ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.7, July 2010, pp.1768−1782
doi: 10.3724/SP.J.1001.2010.03527

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

3GPP 认证与密钥协商协议安全性分析*

陆 峰[1,2,3+], 郑康锋[1,2,3], 钮心忻[1,2,3], 杨义先[1,2,3], 李忠献[1,2,3,4]

[1](北京邮电大学 网络与交换技术国家重点实验室信息安全中心,北京 100876)

[2](北京邮电大学 网络与信息攻防技术教育部重点实验室,北京 100876)

[3](灾备技术国家工程实验室,北京 100876)

[4](天津市国瑞数码安全系统有限公司北京研发中心,北京 100088)

Security Analysis of 3GPP Authentication and Key Agreement Protocol

LU Feng[1,2,3+], ZHENG Kang-Feng[1,2,3], NIU Xin-Xin[1,2,3], YANG Yi-Xian[1,2,3], LI Zhong-Xian[1,2,3,4]

[1](Information Security Center, State Key Laboratory of Network and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

[2](Key Laboratory of Network and Information Attack and Defence Technology of Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China)

[3](National Engineering Laboratory for Disaster Backup and Recovery, Beijing 100876, China)

[4](National Cybernet Security Ltd, Beijing 100088, China)

+ Corresponding author: E-mail: mellowmelon@163.com

Lu F, Zheng KF, Niu XX, Yang YX, Li ZX. Security analysis of 3GPP authentication and key agreement protocol. *Journal of Software*, 2010,21(7):1768−1782. http://www.jos.org.cn/1000-9825/3527.htm

Abstract: The Universal Mobile Telecommunication System (UMTS) adopts 3GPP authentication and key agreement (3GPP AKA) protocol as its security framework, and this protocol has made effective improvements on the hidden security problems of GSM (global system for mobile communications). This paper investigates into the security of the 3GPP authentication and key agreement protocol, and analyzes four types of attacks to which it is vulnerable. To solve the security problems mentioned above, it presents an efficient authentication and key agreement protocol, which is based on public key cryptography, under the circumstances of location updating and location immovability, adopts formal analysis to prove the security of two protocols proposed, and compares it with other protocols from the aspect of security. The results show that this proposed protocol can significantly enhance the security of 3GPP AKA protocol.

Key words: authentication; key agreement; third-generation; wireless security; network security

摘 要: 通用移动通信系统采用3GPP认证与密钥协商协议作为其安全框架,该协议对GSM存在的安全隐患作了有效的改进.对3GPP认证与密钥协商协议进行安全性研究,分析其容易遭受4种类型攻击方式.为了解决上述存在的安全隐患,提出在位置更新与位置不变两种情况下的基于公钥密码学的认证与密钥协商协议,采用形式化的分析

* Supported by the National Natural Science Foundation of China under Grant Nos.90718001, 60821001 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2007AA01Z430 (国家高技术研究发展计划(863))

Received 2008-06-04; Revised 2008-08-07, 2008-10-24; Accepted 2008-11-28

方式证明了所提出算法的安全性,并将该协议与已有协议在安全性方面进行了比较.结果显示,所提出的协议算法能够极大地增强 3GPP 认证与密钥协商协议的安全性.

关键词: 认证;密钥协商;3G;无线安全;网络安全

中图法分类号: TP309 **文献标识码:** A

移动通信系统无线空中接口由于其独特的特性向来是最容易遭受攻击的部位.第一代移动通信系统 AMPS(advanced mobile phone system)和第二代移动通信系统 GSM(global system for mobile communications)都没有全面地考虑安全特性,以至于引发了很多安全问题,比如攻击者可以随意地窃听用户的数据流,甚至可以伪装成合法用户接入网络获得正常的服务[1].第三代移动通信系统 UMTS(universal mobile telecommunications system)安全框架采用了 3GPP 组织建议的 AKA(authentication and key agreement)协议机制[2],但是仍然存在某些安全问题,如序列号 SQN(sequence number)同步、IMSI(Int'l mobile subscriber identity)标识安全保护、VLR/SGSN(visitor location register/serving GPRS support node)与 HE/HLR(home environment/home location register)之间的带宽消耗、VLR/SGSN 认证向量存储负担等问题.本文将深入而全面地研究 3GPP AKA 协议的安全性,并在此基础上借鉴 AKA 协议安全框架,提出一种更为安全的认证与密钥协商协议.

1 3GPP AKA 协议介绍

3GPP AKA 协议中 MS 代表移动站,VLR/SGSN 代表访问者位置寄存器/服务 GPRS 支撑节点,HE/HLR 代表归属环境/归属位置寄存器.为达到相互认证的目的,MS(mobile station)和 HE/HLR 共享密钥 k,MS 的密钥 k 保存在 USIM 中, HE/HLR 的密钥 k 保存在认证中心 AUC 中.另外,HE/HLR 为每个 MS 维护一个计数器 SQN_{HE},MS 自己也维护一个计数器 SQN_{MS} 来记录接收到的最高序列值[2].此外,MS 和 HE/HLR 之间共享 3 个消息摘要函数 $f1$,$f1^*$和 $f2$,以及 4 个密钥生成函数 $f3$,$f4$,$f5$ 和 $f5^*$[3].

为了解决 GSM 系统鉴权与加密存在的单边认证和 MS 与 VLR/SGSN 之间传输信令没有完整性保护等问题[1],3GPP 组织在为 UMTS 系统设计 AKA 协议时就考虑要达到以下 3 个目标:(1) 移动站和网络之间要求达到双向认证;(2) 加密密钥和完整性密钥建立在成功认证的基础之上;(3) 保证建立的加密密钥和完整性密钥的新鲜性.为了使 UMTS 系统与 GSM 系统安全框架达到最大的兼容,便于 MS 能够在两者之间漫游,AKA 协议结合 GSM 系统用户认证密钥协商协议的挑战与响应机制和基于数字一次消息协议(ISO/IEC9798-4)[4]来完成用户认证与密钥协商[2].

根据 3GPP 标准文档[2],AKA 认证与密钥协商协议具体流程如图 1 所示.

(1) VLR/SGSN 首先向 HE/HLR 发送认证数据请求消息,内容包含 MS 的 IMSI.

(2) HE/HLR 接收到来自 VLR/SGSN 的认证数据请求消息后,根据 MS 的 IMSI 从数据库中取得与 MS 共享密钥 K,然后计算认证向量数组 $AV[1…m]$.每个认证向量由以下 5 个元素组成(随机数 $RAND$、期望响应值 $XRES$、加密密钥 CK、完整性密钥 IK 和认证令牌 $AUTH$),其中每一个向量的生成过程如下:首先生成一个序列数 SQH 和一个随机数 $RAND$,并使 $SQN=SQN_{HE}$,然后计算以下值:$MAC=f1_k(SQN||RAND||AMF)$,$XRES=f2_k(RAND)$,$CK=f3_k(RAND)$,$IK=f4_k(RAND)$,$AK=f5_k(RAND)$,$AUTH=SQN⊕AK||AMF||MAC$ 和 $AV:=RAND||XRES||CK||IK||AUTH$,最后将 SQN_{HN} 加 1.其中,匿名密钥 AK 主要用来保护序列数 SQN,防止因暴露 SQN 而泄露 MS 的位置信息,AMF 为认证与密钥管理域.当 HE/HLR 生成向量数组 $AV[1…m]$后,通过认证数据响应消息发送该向量数组给 VLR/SGSN.

(3) VLR/SGSN 接收到来自 HE/HLR 认证向量 $AV[1…m]$后,首先把该向量存放在数据库里,当需要对 MS 认证时取出一个未用的向量,然后向 MS 发送用户认证请求消息,内容包括向量中 $RAND$ 和 $AUTH$.

(4) MS 接收到来自 VLR/SGSN 的数据 $RAND$ 和 $AUTH$ 后,首先计算 $AK=f5_k(RAND)$,$SQN=(SQN⊕AK)⊕AK$ 和 $XMAC=f1_k(SQN||RAND||AMF)$(其中,$MAC$ 和 AMF 包含在 $AUTH$ 中),然后验证 $XMAC=MAC$ 是否成立:假如 $XMAC=MAC$ 不成立,则 MS 向 VLR/SGSN 发送用户认证拒绝消息,并结束验证;否则,MS 继续验证 SQN 是否属

于正常范围内.假如 SQN 不属于正常范围,MS 向 VLR/SGSN 发送同步失败消息,并结束验证和启动 HE/HLR 重新同步 SQN_{HN} 操作;否则,用户 MS 对网络身份认证成功,MS 接着计算 $RES=f2_k(RAND)$,将该值发送给 VLR/SGSN,并置 SQN_{MS} 为 SQN.同时,MS 计算 $CK=f3_k(RAND)$和 $IK=f4_k(RAND)$用作与 VLR/SGSN 之间建立通信时数据流的加密密钥和完整性密钥.

(5) VLR/SGSN 接收到 MS 发送的 RES 后,判断 $XRES=RES$ 是否成立:假如成立,则网络对用户认证成功,VLR/ SGSN 从认证向量中取 CK 和 IK 作为与该 MS 通信时数据流的加密密钥和完整性密钥;否则,网络对用户认证失败,VLR/SGSN 向 HE/HLR 发送认证失败报告.

当 VLR/SGSN 需要对 MS 进行认证时,如果 VLR/SGSN 数据库中有关于该 MS 的认证向量,则直接重复第 3 步~第 5 步操作,对该 MS 进行认证;假如 VLR/SGSN 数据库中没有关于该 MS 的认证向量,则需要重复第 1 步~第 5 步.

