下一代高速铁路异构网络切换安全认证

陈 永, 刘 雯, 詹芝贤

兰州交通大学电子与信息工程学院 兰州 中国 730070

摘要 近年来, 随着高速铁路无线通信技术的快速发展, GSM-R 无线通信系统将逐步向 LTE-R 系统演进。在此演进过程中存在 GSM-R 和 LTE-R 长期共存的局面, 如何实现高速铁路无线通信异构网络之间的快速切换和安全认证成为铁路无线通信研究的热点问题。针对高速铁路无线通信异构网络切换认证过程中, 存在安全性低和认证开销高等问题, 提出了一种适用于下一代高速铁路异构网络的轻量级切换安全认证方案。首先, 采用哈希函数等操作生成切换请求 *Token* 和异构网络切换认证码 *PASS*, 实现了用户身份匿名性和可追溯性等安全要求, 并且高速列车无需多次注册就可实现异构网络间的无缝切换。其次, 设计了基于椭圆曲线密钥交换的轻量级切换算法, 完成了高速列车与目标基站的相互认证和密钥协商, 降低了计算开销和通信开销, 实现了会话协商密钥的前后向安全性。最后, 采用形式化方式 BAN 逻辑进行了安全性验证, 并使用朔黄铁路 LTE-R 线路实测数据进一步对本文所提方案的有效性进行了验证, 分析得出所提方案能够满足可追溯性、匿名性、抗伪装用户攻击、抗中间人攻击和抗重放攻击等安全特性。性能分析表明, 本文方案在通信开销和计算开销方面较比较方法性能更优, 能够满足下一代高速铁路异构通信网络的高效、安全无缝切换的需求。

关键词 异构网络; 切换认证; 哈希函数; 椭圆曲线密钥交换算法; BAN 逻辑; 高速铁路

中图法分类号 TN918.91 U285.2 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.09.07

Safety Certification for Next Generation High-speed Railway Heterogeneous Network Handover

CHEN Yong, LIU Wen, ZHAN Zhixian

School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China

Abstract In recent years, with the rapid development of high-speed railway wireless communication technology, GSM-R wireless communication system will gradually evolve to LTE-R wireless communication system. There is a situation of GSM-R and LTE-R will coexist for a long time during the evolution of the GSM-R communication system to LTE-R system. How to realize fast handover and security authentication between heterogeneous high-speed railway wireless communication networks has become one of the research hotspots in the field of railway wireless communication research. Aiming at the problems of low security and high authentication overhead during the handover authentication process of high-speed railway wireless communication heterogeneous networks, a lightweight handover safety authentication scheme suitable for the next generation of high-speed railway heterogeneous networks is proposed. Firstly, the hash function and other operations are used to generate the handover request *Token* and the heterogeneous network handover authentication code *PASS*, which realized the security requirements of user identity anonymity and traceability, and high-speed trains can achieve seamless switching between heterogeneous networks without multiple registration. Secondly, a lightweight handover algorithm based on elliptic curve key exchange is designed, which completed the mutual authentication and key negotiation between the high-speed train and the target base station, reduced the calculation and communication costs, and realized the forward and backward security of the session negotiation key. Finally, the formal BAN logic was used to verify the security, and the measured data of the Shuohuang Railway LTE-R line was used to further verify and analyze the effectiveness of the proposed scheme. It is concluded that the proposed scheme can satisfy traceability, anonymity, anti-disguised user attacks, anti-man-in-the-middle attacks and anti-replay attacks in the process of railway wireless communication. Performance analysis shows that the proposed scheme has better performance than existing similar comparison methods in terms of communication overhead and computing overhead, and can meet the requirements of efficient, safe and seamless handover for the next generation of high-speed railway heterogeneous communication networks.

Key words heterogeneous network; handover authentication; hash function; elliptic curve key exchange algorithm; BAN logic; high-speed railway

---

通讯作者: 陈永, 博士, 教授, Email:edukeylab@126.com。

本课题得到国家自然科学基金(No. 61963023, No. 61841303)、兰州交通大学天佑创新团队(No. TY202003)资助。

收稿日期: 2021-09-14; 修改日期: 2021-11-12; 定稿日期: 2022-07-19

1 引言

GSM-R(Global System for Mobile Communications for Railway)是我国当前使用的高速铁路无线通信系统, 其承载大量列车控制信息, 其安全性对高速铁路安全至关重要。然而, GSM-R 属于 2G 窄带通信系统, 存在业务承载能力弱等诸多弊端, 已无法满足高速铁路智能化发展的需求[1-2]。未来 GSM-R 将逐步向 LTE-R(the Long-Term Evolution for Railway)演进[3]。LTE-R 作为我国下一代高速铁路无线通信系统, 具有高速率、低延时和高带宽等优点。但因建设周期或设备更新等因素, 演进过程中, 将长期存在 GSM-R 和 LTE-R 系统共存的局面, 列车在高速运行过程中, 将频繁出现交替使用 GSM-R 和 LTE-R 网络的情况[4]。在这种背景下, 在 GSM-R 和 LTE-R 异构网络之间, 高速列车如何快速安全认证及无缝切换, 已成为目前研究的难点问题, 亟待解决。

高速铁路无线通信系统采用 3GPP 定义的 EPS-AKA 协议(Evolved Packet System-Authentication and Key Agreement)作为认证密钥协商协议[5]。目前国内外诸多学者针对高速铁路切换安全认证进行了相关研究。Alezabi 等[6]针对异构网络中 *IMSI*(International Mobile Subscriber Identity)的明文传输和会话密钥未更新的问题, 通过明文传输用户 *ID* 和 *ANID*(Access Network Identity)的方法进行了改进, 但该方案未实现用户匿名性, 易受到伪装用户攻击。张应辉等[7]针对异构网络安全接入问题, 使用用户伪身份结合椭圆曲线密钥算法, 实现了用户匿名性, 增强了异构网络协议的鲁棒性, 但群组切换策略存在单点易受攻击的漏洞。Wang 等[8]提出一种基于椭圆曲线密码系统的匿名代理签名方案, 实现了用户匿名性, 但在 *IMSI* 的传输中易遭受暴力攻击。吴文丰等[9]利用非对称加密技术结合椭圆曲线密钥交换算法解决 *IMSI* 明文传输和会话密钥未更新问题, 但该方案中未实现用户匿名性以及密钥后向安全性。Suvidha 等[10]使用椭圆曲线密钥算法与哈希函数相结合的方法, 有效的阻止了暴力破解和 *IMSI* 的明文传输, 但该认证协议存在不可追溯性问题。

此外, 随着 GSM-R 向 LTE-R 演进的过程中网络复杂性和异构性的增加, 异构网络计算效率和通信成本逐步增加, 如何减少切换认证过程的认证开销也是需要重点解决的问题[11]。Mo 等[12]提出了一种基于双线性配对的匿名认证方案, 实现了匿名性、不可追溯性、相互认证等安全特性, 但双线性配对方法采用指数操作存在计算复杂度较高的问题。Ozhelvaci 等[13]提出了基于身份加密方法的切换认证协议, 解决了异构网络中计算效率和通信成本高的问题, 但该方案未实现可追溯性, 难以抵抗中间人攻击。Zhang 等[14]基于门限哈希函数的碰撞特性和区块链的抗篡改性, 提出了一种切换认证密钥协商协议, 实现了用户匿名性、可追溯性, 但是难以抵抗中间人攻击和伪装用户攻击。

综上所述, 针对 GSM-R 和 LTE-R 异构网络演进场景下, 现有认证密钥协商协议 EPS-AKA 中存在 *IMSI* 明文传输、无追溯性、匿名性等安全漏洞, 以及计算和通信开销较大问题。本文提出了一种基于椭圆曲线密钥交换算法和哈希函数的下一代高速铁路异构网络切换安全认证协商方案。本文所做工作如下:

