(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 103281172 A
(43)申请公布日 2013.09.04

(21)申请号 201310175239.8

(22)申请日 2013.05.13

(71)申请人 天津市天安怡和信息技术有限公司
地址 300384 天津市滨海新区华苑产业区（环外）海泰发展五道16号创新基地B7

(72)发明人 战庆书 伞洪亮

(74)专利代理机构 天津市北洋有限责任专利代理事务所 12201
代理人 温国林

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 29/08(2006.01)

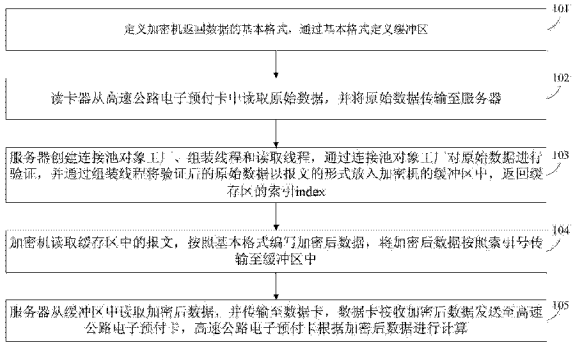
权利要求书2页 说明书7页 附图3页

(54)发明名称

高速公路电子预付卡与加密机之间的池化通信方法

(57)摘要

本发明公开了一种高速公路电子预付卡与加密机之间的池化通信方法，所述方法包括：定义加密机返回数据的基本格式，通过基本格式定义缓冲区；服务器创建连接池对象工厂、组装线程和读取线程，通过连接池对象工厂对原始数据进行验证，并通过组装线程将验证后的原始数据以报文的形式放入加密机的缓冲区中，返回缓存区的索引；加密机读取缓存区中的报文，按照基本格式编写加密后数据，将加密后数据按照索引传输至缓冲区中；服务器从缓冲区中读取加密后数据，并传输至读卡器，读卡器接收加密后数据发送至高速公路电子预付卡，高速公路电子预付卡根据加密后数据进行计算。本发明提高了加密的有效性，并且避免了系统资源的闲置，提高了工作效率。



CN 103281172 A

1. 一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述方法包括：

定义加密机返回数据的基本格式，通过所述基本格式定义缓冲区；

读卡器从高速公路电子预付卡中读取原始数据，并将所述原始数据传输至服务器；

所述服务器创建连接池对象工厂、组装线程和读取线程，通过所述连接池对象工厂对所述原始数据进行验证，并通过所述组装线程将验证后的原始数据以报文的形式放入所述加密机的缓冲区中，返回所述缓存区的索引；

所述加密机读取缓存区中的报文，按照所述基本格式编写加密后数据，将所述加密后数据按照索引传输至所述缓冲区中；

所述服务器从所述缓冲区中读取所述加密后数据，并传输至所述读卡器，所述读卡器接收所述加密后数据发送至所述高速公路电子预付卡，所述高速公路电子预付卡根据所述加密后数据进行计算。

2. 根据权利要求 1 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述定义加密机返回数据的基本格式的过程具体为：

第一和第二个字节拼成一个整数作为加密机返回数据的长度 n；

第三和第四个字节作为返回类型；

第五和第六个字节作为返回结果，结果状态‘0’‘0’表示加密成功；

加密结果长度为 n-6 个字节。

3. 根据权利要求 2 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述通过基本格式定义缓冲区的过程具体为：

设计缓冲区为 byte[X][Y]，每条返回结果作为一行，规划缓存区每一行的约定：

byte[i][0] 和 byte[i][1] 中存储字节的长度；

byte[i][2] 和 byte[i][3] 中存储加密返回类型’M’和’H’；

byte[i][4] 和 byte[i][5] 中存储返回结果状态，‘0’‘0’表示加密成功；

byte[i][6]--byte[i][Y] 中存储加密内容。

4. 根据权利要求 3 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述服务器创建连接池对象工厂、组装线程和读取线程，通过所述连接池对象工厂对所述原始数据进行验证，并通过所述组装线程将验证后的原始数据以报文的形式放入所述加密机的缓冲区中，返回所述缓存区的索引的过程具体为：

1）定义与所述加密机通讯的所述连接池对象工厂，并创建所述连接池对象工厂；

创建所述连接池对象工厂包括：生成对象、激活对象、销毁对象和验证对象；

2）通过所述生成对象生成所述连接池对象工厂中的通讯对象，所述通讯对象被使用后，通过所述激活对象激活所述通讯对象；

3）每次请求从所述连接池对象工厂中获取到所述通讯对象后，通过所述验证对象对所述通讯对象进行链接验证，若返回结果正确，则继续进行加密操作，否则，通过所述销毁对象销毁所述通讯对象，并获取新的通讯对象进行重新链接验证；

