(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 101902324 B
(45)授权公告日 2012.11.07

(21)申请号 201010159675.2

(22)申请日 2010.04.29

(73)专利权人 天维讯达无线电设备检测(北京)有限责任公司
地址 100037 北京市西城区北礼士路 80 号
专利权人 西安西电捷通无线网络通信股份有限公司

(72)发明人 朱林 铁满霞 李琴 葛莉 曹军 张莎 李剑雄 苑克龙

(74)专利代理机构 西安智邦专利商标代理有限公司 61211
代理人 商宇科

(51)Int.Cl.
H04L 9/14(2006.01)
H04L 12/56(2006.01)
H04L 12/28(2006.01)

(56)对比文件
CN 101183934 A,2008.05.21, 全文.
CN 101227272 A,2008.07.23, 全文.
CN 1937558 A,2007.03.28, 说明书第 14 页第 2-5 段,附图 6.

审查员 王瑞

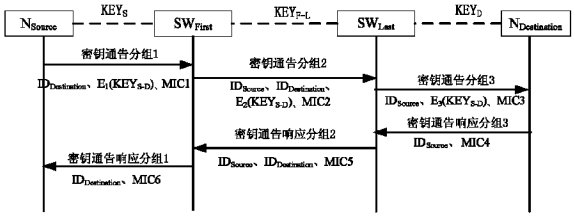
权利要求书 4 页 说明书 8 页 附图 1 页

(54)发明名称

一种节点间通信密钥的建立方法及系统

(57)摘要

本发明为一种节点间通信密钥的建立方法,该方法包括以下步骤:1)发送源节点 N_{Source} 发送第一密钥通告分组给交换设备 SW_{First};2)交换设备 SW_{First} 发送第二密钥通告分组给交换设备 SW_{Last};3)交换设备 SW_{Last} 发送第三密钥通告分组给目的节点 $N_{Destination}$;4)目的节点 $N_{Destination}$ 发送第三密钥通告响应分组给交换设备 SW_{Last};5)交换设备 SW_{Last} 发送第二密钥通告响应分组给交换设备 SW_{First};6)交换设备 SW_{First} 发送第一密钥通告响应分组给发送源节点 N_{Source};7)发送源节点 N_{Source} 接收第一密钥通告响应分组。通过本发明的方法,局域网合法节点之间可以灵活建立及更新它们之间的密钥,无需管理员为全网节点两两之间部署共享的静态密钥。



CN 101902324 B

1. 一种节点间通信密钥的建立方法，其特征在于：所述节点间通信密钥的建立方法包括以下步骤：

1) 发送源节点 N_{Source} 发送第一密钥通告分组给交换设备 SW_{First}；

所述第一密钥通告分组包括 $ID_{Destination}$ 字段、$E_1(KEY_{S-D})$ 字段以及 MIC1 字段；其中：

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

$E_1(KEY_{S-D})$ 字段：表示密钥资料数据，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对 KEY_{S-D} 加密后的数据；其中 KEY_{S-D} 是由发送源节点 N_{Source} 生成的随机数，作为与目的节点 $N_{Destination}$ 之间的通信密钥；

MIC1 字段：表示消息完整性验证码，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对第一密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

2) 交换设备 SW_{First} 发送第二密钥通告分组给交换设备 SW_{Last}；

所述第二密钥通告分组包括 ID_{Source} 字段、$ID_{Destination}$ 字段、$E_2(KEY_{S-D})$ 字段以及 MIC2 字段；

其中：

ID_{Source} 字段：表示发送源节点 N_{Source} 的标识；

$ID_{Destination}$ 字段：值同第一密钥通告分组中 $ID_{Destination}$ 字段值；

$E_2(KEY_{S-D})$ 字段：表示密钥资料数据，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

MIC2 字段：表示消息完整性验证码，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对第二密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

3) 交换设备 SW_{Last} 发送第三密钥通告分组给目的节点 $N_{Destination}$；

所述第三密钥通告分组包括 ID_{Source} 字段、$E_3(KEY_{S-D})$ 字段以及 MIC3 字段；其中：

ID_{Source} 字段：值同第二密钥通告分组中 ID_{Source} 字段值；

$E_3(KEY_{S-D})$ 字段：表示密钥资料数据，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

MIC3 字段：表示消息完整性验证码，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对第三密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

4) 目的节点 $N_{Destination}$ 发送第三密钥通告响应分组给交换设备 SW_{Last}；

所述第三密钥通告响应分组包括 ID_{Source} 字段以及 MIC4 字段；其中：

ID_{Source} 字段：值同第三密钥通告分组中 ID_{Source} 字段值；

MIC4 字段：表示消息完整性验证码，由目的节点 $N_{Destination}$ 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 对第三密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

