LTE/LTE-A网络中基于盲签名的具有条件隐私保护的切换认证协议

秦宁元[1] 付安民[1,2] 陈守国[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 LTE/LTE-A网络的设计为移动应用提供了较低的切换时延,但LTE标准中的切换过程仍存在一定的复杂性和安全缺陷。为了解决LTE标准和传统切换认证协议的缺陷,设计了一个基于盲签名的切换认证协议。在注册接入阶段通过盲签名建立用于切换过程的认证密钥,在切换过程中通过假名的可变换性和在特定条件下变为真名的可逆性来实现匿名性、不可跟踪性和条件隐私保护。理论分析和仿真结果表明,相较于LTE标准和其他切换认证协议,提出的协议在满足更多安全属性的同时,有更好的性能。

关键词 LTE/LTE-A,盲签名,切换认证,条件隐私保护,前/后向安全
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.031

Blind Signature-based Handover Authentication Protocol with Conditional Privacy Preserving in LTE/LTE-A Networks

QIN Ning-yuan[1] FU An-min[1,2] CHEN Shou-guo[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 LTE/LTE-A is designed to provide low handover latency for mobile applications, but there still exist some complexities and security vulnerabilities. To solve the vulnerabilities in the LTE standard and traditional handover authentication protocols, a new handover authentication protocol based on the blind signature was designed. In the registration phrase, the authentication keys used in the handover phrase are provided by the blind signature, and in the handover phrase, anonymity, untraceability and conditional privacy preserving are achieved by the exchange of the pseudonyms and the reversibility of the real identity. The theoretical analysis and simulation results show that the proposed protocol not only satisfies more security properties, but also has better performance compared with the LTE standard and other handover authentication protocols.

Keywords LTE/LTE-A, Blind signature, Handover authentication, Conditional privacy preserving, Forward/Backward security

1 引言

随着无线通信和多媒体应用的迅速发展,如互联网浏览、互动游戏、移动电视、视频流、音频流等,移动通信技术需要满足移动数据、移动计算和移动多媒体应用的不同需求。LTE/LTE-A(Long Term Evolution/LTE-Advanced)系统的设计包含更少的网络元素,这样改善了系统容量和覆盖范围,能提供较高的数据速率、较低的访问延迟、灵活的带宽和与其他现有无线通信系统的无缝集成[1]。为了适应日益增长的移动数据使用和新的多媒体应用,LTE/LTE-A技术已被3GPP(The 3rd Generation Partnership Project)指定为4G移动通信技术之一。

LTE网络的主要体系结构如图1所示[2],它包含演进分组核心网EPC(Evolved Packet Core)和演进通用无线接入网E-UTRANs(Evolved Universal Terrestrial Radio Access Networks)。一个E-UTRAN由很多称为eNodeB(evolved NodeB)的基站组成,每个eNodeB都可以与用户设备UE(User Equipments)进行通信,由同一个移动管理实体MME(Mobile Management Entity)管理的eNodeB通过接口x2进行通信。

当UE连接到EPC时,MME首先联系归属用户服务器HSS(Home Subscriber Server)来获得相应的认证信息,然后代表EPC通过EPS-AKA(Evolved Packet System Authentication and Key Agreement)协议与UE执行双向认证。

到稿日期:2014-09-16 返修日期:2014-11-21 本文受国家自然科学基金项目(61202352),江苏省自然科学基金项目(BK20141404),教育部博士点基金项目(20123219120030),南京理工大学"紫金之星"项目(2013ZJ0209)资助。
秦宁元(1990—),女,硕士生,主要研究方向为网络与信息安全,E-mail:qinningyuan@qq.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;陈守国(1989—),男,硕士生,主要研究方向为密码学、无线网络安全。

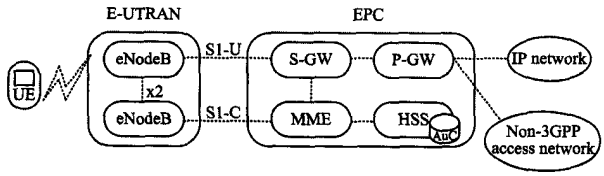

图 1　LTE 网络的体系结构

当 UE 从当前 eNodeB 移动到由同一个 MME 管理的新 eNodeB 进行会话密钥的协商时，也就是执行 MME 之内的切换时，一个稳定和快速的切换过程是必不可少的。一方面，UE 和新 eNodeB 之间需要实现双向认证来抵制恶意攻击；另一方面，因为 UE 是资源受限的设备，所以需要以较低的计算复杂度和较少的通信开销来实现高效的切换。