4）定义所述组装线程，所述组成线程用于对通过验证的原始数据进行组装，形成发送报文，放入到所述加密机的缓冲区中；

5）所述加密机返回缓冲区的索引至所述服务器，定义所述读取线程，所述读取线程用

于根据所述索引从缓冲区中读取所述加密后数据。

5. 根据权利要求 4 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述加密机读取缓存区中的报文，按照所述基本格式编写加密后数据，将所述加密后数据按照索引传输至所述缓冲区中的过程具体为：

填充前六个字节，以获得后续字节的长度 n-6，依据预设规则判定接收的报文是否发生错误，若发生了错误则彻底放弃这个通讯对象；将所述加密后数据按照所述索引传输至缓冲区中。

6. 根据权利要求 5 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述预设规则为：

加密计算的结果长度，不能大于定义的数据长度 n；加密机返回的结果内容是一个完整的数组。

7. 根据权利要求 5 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述方法还包括：

当所述读取线程等待超时后，所述服务器会先唤醒外部等待超时的所述读取线程，所述读取线程再获取所述加密后数据。

8. 根据权利要求 5 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述方法还包括：

当所述服务器超时未读取所述加密后数据时，所述读取线程通过所述销毁对象销毁所述通讯对象。

9. 根据权利要求 5 所述的一种高速公路电子预付卡与加密机之间的池化通信方法，其特征在于，所述方法还包括：

关闭整个服务的时，所述读取线程通过所述销毁对象把建立的所有通讯对象关闭销毁。

高速公路电子预付卡与加密机之间的池化通信方法

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种高速公路电子预付卡与加密机之间的池化通信方法。

背景技术

[0002] 高速公路预付卡的使用已经是未来高速公路收费的趋势，使得电子交易数据量越来越大，应用程序需要实时在线的处理数以千计的并发量，因此需要提高加密计算效率，合理利用加密机资源。

[0003] 现有技术中，高速公路预付卡与加密机之间的交互通常为：建立链接→发送加密指令→等待指定时间→从缓冲区读取→关闭连接。若加密机的等待时间设置太短，可能会导致读取数据不全；若加密机的等待时间设置较长，又会造成资源大量闲置，且每次加密都需重新连接；若业务并发量突然增大，可能会超过加密机连接数限制，无法正常工作。

发明内容

[0004] 本发明提供了一种高速公路电子预付卡与加密机之间的池化通信方法，本方法避免了系统资源的闲置，提高了工作效率，详见下文描述：

[0005] 一种高速公路电子预付卡与加密机之间的池化通信方法，所述方法包括：

[0006] 定义加密机返回数据的基本格式，通过所述基本格式定义缓冲区；

[0007] 读卡器从高速公路电子预付卡中读取原始数据，并将所述原始数据传输至服务器；

[0008] 所述服务器创建连接池对象工厂、组装线程和读取线程，通过所述连接池对象工厂对所述原始数据进行验证，并通过所述组装线程将验证后的原始数据以报文的形式放入所述加密机的缓冲区中，返回所述缓存区的索引；

[0009] 所述加密机读取缓存区中的报文，按照所述基本格式编写加密后数据，将所述加密后数据按照索引传输至所述缓冲区中；

[0010] 所述服务器从所述缓冲区中读取所述加密后数据，并传输至所述读卡器，所述读卡器接收所述加密后数据发送至所述高速公路电子预付卡，所述高速公路电子预付卡根据所述加密后数据进行计算。

[0011] 所述定义加密机返回数据的基本格式的过程具体为：

[0012] 第一和第二个字节拼成一个整数作为加密机返回数据的长度 n；

[0013] 第三和第四个字节作为返回类型；

[0014] 第五和第六个字节作为返回结果，结果状态‘0’‘0’表示加密成功；

[0015] 加密结果长度为 n-6 个字节。

[0016] 所述通过基本格式定义缓冲区的过程具体为：

[0017] 设计缓冲区为 byte[X][Y]，每条返回结果作为一行，规划缓存区每一行的约定：

[0018] byte[i][0] 和 byte[i][1] 中存储字节的长度；

[0019] byte[i][2] 和 byte[i][3] 中存储加密返回类型’M’和’H’；

[0020] byte[i][4] 和 byte[i][5] 中存储返回结果状态，‘0’‘0’表示加密成功；

[0021] byte[i][6]--byte[i][Y] 中存储加密内容。

[0022] 所述服务器创建连接池对象工厂、组装线程和读取线程，通过所述连接池对象工厂对所述原始数据进行验证，并通过所述组装线程将验证后的原始数据以报文的形式放入所述加密机的缓冲区中，返回所述缓存区的索引的过程具体为：

