一种新型的 LTE-A 网络切换认证协议

陈 昕,宋亚鹏,刘志强
(北京信息科技大学计算机学院,北京 100101)

摘 要: 针对典型蜂窝网络 LTE-A 网络的切换认证问题,本文通过引入 SDN(Software Defined Network,软件定义网络),提出了软件定义 LTE-A 异构网络架构,在中心控制器中共享 UE(User Equipment,用户设备)的安全上下文信息,以实现简化切换认证过程,提高认证效率的目标. 中心控制器的加入,使蜂窝与核心网通信时需要增加一次信令开销,而 LTE-A 网络的标准切换认证方法过于复杂,应用在软件定义 LTE-A 异构网络中,会产生较多的信令开销. 基于代理签名的切换认证方法,使 UE 在验证身份时不用经过核心网,减少了信令开销. 在安全性相同的情况下,基于椭圆曲线的加密体系比基于 RSA 的加密体系计算量更小,有利于减少中心控制器的计算压力. 本文采用椭圆曲线代理签名方法,提出了一种新型的切换认证协议,并运用着色 Petri 网进行建模和仿真分析. 仿真结果表明,该协议是有效的,且安全性更高.

关键词: LTE-A; 切换认证; SDN (Software Defined Network); 椭圆曲线代理签名; 着色 Petir 网
中图分类号: TP391.9 **文献标识码:** A **文章编号:** 0372-2112 (2017)02-0485-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.02.030

A New Handover Authentication Protocol for LTE-A Network

CHEN Xin, SONG Ya-peng, LIU Zhi-qiang
(*School of Computer Science, Beijing Information Science & Technology University, Beijing* 100101, *China*)

Abstract: Aiming at the handover authentication in the LTE-A, SDN is introduced and a new heterogeneous network framework named Software Defined LTE-A is proposed. This framework simplifies the handover authentication via the sharing of security context information in the Controllers. The use of Controller leads to one more communication overhead when the base station communicates to the core network. The standard handover authentication in LTE-A is a complex system that will generate a lot of communication overhead. The handover authentication based on proxy signature make the UE (User Equipment) need not to communicate to core network when UE is authenticated, which reduces the communication overhead. Compared to RSA Cryptography, the Elliptic Curve Cryptography needs less computation that will decrease the computation overhead in the Controller. Adopted the proxy signature based on the Elliptic Curve, a new handover authentication protocol is proposed, and is modeled, simulated, and analyzed by the Colored Petri Nets. The results of the simulation show that the proposed handover authentication is efficient and more secure.

Key words: LTE-A; handover authentication; SDN (software defined network); proxy signature based on elliptic curve; colored Petri Nets

1 引言

随着 iPhone、iPad、Kindle 等移动终端设备的普及,移动互联网产生的数据流量迅速增长[1]. 思科预测在 2014 年到 2019 年之间,移动数据流量将增加 10 倍[2]. 为了减少单个基站上数据流量的压力,一个有效的解决方法是增加基站的密度. 然而,基站密度的增加,会使 UE 在移动过程中产生更频繁的切换. LTE-A 标准中,用户的切换认证过程是一个复杂的系统[3],它将在频繁的切换过程中占据较多的时间.

目前,针对稠密基站的管理问题,斯坦福大学的 Aditya Gudipati 等人提出了软件定义的无线接入网模

收稿日期:2015-10-08;修回日期:2016-09-06;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61370065, No. 61502040);国家十二五科技支撑计划(No. 2015BAK12B03-3);北京市优秀人才培养资助青年骨干个人项目(No. 2014000020124G099)

型[4],将 UE 的传输功率控制、切换控制和上行链路资源块分配等控制面功能从 eNB(evolved Node B,演进型基站)分离到中心控制器(Controller)上统一管理,从全局出发平衡各基站的资源,提高管理效率. 贝尔实验室的 Sourjya Bhaumik 等人在文献[5]提出了将基站的数据面和控制面功能全部转移到中心控制器上,基站只保留转发功能和物理层的部分控制功能,该架构能让系统减少 22% 的计算资源. 文献[6]将 SDN 引入 5G 移动网络,通过在接入点中共享用户的安全上下文信息,提高了用户切换认证和隐私保护的效率. 本文将利用 SDN 的思想,把 LTE-A 网络中切换过程的控制面分离到一个中心控制器上,在一定条件下简化了 UE 的切换认证过程.