5) 交换设备 SW_{Last} 发送第二密钥通告响应分组给交换设备 SW_{First}；

所述第二密钥通告响应分组包括 ID_{Source} 字段、$ID_{Destination}$ 字段以及 MIC5 字段，其中：

ID_{Source} 字段：值同第三密钥通告响应分组中 ID_{Source} 字段值；

$ID_{Destination}$ 字段：值同第二密钥通告分组中 $ID_{Destination}$ 字段值；

MIC5 字段：表示消息完整性验证码，由交换设备 SW_{Last} 利用与交换设备 SW_{First} 之间的

密钥 KEY_{F-L} 对第二密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

6) 交换设备 SW_{First} 发送第一密钥通告响应分组给发送源节点 N_{Source}；

所述第一密钥通告响应分组包括 $ID_{Destination}$ 字段以及 MIC6 字段，其中：

$ID_{Destination}$ 字段：值同第二密钥通告响应分组中 $ID_{Destination}$ 字段值；

MIC6 字段：表示消息完整性验证码，由交换设备 SW_{First} 用其与发送源节点 N_{Source} 之间的密钥 KEY_S 对第一密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

7) 发送源节点 N_{Source} 接收第一密钥通告响应分组。

2. 根据权利要求 1 所述的节点间通信密钥的建立方法，其特征在于：所述步骤 2) 中交换设备 SW_{First} 收到第一密钥通告分组后发送第二密钥通告分组给交换设备 SW_{Last}，其具体实现方式是：

2.1) 利用其与发送源节点 N_{Source} 之间的密钥 KEY_S 验证 MIC1 是否正确，若不正确，则丢弃第一密钥通告分组；否则，执行 2.2)；

2.2) 利用其与发送源节点 N_{Source} 之间的密钥 KEY_S 解密 $E_1(KEY_{S-D})$ 字段，得到节点间通信密钥 KEY_{S-D}；

2.3) 构造第二密钥通告分组发送给交换设备 SW_{Last}。

3. 根据权利要求 2 所述的节点间通信密钥的建立方法，其特征在于：所述步骤 3) 中交换设备 SW_{Last} 收到第二密钥通告分组后发送第三密钥通告分组给目的节点 $N_{Destination}$，其具体实现方式是：

3.1) 利用其与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 验证 MIC2 是否正确，若不正确，则丢弃第二密钥通告分组；否则，执行 3.2)；

3.2) 利用其与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 解密 $E_2(KEY_{S-D})$ 字段，得到节点间通信密钥 KEY_{S-D}；

3.3) 构造第三密钥通告分组发送给目的节点 $N_{Destination}$。

4. 根据权利要求 3 所述的节点间通信密钥的建立方法，其特征在于：所述步骤 4) 中目的节点 $N_{Destination}$ 收到第三密钥通告分组后发送第三密钥通告响应分组给交换设备 SW_{Last}，其具体实现方式是：

4.1) 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 验证 MIC3 是否正确，若不正确，则丢弃第三密钥通告分组；否则，执行 4.2)；

4.2) 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 解密 $E_3(KEY_{S-D})$ 字段，得到节点间通信密钥 KEY_{S-D}，该 KEY_{S-D} 即为目的节点 $N_{Destination}$ 与发送源节点 N_{Source} 之间的通信密钥；

4.3) 构造第三密钥通告响应分组发送给交换设备 SW_{Last}。

5. 根据权利要求 4 所述的节点间通信密钥的建立方法，其特征在于：所述步骤 5) 中交换设备 SW_{Last} 收到第三密钥通告响应分组后发送第二密钥通告响应分组给交换设备 SW_{First}，其具体实现方式是：

5.1) 比较第三密钥通告响应分组中 ID_{Source} 字段与之前发送的第三密钥通告分组中 ID_{Source} 字段值是否一致，若不一致，则丢弃第三密钥通告响应分组；否则，执行 5.2)；

5.2) 利用与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 验证 MIC3 是否正确，若不正确，则丢弃

第三密钥通告响应分组；否则，执行 5.3）；

5.3）构造第二密钥通告响应分组发送给交换设备 SW_{First}。

6. 根据权利要求 5 所述的节点间通信密钥的建立方法，其特征在于：所述步骤 6）中交换设备 SW_{First} 收到第二密钥通告响应分组后发送第一密钥通告响应分组给发送源节点 N_{Source}，其具体实现方式是：

6.1）检查第二密钥通告响应分组中的 ID_{Source} 字段、$ID_{Destination}$ 字段与之前发送给交换设备 SW_{Last} 的第二密钥通告分组中对应字段值是否一致，若不一致，则丢弃第二密钥通告响应分组；否则，执行 6.2）；

6.2）利用与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 验证 MIC5 是否正确，若不正确，则丢弃第二密钥通告响应分组；否则，执行 6.3）；

