sensors

MDPI

Article

Port-Based Anonymous Communication Network: An Efficient and Secure Anonymous Communication Network

Xiance Meng [1,2] and Mangui Liang [1,2,*]

[1] Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China; mengxiance@bjtu.edu.cn
[2] Beijing Key Laboratory of Advanced Information Science and Network Technology, Beijing Jiaotong University, Beijing 100044, China
* Correspondence: mgliang@bjtu.edu.cn

Abstract: With the rise of the internet, there has been an increasing focus on user anonymity. Anonymous communication networks (ACNs) aim to protect the identity privacy of users in the network. As a typical ACN, Tor achieves user anonymity by relaying user data through a series of relay nodes. However, this results in higher latency due to the transmission of network traffic between multiple nodes. This paper proposes a port-based anonymous communication network (PBACN) to address this issue. First, we propose a path construction algorithm. This algorithm describes constructing paths by partitioning the communication path information, which can reduce the probability of being discovered by adversaries. Secondly, we design a port-based source routing addressing method. During data transmission from the source to the destination, each node can directly forward the data by resolving the address into the port of each node. This method eliminates the need for table lookups, reducing the complexity of routing. Lastly, we propose an entropy-based metric to measure the anonymity of different ACNs. In terms of experimental evaluation, we quantitatively analyze the anonymity and end-to-end delay of various ACNs. The experimental results show that our proposed method reduces end-to-end delay by approximately 25% compared to Tor. When the adversary fraction is 20%, PBACN can improve the anonymity degree by approximately 4%.

Keywords: anonymous communication networks; anonymity; routing; Tor

Citation: Meng, X.; Liang, M. Port-Based Anonymous Communication Network: An Efficient and Secure Anonymous Communication Network. *Sensors* **2023**, *23*, 8810. https://doi.org/10.3390/s23218810

Academic Editors: Alexandros-Apostolos Boulogeorgos, Panagiotis Sarigiannidis, Thomas Lagkas, Vasileios Argyriou and Pantelis Angelidis

Received: 22 September 2023
Revised: 21 October 2023
Accepted: 27 October 2023
Published: 29 October 2023

1. Introduction

In the internet era, privacy protection and anonymity are becoming increasingly important [1]. Anonymous communication technology is essential for privacy protection, allowing users to communicate anonymously online and avoid surveillance and tracking. However, traditional anonymous communication schemes have high latency and poor anonymity. Therefore, designing an efficient and secure anonymous communication scheme is necessary.

DC-nets (Dining Cryptographers Networks) [2] allow users to exchange messages without revealing their identities. Each user encrypts the message using a secret key and sends it to all other users in the network [3]. Then, the members use a shared key that only they know to decrypt the message. Mix-net uses a series of nodes to confuse and forward messages, making tracing the message's source difficult. Each node in the network only knows the previous and next nodes in the chain and cannot link the message to its sender or receiver. However, these methods are generally plagued by problems such as high latency and poor scalability.

The P2P network [4–6] can also improve anonymous communication, in which users communicate directly without a central server. It can improve scalability and resilience but may also introduce new security risks, such as the possibility of Sybil attacks [7].

Dovetail [8] is an anonymous communication network based on the next-generation internet routing protocol. It provides anonymity against active attackers but still struggles to cope with traffic analysis attacks [9–11].

We aim to construct an anonymous communication method to achieve low-latency transmission and ensure anonymity. A common practice is to use relay routers to encrypt the data passing through and hide the actual information of the packets to improve anonymity. In addition to the delays caused by encryption and decryption, each relay router's transmission time will also increase relatively due to the longer transmission path and more nodes passing through. There are two main methods to reduce end-to-end transmission delay: one is to select nodes with high bandwidth or geographical distance preferentially [12,13] during the relay selection phase to minimize delay in the transmission process; the other is to reduce the number of relay nodes to reduce the transmission path. However, both methods will result in loss of anonymity.

The routing type used in Tor is called hop-by-hop routing. In Tor, each relay node decrypts the message to obtain the IP address of the next hop, and the communication process involves multiple routing lookups. The advantages of the source routing [14] protocol are as follows: the network topology is simpler, and there is no need to maintain complex routing tables, which can avoid data packet loss caused by routing loops and can calculate the shortest path faster, improving routing efficiency. In the case of expanding network scale, source routing can also maintain good scalability. Based on this, we designed an anonymous communication network based on port forwarding. During the routing process, intermediate nodes can directly parse the address into port numbers and forward the data through the corresponding ports. This method eliminates the need for table lookups, thus reducing the complexity of the switch. The reduction in switch complexity is beneficial for energy conservation, which also extends the network lifespan [15].

We evaluated the performance of PBACN and compared it with traditional Tor routing strategies. Due to the mechanism of anonymous communication networks, high latency has always been a common issue. Lower latency in anonymous communication networks will attract more users to join. The experimental results show that PBACN can provide better performance than other routing strategies.

We also analyzed the anonymity of PBACN. Anonymity is the most essential characteristic of anonymous communication networks. Higher anonymity means a higher probability that users will go unnoticed by adversaries in the network. The experimental results show that PBACN can improve anonymity, reduce the success rate of attackers, and thus increase user privacy and security.

The organizational structure of this article is as follows. In Section 1, we introduce the research background of this article. In Section 2, we present the related work. Section 3 introduces the design ideas and technical implementation of PBACN. We describe the performance evaluation of PBACN and compare it with traditional Tor routing strategies in Section 4. Then, in Section 5, we analyze the anonymity of PBACN. Finally, we summarize this article's work and propose future research directions.

2. Related Works

This section will introduce two research fields directly related to our problem: source-controlled routing protocols and network-layer anonymity protocols.

2.1. Source-Controlled Routing Protocols

Source-controlled routing protocols [16,17] are an essential topic for the next-generation internet routing scheme. The information carried in the packets by the initiator controls the routing information of data packets. This method of controlling routing information at the source has robustness and flexibility. It also has benefits because intermediate routers cannot obtain complete path information.

