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*—This paper presents a comparative study of the TOR and I2P networks, focusing on their privacy, security, and performance attributes. TOR uses Onion Routing and robust encryption protocols but is vulnerable to traffic correlation and Sybil attacks. In contrast, I2P employs Garlic Routing, offering enhanced resistance to traffic analysis and lower latency but is susceptible to denial-of-service attacks. Performance comparisons indicate that TOR achieves higher throughput, albeit with greater variability, while I2P provides more consistent and lower latency performance. The discussion highlights the trade-offs between the two networks, suggesting that the choice depends on specific user requirements.**

***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

There are various delimitations which encompass this study, they stem out of necessity to narrow the scope and guarantee a focused approach towards the privacy, security, and performance metrics of the TOR and I2P networks. Our research primarily utilizes data from secondary sources such as comparative studies, technical documentation, academic journals, however original empirical analysis were done in the performance section and subsequently incorporated into the report. This includes calculations of mean, median, mode, and other statistical measures derived from latency and throughput experiments. The inclusion of this empirical analysis provides a more robust and nuanced understanding of the networks' performance metrics but confines the scope to the specific parameters examined in these experiments.

Additionally, the approach for this study targets key metrics in their respective sub-categories such as privacy (anonymity, pseudonymity, unlinkability, and unobservability), security (encryption algorithms and resistance to common attacks), and performance metrics (latency and throughput). The report exempts other potential features involving broader stability problems and usability, meanwhile no consideration is also had for the impact of emerging technologies on these networks. Furthermore, given there are various possible threat models, the comparative structure of this report focuses only on the aforementioned sub-categories, comprising general characteristics and typical scenarios between TOR and I2P. The comparative analysis employs qualitative methods to identify patterns and insights from the existing literature. This choice aligns with the goals of the research but may limit the generalizability of the findings as the results are context-specific.

Lastly, while the study aims to provide a thorough and balanced examination of TOR and I2P, it acknowledges that the findings are based on a specific set of metrics and conditions. Any research accomplished in the future could expand on this work through the inclusion of a broader range of metrics, diverse use cases, and further empirical studies to receive a holistic view of these two networks. By outlining these delimitations, the study aims to provide a clear and focused analysis while acknowledging the areas for future research and potential improvements.

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: Anonymity refers to the ability of the network to hide the user's identity from both the intermediate nodes and the destination server. In TOR, this is achieved through Onion Routing, where each relay only knows its predecessor and successor, not the entire path or the original sender [4] [12]. In I2P, anonymity is maintained through Garlic Routing, which bundles multiple messages together, making it harder to trace individual messages back to their source [8].

Pseudonymity allows users to interact within the network using pseudonyms or aliases without revealing their true identities. This is crucial for maintaining long-term user privacy while allowing for persistent identities. Both TOR and I2P support pseudonymity through their routing mechanisms and encryption protocols [8].

Unlinkability ensures that multiple uses of the network by the same user cannot be linked together. This metric is essential for preventing adversaries from building profiles based on user behavior. TOR's circuit-based approach can sometimes pose risks to unlinkability if circuits are reused for multiple TCP connections. I2P's use of separate inbound and outbound tunnels helps maintain better unlinkability [4] [12].

Unobservability is the ability of the network to conceal the very act of using an anonymity network. This metric is important for users in environments where the use of such networks might attract suspicion. TOR and I2P both strive for unobservability, but the former's susceptibility to traffic correlation attacks and ladders risk from Sybil attacks present challenges [8].

Clear definitions of privacy metrics (anonymity, pseudonymity, etc.) will create a framework to assess how well TOR and I2P protect user privacy. The analysis will involve network performance under various conditions and pinpoint areas for improvement.

2) Security Metrics: Security is an important factor to consider when analysing anonymity networks. If the user does not perceive an anonymity network as secure they are less likely to use it. One common way to measure security in anonymity networks is the resistance to common attacks like sybil attacks, traffic analysis, timing attacks and denial of service attacks. The mentioned attacks impact on Tor and I2P security are discussed. Sybil attacks- which can be described as an attacker who creates a huge number of pseudonymous identities and utilises them to have an excessive significant influence over a computer network service. The two networks appear to be susceptible to attacks where the attacker creates multiple fake nodes to control the network. Ali et al. [8] however, states that I2P is not vulnerable to Sybil attacks, perhaps they assess that the security mechanisms are sufficient against Sybil attacks. Historically Tor has been affected by Sybil attacks [13].

