http://bhxb.buaa.edu.cn jbuaa@buaa.edu.cn
DOI: 10.13700/j.bh.1001-5965.2024.0010

基于NTRU格上的高铁共生网络安全切换认证方案

陈永*，张冰旺，信召凤
(兰州交通大学 电子与信息工程学院，兰州 730070)

摘 要：针对高铁GSM-R无线通信系统向下一代5G-R网络演进过程中，共生网络垂直切换时存在身份泄露、不具备前后向安全性和认证开销大等问题，提出了一种基于NTRU格上的高铁共生网络安全切换认证方案。设计了基于NTRU格的双向认证机制，克服了身份信息SUPI明文传输易泄露的缺点；提出基于共享密钥的哈希链加密方法，设计共享密钥生成和共生网络切换令牌策略，实现切换认证密钥的预生成，确保了共享密钥的动态更新及前后向安全性；采用中国剩余定理及时间戳机制实现了会话密钥的机密性，完成了共生网络的切换认证。通过BAN逻辑形式化理论证明和TAMARIN协议仿真验证工具对所提方法进行安全性分析，结果表明：与同类方法相比，所提方法确保了身份的匿名性和密钥前后向安全性，可有效抵抗DoS攻击和中间人攻击等攻击，具有更低的切换开销，能够满足高铁共生网络安全无缝切换认证的需求。

关 键 词：铁路无线通信；共生网络；切换认证；NTRU格加密；通信效率
中图分类号：U285.2; TP391.9
文献标志码：A **文章编号**：1001-5965(2026)04-1076-12

目前，中国高铁采用GSM-R无线通信系统，但GSM-R属于2G窄带通信技术，已无法满足未来中国高铁智能化、大带宽、多业务的发展需求[1]。5G-R作为中国下一代高铁无线通信系统，具有大带宽、低时延等优点[2]。2023年9月，随着工业和信息化部批复5G-R试验频率，全国范围将逐步开展外场试验，GSM-R网络将逐步向5G-R网络平滑演进。从铁路专用无线通信系统长期演进过程来看，未来将长期出现GSM-R和5G-R网络融合共生的局面[3-4]。然而，高铁共生网络场景下开放的多模空中接口及5G-R全IP的扁平化网络构架，使其更易遭受篡改、假冒欺骗等安全风险[5-6]。因此，如何保障高铁异构共生网络之间的安全认证，对高速列车行车安全至关重要。

在GSM-R与5G-R共生网络间切换认证过程中，被指出存在身份标识泄露、难以抵抗DoS攻击、重放攻击、不具备前后向安全性、通信开销及计算开销大等问题[7-9]。针对5G-R异构网络切换认证过程存在的安全漏洞，国内外学者展开了大量研究。Wang等[7]面向铁路专用无线通信系统，设计了一种基于无证书代理签名的垂直切换认证方案，但其密钥参数以明文方式传输，存在密钥泄露的风险。Cao等[8]提出了一种基于软件定义网络(software-defined network, SDN)的用户设备(user equipment, UE)隐私保护垂直切换认证方法，依据授权票证技术实现了UE和基站间的相互认证，但不能保证会话密钥后向安全性。Alezabi等[9]提出了基于椭圆曲线身份授权机制的垂直切换认证方案，确保了密钥的前后向安全性，但采用明文ID检索来匹配会话密钥，易遭受DoS攻击。Ma等[10]设计了基于非参数检验假设的物理层和上层加密方法，实现了5G异构网络垂直切换认证，但未能充分利用样本

收稿日期：2024-01-08；**录用日期**：2024-02-23；**网络出版时间**：2024-03-12 10:00
网络出版地址：link.cnki.net/urlid/11.2625.V.20240311.1521.004
基金项目：国家自然科学基金(62462043,61963023)；甘肃省自然科学基金(26JRRA589)
*通信作者. E-mail：edukeylab@126.com

引用格式：陈永，张冰旺，信召凤. 基于NTRU格上的高铁共生网络安全切换认证方案[J]. 北京航空航天大学学报，2026，52(4)：1076-1087. CHEN Y，ZHANG B W，XIN Z F. Security handover authentication scheme for high-speed railway symbiotic network based on NTRU lattice[J]. Journal of Beijing University of Aeronautics and Astronautics，2026，52(4)：1076-1087 (in Chinese).

信息, 无法处理交互作用, 且易遭受重放攻击。Yang 等[11] 基于 5G SDN 设计了一种由 UE 位置决定的无线链路签名切换认证, 实现了切换密钥的机密性保护。Cui 等[12] 提出了一种支持边缘计算的统一垂直切换认证框架, 利用基于强化学习的信任评估机制识别非法 UE, 可以抵抗中间人攻击, 但无法抵抗重放攻击。Kalia 等[13] 提出了基于逻辑回归预测的异构网络认证方案, 可抵抗伪基站的欺骗和攻击, 但对异常值较敏感, 在频繁高速切换认证时, 攻击者可引入或模拟异常值欺骗逻辑回归切换认证模型, 继而引发 DoS 攻击。Liu 等[14] 通过依赖于随机数自循环加密结构的掩码验证实现切换, 可有效抵抗去同步攻击, 但掩码数组自循环密钥推导方式增加了计算开销。Divakaran 等[15] 设计了一种基于模糊逻辑的切换认证模型, 降低了垂直切换认证开销, 但存在参数阈值选择主观性的问题, 且无法抵御去同步攻击及重放攻击。Sharma 等[16] 提出了一种移动切换链路协议, 该方案基于椭圆曲线加密技术实现了 UE 跨多个集线器的切换认证, 具有前后向安全性, 但无法抵抗去同步攻击。Zhou 等[17] 利用格密码理论, 设计了一种 UE 隐私保护的切换认证方案, UE 通过伪随机标识符 SID 与认证服务器进行通信, 保护了 UE 身份隐私, 可抵抗量子计算攻击, 但对随机标识符 SID 未识别, 攻击者可伪造大量 SID 发起对认证服务的 DoS 攻击。

综上所述, 针对高铁垂直切换认证中仍存在身份泄露、不具备前后向安全性和认证开销大等问题, 本文提出了一种基于 NTRU 格上的高铁共生网络安全切换认证方案。主要工作有: ①设计了基于 NTRU 格的双向认证机制, 通过生成临时身份信息及时间戳确保认证消息的新鲜性, 实现了列车身份匿名性; ②提出了基于共享密钥的哈希链加密方法, 设计共享密钥生成和共生网络切换令牌策略, 实现垂直切换认证的密钥预生成, 以减少切换认证开销, 同时, 确保了共享密钥的动态更新及会话密钥的前后向安全性; ③采用中国剩余定理密钥协商方法及时间戳机制, 确保了会话密钥的机密性, 完成垂直切换认证。通过 BAN 逻辑形式化理论证明和 TAMARIN 协议仿真验证工具验证了本文所提协议的安全性, 结果表明, 方案具有更高的安全性及更低的切换开销。

1　共生网络架构及切换认证机制

高铁共生网络是一种实现列车 UE 在异构体制网络内安全高效互联的网络体系结构, 由 GSM-R 网络和 5G-R 网络组成[3-4], 如图 1 所示。图中: AuC 为鉴权中心, MSC 为移动交换中心, MEC 为多接入边缘计算。其中, GSM-R 无线接入网采用基站控制器 (base station controller, BSC) 控制基站收发信台 (base transceiver station, BTS) 的结构。列车 UE 与接入网通过空中接口传输 UE 身份信息、行车控制信令等隐私数据。GSM-R 网络向 5G-R 网络演进过程中, 通过 5G 带宽集群通信设备 MCX 实现跨网互联, 网元设备采取按线路平稳升级更新的方法。接入控制和移动管理设备 SGSN 将演进升级为接入和移动管理服务器 (access and mobility management function, AMF), 由 AMF 负责列车 UE 接入注册管理。而归属位置寄存器 (home location register, HLR) 将演进升级为鉴权服务中心 (authentication server function, AUSF), 升级后 AUSF 将集成鉴权算法, 为列车 UE 生成切换认证向量。

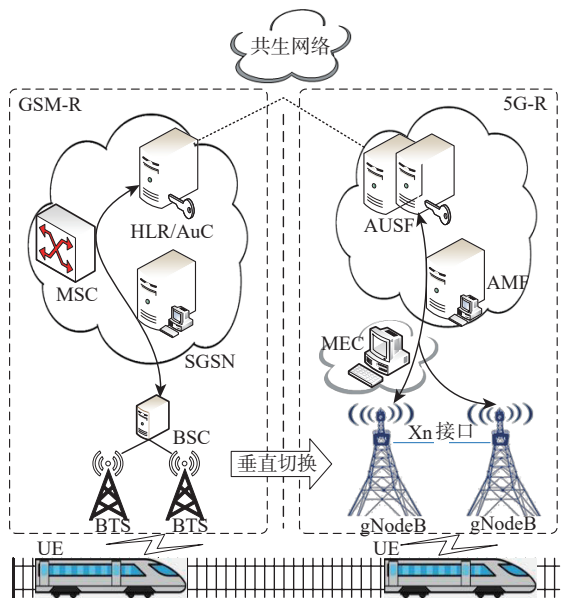

图 1　高铁共生网络架构

Fig. 1　Architecture of high-speed railway symbiotic network

图 1 中, 列车 UE 通过 GSM-R/5G-R 源接入网 BTS/gNodeB 向接入控制和移动管理设备 SGSN/AMF 发起入网请求, 将鉴权和加密信息发送至 HLR/AUSF, 通过身份权限互认证后, UE 通过源 SGSN/AMF 向目标 AMF/SGSN 发起跨网切换请求, 并根据目标 AMF/SGSN 消息响应机制与目标接入网 gNodeB/BTS 建立安全会话, 从而完成高铁共生网络垂直切换认证。GSM-R/5G-R 双向切换认证流程如下:

步骤 1　列车 UE 通过接入网 BTS/gNodeB 向 SGSN/AMF 发起接入请求, HLR/AUSF 为各通信实体生成系统加密参数。

步骤 2　SGSN/AMF 收到接入请求后, 验证列车 UE 身份, 若验证失败, 则终止会话; 否则, 生成

质询消息并发送至基站BTS/gNodeB。

步骤3 基站BTS/gNodeB收到质询信息后，获取列车UE身份信息，并计算响应消息，来验证列车UE和SGSN/AMF身份合法性。若验证失败，则终止接入认证协议；否则，列车UE接入GSM-R/5G-R共生网络。

步骤4 列车UE成功接入GSM-R/5G-R共生网络后，源SGSN/AMF和目标AMF/SGSN通过共享密钥计算双方身份认证消息，完成身份互认证后，进行后续切换认证阶段。

步骤5 源SGSN/AMF和目标AMF/SGSN完成身份互认证后，列车UE计算切换认证消息并发送至目标gNodeB/BTS和目标AMF/SGSN。目标gNodeB/BTS和目标AMF/SGSN验证列车UE身份合法性，若验证通过，则列车UE完成切换认证，否则，终止会话。

2 本文方法

NTRU密码是一种基于格理论的环上带错学习(learning with errors over rings, RLWE)问题的轻量级公钥加密方法，基于格困难问题被证明在随机归约下均属于NP-hard类问题，相比于椭圆曲线加密机制，其可抵抗量子攻击，且具有更快的计算速度和更小的密钥长度[18]。鉴于以上优点，本文提出了一种基于NTRU格的高铁共生网络垂直切换认证方案，主要包括5个阶段：系统初始化阶段、接入认证阶段、共享密钥建立阶段、令牌授权过程和垂直切换认证阶段。

2.1 系统初始化阶段

系统初始化阶段，高速列车UE向移动授权实体SGSN/AMF和认证服务器HLR/AUSF发起入网注册请求。HLR/AUSF生成系统加密参数，该过程基于定义在如下3个截尾多项式环上的NTRU格加密机制进行设计：

$$\begin{cases} R[X]=\dfrac{Z[X]}{X^N-1} \\ R_p[X]=\dfrac{(Z/pZ)[X]}{X^N-1} \\ R_q[X]=\dfrac{(Z/qZ)[X]}{X^N-1} \end{cases} \tag{1}$$

式中：N、p、q为参数集合，N为素数；Z为整数环；多项式环R_p和R_q分别由多项式环R的系数模上p和q所得，整数q，p满足$q\geqslant p$。此外，HLR/AUSF认证服务器通过4个次数为$N-1$的整系数多项式集合$\{L_f, L_g, L_r, L_m\}$生成系统公钥和私钥。其中，记$L(d_1,d_2)=\{F\in R[X]\,|\,|\{i|F_i=1\}|=d_1, |\{i|F_i=-1\}|=d_2\}$，则有

$$\begin{cases} L_f=L(d_f,d_f-1) \\ L_g=L(d_g,d_g) \\ L_r=L(d_r,d_r) \\ L_m=m\in R[X] \end{cases} \tag{2}$$

式中：m的系数位于区间$[-(p-1)/2,(p-1)/2]$，且p为素数。

系统初始化流程如图2所示，步骤如下：

步骤1 HLR/AUSF依据NTRU密钥体制从环$R[X]$选择公共参数$\{N, q, p\}$，以及4个度不超过$N-1$的多项式集合$\{L_f, L_g, L_r, L_m\}$。HLR/AUSF选择2个多项式$\{f_{\mathrm{HLR/AUSF}}\in L_f, g_{\mathrm{HLR/AUSF}}\in L_g\}$，并且要求存在$\{f_{q,\mathrm{HLR/AUSF}}^{-1}\in R_q[X],\ f_{p,\mathrm{HLR/AUSF}}^{-1}\in R_p[X]\}$，且满足：$\{f_{q,\mathrm{HLR/AUSF}}^{-1}*f_{\mathrm{HLR/AUSF}}\equiv 1(\mathrm{mod}\ q),\ f_{p,\mathrm{HLR/AUSF}}^{-1}*f_{\mathrm{HLR/AUSF}}\equiv 1(\mathrm{mod}\ p)\}$。其中，“$*$”为NTRU多项式环上的卷积乘法。若$\{f_{q,\mathrm{UE}}^{-1}, f_{p,\mathrm{UE}}^{-1}\}$在环$R_q$和环$R_p$上不存在，则重新选择原函数。

步骤2 HLR/AUSF计算其公私钥对$\{K_{\mathrm{HLR/AUSF}}^{\mathrm{PK}}=pf_{q,\mathrm{HLR/AUSF}}^{-1}g_{\mathrm{HLR/AUSF}}(\mathrm{mod}\ q),\ K_{\mathrm{HLR/AUSF}}^{\mathrm{SK}}=(f_{\mathrm{HLR/AUSF}}, pf_{q,\mathrm{HLR/AUSF}}^{-1})\}$，并为SGSN/AMF随机选取一个加密密钥$K_{\mathrm{SGSN/AMF}}^{\mathrm{ESK}}$，公布系统参数$\{N, q, p, L_f, L_g, L_r, L_m, h\}$。其中，$h$为哈希加密函数。

步骤3 HLR/AUSF选择3个多项式$f_{\mathrm{UE}}\in L_f$，$f_{\mathrm{SGSN/AMF}}\in L_f$，$f_{\mathrm{AMF/SGSN}}\in L_f$，并计算相应的公钥$K_{\mathrm{UE}}^{\mathrm{PK}}=pf_{q,\mathrm{UE}}^{-1}*g_{\mathrm{HLR/AUSF}}(\mathrm{mod}\ q)$，$K_{\mathrm{SGSN/AMF}}^{\mathrm{PK}}=pf_{q,\mathrm{SGSN/AMF}}^{-1}*g_{\mathrm{HLR/AUSF}}(\mathrm{mod}\ q)$，$K_{\mathrm{AMF/SGSN}}^{\mathrm{PK}}=pf_{q,\mathrm{AMF/SGSN}}^{-1}*g_{\mathrm{HLR/AUSF}}(\mathrm{mod}\ q)$。

步骤4 HLR/AUSF向列车UE发送公钥信息$(K_{\mathrm{HLR/AUSF}}^{\mathrm{PK}}, K_{\mathrm{UE}}^{\mathrm{PK}})$，并分别向源SGSN/AMF和目标AMF/SGSN发送$(K_{\mathrm{HLR/AUSF}}^{\mathrm{PK}}, K_{\mathrm{SGSN/AMF}}^{\mathrm{PK}}, K_{\mathrm{AMF/AUSF}}^{\mathrm{PK}})$。

此阶段完成后，系统各密钥参数初始化完成。

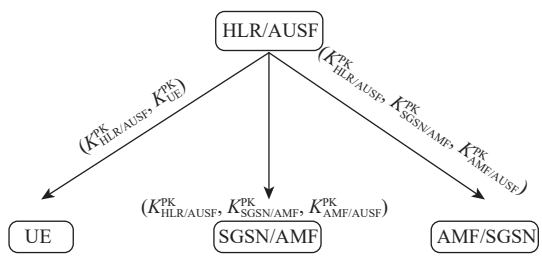

图2 系统初始化流程

Fig. 2 System initialization process

2.2 接入认证阶段

在完成系统初始化后，列车UE运行前，通过接入认证协议安全接入GSM-R/5G-R共生网络。采用NTRU格上双向认证机制生成列车UE伪身份，UE通过检验带有时间戳信息的消息认证码完成与基站BTS/gNodeB身份互认证，UE安全地接入GSM-R/5G-R共生网络。接入认证流程如图3所示，具体

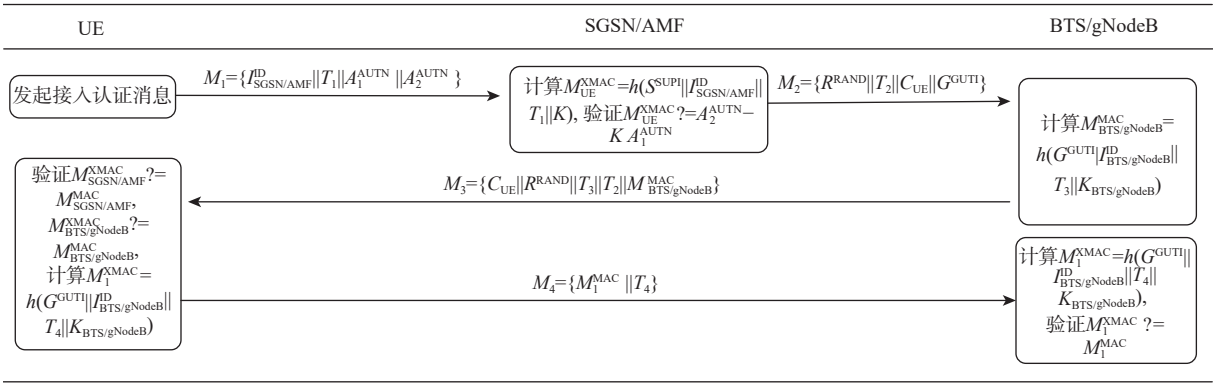

图 3　接入认证流程

Fig. 3　Access authentication process

步骤如下:

步骤 1　UE 选取随机数 $r_{UE}\in L_r$, 同时生成时间戳消息 T_1。计算认证信息 $A^{AUTN}_1=r_{UE}K^{PK}_{SGSN/AMF}+S^{SUPI}$、$M^{MAC}_{UE}=h(S^{SUPI}||I^{ID}_{SGSN/AMF}||T_1||K)$ 和 $A^{AUTN}_2=KA^{AUTN}_1+M^{MAC}_{UE}$, 其中, K 为 UE 与 SGSN/AMF 的共享密钥。通过基站 BTS/gNodeB 发送信息 $M_1=\{I^{ID}_{SGSN/AMF}||T_1||A^{AUTN}_1||A^{AUTN}_2\}$至移动管理中心 SGSN/AMF。