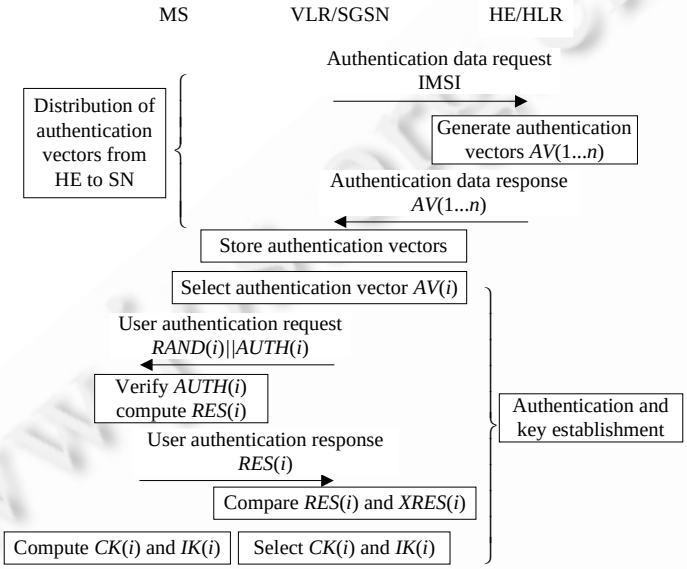


Fig.1 Authentication and key agreement

图 1 AKA 认证与密钥协商协议流程图

2 3GPP AKA 协议安全性研究

2.1 3GPP AKA协议安全性研究进展

自从AKA协议提出后,国外许多学者对该协议进行了研究.文献[5]研究了认证向量数组长度值K与网络信令数据流量消耗成本之间的关系,推荐一种动态 K 选择机制选择认证向量数组长度来降低网络信令的成本.文献[6]建议认证向量数组长度 L 取动态值,根据认证事件到达次数和 MS 在 VLR/SGSN 区域内滞留的时间来动态地预测 L 值.文献[7]研究 MS 离开原 VLR/SGSN 区域进入新 VLR/SGSN 时,原 VLR/SGSN 保留未用认证向量的时间 RT 对于网络信令流量的影响.文献[8,9]研究了 3GPP AKA 协议的安全性,指出该协议存在 VLR/ SGSN 与 HE/HLR 之间交互信息流量大、VLR/SGSN 存储负担重和序列数 SQN 同步 3 个问题,并借鉴了文献[10]的思想提出了基于临时密钥机制的 X-AKA 协议.文献[11]对 3GPP AKA 协议进行了全面分析,指出该协议存在数据流重定向攻击、故障网络中的主动攻击和序列数 SQN 操作困难等安全问题,并提出了增强型 AP-AKA 协议.文献[12]指出文献[11]提出的 AP-AKA 协议存在 IMSI 标识暴露、VLR/SGSN 与 HE/HLR 之间交互信息流量大和 VLR/SGSN 存储负担重等问题,采用临时密钥体制提出了新的 AKA 协议.文献[13]仅提出了 3 种保护 IMSI 方法,并没有对 AKA 协议作其他任何改进.文献[14]通过在系统中采用匿名标识管理模块对 IMSI 标识作了保

护.文献[15]对 UMTS 安全框架进行了全面的评估,分析 AKA 协议如何抵抗各种类型攻击.在国内,学者们对 3GPP AKA 协议的研究较少,文献[16]提出了基于 Diffie-Hellman 协议的增强型 AKA 协议.文献[17,18]各自提出了改进型的 3G 认证与密钥协商协议,然而,这两种方案是基于 VLR/SGSN 与 HE/HLR 之间共享对称密钥 K 而提出来的,具有很大的缺陷.

2.2 3GPP AKA协议脆弱性分析

根据国内外学者对 3GPP AKA 协议的研究进展,结合我们对 AKA 协议的研究深度,本节将对该协议可能遭受的各种攻击方式进行提炼、归纳和总结.

2.2.1 基于假 VLR/SGSN 的串线诱骗攻击

根据 3GPP 标准文档[2],AKA 协议是在以下 3 个假设前提下制定的:(1) MS 的 HE/HLR 相信 VLR/SGSN 能够安全地处理认证信息;(2) VLR/SGSN 至 HE/HLR 之间内部系统是足够安全的;(3) MS 信任自己所属的 HE/HLR.我们曾经对 3GPP AKA 做过深入研究[19],经再次研究后,我们发现,这 3 个假设的前两个假设是不完善的.我们认为,只有 HE/HLR 授权的 VLR/SGSN 能够被 HE/HLR 相信认为能够按照其意愿安全地处理认证信息;VLR/SGSN 至 HE/HLR 之间内部系统未必是足够安全的,因为 VLR/SGSN 至 HE/HLR 之间通信的光纤埋在地下,攻击者破坏光纤进行搭线攻击仍有可能发生.因为搭线攻击的存在和 VLR/SGSN 未经 HE/HLR 授权认证,所以存在一种假 VLR/SGSN 通过串线接入冒充真 VLR/SGSN 诱骗 MS 接入,进而在 MS 与 HE/HLR 之间充当真 VLR/SGSN 功能角色的攻击,本文称这种攻击为基于假 VLR/SGSN 的串线诱骗攻击.由于串线接入的可能性,认证过程中,VLR/SGSN 向 HE/HLR 发送认证数据请求消息时 HE/HLR 未对其身份进行认证,以及 VLR/SGSN 向 MS 发送用户认证请求消息时 MS 对网络身份进行认证但未对 VLR/SGSN 身份进行认证,从而使假 VLR/SGSN 能够像真 VLR/SGSN 一样在 MS 与 HE/HLR 之间辅助 HE/HLR 完成对 MS 的认证.认证完成后,由于假 VLR/SGSN 拥有与 MS 通信用的 CK 和 IK,所以可以监听 MS 的通信数据流.再者,由于 HE/HLR 只负责生成认证向量的功能,VLR/SGSN 直接担负 HE/HLR 对 MS 身份认证的功能,如果假 VLR/SGSN 串线接入成功,那么假 MS 就可以绕过 HE/HLR 的身份验证,直接接入网络获得未授权服务.

2.2.2 基于序列数 SQN 同步的 DoS 攻击

在 3GPP AKA 认证协议中,HE/HLR 为每个 MS 维护一个动态计数器 SQN_{HE},MS 自己也维护一个动态计数器 SQN_{MS} 来记录接收到的 SQN 的最高值,MS 发现接收到的 SQN 不属于正常范围,即刻使 HE/HLR 启动同步 SQN 操作.协议中采用动态计数器 SQN 的主要目的是防止假 VLR/SGSN 利用截获到的数据进行重放诱骗攻击[2].该序列数的设定能够有效防止假 VLR/SGSN 利用截获的认证数据进行重放诱骗攻击,但却引发了一种新的攻击方式:基于序列数 SQN 同步的 DoS 攻击.基于序列数 SQN 同步的 DoS 攻击的原理是,假 VLR/SGSN 向 MS 循环发送截获到的多对认证数据,MS 利用接收到的数据进行认证时发现 SQN 不属于正常范围,立即使 HE/HLR 启动同步 SQN 操作.假如 VLR/SGSN 向 MS 不断发送截获到的同对认证数据是不会引起该种攻击的,AKA 协议对此有相应的防御机制[2].由于 MS 使 HE/HLR 启动同步 SQN 操作交互不仅需要消耗网络带宽,而且会加重 HE/HLR 的计算负担,再加上 HE/HLR 启动同步操作是由 MS 发起的,所以发起这种攻击是很容易实现的.

2.2.3 IMSI 标识被动截取攻击与诱骗主动截取攻击

UMTS 系统中为防止 IMSI 在空中被截获进而暴露 MS 的位置信息,采用 TMSI(temporary mobile subscriber identity)替代方式.但是在某些情况下,IMSI 还是会以明文形式在空中传输,比如用户在第一次入网注册时以及 MS 移动到新 VLR/SGSN 时新 VLR/SGSN 无法根据 TMSI 从旧 VLR/SGSN 中获取 IMSI 时,VLR/SGSN 向 MS 发送用户标识请求消息要求 MS 回传 IMSI,随后 MS 向 VLR/SGSN 发送用户标识响应消息,该消息内容包含明文形式的 IMSI[2],恶意攻击者趁机很容易截获到 MS 的 IMSI.另外,当 VLR/SGSN 向 MS 发送用户标识请求消息时,MS 未验证 VLR/SGSN 身份就直接响应其消息回传 IMSI.这种机制存在很大的缺陷,假 VLR/SGSN 很容易利用向 MS 发送用户标识请求消息诱骗截取到 MS 的 IMSI,我们称这种攻击方式为 IMSI 标识诱骗主动截取攻击.

