(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
2011 年 6 月 23 日 (23.06.2011)

PCT

(10) 国际公布号
WO 2011/072514 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2010/073454

(22) 国际申请日: 2010 年 6 月 2 日 (02.06.2010)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200910219572.8 2009 年 12 月 18 日 (18.12.2009) CN

(71) 申请人 (对除美国外的所有指定国): **西安西电捷通无线网络通信股份有限公司 (CHINA IWNCOMM CO., LTD.)** [CN/CN]; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **铁满霞 (TIE, Manxia)** [CN/CN]; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **曹军 (CAO, Jun)** [CN/CN]; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **李琴 (LI, Qin)** [CN/CN]; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **葛莉 (GE, Li)** [CN/CN]; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **黄振海 (HUANG, Zhenhai)** [CN/CN]; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。

(74) 代理人: **北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW)**; 中国北京市朝阳区建国门外大街 22 号赛特广场 7 层, Beijing 100004 (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, 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, IS, JP,

[见续页]

(54) Title: METHOD AND SYSTEM FOR SECRET COMMUNICATION BETWEEN NODES

(54) 发明名称 : 节点间保密通信方法及系统

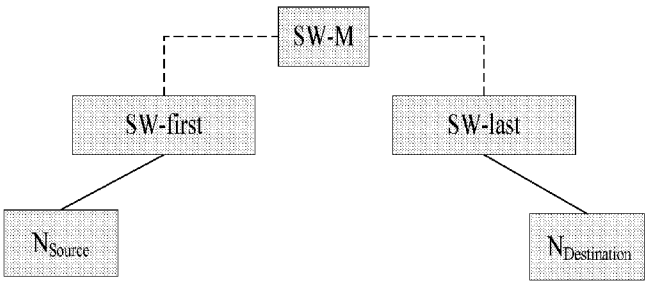

图 2 / Fig. 2

(57) Abstract: The present invention discloses a method and system for secret communication between nodes in a wired Local Area Network (LAN). The method of secret communication between nodes in the wired LAN includes the following steps: 1) a sharing key is established; 2) the route probe is exchanged; 3) the data communication is classified; 4) the secret communication is processed among the nodes. According to the different communication situations among the nodes, the method of secret communication between nodes provided in the present invention can process the classification and select an appropriate secret communication strategy; compared with per-hop encryption, the calculation load of the exchange equipment is reduced, and the transmission delay of data packets is shortened; compared with the method that inter-station keys are established in pairs of nodes in order to protect the communication secret, the key number is reduced, and the key management is simplified.

(57) 摘要: 一种有线局域网节点间保密通信方法及系统，该有线局域网节点间保密通信方法包括以下步骤：1）建立共享密钥；2）交换路由探寻；3）数据通信分类；4）节点间保密通信。本发明中提供的节点间保密通信的方法会根据节点间不同的通信情况进行分类，选择合适的保密通信策略；相对于逐跳加密，减少了交换设备的计算负担，缩短了数据包的传输延时；相对于为所有节点之间两两建立站间密钥来保护通信机密性的方法，减少了密钥的数目，简化了密钥管理。

WO 2011/072514 A1

KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

节点间保密通信方法及系统

本申请要求于 2009 年 12 月 18 日提交中国专利局、申请号为 200910219572.8、发明名称为“节点间保密通信方法及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及网络安全领域，特别涉及一种节点间保密通信方法及系统。

背景技术

有线局域网一般为广播型网络，一个节点发出的数据，其他节点都能收到。网络上的各个节点共享信道，这给网络带来了极大的安全隐患。攻击者只要接入网络进行监听，就可以捕获网络上所有的数据包。现有国家标准 GB/T 15629.3（对应 IEEE 802.3 或者 ISO/IEC 8802-3）定义的局域网 LAN（Local Area Network）并不提供数据保密方法，这样就使得攻击者容易窃取到关键信息。

在有线局域网中，IEEE 通过对 IEEE 802.3 进行安全增强来实现链路层的安全。IEEE 802.1AE 为保护以太网提供数据加密协议，并采用逐跳加密的安全措施来实现网络节点之间数据的安全传达。这种安全措施给局域网中的交换设备带来了巨大的计算负担，容易引发攻击者对交换设备的攻击；且数据包从发送源节点传递到目的节点的延时也会增大，降低了网络传输效率。

有线局域网的拓扑结构比较复杂，涉及到的节点（这里，用户终端和交换设备被统称为节点）数目也比较多，因此网络中的数据通信比较复杂。若为所有的节点两两建立共享密钥，节点需要保存的共享密钥数目比较巨大；若利用相邻节点之间的共享密钥，使用逐跳加密的安全措施，又会给网络交换设备带来巨大的计算负担。

因此，有必要研究一种方法来解决节点间保密通信的问题，一方面既能保证数据在节点间进行保密传输，另一方面又尽量减少密钥的数目和密钥建立的复杂度，同时还需要考虑节点的加解密能力。

发明内容

为了解决背景技术中存在的上述技术问题，本发明提供了一种以节点间交换路由信息为基础划分数据通信的类型，选择不同的保密通信策略的节点间保密通信方法及系统。

本发明的技术解决方案是：本发明提供了一种节点间保密通信方法，其特殊之处在于：所述节点间保密通信方法包括以下四个过程：

1）节点之间建立共享密钥；所述节点之间包括用户终端与交换设备之间、交换设备两两之间以及同一交换设备下两个直连用户终端之间；

2）节点之间根据所述交换路由探寻，得到节点之间的交换路由信息；

3）节点之间根据所述交换路由信息判断节点之间的数据通信类型；

4）根据节点之间不同的数据通信类型采用不同的保密通信策略进行节点间保密通信。

优选的，上述过程1）的具体实现方式是：

1.1）为相邻节点之间建立共享密钥，称为单播密钥 USK（Unicast Session Key）；

1.2）为交换设备两两之间建立共享密钥，称为交换密钥 SWkey（SWitch key）；

1.3）根据本地策略选择，为同一交换设备下两个直连用户终端之间建立共享密钥，称为站间密钥STAkey（STAtion key）。

优选的，从发送源节点N_{Source}到目的节点$N_{Destination}$的节点间交换路由信息定义为一个标识四元组：所述标识四元组包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$；接收到从发送源节点N_{Source}到目的节点$N_{Destination}$的数据包但却未出现在交换路由信息标识四元组中的交换设备，称之为中间交换设备。从发送源节点N_{Source}到目的节点$N_{Destination}$的数据在传输过程中可能不会通过中间交换设备，也可能通过多个中间交换设备；

优选的，上述过程2）的具体实现方式是：

2.1）发送源节点N_{Source}发送交换路由探寻分组给目的节点$N_{Destination}$；该分组中主要包含标识四元组，所述标识四元组包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$；

其中：

ID_{Source}：表示发送源节点 N_{Source} 的标识；

$ID_{SW\text{-}first}$：表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的第一个交换设备 SW-first 的标识，若发送源节点 N_{Source} 为交换设备，则 $ID_{SW\text{-}first}$

就是 ID_{Source}；若发送源节点 N_{Source} 为终端用户，则 $ID_{SW\text{-}first}$ 就是发送源节点 N_{Source} 直连交换设备的标识；

$ID_{SW\text{-}last}$：表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的最后一个交换设备 SW-last 的标识；在交换路由探寻分组中，该字段是未知的；

$ID_{Destination}$：表示目的节点$N_{Destination}$的标识；

2.2）目的节点$N_{Destination}$发送交换路由响应分组给发送源节点N_{Source}；

2.3）各节点接收交换路由响应分组。

优选的，目的节点$N_{Destination}$收到来自发送源节点N_{Source}发送的交换路由探寻分组后，上述步骤2.2）的具体实现方式是：

2.2.1）判断从发送源节点 N_{Source} 发来的数据包经过的最后一个交换设备 SW-last 的信息：若目的节点 $N_{Destination}$ 为交换设备，则 $ID_{SW\text{-}last}$ 就是 $ID_{Destination}$；若目的节点 $N_{Destination}$ 为终端用户，则 $ID_{SW\text{-}last}$ 就是终端用户直连交换设备的标识；

2.2.2）记录下标识四元组，其中 ID_{Source}、$ID_{SW\text{-}first}$ 及 $ID_{Destination}$ 同接收到的交换路由探寻分组中各字段的值，此时四元组的所有字段值都已明确；所述标识四元组包括 ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$ 以及 $ID_{Destination}$；

2.2.3）构造交换路由响应分组发送给发送源节点N_{Source}，该分组包含已明确所有字段值的标识四元组，所述标识四元组包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$。

优选的，各节点收到来自目的节点$N_{Destination}$发送的交换路由探寻响应分组后，上述步骤2.3）的具体实现方式是：

2.3.1）交换设备收到交换路由响应分组后，若自己的标识在该分组中的标识四元组中，则记录下标识四元组再转发；若自己的标识不在该分组中的标识四元组中则直接转发该分组；所述标识四元组包括 ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$ 以及 $ID_{Destination}$；

2.3.2）发送源节点N_{Source}收到交换路由响应分组后，记录下标识四元组，完成此次交换路由探寻过程，所述标识四元组包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$。

优选的，上述过程3）的具体实现方式是：

从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信类型是根据得到的交换路由四元组信息进行判断的，所述四元组信息包括ID_{Source}、$ID_{SW-first}$、$ID_{SW-last}$以及$ID_{Destination}$，其具体的判断方式是:

3.1）判断$ID_{SW-first}$= ID_{Source}是否成立，若成立，则发送源节点N_{Source}是交换设备，执行步骤3.2）；否则，发送源节点N_{Source}是用户终端，执行步骤3.4）；

3.2）判断$ID_{SW-last}$= $ID_{Destination}$是否成立，若成立，则目的节点$N_{Destination}$是交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是交换设备到交换设备的通信，属于交换设备到交换设备的通信类型；否则，目的节点$N_{Destination}$是用户终端，执行步骤3.3）；

3.3）判断$ID_{SW-last}$= $ID_{SW-first}$是否成立，若成立，则从发送源节点N_{Source}到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是交换设备到直连用户终端的通信，属于交换设备到直连用户终端的通信类型；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是交换设备到不直连用户终端的通信，属于交换设备到不直连用户终端的通信类型；

3.4）判断$ID_{SW-last}$=$ID_{Destination}$是否成立，若成立，则目的节点$N_{Destination}$是交换设备，执行步骤3.5）；否则，目的节点$N_{Destination}$是用户终端，执行步骤3.6）；

3.5）判断$ID_{SW-last}$= $ID_{SW-first}$是否成立，若成立，则从发送源节点N_{Source}到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到直连交换设备的通信，属于用户终端到直连交换设备的通信类型；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到不直连交换设备的通信，属于用户终端到不直连交换设备的通信类型；

3.6）判断$ID_{SW-last}$=$ID_{SW-first}$是否成立，若成立，则从发送源节点N_{Source}到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到同一交换设备下其他直连用户终端的通信，属于用户终端到同一交换设备下其他直连用户终端的通信类型；否则，从发送

源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到不同交换设备下直连的用户终端的通信，属于用户终端到不同交换设备下直连用户终端的通信类型。

优选的，上述过程4）的具体实现方式是从发送源节点N_{Source}到目的节点$N_{Destination}$的节点间数据通信，根据数据通信类型的不同，通信过程中所采用的保密通信策略也将有所不同。

