

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 10 月 20 日 (20.10.2016)



(10) 国际公布号
WO 2016/165675 A1

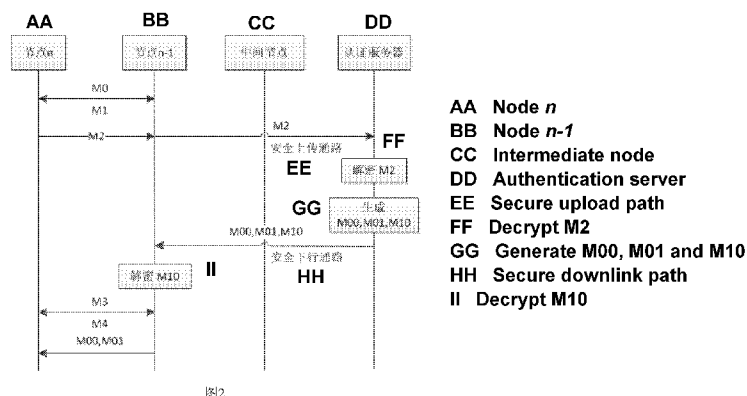
- (51) 国际专利分类号:
H04W 12/04 (2009.01)
- (21) 国际申请号: PCT/CN2016/081247
- (22) 国际申请日: 2016 年 5 月 6 日 (06.05.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510182163.0 2015 年 4 月 17 日 (17.04.2015) CN
- (71) 申请人: 国家电网公司 (STATE GRID CORPORATION OF CHINA) [CN/CN]; 中国北京市西城区西长安街 86 号, Beijing 100031 (CN)。全球能源互联网研究院 (GLOBAL ENERGY INTERCONNECTION RESEARCH INSTITUTE) [CN/CN]; 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。南京大学 (NANJING UNIVERSITY) [CN/CN]; 中国江苏省南京市鼓楼区汉口路 22 号, Jiangsu 210093 (CN)。国网浙江省电力公司 (STATE GRID ZHEJIANG ELECTRIC POWER COMPANY) [CN/CN]; 中国浙江省杭州市西湖区黄龙路 8 号, Zhejiang 310007 (CN)。

- (72) 发明人: 郭经红 (GUO, Jinghong); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。姚继明 (YAO, Jiming); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。黄红兵 (HUANG, Hongbing); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。范驊程 (FAN, Sucheng); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。李炳林 (LI, Binglin); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。梁云 (LIANG, Yun); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。张浩 (ZHANG, Hao); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。王瑶 (WANG, Yao); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。张旭苹 (ZHANG, Xuping); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。许国良 (XU, Guoliang); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。王萍 (WANG, Ping); 中国北京市昌平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。

[见续页]

(54) Title: SECURE COMMUNICATION METHOD OF WIRELESS COMMUNICATION NETWORK BASED ON POWER TRANSMISSION NETWORK

(54) 发明名称: 一种面向输电线路无线通信网络的安全通信方法



(57) Abstract: Provided is a secure communication method of a wireless communication network based on a power transmission network. The method comprises: initializing the wireless communication network, and determining whether a node is newly added, and if so, then authenticating the newly added node and allocating a key for a new device; uploading, by an added node n and via a communicated node $n-1$, state data to a control center; issuing a control command by the control center; checking a link state in real time, and determining whether a malfunctioning node is present, and if so, then using a link self-healing method to repair the wireless communication network. The method provided in the present invention proposes "an adjacent i node key structure" and applies an asymmetrical encryption algorithmic, such that a protocol supports random access of the new device, autonomous broken link monitoring and network repairing, thus addressing, on the basis of ensuring communication security, the problem of vulnerability brought by the network structure, and improving network flexibility.

(57) 摘要:

[见续页]



WO 2016/165675 A1



平区小汤山镇大东流村顺沙路 270 号, Beijing 102211 (CN)。

(74) **代理人:** 北京安博达知识产权代理有限公司 (AMBOYNA INTELLECTUAL PROPERTY AGENT CO., LTD.); 中国北京市海淀区大钟寺 13 号院 1 号楼华杰大厦 B215, Beijing 100098 (CN)。

(81) **指定国** (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国** (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 关于申请人有权要求在先申请的优先权(细则 4.17(iii))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。
— 包括关于请求恢复一项或多项优先权要求的信息(细则 26 之二.3 和 48.2(b)(vii))。

本发明提供了一种面向输电线路无线通信网络的安全通信方法, 包括: 所述方法包括: 初始化所述无线通信网络, 判断是否新增节点, 若有则对新增节点进行认证并为新设备分配密钥; 新增的所述节点 n 通过已通信的节点 $n-1$ 向控制中心上传状态数据; 所述控制中心下发控制命令; 实时检查链路状态, 判断是否出现故障节点, 若出现则运用链路自愈方法修复所述无线通信网络。本发明提供的方法中, 提出了"相邻 i 节点密钥结构"并应用了非对称加密算法, 使协议支持新设备随时接入以及自主对于断点进行监测和网络恢复, 在保证通信安全的基础上克服了由于网络结构本身带来的脆弱性问题, 并且提高了网络的灵活性。

一种面向输电线路无线通信网络的安全通信方法

技术领域

本发明涉及一种电力系统通信技术领域的方法，具体讲涉及一种面向输电线路无线通信网络的安全通信方法。

背景技术

近年来，输电线路的状态监测技术在国内得到一定程度的发展，主要表现为线路覆冰监测技术、绝缘子污秽状况监测技术、线路偷盗监测技术、导线温度监测技术等的研究和应用。在充分利用先进的监测设备和诊断技术的基础上，建立全方位和多要素的输电线路实时监测系统，及时预告灾害信息，实现故障快速定位，缩短故障恢复时间，有效提高供电的可靠性。各类状态监测信息的可靠传输离不开健壮的通信网络支撑。目前，主要输电线路上的网络铺设以 OPGW 为主，其拥有速度快，容量大，抗干扰能力强等优点。但同时，考虑到设备成本、能源供给（设备不可通过高压输电线路直接供电）等问题，在线路区域不是每个杆塔都配备有 OPGW 接入点，在实际环境中，相隔一定距离才有一个接入点。因此，其他杆塔上的节点数据信息需要通过一个链式无线网络（因为输电线路为线型）传输给接入点再通过 OPGW 传输。

由于电力行业的数据安全要求特殊性（通信网络上传的数据可以为电力公司的输电线路检修、巡检提供辅助决策），再加上无线网络本身的开放性，所以需要一套完整的网络安全协议来对通信网络进行保护。包括对于设备是否被伪造和替换、传输过程中数据的完整性、数据本身的加密保护，同时由于实际应用的需要，要考虑在网络构建完成后如何将新的节点加入以完成的网络中。对于链式网络结构本身的对于断点的脆弱性，也要考虑如何通过协议层来解决恢复。

