(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 102984221 B
(45)授权公告日 2016.01.13

(21)申请号 201210455284.4

(22)申请日 2012.11.14

(73)专利权人 西安工程大学
地址 710048 陕西省西安市金花南路19号

(72)发明人 王会燃 黄国兵 马瑞芳 加云岗 薛纪文 卓爱霞

(74)专利代理机构 西安弘理专利事务所 61214
代理人 张瑞琪

(51)Int.Cl.
*H04L 29/08*(2006.01)
*H04L 9/32*(2006.01)
*H04L 9/06*(2006.01)

(56)对比文件
US 2005005093 A1,2005.01.06,
CN 102365884 A,2012.02.29,
CN 1864384 A,2006.11.15,
CN 102281203 A,2011.12.14,
CN 101640581 A,2010.02.03,

审查员 加玉

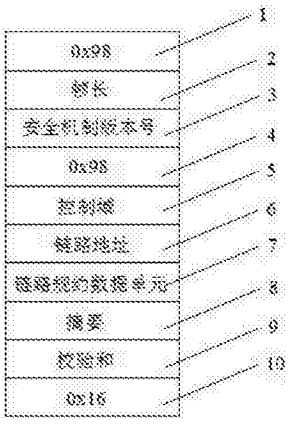
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种电力远动终端的传送方法

(57)摘要

本发明公开了一种电力远动终端的传送方法，远动终端传送的数据被封装成帧，一个帧包括10个字段：第一字段和第四字段固定为十六进制数0x98，表示帧的开始；帧长字段的值等于从控制域开始到校验和之前所有字节的字节个数；安全机制版本号字段表示通信采用安全机制的版本；控制域字段规定通信的工作方式；链路地址字段表示通信的目标地址；链路规约数据单元字段用来封装应用层数据；摘要字段用来存储完整性检验算法产生的消息摘要；校验和字段用于检验通信过程中帧的数据是否发生变化；第十字段固定为十六进制数0x16，表示帧的结束。本发明克服了电网自动化系统规模较大时电力远动终端通信时的安全威胁问题，防止通信内容被篡改或窃听。




CN 102984221 B

1. 一种电力远动终端的传送方法，其特征在于：电力远动终端传送的数据被封装成帧，一个帧包括 10 个字段；

第一字段 (1) 和第四字段 (4) 固定为十六进制数 0x98，表示帧的开始；

帧长字段 (2) 占一个字节，其值等于从控制域开始到校验和之前所有字节的字节个数；

安全机制版本号字段 (3) 占一个字节，表示目前通信采用安全机制的版本；

控制域字段 (5) 占一个字节，规定通信的工作方式；

链路地址字段 (6) 占二个字节，表示通信的目标地址；

链路规约数据单元字段 (7) 用来封装应用层数据；

摘要字段 (8) 用来存储完整性检验算法产生的消息摘要；

校验和字段 (9) 占一个字节，用于检验通信过程中帧的数据是否发生变化；

第十字段 (10) 固定为十六进制数 0x16，表示帧的结束；

所述电力远动终端发送帧的过程如下：

(1) 远动终端按照完整性检验算法计算消息摘要；

(2) 远动终端按照加密机制对链路规约数据单元的数据进行加密处理；

(3) 远动终端按照上述帧的结构构造帧；

(4) 远动终端发送帧；

(5) 远动终端等待接收方的响应；

(6) 如果在规定是时间内，收到接收方的确认，该帧发送完成；

(7) 如果在规定是时间内，没有收到接收方的确认，或接收方给出“完整性检验错”信息，则重传该帧。

2. 根据权利要求 1 所述的电力远动终端的传送方法，其特征在于：所述电力远动终端接收帧的过程如下：

(1) 远动终端等待接收数据；

(2) 收到一个完整帧；

(3) 远动终端按照加密机制对链路规约数据单元的数据进行解密处理；

(4) 远动终端按照完整性检验算法计算消息摘要。

# 一种电力远动终端的传送方法

## 技术领域

[0001] 本发明属于电力自动化系统技术领域，涉及一种电力远动终端的传送方法。

## 背景技术

[0002] 电力是国民经济所依赖的一种最重要的能源。供电系统由发电厂、输出线路、配电系统及负荷等组成，并由调度中心对全系统进行统一管理。远动终端 (RTU) 工作于发电厂或变电所，实时采集电网的运行信息，并通过各种通信方式把采集的信息送往调度中心。RTU 是电网自动化系统成功运行的基础部件。