6.3）构造第一密钥通告响应分组发送给发送源节点 N_{Source}。

7. 根据权利要求 6 所述的节点间通信密钥的建立方法，其特征在于：所述步骤 7）的具体实现方式是：

7.1）检查第二密钥通告响应分组中的 $ID_{Destination}$ 字段与之前发送给交换设备 SWF_{irst} 的第一密钥通告分组中 $ID_{Destination}$ 字段值是否一致，若不一致，则丢弃第一密钥通告响应分组；否则，执行 7.2）；

7.2）利用与交换设备 SW_{First} 之间的密钥 KEY_S 验证 MIC6 是否正确，若不正确，则丢弃第一密钥通告响应分组；否则，即完成发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间通信密钥 KEY_{S-D} 的建立过程，此后发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间可采用该通信密钥 KEY_{S-D} 进行秘密通信。

8. 一种节点间通信密钥的建立系统，其特征在于：所述节点间通信密钥的建立系统包括向交换设备 SW_{First} 发送第一密钥通告分组、接收交换设备 SW_{First} 发送的第一密钥通告响应分组的发送源节点 N_{Source}；接收发送源节点 N_{Source} 发送的第一密钥通告分组、向交换设备 SW_{Last} 发送第二密钥通告分组、接收交换设备 SW_{Last} 发送的第二密钥通告响应分组、向发送源节点 N_{Source} 发送第一密钥通告响应分组的交换设备 SW_{First}；接收交换设备 SW_{First} 发送的第二密钥通告分组、向目的节点 $N_{Destination}$ 发送第三密钥通告分组、接收目的节点 $N_{Destination}$ 发送的第三密钥通告响应分组、向交换设备 SW_{First} 发送第二密钥通告响应分组的交换设备 SW_{Last}；接收交换设备 SW_{Last} 发送的第三密钥通告分组、向交换设备 SW_{Last} 发送第三密钥通告响应分组的目的节点 $N_{Destination}$；

所述第一密钥通告分组包括 $ID_{Destination}$ 字段、$E_1(KEY_{S-D})$ 字段以及 MIC1 字段；其中：

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

$E_1(KEY_{S-D})$ 字段：表示密钥资料数据，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对 KEY_{S-D} 加密后的数据；其中 KEY_{S-D} 是由发送源节点 N_{Source} 生成的随机数，作为与目的节点 $N_{Destination}$ 之间的通信密钥；

MIC1 字段：表示消息完整性验证码，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对第一密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

所述第二密钥通告分组包括 ID_{Source} 字段、$ID_{Destination}$ 字段、$E_2(KEY_{S-D})$ 字段以及 MIC2 字段；

其中：

ID_{Source} 字段：表示发送源节点 N_{Source} 的标识；

$E_2(KEY_{S-D})$ 字段：表示密钥资料数据，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

MIC2 字段：表示消息完整性验证码，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对第二密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

$ID_{Destination}$ 字段：值同第一密钥通告分组中 $ID_{Destination}$ 字段值；

所述第三密钥通告分组包括 ID_{Source} 字段、$E_3(KEY_{S-D})$ 字段以及 MIC3 字段；其中：

$E_3(KEY_{S-D})$ 字段：表示密钥资料数据，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

MIC3 字段：表示消息完整性验证码，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对第三密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

ID_{Source} 字段：值同第三密钥通告分组中 ID_{Source} 字段值；

所述第三密钥通告响应分组包括 ID_{Source} 字段以及 MIC4 字段；其中：

MIC4 字段：表示消息完整性验证码，由目的节点 $N_{Destination}$ 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 对第三密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

ID_{Source} 字段：值同第三密钥通告分组中 ID_{Source} 字段值；

所述第二密钥通告响应分组包括 ID_{Source} 字段、$ID_{Destination}$ 字段以及 MIC5 字段，其中：

MIC5 字段：表示消息完整性验证码，由交换设备 SW_{Last} 利用与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 对第二密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

ID_{Source} 字段：值同第三密钥通告响应分组中 ID_{Source} 字段值；

$ID_{Destination}$ 字段：值同第二密钥通告分组中 $ID_{Destination}$ 字段值；

所述第一密钥通告响应分组包括 $ID_{Destination}$ 字段以及 MIC6 字段，其中：

MIC6 字段：表示消息完整性验证码，由交换设备 SW_{First} 用其与发送源节点 N_{Source} 之间的密钥 KEY_S 对第一密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值；

$ID_{Destination}$ 字段：值同第二密钥通告响应分组中 $ID_{Destination}$ 字段值。

一种节点间通信密钥的建立方法及系统

技术领域

[0001] 本发明涉及通信网络应用领域，尤其涉及一种节点间通信密钥的建立方法及系统。

背景技术

[0002] 有线局域网一般为广播型网络，一个节点发出的数据，其它节点都能收到。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ISO/IEC 8802-3)定义的局域网LAN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。

[0003] 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。

[0004] 有线局域网的拓扑结构比较复杂，涉及到的节点数目也比较多，因此网络中的数据通信比较复杂，终端和交换设备被统称为节点。如果为局域网节点间分配静态密钥来保证节点间的保密通信，其分配和更新过程极为复杂。

