(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109413025 A
(43)申请公布日 2019.03.01

(21)申请号 201810986072.6

(22)申请日 2018.08.28

(71)申请人 浙江工业大学
地址 310014 浙江省杭州市下城区朝晖六区潮王路18号

(72)发明人 李章维 宋焦朋 魏遥 姚飞 周晓根 张贵军

(74)专利代理机构 杭州斯可睿专利事务所有限公司 33241
代理人 王利强

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/06(2006.01)
H04L 12/58(2006.01)

权利要求书2页 说明书6页 附图2页

(54)发明名称

一种基于Socket的实时通讯方法

(57)摘要

一种基于Socket的实时通讯方法，首先，针对数据信息传输问题，分析在数据流量大的时候会存在对服务器造成很大的压力，发生信息阻塞，维护成本高等不足，通过研究分析Socket通讯具备的数据传输的优势，将其引入系统中；其次，结合P2P技术和AES加密算法，提出一种信息收发速度快、保密性好、占用网络带宽资源低的通讯方法。本发明提供一种便捷、高效的基于Socket的实时通讯方法。

CN 109413025 A

1.一种Socket的实时通讯方法,其特征在于,所述实时通讯方法包括以下步骤:

1)创建Socket对象的实例,确定Socket的参数类型和Socket使用的网络协议;

2)选用TCP/IP网络通信协议,TCP协议为数据的进程提供虚电路和传输服务,IP协议负责为数据的网络层提供服务;

3)引入P2P技术,采用P2P和B/S架构模式相结合的方式,首先使用B/S模式获得用户的IP地址和通讯端口,然后用户与用户之间使用P2P技术进行通讯;

4)数据传输加密,发送方数据经AES算法进行加密处理,然后将加密内容发送到网络中,接收方获取网络中的密文信息后,调用AES算法进行解密处理,在计算机之间用Socket进行通信时,实现明文查看,密文传输的功能;过程如下:

4.1)加密过程,在AES算法中使用128位的密钥对数据加密,经过下述的3个步骤得到AESCBC128位的加密密文,过程如下:

4.1.1)字节替换,将一个由16×16字节组成状态矩阵S(x),共256个元素构成S盒,每个元素字节中的高4位作为x值,低4位作为y值,S盒中对应的x和y的元素值就是替换结果;

4.1.2)行位移,将状态矩阵S(x)分组为4×4的矩阵,以循环左移的方式来改变元素的位置,即第n行左移n个字节;重排列后得到一个新的矩阵B(x);

4.1.3)列混合,将状态矩阵S(x)中的每一列与一个固定的多项式相乘,如公式(1)所示:

$$\begin{aligned} S'_{0,c} &= (2\cdot S_{0,c})\oplus(3\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{1,c} &= (1\cdot S_{0,c})\oplus(2\cdot S_{1,c})\oplus(3\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{2,c} &= (1\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(2\cdot S_{2,c})\oplus(3\cdot S_{3,c}) \\ S'_{3,c} &= (3\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(2\cdot S_{3,c}) \end{aligned} \qquad (1)$$

如公式(1)所述,得到新的状态矩阵S′(x),如公式(2)所示:

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \qquad (2)$$

其中,元素{01},{02},{03}是S盒中固定的域元素,S′(x)为列混合矩阵;

4.2)解密过程:经过以下3个解密过程,完成对密文的解密,获取发送的明文,过程如下:

4.2.1)逆行位移:将密文分组成4×4的矩阵,与加密相反,第n行右移n个字节,得到矩阵C(x);

4.2.2)逆列混合:将状态矩阵S(x)逐列与一个固定多项式相乘,得到矩阵S″(x),如公式(2)所示::

$$\begin{bmatrix} S''_{0,c} \\ S''_{1,c} \\ S''_{2,c} \\ S''_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad (2)$$

其中,{09},{0B},{0D},{0E}为S盒中固定的域元素;

4.2.3)逆字节替换:将每个元素字节中的高4位作为x′值,低4位作为y′值,得到替换的逆S盒;

