异构无线网络中基于自更新哈希链的不可否认性计费协议

陈守国[1] 付安民[1,2] 秦宁元[1]
(南京理工大学计算机科学与工程学院 南京 210094)[1]
(中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)[2]

摘 要 异构无线网络融合是下一代网络发展的必然趋势,UMTS、LTE、WiMAX和WiFi等无线网络既相互竞争,又相互补充。安全计费是异构无线网络商用面临的主要挑战。提出了一种在异构网络中基于自更新哈希链的不可否认性计费协议,即通过采用新颖的自更新哈希链,移动终端能够快速更新可用哈希链,保证连续的快速认证。提出的方案能够提供解决计费纠纷的证据,实现计费的不可否认性、机密性和准确性。理论分析和性能仿真表明,提出的方案具有计算开销低、通信时延小等优势,满足异构无线网络的性能要求。

关键词 安全计费,不可否认性,异构无线网络,自更新哈希链
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.023

Non-repudiable Billing Protocol Based on Self-updating Hash Chain for Heterogeneous Wireless Networks

CHEN Shou-guo[1] FU An-min[1,2] QIN Ning-yuan[1]
(School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)[1]
(State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)[2]

Abstract The integration of heterogeneous wireless networks (HWNs) is an inevitable trend in the development of next-generation networks. UMTS, LTE, WiMAX, WiFi and other wireless networks compete and cooperate mutually. Secure billing is the primary challenge faced by the commercialization of HWNs. We proposed a non-repudiable billing protocol based on the self-updating hash chain for HWNs. By using the novel self-updating hash chain technology, mobile stations (MS) can quickly update available hash chain which ensures continuous fast authentication. The proposed protocol provides the evidence to solve billing disputes, therefore, it achieves non-repudiation, confidentiality and accuracy in billing. Moreover, the theoretical analysis and performance simulation demonstrate that the proposed protocol has some advantages in aspects of low computational cost, lightweight delay and can meet the performance requirements of HWNs.

Keywords Secure billing, Non-repudiation, Heterogeneous wireless networks, Self-updating hash chain

1 引言

随着网络技术和信息社会的快速发展,人们对移动通信和无线网络接入服务的要求越来越高。一方面,WiFi网络应用越来越普遍:机场候车室、咖啡厅、餐馆以及图书馆等场所均提供WiFi无线网络服务,而单个WiFi热点的覆盖范围很小。因此,WiMAX网络以其高速率、覆盖范围较大等优点为用户提供无线接入服务。UMTS、LTE等不同的无线技术也都拥有自己的应用优势和特点,它们构成无处不在的异构无线网络环境[1]。另一方面,针对掌上电脑、智能手机等各类移动终端,用户提出了包括无线上网、移动商务、手机支付等一系列新需求。由于移动终端的资源限制和无线网络的异构性,需要一种高效快速的切换认证方案,而且能够在完成切换认证后继续安全计费,用户和服务提供商都承认计费结果,实现计费的不可否认性[3]。

实现不可否认性计费的方法主要包括安全信封、数字签名和哈希链技术[5]。安全信封需要可信第三方(Trusted Third Party,TTP)提供密钥,这就需要对TTP完全信任,在实际计费过程中,TTP的选择和可信度显得尤为关键;数字签名采用非对称加密算法,不需要TTP参与,但是增加了很大的计算开销;而哈希链技术无需TTP参与,只涉及简单的哈希运算。由于哈希函数的单向不可逆性和计算量低等特点,哈希链技术被广泛应用到不可否认性计费中。

Im等人给出了无线移动网络中在漫游情况下的安全互认证过程和公平计费方法[8]。该方案将认证中心(Certificate Authority,CA)作为TTP,利用哈希链的单向不可逆性实现不可否认的目的,TTP和每个移动终端共享密钥K_{MS},从而保证每个MS均能安全地接收数据。然而该方案假设哈希链

到稿日期:2014-04-29 返修日期:2014-07-21 本文受国家自然科学基金资助项目(61202352),国家博士后基金资助项目(2013T60543,2012M521088),江苏省自然科学基金资助项目(BK20141404),教育部博士点基金资助项目(20123219120030),南京理工大学"紫金之星"项目(2013ZJ0209)资助。

陈守国(1989—),男,硕士生,主要研究方向为密码学、无线网络安全,E-mail:sgchen_2012@163.com;付安民(1981—),男,博士,副教授,主要研究方向为密码学、无线网络安全;秦宁元(1990—),女,硕士生,主要研究方向为网络与信息安全。

足够长，如果哈希链耗尽，将会导致计费终止。此外，该计费方案只适用于单个网络环境，当用户切换到邻居网络时，不能保证持续的安全计费。为了实现在不同无线网络服务提供商(Wireless Internet Service Providers，WISPs)之间的切换和安全计费，Zhu 等人使用 U_token 标签实现城域共享网络切换和计费的安全保护[9]，将认证过程中生成的单向哈希链的链首值包含在 U_token 中递交给服务器，并且通过更新标签 Commit 完成可用哈希链的发布(Commit 包含了哈希链的使用情况)。该方案虽然实现了对固定长哈希链的复用，却依然没有从根本上解决哈希链耗尽的问题。

