源路由匿名通信系统中主动路径探测机制研究*)

眭鸿飞　刘宁舜　陈松乔　陈建二
(中南大学信息科学与工程学院　长沙410083)

摘　要　在源路由匿名通信系统中,通信发送者发起建立一条由多个成员组成的重路由路径,并采用嵌套加密技术加密传输数据,以保证通信关系匿名。然而,通过主动破坏重路由路径并迫使其多次重构,合谋成员能采用前驱攻击的方法,推断出通信发送者的真实身份,破坏系统的匿名性。本文提出主动路径探测机制,由通信发送者发送嵌套加密Ping报文以探测重路由路径的状态,根据用户返回的签名响应报文确定路径上的故障点,以确定系统中的主动合谋成员,从而提高匿名通信的安全性。

关键词　信息隐藏,匿名通信

Research of Active Path Detection in Anonymous Communication System Based on Source Routing

SUI Hong-Fei　LIU Ning-Shun　CHEN Song-Qiao　CHEN Jian-Er
(Department of Information Science and Engineering, Central South University, Changsha 410083)

Abstract　To achieve the relationship anonymity, the sender of communication establishes a rerouting path consisted of multiple participants in the Anonymous Communication System based on Source Routing (ACSSR), and nested-encrypt the message. By destroying the rerouting path, however, collaborators in system can force the rerouting path to reset multi-time, thus perform predecessor attack to determine the sender of communication, and compromise the anonymity. In this paper, a strategy based on active path detection mechanism is proposed, which ping every intermediator of the rerouting path by nested-encryption message. Active collaborators can be located precisely according to the response message after the collaborators destroy the rerouting path multi-times. Thus, the security and reliability of system could be enhanced effectively.

Keywords　Information hiding, Anonymous communication

1　引言

随着人们对于网络通信中隐私信息保护的日益重视,兴起了匿名通信的研究。目前已有的匿名通信系统中,Mixes[2]、Anonymous Remailer[3]、Onion Routing[4,5]、Crowds[6]、Hordes[7]、MorphMix[8]以及Tarzan[9]等均采用重路由机制(Rerouting)提供匿名保护。重路由机制是一种应用层路由机制。它为用户提供间接通信。包含在一次通信中的多个主机在应用层存储转发数据,从而形成一条由多个安全信道组成的虚拟路径,称为重路由路径(Rerouting Path)。从安全信道上所传送的IP数据包首部,外部合谋成员无法获得真实的发送者和/或接收者的IP地址信息。因而,通信实体的身份信息被有效地隐藏。

重路由路径的建立依据其路径上成员的确定方式可分为两种。其一是源路由方式(Source Routing),即由通信发送者从匿名网络中选取成员,通过密钥协商机制确定与各成员的会话密钥,进而建立重路由路径。传输数据时,对数据进行多重加密后再发送。通过解密接收到的数据,路径中每个节点获得下一跳节点的地址,却无法获知最终的接收者地址以及传输数据内容,因而能提供强的匿名保护。这一类系统如Onion Routing、Tarzan、MorphMix等,我们称之为源路由匿名通信系统(Anonymous Communication System based on Source Routing, ACSSR)。其二为分布式路由方式(Distributed Routing),即由通信发送者将接收者地址及数据发送给下一跳成员,由每一跳的成员根据该接收者地址顺次选定下一跳成员。这一类系统如Crowds、Hordes等,我们称之为分布式路由匿名通信系统(Anonymous Communication System based on Distributed Routing, ACSDR)。

然而,当系统中的一部分成员由对手所控制时,通过破坏重路由路径迫使其多次重组,对手能够施行前驱攻击(Predecessor Attack),推测通信实体的真实身份,破坏系统的匿名性[6,10,11]。本文针对这种攻击,深入剖析其内在机制,提出基于多重加密Ping报文的主动路径探测机制,根据攻击者的行为定位路径上的攻击者,以提高匿名通信的安全性,并对安全性进行了分析。

