2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications

A Scalable Anonymity Scheme Based on DHT Distributed Inquiry

Wentao Wang
Graduate University of Chinese Academy of Sciences, China
wwt@lois.cn

Yuewu Wang
Graduate University of Chinese Academy of Sciences, China
ywwang@lois.cn

Jiwu Jing
Graduate University of Chinese Academy of Sciences, China
jing@ieee.org

Zhongwen Zhang
Graduate University of Chinese Academy of Sciences, China
zwzhang@ lois.cn

Abstract—**Two key factors in the design of anonymity schemes are the scalability and the security of the relay node selection. In this paper, a scalable, secure anonymity scheme based on DHT inquiry mechanism is presented. Unlike the most existing schemes, every relay node's routing information (RRI) is stored as normal data in DHT overlay. The routing information can be inquired just with corresponding relay node's Relay ID (RID).All RID is maintained by SA to fill a dynamic range. So, user only needs to get the range of RID to select relay nodes, which is a datum with constant size. Such a mechanism significantly improve the scalability of scheme. Furthermore, RID assigned by SA also provides a more stable and provable relationship between relay nodes, which can be used to help validation of RRI storage. With this innovation, security measures are introduced. The framework of the scheme, key technical details and security analysis are described in this paper. In addition, simulation experiments are conducted to validate the effectiveness of this scheme.**

Key words: Anonymous Communication, DHT, Distributed Inquiry, Scalability, Security

I. INTRODUCTION

Anonymous communication is an important technology for network privacy protection to conceal the correspondence between the initiator and responder. Among all anonymity schemes, low-latency anonymity schemes are more prevalent. Two key factors in the design of low-latency anonymity schemes are the scalability and the security of the relay node selection. Currently, substituting the centralized scheme for decentralized P2P scheme to solve the scalability problem is a prevalent trend. The P2P anonymity schemes are potentially more scalable than centralized schemes. However, some new security threats are introduced when P2P mechanism is used for anonymity scheme design, such as the Overlay ID space attacks, the attacks on P2P distributed inquiry, and overly node churn attacks.

In this paper, a novel anonymity scheme is presented. Similar to most existing P2P anonymity scheme, all the relay nodes are also be organized into a P2P overlay. But, instead of select relay in the overlay DHT directly, this scheme takes the anonymous routing information as the normal data stored in P2P overlay. Thus, the traditional P2P data storage security measures can be reused easily to verify the routing data. In addition, some security enhancement measures based on SA can make this scheme more secure.

The major works of this paper include: *I.* A novel anonymity scheme is presented, through taking the anonymous routing information as normal data stored and inquired by P2P mechanism, the scalability of this scheme can be increased obviously; *II.* Necessary security measures based on SA are introduced, which make the scheme can against the major security threats caused by distributed P2P inquiry. *III.* Based on general network simulation software, a scheme simulation model is developed, and some simulation experiments are conducted to validate the effectiveness of this scheme.

The remainder of this paper is structured as follows. Section II describes the related works of low-latency anonymity scheme research. Section III describes the necessary background of the scheme design. The design of the novel anonymity scheme and some key technical details are discussed in Section IV. In Section V, the security features of this scheme are discussed. In Section VI, through simulation experiments, the effectiveness of this scheme is analyzed. Finally, we conclude this paper in section VII with a brief summary.

II. RELATED WORK

The concept of anonymous communication was first presented by CHAUM et al. [1]. The anonymity schemes can be divided into two categories: high-latency anonymity schemes and low-latency anonymity schemes. High-latency anonymity schemes prefer to perfect anonymity with complex technical mechanism. Although the anonymity provided by high-latency schemes is perfect, the communication latency is high, which makes their applications be limited to the scenarios, in which the communication timeliness is less demanding, such as e-mail system.