发明内容

[0005] 为了解决背景技术中存在的上述问题，本发明提供了一种节点间通信密钥的建立方法及系统。

[0006] 本发明的技术解决方案是：本发明为一种节点间通信密钥的建立方法，其特殊之处在于：所述方法包括以下步骤：

[0007] 1) 发送源节点 N_{Source} 发送第一密钥通告分组给交换设备 SW_{First}；

[0008] 2) 交换设备 SW_{First} 发送第二密钥通告分组给交换设备 SW_{Last}；

[0009] 3) 交换设备 SW_{Last} 发送第三密钥通告分组给目的节点 $N_{Destination}$；

[0010] 4) 目的节点 $N_{Destination}$ 发送第三密钥通告响应分组给交换设备 SW_{Last}；

[0011] 5) 交换设备 SW_{Last} 发送第二密钥通告响应分组给交换设备 SW_{First}；

[0012] 6) 交换设备 SW_{First} 发送第一密钥通告响应分组给发送源节点 N_{Source}；

[0013] 7) 发送源节点 N_{Source} 接收第一密钥通告响应分组。

[0014] 上述步骤1)中第一密钥通告分组包括 $ID_{Destination}$ 字段、$E_1(KEY_{S-D})$ 字段以及MIC1字段；其中：

[0015] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识；

[0016] $E_1(KEY_{S-D})$ 字段：表示密钥资料数据，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对 KEY_{S-D} 加密后的数据；其中 KEY_{S-D} 是由发送源节点 N_{Source} 生成的随机数，

作为与目的节点 $N_{Destination}$ 之间的通信密钥；

[0017] MIC1 字段：表示消息完整性验证码，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对第一密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0018] 上述步骤 2）中交换设备 SW_{First} 收到第一密钥通告分组后发送第二密钥通告分组给交换设备 SW_{Last}，其具体实现方式是：

[0019] 2.1）利用其与发送源节点 N_{Source} 之间的密钥 KEY_S 验证 MIC1 是否正确，若不正确，则丢弃该分组；否则，执行 2.2）；

[0020] 2.2）利用其与发送源节点 N_{Source} 之间的密钥 KEY_S 解密 $E_1(KEY_{S-D})$ 字段，得到节点间通信密钥 KEY_{S-D}；

[0021] 2.3）构造第二密钥通告分组发送给交换设备 SW_{Last}，所述第二密钥通告分组包括：ID_{Source} 字段、$ID_{Destination}$ 字段、$E_2(KEY_{S-D})$ 字段以及 MIC2 字段；

[0022] 其中：

[0023] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识；

[0024] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识，其值同收到的密钥通告分组 1 中的 $ID_{Destination}$ 字段的值；

[0025] $E_2(KEY_{S-D})$ 字段：表示密钥资料数据，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

[0026] MIC2 字段：表示消息完整性验证码，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对第二密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0027] 上述步骤 3）中交换设备 SW_{Last} 收到第二密钥通告分组后发送第三密钥通告分组给目的节点 $N_{Destination}$，其具体实现方式是：

[0028] 3.1）利用其与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 验证 MIC2 是否正确，若不正确，则丢弃该分组；否则，执行 3.2）；

[0029] 3.2）利用其与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 解密 $E_2(KEY_{S-D})$ 字段，得到节点间通信密钥 KEY_{S-D}；

[0030] 3.3）构造第三密钥通告分组发送给目的节点 $N_{Destination}$，所述第三密钥通告分组包括：ID_{Source} 字段、$E_3(KEY_{S-D})$ 字段以及 MIC3 字段；其中：

[0031] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识，其值同收到的第二密钥通告分组中的 ID_{Source} 字段的值；

[0032] $E_3(KEY_{S-D})$ 字段：表示密钥资料数据，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

[0033] MIC3 字段：表示消息完整性验证码，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对第三密钥通告分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0034] 上述步骤 4）中目的节点 $N_{Destination}$ 收到第三密钥通告分组后发送第三密钥通告响应分组给交换设备 SW_{Last}，其具体实现方式是：

[0035] 4.1）利用与交换设备 SW_{Last} 之间的密钥 KEY_D 验证 MIC3 是否正确，若不正确，则丢

弃该分组；否则，执行 4.2）；

[0036] 4.2）利用与交换设备 SW_{Last} 之间的密钥 KEY_D 解密 $E_3(KEY_{S-D})$ 字段，得到节点间通信密钥 KEY_{S-D}，该 KEY_{S-D} 即为目的节点 $N_{Destination}$ 与发送源节点 N_{Source} 之间的通信密钥；

[0037] 4.3）构造第三密钥通告响应分组发送给交换设备 SW_{Last}，所述第三密钥通告响应分组包括：ID_{Source} 字段以及 MIC4 字段；其中：