2　源路由匿名通信系统

匿名保护有三种形式:发送方匿名(Sender Anonymity)即报文无法被关联到其发送者;接收方匿名(Recipient Anonymity)即报文无法被关联到其接收者,通信关系匿名(Relationship Anonymity)即无法关联报文的发送者与接收者[1]。源路由匿名通信系统通常提供发送方匿名或通信关系匿名两种形式的保护。

2.1　系统模型

源路由匿名通信系统可被视为一个多代理通信系统,通信数据经多个代理存储转发至接收者,以达到匿名保护的目

*)基金项目:国家自然科学基金(编号:90104028);国家杰出青年科学基金(编号:69928201)。**眭鸿飞**　博士研究生,主要研究领域为网络安全,信息隐藏。**刘宁舜**　硕士研究生,主要研究领域为匿名通信。**陈松乔**　教授,博士导师,主要研究领域为软件工程。**陈建二**　教授,博士导师,主要研究领域为计算机网络与优化理论。

的。我们的讨论将主要针对发送者匿名形式的保护，关系匿名与此类似。一个源路由匿名通信系统为由网络中若干个提供匿名服务的主机组成的集合，设为 $V=\{v_j|0\leqslant j<n\}$，其中的主机 v_j 称为成员(Participant)，系统中成员数为 $|V|=n(n\geqslant 1)$。在系统运行期的某一间隔时间内如一小时，成员数目 n 固定为一常数。通过安全通信信道，两两成员之间可进行直接通信。需要匿名通信服务的用户选择一个成员 $s\in V$ 作为其代理成员，并将接收者地址传送给该代理成员。由该代理成员从系统中选取成员，发起建立一条由若干个成员组成的到达接收者的重路由路径，以用于用户和接收者之间的间接通信。下文的讨论中，我们把该代理视作发送者。

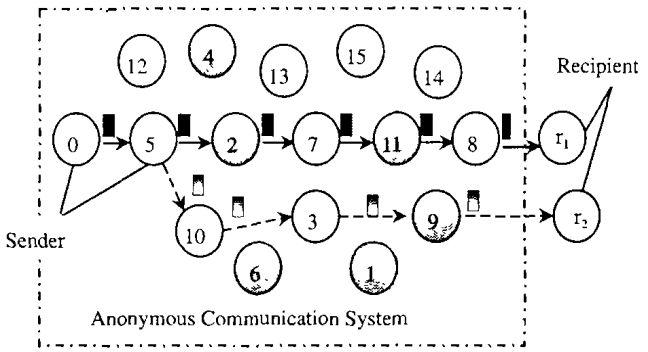

图1 源路由匿名通信系统

形式化地，一条重路由路径可表示为

$$\Gamma=\langle s,I_1,I_2,\cdots,I_t,\cdots,I_l,r\rangle$$

其中 $s\in V$ 称为通信的发送者(Sender)，$r\in V$ 为通信的接收者(Recipient)，I_t ($I_t\in V$，$1\leqslant t\leqslant L$) 为中继节点(Intermediator)，$\langle I_1,I_2,\cdots,I_t,\cdots,I_l\rangle$ 称为中继序列(Intermediator Sequence)。中继序列中的节点数目 $l(l=1,2,\cdots)$ 为路径长度，l 通常为可变。

2.2 重路由路径

用户需要匿名会话时，选定网络中的某一服务器作为代理，将接收者的地址发送给它。该代理作为发送者发起建立一条与接收者之间的重路由路径，并负责路径的维护与重构。发送者从网络中随机选取一些成员形成中继序列，用各中继节点的公钥对原始数据以及各中继节点的地址进行嵌套加密(Nested Encryption)，构成一个嵌套加密的报文。中继节点解密所收到的报文，获取下一跳中继节点地址以及双向会话的加密密钥和加密函数，并对报文进行填充，以保持报文长度不变。最终，发送者与接收者之间就建立一条重路由路径。报文经嵌套加密后结构如下：

$$\{exp\_time,next\_hop,F_f,K_f,F_b,K_b,payload\}_{PK_x}$$

其中 exp_time 为生命周期，$next\_hop$ 为下一个中继节点的地址，(F_f,K_f) 为正向会话函数/密钥对，(F_b,K_b) 为反向会话函数/密钥对，$payload$ 或为下一个结构相同的洋葱包或为一个 $padding$，PK_x 为接收该包的中继节点的公钥。

