Cui et al. Cybersecurity (2023) 6:55
https://doi.org/10.1186/s42400-023-00191-8

Cybersecurity

RESEARCH Open Access

Tor network anonymity evaluation based on node anonymity

Jun Cui[1,2,3], Changqi Huang[1,2,3], Huan Meng[4] and Ran Wei[5*]

Abstract

In order to address the shortcomings of traditional anonymity network anonymity evaluation methods, which only analyze from the perspective of the overall network and ignore the attributes of individual nodes, we proposes a dynamic anonymity model based on a self-built anonymous system that combines node attributes, network behavior, and program security monitoring. The anonymity of evaluation nodes is assessed based on stable intervals and behavior baselines defined according to their normal operating status. The anonymity of the network is evaluated using an improved normalized information entropy method that refines anonymity evaluation to the anonymity of each node and expands the dimensionality of evaluation features. This paper compares the effectiveness of our proposed method with static framework information entropy and single indicator methods by evaluating the degree of anonymity provided by a self-built Tor anonymous network under multiple operating scenarios including normal and under attack. Our approach utilizes dynamically changing network anonymity based on multiple anonymous attributes and better reflects the degree of anonymity in anonymous systems.

Keywords Node anonymity, Behavioral baseline, Network anonymity, Self-built Tor network, Dynamic evaluation

Introduction

As the scale and scope of networks and their applications continue to expand, the importance of information security is growing. It is not only necessary to protect the content and process of communication, but also critical to ensure anonymous communication that hides communication relationships. Anonymous communication systems are developing rapidly, with diverse types and broad usage, and an increasing number of users. Therefore, it is necessary to conduct extensive and in-depth research on the anonymity of such systems.

Anonymity networks, represented by the Tor, serve as a critical technology for ensuring anonymity in the development of the Internet. However, there has been a continuous increase in attack methods targeting anonymous communication systems. For instance, there is the Sybil attack (Zhang et al. 2021), which involves disguising high-performance nodes to interfere with the selection of nodes in path construction. Another example is the denial-of-service attack, which obstructs anonymous communication and enables traffic analysis (Schnitzler et al. 2021). These active attacks not only threaten the anonymity of the network but also cause significant damage to the usage of anonymous systems. Conducting an anonymity evaluation allows for a comprehensive understanding of the state of an anonymous system, enabling not only the evaluation of the effectiveness of anonymity services but also the identification of potential risks and threats. Accurate measurement methods serve to alert

*Correspondence:
Ran Wei
ranwei_tgu@163.com
[1] School of Life Sciences, Tiangong University, 399 Binshui West Road, Xiqing District, Tianjin 300387, China
[2] Tianjin Engineering Research Center of Biomedical Electronic Technology, Tianjin 300387, China
[3] Tianjin Key Laboratory of Quality Control and Evaluation Technology for Medical Devices, Tianjin 300387, China
[4] School of Electronics and Information Engineering, Tiangong University, Tianjin 300387, China
[5] Department of Rehabilitation Engineering, Beijing College of Social Administration (Training Center of the Ministry of Civil Affairs), Beijing 102600, China

users to promptly discontinue system usage in the event of compromised security, thereby safeguarding their identities. Additionally, such evaluation aid developers in improving and designing mechanisms within anonymous networks to counteract attacks, providing them with objective and scientific foundations to work upon.

The current mainstream definition of network anonymity was proposed by Pfitzmann and Köhntopp (2001) in 2001. This definition suggests that a network is considered anonymous when the states and characteristics of the communicating entities within the anonymous set are similar, making it impossible to identify any communication relationships within the system.

In 1998, Reiter and Rubin (1998) used the inhomogeneity of the probability of nodes being identified to formalize a measure of network anonymity, classifying the degree of anonymity into six levels ranging from absolutely hidden to apparently exposed. This formal analysis measures the anonymity of the network in terms of its overall structure, and it is now common to propose assessment frameworks or uniform definitions for anonymity or unobservability, which makes the assessment focus mainly on the threat scenarios in which the environment is embedded (Melloni et al. 2022) or on consistent privacy goals across different assessment frameworks (Kuhn et al. 2019). Although it is possible to compare the threatened levels of anonymous networks under different attacks, the analysis remains at the framework level, lacking specific quantification of anonymity and unable to accurately reflect the actual anonymity of the system.

Therefore, the measurements of anonymity service effectiveness provided by operational anonymous networks primarily relies on quantitative evaluations using quantifiable metrics. Such approach enables developers to obtain timely and definitive feedback on the achieved anonymity during system improvements or when the system is under attack.

Anonymous set-based anonymity Quantitative methods (Chaum 1981; Berthold et al. 2001) evaluate the probability of mapping an attacker's prior knowledge on a node based on the number of users in the system or the attacker's prior knowledge, which, while simplifying the complexity and being generalizable, ignores the influence of the internal operational situation factors of the anonymity network. A quantitative method based on matrix theory (Gkountouna and Terrovitis 2015) calculates the degree of anonymity by constructing a binary tree for anonymized data inference and measuring the difference between the original and inferred data, which generalizes the effect of anonymous members on anonymity as a whole but fails to take into account the different characteristic variations of each node in the network.

The anonymity measurement based on information entropy (Serjantov and Danezis 2003) combines the size of the anonymous set and the uniformity of the distribution of probabilities of identifying members within the anonymous set to calculate the network anonymity. This method exhibits excellent statistical properties and reflects the attacker's uncertainty regarding communication relationships within the system. Therefore, the information entropy-based approach has been widely adopted. Such as the generalized form of Renyi entropy (Clauß and Schiffner 2006), which encompasses the maximum entropy and minimum entropy (Tóth et al. 2004) as special cases, allows for parameter adjustment to achieve an ideal level of discrimination. This generalization provides a broader scope of applicability.

However, the measurement methods based on information entropy theory require the consideration of various specific internal information and external factors within the anonymous network. In particular, the incorporation of node characteristics is necessary to establish accurate mappings. Only through this comprehensive approach can the evaluated anonymity measure become more representative and practical, thus fully reflecting the security of the anonymous system. For instance, entropy measurements that solely analyze from the perspective of attackers, such as the conditional entropy considering the additional information possessed by attackers (Diaz et al. 2007) and the relative entropy based on unobservability measurements (Tan et al. 2015), have limited generality. This is primarily because it is challenging to accurately obtain the amount of information known to attackers in practical applications.

Currently, research on quantifying anonymity lacks an evaluation mechanism for the real-time changes in anonymity during the operation of networks. The factors used to measure anonymity are also relatively limited and one-sided, with weak sensitivity to system state changes. Furthermore, the evaluations only focuse on the overall anonymity of the network. Nevertheless, in the actual operation of Tor, it is necessary to analyze the current state of anonymity in real-time within a complex environment. This enables timely detection of abnormal system states or potential threats, which allows for early adjustments to the network and the maintenance of user anonymity.

The Tor network facilitates anonymous communication through paths composed of multi-hop nodes, making anonymity highly correlated with the participating nodes. Therefore, it is of utmost importance to evaluate the anonymity of individual nodes within the anonymous set. To achieve this, it is necessary to employ a variety of feature indicators that capture the state changes across

different aspects of the nodes. By integrating these indicators, one can obtain evaluation results that reflect the real-time and representative changes in the anonymity status of individual nodes.

Moreover, by integrating network anonymity with node anonymity, the changes in the anonymity status of anonymous members can be reflected in their impact on the overall network. By further incorporating various metrics at the network level, the evaluation mechanism can become more dynamic, and provide a more comprehensive, objective, and fair result.

Contribution

This paper proposes a solution that comprehensively and dynamically evaluates the anonymity of each node in the self-built Tor network to ensure the provision of reliable anonymous services. We collecte evaluation indicators that reflect various activities and statistically evaluate the anonymity of nodes based on their corresponding behavior changes over time, not only focusing on multiple attributes that are prone to change due to attacks or load reasons, but also able to dynamically analyze the aggregated values of these changes. This enables us to promptly detect any abnormal states indicating attacks on nodes, thereby maintaining the anonymity of individuals in anonymous sets. For the overall anonymous system, we unify multiple aspects of attributes into information entropy by analyzing the overall behavioral changes of the anonymous set, in order to evaluate the network anonymity. Compared to a single indicator, this approach enables a more comprehensive and integrated reflection of the network anonymity situation.

As shown in Fig. 1, nodes that are participating in the construction of anonymous network communication paths are dynamically evaluated for anonymity through multiple anonymity features, i.e., by combining the nodes' own attributes, network behavior and security monitoring attribute after joining the network, and analyzed to obtain the behavior base value representing the nodes' operational status. The fluctuations of various indicators of normally functioning nodes will be within a range. Therefore, based on behavior base value of the normal cycle, the stable interval is defined using the Interquartile Range (IQR) method, and the anonymity of nodes is evaluated by modifying the Gaussian function model, so as to detect anomalous nodes and filter out the nodes with high anonymity that can be reliably selected in the construction of paths.