本文在基于票据的快速切换认证基础上[10]，提出异构无线网络中基于自更新哈希链的不可否认性计费协议(NBPH 协议)。NBPH 协议采用一种自更新哈希链快速更新可用哈希链，通过哈希链值比较快速验证移动终端的合法性，保证了服务的连续性，降低了计算开销，因此，NBPH 协议非常适用于异构无线网络中频繁进行网络间切换的场景。安全分析和性能分析表明，NBPH 协议能够防止各类攻击。

2 预备知识

不可否认性服务[11]是生成、收集、传输存储、验证可行有效的证据，保证通信双方无法否认某个事件或行为的发生。在计费过程中，由于计费双方(运营商和用户)的地位不对等，存在潜在的计费纠纷：用户否认运营商的计费结果，可能是运营商伪造信息收取额外的费用，或者被伪装的攻击者伪造。当然，用户也可能蓄意逃避缴费，否认计费结果。我们采用自更新哈希链技术来解决计费纠纷。

2.1 自更新哈希链

哈希链是由 Lamport[12]首次提出，对随机选取的种子值进行若干次哈希运算得到的一个序列值。构建哈希链 w 的过程如式(1)所示。

$$w: x \rightarrow H(x) \rightarrow H^2(x) \rightarrow \cdots H^i(x) \rightarrow H^{i+1}(x) \rightarrow \cdots H^n(x) \tag{1}$$

用户首先随机选取一个种子值 x 并且以 x 为哈希链的第一个节点值，对它重复进行 n 次哈希运算，n 为哈希链 w 的链长。每进行一次计算得到链的一个节点，放到当前链的链首。对于任意 $i(0 \leqslant i < n)$，都有 $H^{i+1}(x) = H(H^i(x))$。

在利用哈希链实现不可否认性计费过程中，如果哈希链的长度太短，则很快使用殆尽，用尽后系统必须重新初始化，哈希链的再生需要使用数字签名技术，会带来很大的计算开销。另外，如果哈希链太长，则会造成存储开销增加，在初始化阶段需要进行链长次的哈希运算操作，导致降低哈希链的使用效率。通过自更新哈希链技术[13,14]可以解决哈希链长度的问题。本文通过映射当前哈希链的链值生成新链的种子值，从而生成新的哈希链，减少了用户端的计算开销。

2.2 计费场景

在大多数情况下，移动终端 MS 从一个无线网络接入点获取网络服务，当 MS 移动后，可能需要切换到邻近的网络接入点继续获取网络服务。本文以 WiMAX 和 WiFi 的异构融合网络设计不可否认性计费协议。计费场景如图 1 所示，在 WiMAX 网络中，接入服务网络(Access Service Network，ASN)由 ASN 网关(ASN-Gateway，ASN-GW)和基站(Base Station，BS)组成。一个 ASN-GW 控制多个基站(构成一个 ASN 域)，负责转发 MS 和 AAA 服务器(AuthenticationAuthorizing and Accounting，AAA)之间的认证消息等功能。在 WiFi 网络中，一个 WiFi 无线互通功能设备(WiFi Interworking Function，WIF)控制多个接入点(Access Point，AP)并构成一个 WiFi 域。ASN-GW 与 WIF 通过主干网与 AAA 服务器连接，假设 MS 从当前的接入点 AP1 获取网络服务，由于位置移动，MS 需要切换到 AP2、AP3，或者切换到 BS1、BS2。在我们提出的基于票据的快速切换认证的基础上，通过切换认证过程附加哈希链使用情况等信息，用户 MS 就可以向目标接入点发布可用的哈希链，避免了切换后重新生成哈希链。

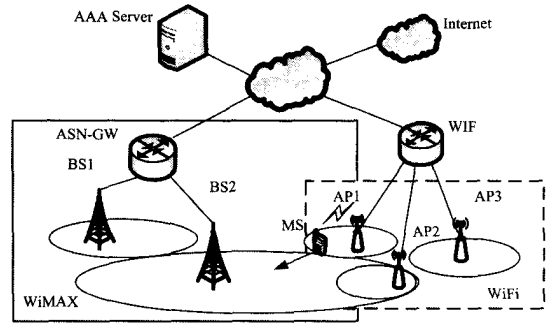

图 1 WiFi-WiMAX 无线网络的漫游场景

3 不可否认性计费协议设计

我们将用户请求的服务分为若干个计费单位，本文以时间为计费标准，采用 Δt 为计费单位进行计费。当以流量为计费标准时，使用计费单位 Δf 替换 Δt 即可。

MS 首先通过可扩展的身份验证协议(Extensible Authentication Protocol，EAP)进行认证接入无线网络，获取信用票据 T_{MS}，然后再利用信用票据快速切换认证并完成计费过程。NBPH 协议分为两个阶段：初始认证和计费阶段与切换认证和计费阶段。在 NBPH 协议设计过程中所使用的符号和意义如表 1 所列。

