一种泛在网络的安全认证协议

戚 湧* 郭诗炜 李千目
(南京理工大学计算机科学与工程学院 南京 210094)

摘 要：泛在网络是标准的异质异构网络，保证用户在网络间的切换安全是当前泛在网的一个研究热点。该文对适用于异构网络间切换的认证协议 EAP-AKA 进行分析，指出该协议有着高认证时延，且面临着用户身份泄露、中间人攻击、DoS 攻击等安全威胁，此外接入网络接入点的有效性在 EAP-AKA 协议中也没有得到验证，使得用户终端即使经过了复杂的认证过程也不能避免多种攻击。针对以上安全漏洞，该文提出一种改进的安全认证协议，将传统 EAP-AKA 的适用性从 3G 系统扩展到泛在网络中。新协议对传播时延和效率进行完善，为用户和接入点的身份信息提供有效性保护，避免主会话密钥泄露，采用椭圆曲线 Diffie Hellman 算法生成对称密钥，在每次认证会话时生成随机的共享密钥，并实现用户终端与家乡域网络的相互认证。通过开展实验，对协议进行比较分析，验证了新协议的有效性及高效率。

关键词：泛在网络；访问控制；安全认证协议；EAP-AKA
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2016)07-1800-08
DOI: 10.11999/JEIT151043

A Secure Authentication Protocol of Ubiquitous Convergent Network

QI Yong GUO Shiwei LI Qianmu
(*School of Computer Science and Engineering, Nanjing University of Science & Technology, Nanjing* 210094, *China*)

Abstract: Ubiquitous network is a kind of standard heterogeneous network. It is a hot research topic to secure switching between networks. This paper analyzes EAP-AKA, which is used during handoff across heterogeneous networks. However, this protocol has high authentication delay and is confronted with several security threats, such as user identity disclosure, man in middle attack and DoS attack. Moreover, access point of the access network is not verified, leaving the user under attack even after heavy authentication procedure. To deal with the above security vulnerabilities, an improved secure authentication protocol for ubiquitous network based on EAP-AKA protocol is proposed, extending the applicability of traditional EAP-AKA protocol from the 3G system to ubiquitous network. The new protocol reduces authentication delay and effectively protects identities of users and access points. In order to avoid main session key leakage, the Diffie Hellman algorithm is used to generate a symmetric key randomly each time. The mutual authentication between user endpoint and the home network is also achieved in new protocol. Experiments and analysis verifies effectiveness and efficiency of the proposed protocol.

Key words: Ubiquitous network; Access control; Secure authentication protocol; EAP-AKA

1 引言

泛在网络通过 ZigBee, Wi-Fi, Wi-MAX，无线传感网等各种异构无线网络的相互融合、互联互通、跨域协同，为用户提供随时随地的专属服务。泛在网络所具有的匿名性、异构性和虚拟性给安全保护带来了巨大挑战，如何更可信地进行泛在接入和信息交互成为亟待解决的问题。认证的目的是验证泛在节点和用户等参与主体身份的合法性以及主体间传递的信息及其来源的真实性。随着用户大量通过泛在的移动终端接入网络，如何保证连接的持久安全成为认证设计的一大难题。根据实验结果，重认证所需时间占了切换总时延的 46%[1]。因此，接近零时延的安全切换在泛在网络中极为重要。

由于 EAP 数据包可以在异构网络间传输，在泛在网络安全认证的领域中，完整的 EAP-AKA 认证

收稿日期：2015-09-06；改回日期：2016-02-25；网络出版：2016-04-26
*通信作者：戚湧 790815561@qq.com
基金项目：国家自然科学基金(61272419)，江苏省未来网络前瞻性研究(BY2013095-3-02)
Foundation Items: The National Natural Science Foundation of China (61272419), Future Network Research Projects in Jiangsu Province (BY2013095-3-02)

方法使用 peer-server 架构进行双向认证，通过重用认证向量来实现快速的重认证[2]。文献[3,4]指出原有 EAP-AKA 协议存在严重的安全隐患。为了减少重认证过程的时延，文献[5]提出一种快速迭代的本地重认证协议，其中认证向量由接入点迭代生成，但是需要对基础设施进行大规模的改造升级。文献[6]提出一种初始化的切换协议，使用预认证技术减少切换时延，然而该协议需要在跨网环境中部署异构互连单元，且预认证中存在的缺陷会增加家乡域服务器的负担。文献[7,8]提出针对用户终端再次连接相同网络域的本地重认证协议。文献[9]提出一种基于椭圆曲线加密和代理签名机制的匿名认证协议，通过让部分移动终端随机共享代理签名密钥对的方式，实现完全匿名和非法认证请求过滤。文献[3]和文献[10]针对 AKA 过程和对称密钥生成提出 ECDH，在不增加公开密钥基础设施负担的情况下，提高公共密钥加密的强度，然而文献[10]中的协议并没有实现 UE 和家乡网络的双向认证。文献[11]使用 ECDH 进行密钥协商，并对接入点进行验证，但是仍然存在密钥泄露的安全隐患。文献[12]针对 LTE 中的 EAP-AKA 协议进行改进，缩短认证过程中消息的长度，但是效率并没有明显提升。