Previous studies often focused on evaluating the network at a macro level or only employed single attributes to assess nodes based on their current states. In this paper, we validate the dynamic nature of our node anonymity evaluation mechanism by subjecting the Tor network to both normal operational and DDoS attack environments. Furthermore, it demonstrates the capability of promptly and effectively detecting anomalous node in the face of DDoS attacks.

At the network layer, a network information matrix is constructed based on the anonymity degrees of nodes, the correlation between nodes, the differences in the runtime duration and data transmission of nodes.The anonymity of the network is dynamically evaluated via normalized Shannon entropy, and the IQR method is also used to detect whether the network is in an abnormal state.

Compared to measurement methods applicable to single-attribute static situations, the network anonymity evaluation mechanism proposed in this paper is capable of reflecting changes in anonymity more promptly, both during normal operation and when facing attacks, within the Tor network. It can provide an accurate depiction of the corresponding changes in network anonymity before and after removing anomalous nodes. Furthermore, it demonstrates a continuous downward trend in anonymity when facing repeated malicious program modification attacks. Thus, the

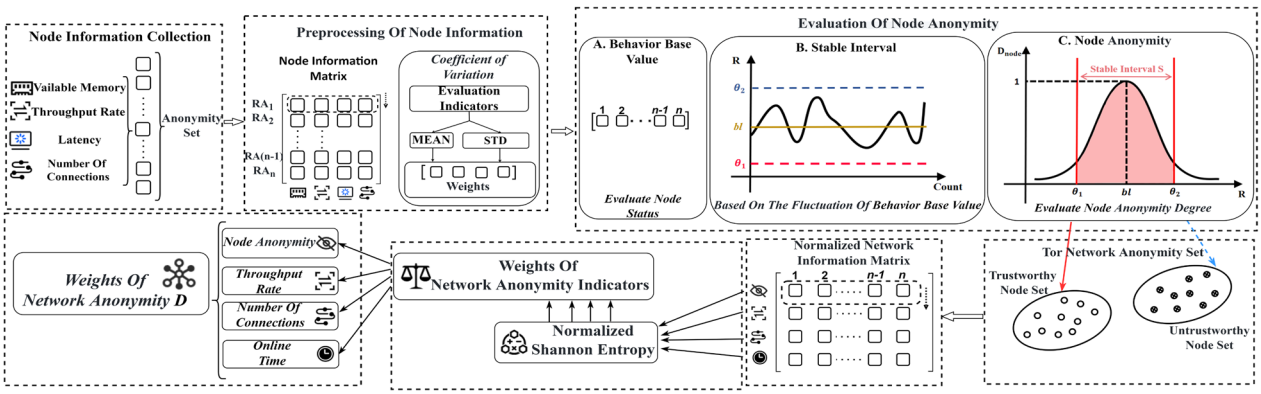

Fig. 1 Anonymity Evaluation Mechanism of Tor Network Based on Node Anonymity

effectiveness of our network anonymity evaluation is verified.

In summary, the main contributions of this paper can be concluded as follows:

- We propose a multi-indicator node anonymity evaluation method, applicable to a self-built Tor network at the node level, which combines the node's own attributes with network behavior-related features. By conducting comprehensive evaluation utilizing multiple attributes, node anonymity is sensitive to various internal or environmental factors, thereby avoiding extreme evaluation caused by a single factor.
- We use the interquartile range method to divide the normal fluctuation interval of node anonymity in the self-built Tor network system, select normal nodes to participate in anonymous communication, and remove abnormal nodes to maintain the anonymity of the system, based on the evaluation results. This mechanism based on stable interval is suitable for dynamically detecting the anonymity status of nodes. By combining the relatively recent states and performances of node during normal operation, a stable interval is derived. This enables more timely differentiation of abnormal nodes that exceed the stability threshold.
- We conduct dynamic quantitative evaluation of network anonymity from multiple perspectives and indicators, by combining node anonymity with network behavior features in anonymous networks and using normalized Shannon entropy. In practical self-built Tor networks, the measurement results are better able to promptly and effectively reflect the worsening of anonymity in the presence of DDoS attacks and malicious program injection attacks, as compared to static methods based on single attributes.
- We evaluates node anonymity and network anonymity in a self-built Tor network using the proposed method under different scenarios: normal operation, DDoS attacks, and malicious program modification attacks. The results indicate that the node anonymity mechanism exhibits dynamic evaluation characteristics, allowing for a more rapid representation of node status changes in corresponding scenarios. The mechanism, when faced with various attacks, combines node anonymity to evaluate network anonymity, enabling a dynamic and instant depiction of specific changes in the network environment.

Related work

Combined with information entropy

There are many studies that evaluate the anonymity of systems from various perspectives, but ultimately combine with information entropy to obtain anonymity. For example, Piotrowska et al. (2017) use coverage traffic and message delay to analyze the anonymity of anonymous networks at different delay parameter traffic rate parameters based on information entropy. Guan et al. (2002) applied conditional entropy to investigate the impacts of path selection strategies, including different path lengths and topologies, on sender anonymity. Sakai et al. (2017) obtained anonymity by combining information entropy with the probability of inferring communication relationships inferred by an attacker. Rochet and Pereira (2017) evaluated anonymity by combining standard entropy, guessing entropy, and empirical measures. Milajerdi and Kharrazi (2015) calculated the entropy value representing the system's anonymity level by statistically computing the proportion of node combinations in the path as the probability of identifying the path. Xia et al. (2021) utilized information entropy to evaluate the anonymity of the T-hybrid network, considering network attributes including the proportion of compromised nodes, the size of anonymous sets, and path length.

These studies on anonymity assessment based on information entropy method have quantified the anonymity on a global level of public anonymous networks, without taking into account the attributes of individual nodes, and none of them have specifically evaluated the effectiveness and anonymity of individual nodes in providing anonymous services. Furthermore, there is a lack of quantitative assessment regarding the changes in anonymity that occur during the actual operation of the network or when facing attacks.

Based on various perspectives

Several studies have quantitatively evaluated the anonymity of anonymous communication systems by borrowing concepts from other fields or proposing new ones. Wails et al. (2018) evaluated the anonymity of an anonymous network solely from a temporal perspective, indicating that anonymity decreases over time. Gkountouna and Terrovitis (2015) compared the differences between the constructed binary tree of raw data and the inferred binary tree of data, only focusing on assessing the risk of system-wide information leakage.

Zhang et al. (2021), solely focusing on the outcome, employed communication status along with historical performance to achieve dynamic evaluation of node reliability. However, they did not thoroughly consider the impact of various parameter changes in nodes resulting from attacks or network mechanisms on anonymity. Furthermore, their evaluation lacks measurement of the overall network anonymity based on node state changes. These studies present novel concepts, but they are not

applicable for real-time dynamic evaluation or only offer measurements from limited perspectives.

There are numerous studies that approach from the adversary's perspective, analyzing the network anonymity based on the disruption or attack on Tor structural characteristics or the resulting output behavior of the network. On the other hand, these studies also lack an evaluation of the overall changes in network anonymity during the attack process.

Tan et al. (2022) evaluated the effectiveness of their proposed Trapper Attacks on Tor based on the time and probability required to construct compromise paths, considering the number of honey nodes and the percentage of disguised bandwidth. However, they did not take into account the impact of this attack on the overall anonymity of the network and the effectiveness of normal nodes in providing anonymous services. Buccafurri et al. (2021) evaluated the probabilities of compromising sender anonymity and relationship anonymity from the perspective of traffic analysis attacks, considering four threat models ranging from external to global levels. But they did not take into account the changes in anonymity caused by the actual characteristics of the improved network structure proposed in their study. Eaton et al. (2022) established the probability of privacy infringement by adversaries controlling nodes of different proportions as the anonymity boundary based on time and network structure parameters. Nevertheless, they were unable to assess the impact of persistent harm caused by malicious nodes on the anonymity network.

Backes et al. (2014), assessed the anonymity threshold of a network based on the mean squared error of an attacker's analysis without taking into account the inherent properties of the network. Cherubin (2017) described the error between the attacker's observations and the actual results to only measure the defense effect of the anonymous system against website fingerprint attacks. Basyoni et al. (2021) evaluated the network anonymity under different side-channel attacks using the latency differences of traffic sent by each node and the throughput differences of paths. But they did not propose a unified metric to measure the network anonymity.

Based on formal qualitative measures

Melloni et al. (2022) provided an anonymity level assessment framework for the Tor network by considering the adversarial targets and capabilities. Yang and Xiao (2022) also proposed a formal analysis framework for anonymity, which analyzes sender anonymity at the structural level of the network by defining mapping relationships such as message equivalence and trace equivalence between senders and attackers. Dahlberg et al. (2021) categorized the impact of HTTPS man-in-the-middle attacks on the Tor into four levels, thereby conducting a qualitative analysis of enhancing the security of the Tor with support for certificate transparency. Reininger et al. (2021) conducted a qualitative analysis of the potential attacks targeting different network composition structures, focusing on the anonymity provided by the improved network in various dimensions.