[0003] 目前，RTU 常采用的规约有：我国电力部制定的循环式数据远动规约 (Cyclic Digital Transmit, 简称 CDT)、国际电工委员会制订的远动设备及系统规约 IEC60870-5、美国电力工程协会制订的分布式网络规约 DNP3.0。这些规约存在的一个不足之处是没有采用安全机制。以前的电网自动化系统规模比较小，并且使用专网通信，安全威胁不是很突出。随着社会信息化的进展和管理要求的提高，自动化电网逐步实现全国联网，并可能与公网 Internet 连接，安全威胁会日益严重。

## 发明内容

[0004] 本发明的目的是提供一种电力远动终端的传送方法，解决了现有电力远动终端通信时的安全威胁问题，防止通信内容被篡改或窃听。

[0005] 本发明所采用的技术方案是：一种电力远动终端的传送方法，电力远动终端传送的数据被封装成帧，一个帧包括 10 个字段；

[0006] 第一字段和第四字段固定为十六进制数 0x98，表示帧的开始；

[0007] 帧长字段占一个字节，其值等于从控制域开始到校验和之前所有字节的字节个数；

[0008] 安全机制版本号字段占一个字节，表示目前通信采用安全机制的版本；

[0009] 控制域字段占一个字节，规定通信的工作方式；

[0010] 链路地址字段占二个字节，表示通信的目标地址；

[0011] 链路规约数据单元字段用来封装应用层数据；

[0012] 摘要字段用来存储完整性检验算法产生的消息摘要；

[0013] 校验和字段占一个字节，用于检验通信过程中帧的数据是否发生变化；

[0014] 第十字段固定为十六进制数 0x16，表示帧的结束。

[0015] 本发明的特征还在于，

[0016] 电力远动终端发送帧的过程如下：

[0017] (1) 远动终端按照完整性检验算法计算消息摘要；

[0018] (2) 远动终端按照加密机制对链路规约数据单元的数据进行加密处理；

[0019] (3) 远动终端按照上述帧的结构构造帧；

[0020] (4) 远动终端发送帧；

[0021] (5) 远动终端等待接收方的响应；

[0022] (6) 如果在规定是时间内，收到接收方的确认，该帧发送完成；

[0023] (7) 如果在规定是时间内，没有收到接收方的确认，或接收方给出“完整性检验错”信息，则重传该帧。

[0024] 电力远动终端接收帧的过程如下：

[0025] (1) 远动终端等待接收数据；

[0026] (2) 收到一个完整帧；

[0027] (3) 远动终端按照加密机制对链路规约数据单元的数据进行解密处理；

[0028] (4) 远动终端按照完整性检验算法计算消息摘要。

[0029] 本发明的有益效果是：本发明电力远动终端通过将电力远动终端传送的数据封装成帧，克服了电网自动化系统规模较大时，电力远动终端通信时的安全威胁问题，防止了通信内容被篡改或窃听。

## 附图说明

[0030] 图 1 是本发明中帧的结构图。

[0031] 图中，1. 第一字段，2. 帧长字段，3. 安全机制版本号字段，4. 第四字段，5. 控制域字段，6. 链路地址字段，7. 链路规约数据单元字段，8. 摘要字段，9. 校验和字段，10. 第十字段。

## 具体实施方式

[0032] 下面结合附图和具体实施方式对本发明进行详细说明。

[0033] 一种电力远动终端的传送方法，电力远动终端传送的数据被封装成帧，参见图 1，一个帧包括 10 个字段；

[0034] 第一字段 1 和第四字段 4 固定为十六进制数 0x98，表示帧的开始；

[0035] 帧长字段 2 占一个字节，其值等于从控制域开始到校验和之前所有字节的字节个数；

[0036] 安全机制版本号字段 3 占一个字节，表示目前通信采用安全机制的版本；

[0037] 控制域字段 5 占一个字节，规定通信的工作方式；

[0038] 链路地址字段 6 占二个字节，表示通信的目标地址；

[0039] 链路规约数据单元字段 7 用来封装应用层数据；

[0040] 摘要字段 8 用来存储完整性检验算法产生的消息摘要；

[0041] 校验和字段 9 占一个字节，用于检验通信过程中帧的数据是否发生变化；

[0042] 第十字段 10 固定为十六进制数 0x16，表示帧的结束。

[0043] 电力远动终端发送帧的过程如下：

[0044] (1) 远动终端按照完整性检验算法计算消息摘要，计算时，需要用户提供一个密钥，密钥最大长度为 64 个字节；完整性检验计算范围包括帧长字段 2、安全机制版本号字段 3、链路地址字段 6 和链路规约数据单元字段 7，计算出的消息摘要长度为 16 个字节；