LTE 标准采用一种链式结构的密钥管理机制，分别将水平密钥派生和垂直密钥派生两种方式作为切换时会话密钥的生成方法，源 eNodeB 可以链接当前密钥和相关参数，同时为多个目标单元生成不同的密钥，若垂直密钥派生所需参数未能及时到达，系统会选择水平密钥派生方式，但这种密钥管理机制仍然存在一些缺陷。文献[3]对 LTE 网络的切换密钥管理机制进行了分析，指出不同的密钥派生方式会增加系统的复杂性。文献[4]指出了水平密钥派生方式缺乏前向安全，也就是攻击者可以从当前会话密钥和一些公开参数获得将来的会话密钥，而垂直密钥派生方式也只是受限的两跳前向安全，因此提出了一种基于代理签名的 LTE 网络统一的切换方案，该方案能抵制去同步攻击，也保证了前向安全，但是不能实现隐私保护。文献[2,5]分析了 LTE 网络的切换过程不能抵抗去同步攻击，恶意 eNodeB 可能会扰乱下一跳链式计数器 NCC(Next-Hop Chaining Counter)值的更新，而 NCC 是垂直密钥派生方式的新鲜参数，若 UE 和目标 eNodeB 的 NCC 值不同步，系统会放弃使用垂直密钥派生方式，而采用水平密钥派生方式，由此会进一步导致将来会话密钥泄露。其中，文献[2]采用一种数学模型，提出了一种周期性更新 LTE 网络根密钥的方法，减小了去同步攻击带来的影响，并且将这个周期进行了最优化处理，使得信号负载和遭受攻击的数据包数量之间得到平衡，但是最优化周期性更新根密钥只能减轻去同步攻击的影响，不能从根本上消除，因而也不能保证前向安全。文献[6]给出了 LTE 网络切换过程不能抵制重放攻击的分析，这样 UE 和目标 eNodeB 就不能建立安全关联，UE 只能尝试发起新的切换请求。文献[7]指出了 4G 网络的切换过程缺乏用户隐私保护机制，用户的私密信息(如身份、移动路径、地理位置等)会暴露，从而导致安全问题。因而文献[7,11]针对无线网络的切换，各提出了一种隐私保护机制，它们均是简单地使用临时身份替代真实身份，但这样只是实现了用户匿名性，不能有条件地保护用户隐私。文献[8-10]指明了在用户匿名性的基础上实现条件隐私保护的重要意义，当用户有违法行为或对系统的不当行为时，安全可信实体能够根据用户的临时身份得到隐藏的真实身份，进而便于执法部门或者系统对用户的违法或不当行为进行仲裁。其中，文献[9]基于双线性对和假名集合，提出了一种无线网络中有条件隐私保护的切换方案；但文献[12]指出该方案不能保证会话密钥的安全性，因为根据扩展的欧几里德算法，由负指数的模运算可以得到乘法逆元，从而导致私钥泄露；文献[10]基于群签名，设计了一种无线网络中有条件隐私保护的切换方案，群管理者拥有透露群成员真实身份的群密钥，但是在实际应用中，从对等用户群中选择一个用户作为可信的群管理者会面临很多问题。

针对上述问题，本文设计了一种基于盲签名的切换认证协议 BHAP(Blind-based Handover Authentication Protocol)，实现了 LTE/LTE-A 网络中 eNodeB 之间安全高效的切换。本文的主要贡献如下：(1)提出了一个基于盲签名的切换认证协议 BHAP，既解决了 LTE/LTE-A 网络切换密钥管理机制存在的安全问题，同时也利用椭圆曲线点乘密码学知识，简化了 LTE/LTE-A 系统中会话密钥的生成方式，实现了安全高效的切换；(2)提出的协议 BHAP 在满足基本安全需求的同时，还能实现条件隐私保护，并通过形式化工具 AVISPA (Automated Validation of Internet Security Protocols and Applications)对协议 BHAP 的安全性进行了仿真分析，结果表明协议 BHAP 能满足其设计的安全目标；(3)在计算开销和通信开销两个方面，用网络仿真工具 NS-3(Network Simulator Version 3)对协议 BHAP 的性能进行了仿真分析，并与 LTE 标准及其他相关方案进行了比较，结果表明协议 BHAP 在满足更多安全属性的同时，依然具有相对较好的性能，可应用于实际场景。

2　提出的切换协议 BHAP

本节给出协议 BHAP 的详细描述，设计的协议 BHAP 分为系统初始化、用户注册、初始认证、切换认证 4 个阶段。表 1 列出 BHAP 所用符号及相应的解释。

表 1　BHAP 所用符号及相应解释

符号	解释
G_1、G_2	循环加法群
q	素数阶
Z_q^*	一个阶为 q−1 的循环群
AuK(AuK_1、AuK_2)	消息认证码密钥
TI_i	UE 的临时身份
Exd	有效时间
tS	时间戳
$ENC_Y(m)$	使用公钥 Y 对消息 m 加密
MAC	使用密钥 AuK 产生的消息认证码
h()	哈希函数 $h():\{0,1\}^* \rightarrow G_1$
$F_{TI}()$	哈希函数 $F_{TI}():\{0,1\}^* \rightarrow Z_q^*$
$F_{KEY}()$	哈希函数 $F_{KEY}():\{0,1\}^* \times G_1 \rightarrow Z_q^*$
K_{eNB}(K_{eNB}^*)	会话密钥

2.1　系统初始化阶段

为了简化系统，MME 作为一个安全管理实体，代表 EPC 按照如下过程设置系统参数。

(1)选择 G_1、G_2 作为两个循环加法群，阶都是大素数 q，P_1、P_2 分别是 G_1、G_2 的生成器。ψ 是 G_2 到 G_1 的同构，满足 $\psi(P_2)=P_1$。

(2)选择随机数 $x \in Z_q^*$ 作为自己的私钥，计算 $Y=xP_2$ 作为公钥。

(3)选择单向哈希函数 $h()$、$F_{TI}()$、$F_{KEY}()$，分别满足映射关系 $h():\{0,1\}^* \rightarrow G_1$，$F_{TI}():\{0,1\}^* \rightarrow Z_q^*$，$F_{KEY}():\{0,1\}^* \times G_1 \rightarrow Z_q^*$。

(4)给每个 UE 和 eNodeB 分发公共系统参数$\{G_1, G_2, q, P_1, P_2, \Psi, Y, h, F_{TI}, F_{KEY}\}$。

2.2　用户注册阶段

当 UE 要连接到 EPC 时，由 MME 代表 HSS/AuC(Au-

thentication Center)完成 UE 到 EPC 的注册，注册过程中的认证还是基于 EPS-AKA 协议中的认证向量 *AVs*(Authentication Vectors)来实现[5]，但是增加了盲签名过程，如图 2 所示。注册完成后，MME 和 UE 之间共享用于切换过程的认证密钥 AuK，同时 MME 为 UE 生成了假名集合，具体过程分为以下几步。