针对上述问题，本发明提供一种新的面向输电线路无线通信网络的安全通信方法。

发明内容

为克服上述现有技术的不足，本发明提供一种面向输电线路无线通信网络的安全通信方法。

实现上述目的所采用的解决方案为：

一种面向输电线路无线通信网络的安全通信方法，所述方法包括：

初始化所述无线通信网络，判断是否新增节点，若有则对新增节点进行认证并为新设

备分配密钥;

新增的所述节点 n 通过已通信的节点 n-1 向控制中心上传状态数据;

所述控制中心下发控制命令;

实时检查链路状态, 判断是否出现故障节点, 若出现则运用链路自愈方法修复所述无线通信网络。

优选地, 所述对新增的节点进行认证, 包括:

S101、所述节点 n 向已安全验证的前一节点 n-1 发送请求交互信息 M0, 所述节点 n-1 接收请求信息后确认交互则返回确认消息 M1, 建立通信关系;

S102、所述节点 n 生成验证信息 $M2 = E_{K_n}(T) \parallel E_T(K_n) \parallel C_2$ 并发送至所述控制中心的认证服务器; E 为加密算法, K_n 为节点 n 的认证密钥, T 为时间戳, C_2 为验证码, $\parallel$ 表示连接关系;

S103、所述认证服务器接收所述验证信息 M2, 运用所述节点 n 的认证密钥 K_n 解密 $E_{K_n}(T)$, 获得解密后的时间戳 T' ;

通过所述解密后的时间戳 T' 解密 $E_T(K_n)$ 获得待验证信息 K_n' , 比较所述节点 n 的认证密钥 K_n 和所述验证信息 K_n' 验证所述节点 n; 若相同则完成验证, 若不同则返回步骤 S101。

优选地, 所述为新设备分配密钥, 包括:

S111、验证后, 所述控制中心的认证服务器生成信息 $M00 = E_{K_n}(PR_n) \parallel C00$ 、 $M01 = E_{K_n}(PU_{n-1}) \parallel C01$ 和 $M10 = E_{K_{n-1}}(PU_n) \parallel C10$;

其中, M00 为节点 n 的私钥, 发给节点 n; M01 和 M10 分别包含验证对象的公钥, 分别发送给节点 n 和节点 n-1; C00、C01、C10 分别表示 M00、M01、M10 的验证码, 用于验证信息在发送过程中是否发生错误; PU_{n-1} 、 PU_n 分别表示节点 n-1 的公钥和节点 n 的公钥; K_n 、 K_{n-1} 为节点 n 和节点 n-1 的认证密钥;

S112、根据相邻 i 节点密钥结构, 所述节点 n 将其公钥 PU_n 以 $M5 = E_{PU_{n-1}}(PU_n \parallel Request) \parallel C5$ 形式发送给节点 n-1, 并广播给剩下的相邻 i 个节点;

所述节点 n-1 将所述相邻 i 个节点的公钥 $M0_j = E_{PU_n}(E_{PU_n}) \parallel C0_j$ ($2 \leq j \leq i, i < n$) 回复给所述节点 n, 完成公钥的分配;

其中, E 为加密算法, PU_{n-1} 、 PU_n 分别表示节点 n-1 的公钥和节点 n 的公钥, Request 表

示请求信息, $C5$ 、 $C0_j$ 表示验证码。

优选地, 所述新增的所述节点上传数据, 包括以下步骤:

S201、所述节点 n 向所述节点 $n-1$ 发送通信握手信息;

S202、所述节点 $n-1$ 解密所述握手信息, 判断其验证无误后, 产生回复信息并发送至并所述节点 n ;

S203、所述节点 n 解密所述回复信息, 判断其信息验证无误, 运行数据加密方法加密上传的数据, 产生加密信息 $Mn,0 = Mn \parallel Mn' \parallel Cn$, 并发送给所述节点 $n-1$;

S204、所述节点 $n-1$ 通过所述校验码 Cn 验证所述加密信息 $Mn,0 = Mn \parallel Mn' \parallel Cn$, 验证通过则重复步骤 S201 至 S204 直到发送到节点 0;

其中, PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥, Mn 表示上传的数据, Mn' 表示解码后的所述上传的数据, Cn 表示验证码; n 、 $n-1$ 表示节点标识。

优选地, 所述数据加密方法包括以下步骤:

从待加密的节点 i 的上一节点 $i+1$ 处接收信息 $Mi+1,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi-1 \parallel Mi+1' \parallel Ci+1$, 从中提取验证段信息 $Mi+1'$, 将所述验证段信息 $Mi+1'$ 与自身的数据信息节点 i 中的数据 Di 异或;

用节点 i 自身的公钥 PUi 加密 Di 获得 Mi ;

将加密后的数据信息 Mi 添加到数据集 $Mn \parallel Mn-1 \parallel \dots \parallel Mi-1$ 完成新信息的数据段;

将所述加密后的数据信息 Mi 再与所述验证段信息 $Mi+1'$ 异或后生成新的验证段 Mi' , 并利用 Mi' 生成新的校验码 Ci ;

组合上述数据, 获得新节点 i 发送的信息 $Mi,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi \parallel Mi' \parallel Ci$ 。

优选地, 所述控制中心向节点发送控制命令, 包括以下步骤:

任意节点接收下发的所述控制命令 $Mk,1 = E_{PU_k}(CM_k) \parallel k \parallel C_k$, E 为加密算法, k 为目标节点标号, CM_k 为控制命令内容, PU_k 为节点 k 的公钥, C_k 为节点 k 的验证码;

通过校验码 C_k 判断信息是否正确; 若错误则不做处理, 若正确则节点标号 k 判断此信息是否为发送给自身的信息;

若是则解密所述控制命令获得命令, 若不是则利用本节点的通信密钥生成新的校验码后发送给下一个节点。

优选地，所述链路自愈方法包括：

若出现故障节点，利用所述故障节点存有的相邻 i 节点密钥结构中的后一节点的公钥生成新的握手信息发送给后一节点，直至握手成功；

更新发送节点和接收节点的默认密钥、通信密钥，通过数据上传和命令下发过程进行通信。

优选地，所述相邻 i 节点密钥结构中存储其前向和后向 i 个节点的公钥；其中， i 等于 2 或 3。

与现有技术相比，本发明具有以下有益效果：

1、本发明针对电力系统的特殊通信安全需求，提出了一种面向输电线路无线通信网络的安全通信方法，提供的方法中对于密钥的结构进行了特殊的设计，并且区别于其他通信协议或方法，使用了非对称加密算法。

2、本发明提供的方法从多个层面进行了安全防护，具体来说，包括硬件设备认证、数据完整性认证以及数据传输过程中的保密性保证，可以弥补单一层面加密的不足，具有更高的安全性。

3、本发明综合考虑输电线路无线通信应用实际情况，对通信方法进行了高适应的相关设计，提出了“相邻 i 节点密钥结构”并应用了非对称加密算法，使协议支持新设备随时接入以及自主对于断点进行监测和网络恢复，在保证通信安全的基础上克服了由于网络结构本身带来的脆弱性问题，并且提高了网络的灵活性。