近几年来,针对 LTE-A 的切换认证问题,许多文献提出了不同方法. 文献[7]通过复用保存在旧 MME 中的密钥,降低跨 MME 切换的认证时间. 文献[8]提出了基于 AAA 认证服务器的切换认证方法,但由于 AAA 认证服务器可能离 eNB 很远,会增加通信时间和连接失败的机率. 并且每次认证都需要 AAA 服务器的参与,会增加系统的复杂性. 文献[9]采用利用 Diffie-Hellman 密钥交换机制进行密钥协商,它比基于 AAA 认证服务器的切换认证机制更简捷. 文献[10]中使用代理签名将源 eNB 或 AAA 认证服务器的权力授予 UE,目标 eNB 根据 UE 持有的代理签名可以验证 UE 的身份. 这种方法必须在源 eNB 和目标 eNB 之间建立可信连接,增加认证过程的复杂性. 文献[11]使用代理签名将 HSS(Home Subscriber Server,归属签约用户服务器)的权力授予 eNB 和 UE,使 UE 直接与目标 eNB 相互验证身份,且通过 Diffie-Hellman 密钥交换机制进行密钥协商. 与前几篇文献相比,文献[11]在通信开销和计算量方面更优. 本文将在文献[11]的基础上,引入 SDN 思想和椭圆曲线代理签名的方法,使得 UE 在一定范围内移动时,其切换认证过程的通信开销和计算量更优于文献[11].

2 软件定义 LTE-A 异构网络架构

软件定义网络(Software Defined Network,SDN)是一种新型的网络架构,它的设计理念是将网络的控制平面与数据转发平面进行分离,从而通过集中的控制器中的软件平台去实现可编程化控制底层硬件,实现对网络资源灵活的按需调配.

在 LTE-A 网络架构中,切换认证属于控制面的功能[12~14],需要 MME(Mobility Management Entity,移动管理实体)和 HSS 的参与. 根据 SDN 的设计思想,将与切换认证有关的控制面功能和数据面功能,分离到 Controller 上统一管理,构建出软件定义 LTE-A 异构网络,如图 1 所示. 其变化是在 E-UTRAN 中加入 Controller,集中周围 20~30 个基站的切换控制功能. 连接在同一个 Controller 上的基站必须属于同一个 MME,不能跨 MME.

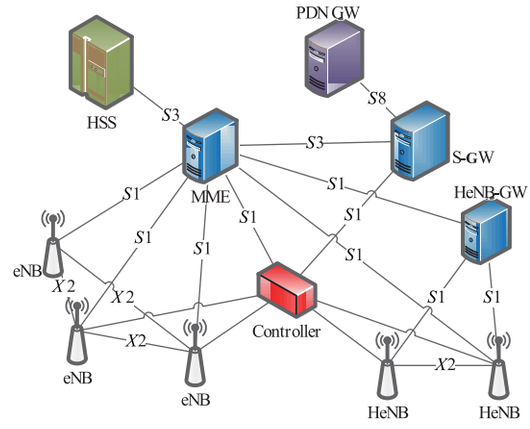

图1 软件定义LTE-A异构网络架构

LTE-A 网络中的基站分为 eNB 和 HeNB[15],这是称之为“异构网络”的原因. 在软件定义 LTE-A 网络中,eNB 和 HeNB 都直接连接在 Controller 上. 取消 eNB\HeNB 到 S-GW 的 S1 接口,建立 Controller 到 S-GW 的 S1 接口,即将 eNB\HeNB 的 IP 报头压缩加密功能,和将用户数据导向 S-GW 的功能分离到 Controller 上. 保留 eNB\HeNB 到 MME 的 S1 接口,并建立 Controller 到 MME 的 S1 接口. Controller 代替 eNB\HeNB 与 MME 进行信令交换,但是这只包括与切换认证和 CSG(Closed Subscriber Group,闭合签约用户组)处理相关的信令,eNB\HeNB 依然能与 MME 进行其它功能的信令交互. 另外,eNB\HeNB 还保留移动和调度的测量、测量报告配置、频谱资源管理和数据转发等其它功能. 由于 Controller 离 eNB\HeNB 较近,所以 Controller 与 eNB\HeNB 的信令交互不会花费太多时间.

3 软件定义 LTE-A 异构网络下的切换认证协议

在标准 LTE-A 网络架构下切换认证时,基站到 MME 需要一次信令交换. 而在软件定义的 LTE-A 异构网络下,基站到 MME 之间需要基站-控制器和控制器-MME 两次信令交换. LTE-A 中的切换认证方法和密钥生成机制过于繁锁[3],在新架构中会大大增加信令交换次数. 针对上述问题,提出了基于椭圆曲线代理签名[16,17]的切换认证方法.