Our work is based on a new type of network addressing method called Vector Network (VN) [18,19]. VN is a source-controlled routing method in which each network node has a particular data-forwarding capability. When the source sends a data packet, the source node stores the sequence of the path in the packet header, and the length of each path segment is related to the number of ports on the node passed through. When the data

pass through each node, it will extract the corresponding port number and forward data to that port. At the same time, the extracted port number will also be removed from the path sequence. Since the source node defines the forwarding path of the data, the intermediate nodes do not need to query the routing table again during the data transmission process, thereby enhancing the robustness and flexibility of the network.

2.2. Low-Latency Anonymous Communication Systems

Some existing research has proposed low-latency anonymous communication schemes based on different routing strategies to meet the needs of some interactive applications, such as web browsing and instant messaging.

Tor can effectively protect users' identity and privacy, allowing users to be free from internet surveillance and tracking. When using Tor, users' network traffic is encrypted and transmitted. Each relay node can only decrypt the information of its next node, and so on, until the final node sends the information to the destination server. In this process, each node only knows the information of the previous and next nodes and does not know the source or destination of the data. It protects the user's IP address and location, thereby protecting their identity and privacy. Since Tor uses multi-layer encryption, it can protect user data from being stolen or tampered with. And because each node only knows the information of the previous and next nodes, even if a node is attacked or monitored, it cannot see the user's real identity and location.

HORNET [20] is a low-latency onion routing system implemented based on the next-generation network architecture. In HORNET, intermediate nodes only need to perform symmetric encryption on the packets. The sender establishes keys with each node along the path during the establishment process. Then, the sender embeds these keys and routing information into the packet header for transmission, thus achieving high scalability. Due to the packet header reused in HORNET, it cannot prevent replay attacks. So attackers can modify packets at will, making it difficult for users to distinguish between modified packets and legitimate packets. Adversaries can insert identifiable fingerprints in the traffic, which helps to de-anonymize the sender. Lightweight anonymous communication systems like LAP [21] and Dovetail [8] defend against topology attacks by encrypting routing information in the packet header. However, in both schemes, the packets remain unchanged during the transmission between hops, allowing adversaries to de-anonymize communication links by analyzing the correlation between packages at different nodes. TARANET [22] adopts end-to-end traffic shaping and packet fragmentation techniques to achieve anonymity at the network layer. It can even defend against active attacks but incurs specific latency.

T-hybrid [23] is a hybrid routing scheme that uses source routing between groups and hop-by-hop routing within groups. It combines mix-nets [24] with TPKE (Threshold Public-Key Encryption) [25] for better key management. The source selects multiple groups to generate the onion and encrypts by TPKE. Each receiving node generates its decryption share in each group and attaches it to the ciphertext. After the share number exceeds the threshold, the last node combines all shares and processes the onion. At the same time, symmetric encryption is used for each hop within the group. T-hybrid effectively combines onion routing with hop-by-hop routing, improving its resilience and increasing its latency by about 20%–25% compared to Sphinx [26].

As shown in Table 1, based on the comparison of existing research work, it is found that balancing anonymity and latency in anonymous communication networks is a challenging task. Taking Hornet as an example, although it has low latency, it faces challenges such as replay attacks. Compared to these anonymous communication networks, our designed port-based source routing addressing method can reduce routing complexity without affecting routing performance, thus achieving lower latency and ensuring anonymity.

Table 1. Comparison of anonymous communication systems.

ACNs	Routing Type	Latency	Challenge
Tor	hop by hop	middle	traffic analysis
LAP	source controlled	low	traffic analysis
Hornet	source controlled	low	replay attack
TARANET	source controlled	middle	increased latency
T-Hybrid	hybrid	middle	increased latency
Dovetail	source controlled	low	traffic analysis

3. Design

PBACN is an anonymous communication network based on port forwarding, which is efficient and has high anonymity. This section outlines the network model and describes the path construction and data packet-forwarding processes.

3.1. Network Model

PBACN consists of various nodes, including user nodes, web nodes, group leader nodes, and directory servers. Users are ordinary users who need anonymous access to the internet, web nodes are the standard websites accessed, and IN nodes are entry nodes in the relay group, which resolve the address assigned by the group leader and perform data forwarding. OUT nodes are the exit nodes in a relay group. They forward data to the next relay group's IN or web nodes. Group leaders are the leader nodes in a relay group, also known as relay group leaders. They are responsible for finding paths between group leaders and the path from the IN nodes to the OUT nodes. The directory server maintains the information of relays and group leaders.

In this network model, users first request to download relay group leader information from the directory server. The directory server randomly selects a part of the online node information from the maintained relay group leader list and sends it to the user. The directory server only knows the data of each group leader. Each group leader only knows the routing information between groups and within the group and does not know the routing information of other groups. If an attacker attempts to destroy the directory server, we only provide partial network information to users, thus protecting the network's anonymity.

3.2. Path Construction

In PBACN, path construction is relatively complex and requires a series of steps. The user first requests the relay group leader information from the directory server and obtains a random selection of online node information from the maintained relay group leader list. Next, the user must request inter-group paths and IN node to OUT node paths for each relay group leader. After the user selects the relay group leader and IN and OUT nodes, each group will generate paths between each node, using a source-controlled routing algorithm and feedback the path information to the sender, who will negotiate the key with each relay group leader, encrypt the data, and then transmit the encrypted data to the next node. The path construction process is described in Algorithm 1. Among them, the number of groups is g, and the list of the relay group leaders obtained by the user from the directory server is gl_list. $gl[i]$ is the relay group leader randomly selected by the user from the list. Once the relay group leader information is determined, the user will sequentially request the address information $addr[i]$ from the sender to the relay group leader and the destination. Finally, we can obtain the source-to-destination address all_addr by merging all the $addr[i]$. Assuming three groups and that the address $addr[i]$ for each segment from the source to the destination is $\{21, 34, 12, 11\}$. The address all_addr from the sender to the destination is $\{21341211\}$, which indicates the path from the sender to the destination.