表 1 NBPH 协议中用到的符号及意义

符号	意义
$MSK_{X\text{-}Y}$	X 和 Y 之间的会话主密钥
MGK	共享的组密钥
TMGK，TCK	临时组密钥和临时 MAC 码密钥
CK，TEK	MAC 码密钥和传输密钥
W(x)	以种子值 x 生成的哈希链
s	新哈希链种子值
T_{MS}	MS 的信用票据
C_{MS}	记录 MS 更新哈希链的次数
C_N	记录 MS 释放的哈希链节点数
$\{m\}_K$	使用密钥 K 加密消息 m
MAC_K	使用密钥 K 生成的 MAC 码
|	连接符
H()	单向哈希函数

3.1 初始认证和计费

初始认证和计费过程如图 2 所示。在初始认证阶段，MS 通过与当前接入的 AP1 和 AAA 服务器完成 EAP 全认证后，MS 和 AP1 会生成主会话密钥(Master Session Key，MSK)，MSK 可以用来加密 MS 和 AP1 之间交互的消息。接着，MS 选择随机数 r_{MS}，假设 r_{MS} 的长度为 n-bits，生成链长为 n 的哈希链 $W(r_{MS})$：

$$r_{MS} \rightarrow H(r_{MS}) \rightarrow H^2(r_{MS}) \rightarrow \cdots\cdots H^{n-1}(r_{MS}) \rightarrow H^n(r_{MS})$$

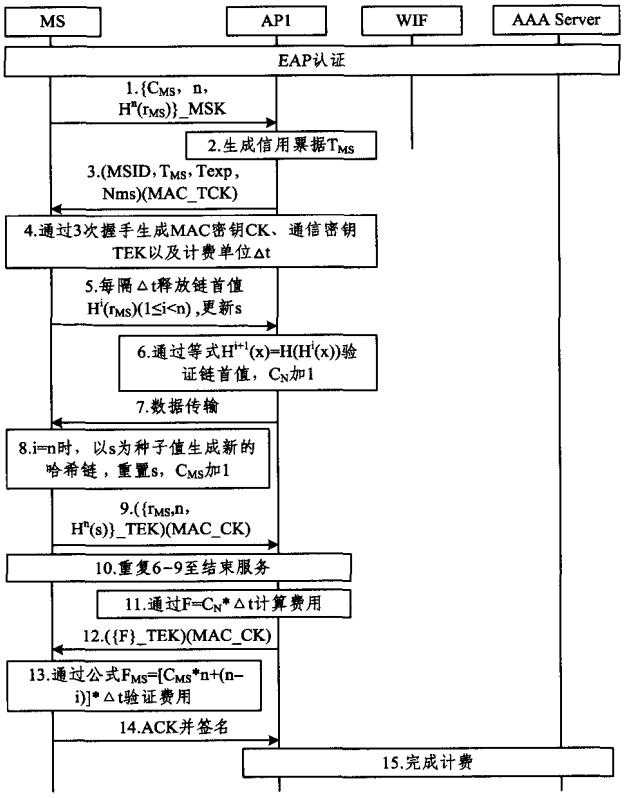

图 2　初始认证和计费

1. MS 向 AP1 发布自己生成的哈希链链长和链首值$\{n, H^n(r_{MS})\}$。AP1 在完成 EAP 认证后同样获得 MSK，并通过式(2)和式(3)计算认证需要的 MAC 密钥 TCK 和临时组密钥 TMGK。

$$TCK = Truncate(MSK, 128) \tag{2}$$

$$TMGK = H(MGK | MSID) \tag{3}$$

其中，$Truncate(x, y)$函数定义为取 x 值的后 y 位比特值，当且仅当 $y \leqslant x$。$MSID$ 为 MS 的身份标示符。

2. AP1 接受 MS 发送的$\{n, H^n(r_{MS})\}_{MSK}$，解密得到链首值 $H^n(r_{MS})$，AP1 按式(4)计算票据 T_{MS}。

$$T_{MS} = \{n, H^n(r_{MS}), MSID, MSK, T_{exp}\}_{TMGK} \tag{4}$$

3. AP1 将生成的票据的值发送给 MS。

4. MS 保存 Δt 并且通过 3 次握手与 MS 协商生成 MAC 密钥 CK、传输密钥 TEK 以及 AP1 的计费单位 Δt。

5. MS 发送服务请求并得到响应之后，每隔一个时间片段 Δt 释放当前链的链首值 $H^i(r_{MS})$，同时更新 s 的值，即附加 1bit 值给 s。

6. AP1 通过 MAC 码验证消息的完整性，解密得到 $H^i(r_{MS})$以及 n。通过等式 $H^{i+1}(r_{MS}) = H(H^i(r_{MS}))$是否成立来验证用户的合法性，如果等式成立，跳转步骤 7，替换 $H^{i+1}(r_{MS})$而保存 $H^i(r_{MS})$，此时将本地保存的 C_N 值加 1；否则，中断服务。