步骤 2　SGSN/AMF 收到消息 M_1 后, 计算 $a=f_{SGSN/AMF}A^{AUTN}_1(\mathrm{mod}\ q)$ 和 $S^{SUPI}=f^{-1}_{p,SGSN/AMF}\ a(\mathrm{mod}\ p)$。依据 S^{SUPI} 查询与对应 UE 的共享密钥 K, 并计算 $M^{XMAC}_{UE}=h(S^{SUPI}||I^{ID}_{SGSN/AMF}||T_1||K)$, 验证 $M^{XMAC}_{UE}?=A^{AUTN}_2-KA^{AUTN}_1$, 验证通过后, 表明 SGSN/AMF 收到了来自合法 UE 的信息, 若验证失败, 则终止会话; 否则, SGSN/AMF 随机选取 R^{RAND} 和消息值有效期 V^{VP}, 并生成时间戳信息 T_2, 依次计算 $K_{SGSN/AMF}=h(S^{SUPI}||I^{ID}_{SGSN/AMF}||R^{RAND}||K)$、$K_{BTS/gNodeB}=h(S^{SUPI}||I^{ID}_{BTS/gNodeB}||K_{SGSN/AMF})$、消息鉴别码 $M^{MAC}_{SGSN/AMF}=h(S^{SUPI}||I^{ID}_{SGSN/AMF}||T_2||K_{SGSN/AMF})$、UE 临时身份 $G^{GUTI}=E_{ES}K_{SGSN/AMF}(S^{SUPI}||V^{VP})$ 和参数加密信息 $C_{UE}=E_{K_{SGSN/AMF}}(R^{RAND}||S^{SUPI}||M^{MAC}_{SGSN/AMF}||G^{GUTI}||K_{BTS/gNodeB})$。发送 $M_2=\{R^{RAND}||T_2||C_{UE}||G^{GUTI}\}$给基站 BTS/gNodeB。

步骤 3　基站 BTS/gNodeB 收到消息 M_2 后, 从中获取 UE 临时身份信息 G^{GUTI}, 并计算 $M^{MAC}_{BTS/gNodeB}=h(G^{GUTI}||I^{ID}_{BTS/gNodeB}||T_3||K_{BTS/gNodeB})$。发送消息 $M_3=\{C_{UE}||R^{RAND}||T_3||T_2||M^{MAC}_{BTS/gNodeB}\}$至 UE。

步骤 4　UE 收到 M_3 后, 计算 $K_{SGSN/AMF}=h(S^{SUPI}||I^{ID}_{SGSN/AMF}||R^{RAND}||K)$ 和 $M^{XMAC}_{SGSN/AMF}=h(S^{SUPI}||I^{ID}_{SGSN/AMF}||T_2||K_{SGSN/AMF})$。验证 $M^{XMAC}_{SGSN/AMF}?=M^{MAC}_{SGSN/AMF}$, 验证通过, 则表明 UE 成功认证 SGSN/AMF 身份。此时, UE 计算 $K_{BTS/gNodeB}=h(S^{SUPI}||I^{ID}_{BTS/gNodeB}||K_{SGSN/AMF})$ 和 $M^{XMAC}_{BTS/gNodeB}=h(G^{GUTI}||I^{ID}_{BTS/gNodeB}||T_3||K_{BTS/gNodeB})$。验证 $M^{XMAC}_{BTS/gNodeB}?=M^{MAC}_{BTS/gNodeB}$, 验证通过, 表明 UE 成功认证基站 BTS/gNodeB 身份。此时, 计算 $M^{XMAC}_1=h(G^{GUTI}||I^{ID}_{BTS/gNodeB}||T_4||K_{BTS/gNodeB})$,发送消息 $M_4=\{M^{MAC}_1||T_4\}$给基站 BTS/gNodeB。

步骤 5　基站 BTS/gNodeB 收到 M_4 后, 计算 $M^{XMAC}_1=h(G^{GUTI}||I^{ID}_{BTS/gNodeB}||T_4||K_{BTS/gNodeB})$, 验证 $M^{XMAC}_1?=M^{MAC}_1$, 验证通过, 表明基站 BTS/gNodeB 成功认证 UE 身份。

此阶段完成后, 列车 UE、基站 BTS/gNodeB 和移动管理中心 SGSN/AMF 完成身份互认证, UE 和基站 BTS/gNodeB 基于协商的密钥 $K_{BTS/gNodeB}$ 实现接入层通信, UE 成功接入 GSM-R/5G-R 共生网络。

2.3　共享密钥建立阶段

在完成接入认证阶段后, 进一步设计了共享密钥建立阶段。为了解决现有高铁共生网络垂直切换认证中, 源 SGSN/AMF 与目标 AMF/SGSN 之间存在的共享密钥长期不更新, 无法保证列车 UE 与目标 AMF/SGSN 间建立会话密钥安全性的问题, 在生成共享密钥之前, 源 SGSN/AMF 与目标 AMF/SGSN 应完成相互身份认证。共享密钥建立流程如图 4 所示, 具体步骤如下:

步骤 1　源 SGSN/AMF 选取 $L_{m,SGSN/AMF}\in L_m$ 和随机多项式 r, 并计算 $R_{SGSN/AMF}=p(r*K^{PK}_{AMF/SGSN})+L_{m,AMF/SGSN}(\mathrm{mod}\ q)$, $Y_{SGSN/AMF}=L_{m,AMF/SGSN}*K^{PK}_{HLR/AUSF}(\mathrm{mod}\ q)$, 身份匿名 $I^{RID}_{SGSN/AMF}=h(K^{PK}_{SGSN/AMF}||L_{m,SGSN/AMF}*K^{PK}_{HLR/AUSF})\oplus I^{ID}_{SGSN/AMF}$, $I^{YID}_{SGSN/AMF}=h(I^{ID}_{SGSN/AMF}\oplus Y_{SGSN/AMF})$。源 SGSN/AMF 将 $\{R_{SGSN/AMF}, I^{RID}_{SGSN/AMF}, I^{YID}_{SGSN/AMF}\}$发送到目标 AMF/SGSN。

步骤 2　目标 AMF/SGSN 选取 $L_{m,AMF/SGSN}\in L_m$, 并计算 $R_{AMF/SGSN}=p(r*K^{PK}_{SGSN/AMF})+L_{m,AMF/SGSN}(\mathrm{mod}\ q)$, $Y_{AMF/SGSN}=L_{m,AMF/SGSN}*K^{PK}_{HLR/AUSF}(\mathrm{mod}\ q)$, $I^{RID}_{AMF/SGSN}=h(K^{PK}_{AMF/SGSN}||L_{AMF/SGSN}*K^{PK}_{HLR/AUSF})\oplus I^{ID}_{AMF/SGSN}$, $I^{YID}_{AMF/SGSN}=h(I^{ID}_{AMF/SGSN}||Y_{AMF/SGSN})$。目标 AMF/SGSN 将 $\{R_{AMF/SGSN}, I^{RID}_{AMF/SGSN}, I^{YID}_{AMF/SGSN}\}$发送到源 SGSN/AMF。

步骤 3　源 SGSN/AMF 接收到消息 $\{R_{AMF/SGSN}, I^{RID}_{AMF/SGSN}, I^{YID}_{AMF/SGSN}\}$后, 应用私钥 $f^{-1}_{q,SGSN/AMF}$ 解密

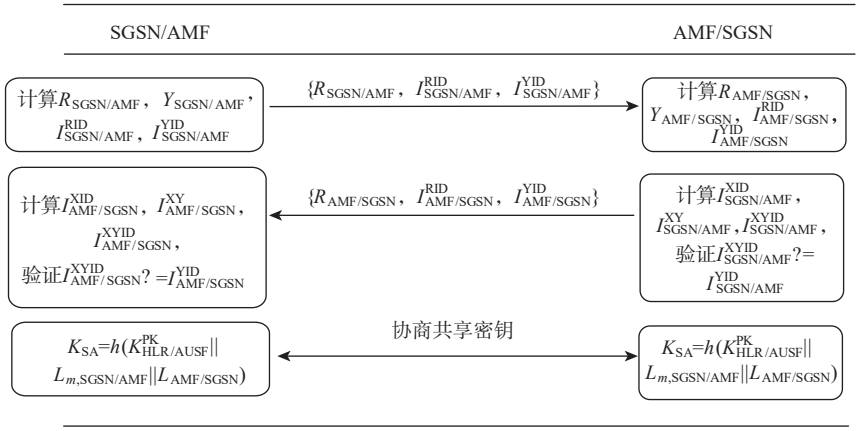

图4 共享密钥建立流程

Fig. 4 Shared key establishment process

$R_{AMF/SGSN}$ 获得 $L_{m,AMF/SGSN}$。

步骤 4 源 SGSN/AMF 计算 $I^{XID}_{AMF/SGSN}=h(K^{PK}_{AMF/SGSN}||L_{m,AMF/SGSN}*K^{PK}_{HLR/AUSF})\oplus I^{RID}_{AMF/SGSN}$，$I^{XY}_{AMF/SGSN}=L_{m,AMF/SGSN}*K^{PK}_{HLR/AUSF}(\mathrm{mod}\ q)$，$I^{XYID}_{AMF/SGSN}=H(I^{ID}_{AMF/SGSN}||Y_{AMF/SGSN})$，验证 $I^{XYID}_{AMF/SGSN}$?=$I^{YID}_{AMF/SGSN}$，验证通过，则表明源 SGSN/AMF 成功认证目标 AMF/SGSN 身份。

步骤 5 目标 AMF/SGSN 接收到消息{$R_{SGSN/AMF}$，$I^{RID}_{SGSN/AMF}$，$I^{YID}_{SGSN/AMF}$}后，应用私钥 $f^{-1}_{q,AMF/SGSN}$ 解密 $R_{SGSN/AMF}$ 获得 $L_{m,SGSN/AMF}$。

步骤 6 目标 AMF/SGSN 计算 $I^{XID}_{SGSN/AMF}=h(K^{PK}_{SGSN/AMF}||L_{m,SGSN/AMF}*K^{PK}_{HLR/AUSF})\oplus I^{RID}_{SGSN/AMF}$，$I^{XY}_{SGSN/AMF}=L_{m,SGSN/AMF}*K^{PK}_{HLR/AUSF}(\mathrm{mod}\ q)$，$I^{XYID}_{SGSN/AMF}=h(I^{ID}_{SGSN/AMF}||Y_{SGSN/AMF})$，验证 $I^{XYID}_{SGSN/AMF}$?=$I^{YID}_{SGSN/AMF}$，验证通过，则表明目标 AMF/SGSN 成功认证源 SGSN/AMF 身份。

