International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.313-328
http://dx.doi.org/10.14257/ijsia.2015.9.1.30

Towards Attacks and Defenses of Anonymous Communication Systems

Tianbo Lu[1,2], Puxin Yao[1], Lingling Zhao[1], Yang Li[1], Feng Xie[3] and Yamei Xia[1]

[1]*School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
[2]*Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada*
[3]*China Information Technology Security Evaluation Center, 100085, Beijing, China*
lutb@bupt.edu.cn, yaopuxin@163.com, wodepengyouzhao@163.com

Abstract

Anonymous communication system has been hot topic in the field of information security, and attack techniques against anonymous systems are endless. This paper first classifies and summarizes the study of attacks against anonymous communication system in recent years, then analyzes the trend of the research on different attack technologies; secondly, it provides a comparative analysis of defense capability the mainstream anonymous communication system to the various attacks; Finally, combining the advantages and disadvantages of different systems, the authors propose an improved node selection and router forwarding algorithms for anonymous communication systems, and design an architecture of anonymous communications software based on the algorithm.

Keywords: *Anonymous communication, attacks, defenses*

1. Introduction

During the last few decades, computer network developed very rapidly. Currently it has been widely used in communications of individuals, groups and government departments. Network security and privacy of communication increasing people's interest and attention. Past focused on improving network security confidentiality, integrity, availability, authenticity and non-repudiation, but it does not hide the sending and receiving address.

Anonymous communication refers to communication relationship is hidden in traffic flows through a certain way to make eavesdropper unable to communicate directly informed or infer one relationship or communication technology on both sides. Since Chaum [1] proposed anonymous communication in 1981 against such problems, anonymous communication and attack more and more people's attention. Anonymous communication widely used, such as privacy protection, anonymous e-mail, instant messaging, electronic voting, online payments and military communications and many other areas.

The rest of the paper is organized as follows. In Section 2, we classify and summarize the study of attacks against anonymous communication system in recent years, then analyzes the trend of the research on different attack technologies; In Section 3, we provide a comparative analysis of defense capability the mainstream anonymous communication system to the various attacks; In Section 4, combining the advantages and disadvantages of different systems, we propose an improved node selection and router forwarding algorithms for anonymous communication

ISSN: 1738-9976 IJSIA

systems, and design an architecture of anonymous communications software based on the algorithm. And the last section is conclusion of this paper.

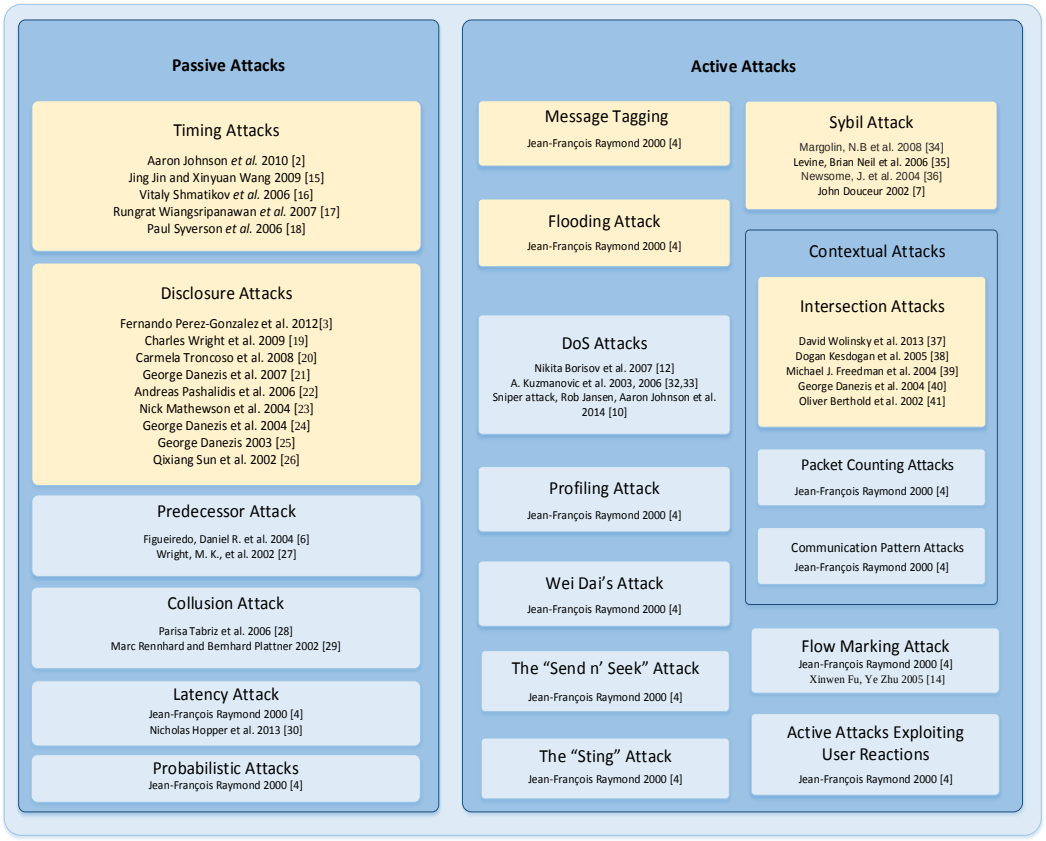


Figure 1. The Category of Attacks against Communication Systems

2. Attacks against Anonymous Communication System

There are many methods to classify the attacks against anonymous communication systems. Here, by different attack methods on dynamic information, we present the passive attacks and active attacks, as shown in Figure 1.

2.1. Passive Attacks

2.1.1. Timing Attacks: Timing attacks are a major challenge in low-latency anonymous communication. They have been observed in some of the earliest low-latency systems, including initial versions of onion routing. These attacks are also closely related to traffic analysis in mix networks.

In a passive timing attack, the adversary observes timing patterns in a network flow, and then correlates them with patterns in other traffic that it observes. If the adversary is able to observe both the user and the destination, he can thereby link the two. The ability of the adversary to perform this correlation has been experimentally demonstrated several times.

A solution to passive timing attacks is to get rid of identifying patterns in the traffic by padding and delaying it. The drawbacks to such an approach are added latency and bandwidth overhead [2].

2.1.2. Disclosure Attacks: Disclosure attack rely on Graph Theory in order to uncover the recipient set of a target user Alice. They seek to identify mutually disjoint sets of receivers amongst the recipient anonymity sets of the messages sent

by Alice, which are intersected with the anonymity sets of Alice's sent messages to find her communication partners. The main drawback of the Disclosure attack is that it is equivalent to solving a constraint satisfaction problem which is well-known to be NP-complete [3].