基于对上述文献的研究，本文提出一种泛在网络的认证协议，对原有的 EAP-AKA 协议进行改进，为用户和接入点的身份信息提供有效保护，避免 MSK 泄露，在每次认证会话时生成随机的共享密钥，并实现 UE 和家乡域网络的相互认证，同时简化原有协议的流程。

2　EAP-AKA 协议分析

2.1 协议认证过程

3GPP 组织提出 EAP-AKA 协议，推荐将其用于异构网络认证。EAP-AKA 协议基于 3GPP 的 AKA 协议，并采用可扩展认证协议 EAP 和 AAA 协议，实现用户的 WLAN 接入认证。

标准的 EAP-AKA 协议的认证过程描述如下：

(1)用户终端通过主动或被动的方式发现接入点，基于信噪比最佳原则从中选择一个建立连接，并通过该接入点向家乡域服务器发送 EAP 身份响应消息，首次认证时发送永久用户标识 IMSI。

(2)由于用户身份所属域的服务器没有发出过身份请求，同时也为了确认中间结点没有篡改数据包，家乡域服务器在接收到 EAP 响应后需要向用户终端发出 EAP 身份请求。

(3)家乡域服务器证实 IMSI 合法后，为用户终端准备 AKA 挑战，生成序列号 SQN 和随机数 RAND，计算匿名密钥 $\mathrm{AK}=\mathrm{F5}(K,\mathrm{RAND})$和消息认证码 $\mathrm{MAC}=\mathrm{F1}(K,\mathrm{SQN},\mathrm{RAND})$，并使用共享密钥 K 生成基于序列号的认证向量组 $\mathrm{AV}(1\cdots n)$。每个认证向量 **AV**=RAND||XRES||CK||IK||AUTN，其中 $\mathrm{AUTN}=\mathrm{SQN}\oplus\mathrm{AK}||\mathrm{MAC}$, $\mathrm{XRES}=\mathrm{F2}(K,\mathrm{seq})$, $\mathrm{CK}=\mathrm{F3}(K,\mathrm{seq})$, $\mathrm{IK}=\mathrm{F4}(K,\mathrm{seq})$。

(4)家乡域服务器从中选择一个认证向量，用 CK 和 IK 生成 MSK，向用户终端发送包含 AUTN 和 RAND 的 EAP 请求/AKA 挑战消息。

(5)用户终端根据 AUTN 和 MAC 对家乡域服务器进行验证，生成完整性可靠的响应消息 RES。

(6)家乡域服务器验证 RES = XRES 后，向接入点和用户终端发送 EAP 成功消息。

(7)家乡域服务器向接入点发送主会话密钥 MSK 和 EAP 成功消息。此时接入点可以通过 4 次握手机制生成临时密钥与用户终端通信。

2.2 安全性分析

EAP-AKA 协议的认证过程中存在如下安全问题：

(1)用户首次与接入点建立连接时，身份信息 IMSI 使用明文传输，容易被攻击者窃取。

(2)接入点的身份没有得到认证。攻击者可以控制位于网络重叠区域的接入点，将认证数据重定向至漫游网络或安全措施较弱的网络，导致用户资费增加或失去安全性[13]，或伪造被攻陷的接入点进行攻击。

(3)在 EAP-AKA 协议中，主会话密钥通过明文传输，容易被攻击者窃取，遭受攻击。

此外，用户和家乡域间始终使用相同的密钥进行通信。一旦该密钥遭到泄露，此后所有的通信都将不可靠。这种基于单钥体系的认证协议，不仅不能提供不可否认性，还会影响异构网络的建立[14]。

3　改进的 EAP-AKA 协议

针对 EAP-AKA 协议中存在的问题，本文提出一种改进的协议。该协议在传输所有密钥和身份信息之前，先进行加密，保证密钥与身份信息的安全性。同时简化原有协议的认证过程，以提高认证效率。

改进的 EAP-AKA 协议相关符号如表 1 所示。泛在网络类似 3GPP 系统，每个用户终端都拥有一个唯一的永久标识 IMSI，且泛在网络中的每个异构子网都有一个 AAA 服务器 HAAA 和归属签约用户服务区 HSS，这些服务器负责维护本网络域中网络资源和服务资源，并管理用户注册、认证、权限。

