



(12)发明专利

(10)授权公告号 CN 104994096 B

(45)授权公告日 2018.03.13

(21)申请号 201510381869.X

(56)对比文件

(22)申请日 2015.07.01

CN 104242447 A, 2014.12.24,

(65)同一申请的已公布的文献号

CN 103067201 A, 2013.04.24,

申请公布号 CN 104994096 A

杨西银 等.变电站二次系统安全防护建设.

(43)申请公布日 2015.10.21

《宁夏电力》.2012,(第6期),

(73)专利权人 中国南方电网有限责任公司

许勇刚 等.智能变电站信息安全防护体系

地址 510623 广东省广州市天河区珠江新城华穗路6号

研究.《电子测量技术》.2014,第37卷(第10期),

审查员 李红玲

(72)发明人 陶文伟 李金 张喜铭 胡荣
樊腾飞

(74)专利代理机构 广州知友专利商标代理有限公司 44104

代理人 周克佑

(51)Int.Cl.

H04L 29/06(2006.01)

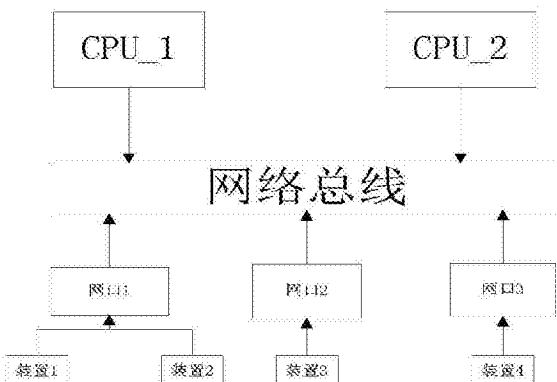
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法

(57)摘要

本发明目的在于为了保证站控层通信的安全性,克服现有技术中存在的不足,本发明提供一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法,采用本发明的方法配置的安全加固机制的智能变电站通讯管理装置的系统能够针对智能站中的通讯管理机,解决过站控层通信传输规约的安全问题。一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法,包括如下过程:硬件配置、传输安全加固和数据安全配置。



1. 一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法,其特征在于包括如下过程:硬件配置、传输安全加固和数据安全配置;

所述硬件配置的具体内容包括:首先,将多块CPU板挂接到虚拟网络总线上,为该CPU板及其接口板进行编号;其次,针对网络总线板对通讯口进行挂接处理,标识出通讯口具体隶属于哪块CPU板,在通讯口挂接站内二次保护及测控装置,并为该站内二次保护及测控装置配置通讯规约;最后配置网络安全参数;

传输安全加固过程采用安全传输层协议TLS,该安全传输层协议TLS协议由两层组成:TLS记录协议(TLS Record)和TLS握手协议(TLS Handshake);具体的传输安全加固过程如下:首先利用TLS握手协议处理对等用户的认证信息;接着,在通讯过程建立后利用TLS记录协议处理数据的加密;接收到加密后的消息后,首先加密消息被解密,然后校验认证码值,解压缩,重组,最后传递给协议的高层客户;

所述数据安全配置过程包括以下步骤:

(1) 配置通讯管理机的系统的硬件参数:配置CPU板个数、板件通讯口的挂接关系;

(2) 配置通讯管理机的规约参数:配置通讯口与变电站二次保护及测控装置的挂接关系、通讯管理机使用的通讯协议以及是否使用安全认证;

(3) 配置证书:本地证书文件路径、CA证书文件路径,如果是服务端且只允许指定的客户端证书接入,则配置“添加对端证书”来接入;

(4) 配置TLS参数:配置TLS重协商所需的固定时间大小、配置TLS重协商的总字节数、配置密钥更新周期、TLS报文生存周期。

2. 根据权利要求1所述的配置方法,其特征在于:所述为该CPU板及其接口板进行编号按照离电源板最近的第一块CPU板编号为1依次递增的顺序为原则。

3. 根据权利要求1所述的配置方法,其特征在于:所述配置网络安全参数是针对每台站内二次保护及测控装置进行配置作为服务器端还是客户端的角色,依据角色不同配置独立的安全证书、TLS重协商周期、字节数以及密钥更换周期,或者根据每台站内二次保护及测控装置实际情况独立配置。