2.1.3. Collusion Attack: Some renegade participants can gather together more valuable than a single message. This use of information may compromise the security of the system, such as the attacker controls anonymous proxy anonymous channel, then these renegade agents can provide more useful information to the attacker.

2.1.4. Latency Attack: The latency attack is probably the most difficult to protect against. It is based on the fact that the latency on different routes will differ, and these latencies can be computed by the attacker. To compute the latency in a communication path going from the user through nodes A, B and C to a server S, an attacker simply needs to use the system to create a route through those nodes to communicate to S and compute the latency (e.g. using ping times) of communication and subtract the latency from the communication path between the attacker and node A. The closer the attacker is to the first node, the more precise his timings will be (communication won't be greatly re-routed by the underlying network). The attacker can then compute the latency between Alice and the first node (this is trivial if he controls the first node). Once the attacker has computed a set of timings, there are several things the attacker can do, depending on the timings he gathered. If some routes clearly differ by their latency timings, it is easy to determine which route Alice was using [4].

2.1.5 Predecessor Attack: The predecessor attack was first pointed out in [MKR1998], where the authors provide an analysis of a specific anonymous protocol known as Crowds. Paper [5] uses a probabilistic framework to evaluate the predecessor attack in various anonymity systems. In particular, they prove that under the assumption that paths are constructed uniformly at random, the attacker always succeeds in correctly revealing the initiator, independent of the protocol being used. They also provide explicit upper bounds for the effort required by an attacker in several concrete protocols.

The predecessor attack works as follows. The attacker nodes collectively maintain a single predecessor counter for each honest node in the system. Initially, all counters are set to zero. When an attacker node is selected to be on a new anonymous path, it first verifies if this path is intended for destination D. If so, the attacker increments the shared counter for its predecessor node in this path. These counters represent the number of times that each node in the system was observed as a predecessor to an attacker node on paths toward destination D. The attacker will then use the value of the predecessor counters to determine the set of nodes that are initiators [6].

2.2 Active Attacks

2.2.1 Message Tagging: An active internal adversary that has control of the first and last node in a message route, can tag (*i.e.* slightly modify) messages at the first node in such a way that the exit node can spot them. Since the entry node knows the sender and the exit node the recipient, the system is broken.

A solution to this problem is to make it difficult to tag messages. The techniques that can be used to do this depend on the implementation. The message tagging

based attacks motivate using extremely rigid message structure and authenticating timing information (in order to prevent message delays and message playbacks).

2.2.2 Flooding Attack: Opponents can achieve the separation of news of interest to the purpose of the system by flooding attacks. Subject to such attacks typical system is dependent on a group of anonymous, that each message can remain anonymous in a group message sent, as in the n-user anonymous system, an attacker fabricated n-a user's identity sends a message, then the message channel n, there are n-1 is the attacker to send yourself, then he could easily keep track of the rest of the message, so as to achieve the purpose of the attack.

2.2.3. Contextual Attacks: These are the most dangerous attacks and, unfortunately, they are very difficult to model in a rigorous manner. The problem is that real-world users don't behave like those in the idealized model. We remark that this class of attack is particularly effective for real-time interactive communications.

A. Communication pattern attacks

By simply looking at the communication patterns (when users send and receive), one can find out a lot of useful information. Communicating participants normally don't "talk" at the same time, that is, when one party is sending, the other is usually silent. The longer an attacker can observe this type of communication synchronization, the less likely it's just an uncorrelated random pattern.

This attack can be mounted by a passive adversary that can monitor entry and exit mix nodes. Law enforcement officials might be quite successful mounting this kind of attack as they often have a-priori information: they usually have a hunch that two parties are communicating and just want to confirm their suspicion.

B. Packet counting attacks

These types of attacks are similar to the other contextual attacks in that they exploit the fact that some communications are easy to distinguish from others. If a participant sends a non-standard (i.e. unusual) number of messages, a passive external attacker can spot these messages coming out of the mix-network. In fact, unless all users send the same number of messages, this type of attack allows the adversary to gain non-trivial information.

A partial solution is to have parties only send standard numbers of messages but this isn't a viable option in many settings.

C. Intersection attack

An attacker having information about what users are active at any given time can, through repeated observations, determine what users communicate with each other. This attack is based on the observation that users typically communicate with a relatively small number of parties. For example, the typical user usually queries the same web sites in different sessions (his queries aren't random). By performing an operation similar to an intersection on the sets of active users at different times it is probable that the attacker can gain interesting information. The intersection attack is a well-known open problem and seems extremely difficult to solve in an efficient manner [4].

2.2.4. Sybil Attack: Douceur first presented the concept of Sybil attacks, that a single node with multiple identities weaken the role of Redundancy by controlling most of the node in the system in a wireless network.

Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities to mitigate the threat of hostile peers. Many systems replicate

computational or storage tasks among several remote sites to protect against integrity violations. Others fragment tasks among several remote sites to protect against privacy violations. In either case, exploiting the redundancy in the system requires the ability to determine whether two ostensibly different remote entities are actually different.

If the local entity has no direct physical knowledge of remote entities, it perceives them only as informational abstractions that we call identities. The system must ensure that distinct identities refer to distinct entities; otherwise, when the local entity selects a subset of identities to redundantly perform a remote operation, it can be duped into selecting a single remote entity multiple times, thereby defeating the redundancy. We term the forging of multiple identities a Sybil attack on the system [7].

2.2.5. DoS Attacks: Traditional architectures, offering no protection against DoS attacks, are subject to complete compromise if the network is contains a majority of dishonest nodes. Traditional mixes aimed to protect a communication even if a single honest mix was on the path, and little previous work has questioned this security assumption [8]. Routes with few honest nodes will be subject to DoS, and only fully honest or fully compromised paths will survive. This intuition in an embryonic form was present in [9] in the context of reputation systems. Such as the Sniper Attack [10], an extremely low cost but highly destructive denial of service attack against Tor that an adversary may use to anonymously disable arbitrary Tor relays, or CellFlood Attack [11] against tor onion routers on the cheap.

Mechanisms to prevent our denial of service based attacks, either by detecting maliciously unreliable nodes, or ensuring an honest majority, will have to be part of any future mix systems design and deployment. Sadly, designs that simply ensure reliability, such as Cashmere and Hydra-Onions, are curing the symptoms rather than the disease: they only focus on reliability while making the anonymity of the system even worse under DoS attacks [12].