表 1 改进协议相关符号表

符号	描述
UE	用户终端，包括各种异构网络中的移动终端
AP	接入点，如：接入网关、基站、无线接入点等
HAAA	家乡域的 AAA 服务器
HSS	归属签约用户服务器，保存 UE 身份信息及其与 HAAA 的共享密钥
K	UE 和家乡域的共享密钥
F(0-9)	AKA 中的安全算法
$\|\|, \oplus$, hash()	消息连接符号，异或符号，哈希表
cIDue	本次会话中 UE 的 ID
cIDap	AP 的加密 ID
rIDue	重认证时 UE 的 ID
CTue, CTap	分别是 UE 和 AP 的加密令牌
MACu, MACap, MACh	分别是 UE, AP 和 HAAA 的鉴别码
Pu, Ph	分别是 UE 和 HAAA 的初始公钥
Su, Sh	分别是 UE 和 HAAA 的私钥
Pus	本次会话中 UE 的公钥
Khu	UE 和家乡域的永久共享密钥，Khu = Ph*Su = Pu*Sh
Khus	本次会话中 UE 和家乡域的共享密钥

假设：

(1)HAAA 与 HSS 数据库之间的连接是安全的。

(2)每个 UE, AP, HSS, HAAA 服务器都有各自唯一的设备 ID。

(3)用户和 HAAA 服务器使用相同的椭圆曲线，并在上面选定同一点 Q 生成各自的密钥对。HSS 的公钥 Ph = Q*Sh。类似地，UE 的公钥 Pu = Q*Su。

(4)每次认证会话开始时，UE 生成随机数 r，计算出本次会话 UE 和 HAAA 的公钥分别为：Pus = Pu*r 和 Phs = Ph*r。UE 与 HAAA 之间的共享密钥 Khus = Phs*Su。

改进的 EAP-AKA 协议的过程如图 1 所示，具体描述如下：

(1)UE 和 AP 建立连接。

(2)AP 向 UE 发送 EAP 请求/身份，并在请求中附上经过加密的身份信息 cIDap = (IDap)_Pus。

(3)UE 收到 EAP 消息后，从中解析出 IDap，用 Khus 加密 IDap 得到 CTap = (IDap)_Khus，生成随机序列号 seq，计算 CTue = (seq)_Khus, cIDue = (IMSI)_Khus 以及 MACu = hash(IMSI || IDap || seq)。

(4)UE 向 AP 发送 EAP 响应/AKA 挑战。

(5)AP 在消息后附上 MACap = hash(IDap)，根据 cIDue 中未加密的家乡域信息发送给相应的 HAAA。

(6)HAAA 从消息中解析出 IDap, seq, CTap 以及 CTue，用 MACap, MACue 验证接入点和消息。验证成功则计算本次会话的共享密钥 Khus = Pus*Sh，将解析出的 IMSI 和 seq 转发给 HSS。

(7)HSS 收到 IMSI 后，验证其是否合法以及 UE 是否有权请求接入网的服务。验证成功则根据 IMSI，HSS 获得对应的永久共享密钥 Khu，生成重认证计数器 R-Count，然后使用 seq 生成如下认证向量 **AV**：

认证应答：RES = F2(Khus, seq)

加密密钥：CK = F3(Khu, seq)

完整性密钥：IK = F4(Khu, seq)

重认证时的临时 ID：nIDue = FIDue(Khu, seq)

随后 HSS 通过安全的连接将计算得到的 **AV** 发给 HAAA。R-Count 和 rIDue 则作为重认证参数。

(8)HAAA 计算 MSK = FMSK(CK,IK,cIDue) 和 Kha = F5(IDap, Pus)，然后用 Kha 加密 MSK 得到 EnMSK = {MSK}_Kha。另外，HAAA 计算鉴别码 MACh = hash(RES||MSK)。

(9)HAAA 向 AP 发送 EnMSK, RES 和 MACh。

(10)AP 使用自己的 ID 和 UE 的公钥计算出共享密钥 Kha，并成功解密 EnMSK，得到 MSK。于是 AP 由未认证的接入点转变为已认证的接入点，并将 HAAA 发来的消息转发给 UE。

(11)UE 计算 CK, IK, MSK 和 XRES，验证 XRES 是否与 RES 相等，以及 hash(RES||MSK)是否与 MACh 相等。验证成功则计算 rIDue 作为重认证 ID，并通过 AP 向 HAAA 发送 EAP-success 消息。

4 协议的分析与验证

4.1 安全性分析

改进的 EAP-AKA 协议安全属性如下：

(1)用户身份保护：在改进的协议中，IMSI 不再使用明文传输，因此对攻击者不可见。只有家乡域的 AAA 服务器可以使用共享密钥 Khus 获取。此外，重认证时的临时 ID 也不再通过消息传输，而是由 HSS 和 UE 分别独立生成。所以用户身份在改进的协议中得到了有力的保障。

(2)双向认证

(a)UE 和家乡域网络间的认证：HAAA 获取 IMSI、验证 MACue 和 UE 验证 MACh 的成功是协议中 UE 和家乡域网络之间相互认证的关键点。只有这些验证都成功，才能实现用户与网络的双向认证。

