文章编号:1671-4598(2017)08-0268-04 DOI:10.16526/j.cnki.11—4762/tp.2017.08.069 中图分类号:TP393 文献标识码:A

可信计算模式下 P2P 匿名通信系统设计

雷 涛
(华南师范大学 物理与电信工程学院,广州 510006)

摘要:为了提高 P2P 匿名通信系统的安全性与可信性,需要对 P2P 匿名通信系统进行设计;当前使用的匿名通信系统,无法在用户节点匿名的情况下,保证 P2P 匿名通信系统匿名节点的可信性;因此,提出一种基于可信计算模式的 P2P 匿名通信系统设计方法;该系统的硬件部分分为系统登录模块、通信模块、数据模块、可信计算模块 4 大模块,模块之间相互合作,形成一个完整的匿名通信系统,匿名通信系统软件设计部分通过建立可信计算的联接,实现在匿名通道中进行数据传递,并对待传递的数据进行层次性打包加密,同时采用可信度计算对匿名通信系统中节点、匿名通道进行计算,形成安全可信的匿名传递通道;实验仿真证明,该方法在保证该系统数据传递的效率的同时提高了匿名通信系统的安全性与可靠性。

关键词:可信计算;P2P;匿名通信系统

Design of P2P Anonymous Communication System Based on Trusted Computing

Lei Tao
(School of Physics and Electronic Engineering, South China Normal University, Guangzhou 510006, China)

Abstract: In order to improve the safety and reliability of P2P anonymous communication system, the need to design P2P anonymous communication system. Anonymous communication system currently in use, not in the anonymous user node, to ensure the credibility of P2P anonymous communication system of anonymous nodes. Therefore, puts forward a design method of P2P anonymous communication system based on trusted computing model. The hardware part is divided into system login module, communication module, data module, trusted computing module 4 modules, mutual cooperation between modules, to form a complete anonymous communication system, anonymous communication system software design through the connection establishment of trusted computing, Realization of data transmission in the anonymous channel, and the level of data transfer encryption package to the credibility of the calculation, the node in anonymous communication system, anonymous channel is calculated, the formation of a safe and reliable delivery channel. Anonymous experiments show that this method improves the safety and reliability of the anonymous communication system to ensure efficiency the system of data transmission at the same time.

Keywords: trusted computing; P2P; anonymous communication system

0 引言

近年来,随着信息时代的发展,计算机的广泛应用和网络技术的快速发展,网络中用户隐私与数据传递安全的问题,已经成为互联网中迫切需要解决的问题[1]。如何使 P2P 匿名通信系统中用户的隐私与数据传递处于匿名状态,达到保护个人隐私的作用,成为当前技术开发人员研究的重点[2]。然而当前使用的匿名通信系统,无法在用户节点匿名的前提下,保证 P2P 匿名通信系统匿名节点的可信性[3]。在这种情况下,如何提高 P2P 匿名通信系统的安全性与可信性,已经成为当前需要解决的主要问题。该系统将硬件部分划分为以下几个部分,系统登录模块对用户的私人信息进行认证,通信模块可以实现一对一或一对多的数据传递,数据模块对将要发出的数据进行打包加密,使得数据更加安全,可信计算模块是计算整个匿名系统节点的可信度,同时使用可信度计算对匿名通信系统中节点、匿名通道进行计算,形成安全可信的传递匿名通信系统。由于可信计算模式下 P2P 匿名通信系统的研究具有重要意义,因此,信息安全的问题受到人们和许多专家的关注,同时取得一定的研究成果[4-5]。

现有的 P2P 匿名通信系统设计方法有:文献[6]提出一种基于 DHT 的 P2P 匿名通信系统设计方法。该方法中使用上下两成的混合式拓扑结构,上层匿名通信系统为全分布非结构化拓扑,下层匿名通信系统为中心化拓扑,形成相对稳定的拓扑结构,同时引入 DHT 算法,形成匿名通信网络内部分成机制,保障匿名通信系统负载均衡,而且系统中匿名通信算法提升节点之间通信的可靠性。该方法能很好地发挥 P2P 网络的优势,同时一定程度上解决了 P2P 网络的不足,但该方法无法解决匿名通信系统信息查找困难、节点管理困难的问题。文献[7]提出一种基于可分级的 P2P 匿名通信系统设计方法。该方法将匿名通信系统分为两大模块,分级模块和信任值模块,分级匿名通信模块利用“高匿名等级,高匿名性,高负载”的匿名通信思想,实现各个模块之间的衔接和融合,同时结合匿名等级对现有的匿名通信系统进行优化和改进,再利用 MFC 界面编程和 Socket 链接通信,Socket 通信等技术实现了