3.1 初始阶段

在 UE 第一次连接 E-UTRAN 时,由 MME 向 UE 发送一个原始签名人为 HSS 的代理签名认证向量($\boldsymbol{\delta}_{\text{H-U}}$, $\boldsymbol{e}_{\text{UE}}$, $\boldsymbol{K}_{\text{H-U}}$),并储存在 UE 中[11]. 其中,

$\boldsymbol{e}_{UE} = h(M_{UE} \| K_{H\text{-}U})$

$\delta = (K_{H\text{-}U})_x t_{H\text{-}U} + e(y_0)_x x_0 \bmod n$

$t_{H\text{-}U}$是由 HSS 生成的随机数,x_o 是 HSS 的私钥.

对于 Controller 也相同,保存一个认证向量($\boldsymbol{\delta}_{H\text{-}C}$, $\boldsymbol{e}_C$,$\boldsymbol{K}_{H\text{-}C}$).

3.2　切换认证阶段

当 UE 从当前 eNB 移动到目标 eNB 时,UE 与目标 eNB 之间需要进行身份的相互验证和密钥协商. 由于 Controller 的作用范围较小,它对于跨 MME 切换的效率没有太大影响. 因此,本协议解决 UE 在同一 MME 下的切换问题,它包括 LTE-A 标准切换中的基于 *X*2 接口的切换、基于 *S*1 接口的 MME 内部切换和基于 *S*1 接口的目标 eNB 是 HeNB 的切换.

(1) UE → eNB2: Handover Request ((((R_{UE}, S_{UE}), M_{UE}, m_{H-U}, K_{H-U}), C_ID)

UE 选择一个随机数 t_{UE},计算 $R_{UE} = t_{UE} G$,根据 Hwang[17] 的签名方法生成代理签名 S_{UE},如公式(1)所示. 其中,M_{UE} 包括 UE 临时 ID(GUTI, Globally Unique Temporary Identify)、PCI、ECGI、目标 TAI、CSG ID,C_ID 是 UE 当前连接的 eNB2 所属的控制器. 然后,UE 将切换请求信息发送给 eNB2.

$$S_{UE} = (R_{UE})_x t_{UE} + \delta_{H-U} h(M_{UE} \| C\_ID \| (R_{UE})_x) \bmod n \tag{1}$$

(2)eNB2 检查切换请求信息中的 C_ID 参数,与 eNB2 所属的 Controller 的身份标识比较. 如果 eNB1 和 eNB2 属于同一个 Controller,则不需要生成新的密钥,跳到(10). 如果 eNB1 与 eNB2 属于不同的 Controller,则将切换请求信息转发给 Controller,即执行(3).

(3) eNB2 → Controller2: Handover Request ((((R_{UE}, S_{UE}), M_{UE}, m_{H-U}, K_{H-U}), C_ID)

(4)验证 S_{UE},并计算共享密钥 K_{U-C}.

接收到切换请求后,Controller2 根据公式(2)验证代理签名是否合法. 如果验证失败,则 UE 的身份不合法,Controller 向 UE 返回切换失败的消息及失败原因.

$$S_{UE}G = (R_{UE})_x R_{UE} + [(K_{H-U})_x (K_{H-U}) + e_{UE}(y_0)_x y_0] h(M_{UE} \| C\_ID \| (R_{UE})_x) \tag{2}$$

如果验证通过,则说明 UE 的身份合法. 然后 Controller 检查 CSG ID,如果 eNB2 是闭合的 HeNB 或混和的 HeNB,则跳转到(5). 如果不是,则跳转到(6).

(5)CSG 验证

(5*a*) Controller2 → MME: Handover Request (CSG ID,Cell Access Mode)

Controller2 将包含 CSG ID 和小区接入模式两个参数的切换请求消息发送给 MME.

(5*b*) MME→Controller2: Handover Request ACK

MME 根据 CSG ID 对 UE 进行接入控制,如果接入控制过程失败,则向 UE 返回切换失败的消息,结束切换认证过程. 否则,MME 决定 UE 的 CSG 成员状态,然后将包含目标 CSG ID 和 CSG 成员状态的切换确认消息发送给 Controller2.