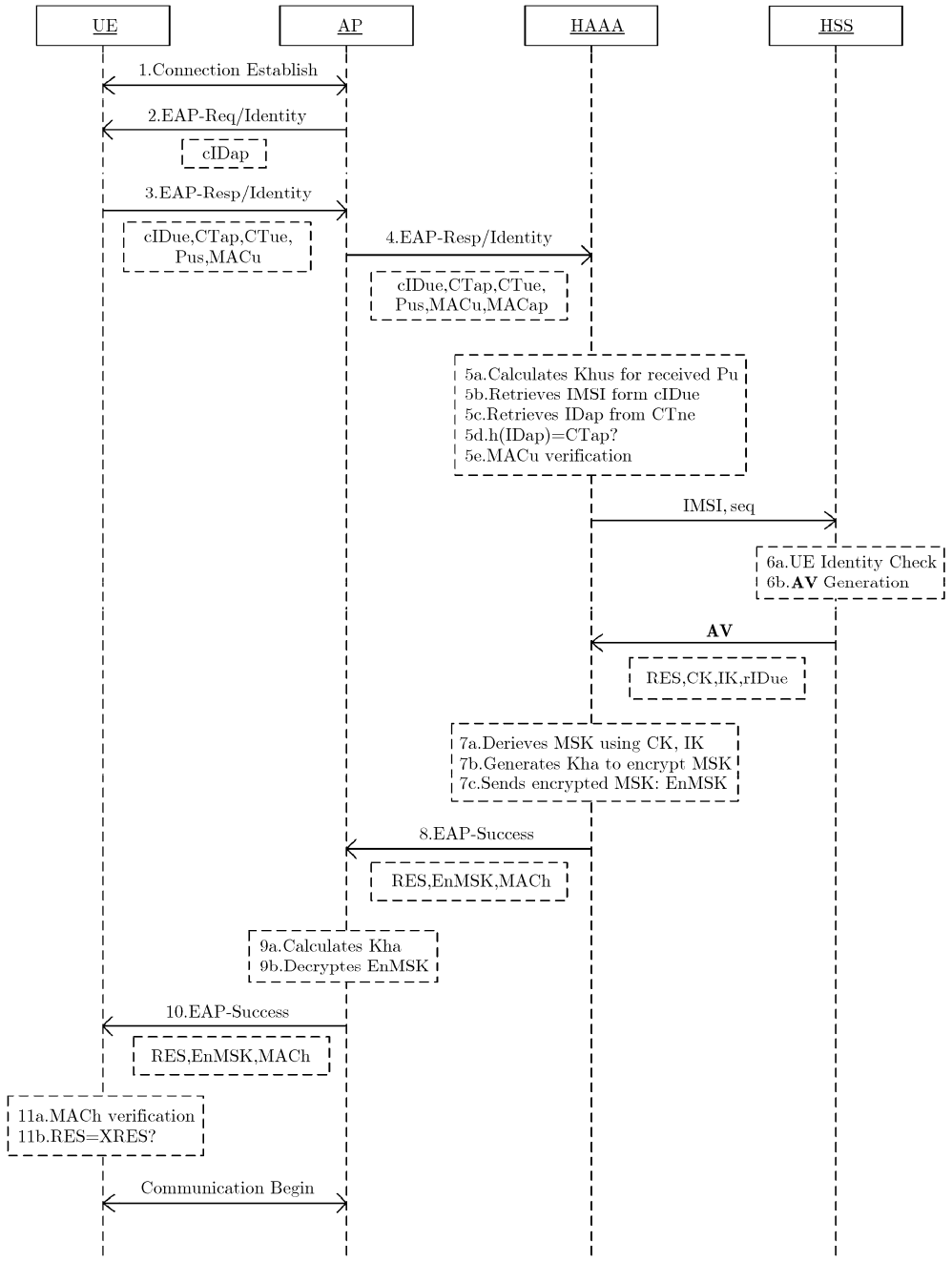

图 1 改进的 EAP-AKA 协议

(b)AP 和家乡域网络间的认证：虽然 AP 和 HAAA 之间没有直接的挑战/响应机制，但是通过 HAAA 对 MACap 的验证和 AP 对 MSK 的解密过程，它们之间进行了间接的认证。只有合法的 AP 使用 ID 和用户公钥才能计算出解密密钥。成功解密 EnMSK 意味着 HAAA 使用正确的 IDap 生成加密密钥。因此，AP 和网络之间的认证在改进的协议中也得到实现，从而避免了重定向攻击。

(3)抵御中间人攻击；

(a)加密 IMSI 的密钥 Khus 根据每次认证时随机生成的 seq 计算得出，攻击者无法获得。

(b)所有消息都有鉴别码 MAC 验证，可以有效抵御中间人攻击。

(c)UE 与 AP 的主会话密钥 MSK 不再通过明文传输，加密 MSK 的共享密钥 Kha 也只能由合法的 AP 计算得到。这保证了 MSK 不会被攻击者获取，从而防止中间人攻击。