Compared to high-latency anonymity schemes, low-latency anonymity schemes pay more attention on the communication timeliness. Currently, Tor is one of the most widely-used low-latency anonymity schemes [2, 3]. Tor is an open system with centralized anonymous relay node discovery. The server keeps a list of active relay nodes. When an anonymity communication service is needed, the user first download the list of relay nodes, then several nodes are selected (usually the number is 3) to establish a circuit by successively exchanging keys with the selected relay nodes in a "telescoping" fashion. The centralized relay nodes selection is easy and reliable. However, compared to pure

978-0-7695-4745-9/12 $26.00 © 2012 IEEE
DOI 10.1109/TrustCom.2012.55

P2P schemes, the scalability of Tor isn't very good. Every user must maintain a global view of all relay nodes. The bandwidth costs will scale quadratically with the number of users and relay nodes. Assuming that the number of user is *n*, and the number of relay nodes is *r*, the bandwidth costs for anonymous relay nodes discovery scales as *O* (*nr*). There are some other similar schemes, such as Crowds [4].

In order to increase the scalability, some schemes are proposed based on DHT P2P mechanism. The major improvement of P2P schemes is substitute the global list of relay nodes. Tarzan is one of the earliest P2P anonymity scheme, but user of Tarzan have to get the entire list of relay node when constructing anonymous circuit [5]. Cashmere anonymity scheme is built on the Pastry DHT. In Cashmere, the relay nodes are divided into different groups, and the nodes in a group share a pair of public\private key. Thus, the information used for anonymous circuit construction can be decreased, and the scalability is increased. On the other hand, the anonymity of Cashmere is weakened because of group mechanism [6, 7]. Salsa is a Chord-like DHT anonymity scheme. The DHT routing mechanism is used for relay nodes identification directly. Although some security measures are taken, it cannot against the DHTID space attack very well [8, 9]. MorphMix don't need a global stable of highly reliable relay nodes. The initiator selects the first relay node, and each node in the anonymous circuit indentifies the next hop node independently. This improvement can increase the scalability obviously. However, in MorphMix, the adversary can operate several malicious nodes to break the anonymity [10]. Torsk improves the scalability of Tor, while retaining the benefits its user-server architecture, by introducing the Myrmic [11] mechanism [12].

III. Background

The scheme presented in this paper is based on the data storage and inquiry in Kad-like [13] DHT P2P mechanism.

In Kad-like DHT, every node is assigned an *ID* called DHTID, and the routing table of node *N* is composed of a group of lists. Every list $i(0 \leq i < 160)$ includes the routing information of *k* nodes. The distance from the *k* nodes to node *N* is between $[2^i ,2^{i+1})$. One list of the routing table is called *k-bucket*. The distance between 2 nodes is defined as the XOR value of DHTID*s* assigned to the 2 nodes. A routing record in a *k-bucket* has the form of (DHTID, IP, Port). Based on IP protocol, all nodes are connected by DHT routing, and form a DHT overlay.

The main function of DHT overlay is distributed data storage and inquiry. When a data is to be stored in the DHT overlay, a *key* value must be calculated firstly with same process of DHTID calculation. The node whose DHTID is nearest to the *key* is called root (*key*). The data will be stored on root (*key*) and its neighbors. When the data is inquired, according to the *key* value, the inquiry can be routed to root (*key*) and its neighbors, on which the data is stored.

The introduction of distributed DHT inquiry brings new security threats to anonymity scheme, while it improves the scalability. The traditional DHT security problems [14] can also impact the security of the anonymity scheme. Andrew Tran et al. analyzed the attacks on anonymity scheme caused by DHT security threats [15]. The threats on anonymity brought by DHT can be divided into 3 categories: *I. Attacks on* DHTID. Through forging and controlling the DHTID, the attacker can compromise the DHT mechanism effectively [16, 17]. *II. Attacks on distributed inquiry*. DHT is an open system. Thus, the inquiry path may include malicious nodes, and the results of inquiry can be compromised [18]. *III. Overlay node churn attacks*. Malicious node may join and leave the overlay frequently, which will produce a lot of routing maintenance messages, and decrease the efficiency of DHT [19]. All these security threats must be considered adequately when DHT overlay is used in anonymity scheme.

IV. Scheme Design

The main technical idea of this scheme is organizing the anonymous relay nodes into a DHT overlay, and taking the relay node routing information as normal data that can be stored and inquired on the DHT overlay. Some necessary security measures are introduced to against the threats brought by DHT mechanism. In this section, we first describe the framework of the scheme in general, and then presented the design of key processes in detail.

