(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103746791 B
(45)授权公告日 2017.02.08

(21)申请号 201310714056.9

(22)申请日 2013.12.19

(65)同一申请的已公布的文献号
申请公布号 CN 103746791 A

(43)申请公布日 2014.04.23

(73)专利权人 广东芬尼克兹节能设备有限公司
地址 511470 广东省广州市南沙区大岗镇兴业路耀华工业园

(72)发明人 张东乾 刘杨 冯炳南 高翔

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 谭英强

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

(56)对比文件
谢林栩.基于TEA加密算法在网络传输中保护文件数据安全的应用.《广西师范学院学报:自然科学版》.2010,第27卷(第2期),
徐小龙.一种基于数据分割与分级的云存储数据隐私保护机制.《计算机科学》.2013,

审查员 陈莹

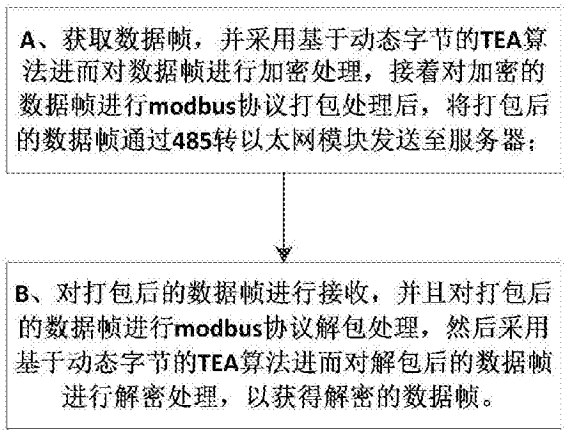
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种应用于工业领域的加密通信装置及方法

(57)摘要

本发明公开了一种应用于工业领域的加密通信装置及方法,该装置包括手操器、控制器、485转以太网模块、服务器以及PC平台。该方法包括:采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理,接着对加密的数据帧进行modbus协议打包处理后,将打包后的数据帧通过485转以太网模块发送至服务器;服务器对打包后的数据帧进行modbus协议解包处理,然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理,以获得解密的数据帧。本发明的方法和装置保证了加密数据的随机性,从而提高通信的安全性,而且能使操作步骤更加简化,从而能极大地提高通信效率。本发明广泛应用于工业领域通信中。



CN 103746791 B

1.一种应用于工业领域的加密通信装置，其特征在于：其包括手操器，所述的手操器依次连接有控制器、485转以太网模块、服务器以及PC平台；

所述的控制器，用于获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧进行modbus协议打包处理后，将打包后的数据帧通过485转以太网模块发送至服务器；

所述的服务器，用于对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧；

所述采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，其具体为：

从获取的数据帧中选取出关键参数，并且对关键参数进行分组，进而使每一个分组含有6个字节的关键参数明文，然后对每一个分组插入2个动态字节的明文，接着，采用固定的密钥对所述的分组进行加密处理，从而得到一组或多组的8个字节的动态密文。

2.根据权利要求1所述一种应用于工业领域的加密通信装置，其特征在于：所述的手操器用于获取数据帧，并且采用脉冲宽度不同的脉冲分别表示二进制的1和0，进而对数据帧进行归零码脉冲协议编码处理，然后将编码处理后的数据帧发送至控制器。

3.根据权利要求1所述一种应用于工业领域的加密通信装置，其特征在于：所述的modbus协议打包处理，其具体为：

采用modbus协议对数据帧进行打包处理，以得到modbus协议数据帧，然后在所述的modbus协议数据帧中插入动态密文，以得到打包后的数据帧。

4.根据权利要求1所述一种应用于工业领域的加密通信装置，其特征在于：所述的控制器用于获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧依次进行modbus协议打包处理以及CRC16校验编码处理后，将打包后的数据帧通过485转以太网模块发送至服务器。

5.一种应用于工业领域的加密通信方法，其特征在于：该方法包括：

A、获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧进行modbus协议打包处理后，将打包后的数据帧通过485转以太网模块发送至服务器；

