Poster: An anonymity metric of anonymous network

Jinli Zhang
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China
zhangjinli@iie.ac.cn

Zhi Wang
School of Cyber Security
University of Chinese Academy of Sciences
Beijing, China
wangzhi@iie.ac.cn

***Abstract*—Since anonymous network was proposed, it has been focused on building, analyzing and attacking. However, it is scarce to measure the anonymity. In this paper, we propose a novel, practical metric to evaluate the anonymity of anonymous networks. Starting from the anonymous network model, a measurement method based on node features and path strategies is proposed. The metric and method are mainly applied to Tor and compared with I2P. The experimental result shows that this metric can evaluate the anonymity of anonymous networks to a certain extent. The metric is useful for evaluating the existing anonymous networks and helpful for building an anonymous network.**

Keywords—anonymous communication network; metric; Tor; I2P; anonymity

I. INTRODUCTION

At present, with the increasing surveillance of online communications, people are paying more attention to personal privacy and privacy-enhancing technologies. Anonymous network hides the true source or destination address of a traffic, preventing the identity of the client or sever from being determined or identified. Therefore, more and more people choose to use the anonymous tools to access the Internet. Anonymous network has received much attention since it was put forward in 1980 by David Chaum. Since then, a body of researches have concerned about anonymous network, mostly about building, analyzing, and attacking.

However, there are few evaluations of anonymous networks. To this end, a novel and practical metric is proposed to measure the anonymity of anonymous networks and quantify the anonymity. We define an anonymous communication network model, and present a formula based on the model and protocol itself to measure the anonymous network. To verify that the metric is practicable, we apply it to popular anonymous networks – Tor and I2P. The metric is also compatible to other anonymous networks.

II. RELATED WORK

Anonymity is the most essential property in anonymous communication networks. Communication consists of communication object (content of a communication) and communication subject (sender and receiver of a communication). Since communication object is often well protected by security protocols, anonymity mainly focuses on the communication subject. Anonymity ensures that the identity and the relationship of a communication subject cannot be identified. Due to its specific configuration and Internet access, ZeroNet is considered as an anonymous network by some people. However, since ZeroNet provides anonymity through Tor and it does not guarantee the anonymity of the communication subject itself, we do not support this view.

Anonymity metrics are helpful for designing a new anonymous network or improving an existing anonymous network. There are some studies on the definition of anonymity. For example, Debajyoti Das et al. [1] gave the anonymity notions with a challenge-response game. Some studies measure anonymity based on relative entropy [2] or a limited particular message [3], but the anonymity is not well quantified. From the perspective of developers, a novel and practical anonymity measurement method based on the model and the protocol is proposed.

III. ANONYMITY METRICS

Since anonymity is critical to an anonymous network, we conduct a measure for the degree of anonymity. We propose a basic anonymous communication model, and classify anonymity into different levels. Then, based on the given conditions of the model, a quantifiable and practical method is given to measure anonymity.

We define a model for anonymous communication network. It is a directed graph $G = < V, E >$. V represents the set of communication nodes. In a standard network, V is the devices of the sender or receiver, and the number is usually 2, i.e. the client and the server. According to the Internet standard, network communication of an application must contain its IP address. Therefore, the anonymous network usually hides the real IPs through multiple hops. The metric we considered contains the size and other features of the nodes. On the other hand, the path selection of nodes is also important. E represents a set of paths between nodes. Paths cannot be fixed, and the path selection algorithm preferably has a certain randomness, which will make it difficult to determine the communication subject.

We define the anonymity grade of the anonymous network based on the model, with a range of (1, 10). V and E in the model are equally important, so they each have half the weight. The simplest level is shown in Formula (1). V and e represent respectively the hops of nodes (not including the necessary sender and receiver nodes) and the numbers of alternative paths. The lowest level is shown in Formula (1) and its grade is 1

when an anonymous network has only one hop and one alternative path without other conditions.