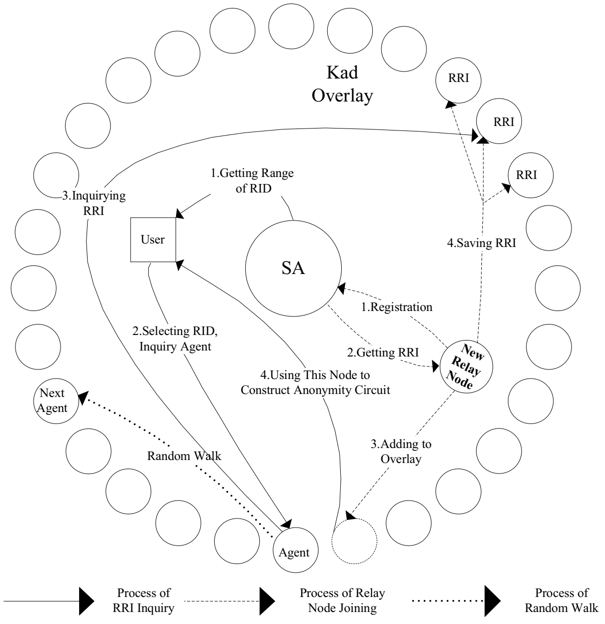


Figure 1. The frmaework of the scheme

A. Framework of The Scheme

The framework of the scheme is shown in Fig 1. The scheme is composed of 3 parts: SA, Kad-like DHT overlay and anonymity user.

The Kad-like DHT overlay is formed by anonymous relay nodes. A node should be registered to SA before joining into DHT overlay as an anonymous relay. In the registration process, SA assembles and provides the anonymous relay routing information to the node. *k* is the RID assigned by SA to the node. The relay routing information (RRI) has the format as follow:

$$RRI=\{k, KadID, List_{Addr}, List_{Pubkey} , T, Sig_{SA}\} \qquad (1)$$

Sig_{SA}=SIG$_{SA}$(RID, $KadID$, IP, $Port$, $List_{Pubkey}$,T) (2)

$List_{Addr}$={ IP^{k-1}, $Port^{k-1}$, IP^k, $Port^k$, IP^{k+1}, $Port^{k+1}$} (3)

$List_{Pubkey}$={ $Pubkey_{k-1}$, $Pubkey_k$, $Pubkey_{k+1}$ } (4)

$KadID$=HASH (IP^k, $Port^k$) (5)

$List_{Addr}$ is a group of IP address as shown in formula 3. {IP^k, $Port^k$} is the IP address of this node. {IP^{k+1}, $Port^{k+1}$} and {IP^{k-1}, $Port^{k-1}$} are the IP address of nodes whose RID are k+1 and k-1. Node k+1 and k-1 are also called validation nodes of node k. $KadID$ is the DHTID of the node. As shown in formula 5, $KadID$ is calculated by SA using a secure Hash function HASH (.). As above description, $KadID$ is used to join the DHT overlay. $List_{Pubkey}$ is a list of 3 public keys. $Pubkey_k$ is the public key possessed by the new node k. $Pubkey_{k-1}$ and $Pubkey_{k+1}$ are the public keys of 2 validation nodes k-1, k+1. $Pubkey_k$ is used to implement anonymous protocol. $Pubkey_{k-1}$ and $Pubkey_{k+1}$ are used to enhance the security of RRIs inquiry. Sig_{SA} is a digital signature generation by SA with its private key. SIG$_{SA}$ represent the signature algorithm adopted by SA. The signature can be verified by user. The generation time of Sig_{SA} is T.

After the new relay node being added to the DHT overlay successfully, the RRI should be stored on the DHT overlay. New node calculates the key of RRI firstly, as formula 6 shows.

