高技术通讯 2009 年 第 19 卷 第 7 期:661 ~ 668

doi:10.3772/j.issn.1002-0470.2009.07.001

异构无线网络的认证算法①

谢胜东② 吴 蒙

(南京邮电大学通信与信息工程学院 南京 210003)

摘 要 本文针对建立在对等方式下的融合网络提出了一种新的认证和密钥更新算法。认证包括三个方面:非漫游状态下的完整认证、漫游状态下的完整认证以及切换状态下的快速认证。密钥更新包括两个方面:非漫游状态下的密钥更新和漫游状态下的密钥更新。在算法中,通过引入认证中心,不仅实现了网络对用户身份的认证,而且实现了节点对网络身份的认证,由此保证了双方身份的合法性;同时为了实现切换的无缝性,采用节点对认证数据包进行中继转发的方式,减少了切换时的认证时间。性能分析表明,该算法能够有效地抵御常见攻击。

关键词 异构无线网络,垂直切换,安全,认证,延时

0 引 言

超三代或第四代移动通信系统将是一种由蜂窝网、无线局域网(WLAN)或无线个人网等多种网络组成的融合网络,这种网络具有覆盖范围广、传输速率高等优点,同时能够满足用户在任何时间和任何地点都能够上网的需求。认证算法是融合网络中的研究热点,主要集中在如何设计一个安全的认证算法,以及减少切换过程中的认证时间[1]。本文针对异构无线网络提出了一种新的认证算法,该算法有良好的性能,能够保证整个网络的安全。

1 认证算法概况及本文算法的提出

一般情况下,每种网络都会采用一定的安全机制来保证网络中用户身份的合法性以及提供用户对网络的访问权限。例如,全球移动通信系统(GSM)采用了基于用户识别模块(SIM)的认证机制[2],通用移动通信系统(UMTS)采用了基于用户服务识别模块(USIM)的认证机制,而 802.11WLAN 采用了基于 802.1X 的认证机制。尽管不同网络的认证算法不相同,它们组成的融合网络垂直切换过程中的认证算法的基本结构却是相同的[3]。

文献[4]提出了一种基于 Hash 链的快速切换认证算法。用户在移动通信的过程中将进行两种形式的认证:完全认证和局部认证。该算法是建立在仅由一个 WLAN,一个 3G 访问网络以及一个 3G 家乡网络组成的混合网络的基础上。文献[5]提出了一种基于信任关系的快速切换认证算法。相互信任的网络之间共享与某个节点通信的主会话密钥,如果节点从一个网络切换到另外一个相互信任的网络时,它只需要进行快速认证,而当切换到其它不具有信任关系的网络时,节点则需要进行一次完整认证。文献[6]提出了一种基于证书的快速认证算法。节点从旧的访问点获得证书,用于证明节点身份的合法性,在切换到新网络时向新访问点提交该证书,在获得初步认证后节点便获得了访问该网络的权力,之后节点和访问点之间再进行一次完整的认证过程。以上算法都采用了将完全认证和局部认证相结合的方法,以减少切换延时。文献[7]利用移动管理协议,将与认证相关的环境信息从旧网关转移到新网关上,接着由新网关实现对移动节点的认证,减少了在新网络中通过家乡认证服务器进行认证的过程。文献[8]将移动 IP 中的 AAA(指鉴定、授权、管理)过程与会话发起协议(SIP)中的 AAA 过程进行综合优化,减少了整个认证过程中数据包的交换次数,它适用于同时采用移动 IP(MIP)和 SIP 的网络。文献[9]针对 UMTS 与 WLAN 组成的融合网络提出了一种提前注册和认证的切换算法,在节点进行第

① 863 计划(2006AA01Z208)资助项目。
② 男,1978 年生,博士生;研究方向:信息安全,无线通信;联系人,E-mail: xie_shd@sina.com
(收稿日期:2008-03-26)

二层切换之前先进行注册和认证,它有助于减少切换延时。

现有文献中的认证算法一般是采用某种方法实现网络对节点的认证,保证了节点身份的合法性。但是考虑到将来的异构网络是由多种不同网络组成的,它们之间的基本结合方式有以下三种:紧耦合方式、松耦合方式和对等方式[10]。前两种方式是欧洲通信标准协会针对无线局域网和 3G 进行融合提出的两种一般性的结合方式,这两种结合方式体现了一种主/从结构的网络构架,即以蜂窝网络作为主网络,而无线局域网作为从网络。在对等方式下,每种网络属于不同的网络管理者,它们之间通过 Internet 进行连接,主要是通过对各自网络进行适当更改,增加一些逻辑设备和签订漫游协议等方式来实现融合,AMC 构架[11]就是一种典型的以对等方式结合的异构网络。在对等方式下,网络之间不一定存在信任关系,甚至还存在恶意网络。节点在切换过程时,就不应该进入到这些恶意网络中。同时,在物理位置上相距较近的两个网络,若采用对等方式进行相连,它们之间的数据包一般是通过 Internet 进行交换,可能要通过多个中间路由器才能到达对方,这必然会导致较长的传输延时,影响切换的性能。