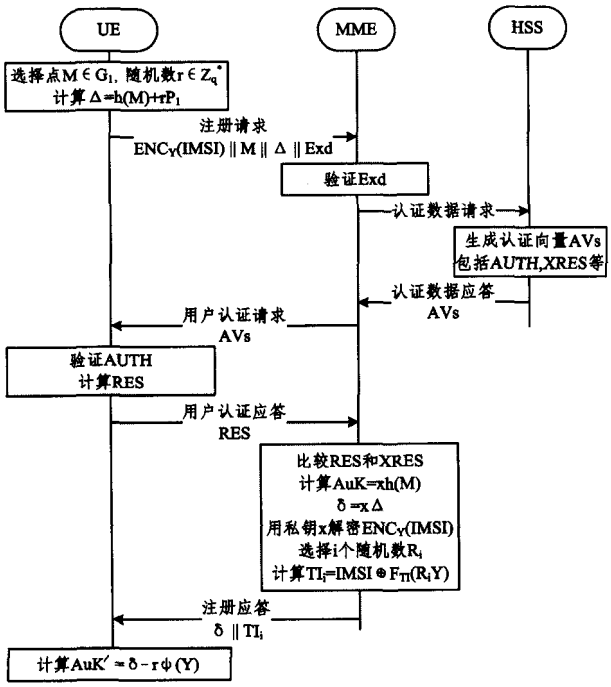

图 2　用户注册过程

(1)UE→MME(注册请求)

UE 随机选择一个点 $M\in G_1$ 作为要被盲化的消息，选择一个随机数 $r\in Z_q^*$ 作为盲化因子，按式(1)将消息 M 盲化成消息 Δ，用公钥 Y 将国际移动用户识别码 *IMSI* (International Mobile Subscriber Identification Number)加密，选择一个合适的失效时间 *Exd*，最后将消息 $ENC_Y(IMSI)\parallel M\parallel\Delta\parallel Exd$ 作为注册请求，发送给 MME。

$$\Delta=M+rP_1 \tag{1}$$

(2)MME→HSS(认证数据请求)

MME 收到注册请求后，首先检验 *Exd* 是否有效，如果失效，则拒绝注册请求；如果有效，则向 HSS 请求关于该用户的认证向量 *AVs*。

(3)HSS→MME(认证数据应答)

HSS 收到认证数据请求后，为用户 UE 生成认证向量 *AVs*，包括认证令牌 *AUTH*(Authentication Token)、预期响应 *XRES*(Expected Response)等消息，将 *AVs* 作为认证数据应答发送给 MME。

(4)MME→UE(用户认证请求)

MME 收到认证数据应答后，向用户 UE 发送认证向量 *AVs* 作为用户认证请求。

(5)UE→MME(用户认证应答)

UE 收到用户认证请求消息 *AVs* 后，首先验证 AUTH 的有效性，如果有效，则计算响应消息 *RES*(Response)，将其作为用户认证应答消息发送给 MME。

(6)MME→UE(注册应答)

MME 收到用户认证应答后，首先比较 *XRES* 和 *RES* 是否相等，如果不相等，则拒绝注册请求；如果相等，根据式(2)和式(3)分别用私钥对消息进行盲签名，生成认证密钥 AuK 和签名 δ，用私钥 x 将 $ENC_Y(IMSI)$ 解密得到 *IMSI*，选择 i 个随机数 R_i，利用式(4)为 UE 生成 i 个临时标识符 TI_i (Temporary ID)，最后将消息 $\delta\parallel TI_i$ 作为注册应答，发送给 UE。

$$AuK=xh(M) \tag{2}$$

$$\delta=x\Delta \tag{3}$$

$$TI_i=IMSI\oplus F_{TI}(R_iY) \tag{4}$$

(7)UE 收到注册应答后，根据式(5)利用自己的盲化因子 r 对盲签名消息 δ 进行去盲化处理，生成认证密钥 AuK'；由式(6)可知 $AuK'=AuK$，即 UE 和 MME 共享认证密钥 AuK。

$$AuK'=\delta-r\Psi(Y) \tag{5}$$

$$AuK'=\delta-r\Psi(Y)=\delta-r\Psi(xP_2)=\delta-xrP_1=x(h(M)+rP_1)-xrP_1=xh(M)=AuK \tag{6}$$

2.3　初始认证阶段

当 UE 第一次连接到 eNodeB 时，需要执行图 3 所示的初始认证，UE 和首次接入的 $eNodeB_1$ 经过两次握手协商会话密钥 K_{eNB}，具体过程分为以下几步。

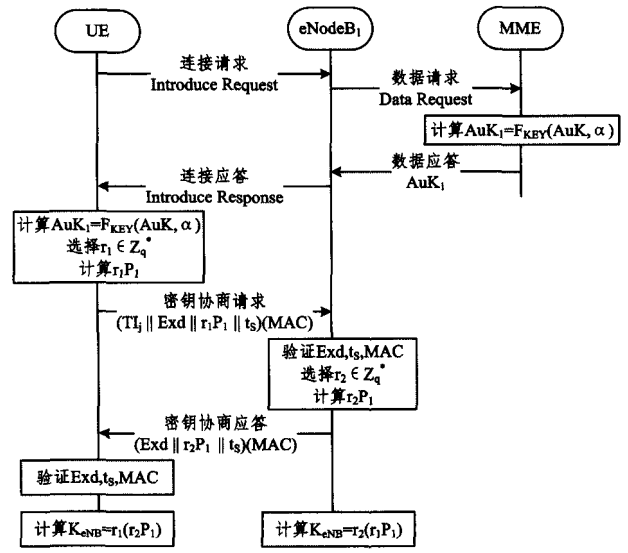

图 3　初始认证过程

(1)UE→$eNodeB_1$(连接请求)。

UE 向 $eNodeB_1$ 发送连接请求消息 Introduce Request。

(2)$eNodeB_1$→MME(数据请求)

