Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN2008/073051

International filing date: 14 November 2008 (14.11.2008)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200710019090.9
Filing date: 16 November 2007 (16.11.2007)

Date of receipt at the International Bureau: 04 February 2009 (04.02.2009)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

中华人民共和国国家知识产权局
STATE INTELLECTUAL PROPERTY OFFICE
OF THE PEOPLE'S REPUBLIC OF CHINA

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　　请　　日：2007.11.16

申　　请　　号：200710019090.9

申　请　类　别：发明专利

发明创造名称：一种密钥管理方法

申　　请　　人：西安西电捷通无线网络通信有限公司

发明人或设计人：铁满霞、曹军、庞辽军、赖晓龙、黄振海

中华人民共和国
国家知识产权局局长 田力普

2009 年 1 月 19 日

07.1.26

权 利 要 求 书

1、一种密钥管理方法，其特征在于：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，构成新的消息（1）后，发送给请求者；

2)、请求者收到新的消息（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）；

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）；

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）；

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单播临时密钥 UTK，并各自得到对方的组播主密钥 GMK。

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，若此次过程为 RSNA 认证成功后的首次 4 步握手协议，则其为认证器产生的随机数，若为密钥更新过程，则其为上一次 4 步握手协议成功后，认证器根据成对主密钥 PMK、$Nonce_A$、$Nonce_S$ 计算得到的值。

4、根据权利要求 1 或 2 或 3 所述的密钥管理方法，其特征在于：若为密钥更新过程，所述步骤 2）中请求者还要验证 KNID 是否正确，不正确，则直接丢弃。

5、根据权利要求 4 所述的密钥管理方法，其特征在于：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。

6、根据权利要求 4 所述的密钥管理方法，其特征在于：所述原有验证均为 IEEE 802.11i-2004 标准文本中的验证过程。

07.1.26

5

说 明 书

一种密钥管理方法

技术领域

本发明涉及一种密钥管理方法，尤其是一种用于RSNA的密钥管理方法。

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 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。该安全机制均较好地解决了 WLAN 的安全问题，但由于这种机制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 DoS 攻击问题。这是由于 4 步握手协议的第一个消息未采取保护措施，裸露的消息 1 可被攻击者利用。

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，请求者可存储多个单播临时密钥 UTK（Unicast Temporal Key），一个为合法的单播临时密钥，其余为临时的单播临时密钥。收到消息 1 时仅更新

临时的单播临时密钥，只有收到带有有效消息完整性码 MIC（Message Integrity Code）的消息 3 时才更新合法的单播临时密钥。若攻击者发送多个携带不同 Nonce 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 及对应的临时的单播临时密钥，直到它完成握手并得到一个合法的单播临时密钥。单播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，而提供一种可防止 DoS 攻击的密钥管理方法。

本发明的技术解决方案是：本发明为一种密钥管理方法，其特殊之处在于：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，构成新的消息 1 后，发送给请求者；

2)、请求者收到新的消息 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；

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；

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；

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单播临时密钥 UTK，并各自得到对方的组播主密钥 GMK。

上述步骤 1）中 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。

上述步骤 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，则其为认证器产生的随机数，若为密钥更新过程，则其为上一次 4 步握手协议成功后，认证器根据 PMK、$Nonce_A$、$Nonce_S$ 计算得到的值。

若为密钥更新过程，步骤 2）中请求者还要验证 KNID 是否正确，不正确，则直接丢弃。

上述消息 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。

上述原有验证均为 IEEE 802.11i-2004 标准文本中的验证过程。

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，构成新的消息 1 后，发送给请求者；

2)、请求者收到新的消息 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；

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；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，则其为认证器产生的随机数，若为密钥更新过程，则其为上一次 4 步握手协议成功后，认证器根据 PMK、$Nonce_A$、$Nonce_S$ 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单播临时密钥 UTK，并各自得到对方的组播主密钥 GMK（Group Master Key）。

名词解释：

$Nonce_A$：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。

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。