Related to Tor and I2P, traffic analysis is mitigated through strong encryption protocols that can identify odd traffic patterns. I2P's garlic routing makes it more difficult to perform traffic analysis because it bundles messages. Both networks are susceptible to timing attacks, though TOR's layered encryption and I2P's message bundling provide some mitigation. Erdin et al. [14] explains timing attacks, the timing pattern of the packets can be utilised to determine the identity of a user as their traffic passes through a specific circuit. An attacker monitoring the data stream's inflow and outflow can establish a connection between the source and the destination, risking the anonymous communication's endpoints.

Continuing with Denial of service attacks and how Tor deals with it. Because of its better organised network and entry guards, it often has a moderate resistance to denial of service attacks. Targeted node attacks and resource exhaustion can still affect it, however. Moving on to I2P it provides a strong decentralised architecture with some degree of defence against denial-of-service assaults. Although its dynamic tunnel design helps to lessen impacts, severe attacks can still cause flooding and performance deterioration. Ali et al. [8] explains how I2P is less vulnerable to Dos attacks in comparison to Tor.

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 [15]. 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 [16]. 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 [17]. 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 [18].

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

The research design employs a mixed-methods approach, integrating quantitative performance testing with qualitative examination of the body of current literature. This method enables a deeper understanding of the networks' advantages and disadvantages.

1) Qualitative Analysis: To learn more about the privacy and security features of TOR and I2P, a comprehensive analysis of the body of research, technical papers, and comparative studies is conducted. This involves reviewing a wide range of academic and industry literature to understand the underlying architecture and protocols of each network. Case studies and known vulnerabilities help us understand the advantages and disadvantages of TOR and I2P in various situations.

2) Quantitative Analysis: This involves measuring and contrasting the latency and throughput of both networks under controlled circumstances through experimental performance testing. By setting up identical test environments for TOR and I2P, we can systematically measure how each network handles data transmission. To evaluate each network's maximum throughput, average latency, and stability under different loads, we run a number of tests. To guarantee the accuracy and consistency of the results, these tests are conducted several times.

B. Data Collection Method

1) Data Collection for Privacy: For the privacy section on comparing TOR and I2P, its data will be collected through comprehensive review from existing literature. This will be specifically sourced from academic journals, comparative studies, and relevant sites. Cornerstone works, which delve into foundational comparisons on privacy , such as "A Survey on Tor and I2P" by Conrad and Shirazi [4], and "TOR vs I2P: A Comparative Study" by Ali et al. [8] will be utilised. Additionally, technical documents from Tor and I2P will be reviewed to understand their specific protocols and weaknesses. Comparative metrics and prior findings will be extracted from relevant comparative studies such as the one by Akbarifar and Shirvani [1] to allow precise evaluations of strength and weaknesses of each network in different contexts.

The data collection process will involve further refinement according to important themes such as associated vulnerabilities and anonymization techniques. Furthermore, anonymization protocols will be meticulously analysed including relevant protocol designs, security features, and any documented vulnerabilities. As a result, the extrapolated data will allow, based on a comprehensive overview, better understanding on the privacy mechanisms and vulnerabilities of both networks. Given that both TOR and I2P support and maintain user anonymity, understanding exactly where their differences and similarities lie are crucial. A thorough and nuanced understanding, by leveraging data from credible sources, will be established in regard to privacy protections and vulnerabilities offered by TOR and I2P.

2) Data Collection for Security: Security data will be gathered by analysing the encryption algorithms and protocols used by TOR and I2P. This includes reviewing technical documentation and research papers. Specific focus will also be on the robustness of these networks against common attacks such as Sybil attacks, Traffic analysis attacks, Timing attacks and DoS attacks.