B、服务器对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧；

所述步骤A中，所述的采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理这一步骤，其具体为：

从获取的数据帧中选取出关键参数，并且对关键参数进行分组，进而使每一个分组含有6个字节的关键参数明文，然后对每一个分组插入2个动态字节的明文，接着，采用固定的密钥对所述的分组进行加密处理，从而得到一组或多组的8个字节的动态密文。

6.根据权利要求5所述一种应用于工业领域的加密通信方法，其特征在于：该方法还包括手操器获取数据帧，并且采用脉冲宽度不同的脉冲分别表示二进制的1和0，进而对数据帧进行归零码脉冲协议编码处理，然后将编码处理后的数据帧发送至控制器这一步骤。

7.根据权利要求5所述一种应用于工业领域的加密通信方法，其特征在于：所述步骤A

中所述的modbus协议打包处理，其具体为：

采用modbus协议对数据帧进行打包处理，以得到modbus协议数据帧，然后在所述的modbus协议数据帧中插入动态密文，以得到打包后的数据帧。

8.根据权利要求5所述一种应用于工业领域的加密通信方法，其特征在于：所述的步骤B，其具体为：

服务器对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧，并且将解密的数据帧发送至PC平台；

所述解密的数据帧中包含缴费状态信息，而所述的PC平台根据所述的缴费状态信息从而激活或禁止客户端机组的使用权限。

一种应用于工业领域的加密通信装置及方法

技术领域

[0001] 本发明涉及通讯领域，尤其涉及一种应用于工业领域的加密通信装置及方法。

背景技术

[0002] 技术词解释：

[0003] CRC：循环冗余校验码

[0004] modbus：一种用于工业现场的总线协议

[0005] 随着营销观念的转变，租赁合作模式将逐步成为主流，因为其能够节省设备使用方不必要的硬件设备投入以及维护。而在租赁合作模式中，对于设备拥有方的资产保护是尤为重要的，特别是核心的通信保护。然而目前应用于工业领域的通信方法，其安全性较低，并不能起到很好的保护作用，因此，发明一种安全性较高的加密通信方法，是目前迫切需要解决的问题。

发明内容

[0006] 为了解决上述技术问题，本发明的目的是提供一种应用于工业领域的加密通信装置。

[0007] 本发明的另一目的是提供一种应用于工业领域的加密通信方法。

[0008] 本发明所采用的技术方案是：一种应用于工业领域的加密通信装置，其包括手操器，所述的手操器依次连接有控制器、485转以太网模块、服务器以及PC平台；

[0009] 所述的控制器，用于获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧进行modbus协议打包处理后，将打包后的数据帧通过485转以太网模块发送至服务器；

[0010] 所述的服务器，用于对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧。

[0011] 进一步，所述采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，其具体为：

[0012] 从获取的数据帧中选取出关键参数，并且对关键参数进行分组，进而使每一个分组含有6个字节的关键参数明文，然后对每一个分组插入2个动态字节的明文，接着，采用固定的密钥对所述的分组进行加密处理，从而得到一组或多组的8个字节的动态密文。

[0013] 进一步，所述的手操器用于获取数据帧，并且采用脉冲宽度不同的脉冲分别表示二进制的1和0，进而对数据帧进行归零码脉冲协议编码处理，然后将编码处理后的数据帧发送至控制器。

[0014] 进一步，所述的modbus协议打包处理，其具体为：

[0015] 采用modbus协议对数据帧进行打包处理，以得到modbus协议数据帧，然后在所述的modbus协议数据帧中插入动态密文，以得到打包后的数据帧。

[0016] 进一步，所述的控制器用于获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧依次进行modbus协议打包处理以及CRC16校验编码处理后，将打包后的数据帧通过485转以太网模块发送至服务器。

[0017] 本发明所采用的另一技术方案是：一种应用于工业领域的加密通信方法，该方法包括：

[0018] A、获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧进行modbus协议打包处理后，将打包后的数据帧通过485转以太网模块发送至服务器；

[0019] B、服务器对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧。

[0020] 进一步，所述步骤A中，所述的采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理这一步骤，其具体为：