2.2.6. Other Active Attacks:

A. Wei Dai's attack on traffic shaping

Wei Dai describes a generic attack against systems that allocate bandwidth to the users as connections are established and implement traffic shaping between nodes. Here the attacker creates an anonymous route to himself, through a pair of nodes he suspects to belong to Alice's route. The attacker then increases the traffic through this route until the total traffic between the pair of nodes reaches the bandwidth limit set by the traffic shaping. At this point the nodes no longer send any padding packets to each other, and the real traffic throughput between them can be deduced by subtracting the traffic sent by the attacker from the bandwidth limit [13].

B. Clogging attack

In a simpler timing attack, an attacker observes the communication between a certain last node C and W1. He then creates a route through a chosen set of nodes and clogs the route with many requests. If he observes a decrease in throughput from C to W1, he can deduce that one of the nodes in the route he created belongs to a route containing C. The attacker can use a binary style search to find all the nodes belonging to a certain route. Once the route to W1 is known, the attacker knows the users first node. He can then use similar techniques to identify the individual user of the possible users of that node. This attack is plausibly deniable as Internet traffic is often bursty.

A variant of the clogging attack is to exploit some IP protocol or implementation flaw to temporarily delay packet delivery at an intermediate router (not necessarily a node) on a targeted route [4, 13].

C. Profiling Attack

Attacker track user preferences by observing the user or the user's unique online news (such as a pseudonym, Cookies), etc. to find the sender. Attacker by observing users online and offline time or other obvious recognizable behavior, which found that communication relationship.

D. Active attacks exploiting user reactions

This attack is, in a sense, the opposite of the "sting" attack of subsection 3.7. Instead of having the recipient try to find the sender's identity, it's the sender that attempts to uncover the recipient's identity. This attack is particularly dangerous against non-interactive processes. For example, privacy protecting e-mail systems can be attacked by sending an easily identifiable number of messages and trying to identify these messages at suspect destinations (*e.g.* POP boxes). Notice that the terms sender and recipient are used very loosely here; the sender refers to the party initiating the connection.

E. The "Sting" attack

The "sting" attack is also mentioned in [4]. If one of the party involved in a dialog is corrupt, he might be able to, in a sense, "encode" information in his messages. For example, government agencies might set up a fake "bomb making instruction web sites" and try to find out who accesses it. Many methods for identifying a user querying the web page come to mind: varying the reply latency, sending messages of a specific length, etc.

In some situations, it might be even easier to compromise user privacy. For example, if the sting web site gives fake information pertaining to financial fraud, the user might (non-anonymously) act upon this information at which point he can be arrested.

F. The "Send n' Seek" attack

If one of the party involved in a dialog is corrupt, he might be able to, in a sense, "encode" information in his messages. For example, government agencies might set up a fake "bomb making instruction web sites" and try to find out who accesses it. Many methods for identifying a user querying the web page come to mind: varying the reply latency, sending messages of a specific length, etc.

In some situations, it might be even easier to compromise user privacy. For example, if the sting web site gives fake information pertaining to financial fraud, the user might (non-anonymously) act upon this information at which point he can be arrested [4].

G. Flow marking attack

Alice is communicating with Bob through a mix network. To find if Alice is communicating with Bob, an adversary, interferer, can embed a series of marks into Alice's traffic by interfering with her link. Another adversary, sniffer, eavesdrops Bob's inbound traffic. If the sniffer discovers a similar pattern of marks in Bob's traffic, she can be sure that Alice is communicating with Bob [14].

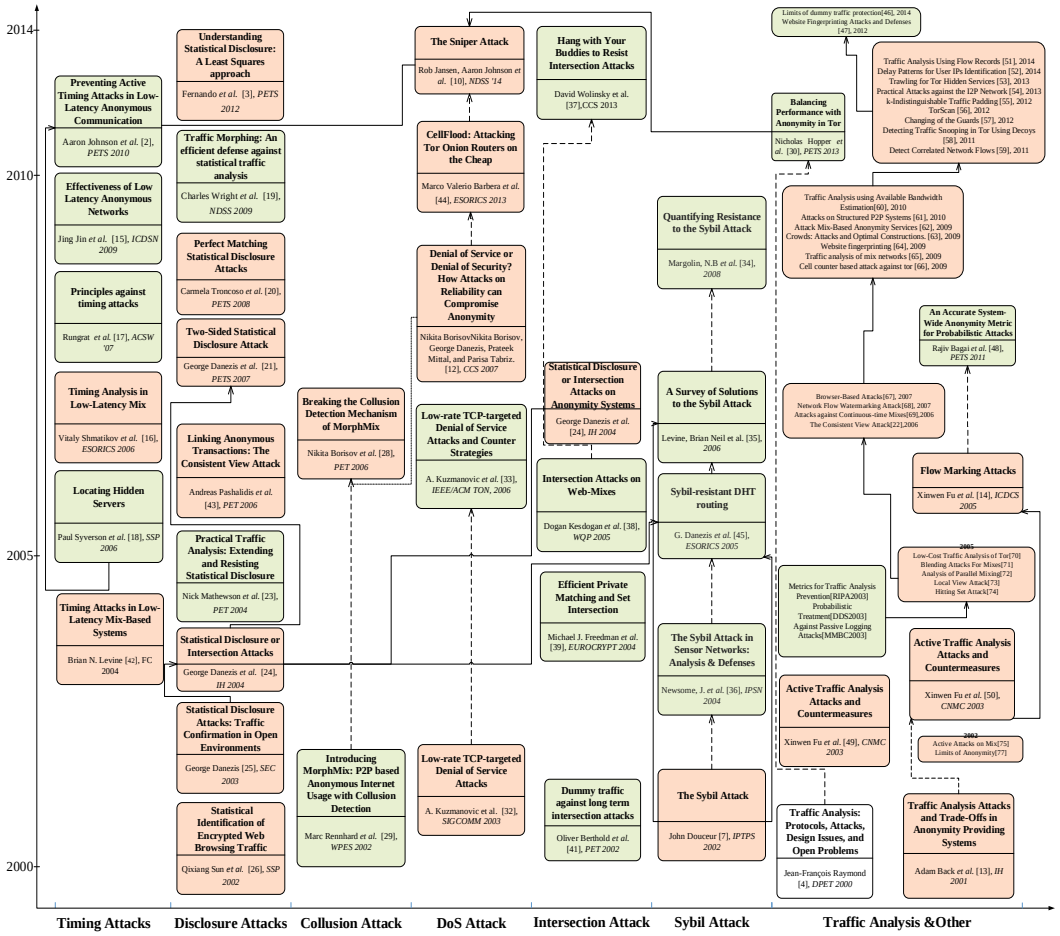


Figure 2. The Research Trends of the Attacks and Defenses on Anonymity

2.3. The Research Trends of the Attacks and Defenses

After analyzing the related work on anonymous communication system, we draw the research trends of the attacks and defenses on communication system, as shown in Figure 2, the research in red background is about attacks and in the green is on defenses.