Algorithm 1 Path construction algorithm

Require: A list of group leaders gl_list fetched from Directory Server, group number g;
Ensure: The address from the user to the website all_addr

for $i \leftarrow 0$ to $g-1$ **do**
  $gl[i] \leftarrow choose\_gl(gl\_list)$
end for
$addr[0] \leftarrow get\_addr(user, gl[0])$
for $i \leftarrow 0$ to $g-2$ **do**
  $addr[i+1] \leftarrow get\_addr(gl[i], gl[i+1])$
end for
$addr[g] \leftarrow get\_addr(gl[g-1], website)$
for $i \leftarrow 0$ to g **do**
  $all\_addr \leftarrow all\_addr + addr[i]$
end for
return all_addr

Next, we will introduce the complete design of PBACN hierarchically. As shown in Figure 1, the user requests the relay group leader information from the directory server and accesses the website through data forwarding based on the obtained information.

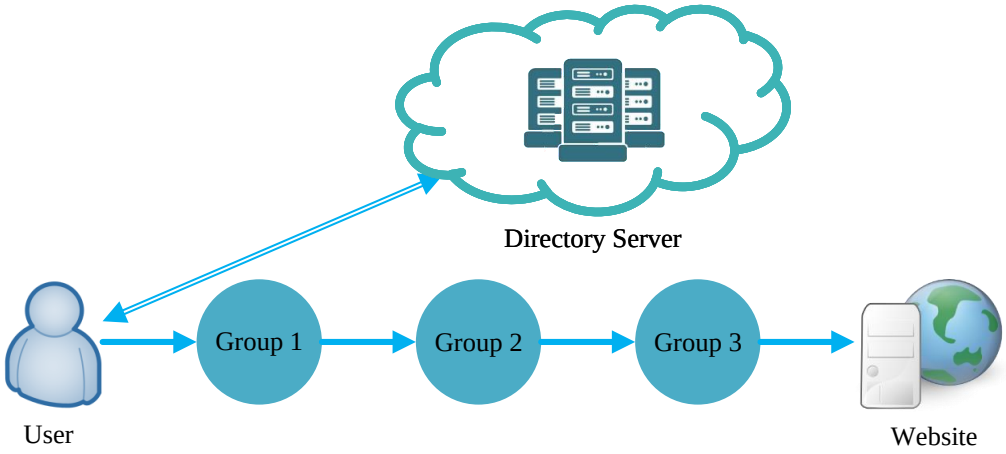

Figure 1. PBACN architecture with three groups.

In PBACN, the directory server can also register nodes and form groups. Any node with high bandwidth, online time, and routing capability can spontaneously register as a group leader. When the directory server receives an application, it will detect if there is a group leader online in the vicinity. The applying node will be registered as a group leader if there is none. Nodes near the group leader that are not part of any group will spontaneously query the directory server for nearby group leaders and join the group. Figure 2 shows the intragroup relationship diagram. After selecting IN and OUT nodes, IN nodes can access OUT nodes through the source routing method. As shown in the figure, after the message passes through the IN node, it can forward data through ports 1, 3, and 2 of each node because the source controls the path, so there is no need to use hop-by-hop routing, thereby saving routing time.

Figure 3 shows the complete architecture. The sender requests relay group leader (GL) information from directory servers. Then, it requests path information between these relay group leaders. Taking GL 1 as an example, GL 1 will request path information from the IN node to the OUT node and OUT to subsequent IN nodes in GL 1 and reply to the sender. In addition, the sender will negotiate keys with GLs separately and encrypt the transmitted data to avoid eavesdropping by adversaries.

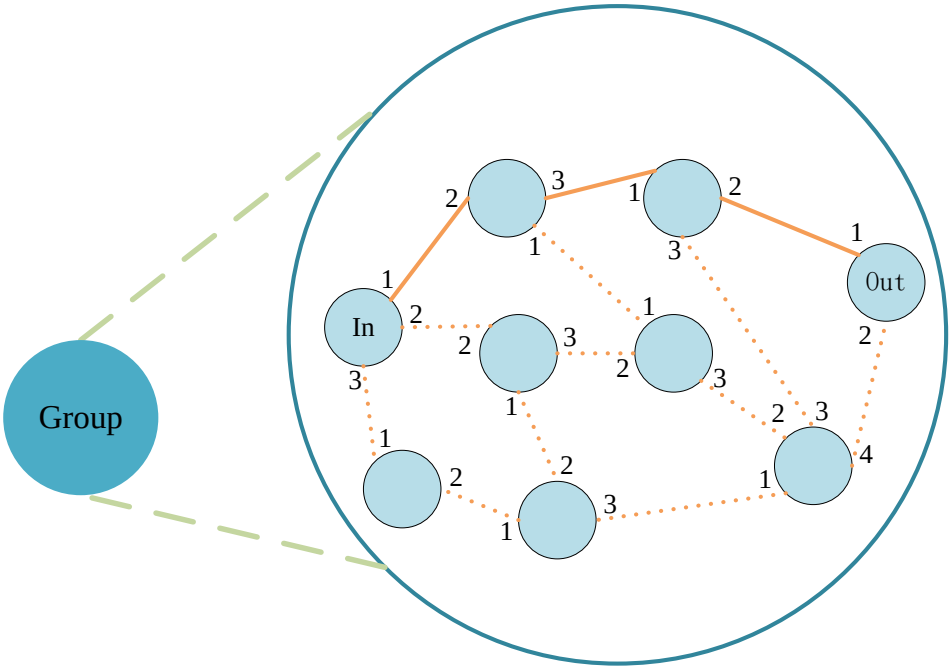

Figure 2. Network topology within the group.