[0023] 1）定义与所述加密机通讯的所述连接池对象工厂，并创建所述连接池对象工厂；

[0024] 创建所述连接池对象工厂包括：生成对象、激活对象、销毁对象和验证对象；

[0025] 2）通过所述生成对象生成所述连接池对象工厂中的通讯对象，所述通讯对象被使用后，通过所述激活对象激活所述通讯对象；

[0026] 3）每次请求从所述连接池对象工厂中获取到所述通讯对象后，通过所述验证对象对所述通讯对象进行链接验证，若返回结果正确，则继续进行加密操作，否则，通过所述销毁对象销毁所述通讯对象，并获取新的通讯对象进行重新链接验证；

[0027] 4）定义所述组装线程，所述组成线程用于对通过验证的原始数据进行组装，形成发送报文，放入到所述加密机的缓冲区中；

[0028] 5）所述加密机返回缓冲区的索引至所述服务器，定义所述读取线程，所述读取线程用于根据所述索引从缓冲区中读取所述加密后数据。

[0029] 所述加密机读取缓存区中的报文，按照所述基本格式编写加密后数据，将所述加密后数据按照索引传输至所述缓冲区中的过程具体为：

[0030] 填充前六个字节，以获得后续字节的长度 n-6，依据预设规则判定接收的报文是否发生错误，若发生了错误则彻底放弃这个通讯对象；将所述加密后数据按照所述索引传输至缓冲区中。

[0031] 所述预设规则为：加密计算的结果长度，不能大于定义的数据长度 n；加密机返回的结果内容是一个完整的数组。

[0032] 所述方法还包括：当所述读取线程等待超时后，所述服务器会先唤醒外部等待超时的所述读取线程，所述读取线程再获取所述加密后数据。

[0033] 所述方法还包括：当所述服务器超时未读取所述加密后数据时，所述读取线程通过所述销毁对象销毁所述通讯对象。

[0034] 所述方法还包括：关闭整个服务的时，所述读取线程通过所述销毁对象把建立的所有通讯对象关闭销毁。

[0035] 本发明提供的技术方案的有益效果是：通过本发明定义的基本格式、缓冲区、服务器创建的连接池对象工厂对需要加密的数据进行处理，获取到加密后的数据，服务器读取加密后数据并最终传输至高速公路电子预付卡，本发明提高了加密的有效性，并且避免了系统资源的闲置，提高了工作效率。通过实验验证，本方法在并发处理 1000 条数据时，最长时间只需要用时 2 秒；与原来每次请求必须等待 0.5 秒相对比，提高了数百倍效率，满足了实际应用中的多种需要。

附图说明

[0036] 图 1 为高速公路电子预付卡与加密机之间的通信框图；

[0037] 图 2 为一种高速公路电子预付卡与加密机之间的池化通信方法的流程图；

[0038] 图 3 为高速公路电子预付卡与加密机之间的通信示意图；

[0039] 图 4 为仿真试验的效果图。

具体实施方式

[0040] 为使本发明的目的、技术方案和优点更加清楚，下面对本发明实施方式作进一步地详细描述。

[0041] 为了避免系统资源的闲置，提高工作效率，本发明实施例提供了一种高速公路电子预付卡与加密机之间的池化通信方法，即预付卡在使用中需要通过卡机进行读写操作，为了保证卡片中存储数据的安全，需要通过加密机进行密钥计算，计算后，将计算结果通过卡机返回到卡片，从而实现整个卡片资料修改或者卡片的消费充值等操作，参见图 1、图 2 和图 3，详见下文描述：

[0042] 101：定义加密机返回数据的基本格式，通过基本格式定义缓冲区；

[0043] 该步骤具体为：

[0044] 1）第一和第二个字节拼成一个整数作为加密机返回数据的长度 n；

[0045] 总数据长度是：0xFFFF(16 进制)=65535（十进制）一个字节 8 位二进制数，即 FF，通过高低移位，即：第一字节是高 8 位，第二字节是低 8 位，来实现数据的长度，(byte[0]&0xFF00)>>8，(byte[1]&0x00FF)。

[0046] 2）第三和第四个字节作为返回类型；

[0047] 实际应用时，每个加密机都会对应一个返回类型，不同厂家的加密机返回类型不同，本发明实施例采用的加密机为：基于 SJL06 密码机的华大指令集，涉及到计算 MAC 值的时候，加密机输出的结果结构为表 1：

[0048] 表 1

[0049]