Key= HASH (k, T) (6)

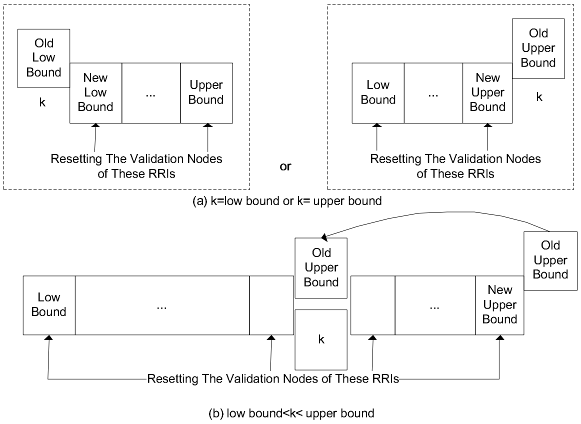
So, according to the definition in Section III, the distance between Key and a DHTID can be calculated easily. Then, a DHTID inquiry find n nodes whose DHTID is closest to Key. The RRI will be stored on these n nodes.

Besides the redundant storage mechanism of Kad-like DHT as above description, two nodes k-1 and k+1 are selected as validation nodes of node k for two extra validation mechanisms. First, all Kad RPC massage (ping, store, find node, find value) to node k should also been send to its validation nodes, and validation nodes should maintain a Kad routing table of node k by these massage for validating k's routing table. Second, RRI of node k should also be stored on these two validation nodes. The specific validation process will be described in detail later. Because the IP addresses of these two validation nodes are included in the RRI, the new node can complete the stored procedure by itself and not increase the burden of SA.

Users only need to update RID range from SA with a very low frequency. When an anonymous service is needed, the user can select and inquire a series of RRI*s* from DHT overlay without communication to SA. Subsequently, an anonymity circuit can be constructed with these RRI*s*. The specific process is described in F part of this Section.

B. *RID Empty Elimination*

The RID empty elimination process is shown in Fig 2. If the RID to be withdrawn is low bound or upper bound of the RID range, the RRI corresponding to the RID will be deleted directly. The validation nodes of the RRIs adjacent to the RID will be reset, as Fig 2 (a) shows. If the RID k is a value between the low and upper bound, the RRI corresponding to k will be deleted and the RRI corresponding to upper bound will be transferred to the position of k. The related validation nodes should be reset also, as Fig 2 (b) shows.



Old Low Bound
k
New Low Bound
...
Upper Bound
Resetting The Validation Nodes of These RRIs
or
Low Bound
...
New Upper Bound
Old Upper Bound
k
Resetting The Validation Nodes of These RRIs
(a) k=low bound or k= upper bound
Low Bound
...
Old Upper Bound
k
...
New Upper Bound
Old Upper Bound
Resetting The Validation Nodes of These RRIs
(b) low bound<k< upper bound

Figure 2. The process of RID empty elimination

C. *RRI Storage*

As the discussion in A part of this Section, the position of RRI storage is determined by Key= HASH (k, T). k is the RID assigned by SA. However, T is variable. In order to keep the consistency of time among all users, T should be measured in big unit. Practically, date is selected as the timing unit, so RRI storage positions are daily changed. Every relay node periodically re-stores its RRI datum into DHT overlay with position according to current date.

D. *RRI Inquiry Agent*

RRI inquiry agents are used to conceal the traffic pattern of anonymous communication users,. In our scheme, SA will provide several nodes to user as initial agents. Then, user selects an agent from the agents list randomly to conduct the RRI inquiry. At the same time, one of the validation nodes of the agent is also been selected to conduct the RRI inquiry. The validation node will generate a signature for the inquiry result with its private key, and the user can verify the inquiry result obtained by validation node with the public key stored in the RRI of the agent.

After the RRI inquiry is completed by the agent, random walks will be used to update the agents list. There are two kinds of random walks: DHT walk and RID walk. DHT walk determines the next hop node by selecting a node from the DHT routing table, while RID walk selects one of its validation nodes as the next hope node. RID walk cannot be disturbed by the DHTID attack, but the next hop node in RID walk is easy to be predicted. The case in DHT walk is just the opposite. A mix walk is adopted in this scheme. When the next hop node of the random walk is determined, RID walk is adopted with a given possibility p and the DHT walk is adopted with 1-p.