步骤 7 源 SGSN/AMF 和目标 AMF/SGSN 分别计算协商出共享密钥 $K_{SA}=h(K^{PK}_{HLR/AUSF}||L_{m,SGSN/AMF}||L_{AMF/SGSN})$。

此阶段完成后，源 SGSN/AMF 和目标 AMF/SGSN 完成身份互认证，并成功建立共享密钥 K_{SA}，实现了密钥的动态更新，为后续令牌授权过程提供安全保障。

2.4 令牌授权过程

UE 完成接入认证后，需提前向共生网络请求切换令牌。依据列车 UE 行车路线可预测性，设计了基于共享密钥的哈希链鉴权令牌授权策略，保证了会话密钥的前后向安全性，目标 AMF/SGSN 为 UE 生成授权令牌，使其能够快速与目标 AMF/SGSN 下辖的目标基站 gNode/BTS 建立会话密钥，进行后续安全通话。令牌授权流程如图 5 所示，具体步骤如下：

步骤 1 UE 安全接入 GSM-R/5G-R 共生网络后，源 SGSN/AMF 使用共享密钥 K_{SA} 加密消息 $M_5=E_{K_{SA}}(G^{GUTI})$，并将其发送至目标 AMF/SGSN。

步骤 2 目标 AMF/SGSN 收到加密消息 M_5 后，利用共享密钥 K_{SA} 解密消息得到 G^{GUTI}。随机选取 $r_{AMF/SGSN}$、$r_{gNodeB/BTS}$，计算会话密钥 $K^{sk}_{AMF/SGSN}=h(r_{AMF/SGSN}||G^{GUTI}||I^{ID}_{AMF/SGSN})$、$K^{sk}_{gNodeB/BTS}=h(r_{gNodeB/BTS}||G^{GUTI}||I^{ID}_{gNodeB/BTS})$，计算 $x=K_{AMF/SGSN}K_{gNodeB/BTS}$、$X_1=K_{AMF/SGSN}$ 和 $X_2=K_{gNodeB/BTS}$，计算令牌消息 $T^{TOKEN}_{AMF/SGSN}=X'_1X(K^{sk}_{AMF/SGSN}||V^{VP}_{AMF/SGSN})+X'_2X(K^{sk}_{gNodeB/BTS}||V^{VP}_{gNodeB/BTS})(\mathrm{mod}\ x)$。

步骤 3 目标 AMF/SGSN 将消息 $M_6=\{V^{VP}_{AMF/SGSN}||V^{VP}_{gNodeB/BTS}||r_{AMF/SGSN}||r_{gNodeB/AMF}\}$ 经源 SGSN/AMF 发送至 UE。将消息 $M_7=\{T^{TOKEN}_{AMF/SGSN}||G^{GUTI}\}$ 发送至共生网络下的目标 gNodeB/BTS。

此阶段完成后，通过消息令牌策略，既实现了有效的会话密钥预生成/预分发，又保证了密钥的前向/后向安全性。

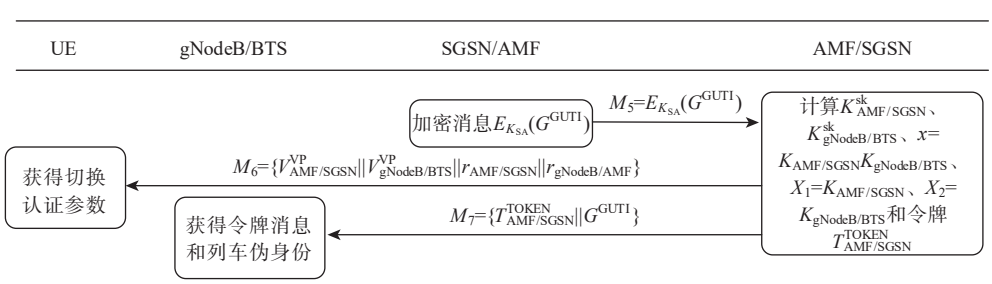

图5 令牌授权流程

Fig. 5 Token authorization process

2.5　垂直切换认证阶段

在垂直切换认证阶段, UE、目标 gNodeB/BTS 和目标 AMF/SGSN 通过基于中国剩余定理的密钥协商机制获得会话密钥, 来实现密钥的机密性。由于列车 UE 提前获取了目标 AMF/SGSN 生成的 $\{V_{\mathrm{AMF/SGSN}}^{\mathrm{VP}}\|V_{\mathrm{gNodeB/BTS}}^{\mathrm{VP}}\|r_{\mathrm{AMF/SGSN}}\|r_{\mathrm{gNodeB/AMF}}\}$, 可以实现共生网络环境下的快速垂直切换认证。垂直切换认证流程如图 6 所示, 具体步骤如下:

步骤 1　UE 计算密钥 $K_{\mathrm{AMF/SGSN}}^{\mathrm{sk}}=h(r_{\mathrm{AMF/SGSN}}\|G^{\mathrm{GUTI}}\|I_{\mathrm{AMF/SGSN}}^{\mathrm{ID}})$、$K_{\mathrm{gNodeB/BTS}}^{\mathrm{sk}}=h(r_{\mathrm{gNodeB/BTS}}\|G^{\mathrm{GUTI}}\|I_{\mathrm{gNodeB/BTS}}^{\mathrm{ID}})$、消息认证码 $M_{\mathrm{UE,gNodeB/BTS}}^{\mathrm{MAC}}=h(T_1\|V_{\mathrm{gNodB/BTS}}^{\mathrm{VP}}\|G^{\mathrm{GUTI}}\|K_{\mathrm{gNodeB/BTS}}^{\mathrm{sk}})$、$M_{\mathrm{UE,AMF/SGSN}}^{\mathrm{MAC}}=h(T_1\|V_{\mathrm{AMF/SGSN}}^{\mathrm{VP}}\|G^{\mathrm{GUTI}}\|K_{\mathrm{AMF/SGSN}}^{\mathrm{sk}})$, 发送消息 $M_8=\{T_1\|G^{\mathrm{GUTI}}\|M_{\mathrm{UE,gNodeB/BTS}}^{\mathrm{MAC}}\|M_{\mathrm{UE,AMF/SGSN}}^{\mathrm{MAC}}\}$至目标 gNodeB/BTS。

步骤 2　目标 gNodeB/BTS 收到消息 M_8 后, 依据 G^{GUTI} 对应令牌消息 $T_{\mathrm{AMF/SGSN}}^{\mathrm{TOKEN}}$, 计算 $M_{\mathrm{UE,gNodeB/BTS}}^{\mathrm{XMAC}}=h(T_1\|V_{\mathrm{gNodB/BTS}}^{\mathrm{VP}}\|G^{\mathrm{GUTI}}\|K_{\mathrm{gNodeB/BTS}}^{\mathrm{sk}})$, 验证 $M_{\mathrm{UE,gNodeB/BTS}}^{\mathrm{XMAC}}?=M_{\mathrm{UE,gNodeB/BTS}}^{\mathrm{MAC}}$, 以及时间戳消息 T_1 新鲜性, 若验证失败, 终止会话; 否则, 证明消息 M_8 来自合法 UE, 获取 $(K_{\mathrm{gNodeB/BTS}}^{\mathrm{sk}}\|V_{\mathrm{gNodeB/BTS}}^{\mathrm{VP}})=T_{\mathrm{gNodeB/BTS}}^{\mathrm{TOKEN}}(\mathrm{mod}\ K_{\mathrm{gNodeB/BTS}})$, 同时将消息 $M_9=\{T_1\|G^{\mathrm{GUTI}}\|M_{\mathrm{UE,AMF/SGSN}}^{\mathrm{MAC}}\}$发送至目标 AMF/SGSN。

步骤 3　目标 AMF/SGSN 收到消息 M_9 后, 依据 G^{GUTI} 确定与对应 UE 的令牌消息 $T_{\mathrm{AMF/SGSN}}^{\mathrm{TOKEN}}$, 计算消息 $(K_{\mathrm{AMF/SGSN}}^{\mathrm{sk}}\|V_{\mathrm{AMF/SGSN}}^{\mathrm{VP}})=T_{\mathrm{AMF/SGSN}}^{\mathrm{TOKEN}}(\mathrm{mod}\,K_{\mathrm{AMF/SGSN}})$。验证 $M_{\mathrm{UE,AMF/SGSN}}^{\mathrm{XMAC}}?=M_{\mathrm{UE,AMF/SGSN}}^{\mathrm{MAC}}$, 若验证成功, 表明目标 AMF/MSC 收到来自合法 UE, 此时计算 $M^{\mathrm{MAC}'}=h(T_2\|V_{\mathrm{AMF/SGSN}}^{\mathrm{VP}}\|V_{\mathrm{gNodB/BTS}}^{\mathrm{VP}}\|G^{\mathrm{GUTI}}\|K_{\mathrm{AMF/SGSN}}^{\mathrm{sk}}\|K_{\mathrm{gNodeB/BTS}}^{\mathrm{sk}})$, 发送消息 $M_{10}=\{T_2\|M^{\mathrm{MAC}'}\}$至 UE。

步骤 4　UE 收到消息 M_{10} 后, 验证时间戳消息 T_2 新鲜性及 $M^{\mathrm{XMAC}'}?=M^{\mathrm{MAC}'}$, 若不通过, 则结束会话; 否则, 使用密钥 $K_{\mathrm{gNodeB/BTS}}^{\mathrm{sk}}$、$K_{\mathrm{AMF/SGSN}}^{\mathrm{sk}}$进行后续 UE 和目标 gNodeB/BTS、UE 和目标 AMF/SGSN 间安全会话。

上述流程完成后, UE 通过源 SGSN/AMF 成功接入目标 AMF/SGSN, 实现了 UE 与目标 gNodeB/BTS、目标 AMF/SGSN 间身份互认证, 从而完成了高铁共生网络下的切换安全认证。