[0045] (2) 远动终端按照加密机制对链路规约数据单元的数据进行加密处理，由于采用 PKCS7 填充方式，所以加密后数据的最后一个字节表示了填充长度；

[0046] (3) 远动终端按照图 1 的格式构造帧 ;

[0047] (4) 远动终端发送帧 ;

[0048] (5) 远动终端等待接收方的响应 ;

[0049] (6) 如果在规定是时间内,收到接收方的确认,该帧发送完成 ;

[0050] (7) 如果在规定是时间内,没有收到接收方的确认,或接收方给出“完整性检验错”信息,则重传该帧。

[0051] 电力远动终端接收帧的过程如下 :

[0052] (1) 远动终端等待接收数据 ;

[0053] (2) 收到一个完整帧 ;

[0054] (3) 远动终端按照加密机制对链路规约数据单元的数据进行解密处理,由于解密后数据的最后一个字节表示了填充长度 ( 设为 k),因此取除解密后数据尾部的 k 个字节,得到链路规约数据单元原始数据 ;

[0055] (4) 远动终端按照完整性检验算法计算消息摘要,如果计算出消息摘要与接收到帧的摘要字段 8 的值相等,说明接收到的帧完整、可以接收,该帧接收完成并返回确认信息 ;如果计算出消息摘要与接收到帧的摘要字段 8 的值不相等,说明接收到的帧已被篡改,丢弃该帧,并向发送方回传“完整性检验错”信息。

[0056] 本发明的加密机制采用美国国家标准局制订的数据加密标准 DES、电子源码书 (Electronic Code Book) 处理模式和 PKCS7 填充方式,加密针对链路规约数据单元的数据进行。

[0057] 本发明的完整性检验机制采用基于密钥的哈希运算消息认证码 (keyed-Hash Message Authentication Code,简称 HMAC),HMAC 以一个密钥和一个消息为输入,利用哈希算法,生成一个消息摘要作为输出 ;本发明采用 MD5 哈希算法,产生的消息摘要长度为 128 位。完整性检验计算范围包括帧长字段、安全机制版本号字段、链路地址字段和链路规约数据单元字段 ;完整性检验是针对链路规约数据单元的数据的原文进行计算,而不是密文。

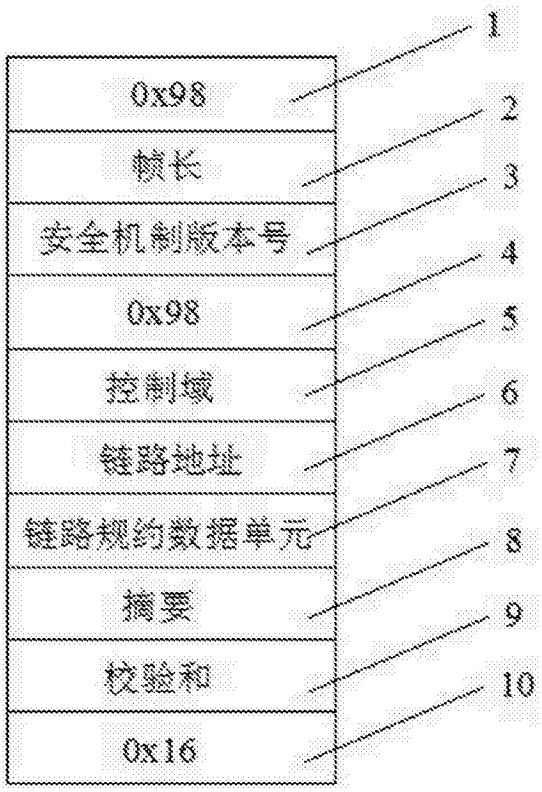

0x98
帧长
安全机制版本号
0x98
控制域
链路地址
链路规约数据单元
摘要
校验和
0x16
1
2
3
4
5
6
7
8
9
10

图 1