7. AP1 继续向 MS 提供数据服务。

8. 当第 n 次验证时，如果用户请求的服务还没有结束，MS 当前的哈希链只剩种子值 r_{MS}，此时 MS 以 s 为种子值生成一条新的哈希链。新链的长度为 n，将 s 的值替换成 $H^n(s)$映射的 1bit 随机值，此时 C_{MS} 的值加 1。

9. MS 向 AP1 发布新的哈希链信息。

10. AP1 解密得到 r_{MS}，n，$H^n(s)$，首先验证 $H(r_{MS})$是否等于本地保存的值，成功则保存新的链首值。重复步骤 6－9 至服务结束。

11. AP1 收到计费请求，根据公式 $F = C_N * \Delta t$ 计算费用。

12. AP1 将计算好的费用 F 发送给 MS。

13. MS 收到 AP1 的计算的结果，通过式(5)进行验证。

$$F_{MS} = [C_{MS} \times n + (n - i)] \times \Delta t \tag{5}$$

14. 如果收到的费用值 F 等于 F_{MS} 的计算结果，则计费成功，MS 向 AP1 发送费用值确认 ACK；否则出现费用欺骗行为，进行纠纷处理。

15. AP1 收到 MS 的 ACK，则向 AAA 服务器发送计费包，完成计费。

3.2　切换认证和计费

当 MS 从 AP1 覆盖区域移动到 BS2 覆盖区域时，MS 并不需要重新生成哈希链，通过更新 T_{MS} 将可用哈希链的当前链首值发布给目标网络接入点。由于不同网络的计费单位不同，因此 BS2 验证票据成功后，将新的 Δt 值发送给 MS。具体切换认证和计费过程如图 3 所示。

