匿名通信技术分析

陆 庆，周世杰，傅 彦

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】针对匿名通信的应用，讨论了匿名通信的基本假设，定义并解释了其涉及的基本术语。依据典型的匿名通信系统，分析了基于重路由技术的匿名通信系统模型，提出了按隐匿对象和所采用技术的匿名通信分类方法，并将其应用到洋葱式路由等具体的匿名通信系统的分析中，从而表明匿名通信技术具有广泛的应用前景。

关 键 词 匿名通信; 匿名系统; 洋葱式路由; 信息隐藏; 信息安全

中图分类号 TP393 文献标识码 A

Analyzing Anonymous Communication Technology

Lu Qing，Zhou Shijie，Fu Yan

(School of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract The application of the anonymous communication technology is discussed. The basic concepts and terms of anonymous communication are also defined and analyzed. After discussing the classifying method of anonymous communication, according to the anonymous objects and technology adopted, a useful classification is also put forward. Then, this paper is focus on analyzing the routing-based anonymous communication system. The model of the anonymous systems and the methods used to evaluate the anonymity degree of system are studied in-depth. Finally, three practical anonymous systems, DC-NET, onion routing, and crowds, are illustrated and summarized. This results show that the anonymous communication technology is not well understood in many aspects. And its application in information security has a nice future.

Key words anonymous communication; anonymous system; onion routing; information hiding; information security

网络环境下的信息安全是全球开放网络环境中的普遍需求，是未来国家信息战的主要内容。广义的信息安全不仅包括信息的机密性、完整性等内容，也涉及与信息流相关的通信连接的安全性。流量分析是威胁通信连接的重要攻击手段。该攻击方法通过分析流经开放网络的信息流，可以大体确定出各种重要的网络实体、重大的网络活动、敏感的通信连接等。网络攻防技术中涉及到信息截获与反截获、破译与反破译、入侵与反入侵等问题，可分为主动攻击(包括各种窃听)和被动防御(包括入侵检测、审计、追踪等)。匿名通信技术属于一种防御性安全保护手段[1, 2]，通过匿名计算方法，可加密网络负载，隐匿网络实体(包括通信连接)。此外，匿名计算技术在电子投票、电子货币，以及匿名电子邮件系统等均有广泛的应用前景。为此，研究匿名通信技术，抵御流量分析攻击和其他网络攻击，提高信息安全的防护级别和网络环境的安全容忍

收稿日期：2003 – 05 – 21
基金项目：国家863引导计划项目(2002AA001042)
作者简介：陆庆(1964 –)，女，学士、工程师，主要从事信息安全方面的研究.

性，具有重大的经济、社会和军事意义。

1 基本假设与定义

匿名通信与加密通信有密切的关系。在匿名通信系统中，假定网络内主机之间的通信具有机密性，即网络外的任何主机不能观察到在网络内流动的信息流的信息。同样，主机之间的通信也经过认证，即不存在欺骗行为，可通过链路级认证来保证。此外，还假定通信实体的具体物理位置信息在系统中保密，若能知道用户的物理位置，匿名通信也失去了其意义。

匿名通信是不能确定通信方(可能是通信双方)身份的通信技术，它保护通信实体的身份，而加密系统是保护数据的机密性,在匿名通信系统中，不仅通信的内容不可知，通信连接也不可知。通信的发起者是信息的发送者，与通信发起者相对应的是消息的接收者，通信双方之间可能存在消息载体。消息代理是与消息传递相关的任何主机，一次通信具有匿名性是指在该通信会话期间，没有任何恶意用户能确切知道通信双方的真实身份(在网络环境中，身份与IP地址等价，因此，身份匿名就是IP地址的匿名)，其“匿名程度”可用确定某主机是通信实体的概率来度量。一个系统是否有足够的匿名性，完全取决于系统的需求。匿名系统的效率取决于计算量、需要的带宽(相对于所传送的数据)和需要进行的通信次数。计算量是加密数据的计算时间，而进行通信的次数可以用来估计一次操作的时延。

2 隐匿通信技术分类

隐匿通信技术有许多不同的分类方法，本文主要根据隐匿对象和采用的技术对隐匿计算进行分类。

2.1 按隐匿对象分类

根据需要隐匿的通信对象不同，匿名系统可分为发送者匿名、接收者匿名和通信双方匿名。发送者匿名是保护通信发起者身份不为恶意用户所知，接收者匿名是保护信息接收者身份机密性，而通信双方匿名则是通信发起者和信息接收者的身份均保密。此外，在一个完整的匿名系统中，还存在节点匿名和代理匿名。节点匿名指组成通信信道的服务器的匿名性，即信息流所经过线路上的服务器的身份不可识别。代理匿名是指某一节点不能确定为是发送者和接收者之间的消息载体。节点匿名要求第三方不能确定某个节点是否与任何通信连接相关，而代理匿名则要求某节点不能确定与某一具体通信连接相关，故代理匿名的隐匿程度较节点匿名低。