Suppose that the probability of n-hop node in random walk being malicious is P_n, P_{n+1} can be calculated with formula 7. Where, f and p are the same as above defined. The limit value of P_n is shown in formula 8. It can be seen from formula 9 that the upper bound of P_n will not exceed f/p. So, the probability of an agent inquiry being compromised in this scheme is f^2/p.

$$\begin{aligned} P_{n+1} &= (1-P_n)f + P_n(1-p) + P_n pf \\ &= f + P_n(1-p)(1-f) \end{aligned} \quad (7)$$

$$\lim_{n\to\infty} P_n = \frac{f}{1-(1-p)(1-f)} \tag{8}$$

$$P_n < \frac{f}{1-(1-p)(1-f)} < \frac{f}{p} \tag{9}$$

For security reasons, p is usually greater than 0.5. As above discussion, if p is too large, the next hop node in random walk can be predicted easily. So, in fact, the value of p is usually be set as 2/3.

E. Validating the Result of the RRI Inquiry

Validation measures are taken to ensure that the result of RRI inquiry is correct. The specific steps of the validation are listed as follow.

1) For security reasons, redundant inquiry is adopted in a RRI inquiry. After all RRI results being obtained, the user will verify the Sig_{SA} in these results with the public key of SA one by one. The RRI with the last T from the results will be selected as the final inquiry result based on above process.

2) From the $List_{Addr}$ in the RRI obtained in last step, the user can get the IP addresses of the 2 validation nodes. Then, the RRIs stored on the 2 validation nodes can be obtained by the user. If the 3 RRIs are Consistent, verification is successful. Otherwise, the one of the 3 RRIs with last T will be selected as the final RRI.

F. Anonymous Circuit Construction

Complete procedure of anonymous circuit construction is shown as follow.

1) A user gets the value range of RID and initial RRI inquiry agent list from SA.

2) User selects a value from range of RID, and calculated the *key* with the current time (date). Then, one inquiry agent is selected from agent list. The agent and one of agent's validation nodes conduct the RRI inquiry in parallel.

3) Update agent list according to the mix random walk process described in D part of this Section.

4) Verify every RRI inquiry result as the description in E parts of this Section.

5) Steps *1* through *4* are repeated until all the RRIs used for the anonymous circuit construction are obtained by the user successfully.

Then user can use these RRIs to construct an anonymous communication circuit. The public key in these RRIs can be used to implement the anonymous communication protocol.

V. Security Discussion

The attack model concerned in this scheme is the same as Tor and other low latency anonymity scheme: an adversary can control a small fraction of relay nodes to generate, modify, delete, delay or log traffic of its own, but cannot monitor the traffic of honest nodes.

As description in above sections, the major threats faced by this scheme include: the attacks on DHTID space, the attacks on the distributed inquiry of RRI, and the churn attack. In this Section, the security features of this scheme against these attacks are discussed.

*A. **The Security Feature against DHTID Space Attacks***

There are many DHTID space attack forms, such as the Sybil attack and Eclipse attack [16, 17]. In the scheme presented in this paper, the anonymous relay nodes are indexed by the RID included in RRI instead of DHTID. Because the RID is generated with security HASH functions, and assigned by SA, an adversary cannot tamper with it easily. In addition, the anonymous relay nodes are indexed by the RID included in RRI instead of DHTID, and a series of verification measures are included in this scheme as the description in E part of Section IV. These verification measures can make the risk of DHTID or RID being forged almost free.

*B. **The Security Feature against DHT Inquiry Attacks***

Inquiry in DHT overlay needs cooperation of quantity of nodes. So even if a small part of the overlay nodes are malicious, a lot of inquiry can be impacted. Now we use the attack model mentioned above to discuss the security feature of this scheme. Considering the worst-case, an adversary controlling a fraction f of node up to 20%, can provide an expired RRI with malicious node to any RID.

1) Misrouting can be launched only if a malicious node has two validation nodes malicious. So, the probability of misrouting is:

$$P_{misrouting} = f^3. \tag{10}$$

When f = 20%, $P_{misrouting}$=0.008. So even if there are considerable malicious nodes in system, DHT routing in this scheme still reliable. If adversary wants to provide an expired RRI to requester, it will be success only in two conditions: *I.* Inquiry agent and the selected validation node of agent both are malicious to provide fake but same RRI to requester. *II.* The root node of RRI and its two neighbors are malicious. Moreover, one of expired RRI validation node is online and malicious, and the other is offline or malicious. According to formula 9, the probability of expired RRI passing validation is:

$$P_{Exp} < 1 - \left(1 - \frac{f^2}{p}\right)\left(1 - f^4\right) \tag{11}$$

When f = 20%, P_{Exp}<0.06.Compared to f, it's still lightweight.