优选的，当数据通信类型是交换设备到交换设备的数据通信类型时，所述其节点间保密通信策略的具体实现方式是:

4.1.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的交换密钥加密数据包；所述发送源节点 N_{Source} 为交换设备，该交换设备既是发送源节点 N_{Source}，又是第一个交换设备 SW-first；所述目的节点 $N_{Destination}$ 为交换设备，该交换设备既是目的节点 $N_{Destination}$，又是最后一个交换设备 SW-last;

4.1.2）若存在中间交换设备，则中间交换设备收到类型为交换设备到交换设备的通信数据包，直接转发；

4.1.3）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的交换密钥解密数据包。

优选的，当数据通信类型是交换设备到直连用户终端的数据通信类型时，所述其节点间保密通信策略的具体实现方式是:

4.2.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包；所述发送源节点 N_{Source} 为交换设备，该交换设备既是发送源节点 N_{Source}，又是第一个交换设备 SW-first 同时还是最后一个交换设备 SW-last；所述目的节点 $N_{Destination}$ 是用户终端；

4.2.2）目的节点$N_{Destination}$使用与发送源节点N_{Source}之间的单播密钥解密数据包。

优选的，当数据通信类型是交换设备到不直连用户终端的数据通信类型时，所述其节点间保密通信策略的具体实现方式是:

4.3.1）发送源节点 N_{Source} 使用与最后一个交换设备 SW-last 之间的交换密钥加密数据包；所述发送源节点 N_{Source} 为交换设备，该交换设备既是发送源节

点 N_{Source}，又是第一个交换设备 SW-first;

4.3.2）若存在中间交换设备，则中间交换设备直接转发类型为交换设备到不直连用户终端的通信的数据包;

4.3.3）最后一个交换设备 SW-last 使用与发送源节点 N_{Source} 的交换密钥解密数据包，然后使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包，然后转发；所述目的节点 $N_{Destination}$ 为用户终端;

4.3.4）目的节点$N_{Destination}$使用与最后一个交换设备SW-last之间的单播密钥解密数据包。

优选的，当数据通信类型是用户终端到直连交换设备的数据通信类型时，所述其节点间保密通信策略的具体实现方式是:

4.4.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包;所述发送源节点 N_{Source} 为用户终端;所述目的节点 $N_{Destination}$ 为交换设备，该交换设备既是目的节点 $N_{Destination}$，又是第一个交换设备 SW-first，同时还是最后一个交换设备 SW-last;

4.4.2）目的节点$N_{Destination}$使用与发送源节点N_{Source}之间的单播密钥解密数据包。

优选的，当数据通信类型是用户终端到不直连交换设备的数据通信类型时，所述其节点间保密通信策略的具体实现方式是:

4.5.1）发送源节点 N_{Source} 使用与第一个交换设备 SW-first 之间的单播密钥加密数据包；所述发送源节点 N_{Source} 是用户终端;

4.5.2）第一个交换设备 SW-first 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，然后使用与目的节点 $N_{Destination}$ 之间的交换密钥加密数据包，然后转发;所述目的节点 $N_{Destination}$ 为交换设备，该交换设备既是目的节点 $N_{Destination}$，又是最后一个交换设备 SW-last;

4.5.3）若存在中间交换设备，则中间交换设备直接转发类型为用户终端到不直连交换设备的通信的数据包;

4.5.4）目的节点$N_{Destination}$使用与第一个交换设备SW-first之间的交换密钥解密数据包。

优选的，当数据通信类型是用户终端到同一交换设备下其他直连用户终端

的数据通信类型时，所述其节点间保密通信策略的具体实现方式是：

4.6.1）对已经建立站间密钥、类型为用户终端到同一交换设备下其他直连用户终端的通信采用的保密通信策略如下：

4.6.1.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的站间密钥加密数据包；所述目的节点 $N_{Destination}$ 是用户终端；

4.6.1.2）第一个交换设备 SW-first 对于类型用户终端到同一交换设备下其他直连用户终端的通信的数据包，直接转发；所述第一个交换设备 SW-first 同时是最后一个交换设备 SW-last；

4.6.1.3）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的站间密钥解密数据包；

4.6.2）对没有建立站间密钥、类型为用户终端到同一交换设备下其他直连用户终端的通信所采用的保密通信如下：

4.6.2.1）发送源节点 N_{Source} 使用与直连交换设备之间的单播密钥加密数据包；

4.6.2.2）第一个交换设备 SW-first 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，再使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包，再转发；所述第一个交换设备 SW-first 同时是最后一个交换设备 SW-last；

4.6.2.3）目的节点 $N_{Destination}$ 使用与直连交换设备之间的单播密钥解密数据包。

优选的，当数据通信类型是用户终端到不同交换设备下直连用户终端的数据通信类型时，所述其节点间保密通信策略的具体实现方式是：

4.7.1）发送源节点 N_{Source} 使用与第一个交换设备 SW-first 之间的单播密钥加密数据包；所述发送源节点 N_{Source} 是用户终端；

4.7.2）第一个交换设备 SW-first 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，然后使用与最后一个交换设备 SW-last 之间的交换密钥加密数据包，再转发；

4.7.3）若存在中间交换设备，则中间交换设备直接转发类型为用户终端到不同交换设备下直连用户终端的通信的数据包；

4.7.4）最后一个交换设备 SW-last 使用与第一个交换设备 SW-first 之间的

交换密钥解密数据包，然后使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包，再转发；所述目的节点 $N_{Destination}$ 是用户终端；

4.7.5）目的节点 $N_{Destination}$ 使用与最后一个交换设备 SW-last 之间的单播密钥解密数据包。

本发明还提供一种节点间保密通信系统，所述系统包括：发送源节点 N_{Source}、第一个交换设备SW-first、第二交换设备SW-last和目的节点 $N_{Destination}$，其中，

发送源节点 N_{Source}，用于向目的节点 $N_{Destination}$ 发送交换路由探寻分组及加密数据包，接收目的节点 $N_{Destination}$ 发送的交换路由探寻响应分组并记录下从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的交换路由信息；

第一个交换设备 SW-first，用于转发从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包，并记录下从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的交换路由信息；

第二交换设备 SW-last，用于转发从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包，并记录下从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的交换路由信息；

目的节点 $N_{Destination}$，用于接收发送源节点 N_{Source} 发送的交换路由探寻分组及加密数据包，向发送源节点 N_{Source} 发送交换路由探寻响应分组并记录下从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的交换路由信息；

其中，所述从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的交换路由信息包括 ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$ 以及 $ID_{Destination}$。

所述系统还包括：中间交换设备，用于直接透传从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的所有数据包。

本发明的优点是：本发明所提供的有线局域网节点间保密通信方法和系统，需要为相邻节点之间建立共享密钥、为交换设备两两之间建立共享密钥、为同一个交换设备下的直连用户终端两两之间建立共享密钥，根据交换路由探寻过程得到节点间的交换路由信息，判断两节点之间的数据通信所属的类型，从而选用对应的保密通信策略。本发明所提供的方法即系统中以交换路由信息为基础划分数据通信的类型，对于不同数据通信类型采用不同的保密通信策略。相对于逐跳加密，减少了交换设备的计算负担，缩短了数据包的传输延时；

相对于为所有节点之间两两建立站间密钥来保护通信机密性的方法，减少了密钥的数目，简化了密钥管理。

附图说明

图 1 为本发明所述局域网基本框架示意图；

图 2 为本发明所述节点间交换路由网络结构示意图；

图 3 为本发明所述交换路由探寻协议示意图；

图 4 为本发明所述节点间交换路由探寻过程示意图；

图 5 为本发明所述节点间数据通信类型判断流程图示意图；

图 6-a 为本发明所述交换设备到交换设备的通信（相邻）示意图；

图 6-b 为本发明所述交换设备到交换设备的通信（不相邻）示意图；

图 7 为本发明所述交换设备到直连用户终端的通信示意图；

图 8 为本发明所述交换设备到不直连的用户终端的通信示意图；

图 9 为本发明所述用户终端到直连交换设备的通信示意图；

图 10 为本发明所述用户终端到不直连的交换设备的通信示意图；

图 11-a 为本发明所述用户终端到同一交换设备下其他直连用户终端的通信（建立站间密钥）示意图；

图 11-b 为本发明所述用户终端到同一交换设备下其他直连用户终端的通信（不建立站间密钥）示意图；

图12为本发明所述用户终端到不同交换设备下直连用户终端的通信示意图。

具体实施方式

本发明中的节点 N（Node）是指网络中的用户终端 STA（STAtion）和交换设备 SW（Switch）。集线器（hub）等物理层设备不作为节点处理。

本发明中定义的直连是指交换设备之间或者交换设备和用户终端之间通过网线或者集线器（hub）等物理层设备直接相连的连接关系。通过其他设备进行连接的节点之间不属于直连关系。

参见图 1-12，本发明提供的有线局域网节点保密通信方法主要包括四个过程：建立共享密钥、交换路由探寻、数据通信分类以及节点间保密通信。其具体实施方式如下：

1）建立共享密钥；即节点之间建立共享密钥；所述节点之间包括用户终端与交换设备之间、交换设备两两之间以及同一交换设备下两个直连用户终端之间，具体包括:

1.1）为相邻节点之间建立共享密钥，称为单播密钥 USK（Unicast Session Key）;

1.2）为交换设备两两之间建立共享密钥，称为交换密钥 SWkey（SWitch key），其中相邻交换设备之间的单播密钥就是它们之间的交换密钥;

1.3）根据本地策略选择，为同一交换设备下两个直连用户终端之间建立共享密钥，称为站间密钥STAkey(STAtion key）。

局域网基本框架如图 1 所示。所有相邻的节点之间都有单播密钥 USK，如相邻的交换设备 SW-A 和 SW-B 之间、相邻的交换设备 SW-E 与用户终端 STA2 之间；交换设备两两之间都具有交换密钥 SWkey，如相邻的交换设备 SW-B 与 SW-E 之间、不相邻的交换设备 SW-E 和 SW-G 之间；同一交换设备下直连的用户终端 STA 之间可建立站间密钥 STAkey，如用户终端 STA1 和 STA2 之间、用户终端 STA7 与 STA9 之间。其中单播密钥和交换密钥是节点成功接入网络时建立的，而站间密钥则是在通信发生时，由发送源节点 N_{Source} 根据本地策略决定是否建立。一般来说若用户终端 STA1 发送给同一交换设备下其他直连用户终端 STA2 的数据量比较大，则需建立站间密钥；若只是简单的数据包信息，则不需建立站间密钥。单播密钥、交换密钥及站间密钥可通过预分发或某种安全机制建立，其建立的具体方法本发明不予限制和定义。

2）交换路由探寻；即节点之间根据所述共享密钥交换路由探寻，得到节点之间的交换路由信息，具体包括:

从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的节点间交换路由信息定义为一个标识四元组:

$$[ID_{Source}, ID_{SW\text{-}first}, ID_{SW\text{-}last}, ID_{Destination}]$$

其中:

ID_{Source}：表示发送源节点 N_{Source} 的标识，其中发送源节点 N_{Source} 可以是用户终端，也可以是交换设备;

$ID_{SW\text{-}first}$：表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的

第一个交换设备 SW-first 的标识;

$ID_{SW\text{-}last}$: 表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的最后一个交换设备 SW-last 的标识;