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: Utilizing the existing literature as our main source of analysis, the approach will involve a combination of qualitative methods and thematic evaluation obtained from the literature. Moreover, the primary focus, in terms of assessing the effectiveness of these anonymity networks, will be to define and explain all applicable privacy metrics.

Qualitative data from gathered documents, such as comparative studies, will be thematically analyzed to identify patterns and insights related to the anonymization techniques and vulnerabilities of TOR and I2P. It is as follows:

- Coding and Categorization: Extracting key themes and categorizing the data into meaningful clusters such as ”anonymization techniques,” ”known vulnerabilities,” and ”attack scenarios.”
- Pattern Recognition: Identifying recurring themes and patterns that highlight the strengths and weaknesses of each network. For example, common vulnerabilities identified in multiple studies will be highlighted and analyzed in depth.

2) Data Analysis for Security: The selected data analysis method is to perform a literature review and comparative analysis of the security of Tor and I2P networks. The effectiveness of encryption algorithms and protocols will be evaluated based on documented vulnerabilities and resistance to specific attacks.

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*

To maintain the integrity and validity of our research, we have followed ethical guidelines in performing this comparison of the TOR and I2P networks. The following factors were considered when designing our research:

1) Data Integrity and Accuracy: We have collected and examined data from credible and trustworthy sources, such as research papers, technical documents, and case studies from the past. We made sure that the information we found was accurate and trustworthy by cross-referencing several sources.
2) Transparency: We kept the study process transparent by outlining all of our procedures, including how we collected and analysed data. This enables other researchers to validate and replicate our findings.
3) Respect for Privacy: We made extra precautions to protect users' privacy because anonymity networks are delicate. We didn't use any intrusive methods or gather any personal information from network users; instead, we concentrated on publicly available data for our analysis.
4) Objective and Unbiased Analysis: We took an impartial stance when conducting our comparison analysis, offering a fair assessment of both TOR and I2P networks. In order to ensure a fair and impartial assessment, our debate points bring both the networks' advantages and disadvantages without favouring one over the other.
5) Acknowledgment of Sources: Information and data sources utilised in this study are properly credited, acknowledging the original authors and adding to the body of knowledge on anonymity networks in academia.

IV. RESULTS

A. *Privacy*

1) Utilised Anonymization Techniques: TOR's Onion Routing utilizes a method where data packets are wrapped in multiple layers of encryption, each peeled away by successive nodes until the packet reaches its destination. This method ensures that no single node can trace the packet's entire path, maintaining user anonymity. Conversely, I2P's Garlic Routing bundles multiple messages into a single, encrypted packet. Each message within the bundle can be routed independently, enhancing resistance to traffic analysis by making it more difficult to trace individual messages back to their source. This decentralized approach spreads the routing responsibilities across many nodes, further complicating traffic analysis efforts [4] [8] [12].

2) Associated Vulnerabilities:

a) TOR: One of the primary vulnerabilities of TOR is its susceptibility to traffic correlation attacks. An adversary monitoring both the entry and exit points of the network can correlate traffic patterns, potentially deducing the source and destination of data. This is feasible if the adversary controls or observes a significant number of nodes [8]. Additionally, timing attacks, where an adversary analyzes the timing of packet transmissions, can correlate activities between entry and exit nodes to infer user identities or content of communications [4]. TOR's exit nodes can also pose risks if traffic is not end-to-end encrypted, allowing malicious exit nodes to read, modify, or log data [8]. A recent security audit revealed a high-risk CSRF vulnerability in the Onion Bandwidth Scanner (Onbasca), which could allow attackers to inject malicious bridges into the network, compromising its integrity [19].

b) I2P: I2P is susceptible to Sybil attacks, where an adversary generates a large number of fake identities (nodes) to control a substantial portion of the network. This can disrupt routing mechanisms and deanonymize users by correlating traffic through controlled nodes [4] [8]. Flooding attacks are another significant threat, where excessive traffic overwhelms the network, degrading performance and potentially leading to denial of service [4]. I2P's reliance on unidirectional tunnels means compromising a single tunnel can expose the entire communication flow for that direction. Constantly rebuilding tunnels to prevent traffic analysis can introduce vulnerabilities if not managed correctly [4].