[0021] 从获取的数据帧中选取出关键参数，并且对关键参数进行分组，进而使每一个分组含有6个字节的关键参数明文，然后对每一个分组插入2个动态字节的明文，接着，采用固定的密钥对所述的分组进行加密处理，从而得到一组或多组的8个字节的动态密文。

[0022] 进一步，该方法还包括手操器获取数据帧，并且采用脉冲宽度不同的脉冲分别表示二进制的1和0，进而对数据帧进行归零码脉冲协议编码处理，然后将编码处理后的数据帧发送至控制器这一步骤。

[0023] 进一步，所述步骤A中所述的modbus协议打包处理，其具体为：

[0024] 采用modbus协议对数据帧进行打包处理，以得到modbus协议数据帧，然后在所述的modbus协议数据帧中插入动态密文，以得到打包后的数据帧。

[0025] 进一步，所述的步骤B，其具体为：

[0026] 服务器对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧，并且将解密的数据帧发送至PC平台；

[0027] 所述解密的数据帧中包含缴费状态信息，而所述的PC平台根据所述的缴费状态信息从而激活或禁止客户端机组的使用权限。

[0028] 本发明的有益效果是：本发明的装置采用了基于动态字节的TEA算法，因此保证了加密数据的随机性，从而提高通信的安全性。而且由于基于动态字节的TEA算法，其是利用动态可变化的字节来保证加密数据的随机性，因此本发明的通信装置不仅能够保证通信的安全性，而且其操作步骤更加简化，从而能极大地提高通信效率。

[0029] 本发明的另一有益效果是：本发明的方法采用了基于动态字节的TEA算法，因此，本发明的方法能够保证加密数据的随机性，从而提高通信的安全性。而且由于基于动态字节的TEA算法，其是利用动态可变化的字节来保证加密数据的随机性，因此，本发明的通信方法更易于实现，操作步骤更加简化，从而能够极大地提高通信效率。

附图说明

[0030] 下面结合附图对本发明的具体实施方式作进一步说明：

[0031] 图1是本发明一种应用于工业领域的加密通信装置的结构框图；

[0032] 图2是本发明一种应用于工业领域的加密通信方法的步骤流程图。

具体实施方式

[0033] 由图1所示，一种应用于工业领域的加密通信装置，其包括手操器，所述的手操器依次连接有控制器、485转以太网模块、服务器以及PC平台；

[0034] 所述的控制器，用于获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧进行modbus协议打包处理后，将打包后的数据帧通过485转以太网模块发送至服务器；

[0035] 所述的服务器，用于对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧。

[0036] 进一步作为优选的实施方式，所述采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，其具体为：

[0037] 从获取的数据帧中选取出关键参数，并且对关键参数进行分组，进而使每一个分组含有6个字节的关键参数明文，然后对每一个分组插入2个动态字节的明文，接着，采用固定的密钥对所述的分组进行加密处理，从而得到一组或多组的8个字节的动态密文。所述获取的数据帧，其包含关键参数以及非关键参数。而所述的关键参数包含ID地址和/或运行状态参数。对于所述动态字节，其动态的方式为，该字节的数值动态变化。还有，由上述可知，采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理后，所得到的加密的数据帧，其是包含了非关键参数的明文以及关键参数的密文。

[0038] 对于上述分组的组数，其根据实际情况而定，若关键参数只含有6个字节，或少于6个字节，则组数为一，另外，若关键参数所含有的字节数并不为6的倍数时，则可补0，从而使每个分组含有6个字节的明文。

[0039] 另外，根据上述可知，采用基于动态字节的TEA算法进而对数据帧进行解密处理，其具体为：采用固定的密钥进而对一组或多组的8个字节的动态密文进行解密，然后将那些插入的动态字节的明文进行删除，从而过滤出关键参数。

