Towards an Analysis of Passive Attacks on Anonymous Communication Systems

Tianbo Lu1,2, Pan Gao1, Lingling Zhao1, Yang Li1 and WanJiang Han1

1School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China
2Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada
lutb@bupt.edu.cn, dianergaopan@163.com, wodepengyouzhao@163.com

Abstract

With the rapid development of communication technology and the Internet, more and more people pay attention to personal privacy. Therefore, the research on anonymous communication system is gradually increasing, at the same time, the study of anonymous communication systems attack techniques are constantly deepened. In a certain sense, the research on anonymous communication system, mainly aims at the attack the anonymous communication may face and the study of how to defense attack and improve the existence of the system. This requires us to classify the attack technology, so as to improve the safety of anonymous communication system. This paper mainly studies the passive attack technology in anonymous communication system. First of all, the paper has carried on the simple classifications of the attack technique on the anonymous system, which mainly divided into active and passive attacks. Secondly, we mainly introduce the passive attack mode. Passive attackers only monitor traffic and analyze related information of the sender and the receiver in the communication. We mainly introduce statistical disclosure attack, timing attack and Predecessor attack in detail. Finally, we study the passive attack other simply.

Keywords: anonymous communication; passive attack; active attack

1. Introduction

The advent of the Internet era makes the life of people cannot do without the network. Therefore, the security of network communication has brought new challenges when a lot of personal information through out on the Internet and personal privacy is easy to leak. Although there are many mature encryption technology to ensure the safety and the reliability of network communication, but personal privacy is difficult to hide because information, message source address, destination address message transported in the physical link layer is part of the message format. When cyber attackers know the message format, they parse out the useful information in the message package, which pose a great threat to personal privacy and information security. In the field of network security, more and more people start to pay attention to the research of Network Anonymous Communication technology. At present the general defense technology are only design for a specific attack methods. So it is necessary to research the attack in anonymous communication system. On the site of Free Haven which is famous project in the field of anonymous communication, the number of papers related anonymous communication system, followed by an anonymous attack, as shown in Figure 1-1.

According to the attacker hypothesis, we will divide attack into different categories at a different angle. We classify the attack in anonymous communication system from different aspects, as shown in Figure1-2.
Figure 1-1. The Research Trend of Anonymous Communication System

Figure 1-2. Anonymous Communication Attack Classification
According to the mode of attack, attack can be divided into passive and active attacks. Passive attackers only monitor traffic and analyze related information of the sender and the receiver in the communication, while active attackers can modify the means, increase, delete and delay the data packets. For example, traffic analysis is passive attacks, and denial of service attacks is active attack. This paper mainly studies the passive attack technology in anonymous communication system. Figure 1-3 shows the classification of the passive attacks.

Figure 1-3. The Classification of Active Attacks

2. Statistical Disclosure Attack

Statistical disclosure attack is not a way to attack the anonymous system directly, but a technology according to the statistical analysis of users' behavior. Important research results of statistical disclosure attack in recent years are shown in Figure 2-1.

Statistical disclosure attack is proposed by Kesdogan, Penz who come from Aachen University of Technology and Agrawal coming from IBM [1]. The attack obtain a large amount of data by monitoring network, and then study and exclude to judge communication relationship between the sender and the recipient.


Nick Mathewson and Roger Dingledine coming from Free Haven project extend the long-term end-end Disclosure Attack, and analyze the scene of more system in 2004 [5]. But there are still a lot of problems, such as that the assumption model has a gap with the reality, only concerning about the impact of the behavior of the message sender A. In defense, they propose that the sender uses a cover flow to increase the attacker's statistical analysis.
Nayantara Mallesh and Matthew Wright coming from The University of Texas at Arlington proposed a defense measure in 2007 [6]. This method called Receiver-bound Cover Traffic (RBC) proposed in this paper uses the mix to generate a cover flow to mimic the transmission mode of the user in the system. Such receivers disrupt an attacker by making up of an existing user. Cover flow is generally sent by the user, but the user cannot be always online so cannot send a continuous cover flow. This defense method solves this problem. For the RBC defense method, the direction still needs to study is how to apply it to the actual system.