(1) 根据下一代高速铁路异构网络切换特点, 加入 *Token* 身份标识和切换认证码 *PASS*, 实现用户身份匿名性和可追溯性等安全特性, 以达到 GSM-R 和 LTE-R 异构网络高效无缝安全切换的需求。

(2) 提出基于椭圆曲线密钥交换算法、哈希函数以及异或等操作的轻量级切换算法, 降低计算和通信开销, 实现了会话协商密钥的前后向安全性, 能够抵抗中间人攻击、伪装用户攻击等攻击, 提高高速列车车地通信的安全性。

(3) 使用 *TMSI* 代替 *IMSI* 明文传输, 实现异构网络环境下列车控制信息的安全传输。

(4) 最后, 采用 BAN 逻辑对所提方法进行了形式化安全性验证, 分析结果表明: 所提方法在安全性等方面均优于现有方案, 并且在计算和通信开销方面也有较高优势, 能够满足下一代高速铁路异构网络切换安全认证中安全无缝及计算和通信成本的要求。

2 基础理论

2.1 高速铁路演进异构网络架构

高速铁路无线通信演进异构网络架构由 GSM-R 网络和 LTE-R 网络共同组成, 如图 1 所示[15]。相比较 GSM-R 网络使用 BSC(Base Station Controller)控制 BS(Base Station)的结构, 下一代高速铁路 LTE-R 无线通信网络结构更为扁平化, 接入网仅由 eNodeB(Evolved Node Base)构成。GSM-R 向 LTE-R 演进过程中, 网络结构中的设备采用平稳升级更新的方法, 如 SGSN(Serving GPRS Support Node)演进升级为 MME(Mobility Management Entity); 而 HLR(Home Location Register)演进升级为 HSS(Home Subscriber Server), 负责生成系统参数, MME/SGSN

为高速列车 UE(User Equipment)提供切换接入服务。在异构网络中, 为了保证高速列车能够在连续的异构网络中实现无缝切换和移动性, 用户都需要在用户归属服务器 HSS 中进行认证, 以便于 HSS 能够为不同的网络之间提供相同的访问控制, 即身份验证和授权。当高速列车 UE 从当前 MME/SGSN 移动到另一个 MME/SGSN 时, 高速列车 UE 和目标 MME/SGSN 必须进行相互认证和密钥协商, 这是切换认证所必须的基本安全需求。

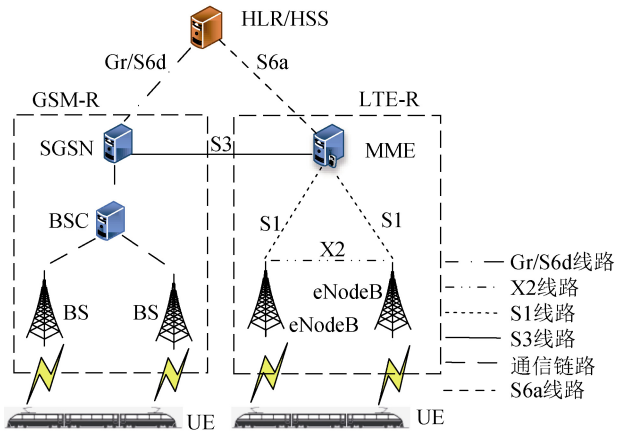

图 1 高速铁路演进异构网络架构

Figure 1 High-speed railway evolution heterogeneous network architecture

2.2 EPS-AKA 认证协议

3GPP 为了未来网络标准化, 定义铁路通信网络采用 EPS-AKA 协议, 作为车地之间的通信协议。参与该协议的主要实体有高速列车 UE、移动授权实体 MME/SGSN 和用户归属服务器 HLR/HSS。在 EPS-AKA 协议中相关符号及含义, 如表 1 所示。

EPS-AKA 协议的流程如图 2 所示, 具体执行步骤如下。

(1) UE→MME/SGSN: M1: $\{IMSI, ID_{HSS}\}$

用户 UE 向 MME/SGSN 发送请求接入消息 M1。

(2) MME/SGSN→HSS: M2: {M1, *SNID*}

MME/SGSN 在收到高速列车 UE 发送的消息 M1 之后, 根据归属服务器 ID_{HSS} 查询网络号, 之后将网络号 *SNID* 和消息 M1 一起打包发送给 HSS。

(3) HSS→MME/SGSN: M3: $\{AV(n)\}$

HSS 接收到 MME 发送的消息 M3 之后, 对网络号 *SNID* 进行验证, 若 *SNID* 为非法 *ID*, 则拒绝接入请求; 否则, HSS 根据 *IMSI* 检索密钥 *K* 并生成认证向量组 $AV(n)$, 并将 $AV(n)$发送给 MME/SGSN。

(4) MME/SGSN→UE: M4: $\{AV(i)\}$

MME/SGSN 将收到的向量组 $AV(n)$存入其数据库, 按照最小序号原则选取出一组向量 $AV(i)$, 将其发送给高速列车 UE。

表 1 符号及含义

Table 1 Symbols and meanings

符号	含义	长度/bit
UE	移动终端设备	—
MME/SGSN	异构网络中 MME 或 SGSN 移动授权实体	—
PID	移动设备伪身份	—
ID_{UE}	移动设备身份	—
E	非奇异椭圆曲线	—
G_1/G_2	循环加法群	—
P	群 *G* 的生成元	—
TMSI/*IMSI*	临时/永久移动用户识别码	128
SNID	网络标识符	48
LAI	区间标识符	40
T_i	*i* 时刻的时间戳	32
K_{ASME}	UE 和 HSS 共享密钥	256
KSI_{ASME}	密钥 K_{ASME} 的标识符	3
K	UE 和 MME/SGSN 共享的长期根密钥	128
SK	MME/SGSN 和 UE 的协商会话密钥	128
AUTN	认证令牌	128
MAC/*XMAC*	消息认证码	64
RES/*XRES*	响应消息	64
s/*r*/*x*/*X*	随机数	128
h	哈希函数	128
H	秘密值	—
R	秘密值的认证参数	—
11	连接符	—
SigK{m}	使用密钥 *K* 对消息 m 签名	—

(5) UE→MME/SGSN: M5: $\{RES\}$

UE 接收到 MME/SGSN 的消息响应之后, 判断同步序列号 *SQN* 是否合法, 若不合法, 则终止认证响应; 否则根据消息认证码公式计算 *XMAC*: $XMAC = f_1(SQN \| RAND \| AMF \| K)$, 比较 *XMAC* 与接收到的 *MAC* 是否相等, 若不相等, 则终止认证; 否则高速列车 UE 完成对 MME/SGSN 和 HSS 的认证, 高速列车 UE 计算响应消息 *RES*: $RES = f_2(RAND \| K)$ 以及共享密钥 K_{ASME}: $K_{ASME} = KDF(SNID \| CK \| IK)$, 将反馈响应消息 *RES* 发送给 MME/SGSN。