$ID_{Destination}$: 表示目的节点 $N_{Destination}$ 的标识，其中目的节点 $N_{Destination}$ 可以是用户终端，也可以是交换设备。

从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的交换路由信息[ID_{Source}, $ID_{SW\text{-}first}$, $ID_{SW\text{-}last}$, $ID_{Destination}$]对应的网络结构如图 2 所示。其中接收到从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包但却未出现在交换路由信息标识四元组中的交换设备，称之为中间交换设备。从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据在传输过程中可能不会通过中间交换设备，也可能通过多个中间交换设备。

在网络中，当需要知晓从节点 N_{Source} 到节点 $N_{Destination}$ 的交换路由信息时，需发起交换路由探寻过程。如图 3 所示，交换路由探寻包括交换路由探寻分组和交换路由响应分组。交换路由探寻过程具体描述如图 4 所示。

2.1）发送源节点 N_{Source} 发送交换路由探寻分组给目的节点 $N_{Destination}$;

发送源节点 N_{Source} 构造交换路由探寻分组发送给目的节点 $N_{Destination}$; 该分组中主要包含标识四元组

$$[ID_{Source}, ID_{SW\text{-}first}, ID_{SW\text{-}last}, ID_{Destination}]$$

其中:

ID_{Source}: 表示发送源节点 N_{Source} 的标识;

$ID_{SW\text{-}first}$: 表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的第一个交换设备 SW-first 的标识，若发送源节点 N_{Source} 为交换设备，则 $ID_{SW\text{-}first}$ 就是 ID_{Source}; 若发送源节点 N_{Source} 为终端用户，则 $ID_{SW\text{-}first}$ 就是发送源节点 N_{Source} 直连交换设备的标识;

$ID_{SW\text{-}last}$: 表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的最后一个交换设备 SW-last 的标识; 在交换路由探寻分组中，该字段是未知的（图 4 中用问号（‘？’）表示）;

$ID_{Destination}$: 表示目的节点 $N_{Destination}$ 的标识;

2.2）目的节点 $N_{Destination}$ 发送交换路由响应分组给发送源节点 N_{Source};

目的节点 $N_{Destination}$ 收到来自发送源节点 N_{Source} 发送的交换路由探寻分组后，进行如下处理:

2.2.1）判断从发送源节点 N_{Source} 发来的数据包经过的最后一个交换设备 SW-last 的信息：若目的节点 $N_{Destination}$ 为交换设备，则 $ID_{SW\text{-}last}$ 就是 $ID_{Destination}$；若目的节点 $N_{Destination}$ 为终端用户，则 $ID_{SW\text{-}last}$ 就是终端用户直连交换设备的标识;

2.2.2）记录下标识四元组[ID_{Source}，$ID_{SW\text{-}first}$，$ID_{SW\text{-}last}$，$ID_{Destination}$]， 其中 ID_{Source}、$ID_{SW\text{-}first}$ 及 $ID_{Destination}$ 同接收到的交换路由探寻分组中各字段的值，此时四元组的所有字段值都已明确;

2.2.3）构造交换路由响应分组发送给发送源节点 N_{Source}，该分组主要包含已明确所有字段值的标识四元组[ID_{Source}, $ID_{SW\text{-}first}$, $ID_{SW\text{-}last}$, $ID_{Destination}$]。

2.3）各节点接收交换路由响应分组;

2.3.1）交换设备收到交换路由响应分组后，若自己的标识在该分组中的标识四元组中，则记录下标识四元组[ID_{Source}, $ID_{SW\text{-}first}$, $ID_{SW\text{-}last}$, $ID_{Destination}$]，再转发；若自己的标识不在该分组中的标识四元组中则直接转发该分组;

2.3.2）发送源节点 N_{Source} 收到交换路由响应分组后，记录下标识四元组[ID_{Source}, $ID_{SW\text{-}first}$, $ID_{SW\text{-}last}$, $ID_{Destination}$]，完成此次交换路由探寻过程。

整个网络中只有发送源节点 N_{Source}、第一个交换设备 SW-first、最后一个交换设备 SW-last 以及目的节点 $N_{Destination}$ 需要记录下从发送源节点 N_{Source} 到目的 $N_{Destination}$ 的交换路由信息。若发送源节点 N_{Source} 是交换设备，则从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的第一个交换设备 SW-first 就是它本身，即 SW-first 就是 N_{Source}；若目的节点 $N_{Destination}$ 是交换设备，则从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的最后一个交换设备 SW-last 就是 $N_{Destination}$，即 SW-last 就是 $N_{Destination}$。

3）数据通信类型分类；即节点之间根据所述交换路由信息判断节点之间的数据通信类型，具体包括:

从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据保密通信根据节点 N_{Source} 与 $N_{Destination}$ 之间的物理连接关系及它们本身的节点类型可划分为如下 7 种类型:

Type1: 交换设备到交换设备的通信;

例如: 图 1 中的 SW-A 到 SW-E、SW-D 到 SW-B 的数据通信;

Type2: 交换设备到直连用户终端的通信;

例如: 图 1 中的 SW-E 到 STA1、SW-G 到 STA9 的数据通信;

Type3: 交换设备到不直连用户终端的通信;

例如: 图 1 中的 SW-A 到 STA1、SW-D 到 STA6 的数据通信;

Type4: 用户终端到直连交换设备的通信;

例如: 图 1 中的 STA2 到 SW-E、STA5 到 SW-F 的数据通信;

Type5: 用户终端到不直连交换设备的通信;

例如: 图 1 中的 STA2 到 SW-F、STA5 到 SW-B 的数据通信;

Type6: 用户终端到同一交换设备下其他直连用户终端的通信;

例如: 图 1 中的 STA2 到 STA3、STA5 到 STA6 的数据通信;

Type7: 用户终端到不同交换设备下直连的用户终端的通信;

例如: 图 1 中的 STA2 到 STA6、STA5 到 STA9 的数据通信;

从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信类型是根据得到的交换路由四元组信息[ID_{Source}, $ID_{SW\text{-}first}$, $ID_{SW\text{-}last}$, $ID_{Destination}$]进行判断的，具体的判断流程如图 5 所示。流程描述如下:

3.1）判断$ID_{SW\text{-}first}$= ID_{Source}是否成立，若成立，则发送源节点N_{Source}是交换设备，执行步骤3.2）；否则，发送源节点N_{Source}是用户终端，执行步骤3.4）;

3.2）判断$ID_{SW\text{-}last}$= $ID_{Destination}$是否成立，若成立，则目的节点$N_{Destination}$是交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是交换设备到交换设备的通信，属于类型Type1；否则，目的节点$N_{Destination}$是用户终端，执行步骤3.3）;

3.3）判断$ID_{SW\text{-}last}$= $ID_{SW\text{-}first}$是否成立，若成立，则从发送源节点N_{Source}到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是交换设备到直连用户终端的通信，属于类型Type2；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是交换设备到不直连用户终端的通信，属于类型Type3;

3.4）判断$ID_{SW-last}$=$ID_{Destination}$是否成立，若成立，则目的节点$N_{Destination}$是交换设备，执行步骤3.5）；否则，目的节点$N_{Destination}$是用户终端，执行步骤3.6）；

3.5）判断$ID_{SW-last}$= $ID_{SW-first}$是否成立，若成立，则从发送源节点N_{Source}到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到直连交换设备的通信，属于类型Type4；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到不直连交换设备的通信，属于类型Type5；

3.6）判断$ID_{SW-last}$=$ID_{SW-first}$是否成立，若成立，则从发送源节点N_{Source}到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到同一交换设备下其他直连用户终端的通信，属于类型Type6；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到不同交换设备下直连的用户终端的通信，属于类型Type7。

4）节点间保密通信；即根据节点之间不同的数据通信类型采用不同的保密通信策略进行节点间保密通信，具体包括：

从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的节点间数据通信，根据数据通信类型的不同，通信过程中所采用的保密通信策略也将有所不同，具体每种通信类型所采用的保密通信策略描述如下：

4.1）Type1：交换设备到交换设备的通信

网络中交换设备两两之间都有交换密钥（交换密钥的建立过程本发明不予定义和限制），类型为 Type1 的数据通信采用的保密通信策略如下：

4.1.1）发送源节点 N_{Source}（此时为交换设备，发送源节点 N_{Source} 同时是第一个交换设备 SW-first）使用与目的节点 $N_{Destination}$（此时为交换设备，目的节点 $N_{Destination}$ 同时是最后一个交换设备 SW-last）之间的交换密钥加密数据包；

4.1.2）若存在中间交换设备，则中间交换设备收到类型为 Type1 的通信数据包，直接转发。

4.1.3）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的交换密钥解密数据包；

交换设备到交换设备的通信包含交换设备到相邻交换设备的通信（如图6-a中交换设备SW-B到交换设备SW-E的通信）、交换设备到不相邻交换设备的通信（如图6-b中交换设备SW-B到交换设备SW-G的通信）。图6-a中直接使用交换密钥 $SWkey_{B-E}$ 来加密解密数据包；图6-b中直接使用交换密钥 $SWkey_{B-G}$ 来加密解密数据包，中间交换设备（如交换设备SW-A、SW-D）直接转发即可。

4.2）Type2：交换设备到直连用户终端的通信

网络中交换设备与直连用户终端之间有单播密钥（单播密钥的建立过程本发明不予定义和限制），类型为Type2的数据通信采用的保密通信策略如下：

4.2.1）发送源节点 N_{Source}（此时为交换设备，发送源节点 N_{Source} 同时是第一个交换设备SW-first、最后一个交换设备SW-last））使用与目的节点 $N_{Destination}$（此时为用户终端）之间的单播密钥加密数据包；

4.2.2）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包。

如图7所示，交换设备SW-E到用户终端STA3的通信属于Type2，交换设备SW-E作为发送源节点使用单播密钥 USK_{3-E} 加密数据包，用户终端STA3作为目的节点使用单播密钥 USK_{3-E} 解密数据包。

4.3）Type3：交换设备到不直连用户终端的通信

网络中交换设备与直连用户终端之间有单播密钥、交换设备之间有交换密钥，类型为Type3的数据通信采用的保密通信策略如下：

4.3.1）发送源节点 N_{Source}（此时为交换设备，发送源节点 N_{Source} 同时是第一个交换设备SW-first）使用与最后一个交换设备SW-last之间的交换密钥加密数据包；

4.3.2）若存在中间交换设备，则中间交换设备直接转发类型为Type3的数据包；

4.3.3）最后一个交换设备SW-last使用与发送源节点 N_{Source} 的交换密钥解密数据包，然后使用与目的节点 $N_{Destination}$（此时为用户终端）之间的单播密钥加密数据包，然后转发；

4.3.4）目的节点 $N_{Destination}$ 使用与最后一个交换设备SW-last之间的单播密

钥解密数据包。

如图 8 所示，交换设备 SW-A 到用户终端 STA3 的通信属于 Type3，SW-E 是最后一个交换设备。交换设备 SW-A 作为发送源节点使用与 SW-E 之间的交换密钥 $SWkey_{A-E}$ 加密数据包；交换设备 SW-B 属于中间交换设备直接转发数据包；交换设备 SW-E 作为最后一个交换设备使用交换密钥 $SWkey_{A-E}$ 解密数据包，然后用与用户终端 STA3 之间的单播密钥 USK_{3-E} 加密数据包，再转发；用户终端 STA3 作为目的节点使用单播密钥 USK_{3-E} 解密数据包；