Troncoso coming from The University of Leuven in Belgium propose Perfect Matching Disclosure Attack (PMDA) in 2008 [7]. The attacker tries to improve the statistical exposure attack by using the views of a sender to send a specific message. This method is well explained by a simple example of the Mix Threshold setup.

Charles V. Wright coming from MIT Lincoln Laboratory, Scott E. Coull from The Johns Hopkins University and Fabian Monrose from University of North Carolina come up with a method of traffic morphing to Defense statistics exposure attack in 2009 [8]. The method chooses a way to change the characteristics of the packet, which can match the user's specificity of the traffic flow. Compared with the traditional traffic filling strategy, Traffic Morphing can provide better privacy. But the selection of the best method as well as the classification of the method still need to be further studied.

Rajiv Bagai from Wichita State University propose an improvement of SDA firstly in 2010 [9]. In this method, the weighted average value of the correlation receiver is adopted, and the method is more accurate than the arithmetic mean value SDA. Then the attack model is demonstrated, and the sender of the model is integrated with the real message, but the improved attack will not be blocked.

Nayantara Mallesh and Matthew Wright from the University of Texas at Arlington propose a new SDA called Reverse Statistical Disclosure Attack [10]. Attackers first apply SDA to all N users. Attackers learn two kinds of information at this stage. First, the attacker gets who the sender A sends the message to by applying the SDA algorithm to the sender. Secondly, the SDA algorithm is used to determine who sends the message to A. Then the attacker will combine these two information to get the communication.
relationship between A and its communication partners.

Nayantara Mallesh and Matthew Wright carry on a further analysis of statistical exposure attack in 2011 [11]. Compared with the study in 2007, it discusses how to apply the RBC method to the anonymous network in the real world, mainly for high-delay Mix system, a preliminary discussion of encryption and non-encryption hide, how to allow the receiver to cover the flow can withstand.

Navid Emamdoost from Sharif University of Technology also proposed the extension of the SDA and the corresponding defense method in 2012 [12]. Improved attack models need to observe less information. The study extended the attack method to the non-threshold Mix protocol, which is called SG-Mix, and the method of increasing the number of observations required by the method of sending false information.

Fernando Pérez-González from University of Vigo and Troncoso from K.U.Leuven propose a method of Least Squares Disclosure Attack based on Maximum Likelihood in 2012 [13]. In the attack, the evaluation of the user's profile information to solve the least square problem. The attack can be resolved and the formula of the LSDA is derived, which can make the attacker more accurate to find out the user's profile information. The researchers further analyzed the method in [14].

Troncoso and Pérez-González F come up with a method to analyze Anonymous communication system with false communication flow based on Mix [15]. After the LSDA method, the authors propose a probability evaluation function for a user to send a message to a receiver. Function can be used to characterize the error of an attacker to collect user profile information or a single probability and system parameters. This method can be used in the design of the false communication flow strategy which can satisfy the standard of the privacy.

The advantage of the exposure attack is that attackers can know the relationship between the two sides of communication by analyzing date without knowing the realization of anonymous system. The limitation is that attackers need to consider all possible assumptions to determine the various factors and very complex computation to improve statistical accuracy.

3. Timing Attacks

Timing Attack is a kind of attack method based on data packet interval. If the attacker can monitor communication connections between a start node and the end node, and get a temporal link by analyzing, they can judge if there are users in the communication connection. The important research results in recent years about the timing of the attack is shown in Figure 3-1.

The concept of timing attack was firstly proposed by PC Kocher coming from Stanford University [16], which mainly analyze Diffie-Hellman, RSA and DSS password system. Research on anonymous communication timing attack is mainly during the period of 2000-2010 years.

Vitaly Shmatikov and Ming-Hsiu Wang from University of Texas-Austin analyze timing attacks, proposing a method of Adaptive padding to defense the attack in 2006 [17], that is adding data packets with different probabilities in route forwarding.