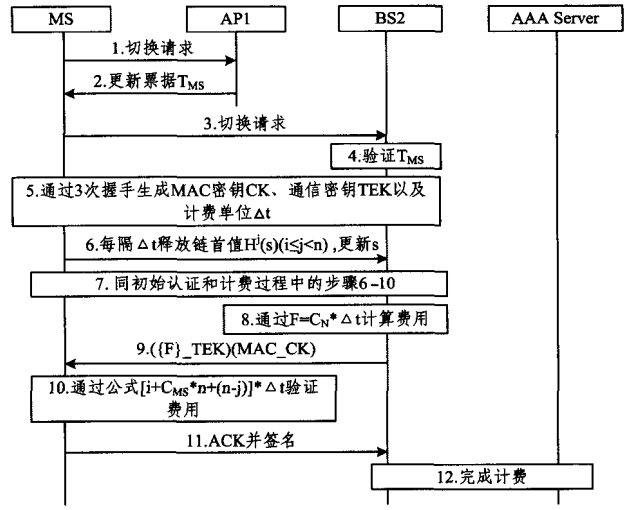

图 3　切换认证和计费

1. MS 向 AP1 发送票据更新请求。

2. AP1 根据式(6)更新票据 T_{MS}，$H^i(s)$为 AP1 最新保存的哈希链链首值 $H^i(s)$。AP1 将更新后的票据 T_{MS}^2 发送给 MS。

$$T_{MS}^2 = \{n, H^i(s), MSID, MSK, T_{exp}\}_{TMGK} \tag{6}$$

3. MS 向 BS2 发送切换请求：$\{MSID, BSID, T_{MS}^2, N_{MS}\}(MAC_{TCK})$，其中 $BSID$ 为目标接入基站的身份标示符。

4. BS2 通过以下步骤验证票据的有效性。

a)通过式(2)计算 TMGK，解密 MS 票据 T_{MS}^2 获取其中的 MSK 和 T_{exp}。判断票据是否过期以及 N_{MS} 的新鲜性。

b)通过 MSK 计算 TCK，验证 MAC 码是否正确。

c)如果 MAC 码有效，则响应 MS 的切换请求。

5. MS 与 BS2 通过 3 次握手建立 MAC 密钥 CK_2、通信密钥 TEK_2 以及新的计费单位 Δt。

6. MS 发送服务请求并得到响应之后，每隔一个时间片段 Δt 释放当前链的链首值，同时更新 s 的值，即随机附加 1bit 数值给 s。

7. 同初始认证和计费过程中的步骤 6－10。

8. BS2 收到计费请求，根据公式 $F=C_N * \Delta t$ 计算费用。

9. BS2 将计算好的费用 F 发送给 MS。

10. MS 收到 BS2 的计算结果，通过式(7)进行验证。

$$F_{MS}=[i+C_{MS}\times n+(n-j)]\times\Delta t \quad (7)$$

11. 如果收到的费用值 F 等于 F_{MS} 的计算结果，则计费成功，MS 向 BS2 发送费用确认 ACK；否则出现费用欺骗行为，进行纠纷处理。

12. BS2 收到 MS 的 ACK，则向 AAA 服务器发送计费包，完成计费。

3.3 纠纷处理

在 3.1 节的步骤 13 和 3.2 节的步骤 10 中，如果 MS 收到来自 AP（或者 BS）的费用 F 不等于 F_{MS}，则可能出现的情况如下：

1）AP 企图欺骗 MS，增大 C_N 值或伪造当前保存的哈希链值 $H^j(s)$，使得 $F>F_{MS}$。

2）MS 企图欺骗 AP，减少 C_{MS} 的值或当前保存的哈希链值 $H^j(s)$，使得 $F>F_{MS}$。

3）MS 和 AP 同时企图欺骗对方，C_N 值增大，C_{MS} 值减小，$F>F_{MS}$。

MS 收到 AP 计费数据包时，需要进行的操作流程如图 4 所示。

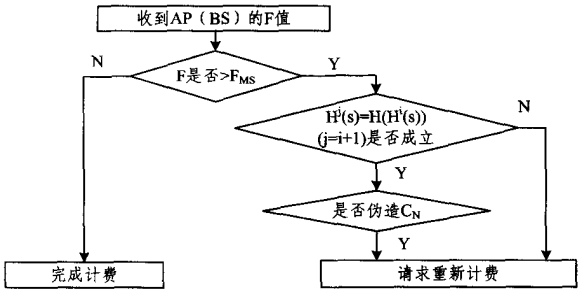

图 4　MS 处理纠纷流程

在第一种情况下，假设 MS 是无欺骗行为的，AP 如果要获得额外的费用，则需要伪造当前保存的哈希链值 $H^j(s)$、C_N 值或者同时伪造 C_N 值和当前保存的哈希链值 $H^j(s)$。

当 MS 收到的来自 AP 的费用值 F 大于根据式(5)或式(6)计算的值 F_{MS} 时，MS 首先请求 AP 发送其当前保存的哈希链值 $H^j(s)$，因为 AP 无法获得种子值 s，所以也无法获得哈希链值 $H^j(s)(j<i+1)$，只要 AP 伪造当前保存的哈希链值 $H^j(s)$ 即可被发现。如果等式 $H^j(s)=H(H^i(s))$ 成立（$H^i(s)$ 为 MS 当前保存的哈希链值），AP 可能恶意修改 C_N 的值，MS 否认 F 值，并请求重新计算费用，在进行若干次请求后无法得到正确的费用值，MS 可选择停止计费甚至断开连接。

在第二种情况下，假设 AP 是无欺骗行为的，如果 MS 想要支付较少的费用，则需要伪造当前哈希链的链首值 $H^k(s)$、伪造 C_{MS} 值，或者同时伪造 C_{MS} 值和伪造当前哈希链的链首值 $H^k(s)$。

MS 通过式(5)或式(7)验证 AP 计算结果的正确性，如果不相等，则 MS 将其计算的费用值发送给 AP。MS 正确给出已更新的哈希链个数，却根据公式 $F_{MS}=[C_{MS} * n+(n-k)] * \Delta t$ 计算费用，即 MS 使用已经释放的 $H^k(s)$ 作为当前链首值，AP 收到 MS 的否认消息以及当前链首值 $H^k(s)$，通过等式 $H^j(s)=H(H^k(s))(k>j)$ 即可防止欺骗行为。对于 C_{MS} 减小导致费用值小于 F，AP 重新发送费用值 F 并附加合法的 C_N 的值，要求 MS 做进一步的验证，如果 MS 仍然不对费用值 F 确认，则 AP 可中断服务，断开连接。

在第三种情况下，计费双方同时企图欺骗对方，可通过结合 1）、2）两种情况进行纠纷处理。

4 安全分析

4.1 安全属性

NBPH 协议能够实现计费的机密性、准确性和不可否认性。

1）机密性与准确性

NBPH 协议安全性关键在于哈希链种子值的保密性，以及哈希函数固有的单向不可逆性。在完成接入认证后，MS 与接入点 AP 已经协商好 MAC 密钥 CK 和通信密钥 TEK，用 MAC 码验证消息的完整性，防止发送的消息被篡改；而 TEK 用于传递消息的加密，保证发送消息的机密性。在 MS 中保存 C_{MS} 值，用于记录更新哈希链的个数，在每次更新哈希链时，C_{MS} 加 1。而在 AP 端，保存一个 C_N 值，每次接收到 MS 释放的哈希值，验证成功后将 C_N 值加 1。AP 直接通过 $C_N * \Delta t$ 得到费用值，而 MS 通过哈希链的使用情况对 AP 计算的费用值进行验证，能够准确地计算费用值，对于可能出现的计费纠纷，在 3.3 节给出了处理方法。

2）不可否认性

在 NBPH 协议中，MS 通过已更新哈希链的个数 C_{MS} 以及当前哈希链的使用情况对 AP 的计费值进行验证。MS 秘密保存种子值 r_{MS} 和 s，每次释放当前链首值时，对 s 的更新也是保密的，因此，AP 无法获取哈希链的种子值。这样，AP 不可能伪造哈希链的链值，另一方面，只有认证过合法的用户才持有正确的哈希链，才能释放正确的哈希值。所以，在正常情况下，只要等式 $H^{i+1}(s)=H(H_i(s))$ 成立，即可正常计费。MS、AP 通过修改当前链值来否认费用是行不通的。此外，通过 C_{MS}、C_N 的伪造来否认计费值将会带来很大的通信开销，计费双方执意恶意否认导致的结果必然是停止服务。

