(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
2009 年6 月4 日 (04.06.2009)

PCT

(10) 国际公布号
WO 2009/067933 A1

(51) 国际专利分类号:
H04L 9/00 (2006.01) *H04L 12/28* (2006.01)
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2008/073051

(22) 国际申请日: 2008 年11 月14 日 (14.11.2008)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200710019090.9
2007 年11 月16 日 (16.11.2007) 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)。 **庞辽军 (PANG, Liaojun)** [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)。 **赖晓龙 (LAI, Xiaolong)** [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, 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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title:** KEY MANAGEMENT METHOD

(54) **发明名称:** 一种密钥管理方法

(57) **Abstract:** A key management method, is an enhanced RSNA four-way Handshake protocol. Its preceding two way Handshake processes comprises: 1), an authenticator sending a new message (1) which is added a Key Negotiation IDentifier (KNID) and a Message Integrity Code (MIC) based on the intrinsic definition content of the message (1) to a applicant; 2), after the applicant receives the new message (1), checking whether the MIC therein is correct; if no, the applicant discarding the received new message (1); if yes, checking the new message (1), if the checking is successful, sending a message (2) to the authenticator; the process of checking the new message (1) being the same as the checking process for the message (1) defined in the IEEE 802.11i-2004 standard document. The method solves the DoS attack problem of the key management protocol in the existing RSNA security mechanism.

(57) **摘要:**

一种密钥管理方法，为一种增强的RSNA 的4 步握手协议。其前两步握手过程为：1)、认证器向请求者发送新消息（1），该新消息（1）为：在消息（1）原有定义内容的基础上，添加密钥协商标识KNID 和消息完整性码MIC 所构成的消息；2)、请求者接收该新消息（1）之后，验证其中的MIC 是否正确；如果否，则丢弃所接收的新消息（1）；如果是，则对该新消息（1）进行验证，若验证成功，则向认证器发送消息（2）；该对新消息（1）进行验证的过程，与IEEE 802.11i-2004 标准文本中定义的对消息（1）的验证过程相同。该方法解决了目前RSNA 安全机制中密钥管理协议存在的DoS 攻击问题。

WO 2009/067933 A1

本国际公布：
— 包括国际检索报告。

一种密钥管理方法

本申请要求于 2007 年 11 月 16 日提交中国专利局、申请号为200710019090.9、发明名称为“一种密钥管理方法”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

本发明涉及一种信息安全技术领域，尤其是一种用于密钥管理方法。

背景技术

为了解决无线局域网 WLAN（Wireless Local Area Network）国际标准 ISO/IEC 8802-11 中定义的有线等效保密 WEP（Wired Equivalent Privacy）安全机制存在的安全漏洞，IEEE 组织颁布了 IEEE 802.11i 标准，在后向兼容的基础上，提出了鲁棒安全网络关联 RSNA（Robust Security Network Association）技术弥补 WEP 存在的安全漏洞。

RSNA 通过基于扩展认证协议 EAP（Extended Authentication Protocol）的 IEEE 802.1x 与 4 步握手协议（4-way Handshake），实现认证与密钥分发功能。RSNA 安全机制较好地解决了 WLAN 的安全问题，但由于其在设计时更多考虑了安全性，而没有过多考虑协议的可用性，因此其 4 步握手协议存在拒绝服务 DoS（Denial of Service）攻击问题。这是由于 4 步握手协议的消息 1 未采取保护措施，裸露的消息 1 可能被攻击者利用。

对于认证器（Authenticator），最多与每个请求者（Supplicant）存在一个握手，并具有超时重发功能，但请求者却不能采用同样的策略。若请求者配置成完全状态的，即仅期望某个特定消息的应答，现考虑请求者接收到消息1并发出消息2这种情况，若消息2由于各种原因丢失了，认证器将得不到期望的消息2，因此认证器超时之后会重传消息1，但由于请求者仅期望收到消息3，则会丢弃该重传的消息1，引起协议失败，则攻击者利用这一点可以抢先在合法消息1之前发送伪造的消息1，造成请求者阻塞协议。因此在握手过程中，请求者必须允许接受多个消息1以保证协议能够继续，即请求者必须允许多个握手实例同时运行。

协议阻塞攻击是由于消息 1 的薄弱性造成的，为回避此问题，在协议实施时，请求者可存储多个成对临时密钥 PTK（Pairwise Transient Key），其中有

一个为合法的成对临时密钥，其余为临时的成对临时密钥。收到消息 1 时仅更新临时的成对临时密钥，只有收到带有有效消息完整性码 MIC（Message Integrity Code）的消息 3 时才更新合法的成对临时密钥。若攻击者发送多个携带不同 Nonce（一次性随机数）的消息 1，为了确保不阻塞合法认证器的协议执行，请求者必须采用相当大的存储空间来存储所有收到的消息 1 中的 Nonce、本地新产生的 Nonce 及对应的临时的成对临时密钥，直到它完成握手并得到一个合法的成对临时密钥。成对临时密钥的计算虽然花费不大，不会造成 CPU 耗尽攻击，但攻击者若有意提高伪造消息 1 的发送频率，则存在存储耗尽的危险。这种伪造攻击易于实施，造成的危害也比较严重，一次成功的攻击将使得先期的对认证过程的种种努力化为泡影。