After 2000, studies on attacks against anonymous communication have gradually increased. The study are mainly focus on timing attack, disclosure attack, DoS attack, and attacks based on traffic analysis. Most attacks are only for a specific anonymous system, especially for Tor.

3. Defense Analysis of Communication Systems

The main objective of anonymous communication is to achieve the sender anonymity, or recipient anonymity, or both. For different applications, some organizations or individuals have developed a number of anonymous communication protocols or systems that may be based on different technologies and the ability of anti-attacks are different.

In this section, based on the related work in anonymous communication, we compare the anti-attack abilities of different anonymous communication systems. As shown in Table 1, we analyze and list the defense capacity of diffent anonymous communication systems.

Mixmaster: Mixmaster is based on D. Chaum's mix-net protocol. It is a mix-net implementation for electronic mail. If the adversary suppresses all Mixmaster messages

from one particular sender and observes that anonymous messages of a certain kind are discontinued at the same time, that sender's anonymity is compromised with high probability.

Table 1. Comparison of Anonymous Technology in Resisting Attack

Types	Mix	Mixmaster	Anonymizer	Crowds	Freedom	Tarzan	Tor	NAS
Timing Attack	✔	✔	✘	Insider: ✘ Outsider: ✔	Partially ✔	✔	Between Onion routers: ✔	✔
Statistic Disclosure Attack	✘	✘ --	--	--	--	--	✘	✘
Message Tagging	✘	✘	✘	✘	✘	✘	✘	✘
Flooding Attack	--	✘	✘	✘	Partially ✔	✔	Between Onion routers: ✔	--
Intersection Attack	✔	✔	✘	✘	✘	✔	✘	✔
Collusion Attack	✔	✔	✘	✘	✘	✘	✔(up to n-1 colluding onion router)	✔
Latency Attack	--	--	--	--	--	--	✘	--
Sniper Attack	--	--	--	--	--	--	✘	--
Denial-of-service Attack	✘	✘	✘	✔			✔	✘
Predecessor Attack	✘	✘	✘	✘	✘	✘	✘	✘

Anonymizer: Anonymizer is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. This system fails if the proxy reveals a user's identity or if an adversary can observe the proxy's traffic. Furthermore, servers can easily block these centralized proxies and adversaries can prevent usage with denial-of-service attacks.

Crowds: Crowds [31] simply assumes an adversary who cannot observe the initiator: it uses no public-key encryption, so any node on a circuit can read users' traffic. Both Crowds and Onion routing do not use the entire set of participants to route messages, they are resilient against denial-of-service attacks.

Freedom: Freedom [78] has been designed to protect the privacy of users sending email, browsing the web, posting to news groups and participating in Internet chat. Counting and timing packets is possible today since traffic shaping and link padding do not offer strong security as implemented. Packages such as Back Orifice, WhoWhatWhere, NetBus, Systems Management Server, PCAnywhere, and other remote management tools totally compromise your privacy if the administrator so chooses. Freedom does not contain defenses against these. Freedom's link authentication is done poorly and there is no link layer serialization, which allows packets to be replayed.

Tarzan and MorphMix: In P2P designs like Tarzan [79] and MorphMix [80], all participants both generate traffic and relay traffic for others.These systems aim to conceal whether a given peer originated a request or just relayed it from another peer. While Tarzan and MorphMix use layered encryption. Tarzan and MorphMix aim to scale to completely decentralized peer-to-peer environments with thousands of short-lived servers, many of which may be controlled by an adversary.

Tor: The Tor network [81] is a widely used system for lowlatency anonymous Internet communication. The network has enjoyed quick growth since its initial deployment in 2003; as of August 2014, Tor is composed of nearly 6000 active relays and more than 3000 bridges supporting hundreds of thousands of users.

Tor is not peer-to-peer and does not claim to completely solve end-to-end timing or intersection attacks. Some approaches, such as having users run their own onion routers, may help. Like all practical low-latency systems, Tor does not protect against a global passive adversary.

We also propose a system named NAS, which will be explain in next section. It draws on the advantages MIX and Crowds by retaining strong anti-attack ability of the MIX and the high efficiency of Crowds, increasing the protocol correctness.

Actually, none of the system we mentioned can resist the message tagging attack, so that is direction to study.

4. Design of Improved Anonymous Communication System

Based on the analysis of related work and comparison of the anonymous technology in resisting attack. The architecture of the system is as shown in Figure 3. The sender client choses node by node selection mechanism, and constructs an anonymous channel by the method of layered encryption to achieve anonymous communication. The recipient would achieve communication with the sender by constructing another anonymous channel as a sender.

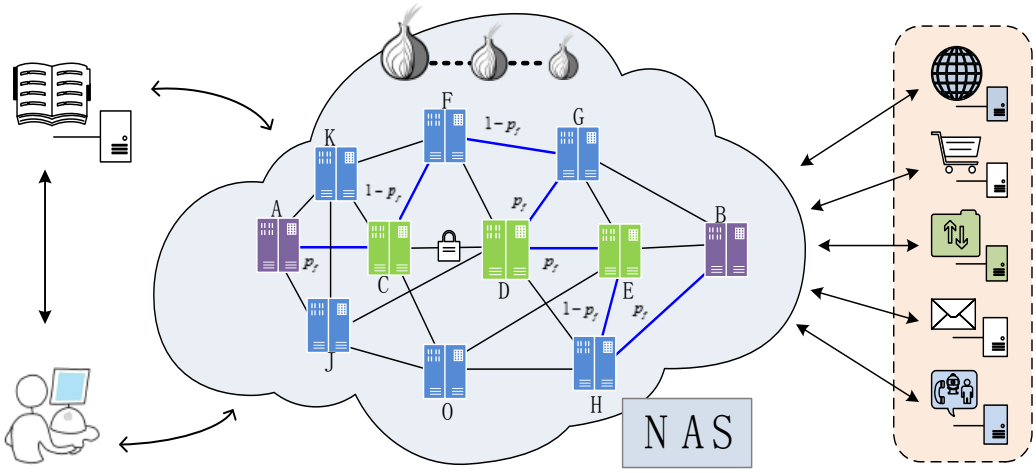


Figure 3. The Concept of the New Anonymous System

This architecture is based on the unstructured P2P networks. Here, we assume that the conspirators in the network are in the same region. To maximize the prevention of collusion attacks at the network layer, we use the node discovery mechanism named Gossip in the network layer.