5)添加系统服务器,将服务器分为登录模块和监听模块,在用户使用输入账号和密码登录系统时,将账号和密码发送到服务器,验证其合法性;在用户之间进行相互通讯时,监听模块负责不断地监听发来的请求,按照请求做相应的操作;

6)实时通讯的实现:用户在发送文件、文字等数据信息时,首先获取对方的IP和TCP端口,使用P2P技术,直接和对方建立连接,启动数据传输线程,使用AES算法对数据信息进行加密传输,如果传送文件,但对方长时间没有接受,将文件暂存到系统服务器中,然后经过AES算法解析,是对方查看到明文信息。

一种基于Socket的实时通讯方法

技术领域

[0001] 本发明涉及一种实时通讯、数据传输、通讯协议、计算机应用领域，尤其涉及的是一种基于Socket的实时通讯方法。

背景技术

[0002] 随着全球信息化进程的不断发展，网络也在飞速发展。出于高效、快速地处理各种事务的目的，越来越多的行业在其内部使用局域网来进行工作。在内部局域网的帮助下，可以简化信息流程，提高信息交换的速度，从而提高工作效率。然而，随着信息数据规模的扩大，数据传输量的增加，在局域网上运行的应用越来越多，如知识库、网络会议、数据库应用和数据的同步与备份等，这些应用局域网的信息吞吐、处理能力的要求也越来越高。这些在内部原有局域网设计之初未曾考虑到的新情况的出现使得局域网不堪重负，容易发生信息阻塞，此时，局域网不但不能提高效率，反而成为发展的瓶颈。

[0003] 为了解决上述矛盾，人们提出了许多方法。提升网络带宽及增加服务器的吞吐能力是解决此矛盾的一种方法。然而，从运行的成本方面考虑，无论是单纯地提升网络带宽或增加服务器的吞吐能力都不能从根本上解决局域网资源紧张的问题，对旧有局域网的大规模硬件改造反而会增加成本的负担。

[0004] 基于Socket的局域网即时通讯工具是此类局域网通讯软件的具体实例之一，它很好地诠释了Socket通讯的原理，并且在通讯、教学、讨论等应用中都具有一定的实用价值。它具有信息收发速度快，保密性好，占用网络带宽资源低，占用服务器吞吐能力低，易于编程实现等优点。

[0005] 基于Socket的局域网通讯软件应用范围广阔，不但可以处理传统的通讯需求，而且也能扩展以适应新型的网络应用，如网络教育，数据影音传输等，拥有广泛的应用前景。

[0006] 基于Socket的局域网即时通讯软件可以为原有的局域网提供一种良好，安全，快速的通信机制。它的实现无需对原有的局域网硬件进行任何改动，具有实现成本低廉的优点，它的使用能有效地降低局域网通信负荷，提高局域网的使用效率，可以很好地解决各种通讯需求。

[0007] 因此，通过对目前局域网实时通讯方法的研究，发现在数据流量大的时候会存在对局域网和服务器造成很大的压力，发生信息阻塞，维护成本高的缺陷，需要改进。

发明内容

[0008] 为了克服目前实时通讯中存在的信息阻塞、传输效率低、高成本等不足，本发明利用Socket传输和P2P相结合的技术，引入AES加密算法，提供一种信息收发速度快，保密性好，占用网络带宽资源低的基于Socket的实时通讯方法。

[0009] 本发明解决其技术问题所采用的技术方案是：

[0010] 一种基于Socket的实时通讯方法，所述实时通讯方法包括以下步骤：

[0011] 1)创建Socket对象的实例，确定Socket的参数类型和Socket使用的网络协议；

[0012] 2)选用TCP/IP网络通信协议,TCP协议为数据的进程提供虚电路和传输服务,IP协议负责为数据的网络层提供服务;

[0013] 3)引入P2P技术,采用P2P和B/S架构模式相结合的方式,首先使用B/S模式获得用户的IP地址和通讯端口,然后用户与用户之间使用P2P技术进行通讯;