2.2.4 基于假 VLR/SGSN 的数据流重定向攻击

攻击者首先利用假 VLR/SGSN 捕获 MS 接入请求,并诱骗 MS 挂接其发出的基站接入信号,使 MS 与真正的基站接入信号失去联系.当 MS 发起请求时,假 VLR/SGSN 接收到请求后通过假 MS 将该请求消息直接转发给远端真 VLR/SGSN,真 VLR/SGSN 接收到该请求后误认为是真 MS 发起的请求,立刻向真 MS 的 HE/HLR 发送认证数据请求消息,HE/HLR 向真 VLR/SGSN 发回认证向量数据,接着,真 VLR/SGSN 开始对真 MS 进行认证.在认证过程中,假 MS 和假 VLR/SGSN 充当中继作用,即真 VLR/SGSN 向假 MS 发送用户认证请求,假 MS 将该用户认证请求通过假 VLR/SGSN 发送给真 MS,真 MS 将用户认证响应反方向通过假 VLR/SGSN 和假 MS 发送给真 VLR/SGSN,认证完毕后进行通话时,由于通信数据流采用了加密和完整性保护,所以假 VLR/SGSN 和假 MS 无法理解或破坏通信数据流,只起到数据流重定向功能.但是在脆弱的网络环境中,虽然 AKA 协议认证建立了加密密钥和完整性密钥,但通信数据流并没有采用加密和完整性保护,这时,假 VLR/SGSN 和假 MS 就可以窃听和篡改通信数据流[11].

2.3 增强型AKA协议需求

根据国内外学者对 3GPP AKA 协议的研究成果,结合我们对 AKA 协议的研究深度,增强型 AKA 协议必须满足以下 7 个条件:

(1) IMSI 保护:IMSI 在空中接口必须以加密方式传送,以抵抗 IMSI 标识被动截取与诱骗主动截取攻击;
(2) 信令流量:VLR/SGSN 与 HE/HLR 之间交互信息时,要求信令数据流量要小;
(3) 存储空间:VLR/SGSN 中数据存储空间负担小;
(4) 双向认证:MS 与 HE/HLR 之间要求双向身份认证,MS 与 VLR/SGSN 之间要求双向身份认证,HE/HLR 要对 VLR/SGSN 身份进行认证;
(5) 认证独立:VLR/SGSN 对 MS 身份认证不是每次都需要在 HE/HLR 的辅助之下完成,以避免因 VLR/SGSN 与 HE/HLR 之间通信暂时阻塞,VLR/SGSN 无法对 MS 进行身份认证;
(6) 抵抗攻击:能够抵抗基于假 VLR/SGSN 的数据流重定向攻击和串线诱骗攻击;
(7) 兼容性:能够与现有 AKA 协议框架达到最大兼容,以避免新协议框架变化带来现有应用的巨大改动.

3 基于公钥密码学的安全认证与密钥协商协议

为了解决 3GPP AKA 协议存在的安全问题,根据增强型 AKA 协议的需求,本文给出了位置不变和位置更新两种情况下的基于公钥密码学的安全认证与密钥协商协议.其中:位置不变情况下的安全认证与密钥协商协议主要适用于对 MS 进行认证的 VLR/SGSN 知道 MS 的 IMSI 或能从旧的 VLR/SGSN 获取 MS 的 IMSI 时,VLR/SGSN 对 MS 进行认证和与密钥协商的情况;位置更新情况下的安全认证与密钥协商协议主要适用于 MS 从旧 VLR/SGSN 移动到新 VLR/SGSN,新 VLR/SGSN 无法从旧 VLR/SGSN 获取 IMSI 时,新 VLR/SGSN 需要对 MS 进行认证与密钥协商的情况.本文算法的 MS 与 HE/HLR 之间需要共享两个消息认证函数 $f1^*$与 $f2^*$,一个临时密钥产生函数 $f5$;MS 与 VLR/SGSN 之间需要共享两个消息认证函数 $f1$ 和 $f2$,两个密钥产生函数 $f3$ 和 $f4$.除函数 $f2^*$ 之外,其他消息认证和密钥产生函数都借用 3GPP 中相应函数[2,3],其中,$f1$,$f1^*$和 $f2^*$产生 64 比特值,$f2$,$f3$ 和 $f4$ 产生 128 比特值,$f5$ 产生 48 比特值.其次,本文中两种算法都需要有公钥认证中心的支撑,该公钥认证中心主要用来存放 VLR/SGSN 的身份信息,每个 VLR/SGSN 配有一对公私密钥(PK_{VLR},SK_{VLR}),HE/HLR 在公钥认证中心辅助下完成对 VLR/SGSN 身份的认证.最后,本文算法需要为每个 HE/HLR 配备一对公私密钥(PK_{HLR},SK_{HLR}),其中,SK_{HLR} 保存在 HE/HLR 中,PK_{HLR} 保存在注册于该 HE/HLR 下的 MS 的 USIM 中.在下文中用到的符号 AMF 表示认证与密钥管理域,ID_{VLR} 为 VLR/SGSN 身份唯一标识,ID_{HLR} 为 HE/HLR 身份的唯一标识.

3.1 位置不变情况下的认证与密钥协商协议算法

位置不变情况下的认证与密钥协商协议算法具体流程如图 2 所示.

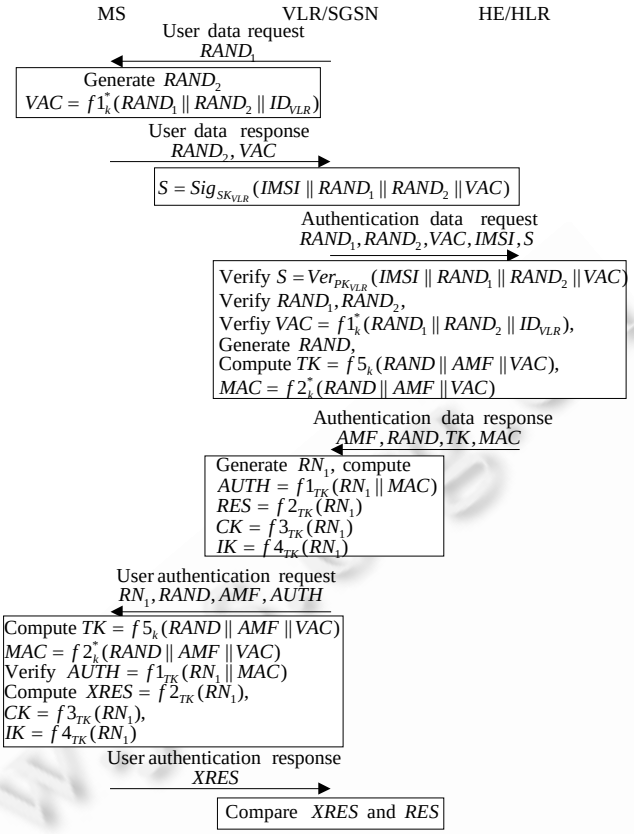


Fig.2 Authentication and key agreement at location immovability

图 2 位置不变情况下的认证与密钥协商协议流程图

(1) VLR/SGSN 首先向 MS 发送用户数据请求消息,内容包括一个随机数 $RAND_1$;

(2) MS 接收到来自 VLR/SGSN 的随机数 $RAND_1$ 后,接着自己生成一个随机数 $RAND_2$,然后计算 $VAC=f1_k^*(RAND_1 \| RAND_2 \| ID_{VLR})$,最后,MS 发送用户数据响应消息给 VLR/SGSN,该消息内容包括 $RAND_2$,VAC;

(3) VLR/SGSN 接收到来自 MS 的 $RAND_2$ 和 VAC 后,从 MS 先前访问的 VLR/SGSN 中取得该 MS 的 IMSI,并用自己的私密钥 SK_{VLR} 计算发送数字签名 $S = Sig_{SK_{VLR}}(IMSI \| RAND_1 \| RAND_2 \| VAC)$,然后,VLR/SGSN 向 HE/HLR 发送认证数据请求消息,该消息内容包括 $RAND_1$,$RAND_2$,VAC,$IMSI$ 和 S;

(4) HE/HLR 接收到来自 VLR/SGSN 的数据 $RAND_1$,$RAND_2$,VAC,$IMSI$ 和 S 后,根据 VLR/SGSN 的标识 ID_{VLR} 到公钥认证中心取得 VLR/SGSN 的公钥 PK_{VLR},计算验证 $S = Ver_{PK_{VLR}}(IMSI \| RAND_1 \| RAND_2 \| VAC)$ 是否成立:假如不成立,HE/HLR 对 VLR/SGSN 认证失败,HE/HLR 断开与 VLR/SGSN 的连接并结束认证;否则,HE/HLR 对 VLR/SGSN 身份认证成功.接着,HE/HLR 根据 IMSI 和 ID_{VLR} 继续验证 $RAND_1$ 和 $RAND_2$ 是否一同出现过:假如这两个随机数一同出现过,则 HE/HLR 断开与 VLR/SGSN 的连接并结束认证;否则,继续验证 $VAC = f1_k^*(RAND_1 \| RAND_2 \| ID_{VLR})$是否成立,假如不成立,HE/HLR 对 MS 认证失败并结束认证,否则 HE/HLR 完成对 MS 的身份认证.假如 HE/HLR 对 VLR/SGSN 和 MS 身份验证都成功,随后选择随机数 $RAND$,计算临时密钥 $TK=f5_k(RAND \| AMF \| VAC)$和认证令牌 $MAC = f2_k^*(RAND \| AMF \| VAC)$,然后向 VLR/SGSN 发送认证数据响应消息,该消息内容包括 $RAND$,AMF,TK 和 MAC;

(5) VLR/SGSN 接收到来自 HE/HLR 的 $RAND$,AMF,TK 和 MAC 后,首先把这些参数存放在数据库里,接着

生成随机数 RN_1 并计算 $AUTH=f1_{TK}(RN_1||MAC)$,$RES=f2_{TK}(RN_1)$,$CK=f3_{TK}(RN_1)$和 $IK=f4_{TK}(RN_1)$,然后向 MS 发送用户认证请求消息,该消息内容包括 RN_1,$RAND$,AMF 和 $AUTH$;

(6) MS 接收到来自 VLR/SGSN 的 RN_1,$RAND$,AMF 和 $AUTH$ 后,首先计算临时密钥 $TK=f5_k(RAND||AMF||VAC)$和 $MAC=f2_k^*(RAND\|AMF\|VAC)$,然后验证 $AUTH=f1_{TK}(RN_1||MAC)$是否成立:假如不成立,则说明 MS 对网络(包括 VLR/SGSN 和 HE/HLR)身份认证失败;否则,计算 $XRES=f2_{TK}(RN_1)$,$CK=f3_{TK}(RN_1)$和 $IK=f4_{TK}(RN_1)$,并向 VLR/SGSN 发送用户认证响应消息,该消息内容包括 $XRES$;

(7) VLR/SGSN 接收到来自 MS 的 $XRES$,接着比较 $XRES$ 和 RES 值:假如相同,则 VLR/SGSN 完成对 MS 的身份验证,接着取出相应的加密密钥 CK 和完整性密钥 IK 用作与该 MS 通信时数据的加密密钥和完整性密钥;否则,VLR/SGSN 对 MS 的身份验证失败.