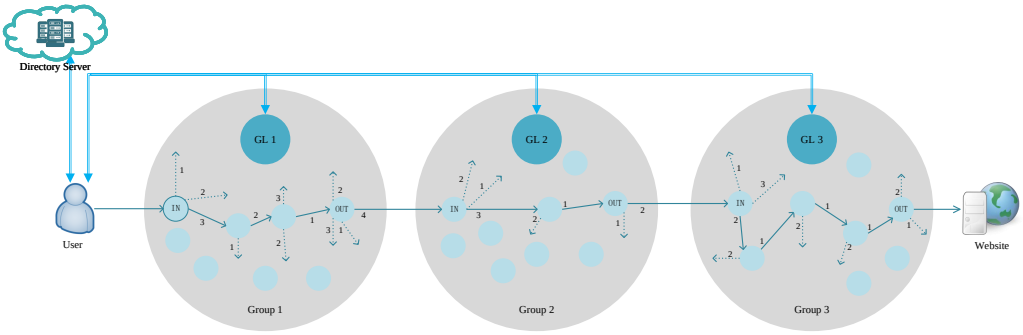

Figure 3. Overview of the PBACN.

These technologies provide good path construction and message transmission guarantees, making PBACN an efficient, real-time, secure, and reliable anonymous communication network.

3.3. Data Forwarding

In PBACN, data forwarding is performed through relay nodes. When a user wants to send a message, the message is first encrypted and sent to the IN node of the first relay group. This node forwards the message in turn until the message reaches the OUT node of the last relay group. Each node decrypts and forwards the message to the next node, ensuring message security and privacy. At the same time, we use relay groups to segment the path information so that directory server nodes and relay group leaders cannot grasp the complete path information, thus protecting the sender's privacy. In addition, source routing based on port forwarding is a very effective routing strategy in PBACN, which can significantly improve the performance of anonymous communication. The working principle of source routing is that when sending a message, the source node adds a set of routing information indicating how the message should reach the destination node. In the relay group, each node can directly parse the following hop address and forward the message to that address until the message reaches the target node location. Compared to the hop-by-hop routing method, this design reduces the table lookup time, as it does not require table lookups. In addition, this design separates the data plane from the control plane, with switches only responsible for data forwarding, and reducing the switches' complexity.

4. Performance Evaluation

We designed simulation experiments to compare and evaluate our proposed method with some existing research work, proving that our method is superior in reducing end-to-end delay, especially in complex data processing and network congestion cases. In addition, we also conducted a detailed analysis of the comparative results, pointing out the critical impact of end-to-end delay on network performance and user experience. The simulation demonstrates that our research can make some improvements in enhancing network transmission efficiency.

4.1. Performance Metrics

End-to-end delay is the time required for a data packet to travel from the sender to the receiver. Evaluating end-to-end delay can help us understand the performance of different methods and improve network transmission efficiency and user experience. In this article, we evaluated the performance of our proposed method and existing research work. We proved that our method is superior in reducing end-to-end delay, especially in complex data processing and network congestion cases.

In Section 2.1, we mentioned the concept of VN. As a source-controlled routing method, nodes only need to parse the address sent by the previous node into a port number and forward it directly when forwarding data. The node does not need to perform table lookup routing, reducing the routing complexity. Compared with existing research, our method can more accurately determine the transmission path of data packets and decrease the delay cost of hop-by-hop routing.

4.2. Simulation Design

We used OMNeT++ [27] to evaluate the performance of different solutions through simulation. We compared three solutions: Tor, T-Hybrid, and the PBACN proposed in this article.

In this experiment, we followed the process below:

1. Construct a simulated real network: We extracted node information by processing the Consensus file, which contains information such as node bandwidth and online time. We set the link parameters between nodes to construct a simulated real network, and Different IDs identify different nodes. Because we want to compare different methods, we designed different node processing rules to correspond to different methods during simulation.

2. Communication: We randomly selected two nodes as the source and destination nodes. The source initiates a communication request to the directory, and the directory queries the address and sends it to the source end. The source end resolves the address and forwards it layer by layer. Compared with other methods, the port-forwarding-based anonymous communication network we constructed does not require hop-by-hop routing, saving the time consumption of hop-by-hop routing and avoiding information leakage during the routing process, which is undoubtedly essential for anonymous communication networks.

4.3. Results Analysis

Tor is the most popular and widely researched low-latency anonymous communication network, providing sender privacy for internet users. T-Hybrid is the latest anonymous communication network that combines onion mix-net with hop-by-hop routing, offering excellent resilience and anonymity. Therefore, we evaluate and compare with the end-to-end latency of Tor and T-Hybrid.

Figure 4 compares the average end-to-end delay results. We simulated Tor, T-Hybrid, and PBACN in OMNeT++ and deployed 100 nodes. The nodes have the same bandwidth, and the links have the same latency. In each experiment, the sender and receiver are randomly selected. We conducted 100 experiments and recorded the end-to-end latency of each method in each experiment. The end-to-end delay is the difference between the

receiving and sending times. In every 20 experiments, we calculated the average end-to-end delay from the beginning to that moment. We used a histogram to present the experimental results, with the abscissa representing the number of experiments and the ordinate representing the average end-to-end delay for each corresponding experiment. We also added error bars to the graph to show that the data obtained are reliable because they exhibit minimal fluctuations. As shown in the diagram, we can observe that the end-to-end delay of PBACN is generally lower than other methods. Compared to Tor, our proposed method reduces the end-to-end delay by approximately 25%.