[0014] 4)数据传输加密,发送方数据经AES算法进行加密处理,然后将加密内容发送到网络中,接收方获取网络中的密文信息后,调用AES算法进行解密处理,在计算机之间用Socket进行通信时,实现明文查看,密文传输的功能;过程如下:

[0015] 4.1)加密过程,在AES算法中使用128位的密钥对数据加密,经过下述的3个步骤得到AESCBC128位的加密密文,过程如下:

[0016] 4.1.1)字节替换,将一个由16×16字节组成状态矩阵S(x),共256个元素构成S盒,每个元素字节中的高4位作为x值,低4位作为y值,S盒中对应的x和y的元素值就是替换结果;

[0017] 4.1.2)行位移,将状态矩阵S(x)分组为4×4的矩阵,以循环左移的方式来改变元素的位置,即第n行左移n个字节;重排列后得到一个新的矩阵B(x);

[0018] 4.1.3)列混合,将状态矩阵S(x)中的每一列与一个固定的多项式相乘,如公式(1)所示:

[0019]
$$\begin{aligned} S'_{0,c} &= (2\cdot S_{0,c})\oplus(3\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{1,c} &= (1\cdot S_{0,c})\oplus(2\cdot S_{1,c})\oplus(3\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{2,c} &= (1\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(2\cdot S_{2,c})\oplus(3\cdot S_{3,c}) \\ S'_{3,c} &= (3\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(2\cdot S_{3,c}) \end{aligned} \qquad (1)$$

[0020] 如公式(1)所述,得到新的状态矩阵S′(x),如公式(2)所示:

[0021]
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \qquad (2)$$

[0022] 其中,元素{01},{02},{03}是S盒中固定的域元素,S′(x)为列混合矩阵;

[0023] 4.2)解密过程:经过以下3个解密过程,完成对密文的解密,获取发送的明文,过程如下:

[0024] 4.2.1)逆行位移:将密文分组成4×4的矩阵,与加密相反,第n行右移n个字节,得到矩阵C(x);

[0025] 4.2.2)逆列混合:将状态矩阵S(x)逐列与一个固定多项式相乘,得到矩阵S″(x),如公式(2)所示::

[0026] $$\begin{bmatrix} S''_{0,c} \\ S''_{1,c} \\ S''_{2,c} \\ S''_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad (2)$$

[0027] 其中,{09},{0B},{0D},{0E}为S盒中固定的域元素;

[0028] 4.2.3)逆字节替换:将每个元素字节中的高4位作为x′值,低4位

[0029] 作为y′值,得到替换的逆S盒;

[0030] 5)添加系统服务器,将服务器分为登录模块和监听模块,在用户使用输入账号和密码登录系统时,将账号和密码发送到服务器,验证其合法性;在用户之间进行相互通讯时,监听模块负责不断地监听发来的请求,按照请求做相应的操作;

[0031] 6)实时通讯的实现:用户在发送文件、文字等数据信息时,首先获取对方的IP和TCP端口,使用P2P技术,直接和对方建立连接,启动数据传输线程,使用AES算法对数据信息进行加密传输,如果传送文件,但对方长时间没有接受,将文件暂存到系统服务器中,然后经过AES算法解析,是对方查看到明文信息。

[0032] 本发明的有益效果主要表现在:本发明实时通讯方法使用Socket传输和P2P相结合的技术,引入AES加密算法,实现实时通讯的目的,且信息收发速度快,保密性好,占用网络带宽资源低。

附图说明:

[0033] 图1是一种基于Socket实时通讯方法的流程图;

[0034] 图2是S盒子的字节替换过程图。

具体实施方式

[0035] 下面结合附图对本发明做进一步说明。

[0036] 参照图1和图2,一种基于Socket实时通讯方法,包括以下步骤:

[0037] 1)创建Socket对象的实例,确定Socket的参数类型和Socket使用的网络协议;

[0038] 2)选用TCP/IP网络通信协议,TCP协议为数据的进程提供虚电路和传输服务,IP协议负责为数据的网络层提供服务;