These formal qualitative measures do not incorporate quantitative integration for the aspect of anonymity, and fail to quantitatively assess the actual fluctuations in the network anonymity during the attack process.

Anonymity evaluation method

In the typical anonymous transmission network Tor (Dingledine et al. 2004), the anonymity of the network is guaranteed by the process of rerouting and network member node forwarding during information transmission. The nodes in the network provide anonymous services mainly through the process of rerouting which involves a series of obfuscation processes for the received information, and finally reaches its intended destination.

The model proposed in this paper is capable of evaluating the anonymity of nodes and networks in a self-built Tor network. Most existing research focuses on public Tor networks, where the nodes are often voluntarily contributing to the network, making it difficult for users outside of the provider community to evaluate node anonymity. Therefore, our work evaluates node anonymity in a self-built Tor network based on multiple attributes, further improving the anonymity, reliability, and security of anonymous communication.

Node anonymity evaluation mechanism

Node anonymity rvaluation indicators

We establish the evaluation of node anonymity based on various indicators of node information. Assuming there are n nodes in the anonymous set and m indicators for evaluating node anonymity, the node information matrix X that reflects the distribution of various indicators in the anonymous set is constructed by measuring the anonymous system as follows:

$$X = \begin{bmatrix} x_{11} & \cdots & x_{1m} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nm} \end{bmatrix} \tag{1}$$

Assuming $i \in [1, n]$, $j \in [1,\ m]$, x_{ij} is used to represent the value of the j-th evaluation indicator of the i-th node in the node set.

By using the initial value method to process different indicators and eliminate dimensions without affecting

other nodes, the node information matrix X is transformed into the initialized node information matrix Y:

$$Y = \begin{bmatrix} y_{11} & \cdots & y_{1m} \\ \vdots & \ddots & \vdots \\ y_{n1} & \cdots & y_{nm} \end{bmatrix} \tag{2}$$

$$y_{ij} = \frac{x_{ij}}{x'_{ij}} \tag{3}$$

Assuming $i \in [1, n]$, $j \in [1, m]$, x'_{ij} is the initial value of the j-th evaluation indicator of the i-th node, and y'_{ij} represents the corresponding initialized value of.

We categorize evaluation indicators into two types based on the source: node' s own attributes and network-related behaviors. Having sound node' s own attributes is crucial for a node to operate stably and process data rapidly in anonymous networks.

For example, a small amount of available running memory may cause the paths that the node is involved in building to become congested or even crash, or be compromised more easily by the attacker, so we choose available running memory as a proxy for the node's own attributes.

Different network-related behaviors reflect the operational status of the node in various aspects of the anonymity system, and by synthesizing the network-related behaviors, a more comprehensive representation of the current anonymity status of the node can be achieved. The network-related behaviors selected in this paper include node throughput rate and latency, and number of connections. Throughput rate reflects the speed at which the node transmits data, while latency reflects the time it takes to transmit data, and the number of connections represents the degree of association with other nodes in terms of participating in building paths.

Weights of evaluation indicators

To avoid interference caused by different evaluation standards for indicators, we adopt the coefficient of variation method to calculate the corresponding weights, which is a commonly used objective weighting method in statistics. Based on the degree of variation in the raw data, values are assigned to the objective, with larger amounts of information contained in greater degrees of variation resulting in higher weights, and vice versa. First, the coefficient of variation v_j is analyzed based on the node information matrix X:

$$v_j = \frac{S_j}{\bar{x}_j} \tag{4}$$

In Eq. (4) $\bar{x}_j$ is the mean value of indicator j in the node information matrix X and S_j is the standard deviation of in indicator j in the node information matrix X, which is calculated as follows:

$$\bar{x}_j = \frac{\sum_{i=1}^{n} x_{ij}}{n} \tag{5}$$

$$S_j = \sqrt{\frac{\sum_{i=1}^{n} \left(x_{ij} - \bar{x}_j\right)^2}{i-1}} \tag{6}$$

In order to make the evaluated indicators always positively correlated with the node anonymity and to make the evaluated node anonymity bounded, the coefficient of variation is normalized by bringing it into Eq. (7), where the constant $\beta \in [1, \infty]$, and the weight w_j of the indicator j can finally be obtained as follows:

$$w_j = \frac{\beta^{v_j}}{\sum_{j=1}^{m} \beta^{v_j}} \tag{7}$$

Node behavior base value

Only relying on multi-dimensional evaluation indicators is not sufficient to fully evaluate the anonymity status of the node under the current state, and it is also necessary to analyze the historical state. When the node is operating normally, each indicator will fluctuate within a range. In order to detect anomalies and remove untrustworthy nodes in the anonymous system, the node behavior base value is proposed to evaluate the operating status.

Each indicator of the node represents different aspects of variation, so the corresponding feature values are weighted to more accurately evaluate the node behavior base value. Then, the behavior base value R_i of node i is:

$$R_j = \sum_{j=1}^{m} w_j \cdot x_{ij} \tag{8}$$

In Eq. (8), assuming that there are indicators, w_j represents the weight of the valuation indicator j in initializing the node information matrix Y, and y_ij is an element in the node information matrix Y, representing the initializing value of evaluation indicator j for node i.

Node stability interval

The behavior base value represents the current state of the node. In this paper, its fluctuation over time is analyzed using the Interquartile Range (IQR) method to determine the normal operating range. Firstly, the behavior base value during the normal operation cycle is collected, and then the first quartile Q_1 and the third quartile Q_3 are calculated. Finally, the node stable interval

$S \in [\theta_1, \theta_2]$ is determined by quartiles Q_1 and Q_3, and the interquartile range (IQR), where θ_1 is the lower threshold and θ_2 is the upper threshold.

$$\begin{cases} \theta_1 = \begin{cases} Q_1 - f \cdot IQR & \text{when } Q_1 > f \cdot IQR \\ 0 & \text{when } Q_1 \leq f \cdot IQR \end{cases} \\ \theta_2 = Q_3 + f \cdot IQR \end{cases} \tag{9}$$

$$IQR = Q_3 - Q_1 \tag{10}$$

$$f = \frac{R_{max} - R_{min}}{\sigma_R} \tag{11}$$

In Eq. (9), IQR represents the interquartile range, which is shown in Eq. (10) as the difference between the first and third quartiles. f represents the fluctuation coefficient, which is shown in Eq. (11). When the range of the behavior base value is constant, a larger standard deviation f leads to a greater distance between the quartiles and extreme values, and the threshold for normal operation should be farther away (Fig. 2).

The mean of the node behavior base value during the normal operational cycle is used as the behavior baseline bl. This represents the ideal normal operating condition for that cycle of time which is in the highest degree of anonymity for the node. In reality, the node's state will fluctuate within a ange during normal operation, and this maximum fluctuation range is defined as the sstable interval of the node.

Node anonymity

In this paper, the node anonymity is evaluated based on the degree of fluctuation of the behavior base value up and down the behavior baseline. The greater the fluctuation, the lower the anonymity of the node. Therefore, a Gaussian function is used to standardize and unify the magnitude of this fluctuation, so as to quantitatively evaluate the anonymity D_{node} of the node.

$$D_{node} = q \cdot \exp\left(-\frac{(R - bl)^2}{d \cdot {\sigma_R}^2}\right) \tag{12}$$

$$q = \alpha^k \tag{13}$$

In Eq. (12), D_{node} represents node anonymity, R represents the most recent measurement of behavior base value, bl represents the behavior baseline, d refers to a constant that determines the distinguishability, and q represents the security monitoring coefficient.

In Eq. (13), the base $\alpha \in (0, 1)$, and k represents the number of times that Tor programs are added, deleted or modified as observed by the program security monitoring. Malicious code injection is accomplished through the active insertion of malicious code into user traffic on the server side, increasing or modifying the content of unencrypted traffic, making it easier for attackers to carry out Man-in-the-Middle attacks (Winter et al. 2014). This paper deploys the Wazuh platform on each relay node to monitor the configuration files related to Tor services, in order to analyze and determine whether intruders have made modifications to the Tor service configuration. Through this, it can promptly reflect situations where programs for self-built Tor networks are modified due to external factors. Evaluators can adjust the base α and modify the importance of the security monitoring coefficient q in anonymity, but the node anonymity degree decays significantly whenever the program is modified several times ($k > 1$).

As node anonymity requires consideration of the behavior baseline and the variance of behavior base value σ_R^2, this model can evaluate an anonymity value between [0,1] based on the fluctuation changes in its own state when targeting nodes in different steady intervals, which demonstrates good applicability (Fig. 3).