(6) Controller2 → eNB2: Handover Response (($R_C S_C$), M_C, $e_C K_C$)

Controller2 选择一个随机数 t_C,计算出 $R_C = t_C G$,然后 Controller2 通过公式 $K_{U-C} = t_C R_{UE} G$ 计算出共享密钥 K_{U-C},K_{U-C}用于对 UE 与 Controller 之间的通信数据加密. 利用公式(1)计算出代理签名 S_C,然后将包含必要参数的认证应答消息发送给 eNB2. 其中,M_C 包括 PCI、ECGI、目标 TAI、可选的 CSG ID 以及其它与加密算法有关的公共参数.

(7) eNB2→UE: Handover Response ((R_C, S_C), M_C, e_C, K_C, $h(K_{U-C}, K_C)$)

(8)验证 S_C,并计算共享密钥 K_{U-C}.

UE 接收到切换响应消息后,根据公式(2)验证代理签名是否合法. 如果验证失败,则 UE 再次发出切换请求. 如果验证成功,则 UE 确定 Controller2 的身份是合法的,然后计算共享密钥 $K_{U-C} = t_{UE} R_C G$. 最后,UE 计算 $h(K_{U-C}, K_C)$,如果得到的散列值与切换响应消息中的相等,则证明产生的密钥是正确的.

(9) UE → eNB2: Handover Acknowledge (Success/Fail)

(10) eNB2→MME: Path Switch Request (target TAI, ECGI, C_ID)

Controller 只参与到切换认证过程中,切换认证完成后,资源分配、小区追踪等功能由 eNB 完成.

4　仿真及安全性分析

4.1　CPN 的建模与分析

用着色 Petri 网(Colored Petri Net,CPN)对切换认证协议的流程建模,分析它的所有终止状态是否与预期相同. 如果存在可疑的终止状态,则说明协议的设计存在漏洞,是不安全的. 仿真工具 CPN Tools 4.0.1 能方便地构建出切换认证协议的着色 Petri 网模型,并自动生成状态空间. 着色 Petri 网模型如图 3 所示.

该认证协议由四种情形组成:(*a*) 不同 Controller 且 eNB 是闭合或混合类型的 HeNB;(*b*) 不同 Controller 且 eNB 不是 HeNB;(*c*)同一 Controller 下且目标 eNB 是闭合或混合类型的 HeNB;(*d*) 同一 Controller 下且目标 eNB 不是 HeNB. 在 CPN 模型中,通过 UE 的 token 的不同,能够模拟这四种过程.