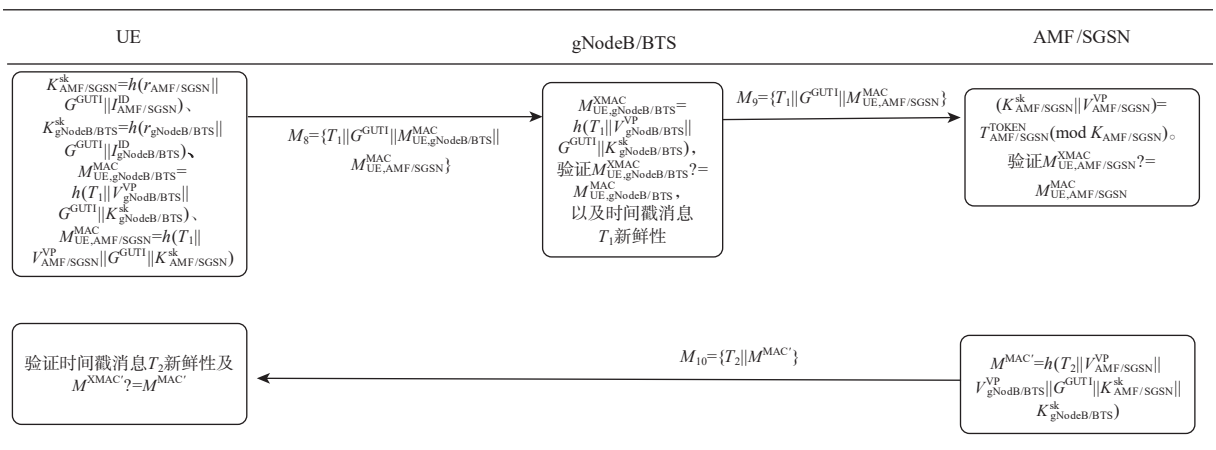

图 6　垂直切换认证流程

Fig. 6　Vertical handover authentication process

3　安全性分析

为验证本文方法的正确性, 分别采取 BAN 逻辑形式化理论证明和 TAMARIN 协议仿真工具验证的方法对所提协议进行安全性证明。

3.1　BAN 逻辑形式化理论证明

为验证本文方法的正确性, 采用 BAN 逻辑的方法对本文方法进行逻辑分析验证[19]。本文方法验证过程分为定义推理规则、拟实现安全目标、理想化协议模型和正确性验证等 4 个阶段。

1) 定义推理规则。为分析所提协议正确性, 给出以下逻辑推理规则:

① 消息含义规则。

$$\frac{P|\equiv Q\overset{K}{\leftrightarrow}P, P\lhd\{X_m\}_K}{P|\equiv Q|\sim X_m}$$

如果 P 信任通信实体 P 和 Q 之间的共享密钥 K, 且 P 接收到由 K 加密的消息 $\{X_m\}_K$, 则 P 信任 Q 曾发送过消息 X_m。

② 暂时验证规则。

$$\frac{P|\equiv\#(X_m), P|\equiv Q|\sim X_m}{P|\equiv Q|\equiv X_m}$$

如果 P 信任消息 X_m 是新鲜的, 并且 P 信任 Q 已经发送过消息 X_m, 则 P 信任 X_m。

③ 管辖规则。

$$\frac{P|\equiv Q|\Rightarrow X_m, P|\equiv Q|\equiv X_m}{P|\equiv X_m}$$

如果 P 信任 Q 对 X_m 有管辖权，并且 P 信任 Q 信任 X_m，则 P 信任消息 X_m。

④ 新鲜度规则。

$$\frac{P|\equiv \#(X_m)}{P|\equiv \#(X_m,Y_m)}$$

如果 P 信任 X_m 是新鲜的，则 P 信任 (X_m,Y_m) 是新鲜的。

⑤ 信任规则。

$$\frac{P|\equiv (X_m,Y_m)}{P|\equiv X_m},\quad \frac{P|\equiv X_m, P|\equiv Y_m}{P|\equiv (X_m,Y_m)}$$

如果 P 信任 X_m 和 Y_m 的消息 (X_m,Y_m) 集合，则 P 信任每个单独的消息。

⑥ 会话密钥规则。

$$\frac{P|\equiv \#(K), P|\equiv Q|\equiv X_m}{P|\equiv P\overset{K}{\longleftrightarrow} Q}$$

如果 P 信任共享密钥 K 是新鲜的，并且 P 也信任 Q 信任消息 X_m，则 P 信任 $P\overset{K}{\longleftrightarrow} Q$。

⑦ 接收规则。

$$\frac{P\lhd (X_m,Y_m)}{P\lhd X_m},\quad \frac{P|\equiv P\overset{K}{\longleftrightarrow} Q, P\lhd \{X_m\}_K}{P\lhd X_m}$$

如果 P 接收到一条消息，并且 P 知道关于该消息的相关密钥，则 P 接收该消息的组成部分。

2）拟实现安全目标。定义接入认证阶段和垂直切换认证阶段需要达到的安全目标如下：

G_1: $U_{\mathrm{UE}}|\equiv I^{\mathrm{ID}}_{\mathrm{BTS/gNodeB}}$

G_2: $U_{\mathrm{UE}}|\equiv I^{\mathrm{ID}}_{\mathrm{SGSN/AMF}}$

G_3: $B_{\mathrm{BTS/gNodeB}}|\equiv U_{\mathrm{UE}}$

G_4: $S_{\mathrm{SGSN/AMF}}|\equiv U_{\mathrm{UE}}$

G_5: $B_{\mathrm{BTS/gNodeB}}|\equiv B_{\mathrm{BTS/gNodeB}}\overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} U_{\mathrm{UE}}$

G_6: $g_{\mathrm{gNodeB/BTS}}|\equiv g_{\mathrm{gNodeB/BTS}}\overset{K^{\mathrm{sk}}_{\mathrm{gNodeB/BTS}}}{\longleftrightarrow} U_{\mathrm{UE}}$

G_7: $A_{\mathrm{AMF/SGSN}}|\equiv A_{\mathrm{AMF/SGSN}}\overset{K^{\mathrm{sk}}_{\mathrm{AMF/SGSN}}}{\longleftrightarrow} U_{\mathrm{UE}}$

其中，目标 G_1、G_2 分别表示 UE 信任基站 BTS/gNodeB 身份、UE 信任移动授权服务器 SGSN/AMF 身份；目标 G_3、G_4 分别表示 BTS/gNodeB 信任 UE 身份、SGSN/AMF 信任 UE 身份；目标 G_5 表示 BTS/gNodeB 信任 BTS/gNodeB 和 UE 之间的会话密钥 $K_{\mathrm{BTS/gNodeB}}$，意味着 UE 成功接入共生网络 GSM-R/5G-R；目标 G_6、G_7 分别表示目标 gNodeB/BTS 信任 gNodeB/BTS 和 UE 之间的会话密钥 $K^{\mathrm{sk}}_{\mathrm{gNodeB/BTS}}$，目标 AMF/SGSN 信任 AMF/SGSN 和 UE 之间的会话密钥 $K^{\mathrm{sk}}_{\mathrm{pAMF/gNodeB}}$，表明 UE 成功完成垂直切换认证。

3）理想化协议模型。对接入认证阶段和垂直切换认证阶段的通信流程及通信实体 UE、BTS/gNodeB 和 SGSN/AMF 进行描述。将实际的交互信息转化为 BAN 逻辑所能识别的公式，定义如下：

S_1: $U_{\mathrm{UE}}\rightarrow S_{\mathrm{SGSN/AMF}}$

$S_{\mathrm{SGSN/AMF}}\lhd \{I^{\mathrm{ID}}_{\mathrm{SGSN/AMF}}\,\|\,T_1\,\|\,A^{\mathrm{AUTH}}_1\,\|\,A^{\mathrm{AUTH}}_2\}$

S_2: $S_{\mathrm{SGSN/AMF}}\rightarrow B_{\mathrm{BTS/gNodeB}}$

$B_{\mathrm{BTS/gNodeB}}\lhd \{R_{\mathrm{RAND}}\|T_2\|V^{VP}\|G^{\mathrm{GUTI}}\}$

S_3: $B_{\mathrm{BTS/gNodeB}}\rightarrow U_{\mathrm{UE}}$

$U_{\mathrm{UE}}\lhd \{C_{\mathrm{UE}}\|R_{\mathrm{RAND}}\|T_3\|T_2\|M^{\mathrm{MAC}}_{\mathrm{BTS/gNodeB}}\}$

S_4: $U_{\mathrm{UE}}\rightarrow B_{\mathrm{BTS/gNodeB}}$

$B_{\mathrm{BTS/gNodeB}}\lhd \{M^{\mathrm{MAC}}_1\|T_4\}$

S_5: $S_{\mathrm{SGSN/AMF}}\rightarrow A_{\mathrm{AMF/SGSN}}$

$A_{\mathrm{AMF/SGSN}}\lhd \{E_{K_{\mathrm{SA}}}(G^{\mathrm{GUTI}})\}$

S_6: $A_{\mathrm{AMF/SGSN}}\rightarrow U_{\mathrm{UE}}$

$U_{\mathrm{UE}}\lhd \{V^{\mathrm{VP}}_{\mathrm{AMF/SGSN}}\|V^{\mathrm{VP}}_{\mathrm{gNodeB/BTS}}\|r_{\mathrm{AMF/SGSN}}\|r_{\mathrm{gNodeB/AMF}}\}$

S_7: $A_{\mathrm{AMF/SGSN}}\rightarrow g_{\mathrm{gNodeB/BTS}}$

$g_{\mathrm{gNodeB/BTS}}\lhd \{T^{\mathrm{TOKEN}}_{\mathrm{AMF/SGSN}}\|G^{\mathrm{GUTI}}\}$

S_8: $U_{\mathrm{UE}}\rightarrow g_{\mathrm{gNodeB/BTS}}$

$g_{\mathrm{gNodeB/BTS}}\lhd \{T_1\|G^{\mathrm{GUTI}}\|M^{\mathrm{MAC}}_{\mathrm{UE,gNodeB/BTS}}\|M^{\mathrm{MAC}}_{\mathrm{UE,AMF/SGSN}}\}$

