[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
H04L 12/56 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510080018.8

[45] 授权公告日 2009 年 12 月 16 日

[11] 授权公告号 CN 100571124C

[22] 申请日 2005.6.24
[21] 申请号 200510080018.8
[73] 专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 肖正飞 李永茂
[56] 参考文献
US2002089979A1 2002.7.11
CN1451212A 2003.10.22
审查员 王 琼

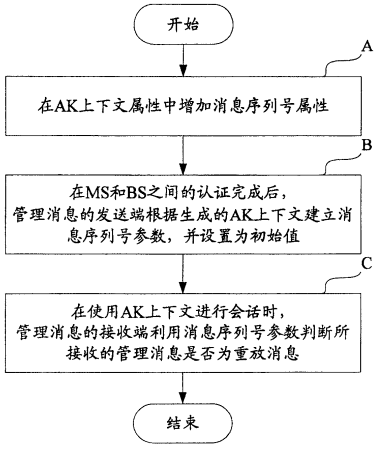
权利要求书 2 页 说明书 9 页 附图 1 页

[54] 发明名称

防止重放攻击的方法以及保证消息序列号不重复的方法

[57] 摘要

本发明公开了一种防止重放攻击的方法，包括：在鉴权密钥的上下文中增加消息序列号属性；在管理消息的交互双方的认证完成，生成鉴权密钥上下文后，管理消息的发送端根据所生成的鉴权密钥上下文中的消息序列号属性建立消息序列号参数，并设置为初始值；在使用该鉴权密钥上下文进行会话的过程中，所述管理消息的发送端发送携带有消息序列号参数的管理消息到接收端，所述接收端根据所接收的消息序列号参数判断接收的管理消息是否为重放消息，如果是，则丢弃该管理消息，否则，接收该管理消息。 本发明还公开了一种保证消息序列号不重复的方法。 应用本发明所述的方法可以保证，在一个鉴权密钥上下文内，消息序列号始终不重复。



1、一种防止重放攻击的方法，其特征在于，所述方法包括：

A、在鉴权密钥的上下文中增加消息序列号属性；

B、在管理消息交互双方之间的认证完成，生成鉴权密钥上下文后，管理消息的发送端根据所生成鉴权密钥上下文中的消息序列号属性建立消息序列号参数，并将建立的消息序列号参数设置为初始值；

C、在使用该鉴权密钥上下文进行会话的过程中，所述管理消息的发送端发送携带有消息序列号参数的管理消息到该管理消息的接收端，所述接收端根据所接收的消息序列号参数判断接收的管理消息是否为重放消息，如果是，则丢弃该管理消息，否则，接收该管理消息。

2、如权利要求 1 所述的方法，其特征在于，步骤 B 所述认证为：初始接入认证或重认证。

3、如权利要求 1 所述的方法，其特征在于，在步骤 C 所述管理消息的发送端在发送所述管理消息之前，进一步包括：将所述消息序列号递增一个预定的数值。

4、如权利要求 3 所述的方法，其特征在于，步骤 C 所述预定的数值为 1。

5、如权利要求 3 所述的方法，其特征在于，步骤 C 所述根据所接收的消息序列号参数判断接收的管理消息是否为重放消息包括：接收端将接收到的消息序列号参数与自身保存的已接收管理消息的消息序列号进行比较，如果小于或等于所述自身保存的已接收管理消息的消息序列号，则接收的管理消息为重放的管理消息；否则，不是重放的管理消息。

6、如权利要求 1 所述的方法，其特征在于，所述方法在步骤 C 进一步包括：在使用该鉴权密钥上下文进行会话的过程中，所述管理消息的发送端实时监测所述消息序列号参数的数值，在所述消息序列号达到最大值之前预定的时间内，发起重认证过程，然后返回步骤 B。

7、如权利要求 6 所述的方法，其特征在于，所述预定时间为完成重认

证过程及启用鉴权密钥上下文所需的时间。

8、如权利要求 1 所述的方法，其特征在于，步骤 C 所述发送携带有消息序列号参数的管理消息到该管理消息的接收端为：通过基于加密的消息认证码摘要将所述消息序列号参数发送到所述接收端。

