[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/28
H04L 9/14 H04L 9/28

[12] 发明专利申请公开说明书

[21] 申请号 03121503.3

[43] 公开日 2004 年 10 月 6 日

[11] 公开号 CN 1534935A

[22] 申请日 2003.3.31 [21] 申请号 03121503.3

[71] 申请人 华为技术有限公司
地址 518057 广东省深圳南山区市科技园科发路 1 号华为用服中心大厦
[72] 发明人 黄迎新

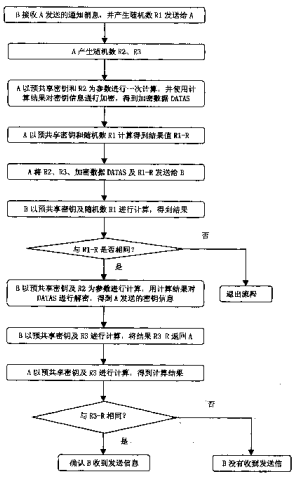
[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 李 强

权利要求书 2 页 说明书 5 页 附图 2 页

[54] 发明名称 一种基于预共享密钥的密钥分发方法

[57] 摘要

本发明涉及基于预共享密钥的密钥分发方法，包括：a、B 接收 A 发送的通知消息，产生随机数 R1 发送给 A；b、A 产生随机数 R2；c、A 以预共享密钥和随机数 R2 为输入参数产生一个加密密钥对要传送的对称密钥进行加密，得到加密后的数据 DATAS；d、A 以预共享密钥和随机数 R1 为输入参数计算得到结果值 R1 – R；e、A 将随机数 R2、加密的数据 DATAS 及结果值 R1 – R 发送给 B；f、B 以预共享密钥及随机数 R1 为参数进行计算，将计算结果和收到的 R1 – R 进行比较，若相同则进入步骤 g；若不同则进行异常处理，退出流程；g、B 以预共享密钥及随机数 R2 为参数进行计算，使用计算结果对 DATAS 进行解密，得到 A 发送的密钥信息。



ISSN1008-4274

知识产权出版社出版

1、一种基于预共享密钥的密钥分发方法，适用于已经设置了共享密钥的通信实体之间，其特征在于包括以下步骤:

a、通信实体 B 接收通信实体 A 发送的通知消息，并产生随机数 R1 发送给通信实体 A;

b、通信实体 A 产生随机数 R2;

c、通信实体 A 使用加密算法以预共享密钥和随机数 R2 为输入参数计算出一个加密密钥，并使用计算出的加密密钥对要传送的密钥信息进行加密，得到加密后数据 DATAS;

d、通信实体 A 使用加密算法以预共享密钥和随机数 R1 为输入参数计算得到结果值 R1-R;

e、通信实体 A 将随机数 R2、加密后数据 DATAS 及结果值 R1-R 发送给通信实体 B;

f、通信实体 B 使用加密算法以预共享密钥及随机数 R1 为参数进行计算，并将计算结果和收到的 R1-R 进行比较，若相同则进入步骤 g；若不同则进行异常处理，退出流程;

g、通信实体 B 使用加密算法以预共享密钥及随机数 R2 为参数进行计算，使用计算结果对 DATAS 进行解密，得到通信实体 A 发送的密钥信息。

2、如权利要求 1 所述的基于预共享密钥的密钥分发方法，其特征在于所述的步骤 b 还产生随机数 R3，所述的步骤 e 还包括把随机数 R3 发送给通信实体 B。

3、如权利要求 2 所述的基于预共享密钥的密钥分发方法，其特征在于还包括步骤:

h、通信实体 B 以预共享密钥及随机数 R3 为参数进行计算，并将计算结果 R3-R 返回给通信实体 A;

i、通信实体 A 以预共享密钥及随机数 R3 为参数进行计算，将计算结果与

R3-R 进行比较，判断通信实体 B 是否收到了通信实体 A 发送的密钥信息。

4、如权利要求 1、2 或 3 所述的基于预共享密钥的密钥分发方法，其特征在于所述的加密算法，为 HMAC_MD5。

5、如权利要求 1、2 或 3 所述的基于预共享密钥的密钥分发方法，其特征在于所述的加密算法，为 HMAC_SHA1。

6、如权利要求 1、2 或 3 所述的基于预共享密钥的密钥分发方法，其特征在于所述的通信实体可以为认证服务器、无线局域网的接入控制器、无线局域网的接入点或者其它无线接入终端。