(6) MME/SGSN 收到高速列车 UE 发送的用户

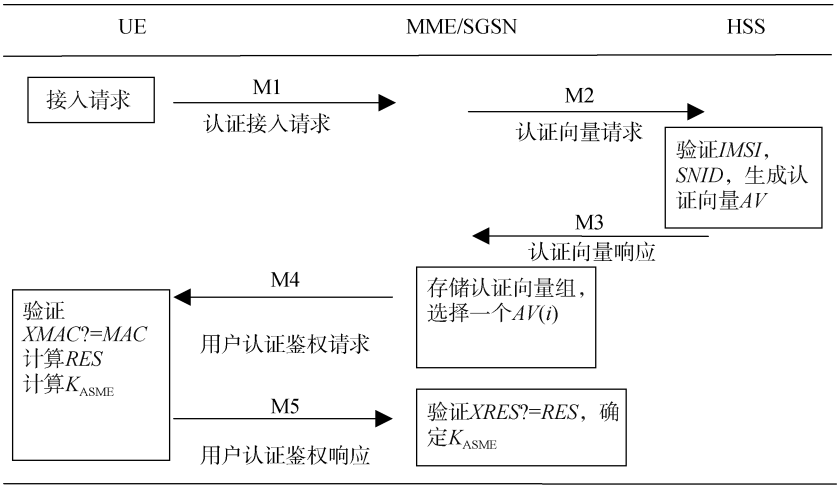

图 2 EPS-AKA 协议流程图

Figure 2 EPS-AKA protocol flow chart

认证响应 RES 之后, 验证 $RES\text{?}=XRES$, 若相等, 则完成对高速列车 UE 的安全认证; 否则, 终止协议认证。

3 高速铁路异构网络切换安全认证

高速铁路GSM-R和LTE-R异构网络之间的切换认证以垂直切换(Vertical Handover, VHO)认证为主, 垂直切换是指从一种无线网络接入到另一种无线网络之中。在 GSM-R 和 LTE-R 异构网络中, 高速列车在线路跨区高速运行时, 将频繁在异构网络中完成越区切换。铁路沿线的基站由于信号覆盖范围有限, 在列车移动至当前基站覆盖范围边缘时, 需要断开与源小区基站的连接, 转为与新的基站建立连接, 且高速列车必须与目标基站进行相互认证和密钥协商, 身份认证和密钥协商对保障列车切换认证过程的安全性具有至关重要的作用。

然而在 GSM-R 和 LTE-R 异构网络演进场景下, 切换认证过程中存在 *IMSI* 明文传输、无追溯性、匿名性等安全漏洞, 以及计算和通信开销较大问题。针对上述问题, 本文提出一种基于椭圆曲线 Diffie-Hellman 密钥协商(Elliptic Curve Diffie–Hellman key Exchange, ECDH)与哈希函数相结合的切换认证方案, 通过加入 *Token* 身份标识和切换认证码 *PASS*, 实现了用户身份匿名性和可追溯性等安全特性, 能够满足车地之间的高效通信需求和通信安全。

根据高速铁路GSM-R和LTE-R异构网络切换实际场景, 本文所提方案中切换认证方案包括初始化阶段、注册阶段、垂直切换认证阶段这 3 个阶段。

3.1 初始化阶段

在本阶段, 高速列车 UE 和移动授权实体 MME/SGSN 利用椭圆曲线密钥生成算法生成各自的公私钥。具体步骤如下:

(1) 选择大素数 q, 生成非奇异椭圆曲线 E: $y^2+ax+b \bmod p$, 选择 G_1、G_2 为两个循环加法群, P 为群 G 的生成元。f 为物理不可克隆函数(Physically Unclonable Function System, PUFS), 满足对于同一激励 T_i, 在容限范围之内会产生相同的结果, 即 $f(T_1)=f(T_2)$。

(2) UE 生成一个随机数 $s_{\mathrm{UE}}\in G_q^*$, 计算 $PK_{\mathrm{UE}}=s_{\mathrm{UE}}P$, 其中 s_{UE} 为 UE 私钥, PK_{UE} 为 UE 公钥。

(3) MME/SGSN 生成一个随机数 $s_{\mathrm{MME/SGSN}}\in G_q^*$, 计算 $PK_{\mathrm{MME/SGSN}}=s_{\mathrm{MME/SGSN}}P$, 其中 $s_{\mathrm{MME/SGSN}}$ 为 MME/SGSN 私钥, $PK_{\mathrm{MME/SGSN}}$ 为 MME/SGSN 公钥。

3.2 注册阶段

在该阶段, 高速列车 UE 和移动授权实体 MME/SGSN 在 HSS 处进行身份信息注册。注册流程如图 3 所示, 其具体步骤如下:

(1) UE 向 HSS 发送消息$\{ID_{\mathrm{UE}}, PK_{\mathrm{UE}}\}$作为注册请求信息。

(2) MME/SGSN 向 HSS 发送消息$\{ID_{\mathrm{MME/SGSN}}, PK_{\mathrm{MME/SGSN}}\}$作为注册请求信息。

(3) HSS 收到 UE 发送的消息之后, 保存 UE 公钥 PK_{UE}, 并与 ID_{UE} 建立对应列表; HSS 生成一个随机数 $r\in G_q^*$, 基于此随机数 r、共享密钥 K 和用户身份标识 ID_{UE} 为用户生成 $Token\{PID, R\}$, 其中 $PID=ID_{\mathrm{UE}}\oplus h(r\| K)$, $R=h(PID\| K)\oplus r$。PID 为伪身份, R 是用于 UE 接收 *Token* 后从中获取 r 并生成秘密值 $H=h(r\| K)$ 的认证参数。随后, HSS 将 *Token*

和 MME 公钥 $PK_{\mathrm{MME/SGSN}}$ 通过安全通道发送到 UE。

(4) HSS 收到 MME/SGSN 的消息之后, 保存 MME/SGSN 公钥 $PK_{\mathrm{MME/SGSN}}$, 并与 $ID_{\mathrm{MME/SGSN}}$ 建立了相应的对应列表。计算切换认证码: $PASS_i = h(H \| f(T_i)) \oplus ID_{\mathrm{UE}}$, 并与 ID_{UE} 建立一一对应的列表。HSS 将 *PASS* 和 UE 公钥 PK_{UE} 通过安全通道发送到 MME/SGSN。

(5) 用户 UE 在终端中保存 *Token*{*PID*, *R*}, $PK_{\mathrm{MME/SGSN}}$。

(6) MME/SGSN 在终端中保存 $PASS_i$, PK_{UE}。

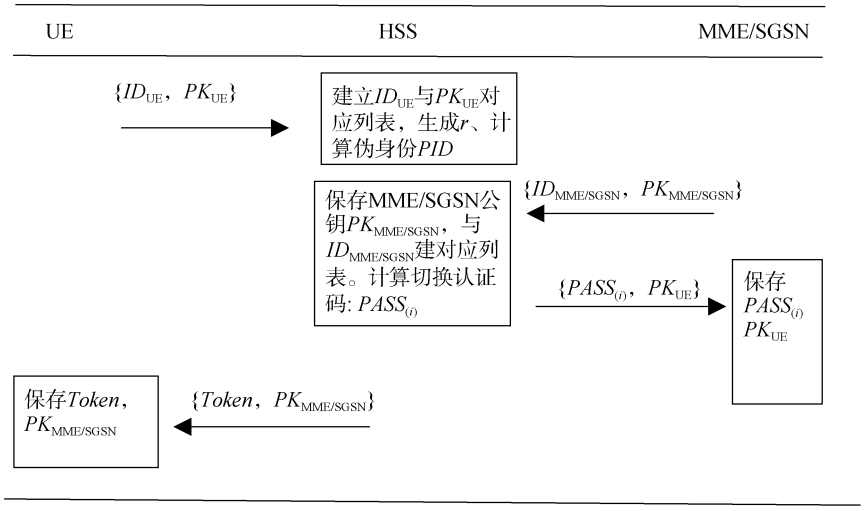

图 3 注册流程图

Figure 3 Registration flow chart

3.3 垂直切换认证阶段

在高速列车跨区域切换过程中, UE 进入 GSM-R 和 LTE-R 共存的异构网络时需要进行异构网络环境下的认证切换。在认证切换过程中, MME/SGSN 无需生成认证向量 *AV*, 目标 MME/SGSN 只需与 UE 协商生成会话密钥即可使用该密钥完成 UE 和 MME/SGSN 之间信息的安全传输。垂直切换认证流程如图 4 所示, 步骤如下:

(1) UE→MME/SGSN 的消息, M_1: {*TMSI*, $PASS_1$, T_1, X_{UE}, $SigPK_{\mathrm{MME/SGSN}}${*PID*, *R*}}

当 UE 处于基站信号覆盖边缘时, 由于网络信号较差, UE 会在当前网络中发起切换接入其他网络的请求:

①UE 生成时间戳 T_1, 计算临时移动用户识别码: $TMSI = IMSI \oplus f(T_1)$, 输入身份 ID_{UE}, 计算秘密值 $H = ID_{\mathrm{UE}} \oplus PID = h(r \| K)$。

②生成随机数 $x_{\mathrm{UE}} \in G_q^*$, 计算 $X_{\mathrm{UE}} = x_{\mathrm{UE}} P$。

③计算切换认证码: $PASS_1 = h(H \| f(T_1)) \oplus ID_{\mathrm{UE}}$。

④UE 使用 MME/SGSN 公钥 $PK_{\mathrm{MME/SGSN}}$ 对 *Token* 进行签名得到 $SigPK_{\mathrm{MME/SGSN}}${*Token*}。UE 发送消息 M_1 给 MME/SGSN。

(2) MME/SGSN→SGSN/MME: M_2: {*TMSI*, *PID*, *R*, $PASS_1$, T_1, X_{UE}}

MME/SGSN 收到 UE 的消息之后:

①使用其私钥 $s_{\mathrm{MME/SGSN}}$ 验证签名确认 UE 身份, 并得到信息{*TMSI*, *PID*, *R*, $PASS_1$, T_1, X_{UE}}。

②MME/SGSN 将消息 M_2 根据列车运行路径发送到目标 SGSN/MME。

(3) SGSN/MME → UE: M_3: {*AV*, *MAC*, $X_{\mathrm{SGSN/MME}}$}

SGSN/MME 收到 MME/SGSN 的消息之后:

①SGSN/MME 得到消息{*TMSI*, *PID*, *R*, $PASS_1$, T_1, X_{UE}}。

②生成时间戳 T_2, 判断 $T_2 - T_1 \leqslant \Delta T$, 若超出请求时间容限, 则不同意切换请求; 否则, 根据 $IMSI = TMSI \oplus f(T_2)$ 得到共享密钥 *K*, 并假设移动授权实体与归属服务器之间的传输信道为安全信道, 从 HSS 获取注册阶段保存的 $PASS_i$, 从而得到 ID_{UE}。

③计算 $r' = h(PID \| K) \oplus R$, $H' = h(r' \| K)$, $ID_{\mathrm{UE}}' = H' \oplus R$, 判断 ID_{UE}'?=ID_{UE}, 若不相等, 则拒绝切换请求; 若相等则进行步骤④。

④根据切换认证码公式计算 $PASS_2$: $PASS_2 = h(H \| f(T_2)) \oplus ID_{\mathrm{UE}}$, 对 $PASS_2 ? = PASS_1$ 进行判断, 若不相等, 则拒绝切换请求; 否则, 满足切换请求, 允许 UE 接入。

⑤SGSN/MME 生成随机数 $x_{\mathrm{SGSN/MME}} \in G_q^*$，计算 $X_{\mathrm{SGSN/MME}} = x_{\mathrm{SGSN/MME}} P$，计算协商会话密钥: $SK = x_{\mathrm{SGSN/MME}} PK_{\mathrm{UE}} + s_{\mathrm{SGSN/MME}} X_{\mathrm{UE}}$。

⑥随后 SGSN/MME 计算消息认证码: $MAC = h(H') \oplus f(T_2)$, SGSN/MME 选择存储在数据库中的认证向量 *AV*, 发送消息 M_3 给 UE, 若认证向量 *AV* 已用完, 则 SGSN/MME 向 HSS 发送请求认证向量消息, 由 HSS 生成认证向量后发送给 SGSN/MME。

(4) UE→SGSN/MME: M_4: {*RES*}

UE 收到 SGSN/MME 的消息之后:

① 计算 $XMAC = h(H) \oplus f(T_1)$，然后判断 $XMAC ?= MAC$，若不是, 则验证失败, 结束会话; 否则, 进行步骤②。

② UE 根据协商会话密钥公式计算 *SK*: $SK = x_{\mathrm{UE}} PK_{\mathrm{SGSN/MME}} + s_{\mathrm{UE}} X_{\mathrm{SGSN/MME}}$，接受 SGSN/MME 发送的认证向量, 计算 $RES = h(SK \| H)$,使用协商会话密钥 *SK* 进行通信。

(5) SGSN/MME 收到 UE 发送的消息之后, 计算 $XRES = h(SK \| H')$，判断 $XRES ?= RES$，若不相等, 则 SGSN/MME 验证 UE 失败, 结束对话; 否则, 使用协商会话密钥 *SK* 进行通信。

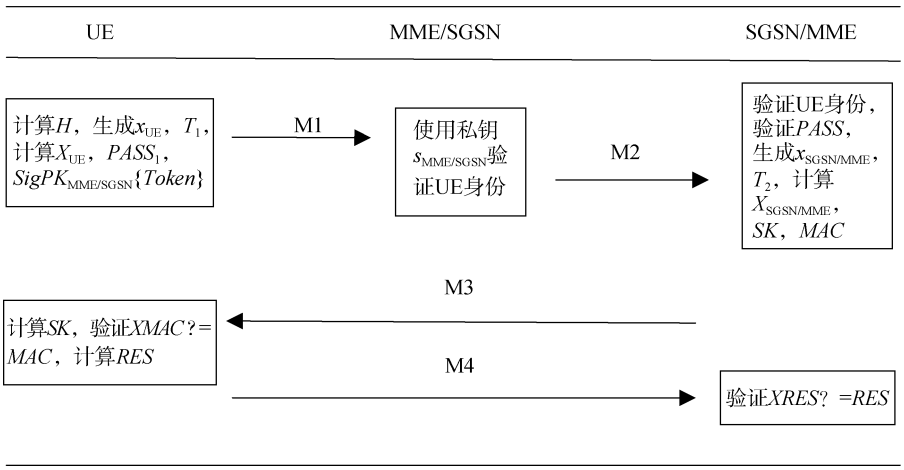

图 4 垂直切换认证流程图

Figure 4 Vertical handover certification flow chart

上述流程完毕后, 用户在接入到新的网络后, 通过与目标网络中的移动授权实体 SGSN/MME 协商出新的会话密钥 *SK*, 使用 *SK* 进行后续通信。

4 安全证明

4.1 理论分析

(1) *IMSI* 机密性保护

IMSI 作为携带很多通信信息的移动标识码, 其在传统的 EPS-AKA 协议中是明文传输的, 若 *IMSI* 泄露, 则会对通信双方造成巨大损失, 故而, 对 *IMSI* 进行机密性保护至关重要。在本文方案中, UE 发送的切换请求消息使用临时身份 *TMSI* 代替 *IMSI* 的明文传输, 由于 *TMSI* 具有一次性, 故攻击者无法通过 *TMSI* 获取协议信息。