9、如权利要求 1、5 或 6 所述的方法，其特征在于，所述管理消息的发送端为移动台；所述接收端为基站；所述消息序列号为上行消息序列号。

10、如权利要求 1、5 或 6 所述的方法，其特征在于，所述管理消息的发送端为基站；所述接收端为移动台；所述消息序列号为下行消息序列号。

11、一种保证消息序列号不重复的方法，其特征在于，所述方法包括：

在鉴权密钥的上下文中增加消息序列号属性；

在管理消息交互双方之间的认证完成，生成鉴权密钥上下文后，管理消息的发送端根据所生成鉴权密钥上下文中的消息序列号属性建立消息序列号参数，并将建立的消息序列号参数设置为初始值。

12、根据权利要求 11 所述的方法，其特征在于，所述方法进一步包括：在所述管理消息交互双方使用该鉴权密钥上下文进行会话的过程中，所述管理消息的发送端实时监测所述消息序列号参数的数值，在所述消息序列号达到预定值之前预定的时间内，发起重认证过程，将消息序列号参数设置为初始值。

13、根据权利要求 12 所述的方法，其特征在于，所述预定时间为完成重认证过程及启用鉴权密钥上下文所需的时间。

14、根据权利要求 11、12 或 13 所述的方法，其特征在于，所述管理消息的发送端为移动台；所述接收端为基站；所述消息序列号为上行消息序列号。

15、根据权利要求 11、12 或 13 所述的方法，其特征在于，所述管理消息的发送端为基站；所述接收端为移动台；所述消息序列号为下行消息序列号。

防止重放攻击的方法以及保证消息序列号不重复的方法

技术领域

本发明涉及到提高无线通信系统安全性的技术，特别涉及到一种防止重放攻击的方法以及一种保证消息序列号不重复的方法。

背景技术

在通信系统中，安全性是评价一个通信系统性能优劣的重要指标，特别是在无线通信系统中，由于无线通信系统具有开放性和移动性的特点，使得无线通信系统的安全性显得尤为重要。随着密码学和密码分析学的发展，可以通过对在无线通信系统的空中接口（简称空口）上传输的数据进行加密的方式提高无线通信系统的安全性。

IEEE 802.16d/e 系列协议定义了无线宽带固定和移动接入空口部分的协议标准。为了保证空口数据传输的安全性，上述系列协议定义了一个安全子层（Privacy Sublayer），用于实现对无线通信系统用户的认证、密钥的分发和管理以及后续的数据加密和认证等等。根据协议规定，在认证方式上，除了可以使用基于数字证书的 RSA 算法（由 Rivest、Shamir、Adleman 开发的公开密钥加密算法）实现对接入移动台（MS）和基站（BS）之间的双向认证之外，还可以使用可扩展认证协议（EAP）实现对接入用户的认证。在认证完成后，MS 和 BS 还需要通过密钥管理协议（PKM）生成、分发并管理对空口数据进行加密的密钥，上述 PKM 过程的结果就是在 MS 和 BS 之间生成一个用于派生其他密钥资源的基本密钥——鉴权密钥（AK，Authorization Key）。根据生成的 AK，MS 和 BS 可以派生出对数据加密或对信令消息认证所使用的密钥，从而提高 MS 和 BS 之间空口数据传输的安全性。

为了进一步增强无线通信系统的安全性，防止网络攻击者恶意破解MS的AK，协议规定MS和BS协商产生的AK仅在一段时间内有效，称为AK的生命周期。因此，在某个AK生命周期终止前，该AK对应的MS和BS需要进行重认证过程，以产生新的AK。除此之外，当MS漫游到新的目标BS时，也需要进行网络重入（Network Re-entry）过程，并根据相应的安全策略，通过重认证产生新的密钥资源或从后端网络获得已有的密钥资源。

上述这种使用AK派生出来的密钥对MS和BS之间空口数据进行加密的方法虽然可以提高无线通信系统的安全性，但是无法防止重放攻击（Replay Attack）。所述的重放攻击是一种常见的网络攻击方法，攻击者首先截获在通信双方在某次交互过程中由其中一方发送的数据包，并在以后某个合适的时机向该数据包的接收端重新发送截获的数据，如果在所述数据包中没有包含足够的信息使接收端能够判断出该数据包是第一次发送的数据包还是重发的数据包，攻击者就能够冒充通信双方中的一方来欺骗另一方，以达到攻击无线通信系统的目的。虽然一般的业务对重放攻击不太敏感，但是，对于一些重要的管理消息而言，重放攻击可能会对系统造成致命的破坏。