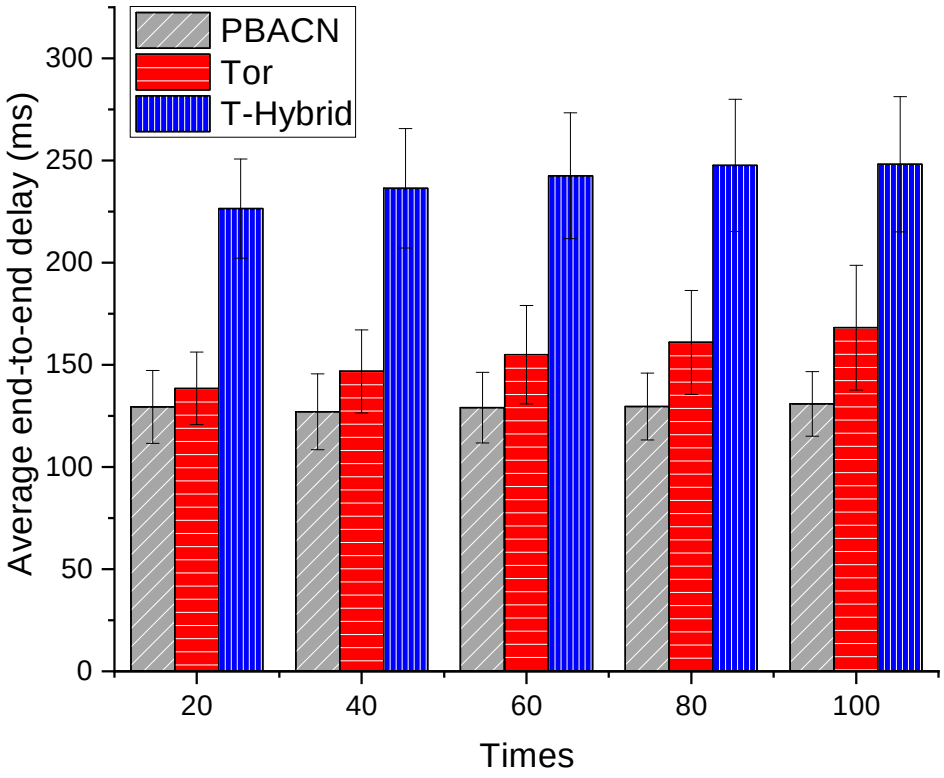

Figure 4. Comparison of average end-to-end delay results.

Figure 5 depicts different methods' CDF (cumulative distribution function) under various end-to-end delays. The x-axis represents the end-to-end delay, and the y-axis represents the CDF. The curves in the graph indicate the proportion of end-to-end delay for different methods in different intervals. We can see that the CDF of our proposed PBACN can reach one faster, indicating that the end-to-end delay of PBACN is much lower than 180 ms, while the maximum end-to-end delay of other methods is higher than that of PBACN.

In summary, onion-based ACNs such as Tor have multiple relays that introduce additional latency in both the encryption and decryption processes and the hop-by-hop routing process. On the other hand, mix-based ACNs such as T-Hybrid combine hybrid routing with TPKE for improved key management. However, each group receiving the mix must collaborate with the sender for cooperative encryption, resulting in additional latency costs.

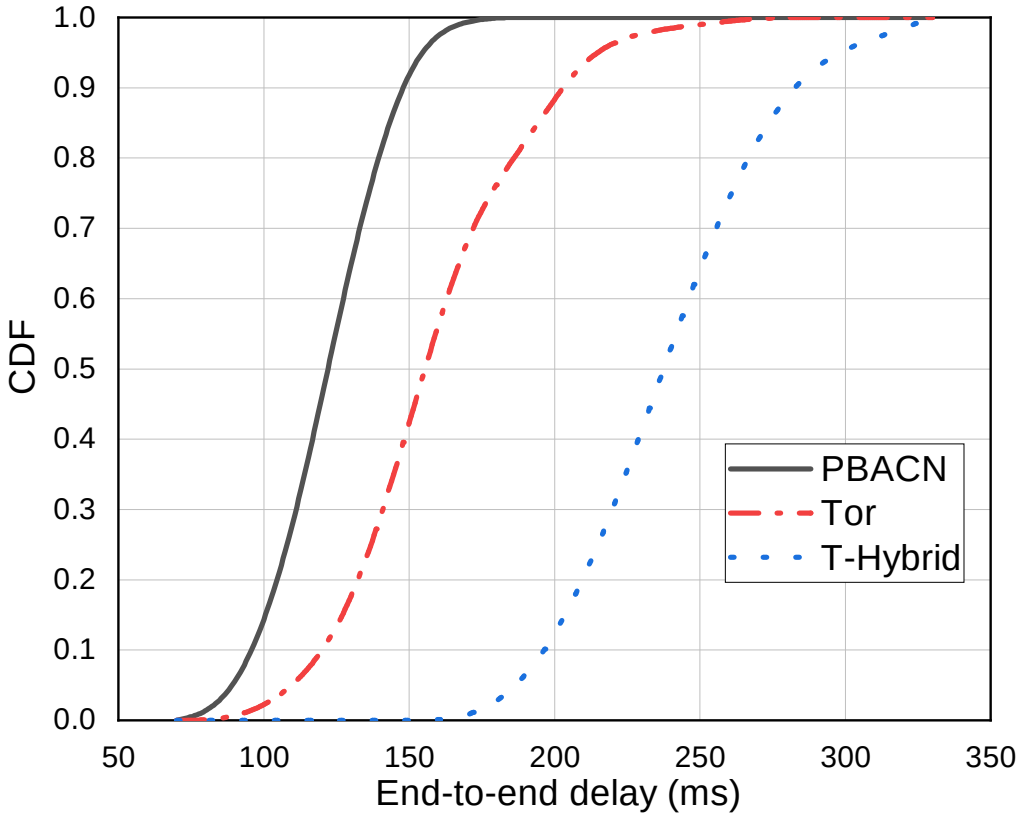

Figure 5. CDF under various end-to-end delays.

In contrast, our proposed PBACN first utilizes source-controlled routing, reducing routing time. Additionally, only the group leader must negotiate encryption with the sender, resulting in more saved encryption time than T-Hybrid. Therefore, PBACN has a lower end-to-end delay than other methods, which can provide users with a better experience and improve network performance and efficiency.

5. Anonymity Analysis

In this section, we introduce threat models and compare the anonymity of different anonymous communication networks.