本文针对建立在对等方式下的融合网络提出了一种新的认证和密钥更新算法,其中认证过程包括非漫游状态和漫游状态下的完整认证以及切换状态下的快速认证三个方面,密钥更新包括两个方面:非漫游状态下的密钥更新和漫游状态下的密钥更新。在算法中,当节点需要切换到新网络时,首先由旧网络实现对新网络的身份认证,这种认证是通过证书进行的。当对新网络的认证成功之后,旧网络将节点对网络资源使用权限以及一些挑战信息等环境信息通过移动节点转发给新网络,同时设定新网络与节点之间的会话密钥,并分别传送给移动节点以及新网络。新网络在得到环境信息后对节点进行认证。本文的创新之处在于:在安全性上,不仅保证移动节点身份的合法性,而且保证了网络身份的合法性;在认证时间上,通过移动节点对数据包进行中继,减少了数据包通过 Internet 的传输延时,提高了切换过程的速度。

2 混合网络构架

在设计认证算法之前,我们首先建立一个简单的混合网络模型,如图 1 所示,不同网络之间采用对等方式结合在一起。在该模型中,我们没有指明每种网络具体采用何种通信标准,也没有将每种网络中的具体设备画出,图中只是画出了与我们所要讨论的认证算法相关的一些逻辑上的设备,这有利于具体认证算法的设计。同时我们假设每种网络都属于不同的网络管理者,那么发生的切换都属于垂直切换,在垂直切换过程中必然要进行一系列的认证与密钥协商过程,以保证整个通信系统的安全。

节点在移动的过程中,主要涉及到三种不同性质的网络:家乡网络,即用户注册登记时的网络,图中标记为 Home;当前网络,即用户当前正在使用的网络,在图中标记为 Pre,如果节点通过家乡网络进行通信,那么家乡网络也就是当前网络;候选网络,即用户切换之后所要使用的网络,与 Pre 相对应,图中标记为 New。这三种网络是我们要研究的对象,因此,在图中只画出了这三种网络。同时我们认为发生切换时所涉及到的两个网络在节点切换处有一定的重叠区域,我们称之为切换区域,在切换区域,节点可以和两个网络进行通信。

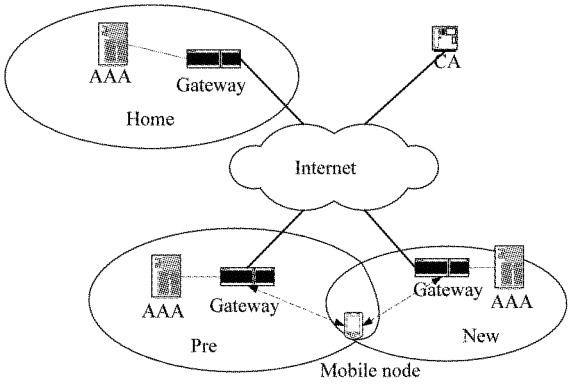

图 1 网络模型

由于不同的网络属于不同的网络管理者,因此每一个网络中都存在一个认证服务器,网络通过网关与 Internet 相连。同时我们注意到,在整个混合网络中,还存在着一个认证中心(certification authority, CA),它负责为每个向其注册的网络颁发证书。每个网络用认证中心颁发的证书来表明自己身份的合法性,凡具有证书的网络都是合法网络,凡没有获得认证中心颁发证书的网络都认为是非法网络。

每个认证服务器上都保存着认证中心的公有密钥。当一个网络向另一个网络证明自己身份时,它必须向对方提供通过自身私有密钥加密过的证书及其公有密钥,对方认证服务器利用接收到的公有密钥对证书解密后,可凭借证书上认证中心的数字签名来判定证书的真伪。若证书为真,且证书上的公

有密钥与接收到的公有密钥一致时,那么可以判定拥有该证书的网络是合法网络。同时,每个认证服务器都具有密钥产生功能,它可以直接为节点与新网络之间设置通信密钥,免去它们之间为了获得通信密钥而需要进行一系列的密钥协商过程。

同时,每个认证服务器都必须具备一份用户密钥表(如表 1)。里面存放着向该网络注册的所有节点的会话密钥,用以记录它们是否已经及时更新了会话密钥,如果是否同步栏中标记为 Y,表明节点已经进行了密钥同步,那么表中会话密钥值将等于新会话密钥,如果标记为 N,表明节点还没有进行密钥同步,那么表中会话密钥值将不等于新会话密钥。

表 1 用户密钥表

节点身份	新会话密钥	会话密钥	是否同步
ID_{node}	k_{home_new}	k_{home}	Y/N
⋮	⋮	⋮	⋮

3 认证算法

与文献[4],[5],[6]相似,本文中节点的一次通信同样要经历两种不同类型的认证过程:完整认证和局部认证。完整认证是节点在通信起始时刻要进行的认证过程,这个认证是必需的;而局部认证只发生在节点从一个网络切换到另外一个网络的过程中,该认证过程所需要的时间越短越好。