[0039] 3)引入P2P技术,采用P2P和B/S架构模式相结合的方式,首先使用B/S模式获得用户的IP地址和通讯端口,然后用户与用户之间使用P2P技术进行通讯;

[0040] 4)数据传输加密,发送方数据经AES算法进行加密处理,然后将加密内容发送到网络中,接收方获取网络中的密文信息后,调用AES算法进行解密处理,在计算机之间用Socket进行通信时,实现明文查看,密文传输的功能;过程如下:

[0041] 4.1)加密过程,在AES算法中使用128位的密钥对数据加密,经过下述的3个步骤得到AESCBC128位的加密密文,过程如下:

[0042] 4.1.1)字节替换,将一个由16×16字节组成状态矩阵S(x),共256个元素构成S盒,每个元素字节中的高4位作为x值,低4位作为y值,S盒中对应的x和y的元素值就是替换结果;

[0043] 4.1.2)行位移,将状态矩阵S(x)分组为4×4的矩阵,以循环左移的方式来改变元素的位置,即第n行左移n个字节;重排列后得到一个新的矩阵B(x);

[0044] 4.1.3)列混合,将状态矩阵S(x)中的每一列与一个固定的多项式相乘,如公式(1)所示:

[0045]
$$\begin{aligned} S'_{0,c} &= (2\cdot S_{0,c})\oplus(3\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{1,c} &= (1\cdot S_{0,c})\oplus(2\cdot S_{1,c})\oplus(3\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{2,c} &= (1\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(2\cdot S_{2,c})\oplus(3\cdot S_{3,c}) \\ S'_{3,c} &= (3\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(2\cdot S_{3,c}) \end{aligned} \qquad (1)$$

[0046] 如公式(1)所述,得到新的状态矩阵S′(x),如公式(2)所示:

[0047]
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \qquad (2)$$

[0048] 其中,元素{01},{02},{03}是S盒中固定的域元素,S′(x)为列混合矩阵;

[0049] 4.2)解密过程:经过以下3个解密过程,完成对密文的解密,获取发送的明文,过程如下:

[0050] 4.2.1)逆行位移:将密文分组成4×4的矩阵,与加密相反,第n行右移n个字节,得到矩阵C(x);

[0051] 4.2.2)逆列混合:将状态矩阵S(x)逐列与一个固定多项式相乘,得到矩阵S″(x),如公式(2)所示::

[0052]
$$\begin{bmatrix} S''_{0,c} \\ S''_{1,c} \\ S''_{2,c} \\ S''_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \qquad (2)$$

[0053] 其中,{09},{0B},{0D},{0E}为S盒中固定的域元素;

[0054] 4.2.3)逆字节替换:将每个元素字节中的高4位作为x′值,低4位作为y′值,得到替换的逆S盒;

[0055] 5)添加系统服务器,将服务器分为登录模块和监听模块,在用户使用输入账号和密码登录系统时,将账号和密码发送到服务器,验证其合法性;在用户之间进行相互通讯时,监听模块负责不断地监听发来的请求,按照请求做相应的操作;

[0056] 6)实时通讯的实现:用户在发送文件、文字等数据信息时,首先获取对方的IP和TCP端口,使用P2P技术,直接和对方建立连接,启动数据传输线程,使用AES算法对数据信息进行加密传输,如果传送文件,但对方长时间没有接受,将文件暂存到系统服务器中,然后经过AES算法解析,是对方查看到明文信息。

[0057] 以一套教学管理系统为例,一种基于Socket的实时通讯方法,包括以下步骤:

[0058] 1)创建Socket对象的实例,确定Socket的参数类型和Socket使用的网络协议;

[0059] 2)选用TCP/IP网络通信协议,TCP协议为数据的进程提供虚电路和传输服务,IP协议负责为数据的网络层提供服务;

[0060] 3)引入P2P技术,采用P2P和B/S架构模式相结合的方式,首先使用B/S模式获得用户的IP地址和通讯端口,然后用户与用户之间使用P2P技术进行通讯;