[0040] 由上述可知，相较于传统的TEA算法，本发明所采用的基于动态字节的TEA算法，其无需对整个数据帧进行分组加密，只对关键参数进行分组加密，因此在保证数据传输的安全性基础上，能够提高数据加密的处理效率，另外，由于其在每个分组数据中插入了动态可变化的字节，因此能够使加密数据具备高的随机性，这样则能够提高通信的安全性，而且，无需采用复杂的动态密钥，因此能够简化算法，从而进一步地提高加密处理的效率，使通信效率得到进一步的提高。

[0041] 进一步作为优选的实施方式，所述的手操器用于获取数据帧，并且采用脉冲宽度不同的脉冲分别表示二进制的1和0，进而对数据帧进行归零码脉冲协议编码处理，然后将编码处理后的数据帧发送至控制器。由于本发明所采用的归零码脉冲协议，其是利用脉冲宽度不同的脉冲来分别表示二进制的1和0，因此，能够降低数据传输的误码率，进而提高数据的正确性，并且能够进一步地提高数据传输的安全性。另外，由上述可知，对于归零码脉冲协议解码处理，其具体为：通过不同脉冲宽度的脉冲，进而分别识别为二进制的1和0，以

实现归零码脉冲协议的解码处理。

[0042] 进一步作为优选的实施方式，所述的modbus协议打包处理，其具体为：

[0043] 采用modbus协议对数据帧进行打包处理，以得到modbus协议数据帧，然后在所述的modbus协议数据帧中插入动态密文，以得到打包后的数据帧。即在标准的modbus协议架构上，插入动态密文，而该动态密文所插入的位置是在标准modbus协议数据帧中功能码与起始地址之间。这样能够提高modbus协议数据帧的安全性。另外，对于所述的动态密文，其可以是由基于动态字节的TEA算法进行加密处理后所得到的。另外，由上述可知，对打包后的数据帧进行modbus协议解包处理，其具体为：采用modbus协议对打包后的数据帧进行解包，然后将插入的动态密文进行提取。

[0044] 进一步作为优选的实施方式，所述的控制器用于获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧依次进行modbus协议打包处理以及CRC16校验编码处理后，将打包后的数据帧通过485转以太网模块发送至服务器。由于还设有CRC16校验编码，因此能够进一步地提高数据的正确性。

[0045] 由图2所述，一种应用于工业领域的加密通信方法，该方法包括：

[0046] A、获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧进行modbus协议打包处理后，将打包后的数据帧通过485转以太网模块发送至服务器；

[0047] B、服务器对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧。

[0048] 进一步作为优选的实施方式，所述步骤A中，所述的采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理这一步骤，其具体为：

[0049] 从获取的数据帧中选取出关键参数，并且对关键参数进行分组，进而使每一个分组含有6个字节的关键参数明文，然后对每一个分组插入2个动态字节的明文，接着，采用固定的密钥对所述的分组进行加密处理，从而得到一组或多组的8个字节的动态密文。

[0050] 进一步作为优选的实施方式，该方法还包括手操器获取数据帧，并且采用脉冲宽度不同的脉冲分别表示二进制的1和0，进而对数据帧进行归零码脉冲协议编码处理，然后将编码处理后的数据帧发送至控制器这一步骤。

[0051] 进一步作为优选的实施方式，所述步骤A中所述的modbus协议打包处理，其具体为：

[0052] 采用modbus协议对数据帧进行打包处理，以得到modbus协议数据帧，然后在所述的modbus协议数据帧中插入动态密文，以得到打包后的数据帧。

[0053] 进一步作为优选的实施方式，所述的步骤B，其具体为：

[0054] 服务器对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧，并且将解密的数据帧发送至PC平台；

[0055] 所述解密的数据帧中包含缴费状态信息，而所述的PC平台根据所述的缴费状态信息从而激活或禁止客户端机组的使用权限。

[0056] 本发明的具体实施例

[0057] 一种应用于工业领域的加密通信方法及装置，该装置包括PC平台、服务器、485转以太网模块、控制器以及手操器，而该方法包括发送步骤和接收步骤。

[0058] 所述的发送步骤，其为手操器将数据发送至PC平台这一步骤，而这一步骤具体包括：

[0059] S1、手操器获取数据帧，并且采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理后，进行CRC16校验编码，然后对CRC16校验编码后的加密的数据帧进行归零码脉冲协议编码处理，然后将处理后的数据帧发送至控制器；

