



## (12)发明专利

(10)授权公告号 CN 105610837 B

(45)授权公告日 2018.12.18

(21)申请号 201511026877.9

(56)对比文件

(22)申请日 2015.12.31

CN 105049434 A, 2015.11.11,

(65)同一申请的已公布的文献号

CN 105162797 A, 2015.12.16,

申请公布号 CN 105610837 A

US 2014315518 A1, 2014.10.23,

(43)申请公布日 2016.05.25

罗斌.《电力SCADA系统网络安全技术与方法研究》.《信息安全与通信保密》.2014,(第6期),全文.

(73)专利权人 上海交通大学

审查员 李俊华

地址 200240 上海市闵行区东川路800号

专利权人 公安部第三研究所

(72)发明人 陈秀真 陆越 金波 陈长松

(74)专利代理机构 上海汉声知识产权代理有限公司 31236

代理人 郭国中

(51)Int.Cl.

H04L 29/06(2006.01)

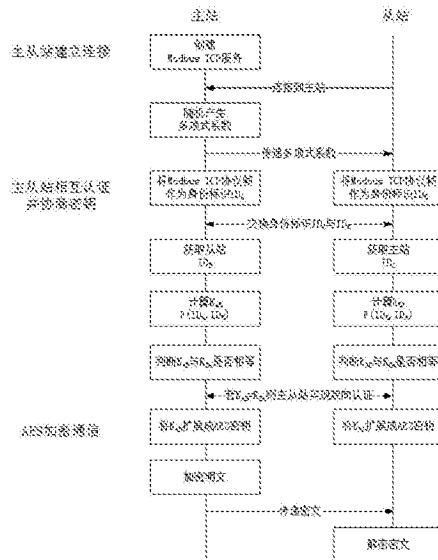
权利要求书1页 说明书7页 附图3页

## (54)发明名称

用于SCADA系统主站与从站间身份认证的方法及系统

## (57)摘要

本发明提供的一种用于SCADA系统主站与从站间身份认证的方法及系统,包括如下步骤:主站A创建服务,产生对称多项式系数 $a_{ij}$ ,从站B根据主站A服务器的IP地址与主站A建立连接,连接建立成功后从站B与主站A共享对称二元多项式参数;主从站均采用通信协议的数据帧作为自身身份标识符 $ID_A$ 与 $ID_B$ ;主站A与从站B交换彼此的身份标识符,并将两者的身份标识符带入对称多项式进行计算;如果 $f(ID_A, ID_B) = f(ID_B, ID_A)$ ,则主站A与从站B实现双向认证,并计算,扩展得到对称加密密钥 $K_{AB}$ 。本发明选用对称多项式产生共享密钥,并将之作为对称加密密钥,报文交换过程中选用对称加密算法,降低了计算复杂度。



1. 一种用于SCADA系统主站与从站间身份认证的方法,其特征在于,包括如下步骤:

步骤A:主站A创建服务,产生对称多项式系数 $a_{ij}$ ,从站B根据主站A服务器的IP地址与主站A建立连接,连接建立成功后从站B与主站A共享二元对称多项式参数,主站A与从站B均持有完整的二元对称多项式表达式;

步骤B:连接建立完毕后,在应用层选取通信协议,主站A、从站B分别采用通信协议的数据帧作为自身身份标识符 $ID_A, ID_B$ ;

步骤C:通信建立完毕后,主站A与从站B交换彼此的身份标识符,主站A、从站B分别将两者的身份标识符带入二元对称多项式进行计算,得到计算结果 $f(ID_A, ID_B), f(ID_B, ID_A)$ ;

步骤D:主站A与从站B交换彼此二元对称多项式计算结果,如果 $f(ID_A, ID_B) = f(ID_B, ID_A)$ ,则主站A与从站B实现双向认证,并计算 $K_{AB} = f(ID_A, ID_B) = f(ID_B, ID_A)$ ,进入步骤E继续执行;否则,返回步骤B;

步骤E:扩展计算得到加密密钥 $K_{AB}$ ,使 $K_{AB}$ 符合AES密钥长度要求,并采用加密算法对主从站间传送的数据内容进行加密。

2. 根据权利要求1所述的用于SCADA系统主站与从站间身份认证的方法,其特征在于,所述步骤C中的二元对称多项式为二元t次对称多项式,满足:

$$f(x, y) = \sum_{i+j=0}^t a_{ij} x^i y^j$$

其中,二元t次对称多项式定义在有限域 $GF(q)$ 上,q的取值为大于 $10^k$ 的素数,k为密钥的长度;而且对于任意的i,j,都满足等式 $a_{ij} = a_{ji}$ ; $a_{ij}$ 表示对称多项式系数;x,y表示两随机变量。

3. 根据权利要求2所述的用于SCADA系统主站与从站间身份认证的方法,其特征在于,所述二元t次对称多项式的对称多项式系数 $a_{ij}$ 由主站A在通信建立过程中随机产生。