(2) 前/后向安全性

前/后向安全性是指攻击者在获得当前密钥的情况下, 无法获得前次和后次通信的会话密钥。在本文方案中, 列车 UE 和移动授权实体 SGSN/MME 的协商密钥 *SK* 由本文所提的椭圆曲线密钥交换方法生成。但由于椭圆曲线离散对数问题和 Diffie-Hellman 计算问题, 攻击者无法从参数(X_{UE}, $x_{\mathrm{UE}}P$)和($X_{\mathrm{SGSN/MME}}$, $x_{\mathrm{SGSN/MME}}P$)得到随机生成的 x_{UE} 和 $x_{\mathrm{SGSN/MME}}$, 因此前/后两次切换的协商会话密钥是不相关的, 故攻击者无法根据当前的会话密钥推导出之前或之后的密钥, 所以本文方案具有前/后向安全性。

(3) 抵抗重放攻击

重放攻击是指攻击者将截获的 *n* 组信息原封不动的发送给服务器, 欺骗服务器, 破坏认证正确性。在本文方案中, UE 发送的切换请求消息{*TMSI*, *PID*, *R*, $PASS_1$, T_1, X_{UE}}中包含时间戳 T_1, SGSN/MME 在接收到消息之后会生成新的时间戳 T_2, 通过判断是否满足 $T_2 - T_1 \leqslant \Delta T$ 条件从而抵抗重放攻击。

(4) 抵抗伪装用户攻击

在异构网络中, 由于 UE 身份 ID_{UE} 的明文传输致使攻击者可通过截获 ID_{UE}, 从而假冒真实合法的 UE 对服务器发起攻击, 导致异构网络出现安全隐

患。在本文方案中, UE 向 SGSN/MME 请求切换时, $Token\{PID, R\}$是基于随机数 r 和共享密钥 K 共同计算得出, 攻击者无法同时获取 r 和 K 这两个参数, 因此攻击者无法构建出 $Token' = Token$ 并发送至 SGSN/MME。故本文方案能够抵抗伪装用户攻击。

(5) 抵抗中间人攻击

在本文方案中, 通信双方的协商会话密钥 SK 由通信双方的公私钥经过点乘和倍加运算之后得到的结果, 攻击者若想要破解协商会话密钥 SK, 需要攻破椭圆曲线离散对数和 CDHP 问题, 所以本文方案能够抵抗中间人攻击。

(6) 相互认证

在异构网络通信中, 为了通信的安全性得到保障, 需要实现 UE 与 SGSN/MME 之间的双向身份验证, 以防多种攻击。

① UE 对于 SGSN/MME 的验证。UE 向 SGSN/MME 发送切换请求消息之后, SGSN/MME 发送 MAC 作为应答响应。然后, UE 方通过计算 $XMAC = h(H) \oplus f(T_1)$, 判断 $XMAC ? = MAC$ 是否成立完成对 SGSN/MME 的验证。

②SGSN/MME 对 UE 的验证。AKA 作为一种基于挑战应答响应机制的协议, SGSN/MME 在收到 UE 方发送的应答响应消息之后, 计算 $XRES = h(SK \| H')$, 判断 $XRES ? = RES$, 是否成立完整对 UE 的认证。

以上两点证明本文方案可以满足相互认证。

(7) 用户匿名性

在异构网络切换认证协议中, UE 需要发送身份 ID_{UE} 用于 SGSN/MME 接受请求消息之后进行身份验证, ID_{UE} 以明文形式传输, 在本文方案中, 用户的 $Token\{PID, R\}$由 HSS 生成, 且 UE 对 $Token$ 使用 $PK_{\mathrm{MME/SGSN}}$进行签名, 只有真正的 MME/SGSN 才拥有对应的私钥 $s_{\mathrm{MME/SGSN}}$ 对该消息进行验证, 攻击者很难篡改 $Token$ 信息。PID 是由用户 ID_{UE} 和秘密值 H 异或生成的, 其中秘密值 H 是由随机数 r 和共享密钥 K 通过 $Hash$ 函数计算得出, 而攻击者即便获取 K 也无法得到 r, 进而不能计算出 H, 也就无法得到用户的真实 ID_{UE}, 因此本方案满足用户匿名性。

(8)可追溯性

假设有恶意用户伪装成用户 UE 使用伪身份窃取信息时。其移动授权实体 SGSN/MME 执行以下操作: 首先根据 UE 发送的切换请求消息, 计算 $ID_{\mathrm{UE'}} = h(r \| K) \oplus PID$; 其次, 获取注册阶段保存的 $PASS_i$, 得到真实的 ID_{UE}; 比较 $ID_{\mathrm{UE'}} ? = ID_{\mathrm{UE}}$, 若不成立, 则 MME/SGSN 揭露恶意用户的真实身份 $ID_{\mathrm{UE'}}$。因此, 本文方案具有可追溯性。

4.2 BAN 逻辑证明

BAN(Burrows, Abadi and Needham)逻辑是一种形式化分析方法, 其广泛适用于加密协议的安全性分析[16]。BAN 逻辑主要由通信主体, BAN 逻辑公式和加密密钥三部分组成, BAN 逻辑符号说明, 如表 2 所列。

表 2 BAN 逻辑符号说明

Table 2 BAN logic symbol description

符号	含义
A、B	参加协议的实体
N、M	公式, 为协议中消息的含义
$\mathrm{A} \mid\equiv N$	实体 A 相信消息 N 是真的
$\mathrm{A} \lhd N$	实体 A 收到消息 N
$\mathrm{A} \mid\sim N$	实体 A 发送过消息 N
$\mathrm{A} \mid\Rightarrow N$	实体 A 对 N 有仲裁权
$\#(N)$	N 是新鲜的随机数
$\mathrm{A} \xleftrightarrow{K} \mathrm{B}$	K 是 A 和 B 共享的会话密钥

为了便于描述, 证明过程中 GSM-R 和 LTE-R 异构网络中的移动授权实体 SGSN 和 MME 统一用 C 表示。

(1) 形式化描述

消息 1: UE→C:

$$\{TMSI, PID, R, PASS_1, T_1, x_{\mathrm{UE}} P\} \tag{1}$$

消息 2: C→UE:

$$\{AV, MAC, x_{\mathrm{C}} P\} \tag{2}$$

(2) 初始状态假设

在该阶段, x_{UE} 和 T 是由 UE 临时生成随机数和时间戳, 具有一次性。故假设式(3)和式(4)成立。

$$\mathrm{UE} \mid\equiv \#(T) \tag{3}$$

$$\mathrm{UE} \mid\equiv \#(x_{\mathrm{UE}}) \tag{4}$$

x_{C} 是由 C 生成的随机数, 满足一次性特点, 具有新鲜性。故假设式(5)成立。

$$\mathrm{C} \mid\equiv \#(x_{\mathrm{C}}) \tag{5}$$

UE 和 C 之间进行信息交互时, 密钥 K 为 UE 和 C 共享, 攻击者无法获取该密钥, 故 UE 和 C 都能确信彼此可以使用该密钥进行信息传递。假设式(6)~式(9)成立。

$$\mathrm{UE} \mid\equiv \left(\mathrm{UE} \xleftrightarrow{K} \mathrm{C}\right) \tag{6}$$

$$\mathrm{C} \mid\equiv \left(\mathrm{UE} \xleftrightarrow{K} \mathrm{C}\right) \tag{7}$$

$$\mathrm{UE}\left|\equiv \mathrm{C}\right|\Rightarrow\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right) \tag{8}$$

$$\mathrm{C}\left|\equiv \mathrm{UE}\right|\Rightarrow\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right) \tag{9}$$

(3) 预期目标

目标 1: $\mathrm{UE}\left|\equiv \mathrm{C}\right|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)$

目标 2: $\mathrm{UE}\left|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)\right.$

目标 3: $\mathrm{C}\left|\equiv \mathrm{UE}\right|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)$

目标 4: $\mathrm{C}\left|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)\right.$