当 MS 在该 VLR/SGSN 内再次需要认证时,无论需要认证多少次,只需重复第 5 步~第 7 步,从而极大地减少了 VLR/SGSN 与 HE/HLR 之间的通信流量,减轻了 VLR/SGSN 的存储负担.

3.2 位置更新情况下的认证与密钥协商协议算法

位置更新情况下的认证与密钥协商协议算法的具体流程如图 3 所示.

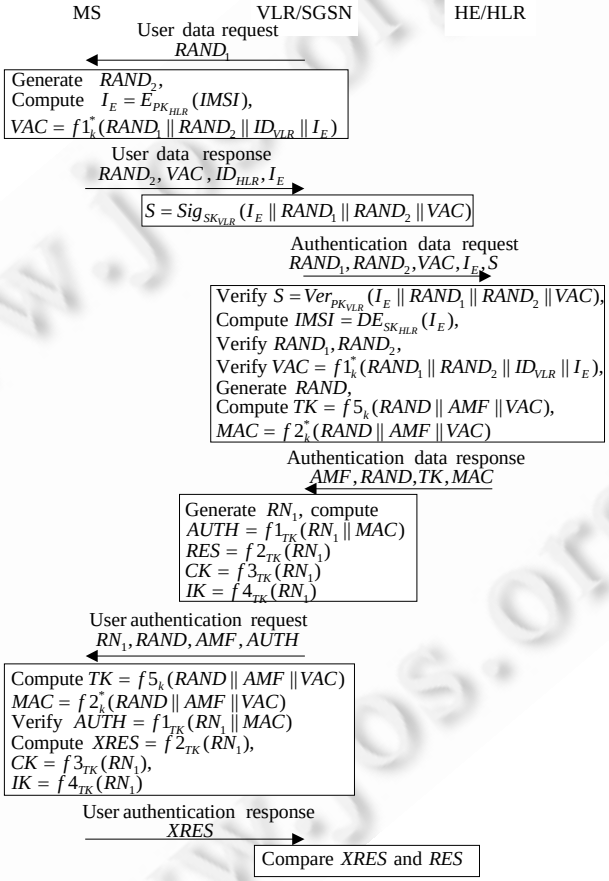


Fig.3 Authentication and key agreement at location updating

图 3 位置更新情况下的认证与密钥协商协议流程图

(1) VLR/SGSN 首先向 MS 发送用户数据请求消息,内容包括一个随机数 $RAND_1$;

(2) MS 接收到 VLR/SGSN 发送过来的随机数 $RAND_1$ 后,取出 HE/HLR 的公钥 PK_{HLR},并用该公钥加 IMSI:

$I_E = E_{PK_{HLR}}(IMSI)$,同时,自己也生成一个随机数 $RAND_2$ 并计算 $VAC = f1_k^*(RAND_1 \| RAND_2 \| \mathrm{ID}_{VLR} \| I_E)$,然后向 VLR/SGSN 发送用户数据响应消息,该消息内容包括 $RAND_2$,VAC,ID_{HLR} 和 I_E;

(3) VLR/SGSN 接收到 MS 发送过来的 $RAND_2$,VAC,ID_{HLR} 和 I_E 后,用自己的私密钥 SK_{VLR} 计算发送数字签名 $S = Sig_{SK_{VLR}}(I_E \| RAND_1 \| RAND_2 \| VAC)$,然后向 HE/HLR 发送认证数据请求消息,该消息内容包括 $RAND_1$,$RAND_2$,VAC,I_E 和 S;

(4) HE/HLR 接收到来自 VLR/SGSN 的数据 $RAND_1$,$RAND_2$,VAC,I_E 和 S 后,根据 VLR/SGSN 的标识 ID_{VLR},到公钥认证中心取得 VLR/SGSN 的公钥 PK_{VLR},验证 $S = Ver_{PK_{VLR}}(I_E \| RAND_1 \| RAND_2 \| VAC)$ 是否成立:假如不成立,则 HE/HLR 对 VLR/SGSN 的身份认证失败,HE/HLR 断开与 VLR/SGSN 的连接并结束认证;否则,HE/HLR 对 VLR/SGSN 的身份认证成功,HE/HLR 继续用自己的私密钥 SK_{HLR} 解密 I_E 获取 MS 的 $IMSI = DE_{SK_{HLR}}(I_E)$,根据 IMSI 获取与 MS 的共享密钥 k,然后验证 $VAC = f1_k^*(RAND_1 \| RAND_2 \| \mathrm{ID}_{VLR} \| I_E)$ 是否成立:假如不成立,则断开连接结束认证;否则,HE/HLR 继续根据 ID_{VLR} 和 IMSI 判断 $RAND_1$ 和 $RAND_2$ 是否一同出现过,假如一同出现过,则 HE/HLR 对 MS 认证失败断开连接并结束认证,否则完成对 MS 的身份验证.假如 HE/HLR 对 VLR/SGSN 和 MS 的身份验证都成功,则 HE/HLR 接着生成一个随机数 $RAND$,计算临时密钥 $TK=f5_k(RAND||AMF||VAC)$和 $MAC = f2_k^*(RAND||AMF||VAC)$,然后向 VLR/SGSN 发送认证数据响应消息,该消息内容包括 $RAND$,AMF,MAC 和 TK;

(5) VLR/SGSN 接收到来自 HE/HLR 的 $RAND$,AMF,MAC 和 TK 后,生成随机数 RN_1,计算 $AUTH=f1_{TK}(RN_1||MAC)$,$RES=f2_{TK}(RN_1)$,$CK=f3_{TK}(RN_1)$和 $IK=f4_{TK}(RN_1)$,然后向 MS 发送用户认证请求消息,该消息内容包括 RN_1,$RAND$,AMF 和 $AUTH$;

(6) MS 接收到来自 VLR/SGSN 的 RN_1,$RAND$,AMF 和 $AUTH$,首先计算 $TK=f5_k(RAND||AMF||VAC)$和 $MAC=f2_k^*(RAND \| AMF \| VAC)$,然后验证 $AUTH=f1_{TK}(RN_1||MAC)$:假如验证失败,则 MS 对网络(包括 VLR/SGSN 和 HE/HLR)的身份认证失败;否则,认证成功并继续计算 $XRES=f2_{TK}(RN_1)$,$CK=f3_{TK}(RN_1)$和 $IK=f4_{TK}(RN_1)$,然后向 VLR/ SGSN 发送用户认证响应消息,该消息内容包括 $XRES$;

(7) VLR/SGSN 接收到来自 MS 的 $XRES$,接着比较 $XRES$ 和 RES 值:假如相同,VLR/SGSN 完成对 MS 的身份验证,接着取出相应的加密密钥 CK 和完整性密钥 IK 用作与该 MS 通信时数据的加密密钥和完整性密钥;否则,VLR/SGSN 对 MS 的身份验证失败.

当 MS 在该 VLR/SGSN 内再次需要认证时,无论需要认证多少次,只需重复第 5 步~第 7 步,从而极大地减少了 VLR/SGSN 与 HE/HLR 之间的通信流量,减轻了 VLR/SGSN 的存储负担.

4 安全认证与密钥协商协议形式化分析

本节采用基于串空间理论的认证测试方法来形式化分析本文的协议算法.

4.1 串空间理论介绍

本节介绍串空间模型的定义和串空间的构造方法,有关串空间的理论详细介绍请见文献[20−25].

定义 1. 符号项是一个二元组$\langle \sigma,a \rangle$,其中,$a \in A$ 且$\sigma \in \{+,-\}$,记符号项为$+t$ 或$-t$,$(\pm A)^*$为符号项有限序列集合,记$(\pm A)^*$中的元素为$\langle\langle \sigma_1,a_1 \rangle,\ldots,\langle \sigma_n,a_n \rangle\rangle$.

定义 2. A 上的串空间为Σ和迹映射 $tr:\Sigma \to (\pm A)^*$.