输出域	长度	类型	内容
应答码	2	A	MH
错误代码	2	H	00 表示正确
MAC	1-8	B	

[0050] 通过表 1 可以看出 A 为可打印字符；B 为任意字符，0x00-0xFF；H 为十六进制字符‘0’－‘F’，加密机的返回类型为 MH，本发明实施例对加密机的返回类型不做限制。

[0051] 3）第五和第六个字节作为返回结果；

[0052] 第五和第六个字节返回的结果状态‘0’‘0’表示加密成功，其他返回结果例如：‘0’‘1’、‘1’‘0’和‘1’‘1’均表示加密不成功。

[0053] 即加密机最终返回的数据中，前 6 个字节表示基本格式，加密结果长度为 n-6 个字节，当数据长度和前 6 个字节都正确，表示返回加密数据成功。

[0054] 4）根据加密机返回数据的基本格式定义缓冲区。

[0055] 该步骤具体为：设计缓冲区为 byte[X][Y]，该缓冲区可同时存储多条返回结果，

并且每条返回结果作为一行，规划缓存区每一行的约定：

[0056] byte[i][0] 和 byte[i][1] 中存储字节的长度；

[0057] byte[i][2] 和 byte[i][3] 中存储加密返回类型’M’和’H’；

[0058] byte[i][4] 和 byte[i][5] 中存储返回结果状态，‘0’‘0’表示加密成功；

[0059] byte[i][6]--byte[i][Y] 中存储加密内容。

[0060] 102：读卡器从高速公路电子预付卡中读取原始数据，并将原始数据传输至服务器；

[0061] 该步骤的操作为本领域技术人员所公知，由每个读卡器本身确定，本发明实施例对此不做限制。

[0062] 103：服务器创建连接池对象工厂、组装线程和读取线程，通过连接池对象工厂对原始数据进行验证，并通过组装线程将验证后的原始数据以报文的形式放入加密机的缓冲区中，返回缓存区的索引 index；

[0063] 为了在超时后不做处理，而又要在不关闭连接的情形下保证后续请求返回准确的结果，为每个通讯对象 Socket 提供一个读取线程去读取数据，严格把握数据格式，并把数据以严格的格式写在缓冲区中。

[0064] 1）定义与加密机通讯的连接池对象工厂，并创建连接池对象工厂；

[0065] 通过连接池对象工厂实现对通讯对象 Socket 的管理，创建连接池对象工厂包括：生成对象 makeObject（）、激活对象 activateObject、销毁对象 destroyObject 和验证对象 validateObject。

[0066] 其中，生成对象 makeObject（）是在系统启动的时候，根据定义的连接池深度，程序自动与加密机进行通信，生成了通讯对象 socket（例如：生成对象 makeObject（）可以作为连接池对象工厂中的一个机器，通过这个机器，就可以制作通信对象 socket）；同时在面向对象的语言中，本发明定义了一个完整的连接池对象，该连接池对象的核心是通信对象 socket，同时有激活对象属性、销毁对象属性、验证对象属性等。

[0067] 通讯对象 Socket 有两个属性分别为：正常运行水平线参数和最大运行水平线参数，其中，正常运行水平线参数默认在连接池中创建通讯对象 Socket 的数量；最大运行水平线参数可扩充最大限度的通讯对象 Socket 的数量，为临时请求并发量增长提供备用。

[0068] 正常情况下，连接池对象工厂中的通讯对象 socket 已经可以满足要求，当临时需要更多的通讯对象 socket 的时候，会创建（最大限度数量 - 正常数量）的通讯对象，使用完毕后，通过销毁对象 destroyObject 释放资源。

[0069] 2）连接池对象工厂中的通讯对象 Socket 被使用后，该通讯对象 Socket 被激活；

[0070] 实际应用中防止多个线程同时持有一个通讯对象 Socket，通过激活操作保证了其他线程无法使用已经激活的通讯对象 Socket。

[0071] 3）每次请求从连接池对象工厂中获取到通讯对象 socket 后，对通讯对象 socket 进行链接验证，若返回结果正确，则继续进行加密操作，否则，销毁连接池对象，并获取新的对象进行重新链接验证；

[0072] 其中，在使用每个通讯对象 socket 的时候，为保证通讯对象 socket 在连接池对象工厂中仍然正常存活有效，通过验证 validateObject 方法，对通讯对象 socket 是否存活进行验证，验证的规则是：对通讯对象 socket 与加密机进行心跳验证，发送链接验证码 16 个

0（加密机支持的心跳验证码）:0000000000000000，如果通讯对象 socket 返回结果正常，继续进行加密操作；否则通过销毁对象 destroyObject 终止这个通讯对象 socket，并获取新的通讯对象 socket 进行重新链接验证。