首先,定义一些变量以及表达式,其含义如下:

k_{home} :移动节点与 Home 网络的会话密钥,它是节点与 Home 认证服务器之间共享的。

k_{home_new} :移动节点与 Home 网络的新会话密钥,由 Home 认证服务器产生,在通知移动节点更新密钥之后, $k_{home} = k_{home\_new}$。

k_{pre} :移动节点与 Pre 网络的会话密钥。当前网络如果是 Home 网络,那么 $k_{pre} = k_{home}$。

k_{new} :移动节点与 New 网络之间的会话密钥。

CI_{node} :移动节点对网络的访问权限的信息资料。

$ID_{node}, ID_{home}, ID_{pre}, ID_{new}$:移动节点、Home 网络、Pre 网络以及 New 网络的身份。

$SK_{home}, SK_{pre}, SK_{new}$: Home 网络,Pre 网络以及 New 网络的私有密钥。

$PK_{home}, PK_{pre}, PK_{new}$: Home 网络,Pre 网络以及 New 网络的公有密钥。

$Cred_{home}, Cred_{pre}, Cred_{new}$: Home 网络,Pre 网络以及 New 网络的证书。

$Addr_{home}, Addr_{pre}, Addr_{new}$: Home 网络,Pre 网络以及 New 网络的地址。

r, s: 随机值。

$E_X(Y)$: 采用密钥 X 对数据 Y 进行对称加密。

$PKI_X(Y)$: 采用密钥 X 对数据 Y 进行非对称加密。

3.1 完全认证过程

节点在开始进行一次通信前,要进行一次完整认证,它包含两种情况:非漫游状态下的完整认证过程和漫游状态下的完整认证过程。一般情况下,我们认为移动节点知道家乡网络的公开密钥。

3.1.1 非漫游状态下的完整认证过程

该认证过程比较简单,信息交换如图 2 所示。

M_1: 移动节点产生随机数 s, 计算 $E_{k_{home}}(s)$, 向 Home 网关申请接入,提交 ID_{node} 和 s 。

M_2: Home 网关向认证服务器请求对节点进行认证,将 ID_{node} 和 s 转发给认证服务器。

M_3: 认证服务器产生随机数 r, 根据 ID_{node} 从用户密钥表中查找新会话密钥 k_{home_new}, 旧会话密钥 k_{home} 以及是否更新栏中的状态,我们假设是否更新栏状态为 Y, 它表明移动节点已经知道新会话密钥,并且已经用 k_{home_new} 的值更新了 k_{home} 的值,同时对应的用户密钥表中 k_{home} 的值也等于 k_{home_new} 的值。于是计算 $E_{k_{home}}(r)$ 和 $E_{k_{home}}(s)$, 并将 $E_{k_{home}}(s)$ 和立即数 r 一起发送给网关;对于是否更新栏状态为 N 的情况,它表明移动节点还不知道新会话密钥,我们将在后面的密钥更新过程部分进行讨论。

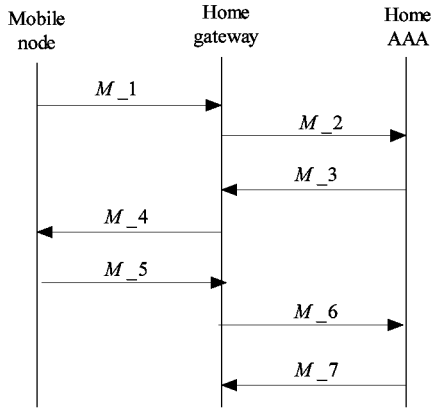

图 2 非漫游状态下的完整认证

M_4: 网关将立即数 r 和 $E_{k_{home}}(s)$ 转发给移动节点。

M_5：移动节点比较接收到的数据 $E_{k_{home}}(s)$ 是否等于自己计算出的 $E_{k_{home}}(s)$，如果相等，表明家乡网络是合法的，接着移动节点用会话密钥 k_{home} 对 r 进行加密后传递给网关。

M_6：网关将收到的数据转交给认证服务器。

M_7：服务器比较接收到的数据是否等于 $E_{k_{home}}(r)$，如果相等就向网关发送接受节点的信息，同时将节点的访问权限信息 CI_{node} 以及会话密钥 k_{home} 发送给网关；否则发送拒绝信息。

至此，一个完整的认证过程结束，节点和 Home 网关之间可以采用密钥 k_{home} 进行通信。

3.1.2 漫游状态下的完整认证

由于移动，用户可能会在漫游到非家乡网络的时候发起会话，在这种情况下的完整认证过程就比较复杂，因为非家乡网络的认证服务器中没有用户的资料，同时节点也不知道该网络是否是一个合法网络。以图 1 为例，假设用户在标记为 pre network 的非家乡网络中发起通信请求，则整个认证过程的信息交换如图 3 所示。