In addition to quantitatively evaluating the anonymity of nodes, excluding untrustworthy nodes from anonymous systems plays a significant role in maintaining the anonymity of the system. By setting the behavior base value outside the stable interval S to be in the rejection region, nodes are deemed untrustworthy and are rejected from continuing to engage in anonymous communication within the anonymous network.

Algorithm 1: Trusted node screening mechanism

Input: Anonymous set $P = \{n_1, n_2, \cdots, n_i, \cdots\}$
Evaluation indicators $C = \{throughput\ rate, available\ memory, latency, number\ of\ connections\}$
Output: Anonymous set $P' = \{n'_1, n'_2, \cdots, n'_i, \cdots\}$
Node anonymity set $D_{node} = \{d_1, d_2 \cdots, d_i, \cdots\}$

1: Construct the node information matrix X by collecting evaluation indicators C for all nodes in the anonymous set P;
2: Based on the node information matrix X, calculate the set of indicator weights W, where $W = \{w_1, w_2, w_3, w_4\}$;
3: Calculate the behavior base value R for each node in the anonymous set P;
4: Counting the upper threshold θ_1, lower threshold θ_2, behavioral baseline bl, variance σ_R^2, node stability interval $S = [\theta_1, \theta_2]$ for each node after the last normal operating cycle T;
5: Compute behavior base value R' for the next cycle $T\prime$;
6: Based on the behavior base value R', compute the node anonymity D_{node};
7: Remove nodes whose behavior base value exceed the stable interval S from the anonymity set, then forming a new trusted anonymity set $P' = \{n'_1, n'_2, \cdots, n'_i, \cdots\}$;
8: **return** node anonymity D_{node}, anonymity set P'

The aforementioned trusted node selection mechanism is designed to ensure that the anonymous network is always able to provide effective anonymous services.

Network anonymity evaluation mechanism

Shannon entropy is an anonymity evaluation method based on the size of the anonymity set and the probability of members being recognized by the attacker asevaluation indicators, which uses a specific mathematical model to quantify the anonymity, but only uses the static anonymity features at the overall network layer.

First, evaluation indicators that represent aspects of the network performance are collected from the anonymity set to construct the network information matrix. Then The coefficient of variation method is also used to determine the weights of each indicator. Finally, the distribution of the evaluation indicator values in the anonymity set is analyzed based on the network information matrix, and the network anonymity is calculated using normalized Shannon entropy.

Network anonymity evaluation indicators

Node anonymity, throughput rate, online time, and number of connections represent different aspects of node network behavior in the system. They respectively reflect the current anonymity degree of nodes, data transmission speed, normal operating time in an anonymous network, and probability of being selected to build a path. Although some indicators are identical to the node anonymity, network anonymity evaluation analyzes the uneven distribution of indicators among nodes at the anonymity set.

(1) Using node anonymity as an evaluation indicator of network anonymity can reflect the changes in anonymity degree of a certain node on the overall network anonymity.
(2) If the difference in throughput rates between nodes is significantly large, it indicates that a node may be subject to Sniper attacks (Jansen et al. 2014) with maliciously high traffic, and susceptible to traffic analysis attacks (Mittal et al. 2011) that compromise anonymity.
(3) If there is a significant discrepancy in the online time of nodes, nodes with excessively long online time are more likely to be identified for communication due to fingerprint attacks and other means (Kwon et al. 2015). On the other hand, nodes with a short online time indicate insufficient utilization, necessitating frequent selection of new nodes to join the network, which increases costs. Therefore, keeping the online time of nodes at an appropriate level can improve both network anonymity and efficiency.
(4) If there is a significant discrepancy in the frequency at which nodes are selected, highly frequent nodes are more susceptible to BGP hijacking and manipulation by AS-level adversaries (Sun et al. 2015). In addition, low-frequency nodes represent insufficient utilization of nodes in the system, resulting in a smaller anonymous set of nodes, thereby affecting anonymity.

Similar to the node information matrix X, assuming there are n nodes in the anonymous set and m evaluation indicators, the network information matrix X_{net} obtained through measuring the anonymous system is as follows:

$$\mathrm{X}_{\mathrm{net}} = \begin{bmatrix} \mathrm{X}_{\mathrm{net}\,11} & \cdots & \mathrm{x}_{\mathrm{net}\,1m} \\ \vdots & \ddots & \vdots \\ \mathrm{x}_{\mathrm{net}\,n1} & \cdots & \mathrm{x}_{\mathrm{net}\,\mathrm{nm}} \end{bmatrix} \tag{14}$$

In Eq. (14), assuming $i \in [1, n]$, $j \in [1, m]$, then $X_{net_{ij}}$ represent the value of the evaluation indicator j of the node i in the network information matrix X_{net}.

Because network anonymity requires comparing the unevenness of the distribution of evaluation indicators among nodes, data normalization is performed to eliminate dimensional differences among data. the normalized value of $X_{net_{ij}}$ is as follows:

$$\mathrm{y}_{\mathrm{net}_{\mathrm{ij}}} = \frac{\mathrm{x}_{\mathrm{net}_{\mathrm{ij}}}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{x}_{\mathrm{net}_{\mathrm{ij}}}} \tag{15}$$

Thus, X_{net} is transformed into a normalized network information matrix Y_{net}:

$$\mathrm{Y}_{\mathrm{net}} = \begin{bmatrix} \mathrm{y}_{\mathrm{net}\,11} & \cdots & \mathrm{y}_{\mathrm{net}\,1\mathrm{m}} \\ \vdots & \ddots & \vdots \\ \mathrm{y}_{\mathrm{net}\,\mathrm{n1}} & \cdots & \mathrm{y}_{\mathrm{net}\,\mathrm{nm}} \end{bmatrix} \tag{16}$$

In Eq. (16), assuming $i \in [1, n], j \in [1, m]$, then $\mathrm{y}_{\mathrm{net}_{\mathrm{ij}}}$ represent the normalized value of the evaluation indicator j of the node i in the network information matrix Y_{net}.

Network anonymity

In this paper, we modify the normalized Shannon entropy and use the normalized network information matrix to analyze the differences of various indicators in the anonymous set. Then, the weighted sum is calculated using the coefficient of variation, and the network anonymity degree can be obtained.

Assuming there are n nodes and m evaluation indicators in the anonymous network, w is the weight of the indicator, and $y_{net_{ij}}$ represents the normalized value of evaluation indicator j for node i, the network anonymity D_{net} can be calculated as follows:

$$D_{net} = \frac{H(x)}{H_{\max}(x)} = \frac{-\sum_{j=1}^{m} w_i \sum_{i=1}^{n} y_{net_{ij}} \cdot \log_2 y_{net_{ij}}}{\log_2 n} \quad (17)$$

We dynamically evaluate anonymity based on multiple attributes from node to network.Network anonymity represents the overall anonymity of all nodes and changes in the anonymity of a single node can affect the overall network anonymity degree. By combining various network behavioral characteristics, we comprehensively evaluate the anonymity, avoiding the one-sidedness of a single or static evaluation indicator and accurately analyzing the anonymity degree of complex networks.

Similarly, a stable interval S_{net} can be delineated based on the network anonymity degree during the last normal operation cycle, where $S_{net} = [\theta_{net\,1}, \theta_{net\,2}]$. When the current cycle's network anonymity exceeds this range S_{net}, it is deemed that the anonymous network is in an abnormal state.

Experiment and evaluation

The anonymity evaluation method proposed in this paper is designed to measure the anonymity degree of nodes or network in a self-built Tor network. To verify the effectiveness of the anonymity evaluation method based on node anonymity, we first measured its anonymity status under normal operation in a self-built Tor network and observed the dynamics of the multi-indicator evaluation for anonymity degree (Table 2).

Subsequently, we conducted a DDoS attack on the network to compare the multi-attribute anonymity proposed in this paper with the entropy-based anonymity of a single evaluation indicator, to examine the advantages of evaluating multi-attribute anonymity and to check whether abnormal node can be detected and whether the network is in an abnormal state. Finally, we evaluated the accuracy of the anonymity evaluation method by removing abnormal node and conducting malicious code injection attacks (Fig. 4).