[0061] 4)数据传输加密,发送方数据经AES算法进行加密处理,然后将加密内容发送到网络中,接收方获取网络中的密文信息后,调用AES算法进行解密处理,在计算机之间用Socket进行通信时,实现明文查看,密文传输的功能;过程如下:

[0062] 4.1)加密过程,在AES算法中使用128位的密钥对数据加密,经过下述的3个步骤得到AESCBC128位的加密密文,过程如下:

[0063] 4.1.1)字节替换,将一个由16×16字节组成状态矩阵S(x),共256个元素构成S盒,每个元素字节中的高4位作为x值,低4位作为y值,S盒中对应的x和y的元素值就是替换结果;

[0064] 4.1.2)行位移,将状态矩阵S(x)分组为4×4的矩阵,以循环左移的方式来改变元素的位置,即第n行左移n个字节;重排列后得到一个新的矩阵B(x);

[0065] 4.1.3)列混合,将状态矩阵S(x)中的每一列与一个固定的多项式相乘,如公式(1)所示:

[0066]
$$\begin{aligned} S'_{0,c} &= (2\cdot S_{0,c})\oplus(3\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{1,c} &= (1\cdot S_{0,c})\oplus(2\cdot S_{1,c})\oplus(3\cdot S_{2,c})\oplus(1\cdot S_{3,c}) \\ S'_{2,c} &= (1\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(2\cdot S_{2,c})\oplus(3\cdot S_{3,c}) \\ S'_{3,c} &= (3\cdot S_{0,c})\oplus(1\cdot S_{1,c})\oplus(1\cdot S_{2,c})\oplus(2\cdot S_{3,c}) \end{aligned} \qquad (1)$$

[0067] 如公式(1)所述,得到新的状态矩阵S′(x),如公式(2)所示:

[0068]
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \qquad (2)$$

[0069] 其中,元素{01},{02},{03}是S盒中固定的域元素,S′(x)为列混合矩阵;

[0070] 4.2)解密过程:经过以下3个解密过程,完成对密文的解密,获取发送的明文,过程如下:

[0071] 4.2.1)逆行位移:将密文分组成4×4的矩阵,与加密相反,第n行右移n个字节,得到矩阵C(x);

[0072] 4.2.2)逆列混合:将状态矩阵S(x)逐列与一个固定多项式相乘,得到矩阵S″(x),如公式(2)所示::

[0073] $$\begin{bmatrix} S''_{0,c} \\ S''_{1,c} \\ S''_{2,c} \\ S''_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad (2)$$

[0074] 其中,{09},{0B},{0D},{0E}为S盒中固定的域元素;

[0075] 4.2.3)逆字节替换:将每个元素字节中的高4位作为x′值,低4位作为y′值,得到替换的逆S盒;

[0076] 5)添加系统服务器,将服务器分为登录模块和监听模块,在用户使用输入账号和密码登录系统时,将账号和密码发送到服务器,验证其合法性;在用户之间进行相互通讯时,监听模块负责不断地监听发来的请求,按照请求做相应的操作;

[0077] 6)实时通讯的实现:用户在发送文件、文字等数据信息时,首先获取对方的IP和TCP端口,使用P2P技术,直接和对方建立连接,启动数据传输线程,使用AES算法对数据信息进行加密传输,如果传送文件,但对方长时间没有接受,将文件暂存到系统服务器中,然后经过AES算法解析,是对方查看到明文信息。

[0078] 以上阐述的是本发明给出的一个实施例展现出来的一个优良结果,显然本发明不仅适合上述实施例,在不偏离本发明基本精神及不超出本发明实质内容所涉及内容的前提下可对其做种种变化加以实施。