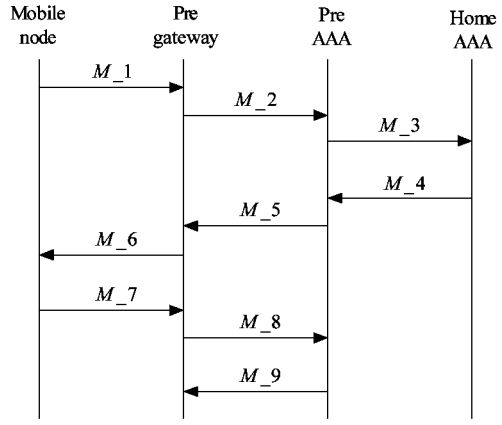

图 3 漫游状态下的完整认证

M_1：移动节点产生随机数 s，向 Pre 网关申请接入，发送信息 $E_{K_{home}}(s) \| ID_{node} \| Addr_{home} \| Pk_{home}$ 给 Pre 网关。

M_2：Pre 网关向 Pre 认证服务器请求对节点进行认证，将信息 $E_{K_{home}}(s) \| ID_{node} \| Addr_{home} \| Pk_{home}$ 转发给 Pre 认证服务器。

M_3：Pre 服务器利用节点提供的家乡网络的地址 $Addr_{home}$ 发送信息 $PKI_{PK_{home}}(PKI_{SK_{pre}}(Cred_{pre}) \| PK_{pre} \| ID_{node} \| ID_{pre} \| E_{K_{home}}(s))$ 给 Home 服务器。

M_4：Home 认证服务器通过证书对 Pre 网络的身份进行认证，如果 Pre 网络不合法，就发送拒绝信息；如果合法，Home 认证服务器则根据节点 ID_{node} 从用户密钥表中查找新会话密钥 k_{home_new}，旧会话密钥 k_{home} 以及是否更新栏中的状态。我们假设是否更新栏状态为 Y，对于为 N 的情况，它表明节点还不知道新会话密钥，我们将在后面的密钥更新过程部分进行讨论。Home 认证服务器接着产生立即数 r，生成节点与 Pre 网络的会话密钥 k_{pre}，并向 Pre 认证服务器发送 $PKI_{Sk_{pre}}(PKI_{SK_{home}}(Cred_{home}) \| PK_{home} \| ID_{node} \| ID_{home} \| E_{K_{home}}(r) \| K_{pre} \| E_{K_{home}}(r \| s \| K_{pre}) \| CI_{node})$。

M_5：Pre 认证服务器通过证书对 Home 网络的身份进行认证；如果 Home 网络合法，那么 Pre 认证服务器向 Pre 网关发送 $E_{K_{home}}(r \| s \| K_{pre}) \| PK_{pre}$。

M_6：网关将收到的数据 $E_{K_{home}}(r \| s \| K_{pre}) \| PK_{pre}$ 转交给移动节点。

M_7：移动节点利用密钥 K_{home} 从收到的数据中提取出随机数 r、s 以及会话密钥 K_{pre}，并记下 Pre 网络的公开密钥，这个密钥将用于切换认证过程中。如果 s 是节点在 M_1 时产生的，那么表明 Home Network 已经对 Pre Network 进行了身份验证，其身份合法。接着将 $E_{K_{home}}(r)$ 发送给 Pre 网关。

M_8：网关将收到的数据 $E_{K_{home}}(r)$ 转交给认证服务器。

M_9：服务器比较接收到的数据是否等于来自于 Home 认证服务器的 $E_{k_{home}}(r)$，如果相等就向网关发送接收信息，同时将节点的访问权限信息 CI_{node} 发送给网关；否则发送拒绝信息。

至此，一个完整的认证过程结束，节点和 Pre 网关之间可采用会话密钥 K_{pre} 进行通信。

3.2 发生切换时的局部认证

用户在移动过程中，不可避免地会发生切换。当用户从一个管理者管理的网络切换到另外一个管理者管理的网络时，为了保证整个混合网络的安全，必须再次进行认证。然而这个认证过程的时间不能太长，否则会影响某些实时应用程序的通信质量。以图 1 为例，假设节点准备从 Pre 网络切换到 New 网络，则整个认证过程的信息交换如图 4 所示。

M_1：移动节点产生随机数 s，向 New 网关申请接入，发送信息 $E_{K_{pre}}(s) \| ID_{node} \| Addr_{pre} \| PK_{pre}$；

M_2：网关向 New 认证服务器请求对节点进行认证，将信息 $E_{K_{pre}}(s) \| ID_{node} \| Addr_{pre} \| PK_{pre}$ 转发给认证服务器；

M_3:New服务器将信息$PKI_{PK_{pre}}(PKI_{SK_{new}}(Cred_{new})\|PK_{new}\|ID_{node}\|ID_{new}\|E_{K_{pre}}(s))$发送给New网关;