收稿日期:2017-04-18; **修回日期**:2017-05-07。
基金项目:广东省省级科技计划项目(2013B010204019)。
作者简介:雷 涛(1973-),女,四川成都人,博士研究生,讲师,主要从事信息安全方向的研究。

“集中处理，分层传递”的匿名通信系统信任机制软件构架，构建匿名通信系统的模型。该方法使得 P2P 匿名通信系统具有一定的灵活性和可靠性，但该方法设计的 P2P 匿名通信系统不能满足用户的自主选择性。文献［8］提出一种基于信誉度计算的 P2P 匿名通信系统设计方法。该方法在现有的匿名通信系统上进行信誉度评价改进，以匿名通信过程中通信时间作为信誉度向量权重变化的参考量，再对当前节点的信任度进行评价，以节点信任度的经验值及其变化趋势来评价，同时将匿名通信系统中匿名服务进行分级，满足不同用户的需求，最后通过分成加密方法和非对称加密的方法对将要传递的数据进行打包加密，完成数据的安全传递。该方法提高了 P2P 匿名通信系统的匿名度，但该方法设计的 P2P 匿名通信系统的节点稳定程度较低，影响了通信信息的传递效率[9-10]。

针对上述问题，提出一种基于可信计算模式的 P2P 匿名通信系统设计方法。实验仿真证明，该方法在保证该系统数据传递的效率的同时提高了匿名通信系统的安全性与可靠性。

1　可信计算模式下 P2P 匿名通信系统设计

1.1　可信计算模式下 P2P 匿名通信硬件系统设计

本文提出可信计算模式的 P2P 匿名通信系统，该系统为网络用户提供了一个安全可靠的信息交流平台，系统的硬件结构如图 1 所示。

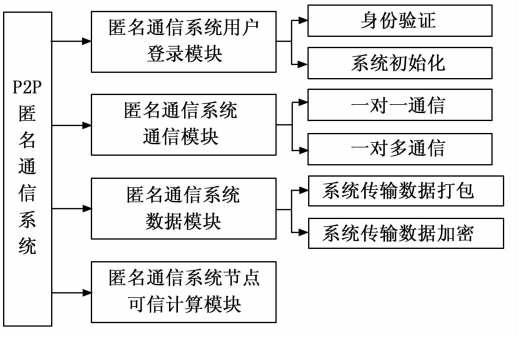

图 1　P2P 匿名通信系统硬件结构图

在用户登入匿名通信系统时，首先通过用户登录模块进行身份的验证，在 P2P 匿名通信网络中记录登录状态，如果是首次登录的情况下，系统将建立一个配置文件，将用户名、密码信息存入该文件中。登入成功后 P2P 匿名通信网络将自动进行初始化操作。匿名通信系统中网络通信模块起到节点之间交互的作用。可以一对一交互信息，也可以一对多交互资源。数据模块负责将要传递的数据进行打包，并对数据包进行加密。而可信计算模块是整个系统中计算量最大的模块，主要负责计算匿名通信系统的可信度与安全度。

1.2　可信计算模式下 P2P 匿名通信软件系统设计

首先对 P2P 匿名通信系统的匿名通道进行设计，假设 L 是匿名通信系统中新增的属性，该属性描述了数据包的生命周期；M 是匿名通信系统中已经传递的匿名数据包；A 表示接收匿名数据包目的地地址；目的地的签注密钥的公共密钥为 K_a，K_i 为可信计算签注密钥的公共密钥，因此有下列表达式：

$$L_1,K_1[R_1,K_a(R_0,M),A]\rightarrow L_2,K_a[(R_0,M),A] \quad (1)$$

式中，L_1 为已发送的匿名数据包在没经过可信计算之前的生命周期；L_2 为已发送的匿名数据包经过可信计算之后的生命周期；R_1、R_0 是 P2P 匿名通信系统中附加的匿名数据包，是用来保证数据包传递前后一致性。建立一个可信计算的联接，称之为可信计算匿名通道。在 P2P 系统中有许多可供可信计算的节点，在数据包传递之前，这些节点将通过可信计算来计算匿名通道的可信性，数据包沿着已经计算过的匿名通道进行传递，但在数据包传递时，在通道中数据包将要经过的节点必须在线，否则数据包传递将失败。