S_9: $g_{\mathrm{gNodeB/BTS}}\rightarrow A_{\mathrm{AMF/SGSN}}$

$A_{\mathrm{AMF/SGSN}}\lhd \{T_1\|G^{\mathrm{GUTI}}\|M^{\mathrm{MAC}}_{\mathrm{UE,AMF/SGSN}}\}$

S_{10}: $A_{\mathrm{AMF/SGSN}}\rightarrow U_{\mathrm{UE}}$

$U_{\mathrm{UE}}\lhd \{T_2\|M^{\mathrm{MAC}'}\}$

对通信实体 UE、BTS/gNodeB 和 SGSN/AMF 的状态描述如下：

A_1: $U_{\mathrm{UE}}\lhd S^{\mathrm{SUPI}}$

A_2: $U_{\mathrm{UE}}|\equiv G^{\mathrm{GUTI}}$

A_3: $S_{\mathrm{SGSN/AMF}}|\equiv \#(T_1)$

A_4: $S_{\mathrm{SGSN/AMF}}|\equiv \#(I^{\mathrm{ID}}_{\mathrm{SGSN/AMF}})$

A_5: $B_{\mathrm{BTS/gNodeB}}|\equiv U_{\mathrm{UE}}|\Rightarrow B_{\mathrm{BTS/gNodeB}}\overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} U_{\mathrm{UE}}$

A_6: $U_{\mathrm{UE}}|\equiv U_{\mathrm{UE}}|\Rightarrow U_{\mathrm{UE}}\overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} B_{\mathrm{BTS/gNodeB}}$

A_7: $U_{\mathrm{UE}}|\equiv \#(T_2\|T_3)$

A_8: $S_{\mathrm{SGSN/AMF}}|\equiv S_{\mathrm{SGSN/AMF}}\overset{K_{\mathrm{SA}}}{\longleftrightarrow} A_{\mathrm{AMF/SGSN}}$

A_9: $B_{\mathrm{BTS/gNodeB}}|\equiv \#(T_4)$

A_{10}: $B_{\mathrm{BTS/gNodeB}}|\equiv U_{\mathrm{UE}}|\Rightarrow B_{\mathrm{BTS/gNodeB}}\overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} U_{\mathrm{UE}}$

A_{11}: $B_{\mathrm{BTS/gNodeB}}|\equiv (S_{\mathrm{SGSN/AMF}}|\Rightarrow B_{\mathrm{BTS/gNodeB}}\overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} U_{\mathrm{UE}})$

A_{12}: $U_{\mathrm{UE}}|\equiv \#(V^{\mathrm{VP}}_{\mathrm{AMF/SGSN}}\|V^{\mathrm{VP}}_{\mathrm{gNodeB/BTS}})$

A_{13}: $A_{\mathrm{AMF/SGSN}}|\equiv U_{\mathrm{UE}}|\Rightarrow U_{\mathrm{UE}}\overset{K^{\mathrm{sk}}_{\mathrm{AMF/SGSN}}}{\longleftrightarrow} A_{\mathrm{AMF/SGSN}}$

A_{14}: $g_{\mathrm{gNodeB/BTS}}|\equiv U_{\mathrm{UE}}|\Rightarrow U_{\mathrm{UE}}\overset{K^{\mathrm{sk}}_{\mathrm{BTS/gNode}}}{\longleftrightarrow} g_{\mathrm{gNodeB/BTS}}$

4）正确性验证。完成协议模型建立后，根据 BAN 逻辑推理规则证明待验证安全目标 $G_1\sim G_7$，证明如下。

由 S_1 和 A_1 及消息含义规则可得

$$\frac{U_{\mathrm{UE}}|\equiv B_{\mathrm{BTS/gNodeB}}\overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} U_{\mathrm{UE}}, U_{\mathrm{UE}}\lhd \{I^{\mathrm{ID}}_{\mathrm{BTS/gNodeB}}\}_{K_{\mathrm{BTS/gNodeB}}}}{U_{\mathrm{UE}}|\equiv B_{\mathrm{BTS/gNodeB}}|\sim I^{\mathrm{ID}}_{\mathrm{BTS/gNodeB}}}\quad (3)$$

由 S_2、S_3 和 A_2 及暂时验证规则和新鲜度规则

可得

$$S_{\mathrm{SGSN/AMF}}| \equiv U_{\mathrm{UE}}| \sim \{R_{\mathrm{RAND}} \| T_2 \| C_{\mathrm{UE}} \| G^{\mathrm{GUTI}}\} \quad (4)$$

由式 (3)、式 (4)、A_4 及接受规则可得

$$\frac{B_{\mathrm{BTS/gNodeB}}| \equiv \#(M^{\mathrm{MAC}}\|T_4), B_{\mathrm{BTS/gNodeB}}| \equiv U_{\mathrm{UE}}| \sim (M^{\mathrm{MAC}}\|T_4)}{B_{\mathrm{BTS/gNodeB}}| \equiv U_{\mathrm{UE}}| \equiv (M^{\mathrm{MAC}}\|T_4)} \quad (6)$$

由式 (5)、式 (6)、S_5 及暂时验证规则可得

$$\begin{cases} B_{\mathrm{BTS/gNodeB}}| \equiv U_{\mathrm{UE}} \\ S_{\mathrm{SGSN/AMF}}| \equiv U_{\mathrm{UE}} \end{cases} \quad (7)$$

$$B_{\mathrm{BTS/gNodeB}}| \equiv S_{\mathrm{SGSN/AMF}}| \sim \{K_{\mathrm{BTS/gNodeB}}\|G^{\mathrm{GUTI}}\} \quad (8)$$

由式 (8)、S_5、A_6 及会话密钥规则可得

$$\frac{U_{\mathrm{UE}}| \equiv \#(K_{\mathrm{BTS/gNodeB}}), U_{\mathrm{UE}}| \equiv B_{\mathrm{BTS/gNodeB}}| \equiv G^{\mathrm{GUTI}}}{U_{\mathrm{UE}}| \equiv U_{\mathrm{UE}} \overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} B_{\mathrm{BTS/gNodeB}}} \quad (9)$$

$$S_{\mathrm{SGSN/AMF}}| \equiv B_{\mathrm{BTS/gNodeB}} \overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} U_{\mathrm{UE}} \quad (10)$$

由式 (9)、式 (10) 及接收规则可得

$$B_{\mathrm{BTS/gNodeB}}| \equiv B_{\mathrm{BTS/gNodeB}} \overset{K_{\mathrm{BTS/gNodeB}}}{\longleftrightarrow} U_{\mathrm{UE}} \quad (11)$$

由 S_6、S_7、A_7、A_8 及管辖规则可得

$$\frac{A_{\mathrm{AMF/SGSN}}| \equiv U_{\mathrm{UE}}| \Rightarrow (M^{\mathrm{MAC}'}), A_{\mathrm{AMF/SGSN}}| \equiv U_{\mathrm{UE}}| \equiv (M^{\mathrm{MAC}'})}{A_{\mathrm{AMF/SGSN}}| \equiv (M^{\mathrm{MAC}'})} \quad (16)$$

$$U_{\mathrm{UE}}| \equiv U_{\mathrm{UE}}| \equiv A_{\mathrm{AMF/SGSN}}| \sim \{K^{\mathrm{sk}}_{\mathrm{AMF/SGSN}}\} \quad (17)$$

由式 (16)、式 (17) 及会话密钥规则可得

$$A_{\mathrm{AMF/SGSN}}| \equiv A_{\mathrm{AMF/SGSN}} \overset{K^{\mathrm{sk}}_{\mathrm{AMF/SGSN}}}{\longleftrightarrow} U_{\mathrm{UE}} \quad (18)$$

综合式 (5)、式 (7)、式 (11)、式 (15) 和式 (18) 可知，待验证安全目标 G_1～G_7 验证通过。其中，式 (5) 和式 (7) 表明 UE、BTS/gNodeB 和 SGSN/AMF 完成身份互认证。式 (11) 表明 UE 与 BTS/gNodeB 安全地协商密钥 $K_{\mathrm{BTS/gNodeB}}$ 用于后续通信，UE 成功接入 GSM-R/5G-R 共生网络。式 (15) 和式 (18) 分别表明目标 gNodeB/BTS 和 UE 之间成功建立会话密钥 $K^{\mathrm{sk}}_{\mathrm{gNodeB/BTS}}$、目标 AMF/SGSN 和 UE 之间的成功建立会话密钥 $K^{\mathrm{sk}}_{\mathrm{AMF/gNodeB}}$，UE 成功完成切换认证。

通过上述 BAN 逻辑理论安全目标的证明，验证了本文方法的安全性。

3.2　基于 TAMARIN 协议仿真工具验证

为进一步验证本文方案的正确性，采用 TAMARIN 协议仿真工具来验证方法的安全性。TAMARIN 是自动验证工具，支持异或操作和多种加密原语，可以对协议进行安全性分析[20]。TAMARIN 验证过程是对密码协议中需要验证的安全属性用 lemma 引理的方式进行定义，当协议具备所定义的

$$\begin{cases} U_{\mathrm{UE}}| \equiv I^{\mathrm{ID}}_{\mathrm{BTS/gNodeB}} \\ U_{\mathrm{UE}}| \equiv I^{\mathrm{ID}}_{\mathrm{SGSN/AMF}} \end{cases} \quad (5)$$

由 S_4、A_5 及信任规则可得

$$\frac{g_{\mathrm{gNodeB/BTS}}| \equiv U_{\mathrm{UE}}| \Rightarrow (V^{\mathrm{VP}}), g_{\mathrm{gNodeB/BTS}}| \equiv U_{\mathrm{UE}}| \equiv (V^{\mathrm{VP}})}{g_{\mathrm{gNodeB/BTS}}| \equiv (V^{\mathrm{VP}})} \quad (12)$$