(4)防止重放攻击：改进的协议中，共享密钥 Khus 在对于每次认证会话都是唯一的，seq 也是随机生成的。因此，由该密钥计算得出的所有参数都至于当前会话相关。

(5)密钥机密性：共享密钥 Khus 是用 ECDH 技

术生成的。攻击者难以计算得到。同时，认证向量 AV 的生成也使用密钥 Khus 和 Khu 来计算不同的参数，而 Khus 和 Khu 在协议中都是由 UE 和 HAAA 各自生成的，攻击者无法获得。另一方面，尽管 MSK 的生成与 IDap 有关，但 IDap 在协议中都是以加密形式传输的，攻击者无法据此获得密钥 Kha，进而解密 EnMSK 获得 MSK。本协议中的所有会话密钥的机密性都得到了保障。

(6)抵御重定向攻击：假设攻击者使用仿冒的 IDap 与 UE 建立了连接。为了完成认证过程，攻击者仍然需要通过合法的接入点来转发认证消息。此时，认证消息中会出现多个 IDap：攻击者仿冒的 IDap 以及合法接入点的 IDap。收到认证消息 HAAA 将据此判定本次认证遭受了攻击，认证失败，从而抵御了重定向攻击。

4.2 使用认证测试方法对改进的协议进行安全性证明

认证测试方法是基于串空间模型的一种安全协议形式化分析与验证方法。通过构造测试分量验证认证协议是否能达到身份认证及消息保密性等安全目标。

根据第 3 节中的假设 1, HAAA 服务器和 HSS 数据库可视为一个通信实体。利用串空间模型的理论和概念，改进的协议可以形式化抽象为如图 2 所示的模型。

图 2 中：

$M1$ = cIDap

$M2$ = cIDue||CTap||CTue||K_U||MACu

$M3$= cIDue||CTap||CTue||K_U||MACu||MACap

$M4$ = RES||EnMSK||MACh

$M5$ = RES||EnMSK||MACh

改进的协议严格来说是一个三方协议。文献[15]曾经证明：如果三方协议的主体间能够保证两两交换消息的安全性，那么由它们组成的三方协议就能保证整个协议的安全性。因此，该协议可以简化为 3 个双方协议：UE 和 HAAA 之间的认证、AP 和 HAAA 之间的认证以及 UE 和 AP 之间的认证。只要证明 UE 与 HAAA 之间以及 UE 与 AP 之间安全，通过信任的可传递性，可推出 UE 和 AP 之间也是安全的。

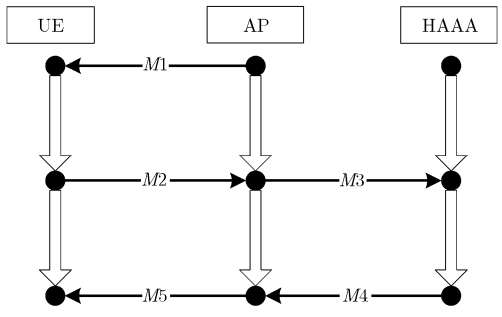

图 2 改进协议的正常串空间束

令 C 为串空间 Σ中的束，s_h 为 HAAA 串，s_u 为 UE 串，s_a 为 AP 串。首先列出如下前提：

安全密钥假设：在每一个 UE 和 HAAA 之间都有唯一的一个共享密钥 K_{HU} 与之对应，而且这个共享密钥并不为攻击者所知。假定攻击者的已知密钥集为 K_P，则 $K_{\mathrm{HU}} \notin K_P$。

在改进协议的 Bundle 中，seq 是 s_u 串唯一产生的。

(1)用户终端和家乡域网络之间的安全性验证：根据改进协议的具体运行流程，可以得到该双方协议的串和轨迹如下：

用户终端的串和轨迹：

Init[{cIDue, CTap, CTue, K_U, MACu}, {RES, EnMSK, MACh}]

=⟨+{cIDue, CTap, CTue, K_U, MACu}, −{RES, EnMSK, MACh}⟩

家乡域网络的串和轨迹：

Resp[{cIDue, CTap, CTue, K_U, MACu}, {RES, EnMSK, MACh}]

=⟨−{cIDue, CTap, CTue, K_U, MACu}, +{RES, EnMSK, MACh}⟩

用户终端和家乡域网络的双方协议的 Bundle 如图 3 所示。

(a)用户终端对家乡域网络的认证：

步骤 1 构造测试分量。在该 Bundle 中，seq 唯一产生于$<s_u, 1>$，seq $\subset$ CTue 。又因为 seq 是随机数， RES = F2(Khus, seq)，所以 CTue 是 seq 对于$<s_u, 1>$的测试分量。$<s_u, 1> \Rightarrow^{+} <s_u, 2>$是 seq 的入测试。

步骤 2 定义节点 m。按照认证测试规则，节点 m 为负节点。因此 m 为某个 HAAA 串中的节点。假设该串为 $s_h^{'}$=Resp[{cIDue′, CTap′, CTue′, $K_U^{'}$, MACu′}，{RES′, EnMSK′, MACh′}]，且 $m = <s_h^{'}, 1>$, term $(<s_h^{'}, 1>)$= {cIDue′, CTap′, CTue′, $K_U^{'}$, MACu′}。