2.2 按采用的技术分类

随着匿名技术的发展，根据所采用的技术，主要分为基于路由的匿名通信和非路由的匿名通信。传统的TCP/IP网络协议在数据包中均标记了消息源的IP地址，因此不能提供匿名通信服务。基于路由的匿名通信是采用网络路由技术来保证通信的匿名性，即采用路由技术改变消息中的消息源的真实身份，从而保证通信匿名。依据所采用的路由技术不同，又可分为广播式路由匿名通信系统和重路由匿名通信系统。广播式路由匿名通信是采用TCP/IP协议的广播协议(如Multicast)来隐匿通信双方的身份，这是因为诸如多投协议采用了D类网络地址，它没有消息发送者的IP地址信息。重路由匿名通信则通过消息中间节点来改变消息源：发送者将消息发送到中间节点，由该节点作为消息的代理来转发消息，从而除了消息的代理节点外，不能确定消息源。

由上分析，基于路由的匿名通信可视为一个映射：$f: M_s \to M_a$，其中，M_s是原始消息，M_a是改变消息源的代理消息，其变换示意如图1所示。因此，可以设计不同的消息转换器来改变消息源。一旦消息经过消息转换器，新得到的代理消息中不再包含消息源的真实身份信息，从而提供了匿名服务。因此可见，基于路由的匿名通信系统存在多种形式，也是目前匿名计算的重要发展方向。

非路由的匿名通信系统一般建立在Shamir的秘密共享机制基础上[3~5]。Shamir的秘密共享机制允许n个用户分别拥有不同的秘密信息 $s_1, s_2, s_3, \cdots, s_n$，完整秘密信息可不显示任何人单独拥有的秘密信息，计算得到 $S = \sum_{i=1}^{n} s_i$。通信参与者可通过以下过程进行匿名通信：

STEP 1　用户i拥有秘密S_i并加入匿名通信

$$S_i=\begin{cases}X & \text{希望进行通信}\\ 0 & \text{其他}\end{cases}$$

式中 X是两个消息的连接结果，$X=E_j(k)|E_k(M)$，E_j用接收者j的公钥进行非对称加密，E_k是用共享密钥k进行对称加密。

STEP 2A 除了发送者之外，每个用户均试图用自己的私有密钥解密结果$S(T)$。如果某个用户解密成功，则该用户知道消息发送给自己，并转STEP 3，否则转STEP 1。

STEP 2B 发送者判断$S(T)=X$，如果不成立，则出现冲突，取消STEP 1中发送的消息，并等待一随机时间间隔T'后重发，直到成功。

STEP 3 接收者j通过解密得到消息M，如果需要发送应答消息M_2，则设置秘密$S_j=E_kM_2$转STEP 1。

STEP 4 转STEP 1。

根据上述分析，可得到匿名通信的分类如图2所示。从系统实现来看，按采用的匿名技术分类具有更好的应用范围。依据所采用的技术不同，既可以实现单方匿名(发送者匿名或接收者匿名)，也可实现双方匿名。因匿名对象的要求不同，对所采用的技术有很大的影响。从技术角度来看，路由式匿名技术易实现双方通信匿名，而采用非路由式匿名技术则较为复杂。

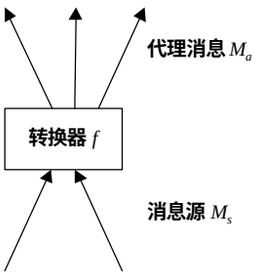

图1 基于路由的匿名通信系统示意图

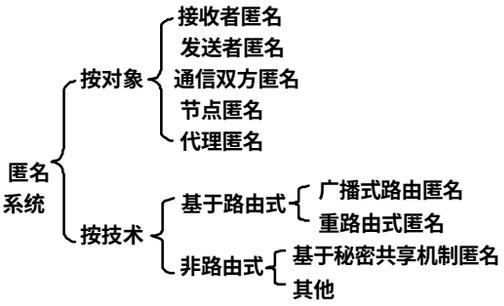

图2 匿名通信分类

5 匿名通信系统及评估

由于非路由匿名技术目前应用较少，而广播式路由匿名技术与Multicast技术相关[6, 7]，因此，本文仅就采用重路由技术的匿名系统进行详细分析和讨论。

一个基于重路由的匿名系统包含N个节点的集合$V=\{v_i:0\le i\le N\}$，该N节点相互合作，从而使系统的通信服务具有匿名性。考虑到实际情况，假设接收者R在通常情况下容易被攻击，因此R是非安全节点，它不包含在N节点集合中。此外，为了讨论的方便，假设网络在传输层通信，因此，节点集V中的节点均能相互通信，故匿名系统可视为一个具有团性质的图，其边代表从源到目的的一条路径。