由式 (12)、S_8、A_9、A_{10} 及消息含义规则可得

$$\frac{U_{\mathrm{UE}}| \equiv g_{\mathrm{gNodeB/BTS}} \overset{K^{\mathrm{sk}}_{\mathrm{gNodeB/BTS}}}{\longleftrightarrow} U_{\mathrm{UE}}, U_{\mathrm{UE}} \lhd \{V^{\mathrm{VP}}\}_{K^{\mathrm{sk}}_{\mathrm{gNodeB/BTS}}}}{U_{\mathrm{UE}}| \equiv g_{\mathrm{gNodeB/BTS}}| \sim V^{\mathrm{VP}}} \quad (13)$$

$$U_{\mathrm{UE}}| \equiv U_{\mathrm{UE}}| \equiv g_{\mathrm{gNodeB/BTS}}| \sim \{K^{\mathrm{sk}}_{\mathrm{gNodeB/BTS}}\} \quad (14)$$

由式 (13)、式 (12)、A_{11}、A_{12} 及会话密钥规则可得

$$g_{\mathrm{gNodeB/BTS}}| \equiv g_{\mathrm{gNodeB/BTS}} \overset{K^{\mathrm{sk}}_{\mathrm{gNodeB/BTS}}}{\longleftrightarrow} U_{\mathrm{UE}} \quad (15)$$

由 S_9、M_{10}、A_{13}、A_{14} 及管辖规则可得

安全属性时，输出结果为 verified，不具备安全性时为 unverified。使用 TAMARIN 工具对本文方案进行规范化并定义所要验证的安全属性，经 Spthy 语言建模后，基于 Dolev-Yao 攻击模型[21]，对上述引理施加可能的攻击，采用 TAMARIN 工具执行后，验证结果如图 7 所示。可以看出，所有待验证属性均为 verified，表明本文方案安全性验证通过。结果①表明 UE 身份信息 SUPI 保密性得到验证，可以防止身份伪造和重放攻击。结果②表明源基站 BTS/gNodeB 和目标基站 gNodeB/BTS 身份信息具备保密性。结果③表明 UE 与目标 AMF/SGAN 间会话密钥 $K^{\mathrm{sk}}_{\mathrm{AMF/SGSN}}$ 具有保密性，且具有实时更新的特性，实现了会话密钥的前后安全性。结果④表明

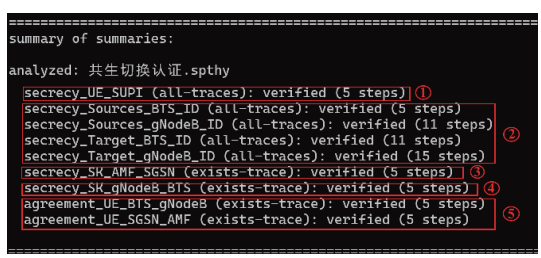

图 7　协议安全性验证结果

Fig. 7　Protocal security verification results

UE和目标gNodeB/BTS间会话密钥$K^{sk}_{gNodeB/BTS}$具备保密性，保证了认证消息仅可由合法UE和目标gNodeB/BTS生成，可抵抗重放攻击。结果⑤表明UE和BTS/gNodeB、UE和SGSN/AMF间实现了身份互认证，可抵抗中间人攻击。

综上，从BAN逻辑形式化理论证明和TAMARIN协议仿真工具验证可知，本文方案实现了SUPI身份信息匿名性，可防止身份伪造、抵抗重放攻击；此外，在共生网络垂直切换过程中，实现了密钥前后向安全性，并可抵抗中间人攻击等。

4 性能分析

4.1 安全性分析对比

进行安全性能比较，主要从SUPI身份保密性、UE、BTS/gNodeB和SGSN/AMF身份互认证、会话密钥保密性、前后向安全性、可追踪性、抗重放攻击、抗量子计算攻击、抗DoS攻击及抗中间人攻击等安全性进行分析对比，比较结果如表1所示。

从表1可以看出，文献[8]使用了票据授权机制，UE和目标基站/服务器之间可以基于先前访问的源基站/服务器生成的凭证票据完成协议实体间身份认证和密钥协商，保护了UE身份隐私，该方法通过随机数和SEQ计数机制，可以抵抗重放攻击和中间人攻击，但不具备会话密钥的后向安全性，攻击者可通过截获先前认证票据推演后续通话密钥，继而发起攻击，导致会话密钥泄露。文献[9]通过计数器和随机数规则，实现了UE和认证服务器间身份互认证，可抵抗中间人攻击，但ID检索号以明文方式传输，易被攻击者截获，导致UE身份信息泄露，继而发起DoS攻击；同时，该方法基于椭圆曲线加密机制，无法抵抗量子计算攻击。文献[14]依据掩码数组的密钥推导方式，保证了密钥的前后向安全性，但不满足可追溯性，无法实时追踪恶意用户攻击行为；同时，该方法采用了AES对称加密协议，无法抵抗量子计算攻击。文献[16]基于椭圆曲线加密技术实现了UE跨多个集线器的切换认证，通过密钥衍生技术生成会话密钥，中间密钥由Diffie-Hellman密钥交换算法生成，确保了密钥的前后向安全性，但无法抵抗重放攻击和量子计算攻击。文献[17]利用格密码理论，设计了一种有条件UE隐私保护的切换认证方案，UE通过伪随机标识符SID保护了UE身份隐私，该方法通过格密码密钥协商机制，可抵抗量子计算攻击，但会话密钥的生成依赖于SID的随机性，缺乏对SID识别策略，攻击者可伪造大量SID发起对认证服务的DoS攻击。本文方案中，UE通过认证消息$A_1^{AUTN}=r_{UE}K^{PK}_{SGSN/AMF}+S^{SUPI}$及临时身份$G^{GUTI}$传输UE身份信息$S^{SUPI}$，保护了UE身份隐私，而且通信实体间通过互相验证带有伪身份G^{GUTI}和时间戳消息的M^{MAC}认证码实现了身份互认证，可抵抗中间人攻击及重放攻击，并设计了切换认证令牌授权策略，保证了会话密钥的前后向安全性；此外，本文方法采用了基于多项式环上的最近、最短向量问题的NTRU加密算法加密协议中变量和认证消息，可抵抗量子计算攻击[18]。综合安全性对比分析后，相较于同类方法，本文方法具有更高的安全性。

表1 安全性能对比

Table 1 Safety performance comparison

方案对比	SUPI身份保密性	身份互认证	密钥前/后向安全性	可追踪性	抗重放攻击	抗DoS攻击	抗量子计算攻击	抗中间人攻击
文献[8]	√	√	×	√	√	√	×	√
文献[9]	×	√	√	√	√	×	×	√
文献[14]	√	√	√	×	×	×	×	√
文献[16]	√	√	√	√	×	√	×	√
文献[17]	√	×	√	√	√	×	√	×
本文方法	√	√	√	√	√	√	√	√

注：“√”表示满足相应安全属性，“×”表示不满足相应安全属性。

4.2 计算开销与通信开销对比

在完成安全性能比较后，进一步进行通信与计算开销比较。其中，通信开销指计算各个通信实体之间比特信息交互总量，在计算开销方面，主要列举了单向哈希运算耗时T_{HASH}、对称加解密耗时T_S、模指数运算耗时T_M、椭圆曲线点积运算耗时T_{ECC}、椭圆曲线点加运算耗时T_A、NTRU加密耗时T_{NE}、NTRU解密耗时T_{ND}、NTRU模乘运算耗时T_{NM}。比较结果如表2所示。可知，文献[9,14]虽不涉及接入认证阶段，但2种方法分别通过公钥随机数和身份检索规则、掩码阵列机制生成切换认证信息，过程涉及复杂的椭圆曲线点积、点加运算，造成方法切换认证耗时较高。文献[8]采取公钥票据授权机制，通过椭圆曲线加密机制批量生成会话密钥和加密票据，且需额外认证票据ID，带来了较高的切换认证耗时。文献[16]采用密钥衍生技术来提前传

表 2　通信开销及计算开销对比

Table 2　Comparison of communication overhead and computing overhead

方案	UE通信量/bit	核心网通信量/bit	总通信量/bit	预认证耗时/ms	切换认证耗时/ms	总耗时/ms
文献[8]	863	2 302	2 965	$15T_{HASH}+7T_S+T_M\approx15.4$	$15T_{HASH}+7T_S+T_M\approx12.7$	28.1
文献[9]	960	2 588	3 548		$5T_{HASH}+7T_A+T_M+8T_{ECC}\approx26.8$	26.8
文献[14]	1 102	2 652	3 754		$8T_{HASH}+5T_A+3T_M+9T_{ECC}\approx31.7$	31.7
文献[16]	1 263	2 897	4 160		$4T_{HASH}+3T_A+T_M+7T_{ECC}\approx24.5$	24.5
文献[17]	974	2 929	3 903	$5T_{HASH}+T_{NE}+T_{ND}+T_{NM}\approx11.6$	$9T_{HASH}+2T_{NE}+2T_{ND}+T_{NM}\approx9.8$	21.4
本文方案	765	2 667	3 432	$4T_{HASH}+3T_{NE}+2T_{ND}+2T_{NM}\approx12.8$	$7T_{HASH}+2T_{NM}\approx7.4$	20.2

递中间密钥, 相较于文献 [9], 降低了一定的切换认证耗时, 但中间密钥和参数信息由椭圆曲线密钥交换算法生成, 仍存在较大的通信开销。文献 [17] 基于格的认证方法, 在 6 类方法中总耗时较小, 这是因为该方法在接入认证阶段采取了 NTRU 算法保护 UE 身份隐私, 但在切换认证过程中需重复执行加密算法传递伪身份 SID, 因此, 切换认证耗时高于本文方法。本文方法在 6 种方法中总耗时最小, 这是由于在接入认证阶段引入了高效的 NTRU 算法生成 UE 临时身份, 仅需列车首次接入共生网络时执行一次, 同时, 在垂直切换认证过程中, 通过哈希操作和中国剩余定理生成切换认证令牌, 实现了会话密钥的预生成, 减少了通信总耗时。