2) RRI inquiry could be broken by adversary in two conditions: *I.* Getting RRI failure. This condition need at least the root node of RRI and its two neighbors are malicious to refuse providing RRI. *II.* RRI cannot be validated. According to these two condition, the probability of successful Dropping is:

$$P_{drop} = 1 - (1 - f^3)(1 - f^2) \tag{12}$$

When f = 20%, P_{drop}=0.048. So adversary cannot impact inquiry much by selective dropping.

3) User implement RRI inquiry through the agent, so user can only be correlated with RRI inquiry by agent. As the description in D part of Section IV, the upper bound of the probability of an agent being malicious is f/p. Probability of passive logging is:

$$P_{logging} < f/p \qquad (13)$$

When f = 20%, $P_{logging}$ <0.3. Comparing to f, the probability of passive logging cannot be enlarged effectively. So, the cost of network monitoring with passive logging is still expensive in this scheme.

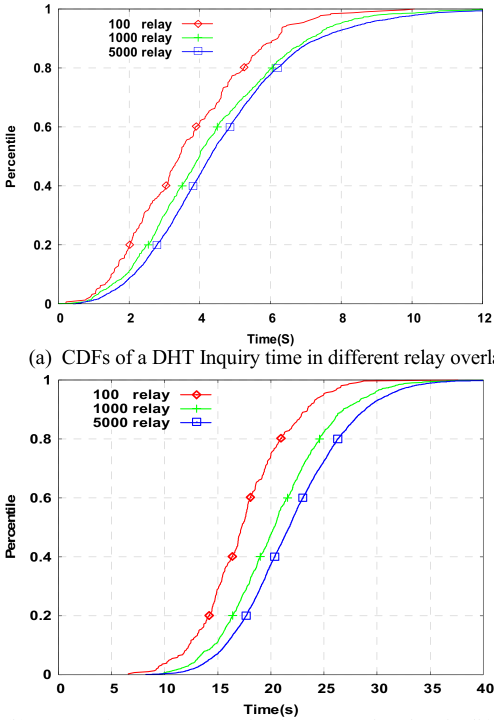
C. The Security Feature against DHT Churn Attacks

If churn attack of node joining is launched, the SA can control the pace of the relay node registration. According to existing research work, DHT overlay is very robust. Even if the fraction of leaving node is 20%, the connectivity of the overlay cannot be destroyed very seriously. Although the performance of the scheme can be degraded in a period of time after churn attack, the impact can be eliminated gradually with the RID empty elimination procedure described in B parts of Section IV.

VI. Performance Analysis.

In order to validate the effectiveness of this scheme, a simulation mode is constructed based on GTNets [21]. The scalability of the scheme and the impact of churn attack are analyzed with the simulation model. In the simulation model, a Kad-like DHT overlay is implemented with the modules in GTNets. The communication delay between different relay node modes is set as a random value with exponential distribution and the mean value is 500ms.

A. The Scalability of the Scheme



(a) CDFs of a DHT Inquiry time in different relay overlay scale

(b) CDFs of an anonymous circuit construction time in different relay overlay scale

Figure 3. The results of scalability validation experiment

By setting the number of anonymous relay nodes as 100, 1000 and 5000, different simulation experiments are conducted. The time of single DHT inquiry and anonymous circuit construction is recorded. A circuit is constructed with 3 relay nodes. The simulation results are shown in Fig 3.

The time-consuming for anonymous circuit construction will increase with the scale of the anonymous overlay. When the number of relay nodes is 100, the time-consuming for 80% of the anonymous circuit construction is no more than 21 S, and the time-consuming for 80% of the single DHT inquiry is no more than 5.4 S. When the number of relay nodes is 5000, the average time-consuming for anonymous circuit construction is about 22.0558 S, and the single DHT inquiry time is increased obviously too, as Fig 3 (a) shows.