(1)不同 Controller 且目标 eNB 是 HeNB

(*a*)情形分析

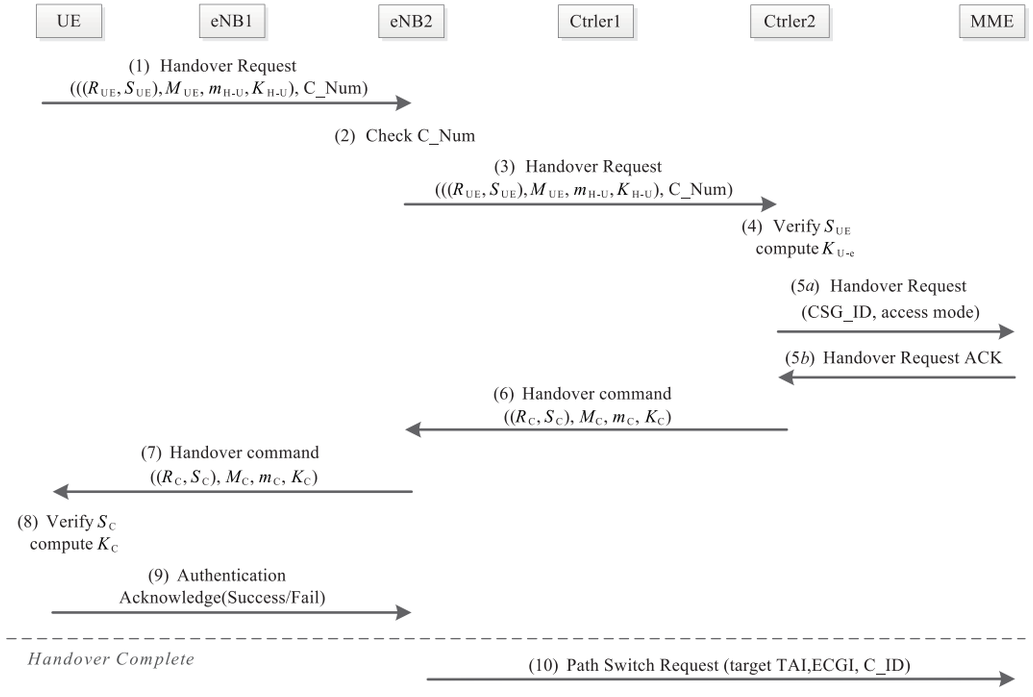

图2 基于椭圆曲线代理签名的切换认证协议

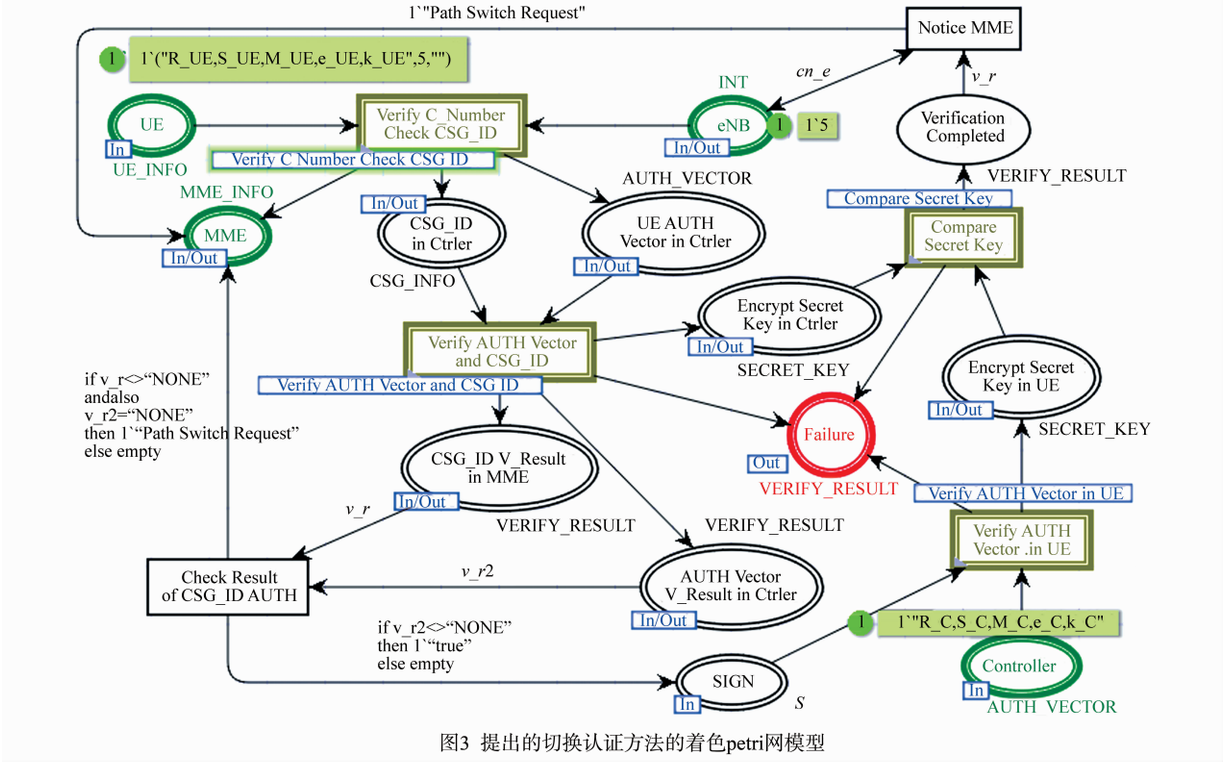

图3 提出的切换认证方法的着色petri网模型

UE 的 token 设置为 $(`R_{UE}, S_{UE}, M_{UE}, e_{UE}, K_{UE}`, 1, `csg`)$，其中第一项表示与 UE 身份验证相关的数字签名和密钥，第二项是整数“1”，表示源 eNB 所属的 Controller 的身份标识. 由于事先将库所 eNB 的 token 设置为 5，表示目标 eNB 属于身份标识为“5”的 Controller，因此源 eNB 和目标 eNB 属于不同的 Controller. 第三个参数设置为非空，表示 eNB 是闭合或混合类型的 HeNB，则 UE 的切换需要经过闭合用户组信息的检查. 由 CPN

Tools 产生该 CPN 模型状态空间报告,通过整合得到报告的部分内容如表 1 所示.