$eNodeB_1$ 收到 UE 的连接请求后，向 MME 发送数据请求消息 Data Request。

(3)MME→$eNodeB_1$(数据应答)

MME 收到数据请求后，利用式(7)计算新的认证密钥 AuK_1，α 表示单元级的一些值[2]，如目标单元的物理 ID 和频率，然后将消息 AuK_1 作为数据应答发送给 $eNodeB_1$。

$$AuK_1=F_{KEY}(AuK,\alpha) \tag{7}$$

(4)$eNodeB_1$→UE(连接应答)

$eNodeB_1$ 收到 MME 发送的认证密钥后，向 UE 发送连接应答消息 Introduce Response。

(5)UE→$eNodeB_1$(密钥协商请求)

UE 收到连接应答后，按照式(7)计算 AuK_1，选择随机数 $r_1\in Z_q^*$，计算 r_1P_1，选择临时身份 TI_j($j<j+1\leqslant i$)、合适的

失效时间 Exd 和时间戳 t_S，将消息 $TI_j \| Exd \| r_1P_1 \| t_S$ 和它们的 MAC 值(认证密钥 AuK_1 对消息的加密值)作为密钥协商请求发送给 eNodeB$_1$。

(6)eNodeB$_1$→UE(密钥协商应答)

eNodeB$_1$ 收到密钥协商请求后，首先检验 Exd 和 t_S 是否有效，如果失效，则拒绝请求；如果有效，则利用步骤(3)中收到的 AuK_1 对收到的消息 $TI_j \| Exd \| r_1P_1 \| t_S$ 加密计算 MAC 值，将其与收到的 MAC 值进行比较，如果不同则拒绝请求；如果相同，则选择随机数 $r_2 \in Z_q^*$，计算 r_2P_1，选择合适的失效时间 Exd 和时间戳 t_S，将消息 $Exd \| r_2P_1 \| t_S$ 和它们的 MAC 值作为密钥协商应答，发送给 UE。

(7)UE 收到密钥协商应答后，首先检验 Exd 和 t_S 是否有效，如果失效，则拒绝请求；如果有效，则利用 AuK_1 对收到的消息 $Exd \| r_2P_1 \| t_S$ 加密计算 MAC 值，将其与收到的 MAC 值进行比较，如果不同，则拒绝；如果相同，则生成会话密钥。

在成功完成上面的交互后，UE 和 eNodeB$_1$ 共享会话密钥 $K_{eNB}=r_1(r_2P_1)=r_2(r_1P_1)=r_1r_2P_1$。

2.4 切换认证阶段

UE 由于移动需要从当前 eNodeB$_1$ 切换到目标 eNodeB$_2$ 时，要执行如图 4 所示的切换认证。UE 和目标 eNodeB$_2$ 经过两次握手，协商新的会话密钥 K_{eNB}^*，具体过程分为以下几步。

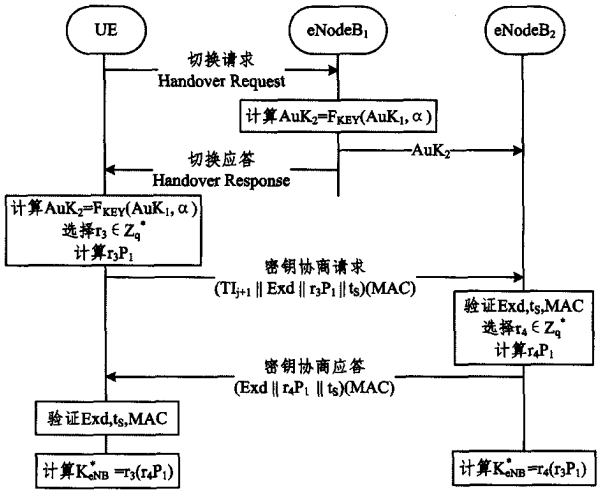

图 4 切换认证过程

(1)UE→eNodeB$_1$(切换请求)

UE 向 eNodeB$_1$ 发送切换请求消息 Handover Request。

(2)eNodeB$_1$→eNodeB$_2$(AuK_2)

eNodeB$_1$→UE(切换应答)

eNodeB$_1$ 收到切换请求后，利用式(8)计算新的认证密钥 AuK_2，将消息 AuK_2 发送给 eNodeB$_2$，然后再向 UE 发送切换应答消息 Handover Response。

$$AuK_2=F_{KEY}(AuK_1,\alpha) \tag{8}$$

(3)UE→eNodeB2(密钥协商请求)

UE 收到切换应答后，按照式(8)计算 AuK_2，选择随机数 $r_3 \in Z_q^*$，计算 r_3P_1，选择临时身份 TI_{j+1}、合适的失效时间 Exd 和时间戳 t_S，将消息 $TI_{j+1} \| Exd \| r_3P_1 \| t_S$ 和它们的 MAC 值作为协商请求发送给 eNodeB$_2$。

(4)eNodeB$_2$→UE(密钥协商应答)

eNodeB$_2$ 收到密钥协商请求后，按照初始认证过程中步骤(6)的方法分别检验 Exd、t_S 和 MAC 值是否有效，如果失效则拒绝请求；如果有效，则选择随机数 $r_4 \in Z_q^*$，计算 r_4P_1，选择合适的失效时间 Exd 和时间戳 t_S，将消息 $Exd \| r_4P_1 \| t_S$ 和它们的 MAC 值作为密钥协商应答消息发送给 UE。

(5)UE 收到密钥协商应答消息后，按照初始认证过程中步骤(7)的方法分别检验 Exd、t_S 和 MAC 值是否有效，如果失效则拒绝请求；如果有效，则生成会话密钥。