为了隐藏通信方的真实身份，消息源发送的消息通过一个或多个中间节点才能到达信宿，消息经过的路径定义为重路由路径

$$P=\langle s,I_1,I_2,\cdots,I_L,R\rangle \tag{1}$$

式中 $s\in V$是发送者，$I_k\in V(1<k<L)$是路径中的第k个中间节点。需要注意的是，$R\notin V$。图3所示的匿名通信系统模型包含11个节点，标号为0的节点是消息发送者，消息的重路由路径根据匿名系统的需要决定(图中所示为$\langle 0,3,7,9,R\rangle$)，并最终到达R。重路由路径中中间节点的个数被定义为路径长度(Path Length，图3中所示路径长度为3)

$$|p|=|P_r| \qquad P_r\subset P;s,R\notin P_r \tag{2}$$

在基于重路由的匿名系统中，关键是重路由路径P的选择，依据P的长度是否固定，可分为固定路径(Fixed Path Length)重路由匿名系统和变路径(Variable Path Length)重路由匿名系统，路径选择算法如下：

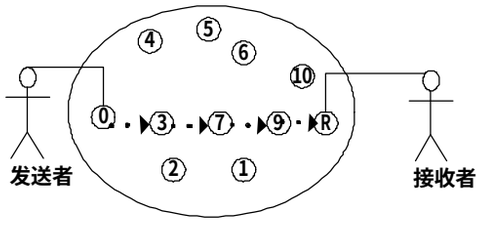

图3 匿名通信系统模型示意图

输入：发送者s，接收者R。

1)Select path length L;

2) Chose a sequence of intermediate nodes, I_1, I_2, …, I_L;

3) Return the path: <s, I_1, I_2, …, I_L, R>。

4　匿名系统实例分析

4.1 DC-NET

DC-NET是采用非路由技术并实现发送者匿名的匿名系统[4]。在DC-NET系统中，每个参与匿名通信的用户与其他用户共享安全令牌，并向用户通告自己观察到令牌数的奇偶性。由于每个令牌被通告了两次，因此最后的奇偶性为偶。发送者通过控制自己宣告的奇偶性，可以使结果为奇，从而可以和接收者匿名通信。从分类来看，DC-NET是典型的非路由式匿名通信系统。

4.2 洋葱式路由

洋葱式路由(Onion-routing)是基于重路由技术的并可提供双方匿名通信的匿名系统[5, 8]。使用称为Onion Router的代理，将发起者所要传送的消息转发到接收者，因此发送者只需要知道代理的身份，而不需要其他信息，从而实现匿名通信。为了增加系统的匿名度，一个Onion Routing 匿名系统往往存在许多Onion Routers，这些Routers知道彼此的身份和相应的公钥。在Onion Routing协议中，发送者s在这些Routers中选择一个作为自己的消息代理 s ，并构造一条可到达接收者的路径字符串，并存储在数据包中，即

$$s : s \sim s \sim s' \sim s'' \sim R$$

式中 $\sim$ 代表路径中的一个连接，s 代表Onion Routers。

Routers通过加密信道来协作转发消息，即将消息封装加密，在传送过程中，分层加密的数据逐层剥离，得到路由信息，从而保证消息继续向下一节点转发，并能最终到达信宿。发送者必须构造整个路径的路由信息(即下一个Router的IP地址)，因此构造的包为

$$s \to s : \mathrm{ACI}, k, \{s', k', \{s'', k'', \{R, data\}K_{s''+}\}K_{s'+}\}K_{s+}$$

式中 s 是发送者s的消息代理，K_{s+} 表示用对应Router的公钥加密数据，k是下一个Router的地址信息，ACI是匿名连接标示符，包的中间即为接收者身份信息和需要传送的数据。