重路由路径的重构在两种情况下发生。其一为主动重构(Active Reset)，即在系统默认的周期超时后，系统中所有的重路由路径都将被拆除并进行重构。其二为被动重构(Passive Reset)，即由于重路由路径上的中继节点或通信信道失效使路径被破坏而导致重构。因此，用户的一次会话过程中，重路由路径将可能被多次重构。在下文的分析中我们将看到，前驱攻击正是利用这一特点进行匿名攻击。

2.3 前驱攻击

由于匿名通信系统中未采用严格的信任机制限制成员的加入，对手有可能控制系统中的部分节点，即系统中存在一部分敌对成员。这些敌对成员被选中到某条重路由路径上时，能够观测其在路径上的前驱、后继等相邻中继节点的地址等信息，共享观测到的信息，并且在必要时能通过停止转发数据的方式破坏数据传输，导致重路由路径的重构。这部分成员被称为合谋成员(Collaborator)。通过进行前驱攻击，合谋成员能够推测出通信发送者。

如前所述，发送者发起建立重路由路径时，以随机均匀的方式从系统中选取一部分成员构成一个中继序列。当系统中存在有合谋成员，则合谋成员将以同等的概率被选中到重路由路径上。假设一个匿名系统中，存在合谋成员集 $C\subset V$，($|C|=c$)，在发送者与接收者的一次会话中，当中继序列的首个和最后一个中继节点，即 I_1 和 I_l 为合谋成员时，通过计时攻击，合谋成员能够确认自身在重路由路径上的位置，并进而推断首个合谋成员的前驱为发送者，前驱攻击就将成功。

根据 Wright 的分析，在单轮(single-round)的情况下，攻击成功的概率为 $(c/n)^2$，应用 Chernoff 上界[12]，可以推出当重路由路径重构次数大于 $T=2(n/c)^2\ln n$，攻击成功至少一次的概率达到 $(n-1)/n$。

3 基于嵌套加密 Ping 报文的主动路径探测机制

由上文分析可以看出，进行前驱攻击的关键在于，在用户的单次会话中，使重路由路径多次重构，对观测到的前驱进行统计，从而推断出发送者。对于合谋成员利用重路由路径的主动重构进行攻击的情况，防御措施相对较简单，可以通过加大系统默认的重构周期，从而降低用户会话时重路由路径重构次数来防止。

当合谋成员采用停止转发数据等方式迫使重路由路径多次被动重构的方式进行攻击时，情况将比较复杂。首先便是由于网络传输的不可靠性，通信信道和成员有可能失效，导致重路由路径重组。其次为当路径上的合谋成员停止转发数据的同时，有可能假冒是其他成员导致了失效。

针对这种情况，我们提出基于嵌套加密 Ping 报文的主动路径探测机制(Active Path Detection，APD)，通过检测重路由路径上每个结点的状态来获得路径中每个结点的可用信息，确定系统中的合谋成员和不稳定成员，以用于重路由路径的建立及重构，最终提高系统的安全性。在策略中，将合谋成员和不可靠成员同等对待。用于探测路径上各中继节点状态的 Ping 报文被嵌套加密后发送，以防止合谋成员将其从正常传输数据中区分出来。算法如图2所示。

输入：匿名网络成员集 $V=\{v_j|0\leqslant j<n\}$，重路由路径 $\Gamma=\langle s,I_1,I_2,\cdots,I_t,\cdots,I_l,r\rangle$，合谋成员集 $C\subset V$