步骤 3 比较串的内容。由于 seq 是 UE 串中唯一产生的随机数，且 seq $\subset$ CTue ，因此 CTue′ = CTue。通过比较 term$(<s_h^{'}, 1>)$和 UE 串中的内容可以得到串 $s_h^{'}$=s_h。因此用户终端能够认证家乡域网络。

(b)家乡域网络对用户终端的认证：

步骤 1 构造测试分量。在 Bundle 中，随机数 seq 唯一产生于$<s_u, 1>$，所以$<s_h, 1>$为 seq 的主动测试。

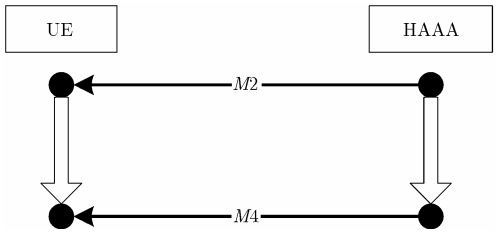

图 3 用户终端和家乡域网络的双方协议的Bundle

步骤 2　定义节点 m。由于 $K_{\mathrm{HU}} \notin K_P$，根据认证测试规则，{cIDue, CTap, CTue, K_U, MACu}只能产生于 C 中正的正常节点 m。m 必为某个 UE 串 s_u' 中的节点。s_u' = Init[{cIDue′, CTap′, CTue′, K_U', MACu′}, {RES′, EnMSK′, MACh′}], m=<s_u', 1>, term(<s_u',1>)={cIDue′, CTap′, CTue′, K_U', MACu′}。

步骤 3　cIDue, CTap, CTue, K_U和 MACu 唯一产生于 s_u串，$K_{\mathrm{HU}} \notin K_P$，则RES′ = RES, EnMSK′ = EnMSK, MACh′ = MACh，从而串 s_u' = s_u。因此家乡域网络能够认证用户终端。

综上所述，用户终端至家乡域网络之间的通信协议的双向认证是成功的。

(2)用户终端和接入点之间的安全性验证：根据改进协议的具体运行流程，可以得到该双方协议的串和轨迹如下：

接入点的串和轨迹：

Init[cIDap, {cIDue, CTap, CTue, K_U, MACu}, {RES, EnMSK, MACh}]
= {+cIDap, −{cIDue, CTap, CTue, K_U, MACu}, +{RES, EnMSK, MACh}}

用户终端的串和轨迹：

Resp[cIDap, {cIDue, CTap, CTue, K_U, MACu}, {RES, EnMSK, MACh}]
= {− cIDap,+{cIDue, CTap, CTue, K_U, MACu}, −{RES, EnMSK, MACh}}

用户终端至接入点的双方协议的 Bundle 如图 4 所示。

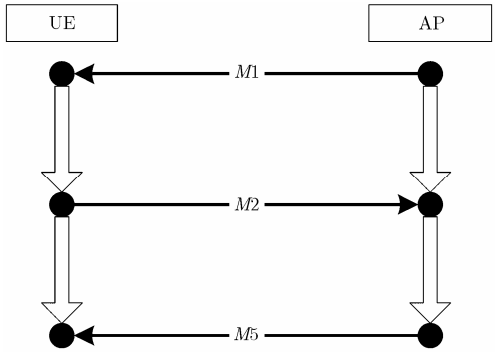

图 4 用户终端和接入点的双方协议的Bundle

(a)接入点对用户终端的认证：

步骤 1　构造测试分量。在 Bundle 中，IDap 唯一产生于 <s_a, 1>, IDap ⊂ cIDap 。因为 CTap = {IDap}K_{HU} , $K_{\mathrm{HU}} \notin K_P$, 所以 CTap 是 IDap 对于<$s_a$, 1>的测试分量。<$s_a$,1>⇒$^+$<$s_a$,2> 是 IDap 的入测试。

步骤 2　定义节点 m。按照认证测试规则，节点 m 为负节点。因此 m 为某个 UE 串中的节点。假设该串为 s_u'= Resp[cIDap′, {cIDue′,CTap′,CTue′, K_U', MACu′}, {RES′, EnMSK′, MACh′}]，且 m = <s_u', 1>, term(<s_u', 1>) = cIDap。

步骤 3　由于 IDap 是在 AP 串中唯一产生的，且 IDap⊂cIDap，因此cIDap′= cIDap。通过比较 term(<s_u', 1>)和 UE 串中的内容得串 s_u' = s_u。因此接入点能够对用户终端进行认证。

(b)用户终端对接入点的认证：

步骤 1　构造测试分量。由于在该 Bundle 中，IDap 唯一产生于<s_a, 1>，且 IDap ⊂ cIDap 。所以对于 IDap 来说，<s_u, 1>构成的测试量为 IDap 的主动测试。