4.4）Type4: 用户终端到直连交换设备的通信

网络中用户终端与直连交换设备之间有单播密钥，类型为 Type4 的数据通信采用的保密通信策略如下:

4.4.1）发送源节点 N_{Source}（此时为用户终端）使用与目的节点 $N_{Destination}$（此时为交换设备，目的节点 $N_{Destination}$ 同时是第一个交换设备 SW-first、最后一个交换设备 SW-last）之间的单播密钥加密数据包;

4.4.2）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包。

如图 9 所示，用户终端 STA3 到交换设备 SW-E 的通信属于 Type4，用户终端 STA3 作为发送源节点使用单播密钥 USK_{3-E} 加密数据包；交换设备 SW-E 作为目的节点使用单播密钥 USK_{3-E} 解密数据包。类型 Type4 的通信和类型 Type2 的通信只是方向不同，都是使用发送源节点与目的节点之间的单播密钥来加密解密数据包。

4.5）Type5: 用户终端到不直连交换设备的通信

网络中用户终端与直连交换设备之间有单播密钥、交换设备之间有交换密钥，类型为 Type5 的数据通信采用的保密通信策略如下:

4.5.1）发送源节点 N_{Source}（此时为用户终端）使用与第一个交换设备 SW-first 之间的单播密钥加密数据包;

4.5.2）第一个交换设备 SW-first 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，然后使用与目的节点 $N_{Destination}$（此时为交换设备，目的节点 $N_{Destination}$ 同时是最后一个交换设备 SW-last）之间的交换密钥加密数据包，然后转发;

4.5.3）若存在中间交换设备，则中间交换设备直接转发类型为 Type5 的数据包；

4.5.4）目的节点 $N_{Destination}$ 使用与第一个交换设备 SW-first 之间的交换密钥解密数据包。

如图 10 所示，用户终端 STA3 到交换设备 SW-A 的通信属于 Type5，SW-E 是第一个交换设备。用户终端 STA3 作为发送源节点使用单播密钥 $USK_{3\text{-}E}$ 加密数据包；交换设备 SW-E 作为第一个交换设备使用单播密钥 $USK_{3\text{-}E}$ 解密数据包，然后用与目的节点 SW-A 之间的交换密钥 $SWkey_{A\text{-}E}$ 加密数据包，再转发；交换设备 SW-A 作为目的节点使用与 SW-E 之间的交换密钥 $SWkey_{A\text{-}E}$ 解密数据包。类型 Type5 的通信和类型 Type3 的通信只是方向不同，过程相反，中间使用的密钥都是一样的。

3.2.6）Type6: 用户终端到同一交换设备下其他直连用户终端的通信

网络中用户终端与直连交换设备之间有单播密钥、同一交换设备下直连的用户终端之间根据本地决策可选择建立站间密钥（站间密钥的建立过程本发明不予定义和限制）。类型为 Type6 的数据通信根据是否已建立站间密钥，所采用的保密通信有所不同。

4.6.1）对已经建立站间密钥、类型为 Type6 的数据通信采用的保密通信策略如下：

4.6.1.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$（此时为用户终端）之间的站间密钥加密数据包；

4.6.1.2）第一个交换设备 SW-first（此时，第一个交换设备 SW-first 同时是最后一个交换设备）对于类型 Type6 的数据包，直接转发；

4.6.1.3）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的站间密钥解密数据包。

4.6.2）对没有建立站间密钥、类型为 Type6 所采用的保密通信如下：

4.6.2.1）发送源节点 N_{Source} 使用与直连交换设备之间的单播密钥加密数据包；

4.6.2.2）第一个交换设备 SW-first（此时，第一个交换设备 SW-first 同时是最后一个交换设备）使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，

再使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包，再转发；

4.6.2.3）目的节点 $N_{Destination}$ 使用与直连交换设备之间的单播密钥解密数据包。

如图 11-a、11-b 所示，用户终端 STA1 到 STA3 之间的数据通信属于类型 Type6。

图 11-a 是已建立了站间密钥的通信图示，用户终端 STA1 作为发送源节点使用与 STA3 之间的站间密钥 $STAkey_{1-3}$ 加密数据包；交换设备 SW-E 直接转发数据包；用户终端 STA3 作为目的节点使用与 STA1 之间的站间密钥 $STAkey_{1-3}$ 解密数据包。

图 11-b 是没有建立站间密钥的通信图示，用户终端 STA1 作为发送源节点使用交换设备 SW-E 之间的单播密钥 USK_{1-E} 加密数据包；交换设备 SW-E 使用单播密钥 USK_{1-E} 解密数据包，然后用单播密钥 USK_{3-E} 加密数据包，再转发；用户终端 STA3 作为目的节点使用单播密钥 USK_{3-E} 解密数据包。

4.7）Type7：用户终端到不同交换设备下直连的用户终端的通信

网络中用户终端与直连交换设备之间有单播密钥，交换设备之间有交换密钥，类型为 Type7 的数据通信采用的保密通信策略如下：

4.7.1）发送源节点 N_{Source}（此时为用户终端）使用与第一个交换设备 SW-first 之间的单播密钥加密数据包；

4.7.2）第一个交换设备 SW-first 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，然后使用与最后一个交换设备 SW-last 之间的交换密钥加密数据包，再转发；

4.7.3）若存在中间交换设备，则中间交换设备直接转发类型为 Type7 的数据包；

4.7.4）最后一个交换设备 SW-last 使用与第一个交换设备 SW-first 之间的交换密钥解密数据包，然后使用与目的节点 $N_{Destination}$（此时为用户终端）之间的单播密钥加密数据包，再转发；

4.7.5）目的节点 $N_{Destination}$ 使用与最后一个交换设备 SW-last 之间的单播密钥解密数据包。

如图 12 所示，用户终端 STA3 到 STA9 的通信属于类型 Type7。类型 Type7

的数据通信可以分三段，发送源节点到第一个交换设备、第一个交换设备到最后一个交换设备、最后一个交换设备到目的节点。图 12 中，用户终端 STA3 作为发送源节点使用与交换设备 SW-E 之间的单播密钥 $USK_{3\text{-}E}$ 加密数据包；交换设备 SW-E 作为第一个交换设备使用与发送源节点之间的单播密钥 $USK_{3\text{-}E}$ 解密数据包，再使用与最后一个交换设备 SW-G 之间的交换密钥 $SWkey_{E\text{-}G}$ 加密数据包，再转发；交换设备 SW-D、SW-A、SW-D 作为中间交换设备直接转发数据包；交换设备 SW-G 作为最后一个交换设备使用与第一个交换设备 SW-E 之间的交换密钥 $SWkey_{E\text{-}G}$ 解密数据包，再使用与目的节点之间的单播密钥 $USK_{9\text{-}G}$ 加密数据包，再转发；用户终端 STA9 作为目的节点使用与最后一个交换设备 SW-G 之间的单播密钥 $USK_{9\text{-}G}$ 解密数据包。

本发明的节点间保密通信系统包括：发送源节点N_{Source}、第一个交换设备SW-first、第二交换设备SW-last（即最后一个交换设备SW-last）和目的节点$N_{Destination}$，其中，

发送源节点N_{Source}，用于向目的节点$N_{Destination}$发送交换路由探寻分组及加密数据包，接收目的节点$N_{Destination}$发送的交换路由探寻响应分组并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息[ID_{Source}，$ID_{SW\text{-}first}$，$ID_{SW\text{-}last}$，$ID_{Destination}$]；第一个交换设备SW-first，用于转发从发送源节点N_{Source}到目的节点$N_{Destination}$的数据包，并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息[ID_{Source}，$ID_{SW\text{-}first}$，$ID_{SW\text{-}last}$，$ID_{Destination}$]；第二交换设备SW-last，用于转发从发送源节点N_{Source}到目的节点$N_{Destination}$的数据包，并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息[ID_{Source}，$ID_{SW\text{-}first}$，$ID_{SW\text{-}last}$，$ID_{Destination}$]；目的节点$N_{Destination}$，用于接收发送源节点N_{Source}发送的交换路由探寻分组及加密数据包，向发送源节点N_{Source}发送交换路由探寻响应分组并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息[ID_{Source}，$ID_{SW\text{-}first}$，$ID_{SW\text{-}last}$，$ID_{Destination}$]。其中，所述从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$。

优选的，所述系统还可以包括：中间交换设备，用于直接透传从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的所有数据包。

本发明中提供的节点间保密通信的方法会根据节点间不同的通信情况进

行分类，选择合适的保密通信策略。相对于逐跳加密，减少了交换设备的计算负担，缩短了数据包的传输延时；相对于为所有节点之间两两建立站间密钥来保护通信机密性的方法，减少了密钥的数目，简化了密钥管理。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权 利 要 求

1、一种有线局域网节点间保密通信方法，其特征在于：包括:

1）节点之间建立共享密钥；所述节点之间包括用户终端与交换设备之间、交换设备两两之间以及同一交换设备下两个直连用户终端之间；

2）节点之间根据所述共享密钥交换路由探寻，得到节点之间的交换路由信息；

3）节点之间根据所述交换路由信息判断节点之间的数据通信类型；

4）根据节点之间不同的数据通信类型采用不同的保密通信策略进行节点间保密通信。

2、根据权利要求1所述的有线局域网节点间保密通信方法，其特征在于：所述步骤1）的具体实现方式是:

1.1）为相邻节点之间建立共享密钥，称为单播密钥 USK（Unicast Session Key）;

1.2）为局域网交换设备两两之间建立共享密钥，称为交换密钥 SWkey（SWitch key）;

1.3）根据本地策略选择，为同一交换设备下两个直连用户终端之间建立共享密钥，称为站间密钥STAkey（STAtion key）。

3、根据权利要求1所述的有线局域网节点间保密通信方法，其特征在于：

从发送源节点N_{Source}到目的节点$N_{Destination}$的节点间交换路由信息定义为一个标识四元组；接收到从发送源节点N_{Source}到目的节点$N_{Destination}$的数据包但却未出现在交换路由信息标识四元组中的交换设备，称之为中间交换设备；所述步骤2）的具体实现方式是:

2.1）发送源节点 N_{Source} 发送交换路由探寻分组给目的节点 $N_{Destination}$；该分组中主要包含标识四元组，所述标识四元组包括 ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$ 以及 $ID_{Destination}$;

其中:

ID_{Source}：表示发送源节点 N_{Source} 的标识;

$ID_{SW\text{-}first}$：表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的第一个交换设备 SW-first 的标识，若发送源节点 N_{Source} 为交换设备，则 $ID_{SW\text{-}first}$

就是 ID_{Source}；若发送源节点 N_{Source} 为终端用户，则 $ID_{SW\text{-}first}$ 就是发送源节点 N_{Source} 直连交换设备的标识；

$ID_{SW\text{-}last}$：表示从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的最后一个交换设备 SW-last 的标识；在交换路由探寻分组中，该字段是未知的；