一种基于预共享密钥的密钥分发方法

技术领域

本发明涉及加密领域及无线通信领域，尤其涉及一种基于预共享密钥的密钥分发方法。

技术背景

在无线局域网中，无线接入终端（STA）与无线局域网接入点（AP）之间的信息是通过无线传播的，因此STA与AP之间就存在很大的安全隐患，需要对传输的信息进行保密。要对信息进行保密，STA与AP之间就要共享密钥。目前有一种能够在STA与认证服务器之间通过交互某些不需要保密的数据而生成对称密钥的方法，这样STA就与认证服务器共享了密钥。认证服务器处的对称密钥需要安全的传递到AP以达到STA与AP共享密钥的目的。AP到认证服务器之间可以是直接连接，也可以是通过无线局域网接入控制器（AC）转接。直接连接时密钥需要在 认证服务器到AP之间传输。当为AC转接的方式时，密钥需要在 认证服务器到AC之间和AC到AP之间传输。 但目前没有安全协议来保证密钥安全传输，所以密钥从 认证服务器传递到AP时很容易被窃取，从而最终导致STA与AP间加密信息的泄漏。

两个通信实体在建网时就通过人工方式设置了对称密钥。它们之间要传送保密信息时，一端使用这个密钥加密，而另一端使用相同的密钥解密。一次单向的消息传递完成保密信息传送的过程。

这种方式只能进行简单的保密信息传送，传递保密信息的两端不能够进行互相确认，从而无法抵御中间人的攻击。

发明内容

本发明的目的就是解决通信实体之间密钥安全传递的问题

为此，本发明采用如下方案：

一种基于预共享密钥的密钥分发方法，适用于已经设置了共享密钥的通信实体之间，其包括以下步骤：

a、通信实体 B 接收通信实体 A 发送的通知消息，并产生随机数 R1 发送给通信实体 A；

b、通信实体 A 产生随机数 R2；

c、通信实体 A 使用加密算法以预共享密钥和随机数 R2 为输入参数计算出一个加密密钥，并使用计算出的加密密钥对要传送的密钥信息进行加密，得到加密后的数据 DATAS；

d、通信实体 A 使用加密算法以预共享密钥和随机数 R1 为输入参数计算得到结果值 R1-R；

e、通信实体 A 将随机数 R2、加密数据 DATAS 及结果值 R1-R 发送给通信实体 B；

f、通信实体 B 使用加密算法以预共享密钥及随机数 R1 为参数进行计算，并将计算结果和收到的 R1-R 进行比较，若相同则进入步骤 g；若不同则进行异常处理，退出流程；

g、通信实体 B 使用加密算法以预共享密钥及随机数 R2 为参数进行计算，使用计算结果对 DATAS 进行解密，得到通信实体 A 发送的密钥信息。

所述的步骤 b 还产生随机数 R3，所述的步骤 e 还包括把随机数 R3 发送给通信实体 B。

所述的基于预共享密钥的密钥分发方法，还包括步骤：

h、通信实体 B 以预共享密钥及随机数 R3 为参数进行计算，并将计算结果 R3-R 返回给通信实体 A；

i、通信实体 A 以预共享密钥及随机数 R3 为参数进行计算，将计算结果与 R3-R 进行比较，判断通信实体 B 是否收到了通信实体 A 发送的密钥信息。

所述的加密算法，为 HMAC_MD5。

所述的加密算法，为 HMAC_SHA1。

所述的通信实体可以为认证服务器、无线局域网的接入控制器、无线局域网的接入点或者其它无线接入终端。

根据本发明，通信实体之间能够互相确认身份、完成对传送密钥信息的加密、解密，从而能够安全的完成密钥的传递。

附图说明

图 1 是现有技术中 WLAN 网络结构示意图；

图 2 为本发明的流程图。

具体实施方式

下面结合说明书附图来说明本发明的具体实施方式。

如图 2 所示，是本发明的流程示意图，这种技术方案的前提是在通信实体之间已经安全的共享了密钥，即通信实体间有了预共享密钥。该通信实体可以是认证服务器、无线局域网的接入控制器、无线局域网的接入点或者其它无线接入终端。以通信实体分别为 AC 及 AP 为例，实现的方法步骤如下：