4. 根据权利要求1所述的用于SCADA系统主站与从站间身份认证的方法,其特征在于,所述步骤B中,所述通信协议为ModbusTCP协议。

5. 根据权利要求1所述的用于SCADA系统主站与从站间身份认证的方法,其特征在于,所述步骤E中,所述加密算法为AES对称加密算法。

6. 一种用于SCADA系统主站与从站间身份认证方法的系统,其特征在于,所述系统采用权利要求1至5任意一项所述的用于SCADA系统主站与从站间身份认证的方法。

## 用于SCADA系统主站与从站间身份认证的方法及系统

### 技术领域

[0001] 本发明涉及的是一种用于SCADA系统主从站间的身份认证技术,尤其是一种基于对称多项式加密机制的双向认证技术,具体涉及SCADA系统的主从站通信安全的保证。

### 背景技术

[0002] 随着信息技术的不断发展,工业的现代化水平与日俱增,工业控制系统(Industry Control System, ICS)被广泛地应用于诸多与国计民生息息相关的行业,诸如冶金、水电供应、油气输送、航空航天、道路交通等,其在社会生产与保障性基础设施建设中发挥着不可替代的作用。典型的SCADA(Supervisory Control and Data Acquisition)系统主要用于远程监控和数据采集,综合运用计算机、控制、通信与网络等技术,通过对远程分散测控点采集的数据进行监控与分析,为整个生产过程的调度、管理、故障诊断等操作提供技术和数据支持。通过以太网,整个控制系统能够与远程终端设备便捷地相互连接。目前工业控制系统的性能、可靠性、灵活性等因素被给予高度关注,但其信息安全问题却没有得到足够重视。

[0003] 工业化和信息化的深度融合使得标准控制协议的使用越来越广泛,工业控制系统的开放性也随之提升,通用的协议、软硬件设备、操作系统等已经被广泛应用,这直接导致针对工控系统的攻击事件频发,一系列网络安全问题逐渐暴露出来。以“震网病毒”为例,它利用微软Windows操作系统与西门子WinCC操作系统的漏洞实现对系统的直接破坏,黑客能够完全控制远程被感染的主机,使之成为僵尸计算机。“震网病毒”向公共事业机构和控制系统发动恶意攻击,各类通信设施、民用和工业基础设施等均暴露在其攻击下,伊朗布什尔核电站也没能幸免,核电站中铀分离机的控制逻辑被恶意修改,导致电动机转速异常而产生了严重的损失。在“震网病毒”事件发生后,世界各地针对工业控制系统的攻击事件频频发生,并愈演愈烈,造成了严重的破坏与损失,诸如比“震网病毒”强大20倍的“Flame火焰病毒”肆虐中东地区。针对工业控制系统接连不断的攻击事件已经造成严重的后果,这些网络安全问题给工业控制系统带来了严峻的挑战,将人们对于工业网络安全的关注推向一个新的高潮。

[0004] 事实上,很多工业控制网络疏于严格的系统管理,可能出现内部人员接入已感染病毒的移动设备或外部人员通过非法手段截获而导致信息泄漏、篡改,从而使一些不法分子有机可乘。SCADA系统的信息安全机制并不完善,身份认证环节存在诸多漏洞,很容易暴露给攻击者。攻击者可以通过伪造的用户管理员身份与主站进行通信,非法接入工业控制网络中。攻击者也可以通过入侵主站与从站之间的通信网络,窃取通信内容,影响主从站间正常通信,致使SCADA系统中基础设施和工业服务中断,产生严重的破坏。身份认证对于实现SCADA系统的安全接入控制而言十分重要,其承担整个安全体系的“门禁”职能,好比整个信息安全体系的第一道大门,对PLC控制设备节点、管理员用户的身份进行核对,保障了使用者物理与数字身份的相互统一。这一环节实现了对系统资源的有效保护,防止用户身份被非法冒用,拒绝对敏感数据的非法访问请求。如果体系中的身份认证环节受到挑战,那么

体系中其他的防护方案也将难以实现。由于控制环节在工业系统中处于至关重要的地位，要求对所有接入对象进行安全认证，包括用户接入和PLC等控制设备接入，SCADA系统对于主从站间的通讯认证有着严格的要求。

[0005] 然而，工业控制系统的安全需求不同于传统的Internet，其更加关注系统的高可用性、实时性与业务连续性。在紧急情况下，工业控制系统需要应急处理程序能够快速响应，以降低由于处理紧急情况时间较长导致的损失。因此，现有的成熟且健壮的密码机制不能直接应用在SCADA系统中设备节点身份认证，需要设计轻量级的身份认证机制，以保证控制系统应急响应的速度。本发明采用适合SCADA系统的轻量级加密机制，保证主从站通信安全，并实现主从站间双向认证的技术体系，实现对系统的安全接入访问控制。