步骤 2　定义节点 m。由于 $K_{\mathrm{HU}} \notin K_P$，根据认证测试规则，cIDap 只能产生于 C 中的正的正常节点 m。m 必为某个 AP 串 s_a' 中的节点。s_a'= Init[cIDap′, {cIDue′, CTap′, CTue′, K_U', MACu′}, {RES′, EnMSK′, MACh′}], m =< s_a', 1>, term (<s_a',1>)= cIDap′。

步骤 3　cIDap 唯一产生于 s_a串，$K_{\mathrm{HU}} \notin K_P$，则 cIDap' =cIDap，从而串 s_a' = s_a。因此用户终端能够认证接入点。

综上所述，用户终端至接入点之间的通信协议的双向通信是安全的。

(3)家乡域网络与接入点之间的安全性验证：通过 Guttman 提出的信任传递性规律，由于家乡域网络和用户终端之间以及用户终端和接入点之间的通信都满足安全需求，所以家乡域网络与接入点之间的通信也是安全的。

4.3 使用验证工具对改进的协议进行安全性验证

针对 EAP-AKA 协议中存在的安全问题，改进协议采取相应措施进行完善。使用安全协议验证工具 AVISPA[16]进行安全性验证的结果表明，改进的协议是安全的(SUMMARY: SAFE)，结果中的统计量还包含运行访问的节点总数 5 个，深度 3 等。

4.4 性能分析

通过开展实验，并与相关协议进行详细的对比分析，具体结果如表 2 所示。

表 2 协议对比

协议	安全性	遍历节点	深度	认证时延(s)
EAP-AKA	不安全	13	5	1.568
EAP-FAKA[8]	安全	10	5	1.418
EAP-SAKA[11]	安全	6	5	1.418
EEPS-AKA[12]	安全	24	6	1.403
改进的 EAP-AKA 协议	安全	5	3	1.343

改进的协议与其它协议相比，具有以下优势：

(1)减少了认证时延：根据文献[1]的模拟结果，完整认证的平均时延为 1.568 s。认证时延 Dauth 可以进一步分为 3 部分：EAP 消息由 UE 发送到接入网信道的发送时延 Dtrans, EAP 消息从 UE 传输到 HAAA 的传播时延 Dprop，以及处理时延 Dtre(数据访问、密钥和标签生成、计算、加解密等)。

此外，在 11 Mbps 的网络中 Dtrans 可忽略不计，因此 Dtrans 远小于 Dprop+Dtre。在改进的协议中：

(a)UE 与 HAAA 之间的传播时延 Dprop_uh 的大小取决于 UE 所处的位置以及本地是否存在 AAA 服务器或代理服务器。传播时延 Dprop 可以分为两部分：UE 与 AP 之间的传播时延 Dprop_ua，以及 AP 与 HAAA 之间的传播时延 Dprop_ah。

完整的 EAP-AKA 协议的认证时延为：Dauth = Dtre + 4Dprop_ua + 4Dprop_ah。改进的协议的认证时延为 Dauth′ = Dtre′ +Dprop_ua+ Dprop_ah。然而根据文献[7]和文献[10], Dprop_uh = Dprop_ua + Dprop_ah 的时间大约是 75 ms。因此，改进的协议在完整的认证过程中，就比原有 EAP-AKA 协议减少了 225 ms，也就是 14.34%的时延。

(b)与 EAP-AKA 相比，改进的协议能更快地检测出认证过程中出现的攻击者和被篡改的参数。协议使用 ECDH 生成密钥，不是需要证书的公钥基础设施，这为家乡域的 AAA 服务器节省了大量的处理时间。

(2)减少了带宽消耗：

(a)在 EAP-AKA 协议中，为了保证 EAP 响应没有被中间结点篡改，需要发送 AKA-身份请求。然而，在改进的协议中，步骤 1 中对 cIDue 和 CTue 的成功解密和对 IDap 的成功验证足以满足这一安全需求，无需再次向 UE 发出身份请求。

(b)改进的协议中不再需要序列号同步过程。因此，原有协议在同步失败的情况下发送重同步消息的带宽消耗也被消除。

5 结束语

本文讨论原有 EAP-AKA 认证协议的缺陷，为了从用户的角度理解安全和服务质量的平衡，回顾对 EAP-AKA 进行改进的相关文献，并指出它们所提出的协议的弱点。在此基础上，提出一种适用于泛在网络中身份认证的改进协议，将传统 EAP-AKA 的适用性从 3G 系统扩展到泛在网络中。新协议简化 EAP-AKA 的认证过程，提高了认证效率，为用户和接入点的身份信息提供有效保护，实现用户终端、家乡域网络以及接入点的相互认证，最后使用认证测试方法和安全协议分析工具证明所提出的改进协议的安全性，并通过开展实验对协议进行比较分析，从而验证了新协议的有效性和高效率。

参 考 文 献

[1] KWON H, CHEON K Y, ROH K H, *et al*. USIM based authentication test-bed for UMTS-WLAN handover[OL]. http://infocom2006.ieee-infocom.org/Posters/1568980767_USIM%20based%20Authentication%20 Test-bed/1568980767_USIM%20based%20Authentication%20Test-bed%20.pdf. 2015.