B. Security

1) Utilised Encryption Algorithms & Protocols: The results showed that both TOR and I2P have strong security features and distinctive methods for data protection and encryption. When it comes to encryption algorithms and protocols. Tor uses RSA encryption for establishing keys with 1024-bit RSA keys and AES is used for data encryption within the circuit with 128-bit AES in counter mode [20]. Diffie Hellman is also used for forward secrecy which makes sure that session keys are derived securely and not retroactively decrypted if keys are compromised. Tor uses the TLS protocol for securing communications and Onion routing for creating multiple layers of encryption [1].

I2P uses the encryption algorithms ElGamal/AES for end-to-end encryption [7]. Messages are encrypted with ElGamal keys and then with AES-256 for data encryption. Elliptic Curve Digital Signature Algorithms are used for signing messages. AES-256 is also used for tunnel encryption. The website of the I2P project [21] explains that I2P uses the protocols Garlic Routing, NTCP (NTCP2) and SSU (Secure Semantics UDP). Garlic Routing is similar to onion routing but with "garlic" cloves, where multiple messages are bundled together, making it harder to perform traffic analysis. NTCP (NTCP2) is a network protocol for establishing and managing encrypted communication channels. SSU is a protocol for encrypting and authenticating UDP communication.

2) Robustness Against Common Attacks: Sybil attacks involve creating numerous fake identities to control a network, and both Tor and I2P can be susceptible, though I2P is considered more resilient. Tor has historically faced Sybil attacks, while I2P's security mechanisms are assessed to be sufficient against them. I2P's garlic routing makes traffic analysis harder by bundling messages together, which complicates identifying traffic patterns. Both networks are vulnerable to timing attacks, where monitoring packet timing can reveal user identities, despite Tor's layered encryption and I2P's message bundling providing some mitigation. Tor offers moderate resistance to denial-of-service (DoS) attacks due to its organised network and entry guards, but targeted node attacks can still impact it. I2P's decentralised architecture and dynamic tunnel design provide defence against DoS attacks, though severe attacks can still cause flooding and performance issues. Overall, while both networks have robust security measures, they each have specific vulnerabilities that attackers can exploit.The decision between choosing either network is based on particular use cases and threat models that users face.

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

This chapter discusses the findings from our study, comparing the TOR and I2P networks in terms of privacy, security, and performance. Our primary research question is: How do the TOR and I2P networks compare in terms of privacy, security, and performance? To address this, we have derived sub-questions for each factor, which we will explore methodically in the following sections.

A. Privacy

TOR uses Onion Routing, which involves wrapping data packets in multiple layers of encryption. Each layer is peeled away by successive nodes, ensuring that no single node knows the entire path of the packet, thereby preserving user anonymity. This method provides robust anonymity but can be vulnerable to certain types of traffic analysis if an adversary can observe both the entry and exit nodes. In contrast, I2P employs Garlic Routing, which bundles multiple messages into a single, encrypted packet. Each message within the bundle can be routed independently, enhancing resistance to traffic analysis. This decentralized approach spreads the routing responsibilities across many nodes, making it more difficult for an adversary to trace individual messages back to their source. The increased complexity of I2P's routing method can provide superior anonymity in certain scenarios.

TOR's primary vulnerability lies in its susceptibility to traffic correlation attacks. If an adversary can monitor both the entry and exit points of the network, they can correlate traffic patterns to identify users. The relatively small number of exit nodes also increases the risk of traffic analysis attacks, making it easier for adversaries to perform such correlations. I2P, designed to resist traffic analysis through its dynamic tunnel creation and layered encryption, faces different challenges. Its nodes can be susceptible to denial-of-service (DoS) attacks, which can flood the network, compromising performance and, consequently, anonymity. Both networks also face threats from Sybil attacks, where an adversary controls a large number of nodes to disrupt the network's integrity. While I2P's decentralized nature provides a layer of resistance, it is not immune to such attacks.