[0006] 经文献检索发现，现有SCADA系统的主从站身份认证及通信的安全保障措施有以下几种：

[0007] (1) 对称加密算法

[0008] 通信过程中主从站通过通信线路交换信息，入侵者可以通过窃取通信线路的方式，获取主从站的通讯数据，实现对工控系统的攻击，故需要在从站和主站的入口和出口处加入加解密功能模块。由于SCADA系统对于数据传输过程的效率和安全性都有着极高的要求，因此选取轻量级的加密机制能保证系统中断后快速恢复，降低系统损失。通过分析对称和非对称两种加密算法的加解密时间，相比之下，对称加密算法复杂度较低，加解密时间较短，且产生的密钥数量较少。因此，对称加密算法被应用到主从站的安全通信领域，以保证系统中断后快速恢复，降低系统损失。常用的对称加密算法有AES、DES、IDEA算法等。采用对称加密在密钥节点数量与响应时间花费上具有优越性，符合系统轻量级加密机制的需求，但对称加密中加解密密钥唯一、密钥的安全性难以得到保证。

[0009] (2) 密钥更新机制

[0010] 引入一种新的加密密钥管理方案，采用密钥更新的方式降低密钥泄露风险。主站既是通信的发起者也是会话密钥生成器，可以通过在密钥产生过程中增加会话密钥更新阶段和主密钥更新阶段增强密钥的安全性。主站与从站之间共享的主密钥，在会话密钥更新阶段，主站随机产生会话密钥，用主密钥加密会话密钥，并把加密后的会话密钥传递给相应的从站。从站接收密钥，用主密钥进行解密，并向主站传递确认信息。主密钥更新阶段中，主站和从站接收到彼此加密后的主密钥，分别用会话密钥进行解密，并对主密钥进行更新，使用更新后的主密钥发送新的会话密钥。在主密钥更新阶段中，通过引入赫尔曼椭圆曲线密钥协议，降低了密钥泄露的可能性。密钥更新机制增强了密钥的安全性，但并未实现主从站间的身份认证，攻击者可以通过盗用通信方身份，窃取共享密钥。

[0011] (3) 与硬件设备结合

[0012] 通过硬件设备保护通信过程中密钥分配的安全，无需对SCADA节点进行修改，而是采用直接与传统的设备相集成的方式。这种方法是在SCADA系统主从站通信环节引入的身份验证，防范攻击者变更消息或冒充通信方身份。该方法操作简单，密钥存储设备可以直接集成到SCADA设备中，兼容性与可移植性十分突出，但更新硬件设备将增加部署成本。

[0013] 以上研究表明，SCADA系统主要选用对称加密算法实现数据的加密传输与解密验证过程，但会话密钥的安全性有待增强，通信双方的身份认证机制有待完善，现有的安全防护机制不能有效阻止用户及设备的非法接入。

## 发明内容

[0014] 针对现有技术中的缺陷,本发明的目的是提供一种关注系统轻量级加密机制需求的同时,兼顾了密钥的安全性,有效实现了主站与从站间的双向认证的用于SCADA系统主站与从站间身份认证的方法及系统。

[0015] 为解决上述技术问题,本发明提供的一种用于SCADA系统主站与从站间身份认证的方法,包括如下步骤:

[0016] 步骤A:主站A创建服务,产生对称多项式系数 $a_{ij}$ ,从站B根据主站A服务器的IP地址与主站A建立连接,连接建立成功后从站B与主站A共享二元对称多项式参数,主站A与从站B均持有完整的二元对称多项式表达式;

[0017] 步骤B:连接建立完毕后,在应用层选取通信协议,主站A、从站B分别采用通信协议的数据帧作为自身身份标识符 $ID_A$ 、 $ID_B$ ;

[0018] 步骤C:通信建立完毕后,主站A与从站B交换彼此的身份标识符,主站A、从站B分别将两者身份标识符带入二元对称多项式进行计算,得到计算结果 $f(ID_A, ID_B)$ 、 $f(ID_B, ID_A)$ ;

[0019] 步骤D:主站A与从站B交换彼此二元对称多项式计算结果,如果 $f(ID_A, ID_B) = f(ID_B, ID_A)$ ,则主站A与从站B实现双向认证,并计算 $K_{AB} = f(ID_A, ID_B) = f(ID_B, ID_A)$ ,进入步骤E继续执行;否则,返回步骤B;

[0020] 步骤E:扩展计算得到加密密钥 $K_{AB}$ ,使 $K_{AB}$ 符合AES密钥长度要求,并采用加密算法对主从站间传送的数据内容进行加密。

[0021] 优选地,所述步骤C中的二元对称多项式为二元t次对称多项式,满足:

$$[0022] f(x, y) = \sum_{i+j=0}^t a_{ij} x^i y^j$$

[0023] 其中,二元t次对称多项式定义在有限域 $GF(q)$ 上,q的取值为大于 $10^k$ 的素数,k为密钥的长度;而且对于任意的i、j,都满足等式 $a_{ij} = a_{ji}$ ; $a_{ij}$ 表示对称多项式系数;x,y表示两随机变量。

[0024] 优选地,所述二元t次对称多项式的对称多项式系数 $a_{ij}$ 由主站A在通信建立过程中随机产生。

[0025] 优选地,所述步骤B中,所述通信协议为Modbus TCP协议。

[0026] 优选地,所述步骤E中,所述加密算法为AES对称加密算法。

[0027] 一种系统,所述系统采用用于SCADA系统主站A与从站B间身份认证的方法。

[0028] 与现有技术相比,本发明的有益效果如下:

[0029] 1、本发明选用对称多项式产生共享密钥,并将之作为对称加密密钥,报文交换过程中选用对称加密算法,降低了计算复杂度,且整个过程中产生的密钥数量比非对称方式少。符合SCADA系统主站A与从站B通信过程中轻量级的密码机制的需求,使得系统在应对紧急情况时仍能快速反应。

[0030] 2、本发明关注系统快速响应的同时,兼顾了密钥的安全性。由于传统的对称加密算法加解密使用的密钥相同,因此其安全性不仅受到加密算法本身复杂度的影响,密钥管

理的安全性问题也尤为突出。

[0031] 1) 会话密钥保密性增强

[0032] 在对称多项式加密过程中,通过对称多项式建立了密钥协商阶段使用的会话密钥,其中包含了主站A与从站B两者身份标识信息,有效地防止密钥被窃取。由于在二元t次多项式中,一共需要t+1个元素的值才能实现对于多项式的重构,所以攻击者需要至少截获t+1个成员的节点密钥值才能将多项式重构。由此可见,攻击者即使获取了整个通信系统中所有成员的节点密钥值,也无法计算出对称多项式的值,从而保证了会话密钥的安全性。而且通过节点计算的共享密钥是独立的,其他节点无法获取,具有良好的保密性和独立性。

[0033] 2) 主从站双向身份认证

[0034] 主站A与从站B利用自身身份标识 $ID_A$ 和 $ID_B$ 构建一元一次多项式 $f(ID_A, y)$ 和 $f(ID_B, y)$ 。通过建立会话,主站A、从站B分别计算出 $K_{AB} = f(ID_A, y) | y = ID_B$ 、 $K_{BA} = f(ID_B, y) | y = ID_A$ 。主从站交换彼此对称多项式计算结果,并比较 $K_{AB}$ 与 $K_{BA}$ 是否相同,完成相互认证与安全会话密钥的建立。在主从站对称多项式值交换过程中,实现了对彼此的身份认证,有效地防止了非法节点冒用,保证了传输消息的完整性和可用性,能有效避免消息被篡改和非法获取,能够较好地满足SCADA系统加密机制的要求。

## 附图说明

[0035] 通过阅读参照以下附图对非限制性实施例所作的详细描述,本发明的其它特征、目的和优点将会变得更明显:

[0036] 图1为本发明用于SCADA系统主站与从站间身份认证的方法主站与从站间身份认证系统的整体框架示意图;

[0037] 图2为本发明用于SCADA系统主站与从站间身份认证的方法主从站通信流程示意图;

[0038] 图3为本发明用于SCADA系统主站与从站间身份认证的方法Modbus TCP数据帧示意图;

[0039] 图4为本发明用于SCADA系统主站与从站间身份认证的方法主从站对称多项式示意图。

## 具体实施方式

[0040] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明,但不以任何形式限制本发明。应当指出的是,对本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变化和改进。这些都属于本发明的保护范围。

[0041] 由于SCADA系统需要在短时间内处理大量数据,因此轻量级的加密机制能保证系统中断后快速恢复,降低系统损失。采用对称加密在密钥节点数量与响应时间花费上具有优越性,符合系统轻量级加密机制的需求。但由于对称加密过程中使用的加解密密钥唯一,因此会话密钥的安全问题不容忽视,密钥存在泄露的隐患。由此可鉴,通信过程中密钥的保密传输十分重要。本发明通过在对称密钥产生环节引入二元对称多项式进行计算,解决了单一密钥在建立过程中容易泄露的安全问题,并以此保证会话密钥产生过程中的安全性,

实现主站与从站的身份认证。

[0042] 具体地,本发明用于SCADA系统主站与从站间身份认证的方法将对称多项式加密的方式引入SCADA系统中主站与从站的身份认证。在加密过程中运用分散密钥机制建立认证机制,使用了以身份标识(ID)为基础的密钥机制与对称多项式算法。在基于通信双方身份标识的密钥体系中,会话密钥从通信者唯一身份标识中衍生而来。主从站各自保存一个二元对称多项式,主站在通信建立过程中产生对称多项式系数,并传递给从站,以此保证主从站拥有相同的多项式函数。通信过程中,主从站利用其自身身份标识值计算多项式的值,并交换彼此身份标识值。最终主从站把两者身份标识值代入对称多项式进行计算,以此共享对称密钥。在此过程中,主从站均能通过使用基于对称多项式的密钥产生机制计算出会话密钥,且由多项式的对称性可知,双方计算结果相同。

[0043] 如图1所示,根据本发明所提供方法的具体实施过程分为3个主要的阶段,包括主从站建立连接阶段、主从站相互认证并协商密钥阶段和主从站加密通信阶段。为了更加清晰形象地阐述整个SCADA系统的主站A与从站B间身份认证的过程,附上相关附图并对其进行说明。