1 AC发送一条通知消息给AP，准备向AP发送秘密信息（密钥）。

2 AP收到通知消息后，产生一个随机数Random1发送给AC。

3 AC进行如下的处理

a) 产生随机数Random2， Random3。

b) 随机数Random2用于和预共享密钥一同加密要传送的密钥信息。首先使用HMAC_MD5或HMAC_SHA1算法进行计算（输入参数为预共享密钥和Random2），然后使用计算结果对密钥信息进行加密，得到加密数据DATAs。

c）AC使用HMAC_MD5或HMAC_SHA1算法函数，以预共享密钥及随机数Random1作为输入参数进行计算得出一个结果值Random1_Result。

d) AC将DATAs，Random1_Result，Random2 ，Random3一起发送给AP

4 AP收到AC发送的数据后，进行如下的处理:

a）AP使用HMAC_MD5或HMAC_SHA1算法函数，以预共享密钥及随机数Random1为参数进行计算，将得到的结果值和收到的Random1_Result进行比较，如果相同则验证了AC的身份，如果不同则进行异常处理。

b）AP使用HMAC_MD5或HMAC_SHA1算法函数，以预共享密钥及随机数Random2为参数进行计算，使用计算结果对收到的DATAs进行解密得到AC要发送的密钥信息。

c) AP使用HMAC_MD5或HMAC_SHA1算法函数，以预共享密钥及随机数Random3为参数进行计算，将计算的结果Random3_Result返回给AC。

5 AC收到AP的返回消息后，使用HMAC_MD5或HMAC_SHA1算法函数，以预共享密钥及随机数Random3进行同样的计算，将计算所得结果与收到的Random3_Result进行比较，如果相同则认为确实是AP收到了发送的密钥信息。

6 AC发送密钥信息到AP的过程完成。同理AP也可以将消息流程反过来发送保密信息到AC。

实施例1:

该实例中AC要将密钥发送给AP，这里，需要AC和AP具备如下功能:

产生随机数，使用HMAC_MD5或HMAC_SHA1进行计算

处理流程如下:

1、AC通知AP将要发送保密数据给AP;

2、AP收到该消息后产生一个随机数 Random1,并将Random1作为应答消息内容发送给AC;

3、AC使用Random1和预共享密钥作为选定算法的参数输入，计算出结果值Random1_Result以便AP确认AC身份。AC产生随机数Random2和Random3，使用Random2和预共享密钥对要传送的保密信息进行加密，产生密文数据DATAs。Random3用于对AP的身份进行确认。AC将Random1_Result、DATAs 、

Random2、 Random3作为消息内容发送给AP;

4、AP使用Random1_Result检验AC的身份，Random1和预共享密钥计算对DATAs数据解密取得数据。AP使用选取的算法以Random3和预共享密钥为参数计算出一个结果值Random3_Result，这个结果值作为AP确认消息的内容发送给AC。AC收到该消息后进行确认计算。

实施例2:

在无线局域网中，AC要发送密钥给AP。AC首先发送通知消息给AP，AP收到通知后产生一个随机数用于对AC的确认，并将这个随机数作为应答消息内容发送给AC。AC使用AP发来的随机数计算出一个待检验的结果，并产生两个随机数，一个用于加密一个用于检验AP，AC的计算完成后将计算的结果以及随机数发送到AP。AP首先检验AC的身份，然后解密数据取得密钥，并使用AC发来的随机数计算出一个结果值返回给AC，用于AC对确实是AP收到密钥的确认。

本专利提供的密钥传递的方法也可以应用到STA与AP之间。当对称密钥只在认证服务器产生而不是同时在STA与认证服务器同时产生时，认证服务器就要将对称密钥下发到STA。对称密钥传送到AP后，AP和STA使用本发明中的交互流程，就可以完成AP安全传送对称密钥到STA的过程。将这种密钥分发的方法和现有的WEP加密（也可以是更好的加密算法）相结合就可以来完成空中信息的保密。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求书的保护范围为准。