(4) 推理证明

由式(1)可得:

$$\mathrm{C}\lhd\{TMSI,PID,R,PASS_1,T_1,x_{\mathrm{UE}}P\} \tag{10}$$

由式(7)和式(10), 运用消息含义规则可得:

$$\frac{\mathrm{C}\left|\equiv\left(\mathrm{UE}\overset{K}{\longleftrightarrow}\mathrm{C}\right),\mathrm{C}\lhd\{TMSI,PID,R,PASS_1,T_1,x_{\mathrm{UE}}P\}\right.}{\mathrm{C}\left|\equiv \mathrm{UE}\right|\sim x_{\mathrm{UE}}} \tag{11}$$

由式(5), 运用消息新鲜性规则可得:

$$\frac{\mathrm{C}\left|\equiv\#(x)\right.}{\mathrm{C}\left|\equiv\#(x,x_{\mathrm{UE}})\right.} \tag{12}$$

由式(11)式(12), 运用随机数验证规则可得:

$$\frac{\mathrm{C}\left|\equiv\#(x_{\mathrm{C}},x_{\mathrm{UE}}),\mathrm{C}\right|\equiv \mathrm{UE}\left|\sim x_{\mathrm{UE}}\right.}{\mathrm{C}\left|\equiv \mathrm{UE}\right|\equiv(x_{\mathrm{C}},x_{\mathrm{UE}})} \tag{13}$$

由式(2)得:

$$\mathrm{UE}\lhd\{AV,MAC,x_{\mathrm{C}}P\} \tag{14}$$

由式(6)和式(14), 运用消息含义规则可得:

$$\frac{\mathrm{UE}\left|\equiv\left(\mathrm{UE}\overset{K}{\longleftrightarrow}\mathrm{C}\right),\mathrm{UE}\lhd\{AV,MAC,x_{\mathrm{C}}P\}\right.}{\mathrm{UE}\left|\equiv \mathrm{C}\right|\sim x_{\mathrm{C}}} \tag{15}$$

由式(3)式(4), 运用相信规则可得:

$$\frac{\mathrm{UE}\left|\equiv\#(T),\mathrm{UE}\right|\equiv\#(x_{\mathrm{UE}})}{\mathrm{UE}\left|\equiv\#(x_{\mathrm{UE}},T)\right.} \tag{16}$$

由式(16), 运用消息新鲜性规则可得:

$$\frac{\mathrm{UE}\left|\equiv\#(x_{\mathrm{UE}},T)\right.}{\mathrm{UE}\left|\equiv\#(x_{\mathrm{UE}},T,x_{\mathrm{C}})\right.} \tag{17}$$

由式(15)和式(17), 运用随机数验证规则可得:

$$\frac{\mathrm{UE}\left|\equiv \mathrm{C}\right|\sim x_{\mathrm{C}},\mathrm{UE}\left|\equiv\#(x_{\mathrm{UE}},T,x_{\mathrm{C}})\right.}{\mathrm{UE}\left|\equiv \mathrm{C}\right|\equiv(x_{\mathrm{C}},x_{\mathrm{UE}})} \tag{18}$$

由于 $SK=x_{\mathrm{C}}PK_{\mathrm{UE}}+s_{\mathrm{C}}x_{\mathrm{UE}}P=x_{\mathrm{UE}}PK_{\mathrm{C}}+s_{\mathrm{UE}}x_{\mathrm{C}}P$

由式(15)式(18)得到:

$$\mathrm{UE}\left|\equiv \mathrm{C}\right|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right) \quad \text{(目标 1 得证)} \tag{19}$$

$$\mathrm{C}\left|\equiv \mathrm{UE}\right|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right) \quad \text{(目标 3 得证)} \tag{20}$$

由式(8)式(19), 运用仲裁规则可得:

$$\frac{\mathrm{UE}\left|\equiv \mathrm{C}\right|\Rightarrow\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right),\mathrm{UE}\left|\equiv \mathrm{C}\right|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)}{\mathrm{UE}\left|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)\right.} \tag{21}$$

(目标 2 得证)

由式(9)式(20), 运用仲裁规则可得:

$$\frac{\mathrm{C}\left|\equiv \mathrm{UE}\right|\Rightarrow\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right),\mathrm{C}\left|\equiv \mathrm{UE}\right|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)}{\mathrm{C}\left|\equiv\left(\mathrm{UE}\overset{SK}{\longleftrightarrow}\mathrm{C}\right)\right.} \tag{22}$$

(目标 4 得证)

通过初始状态和 BAN 逻辑推理, 最终推导出了预期的 4 个目标, UE 和 C 相信协商会话密钥 *SK* 的真实性和完整性, UE 和 C 的后续通话可基于此密钥推导计算, 从而保证了通信的加密密钥和完整性保护密钥的安全性, 实现了 GSM-R 向 LTE-R 演进过程中异构网络通信双方互相认证和保密性, 满足异构网络中切换安全需求。

5 性能分析

为了更好的体现本文方案的有效性, 将本文方案与其他相关方案进行安全性能对比分析, 硬件配置环境为 Intel(R) Core i7-10700K CPU @3.80 GHz, 32.0 GB RAM, NVIDIA GeForce RTX 2060 SUPER, 对比实验均在相同配置环境下进行。分析结果如表 3 所列。在表 3 中, 列出了拟议方案与传统 EPS-AKA 协议、文献[8]、文献[9]以及文献[14]在各个安全性能方面的比较。主要性能比较包括: 抗伪装用户攻击、可追溯性、匿名性以及抗中间人攻击等方面。从表 3 可以看出: 传统的 EPS-AKA 协议在安全方面存在较大漏洞, 无法实现抗中间人攻击、抗伪装用户攻击和可追溯性等功能。文献[8]采用椭圆曲线匿名代理签名方案实现用户的匿名传输, 能够抵抗中间人、重放等一系列攻击, 但是在该方案中, 恶意用户可以假装成真实的用户接入网络, 文献[8]方法无法对恶意用户的身份 *ID* 进行揭露。文献[9]中没有实现用户身份信息的匿名传输, 易遭受伪装用户攻击, 该方法无法为移动授权实体提供可追溯性验证, 对于恶意用户无法进行 *ID* 揭露。文献[14]利用区块链的抗篡改性, 结合使用门限散列函数可以揭露恶意用户 *ID*, 实现了抗伪装用户攻击, 但是该方案存在中间人攻击和无密钥后向安全性的问题。而本文方案采用椭圆曲线密钥交换 ECDH、哈希函数以及异或操作相结合的方法, 解决了协商会话密钥无前后向安全性、中间人攻击、无匿名性、以及重放攻击等问题。此外, 本文方法中引入 *Token* 和

PASS, 不仅实现了抗伪装用户攻击和可追溯性, 而且实现了用户在异构网络的无缝切换。相较于其他文献而言, 本文方法在安全性方面有着较高的优势, 很好的解决了伪装用户攻击、中间人攻击、无匿名性以及不可追溯性等问题, 提高了异构网络下铁路无线通信网络的切换认证安全性。

表 3 安全性能对比

Table 3 Comparison of safety performance

协议	抗伪装用户攻击	前向安全性	可追溯性	抗重放攻击	抗中间人攻击	相互认证	协商会话密钥更新	匿名性	后向安全性
EPS-AKA	×	×	×	×	×	×	×	×	×
文献[8]	×	√	√	√	√	√	√	√	√
文献[9]	×	√	×	√	√	√	√	×	×
文献[14]	√	√	√	√	×	√	√	√	×
本文方案	√	√	√	√	√	√	√	√	√