[0044] 在主从站建立连接阶段,主从站选用Modbus TCP作为应用层通信协议,它是基于TCP/IP网络协议建立,传输层采用TCP通信模式。端口502是Modbus TCP用于连接的专用端口,通过IP地址与端口实现寻址过程,由于TCP是面向连接的可靠通信,其自身包含了校验部分。在整个通信协议中,应用层使用Modbus协议,所以主要使用Master/Slave的通信架构。在数据传输前,首先应该通过使用套接字接口,在客户和主站A之间建立TCP/IP连接,一旦客户和主站A之间的通信连接建立完成,用户与主站A之间就可以进行报文交换与数据传输。Modbus TCP采用Master/Slave的模式进行信息的实时交换,在此模式下,主从站通信过程中主要涉及四种报文类型,即:请求、确认、指示、响应。

[0045] 具体地,主从站间采用Winsock构建Modbus TCP通信,其中Winsock套接字能够标识通信过程,套接字中涵盖主从站的IP地址、目前链接情况等信息,可以通过协议、地址、端口唯一确定套接字,主从站通过TCP/IP协议在网络中传输符合Modbus协议要求的信息帧。主站A采用并发模式,通过运用独立的线程处理每个从站B的请求,实现了系统的高效传输,套接字可以被应用程序请求调用,通过调用套接字实现系统资源的按需分配。

[0046] 连接建立过程中,主站A执行的操作如下:

[0047] 套接字创建完成后,必须首先对套接字库进行初始化,此时其端口号与IP地址均为空。通过调用bind()绑定套接字地址,实现对于通信端口号(502)和本地IP地址的写入操作,主站A使用listen()函数将套接字模式设置成被动,实现对从站B端发送请求的侦听,主站A通过accept()函数,提取从站B进程发送的链接请求,并调用send()与recv()函数实现信息的收发过程,最终通过close()函数关闭套接字,并利用cleanup()释放系统资源。具体地,如图2所示。

[0048] 从站B与主站A连接过程中执行的操作如下:

[0049] 首先通过socket()创建套接字,并通过connect()函数向主站A发送连接请求,send()与recv()函数可以实现通信过程中信息的收发。最终通过close()关闭套接字,并利用cleanup()实现系统资源的释放。具体地,如图2所示。

[0050] 通信过程中采用Modbus TCP数据帧作为主从站身份标识,数据帧格式如图3所示。

其中,MBAP表示整个Modbus TCP的头部,涵盖了整个数据帧的前7个Byte;事务处理标识符用来表示Modbus请求和响应的相关操作;协议标识符主要表示应用层选取的通信协议,通常取0表示应用层采用了用Modbus通信协议,取1则表示其他;长度用来表示从当前字节之开始计算,后续数据量的大小;单元标识符主要用于识别串行链路或其他链接在其他总线上的设备单元;功能码用来指明通信流程中具体执行的指令模式。

[0051] 由此可见,Modbus TCP数据帧不仅传递了通信信息,而且具有唯一性,能够用来标识主从站身份。因此,本发明使用Modbus TCP数据帧作为 $ID_A$ 与 $ID_B$ 。

[0052] 在主从站相互认证并协商密钥阶段,主站A与从站B交换身份标识符,并将身份标识符带入多项式进行计算。主站A与从站B交换对称多项式计算结果,如果结果一致,则主站A与从站B实现双向认证,并获得共享的对称多项式的值。主从站对称多项式计算流程如图4所示。

[0053] 具体地,对称多项式的定义如下:

[0054] 设 $f(x_1, x_2, \dots, x_n) \in P(x_1, x_2, \dots, x_n)$ ,若对任意的 $i, j (1 \leq i, j \leq n)$ 有:

[0055]  $f(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = f(x_1, \dots, x_j, \dots, x_i, \dots, x_n)$

[0056] 则称该多项式为对称多项式。

[0057] 下列n个多项式:

[0058]  $\sigma_1 = x_1 + x_2 + x_3 + \dots + x_n;$

[0059]  $\sigma_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + \dots + x_{n-1} x_n;$

[0060] ...

[0061]  $\sigma_n = x_1 x_2 x_3 \dots x_{n-1} x_n;$

[0062] 称为n个未知数 $x_1, x_2, \dots, x_n$ 的初等对称多项式。

[0063] 对称多项式的和、积仍是对称多项式,特别地,初等对称多项式的多项式仍为对称多项式。在一个对称多项式中,交换其中任意两个变量的值,对称多项式的值仍保持不变。

[0064] 对于二元t次多项式 $f(x, y)$ ,x,y表示两随机变量,若对任意x,y都满足 $f(x, y) = f(y, x)$ ,则称二元多项式 $f(x, y)$ 为对称二元多项式。二元t次对称多项式满足:

$$[0065] f(x, y) = \sum_{i,j=0}^t a_{ij} x^i y^j$$

[0066] 其中,二元t次对称多项式定义在有限域 $GF(q)$ 上,q的取值为大于 $10^k$ 的素数,k为密钥的长度(例如,密码长度为16位,则q可以取大于 $10^{16}$ 的大素数)。而且对于任意的i,j,都满足等式 $a_{ij} = a_{ji}$ 。

[0067] 主从站采用对称多项式建立会话密钥过程如下:

[0068] 主站A创建服务,产生对称多项式系数 $a_{ij}$ ( $a_{00}, a_{01}, a_{11}$ ),从站B输入服务器的IP地址与主站A进行连接,连接建立成功后从站B与主站A共享对称多项式参数。连接建立完毕后,主站A与从站B交换身份标识符,主从站均采用MODBUS TCP数据帧作为自身身份标识符。主从站将两者的身份标识符带入对称多项式进行计算,得到 $f(ID_A, ID_B)$ 与 $f(ID_B, ID_A)$ 。主站A与从站B交换对称多项式计算结果,如果 $f(ID_A, ID_B) = f(ID_B, ID_A)$ ,则主站A与从站B实现双向认证,并获得 $K_{AB} = f(ID_A, ID_B) = f(ID_B, ID_A)$ 。将扩展计算得到加密密钥 $K_{AB}$ 扩展成AES密钥,并采用AES对称加密算法对主从站间传送的数据内容进行加密。

[0069] 主从站加密通信阶段,把协商所得的对称多项式的值扩展成为128比特,使之符合AES密钥长度标准,最终采用AES算法对主从站间传送的数据内容进行加密传输并解密验证。

[0070] 具体地,由于AES加密区块固定,且密钥长度固定(本实施例选用128比特),应首先将对称多项式计算而得的结果进行扩展,使之符合AES加密需求。AES加密主要在一个 $4 \times 4$ 的“状态矩阵上进行”,通过“Add Round Key、Sub Bytes、Shift Rows、Mix Columns”四个步骤进行加密。AES具有加解密迅速、整体编码密度高的特点,且四个计算环节简洁明了,易于在软硬件上实施,整个过程对存储器的需求也相对较小,符合工业控制系统轻量级加密的需求。

[0071] 本发明还提供一种采用用于SCADA系统主站A与从站B间身份认证的方法的系统。

[0072] 以上对本发明的具体实施例进行了描述。需要理解的是,本发明并不局限于上述特定实施方式,本领域技术人员可以在权利要求的范围内做出各种变化或修改,这并不影响本发明的实质内容。在不冲突的情况下,本申请的实施例和实施例中的特征可以任意相互组合。