Due to the low efficiency of the flooding method used in unstructured P2P network, although using the index node which can help other nodes obtain the node information would increase the efficiency, in a P2P network with nodes entering and exiting, even with a fixed alternate index node, it is still difficult to increase the efficiency.

We make some improvement to the system for the above reason, we add some un-fixing nodes, which generated by other nodes in the network through voting. Each node would vote for other nodes. And one node will become an index node when it get a number of votes. An on-line node need send some request to neighbor nodes so that new

nodes can join the network. The specific workflow includes initialization, members joining and exiting.

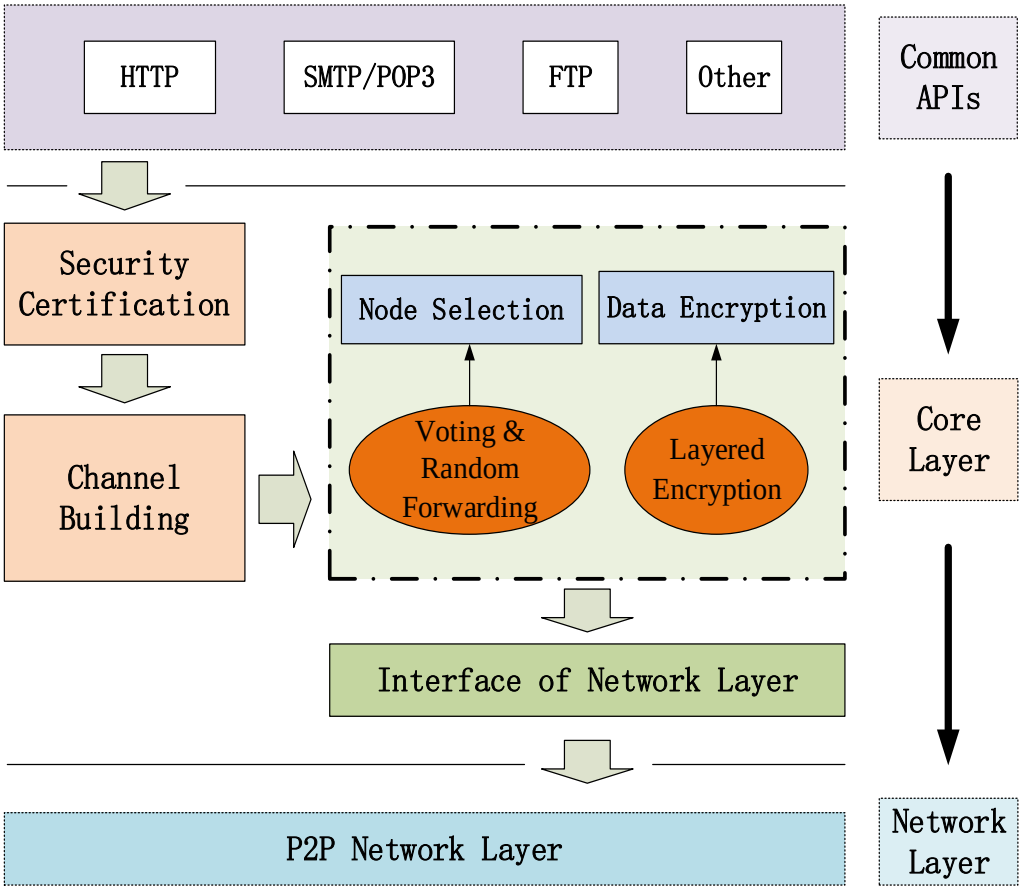


Figure 4. The Architecture of the NAS

NAS is a P2P overlay network on the Internet. Its basic function is to provide users with anonymity service by forwarding the data. It draws on the advantages MIX and Crowds by retaining strong anti-attack ability of the MIX and the high efficiency of Crowds, increasing the protocol correctness. By layered encryption and random forwarding, made a strong anonymity and high efficiency. Agreement to ensure the correctness of its superior Mix and Crowds a feature.

NAS system is designed as shown above, the anonymous sender A To send a message m to the receiver B, A First select the node C, D and E, and then use them to drill three public key to encrypt the message m and send to a C probability. C after receiving the message, use their private key to decrypt it knows the next node D. C be throwing coins to decide whether to send the message to D or sent to a randomly selected node F, the results of C and F of the message sent to the next hop is telling F D. Credits are to be cast directly to the decision to send the message to the next node is transmitted to a randomly chosen node after each node receives the message. Alice selected in advance by the node C, D and E will receive the message stratified decrypt the message randomly selected nodes F, G and H do not layered decrypt the received message, they just forward.

The architecture of the improved anonymous communication system consists of three modules, as shown in Figure 4.

A. P2P network layer.

P2P network is different from traditional networks. Due to its characteristics of peer to peer, how to notice the node status in the absence of server, is a problem to be solved.

B. Anonymous communication module.

As anonymous communication system, the system should meet the requirement that intermediate nodes do not know the information of source node, and cannot resolve the real content of the message, they are only responsible for forwarding message. For the nodes outside the channel of communication information is completely hidden. In specific design, it consists of the following modules:

a) Security authentication module. The main role of security authentication is to confirm whether the client or a neighbor node the user is entitled to use the node for anonymous communications. Also can verify the anonymous Services node level, after being certified as a malicious node authentication module or unsafe node, the node will be deleted anonymity network, and after the general section through an internal certification can be upgraded to an index node. This module can be achieved through controllable anonymous communication systems.

b) Nodes selection module. This system is the most important one module. Its mission is the central node or a neighbor node discovery, to select nodes based on node level, through this module hierarchical routing system, credit rating and other functions.

c) Data encryption module. This module is mainly used for key negotiation, encryption and decryption of data. The idea of a layered encryption, the information sent by certified or nodes or users received information encryption and decryption.

d) Module for establishment and removal of an anonymous channel. This module provides the information you need to select the module according to the node, in accordance with predetermined steps and target users to establish anonymous communication channel. When the communication between the user and all goals completed, the system must remove it established an anonymous channel. Removal process and the anonymous channel anonymous channel establishment process in the opposite direction. To improve efficiency, the module can also change the channel in a certain part of the process of communication as needed, rather than completely dismantled and re-establish the tunnel passage.

e) Network layer interface. The main function of the network layer is the interface with the P2P network layer to securely and efficiently transmit data.