[0038] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识，其值同收到的第三密钥通告分组中的 ID_{Source} 字段的值；

[0039] MIC4 字段：表示消息完整性验证码，由目的节点 $N_{Destination}$ 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 对第三密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0040] 上述步骤 5）中交换设备 SW_{Last} 收到第三密钥通告响应分组后发送第二密钥通告响应分组给交换设备 SW_{First}，其具体实现方式是：

[0041] 5.1）比较 ID_{Source} 字段与之前发送的第三密钥通告分组中 ID_{Source} 字段值是否一致，若不一致，则丢弃该分组；否则，执行 5.2）；

[0042] 5.2）利用与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 验证 MIC3 是否正确，若不正确，则丢弃该分组；否则，执行 5.3）；

[0043] 5.3）构造第二密钥通告响应分组发送给交换设备 SW_{First}，所述第二密钥通告响应分组包括：ID_{Source} 字段、$ID_{Destination}$ 字段以及 MIC5 字段，其中：

[0044] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识，其值同收到的第二密钥通告分组中的 ID_{Source} 字段的值；

[0045] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识，其值同收到的第二密钥通告分组中的 $ID_{Destination}$ 字段的值；

[0046] MIC5 字段：表示消息完整性验证码，由交换设备 SW_{Last} 利用与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 对第二密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0047] 上述步骤 6）中交换设备 SW_{First} 收到第二密钥通告响应分组后发送第一密钥通告响应分组给发送源节点 N_{Source}，其具体实现方式是：

[0048] 6.1）检查分组中的 ID_{Source} 字段、$ID_{Destination}$ 字段与之前发送给交换设备 SW_{Last} 的第二密钥通告分组中对应字段值是否一致，若不一致，则丢弃该分组；否则，执行 6.2）；

[0049] 6.2）利用与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 验正 MIC5 是否正确，若不正确，则丢弃该分组；否则，执行 6.3）；

[0050] 6.3）构造第一密钥通告响应分组发送给发送源节点 N_{Source}，所述第一密钥通告响应分组包括：$ID_{Destination}$ 字段以及 MIC6 字段，其中：

[0051] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识，其值同收到的第一密钥通告分组中的 $ID_{Destination}$ 字段的值；

[0052] MIC6 字段：表示消息完整性验证码，由交换设备 SW_{First} 用其与发送源节点 N_{Source} 之间的密钥 KEY_S 对第一密钥通告响应分组中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0053] 上述步骤 7）的具体实现方式是：

[0054] 7.1) 检查分组中的 $ID_{Destination}$ 字段与之前发送给交换设备 SW_{First} 的第一密钥通告分组中 $ID_{Destination}$ 字段值是否一致，若不一致，则丢弃该分组；否则，执行 7.2)；

[0055] 7.2) 利用与交换设备 SW_{First} 之间的密钥 KEY_S 验证 MIC6 是否正确，若不正确，则丢弃该分组；否则，即完成发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间通信密钥 KEY_{S-D} 的建立过程，此后发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间可采用该通信密钥 KEY_{S-D} 进行秘密通信。

[0056] 一种节点间通信密钥的建立系统，其特殊之处在于：所述节点间通信密钥的建立系统包括向交换设备 SW_{First} 发送第一密钥通告分组、接收交换设备 SW_{First} 发送的第一密钥通告响应分组的发送源节点 N_{Source}；接收发送源节点 N_{Source} 发送的第一密钥通告分组、向交换设备 SW_{Last} 发送第二密钥通告分组、接收交换设备 SW_{Last} 发送的第二密钥通告响应分组、向发送源节点 N_{Source} 发送第一密钥通告响应分组的交换设备 SW_{First}；接收交换设备 SW_{First} 发送的第二密钥通告分组、向目的节点 $N_{Destination}$ 发送第三密钥通告分组、接收目的节点 $N_{Destination}$ 发送的第三密钥通告响应分组、向交换设备 SW_{First} 发送第二密钥通告响应分组的交换设备 SW_{Last}；接收交换设备 SW_{Last} 发送的第三密钥通告分组、向交换设备 SW_{Last} 发送第三密钥通告响应分组的目的节点 $N_{Destination}$。

[0057] 本发明的优点是：发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间的通信密钥是通过发送源节点 N_{Source} 临时生成，并通过已建立的安全连接通道逐步通告给目的节点 $N_{Destination}$ 的。节点间共享密钥的建立和更新过程可由发送源节点 N_{Source} 发起该过程触发。通过该方法，局域网合法节点之间可以灵活建立及更新它们之间的密钥，无需管理员为全网节点两两之间部署共享的静态密钥。

附图说明

[0058] 图 1 为本发明所提供的节点间通信密钥建立过程示意图。

具体实施方式

[0059] 本发明中定义的节点 N(Node) 是指局域网中的用户终端 STA(STAtion) 和交换设备 SW(SWitch)。局域网中的集线器等物理层设备不作为节点处理。