构造串空间的方法如下:对于一个串空间Σ,

(1) 节点是一个二元组$\langle s,i \rangle$,其中,$s \in \Sigma$且 i 满足 $1 \leqslant i \leqslant length(tr(s))$的整数,节点的集合记为 N,称节点$\langle s,i \rangle$属于串 s,显然,每个节点属于一个特定的串;

(2) 假如 $n=\langle s,i \rangle \in N$,则 $index(n)=i$ 且 $strand(n)=s$.定义 $term(n)=(tr(s))_i$,即串 s 的迹中的第 i 个符号项,定义 $uns\_term(n)=((tr(s))_i)_2$,即串 s 的迹中的第 i 符号项的无符号部分;

(3) 假如 $n_1,n_2 \in N$,边 $n_1 \to n_2$ 表示 $term(n_1)=+a$ 和 $term(n_2)=-a$,该边表示 n_1 发送消息 a,该消息被 n_2 接收到,

创建了串之间的一种因果联系;

(4) 假如 $n_1,n_2\in N$,边 $n_1\Rightarrow n_2$ 表示 n_1,n_2 出现在相同的串上,且 $index(n_1)=index(n_2)-1$,该边表示 n_1 是 n_2 在串 s 的直接因果前驱.记 $n'\Rightarrow^+n$ 表示 n' 是 n 在串 s 上的前驱(不一定是直接因果前驱);

(5) 无符号项 t 出现在 $n\in N$,当且仅当 $t\subset term(n)$;

(6) 假设 I 为无符号项集合,节点 $n\in N$ 是 I 的进入点,当且仅当 $term(n)=+t$,其中 $t\in I$,并且对所有 $n'\Rightarrow^+n$,$term(n')\notin I$;

(7) 无符号项 t 产生于 $n\in N$,当且仅当 n 是集合 $I=\{t':t\subset t'\}$的进入点;

(8) 无符号项 t 是唯一产生的,当且仅当 t 唯一产生于 $n\in N$.

如果 t 唯一产生于一个特定的串空间,则它在该结构中代表随机数或起着会话密钥的作用.

N 以及两类边 $n_1\rightarrow n_2$ 和 $n_1\Rightarrow n_2$ 的集合是一个有向图$\langle N,(\rightarrow\cup\Rightarrow)\rangle$,包是这个图的有限子图,它表示节点之间的因果依懒关系.

定义 3. 假设$\rightarrow_C\subset\rightarrow$且$\Rightarrow_C\subset\Rightarrow$,假设 $C=\langle N_C,(\rightarrow_C\cup\Rightarrow_C)\rangle$是$\langle N,(\rightarrow\cup\Rightarrow)\rangle$的子图,$C$ 是包当且仅当

(1) C 是有限的;

(2) 假如 $n_2\in N_C$ 且 $term(n_2)$符号为负,则存在唯一的 n_1,使得 $n_1\rightarrow_C n_2$;

(3) 假如 $n_2\in N_C$ 且 $n_1\Rightarrow n_2$,则 $n_1\Rightarrow_C n_2$;

(4) C 是无环的.

假如 $n\in N_C$,则称节点 n 在包 $C=\langle N_C,\rightarrow_C,\Rightarrow_C\rangle$中,记为 $n\in C$.假如串的所有节点都属于 N_C,则称串 s 在包中.假如 C 是一个包,则串 s 的高度,记为 $C\text{–}hight(s)$,是满足$\langle s,i\rangle\in C$ 的最大 i 值.$C\text{–}trace(s)=\langle tr(s)(1),\ldots,tr(s)(m)\rangle$,其中,$m=C\text{–}height(s)$.

4.2 认证测试方法介绍

本节介绍认证测试方法的定义和定理,有关认证测试方法的详细介绍请见文献[25].

定义 4. 若 $t_0\subset t,t_0$ 不是级连项,且任何满足 $t_0\subset t_1\subset t$ 的 $t_1\neq t_0$ 是级连项,则称项 t_0 为项 t 的分量.显然,分量或是原子项或是加密项.如果 t 是项 $term(n)$的分量(其中,$n=\langle s,i\rangle$)但 t 不是节点$\langle s,j\rangle$的分量(其中,$j<i$),则称 t 在节点 $n=\langle s,i\rangle$是新项.

定义 5. 在串空间Σ下,称正常串的某个部分为测试,它的存在将保证其他正常串在包中存在.称项 $t=\{h\}_K$ 为项 a 在节点 n 中的测试分量,如果:(1) $a\subset t$ 且 t 是 n 的分量;(2) t 不是任何正常节点 $n'\in\Sigma$的分量的真子项.

定义 6. 如果 n_1 为正,n_2 为负(如果 n_1 为负且 n_2 为正),$a\subset term(n_1)$且存在一个 n_2 的新分量 t_2,使得 $a\subset t_2$,则边 $n_1\Rightarrow^+n_2$ 是对于 $a\in A$ 的被变换边(变换边).

定义 7. 如果 a 唯一地产生在 n_0,且 $n_0\Rightarrow^+n_1$ 是对于 a 的被变换边,则称边 $n_0\Rightarrow^+n_1$ 是对于 a 的测试.

共有 3 种重要的认证测试方法:出测试方法、入测试方法以及主动测试方法.

- 称边 $n_0\Rightarrow^+n_1$ 是 a 在 $t=\{h\}_K$ 中的出测试,如果它是对于 a 的测试且 $K^{-1}\notin\overline{K}$.这里,$\overline{K}$ 表示不安全密钥集合,除 t 外,a 不在 n_0 的任何分量中出现,且 t 是 a 在 n_0 中的测试分量;
- 称边 $n_0\Rightarrow^+n_1$ 是 a 在 $t_1=\{h\}_K$ 中的入测试,如果它是对于 a 的测试且 $K\notin\overline{K}$,并且 t_1 是对于 a 在 n_1 中的测试分量;
- 称负节点 n 是对于 $t=\{h\}_K$ 的主动测试,如果 t 是对于 n 中任何 a 的测试分量,且 $K\notin\overline{K}$.

定理 1.

出测试原理:令 C 为包,$n'\in C,n\Rightarrow^+n'$是 a 在 t 中的出测试,于是:

(1) 存在正常节点 $m,m'\in C$,使得 t 是 m 的分量,且 $m\Rightarrow^+m'$是对于 a 的变换边;

(2) 假设除此之外,a 只在 m'的分量 $t_1=\{h_1\}_{K_1}$ 中出现且 t_1 不是任何正常分量的真子项,并且 $K^{-1}\notin\overline{K}$,于是,存在一个负正常节点 m'',其中,t_1 是 m''的分量.

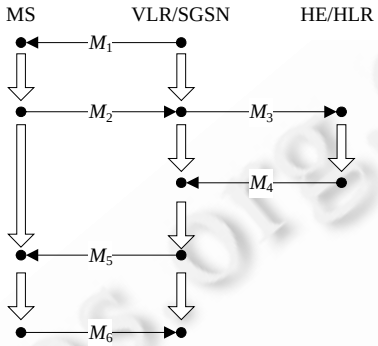
入测试原理:令 C 为包,$n'\notin C,n\Rightarrow^+n'$为对于 a 在 t'中的入测试,于是,存在正常节点 $m,m'\in C$,使得 t'是 m'的分

量,且 $m\Rightarrow^{+}m'$是对于 a 的变换边.

主动测试原理:令 C 为包,$n\in C$,n 是对于 $t=\{h\}_K$ 的主动测试,于是,存在一个正常节点 $m\in C$,使得 t 是 m 的分量.

4.3 改进AKA协议的形式化分析

本节主要讨论位置不变情况下的基于公钥密码学的安全认证与密钥协商协议的形式化分析.由于位置更新情况下的基于公钥密码学的安全认证与密钥协商协议的形式化分析与位置不变情况下完全类同,基于篇幅,在此不再作重复分析与证明.位置不变情况下的基于公钥密码学的安全认证与密钥协商协议形式化为包含 3 类正常的串,如图 4 所示.



$M_1=RAND_1$; $M_2=RAND_2,VAC$; $M_3=RAND_1,RAND_2,VAC,IMSI,S$;
$M_4=AMF,RAND,TK,MAC$; $M_5=RN_1,RAND,AMF,AUTH$; $M_6=XRES$

Fig.4 A bundle of authentication and key agreement at location immovability

图 4 位置不变情况下认证与密钥协商协议中的正常包图

(1) 移动用户 MS 的串,其迹为$\langle -M_1,+M_2,-M_5,+M_6\rangle$.其中,$\mathrm{ID}_{VLR}\in T_{name},RAND_1,RAND_2,RN_1,RAND,AMF\in T,k,TK\in K\cap k^{-1},TK^{-1}\notin \overline{K}$ ($\overline{K}$ 表示不安全密钥集合),TK 虽然可形式化为其他项的加密项,但由于其值分别直接作为密钥值,因而在此形式化为原子项.$MS[RAND_1,RAND_2,RN_1,RAND,AMF,\mathrm{ID}_{VLR},k,TK]$表示所有具有上述迹的串集合,所以 MS 的串 $S_{MS}\in MS[RAND_1,RAND_2,RN_1,RAND,AMF,ID_{VLR},k,TK]$.