发明内容

本发明为解决背景技术中存在的上述技术问题，而提供一种密钥管理方法，以防止通过伪造和重放消息 1 而进行的 DoS 攻击。技术方案如下：

本发明提供一种密钥管理方法，该方法为一种增强的 RSNA 的 4 步握手协议，其包括以下步骤：

1）、认证器向请求者发送新消息 1，所述新消息 1 为：在消息 1 原有定义内容的基础上，添加密钥协商标识 KNID 和消息完整性码 MIC 所构成的消息；

2）、请求者接收所述新消息 1 之后，验证其中的 MIC 是否正确；

如果否，则丢弃所接收的新消息 1；

如果是，则对所述新消息 1 进行验证，若验证成功，则向认证器发送消息 2；

3）、认证器接收所述消息 2 之后，对消息 2 进行验证，若验证成功，则向请求者发送消息 3；

4）、请求者接收所述消息 3 之后，对消息 3 进行验证，若验证成功，则向认证器发送消息 4；

5）、认证器接收所述消息 4 之后，对消息 4 进行验证，若验证成功，则 4 步握手协议成功完成，认证器和请求者协商出一致的成对临时密钥 PTK，并各自得到对方的组播主密钥 GMK；

其中，所述消息 1 原有定义内容以及消息 2、消息 3 和消息 4 的内容分别

与 IEEE 802.11i-2004 标准文本中的定义相同，所述对新消息 1、消息 2、消息 3 和消息 4 进行的验证过程分别与 IEEE 802.11i-2004 标准文本中的定义相同。

其中，上述步骤 1）中消息完整性码 MIC 为:

认证器利用认证阶段已协商的成对主密钥 PMK 对 MIC 字段之前的所有字段计算的杂凑值。

其中，上述步骤 1）中的密钥协商标识 KNID:

若所述握手过程为鲁棒安全网络关联 RSNA 认证成功后的首次 4 步握手过程，则所述 KNID 为认证器产生的随机数;

若所述握手过程为密钥更新过程，则所述 KNID 为上一次 4 步握手协议过程成功时，认证器根据成对主密钥 PMK、认证器产生的一次性随机数、请求者产生的一次性随机数 $Nonce_S$ 计算得到的值。

本发明通过在原有的 RSNA 的 4 步握手方法的消息 1 的基础上添加消息完整性码 MIC 和密钥协商标识 KNID，防止对消息 1 的伪造和重放，以增强协议的安全性和健壮性，解决了目前 RSNA 安全机制中密钥管理协议存在的 DoS 攻击问题。

具体实施方式

本发明的具体方法如下:

1）、认证器在消息 1 原有定义内容的基础上，添加密钥协商标识 KNID（Key Negotiation IDentifier）和消息完整性码 MIC，构成新消息 1 后，发送给请求者;

2）、请求者收到新消息 1 之后，验证其中的 MIC 字段是否正确，若不正确，则直接丢弃；否则，进行原有验证，若验证成功，则向认证器发送消息 2;消息 2 的内容与原有定义相同；在本说明书中，所述原有定义和原有验证指的是 IEEE 802.11i-2004 标准文本中的定义和验证。

需说明的是：新消息 1 中的 MIC 为认证器利用认证阶段已协商的成对主密钥 PMK（Pairwise Master Key）对 MIC 字段之前的所有字段计算的杂凑值;对于新消息 1 中的 KNID，若此次过程为 RSNA 认证成功后的首次 4 步握手协议过程，则 KNID 为认证器产生的随机数；若此次过程为密钥更新过程，则

KNID 为上一次 4 步握手协议过程成功后，认证器根据 PMK、$Nonce_A$（认证器产生的一次性随机数）、$Nonce_S$（请求者产生的一次性随机数）计算得到的值。MIC 字段的添加杜绝了攻击者对消息 1 的伪造，KNID 的这种设计使认证器和请求者能够实现同步功能，杜绝了攻击者对消息 1 的重放。在密钥更新过程中，请求者对消息 1 的验证还应包含对 KNID 的验证。

3）、认证器收到消息 2 之后，进行原有验证，若验证成功，则向请求者发送消息 3；消息 3 的内容与原有定义相同；

4）、请求者收到消息 3 之后，进行原有验证，若验证成功，则向认证器发送消息 4；消息 4 的内容与原有定义相同；

5）、认证器收到消息 4 之后，进行原有验证，若验证成功，则 4 步握手协议成功完成，认证器和请求者协商出一致的成对临时密钥 PTK，并各自得到对方的组播主密钥 GMK（Group Master Key）。

权 利 要 求

1、一种密钥管理方法，其特征在于，握手过程包括以下步骤:

1)、认证器向请求者发送新消息1，所述新消息1为：在消息1原有定义内容的基础上，添加密钥协商标识KNID和消息完整性码MIC所构成的消息;

2)、请求者接收所述新消息1之后，验证其中的MIC是否正确;