[0073] 4）定义组装线程，组成线程用于对通过验证的原始数据进行组装，形成发送报文，放入到加密机的缓冲区中；

[0074] 上述操作使得当有需要计算的请求访问后，不需要该请求立刻与加密机进行通信，而是把请求的内容提交后，等待读取线程来通知该请求，从而可以提高工作效率。因为传统每次请求后，建立 Socket 通信，然后需要 wait，这种等待只能设置为固定长度，而实际计算过程中，根据计算的业务类型、加密机的负载，这些等待时间是不相同的，没有必要进行固定的时间等待，从而耗费了加密机的等待资源。

[0075] 5）加密机返回缓冲区 byte[index] 的索引 index 至服务器，定义读取线程，读取线程用于根据索引 index 从缓冲区中读取加密后数据。

[0076] 通过该操作服务器就可以到缓冲区的指定索引下，通过读取线程读取加密后的数据，避免了资源的浪费。

[0077] 104：加密机读取缓存区中的报文，按照基本格式编写加密后数据，将加密后数据按照索引号传输至缓冲区中；

[0078] 即设置一个无限的循环，每次循环为下一个 byte[i] 填充数据，该步骤具体为：

[0079] 填充前六个字节，以获得后续字节的长度 n-6，依据预设规则判定接收的报文是否发生错位或错误，若发生了错误则彻底放弃这个连接；将加密后数据按照索引号传输至缓冲区中。

[0080] 预设规则为：1、加密计算的结果长度，不能大于定义的数据长度 n；2、加密机返回的结果内容是一个完整的数组（加密机计算结果填充的是否正确，不需要考虑）。

[0081] 其中，上述所述的错位指的是：在并发处理中计算中，只能根据 byte[2]’M’，byte[3]’H’ 来校验存储位置是否正确，来影响整个结果。

[0082] 105：服务器从缓冲区中读取加密后数据，并传输至数据卡，数据卡接收加密后数据发送至高速公路电子预付卡，高速公路电子预付卡根据加密后数据进行计算。

[0083] 例如：目前高速公路使用的电子预付卡是一种 CPU 卡，使用基于分散算法的密钥管理，即加密机中存放母钥，在卡片发行初始化的时候，母钥使用分散算法，并根据卡号，计算出一个子密钥，放到到卡片中。

[0084] 当需要对卡片操作的时候，比如：把 A 信息写到卡中，此时，需要把写卡时间、写卡数据、卡号以及卡片自动生成一个随机数等信息发送到加密机中，加密机根据这些信息进行计算，生成一个 MAC 码，返回到卡片中，卡片同样也会根据子密钥，把上述的内容进行计算，也会得到一个 MAC 码，如果这 2 个 MAC 码相同，说明合法允许进行写卡操作。

[0085] 当缓存区中有加密后数据时，读取线程会通过索引 index 去获得缓存区中指定的 byte[]，获取加密后数据，并校验有效长度后返回加密的字符串。其中，当读取线程等待超时后，服务器会先唤醒外部等待超时的读取线程，读取线程再获取加密后数据。

[0086] 本方法根据定义的数据长度和前六位来校验有效长度，加密机将计算结果存储在 n-6 的缓存中，当缓存区中指定的 byte[] 大于 n-6 时，表明缓存区中存储的字节是非法的，非有效数据结果。

[0087] 当服务器超时未读取加密后数据时，即存在长时间未处理的索引时，读取线程会销毁该通讯对象 Socket，确保连接池对象工厂中的通讯对象 Socket 总处于相对稳定的状态。

[0088] 具体实现时，为了释放资源，本方法还包括：关闭整个服务的时候，把建立的所有通讯对象 socket 进行关闭销毁，释放资源。

[0089] 其中，本发明实施例对高速公路电子预付卡、读卡器、服务器和加密机的类型不做限制，只要能完成上述功能的器件均可。

[0090] 下面以具体的试验来验证本发明实施例提供的高速公路电子预付卡与加密机之间的池化通信方法的可行性，详见下文描述：

[0091] 在实验中，根据需要的硬件：航天金卡卡机 *3，普通高速公路电子支付预付卡 *3、华大加密机 *1、应用服务器 *1、操作 PC*3 等实验硬件，并将设备组合成互联互通的局域网环境。

[0092] 在实验的环境中，为了实现并发处理的效果，还需要一套自动读写卡操作的模拟程序，该程序实现了对每台操作 PC 上的卡机进行自动读写操作，并记录每次的读写内容，生成数据报告，具体的实验如下：