B. Security

TOR uses a combination of RSA encryption for session establishment and AES for data encryption within the circuit. This includes the use of Diffie-Hellman for forward secrecy, ensuring that session keys are derived securely and not vulnerable to retroactive decryption. These robust encryption protocols make TOR highly secure against many types of cryptographic attacks. I2P, on the other hand, utilizes ElGamal/AES for end-to-end encryption, with elliptic curve cryptography for signing messages. I2P also employs AES-256 for tunnel encryption, combining Garlic Routing and the Secure Semireliable UDP (SSU) protocol for enhanced security. The use of elliptic curve cryptography provides I2P with an edge in computational efficiency and resistance to future quantum attacks, making it a strong contender in terms of security.

Both TOR and I2P are designed to be robust against many common attacks, yet they each have specific vulnerabilities. TOR's architecture makes it vulnerable to traffic correlation and Sybil attacks, where adversaries could potentially compromise multiple nodes to analyze traffic patterns and deanonymize users. I2P's dynamic tunnel design offers better resistance to traffic analysis but can be vulnerable to DoS attacks that target the network's capacity. In terms of encryption, both networks employ strong algorithms; however, I2P's use of more recent elliptic curve cryptography provides a slight edge in terms of computational efficiency and future-proofing against quantum attacks.

C. Performance

Our latency experiments indicated that I2P generally offers lower latency compared to TOR. This lower latency is due to I2P's efficient handling of requests, which translates to faster access to resources and a more responsive user experience. The consistency of I2P's latency also suggests a more stable performance, making it suitable for applications where timely access to information is critical.

In terms of throughput, TOR demonstrated higher peak data transfer rates but with greater variability. This variability can affect the user experience, particularly in applications requiring consistent data transfer rates. While I2P's throughput is generally lower, it is more consistent, providing a more predictable performance. This consistency can be advantageous in scenarios where stability is more critical than peak performance.

D. Conclusion

In summary, TOR and I2P each have distinct strengths and weaknesses across privacy, security, and performance dimensions. Our study indicates that TOR excels in data transfer rates and provides strong encryption mechanisms but is more susceptible to traffic correlation and Sybil attacks. I2P offers lower latency and more consistent performance, with robust encryption and dynamic routing that enhances privacy. However, it can be vulnerable to DoS attacks.

The choice between TOR and I2P should be guided by the specific requirements of the user, considering the trade-offs in privacy, security, and performance. Future research could explore hybrid models that leverage the strengths of both networks, potentially providing a more comprehensive solution for secure and anonymous communication.

E. Future Research

Future research should aim to further compare and validate the findings of this study through diverse methodologies and experimental designs. Comparative studies involving larger and more varied datasets could provide a broader understanding of the performance and security nuances between TOR and I2P. Longitudinal studies observing these networks over extended periods could reveal how they adapt to evolving threats and user demands. Additionally, employing simulation models and real-world testing environments could offer more granular insights into the operational behaviors of both networks under different conditions. By integrating qualitative methods, such as expert interviews and user surveys, researchers could also gather contextual insights into the practical implications of using TOR and I2P, helping to triangulate quantitative data and enhance the robustness of the conclusions. These multifaceted approaches would contribute to a more comprehensive evaluation of these anonymization networks, guiding future enhancements and developments.

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] "What attacks remain against onion routing?" accessed 17.04.2024. [Online]. Available: https://support.torproject.org/about/attacks-on-onion-routing/

[13] "Tor security advisory: ”relay early” traffic confirmation attack," accessed 17.04.2024. [Online]. Available: https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack/

[14] E. Erdin, C. Zachor, and M. H. Gunes, "How to Find Hidden Users: A Survey of Attacks on Anonymity Networks," in *2015 IEEE Communications Surveys and Tutorials*, 2015, pp. 2296–2316.

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

[16] 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/

[17] 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.

[18] 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.

[19] E. Kovacs, "Tor Code Audit Finds 17 Vulnerabilities," accessed 17.04.2024. [Online]. Available: https://www.securityweek.com/tor-code-audit-finds-17-vulnerabilities/

[20] "Tor Specifications: Preliminaries," accessed 17.04.2024. [Online]. Available: https://spec.torproject.org/tor-spec/preliminaries.html

[21] "I2P: Intro," accessed 17.04.2024. [Online]. Available: https://geti2p.net/en/about/intro