4. 根据权利要求1所述的配置方法,其特征在于:所述TLS握手协议处理过程中使用了通过配置获取的公共密钥和证书,并协商算法和加密实际数据传输的密钥,该TLS握手协议处理过程在TLS记录协议之前进行。

5. 根据权利要求1所述的配置方法,其特征在于:所述TLS握手协议处理过程中,客户端和服务器端利用这TLS握手协议提供的10种消息相互认证,协商哈希函数和加密算法并相互提供产生加密密钥的机密数据。

6. 根据权利要求1所述的配置方法,其特征在于:所述TLS记录协议处理数据的加密即TLS记录协议得到要发送的消息之后,将消息分成易于处理的数据分组,计算数据分组的消息认证码,并加密消息再发送该加密的消息。

7. 根据权利要求1所述的配置方法,其特征在于:所述加密解密时均使用对称算法。

一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法

技术领域

[0001] 本发明涉及电力信息安全领域,具体是设计一种适用于智能变电站站内二次系统传输规约加密传输的通信管理机的模块。

背景技术

[0002] 智能电网极大的促进了电力公司信息化业务的发展,随之而来的是信息安全问题的日益突出。随着电网终端设备智能化的浪潮,基于TCP/IP协议的电力标准传输规约在电力系统中得到广泛应用,这些技术的应用,一方面实现了设备运行的网络化和自动化,大大提高了设备的互操作性,另一方面,传输规约的开放性和标准性也带来很多信息安全问题。其原因在于,在传输规约设计之初,设计者很少考虑任何信息安全防护措施;同时,通过TCP/IP网络的数据通信也面临着传统TCP/IP网络的安全风险与隐患。传输规约安全性的缺失使得攻击者一旦利用安全漏洞,就可直接通过传输规约实现对电网系统和设备的控制。

发明内容

[0003] 本发明为了克服现有技术中存在的不足,针对智能站中的通讯管理机提供一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法,解决过站控层通信传输规约的安全问题。

[0004] 为实现上述目的,本发明采用如下技术方案:

[0005] 一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法,包括如下过程:硬件配置、传输安全加固和数据安全配置;

[0006] 所述硬件配置的具体内容包括:首先,将多块CPU板挂接到虚拟网络总线上,为该CPU板及其接口板进行编号,编号按照离电源板最近的第一块CPU板编号为1依次递增的顺序为原则;其次,针对网络总线板对通讯口进行挂接处理,标识出通讯口具体隶属于哪块CPU板,在通讯口挂接站内二次保护及测控装置,并为该站内二次保护及测控装置配置通讯规约;最后配置网络安全参数。所述配置网络安全参数是针对每台站内二次保护及测控装置进行配置作为服务器端还是客户端的角色,依据角色不同配置独立的安全证书、TLS重协商周期、字节数以及密钥更换周期,或者根据每台站内二次保护及测控装置实际情况独立配置。

[0007] 传输安全加固过程采用安全传输层协议TLS,该安全传输层协议TLS用于在两个通信应用程序之间提供保密性和数据完整性。该安全传输层协议TLS协议由两层组成:TLS记录协议(TLS Record)和TLS握手协议(TLS Handshake);具体的传输安全加固过程如下:首先利用TLS握手协议处理对等用户的认证信息,在TLS握手协议处理过程中使用了通过配置获取的公共密钥和证书,并协商算法和加密实际数据传输的密钥,该TLS握手协议处理过程在TLS记录协议之前进行;