[0093] 1) 使用模拟程序，对每张卡片进行写申请，并记录申请的数据和返回的结果数据，每张卡片的操作 1000 次，并记录保存数据，可参考表 1；

[0094] 2) 模拟程序在实现对每张卡片的 1000 次操作申请后，读取表 1 的数据，并调用应用服务，进行计算，并将计算结果记录到表 1 的 MAC 值；

[0095] 3) 在运行这 3000 次的调用加密机的服务中，使用的是线程池运行池数量为 500，最大上限为 1000 的模拟测试，程序运行内存调整为 4G；

[0096] 4) 记录总的运行时间和单笔时间分布情况，可参考图 4。

[0097] 5) 模拟程序根据加密机计算的结果，按照次序，依次写卡操作，写卡后，重新读卡，并记录读取的内容，填写到表 2 中的读取结果项(仅列出几次数据处理的结果进行说明)。

[0098] 表 2

[0099]

卡号	写入内容	写入时间	随机数	MAC 值	读取结果	结果
0902220100002123	测试数据 A	20130401103011	123FF	987C	测试数据 A	成功
0902220100002123	测试数据 B	20130401103021	123FF	6510	测试数据 B	成功
0902220100002125	测试数据 A	20130401103011	123EF	89AC	测试数据 A	成功

[0100]

[0101] 通过表 2 和图 4 可以看出，读卡器对卡片进行并发读取获取计算结果，并通过测试程序，将这些计算结果提交给服务器中的连接池服务，连接池服务将待计算的数据并发提

交到加密机中实现数据结果的计算。通过表 2 可以看出，每次计算的结果是准确的，实现了对卡片的成功写卡操作。

[0102] 通过图 4 可以看出，在进行 3000 次的请求计算中，20ms 内计算完成的次数大约在 1500 次，40ms 左右计算完成的大约在 1200 次，60ms 到 80ms 内，大约在 200 次左右，80ms 以上的在 100 次左右。通过图 4 的计算结果分布，说明了服务器在处理过程是满足处理要求的。

[0103] 本领域技术人员可以理解附图只是一个优选实施例的示意图，上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0104] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