4、本发明中各设备的供电均可采用清洁能源的供电方式，在设备的成本和构筑网络的灵活性方面也更具优势，另外，考虑到清洁能源的供电稳定性问题，提出了系统能耗优化方式。

附图说明

图 1 为本实施例中面向输电线路的网络通信模型图；

图 2 为本实施例中初始化中认证和私钥分配的流程图；

图 3 为本实施例中初始化过程中公钥分配过程流程图；

图 4 为本实施例中上传数据流程图；

图 5 为本实施例中数据上传进程中加密函数的数据处理流程图；

图 6 为本实施例中下发控制命令的流程图；

图 7 为本实施例中对于故障点的检测及链路自愈流程图。

具体实施方式

下面结合附图对本发明的具体实施方式做进一步的详细说明。

本发明提供一种面向输电线路无线通信网络的安全通信方法，包括以下步骤：

初始化所述无线通信网络，判断是否新增节点，若有则对新增节点进行认证并为新设备分配密钥；

新增的所述节点 n 通过已通信的节点 $n-1$ 向控制中心上传状态数据；

所述控制中心下发控制命令；

实时检查链路状态，判断是否出现故障节点，若出现则运用链路自愈方法修复所述无线通信网络。

上述，对新增的节点进行认证，具体包括以下步骤：

S101、所述节点 n 向已安全验证的前一节点 $n-1$ 发送请求交互信息 $M0$ ，所述节点 $n-1$ 接收请求信息后确认交互则返回确认消息 $M1$ ，建立通信关系；

S102、所述节点 n 生成验证信息 $M2 = E_{K_n}(T) \parallel E_T(K_n) \parallel C_2$ 并发送至所述控制中心的认证服务器； E 为加密算法， K_n 为节点 n 的认证密钥， T 为时间戳， C_2 为验证码， $\parallel$ 表示连接关系；

S103、所述认证服务器接收所述验证信息 $M2$ ，运用所述节点 n 的认证密钥 K_n 解密 $E_{K_n}(T)$ ，获得解密后的时间戳 T' ；

通过所述解密后的时间戳 T' 解密 $E_T(K_n)$ 获得待验证信息 K'_n ，比较所述节点 n 的认证密钥 K_n 和所述验证信息 K'_n 验证所述节点 n ；若相同则完成验证，若不同则返回步骤 S101。

上述，为新设备分配密钥，具体包括以下步骤：

S111、验证后，所述控制中心的认证服务器生成信息 $M00 = E_{K_n}(PR_n) \parallel C00$ 、 $M01 = E_{K_n}(PU_{n-1}) \parallel C01$ 和 $M10 = E_{K_{n-1}}(PU_n) \parallel C10$ ；

其中， $M00$ 为节点 n 的私钥，发给节点 n ； $M01$ 和 $M10$ 分别包含验证对象的公钥，分别发送给节点 n 和节点 $n-1$ ； $C00$ 、 $C01$ 、 $C10$ 分别表示 $M00$ 、 $M01$ 、 $M10$ 的验证码，用于验证信息在发送过程中是否发生错误； PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥；

K_n 、 K_{n-1} 为节点 n 和节点 $n-1$ 的认证密钥；

S112、根据相邻 i 节点密钥结构，所述节点 n 将其公钥 PU_n 以 $M5 = E_{PU_{n-1}}(PU_n \parallel Request) \parallel C5$ 形式发送给节点 $n-1$ ，并广播给剩下的相邻 i 个节点；

所述节点 $n-1$ 将所述相邻 i 个节点的公钥 $M0_j = E_{PU_n}(E_{PU_n}) \parallel C0_j$ ($2 \leq j \leq i, i < n$) 回复给所述节点 n ，完成公钥的分配；

其中， E 为加密算法， PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥， $Request$ 表示请求信息， $C5$ 、 $C0_j$ 表示验证码。

上述，新增的所述节点上传数据，具体包括以下步骤：

S201、所述节点 n 向所述节点 $n-1$ 发送通信握手信息；

S202、所述节点 $n-1$ 解密所述握手信息，判断其验证无误后，产生回复信息并发送至并所述节点 n ；

S203、所述节点 n 解密所述回复信息，判断其信息验证无误，运行数据加密方法加密上传的数据，产生加密信息 $Mn,0 = Mn \parallel Mn' \parallel Cn$ ，并发送给所述节点 $n-1$ ；

S204、所述节点 $n-1$ 通过所述校验码 Cn 验证所述加密信息 $Mn,0 = Mn \parallel Mn' \parallel Cn$ ，验证通过则重复步骤 S201 至 S204 直到发送到节点 0；

其中， PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥， Mn 表示上传的数据， Mn' 表示解码后的所述上传的数据， Cn 表示验证码； n 、 $n-1$ 表示节点标识。

上述，数据加密方法，具体包括以下步骤：

从待加密的节点 i 的上一节点 $i+1$ 处接收信息 $Mi+1,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi-1 \parallel Mi+1' \parallel Ci+1$ ，从中提取验证段信息 $Mi+1'$ ，将所述验证段信息 $Mi+1'$ 与自身的数据信息节点 i 中的数据 Di 异或；

用节点 i 自身的公钥 PUi 加密 Di 获得 Mi ；

将加密后的数据信息 Mi 添加到数据集 $Mn \parallel Mn-1 \parallel \dots \parallel Mi-1$ 完成新信息的数据段；

将所述加密后的数据信息 Mi 再与所述验证段信息 $Mi+1'$ 异或后生成新的验证段 Mi' ，并利用 Mi' 生成新的校验码 Ci ；

组合上述数据，获得新节点 i 发送的信息 $Mi,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi \parallel Mi' \parallel Ci$ 。

上述，控制中心向节点发送控制命令，具体包括以下步骤：

任意节点接收下发的所述控制命令 $Mk,1 = E_{PU_k}(CM_k) \parallel k \parallel C_k$, E 为加密算法, k 为目标节点标号, CM_k 为控制命令内容, PU_k 为节点 k 的公钥, C_k 为节点 k 的验证码;

通过校验码 C_k 判断信息是否正确; 若错误则不做处理, 若正确则节点标号 k 判断此信息是否为发送给自身的信息;

若是则解密所述控制命令获得命令, 若不是则利用本节点的通信密钥生成新的校验码后发送给下一个节点。

上述, 链路自愈方法, 具体包括以下步骤:

若出现故障节点, 利用所述故障节点存有的相邻 i 节点密钥结构中的后一节点的公钥生成新的握手信息发送给后一节点, 直至握手成功;

更新发送节点和接收节点的默认密钥、通信密钥, 通过数据上传和命令下发过程进行通信。

所述相邻 i 节点密钥结构中存储其前向和后向 i 个节点的公钥; 其中, i 等于 2 或 3。

图 1 为本实施例中面向输电线路的网络通信模型图; 本实施例中, 提供一种面向输电线路的网络通信模型, 包括控制中心和通信网络的各个节点, 其中, 通信网络节点包括: 双向网关数据采集单元 (DGD) 和多个数据采集单元 (DAU)。