Experimental environment

We established a self-built Tor network with one directory server (DA) and five relay nodes (RA) that constructed anonymous communication paths of length $l = 3$. A program security monitoring plugin was installed on all nodes to observe any abnormal modifications made to the programs. All nodes used Intel(R) Xeon(R) E5-2696v4 as the CPU, had a 200 G hard disk capacity, and a 16GB memory capacity. The overall

Table 1 Notations and their descriptions

Notations	Descriptions
Y	Initialized node information matrix
X	Node information matrix
x'_{ij}	Initial value of the jth evaluation metric for the i-th node in X
y_{ij}	Initialized value of the jth evaluation metric of the i-th node in Y
v_j	The coefficient of variation of indicator j
$\overline{x}_j$	The average value of indicator j
S_j	Standard deviation of indicator j
w_j	Weight of indicator j
R_i	Behavior base value of node
IQR	Interquartile distance
D_{node}	Node anonymity
D_{net}	Network anonymity
X_{net}	Network information matrix
Y_{net}	Initialized Network information matrix
$x_{net_{ij}}$	Initial value of the jth evaluation metric for the i-th node in X_{net}
$y_{net_{ij}}$	Initialized value of the jth evaluation metric of the i-th node in Y_{net}

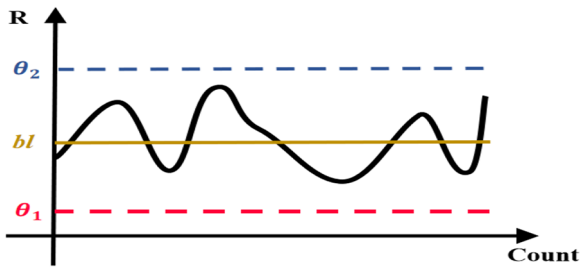

Fig. 2 Node stability interval

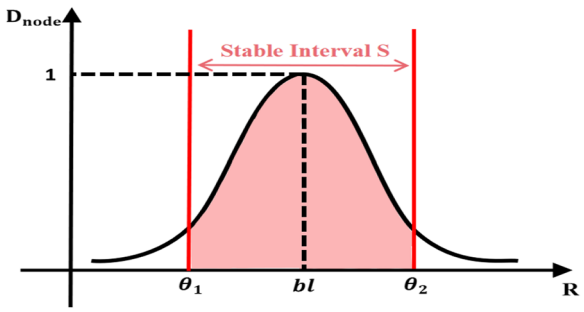

Fig. 3 Node anonymity evaluation

Table 2 Statistics of evaluation indicators for all RA in normal operation

Indicators Range /Mean Nodes	Latency (ms)	Vailable running memory (kb)	Throughput rate (kb/s)	Number of connections (count)
RA1	[5.278,208.400] /60.253	[12351640,12420368] /12387923	[3.670,30.210] /8.393	[8,25] /11.833
RA2	[9.264,197.600] /75.069	[12954004,13023700] /12984364	[3.640,43.270] /8.637	[8,25] /11.438
RA3	[8.356,11.360] /9.792	[13177076,13255924] /13204399	[3.480,44.450] /9.501	[9,31] /13.229
RA4	[8.576,11.140] /10.030	[13790416,13890392] /13845799	[3.960,46.520] /11.703	[11,27] /13.423
RA5	[8.376,11.340] /9.812	[13084888,13191640] /13154152	[3.680,51.07] /11.117	[9,30] /13.458

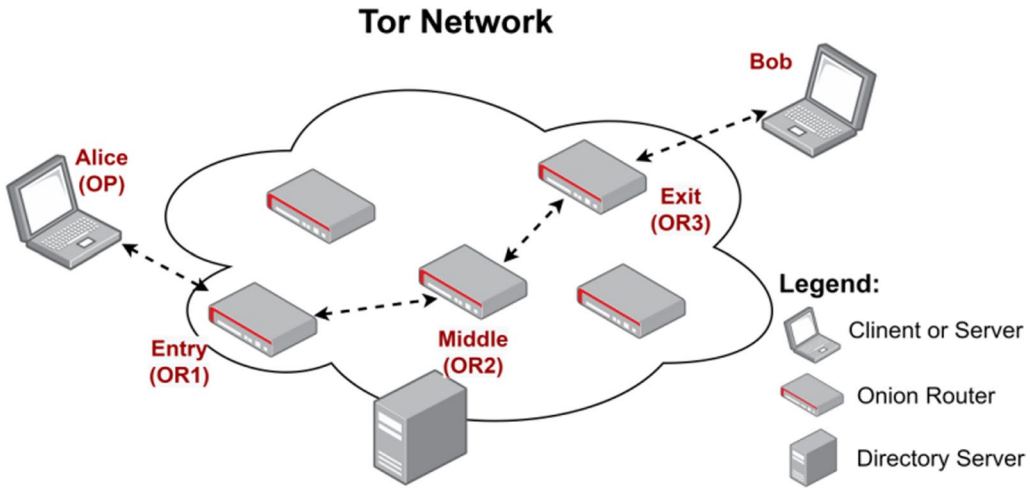

Fig. 4 Tor network structure diagram

anonymous network was operated using Tor version 0.4.5.7.

Normal operation comparison

Through experiment when the anonymity system is in normal operation, we compared our anonymity evaluation method with existing methods that only rely on a single indicator. Typical applications include evaluating information entropy anonymity based on the distribution of star-end-combs during path construction (Milajerdi and Kharrazi 2015) and calculating Gini coefficient anonymity based on the frequency of node selection (Snader and Borisov 2008), thus testing the dynamics and applicability of our anonymity evaluation method in normal operation.

Using a 12-hour period as one cycle, the Tor network runs for T1 cycle under normal conditions, and collects all anonymity evaluation indicators at intervals of 5 min during the operation.

The network anonymity is evaluated using our method proposed and the two methods mentioned above respectively, where the present method sets the constant $\beta = 2$ when calculating the weights in Eq. (7), sets the constant $d = 10$,the base $\alpha = \frac{1}{2}$ for calculating the node anonymity in Eq. (13) and (14). To better analyze the impact of each evaluation indicator on node behavior base value and network anonymity, the statistics of the evaluation indicators for all RA after T1 cycle are summarized in Table 1.

Table 1 indicates that the vailable running memory, throughput rate, and number of connections of the five RA nodes are very similar in both range and mean values. However, compared to the other three nodes, the latency of RA1 and RA2 has higher maximum and mean values,