4.2 形式化检测

为了保证 NBPH 协议的安全性，使用 AVISPA[15]（Automated Validation of Internet Security Protocols and Applications）工具进行形式化检测。AVISPA 是一套建立和自动分析安全协议模型的工具，融合了 4 种不同的分析终端：OFMC（On-the fly Model-Checker）、基于约束逻辑的定理证明器（Constraint Logic-Attack Searcher，CL-AtSe）、基于 SAT 的模型检测器（SAT-based Model-Checker，SATMC）和树自动化分析器（Tree Automata-based Protocol Analyzer，TA4SP）。AVISPA 采用高层协议描述语言（High Level Protocol Specification Language，HLPSL）来建立安全协议的分析模型。

采用 HLPSL 对 NBPH 协议建模：定义 ms 和 bs 两个基本角色，分别代表协议的两个主要参与者 MS 和 BS2。另外定义一个 session 混合角色和 environment 高层角色，session 角色用于实例化 ms 和 bs 两个基本角色，environment 角色包含全局变量、几个会话的混合角色和入侵者的相关信息。图 5 给出了切换认证和计费阶段 ms 角色的 HLPSL 代码。

```
SPAN 1.6 - Protocol Verification : NBPH.hlpsl
File
role ms(
        MS,BS:agent,
        Rms:text,
        Kmsk:symmetric_key,
        Hash,Trun,Dot:hash_func,
        SND_MB,RCV_MB:channel(dy))
played_by MS def=
 local State :nat,
       H1,H2,Cms,Cbs,L,J,N:text,
       Kpmk,Ktck,Ktek,Kck:symmetric_key,
       Tms:{text.agent.symmetric_key}_symmetric_key,
       Cmac:{agent.text.{text.agent.symmetric_key}
            _symmetric_key}_symmetric_key
 init State :=0/\H1:=Hash(rms)
 transition
 1.State=0/\RCV_MB(start)=|>
  State':=2/\Kpmk':=Dot(Kmsk.BS.160)
         /\Ktck':=Trun(Kpmk'.128)
         /\H2':=Hash(H1)
         /\Cmac':={MS.H2'.Tms}_Ktck'
         /\SND_MB({MS.H2'.Tms}.Cmac')
         /\secret(rms,r,{MS})
 2.State =2/\RCV_MB(MS.Tms'.Cmac')=|>
  State':=4/\SND_MB(MS.H1.Cmac')
         /\request(MS,BS.bs_ms_cmac,Cmac')
         /\witness(MS,BS.ms_bs_cmac,Cmac')
 3.State =4/\RCV_MB(L.Cbs'.Cmac')=|>
  State':=6/\J':=new()
         /\N':=new()
         /\Cms':=new()
         /\SND_MB(L.Cms'.J'.N'.Cmac')
end role
```

图 5　切换认证和计费阶段角色 ms 的 HLPSL 代码

AVISPA 检测结果如图 6 所示。OFMC、CL-AtSe 以及 SATMC 模块的检测结果表明，NBPH 协议是安全的(SAFE)，我们给出的安全目标是：组密钥和随机数的保密性。MS 与 AP 通过哈希链值验证实现快速认证，通过 MAC 码验证判断数据在传输过程中是否被修改。因此，NBPH 协议能够防止伪装攻击、篡改攻击、中间人攻击等恶意攻击。TA4SP 验证模型结果显示不确定(INCONCLUSIVE)，主要因为 NBPH 协议设计过程中使用了单向哈希函数，而目前 TA4SP 模块不支持单向哈希函数。

```
AVISPA Tool Summary

OFMC    : SAFE
CL-AtSe : SAFE
SATMC   : SAFE
TA4SP   : INCONCLUSIVE
```

图 6　AVISPA 检测结果

5　性能分析

通过对比 Im 等人方案[8]、Zhu 等人方案[9]和本文设计的 NBPH 协议，分析切换认证和计费过程中的计算开销和通信开销。

5.1　计算开销

计算开销包括了切换认证和计费过程中涉及的密码学和费用值等相关的计算量。具体的计算开销缩写及含义如表 2 所列。NBPH 协议在切换认证过程以及计费过程中，计算开销主要涉及哈希运算、对称加解密运算和 MAC 运算，这些加密算法的开销小。计算费用值 F 只涉及乘法运算，计算时间可以忽略。表 3 统计了文献[8,9]以及 NBPH 协议的计算开销。

表 2　计算开销缩写及含义

符号	意义
T_H	一次哈希运算的时间
T_S	一次对称加/解密运算的时间
T_{AS}	一次非对称加/解密运算的时间
T_M	一次 MAC 运算的时间
T_{MUL}	一次点乘运算的时间
T_{EXP}	一次指数运算的时间