数据包在未传递之前，应该按照 P2P 匿名通信系统中匿名通道节点的个数，对数据进行层次性打包，将要传递的数据包放在最内层，并且将该数据包进行加密，只有相关结点的签注密钥才能将其打开。以这种方法层层打包数据，并通过各个节点，当该数据包达到最后一个节点时，即目的地节点，以该节点的签注密钥进行解密。在 P2P 匿名通信系统中数据包的格式如图 2 所示。

The eype of the package	Life time	The encryptde information about routing

图 2　数据包格式

匿名通道中每个节点都将接到一个数据包，并用签注密钥对已经加密的数据包进行解密，然后根据 P2P 匿名通信系统的指示进行转发。则数据包的传递过程为：

$$\begin{aligned}&L_1,K_n[R_n,K_{n-1}(R_{n-1},\ldots,K_2(R_2,K_1(R_1,K_a(R_0,M),A))\ldots)]\\&\rightarrow L_2,K_{n-1}[R_{n-1},\ldots,K_2(R_2,K_1(R_1,K_a(R_0,M),A))\ldots]\\&\rightarrow\ldots\ldots\ldots\rightarrow L,K(R,M),A\end{aligned} \quad (2)$$

当 A 是可信计算匿名网络通道节点的地址时，已传递的数据包将由该节点接收，数据包只有两种状态，一种状态是数据包已达到目的节点；另一种状态是数据包生命周期已到期被抛弃。

P2P 匿名通信系统中有相应的储存节点，当储存节点不在线时目的节点将进行缓存，当时间过长时，会将数据传递给相邻的节点进行保存，需要查询数据时，目的节点会向相邻节点发出查询请求，同时获取相关的更新信息。

1.3　可信计算模式下 P2P 匿名通信系统可信度计算

P2P 匿名通信系统中，每个节点都将保护用户个人隐私，为了使 P2P 匿名通信系统中没有泄密的网络节点，通过可信度计算来计算匿名通信系统的各个节点是否可信。

假设 P2P 匿名通信系统节点数为 n，系统中还将设立 m 个系统登入口，且 $m<n$，将系统中所有节点平均分为 g 个组，假设每个组中包含 c 个泄密节点，z 个自私节点。为了方便计算 P2P 匿名通信系统的安全性，将引用匿名通信协议。假设 I 匿名通信通道上第 1 个泄密节点的前驱节点恰是发送源的事件；H_k 且 $k\geqslant 1$ 表示匿名通信通道上第 1 个泄密节点占据匿名通道节点第 k 个位置的事件；则有第 1 个泄密节点占匿名通道节点据第 k 个位置之后（包括第 k 个位置）的事件公式为：

$$H=H_1+H_2+\ldots+H_k \quad (3)$$

式中，$P(I/H)$ 表示 P2P 匿名通信系统中有泄密者的情况，并准确猜出数据包发送源的概率。匿名通信系统中可信的节点有 $n+m+z$ 个，设发送源的可信值为 e，匿名通道的长度为 $k+1$，假设：

$$n+m+z=t \quad (4)$$

$$\frac{n+m+z+c}{n+m+z}=q \tag{5}$$

当 $e=10$ 时，则以最高可信度值计算 P2P 匿名通信系统中安全度，第 1 个泄密节点位于匿名通道第 i 个节点位置的概率为：

$$P(H_i)=\frac{c}{n+m+z}\left(\frac{n+m+z+c}{n+m+z}\right)^{i-1}=(1-q)q^{i-1} \tag{6}$$