C. Common Application Programming Interface (API).

The anonymous communication system is expected to support a variety of high-level applications, such as Web browsing, e-mail, file transfer, etc., corresponding to the HTTP, SMTP, POP3 and FTP protocols. Anonymous system should be able to achieve a request for information acquisition and processing applications for different users, as well as the corresponding request access to information and submit returns. Therefore, the new system will be designed to interface to a scalable application and agent between the completions of data between the applications and submit an anonymous system. Through this group of users can quickly and easily interfaces anonymous service integration in their systems.

5. Conclusion

In this paper, we summarize the study of attacks against anonymous communication system in recent years, and divide them into two categories of active attacks and passive attacks. Then we analyze the trend of the research on different

attack technologies; we provide a comparative analysis of defense capability the mainstream anonymous communication system to the various attacks, no single system can resist all the types of attack, so we have to make compromise between in efficiency and the capacity of anti-attack. Finally, combining the advantages and disadvantages of different systems, we propose an improved node selection method and a router forwarding algorithms for anonymous communication systems. Specifically we use the layered encryption and random forwarding method to ensure a strong anonymity and high efficiency. At last we design an architecture prototype of anonymous communications software based on the algorithm.

Acknowledgements

This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; the China Scholarship Council under Grant No.[2013]3050; Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (NO.CAAC-ITRB-201201); 2010 Information Security Program of China National Development and Reform Commission with the title "Testing Usability and Security of Network Service Software".

References

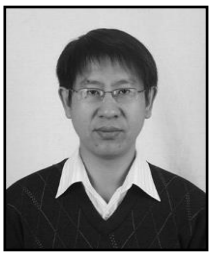
[1] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", In Communications of the ACM, vol. 24, no. 2, **(1981),** vol. 24 pp.84-90.
[2] A. Johnson, J. Feigenbaum, and P. Syverson, "Preventing Active Timing Attacks in Low-Latency Anonymous Communication", At the 10th Privacy Enhancing Technologies Symposium (PETS 2010), Berlin, Germany, **(2010)** July 22, pp.166-183.
[3] F. Perez-Gonzalez and C. Troncoso, "Understanding Statistical Disclosure: A Least Squares approach", In the Proceedings of the 12th Privacy Enhancing Technologies Symposium (PETS 2012), **(2012)** pp. 38-57.
[4] J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems", In the Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, **(2000)** pp. 10-29.
[5] M. Wright, M. Adler, B. N. Levine, and C. Shields, "An analysis of the degradation of anonymous protocols", In Proc. ISOC Network and Distributed System Security Symposium (NDSS 2002), **(2002).**
[6] D. R. Figueiredo, P. Nain, and D. Towsley, "On the analysis of the predecessor attack on anonymity systems", Computer Science Technical Report, **(2004).**
[7] J. Douceur, "The Sybil Attack", In the Proceedings of the 1st International Peer To Peer Systems Workshop (IPTPS 2002) **(2002).**
[8] O. Berthold, A. Pfitzmann, and R. Standtke, "The disadvantages of free MIX routes and how to overcome them", In the Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, **(2000)**, pp. 30-45.
[9] R. Dingledine and P. F. Syverson, "Reliable MIX cascade networks through reputation", In M. Blaze, editor, Financial Cryptography, vol. 2357 of Lecture Notes in Computer Science, Southampton, Bermuda **(2003)** pp. 253–268,
[10] R. Jansen, F. Tschorsch, A. Johnson, and B. Scheuermann, "The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network", In the Proceedings of the Network and Distributed Security Symposium - NDSS '14 **(2014).**
[11] M. V. Barbera, V. P. Kemerlis, V. Pappas, and A. Keromytis, "CellFlood: Attacking Tor Onion Routers on the Cheap", In the Proceedings of ESORICS 2013 **(2013),** pp. 664-681.
[12] N. Borisov, G. Danezis, P. Mittal, and P. Tabriz, "Denial of Service or Denial of Security?", How Attacks on Reliability can Compromise Anonymity, In the Proceedings of CCS 2007, **(2007).**
[13] A. Back, U. Möller, and A. Stiglic, "Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems", In the Proceedings of Information Hiding Workshop (IH 2001) **(2001),** pp. 245-257.
[14] X. Fu, Y. Zhu, B. Graham, R. Bettati, and W. Zhao, "On Flow Marking Attacks in Wireless Anonymous Communication Network", In the Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS) **(2005),** pp. 493-503.
[15] J. Jin and X. Wang, "On the Effectiveness of Low Latency Anonymous Networks in the Presence of Timing Attacks", In the Proceedings of the 41st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Lisbon, **(2009)** pp. 429-438.
[16] V. Shmatikov and M.-H. Wang, "Timing Analysis in Low-Latency Mix Networks: Attacks and Defenses", In the Proceedings of ESORICS **(2006),** pp.18-23.