[0060] S2、控制器对由手操器传来的数据帧进行接收，然后通过归零码脉冲协议进而对接收到的数据帧进行解码，接着，进行CRC16校验解码，以得到CRC16解码数据，此时，若CRC16解码数据为正确的，则此时的CRC16解码数据即为采用基于动态字节的TEA算法进行加密后所得到的加密数据帧，然后，采用基于动态字节的TEA算法进而对CRC16解码数据进行解密，以得到关键参数的明文和非关键参数的明文，并且对其进行处理；

[0061] S3、控制器获取数据帧，并且采用采用基于动态字节的TEA算法进而对获取的数据帧进行加密处理，接着对加密的数据帧依次进行modbus协议打包处理以及CRC16校验编码处理后，将打包后的数据帧通过485转以太网模块发送至服务器；

[0062] S4、服务器对由控制器传来的数据帧依次进行CRC16校验解码处理以及modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包的数据帧进行解密处理，以获得解密的数据帧，接着，从解密的数据帧中取出ID地址，判断该ID地址是否与预存的ID地址一致，若是，则对该解密后的数据帧，即关键参数的明文和非关键参数的明文，进行处理，并且将处理的结果发送至PC平台上进行处理和显示；反之，则结束。另外，当解密后的数据帧中含有缴费状态信息时，则将缴费状态信息发送至PC平台，然后PC平台则根据所述的缴费状态信息从而激活或禁止客户端机组的使用权限。

[0063] 上述步骤中所述的关键参数，其包含ID地址。

[0064] 所述的接收步骤，其为手操器接收由PC平台传来的数据的步骤，而这一步骤包括：

[0065] S5、PC平台通过TCP协议进而将数据帧发送给服务器；

[0066] S6、服务器通过TCP协议对由PC传来的数据帧进行接收并保存；

[0067] S7、服务器采用基于动态字节的TEA算法进而对接收的数据帧进行加密处理后，以得到一组或多组的密文，然后对整帧数据，即关键参数的密文以及非关键参数的明文，进行modbus协议打包处理，然后将打包后的数据帧进行CRC16校验编码，接着，再通过TCP协议发送给485转以太网模块，而485转以太网模块将该数据发送至控制器，此时，所述的关键参数包含ID地址以及运行状态参数；

[0068] S8、控制器将接收到的数据进行CRC16校验解码，然后将modbus协议数据帧进行解包处理，接着，则对解包后的数据帧进行基于动态字节的TEA算法的解密处理，然后判断该解密数据中的ID地址是否与预存的地址一致，若是，则对该解密后的数据进行处理；

[0069] S9、控制器将相关的数据帧依次进行基于动态字节的TEA算法的加密处理、CRC16校验编码处理以及归零码脉冲协议编码处理后，将处理后的数据帧发送至手操器；

[0070] S10、手操器对由控制器传来的数据进行接收，并且对接收的数据依次进行归零码脉冲协议解码处理、CRC16校验解码处理以及基于动态字节的TEA算法的解密处理，然后对解密后的数据进行相应的处理。

[0071] 由上述可知，相较于传统的应用于工业领域的通信方式，本发明具有更高的安全性和准确性，以及数据处理的效率更高。

[0072] 另外，对于上述的手操器、控制器、PC以及服务器，它们各自的功能分别为：

[0073] 1、手操器在正常情况下只显示机组温度、负载状态、故障、参数等，只有在长按特殊按键的情况下才能进入8位密码界面，并输入正确的8位密码后才能进入ID显示和ID设置界面，该界面实时显示控制器ID，并且可以设置新的控制器ID，同时发送给控制器，并且会回读控制器的最新ID，进而提示设置是否成功；