表 1　不同 Controller 且目标 eNB 是 HeNB 时 CPN 模型状态空间报告的部分内容

Statistics	State Space	Nodes	20
		Arcs	51
		Secs	0
		Status	Full
	Scc Graph	Node2	20
		Arcs	51
		Secs	0
Liveness Properties	Dead Markings	5[6,10,15,19,20]	

统计信息显示,CPN 模型的状态空间(State Space)包括 20 个节点(Node)和 51 条弧(Arcs). 状态空间图中强连通组件(SCC Graph)的数目与状态空间的节点数目相等,说明认证协议的流程没有出现死锁的情况,即协议中没有任何一个流程会产生循环. 活性信息中显示了模型有 5 个死标识 6、10、15、19 和 20,说明 CPN 模型在到达这 5 个标识后,没有变迁可以触发.

用 State Space 工具能得到这些死标识的详细情况. 对于死标识 6,库所“Failure”中产生了托肯“UE AUTH_V failure”,说明模型在对 UE 的数字签名身份进行验证时失败了,即 UE 的身份不合法,这是协议预期达到的状态,说明协议运行正确. 对于死节点 10,库所“Failure”中产生了 token“CSG_ID_V failure”,说明协议在验证用户的闭合用户组信息时失败了. 死标识 15 中,库所“Failure”中产生托肯“Ctrler AUTH_V failure”,表示 UE 在验证 Controller 的身份时失败了. 死标识 19 中,库所“Failure”中产生托肯“Secret_Key_C failure”,表示 UE 在验证共享密钥时失败了. 死标识 20,库所 MME 产生了托肯“Path Switch Request”,且其他库所的托肯数没有异常情况,表示切换认证成功. 这些死标识都符合预期,说明协议的运行是正确的.

(2)(*b*)、(*c*)、(*d*)情形分析　可执行性采用与情形(a)相同的分析方法,可验证得知,在(b)、(c)、(d)三种情形下,协议的运行也是正确的.

步骤 1 和 2 分析了在四种切换场景下,协议的执行结果都是正确的. 现在将 UE 的 token 设置为

$1'("R\_UE,S\_UE,M\_UE,e\_UE,k\_UE",1,"") + +$
$1'("R\_UE,S\_UE,M\_UE,e\_UE,k\_UE",1,"csg") + +$
$1'("R\_UE,S\_UE,M\_UE,e\_UE,k\_UE",5,"") + +$
$1'("R\_UE,S\_UE,M\_UE,e\_UE,k\_UE",5,"csg")$

即 UE 的 token 包含了上述四种情况,用 State Space 工具能得到它的活性信息如表 2 所示. 由表 2 可知模型中没有死变迁(Dead Transition Instances),即每个变迁都至少在一种标识下是可触发的,说明协议的设计中没有冗余步骤. 模型中没有家态标识(Home Marking),说明协议流程中没有循环,协议的执行总是能够到达终点.

表 2　四种切换场景下 CPN 模型状态空间报告的部分内容

Liveness Properties	Dead Transition Instances	None
	Home Markings	None

4.2　安全性分析

不可伪造性　在切换认证前,只有被 HSS 授权的 UE/Controller 才能产生出合法的代理签名. 由于代理签名 S_{UE} 和 S_C 是根据椭圆曲线上的离散对数问题产生的,从而攻击者很难伪造出它们.

不可抵赖性　当 S_{UE} 和 S_C 被验证时,被授权的身份信息 e_{UE} 和 e_C 也同时被验证,其中包括 HSS 所产生的公钥,使得 HSS 不能否认作为 UE 和 Controller 原始签名者的身份.

可识别性　在本方案中,HSS 所产生的公钥被用来验证其签名,当 UE 和 Controller 验证完原始签名的合法身份后,HSS 身份信息也同时被验证. HSS 作为原始签名者,UE 和 Controller 被授予代理签名时身份信息也同时被确认.

相互认证和密钥协商　在切换认证阶段,UE 和 Controller 相互验证对方签名是否为 HSS 代理签名,并验证其合法性,验证通过后,根据各自的私钥对协商出会话密钥,该算法的安全性是建立在计算 Diffie-Hellman 问题的困难性之上. 从而实现了双向认证和密钥协商.

中间人攻击　由于密钥协商采用的是 Diffie-Hellman 密钥交换协议,攻击者无法根据 UE 和 Controller 之间的公开消息推导出会话密钥. 此外,由于攻击者没有私钥信息,不能产生出合法的代理签名,从而攻击者通过篡改公开信息内容以达到攻击目的是不可行的.

完善前向/后向保密性　完善前向/后向保密性是指,即使某一个长期密钥被盗用,攻击者也无法获取到该会话之前或之后的会话密钥. 在本方案中,长期密钥 $K_{H\text{-}U}$ 和 $K_{H\text{-}C}$ 将作为安全信息保存在 UE 和 Controller 中,攻击者获取到它们是很困难的. 即使攻击者已经获取到了长期密钥,由于会话密钥是根据两个节点的随机值(t_C 和 t_{UE})产生的,攻击者也无法获取会话之前或之后的会话密钥.