在成功完成上面的交互后，UE 和 eNodeB$_2$ 共享新的会话密钥 $K_{eNB}^*=r_3(r_4P_1)=r_4(r_3P_1)=r_3r_4P_1$。

3 安全性分析

本节对协议 BHAP 的安全属性进行了分析，并将其与 LTE 标准及其他切换方案[9,11]进行了比较，分析表明协议 BHAP 能满足更多的安全属性。最后利用形式化验证工具 AVISPA 对 BHAP 的安全性进行了仿真验证，结果表明 BHAP 能够抵制中间人攻击、重放攻击、并行会话攻击等恶意攻击，满足其设计的安全目标。

3.1 安全属性分析

针对 LTE 网络 eNodeB 之间切换的安全需求，从以下几个方面给出协议 BHAP 的安全属性分析。

(1)相互认证：在用户注册阶段，UE 和 MME 主要是通过 LTE 标准中的 EPS-AKA 协议来实现接入过程中的相互认证。我们在 EPS-AKA 协议的基础上增加了一个盲签名机制，UE 通过引入随机数 r 这个盲因子对消息 M 进行盲化(见式(1))；MME 收到被盲化的消息后，用私钥 x 对其进行盲签名，分别生成认证密钥 AuK(见式(2))和盲签名 δ(见式(3))，UE 收到盲签名消息 δ 后，利用只有 UE 自己知道的盲因子 r 将签名的消息 δ 进行去盲化操作，生成认证密钥 AuK'(见式(5))；而 $AuK=AuK'$(见式(6))，因此 UE 和 MME 通过盲签名机制建立了一个共享的认证密钥 AuK，并且 MME 随后将 AuK 和参数 α 单向哈希后生成 AuK_1(见式(7))；安全传输给 UE 首次接入的 eNodeB$_1$，UE 也能由自己的 AuK 和参数 α 生成 AuK_1，这样 UE 和 eNodeB$_1$ 共享 MAC 码密钥 AuK_1，进而可以实现对 MAC 值的验证。由于二次握手协议本来就是一个双向认证协议，因此 UE 和 eNodeB$_1$ 轻易地实现了双向认证。在切换阶段，UE 和 eNodeB$_2$ 共享 MAC 码认证密钥 AuK_2(见式(8))，UE 和 eNodeB$_2$ 依然执行二次握手协议，UE 和 eNodeB$_2$ 也实现了双向认证。因此，无论是在初始认证阶段还是切换认证阶段，UE 和 eNodeB 都实现了双向认证，也就是协议 BHAP 能够检测出非法用户和流氓基站。

(2)前/后向安全：前/后向安全分别指攻击者不能从已获得的密钥材料中导出将要产生的会话密钥和已产生的会话密钥。在协议 BHAP 中，会话密钥 K_{eNB}(或 K_{eNB}^*)是由 UE 和 eNodeB 分别提供的安全参数 r_1 和 r_2(或 r_3，r_4)生成。由于椭圆曲线离散对数问题 ECDLP 和计算性 Diffie-Hellman 问题 CDHP[13]，攻击者无法从参数对 (P,r_iP) 中计算出秘密参数 r_i，也不能通过 (r_1P,r_2P) 计算出密钥 r_1r_2P，因此能够保证后向安全。此外，由于前后两次切换认证是不相关的，协议 BHAP 依然能够提供前向安全。

(3)隐私保护：协议 BHAP 中，在注册阶段，UE 将真实身份用公钥 Y 加密传输，只有 MME 能用私钥 x 对其解密，这样也解决了 UE 通过 EPS-AKA 接入到 EPC 时因明文传输

IMSI 而带来的用户隐私泄露的安全问题[5,14]；在切换过程中，使用临时身份来替代真实身份，由于 R_i 只有安全实体 MME 知道，由式(4)可知，攻击者不能从临时身份 TI_i 推导出 UE 的真实身份 *IMSI*；由于 R_i 的随机性，UE 在不同的切换过程中使用不相关的临时身份，攻击者无法将一个 UE 不同的切换认证阶段联系起来，因此不能跟踪 UE 的移动路径。

在一些紧急情况下，如 UE 违反了法律或者 UE 的不当行为对系统造成了伤害，需要由安全实体 MME 提供 UE 的真实身份，以便执法部门或系统对 UE 的违法行为或不当行为进行仲裁。根据异或运算的性质[15]，MME 可以利用式(9)计算得到用户的真实身份 *IMSI*。因此，协议 BHAP 能够实现条件隐私保护。

$$IMSI = TI_i \oplus F_{TI}(R_i Y) \tag{9}$$

(4)反重放攻击：目前，抵制重放攻击的有效方法是在消息中添加随机数或者时间戳。在协议 BHAP 中，由于密钥协商消息都增加了时间戳 t_S，因此攻击者无法发动重放攻击。

(5)安全性比较：表 2 给出了协议 BHAP 和 LTE 标准、基于双线性对的条件隐私保护切换方案[9]及基于代理签名的隐私保护切换方案[11]在安全属性方面的比较，其中 Y 表示满足该条安全属性，N 表示不满足该条安全属性。从表 2 中可以看出：协议 BHAP 相比 LTE 标准和其他切换方案[9,11]更加安全。

表 2　不同方案的安全属性比较

	BHAP	LTE 标准	文献[9]	文献[11]
相互认证	Y	Y	Y	Y
前/后向安全	Y	N	N	Y
隐私保护	Y	N	Y	Y
条件隐私保护	Y	N	Y	N
反重放攻击	Y	N	Y	Y

3.2　形式化验证

除了上述安全属性的分析和比较，为了确保协议 BHAP 能抵制恶意攻击，满足其设计的安全目标，利用形式化工具 AVISPA 对协议 BHAP 安全性进行了验证。作为网络安全协议和应用的形式化验证工具，AVISPA 被安全协议的开发者广泛用于安全协议潜在攻击的检测[4,10,16]。此外，AVISPA 项目组将网络工程任务组 IETF(Internet Engineering Task Force)标准化的安全协议用来分析，发现了一些存在的安全缺陷[16]。