5.1. Threat Model

As an anonymous communication network, while it provides anonymity to users, some malicious adversaries will inevitably come to disrupt its anonymity. To better deal with these vicious attacks, we need to define the adversary's capabilities to analyze their threat better.

We use the threat model proposed by Syverson et al. [28] as the basis for the adversary. Taking Tor as an example, Tor's entry node knows the client's IP address in the anonymous communication network, while the exit node knows the server's IP address. When an adversary controls these two nodes [29,30], they can use traffic analysis to confirm the communication relationship, thereby breaking the anonymity of the link.

We assume that the adversary can control a portion of the relay nodes. Secondly, since active adversaries are more likely to be discovered by users, the adversary cannot modify, delete, or delay traffic. The adversary can use the controlled nodes to monitor and analyze network traffic and the traffic of user requests and responses, thereby inferring the sender and receiver of the message and breaking anonymity. The model is also the most prevalent threat model faced by anonymous networks.

5.2. Anonymity Degree

A system can achieve maximum anonymity when an attacker assumes that all nodes in the anonymity set have an equal probability of being the sender of the message [31]. Thus, the probability distribution determines the anonymity degree. For a given probability distribution, the concept of entropy [32] in information theory provides a measure of information. Therefore, we can use entropy to calculate the anonymity of the system [33].

Let N be the number of nodes in the system and p_i be the probability that each node is inferred as the sender by the adversary. We define $H(N)$ as the maximum entropy of the system, which is:

$$H(N) = -\sum_{i=1}^{N} p_i \log_2(p_i). \tag{1}$$

When the adversary reduces the anonymity set to S through an attack, the new entropy is $H(S)$, and the information obtained by the adversary is $H(N) - H(S)$. We use the maximum entropy $H(N)$ to normalize this value, and therefore the anonymity degree is:

$$d = 1 - \frac{H(N) - H(S)}{H(N)} = \frac{H(S)}{H(N)}. \tag{2}$$

If $S = N$, the adversary fails to reduce the anonymity set and $d = 1$. The system has the maximum anonymity degree. When the adversary receives the sender's identification, the system entropy is 0, and $d = 0$. The system has the minimum anonymity degree. We can compare the anonymity degrees in different anonymity systems based on the above definition.

In Tor: According to our threat model, assuming the proportion of nodes controlled by the adversary is f, we analyze the system's anonymity under different situations, where the probability of each scenario occurring is q_i and the corresponding anonymity degree is d_i. The anonymity degree of the system is:

$$D = \sum_{i=1}^{3} q_i * d_i. \tag{3}$$

(1) When the adversary controls the sender:

$$q_1 = f, \tag{4}$$

$$d_1 = 0. \tag{5}$$

(2) When the adversary does not control the sender but controls both the entry and exit nodes of Tor:

$$q_2 = (1 - f) * f^2, \tag{6}$$

$$d_2 = 0. \tag{7}$$

(3) When the adversary does not control the sender and neither the entry nor the exit nodes of Tor:

$$q_3 = (1 - f)(1 - f^2). \tag{8}$$

According to Equations (1) and (2), in this case:

$$p_i = 1/S = 1/N(1 - f), \tag{9}$$

$$H(S) = \log_2(N(1 - f)), \tag{10}$$

$$d_3 = \frac{\log_2(N(1 - f))}{\log_2(N)}. \tag{11}$$

Therefore, according to Equation (3), Tor's anonymity degree is:

$$D_{Tor} = (1-f)(1-f^2)\frac{\log_2(N(1-f))}{\log_2(N)}. \tag{12}$$

In T-Hybrid: T-Hybrid consists of multiple groups, with an average group size of g. For one of these groups, the probability that at least one node is compromised is $1-(1-f)^g$.

We still consider three cases:

(1) When the adversary controls the sender:

$$q_1 = f, \tag{13}$$

$$d_1 = 0. \tag{14}$$

(2) When the adversary does not control the sender, but at least one node in the first group and the last group of T-Hybrid are controlled by the adversary:

$$q_2 = (1-f)((1-(1-f)^g)^2), \tag{15}$$

$$d_2 = 0. \tag{16}$$

(3) When the adversary does not control the sender, and at least one group is entirely uncontrolled by the adversary:

$$q_3 = (1-f)(2*(1-f)^g - ((1-f)^2)^g), \tag{17}$$

$$d_3 = \frac{\log_2(N(1-f))}{\log_2(N)}. \tag{18}$$

Therefore, the anonymity degree of T-hybrid is:

$$D_{T\_hybrid} = (1-f)(2*(1-f)^g - ((1-f)^2)^g)\frac{\log_2(N(1-f))}{\log_2(N)}. \tag{19}$$

In PBACN: Our proposed method has multiple groups compared to Tor, and the first node of each group cannot directly obtain the address information of the previous node. Therefore, the adversary must control both the leader node and the group's first node to compromise the anonymity. There are three cases:

(1) When the adversary controls the sender:

$$q_1 = f, \tag{20}$$

$$d_1 = 0. \tag{21}$$

(2) When the adversary does not control the sender but controls the entry node of the first group and the exit node of the last group in PBACN, as well as the leaders of both groups:

$$q_2 = (1-f)f^4, \tag{22}$$

$$d_2 = 0. \tag{23}$$

(3) Other cases not mentioned above:

$$q_3 = (1-f)(1-f^4), \tag{24}$$

$$d_3 = \frac{\log_2(N(1-f))}{\log_2(N)}. \tag{25}$$

Therefore, the anonymity degree of PBACN is:

$$D_{PBACN} = (1-f)(1-f^4)\frac{\log_2(N(1-f))}{\log_2(N)}. \tag{26}$$

In the PBACN we propose, multiple groups and leaders exist. Each group leader can only access a portion of the addresses from the source to the destination. Therefore, for an adversary to de-anonymize the sender's identity, they must simultaneously control all group leaders and the first node of the first group. In contrast, if an adversary wants to de-anonymize the sender in Tor, they only need to control the entry and exit nodes simultaneously. Therefore, PBACN offers higher anonymity. The diagram can also demonstrate our conclusion.