[0008] 所述TLS握手协议处理过程中,客户端和服务器端利用这TLS握手协议提供的10种

消息相互认证，协商哈希函数和加密算法并相互提供产生加密密钥的机密数据。

[0009] 接着，在通讯过程建立后利用TLS记录协议处理数据的加密，即TLSTLS记录协议得到要发送的消息之后，将消息分成易于处理的数据分组，计算数据分组的消息认证码，并加密消息再发送该加密的消息；接收到加密后的消息后，首先加密消息被解密，然后校验认证码值，解压缩，重组，最后传递给协议的高层客户。所述加密解密时均使用对称算法。

[0010] 所述数据安全配置过程包括以下步骤：

[0011] (1) 配置通讯管理机的系统的硬件参数：配置CPU板个数、板件通讯口的挂接关系；

[0012] (2) 配置通讯管理机的规约参数：配置通讯口与变电站二次保护及测控装置的挂接关系、通讯管理机使用的通讯协议以及是否使用安全认证；

[0013] (3) 配置证书：本地证书文件路径、CA证书文件路径，如果是服务端且只允许指定的客户端证书接入，则配置“添加对端证书”来接入；

[0014] (4) 配置TLS参数：配置TLS重协商所需的固定时间大小、配置TLS重协商的总字节数、配置密钥更新周期、TLS报文生存周期。

[0015] 有益效果：本发明的安全加固机制的智能变电站通讯管理机的系统能够保证站控层通信的安全性。

附图说明

[0016] 图1装置硬件结构示意图；

[0017] 图2通讯交互过程图。

具体实施方式

[0018] 下面结合实施例和附图对本发明作更进一步的说明。

[0019] 在智能变电站自动化系统工程实施过程中，配置工程师首先需要根据全站的安全需求以及网络拓扑来对通讯机进行合理配置。

[0020] 本发明即提供一种动态加载于智能变电站通讯管理机的安全加固机制模块的配置方法，包括如下内容：硬件配置、传输安全加固和数据安全配置；

[0021] 所述硬件配置的具体内容包括：如图1所示，首先，为了将多块CPU板挂接到虚拟网络总线上，为该CPU板及其接口板进行编号，编号按照离电源板最近的第一块CPU板编号为1依次递增的顺序为原则，最大支持5块。其次，针对网络总线板对通讯口进行挂接处理，标识出通讯口具体隶属于哪块CPU板，在通讯口挂接站内二次保护及测控装置，并为该站内二次保护及测控装置配置通讯规约。最后配置网络安全参数，所述网络安全参数是针对每台站内二次保护及测控装置进行配置作为服务器端还是客户端的角色，依据角色不同配置独立的安全证书、TLS重协商周期、字节数以及密钥更换周期，也可根据每台站内二次保护及测控装置实际情况独立配置。

[0022] 传输安全加固采用安全传输层协议TLS，该安全传输层协议TLS用于在两个通信应用程序之间提供保密性和数据完整性。该安全传输层协议TLS协议由两层组成：TLS记录协议(TLS Record)和TLS握手协议(TLS Handshake)。首先利用TLS握手协议处理对等用户的认证信息(对等用户指采用分散管理的方式，网络中的每个用户既作为客户端又可作为服务器来工作)，装置内部软件也分处理数据单元和数据加密、解密单元是多个软件模块组成

的,这里指在通讯管理机内部软件并不区分服务器还是客户端,这两个角色都可以胜任。

[0023] 变电站二次保护及测控装置是指客观上在变电站中起实际应用作用的装置,客户端和服务器端是通讯上的概念意在指明双方(通讯机与二次保护、测控装置之间)沟通时的角色、对等用户是指在同一交换机上的所有成员(包括通讯机、变电站二次保护及测控装置),之所以如此写是为了更好的区分在不同层面(实际作用,还是通讯过程,异或是网络层面)。

[0024] 在TLS握手协议处理过程中使用了通过配置获取的公共密钥和证书,并协商算法和加密实际数据传输的密钥,该TLS握手协议处理过程在TLS记录协议之前进行。