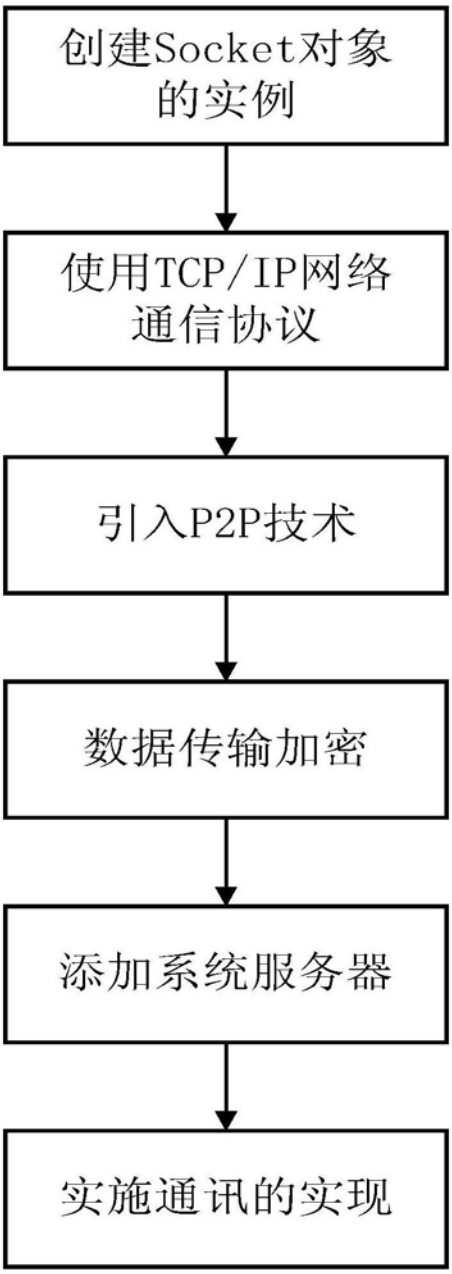
创建Socket对象的实例
使用TCP/IP网络通信协议
引入P2P技术
数据传输加密
添加系统服务器
实施通讯的实现

图1

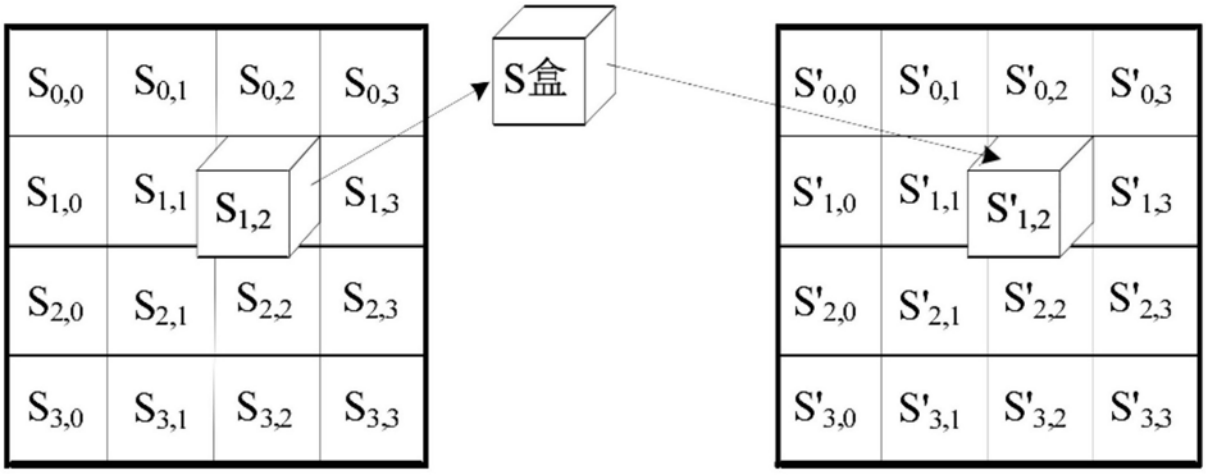
S0,0 S0,1 S0,2 S0,3
S1,0 S1,1 S1,2 S1,3
S2,0 S2,1 S2,2 S2,3
S3,0 S3,1 S3,2 S3,3
S盒
S'0,0 S'0,1 S'0,2 S'0,3
S'1,0 S'1,1 S'1,2 S'1,3
S'2,0 S'2,1 S'2,2 S'2,3
S'3,0 S'3,1 S'3,2 S'3,3

图2