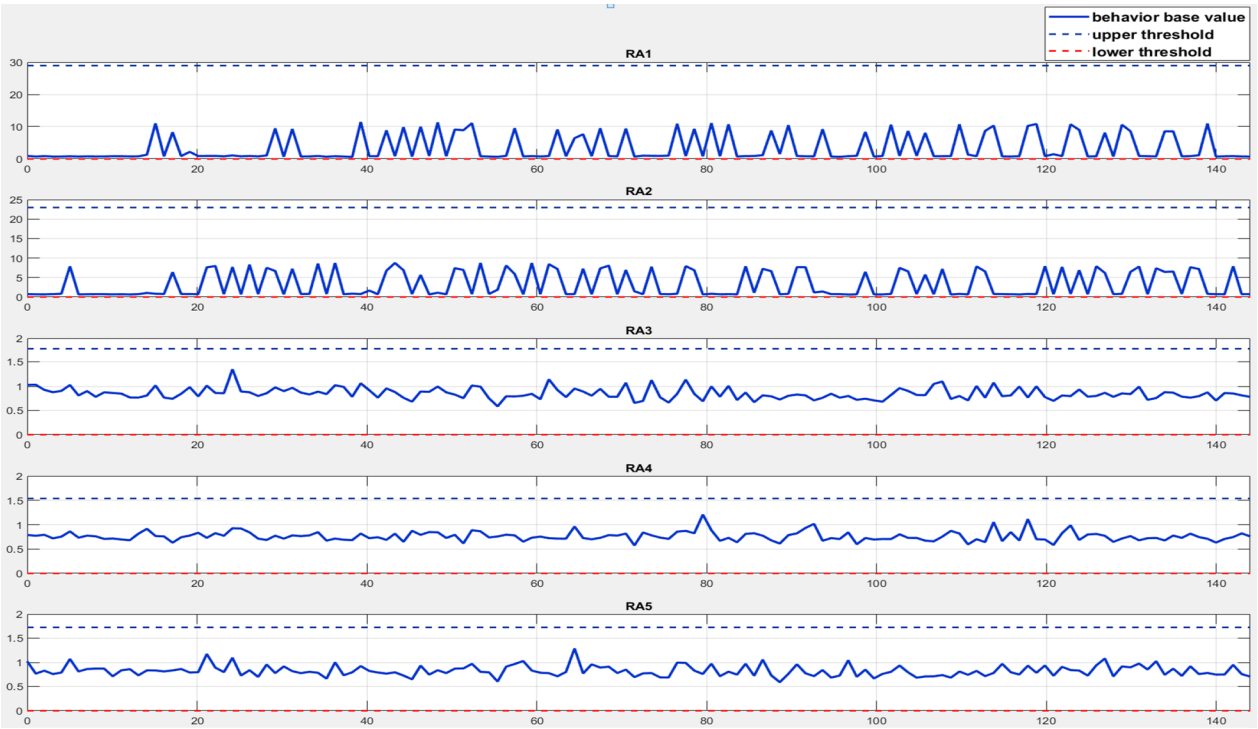

Fig. 5 Comparison of behavior base values of all RA in normal operation for 12 h

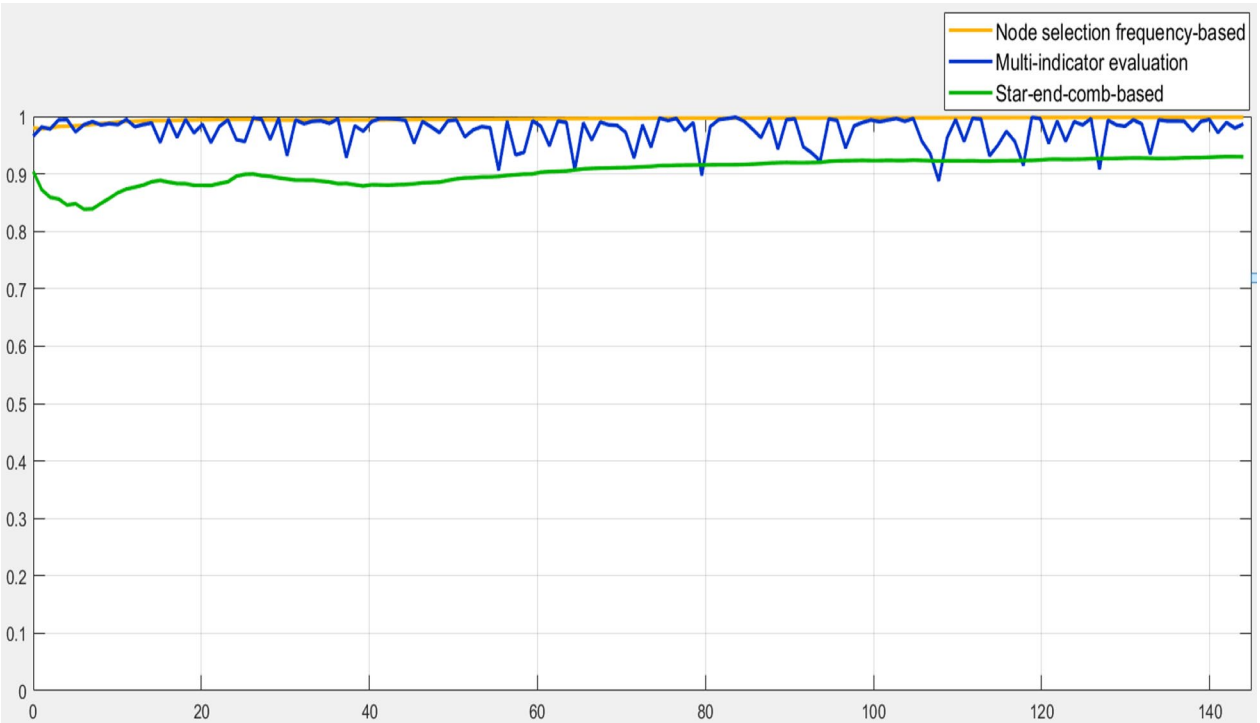

Fig. 6 Comparison of three network anonymity evaluation methods

indicating that there is a greater variation in the latency of RA1 and RA2 during normal operation.

As shown in Fig. 5, the different ranges of evaluation indicators can lead to relatively large behavior base value. Nonetheless, both node anonymity and stability interval models are related to the changing characteristics of the node's own behavior base value, which ultimately ensures that the network anonymity will not significantly decrease as a result, and all behavior base values are within their respective stable interval.

Figure 6 demonstrates a comparison of network anonymity in a self-built Tor network during cycle T1 using the multi-indicator evaluation method combined with the node selection frequency-based and star-end-comb-based methods. It can be observed that the network anonymity based on the node selection frequency method has small fluctuations during the cycle and is very close to 1, and the star-end-comb method produces slightly more fluctuations, but overall also tends towards 1. These two methods are relatively static and one-sided in evaluating anonymity. But when using our evaluation method proposed, the network anonymity exhibits more obvious changes. This is because the multi-indicator evaluation method can observe the network from multiple perspectives, thus providing a comprehensive and dynamic evaluation of network anonymity.

Comparison under DDos attack

Due to the broad applicability of anonymous communication technology, the Tor network has also received much attention and has been the target of an increasing number of traceback attacks. DDoS attacks (Jansen et al. 2019) are a type of denial-of-service attack that involves flooding a network with a sufficient burst of traffic in a short amount of time to cause congestion and disrupt communication along the entire chain. Such attacks can be used to cripple Tor relay nodes, and have a very low cost of attack, but they are extremely destructive.

To verify the effectiveness of our anonymity evaluation mechanism in the face of attacks, during cycle T2 of a self-built Tor network, a sustained DDoS attack was launched against relay node R1 for 3 h. The network anonymity was evaluated using the three methods mentioned in Section 3.2 under this attack scenario.

As shown in Fig. 7, due to the DDoS attack, the throughput rate of relay node R1 surged dramatically, as it was flooded with a large burst of traffic. Its behavior base value had far exceeded the stable interval defined during normal operation in cycle T1, while other nodes were still within their respective stable interval, operating normally.

Figure 8 shows the network anonymity under a DDoS attack evaluated by the three methods. Due to the dramatic change in behavior base value of RA1 and its far

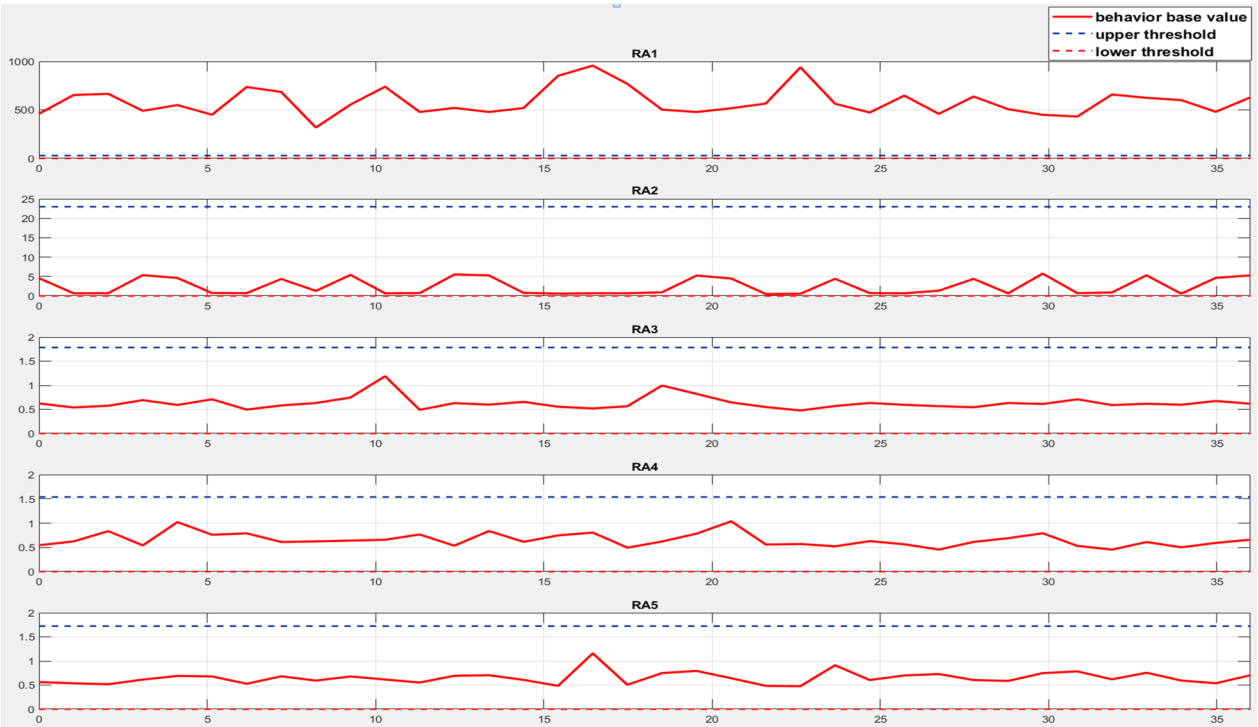

Fig. 7 Comparison of the behavior base values of all RA when RA1 is under DDos attack