[0025] 握手时,客户端和服务器端利用这TLS握手协议提供的10种消息相互认证,协商哈希函数和加密算法并相互提供产生加密密钥的机密数据。

[0026] 通讯过程中会在加密算法中用到这些加密密钥,从而提供数据保密性和一致性保护。在通讯过程建立后利用TLS记录协议处理数据的加密,即TLS记录协议得到要发送的消息之后,将消息分成易于处理的数据分组,进行数据压缩处理(可选),计算数据分组的消息认证码,并加密消息再发送该加密的消息;接收到加密后的消息后,首先加密消息被解密,然后校验认证码值,解压缩,重组,最后传递给协议的高层客户。考虑到变电站内对通讯可靠性和性能的需求,加密解密时均使用对称算法。

[0027] 所述数据安全配置包括以下步骤:

[0028] (21) 配置通讯管理机的系统的硬件参数:配置CPU板个数、板件通讯口的挂接关系;

[0029] (22) 配置通讯管理机的规约参数:配置通讯口与变电站二次保护及测控装置的挂接关系、通讯管理机使用的通讯协议以及是否使用安全认证;

[0030] (23) 配置证书:本地证书文件路径、CA证书文件路径,如果是服务端且只允许指定的客户端证书接入,则配置“添加对端证书”来接入;

[0031] (24) 配置TLS参数:配置TLS重协商所需的固定时间大小、配置TLS重协商的总字节数、配置密钥更新周期、TLS报文生存周期。

[0032] 作为应用示例描述了利用本发明方法配置了安全加固机制模块的通讯管理机与变电站内二次设备之间的通信流程,通讯管理机作为客户端与作为服务器端的二次设备服务器进行安全密文通信,具体流程如图2所示,包括以下步骤,

[0033] (1) 客户端需要建立通信对象IP地址与密钥对照表;

[0034] (2) 对服务器端发起连接请求,普通的TCP握手

[0035] (3) 收到肯定响应后开始进行TLS连接,此时传送本地证书文件进行认证关联

[0036] (4) 服务器端验证通过后传送服务器端密钥回客户端,利用解密模块进行验证

[0037] (5) 验证通过后进行正常TCP通讯,此时报文为客户端与服务器端商议后的密钥加密后报文形式。

[0038] (6) 在通讯过程中会根据TLS设置的参数比如时间周期或者数据流量进行判断,当某项达到设定值后,重新与服务器协商更换当前密钥继续通信。

[0039] 本发明的通讯管理机进行消息认证和消息加密能够实现如下效果:

[0040] (1) 通过数字签名,提供系统中各个独立通讯管理机装置的双向身份认证;

[0041] (2) 通过加密,提供传输层认证、加密密钥的机密性;

- [0042] (3) 通过加密, 提供传输层及以上层次消息的机密性, 防止窃听;
- [0043] (4) 通过消息鉴别码, 提供传输层及以上层次消息的完整性;
- [0044] (5) 通过定义传输序列号有效性, 防止传输层的重放和欺骗;
- [0045] (6) 使用RSA算法对数据加密;
- [0046] (7) 通过配置会自动重新协商密钥;
- [0047] 本发明的实施方式不限于此, 在本发明上述基本技术思想前提下, 按照本领域的普通技术知识和惯用手段对本发明内容所做出其它多种形式的修改、替换或变更, 均落在本发明权利保护范围之内。