[0060] 假设，在网络中相邻的交换设备与用户终端之间通过预分发或其他安全机制均已建立安全连接，即已具有共享的密钥；所有的交换设备两两之间通过预分发或其他安全机制已建立安全连接，即已具有共享的密钥。

[0061] 以发送源节点 N_{Source} 与目的节点 $N_{Destination}$ 之间通信密钥的建立为例进行说明，交换设备 SW_{First} 是指从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的第一个交换设备，交换设备 SW_{Last} 是指从发送源节点 N_{Source} 到目的节点 $N_{Destination}$ 的数据包经过的最后一个交换设备。

[0062] 根据上述的假设，发送源节点 N_{Source} 与交换设备 SW_{First} 已建立安全连接，共享的密钥记为 KEY_S，目的节点 $N_{Destination}$ 与交换设备 SW_{Last} 已建立安全连接，共享的密钥记为 KEY_D，交换设备 SW_{First} 与交换设备 SW_{Last} 已建立安全连接，共享的密钥记为 KEY_{F-L}。

[0063] 参见图 1，本发明所提供的一种节点间通信密钥的建立方法为发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间通信密钥的建立具体方案如下：

[0064] 1) 发送源节点 N_{Source} 发送密钥通告分组 1 给交换设备 SW_{First} ；

[0065] 该密钥通告分组 1 包括：

[0066]

$ID_{Destination}$	$E_1(KEY_{S-D})$	MIC1

[0067] 其中：

[0068] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识；

[0069] $E_1(KEY_{S-D})$ 字段：表示密钥资料数据，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对 KEY_{S-D} 加密后的数据；其中 KEY_{S-D} 是由发送源节点 N_{Source} 生成的随机数，作为与目的节点 $N_{Destination}$ 之间的通信密钥；

[0070] MIC1 字段：表示消息完整性验证码，由发送源节点 N_{Source} 利用其与交换设备 SW_{First} 之间的密钥 KEY_S 对该密钥通告分组 1 中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0071] 2) 交换设备 SW_{First} 发送密钥通告分组 2 给交换设备 SW_{Last} ；

[0072] 交换设备 SW_{First} 收到密钥通告分组 1 后，进行如下处理：

[0073] 2.1) 利用其与发送源节点 N_{Source} 之间的密钥 KEY_S 验证 MIC1 是否正确，若不正确，则丢弃该分组；否则，执行 2.2)；

[0074] 2.2) 利用其与发送源节点 N_{Source} 之间的密钥 KEY_S 解密 $E_1(KEY_{S-D})$ 字段，即可得到节点间通信密钥 KEY_{S-D} ；

[0075] 2.3) 构造密钥通告分组 2 发送给交换设备 SW_{Last}。

[0076] 该密钥通告分组 2 包括：

[0077]

ID_{Source}	$ID_{Destination}$	$E_2(KEY_{S-D})$	MIC2

[0078] 其中：

[0079] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识；

[0080] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识，其值同收到的密钥通告分组 1 中的 $ID_{Destination}$ 字段的值；

[0081] $E_2(KEY_{S-D})$：表示密钥资料数据，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

[0082] MIC2 字段：表示消息完整性验证码，由交换设备 SW_{First} 利用其与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 对该密钥通告分组 2 中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0083] 3) 交换设备 SW_{Last} 发送密钥通告分组 3 给目的节点 $N_{Destination}$ ；

[0084] 交换设备 SW_{Last} 收到密钥通告分组 2 后，进行如下处理：

[0085] 3.1) 利用其与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 验证 MIC2 是否正确，若不正确，则丢弃该分组；否则，执行 3.2)；

[0086] 3.2) 利用其与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 解密 $E_2(KEY_{S-D})$ 字段，即可得到节点间通信密钥 KEY_{S-D} ；

[0087] 3.3) 构造密钥通告分组 3 发送给目的节点 $N_{Destination}$。

[0088] 该密钥通告分组 3 中包括：

[0089]

ID_{Source}	$E_3(KEY_{S-D})$	MIC3

[0090] 其中：

[0091] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识，其值同收到的密钥通告分组 2 中的 ID_{Source} 字段的值；

[0092] $E_3(KEY_{S-D})$ 字段：表示密钥资料数据，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对解密得到的节点间通信密钥 KEY_{S-D} 加密后的数据；

[0093] MIC3 字段：表示消息完整性验证码，由交换设备 SW_{Last} 用其与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 对该密钥通告分组 3 中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0094] 4) 目的节点 $N_{Destination}$ 发送密钥通告响应分组 3 给交换设备 SW_{Last}；

[0095] 目的节点 $N_{Destination}$ 收到密钥通告分组 3 后，进行如下处理：

[0096] 4.1) 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 验证 MIC3 是否正确，若不正确，则丢弃该分组；否则，执行 4.2)；