As shown in Figure 6, according to Equations (12), (19), and (26), we compared the anonymity of different anonymous communication networks under varying fractions of attackers. For T-hybrid, we also compared the changes in group size. The diagram shows that when the fraction of attackers increases, the anonymity degree of the network decreases. When there are no attackers in the network, it has the highest anonymity degree. We found that, except when approaching the lowest and highest fraction of attackers, we can easily distinguish the anonymity degree of each curve. Therefore, our definition of anonymity degree effectively expresses the anonymity of different ACNs. We can see that PBACN has a higher anonymity degree than other methods. When the adversary fraction is 20%, PBACN can improve the anonymity degree by approximately 4%.

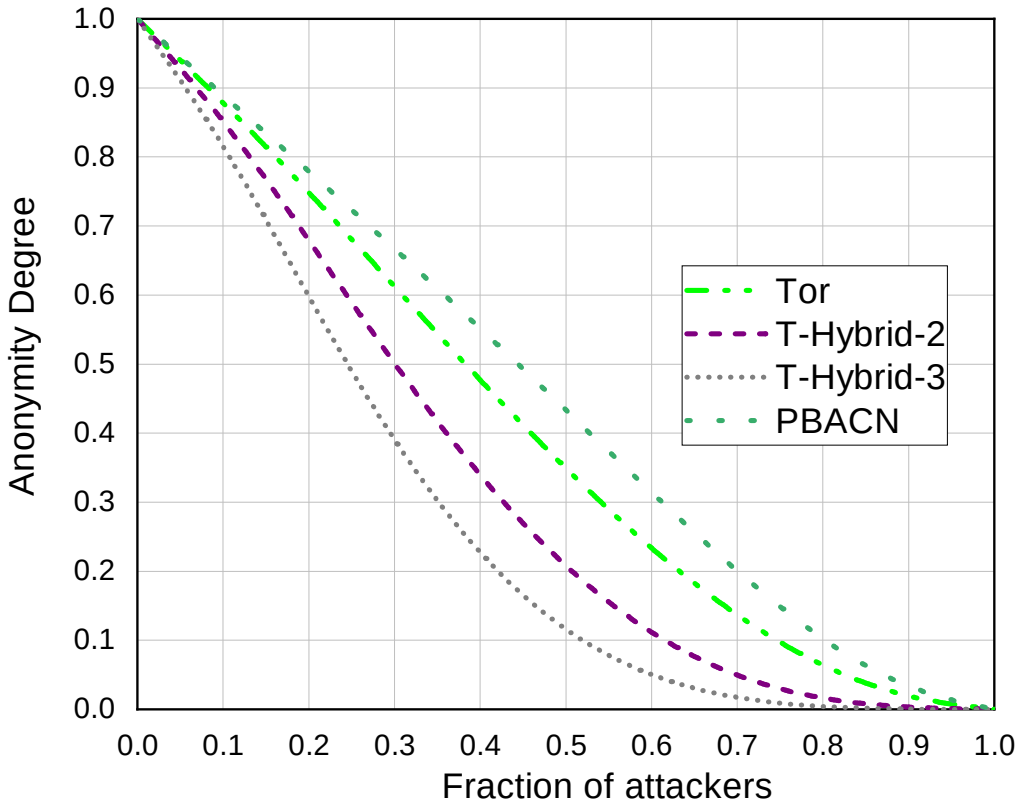

Figure 6. Anonymity degree.

6. Conclusions

This paper proposes a port-based anonymous communication network called PBACN, which uses a source routing method based on port forwarding for rerouting. Compared with other anonymous communication networks, the PBACN can significantly reduce routing time while ensuring anonymity. The experimental results of this method show that it can dramatically improve the efficiency and anonymity of anonymous communication

and is a feasible anonymous communication solution. In the implementation process, we improved the traditional routing strategy and proposed a new source routing method. The source routing method uses port forwarding to reroute messages, allowing messages for which the sender required hop-by-hop routing to reach the destination directly, thus reducing the routing time. The PBACN method can also ensure communication security and anonymity by improving the traditional routing strategy. In the experiment, we compared the PBACN method with the other anonymous communication networks, proving that it enhances communication efficiency while ensuring anonymity.

We will work on integrating the next-generation network with the existing network system in the future based on our current research. This work focuses on deploying our proposed methods in real networks and improving the transmission efficiency and anonymity of the network in practical applications. Additionally, ACN will encounter various attack methods and adversaries in practical applications. Therefore, we will analyze the characteristics of different adversary nodes and study a node selection strategy that can detect malicious nodes.