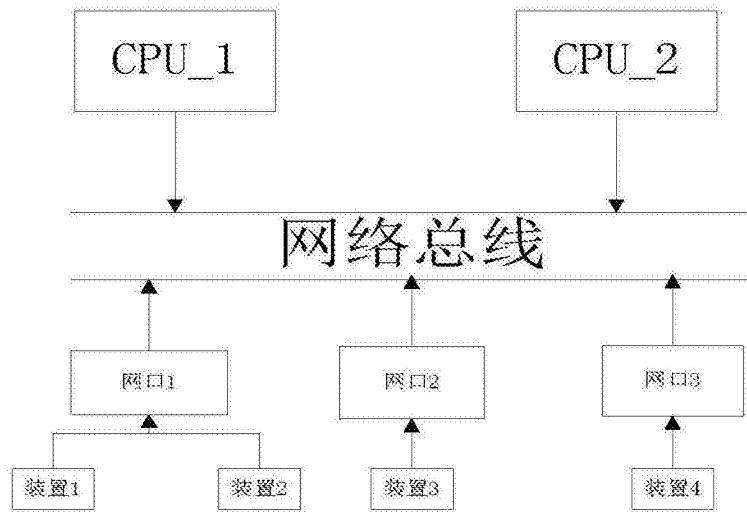


图1

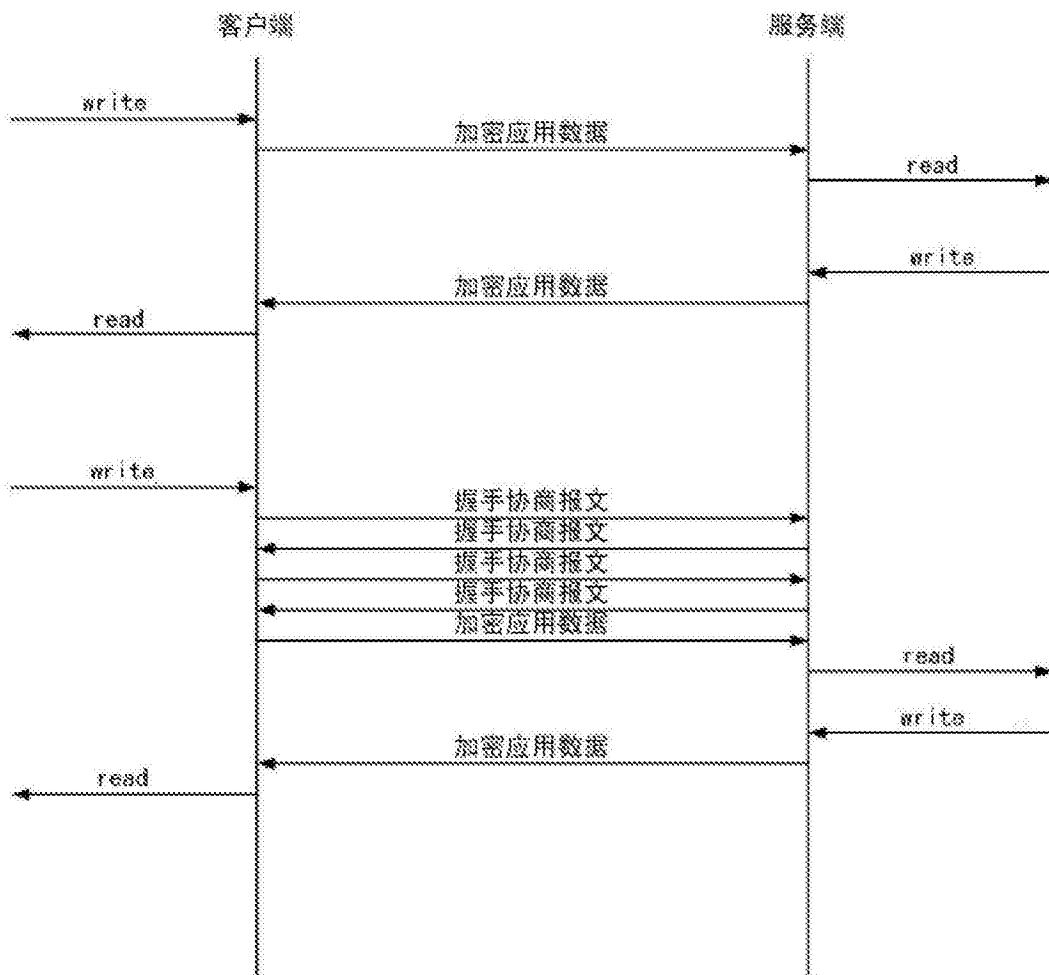


图2