Andreas Pashalidis and Bernd Meyer from Siemens AG, Corporate Technology come up with an attack method based on continuous observation [18], the first stage uses the time attack to find out the user's pseudonym, the second stage is the link of pseudonyms and session.

Wiangsripanawan from University of Wollongong propose two systems design principles for resistance against time attacks in 2007 [19]. (1) Preventing each node from gathering information about the entire network. (2) In the network communication flow, a mask is inserted to make the network unable to find the flow characteristics.

Tim Abbott from MIT propose a timing attack method for using TOR browse the web
anonymously in 2007 [20]. The program can identify the part of users who use a malicious exit node and keep the browser window open for at least 1 hours.

Mehul Motani, Wei Wang and Vikram Srinivasan from National University of Singapore propose Dependent Link Padding for timing attack in 2008 [21]. The proposed method provides strict delay constraints and does not drop packets, dynamically change the fill rate according to the input flow and try to provide the maximum anonymity with the minimum transmission rate. But its disadvantage is that when the user flow increase, the filling rate of the filling algorithm will increase rapidly, which seriously affects the performance of the algorithm.

Jing Jin and Xinyuan Wang from George Mason University introduce a new method to quantitatively determine the real efficiency of low delay anonymous network in the face of time attack in 2009 [22]. The metric method based on wavelet analysis is used to measure the distortion of variability of the information packet interval from the anonymous system.

Joan Feigenbaum from Yale University, Aaron Johnson from the University of Texas at Arlington and Paul Syverson from Naval Research Laboratory propose the method Black-box Padding to defend timing attack with active attack in 2010 [23]. Because they pointed out that the protocol of low latency anonymous communication, especially the onion routing protocol is not available for the time attack. The general filling (Padding) method can defend the passive attacker, but the attacker can be active insertion delay and discard the message to destroy the filling.

Swagatika Prusty and Brian N Levine from University of Massachusetts proved that the OneSwarm anonymous system was vulnerable to a specific time attack in 2011 [24].

Michael Backes from Saarland University presents a framework for resisting time sensitive attacks in 2013 [25].

![Figure 3-1. The General Situation of Research on Time Attack](image-url)

In recent years, the research for the attack is less, and mainly focuses on the specific
methods and defense system framework. The basic model of anonymous communication system has been decent. With the design of anonymous communication system new emerging, the main focus of future research has been gradually from the theoretical research to attack strategy and defense method of the specific system.

4. Predecessor Attack

The predecessor attack is a kind of passive attacks on anonymous communication system, jointly launched by the conspiracy of the members in the system. There are two points to achieve the predecessor attack: First, there are repeated connection between the message sender and receiver; second, data packets sent by the system must have special session ID, by this way, an attacker can correctly identify the session. We assume that the sender get in touch with the receiver in a longer period of time. The connection between the sender and the receiver may be reset many round. The time interval of two consecutive reset is called a round. The attackers will intrigue with the nodes in the system to collect the relevant data from the sender. The research results of predecessor attack is shown in Figure 4-1 in recent year

When K. Reiter Aviel and D. Rubín Michael et al. proposed crowds [26] system for anonymous communication system in 1998, the author described predecessor attack firstly in the paper.

Matthew Wright, Micah Adlery, Brian N. Leviney from University of Massachusetts and Clay Shields from Georgetown University describe the definition of the predecessor attack in 2002 [27]. Statistics of the number of messages sent by each node is part of information by which the attacker can identify the communication flow. The attack does not need to analyze the size and time of the packet, but the process of path initialization.

Daniel R. Figueiredo from Hearst at the University of Massachusetts Amherst introduce a model of anonymous communication that can be independent of a specific protocol in 2004 [28].

A. Panchenko from RWTH Aachen University proposed a method of accelerating the attack by using the information of the application layer in 2006 [29].