Author Contributions: Conceptualization, X.M. and M.L.; methodology, X.M. and M.L.; software, X.M.; writing and editing, X.M.; analysis, X.M. and M.L.; investigation, X.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Joint Project of the National Natural Science Foundation of China under Grant No. U1636109.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Montieri, A.; Ciuonzo, D.; Aceto, G.; Pescapé, A. Anonymity services tor, i2p, jondonym: Classifying in the dark (web). *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 662–675. [CrossRef]
2. Chaum, D. The dining cryptographers problem: Unconditional sender and recipient untraceability. *J. Cryptol.* **1988**, *1*, 65–75. [CrossRef]
3. Mödinger, D.; Heß, A.; Hauck, F.J. Arbitrary length K-anonymous dining-cryptographers communication. *arXiv* **2021**, arXiv:2103.17091. [CrossRef]
4. Freedman, M.J.; Sit, E.; Cates, J.; Morris, R. Tarzan: A peer-to-peer anonymizing network layer. *Proc. ACM Conf. Comput. Commun. Secur.* **2002**, *2429*, 193–206. [CrossRef]
5. Rennhard, M.; Plattner, B. Introducing morphmix: Peer-to-peer based anonymous internet usage with collusion detection. In Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society, Washington, DC, USA, 21 November 2002; pp. 91–102. [CrossRef]
6. Mathieu, B.; Song, M.; Kleis, M. A p2p approach for the selection of media processing modules for service specific overlay networks. In Proceedings of the Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06), Washington, DC, USA, 19–25 February 2006; p. 103. [CrossRef]
7. Winter, P.; Ensafi, R.; Loesing, K.; Feamster, N. Identifying and characterizing Sybils in the Tor network. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 1169–1185. [CrossRef]
8. Sankey, J.; Wright, M. Dovetail: Stronger anonymity in next-generation internet routing. In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Amsterdam, The Netherlands, 16–18 July 2014; pp. 283–303. [CrossRef]
9. Back, A.; Möller, U.; Stiglic, A. Traffic analysis attacks and trade-offs in anonymity providing systems. *Lect. Notes Comput. Sci. (Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinform.)* **2001**, *2137*, 245–257. [CrossRef]
10. Murdoch, S.J.; Danezis, G. Low-cost traffic analysis of Tor. In Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P'05), Oakland, CA, USA, 8–11 May 2005; pp. 183–195. [CrossRef]
11. Tusing, N.; Oakley, J.; Barrineau, G.; Yu, L.; Wang, K.C.; Brooks, R.R. Traffic analysis resistant network (tarn) anonymity analysis. In Proceedings of the 2019 IEEE 27th International Conference on Network Protocols (ICNP), Chicago, IL, USA, 8–10 October 2019; pp. 1–2. [CrossRef]
12. Akhoondi, M.; Yu, C.; Madhyastha, H.V. LASTor: A low-latency AS-aware tor client. *IEEE/ACM Trans. Netw.* **2014**, 22, 1742–1755. [CrossRef]

13. Kohls, K.; Jansen, K.; Rupprecht, D.; Holz, T.; Pöpper, C. On the Challenges of Geographical Avoidance for Tor. In Proceedings of the NDSS, San Diego, CA, USA, 24–27 February 2019. [CrossRef]
14. Yang, X.; Clark, D.; Berger, A.W. NIRA: A new inter-domain routing architecture. *IEEE/ACM Trans. Netw.* **2007**, *15*, 775–788. [CrossRef]
15. de Farias, C.M.; Pirmez, L.; Delicato, F.C.; Pires, P.F.; Guerrieri, A.; Fortino, G.; Cauteruccio, F.; Terracina, G. A multisensor data fusion algorithm using the hidden correlations in Multiapplication Wireless Sensor data streams. In Proceedings of the 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC), Calabria, Italy, 16–18 May 2017; pp. 96–102. [CrossRef]
16. Shirazi, F.; Simeonovski, M.; Asghar, M.R.; Backes, M.; Diaz, C. A survey on routing in anonymous communication protocols. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–39. [CrossRef]
17. Zhang, X.; Hsiao, H.C.; Hasker, G.; Chan, H.; Perrig, A.; Andersen, D.G. SCION: Scalability, control, and isolation on next-generation networks. In Proceedings of the 2011 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 22–25 May 2011; pp. 212–227. [CrossRef]
18. Zhao, A.; Liu, Z.; Pan, J.; Liang, M. A novel addressing and routing architecture for cloud-service datacenter networks. *IEEE Trans. Serv. Comput.* **2019**, *15*, 414–428. [CrossRef]
19. Liang, M.; Zhang, J.; Wang, S. A new network based on vector address. In Proceedings of the IET 2nd International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2008), Beijing, China, 12–15 October 2008; pp. 118–122. [CrossRef]
20. Chen, C.; Asoni, D.E.; Barrera, D.; Danezis, G.; Perrig, A. HORNET: High-speed onion routing at the network layer. In Proceedings of the ACM Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; Volume 2015, pp. 1441–1454. [CrossRef]
21. Hsiao, H.C.; Kim, T.H.J.; Perrig, A.; Yamada, A.; Nelson, S.C.; Gruteser, M.; Meng, W. LAP: Lightweight anonymity and privacy. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012; pp. 506–520. [CrossRef]
22. Chen, C.; Asoni, D.E.; Perrig, A.; Barrera, D.; Troncoso, C. TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018.
23. Xia, Y.; Chen, R.; Su, J.; Zou, H. Balancing anonymity and resilience in anonymous communication networks. *Comput. Secur.* **2021**, *101*, 102106. [CrossRef]
24. Chaum, D.L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* **1981**, *24*, 84–90. [CrossRef]
25. Shoup, V.; Gennaro, R. Securing threshold cryptosystems against chosen ciphertext attack. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Espoo, Finland, 31 May–4 June 1998; pp. 1–16. [CrossRef]
26. Danezis, G.; Goldberg, I. Sphinx: A compact and provably secure mix format. In Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, Oakland, CA, USA, 17–20 May 2009; pp. 269–282. [CrossRef]
27. Varga, A. The OMNET++ discrete event simulation system. In Proceedings of the European Simulation Multiconference, Prague, Czech Republic, 6–9 June 2001; pp. 319–324.
28. Syverson, P. Onion routing for resistance to traffic analysis. In Proceedings of the DARPA Information Survivability Conference and Exposition, Washington, DC, USA, 22–24 April 2003; Volume 2, pp. 108–110. [CrossRef]
29. Overlier, L.; Syverson, P. Locating hidden servers. In Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06), Berkeley, CA, USA, 21–24 May 2006; p. 15. [CrossRef]
30. Johnson, A.; Wacek, C.; Jansen, R.; Sherr, M.; Syverson, P. Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. In Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013. [CrossRef]
31. Díaz, C.; Seys, S.; Claessens, J.; Preneel, B. Towards measuring anonymity. *Lect. Notes Comput. Sci. (Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinform.)* **2003**, *2482*, 54–68. [CrossRef]
32. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
33. Grube, T.; Egert, R.; Mühlhäuser, M.; Daubert, J. The Cost of Path Information: Routing in Anonymous Communication. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–6. [CrossRef]