注: 表中×表示未达到安全需求, √表示达到安全需求。

下面进一步对通信开销、计算开销等性能进行分析, 并与其他方案(EPS-AKA、文献[8]、文献[9]、文献[14])进行比较。通信开销是指在通信的过程中信息交互的次数, 在 LTE-R 异构网络中主要包括 HSS、MME 和 UE 之间的信息交互次数[17]。在比较不同方法通信开销时, 设 UE 和 MME 之间的认证消息传递成本为 α、MME 和 MME 之间为 β、MME 和 HSS 之间为 γ, 因为在铁路实际运行场景下, 不同的通信实体通信距离不同, 因此要求满足 $0<\alpha<\beta<\gamma$ 的条件[8]。通信开销的计算如式(23)所示, 其中 i 表示不同的通信实体。

$$y=\sum_{1}^{n}\alpha(i)+\sum_{1}^{n}\beta(i)+\sum_{1}^{n}\gamma(i) \tag{23}$$

计算开销是指在通信过程中耗费的时间量, 通常以双线性对运算、标量乘、模幂、模乘、求逆、模平方、模平方根、点映射等操作的个数来衡量[18]。计算开销求解如式(24)所示, 其中函数 *fun* 为上述各类操作, 其中 j 表示不同类型的通信操作。

$$z=\sum_{1}^{n}fun(j) \tag{24}$$

经过对不同比较方法计算开销的理论分析, 计算不同方法的通信开销后, 比较结果如表 4 所列。从表 4 中可以发现: 在通信开销方面, 文献[14]采用基于门限哈希函数的碰撞特性和区块链的抗篡改方法, 其通信开销最低, 但从表 3 可知, 该文献无法抵抗中间人攻击和实现密钥后向安全性。传统 EPS-AKA 协议通信开销最高, 这是因为传统 EPS-AKA 协议中, UE 和目标网络之间必须执行完整的认证协议流程才能发生切换。文献[8]和文献[9]通信开销相同, 且均高于本文方案的通信开销, 其原因在于文献[8]和文献[9]在 UE 请求认证协议时, 其切换过程中目标移动授权实体和 UE 的通信信息都需要源移动授权实体转发到 UE, 这种过程不仅增加了交互次数而且容易引起通信过程中的安全隐患。综合表 3 和表 4 的通信开销, 本文方案有着较少的交互次数, 通信开销较少, 更能保障 GSM-R 向 LTE-R 演进过程中异构网络的切换安全。

表 4 计算开销和通信开销对比

Table 4 Comparison of computing overhead and communication overhead

方案	计算开销/ms	通信开销/bit
EPS-AKA	$12T_h$	$2\alpha+2\gamma$
文献[8]	$15T_h+2T_m+T_{ae}+T_{ad}$	$3\alpha+2\beta$
文献[9]	$5T_h+2T_m$	$3\alpha+2\beta$
文献[14]	$9T_h+6T_m+6T_a$	3α
本文方案	$8T_h+2T_m+2T_a$	$3\alpha+\beta$

注: $0<\alpha<\beta<\gamma$, 其中 T_{ae}: 对称加密, T_{ad}: 对称解密, T_m: 标量乘法, T_a: 点加法, T_h: 哈希时间。

下面进行 UE 数量改变对异构网络计算开销的影响分析。计算开销计算时, 采用文献[19]中单次计算操作开销时间作为分析参数值, 其中对称加密为 0.071ms、对称解密为 0.084ms、标量乘法为 1.038ms、点加法为 0.006ms, 哈希操作为 0.005ms[19]。将上述参数值代入表 4 中, 得到的不同比较方法单个 UE 的计算开销。比较方法是在 AES-256(Advanced Encryption Standard 256)作为对称加密算法, 及椭圆曲线群(G)的阶数为 160 的条件下得到的结果。不同 UE 条件下计算开销对比结果, 如图 5 所示。

由图 5 可以看出: 在异构网络切换过程中, UE 数量和计算开销整体上呈现出正相关关系, 原因是随着 UE 数量的增加, 服务器接收到的切换请求越多, 其执行时间则越长。其中, 传统 EPS-AKA 的计算开

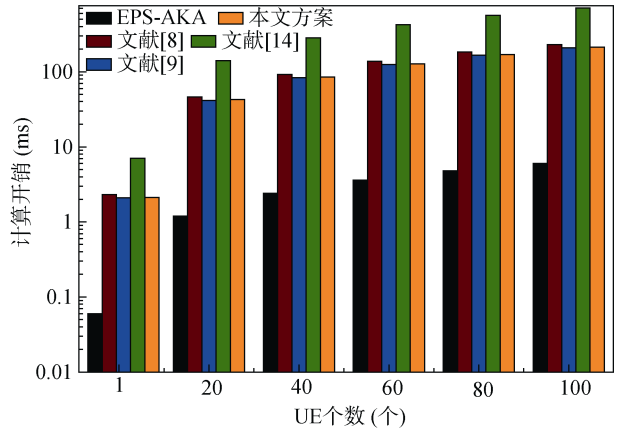

图 5　切换认证阶段计算开销对比

Figure 5　Comparison of calculation costs

销最少, 但其安全性在 5 种方法中最低, 无法满足大部分安全需求, 不适用于高速铁路中异构网络切换安全需求。文献[14]计算开销最大, 也不适合高速列车运行场景。文献[9]方案得到的计算开销比本文方案略低, 但是该方案无法满足可追溯性、匿名性和抗伪装用户攻击等一系列的安全需求, 无法对通信过程中的恶意用户实现追踪, 不能很好的为异构网络无缝切换提供安全保障。而本文方案采用基于椭圆曲线密钥交换算法结合哈希函数以及异或操作, 在异构网络切换认证中, 能够实现 UE 的匿名传输和无缝切换, 且哈希函数和椭圆曲线密钥交换算法较其余原始加密操作执行时间最少, 故本文方案的计算开销低于文献[8]和文献[14]。

为了进一步验证本文所提方案的有效性, 下面以朔黄铁路 LTE-R 线路实测数据进行不同方法对比分析[3]。朔黄铁路是一条重载铁路, 采用 LTE-R 宽带移动通信网络作为无线通信支撑网络, 其正线全长 598km, 站线全长 217.916, 共有车站 33 个, 对于朔黄铁路实测数据, 采用本文方案较其他比较方法在计算机开销和通信开销对比结果, 如表 5 所示。

表 5　朔黄铁路计算开销和通信开销对比

Table 5　Comparison of computing overhead and communication overhead in Shuohuang Railway

方案	计算开销/ms	通信开销/bit
EPS-AKA	20.160	38400
文献[8]	73.792	52224
文献[9]	67.232	39520
文献[14]	201.888	34816
本文方案	68.096	36864

由表 5 可知, 在朔黄铁路实测数据对比中, 本文方案所需计算开销低于文献[8]和文献[14], 略高于文献[9]和传统 EPS-AKA 方法, 其原因是在通信协议的身份认证和密钥协商过程中, 传统 EPS-AKA 协议中仅采用哈希操作实现, 文献[9]使用椭圆曲线密钥算法, 上述两种方法计算开销较小, 但从表 3 可知 EPS-AKA 安全性能在所有方案中最低, 文献[9]无法满足抗伪装用户攻击和可追溯性等安全需求。文献[14]方法多次采用标量乘操作进行异构网络之间的切换认证和密钥协商, 导致其计算开销在五种方法中最高。而本文方案采用点加操作完成身份认证和密钥协商, 具有较少的计算开销, 此外结合表 3 的性能分析可知, 本文方案具有较高的安全性能。