M_4:网关将收到的信息$PKI_{PK_{pre}}(PKI_{SK_{new}}(Cred_{new})\|PK_{new}\|ID_{node}\|ID_{new}\|E_{K_{pre}}(s))$转交给移动节点;

M_5:节点将数据包$PKI_{PK_{pre}}(PKI_{SK_{new}}(Cred_{new})\|PK_{new}\|ID_{node}\|ID_{new}\|E_{K_{pre}}(s))$转交给Pre网关。因为此时节点处于切换区域中,可以和两个网络进行通信。

M_6:Pre网关将数据包$PKI_{PK_{pre}}(PKI_{SK_{new}}(Cred_{new})\|PK_{new}\|ID_{node}\|ID_{new}\|E_{K_{pre}}(s))$转交给Pre认证服务器。

M_7:Pre服务器通过证书对New网络进行身份认证;如果New网络合法,服务器则产生立即数r和节点与New网络的通信密钥k_{new},接着认证服务器向网关发送$PKI_{PK_{new}}(PKI_{SK_{pre}}(Cred_{pre})\|PK_{pre}\|ID_{node}\|ID_{pre}\|E_{K_{pre}}(r)\|K_{new}\|E_{K_{pre}}(r\|s\|K_{new})\|CI_{node})$;否则发送拒绝信息;

M_8:Pre网关将收到的数据转发给移动节点;

M_9:移动节点再将收到的数据转发给New网关;

M_10:New网关将收到的数据转发给New认证服务器;

M_11:New认证服务器通过证书对Pre网络的身份进行认证;如果Pre网络合法,那么New认证服务器向New网关发送$E_{K_{pre}}(r\|s\|K_{new})\|PK_{new}$;

M_12:网关将收到的数据$E_{K_{pre}}(r\|s\|K_{new})\|PK_{new}$转交给移动节点;

M_13:移动节点从收到的数据中提取出随机数r和s及会话密钥K_{new},如果s是节点M_1时产生的,那么表明Pre Network已经对New Network进行了身份验证,其身份合法。接着将$E_{K_{pre}}(r)$发送给Pre网关。

M_14:网关将收到的数据$E_{K_{pre}}(r)$转交给认证服务器;

M_15:服务器比较接收到的数据是否等于来自于Pre认证服务器的$E_{k_{pre}}(r)$,如果相等就向网关发送接收信息,同时将节点的访问权限信息发送给网关CI_{node};否则发送拒绝信息。

至此,一个切换过程中的快速认证过程结束,移动节点和New网关之间可以采用会话密钥K_{new}进行安全的通信。如果无线网络本身不稳定,使得认证服务器之间的密钥不同步,这必然会导致切换过程时的认证失败。遇到这种情况,节点只需再进行一次完整认证过程,便可以达到认证服务器之间密钥同步的目的。

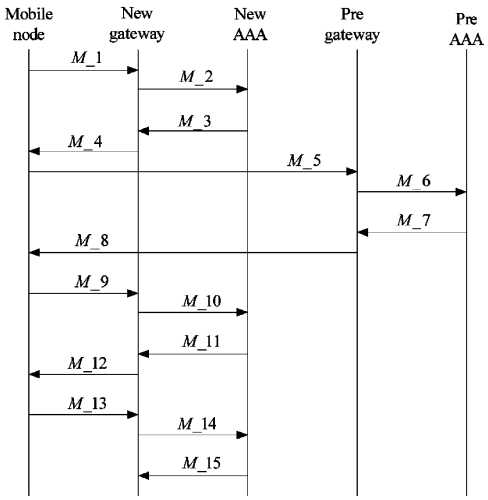

图4 切换过程中的快速认证

4 密钥对更新过程

为了保证网络的安全,移动节点与Home网络之间的会话密钥k_{home}应当定期更新。在Home认证服务器将会话密钥更新成k_{home_new}后,它必须及时通知移动节点。我们从前面认证过程可以看到,在切换过程中,Home网络不参与认证,即切换认证对Home网络是透明的,因此密钥对同步过程只是发生在完整的认证过程之中。

4.1 非漫游状态下的密钥对更新过程

该过程如图5所示,图中虚线表示与图2的不同之处。

M_1与M_2与非漫游状态下的完整认证过程一样。

M_3:认证服务器产生随机数r,根据ID_{node}从用户密钥表中查找新会话密钥k_{home_new},旧会话密钥k_{home}以及是否更新栏中的状态,我们假设是否更新栏状态为N,它表明移动节点还不知道新会话密钥。服务器计算$E_{k_{home}}(r)$和$E_{k_{home}}(s)$,并将$E_{k_{home}}(s)$和立即数r一起发送给网关。