$ID_{Destination}$：表示目的节点$N_{Destination}$的标识；其中目的节点$N_{Destination}$是用户终端或交换设备；

2.2）目的节点 $N_{Destination}$ 发送交换路由响应分组给发送源节点 N_{Source}；

2.3）各节点接收交换路由响应分组。

4、根据权利3要求所述的有线局域网节点间保密通信方法，其特征在于：目的节点$N_{Destination}$收到来自发送源节点N_{Source}发送的交换路由探寻分组后，所述步骤2.2）的具体实现方式是：

2.2.1）判断从发送源节点 N_{Source} 发来的数据包经过的最后一个交换设备 SW-last 的信息：若目的节点 $N_{Destination}$ 为交换设备，则 $ID_{SW\text{-}last}$ 就是 $ID_{Destination}$；若目的节点 $N_{Destination}$ 为终端用户，则 $ID_{SW\text{-}last}$ 就是终端用户直连交换设备的标识；

2.2.2）记录下标识四元组，其中 ID_{Source}、$ID_{SW\text{-}first}$ 及 $ID_{Destination}$ 同接收到的交换路由探寻分组中各字段的值，此时四元组的所有字段值都已明确；所述标识四元组包括 ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$ 以及 $ID_{Destination}$；

2.2.3）构造交换路由响应分组发送给发送源节点N_{Source}，该分组包含已明确所有字段值的标识四元组，所述标识四元组包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$。

5、根据权利4要求所述的有线局域网节点间保密通信方法，其特征在于：各节点收到来自目的节点$N_{Destination}$发送的交换路由探寻响应分组后，所述步骤2.3）的具体实现方式是：

2.3.1）交换设备收到交换路由响应分组后，若自己的标识在该分组中的标识四元组中，则记录下标识四元组再转发；若自己的标识不在该分组中的标识四元组中则直接转发该分组；所述标识四元组包括 ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$ 以及 $ID_{Destination}$；

2.3.2）发送源节点N_{Source}收到交换路由响应分组后，记录下标识四元组，

完成此次交换路由探寻过程，所述标识四元组包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$。

6、根据权利要求5所述的有线局域网节点间保密通信方法，其特征在于：所述步骤3）的具体实现方式是：

从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信类型是根据得到的交换路由四元组信息进行判断的，所述四元组信息包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$，其具体的判断方式是：

3.1）判断$ID_{SW\text{-}first}= ID_{Source}$是否成立，若成立，则发送源节点$N_{Source}$是交换设备，执行步骤3.2）；否则，发送源节点$N_{Source}$是用户终端，执行步骤3.4）；

3.2）判断$ID_{SW\text{-}last}= ID_{Destination}$是否成立，若成立，则目的节点$N_{Destination}$是交换设备，从发送源节点$N_{Source}$到目的节点$N_{Destination}$的数据通信是交换设备到交换设备的通信，属于交换设备到交换设备的通信类型；否则，目的节点$N_{Destination}$是用户终端，执行步骤3.3）；

3.3）判断$ID_{SW\text{-}last}= ID_{SW\text{-}first}$是否成立，若成立，则从发送源节点$N_{Source}$到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点$N_{Source}$到目的节点$N_{Destination}$的数据通信是交换设备到直连用户终端的通信，属于交换设备到直连用户终端的通信类型；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是交换设备到不直连用户终端的通信，属于交换设备到不直连用户终端的通信类型；

3.4）判断$ID_{SW\text{-}last}=ID_{Destination}$是否成立，若成立，则目的节点$N_{Destination}$是交换设备，执行步骤3.5）；否则，目的节点$N_{Destination}$是用户终端，执行步骤3.6）；

3.5）判断$ID_{SW\text{-}last}= ID_{SW\text{-}first}$是否成立，若成立，则从发送源节点$N_{Source}$到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点$N_{Source}$到目的节点$N_{Destination}$的数据通信是用户终端到直连交换设备的通信，属于用户终端到直连交换设备的通信类型；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到不直连交换设备的通信，属于用户终端到不直连交换设备的通信类型；

3.6）判断$ID_{SW-last}=ID_{SW-first}$是否成立，若成立，则从发送源节点$N_{Source}$到目的节点$N_{Destination}$的数据只经过一个交换设备，从发送源节点$N_{Source}$到目的节点$N_{Destination}$的数据通信是用户终端到同一交换设备下其他直连用户终端的通信，属于用户终端到同一交换设备下其他直连用户终端的通信类型；否则，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据经过两个以上的交换设备，从发送源节点N_{Source}到目的节点$N_{Destination}$的数据通信是用户终端到不同交换设备下直连的用户终端的通信，属于用户终端到不同交换设备下直连用户终端的通信类型。

7、根据权利要求6所述的有线局域网节点间保密通信方法，其特征在于：当数据通信类型是交换设备到交换设备的数据通信类型时，其节点间保密通信策略的具体实现方式是：

4.1.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的交换密钥加密数据包；所述发送源节点 N_{Source} 是交换设备或第一个交换设备 SW-first；所述目的节点 $N_{Destination}$ 是交换设备或是最后一个交换设备 SW-last;

4.1.2）若存在中间交换设备，则中间交换设备收到类型为交换设备到交换设备的通信数据包，直接转发；

4.1.3）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的交换密钥解密数据包。

8、根据权利要求6所述的有线局域网节点间保密通信方法，其特征在于：当数据通信类型是交换设备到直连用户终端的通信时，其节点间保密通信策略的具体实现方式是：

4.2.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包；所述发送源节点 N_{Source} 是交换设备、第一个交换设备 SW-first 或是最后一个交换设备 SW-last；所述节点 $N_{Destination}$ 是用户终端；

4.2.2）目的节点$N_{Destination}$使用与发送源节点N_{Source}之间的单播密钥解密数据包。

9、根据权利要求6所述的有线局域网节点间保密通信方法，其特征在于：当数据通信类型是交换设备到不直连用户终端的数据通信类型时，其节点间保密通信策略的具体实现方式是：

4.3.1）发送源节点 N_{Source} 使用与最后一个交换设备 SW-last 之间的交换密钥加密数据包；所述发送源节点 N_{Source} 是交换设备或是第一个交换设备 SW-first;

4.3.2）若存在中间交换设备，则中间交换设备直接转发类型为交换设备到不直连用户终端的通信的数据包;

4.3.3）最后一个交换设备 SW-last 使用与发送源节点 N_{Source} 的交换密钥解密数据包，然后使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包，然后转发；所述目的节点 $N_{Destination}$ 是用户终端;

4.3.4）目的节点 $N_{Destination}$ 使用与最后一个交换设备SW-last之间的单播密钥解密数据包。

10、根据权利要求6所述的有线局域网节点间保密通信方法，其特征在于：当数据通信类型是用户终端到直连交换设备的数据通信类型时，其节点间保密通信策略的具体实现方式是:

4.4.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包;所述发送源节点 N_{Source} 是用户终端，所述目的节点 $N_{Destination}$ 是交换设备、第一个交换设备 SW-first 或是最后一个交换设备 SW-last;

4.4.2）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包。

11、根据权利要求6所述的有线局域网节点间保密通信方法，其特征在于：当数据通信类型是用户终端到不直连交换设备的数据通信类型时，其节点间保密通信策略的具体实现方式是:

4.5.1）发送源节点 N_{Source} 使用与第一个交换设备 SW-first 之间的单播密钥加密数据包；所述发送源节点 N_{Source} 是用户终端;

4.5.2）第一个交换设备 SW-first 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，然后使用与目的节点 $N_{Destination}$ 之间的交换密钥加密数据包，然后转发；所述目的节点 $N_{Destination}$ 是交换设备或是最后一个交换设备 SW-last;

4.5.3）若存在中间交换设备，则中间交换设备直接转发类型为用户终端到不直连交换设备的通信的数据包;

4.5.4）目的节点 $N_{Destination}$ 使用与第一个交换设备SW-first之间的交换密钥解

密数据包。

12、根据权利要求6所述的有线局域网节点间保密通信方法，其特征在于：当数据通信类型是用户终端到同一交换设备下其他直连用户终端的数据通信类型时，其节点间保密通信策略的具体实现方式是：

4.6.1）对已经建立站间密钥、类型为用户终端到同一交换设备下其他直连用户终端的通信采用的保密通信策略如下：

4.6.1.1）发送源节点 N_{Source} 使用与目的节点 $N_{Destination}$ 之间的站间密钥加密数据包；所述目的节点 $N_{Destination}$ 是用户终端；

4.6.1.2）第一个交换设备 SW-first 所有交换设备对于类型用户终端到同一交换设备下其他直连用户终端的通信的数据包，直接转发；所述第一个交换设备 SW-first 同时是最后一个交换设备 SW-last；

4.6.1.3）目的节点 $N_{Destination}$ 使用与发送源节点 N_{Source} 之间的站间密钥解密数据包；

4.6.2）对没有建立站间密钥、类型为用户终端到同一交换设备下其他直连用户终端的通信所采用的保密通信如下：

4.6.2.1）发送源节点 N_{Source} 使用与直连交换设备之间的单播密钥加密数据包；

4.6.2.2）第一个交换设备 SW-first 交换设备使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，再使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包，再转发；所述第一个交换设备 SW-first 同时是最后一个交换设备 SW-last；

4.6.2.3）目的节点 $N_{Destination}$ 使用与直连交换设备之间的单播密钥解密数据包。

13、根据权利要求6所述的有线局域网节点间保密通信方法，其特征在于：当数据通信类型是用户终端到不同交换设备下直连用户终端的数据通信类型时，其节点间保密通信策略的具体实现方式是：

4.7.1）发送源节点 N_{Source} 使用与第一个交换设备 SW-first 之间的单播密钥加密数据包；所述发送源节点 N_{Source} 是用户终端；

4.7.2）第一个交换设备 SW-first 使用与发送源节点 N_{Source} 之间的单播密钥解密数据包，然后使用与最后一个交换设备 SW-last 之间的交换密钥加密数据

包，再转发；

4.7.3）若存在中间交换设备，则中间交换设备直接转发类型为用户终端到不同交换设备下直连用户终端的通信的数据包；

4.7.4）最后一个交换设备 SW-last 使用与第一个交换设备 SW-first 之间的交换密钥解密数据包，然后使用与目的节点 $N_{Destination}$ 之间的单播密钥加密数据包，再转发；所述目的节点 $N_{Destination}$ 是用户终端；

4.7.5）目的节点$N_{Destination}$使用与最后一个交换设备SW-last之间的单播密钥解密数据包。

14、一种有线局域网节点间保密通信系统，其特征在于：包括：发送源节点N_{Source}、第一个交换设备SW-first、第二交换设备SW-last和目的节点$N_{Destination}$，其中，

发送源节点N_{Source}，用于向目的节点$N_{Destination}$发送交换路由探寻分组及加密数据包，接收目的节点$N_{Destination}$发送的交换路由探寻响应分组，并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息；

第一个交换设备SW-first，用于转发从发送源节点N_{Source}到目的节点$N_{Destination}$的数据包，并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息；

第二交换设备SW-last，用于转发从发送源节点N_{Source}到目的节点$N_{Destination}$的数据包，并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息的；

目的节点$N_{Destination}$，用于接收发送源节点N_{Source}发送的交换路由探寻分组及加密数据包，向发送源节点N_{Source}发送交换路由探寻响应分组并记录下从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息；

其中，所述从发送源节点N_{Source}到目的节点$N_{Destination}$的交换路由信息包括ID_{Source}、$ID_{SW\text{-}first}$、$ID_{SW\text{-}last}$以及$ID_{Destination}$。