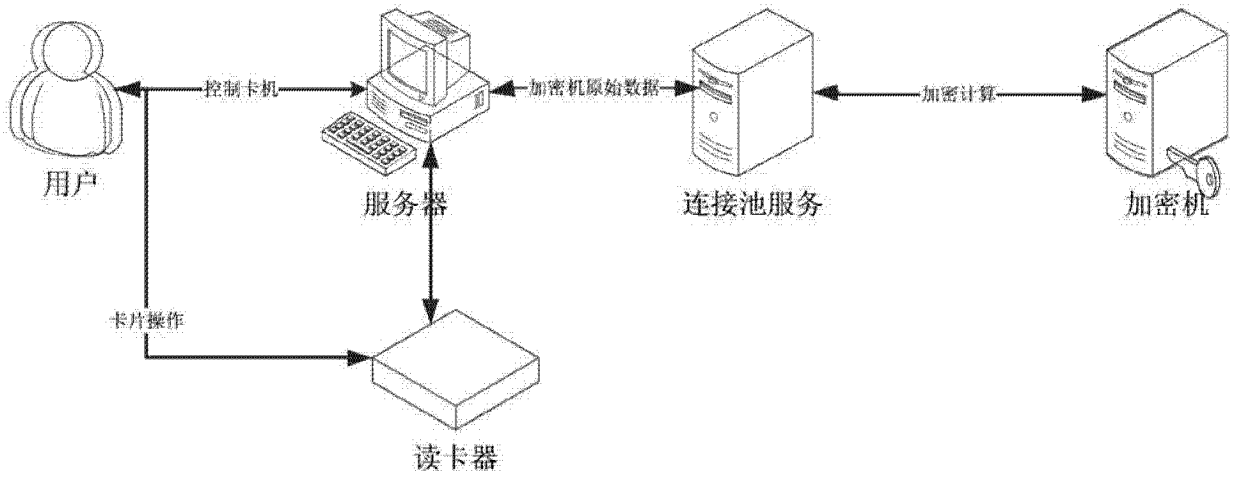

用户
控制卡机
服务器
加密机原始数据
连接池服务
加密计算
加密机
卡片操作
读卡器

图 1

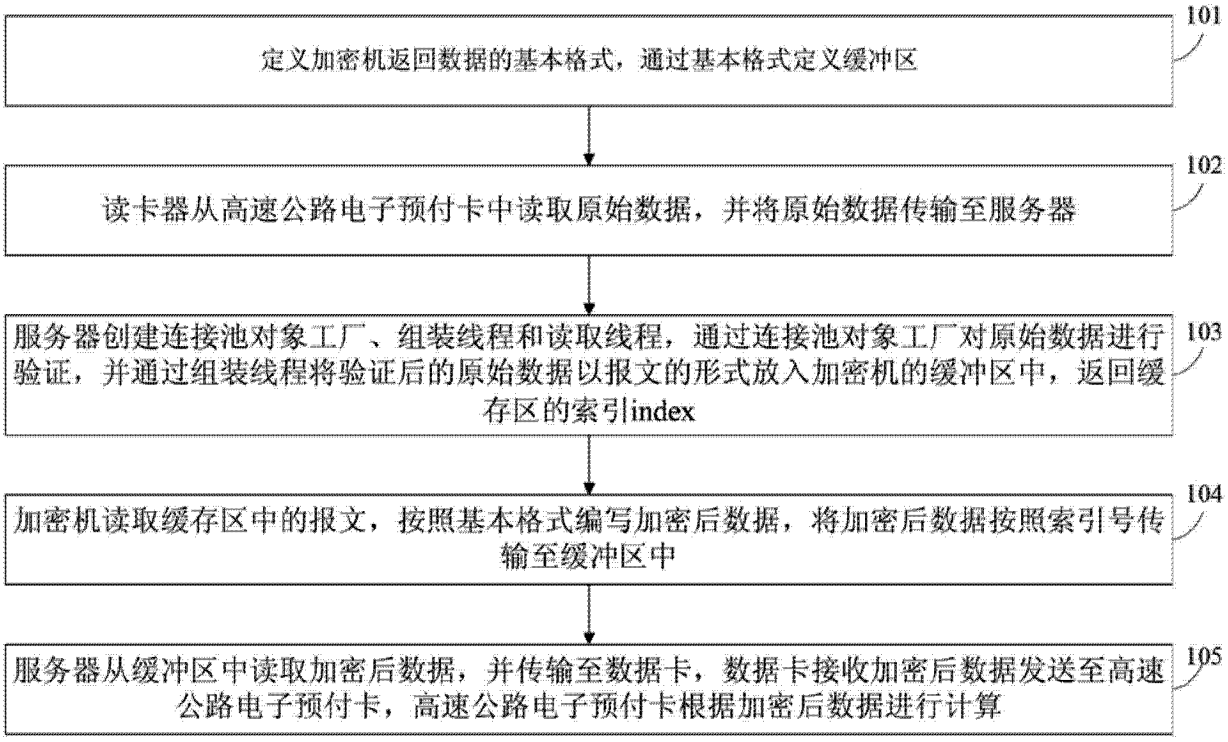

101
定义加密机返回数据的基本格式，通过基本格式定义缓冲区
102
读卡器从高速公路电子预付卡中读取原始数据，并将原始数据传输至服务器
103
服务器创建连接池对象工厂、组装线程和读取线程，通过连接池对象工厂对原始数据进行验证，并通过组装线程将验证后的原始数据以报文的形式放入加密机的缓冲区中，返回缓存区的索引index
104
加密机读取缓存区中的报文，按照基本格式编写加密后数据，将加密后数据按照索引号传输至缓冲区中
105
服务器从缓冲区中读取加密后数据，并传输至数据卡，数据卡接收加密后数据发送至高速公路电子预付卡，高速公路电子预付卡根据加密后数据进行计算