输出：重构后的重路由路径 $\Gamma'=\langle s,I_1,I_2,\cdots,I_t,\cdots,I_l,r\rangle$，新合谋成员集 $C'\subset V$

```
Begin
    s_l = Random();
    p_l = (s_l)_{K_l};
    for i = l-1 to 1
        s_i = Random();
        p_i = (p_{i+1}, s_i, I_{i+1})_{K_i};
    send ping_request(p_l) to I_l via Γ;
    rc = wait for ping_response;
    if rc ∈ {!ok, timeout}
        for i = 1 to l
          send ping_request(p_i) to I_i via Γ;
          rc = wait for ping_response;
          if rc ∈ {!ok, timeout}
            C = C ∪ {I_i}
            i = i-1;
            While rc ∈ {!ok, timeout}
              I_{i+1} ∈_R V/C;
              send reset_path_request(I_{i+1}) to I_i
              rc = wait for reset_path_response;
End
```

图2 主动路径探测算法

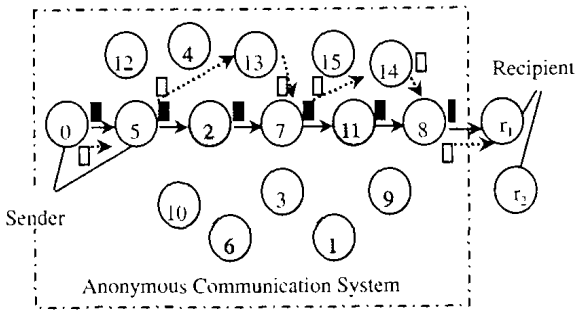

图3 主动路径探测

算法的主要思想为：在重路由路径建立后，发送者不定期地沿重路由路径发送 Ping 报文到 I_l，并且等待响应。Ping 报文的构造采用路径上的节点的公钥对随机数进行嵌套加密而成。其结构为

$$p_i=(p_{i+1},s_i,I_{i+1})_{K_i}$$

其中，p_{i+1}为发送给中继节点 I_{i+1}的数据，s_i 为产生用于中继节点 I_i 签名的随机数，I_{i+1}为中继节点 I_i 的下一跳，也即中继节点 I_{i+1}的地址，K_i 为中继节点 I_i 的公钥，(p_{i+1},s_i,I_{i+1})用 K_i 加密。p_i 的完整结构如下：

$$p_i=((\cdots(s_l)K_l,\cdots,s_{i+1},I_{i+2})K_{i+1},s_i,I_{i+1})_{K_i}$$

路径上各中继节点解密接收到的报文，获得相应的随机数 s_i，并在接收到由下一跳返回的报文后，连同该随机数采用私钥加密后返回。

发送者接收到对于 Ping 的响应后，解密获得各随机数 si 进行比较，若错误将开始路径探测及重构。若超时也将开始探测与重构。探测过程主要为发送者向路径上每个成员发送 Ping 报文并等待响应来确定故障点。

若响应 Ping 报文的为 $I_i(i\leqslant l)$，I_{i+1}为不可达，则发送者将从节点 I_{i+1}开始重构路径 $\Gamma'=\langle I_1,\cdots,I_i,I_{i+1},\cdots,I_l,r\rangle$。重构过程为，首先将 I_{i+1}作为合谋成员加入到集合 C 中。从正常成员集 $V-C$ 中随机选取一节点作为 I_{i+1}，依此递增继续重构路径。

图3中，初始重路由路径为 $\Gamma=\langle v_0,v_5,v_2,v_7,v_{11},v_8,r_1\rangle$，其中包含合谋成员 v_2与 v_{11}，经主动探测后从中继节点 v_2开始重构形成新的路径为 $\Gamma'=\langle v_0,v_5,v_{13},v_7,v_{14},v_8,r_1\rangle$。

4 安全性分析

可以看到，重构路径时，发送者从网络的正常成员中伪随机地选择一系列的成员，并且沿原路径的正常部分发送 Ping 报文，以及路径重构请求。即从发送者到成员 I_i 建立路径的请求被 $I_1\cdots I_{i-1}$作为正常的报文传递。由于报文被多重加密，I_i 无法确定该报文源于 I_{i-1}或是其他的前驱成员，I_{i-1}无法区分出建路请求报文和普通的数据。因此，发送者的身份不被暴露，整个路径检测和重构过程是安全的。