15、根据权利要求 14 所述的有线局域网节点间保密通信系统，其特征在于：还包括：

中间交换设备，用于直接透传从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的所有数据包的中间交换设备。

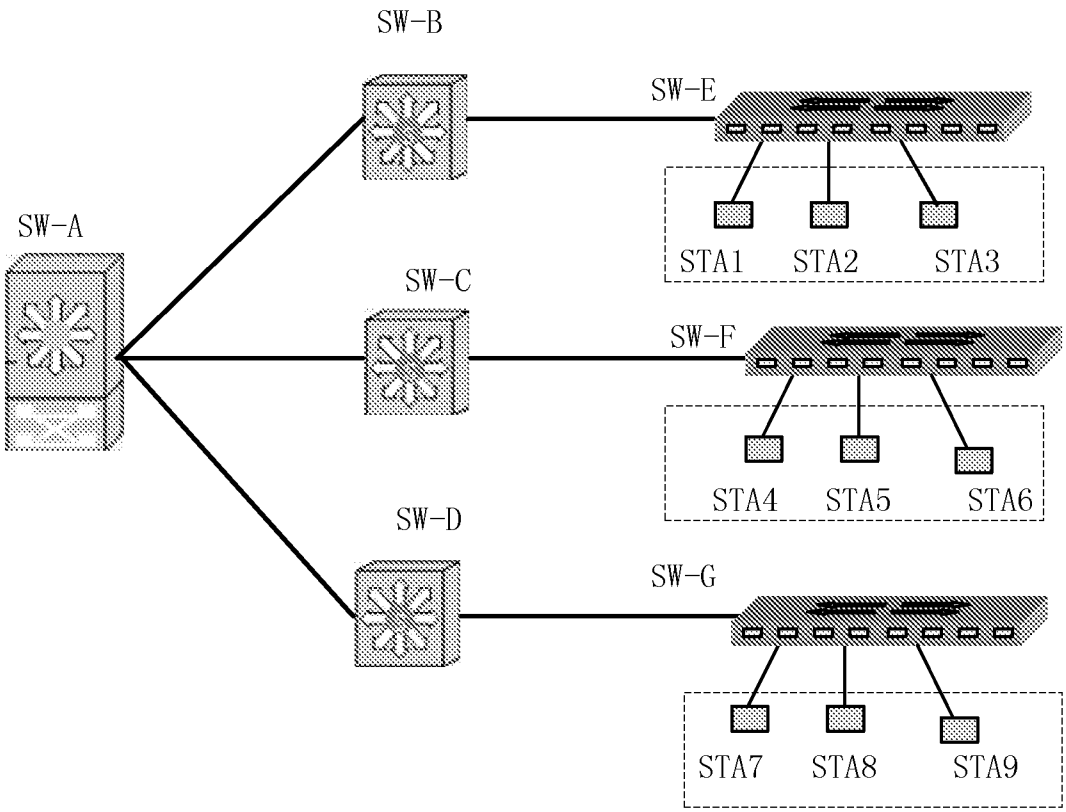
SW-B
SW-E
SW-A
STA1
STA2
STA3
SW-C
SW-F
STA4
STA5
STA6
SW-D
SW-G
STA7
STA8
STA9

图1

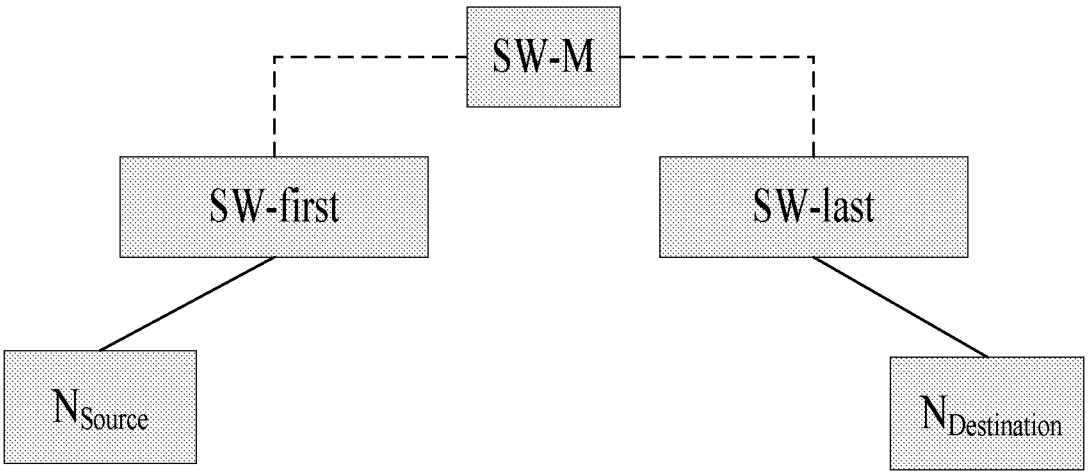
SW-M
SW-first
SW-last
N Source
N Destination

图2


N_{Source}
SW
$N_{Destination}$
交换路由探寻分组
交换路由响应分组

图 3

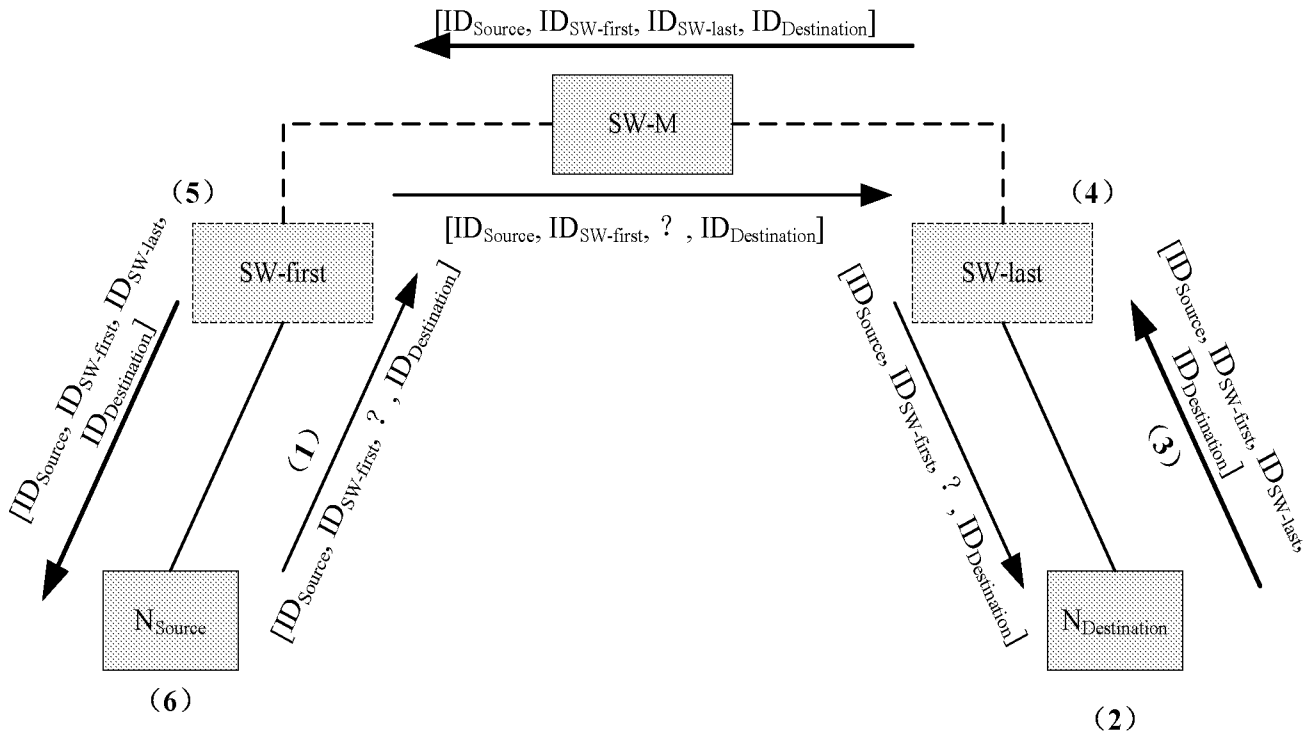
[ID_Source, ID_SW-first, ID_SW-last, ID_Destination]
SW-M
(5)
(4)
[ID_Source, ID_SW-first, ？, ID_Destination]
SW-first
SW-last
[ID_Source, ID_SW-first, ID_SW-last, ID_Destination]
(1)
[ID_Source, ID_SW-first, ？, ID_Destination]
[ID_Source, ID_SW-first, ？, ID_Destination]
(3)
[ID_Source, ID_SW-first, ID_SW-last, ID_Destination]
N_Source
N_Destination
(6)
(2)

图4

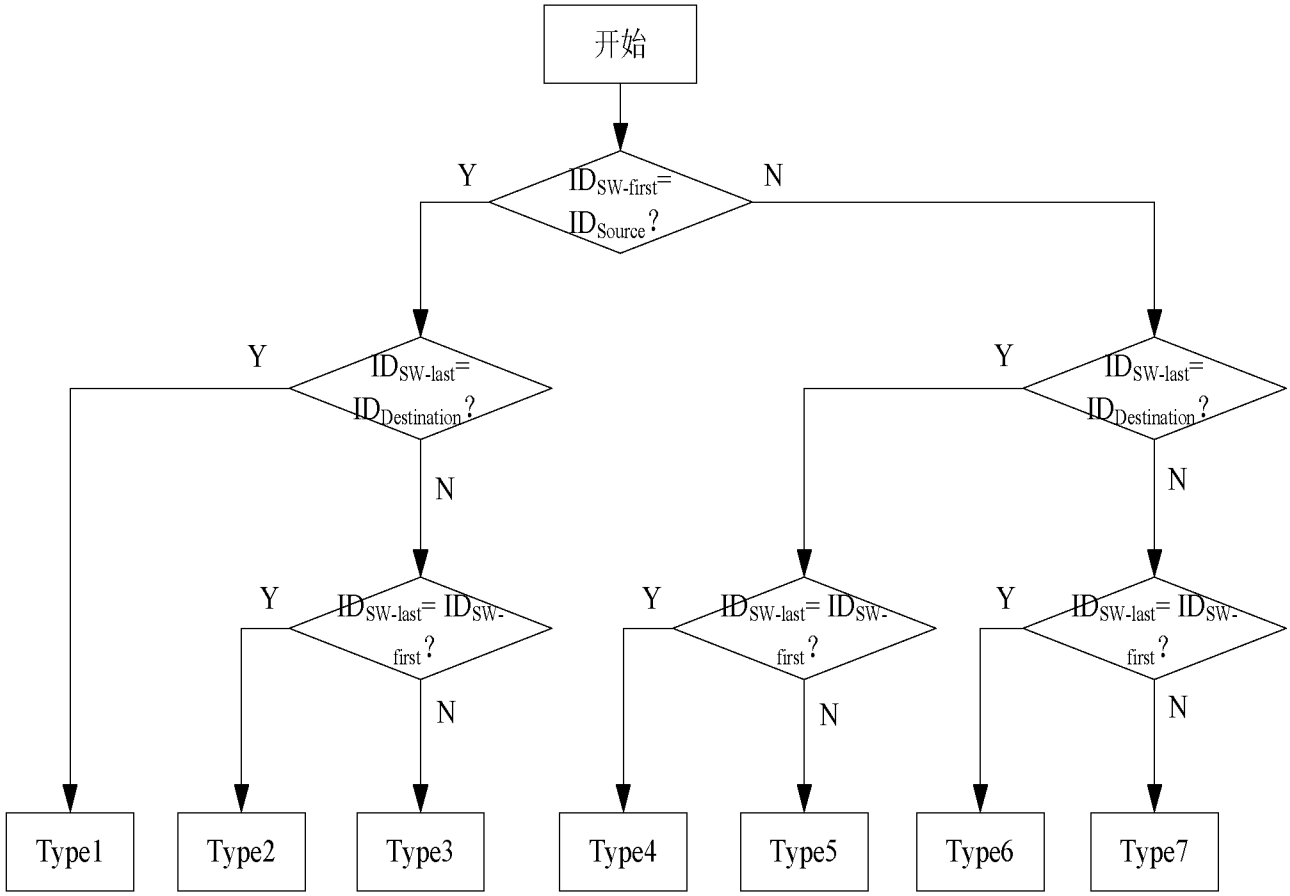
开始
Y
$ID_{SW-first}$= ID_{Source}?
N
Y
$ID_{SW-last}$= $ID_{Destination}$?
Y
$ID_{SW-last}$= $ID_{Destination}$?
N
N
Y
$ID_{SW-last}$= $ID_{SW-first}$?
Y
$ID_{SW-last}$= $ID_{SW-first}$?
Y
$ID_{SW-last}$= $ID_{SW-first}$?
N
N
N
Type1
Type2
Type3
Type4
Type5
Type6
Type7