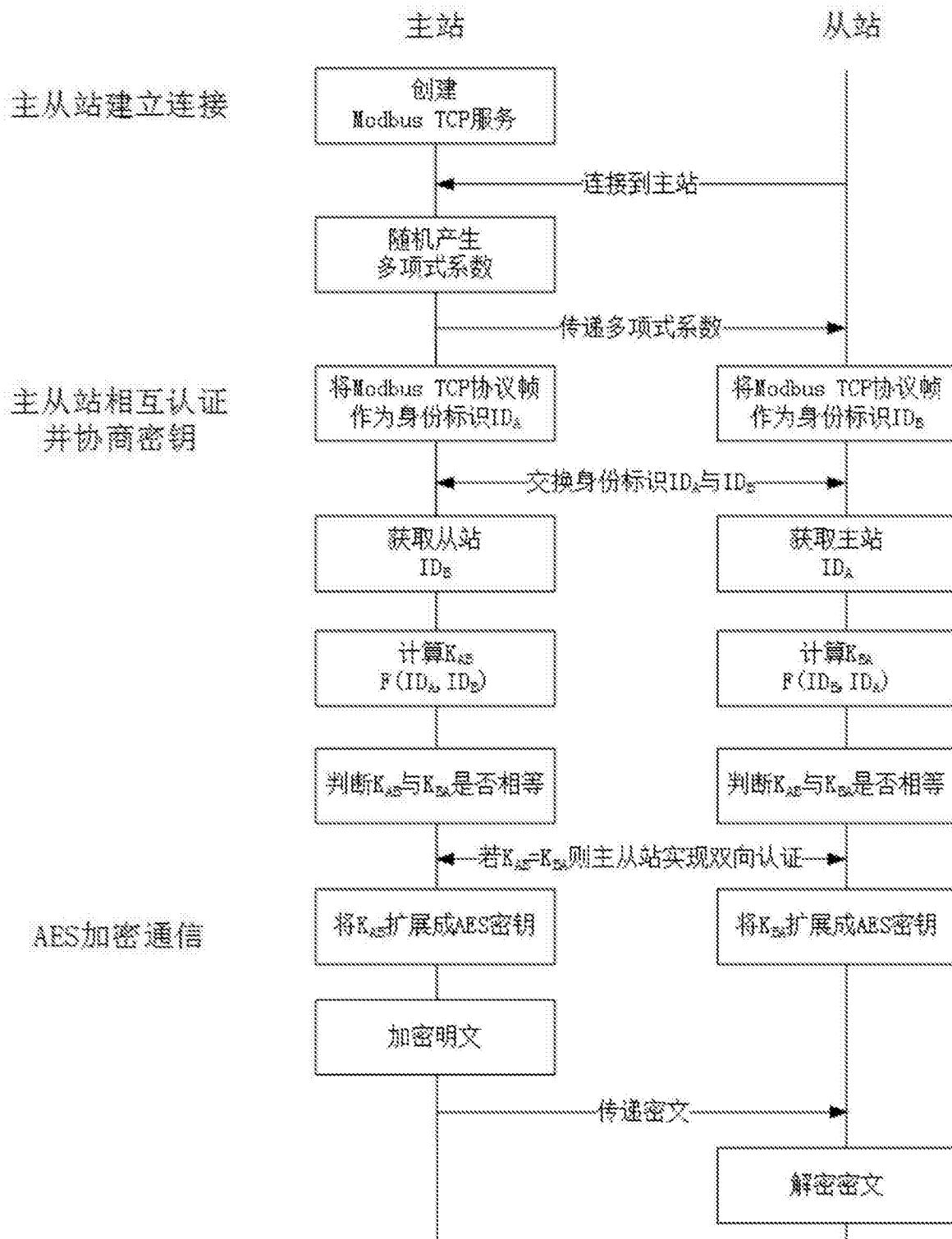


图1

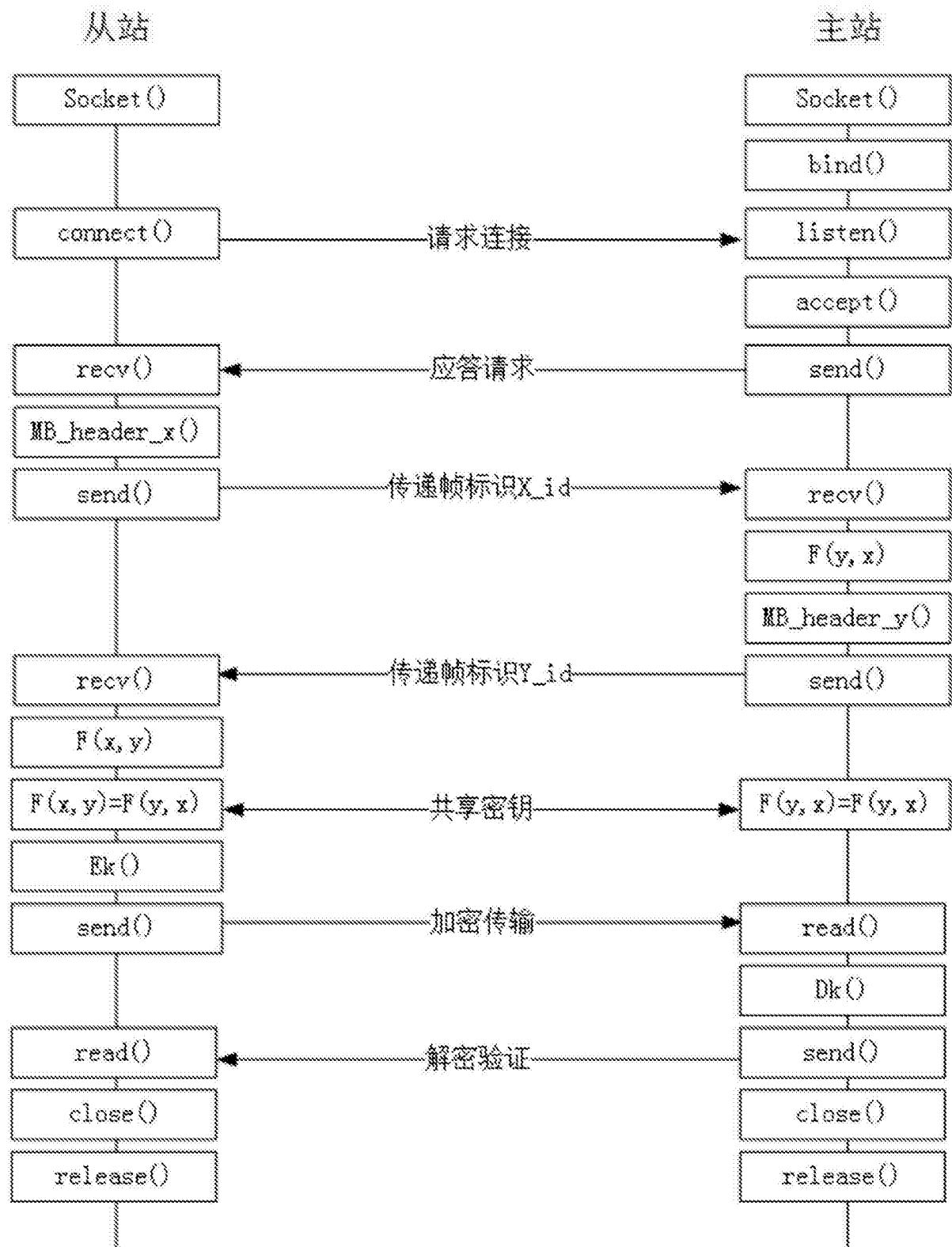


图2