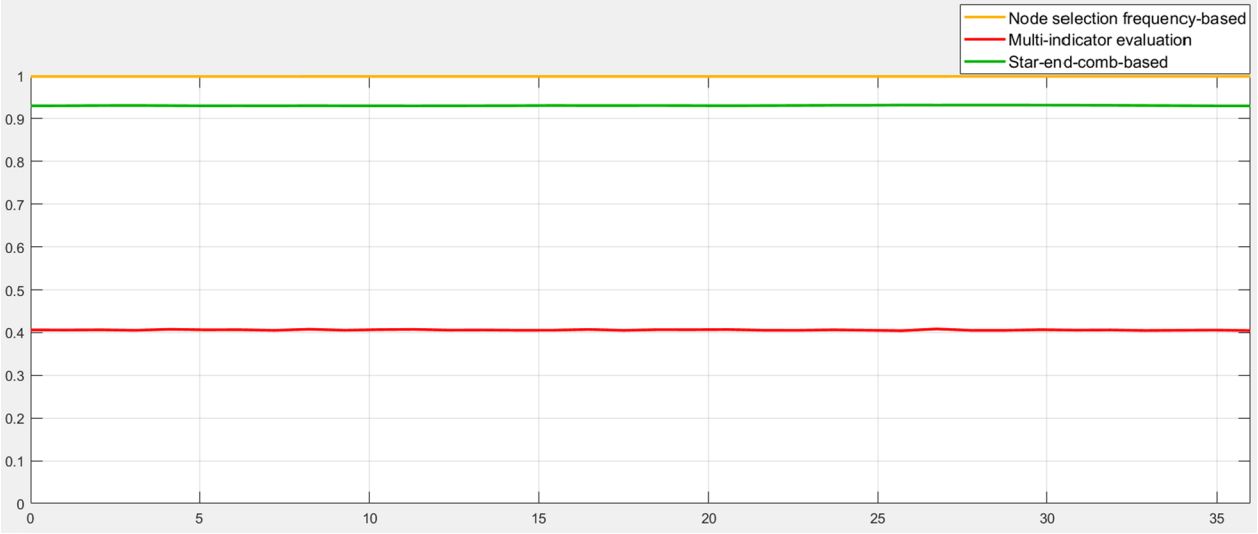

Fig. 8 Comparison of the three network anonymity evaluation methods when relay authority RA1 is subject to a DDoS attack

exceeding the upper threshold, the network anonymity evaluated by our multi-indicator evaluation method, which considers node anonymity, was significantly lower than that obtained by the other two methods under normal operation. This demonstrates the effectiveness of the anonymity evaluation mechanism proposed in this paper against DDoS attacks and its ability to reflect the threat to network anonymity when under attack.

Validation of anonymity evaluation

Remove abnormal node

If the anonymity degree can be restored to normal operation by removing abnormal node after an attack, it further demonstrates that our anonymity evaluation mechanism can correctly reflect the anonymity status of nodes and network. In cycle T2, after a 3-hour DDoS attack, node RA1, whose behavior base value exceeded the stable interval, was removed from the anonymous network. The network was allowed to continue running for 3 h while evaluating the anonymity using the multi-indicator evaluation method.

As shown in Fig. 9, during the normal operation cycle T1 and in the 3 h after removing abnormal nodes in cycle T2, the network anonymity was within the corresponding stable interval. However, during the 3-hour attack period in cycle T2, the network anonymity was significantly below the lower threshold, indicating that the network was in an abnormal state. This demonstrates that our evaluation mechanism can correctly evaluate changes in network anonymity, and that the stable interval can reflect whether nodes or network is in a normal state.

Face abnormal program modifications

The program monitoring is achieved by installing the host logging software Wazuh-agent on each node of the anonymous network to monitor attack behaviors against the hosts, such as brute-force cracking, file tampering, Trojan file implantation, and changes in system permissions, thereby securing the monitoring of all nodes in the anonymous network.

After removing abnormal nodes during cycle T2 for 3 h, the anonymity of the remaining nodes was still evaluated by collecting 60 evaluation indicators at 5-minute intervals. During normal operation (20 times), node RA2 was subjected to a malicious program injection attack, and during the subsequent 20 runs, it was subjected to the second malicious program injection attack.

Figure 10 illustrates the 60 anonymity evaluations of the RA2 node. Due to the adoption of $\alpha = \frac{1}{2}$ in Eq. (13), it is apparent that the anonymity of the RA2 node dropped below 0.5 after the first malicious program modification, compared to its normal operation. Furthermore, the node's anonymity experienced an even greater decrease after the second malicious program modification.

Conclusion and future work

This paper proposes a multi-indicator node anonymity evaluation method that is applicable to self-built Tor networks, which combines the node's own attributes and network behavior-related indicators at the node layer; We then propose an anomaly detection mechanism that enables the monitoring of anomalous states by counting their fluctuating changes on a time series based on behavior base value or network anonymity

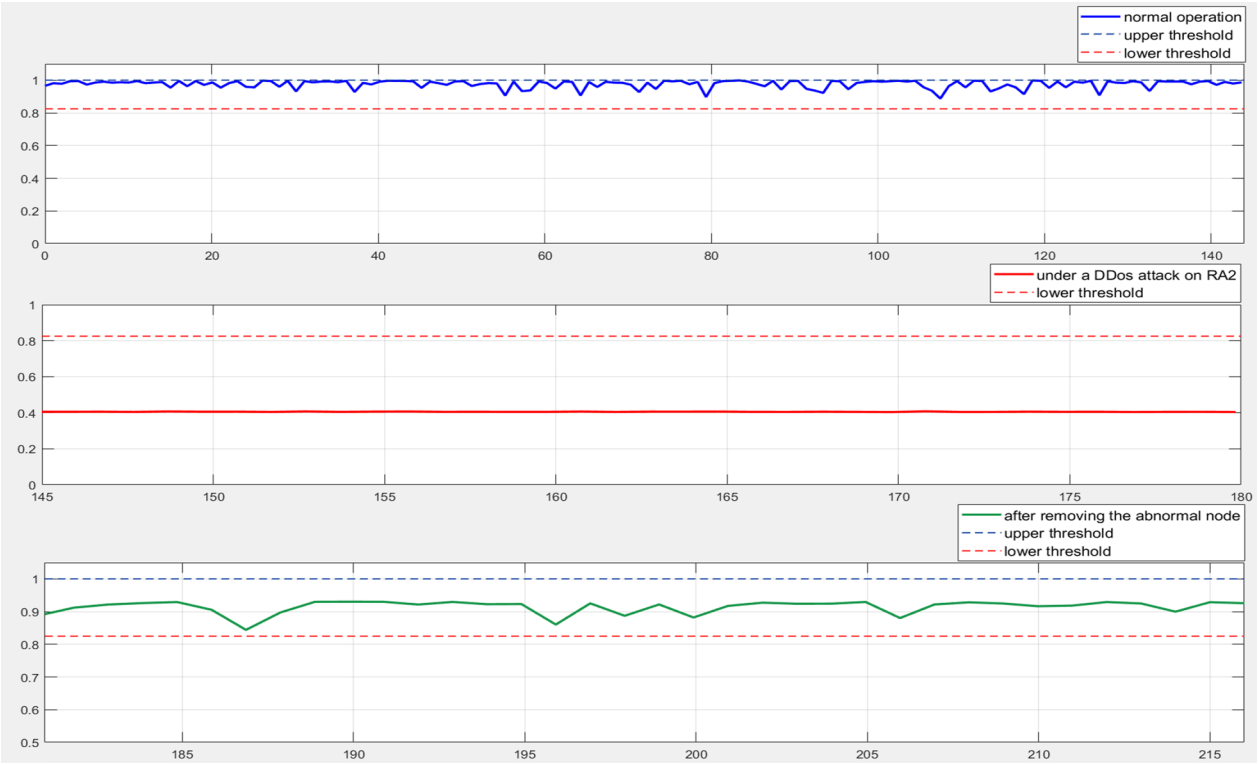

Fig. 9 Comparison of network anonymity before and after removeing anomalous nodes

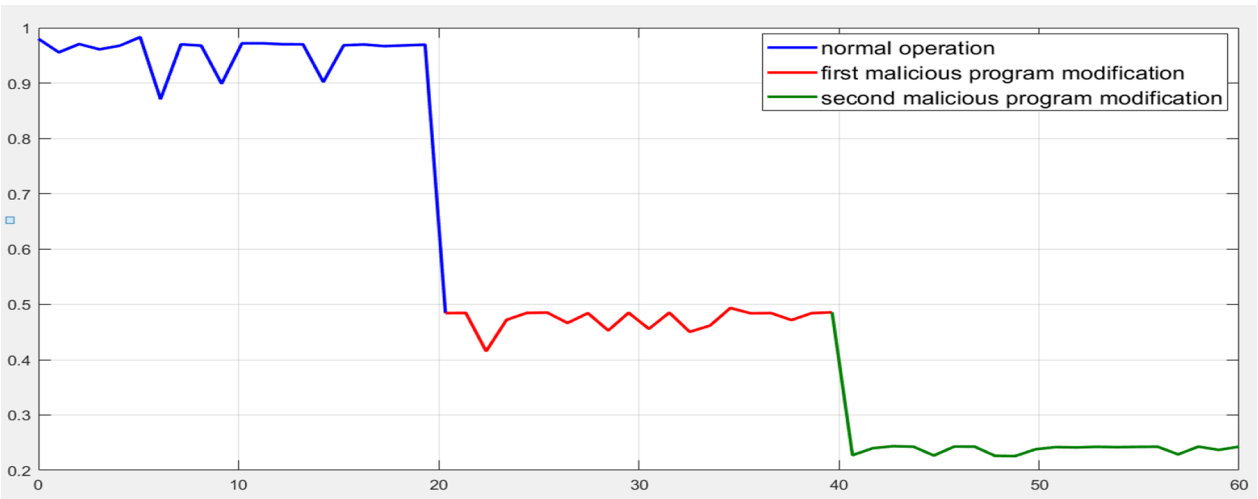

Fig. 10 Comparison of node anonymity of RA2 before and after the introduction of malicious program modifications

during normal operation, and then using the Interquartile Range (IQR) method to delineate the stability interval; Subsequently, a network anonymity evaluation mechanism was implemented based on normalized Shannon entropy, which combines the network behavior indicators of anonymous systems and node anonymity; Finally, the anonymity of our proposed method is evaluated and compared with other methods based on node selection probability and star-end-comb in various situations, including normal operation, DDos attack, and removal of abnormal node demonstrating its effectiveness in various network scenarios and superiority of possessing dynamic real-time analysis capabilities on a self-built Tor network.1

The next objective of this paper is to conduct a comprehensive analysis of various attacks against anonymous networks, in order to develop corresponding mechanisms for anonymity evaluation method when facing different attacks, and integrate them into a unified model to enhance the accuracy of anonymity degree.