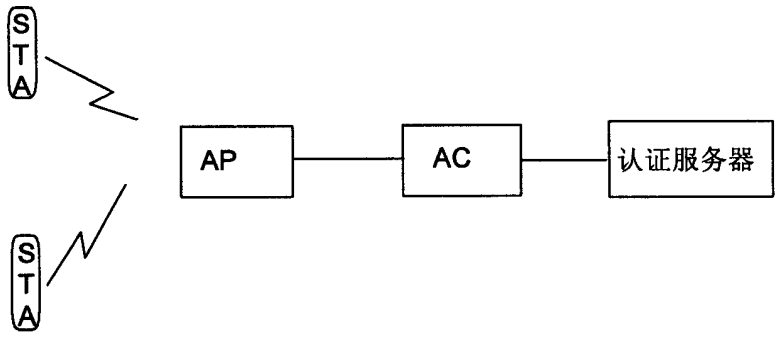


图 1

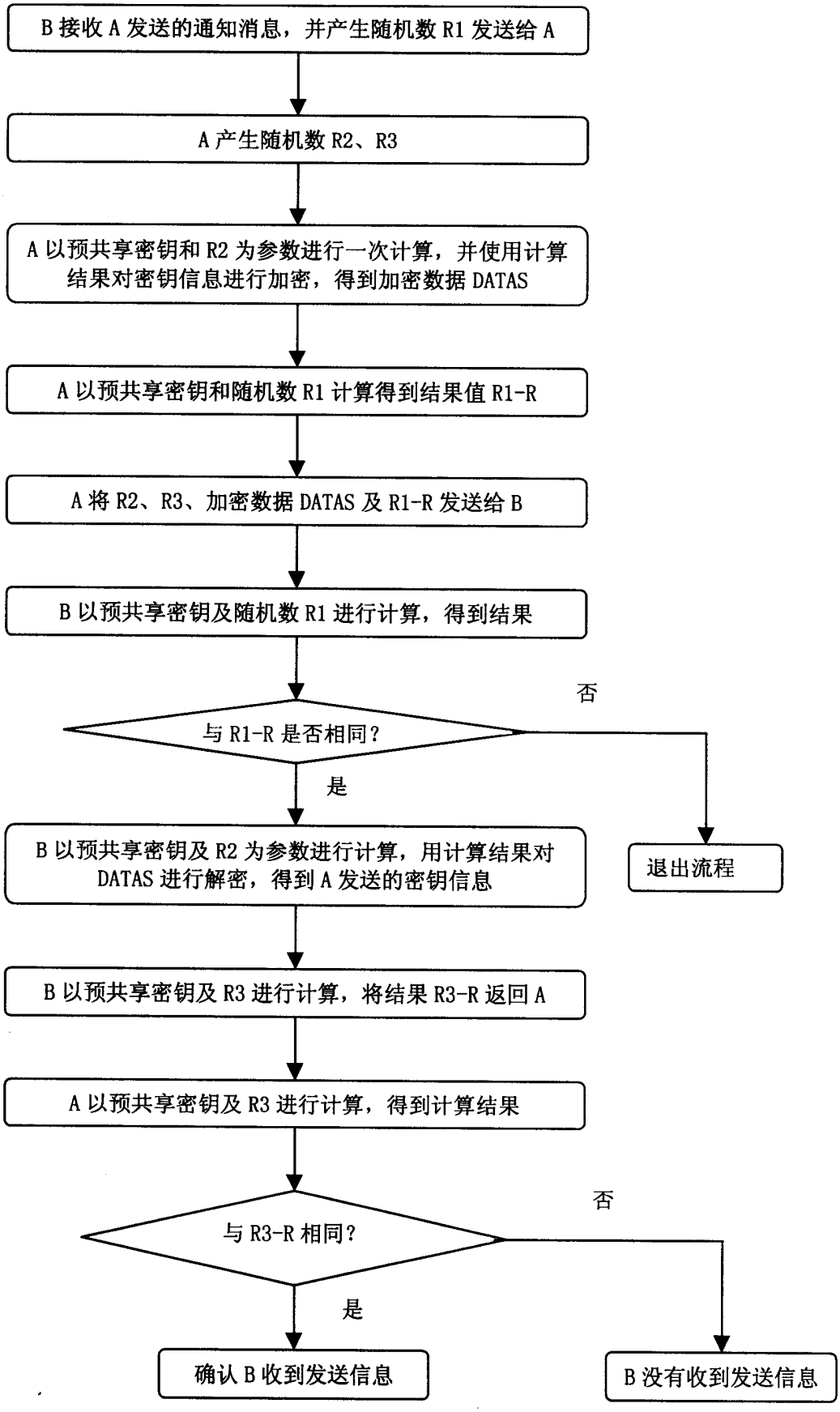

B 接收 A 发送的通知消息，并产生随机数 R1 发送给 A
A 产生随机数 R2、R3
A 以预共享密钥和 R2 为参数进行一次计算，并使用计算结果对密钥信息进行加密，得到加密数据 DATAS
A 以预共享密钥和随机数 R1 计算得到结果值 R1-R
A 将 R2、R3、加密数据 DATAS 及 R1-R 发送给 B
B 以预共享密钥及随机数 R1 进行计算，得到结果
与 R1-R 是否相同？
否
是
退出流程
B 以预共享密钥及 R2 为参数进行计算，用计算结果对 DATAS 进行解密，得到 A 发送的密钥信息
B 以预共享密钥及 R3 进行计算，将结果 R3-R 返回 A
A 以预共享密钥及 R3 进行计算，得到计算结果
与 R3-R 相同？
否
是
确认 B 收到发送信息
B 没有收到发送信息

图 2