5　性能分析

5.1　通信开销

假设 UE 与 eNB 之间的通信需要 u_e 个时间单位,eNB 与 Controller 之间的需要 e_c 个时间单位,Controller 与 MME 之间需要 c_m 个时间单位,eNB 与 MME 之

间需要 e_m 个时间单位,两个 eNB 之间需要 e_e 个时间单位. 由于 MME 一般离 eNB 很远,而 Controller 离 eNB 很近,所以 e_c 远小于 e_m 和 c_m,u_e 也远小于 e_m 和 c_m. 将提出的切换认证协议与 LTE-A 标准的切换认证协议以及同样使用代理签名方法的切换认证协议[11]比较,得到如表 3 所示的结果.

表 3 通信开销的比较

	基于 *X*2 的切换	基于 *S*1 的同一 MME 下切换	基于 *S*1 到 HeNB 的切换
LTE-A 标准	$3u\_e+2e\_e$	$4e\_m+3u\_e$	$4e\_m+3u\_e$
文献[11]	$3u\_e$	$3u\_e$	$2e\_m+3u\_e$
本文的协议	小于 $3u\_e$	小于 $3u\_e$	$2e\_c+2c\_m+3u\_e$

在软件定义 LTE-A 网络架构中,基于 *X*2 的切换和基于 *S*1 的切换都分为两种情况,即 eNB1 和 eNB2 属于同一个 Controller,以及 eNB1 和 eNB2 不属于同一 Controller. 假设用户在移动时,发生前一种情况的概率是 α,发生后一种情况的概率是 β,$\alpha+\beta=1$,则 *X*2 切换和 *S*1 切换的通信开销都是 $\alpha u\_e+\beta(3u\_e+2e\_c)$. 由于 e_c 的大小接近于 a_u,则 *X*2 切换和 *S*1 切换的通信开销约等于 $\alpha u\_e+5\beta u\_e$. 用户在小范围移动的概率大于大范围移动的概率,即 α 的值大于 β,所以($\alpha u\_e+5\beta u\_e$)的值小于 $3u\_e$. 因此,在平均情况下,当发生 *X*2 切换和同一 MME 下的 *S*1 切换时,本文提出的协议的通信开销好于 LTE-A 标准协议以及[11]中提出的协议. 特别是当用户在进行小范围移动时(β 接近于 0),每次切换的通信开销接近于 u_e. 在稠密的基站环境中,这会极大地减少用户切换认证的开销,提高切换速度.

当切换的目标 eNB 是 HeNB 时,本文的协议略差于文献[11]中提出的协议,但是好于 LTE-A 标准协议.

5.2 计算开销

基于椭圆曲线上离散对数问题的公钥加密算法,比基于 RSA 的公钥加密算法有更高的单位安全强度,160 位的椭圆曲线密钥与 1024 位的 RSA 密钥安全性相同[18]. 本文在 Pentium Dual-Core 3.0GHz 处理器上,用 C\C++ OpenSSL 库测得基本加密运算时间,如表 4 所示.

表 4 基本加密运算的计算开销

(单位:ms)	模指数 T_E	ECC 乘法 T_{EM}	哈希 T_H	整数乘法 T_M
RSA(1024bits)	0.460	×	0.103	0.035
ECC(160bits)	×	0.198	0.105	0.003

LTE-A 标准的切换认证协议采用对称加密方法,它在切换认证过程中的计算开销接近于 0,远好于本文的协议和文献[11]. 现将本文的协议与文献[11]的协议对比,结果如表 5 所示. 由于本文采用了基于椭圆曲线的加密方法,在计算开销好于文献[11].

表 5 协议间计算开销的比较

(单位:ms)	UE	eNB	总和
本文	$13T_{EM}^{ECC}+2T_H^{ECC}+3T_M^{ECC}=2.793$	$13T_{EM}^{ECC}+2T_H^{ECC}+3T_M^{ECC}=2.793$	5.586
[11]	$7T_{EM}^{RSA}+2T_H^{RSA}+3T_M^{RSA}=4.476$	$7T_{EM}^{RSA}+2T_H^{RSA}+3T_M^{RSA}=4.476$	8.952

6 结论

本文研究了 LTE-A 网络中的切换认证问题,通过对 LTE-A 网络中安全架构的分析,综合考虑了网络架构的易扩展性和切换认证协议流程的可实施性,利用 SDN 的思想,以优化切换认证过程为目标,建立了软件定义 LTE-A 异构网络架构. 该架构将局部范围内基站的切换认证控制面功能,以及基站的数据面功能,分离到一个中心控制器上,基站只负责数据的转发和小部分控制面功能.