此外, 在通信开销实测对比中, 本文方案所需通信开销低于传统 EPS-AKA、文献[8]和文献[9]方法, 略高于文献[14], 其原因是本文使用切换认证码 *PASS* 实现异构网络之间的无缝切换, 减少了通信开销, 而文献[8]和文献[9]进行异构网络之间的切换时, 均都需要源移动授权实体参与到切换过程中, 增加了交互次数, 导致通信开销增大, 而且根据表 3 中的性能分析可知, 传统 EPS-AKA、文献[8]、文献[9]和文献[14]均无法满足实际铁路通信过程中安全性需求。综上所述, 上述性能理论分析和朔黄铁路实测数据对比分析表明: 本文方案不仅具有较高的安全性能, 又有较低的通信开销和计算开销, 能够满足异构网络的无缝切换需求。

6　总结

针对下一代高速铁路通信异构网络中存在的安全及切换效率问题, 本文提出了一种基于椭圆曲线密钥交换算法、哈希技术以及切换认证码 *PASS* 的切换认证密钥协商方案, 并根据异构网络无缝切换的实际需求设计了初始化、注册认证协议及垂直切换认证协议, 最后采用 BAN 逻辑进行了形式化安全性验证。结果表明:

(1) 本文方案实现了 UE 的匿名接入和服务器的可追溯性, 能够抵抗伪装用户攻击, 服务器通过验证用户 *ID* 可以揭露恶意用户 *ID*。通过切换认证码 *PASS* 实现异构网络之间的无缝切换。

(2) 本文方案利用椭圆曲线密钥交换算法 ECDH 实现会话协商密钥的动态更新, 实现了密钥的前后向安全性, 能够有效抵抗中间人攻击和重放攻击。

(3) 本文方案中不仅使异构网络具有健壮性, 而且在通信开销和计算开销方面也有很好的表现, 能够更好的为异构网络中的切换认证服务, 且研究结果表明该方案对切换认证提供了一定的理论依据。

GSM-R 和 LTE-R 组成的异构网络在我国高速铁路运行中扮演者至关重要的角色，作为异构网络其无缝切换安全对于保障列车运行安全具有重要的理论意义和现实意义。

参考文献

[1] Yang J Y, Ai B, Salous S, et al. An Efficient MIMO Channel Model for LTE-R Network in High-Speed Train Environment[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(4): 3189-3200.

[2] Wen T, Ge Q B, Lyu X N, et al. A Cost-Effective Wireless Network Migration Planning Method Supporting High-Security Enabled Railway Data Communication Systems[J]. *Journal of the Franklin Institute*, 2021, 358(1): 131-150.

[3] Chen Y, Chen Y, Zhang W. Modeling and Analysis of LTE-R Wireless Communication Reliability Based on SPN[J]. *Journal of the China Railway Society*, 2020, 42(9): 111-119.
(陈永, 陈耀, 张薇. 基于 SPN 的 LTE-R 无线通信可靠性建模与分析[J]. *铁道学报*, 2020, 42(9): 111-119.)

[4] Wang L, Zhang L H. Analysis on a Double-Network Mutual Aid Method for GSM-R/LTE-R Dual-Mode Terminal[J]. *China Railway*, 2020(5): 100-104.
(王亮, 张路昊. GSM-R/LTE-R 双模终端的一种双网互助方法分析[J]. *中国铁路*, 2020(5): 100-104.)

[5] 3GPP TS33.401.Technical Specification. 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects, 2020, 7.

[6] Alezabi K A, Hashim F, Hashim S J, et al. Efficient Authentication and re-Authentication Protocols for 4G/5G Heterogeneous Networks[J]. *EURASIP Journal on Wireless Communications and Networking*, 2020, 2020(1): 105.

[7] Zhang Y H, Li Y M, Li Y F. et al. Group-based handover authentication scheme for 5G heterogeneous networks[J]. *Computer Engineering and Applications*, 2021: 1-11.
(张应辉, 李一鸣, 李怡飞,等. 5G 异构网络中基于群组的切换认证方案[J]. *计算机工程与应用*, 2021: 1-11.)

[8] Wang Y, Zhang W F, Wang X M, et al. Improving the Security of LTE-R for High-Speed Railway: From the Access Authentication View[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(2): 1332-1346.

[9] Wu W F, Zhang W F, Wang X M, et al. A Security Enhanced Train to Ground Wireless Communication Authentication Key Agreement Scheme for LTE-R[J]. *Journal of the China Railway Society*, 2019, 41(12): 66-74.
(吴文丰, 张文芳, 王小敏, 等. 一种安全增强的 LTE-R 车-地无线通信认证密钥协商方案[J]. *铁道学报*, 2019, 41(12): 66-74.)

[10] Suvidha K S, Kamath S S. Secure 4G SEPS-AKA protocol for UMTS networks[C]. *2020 5th International Conference on Computing, Communication and Security*, 2020: 1-6.

[11] Cai N, Han Y N, An W, et al. A Survey of Distributed SDN Controller Placement Problem[J]. *Journal of Cyber Security*, 2021, 6(2): 46-72.
(蔡宁, 韩言妮, 安伟, 等. 分布式 SDN 控制器放置问题研究[J]. *信息安全学报*, 2021, 6(2): 46-72.)

[12] Mo J Q, Li K M. A Secure and Efficient Anonymous User Authentication and Key Agreement Scheme for Global Mobility Networks Based on Bilinear Pairing[C]. *2020 IEEE 3rd International Conference on Electronic Information and Communication Technology*, 2021: 579-584.

[13] Ozhelvaci A, Ma M. A Fast and Secure Uniform Handover Authentication Scheme for 5G HetNets[M]. Switzerland:2021 Springer Nature Switzerland AG, 2021: 119-131.

[14] Zhang Y H, Deng R H, Bertino E, et al. Robust and Universal Seamless Handover Authentication in 5G HetNets[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(2): 858-874.

[15] Chen R, Long W X, Mao G Q, et al. Development Trends of Mobile Communication Systems for Railways[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(4): 3131-3141.

[16] Haq U I, Wang J, Zhu Y W. Secure Two-Factor Lightweight Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server 5G Networks[J]. *Journal of Network and Computer Applications*, 2020, 161: 102660.

[17] Fu Y, Li Q D, Zhang Z H, et al. Data Integrity Verification Scheme for Privacy Protection and Fair Payment[J]. *Journal of Computer Research and Development*, 2022, 59(6): 1343-1355.
(富瑶, 李庆丹, 张泽辉, 等. 支持隐私保护和公平支付的数据完整性验证方案[J]. *计算机研究与发展*, 2022, 59(6): 1343-1355.

[18] He Y X, Sun F J, Li Q G, et al. A Survey on Public Key Mechanism in Wireless Sensor Networks[J]. *Chinese Journal of Computers*, 2020, 43(3): 381-408.
(何炎祥, 孙发军, 李清安, 等. 无线传感器网络中公钥机制研究综述[J]. *计算机学报*, 2020, 43(3): 381-408.)

[19] Xue J B, Bai Z M. Security and Efficient Authentication Scheme for Mobile Edge Computing[J]. *Journal of Beijing University of Posts and Telecommunications*, 2021, 44(1): 110-116.
(薛建彬, 白子梅. 边缘计算中移动终端安全高效认证协议[J]. *北京邮电大学学报*, 2021, 44(1): 110-116.)

陈永 于 2014 年在兰州交通大学智能交通与信息系统工程专业获得博士学位。现任兰州交通大电子与信息工程学院教授。研究领域为高可信铁路无线通信、软件形式化方法。Email:edukeylab@126.com

刘雯 于 2017 年在兰州交通大学物联网工程专业获得学士学位。现在兰州交通大学计算机科学与技术专业攻读硕士学位。研究领域为高速铁路无线通信安全。Email:1476870435@qq.com

詹芝贤 于 2019 年在厦门大学嘉庚学院软件工程专业获得学士学位。现在兰州交通大学电子信息专业攻读硕士学位。研究领域为铁路无线通信可靠性理论。
Email:edukeylab@126.com