4.3 Crowds

Crowds与Onion Routing相似，Crowds协议也使用相互协作的代理来提供匿名服务[9]，但不同的是，在Crowds中发送者不需要选择所有的路由信息，相反，该路径信息在信息传送过程中随机生成。因此，Crowds属于非固定路径重路由匿名通信系统。Crowds匿名通信原理如下

$$s \to s_j : \{R, p, data\}_{K_{sj}}$$

式中 s_j 是随机选择的一个Router，p是路径标示符，k_{sj} 是s和 s_j 共享的密钥。当 s_j 收到数据包后，按概率决定是继续传送到下一Router还是直接传送到接收者

$$s_j \to s'_j : \{R, p', data\}_{K_{jj'}}$$

或

$$s_j \to R, p', data$$

综上所述，消息经过代理的转发，最终可到达信宿，并保证消息传送过程的匿名性。

5　结 束 语

匿名通信是一门崭新的信息安全学科[10]，与信息隐藏有密切的关系，也可视为匿名通信是信息隐藏的一个分支。实现匿名通信可用不同的技术，最终提供匿名服务的匿名度不同。要对匿名通信进行深入研究，必须掌握匿名通信系统的分类、匿名度的评估模型并结合应用需求来考虑。本文提出的匿名通信系统分类方法对该领域的研究工作有一定的指导作用，其匿名度评估模型具有参考价值。

(下转第179页)

4 结 束 语

综上所述，在整个车辆定位系统不同阶段的开发过程中，对不同的部件需根据系统的需求采用不同的软件体系结构风格来设计和开发相应的模块，提高设计重用、带来代码重用，方便其他人对于该系统组织方式的理解，使用标准的体系结构风格支持彼此协作能力，从而提高软件质量和可靠性。

本文研究工作也得到了电子科技大学青年基金资助，在此表示感谢。

参 考 文 献

[1] Zhang F, Deng M. Trigger for moving object databases based on the Web environment[C]. Proceedings of the 17th International Conference on Advanced Science and Technology (ICAST01), Chicago, IL, 2001, 162-169

[2] Wolfson O, Xu B, Chamberlain S. Location prediction and queries for tracking moving objects[C]. Proceedings of the 16th International Conference on Data Engineering (ICDE00), San Diego, 2000, 687-688

[3] Medvidovic N, Taylorm R N. Exploiting architectural style to develop a family of application[J]. IEE. Software Eng. 1997, 14(5-6): 237-248

[4] 车敦仁, 周立柱. 软件体系结构、应用平台及框架仓库技术[J]. 计算机研究与发展, 1996, 33(7): 501-506

[5] Robert T M, Andrew K, Ralph M, *et al.* Architectural styles, design pattern, and objects[J]. IEEE Software, 1997, 14(1): 43-52

[6] Dewayne P, Aleander L W. Foundations for the study of software architecture[J]. ACM SIGSOFT Software Engineering Notes, 1992, 17(4): 40-52

编　辑　徐培红

(上接第165页)

参 考 文 献

[1] Clark I, Sandberg O, Wiley B, *et al.* Freenet: a distributed anonymous information storage and retrieval system[C]. In Proc. of the Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, 2000

[2] Michael J F, Emil S S, Josh C, *et al.* Tarzan: a peer-to-peer anonymizing network layer[C]. In Proc. of the 1st International Workshop on Peer-to-Peer Systems, Proceedings of the 1st International Workshop on Peer-to-Peer Systems, Cambridge, MA, USA , 2002

[3] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms[J], VACM, 1982,24(2): 84-88

[4] Chaum D. The dining cryptographers problems: unconditional sender and recipient untraceability[J]. Journal of Cryptology, 1988, 1(1): 65-75

[5] Goldschlag D, Reed M, Syverson P, *et al.* Onion.routing for anonymous and private internet connections[J]. Communication of the ACM, 1999, 42(2): 39-41

[6] Guan Y, Fu X, Bettati R, *et al.* A optimal strategy for anonymous communication[R]. Technical Report: tr2002-3-1, Dept. of Computer Science Texas A&M University, November 2001

[7] Scalatta V, Levine B, Shields C, *et al.* A protocol for anonymity and anonymous peer-to-peer file sharing[C]. Proceedings of IEEE International Conference on Network Protocols, Nov. 2001

[8] Syverson P, Goldschlag D , Reed M, *et al.* Anonymous connections and onion routing[C]. Proceedings of IEEE Symposium on Security and Privacy, IEEE CS Pres, Oakland, CA, 1997

[9] Reiter M K , Rubin A D. Crowds: anonymity for web transactions[J]. ACM Transactions on Information and System Security, 1998, 1(1): 62-92

[10] 周世杰, 秦志光, 耿　技. 一个安全用户认证协议[J]. 电子科技大学学报, 2001, 29(2): 201-204

编　辑　徐培红