图5

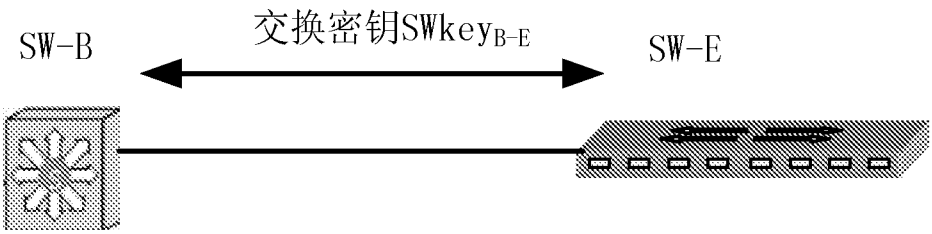
SW-B
交换密钥$SWkey_{B-E}$
SW-E

图6-a

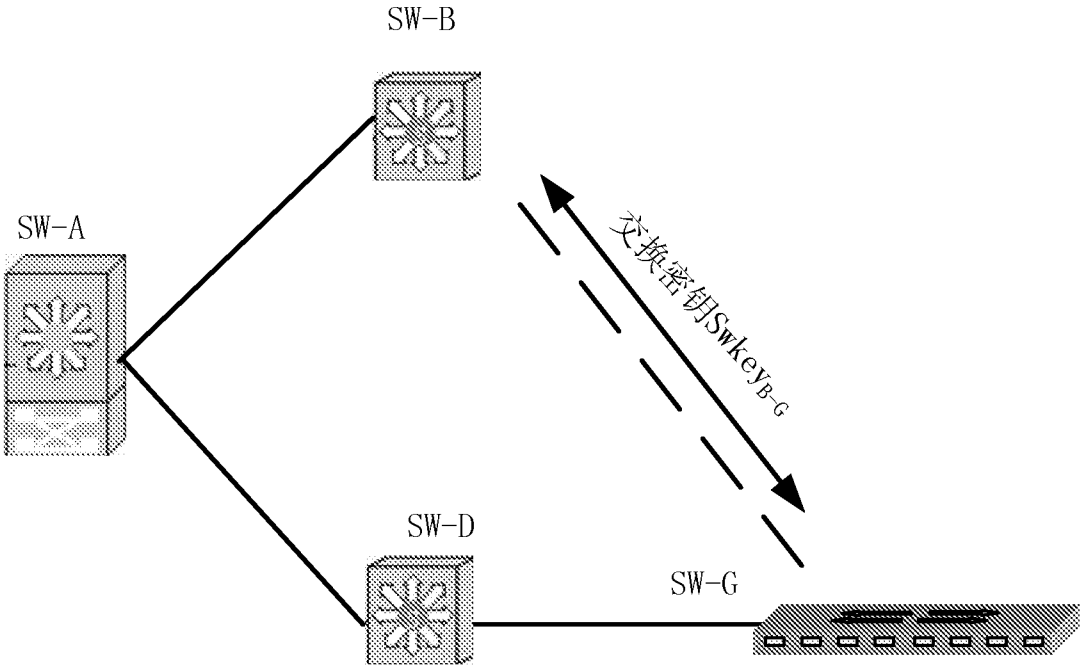

图6-b

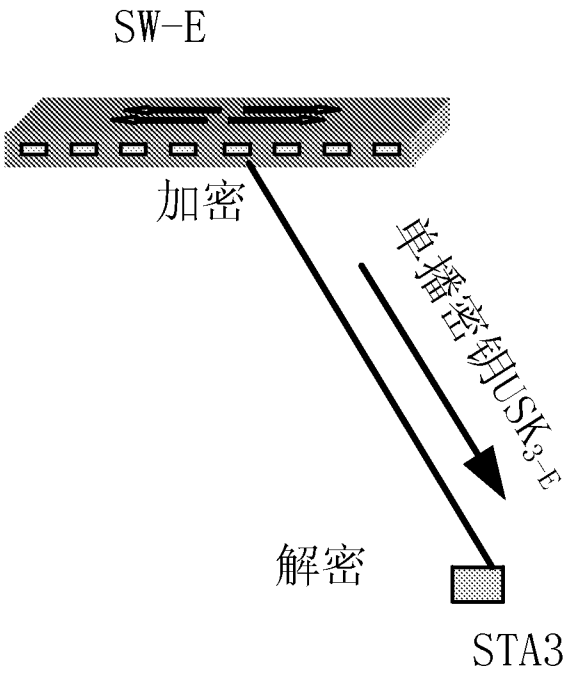

图7

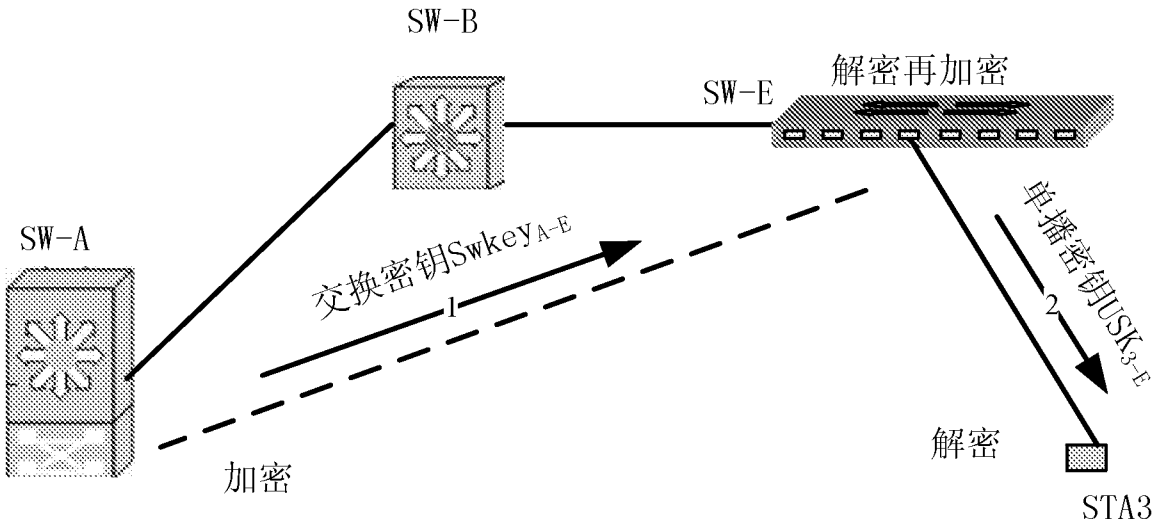
SW-B
解密再加密
SW-E
SW-A
交换密钥Swkey A-E
1
单播密钥USK 3-E
2
加密
解密
STA3

图8

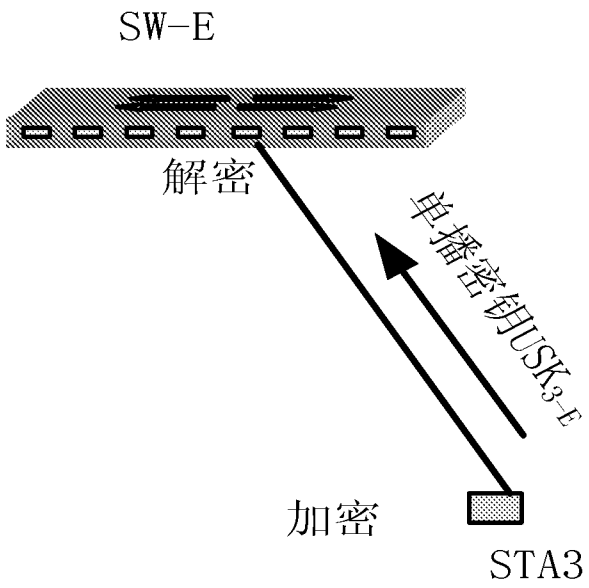
SW-E
解密
单播密钥USK 3-E
加密
STA3

图9

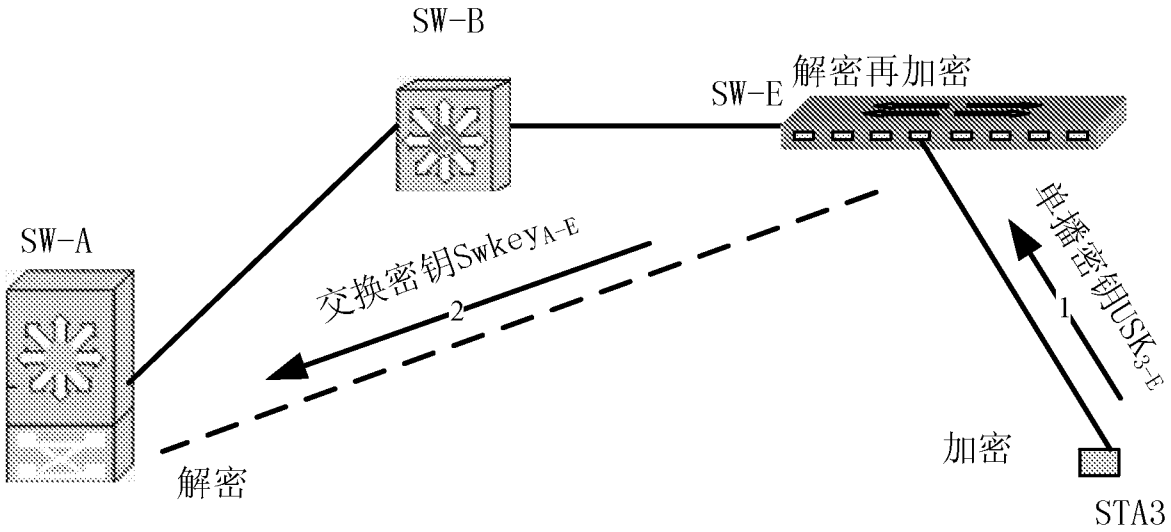
SW-B
SW-E
解密再加密
SW-A
交换密钥SwkeyA-E
2
单播密钥USK3-E
1
加密
解密
STA3