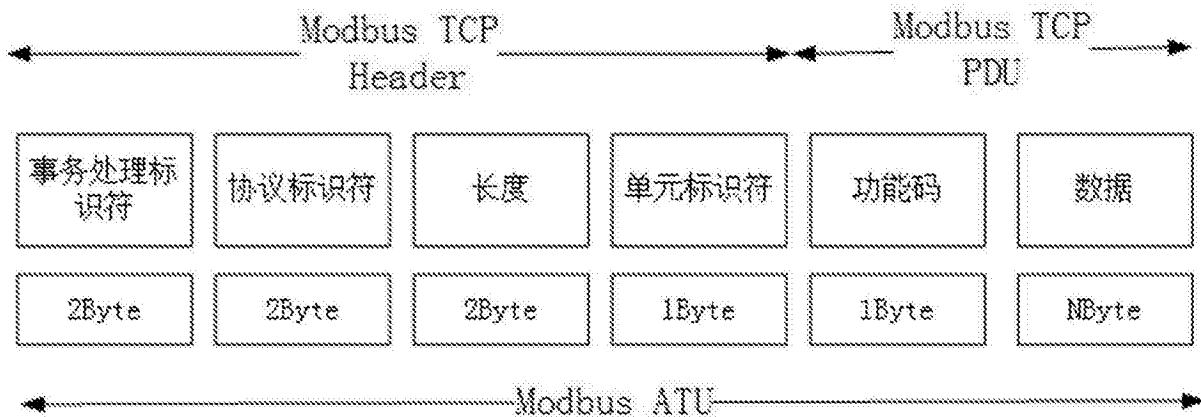


图3

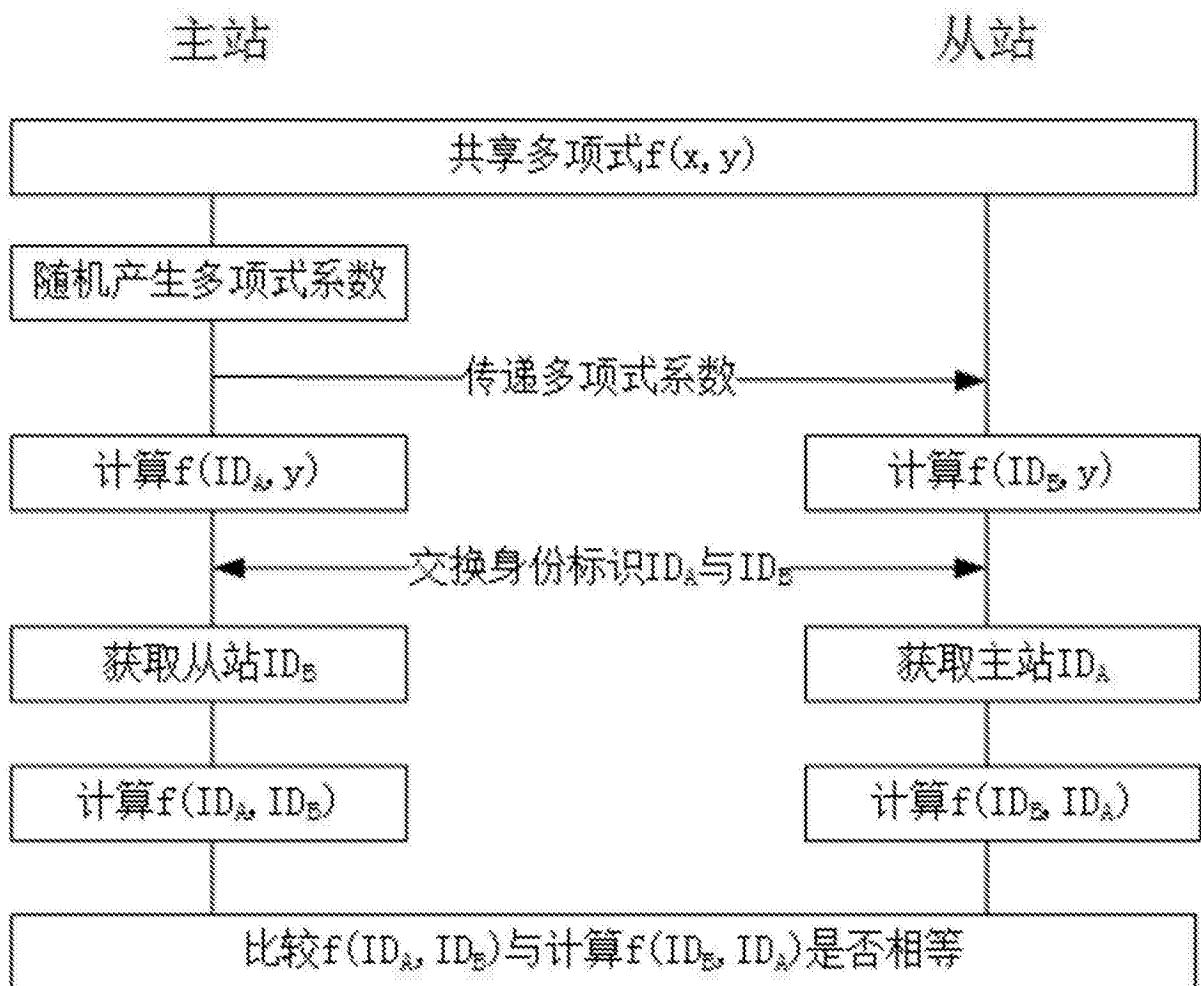


图4