为此，IEEE 802.16e在PKM版本2中提供了一种防止管理消息重放攻击的方法，该方法通过协议定义的基于加密的消息认证码（CMAC）的摘要（Digest）实现防重放攻击，同时实现对管理消息的认证。在该方法中，CMAC Digest由一个32位的消息序列号（CMAC_PN）及一个CMAC值（CMAC Value）组成，通常情况下，消息序列号CMAC_PN是在发送方（MS或BS）递增变化的序列号，用于标识不同的管理消息，在这里，所述的消息序列号CMAC_PN既可以表示上行消息序列号CMAC_PN_U，也可以表示下行消息序列号CMAC_PN_D；CMAC Value是用AK派生出来的密钥对消息序列号CMAC_PN、管理消息体以及其他信息进行加密后得到的信息摘要。在实际的应用中，发送方在发送管理消息时，会首先将CMAC摘要中的消息序列号CMAC_PN递增某一个数值，例如1，再将递增后的消息序列号CMAC_PN与通过加密算法计算得到的CMAC Value一起作为CMAC Digest发送给接

收方。接收方（BS 或 MS）在接收到该管理消息时，首先使用接收端保存的密钥采用和发送端一样的方法计算 CMAC Value，并与消息中携带的 CMAC Value 比较，从而实现了对消息的认证，同时根据 CMAC_PN 判断消息是否为重放消息。

在现有的方法中，CMAC_PN 是 32 位的无符号整数，其取值空间从 0X00000000 到 0XFFFFFFFF，如果每次递增值为 1，通常可以保证 CMAC_PN 在很长的周期内不会重复。但是，由于在上述方法中 CMAC_PN 与 AK 没有直接关系，可能会出现在一个 AK 的上下文中，CMAC_PN 从一个较大的数值开始计数，并在计数到最大值后又从初始值开始计数的情况，从而不能保证在一个 AK 的上下文中 CMAC_PN 始终向上递增，导致接收方在根据消息序列号 CMAC_PN 判断所接收消息是否为重放消息时的处理非常复杂。

发明内容

为了解决上述技术问题，本发明提供了一种防止重放攻击的方法，保证在一个 AK 上下文中使用的消息序列号始终不会重复，从而使得接收端可以根据消息序列号判断所接收消息是否为重放消息。

除此之外，本发明还提供了一种保证在一个 AK 上下文中所使用的消息序列号不重复的方法，避免在一个 AK 上下文中消息序列号从一个较大的数值开始计数，并在计数到最大值后又从初始值开始计数的情况所导致的接收端处理复杂的问题。

本发明所述的防止重放攻击的方法包括：

A、在 AK 上下文中增加消息序列号属性；

B、在管理消息交互双方之间的认证完成，生成 AK 上下文后，管理消息的发送端根据所生成 AK 上下文中的消息序列号属性建立消息序列号参数，并将建立的消息序列号参数设置为初始值；

C、在使用该 AK 上下文进行会话的过程中，所述管理消息的发送端发送管携带有消息序列号参数的管理消息到该管理消息的接收端，所述接收端

根据所接收的消息序列号参数判断接收的管理消息是否为重放消息，如果是，则丢弃该管理消息，否则，接收该管理消息。

步骤 B 所述认证为：初始接入认证或重认证。

在步骤 C 所述管理消息的发送端在发送所述管理消息之前，进一步包括：将所述消息序列号递增一个预定的数值。

步骤 C 所述预定的数值为 1。

步骤 C 所述根据所接收的消息序列号参数判断接收的管理消息是否为重放消息包括：接收端将接收到的消息序列号参数与自身保存的已接收管理消息的消息序列号进行比较，如果小于或等于所述自身保存的已接收管理消息的消息序列号，则接收的管理消息为重放的管理消息；否则，不是重放的管理消息。