匿名通信系统中第 1 个泄密节点在第 1 个匿名通信节点位置或之后的概率为：

$$P(H_1)=\sum_{i=1}^{k}P(H_i)=1-q^k \tag{7}$$

匿名通信系统中第 2 个泄密节点在第 2 个匿名通信节点位置或之后的概率为：

$$P(H_2)=\sum_{i=2}^{k}P(H_i)=q(1-q^{k-1}) \tag{8}$$

当匿名通信系统中第 1 个泄密者位于第 1 个匿名通信节点位置时，它前一个节点一定是数据包的发送源，则事件 I 成立，因此，得到 $P(I/H)=1$。当匿名通信系统中第 1 个泄密者位于第 2 个匿名通信节点位置或之后时，它前一个匿名通信系统节点是数据包发送源的概率是 $1/(t-c)$，匿名通信系统中出现非匿名节点的概率是相同的，即：

$$P(I/H)=\frac{1}{t-c} \tag{9}$$

$$P(I)=P(H_1)P(I/H_1)+P(H_2)P(I/H_2)=(1-q)+q(1-q^{k-1})\frac{1}{t-c} \tag{10}$$

$$P(I/H_1)=\frac{P(\Lambda H_1)}{P(H_1)}=\frac{1}{\sum_{i=0}^{k-1}q^i}+\frac{q(1-q^{k-1})}{(t-c)(1-q^{k-1})} \tag{11}$$

因为式中 $q\leqslant 1$，所以 $1-q^{k-1}<1-q^k$，因此，当满足公式 (11) 时，则有：

$$\sum_{i=0}^{k-1}q^i\geqslant 2+\frac{4}{t-2} \tag{12}$$

$$P(I/H)\leqslant\frac{1}{2} \tag{13}$$

即 P2P 匿名通信系统达到可信安全的程度。

2 实验与分析

该实验将在 Xen 隔离 Compartment 的平台上进行，该系统采用 TPM 安全芯片、源虚拟机监控器 Xen－3.0.2、匿名通信系统可信服务层的 TCMG、TSMG、MA 等模块。在 P2P 匿名通信系统中，系统匿名性以匿名通信系统的可信度来进行评估。假设 $N(N>1)$ 为 P2P 匿名通信系统的规模，S 为匿名通信系统中数据泄密的情况下系统的规模，$H(X)$ 为匿名通信系统的熵值，p_i 为匿名通信系统中第 i 个节点被认为发送源的概率。推断发送源的方法一般采用排除法，以泄密节点为中心，排除附近不可能的节点，获得一个较小的集合，再进行最终的判断。在不考虑泄密节点的情况下，匿名通信系统的可信度可以表示为：

$$D(X)=\frac{H(X)}{H^*(X)}=\frac{-\sum_{n=1}^{S}p_i\log_2(p_i)}{-\sum_{n=1}^{N}p_i\log_2(p_i)}=\frac{-\sum_{n=1}^{S}\frac{1}{S}\log_2\left(\frac{1}{S}\right)}{-\sum_{n=1}^{N}\frac{1}{N}\log_2\left(\frac{1}{N}\right)}=\frac{\log_2(S)}{\log_2(N)} \tag{14}$$

式中，$H^*(X)$ 表示匿名通信系统在没有泄密节点情况下的理想熵值。

通过上述公式的定义可以得出匿名通信系统的可信度与匿名通信系统中每个节点的区分度有关。匿名通道中节点区分度越大，数据泄密的越多，熵值越小，因此系统的可信度越弱，反之匿名通道中节点区分度越小，数据泄密的越少，熵值越大，因此系统的可信度越强。如果可以保持匿名通信系统中节点在一个较的小区分度内，则提高匿名通信系统的可信性。则 S 越大，匿名通信系统的可信度越高。而利用本文提出的可信度计算方法，可以计算出该节点的可信性，同时对节点进行再次加密。

P2P 匿名通信系统节点数为 n，其中有 B 个节点经过可信计算，在 x 个周期后，攻击者收集到匿名通信系统中可疑的 IP 地址数量为 $n+(x-1)B$ 个，在泄密节点存在的情况下，匿名通信系统的可信度可以表示为：

$$D(X)=\frac{H(X)}{H^*(X)}=\frac{\log_2[S+S(x-1)B/n]}{\log_2[n+(x-1)B]} \tag{15}$$