[17] R. Wiangsripanawan, W. Susilo, and R. Safavi-Naini, "Design principles for low latency anonymous network systems secure against timing attacks", In the Proceedings of the fifth Australasian symposium on ACSW frontiers (ACSW '07), Ballarat, Australia **(2007),** pp.183-191.
[18] L. Ø verlier and P. Syverson, " Locating Hidden Servers", In the Proceedings of the 2006 IEEE Symposium on Security and Privacy, **(2006)** pp. 100-104.
[19] C. Wright, S. Coull, and F. Monrose, "Traffic Morphing: An efficient defense against statistical traffic analysis", In the Proceedings of the Network and Distributed Security Symposium - NDSS '09, **(2009).**
[20] C. Troncoso, B. Gierlichs, B. Preneel, and I. Verbauwhede, "Perfect Matching Statistical Disclosure Attacks", In the Proceedings of the Eighth International Symposium on Privacy Enhancing Technologies (PETS 2008), Leuven, Belgium, **(2008)** pp. 2-23.
[21] G. Danezis, C. Diaz, and C. Troncoso, "Two-Sided Statistical Disclosure Attack", In the Proceedings of the Seventh Workshop on Privacy Enhancing Technologies (PET 2007), Ottawa, Canada, **(2007)** pp. 30-34.
[22] A. Pashalidis and B. Meyer, "Linking Anonymous Transactions: The Consistent View Attack", In the Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006), Cambridge, UK, **(2006)** pp. 384-392.
[23] N. Mathewson and R. Dingledine, "Practical Traffic Analysis: Extending and Resisting Statistical Disclosure", In the Proceedings of Privacy Enhancing Technologies workshop (PET 2004), **(2004),** pp.17-34.
[24] G. Danezis and A. Serjantov, "Statistical Disclosure or Intersection Attacks on Anonymity Systems", In the Proceedings of 6th Information Hiding Workshop (IH 2004), Toronto, **(2004)** pp. 293-308.
[25] G. Danezis, "Statistical Disclosure Attacks: Traffic Confirmation in Open Environments", In the Proceedings of Security and Privacy in the Age of Uncertainty, (SEC2003), Athens, **(2003)** pp. 421-426.
[26] Q. Sun, D. R. Simon, Y.-M. Wang, W. Russell, V. N. Padmanabhan, and L. Qiu, "Statistical Identification of Encrypted Web Browsing Traffic", In the Proceedings of the 2002 IEEE Symposium on Security and Privacy, Berkeley, California, **(2002)** pp. 19-30.
[27] M. K. Wright, M. Adler, B. N. Levine, and C. Shields, "An analysis of the degradation of anonymous protocols", In Proceedings of the Network and Distributed Security Symposium (NDSS), **(2002).**
[28] P. Tabriz and N. Borisov, "Breaking the Collusion Detection Mechanism of MorphMix", In the Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006), Cambridge, UK, **(2006),** pp. 368-384.
[29] M. Rennhard and B. Plattner, "Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection", In the Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2002), Washington, DC, USA, **(2002)** pp. 91-102.
[30] J. Geddes, R. Jansen, and N. Hopper, "How Low Can You Go: Balancing Performance with Anonymity in Tor", In the Proceedings of the 13th Privacy Enhancing Technologies Symposium (PETS 2013), **(2013).**
[31] M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions", ACM Transactions on Information and System Security, vol. 1, no. 1, **(1998),** pp.66-92.
[32] A. Kuzmanovic and E. W. Knightly, "Low-rateTCP-targeted denial of service attacks," in Proceedings of ACM SIGCOMM, Oakland, California, **(2003),** pp. 75-86.
[33] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted Denial of Service Attacks and Counter Strategies," IEEE/ACM TON, vol. 14 no. 4, **(2006),** pp. 683-696.
[34] Margolin, N. Boris, and B. N. Levine, "Quantifying resistance to the sybil attack", Financial Cryptography and Data Security. Springer Berlin Heidelberg, **(2008)**, pp. 1-15.
[35] B. Neil Levine, C. Shields, and N. B. Margolin, "A Survey of Solutions to the Sybil Attack", University of Massachusetts Amherst, Amherst, MA, **(2006).**
[36] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", In Proceedings of the 3rd international symposium on Information processing in sensor networks **(2004)** April, pp. 259-268.
[37] D. Wolinsky, E. Syta, and B. Ford, "Hang with Your Buddies to Resist Intersection Attacks", In the Proceedings of the 20th ACM conference on Computer and Communications Security (CCS 2013), **(2013),** pp. 1153-1166.
[38] D. Kesdogan, L. Pimenidis, and T. Kölsch, "Intersection Attacks on Web-Mixes: Bringing the Theory into Praxis", In the Proceedings of First Workshop on Quality of Protection, **(2005)** pp. 159-171.
[39] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient Private Matching and Set Intersection", In the Proceedings of EUROCRYPT 2004, Interlaken, Switzerland **(2004).**
[40] G. Danezis and A. Serjantov, "Statistical Disclosure or Intersection Attacks on Anonymity Systems", In the Proceedings of 6th Information Hiding Workshop (IH 2004), Toronto **(2004),** pp. 293-308.
[41] O. Berthold and H. Langos, "Dummy traffic against long term intersection attacks", In the Proceedings of Privacy Enhancing Technologies workshop (PET 2002), **(2002),** pp. 110-128.
[42] B. N. Levine, M. K. Reiter, C. Wang, and M. K. Wright, "Timing Attacks in Low-Latency Mix-Based Systems", In the Proceedings of Financial Cryptography (FC '04), **(2004),** pp. 251-265.