图 2

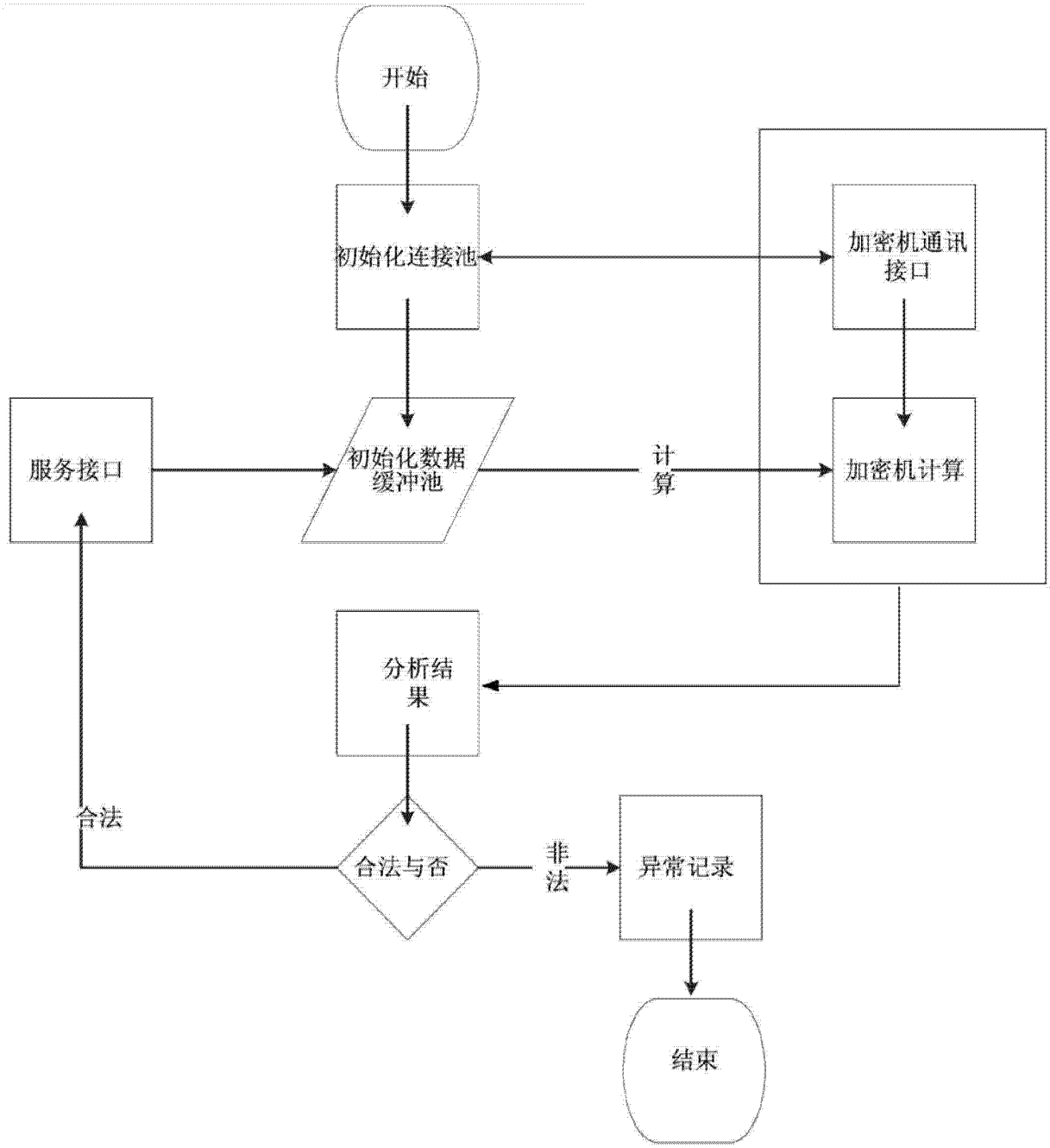

开始
初始化连接池
加密机通讯接口
服务接口
初始化数据缓冲池
计算
加密机计算
分析结果
合法
合法与否
非法
异常记录
结束

图 3

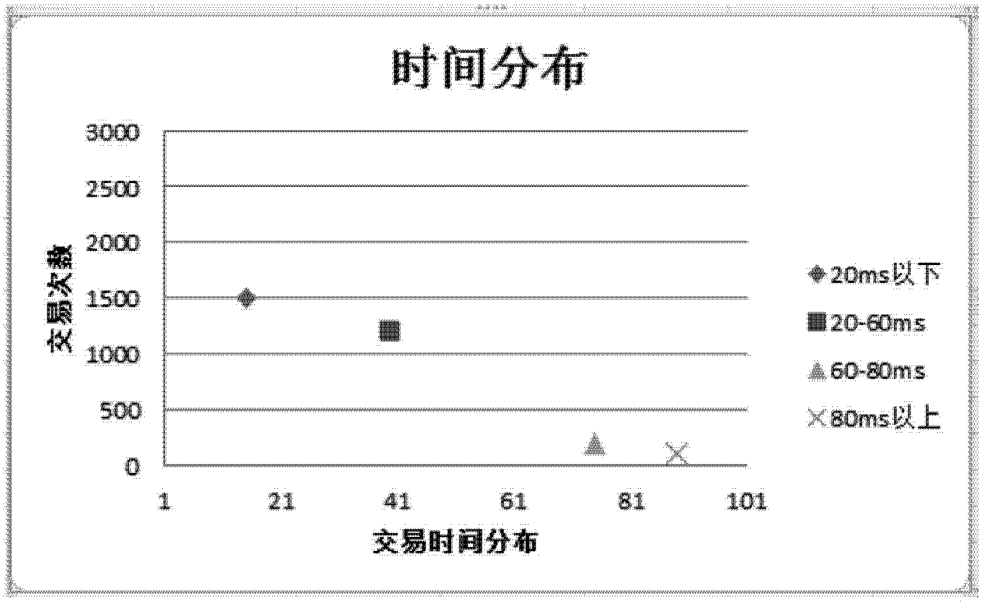

时间分布
3000
2500
2000
1500
1000
500
0
交易次数
1
21
41
61
81
101
交易时间分布
20ms以下
20-60ms
60-80ms
80ms以上

图 4