Nikita Borisov, Prateek Mittal from University of Illinois, Urbana-Champaign, George Danezis from The University of Leuven in Belgium and Parisa Tabriz from Google proposes that the user randomly selects a path in the Tor network, one of which is likely to be attacked with a high probability in 2007 [30]. The method of Tor defense against the attack of the predecessor attack is that each user choose a small set of protected nodes, using as the first node in the tunnel. The user selects the honest node to defend the attack.

Krishna P.N Puttaswamy from University of California, Santa Barbara propose an anonymous protocol named Bluemoon for the predecessor attack in 2008 [31]. This protocol can be used to resist the attack by using a permanent anonymous connection known as hooks. When these links are connected together, they can produce robust anonymous paths, which can avoid path collapse and rebuild cross node failure.

Research on predecessor attack begin early, the main research is still concentrated in the universities in the United States from 2004 to 2008, such as the University of Massachusetts, University of California. With the appearance of the new anonymous communication technology, threats of Predecessor attack are getting weak, and there are few ones researching on it.
5. Other Passive Attack

a. Collusion Attack

Collusion attack is an attack technology to destroy the anonymity of the anonymous communication system, which is based on many of the nodes that have been controlled by them. If the attacker has controlled the anonymous communication system in a part of anonymous nodes, the attacker can infer the relationship between the sender and receiver in the anonymous communication network by collecting the relevant information from the anonymous nodes, so as to destroy the anonymity of the system.

The effective method of the current defense collusion attack is the introduction of the node reputation mechanism, and timely detection and removal of bad nodes in the anonymous system.

b. Latency Attack

Attack Latency [32] is based on different delays from different routers, and these delays can be computed by attackers. In order to calculate the delay in the path from the user to the node A, B, C and the server S, an attacker only needs to use the system to create a route that passes through these nodes to communicate with the S, then calculate the communication delay, and subtract the delay from the communication path between the attacker and the node A. The more accurate the attacker when the first node is closer. An attacker can calculate the delay between the A and the first node. If the attacker controls the first node, the delay can be ignored. Once calculated a set of timing, an attacker can do a lot of things depending on the timing of his collection. If some route according to the delay time is very different, it is easy to determine which route is the use of A.

The main method of defending the latency attack is to add the delay strategy to the
node.

c. **Message Coding Attacks**

Message Coding Attack [32] is the case that without changing message encoding mechanism in the process of communication, attackers determine the corresponding relationship between the packets in and out the network, so as to destroy the anonymity of anonymous communication system.

At present, the information encryption technology is the primary defense method for the encoding attack.

6. **Conclusion**

In the field of network security, more and more researchers begin to pay more attention to the research of anonymous communication technology. Therefore, the research on the technology of anonymous communication system will be helpful to the development of the anonymous communication system. This paper mainly research on the analysis of the passive attack technology in anonymous communication system. We analyzes the advantages and disadvantages of passive attack.

Firstly, the paper introduce the background and development of anonymous communication system attack technology. We counted the number of papers related anonymous communication system. We classify the attack in anonymous communication system from different aspects.

Secondly, the paper introduced the Statistical disclosure attack, timing attack, and predecessor attack in detail. We describe the emergence and development of these methods. The research results of the scholars from different countries have been counted.

Finally, the paper introduces the other passive attack simply. We simply introduce the principles and methods of defense of these methods.

With the development of the anonymous system, passive attack technology will be further development.

**Acknowledgements**

This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; 2010 Information Security Program of China National Development and Reform Commission with the title “Testing Usability and Security of Network Service Software”.

**References**


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.

Pan Gao. He was born in Hebei Province, China, 1989. He is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information and network security, 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.

Wan-Jiang HAN. She was born in HeiLongJiang province, China, 1967. She received her Bachelor Degree in Computer Science from Hei Long Jiang University in 1989 and her Master Degree in Automation from Harbin Institute of Technology in 1992. She is an assistant professor in School Of Software Engineering, Beijing University of Posts and Telecommunication, China. Her technical interests include software project management and software process improvement.