控制中心包括认证服务器 (AS) 和数据采集中心服务器 (DCC) 等主要处理单元, 利用光纤复合架空地线 (OPGW) 与位于输电线路沿线杆塔上的双向网关数据采集单元 (DGD) 建立连接。

每两个双向网关数据采集单元 (DGD) 之间的数据采集单元 (DAU) 与前一个双向网关数据采集单元 (DGD) 通过无线链型网络构成一个通信区域, 再经过双向网关数据采集单元 (DGD) 汇聚后通过光纤复合架空地线 (OPGW) 传送给控制中心。

运用上述面向输电线路无线通信网络的安全通信方法实现各节点的通信。

图 2 为本实施例中初始化中认证和私钥分配的流程圖; 本实施例中, 初始化无线通信网络包括两部分: 一、对新设备的认证, 二、为新设备分配密钥。

节点 n 为新接入电网的设备, 节点 $n-1$ 为与控制中心已建立安全网络的设备, 节点 n 需通过节点 $n-1$ 建立网络关系。具体包括以下步骤:

①、节点 n 向节点 $n-1$ 发送请求交互信息 $M0$, 节点 $n-1$ 接收请求信息后确认交互则返回确认消息 $M1$, 通过双方的交互信息 $M0$ 和 $M1$, 节点 n 和节点 $n-1$ 进行简单握手;

②、节点 n 仍不能信任节点 $n-1$ 且暂无手段验证，对其验证信息进行加工生成新的验证信息 $M2 = E_{K_n}(T) \parallel E_T(K_n) \parallel C_2$ 后进行传输，通过节点 $n-1$ 发送到控制中心的认知服务器 AS；

其中， E 表示加密算法， K_n 为节点 n 的认证密钥， T 为时间戳，用于防止重复攻击， C_2 为验证码， $\parallel$ 表示连接关系。

③、认知服务器 AS 收到验证消息 $M2$ 后先用存在自身的节点 n 的认证密钥 K_n 对 $E_{K_n}(T)$ 解密，获得解密后的时间戳 T' ，再用 T' 解密 $E_T(K_n)$ 获得待验证消息 K_n' ，通过比较 K_n 和 K_n' 验证节点 n ，若 K_n 和 K_n' 相同，则完成验证进入步骤④，否则返回步骤①。

④、完成验证后，认知服务器 AS 生成 3 个信息 $M00 = E_{K_n}(PR_n) \parallel C00$ 、 $M01 = E_{K_n}(PU_{n-1}) \parallel C01$ 和 $M10 = E_{K_n-1}(PU_n) \parallel C10$ 。

其中， E 表示加密算法， PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥；

$M00$ 发给节点 n ，为节点 n 的私钥（该私钥为节点 n 和服务端端独有的，对其他节点是不公开的密钥）；

$M01$ 和 $M10$ 分别发送给节点 n 和节点 $n-1$ ，分别包含验证对象的公钥，不同于私钥，该公钥用于发送给对方进行身份验证的，让节点 n 和节点 $n-1$ 可以互相验证；

$C00$ 、 $C01$ 、 $C10$ 分别表示 $M00$ 、 $M01$ 、 $M10$ 的验证码，用来验证信息在发送过程中是否发生错误。

⑤、根据“相邻 i 节点密钥结构”的要求，节点 n 将其公钥 PU_n 以 $M5 = E_{PU_{n-1}}(PU_n \parallel Request) \parallel C5$ 形式发送给节点 $n-1$ 并以类似的形式以此广播给剩下的 i 个节点；

同时，节点 $n-1$ 将后 i 节点的公钥以 $M0_j = E_{PU_n}(E_{PU_n}) \parallel C0_j$ ($2 \leq j \leq i, i < n$)， $C0_j$ （表示 $M0_j$ 的验证码）的形式回复给节点 n ，以完成公钥的分配，如图 3 本实施例中初始化过程中公钥分配过程流程图所示。

其中， E 表示加密算法， PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥， $Request$ 表示请求信息， $C5$ 、 $C0_j$ 表示验证码。

上述“相邻 i 节点密钥结构”，是指一个节点同时拥有其前向和后向 i 个节点的公钥。

图 4 为本实施例中上传数据流程图；本实施例中，在一个安全网络已经构建完成的环境

下, 当要进行数据的上传时候 (如从节点 n 开始, 将数据传输至认证服务器 AS), 其上传数据过程如下:

①、节点 n 向节点 $n-1$ 发送握手信息 $Mh,0 = E_{PU_{n-1}}(PU_n(hello) \parallel n)$, 节点 $n-1$ 接收握手信息后对其解密并判断, 若验证信息无误, 产生答复信息 $Mr,0 = E_{PU_n}(PU_{n-1}(response) \parallel n-1)$, 将答复信息发送给节点 n ; 节点 n 接收答复信息后对其解密并判断, 若验证信息无误后, 完成验证过程。 PU_n 、 PU_{n-1} 分别表示节点 n 和节点 $n-1$ 的公钥; n 、 $n-1$ 表示节点标识。

通过上述握手信息 $Mh,0 = E_{PU_{n-1}}(PU_n(hello) \parallel n)$ 和答复信息 $Mr,0 = E_{PU_n}(PU_{n-1}(response) \parallel n-1)$ 完成通信双方节点 n 和节点 $n-1$ 的验证。

②、由节点 n 执行数据加密函数 (function encryption, FEn), 将经过 FEn 处理后获得加密后的上传数据 $Mn,0$, $Mn,0 = Mn \parallel Mn' \parallel Cn$, 将其发给节点 $n-1$, 当节点 $n-1$ 通过校验码 Cn (Cn 为 $Mn,0$ 信息的验证码) 验证完 $Mn,0 = Mn \parallel Mn' \parallel Cn$ 后, 节点 $n-1$ 将重复如图 4 的过程直到节点 0 (DGD)。

图 5 为本实施例中数据上传中加密函数的数据处理流程图; 本实施例中, 对节点 i 的上传数据进行加密。

确定节点 i 的加密函数 FEi , 首先, 其从节点 $i+1$ 处收到的信息 $Mi+1,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi-1 \parallel Mi+1' \parallel Ci+1$ 中的提取中间验证段信息 (与下方对应) $Mi+1'$, 将 $Mi+1'$ 与自身的数据信息节点 i 中的待加密的数据 Di 异或, 通过增强关联性提升雪崩效应提高安全性;

然后, 用节点 i 自身的公钥 PUi 加密 Di 获得 Mi , 确保只有拥有节点 i 私钥的服务器端和其自身可以解密;

接着, 将加密后的数据信息 Mi 添加到数据集 $Mn \parallel Mn-1 \parallel \dots \parallel Mi-1$ 之后完成新信息的数据段; Mi 再与 $Mi+1'$ 异或后生成新的验证段 Mi' , 并利用 Mi' 生成新的校验码 Ci ;

最后, 将以上过程中产生的各类数据组合在一起, 获得新节点 i 发送的信息 $Mi,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi \parallel Mi' \parallel Ci$ 。

控制命令的下发流程区别于数据的上传流程主要有三点:

- 1、监测数据一般为定时发送, 命令发送时间有一定的随机性。
- 2、数据文件一般较大, 而控制命令一般较小。

3、上传的数据需包含所有节点，命令可能只针对个别节点。

图 6 为本实施例中下发控制命令的流程图，本实施例中，下发控制命令的过程如下：

任意节点收到下发的命令 $Mk, 1 = E_{PU_k}(CM_k) \parallel k \parallel C_k$ ，E 表示加密算法，k 为目标节点标号， CM_k 为控制命令内容， PU_k 为节点 k 的公钥， C_k 为节点 k 的验证码。

通过校验码 C_k 判断信息是否出错，若错误，接收命令的节点不做任何处理，若正确，则通过信息中间的目的节点标号 k 判断此信息是否是发给自己的；

若是，则通过自身的私钥 PU_k 解密获得命令（非对称加密中公钥加密的信息必须用私钥才能解密，而 k 的私钥只有 k 和服务端存有，通过此保证安全性），若不是则利用本节点的通信密钥生成新的校验码 C_k 发送给下一个节点。至此，完成整个数据上传、命令下发的保护过程。

图 7 为本实施例中对于故障点的检测及链路自愈流程图。本实施例中，系统运行过程中，实时监测通信网络是否出现故障，若遇到故障则进行链路自愈。具体过程如下：

首先，需对故障节点进行判断，并找到最近的一个可以正常工作的节点；

其次，需要对发送方和接收方的默认密钥、通信密钥进行更新；

然后，通过进行上述数据上传和命令下发操作。

故障点的检测方法：通过握手信息是否完成确定故障点，当发送节点的握手信息得不到回复，或回复错误时候，认为该发送节点为故障节点，并利用“相邻 i 节点密钥结构”中存储的后一节点的公钥生成新的握手信息发送给后一节点，直至握手成功。

握手成功后，接收双方均将默认密钥更新，并生成新的通信密钥，进行正常通信。从而，下次通信时候可避免重复的检测，直至故障点修复，重新进行初始化进程。

经过测试发现，跳过故障点进行通信会增大能耗，考虑到设备是自身供电，因此对能耗有一定要求。通过模拟发现，一定程度的提高发射功率可以在跳过节点时有效的减少能耗，并得出 $i=2$ 或 3 是最理想的状况， $i=4$ 或者 5 时设备需要较高的发射功率和能耗进行工作， $i \geq 6$ 时由于能耗过高，不宜采用。

最后应当说明的是：以上实施例仅用于说明本申请的技术方案而非对其保护范围的限制，尽管参照上述实施例对本申请进行了详细的说明，所属领域的普通技术人员应当理解：本领域技术人员阅读本申请后依然可对申请的具体实施方式种种变更、修改或者等同替换，但这些变更、修改或者等同替换，均在申请待批的权利要求保护范围之内。

权 利 要 求

1、一种面向输电线路无线通信网络的安全通信方法，其特征在于：所述方法包括：

初始化所述无线通信网络，判断是否新增节点，若有则对新增节点进行认证并为新设备分配密钥；

新增的所述节点 n 通过已通信的节点 n-1 向控制中心上传状态数据；

所述控制中心下发控制命令；

实时检查链路状态，判断是否出现故障节点，若出现则运用链路自愈方法修复所述无线通信网络。

2、如权利要求 1 所述的方法，其特征在于：所述对新增的节点进行认证，包括：

S101、所述节点 n 向已安全验证的前一节点 n-1 发送请求交互信息 M0，所述节点 n-1 接收请求信息后确认交互则返回确认消息 M1，建立通信关系；

S102、所述节点 n 生成验证信息 $M2 = E_{K_n}(T) \parallel E_T(K_n) \parallel C_2$ 并发送至所述控制中心的认证服务器；E 为加密算法， K_n 为节点 n 的认证密钥，T 为时间戳， C_2 为验证码， $\parallel$ 表示连接关系；

S103、所述认证服务器接收所述验证信息 M2，运用所述节点 n 的认证密钥 K_n 解密 $E_{K_n}(T)$ ，获得解密后的时间戳 T' ；

通过所述解密后的时间戳 T' 解密 $E_T(K_n)$ 获得待验证信息 K'_n ，比较所述节点 n 的认证密钥 K_n 和所述验证信息 K'_n 验证所述节点 n；若相同则完成验证，若不同则返回步骤 S101。

3、如权利要求 1 所述的方法，其特征在于：所述为新设备分配密钥，包括：

S111、验证后，所述控制中心的认证服务器生成信息 $M00 = E_{K_n}(PR_n) \parallel C00$ 、 $M01 = E_{K_n}(PU_{n-1}) \parallel C01$ 和 $M10 = E_{K_{n-1}}(PU_n) \parallel C10$ ；

其中，M00 为节点 n 的私钥，发给节点 n；M01 和 M10 分别包含验证对象的公钥，分别发送给节点 n 和节点 n-1；C00、C01、C10 分别表示 M00、M01、M10 的验证码，用于验证信息在发送过程中是否发生错误； PU_{n-1} 、 PU_n 分别表示节点 n-1 的公钥和节点 n 的公钥； K_n 、 K_{n-1} 为节点 n 和节点 n-1 的认证密钥；

S112、根据相邻 i 节点密钥结构，所述节点 n 将其公钥 PU_n 以 $M5 = E_{PU_{n-1}}(PU_n \parallel Request) \parallel C5$ 形式发送给节点 n-1，并广播给剩下的相邻 i 个节点；

所述节点 $n-1$ 将所述相邻 i 个节点的公钥 $M0_j = E_{PU_n}(E_{PU_n}) \parallel C0_j$ ($2 \leq j \leq i, i < n$) 回复给所述节点 n , 完成公钥的分配;

其中, E 为加密算法, PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥, $Request$ 表示请求信息, $C5$ 、 $C0_j$ 表示验证码。

4、如权利要求 1 所述的方法, 其特征在于: 所述新增的所述节点上传数据, 包括以下步骤:

S201、所述节点 n 向所述节点 $n-1$ 发送通信握手信息;

S202、所述节点 $n-1$ 解密所述握手信息, 判断其验证无误后, 产生回复信息并发送至并所述节点 n ;

S203、所述节点 n 解密所述回复信息, 判断其信息验证无误, 运行数据加密方法加密上传的数据, 产生加密信息 $Mn,0 = Mn \parallel Mn' \parallel Cn$, 并发送给所述节点 $n-1$;

S204、所述节点 $n-1$ 通过所述校验码 Cn 验证所述加密信息 $Mn,0 = Mn \parallel Mn' \parallel Cn$, 验证通过则重复步骤 S201 至 S204 直到发送到节点 0;

其中, PU_{n-1} 、 PU_n 分别表示节点 $n-1$ 的公钥和节点 n 的公钥, Mn 表示上传的数据, Mn' 表示解码后的所述上传的数据, Cn 表示验证码; n 、 $n-1$ 表示节点标识。

5、如权利要求 4 所述的方法, 其特征在于: 所述数据加密方法, 包括以下步骤:

从待加密的节点 i 的上一节点 $i+1$ 处接收信息 $Mi+1,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi-1 \parallel Mi+1' \parallel Ci+1$, 从中提取验证段信息 $Mi+1'$, 将所述验证段信息 $Mi+1'$ 与自身的数据信息节点 i 中的数据 Di 异或;

用节点 i 自身的公钥 PUi 加密 Di 获得 Mi ;

将加密后的数据信息 Mi 添加到数据集 $Mn \parallel Mn-1 \parallel \dots \parallel Mi-1$ 完成新信息的数据段;

将所述加密后的数据信息 Mi 再与所述验证段信息 $Mi+1'$ 异或后生成新的验证段 Mi' , 并利用 Mi' 生成新的校验码 Ci ;

组合上述数据, 获得新节点 i 发送的信息 $Mi,0 = Mn \parallel Mn-1 \parallel \dots \parallel Mi \parallel Mi' \parallel Ci$ 。

6、如权利要求 1 所述的方法, 其特征在于: 所述控制中心向节点发送控制命令, 包括以下步骤:

任意节点接收下发的所述控制命令 $Mk,1 = E_{PU_k}(CM_k) \parallel k \parallel C_k$, E 为加密算法, k 为目标节

点标号, CM_k 为控制命令内容, PU_k 为节点 k 的公钥, C_k 为节点 k 的验证码;

通过校验码 C_k 判断信息是否正确; 若错误则不做处理, 若正确则节点标号 k 判断此信息是否为发送给自身的信息;

若是则解密所述控制命令获得命令, 若不是则利用本节点的通信密钥生成新的校验码后发送给下一个节点。

7、如权利要求 1 所述的方法, 其特征在于: 所述链路自愈方法包括:

若出现故障节点, 利用所述故障节点存有的相邻 i 节点密钥结构中的后一节点的公钥生成新的握手信息发送给后一节点, 直至握手成功;