[0097] 4.2) 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 解密 $E_3(KEY_{S-D})$ 字段，即可得到节点间通信密钥 KEY_{S-D}，该 KEY_{S-D} 即为目的节点 $N_{Destination}$ 与发送源节点 N_{Source} 之间的通信密钥；

[0098] 4.3) 构造密钥通告响应分组 3 发送给交换设备 SW_{Last}。

[0099] 该密钥通告响应分组 3 包括：

[0100]

ID_{Source}	MIC4

[0101] 其中：

[0102] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识，其值同收到的密钥通告分组 3 中的 ID_{Source} 字段的值；

[0103] MIC4 字段：表示消息完整性验证码，由目的节点 $N_{Destination}$ 利用与交换设备 SW_{Last} 之间的密钥 KEY_D 对该密钥通告响应分组 3 中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0104] 5) 交换设备 SW_{Last} 发送密钥通告响应分组 2 给交换设备 SW_{First}；

[0105] 交换设备 SW_{Last} 收到密钥通告响应分组 3 后，进行如下处理：

[0106] 5.1) 比较 ID_{Source} 字段与之前发送的密钥通告分组 3 中 ID_{Source} 字段值是否一致，若不一致，则丢弃该分组；否则，执行 5.2)；

[0107] 5.2) 利用与目的节点 $N_{Destination}$ 之间的密钥 KEY_D 验证 MIC3 是否正确，若不正确，则丢弃该分组；否则，执行 5.3)；

[0108] 5.3) 构造密钥通告响应分组 2 发送给交换设备 SW_{First}。

[0109] 该临时密钥协商响应分组包括：

[0110]

ID_{Source}	$ID_{Destination}$	MIC5

[0111] 其中：

[0112] ID_{Source} 字段：表示发送源节点 N_{Source} 的标识，其值同收到的密钥通告分组 2 中的 ID_{Source} 字段的值；

[0113] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识，其值同收到的密钥通告分组 2 中的 $ID_{Destination}$ 字段的值；

[0114] MIC5 字段：表示消息完整性验证码，由交换设备 SW_{Last} 利用与交换设备 SW_{First} 之间的密钥 KEY_{F-L} 对该密钥通告响应分组 2 中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0115] 6) 交换设备 SW_{First} 发送密钥通告响应分组 1 给发送源节点 N_{Source}；

[0116] 交换设备 SW_{First} 收到密钥通告响应分组 2 后，进行如下处理：

[0117] 6.1) 检查分组中的 ID_{Source} 字段、$ID_{Destination}$ 字段与之前发送给交换设备 SW_{Last} 的密钥通告分组 2 中对应字段值是否一致，若不一致，则丢弃该分组；否则，执行 6.2)；

[0118] 6.2) 利用与交换设备 SW_{Last} 之间的密钥 KEY_{F-L} 验证 MIC5 是否正确，若不正确，则丢弃该分组；否则，执行 6.3)；

[0119] 6.3) 构造密钥通告响应分组 1 发送给发送源节点 N_{Source}。

[0120] 该密钥通告响应分组 1 包括：

[0121]

$ID_{Destination}$	MIC6

[0122] 其中：

[0123] $ID_{Destination}$ 字段：表示目的节点 $N_{Destination}$ 的标识，其值同收到的密钥通告分组 1 中的 $ID_{Destination}$ 字段的值；

[0124] MIC6 字段：表示消息完整性验证码，由交换设备 SW_{Fir}st 用其与发送源节点 N_{Source} 之间的密钥 KEY_S 对密钥通告响应分组 1 中本字段外的其他字段通过杂凑函数计算得到的杂凑值。

[0125] 7) 发送源节点 N_{Source} 接收密钥通告响应分组 1；

[0126] 发送源节点 N_{Source} 收到密钥通告响应分组 1 后，进行如下处理：

[0127] 7.1) 检查分组中的 $ID_{Destination}$ 字段与之前发送给交换设备 SW_{First} 的密钥通告分组 1 中 $ID_{Destination}$ 字段值是否一致，若不一致，则丢弃该分组；否则，执行 7.2)；

[0128] 7.2) 利用与交换设备 SW_{First} 之间的密钥 KEY_S 验证 MIC6 是否正确，若不正确，则丢弃该分组；否则，即完成发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间通信密钥 KEY_{S-D} 的建立过程，此后发送源节点 N_{Source} 和目的节点 $N_{Destination}$ 之间可采用该通信密钥 KEY_{S-D} 进行秘密通信。