图10

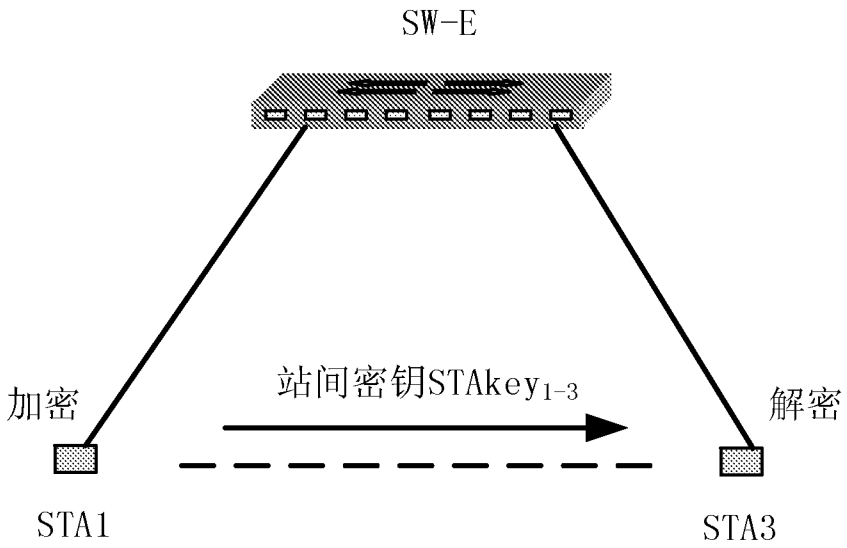
SW-E
加密
站间密钥STAkey1-3
解密
STA1
STA3

图11-a

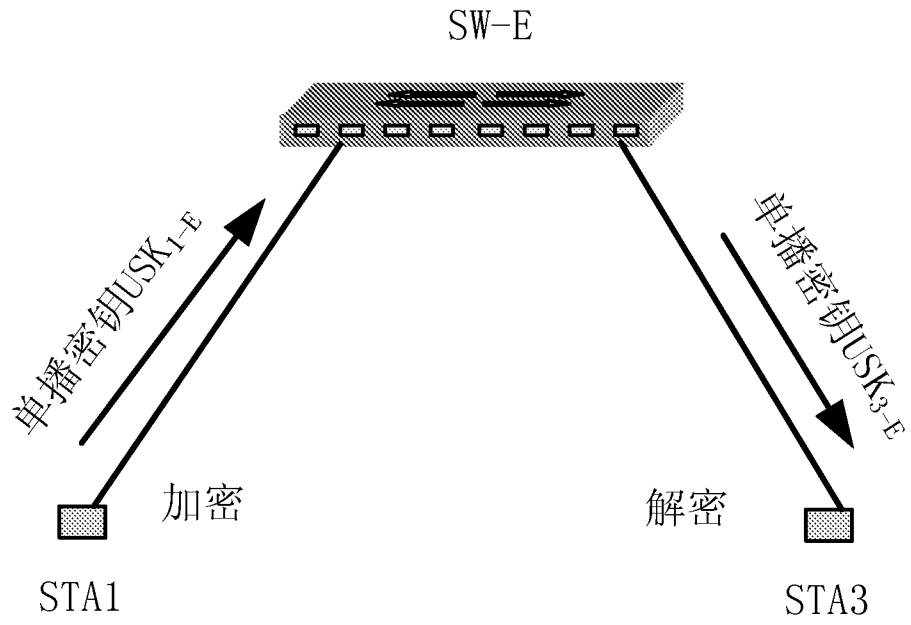
解密再加密再转发
SW-E
单播密钥USK1-E
单播密钥USK3-E
加密
解密
STA1
STA3

图11-b

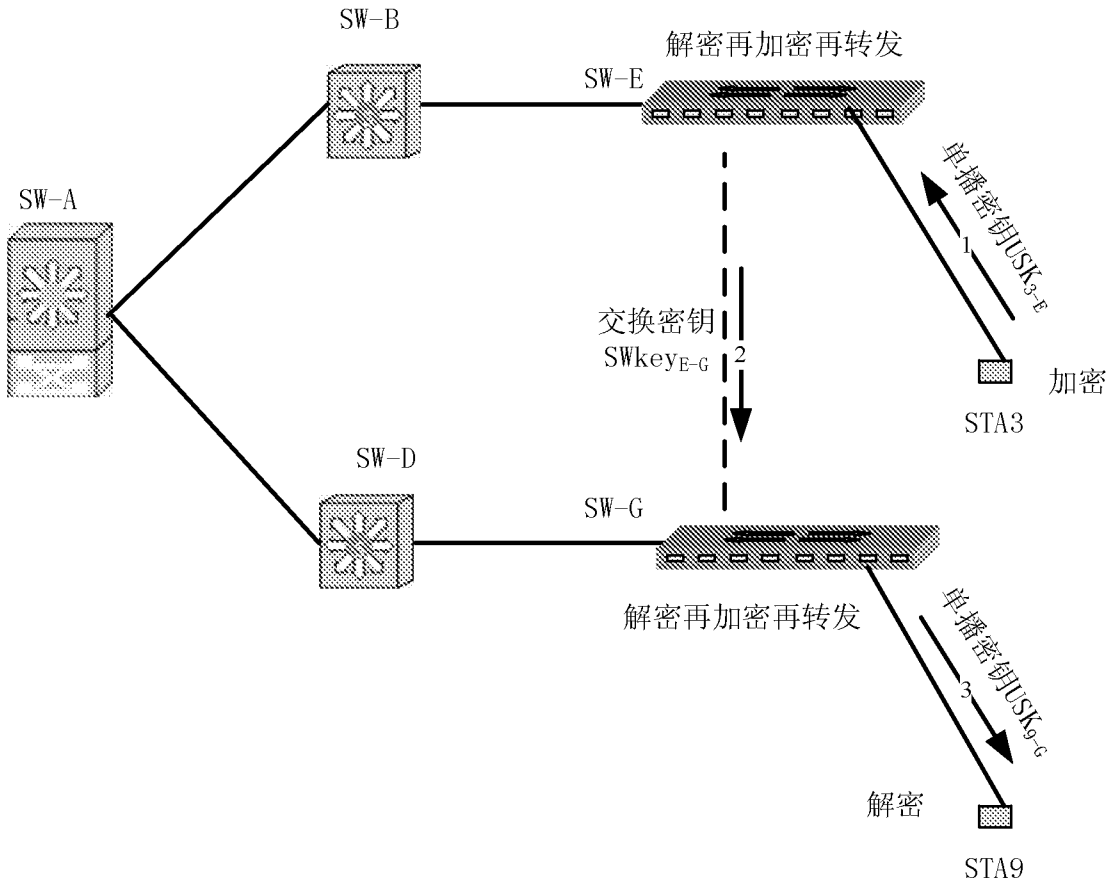
SW-B
解密再加密再转发
SW-E
SW-A
单播密钥USK3-E
1
交换密钥
SWkeyE-G
2
加密
STA3
SW-D
SW-G
解密再加密再转发
单播密钥USK9-G
3
解密
STA9

图12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2010/073454

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08 (2006.01) 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)

IPC: H04L9/08

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, CNKI, WPI, EPODOC: node, type, communicat+, key, share, sharing, switch+, rout+, four, element

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN101594271A (HUAWEI TECHNOLOGY CO LTD. ET AL.) 02 Dec. 2009(02.12.2009) see the claims 1-14; the description, pages 3-13; figures 1-6	1-2
A	See the same as above	3-15
Y	CN101155024A (UNIV HUNAN) 02 Apr. 2008(02.04.2008) see the claims 1-4	1-2
A	See the same as above	3-15
X	CN101068206A (BROADCOM CORP) 07 Nov. 2007(07.11.2007) see the claims 1-10; the description, pages 6-20; figures 1-11	14-15
A	See the same as above	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 Aug. 2010(06.08.2010)	**30 Sep. 2010 (30.09.2010)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer LI Jing Telephone No. (86-10)62411264

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/073454

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101594271A	02.12.2009	None	
CN101155024A	02.04.2008	None	
CN101068206A	07.11.2007	EP1853021A1	07.11.2007
		US2007258437A1	08.11.2007
		US2007258449A1	08.11.2007
		US2007258450A1	08.11.2007
		US2007258468A1	08.11.2007
		US2007258469A1	08.11.2007
		US2007260552A1	08.11.2007
		US2008019352A1	24.01.2008
		CN101068204A	07.11.2007
		CN101068205A	07.11.2007
		CN101068207A	07.11.2007
		CN101068253A	07.11.2007
		CN101115003A	30.01.2008
		CN101123583A	13.02.2008
		TW200814640A	16.03.2008
		TW200814674A	16.03.2008
		TW200814675A	16.03.2008
		TW200814676A	16.03.2008
		TW200812318A	01.03.2008
		TW200812319A	01.03.2008
		TW200816712A	01.04.2008
		TW200820680A	01.05.2008
		US7596137B2	29.09.2009
		US2010008360A1	14.01.2010

国际检索报告

国际申请号
PCT/CN2010/073454

A. 主题的分类

H04L9/08 (2006.01) 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)

IPC: H04L9/08

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, CNKI, WPI, EPODOC: 节点，类型，通信，密钥，共享，交换，路由，保密，四元组，node, type, communicat+ key, share, sharing, switch+, rout+, four, element

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
Y	CN101594271A（华为技术有限公司等）02.12 月 2009(02.12.2009) 参见权利要求书 1－14，说明书第 3－13 页，图 1－6	1-2
A	同上	3-15
Y	CN101155024A（湖南大学）02.4 月 2008(02.04.2008) 参见权利要求 1-4	1-2
A	同上	3-15
X	CN101068206A（美国博通公司）07.11 月 2007(07.11.2007) 参见权利要求 1-10；说明书第 6－20 页；图 1－11	14-15
A	同上	1-13

☐ 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	国际检索报告邮寄日期
06.8 月 2010(06.08.2010)	**30.9 月 2010 (30.09.2010)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 李菁 电话号码：(86-10) **62411264**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2010/073454

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101594271A	02.12.2009	无	
CN101155024A	02.04.2008	无	
CN101068206A	07.11.2007	EP1853021A1	07.11.2007
		US2007258437A1	08.11.2007
		US2007258449A1	08.11.2007
		US2007258450A1	08.11.2007
		US2007258468A1	08.11.2007
		US2007258469A1	08.11.2007
		US2007260552A1	08.11.2007
		US2008019352A1	24.01.2008
		CN101068204A	07.11.2007
		CN101068205A	07.11.2007
		CN101068207A	07.11.2007
		CN101068253A	07.11.2007
		CN101115003A	30.01.2008
		CN101123583A	13.02.2008
		TW200814640A	16.03.2008
		TW200814674A	16.03.2008
		TW200814675A	16.03.2008
		TW200814676A	16.03.2008
		TW200812318A	01.03.2008
		TW200812319A	01.03.2008
		TW200816712A	01.04.2008
		TW200820680A	01.05.2008
		US7596137B2	29.09.2009
		US2010008360A1	14.01.2010