M_4:网关将立即数r和$E_{k_{home}}(s)$转发给移动节点。

M_5：移动节点比较接收到的数据 $E_{k_{\text{home}}}(s)$ 是否等于自己计算出的 $E_{k_{\text{home}}}(s)$，如果相等，表明家乡网络是合法的，接着移动节点用会话密钥 k_{home} 对 r 进行加密后传递给网关。

M_6：网关将收到的数据转交给认证服务器。

M_7：服务器比较接收到的数据是否等于 $E_{k_{\text{home}}}(r)$，如果不相等，则发送拒绝信息；如果相等，则将 $E_{k_{\text{home}}}(k_{\text{home\_}new})$ 发送给网关。

M_8：网关将 $E_{k_{\text{home}}}(k_{\text{home\_new}})$ 转发给移动节点。

M_9：移动节点提取新会话密钥 $k_{\text{home\_new}}$，用来代替 k_{home}，代替后的 k_{home} 的值将等于 $k_{\text{home\_new}}$ 的值。接着用会话密钥 k_{home} 对 r 进行加密后传递给网关。

M_10：网关将接收到的数据转交给认证服务器。

M_11：服务器比较接收到的数据是否等于自己计算出的 $E_{k_{\text{home\_new}}}(r)$ 值，如果相等表明节点已经更新了会话密钥，于是向网关发送接受节点的信息，同时将节点的访问权限信息 CI_{node} 以及会话密钥 $k_{\text{home\_new}}$ 发送给网关，并将对应的用户密钥表的是否同步栏中置为 Y，同时将 $k_{\text{home\_new}}$ 值赋给 k_{home}，这样表中的会话密钥值就等于新会话密钥；如果不相等，表明节点可能没有收到更新后的密钥，于是跳转到第 M_8 步重新执行密钥对更新过程。

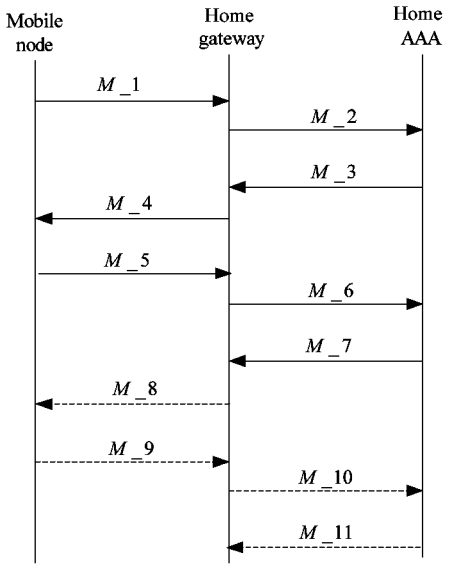

图 5 非漫游状态下的密钥对更新过程

4.2 漫游状态下的密钥对更新过程

该过程如图 6 所示，图中虚线表示与图 3 的不同之处。

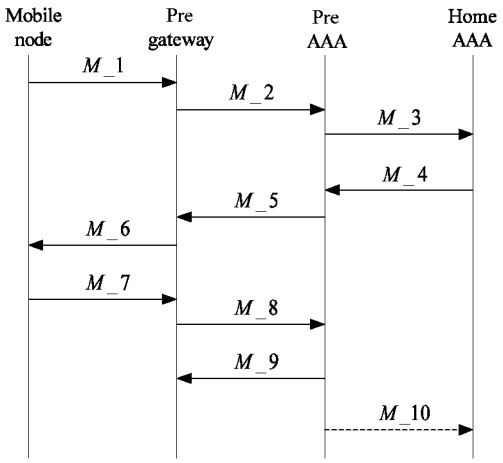

图 6 漫游状态下的密钥对更新过程

M_1 到 M_3 都与漫游状态下的完整认证过程一样。

M_4：Home 认证服务器通过证书对 Pre 网络的身份进行认证；如果 Pre 网络不合法，则发送拒绝信息；如果合法，Home 认证服务器则根据节点 ID_{node} 从用户密钥表中查找会话密钥 k_{home}、$k_{\text{home\_new}}$ 以及是否同步栏中的标记，如果标记值为 N，表明节点还没有进行密钥更新，应当立即让移动节点进行密钥更新，在这种情况下 $k_{\text{home\_new}}$ 的值不一定等于 k_{home}。Home认证服务器发送信息 $PKI_{Sk_{\text{pre}}}(PKI_{SK_{\text{home}}}(Cred_{\text{home}}) \| PK_{\text{home}} \| ID_{\text{node}} \| ID_{\text{home}} \| E_{K_{\text{home\_new}}}(r) \| K_{\text{pre}} \| E_{K_{\text{home}}}(r \| s \| K_{\text{pre}} \| K_{\text{home\_new}}) \| CI_{\text{node}})$ 给 Pre 认证服务器。

M_5：Pre 认证服务器通过证书对 Home 网络的身份进行认证；如果 Home 网络合法，那么 Pre 认证服务器向 Pre 网关发送 $E_{K_{\text{home}}}(r \| s \| K_{\text{pre}} \| K_{\text{home\_new}})$。