本发明所述方法在步骤 C 进一步包括：在使用该 AK 上下文进行会话的过程中，所述管理消息的发送端实时监测所述消息序列号参数的数值，在所述消息序列号达到最大值之前预定的时间内，发起重认证过程，然后返回步骤 B。

本发明所述预定时间为完成重认证过程及启用 AK 上下文所需的时间。

步骤 C 所述发送携带有消息序列号参数的管理消息到该管理消息的接收端为：通过基于加密的消息认证码摘要将所述消息序列号参数发送到所述接收端。

本发明所述管理消息的发送端为移动台；所述接收端为基站；所述消息序列号为上行消息序列号。

本发明所述管理消息的发送端为基站；所述接收端为移动台；所述消息序列号为下行消息序列号。

本发明所述保证消息序列号不重复的方法包括：

在鉴权密钥的上下文中增加消息序列号属性；

在管理消息交互双方之间的认证完成，生成鉴权密钥上下文后，管理消息的发送端根据所生成鉴权密钥上下文中的消息序列号属性建立消息序列号参

数，并将建立的消息序列号参数设置为初始值。

所述方法进一步包括：在所述管理消息交互双方使用该鉴权密钥上下文进行会话的过程中，所述管理消息的发送端实时监测所述消息序列号参数的数值，在所述消息序列号达到预定值之前预定的时间内，发起重认证过程，将消息序列号参数设置为初始值。

所述预定时间为完成重认证过程及启用鉴权密钥上下文所需的时间。

由此可以看出，本发明所述的防止重放攻击的方法通过将上行消息序列号和下行消息序列号加入 AK 上下文，作为 AK 上下文的属性，保证在每次认证过程完成后，产生新的 AK 时，MS 和 BS 所使用的上行、下行消息序列号也相应的重置为初始值，从而保证在一个 AK 上下文中，上行、下行消息序列号始终是不重复的。

另外，本发明所述的防止重放攻击的方法，通过在所述上行、下行消息序列号到达最大值之前，发起重认证过程，以重置所述上行、下行消息序列号，保证上行、下行消息序列号在一个 AK 上下文中不会重复。

附图说明

图 1 为本发明所述防重放攻击方法的流程图。

具体实施方式

为了解决现有技术中的问题，本发明提供了一种防止重放攻击的方法以及保证所发送管理消息的消息序列号不重复的方法，该方法主要思想是：在 AK 的上下文属性中增加上行、下行消息序列号属性，建立 AK 与上行、下行消息序列号之间的关系，使得 MS 和 BS 之间在初始接入认证或重认证完成，产生新的 AK 时，所述上行、下行消息序列号也重新设置为初始值，从而保证在一个 AK 上下文中所使用的 CMAC_PN 不重复，例如可以始终向上递增或向下递减或存在其它对应关系等等。

本发明所述的防止重放攻击的方法，主要包括：

A、在 AK 的上下文属性中增加消息序列号属性。

其中，所述消息序列号包括：用于标识上行管理消息的上行消息序列号 CMAC_PN_U 及用于标识下行管理消息的下行消息序列号 CMAC_PN_D。

B、在 MS 和 BS 之间的认证完成，生成 AK 上下文后，空中接口上管理消息的发送端，包括 MS 或 BS，根据该 AK 上下文建立消息序列号参数，并将建立的消息序列号参数设置为初始值。

对于上行管理消息来讲，其发送端为 MS，MS 根据该 AK 上下文建立上行消息序列号 CMAC_PN_U 参数，该参数可以采用 32 位的无符号整数，其取值空间从 0X00000000 到 0XFFFFFFFF，并设置为初始值 0X00000000；对下行管理消息来讲，其发送端为 BS，BS 根据该 AK 上下文建立下行消息序列号 CMAC_PN_D，该参数也可以采用 32 位的无符号整数，其取值空间从 0X00000000 到 0XFFFFFFFF，并设置为初始值 0X00000000。