Acknowledgements
We would like to thank the anonymous reviewers for their detailed comments and useful feedback.

Author contributions
The design of the proposed method, the experiment deployment and the draft of the manuscript: JC and CH. Revising the manuscript critically for important intellectual content: HM and RW. All authors read and approved the fnal manus.

Funding
This work was supported by the Tianjin Education Commission Research Program Project No.2019KJ024

Availability of data and materials
Not applicable.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 12 May 2023 Accepted: 11 September 2023
Published online: 08 November 2023

References

Backes M, Kate A, Meiser S, Mohammadi E (2014) (nothing else) mator(s) monitoring the anonymity of Tor's path selection. In: Proceedings of the 2014 ACM SIGSAC conference on computer and communications security, pp 513–524
Basyoni L, Erbad A, Alsabah M, Fetais N, Mohamed A, Guizani M (2021) QuicTor: Enhancing tor for real-time communication using QUIC transport protocol. IEEE Access 9:28769–28784
Berthold O, Federrath H, Köpsell S (2001) Web mixes: a system for anonymous and unobservable internet access. In: Designing privacy enhancing technologies: international workshop on design issues in anonymity and unobservability Berkeley, Springer, pp. 115–129
Buccafurri F, De Angelis V, Idone MF, Labrini C, Lazzaro S (2021) Achieving sender anonymity in tor against the global passive adversary. Appl Sci 12(1):137
Chaum DL (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. Commun ACM 24(2):84–90
Cherubin G (2017) Bayes, not naïve: security bounds on website fingerprinting defenses. Proc Priv Enhancing Technol 2017(4):215–231
Clauß S, Schiffner S (2006) Structuring anonymity metrics. In: Proceedings of the second ACM workshop on digital identity management, pp 55–62
Dahlberg R, Pulls T, Ritter T, Syverson P (2021) Privacy-preserving & incrementally-deployable support for certificate transparency in Tor. Proc Priv Enhancing Technol 2021(2):194–213
Diaz C, Troncoso C, Danezis G (2007) Does additional information always reduce anonymity? In: Proceedings of the 2007 ACM workshop on privacy in electronic society, pp 72–75
Dingledine R, Mathewson N, Syverson P (2004) Tor: the second-generation onion router. Technical report, Naval Research Lab Washington DC
Eaton E, Sasy S, Goldberg I (2022) Improving the privacy of Tor onion services. In: International conference on applied cryptography and network security, Springer, pp 273–292
Gkountouna O, Terrovitis M (2015) Anonymizing collections of tree-structured data. IEEE Trans Knowl Data Eng 27(8):2034–2048
Guan Y, Fu X, Bettati R, Zhao W (2002) An optimal strategy for anonymous communication protocols. In: Proceedings 22nd international conference on distributed computing systems, IEEE, pp 257–266
Jansen R, Tschorsch F, Johnson A, Scheuermann B (2014) The sniper attack: anonymously deanonymizing and disabling the tor network. Technical report, Office of Naval Research Arlington, VA
Jansen R, Vaidya T, Sherr M (2019) Point break: a study of bandwidth denial-of-service attacks against tor. In: USENIX security symposium, pp 1823–1840
Kuhn C, Beck M, Schiffner S, Jorswieck E, Strufe T (2019) On privacy notions in anonymous communication. Proc Priv Enhancing Technol 2:105–125
Kwon A, AlSabah M, Lazar D, Dacier M, Devadas S (2015) Circuit fingerprinting attacks: passive deanonymization of tor hidden services. In: 24th {USENIX} security symposium ({USENIX} Security 15), pp 287–302
Melloni A, Stam M, Ytrehus Ø (2022) On evaluating anonymity of onion routing. In: Selected areas in cryptography: 28th international conference, virtual event, Springer, pp 3–24
Milajerdi SM, Kharrazi M (2015) A composite-metric based path selection technique for the tor anonymity network. J Syst Softw 103:53–61
Mittal P, Khurshid A, Juen J, Caesar M, Borisov N (2011) Stealthy traffic analysis of low-latency anonymous communication using throughput fingerprinting. In: Proceedings of the 18th ACM conference on computer and communications security, pp 215–226
Pfitzmann A, Köhntopp M (2001) Anonymity, unobservability, and pseudonymity-a proposal for terminology. In: Designing privacy enhancing technologies: international workshop on design issues in anonymity and unobservability Berkeley, Springer, pp 1–9
Piotrowska AM, Hayes J, Elahi T, Meiser S, Danezis G (2017) The loopix anonymity system. In: 26th {USENIX} security symposium ({USENIX} security 17), pp 1199–1216
Reininger M, Arora A, Herwig S, Francino N, Hurst J, Garman C, Levin D (2021) Bento: safely bringing network function virtualization to Tor. In: Proceedings of the 2021 ACM SIGCOMM 2021 conference, pp 821–835
Reiter MK, Rubin AD (1998) Crowds: anonymity for web transactions. ACM Trans Inf Syst Security (TISSEC) 1(1):66–92
Rochet F, Pereira O (2017) Waterfilling: balancing the tor network with maximum diversity. Proc Privacy Enhancing Technol 207(2):4–22
Sakai K, Sun M-T, Ku W-S, Wu J, Alanazi FS (2017) Performance and security analyses of onion-based anonymous routing for delay tolerant networks. IEEE Trans Mob Comput 16(12):3473–3487
Schnitzler T, Pöpper C, Dürmuth M, Kohls K (2021) We built this circuit: exploring threat vectors in circuit establishment in Tor. In: 2021 IEEE European symposium on security and privacy (EuroS &P), IEEE, pp 319–336
Serjantov A, Danezis G (2003) Towards an information theoretic metric for anonymity. In: Privacy enhancing technologies: second international workshop, PET 2002 San Francisco, Springer, pp 41–53
Snader R, Borisov N (2008) A tune-up for Tor: improving security and performance in the tor network. In: NDSS, vol 8, p 127
Sun Y, Edmundson A, Vanbever L, Li O, Rexford J, Chiang M, Mittal P (2015) {RAPTOR}: routing attacks on privacy in tor. In: 24th {USENIX} security symposium ({USENIX} security 15), pp 271–286
Tan Q, Shi J, Fang B, Guo L, Zhang W, Wang X, Wei B (2015) Towards measuring unobservability in anonymous communication systems. J Comput Res Dev 52(10):2373–2381
Tan Q, Wang X, Shi W, Tang J, Tian Z (2022) An anonymity vulnerability in Tor. IEEE/ACM Trans Netw 30(6):2574–2587
Tóth G, Hornák Z, Vajda F (2004) Measuring anonymity revisited. In: Proceedings of the ninth Nordic workshop on secure IT systems, pp 85–90
Wails R, Sun Y, Johnson A, Chiang M, Mittal P (2018) Tempest: temporal dynamics in anonymity systems. Preprint arXiv:1801.01932
Winter P, Köwer R, Mulazzani M, Huber M, Schrittwieser S, Lindskog S, Weippl E (2014) Spoiled onions: exposing malicious tor exit relays. In: Privacy enhancing technologies: 14th international symposium, PETS 2014, Amsterdam, Springer, pp 304–331

Xia Y, Chen R, Su J, Zou H (2021) Balancing anonymity and resilience in anonymous communication networks. Comput Secur 101:102106
Yang K, Xiao M, et al (2022) A Framework for formal analysis of anonymous communication protocols. Security and Communication Networks 2022
Zhang W, Lu T, Du Z (2021) TNRAS: Tor nodes reliability analysis scheme. In: 2021 the 11th international conference on communication and network security, pp 21–26

Publisher's Note