M_6：网关将收到的数据 $E_{K_{\text{home}}}(r \| s \| K_{\text{pre}} \| K_{\text{home\_new}})$ 转交给移动节点。

M_7：移动节点利用密钥 K_{home} 从收到的数据中提取出随机数 r、s、会话密钥 K_{pre} 以及与家乡网络的新会话密钥 $K_{\text{home\_new}}$，记下 Pre 网络的公开密钥，同时用 $K_{\text{home\_new}}$ 来代替 k_{home}，此时 k_{home} 的值将等于 $k_{\text{home\_new}}$ 的值。如果 s 是节点在 M_1 时产生的，那么表明 Home Network 已经对 Pre Network 进行了身份验证，其身份合法。接着用新的 k_{home} 对 r 加密后发送给 Pre 网关。

M_8：网关将受到的数据 $E_{K_{\text{home}}}(r)$ 转交给认证服务器。

M_9:服务器比较接收到的数据是否等于来自于 Home 认证服务器的 $E_{k_{home\_new}}(r)$,如果相等就向网关发送接收信息,同时将节点的访问权限信息 CI_{node} 发送给网关;否则发送拒绝信息,且不执行 M_10。

M_10:Pre 认证服务器向 Home 认证服务器发送节点已经更新其与家乡网络之间的会话密钥的消息。Home 认证服务器在收到该消息之后,将对应的用户密钥表的是否同步栏中置为 Y,同时将 k_{home_new} 值赋给 k_{home}。

从上面的分析过程中,我们看到,密钥对更新过程是穿插在完整认证过程中进行的,但每个设备可以根据其处理的数据包的长度以及内容来判断当前是处于哪个过程之中,并执行相应的动作。

5 协议安全性分析

这部分将对本文所提认证算法进行安全性分析,即分析该算法是否能够防止一些常见性的网络攻击,包括猜测攻击、回放攻击、伪造攻击和中间人攻击。

在对网络身份进行认证时,采用的是证书验证方式。该混合网络中存在一个每个网络都认可的认证中心,每一个认证服务器上都保存着认证中心的公有密钥。当一个网络向另外一个网络证明自己身份时,它必须向对方提供用自身私有密钥加密过的证书及相应的公有密钥,对方认证服务器通过接收到的公有密钥对证书解密后,可以凭借证书上认证中心的数字签名来判定证书的真伪。若证书为真,同时证书上的公有密钥与接收到的公有密钥一致时,那么可以判定拥有该证书的网络是合法网络。从图 3 和图 4 中我们发现,无论时 Pre 网络还是 New 网络,它们之间都需要向对方递交证书以证明自己身份的合法性。在图 4 中,当 Pre 网路信任 New 网络时才会将节点对网络的访问权限信息 CI_{node} 传递给 New 网络,同时会通过 New 网络向移动节点发送包含信任 New 网络信息的数据包。当 New 网络通过证书对 Pre 网络验证并相信 Pre 网络后,才会进一步对移动节点的身份进行认证。

猜测攻击:在图 2、图 3 的认证过程中,用户与家乡网络之间共享的会话密钥 k_{home} 没有以任何形式出现在传输链路上,只要其足够长,攻击者就很难在较短的时间内猜测出该密钥。对于图 3 和图 4 认证过程中产生的会话密钥 k_{pre} 以及 k_{new},尽管其出现在传输链路上,但它是经过加密的,而且从图中我们可以看到,在与一个网络的一次通话过程中,该密钥只使用一次。攻击者即使获得了该密钥也没有太大意义。

回放攻击:在图 2、图 3 和图 4 的认证过程中,当网络需要认证节点身份时,采用的是挑战认证方式,随机数 r 是一次性的,采用随机数的挑战认证方式可以避免回放攻击。在图 4 的认证过程中,Pre 认证服务器和 New 认证服务器之间的数据是通过移动节点进行转发的。如果存在恶意节点对接收到的数据包进行回放攻击,如第 M_5 步,但数据包中的随机数 s 是一次性的,其加密后的数据 $E_{K_{pre}}(s)$ 值也将是一次性的,如果在较短的时间内 Pre 认证服务器发现接收到的数据中又有 $E_{K_{pre}}(s)$,可以认为遭受到了回放攻击而不予理睬。即使回放攻击没有被 Pre 认证服务器察觉,我们从 M_13 中看到,由于恶意节点没有善意节点与 Pre 网络间的通信密钥 k_{pre},它也无法从数据包中提取出善意节点与 New 网络间的会话密钥 k_{new}。

伪造攻击:假设存在一个恶意节点伪装成一个善意节点准备对网络进行访问,但是由于恶意节点中没有善意节点与家乡网络通信的会话密钥 k_{home};在图 2 和图 3 中,网络通过挑战认证方式很容易发现恶意节点的身份;在图 4 中,尽管没有用到密钥 k_{home},但是在挑战认证过程中用到了会话密钥 k_{pre},从图 3 中可以发现,该会话密钥只有当节点拥有密钥 k_{home} 时才能获得。