AVISPA 提供一种称为 HLPSL(High Level Protocol Specification Language)的形式化语言用于协议的建模和 4 种不同的分析终端即 OFMC(On-the-fly Model Checker)、CL-AtSe(Constraint-Logic-based Attack Searcher)、SATMC(SAT-based Model-Checker)、TA4SP(Tree Automata based on Automatic Approximations for the Analysis of Security Protocols)用于协议的安全性检测。4 种终端的分析原理和侧重点均有不同，不同的终端可能会产生不同的分析结果。如果协议达到了预期的安全目标，则给出安全的结果及相应的分析数据。如果协议不安全，分析终端将说明是哪一个预期的安全目标未实现，并给出相应的攻击轨迹。

协议 BHAP 切换过程的 HLPSL 描述中，有两个基本角色 ue 和 bs 分别代表 UE 和 $eNodeB_2$，这里只给出了 ue 的 HLPSL 描述，如图 5 所示。目前版本的 HLPSL 的描述只支持保密和认证两个安全目标，但这足以用来说明大量的安全问题[4]，如保密性、双向认证性、中间人攻击检测、重放攻击检测、并行会话攻击检测等。图 5 中“witness(UE,BS,bs_ue_mac,Mac1′)”用于 UE 对 $eNodeB_2$ 基于 *MAC* 值的认证；类似地，“request(UE,BS,ue_bs_mac,Mac2′)”用于 eNodeB2 对 UE 基于 *MAC* 值的认证，从而保证了双向认证；另外，“secret(PTK1′,ptk1,{UE,BS})”保证了主会话密钥 K_{eNB}^{*} 不被攻击者获取，攻击者无法获取保密值，也就无法发动恶意攻击。

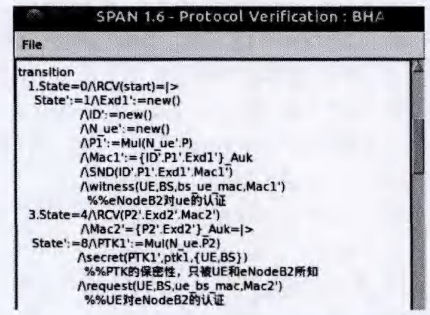

图 5　UE 的 HLPSL 描述

AVISPA 检测结果如图 6 所示，OFMC、CL-AtSe 以及 SATMC 的检测结果表明，协议 BHAP 的切换过程是安全的(SAFE)，能够实现预期的安全目标，抵制重放攻击、中间人攻击等恶意攻击；TA4SP 验证模型结果显示不确定(INCONCLUSIVE)，是因为目前 TA4SP 模块不支持单向哈希运算，而本文设计的协议 BHAP 涉及到了单向哈希运算。

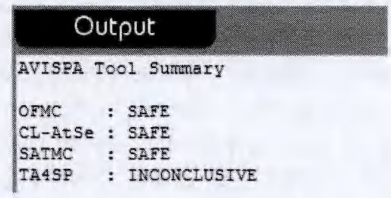

图 6　AVISPA 的仿真结果

4　性能分析

考虑到 UE 是资源受限的设备，协议 BHAP 在满足安全需求、保证安全性的同时，也要具有较好的性能。计算开销和通信开销是切换时延的两个重要度量，本节将协议 BHAP 和 LTE 标准以及其他切换方案[9,11]在这两个方面进行了分析比较。由于上述各方案的网络环境存在一定的差异，为了实验数据的可对比性，均以 LTE 网络为仿真环境。结果表明，协议 BHAP 在满足更多安全属性的基础上，依然有较好的性能。

4.1　计算开销

计算开销指参与切换过程的实体进行密码学操作的时间和。表 3 给出了具体的计算开销缩写及含义；表 4 分别统计了协议 BHAP、LTE 标准和其他切换方案[9,11]在 UE 和 eNodeB 两端的计算开销。

表 3　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_{MAC}	一次 MAC 运算的时间
T_M	一次点乘运算的时间
T_P	一次线性对运算时间

表4 计算开销比较

方案	计算开销 $[T_H, T_S, T_{MAC}, T_M, T_P]$	
	UE	eNodeB
LTE 标准	[4,0,0,0,0]	[2,0,0,0,0]
[9]	[4,0,0,2,1]	[2,0,0,2,3]
[11]	[1,0,1,2,0]	[3,2,1,5,0]
BHAP	[1,0,2,2,0]	[1,0,2,2,0]

从表4中可以看出，协议 BHAP 在切换认证过程中主要涉及点乘运算、MAC 运算和哈希运算。协议 BHAP 的计算开销明显小于文献[9]的，高于只涉及 6 次哈希运算的 LTE 标准；但是，简单的哈希运算不能保证会话密钥的前向安全性。文献[9]在 UE 和 eNodeB 两端主要涉及双线性对运算、点乘运算和哈希运算，这些计算会带来很大的计算开销，尤其是在计算能力有限的 UE 端，因此在切换认证过程中大大增加了切换时延；文献[11]使用代理签名实现隐私保护，主要涉及 MAC 运算、点乘运算和哈希运算，相比文献[11]，协议 BHAP 少了 3 次点乘运算，减小了切换认证过程中的计算开销。