更新发送节点和接收节点的默认密钥、通信密钥, 通过数据上传和命令下发过程进行通信。

8、如权利要求 3 或 7 所述的方法, 其特征在于: 所述相邻 i 节点密钥结构中存储其前向和后向 i 个节点的公钥; 其中, i 等于 2 或 3。

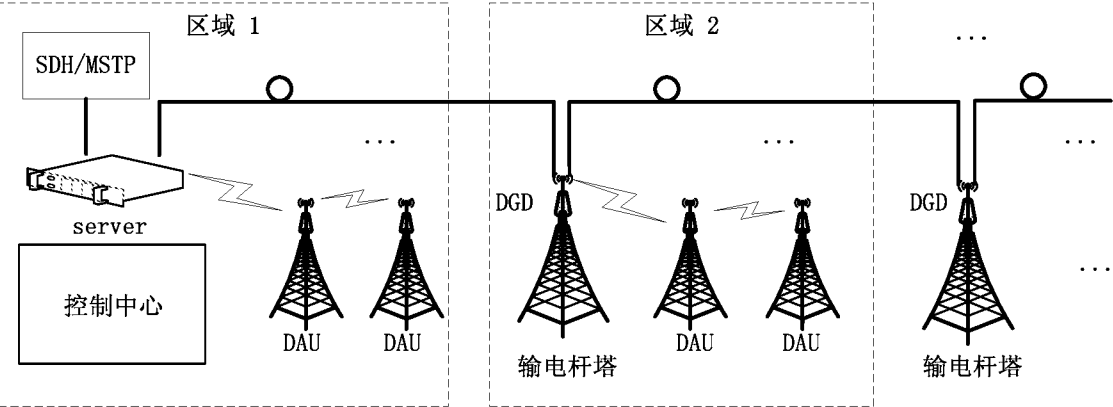


图1

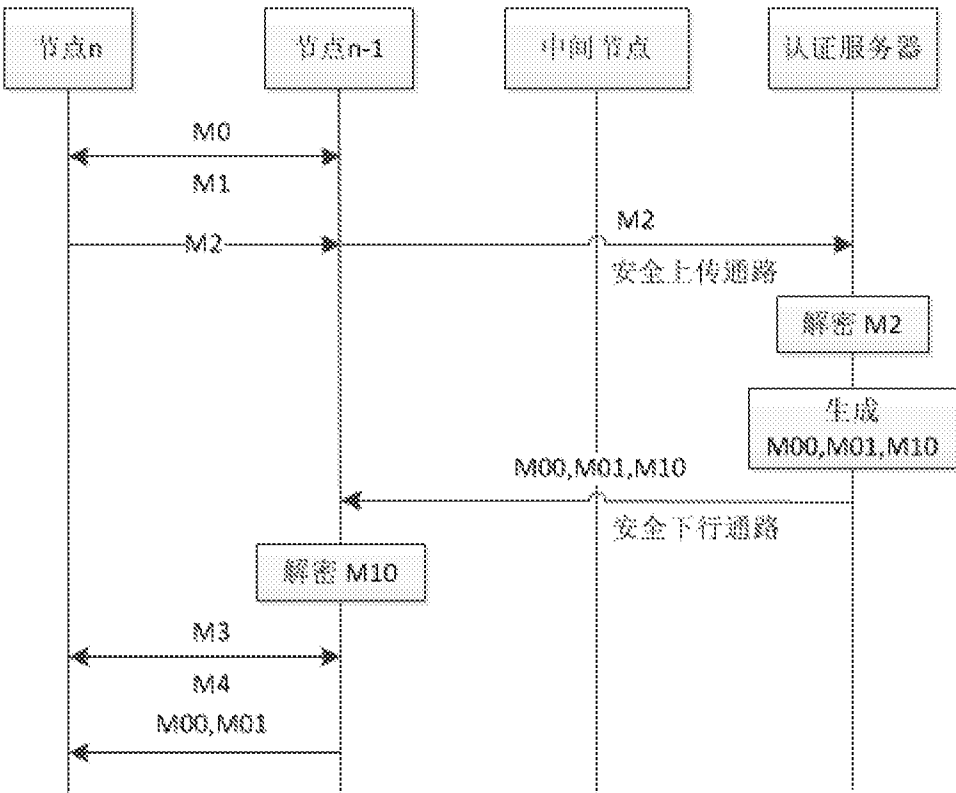


图2

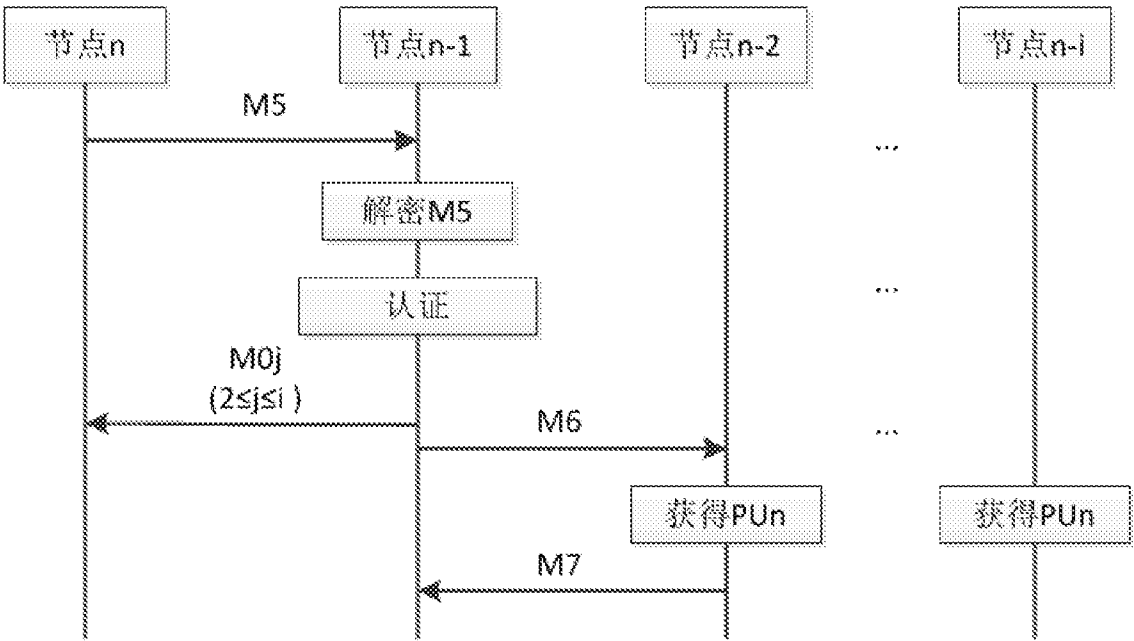


图3

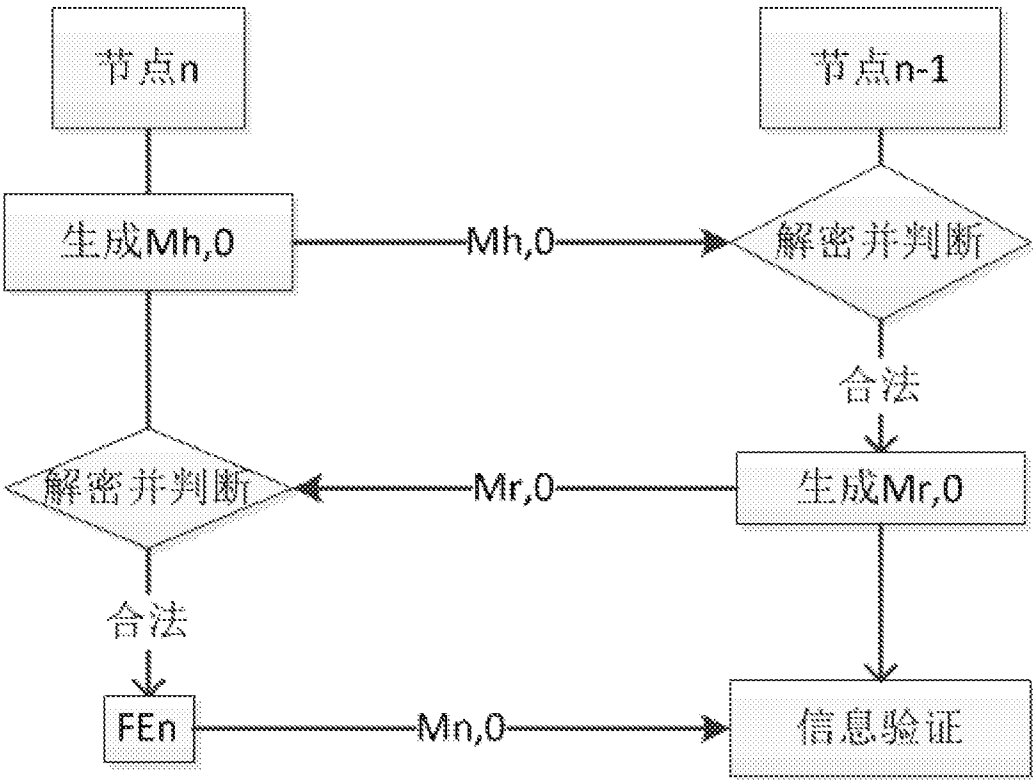


图4

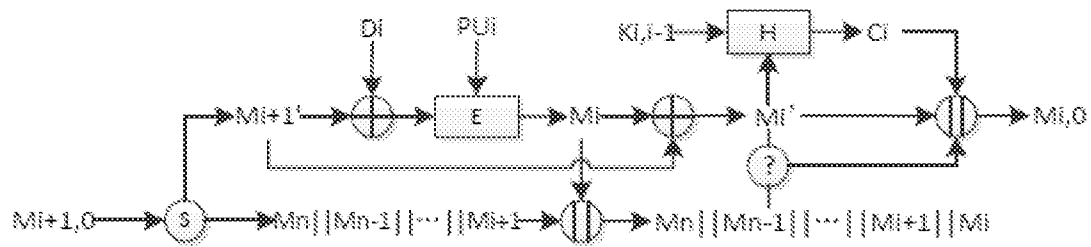


图5

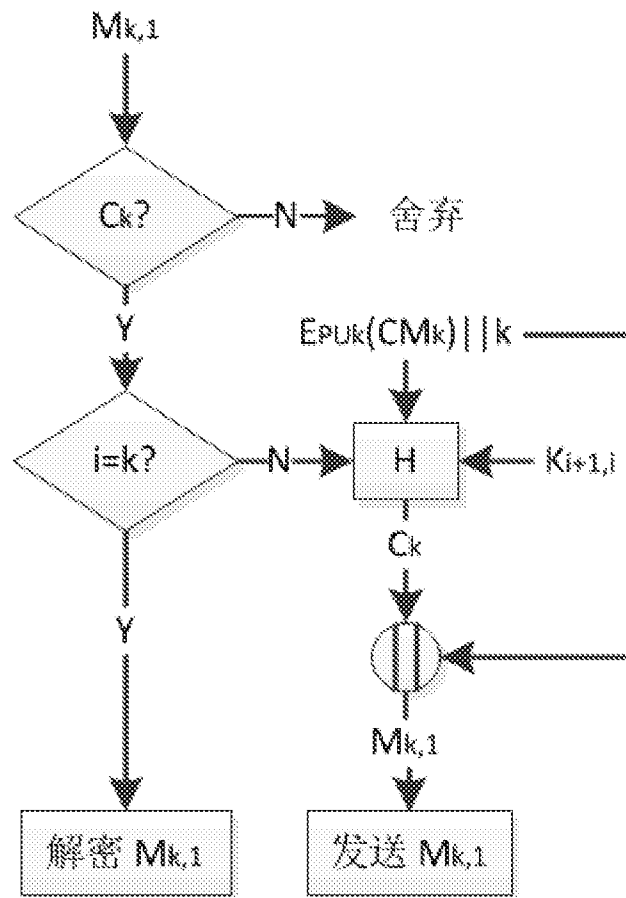


图6

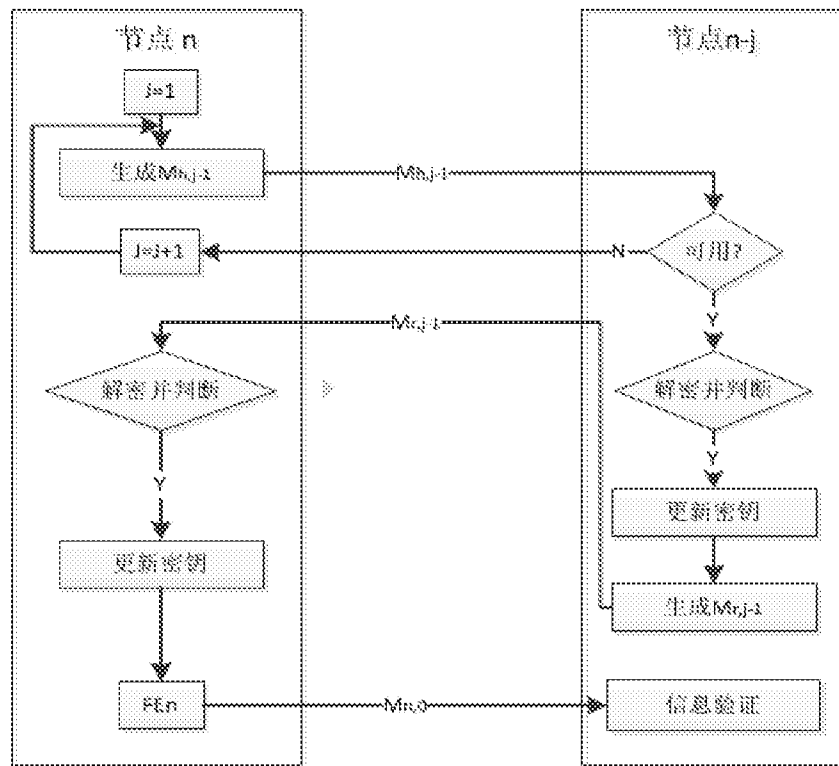


图7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/081247

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; WPI; EPODOC; GOOGLE; CNKI: transmission line, wire, increase, join, before, send, upload, transfer, control centre, authentication server, AC, AS, self-healing, time point, verification code, verification information, handshake, electric, power, transmi+, new, node, adjacent, neighbor, father, authenticat+, key, encrypt+, decrypt+, failure, state, data, natural, repair+, server, timestamp, code

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104902469 A (STATE GRID CORPORATION OF CHINA et al.), 09 September 2015 (09.09.2015), description, paragraphs [0056]-[0091], and claims 1-8	1-8
A	CN 103686709 A (ZTE CORP.), 26 March 2014 (26.03.2014), the whole document	1-8
A	CN 202353820 U (FUJIAN HOPETRUE ELECTRONICS CO., LTD.), 25 July 2012 (25.07.2012), the whole document	1-8
A	CN 103647788 A (STATE GRID CHONGQING ELECTRIC POWER COMPANY), 19 March 2014 (19.03.2014), the whole document	1-8
A	CN 101621434 A (HUAWEI TECHNOLOGIES CO., LTD.), 06 January 2010 (06.01.2010), the whole document	1-8
A	CN 102421095 A (GCI SCIENCE & TECHNOLOGY CO., LTD.), 18 April 2012 (18.04.2012), the whole document	1-8

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 27 May 2016 (27.05.2016)	Date of mailing of the international search report 28 June 2016 (28.06.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Qian Telephone No.: (86-10) 010-62413845

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/081247

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014013117 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE), 09 January 2014 (09.01.2014), the whole document	1-8
A	US 2007011435 A1 (SAMSUNG ELECTRONICS CO., LTD.), 11 January 2007 (11.01.2007), the whole document	1-8

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/081247