列车在高铁共生网络沿线运行中, 将会频繁发生垂直切换, 为了更清晰地得到 6 种方案的认证执行效率关系, 给出了各方案切换认证次数与通信开销和计算开销关系, 如图 8 和图 9 所示。可以看出, 整体上, 不同方法的通信开销和计算开销均随着切换认证次数的增加而呈现增加的趋势。图 8 中, 文献 [14] 采用自循环加密结构及 AES 加密算法, 给计算资源受限的列车 UE 带来了较高的通信开销。文献 [8] 采用票据授权技术批量生成会话密钥, 在切换认证次数较少时, 通信开销优于本文方法, 但随着切换认证次数增加, 本地密钥消耗殆尽, 需重新执行切换认证协议, 带来了更高的通信开销, 且不具备密钥后向安全性, 无法抵抗量子计算攻击。图 8 和图 9 中, 本文方案切换认证耗时较其他同类方案最低, 这是由于在接入认证中引入了高效的 NTRU 算法, 通过中国剩余定理和哈希加密实现了认证参数及密钥预生成, 当切换发生时, UE 和 SGSN/AMF 通过预分发的参数计算认证码 MAC 以会话密钥 $K^{sk}_{gNodeB/BTS}$, 因此, 直接发送由 $k^{sk}_{gNodeB/BTS}$ 计算的 MAC 即可快速保证完成切换认证。

综上, 本文方案具有较高的安全性, 同时也具备较高的认证效率, 能够满足 GSM-R/5G-R 共生网络切换认证高安全和实时性的要求。然而, 高铁共生网络场景复杂, 还涉及诸多设备与设备之间的端

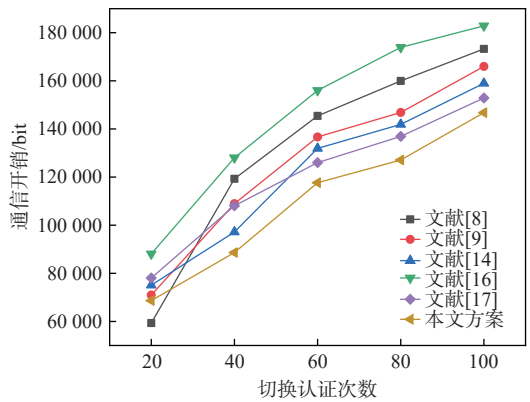

图 8　切换认证次数与通信开销对比

Fig. 8　Comparison of handover authentication frequency and communication overhead

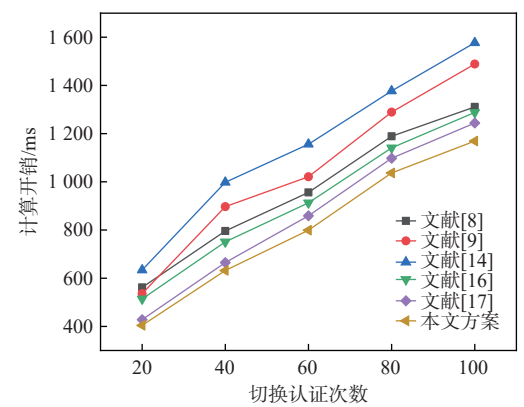

图 9　切换认证次数与计算开销对比

Fig. 9　Comparison of handover authentication frequency and computational overhead

到端认证通信安全, 本文所提基于 NTRU 格上的切换认证方案仅考虑了列车与基站之间的认证问题, 未涉及大量的接入终端设备, 后续将进一步结合基于区块链共识技术来增强共生网络的设备间安全性。

5　结　论

1) 设计 NTRU 格上双向认证机制和哈希操作生成临时身份信息, 完成共生网络初始接入认证, 实现了列车身份匿名性, 可有效抵抗重放攻击。

2) 基于共享密钥的哈希链加密方法, 设计了共

享密钥生成和共生网络切换令牌策略，实现了垂直切换认证的密钥预生成，确保了密钥前后向安全性，减少了切换认证开销。

3）采用中国剩余定理密钥协商方法及时间戳机制，确保了会话密钥的机密性，可抵抗 DoS 攻击，能够满足高铁共生网络高效、安全无缝切换认证的需求。

参考文献（References）

[1] 陈永, 刘雯, 詹芝贤. 基于混合密钥增强的 LTE-R 车地认证密钥协商方案[J]. 铁道学报, 2023, 45(6): 69-79.
CHEN Y, LIU W, ZHAN Z X. A train-to-ground authentication key agreement enhanced scheme based on hybrid secrurity key for LTE-R[J]. Journal of the China Railway Society, 2023, 45(6): 69-79(in Chinese).

[2] HE R S, AI B, ZHONG Z D, et al. 5G for railways: next generation railway dedicated communications[J]. IEEE Communications Magazine, 2022, 60(12): 130-136.

[3] 张馨丹, 李辉, 郭强亮. 5G-R 和 GSM-R 网络列车调度通信业务平滑过渡方案研究[J]. 铁道标准设计, 2022, 66(10): 166-172.
ZHANG X D, LI H, GUO Q L. Research on smooth transition scheme of 5G-R and GSM-R network train dispatching communication services[J]. Railway Standard Design, 2022, 66(10): 166-172 (in Chinese).

[4] 陈永, 康婕, 陶瑄. 改进 5G-R 自适应高速铁路越区切换算法[J]. 北京航空航天大学学报, 2025, 51(3): 724-731.
CHEN Y, KANG J, TAO X. An improved 5G-R adaptive high-speed railway handover algorithm[J]. Journal of Beijing University of Aeronautics and Astronautics, 2025, 51(3): 724-731(in Chinese).

[5] TANG Q, ERMIS O, NGUYEN C D, et al. A systematic analysis of 5G networks with a focus on 5G core security[J]. IEEE Access, 2022, 10: 18298-18319.

[6] SUN B, GUO Y, YU Y J, et al. Reliability analysis of CTCS-3 train-ground communication system based on 5G-R[J]. IEEE Transactions on Vehicular Technology, 2023, 72(10): 12927-12940.

[7] 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.

[8] CAO J, MA M D, FU Y L, et al. CPPHA: capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1182-1195.

[9] 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: 105.

[10] MA T, HU F. A cross-layer collaborative handover authentication approach for 5G heterogeneous network[J]. Journal of Physics: Conference Series, 2019, 1169: 012066.

[11] YANG J, JI X S, HUANG K Z, et al. Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet[J]. IET Communications, 2019, 13(2): 144-152.

[12] CUI Q M, ZHU Z B, NI W, et al. Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5G systems[J]. IEEE Wireless Communications, 2021, 28(2): 78-85.

[13] KALIA P, KUMAR A. 5G enabled universal seamless HO authentication in heterogeneous networks[C]//Proceedings of the 2nd International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering. Piscataway: IEEE Press, 2022: 1-5.

[14] LIU Y B, HUO L J, WU J, et al. MRSA: mask random array protocol for efficient secure handover authentication in 5G HetNets[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(5): 3809-3827.

[15] DIVAKARAN J, CHAKRAPANI A, SRIHARI K. Fuzzy logic based handover authentication in 5G telecommunication heterogeneous networks[J]. Computer Systems Science and Engineering, 2023, 46(1): 1141-1152.

[16] SHARMA V, YOU I, LEU F Y, et al. Secure and efficient protocol for fast handover in 5G mobile Xhaul networks[J]. Journal of Network and Computer Applications, 2018, 102: 38-57.

[17] ZHOU Y S, WANG L A. A lattice-based authentication scheme for roaming service in ubiquitous networks with anonymity[J]. Security and Communication Networks, 2020, 2020: 2637916.

[18] 李瑞琪, 贾春福, 王雅飞. 基于 NTRU 的多密钥同态代理重加密方案及其应用[J]. 通信学报, 2021, 42(3): 11-22.
LI R Q, JIA C F, WANG Y F. Multi-key homomorphic proxy re-encryption scheme based on NTRU and its application[J]. Journal on Communications, 2021, 42(3): 11-22(in Chinese).

[19] ABDEL-MALEK M A, AKKAYA K, BHUYAN A, et al. A proxy signature-based swarm drone authentication with leader selection in 5G networks[J]. IEEE Access, 2022, 10: 57485-57498.

[20] CORTIER V, DELAUNE S, DREIER J, et al. Automatic generation of sources lemmas in tamarin: towards automatic proofs of security protocols[J]. Journal of Computer Security, 2022, 30(4): 573-598.

[21] RAM S B, ODELU V. Security analysis of a key exchange protocol under Dolev-Yao threat model using tamarin prover[C]//Proceedings of the IEEE 12th Annual Computing and Communication Workshop and Conference. Piscataway: IEEE Press, 2022: 667-672.

Security handover authentication scheme for high-speed railway symbiotic network based on NTRU lattice

CHEN Yong*，ZHANG Bingwang，XIN Zhaofeng

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

Abstract：A high-speed railway symbiotic network security handover authentication scheme based on NTRU lattice is proposed to address the issues of identity leakage, lack of forward and backward security, and high authentication overhead during the evolution of the high-speed railway GSM-R wireless communication system to the next generation 5G-R network during vertical handover. Firstly, a bidirectional authentication mechanism based on NTRU lattice was designed to overcome the vulnerability of identity information SUPI plaintext transmission to leakage. Second, a shared key-based hash chain encryption technique is suggested. To accomplish pre-creation of handover authentication keys, shared key generation and symbiotic network switching token strategies are created, guaranteeing dynamic updates of shared keys and forward and backward security. Then, using the Chinese remainder theorem and timestamp mechanism, the confidentiality of the session key was achieved, and the handover authentication of the symbiotic network was completed. Finally, the security of the proposed method was analyzed using BAN logic theory and TAMARIN protocol simulation verification tools. The findings demonstrate that, in comparison to comparable techniques, the suggested approach guarantees identity anonymity and forward and backward key security, can successfully fend off DoS and man-in-the-middle attacks, has lower switching costs, and can satisfy the demands of seamless handover authentication for high-speed rail symbiotic network security.

Keywords：railway wireless communication；symbiotic network；handover authentication；NTRU lattice encryption；communication efficiency

Received：2024-01-08；**Accepted**：2024-02-23；**Published Online**：2024-03-12 10：00

URL：link.cnki.net/urlid/11.2625.V.20240311.1521.004

Foundation items：National Natural Science Foundation of China (62462043,61963023); Gansu Provincial Nature Science Foundation (26JRRA589)

* **Corresponding author**. E-mail：edukeylab@126.com