图 3 显示出 S 减小后匿名通信系统可信度的变化情况。与当前使用的匿名通信系统相比，该匿名通信系统随着使用的时间变长，可信度减少现象变慢，这种现象相对于 P2P 匿名通信系统来讲是一个有意义的结果，匿名通信系统使用的时间越长，产生的 IP 地址会越多，IP 地址越多分析难度越大，并延长匿名通信系统的分析时间，因此，使得匿名通信系统的可信度增加，在极端的情况下，目的节点将自己已知节点广播给相邻的两个节点，从而实现相邻节点之间的信息交互，使得匿名通信系统中节点获得更多的邻居。当 $S=1$ 时，对于当前使用的匿名通信系统来说，攻击者已经找到发送源节点，即 $D(X)=0$，而对 P2P 匿名通信系统而言，攻击者只是找到了发送源节点所在的网段，发送源节点并没有完全的暴露，即发送信息与发送者的隐私没有暴露。

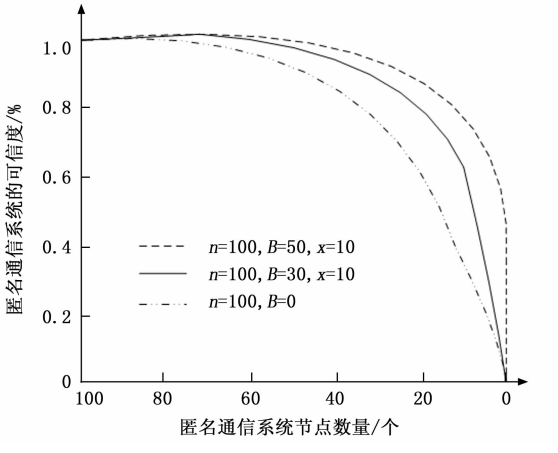

图 3 可信度与匿名通信系统规模的关系

而影响匿名通信系统可信度与安全度的还有 TCP 匿名网络通道连接。当一个匿名通信节点与一个主机构建一个 TCP

匿名网络通道连接，为了保证数据传递的过程中 TCP 匿名通道不被切断，过期的匿名通信网络节点也会被继续使用，过期的节点仅被以前建立的匿名通道使用，新建立的 TCP 匿名通道连接，还是需要使用新的匿名通道节点，在这种情况下即使攻击者获得相关的网络节点之间的联系，也仅仅解除了发送源节点第一层加密，攻击者的攻击对匿名通信系统整体影响并不大，因此，可以认为本文的方法起到一定的作用。

我们不仅对 P2P 匿名通信系统的安全性进行了实验，而且对本系统的性能也进行了相关的实验，在保证匿名通信系统可靠性与安全性的同时，该系统是否可以保证匿名通信系统的传递效率，因此，展开匿名通信系统传递效率的实验。

虽然该系统的可信度、安全度较强，但匿名通信系统传递的效率也是广大使用者关注的热点之一，是否在保证安全可靠的匿名通信的前提下，提高匿名通信系统的传递效率。影响传递效率的主要因素有传递数据的大小、传递通道中经过的节点个数（中间节点）、IP 地址的冲突。前两个因素一直是匿名通信效率研究关注的重点，本实验也将关注 IP 地址的冲突的研究。

该实验通过理论与实践的方法证明 IP 地址冲突的冲突率。首先，在北京大学校园中 DHCPv5 服务器中申请了 150 个连续的 IP 地址作为 SIP 地址，利用这 150 个地址生成可变的 IP 地址，为了保证实验的严谨性，经过 2000 次的循环实验，得到的结果显示，这 150 个 IP 地址之间并没有出现冲突，可以认为在该网段中，不会因为 IP 地址冲突导致匿名通信系统数据传递效率，因此推断在 P2P 匿名通信系统中 IP 地址的变更不会造成大量的 IP 地址冲突，影响匿名通信系统的数据传递效率。

此外，还对其他两个因素进行研究，首先将北大的匿名通信节点在北大的校园网中进行匿名通信效率的测试，图 4 表示匿名通道中节点的个数对匿名通信系统传递效率的影响，图 4 还同时显示了传递数据包大小对匿名通信系统传递效率的影响，而数据包越大，经过匿名通道中间节点越多，匿名通信系统传递的效率越低，数据包越大匿名通信系统传递得到时间越长，这是不可避免的问题。但是与当前匿名通信系统相比，传递效率有显著的提高。