4.2 通信开销

通信开销指参与切换过程的实体之间进行消息交互的时间和。在切换认证过程中，记 T_W 为 UE/MN(Mobile Node)与 eNodeB/AP(Access Point)之间的通信时延，T_A 为 eNodeB/AP 与 MME/AAA(Authentication Authorizing and Accounting)服务器之间的通信时延，T_E 为 eNodeB/AP 之间的通信时延。由于 MME/AAA 服务器与 eNodeB/AP 之间的距离很远，因此 T_A 的值远大于 T_W 和 T_E 的值。表5给出了各个协议的通信时延比较。从表5中可以看出，协议 BHAP 完成一次切换认证的通信开销比 LTE 标准和文献[11]低，因为 LTE 标准中 UE 需要与 MME 通信，这会带来很大的通信开销；文献[11]虽然不涉及 eNodeB 之间的通信，但是有 5 次 T_W。文献[9]由于在初始认证阶段由 AAA 服务器为所有 AP 分发公私钥，因此在切换过程中只需两次握手，只有 2 次 T_W。相比文献[9]，协议 BHAP 没有采用事先全部分发认证密钥，而是采用先请求再分发，通信性能上虽然没有明显的优势，但是更安全。

表5 通信开销比较

方案	T_W	T_A	T_E
LTE 标准	3	1	2
[9]	2	0	0
[11]	5	0	0
BHAP	4	0	1

4.3 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)，利用网络仿真工具 NS3.19[17] 对以上各方案的切换过程进行仿真。仿真机器配置如下：32 位操作系统，Intel Core I5(3470)处理器，主频 3.2GHz。仿真参数如下[18]：信噪比为 5dB，传输功率是 30dB，eNodeB 与 MME 之间有线链路带宽为 2Gbps，eNodeB 之间的有线连接带宽 500Mbps，采用基于 x2 接口的切换模式来模拟源 eNodeB 与目标 eNodeB 之间的切换，MAC 层的调度为 ns3::RrFfMacScheduler，无线资源控制协议 RRC(Radio Resource Control)设置为 IdealRrc，通过手动触发模式来触发切换认证过程，切换算法为 NoOpHandoverAlgorithm。仿真环境如下：创建一个源 eNodeB 和一个目标 eNodeB，两个节点之间相距 200m，创建一个 MME 节点与 eNodeB 相距 10km，UE 节点从源 eNodeB 切换到目标 eNodeB，改变 UE 节点的个数，分别统计切换时延(ms)。

各方案的切换时延与 UE 个数的变化关系如图7所示。由图7可以看出，协议 BHAP 的切换时延比 LTE 标准和文献[9,11]小，尤其相比文献[9]，切换时延减少了近 70%。上述所有方案的切换时延都随 UE 个数的增加而近似线性增长，因为接入点 eNodeB 能够处理多个 UE 的切换请求，随着 UE 的增加，切换时延不会成倍增加，而多个 UE 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。

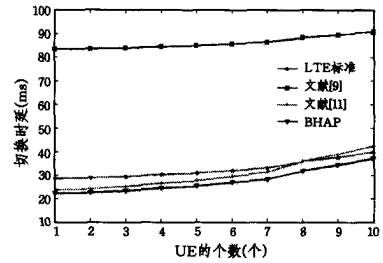

图7 切换时延与 UE 个数的关系

总之，协议 BHAP 在满足更多安全属性的同时，相比 LTE 标准和文献[9,11]有更好的性能，可应用于实际场景。

结束语 本文针对 LTA/LTE-A 网络中 eNodeB 之间的切换，提出了一种基于盲签名的切换协议 BHAP。该方案在解决了现存 LTE 机制安全缺陷的基础上，还能实现条件隐私保护。安全和性能分析表明，协议 BHAP 在满足更多安全属性的条件下，也有相对较好的性能，可应用于实际场景。由于 LTE-A 网络引入了 HeNB(Home-eNodeB)，在接下来的工作中，将对 BHAP 协议进行优化和扩展并将其应用于 eNodeB 之间、HeNB 之间、eNodeB 和 HeNB 之间以及 MME 之间安全高效的切换。

参 考 文 献

[1] Astely D, Dahlman A, Furuskar A, et al. LTE: The Evolution of Mobile Broadband[J]. IEEE Communications Magazine, 2009, 47(4): 44-51

[2] Han C, Choi H. Security Analysis of Handover Key Management in 4G LTE/SAE Networks[J]. IEEE Transactions on Mobile Computing, 2014, 13(2): 457-468

[3] Forsberg D. LTE key management analysis with session keys context[J]. Computer Communications, 2010, 33(16): 1907-1915

[4] Cao J, Li H, Ma M, et al. A simple and robust handover authentication between HeNB and eNB in LTE networks[J]. Computer Networks, 2012, 56(8): 2119-2131

[5] Cao J, Ma M, Li H, et al. A Survey on Security Aspects for LTE and LTE-A Networks[J]. IEEE Communications Surveys and Tutorials, 2014, 16(1): 283-302

[6] Han C K. Security Analysis and Enhancements in LTE-Advanced Networks[D]. Seoul: Sungkyunkwan University, 2011

[7] Nicanfar H, Hajipour J, Agharebparast F, et al. Privacy-preserving handover mechanism in 4G[C]//IEEE Conference on Communications and Network Security. Washington, 2013: 373-374

[8] He D, Chen C, Bu J, et al. Security and efficiency in roaming

services for wireless networks: challenges, approaches, and prospects[J]. IEEE Communications Magazine, 2013, 51(2): 142-150

[9] He D, Chen C, Chan S, et al. Secure and efficient handover authentication based on bilinear pairing functions[J]. IEEE Transactions on Wireless Communications, 2012, 11(1): 48-53

[10] He D, Bu J, Chan S, et al. Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks [J]. IEEE Transactions on Computers, 2013, 62(3): 616-622

[11] Jing Q, Zhang Y, Fu A, et al. A privacy preserving handover authentication scheme for EAP-based wireless networks [C] // IEEE Global Telecommunications Conference. Houston, 2011: 1-6

[12] He D, Chen C, Chan S, et al. Analysis and improvement of a secure and efficient handover authentication for wireless networks [J]. IEEE Communications Letters, 2012, 16(8): 1270-1273