[0129] 发送源节点 N_{Source} 需要与目的节点 $N_{Destination}$ 建立通信密钥 KEY_{S-D}，当利用上述方案进行具体实施时，发送源节点 N_{Source} 还可生成一个数值，作为此次通信密钥建立过程的标识，该标识可为时钟、顺序号或随机数，且在每个消息中进行携带，相应地交换设备 SW_{Last} 收到密钥通告响应分组 3 后需验证分组中的标识值与其之前接收的密钥通告分组 2 中的标识值是否一致；交换设备 SW_{First} 收到密钥通告响应分组 2 后需验证分组中的标识值与其之前接收的密钥通告分组 1 中的标识值是否一致；发送源节点 N_{Source} 收到密钥通告响应分组 1 后

需验证分组中的标识值与其之前发送的密钥通告分组 1 中的标识值是否一致。

[0130] 当利用上述方案进行具体实施时，也可以由发送源节点 N_{Source}、交换设备 SW_{First} 及交换设备 SW_{Last} 在发送密钥通告分组 1、密钥通告分组 2 及密钥通告分组 3 时，各自独立生成一个数值作为通告标识分别携带在上述分组中，该通告标识可为时钟、顺序号或随机数，相应地交换设备 SW_{Last}、交换设备 SW_{First} 及发送源节点 N_{Source} 收到密钥通告响应分组 3、密钥通告响应分组 2 及密钥通告响应分组 1 后均需验证分组中的通告标识值与其之前发送的分组中的标识值是否一致。

[0131] 一种节点间通信密钥的建立系统，其特殊之处在于：所述节点间通信密钥的建立系统包括向交换设备 SW_{First} 发送密钥通告分组 1、接收交换设备 SW_{First} 发送的密钥通告响应分组 1 的发送源节点 N_{Source}；接收发送源节点 N_{Source} 发送的密钥通告分组 1、向交换设备 SW_{Last} 发送密钥通告分组 2、接收交换设备 SW_{Last} 发送的密钥通告响应分组 2、向发送源节点 N_{Source} 发送密钥通告响应分组 1 的交换设备 SW_{First}；接收交换设备 SW_{First} 发送的密钥通告分组 2、向目的节点 $N_{Destination}$ 发送密钥通告分组 3、接收目的节点 $N_{Destination}$ 发送的密钥通告响应分组 3、向交换设备 SW_{First} 发送密钥通告响应分组 2 的交换设备 SW_{Last}；接收交换设备 SW_{Last} 发送的密钥通告分组 3、向交换设备 SW_{Last} 发送密钥通告响应分组 3 的目的节点 $N_{Destination}$。

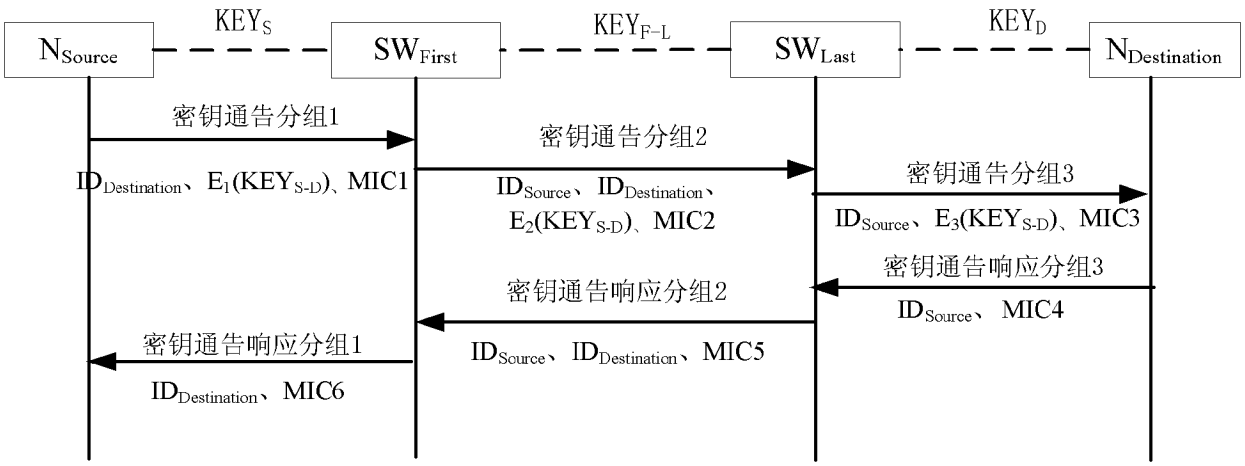

N_{Source}
KEY_S
SW_{First}
KEY_{F-L}
SW_{Last}
KEY_D
$N_{Destination}$
密钥通告分组1
$ID_{Destination}$、$E_1(KEY_{S-D})$、MIC1
密钥通告分组2
ID_{Source}、$ID_{Destination}$、
$E_2(KEY_{S-D})$、MIC2
密钥通告分组3
ID_{Source}、$E_3(KEY_{S-D})$、MIC3
密钥通告响应分组3
ID_{Source}、MIC4
密钥通告响应分组2
ID_{Source}、$ID_{Destination}$、MIC5
密钥通告响应分组1
$ID_{Destination}$、MIC6

图 1