由于根据协议规定，在 MS 和 BS 的认证过程完成后，将为 MS 和 BS 之间的会话生成一个 AK 的上下文，在这里，所述的认证包括初始接入认证和重认证，所述的上下文是指本次会话各个属性的集合，该 AK 上下文至少包括：本次会话使用的 AK、AK 的生命周期及由 MS 所维护的上行消息序列号 CMAC_PN_U 及由 BS 所维护的下行消息序列号 CMAC_PN_D。由于 AK 上下文具有一定的作用域和生命周期。因此，AK 上下文在产生后，仅能够在一个有限的作用域内使用，例如仅能够在对应的 MS 和 BS 之间使用，并且它所包含的各个属性仅在其生命周期内有效，即当该 AK 生命周期结束时，该 AK 上下文中所包含的属性也相应失效。

由此可以看出，通过将上行消息序列号 CMAC_PN_U 和下行消息序列号 CMAC_PN_D 作为 AK 上下文的属性，使得在每次认证过程完成后（包括初始接入认证过程和重认证过程），由于生成了新的 AK 上下文，MS 会自动将上行消息序列号 CMAC_PN_U 重新设置为初始值；BS 会自动将下行消息序列号 CMAC_PN_D 重新设置为初始值，保证在一个 AK 上下文中上行消息序列号 CMAC_PN_U 和下行消息序列号 CMAC_PN_D 可以从初始值

向上递增，因此，接收端可以通过判断所接收管理消息的消息序列号是否大于自身保存的已接收管理消息的消息序列号来判断所接收管理消息是否为重放消息，从而大大简化接收端对消息序列号的处理。

C、在 MS 和 BS 使用该 AK 上下文进行会话的过程中，管理消息的发送端先将消息序列号参数递增一个预定的数值，例如 1，再将递增后的消息序列号参数与管理消息一起发送到接收端，所述接收端根据所接收管理消息中的消息序列号参数判断该管理消息是否为重放消息，如果是，则丢弃该管理消息，否则，接收所述管理消息，从而实现防重放攻击的目的。

下面将具体说明在一个 AK 上下文的生命周期内，MS 和 BS 利用上行消息序列号 CMAC_PN_U 及下行消息序列号 CMAC_PN_D 进行防重放攻击的过程。

MS 使用上行消息序列号 CMAC_PN_U 标识所发送的上行管理消息，具体包括：MS 在发送上行管理消息之前，首先将上行消息序号 CMAC_PN_U 递增某一个数值，例如 1，再将递增后的 CMAC_PN_U 与通过加密算法计算得到的 CMAC Value 一起作为 CMAC Digest 发送给 BS；BS 在接收到该管理消息后，首先用本地保存的密钥采用和 MS 一样的方法计算 CMAC Value，并与消息中携带的 CMAC Value 比较，从而实现了对消息的认证，同时根据上行消息序列号 CMAC_PN_U 判断消息是否为重放消息。

BS 使用下行消息序列号 CMAC_PN_D 标识所发送的下行管理消息的方法与上述方法基本相同，包括：BS 在发送下行管理消息之前，首先将下行消息序号 CMAC_PN_D 递增某一个数值，再将递增后的 CMAC_PN_D 与 CMAC Value 一起作为 CMAC Digest 发送给 MS；MS 在接收到该下行管理消息后，首先用本地保存的密钥采用和 BS 一样的方法计算 CMAC Value，并与消息中携带的 CMAC Value 比较，从而实现了对消息的认证。同时根据下行消息序列号 CMAC_PN_D 判断消息是否为重放消息。

MS 和 BS 根据所述上行消息序列号或下行消息序列号判断所接收管理消息是否为重放管理消息的方法有很多种。例如，在本发明的一个优选实施

例中，由于发送端所发送管理消息中的消息序列号是递增的，因此，接收端可以将接收到管理消息中的消息序列号与自身保存的已接收管理消息的消息序列号进行比较，如果小于或等于自身保存的消息序列号，则说明该管理消息为重放的管理消息。通过这种方法，接收端可以非常简单的识别出重放的管理消息。本发明所述的方法通过将消息序列号作为 AK 上下文的属性，建立 AK 与消息序列号的关联关系，使得 MS 和 BS 在认证完成后，产生新的 AK 时，MS 和 BS 所维护的消息序列号也能够随之重新置为初始值，并在随后的会话过程中从初始值递增计数，保证在一个 AK 上下文中，消息序列号始终递增。

为了避免在某些特殊的情况下出现的由消息序列号的重复周期小于 AK 生命周期所导致的在一个 AK 上下文内出现消息序列号重复的情况，本发明所述的方法进一步包括:

在上行方向，MS 实时监测上行消息序列号 CMAC_PN_U 的值，在上行消息序列号 CMAC_PN_U 达到最大值之前预定的时间内，主动发起重认证过程，在重认证过程完成后，根据所生成的、新的 AK 上下文，MS 所维护的上行消息序列号 CMAC_PN_U 参数及 BS 所维护的下行消息序列号 CMAC_PN_D 参数将被重新设置为初始值。

在下行方向，BS 实时检测下行消息序列号 CMAC_PN_D 的值，在下行消息序列号 CMAC_PN_D 达到最大值之前预定的时间内，发送鉴权失效（Authentication Invalid）消息到 MS，通知 MS 发起重认证过程，在重认证过程完成后，根据所生成、新的 AK 上下文，MS 所维护的上行消息序列号 CMAC_PN_U 参数和 BS 所维护的下行消息序列号 CMAC_PN_D 参数将被重新设置为初始值。

其中，所述的预定时间为完成重认证过程并启用新的 AK 上下文所需的时间。这样一来，通过上述方法，就可以保证在上行或下行消息序列号在达到最大值之前 MS 和 BS 能够启用新的 AK 上下文，从而有效的避免所述上行或下行消息序列号出现重复。

需要说明的是，在重认证完成，生成新的 AK 之后，MS 会立即使用新的 AK 对后续的会话进行加密。但 BS 不会立即使用新的 AK，它只有在接收到 MS 发送的密钥更新请求(Key Request)消息，并且检测到该 Key Request 消息携带的 CMAC Digest 中的 CMAC Value 是由新的 AK 派生的密钥计算得到的之后，即判断出当前 MS 已经成功完成重认证并获得了新的 AK 时，才使用新的 AK 对后续的会话进行加密和计算消息校验码。

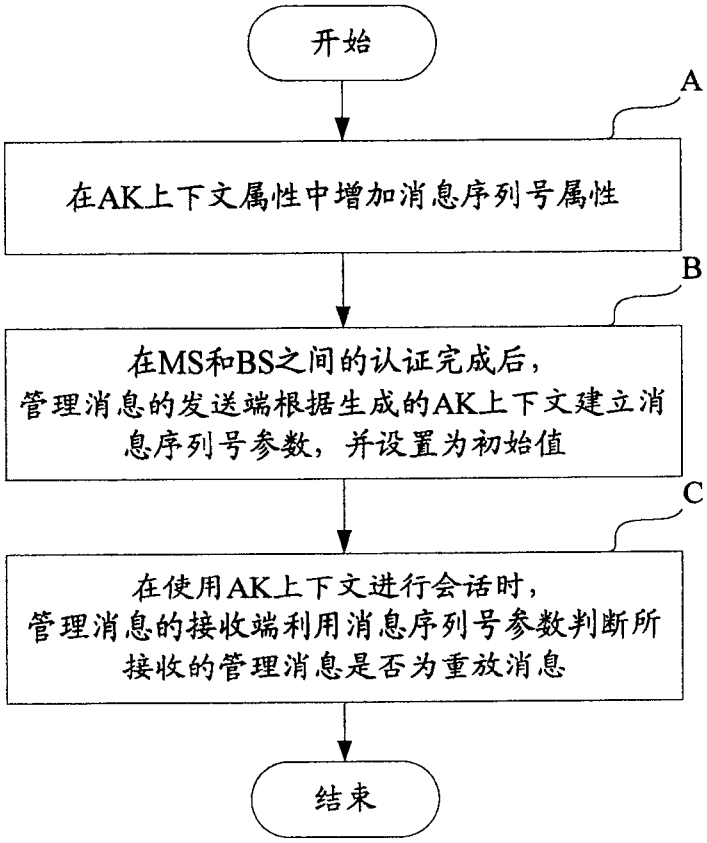

开始
A
在AK上下文属性中增加消息序列号属性
B
在MS和BS之间的认证完成后，
管理消息的发送端根据生成的AK上下文建立消息序列号参数，并设置为初始值
C
在使用AK上下文进行会话时，
管理消息的接收端利用消息序列号参数判断所接收的管理消息是否为重放消息
结束

图 1