[43] A. Pashalidis and B. Meyer, "Linking Anonymous Transactions: The Consistent View Attack", In the Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006), Cambridge, UK, **(2006)** pp. 384-392.
[44] M. V. Barbera, V. P. Kemerlis, V. Pappas, and A. Keromytis, "CellFlood: Attacking Tor Onion Routers on the Cheap", In the Proceedings of ESORICS **(2013),** pp. 664-681.
[45] G. Danezis, C. Lesniewski-Laas, M. F. Kaashoek, and R. Anderson, "Sybil-resistant DHT routing", In Proc. ESORICS, **(2005)** pp. 305-318.
[46] C. T. Oya and F. Pérez-González, "Do dummies pay off? Limits of dummy traffic protection in anonymous communications", In the Proceedings of the 14th Privacy Enhancing Technologies Symposium (PETS 2014), **(2014),** pp. 204-223.
[47] X. Cai, X. Zhang, B. Joshi, and R. Johnson, "Touching from a Distance: Website Fingerprinting Attacks and Defenses", In the Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012), **(2012),** pp. 605-616.
[48] R. Bagai, H. Lu, R. Li, and B. Tang, "An Accurate System-Wide Anonymity Metric for Probabilistic Attacks", In the Proceedings of the 11th Privacy Enhancing Technologies Symposium (PETS 2011), Waterloo, Canada, **(2011)** pp. 117-133.
[49] M. Wright, M. Adler, B. N. Levine, and C. Shields, "An Analysis of the Degradation of Anonymous Protocols", In the Proceedings of the Network and Distributed Security Symposium, NDSS '02, **(2002).**
[50] X. Fu, B. Graham, R. Bettati, and W. Zhao, "Active Traffic Analysis Attacks and Countermeasures", In the Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, **(2003),** pp. 31-39.
[51] S. Chakravarty, M. V. Barbera, G. Portokalidis, M. Polychronakis, and A. D. Keromytis, "On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records", In the Proceedings of the 15th Passive and Active Measurements Conference (PAM '14), **(2014),** pp. 247-257.
[52] V. C. Perta, M. V. Barbera, and A. Mei, "Exploiting Delay Patterns for User IPs Identification in Cellular Networks", In the Proceedings of the 14th Privacy Enhancing Technologies Symposium (PETS 2014), **(2014)** pp. 224-243.
[53] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, "Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization", In the Proceedings of the 2013 IEEE Symposium on Security and Privacy, **(2013),** pp. 80-94.
[54] C. Egger, J. Schlumberger, C. Kruegel, and G. Vigna, "Practical Attacks against the I2P Network", In the Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2013), **(2013),** pp. 432-451.
[55] W. M. Liu, L. Wang, K. Ren, P. Cheng, and M. Debbabi, "K-Indistinguishable Traffic Padding in Web Applications", In the Proceedings of the 12th Privacy Enhancing Technologies Symposium (PETS 2012), **(2012).**
[56] A. Biryukov, I. Pustogarov, and R. P. Weinmann, "TorScan: Tracing Long-lived Connections and Differential Scanning Attacks", In the Proceedings of the European Symposium Research Computer Security - ESORICS'12, **(2012).**
[57] T. Elahi, K. Bauer, M. AlSabah, R. Dingledine, and I. Goldberg, "Changing of the Guards: A Framework for Understanding and Improving Entry Guard Selection in Tor", In the Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2012), Raleigh, NC, USA, **(2012).**
[58] S. Chakravarty, G. Portokalidis, M. Polychronakis, and A. D. Keromytis, "Detecting Traffic Snooping in Tor Using Decoys", In the Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection, Menlo Park, CA, **(2011),** pp. 222-241.
[59] A. Houmansadr and N. Borisov, "SWIRL: A Scalable Watermark to Detect Correlated Network Flows", In the Proceedings of the Network and Distributed Security Symposium - NDSS'11, **(2011).**
[60] S. Chakravarty, A. Stavrou, and A. D. Keromytis, "Traffic Analysis Against Low-Latency Anonymity Networks Using Available Bandwidth Estimation", In the Proceedings of the European Symposium Research Computer Security - ESORICS'10, **(2010)** pp. 249-264.
[61] Q. Wang, P. Mittal, and N. Borisov, "In Search of an Anonymous and Secure Lookup: Attacks on Structured Peer-to-peer Anonymous Communication Systems", In the Proceedings of the 2010 ACM Conference on Computer and Communications Security (CCS 2010), Chicago, Illinois, USA, **(2010)** pp. 308-318.
[62] Using Linkability Information to Attack Mix-Based Anonymity Services. Stefan Schiffner and Sebastian Clauß. In the Proceedings of Privacy Enhancing Technologies, 9th International Symposium (PETS 2009), **(2009),** pp. 94-107.
[63] G. Danezis, C. Díaz, E. Käsper, and C. Troncoso, "The Wisdom of Crowds: Attacks and Optimal Constructions", In the Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS 2009), Saint-Malo, France, **(2009)** pp. 406-423.
[64] D. Herrmann, R. Wendolsky, and H. Federrath, "Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naïve-bayes classifier", In the Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09), Chicago, Illinois, USA, **(2009)** pp. 31-42.

[65] C. Troncoso and G. Danezis, "The bayesian traffic analysis of mix networks", In the Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, **(2009),** pp. 369-379.
[66] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A new cell counter based attack against tor", In the Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, **(2009)**, pp. 578-589.
[67] T. Abbott, K. J. Lai, M. R. Lieberman, and E. C. Price, "Browser-Based Attacks on Tor", In the Proceedings of the Seventh Workshop on Privacy Enhancing Technologies (PET 2007), Ottawa, Canada, **(2007).**
[68] X. Wang, S. Chen, and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems", In the Proceedings of the 2007 IEEE Symposium on Security and Privacy, **(2007)** pp. 116-130.
[69] G. Tóth and Z. Hornák, "The Chances of Successful Attacks against Continuous-time Mixes", In the Proceedings of the 11th Nordic Workshop on Secure IT-systems, Linköping, Sweden, **(2006).**
[70] S. J. Murdoch and G. Danezis, "Low-Cost Traffic Analysis of Tor", In the Proceedings of the 2005 IEEE Symposium on Security and Privacy, **(2005)** pp. 183-195.
[71] L. O'Connor, "On Blending Attacks For Mixes with Memory", In the Proceedings of Information Hiding Workshop (IH 2005), **(2005)** pp. 39-52.
[72] N. Borisov, "An Analysis of Parallel Mixing with Attacker-Controlled Inputs", In the Proceedings of Privacy Enhancing Technologies workshop (PET 2005), **(2005)**, pp. 12-25.
[73] M. Gogolewski, M. Klonowski, and M. Kutylowski, "Local View Attack on Anonymous Communication", In the Proceedings of ESORICS **(2005),** pp. 475-488.
[74] D. Kesdogan and L. Pimenidis, "The Hitting Set Attack on Anonymity Protocols. In the Proceedings of 6th Information Hiding Workshop (IH 2004), Toronto, **(2004)** pp. 326-339.
[75] A. Serjantov, R. Dingledine, and P. Syverson, "From a Trickle to a Flood: Active Attacks on Several Mix Types", In the Proceedings of Information Hiding Workshop (IH 2002), **(2002)** pp. 36-52.
[76] W. Dai, "Two attacks against freedom", http://www.eskimo.com/˜weidai/freedomattacks.txt, **(2000).**
[77] D. Kesdogan, D. Agrawal, and S. Penz, "Limits of Anonymity in Open Environments. In the Proceedings of Information Hiding Workshop (IH 2002), **(2002)**
[78] [78] Philippe Boucher, Adam Shostack, and Ian Goldberg. Freedom Systems 2.0 Architecture, Zero Knowledge Systems, Inc. White Paper , **(2000)**
[79] [79] M. J. Freedman and R. Morris. Tarzan: A peer-to-peer anonymizing network layer. In 9th ACM Conference on Computer and Communications Security (CCS 2002),Washington, DC, **(2002)** pp.121-129
[80] [80] M. Rennhard and B. Plattner. Practical anonymity for the masses with morphmix. In A. Juels, editor, Financial Cryptography. Springer-Verlag, LNCS, **(2004)**
[81] [81] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The Second-Generation Onion Router", In the Proceedings of the 13th USENIX Security Symposium, **(2004).**

Authors



Tian-Bo Lu, he was born in Guizhou Province, China, 1977. He is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.

Pu-Xin Yao, he is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include network security and P2P anonymous communication.

Ling-Ling Zhao, she is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include Cyber-Physical System and P2P network.

Yang Li, he was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.

Feng Xie, he was born in 1977. He obtained his PhD from Chinese Academy of Science. His technical interests include information and network security, risk assessment.

Ya-Mei Xia, she is a lecturer in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include information and network security.