[2] IETF. RFC 4187 -2006. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)[S]. J Arkko, H Haverinen, 2006.

[3] MUN H, HAN K, and KIM K. 3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA[C]. Wireless Telecommunications Symposium, Prague, 2009: 1–8. doi: 10.1109/WTS.2009.5068983.

[4] CAO J, MA M, LI H, *et al*. A survey on security aspects for LTE and LTE-A networks[J]. *IEEE Communications Survey & Tutorials*, 2014, 16(1): 283–302. doi: 10.1109/SURV.2013.041513.00174.

[5] ANANTHA NARAYANAN V, SURESH KUMAR V, and RAJESWARE A. Enhanced fast iterative localized re-authentication protocol for UMTS-WLAN interworking[C]. 2014 International Conference on Electronics and

Communication Systems (ICECS), Marseille, 2014: 1–5. doi: 10.1109/ECS.2014.6892696.

[6] BOUABIDI I E, DALY I, and ZARAI F. Secure handoff protocol in 3GPP LTE networks[C]. 3rd International Conference on Communication and Networking (ComNet), Hammamet, 2012: 1–6. doi: 10.1109/ComNet.2012.6217746.

[7] SHIDHANI A A and LEUNG V. Local fast re-authentication protocol for 3G-WLAN interworking architecture[C]. Wireless Telecommunications Symposium, Pomona, CA, 2007: 1–8. doi: 10.1109/WTS.2007.4563332.

[8] EL H E I Y, ZAHID N, and JEDRA M. A new fast re-authentication method for the 3G-WLAN interworking based on EAP-AKA[C]. 20th International Conference on Telecommunications (ICT), Casablanca, 2013: 1–5. doi: 10.1109/ICTEL.2013.6632107.

[9] 傅建庆, 陈健, 范容, 等. 基于代理签名的移动通信网络匿名漫游认证协议[J]. 电子与信息学报, 2011, 33(1): 156–162. doi: 10.3724/SP.J.1146.2009.01455.

FU Jianqing, CHEN Jian, FAN Rong, *et al*. Delegation-based protocol for anonymous roaming authentication in mobile communication network[J]. *Journal of Electronics & Information Technology*, 2011, 33 (1): 156–162. doi: 10.3724/SP.J.1146.2009.01455.

[10] IDRISSI Y E H E, ZAHID N, and JEDRA M. Security analysis of 3GPP (LTE)-WLAN interworking and a new local authentication method based on EAP-AKA[C]. 2012 International Conference on Future Generation Communication Technology (FGCT), London, 2012: 137–142. doi: 10.1109/FGCT.2012.6476561.

[11] PATKAR S S and AMBAWADE D D. Secure 3GPP-WLAN authentication protocol based on EAP-AKA[C]. IEEE International Advance Computing Conference (IACC), Banglore, 2015: 1011–1016. doi: 10.1109/IADCC.2015.7154857.

[12] ALEZABI K A, HASHIM F, HASHIM S J, *et al*. An efficient authentication and key agreement protocol for 4G (LTE) networks[C]. 2014 IEEE Region 10 Symposium, Kuala Lumpur, 2014: 502–507. doi: 10.1109/TENCONSpring.2014.6863085.

[13] YU Binbin, ZHANG Jianwu, and WU Zhendong. Improved EAP-AKA protocol based on redirection defense[C]. 9th IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Guangdong, 2014: 543–547. doi: 10.1109/3PGCIC.2014.106.

[14] 侯惠芳, 刘光强, 季新生, 等. 基于公钥的可证明安全的异构无线网络认证方案[J]. 电子与信息学报, 2009, 31(10): 2385–2391. doi: 10.3724/SP.J.1146.2008.01411.

HOU Huifang, LIU Guangqiang, JI Xinsheng, *et al*. Provable security authentication scheme based on public key for heterogeneous wireless network[J]. *Journal of Electronics & Information Technology*, 2009, 31(10): 2385–2391. doi: 10.3724/SP.J.1146.2008.01411.

[15] GUTTMAN J D. Security protocol design via authentication tests[C]. Proceedings of the IEEE Computer Security Foundations Workshop, Cape Breton, 2002: 92–103. doi: 10.1109/CSFW.2002.1021809.

[16] BOZGA L, LAKHNECH Y, and PERIN M. HERMES: An automatic tool for verification of secrecy in security protocols[C]. CAV 2003, LNCS 2725, Berlin Heidelberg, 2003: 219–222. doi: 10.1007/978-3-540-45069-6_23.

戚　湧：男，1970 年生，博士，教授，博士生导师，研究方向为网络信息安全.

郭诗炜：女，1990 年生，硕士生，研究方向为网络信息安全.

李千目：男，1979 年生，博士，教授，博士生导师，研究方向为网络信息安全.