, "Lira: Lightweight incentivized routing for anonymity," in *Proceedings of the Network and Distributed System Security Symposium (NDSS 2013)*, 2013. [Online]. Available: https:

//www.ndss-symposium.org/ndss2013/ndss-2013-programme/lira-lightweight-incentivized-routing-anonymity/

[14] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson, "Users get routed: Traffic correlation on tor by realistic adversaries," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*. ACM, 2013, pp. 337–348.

[15] L. Overlier and P. Syverson, "Locating hidden servers," in *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P '06)*. IEEE, 2006, pp. 15–pp.