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104902469 A	09 September 2015	None	
CN 103686709 A	26 March 2014	US 2015249921 A1	03 September 2015
		WO 2014040481 A1	20 March 2014
		EP 2897442 A1	22 July 2015
CN 202353820 U	25 July 2012	None	
CN 103647788 A	19 March 2014	None	
CN 101621434 A	06 January 2010	None	
CN 102421095 A	18 April 2012	None	
US 2014013117 A1	09 January 2014	KR 20140007544 A	20 January 2014
US 2007011435 A1	11 January 2007	KR 20060125612 A	06 December 2006

A. 主题的分类 H04W 12/04 (2009.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04W; H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNPAT; WPI; EPDOC; GOOGLE; CNKI: 电力, 输电线路, 电线, 新, 增加, 加入, 节点, 认证, 密钥, 相邻, 邻居, 父, 前, 发送, 上传, 传输, 传送, 状态, 数据, 控制中心, 认证服务器, AC, AS, 故障, 自愈, 加密, 解密, 时间戳, 时戳, 时间点, 时点, 验证码, 验证信息, 握手, electric, power, transmi+, new, node, adjacent, neighbor, father, authenticat+, key, encrypt+, decrypt+, failure, state, data, natural, repair+, server, timestamp, code		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 104902469 A (国家电网公司 等) 2015年 9月 9日 (2015 - 09 - 09) 说明书第[0056]-[0091]段, 权利要求1-8	1-8
A	CN 103686709 A (中兴通讯股份有限公司) 2014年 3月 26日 (2014 - 03 - 26) 全文	1-8
A	CN 202353820 U (福建望诚电子有限公司) 2012年 7月 25日 (2012 - 07 - 25) 全文	1-8
A	CN 103647788 A (国网重庆市电力公司) 2014年 3月 19日 (2014 - 03 - 19) 全文	1-8
A	CN 101621434 A (华为技术有限公司) 2010年 1月 6日 (2010 - 01 - 06) 全文	1-8
A	CN 102421095 A (广州杰赛科技股份有限公司) 2012年 4月 18日 (2012 - 04 - 18) 全文	1-8
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2016年 5月 27日		国际检索报告邮寄日期 2016年 6月 28日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		授权官员 李倩 电话号码 (86-10) 010-62413845

C. 相关文件		
类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US 2014013117 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 2014年 1月 9日 (2014 - 01 - 09) 全文	1-8
A	US 2007011435 A1 (SAMSUNG ELECTRONICS CO. , LTD.) 2007年 1月 11日 (2007 - 01 - 11) 全文	1-8

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/081247

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104902469	A	2015年 9月 9日	无			
CN	103686709	A	2014年 3月 26日	US	2015249921	A1	2015年 9月 3日
				WO	2014040481	A1	2014年 3月 20日
				EP	2897442	A1	2015年 7月 22日
CN	202353820	U	2012年 7月 25日	无			
CN	103647788	A	2014年 3月 19日	无			
CN	101621434	A	2010年 1月 6日	无			
CN	102421095	A	2012年 4月 18日	无			
US	2014013117	A1	2014年 1月 9日	KR	20140007544	A	2014年 1月 20日
US	2007011435	A1	2007年 1月 11日	KR	20060125612	A	2006年 12月 6日