表 3　计算开销比较

方案	计算开销[T_M,T_H,T_{MUL},T_{EXP},T_S,T_{AS}]			
	MS	AP /BS	ASN-GW/WIF	AAA 服务器
文献[8]	[1,N+1,0,0,0,0]	[0,2,0,0,2,4]	[1,2,0,0,0,2]	[1,0,0,0,0,1]
文献[9]	[1,N+4,7,2,4,0]	[0,3,0,1,4,0]	[1,0,0,0,1,0]	[0,0,1,2,0,2]
NBPH 协议	[6,n+2,1,0,2,0]	[6,3,0,1,4,1]	[0,1,1,0,1,0]	[0,0,0,0,0,0]

注：N,n 为哈希链的长度，NBPH 采用自更新哈希链技术，取 $n=500$，文献[8,9]需较大的哈希链长度，取 $N=1000$

从计算开销比较表中可以看出，文献[8]涉及到多次非对称加/解密运算(包括数字签名)，带来很大的计算开销。文献[9]也采用了如指数、乘法、取反、平方、对称加/解密等操作，需要大量的计算开销。NBPH 协议采用自更新哈希链技术，初始哈希链的链长度值 n 无需太大，其他方案中均需选择满足需求的较大的长度 N。此外，切换和计费过程中涉及到的运算包括 MAC 操作、哈希运算和对称加/解密运算。而这些操作计算量小，不会带来较大的计算开销。

5.2　通信开销

通信开销为切换认证和计费过程中各个相关联实体间的通信时延。NBPH 协议中 MS 只和 AP 进行通信而不涉及第三方，我们记 T_W 为 MS 与 AP 之间的通信时延，T_E 为 AP 与 WIF(ASN-GW)之间的通信时延，T_A 为 ASN-GW(WIF)与 AAA 服务器之间的通信时延，T_B 为两个相关联设备之间的通信时延。表 4 给出了文献[8,9]以及 NBPH 协议的通信开销。

表 4　通信开销比较

方案	T_W	T_A	T_B	T_E
文献[8]	7	2	3	0
文献[9]	9	4	0	1
NBPH 协议	7	1	0	2

从通信时延比较表中可以看出，完成一次切换和计费过程，NBPH 协议的通信开销是比较小的。与文献[8]和文献[9]相比，NBPH 协议在切换认证过程中没有 AAA 服务器的参与，只需要在最后计费阶段与 AAA 服务器进行通信。在没有纠纷的情况下，MS 与 AP 不需要频繁地通信。总体来说，NBPH 协议满足资源受限的 MS 的性能需求。

5.3　仿真结果

为了进一步评估上述方案的性能(包括计算开销和通信开销)，利用 ns3.9 网络仿真工具[16]对以上各方案切换和计费过程进行仿真。仿真机器的配置如下：32 位操作系统，Intel Core I5(3470)处理器，主频 3.2GHz。仿真参数如下：信噪比为 5db，传输功率是 30db，此外，BS/AP 与 ASN-GW/WIF 之间有线链路带宽为 50Mbps，两个 ASN-GWS 之间的有线连接带宽为 500Mbps，ASN-GW/WIF 和 AAA 服务器之间的有线带宽为 2Gbps。仿真环境如下：创建源接入点 AP 和目标接入点 BS 相距 100 米，MS 从 AP 切换到 BS，我们通过改变 MS 的个数(1—10)统计切换认证和计费的总时延。

各方案的总时延与 MS 个数的变化关系如图 7 所示。从图 7 可以看出，各方案的切换认证和计费总时延都随 MS 个数增加而近似线性增长，因为无线接入点 AP 或 BS 为多输入多输出(Multiple-input and Multiple-output，MIMO)模式，能够处理多个 MS 的切换请求，随着 MS 的增加，切换时延不会成倍增加，而多个 MS 同时请求切换认证会带来排队延迟和丢包率的增加，所以在一定范围内平均的切换时延近似线性

增长。其中我们设计的 NBPH 协议总时延明显低于文献[8,9],尤其是相比文献[9],总时延降低了近 50%。这是因为 NBPH 协议在切换过程中不需要与 AAA 服务器通信,减少了通信开销。此外,通过采用自更新哈希链,只需通过哈希链值的简单比较即可快速验证请求服务用户的合法性。总体来说,NBPH 协议可以满足异构网络中资源受限的移动终端,保证计费的连续性和安全性。

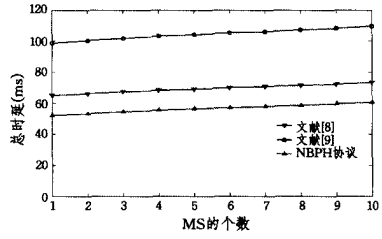

图 7 总时延与 MS 个数的关系

结束语 安全计费是异构无线网络融合和商用过程中亟待解决的主要问题。针对该问题,NBPH 协议中基于时长或者流量为计费单位对数据服务分片,每隔一个计费单位(Δt 或者 Δf)对用户进行快速认证。NBPH 协议将自更新哈希链应用于不可否认性计费中,采用信用票据的思想将哈希链的使用情况附加在票据中,在 MS 完成切换认证的同时,也向目标接入点发布了可用哈希链的信息,实现了计费的连续性。链值的不可伪造提供了不可否认性计费的依据,能够解决可能出现的计费纠纷。此外,由于不同网络的计费单位 Δt 的设定值不同,在切换认证完成后,目标接入点将本网络的 Δt 发送给 MS,从而提出的计费协议适用于不同带宽的网络。通过安全和性能分析,以及相应的仿真实验,表明 NBPH 协议能够抵御伪装、篡改等恶意攻击且负担较小的计算和通信开销,因此特别适用于异构无线网络复杂的环境。