中间人攻击:从非漫游状态下和漫游状态下的完整认证过程和切换时的快速认证过程中,我们可以看到,用户在家乡网络发起通话请求时,不仅实现了网络对用户的认证,而且实现了用户对网络的认证;如果用户在非家乡网络发起通话请求,则首先进行家乡网络与访问网络间的双向认证,接着再由访问网络实现了对移动节点的认证;对于用户在切换过程中发起认证,则首先实现当前网络实现与新网络间的双向认证,接着由新网络实现对节点的认证。这些认证过程既保证了网络的合法,也保证了用户的合法,可以有效的防止中间人攻击。

6 结 论

本文针对异构无线网络提出了一种新的认证和密钥更新算法。认证包括三个方面:非漫游状态下的初始完整认证、漫游状态下的初始完整认证以及

切换状态下的快速认证。密钥更新包括两个方面：非漫游状态下的密钥更新和漫游状态下的密钥更新。在认证过程中，如果用户在家乡网络发起通话请求，则网络和用户采用挑战认证方式实现双向认证；如果用户在非家乡网络发起通话请求，则首先通过家乡网络实现对访问网络的认证，接着再由访问网络实现对移动节点的认证；如果用户在切换过程中发起认证，则首先通过当前网络实现对新网络的认证，接着由新网络实现对节点的认证。在切换过程中，考虑到两个网络之间的信息交换如果通过 Internet 进行传输，可能会导致很大的延时，对实时性要求较高的应用程序产生影响，因此，本文利用移动节点的中继对两网络之间的数据包进行转发。最后，对认证算法的安全性进行了分析，分析表明，该算法具有良好的性能，能够保证整个网络的安全。

参考文献

[1] Karopoulos G, Kambourakis G, Gritzalis S. Survey of secure handoff optimization schemes for multimedia services over all IP wireless heterogeneous networks. *IEEE Communications Survey & Tutorials*, 2007, 9(3):18-28

[2] LEE C C, Hwang M S, Yang W P. Extension of authentication protocol for GSM. *IEE Proc-Commun*, 2003, 150(2): 91-95

[3] Braun T, Kim H. Efficient authentication and authorization of mobile users based on peer to peer network mechanisms. In: Proceedings of the 38th Hawaii International Conference on System Sciences, Big Island, Hawaii, USA, 2005.306-311

[4] Yang C C, Yang Y W, Liu W T. A robust authentication protocol with non-repudiation service for integrating WLAN and 3G network. *Wireless Personal Communications*, 2006, 39: 229-251

[5] Hassan J, Sirisena H, Landfeldt B. Trust-based fast authentication for multi-owner wireless networks. *IEEE Transactions on Mobile Computing*, 2008, 7(2): 247-261

[6] Aura T, Roe M. Reducing reauthentication delay in wireless networks. In: Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, Athens, Greece, 2005. 139-148

[7] Georgiades M, Akhtar N, Politis C, et al. AAA context transfer for seamless and secure multimedia services over all IP infrastructures. In: Proceedings of the 5th European Wireless Conference, Barcelona, Spain, 2004. 213-218

[8] Xu P, Liao J X, Wen X P, et al. Optimized integrated registration procedure of mobile IP and SIP with AAA operations. In: Proceedings of the 20th International Conference on AINA, Vienna, Austria, 2006. 926-931

[9] Choi H H, Song O, Cho D H. Seamless handoff scheme based on pre-registration and pre-authentication for UMTS-WLAN inter-working. *Wireless Personal Communications*, 2007, 41: 345-364

[10] Varma V K, Ramesh S, Wong K D, et al. Mobility management in integrated UMTS/WLAN networks. *IEEE international Conference on Communications*, 2003, (2):1048-1053

[11] Mohanty S, Xie J. Performance analysis of a novel architecture to integrate heterogeneous wireless systems. *Computer Networks*, 2007, 51: 1095-1105

An authentication algorithm for heterogeneous networks

Xie Shengdong, Wu Meng

(Communication and Information Engineering Institute, Nanjing University of Posts and Telecommunications, Nanjing 210003)

Abstract

This paper proposes an authentication and key-update algorithm for heterogeneous wireless networks which are based on the peer to peer network architecture. The authentication includes three aspects: the full authentication in the state of non-roaming, the full authentication in the state of roaming, and the local fast authentication in the state of handoff. The key-update includes two aspects: the update in the state of non-roaming and the update in the state of roaming. A certification authority is introduced, and thus not only a node could authenticate a new network, but also a new network could authenticate a node. In order to reduce the authentication time during handoff, the algorithm makes nodes relay the authentication packets between two networks. The analyses of the authentication protocol from some aspects show that the algorithm could defense the common attacks effectively.

Key words: heterogeneous wireless networks, vertical handoff, security, authentication, delay