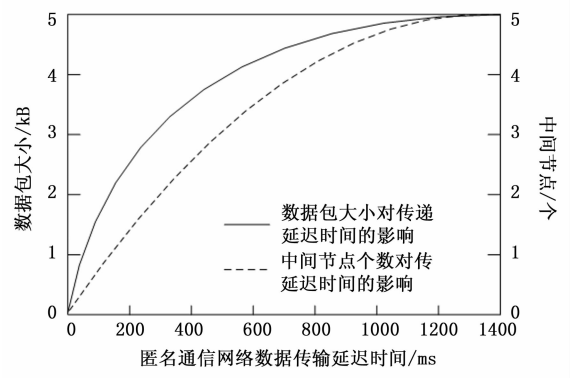

图 4　传递延迟与中间节点及数据包大小的关系

表 1 给出了当前匿名通信系统与 P2P 匿名通信系统数据传递延迟的比较结果，表中的延迟数值是从匿名通信系统起始节点发出请求到请求内容传递回来的时间。

表 1　当前系统与 P2P 系统数据包传递延迟时间比较

数据包大小/KB	匿名通信系统	传递延迟时间/s				
		1 个中途节点	2 个中途节点	3 个中途节点	4 个中途节点	5 个中途节点
1	当前系统	265	427	625	824	1025
	P2P 系统	152	254	502	625	901
2	当前系统	281	524	634	846	1109
	P2P 系统	198	295	538	694	964
3	当前系统	301	564	682	863	1180
	P2P 系统	205	340	562	719	996
4	当前系统	324	592	709	916	1246
	P2P 系统	264	367	624	758	1052
5	当前系统	354	637	756	1054	1342
	P2P 系统	290	451	687	8035	1108

从表 1 中可知 P2P 匿名通信系统要比当前系统的延迟时间短，而且因为当前系统已经被广大用户认可，所以可以认为本文可信技术模式下 P2P 匿名通信系统设计可以满足匿名通信系统的基本需求。

3　结论

针对当前使用的方法，无法在用户节点匿名的前提下，保证 P2P 匿名通信系统的匿名节点可信性。本文提出一种基于可信计算模式 P2P 匿名通信系统设计方法。仿真实验结果表明，所提方法在保证该系统数据传递效率的同时提高了匿名通信系统的安全性与可靠性。

参考文献：

[1] 王少辉，蒋季宏，肖　甫. 基于重路由匿名通信系统的设计 [J]. 计算机科学，2016，43 (10)：154 - 159.

[2] 谭庆丰，方滨兴，时金桥，等. StegoP2P：一种基于 P2P 网络的隐蔽通信方法 [J]. 计算机研究与发展，2014，51 (8)：1695 - 1703.

[3] 韩祺祎，任梦吟，文　红. 基于拓扑势的 P2P 社区推荐信任模型 [J]. 电子与信息学报，2015，37 (6)：1279 - 1284.

[4] 王嘉慧，程久军. P2P 模式下基于网格扩增的位置匿名算法 [J]. 计算机科学，2014，41 (4)：90 - 94.

[5] 罗　健，廖俊国，李　雄. P2PSpaceTwist：一种主动式用户协作的位置隐私保护方法 [J]. 计算机工程与科学，2016，38 (8)：1661 - 1668.

[6] 周　璇，宦国强，宋占杰. 基于 P2P 网络的机顶盒 VoD 系统条件接收机制 [J]. 计算机科学，2015，42 (4)：72 - 75.

[7] 王昱华，江　林，胡志刚，等. 基于 DHT 的 P2P 系统负载均衡算法 [J]. 计算机工程与应用，2015，51 (23)：100 - 105.

[8] 曾明霏，余顺争. 使用虚拟参与人和博弈论的 P2P 网络信用系统模型 [J]. 小型微型计算机系统，2014，35 (6)：1309 - 1314.

[9] 刘晓坦，李晓雯，崔　翔. 基于可信计算的多级安全策略研究 [J]. 电子设计工程，2016，24 (7)：148 - 150.

[10] 谭庆丰，时金桥，方滨兴，等. 匿名通信系统不可观测性度量方法 [J]. 计算机研究与发展，2015，52 (10)：2373 - 2381.