$$G = \frac{1}{2} v + \frac{1}{2} e \quad (1)$$

Considering other conditions, *V* depends on the number of hops and other node-related features, including the number and the breadth of total nodes. Each node-related feature has a certain weight in the evaluation. *E* depends on the random paths and the path selection policies which also have weights. And the size of the weight represents how much contribution to the anonymity. The formula of anonymity level is as follows:

$$G = \frac{1}{2} v + \sum_i n_i w_i + \frac{1}{2} e + \sum_j p_j w_j \quad (2)$$

The explanations of the formula are as follows:

- V represents the number of the used nodes and e represents the randomness and importance of the path.
- Both of v and e range from (1, 10). In general, anonymous networks have 2-6 nodes because less than 2 are easy to track, and more than 6 have high latency.
- N represents the node features and p represents the routing policy of the path. The value of n and p are usually 1, and they just represent one option.
- W represents the weight of each condition and ranges from (0.1, 0.5), as they are outside the coefficient 1/2.
- I and j take integer values.

IV. Experimental Evaluation

In this section, we apply this anonymity metric mainly to Tor and compare it with I2P. The anonymity of the two anonymous networks are analyzed and evaluated. All the following values are result from comparison between Tor and I2P, and are given empirically.

The evaluation of Tor and I2P is discussed simultaneously. Generally Tor has 3 hops (v = 3) and I2P has 6 hops in each path. However, Tor and I2P are more than just a simple multi-agent. So far Tor has more than 7,000 total running nodes. Considering that I2P has about 50,000 nodes and Freenet has more than 60,000 nodes, this disadvantage causes Tor to have a lower weight of 0.3 in this feature and a higher weight of I2P. In addition, Tor's nodes are composed of volunteers from all over the world and it is difficult to track users through any three nodes across countries and regions. Although it is of high importance, I2P has the same feature and therefore weighs 0.35. Tor has one random path (e = 1) and I2P has two paths (e = 2). Both Tor and I2P's garlic use onion layer encryption that the MITM cannot decipher all IP addresses, so the value is 0.4. Tor can also exclude nodes in insecure countries, so this feature has a weight of 0.4. In addition, the path of Tor changes every ten minutes, making decryption even more difficult, with a value of 0.45. I2P has a P2P structure that prevents a single point of failure and can have a value of 0.35. Finally, the anonymous grade of Tor is 4.0, lower than I2P with 5.53. There is no absolute anonymity. Although the anonymity grade of Tor is not high theoretically, deanonymization is still very difficult in reality. The anonymity comparison results of Tor and I2P are shown in Table 1.

TABLE I. Anonymity Comparison Result

Metrics	**Anonymous networks**			
	Tor	**Value**	**I2P**	**Value**
Hops	v=3	1.5	v=6	3
n_1	about 7,000 nodes	0.35	about 50,000 nodes	0.4
n_2	nodes from all over the world	0.38	nodes from all over the world	0.38
Paths	e=1	0.5	e=2	1
p_1	onion layer encryption	0.4	onion layer encryption	0.4
p_2	exclude insecure nodes	0.42	P2P structure	0.35
p_3	changing path	0.45		
Grade		4.0		5.53

V. Conclusion

In this work, we present a novel and practical anonymity metric. From the evaluation results, we can conclude that I2P has better anonymity than Tor. In practical, however, Tor is popular and widely used. This metric is based on a model that only considers the node's obvious features and routing strategies and this is a simple method to quantify anonymous metrics. In future work, more features will be considered, such as availability, which is also important. The metric has proven to be very useful in evaluating existing anonymous networks, and this helps establish new anonymous networks. In the future, we will learn and evaluate various features of anonymity from the perspective of protocols.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful comments for improving this paper. This work is supported by the Key Laboratory of Network Assessment Technology at Chinese Academy of Sciences and Beijing Key Laboratory of Network Security and Protection Technology.

References

[1] Das D, Meiser S, Mohammadi E, et al. Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two[R]. ETH Zurich, 2017.

[2] Jaggi N, MarappaReddy U, Bagai R. A three-dimensional approach towards measuring sender anonymity[C]//Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, 2011: 994-999.

[3] Diaz C, Seys S, Claessens J, et al. Towards measuring anonymity[C]//International Workshop on Privacy Enhancing Technologies. Springer, Berlin, Heidelberg, 2002: 54-68.