[13] Fu A, Lan S, Huang B, et al. A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks[J]. IEEE Communications Letters, 2012, 16(11): 1744-1747

[14] Lai C, Li H, Lu R, et al. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks [J]. Computer Networks, 2013, 57(17): 3492-3510

[15] Lee C, Lai Y M. Toward a secure batch verification with group testing for VANET[J]. Wireless networks, 2013, 19(6): 1441-1449

[16] Chen C, He D, Chan S, et al. Lightweight and provably secure user authentication with anonymity for the global mobility network [J]. International Journal of Communication Systems, 2011, 24(3): 347-362

[17] The NS-3 Consortium. NS3 tutorial[OL]. http://www.nsnam.org

[18] Baldo N, Requena-Esteso M, Miozzo M, et al. An open source model for the simulation of LTE handover scenarios and algorithms in ns-3 [C] // Proceedings of 16th ACM International Conference on Modeling, Analysis & Simulation of Wireless and Mobile Systems. Barcelona, 2013: 289-298

(上接第 144 页)

[4] Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations: ESD-TR-73-278, I(AD)770768[R]. Bedford, UK: MITRE Corporation, 1973

[5] Bell D E, LaPadula L J. Secure Computer System: A Mathematical Model[R]. Bedford, MA: Electronic Systems Division, Air Force System Command, Hanscom AFB, 1973

[6] Shen Ying, Xiong L R. Lattic based BLP extended model [C]// Proc of the 2nd International Conference on Future Information Technology and Management Engineering. 2009: 309-312

[7] Liang H L, Sun Y F, Zhao Q S, et al. Design and implementation of a security label common framework [J]. Journal of Software, 2003, 14(3): 547-552

[8] 蔡谊, 郑志蓉, 沈昌祥. 基于多级安全策略的二维标识模型[J]. 计算机学报, 2004, 27(5): 619-624
Cai Yi, Zheng Zhi-rong, Shen Chang-xiang. A Planar Attributes Model Based on Multi Level Security Policy [J]. Chinese Journal of Computers, 2004, 27(5): 619-624

[9] 刘彦明, 董庆宽, 李小平. BLP 模型的完整性增强研究[J]. 通信学报, 2010, 31(2): 100-106
Liu Yan-ming, Dong Qing-kuan, Li Xiao-ping. Study on enhancing integrity for BLP model[J]. Journal on Communications, 2010, 31(2): 100-106

[10] Lee T M P. Using mandatory integrity to enforce "commercial" security[C]// Proc of IEEE Conference on Security and Privacy. Washington DC: IEEE Computer Society, 1998: 140-146

[11] Schell R, Tao T F, Heckmn M. Designing the GEMSOS security kernel for security and performance[C]// Proc of the 8th National Computer Security Conference. 1985: 108-119

[12] 聂晓伟, 冯登国. 基于动态可信度的可调节安全模型[J]. 通信学报, 2008, 29(10): 37-44
Nie Xiao-wei, Feng Deng-guo. Modified security model based on dynamic trusted degree [J]. Journal on Communications, 2008, 29(10): 37-44

[13] 谭智勇, 刘铎, 司天歌, 等. 一种具有可信度特征的多级安全模型[J]. 电子学报, 2008, 36(8): 1637-1641
Tan Zhi-yong, Liu Duo, Si Tian-ge, et al. Multilevel Security Model with Credibility Characteristics [J]. Acta Electronica Sinica, 2008, 36(8): 1637-1641

[14] Yamaguchi F, Lindner F, Rieck K. Vulnerability extrapolation: Assisted discovery of vulnerabilities using machine learning[C]// Proceedings of the 5th USENIX Conference on offensive Technologies. USENIX Association, 2011: 13-13

[15] 顾亚祥, 丁世飞. 支持向量机研究进展[J]. 计算机科学, 2011, 38(2): 14-17
Gu Ya-xiang, Ding Shi-fei. Advances of Support Vector Machines [J]. Computer Science, 2011, 38(2): 14-17

[16] Bozorgi M, Saul L K, Savage S, et al. Beyond heuristics: learning to classify vulnerabilities and predict exploits[C]// Proc. of 16th Int. Conf. on Knowledge discovery and Data Mining. ACM, 2010: 105-144

[17] 谭小彬, 王卫平, 奚宏生, 等. 计算机系统入侵检测的隐马尔可夫模型[J]. 计算机研究与发展, 2003, 40(2): 245-250
Tan Xiao-bin, Wang Wei-ping, Xi Hong-sheng, et al. A Hidden Markov Model Used in Intrusion Detection [J]. Journal of Computer Research and Development, 2003, 40(2): 245-250

[18] Tjhai G C, Furnell S M, PaPadaki M, et al. A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm [J]. Computers & Security, 2010, 29(6): 712-723

[19] 王辉, 陈泓予, 刘淑芬, 等. 基于改进朴素贝叶斯算法的入侵检测系统[J]. 计算机科学, 2014, 41(4): 111-115, 119
Wang Hui, Chen Hong-yu, Liu Shu-fen, et al. Intrusion Detection System Based on Improved Naïve Bayesian Algorithm[J]. Computer Science, 2014, 41(4): 111-115, 119

[20] Seifert C, Welch I, Komisarczuk P. Identification of malicious Web pages with static heuristics[C]// Proc. of Telecommunication Networks and Applications Conference. 2008: 91-96

[21] 张健, 陈松乔. 一种基于最大熵原理系统异常检测模型研究[J]. 小型微型计算机系统, 2008, 29(4): 643-648
Zhang Jian, Chen Song-qiao. Research on an Abnormal Detect Model for System Call Sequence Using Maximum Entropy Principle [J]. Journal of Chinese Computer System, 2008, 29(4): 643-648