[0074] 2、控制器实时将当前的温度、参数等，发送给手操器，只有在接收到手操器请求时，控制器才会ID送给手操器，控制器每5min会将实时的温度、参数等发送给服务器，服务器进行接收，成功接收后会向控制器进行反馈，控制器连续30min没有成功接收，服务器反馈的数据，默认为通信故障，运行3天后自动关机，而控制器每隔8个小时向服务器请求运行状态，如果服务器反馈运行状态为关机时，此时控制器会立刻关机；

[0075] 3、PC平台实时向服务器读取机组温度、负载状态、故障、参数、ID和运行状态等，同时可以在PC平台设置ID、运行状态和参数，并发送给服务器；

[0076] 4、服务器实时将控制器的温度、负载状态、故障、参数、ID和运行状态等发送给PC平台，同时接收PC平台的ID和运行状态设置，并保存在服务器，同时服务器每5min接收一次控制器的温度、负载状态、故障和参数等数据，并将结果反馈给控制器；而服务器每8个小时接收一次控制器的运行状态请求，并将当前运行状态反馈给控制器。

[0077] 以上是对本发明的较佳实施进行了具体说明，但本发明创造并不限于所述实施例，熟悉本领域的技术人员在不违背本发明精神的前提下还可做作出种种的等同变形或替换，这些等同的变形或替换均包含在本申请权利要求所限定的范围内。

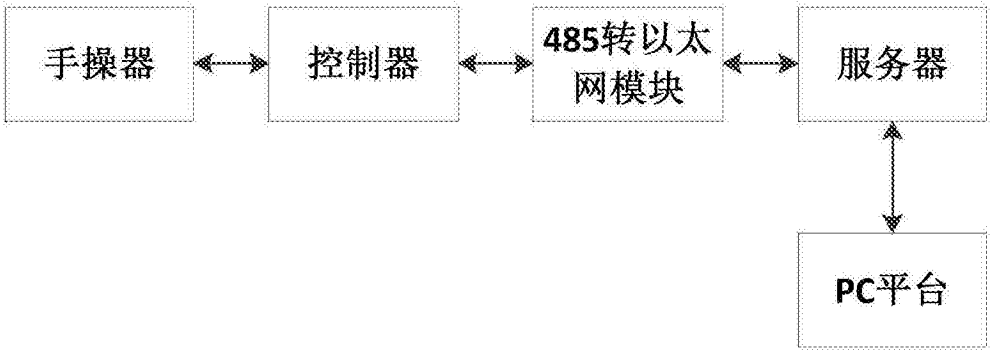

手操器
控制器
485转以太网模块
服务器
PC平台

图1

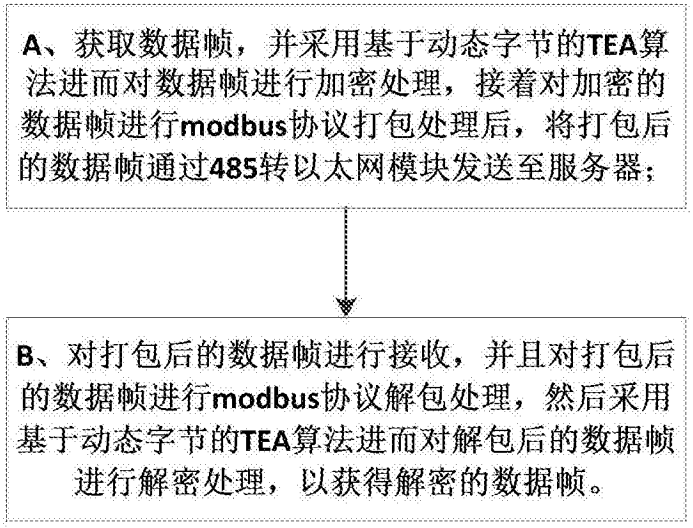

A、获取数据帧，并采用基于动态字节的TEA算法进而对数据帧进行加密处理，接着对加密的数据帧进行modbus协议打包处理后，将打包后的数据帧通过485转以太网模块发送至服务器；
B、对打包后的数据帧进行接收，并且对打包后的数据帧进行modbus协议解包处理，然后采用基于动态字节的TEA算法进而对解包后的数据帧进行解密处理，以获得解密的数据帧。

图2