如果否，则丢弃所接收的新消息1;

如果是，则对所述新消息1进行验证，若验证成功，则向认证器发送消息2;

3)、认证器接收所述消息2之后，对消息2进行验证，若验证成功，则向请求者发送消息3;

4)、请求者接收所述消息3之后，对消息3进行验证，若验证成功，则向认证器发送消息4;

5)、认证器接收所述消息4之后，对消息4进行验证，若验证成功，则4步握手协议成功完成，认证器和请求者协商出一致的成对临时密钥 PTK，并各自得到对方的组播主密钥GMK;

其中，所述消息1原有定义内容以及消息2、消息3和消息4的内容分别与IEEE 802.11i-2004标准文本中的定义相同，所述对新消息1、消息2、消息3和消息4进行的验证过程分别与IEEE 802.11i-2004标准文本中的定义相同。

2、根据权利要求 1 所述的密钥管理方法，其特征在于：所述步骤 1）中消息完整性码MIC为:

认证器利用认证阶段已协商的成对主密钥PMK对MIC字段之前的所有字段计算的杂凑值。

3、根据权利要求 1 所述的密钥管理方法，其特征在于，所述步骤 1）中的密钥协商标识KNID:

若所述握手过程为鲁棒安全网络关联RSNA认证成功后的首次4步握手过程，则所述KNID为认证器产生的随机数;

若所述握手过程为密钥更新过程，则所述KNID为上一次4步握手协议过程成功时，认证器根据成对主密钥 PMK、认证器产生的一次性随机数、请求者产生的一次性随机数 $Nonce_S$ 计算得到的值。

4、根据权利要求 1、2 或 3 所述的密钥管理方法，其特征在于，若所述握手过程为密钥更新过程，则所述步骤 2）中，请求者在接收所述新消息 1 后，验证 MIC 和 KNID 是否正确;

如果所述 MIC 和/或 KNID 不正确，则丢弃所接收的新消息 1;

如果所述 MIC 和 KNID 正确，则进行原有验证 1，若验证成功，则向认证器发送消息 2。

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2008/073051

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

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/-; H04L29/-; H04L12/-

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, PAJ: key MIC KNID handshake negotiation integrity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PY	CN101159538A, (XIDIAN JIETONG RADIO NETWORK COMMUNICATION CO LTD), 09 Apr. 2008(09.04.2008), claims 1-6	1-4
Y	US20060107050A1, (DRAYTEK CORP), 18 May 2006(18.05.2006), description segment [0018]	1-4
A	CN101039180A, (ZHONGXING COMMUNICATION CO LTD), 19 Sep. 2007(19.09.2007), the whole document	1-4
A	WO2006093161A1, (MATSUSHITA ELECTRIC IND CO LTD), 08 Sep. 2006(08.09.2006), the whole document	1-4

☐ 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
14 Feb. 2009(14.02.2009)	**26 Feb. 2009 (26.02.2009)**
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 HAN, Yan Telephone No. (86-10)62411765

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2008/073051

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101159538A	09.04.2008	NONE	
US20060107050A1	18.05.2006	EP1722503A1	15.11.2006
		TW268083B1	01.12.2006
CN101039180A	19.09.2007	NONE	
WO2006093161A1	08.09.2006	EP1843508A1	10.10.2007
		CN101133592A	27.02.2008
		JP2007505966T	07.08.2008

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2008/073051

Continuation of the second sheet:

CLASSIFICATION OF SUBJECT MATTER

H04L9/00(2006.01)i
H04L29/06(2006.01)n
H04L12/28(2006.01)n

国际检索报告

国际申请号
PCT/CN2008/073051

A. 主题的分类

参见附加页

按照国际专利分类表(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/-; H04L29/-; H04L12/-

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,PAJ:密 握手 协商 完整 钥 key MIC KNID handshake negotiation integrity

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
PY	CN101159538A, (西安西电捷通无线网络通信有限公司), 09.4 月 2008(09.04.2008), 权利要求 1-6	1-4
Y	US20060107050A1, (DRAYTEK CORP), 18.5 月 2006(18.05.2006), 说明书第[0018]段	1-4
A	CN101039180A, (中兴通讯股份有限公司), 19.9 月 2007(19.09.2007), 全文	1-4
A	WO2006093161A1, (松下电器产业株式会社), 08.9 月 2006(08.09.2006), 全文	1-4

☐ 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

"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
14.2 月 2009(14.02.2009)	**26.2 月 2009 (26.02.2009)**
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	受权官员 **韩燕** 电话号码：(86-10) **62411765**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2008/073051

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101159538A	09.04.2008	无	
US20060107050A1	18.05.2006	EP1722503A1	15.11.2006
		TW268083B1	01.12.2006
CN101039180A	19.09.2007	无	
WO2006093161A1	08.09.2006	EP1843508A1	10.10.2007
		CN101133592A	27.02.2008
		JP2007505966T	07.08.2008

续第二页

主题的分类

H04L9/00(2006.01)i
H04L29/06(2006.01)n
H04L12/28(2006.01)n