参 考 文 献

[1] 姜奇,马建峰,李光松,等. 基于 WAPI 的 WLAN 与 3G 网络安全融合[J]. 计算机学报,2010,33(9):1675-1685

[2] Prabhavathi P, Nithyanandan L. Network selection in wireless heterogeneous networks[C]// Proceedings of 2013 International Conference on Communications and Signal Processing. Melmaruvathur,2013:357-361

[3] He Dao-jing, Chen Chun, Bu Jia-jun, et al. Security and Efficiency in Roaming Services for Wireless Networks: Challenges, Approaches, and Prospects[J]. IEEE Communications Magazine, 2013,51(2):142-150

[4] 傅建庆. 面向 3G_WLAN 互联网络的安全协议研究[D]. 杭州:浙江大学,2010

[5] Rainer S, Christoph R. On the Security of the Non-Repudiation of Forwarding Service[C]// Proceedings of 2012 International Conference on Trust, Privacy and Security in Digital Business. Vienna, Austria, 2012:167-178

[6] Wu Wei, Zhou Jian-ying, Xiang Yan, et al. How to achieve non-repudiation of origin with privacy protection in cloud computing [J]. Journal of Computer and System Sciences, 2013, 79(8): 1200-1213

[7] Xiao Zhi-feng, Xiao Yang, Du D. Non-repudiation in neighborhood area networks for smart grid[J]. IEEE Communications Magazine, 2013, 51(1): 18-26

[8] Im T, Lee H, Cho K, et al. Secure Mutual Authentication and Fair Billing for Roaming Service in Wireless Mobile Networks [C]// Proceedings of the Third International Conference on Convergence and Hybrid Information Technology. Busan, 2008: 466-471

[9] Zhu Hao-jin, Lin Xiao-dong, Shi Ming-hui, et al. PPAB: A Privacy-Preserving Authentication and Billing Architecture for Metropolitan Area Sharing Networks[J]. IEEE Transactions on Vehicular Technology, 2009, 58(5): 2529-2543

[10] Fu An-min, Zhang Yu-qing, Zhu Zhen-chao, et al. An efficient handover authentication scheme with privacy preservation for IEEE 802. 16m network[J]. Computers & Security, 2012, 31 (6): 741-749

[11] BS ISO/IEC. 13888-1/2 Information technology-Security techniques- Non-repudiation[S]. Switzerland: The Standards Policy and Strategy Committee, 2009

[12] Lamport L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24(11): 770-772

[13] 瓮佳佳,张敏情,刘昀昊. 基于几何方法的自更新 Hash 链构造方案[J]. 计算机应用,2010,30(12):3343-3345

[14] 陈孟奇,严新荣,张彬祥. 改进的基于自更新哈希链的认证方案[J]. 信息安全与通信保密,2013(2):73-75

[15] AVISPA Team. European Community under the Information Society Technologies Program [OL]. http://www.avispa-project.org, 2012

[16] The NS-3 Consortium. NS3 tutorial & ns-allinone-3.9.tar.bz2 [OL]. http://www.nsnam.org/release/ns-allinone-3.9.tar.bz2, 2013

(上接第 84 页)

[8] Hao Jin, Deng Pan, Jing Xu, et al. Efficient VM Placement with Multiple Deterministic and Stochastic Resources in Data Centers [C]// Proceedings of 2012 IEEE Global Communications Conference (GLOBECOM). 2012: 2505-2510

[9] Hwang I, Pedram M. Hierarchical Virtual Machine Consolidation in a Cloud Computing System[C]// Proceedings of 2013 IEEE Sixth International Conference on Cloud Computing. 2013: 196-203

[10] Gao Yong-qiang, Guan Hai-bing, Qi Zheng-wei, et al. A multi-objective ant colony system algorithm for virtual machine placement in cloud computing[J]. Journal of Computer and System Sciences, 2013, 79(8): 1230-1242

[11] Dong Jian-kang, Jin Xing, Wang Hong-bo, et al. Energy-Saving Virtual Machine Placement in Cloud Data Centers[C]// Proceedings of 2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing. 2013: 618-624

[12] 杨星,马自堂,孙磊. 云环境下基于改进蚁群算法的虚拟机批量部署研究[J]. 计算机科学,2012,39(9):33-37

[13] Fan Xiao-bo, Weber W-D, Barroso L A. Power Provisioning for a Warehouse-sized Computer[C]// Proceedings of the 34th ACM International Symposium on Computer Architecture. 2007: 13-23

[14] Xu Jing, Fortes J A B. Multi-objective Virtual Machine Placement in Virtualized Data Center Environments [C] // 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing. 2010: 179-188