(2) 服务网络 VLR/SGSN 的串,其迹为$\langle +M_1,-M_2,+M_3,-M_4,+M_5,-M_6\rangle$.其中,$ID_{VLR},IMSI\in T_{name},RAND_1,RAND_2,RN_1,RAND,AMF,S\in T,TK\in K\cap TK^{-1}\notin \overline{K}$ ($\overline{K}$ 表示不安全密钥集合).TK 虽然可形式化为其他项的加密项,但由于其值分别直接作为密钥值,因而在此形式化为原子项.$VLR/SGSN[RAND_1,RAND_2,RN_1,RAND,AMF,ID_{VLR},IMSI,S,TK]$表示所有具有上述迹的串集合,所以,VLR/SGSN 的串 $S_{VLR/SGSN}\in VLR/SGSN[RAND_1,RAND_2,RN_1,RAND,AMF,ID_{VLR},IMSI,S,TK]$.此外,当 VLR/SGSN 与 HE/HLR 交互时,VAC 形式化为原子项,并包含在上述串集合中.

(3) 本地网络 HE/HLR 的串,其迹为$\langle -M_3,+M_4\rangle$.其中,$ID_{VLR},IMSI\in T_{name},RAND_1,RAND_2,RN_1,RAND,VAC,AMF,S\in T,k,TK\in K\cap k^{-1},TK^{-1}\notin \overline{K}$ ($\overline{K}$ 表示不安全密钥集合),VAC,TK 虽然可形式化为其他项的加密项,但由于其值分别直接作为密钥值,因而在此形式化为原子项.$HE/HLR[RAND_1,RAND_2,RN_1,RAND,VAC,AMF,ID_{VLR},IMSI,S,k,TK]$表示所有具有上述迹的串集合,所以,HE/HLR 的串:$S_{HE/HLR}\in HE/HLR[RAND_1,RAND_2,RN_1,RAND,VAC,AMF,ID_{VLR},IMSI,S,TK]$.

① 证明 MS 对服务网络(包括 VLR/SGSN 和 HE/HLR)身份的认证

设 C 为包,$S_{MS}\in MS[RAND_1,RAND_2,RN_1,RAND,AMF,ID_{VLR},k,TK]$且 $C\text{–}hight(S_{MS})=4$, $k^{-1}\notin \overline{K}$,ID_{VLR} 唯一产生在$\langle S_{MS},2\rangle$.边$\langle S_{MS},2\rangle\Rightarrow^{+}\langle S_{MS},3\rangle$是 ID_{VLR} 在 VAC 中的出测试,根据出测试原理(1),存在正常节点 $m,m'\in C$,使得 VAC 是 m 的分量且 $m\Rightarrow m'$是 ID_{VLR} 的变换边.这时,m 只可能是$\langle S_{VLR/SGSN},2\rangle$,其中,$S_{VLR/SGSN}\in VLR/SGSN[RAND_1,RAND_2,RN_1,RAND,AMF,ID_{VLR},IMSI,S,TK]$.于是,变换边 $m\Rightarrow m'$必为$\langle S_{VLR/SGSN},2\rangle\Rightarrow^{+}\langle S_{VLR/SGSN},4\rangle$且 $C\text{–}hight(S_{VLR/SGSN})=5$.由于 $AUTH$ 既包含 HE/HLR 身份信息又包含 VLR/SGSN 身份信息,因此我们证明了 MS 对服务网络(包括 VLR/

SGSN 和 HE/HLR)的身份认证.

② 证明 VLR/SGSN 对 MS 的身份认证

设 C 为包,$S_{VLR/SGSN}\in VLR/SGSN[RAND_1,RAND_2,RN_1,RAND,AMF,ID_{VLR},IMSI,S,TK]$且 $C\text{–}hight(S_{VLR/SGSN})=5$, $TK^{-1}\notin \bar{K}$,RN_1 唯一产生在$\langle S_{VLR/SGSN},4\rangle$.边$\langle S_{VLR/SGSN},4\rangle\Rightarrow^{+}\langle S_{VLR/SGSN},5\rangle$是 RN_1 在 $AUTH$ 中的出测试,根据出测试原理(1),存在正常节点 $m,m'\in C$,使得 RN_1 是 $AUTH$ 的分量且 $m\Rightarrow m'$是 RN_1 的变换边.这时,m 只可能为$\langle S_{MS},3\rangle$,其中,$S_{MS}\in MS[RAND_1,RAND_2,RN_1,RAND,AMF,ID_{VLR},k,TK]$.于是,变换边 $m\Rightarrow m'$必为$\langle S_{MS},3\rangle\Rightarrow^{+}\langle S_{MS},4\rangle$且$C\text{–}hight(S_{MS})=4$,因此我们证明了 VLR/SGSN 对移动用户 MS 的身份认证.

③ 证明 HE/HLR 对 MS 和 VLR/SGSN 的身份认证

设 C 为包,$S_{VLR/SGSN}\in VLR/SGSN[RAND_1,RAND_2,RN_1,RAND,AMF,VAC,ID_{VLR},IMSI,S,TK]$且 $C\text{–}hight(S_{VLR/SGSN})=5$, $k^{-1}\notin \bar{K}$,VAC 唯一产生在$\langle S_{VLR/SGSN},2\rangle$(当 VLR/SGSN 交互时,$VAC$ 形式化为原子项,并视为是该节点唯一产生的).边$\langle S_{VLR/SGSN},2\rangle\Rightarrow^{+}\langle S_{VLR/SGSN},3\rangle$是 VAC 在 MAC 中的入测试,根据入测试原理,存在正常节点 $m,m'\in C$,使得 VAC 是 MAC 的分量且 $m\Rightarrow m'$是 VAC 的变换边.这时,m'只可能为$\langle S_{HE/HLR},2\rangle$,其中,$S_{HE/HLR}\in HE/HLR[RAND_1,RAND_2,RN_1,RAND,VAC,AMF,ID_{VLR},IMSI,S,TK]$.于是,变换边 $m\Rightarrow m'$必为$\langle S_{HE/HLR},1\rangle\Rightarrow^{+}\langle S_{HE/HLR},2\rangle$且 $C\text{–}hight(S_{HE/HLR})=2$.由于 VAC 既包含 MS 身份信息又包含 VLR/SGSN 身份信息,因此证明了 HE/HLR 对 MS 和 VLR/SGSN 的身份认证.

上文采用基于串空间模型的认证测试方法证明了本文提出的算法可以实现多重身份的认证,从根本上保证了本文提出算法的安全性.

5 算法安全性及优点比较

本文提出的在位置不变和更新两种情况下认证与密钥协商协议很好地满足了增强型 AKA 的协议需求.在位置更新情况下,为避免 IMSI 以明文方式在空中传播,采用了公钥加密传输方法,有效地抵抗了 IMSI 标识被动截取与诱骗主动截取攻击;通过采用临时密钥体制,降低了 VLR/SGSN 与 HE/HLR 之间的信息流量,减轻了 VLR/SGSN 的存储负担,提高了 VLR/SGSN 对 MS 的认证独立性;通过采用数字签名和完整性保护,增强了抵抗基于假 VLR/SGSN 的数据流重定向攻击和串线诱骗攻击能力.同时,本文算法框架严格借鉴 3GPP AKA 协议,能够与其达到最好的兼容.与 AKA 协议算法和其他改进算法相比,本文算法还具有以下几个独特的优点:

(1) 实现多重相互身份验证,彻底地杜绝多种诱骗攻击.多重相互身份验证包括:① HE/HLR 对 MS 的身份验证;② HE/HLR 对 VLR/SGSN 的身份验证;③ MS 对 HE/HLR 的身份验证;④ MS 对 VLR/SGSN 的身份验证;⑤ VLR/SGSN 对 MS 的身份验证.相比之下,3GPP AKA 协议和文献[8,9,14,17,18]实现了第①种、第③种、第⑤种 3 种类型认证,容易遭受基于假 VLR/SGSN 的数据流重定向攻击和串线诱骗攻击.文献[11,12,16]实现了第①种、第③~⑤种这 4 种类型认证,容易遭受基于假 VLR/SGSN 的串线诱骗攻击.如果 HE/HLR 不对 VLR/SGSN 的身份 ID_{VLR} 进行有效验证,则假 VLR/SGSN 就能通过串线接入后在 HE/HLR 与 MS 之间冒充合法 VLR/SGSN 担负起 HE/HLR 对 MS 认证的功能.3GPP AKA 协议和文献[8,9,14,17,18]提出的改进协议都无法察觉到这两种攻击的发生.文献[11,12,16]在 VAC 中包含 VLR/SGSN 的标识 ID_{VLR},虽然 HE/HLR 通过验证接收到的 VAC 能够抵抗数据流重定向攻击,但是对于串线诱骗攻击,由于假 VLR/SGSN 直接在 MS 与 HE/HLR 之间扮演合法 VLR/SGSN 角色,假 VLR/SGSN 向 MS 和 HE/HLR 分别传送的 ID_{VLR} 与 ID'_{VLR} 是同一个标识符,使得 HE/HLR 计算得到的 VAC 与接收到的 VAC 是相等,所以无法察觉该种攻击.文献[16–18]虽然采用协商 VLR/SGSN 与 HE/HLR 之间会话密钥或通过拥有 VLR/SGSN 与 HE/HLR 之间的共享密钥方法,对 VLR/SGSN 与 HE/HLR 之间传送数据作加密保护,但是并未对 VLR/SGSN 的身份进行验证,所以仍然无法抵御基于假 VLR/SGSN 的串线诱骗攻击.再者,3G 网络是一个全球化的开放网络,大规模共享对称密钥的管理是很难的问题.本文的算法借鉴公钥思想采用数字签名,一方面,对 VLR/SGSN 的身份 ID_{VLR} 进行了强有效的验证,保证 VLR/SGSN 身份的真实性,另一方面,对 VLR/SGSN 与 HE/HLR 之间的传输数据作了完整性保护,从而彻底杜绝了多种方式攻击的发生.