在上述架构下,本文提出了基于椭圆曲线代理签名的切换认证方法. 在该认证方法中,中心控制器代替了 eNB 与 UE 进行身份验证. 使用基于椭圆曲线的代理签名,比使用基于 RSA 的签名算法有更少的计算量,有利于减少中心控制器的计算负荷. 在通信开销方面,当 UE 移动范围不大时,本文的协议比在通信开销方面做的很好的文献[11]有更小的开销,适用于基站密度较大、UE 切换频繁的环境中.

参考文献

[1] Niafar,S,X Tan,D H K Tsang. The optimal user scheduling for LTE-A downlink with heterogeneous traffic types [A]. International Conference on Heterogeneous Networking for Quality,Reliability,Security and Robustness[C]. Rhodes Greece:IEEE,2014.56-62.

[2] Cisco. Global Mobile Data Traffic Forecast Update 2014-2019 White Paper,Feb 2015[J/OL]. See: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html,2015.

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

[4] Gudipati A,Perry D,Li L E. SoftRAN: Software defined radio access network[A]. ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking[C]. Hong Kong:ACM,2013.25-30.

[5] Bhaumik S,Chandrabose S P,Jataprolu M K. CloudIQ: a

framework for processing base stations in a data center [A]. Proceedings of the 18th Annual International Conference on Mobile Computing and Networking[C]. Istanbul, Turkey:ACM,2012. 125 – 136.

[6] Duan X, Wang X. Authentication handover and privacy protection in 5G hetnets using software-defined networking [J]. IEEE Communications Magazine,2015,53(4): 28 – 35.

[7] Song M, Choi J Y, Cho J D. Reduction of authentication cost based on key caching for inter-MME handover support [A]. The 2014 International Conference on High Performance Computing & Simulation(HPCS 2014)[C]. Bologna, Italy:IEEE,2014. 885 – 892.

[8] A Bohk, L Buttyn, L Dra. An authentication scheme for fast handover between WiFi access points[A]. Proceeding of ACM Wireless Internet Conference (WICON 2007)[C]. Austin, USA:ACM,2007. 22 – 24.

[9] Choi J, Jung S. A handover authentication using credentials based on chameleon hashing[J]. IEEE Communications Letters,2010,14(1): 54 – 56.

[10] Jing Q, Zhang Y, Fu A. A privacy preserving handover authentication scheme for EAP-based wireless networks [A]. Global Telecommunications Conference (GLOBECOM 2011)[C]. Houston, USA:IEEE,2011. 1 – 6.

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

[12] 3GPP TS 36. 300 v10. 4. 0. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)[S]. 2011.

[13] 3GPP TS 36. 401 v10. 3. 0. Evolved Universal Terrestrial Radio Access Network (E-UTRAN): Architecture description[S]. 2011.

[14] 3GPP TS 33. 401 v10. 5. 0. 3GPP System Architecture Evolution (SAE); Security architecture[S]. 2011.

[15] 3GPP TS 23. 401 V10. 5. 0. General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN)[S]. 2011.

[16] Mambo M, Usuda K, Okamoto E. Proxy signatures: delegation of the power to sign messages[J]. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences,1996,79(9):1338 – 1354.

[17] Hwang M S, Tzeng S F, Tsai C S. Generalization of proxy signature based on elliptic curves[J]. Computer Standards & Interfaces,2004,26(2):73 – 84.

[18] Jacobson, Michael Jr. Elliptic curves and cryptography [J]. Dr Dobbs Journal,1997,19(3):173 – 193.

作者简介

陈　昕　男,1965 年出生,教授,兼职博士生导师,于 2003 年在北京理工大学获得博士学位,现为北京信息科技大学计算机学院教授,主要研究领域为计算机网络及性能评价、网络安全、航电网络,曾在《The Journal of Supercomputing》、《Multimedia Tools and Applications》、《电子学报》和《计算机科学》等期刊上发表多篇论文.
E-mail: chenxin@ bistu. edu. cn

宋亚鹏　男,1990 年出生,硕士,于 2016 年在北京信息科技大学获得硕士学位,主要研究方向为无线网络与安全.
E-mail:songyapeng _ bistu@ sina. com