However, the time-consuming growth shows an obvious trend of slow down. The average time of anonymous circuit construction in different scale is shown in table I. When the scale of relay overlay became 10 times and 50 times of the 100 nodes scale, the average time-consuming for anonymous circuit construction is increased by 17.3% and 25.6% separately. The simulation results demonstrate that this anonymity scheme has a good performance in scalability.

TABLE I. Average Circuit build Time in different scale

Scale of the Relay Overlay	Average Time of Circuit Construction
100 relay nodes	17.5635 S
1000 relay nodes	20.6014 S
5000 relay nodes	22.0558 S

The bandwidth-consuming of SA is another important metric of the scalability of this scheme. The comparison of bandwidth-consuming with other major schemes is shown in Table II. The bandwidth-consuming in the scheme presented in this paper demonstrate a linear growth.

TABLE II. Bandwidth-consuming Between Different Schemes

Scheme	Bandwidth-consuming
Tor	$O(nr)$
I2P	$O(n\log r)$
Salsa	$O(n\log r)$
AP3	$O(n\log r)$
Cashmere	$O(n\log r)$
Crowds	$O(n^2)$
MorphMix	$O(n)$
Tarzan	$O(n^2)$
Torsk	$O(n\log r)$
Scheme in this paper	$O(n)$

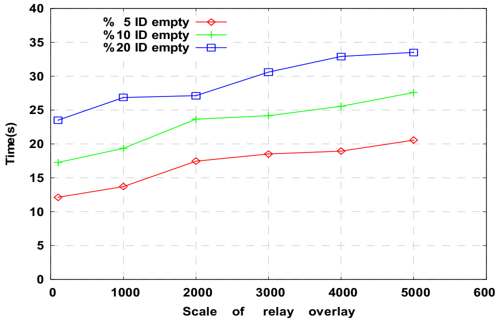


Figure 4. The time of RID empty recovery in different relay overlay scale

B. The RID Empty Recovery Ability

Experiments are conducted with different relay overlay scale, and the worst case that 20% relay nodes exit is considered. 95% of the RID empties being eliminated can be thought as complete. The time used for RID empty recovery is recorded. Experiment results are shown in Fig 4.

The increase of recovery time is not as large as the scale of relay overlay enlarges. So, the RID empty elimination mechanism can support the scalability of scheme well.

By setting the relay overlay scale from 1000 to 5000 and 20% of the relay nodes exiting from the overlay simultaneously, experiments of bandwidth-consuming of SA are conducted. The peak values of bandwidth-consuming in different scale are recorded. The results are shown in Fig 5.

The bandwidth-consuming show a linear growth with the scale-up of relay overlay. It can be inferred that if the bandwidth of SA is 100Mb, SA can support the scale of 520800 relay nodes, 20% of the relay nodes exiting from the overlay simultaneously.

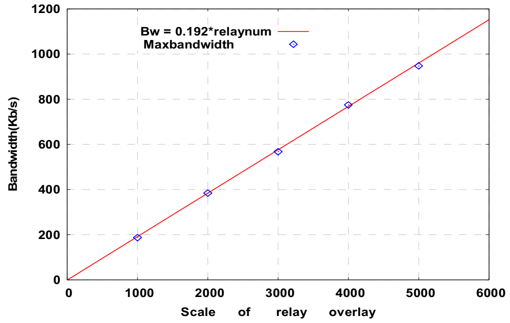


Figure 5. The peak value of bandwidth-consuming of SA

VII. Conclusion

A novel anonymity scheme is presented in this paper. In this scheme, a mechanism of anonymity relay node inquiry based on DHT storage is introduced to improve the scalability. Different from most existing scheme, this scheme adopt RID to index and inquire the anonymity relay node. The entire anonymity relay node routing information including RID are assembled in a verifiable data RRI which is stored as a normal data into DHTs overlay. Thus, the anonymity relay node routing can be equated with normal data inquiry based on DHT mechanism, which can facilitate the introduction of DHT security measures. In addition, a series of enhanced security measures are also included by introducing the mechanism of validation node. The security is discussed in detail and simulation experiments are conducted to validate the effectiveness of this scheme. The analysis and simulation results demonstrate that this scheme can have a good performance in scalability and security.