采用主动的路径探测机制后，当合谋成员施行主动攻击，以破坏重路由路径并迫使其重组时，系统将能够精确定位合谋成员，并且在随后的路由中将其排除。即网络中 c_1个合谋成员进行主动攻击时，发送者可以准确定位并避开这 c_1个节点，使得系统中的合谋成员数目降到 $c-c_1$。

因此在单轮情况下，攻击成功率为$(\frac{c-c_1}{n-c_1})^2$。应用 Chernoff 上界，如果要使得攻击成功至少一次的概率达到$\frac{n-1}{n}$，重路由路径重构次数必须多于 $T'=2(\frac{n-c_1}{c-c_1})^2\ln(n-c_1)$。图4为两者的比较曲线图。从中可以看出，采用主动路径检测机制后，攻击所需的时间轮数显著增加，匿名系统的安全可靠性进一步增强。

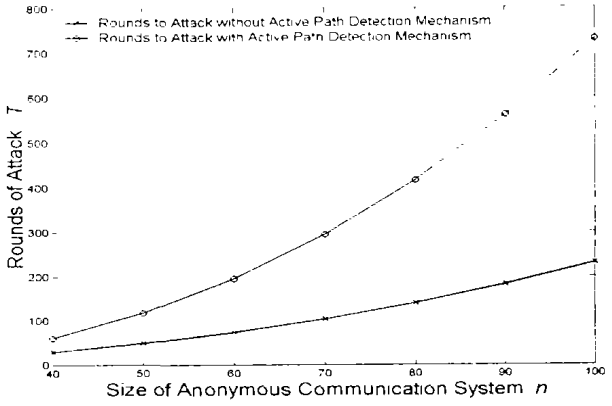

图4

结论 在匿名通信系统中如何识别合谋成员，防止前驱攻击一直是一个热点问题。本文提出的路径探测机制能有效地识别系统中的合谋以及不可靠成员，保证发送者的匿名性，并且该机制能够用于在对传输的可靠性要求较高的网络中。

本文的下一步工作将计算采用主动路径探测机制时，识别出合谋成员所需的时间复杂度。并将其与合谋成员识别出通信发送者的时间复杂度进行定量比较，以全面评价该机制的性能。

参 考 文 献

1 Pfitzmann A, Köhntopp M. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In: Hannes, F. ed. Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability. Berkeley, CA, USA: Springer-Verlag, Lecture Notes in Computer Science 2009, 2000. 1～9

2 Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24(2): 84～90

3 Anonymous Remailer. http://www.lcs.mit.edu/research/anonymous.html

4 Syverson P, Goldschlag D, Reed M. Anonymous Connections and Onion Routing. In: Proc. of the IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE Computer Society Press, 1997. 44～54

5 Goldschlag D, Reed M, Syverson P. Onion Routing for Anonymous and Private Internet Connections. Communications of the ACM, 1999, 42(2): 39～41

6 Reiter M K, Rubin A D. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, 1998, 1(1): 66～92

7 Shields C, Levine B N. A Protocol for Anonymous Communication Over the Internet. In: Proc. of 7th ACM Conf. on Computer and Communication Security. New York: ACM Press, 2000. 33～42

8 Rennhard M, Plattner B. Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection. In: Proc. of the Workshop on Privacy in the Electronic Society, Washington, DC, USA, Nov. 2002

9 Freedman M J, Morris R. Tarzan: A Peer-to-Peer Anonymizing Network Layer. In: Proc. of the 9th ACM Conf. on Computer and Communications Security (CCS 2002), Washington, DC, USA, Nov. 2002

10 Wright M, et al. An Analysis of the Degradation of Anonymous Protocols. In: Proc. of the Network and Distributed Security Symposium - NDSS '02, Feb. 2002

11 Wright M, et al. Defending Anonymous Communication Against Passive Logging Attacks. In: Proc. of the 2003 IEEE Symposium on Security and Privacy, May 2003

12 Mtotawani R, Raghavan P. Randomized Algorithms, chapter 4. Cambridge University Press, 1995