(2) 采用公钥加密传送 IMSI,杜绝 MS 身份与位置等信息的泄漏.3GPP AKA 协议与文献[8,9,11,16,18]提出

的协议算法,IMSI 在某些情况下会在空中接口中以明文方式传送,进而会暴露 MS 的相关信息.文献[14]提出的算法虽然能够起到保护 IMSI 的作用,但是该算法涉及到保护 IMSI 功能部分的流程较为复杂,对 MS,VLR/SGSN 和 HE/HLR 各个部件都需要作改动,而且该算法不能抵抗基于假 VLR/SGSN 的数据流重定向攻击与串线诱骗攻击.文献[13]虽然提出了 3 种保护 IMSI 的方法,但是每种方法都存在一定的弊端.文献[12]提出的算法虽然能够起到保护 IMSI 的作用,但是与本文提出的采用公钥加密传送 IMSI 的方式相比,在减少 VLR/SGSN 与 HE/HLR 之间通信流量和与原有协议框架的兼容上,该算法无法与本文算法相比拟.虽然采用公钥加密传送 IMSI 会增加移动终端计算量,但是对带操作系统的 3G 移动终端来说,采用公钥加密 IMSI 显然不是问题.

(3) 采用临时密钥体制,简化了认证向量分发的步骤,减小了 VLR/SGSN 与 HE/HLR 之间的通信流量,减轻了 VLR/SGSN 的存储压力,降低了系统的通信负担,提高了系统的健壮性.3GPP AKA 协议和文献[11,14,16–18]提出的协议算法,当 MS 始终处于特定的 VLR/SGSN 中,该 VLR/SGSN 把认证向量消耗完时,VLR/SGSN 需要重新请求认证向量,HE/HLR 需要重新分发认证向量.这就加大了 VLR/SGSN 与 HE/HLR 之间的通信流量,加重了 VLR/SGSN 的存储负担.另一方面,假如当 VLR/SGSN 与 HE/HLR 之间通信短时间阻塞且 VLR/SGSN 用来对 MS 认证的向量消耗完时,VLR/SGSN 就无法对 MS 实施认证.文献[5–7]研究了认证向量数组长度和 MS 离开原 VLR/SGSN 后,原 VLR/SGSN 保留认证向量的时间长度对网络信令流量的影响,然而并没有从根本上解决 VLR/SGSN 与 HE/HLR 之间的通信流量大和 VLR/SGSN 存储负担重等问题.文献[8,9,11]借鉴了文献[10]算法的思想,采用了临时密钥机制降低了网络信令流量,但是文献[8,9,12]中所提算法仍然存在上文提到的缺点.

(4) 采用一次性随机数,强有力地抵抗重放攻击.文献[14,16–18]采用了相同的机制来抵抗重放攻击,但是抵抗重放攻击依靠序列数 SQN,由此换来基于序列数 SQN 同步的 DoS 攻击.本文算法取消了序列数机制,采用了一次性随机数,能够强有力地抵抗重放攻击.

(5) 通信流量比较:为比较 AKA 协议及其他改进协议(指给出协议具体流程的算法)与本文算法在对系统通信流量上的影响,本文采用统一的数据度量.统一的数据度量即要求各个协议产生的加密密钥、完整性密钥和完整性校验值有相同的长度,本文对只给出协议算法流程但未给出参数长度的其他改进协议中的参数都按照 AKA 协议的标准来设定,即本文所作比较是在公平条件下的对比,具有可比性.本文算法采用的 IMSI 号码长度为 15 位十进制数(折合二进制,用 64 比特表示);IMSI 公钥加密后长度为 1 024 比特(本文采用 RSA 算法,为保证安全性,密钥长度取 1 024 比特);数字签名长度为 128 比特;AV 向量组的长度取 3GPP 建议值为 5.各种算法通信流量和存储容量对比如图 5~图 8 所示.

从图 5~图 8 中我们看到,本文提出的算法无论是在位置不变还是位置更新情况下,VLR/SGSN 与 HE/HLR 之间的流量以及 VLR/SGSN 的存储负担不随 VLR/SGSN 对 MS 认证次数的增加而线性增加,始终保持一个恒定值,从而大大降低了 VLR/SGSN 与 HE/HLR 之间的网络流量和 VLR/SGSN 的存储负担.虽然相比个别算法,本文算法的 VLR/SGSN 与 HE/HLR 之间要多传送些数据或 VLR/SGSN 要多存储些数据,但是本文算法能够抵抗各种攻击,极大地增强了系统的安全性.

(6) 公钥算法使用的影响:本文算法均采用 VLR/SGSN 用其私密钥 SK_{VLR} 对其发送数据作数字签名,HE/HLR 用 VLR/SGSN 的公钥 PK_{VLR} 对 VLR/SGSN 发送过来的数据作身份验证.其中,在位置更新情况下,MS 用 HE/HLR 的公钥 PK_{HLR} 对 IMSI 加密,HE/HLR 用其私密钥 SK_{HLR} 解密.本文算法均采用公钥算法自然会带来计算量的增加,但是由于本文算法有如下设计,会使得公钥算法的设计对网络的影响是轻量的:① 本文均采用了临时密钥机制,从根本上减轻了 VLR/SGSN 签名和 HE/HLR 验证签名带来的巨大计算量.因为采用临时密钥机制后,不是 MS 每次发起请求时都要求 VLR/SGSN 签名和 HE/HLR 验证签名,当且仅当 MS 初次进入某个 VLR/SGSN, VLR/SGSN 请求认证向量时才需要其签名和 HE/HLR 验证签名.假如 MS 始终处于特定 VLR/SGSN 内,无论随后 MS 发起多少次呼叫请求,随后的认证都是 VLR/SGSN 在临时密钥的辅助下独立完成对 MS 的认证,根本不需要通过 VLR/SGSN 签名和 HE/HLR 验证签名等计算量大的步骤来请求认证向量,从而彻底减轻了公钥算法计算量的影响;② 在位置更新情况下,本文算法的 MS 用 HE/HLR 的公钥 PK_{HLR} 对 IMSI 加密,HE/HLR 用其私密钥 SK_{HLR} 解密,这种情况当且仅当 MS 从原 VLR/SGSN 进入到新 VLR/SGSN 且新 VLR/SGSN 无法从

原 VLR/SGSN 获取 IMSI 时才需要用公钥加密传送.这样的情况是很少发生的,因此计算量增加也是轻量的;③公钥算法对呼叫时延的影响也是轻量的,因为 VLR/SGSN 签名请求认证向量,HE/HLR 验证签名分发向量不是发生在 MS 每次呼叫时,而只是发生在 MS 第一次进入 VLR/SGSN 时,随后对 MS 的认证都是 VLR/SGSN 在临时密钥的辅助下独立完成,不牵涉到公钥加密解密计算;④ 本文用公钥签名和加密都是对少量数据而言,数据量小,签名和加密的速度自然会大大提高;⑤ 公钥计算带给 MS 的计算量增加是可控的,采用基于 RSA 算法的签名技术,合理分配公私钥的长度来平衡 MS 和 HE/HLR 各自的计算量,使得公钥算法在 MS 上也能实用.与 3GPP AKA 协议和其他改进算法相比,虽然本文算法计算量有少量增加,但却能彻底抵抗各种恶意攻击,极大地提高了系统安全性.