Acknowledgement

This work is supported by the National Natural Science Foundation of China grant 70890084/G021102, 61003273, 61003274, and Strategy Pilot Project of Chinese Academy of Sciences, sub-project XDA06010702.

References

[1] Chaum, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of ACM 24, 2 (1981), 84–88.

[2] DINGLEDINE, R., MATHEWSON, N., AND SYVERSON, P. Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium (August 2004).

[3] LOESING, K. Measuring the tor network: Evaluation of client requests to the directories. Tech. rep., Tor Project, June 2009. https://git.torproject.org/checkout/metrics/master/report/dirreq/directory-requests-2009-06-26.pdf.

[4] REITER,M.,AND RUBIN, A. Crowds:Anonymity for web transactions.ACM Transactions on Information and System Security ,1(June 1998).

[5] FREEDMAN, M. J., AND MORRIS, R. Tarzan: a peer-to-peer anonymizing network layer. In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security (New York, NY, USA, 2002), ACM Press, pp. 193–206.

[6] ROWSTRON, A., AND DRUSCHEL, P. Pastry: Scalable, distributed object location and routing for large-scale p2p systems. (2001).

[7] ZHUANG, L., ZHOU, F., ZHAO, B. Y.,AND ROWSTRON, A. Cashmere: resilient anonymous routing. In NSDI'05 (Berkeley, CA, USA, 2005), pp. 301–314.

[8] STOICA, I., MORRIS, R., KARGER, D., KAASHOEK, F., AND BALAKRISHNAN, H. Chord: A peer-to-peer lookup service for internet applications. In SIGCOMM (2001).

[9] NAMBIAR, A., AND WRIGHT, M. Salsa: A structured pproach to large-scale anonymity. In Proceedings of CCS 2006 (October 2006).

[10] RENNHARD, M., AND PLATTNER, B. Introducing MorphMix: peer-to-peer based anonymous Internet usage with collusion detection. In WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society (NY, USA, 2002), ACM Press, pp. 91–102.

[11] WANG, P., OSIPKOV, I., HOPPER, N., AND KIM, Y. Myrmic: Secure and robust dht routing. Tech. Rep. 2006/20, University of Minnesota DTC Research Report, 2006.

[12] Jon Mclachlan, Andrew Tran, Nicholas Hopper. Scalable Onion Routing With Torsk. In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security (Chicago, Illinous, USA, 2009), ACM Press, pp. 590–599.

[13] P. Maymounkov, D. Mazieres. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric. In Proceedings of the 1st International Workshop on Peer-to-Peer Systems, 2002, 53–65.

[14] CASTRO, M., DRUSCHEL, P., GANESH, A., ROWSTRON, A., AND WALLACH, D. Security for structured peer-to-peer overlay networks. In Proc. of the Fifth Symposium on Operating System Design and Implementation (OSDI) (2002).

[15] Andrew Tran, Nicholas Hopper, Yongdae Kim. Hashing it out in public. In Proceedings of WPES'09, Chicago, Illinous, USA, 2009.

[16] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman. SybilGuard: Defending Against Sybil Attacks via Social Networks. In Proceedings of SIGCOMM' 06, Pisa, Italy, 2006.

[17] Atul Singh, Tsuen-Wan "Johnny" Ngan, Peter Druschel., and Dan S. Wallach. Eclipse Attacks on Overlay Networks: Threats and Defenses. In Proceedings of the 25th IEEE INFOCOM, Barcelona, Spain, 2006.

[18] MITTAL, P., AND BORISOV, N. Information leaks in structured peer-to-peer anonymous communication systems. In CCS '08: Proceedings of the 15th ACM conference on Computer and Communications Security (NY, USA, 2008), ACM, pp. 267–278.

[19] D. Stutzbach and R. Rejaie. Understanding Churn in Peer-to-Peer Networks. (IMC 2006)

[20] DANEZIS, G., AND SYVERSON, P. Bridging and fingerprinting: Epistemic attacks on route selection. In Proceedings of the Eighth International Symposium on Privacy Enhancing Technologies (PETS 2008) (Leuven, Belgium, July 2008), Eds., Springer, pp. 133–150.

[21] http://www.ece.gatech.edu/research/labs/MANIACS/GTNet