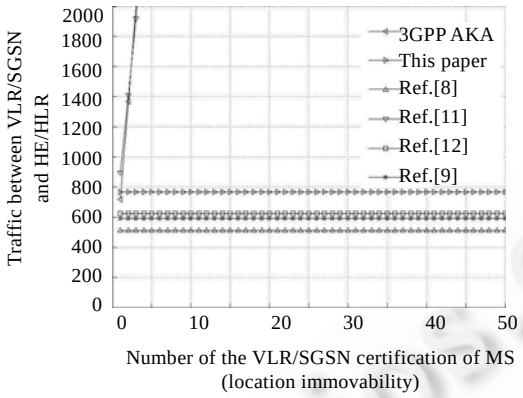


Fig.5 Traffic at location immovability

图 5 位置不变情况下的流量

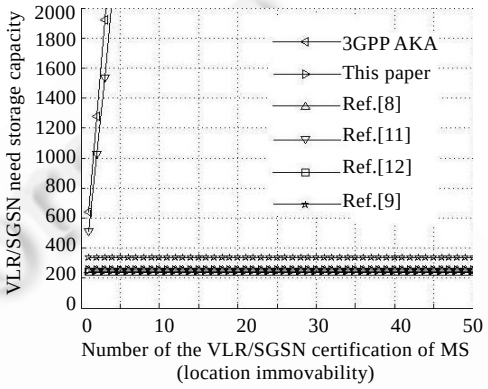


Fig.6 Memory capacity at location immovability

图 6 位置不变情况下的存储容量

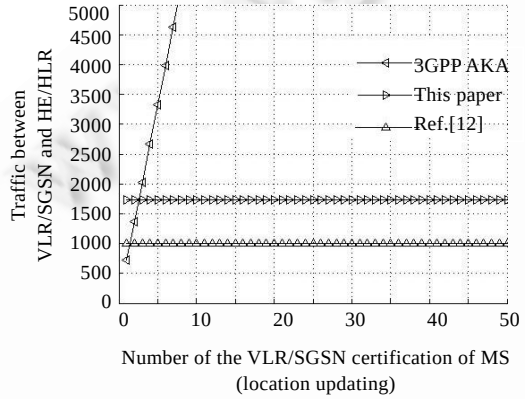


Fig.7 Traffic at location updating

图 7 位置更新情况下的流量

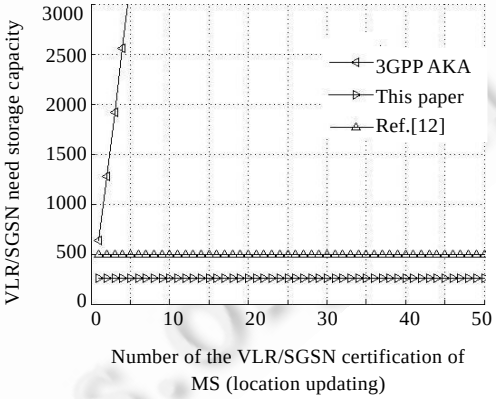


Fig.8 Memory capacity at location updating

图 8 位置更新情况下的存储容量

本文算法与已有算法优缺点比较总结见表 1.其中,序号 1 表示抵抗基于假 VLR/SGSN 的数据流重定向攻击;序号 2 表示抵抗基于假 VLR/SGSN 的串线诱骗攻击;序号 3 表抵抗 IMSI 标识被动截取攻击与诱骗主动截取攻击;序号 4 表示降低 VLR/SGSN 与 HE/HLR 之间的通信流量;序号 5 表示降低 VLR/SGSN 存储负担;序号 6 表示抵抗重放攻击;序号 7 表示抵抗基于序列数 *SQN* 同步的 DoS 攻击;序号 8 表示 HE/HLR 不是每次认证中都需要涉及.

Table 1 Summary of algorithms' advantages and disadvantages

表 1 各种算法优缺点比较总结

	This paper	Ref.[2]	Ref.[8]	Ref.[11]	Ref.[12]	Ref.[14]	Ref.[9]	Ref.[16]	Ref.[17]	Ref.[18]
1	Yes	No	No	Yes	Yes	No	No	Yes	No	No
2	Yes	No	No	No	No	No	No	No	No	No
3	Yes	No	No	No	Yes	Yes	No	No	Yes	No
4	Yes	No	Yes	No	Yes	No	Yes	No	No	No
5	Yes	No	Yes	No	Yes	No	Yes	No	No	No
6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No
8	Yes	No	Yes	No	Yes	No	Yes	No	No	No

6 总 结

本文提出的基于公钥密码学的安全认证与密钥协商协议取消了 AKA 协议中序列数 *SQN* 的同步,提高了系统的健壮性;采用公钥加密传送 IMSI,有效地抵抗了 IMSI 标识被动截取与主动诱骗截取攻击;采用数字签名加强了多个不同实体间的相互身份认证,彻底杜绝了基于假 VLR/SGSN 数据流重定向攻击与串线诱骗攻击.本文所提算法不仅安全性高,能够大大提高系统的健壮性,而且与 AKA 协议框架兼容性好,具有很强的实用性.

致谢 在此,我们向本文参考文献中的相关作者表示感谢,向对本文的工作给予支持和建议的同行,尤其是北京邮电大学网络与交换技术国家重点实验室信息安全中心、北京邮电大学灾备国家工程实验室、北京邮电大学网络与信息攻防教育部重点实验室对该论文做出过帮助的老师和同学表示感谢.

References:

[1] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects, 3G Security, Security Principles and Objectives. 3GPP TS 33.120 V3.0.0, 1999.

[2] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects, 3G Security, Security Architecture (Release 1999). 3GPP TS 33.102 V3.13.0, 2002.

[3] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects, 3G Security, Cryptographic Algorithm Requirements (Release 1999). 3GPP TS 33.105 V3.8.0, 2001.

[4] Information technology—Security techniques—Entity authentication—Part4: Mechanisms using a cryptographic check function. ISO/IEC9798-4.

[5] Lin YB, Chen YK. Reducing authentication signaling traffic in third-gerneraion mobile network. IEEE Trans. on Wireless Communications, 2003,2(3):493−501. [doi: 10.1109/TWC.2003.811171]

[6] Saraireh JA, Yousef S. Analyses authentication and key agreement protocol for UMTS mobile networks. In: Proc. of the 1st Int'l Conf. on Mobile Computing and Wireless Communication. Washington: IEEE Computer Society Press, 2006. 27−31.

[7] Wu LY, Lin YB. Authentication vector management for UMTS. IEEE Trans. on Wireless Communications, 2007,6(11):4101−4107. [doi: 10.1109/TWC.2007.060245]

[8] Huang CM, Li JW. Authentication and key agreement protocol for UMTS with low bandwidth consumption. In: Proc. of the 19th Int'l Conf. on Advanced Information Networking and Applications. Washington: IEEE Computer Society Press, 2005. 392−397.

[9] Saraireh JA, Yousef S. Extension of authentication and key agreement protocol (AKA) for universal mobile telecommunication system (UMTS). Int'l Journal of Theoretical and Applied Computer Sciences, 2006,1(1):109−118.

[10] Lee CC, Hwang MS, Yang WP. Extension of authentication protocol for GSM. IEE Proc. of Communications, 2003,150(2):91−95. [doi: 10.1049/ip-com:20030290]

[11] Zhang MX, Fang YG. Security analysis and enhancements of 3GPP authentication and key agreement protocol. IEEE Trans. on Wireless Communications, 2005,4(2):734−742. [doi: 10.1109/TWC.2004.842941]

[12] Juang WS, Wu JL. Efficient 3GPP authentication and key agreement with robust user privacy protection. In: Proc. of the IEEE Wireless Communications and Networking Conf. 2007. 2722−2727.

[13] Barbeau M, Robert JM. Perfect identity concealment in UMTS over radio access links. In: Proc. of the IEEE Int'l Conf. on Wireless and Mobile Computing, Networking and Communications. Washington: IEEE Computer Society Press, 2005. 72−77.

[14] Sattarzadeh B, Asadpour M, Jalili R. Improved user identity confidentiality for UMTS mobile networks. In: Proc. of the 4th European Conf. on Universal Multiservice Networks. Washington: IEEE Computer Society Press, 2007. 401−409.

[15] Bais A, Penzhorn WT, Palensky P. Evaluation of UMTS security architecture and services. In: Proc. of the IEEE Int'l Conf. on Industrial Informatics. Washington: IEEE Computer Society Press, 2006. 570−575.

[16] Jiang R, Li JH, Pan L. Formal analysis of 3GPP authentication and key agreement based on the strand space model. Journal of Shanghai Jiaotong University, 2006,40(5):791−795 (in Chinese with English abstract).

[17] Yuan YF, Lian YZ. Logic analysis of authentication key agreement protocol of 3G mobile communication. Journal of Information Engineering University, 2004,5(4):15−17 (in Chinese with English abstract).

[18] Liu F, Li DX. Amelioration of authentication and key agreement protocol in 3G. Computer Engineering and Design, 2006,27(14): 2705−2707 (in Chinese with English abstract).

[19] Yao HM, Sui AF, Yang YX. The designs for the 3GPP authentication and key generation functions. Journal of Beijing University of Posts and Telecommunications, 2002,25(3):98−102 (in Chinese with English abstract).

[20] Thayer FJ, Herzog JC, Guttman JD. Honest ideals on strand spaces. In: Proc. of the 11th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1998. 66−77.

[21] Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Why is a security protocols correct? In: Proc. of the '98 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998. 160−171.

[22] Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999,7(2-3): 191−230.

[23] Thayer FJ, Herzog JC, Guttman JD. Mixed strand spaces. In: Proc. of the 12th IEEE Computer Security Foundations Workshop. Washington: IEEE Computer Society Press, 1999. 72−82.

[24] Guttman JD, Thayer FJ. Authentications tests. In: Proc. of the 2000 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 2000. 96−109.

[25] Qing SH. A comparison between two formal analysis methods on authentication protocol. Journal of Software, 2003,14(12): 2028−2036 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/2028.htm

附中文参考文献:

[16] 蒋睿,李建华,潘丽.基于串空间的 3GPP 认证密钥交换协议分析.上海交通大学学报,2006,40(5):791−795.

[17] 袁亚飞,廉玉忠.3G 认证与密钥分发逻辑化分析.信息工程大学学报,2004,5(4):15−17.

[18] 刘峰,李大兴.3G 认证与密钥分配协议改进.计算机工程与设计,2006,27(14):2705−2707.

[19] 姚惠明,隋爱芬,杨义先.3GPP 网络 AKA 协议中若干算法的设计.北京邮电大学学报,2002,25(3):98-102.

[25] 卿斯汉.认证协议的两种形式化分析方法比较.软件学报,2003,14(12):2028−2036. http://www.jos.org.cn/1000-9825/14/2028.htm

陆峰(1982－),男,浙江湖州人,博士生,主要研究领域为网络与信息安全,移动通信安全,分布式系统.

杨义先(1961－),男,博士,教授,博士生导师,主要研究领域为网络与信息安全,密码学.

郑康锋(1975－),男,博士,讲师,主要研究领域为信息安全.

李忠献(1964－),男,博士,副研究员,主要研究领域为网络安全,信息安全.

钮心忻(1963－),女,博士,教授,博士生导师,主要研究领域为网络与信息安全,数字水印.