基于 AKA 的轻量级天地一体化网络终端接入认证方案

李 莉 马璐瑶 李秀滢
(北京电子科技学院 北京 100070)

摘 要 针对认证与密钥协商(AKA)协议接入认证方案中存在随机数明文传输、接入点存储成本过高和认证所需的比特通信量大等问题,提出一种轻量级的 AKA 协议加密接入认证方案。该方案用轻量级的密码算法 ZUC 加密需要传输的信息,调整信息传输的次序,引入哈希链技术,提高接入认证安全性的同时,减少了通信次数和存储负担,能够更好地适用于计算能力、存储空间、电功率等属性受限、信道带宽受限的天地一体化网络环境。

关键词 AKA 协议 接入认证 重认证 天地一体化

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.07.044

LIGHTWEIGHT SPACE-GROUND INTEGRATED NETWORK TERMINAL ACCESS AUTHENTICATION SCHEME BASED ON AKA

Li Li Ma Luyao Li Xiuying
(*Beijing Electronic Science and Technology Institute, Beijing 100070, China*)

Abstract In the view of the problems of plain text transmission of random numbers, high storage cost of access points and large amount of bit communication required for authentication in authentication and key agreement (AKA) protocol access authentication scheme, a lightweight AKA protocol encryption access authentication scheme is proposed. The scheme used a lightweight cryptographic algorithm ZUC to encrypt the information needed to be transmitted, adjusted the order of transmission, and introduced Hash chain technology, which improved the security of access authentication and reduced the communication times and storage burden. The scheme could be better applied to the space-ground integrated network environment with limited computing capacity, storage space, power and channel bandwidth.

Keywords AKA protocol Access authentication Re-authentication Space-ground integration

0 引 言

天地一体化网络密码服务包括网络基础密码服务、用户业务密码服务和私有网络密码服务,接入认证密码服务作为网络基础密码服务的一种,包括卫星用户终端接入网络时与接入网关进行的双向认证,以及接入网关、互联网关、星载设备、服务器等一体化网络基础设备的实体认证。在接入认证过程中,密码按需服务系统对认证信息进行加密并生成认证所需的参数元组[1-2]。

天地一体化网络由于卫星高速运转,终端接入认证对象的计算能力、存储空间、电功率及卫星信道带宽受限等特点,对接入认证方案提出了更高的要求,普通的加密认证在终端接入应用中受到极大限制。一些安全性强但开销大的密码算法无法适用,必须降低密码安全服务业务开销,采用计算复杂度低、存储量小的接入认证方案[3]。

1 相关研究

接入认证的目的是保证接入网络设备的可信,通过运用密码算法和协议进行身份认证、密钥分配等,从而实现授权用户间的安全信息传递。认证与密钥交换(AKA)协议是网络通信中应用最普遍的一种安全协议,常见的认证和密钥交换协议有互联网密钥交换

收稿日期:2020-12-26。国家重点研发计划项目(2017YFB0801803)。**李莉**,副教授,主研领域:网络与系统安全,嵌入式系统安全应用。**马璐瑶**,硕士生。**李秀滢**,副教授。

(IKE)协议、分布认证安全服务(DASS)协议、Kerberos 认证协议。

在接入认证架构的研究中,IEEE 802.1x 最早用于无线局域网的安全认证,由于移动路由易遭受黑客攻击,Park 等[4]针对 WLAN 中欺诈接入点 AP 攻击,提出使用 TPM 增强接入认证安全性。蒋华等[5]针对认证双方间的不平等以及控制帧和管理帧的明文传输问题,提出一种基于公钥密码体制的 802.1x 双向认证改进方案。Potthast 等[6]引入一种由可信第三方完成用户身份验证的接入方案,从而实现用户隐私的保护。继 Boneh 等[7]提出聚合签名概念后,多种无证书聚合签名方案陆续提出并用于接入认证,由于聚合签名方案通常基于双线性对映射,签名长度与签名数量线性相关,在常数配对情况下,签名长度较长,从而导致运算量过大,认证方案存在计算复杂、存储开销大、单向认证等问题。

天地一体化网络由于存在结构复杂、节点高度暴露、计算能力受限等特点,为保证安全对于接入认证的要求更高。Zheng 等[8]提出了一种在用户、网关和 NCC 三者之间进行的接入认证方案,强调网关的作用,实现了双向认证,减少 NCC 的计算负担,但由于加入了网关导致认证复杂度增加,额外增加了通信开销。胡志言等[9]提出一种基于软件定义网络(SDN)的天地一体化网络接入认证架构和方法,将层次分析法与逼近理想解的排序方法相结合提出一种接入点决策算法,并进行了仿真实现,但该研究处于初级阶段,部署与实现困难。薛开平等[10]提出了一种基于安全凭证(Token)与散列链相结合的接入认证方案,适用于天地一体化网络无缝切换和跨域漫游场景,同时支持用户在拜访域的计费,但其计费使用计费凭证证书实现,使得用户端与服务器端都需要对证书进行处理和存储。赵国锋等[11]提出一种基于双线性配对的天地一体化网络安全身份认证方案,认证过程无须第三方参与,可抵御多种攻击,但双线性对计算导致消耗与通信延时较大。

AKA 协议作为常用的安全协议,现如今被广泛应用于 5G 网络[12-13]、LTE[14](Long Term Evolution)网络等,AKA 协议向安全性更高、存储与计算消耗量更小的方向发展。许名松等[15]提出了 SE AKA 协议,利用公钥密码体制加密用户与服务网络的身份信息,引入了数字签名机制,抵御重定向攻击。Purkhiabani 等[16]提出了改进的 AKA 协议,通过 SN 和 HN 生成联合认证向量,减少了认证过程中的带宽消耗,在安全性上有所提高,但仍旧存在易遭受中间人攻击等问题。Hamandi 等[17]提出了 HSK-AKA 协议,引入了数字签名机制,并利用随机移动用户身份标识 RMSI(Random Mobile Subscriber Identity)机制保护 IMSI。Lu 等[18]提出了一种新型基于证书的 AKA 协议,此协议具有很高的安全性,可以抵抗公钥替换攻击。

本文将结合天地一体化对于接入认证的安全要求,对 AKA 协议依然存在随机数明文传输、接入点存储成本过高和认证所需的比特通信量大等问题进行优化,提出一种轻量级的 AKA 协议加密接入认证方案。

2 天地一体化网络终端接入认证架构

天地一体化网络的终端接入认证是指卫星用户终端在接入一体化网络时与接入点进行的双向认证,根据接入点的不同,终端接入认证可分为本地接入认证和漫游接入认证。本地接入认证为用户终端在注册登记地接入网络进行认证;漫游接入认证为用户终端在注册登记地之外接入网络进行认证。接入认证架构如图 1 所示。

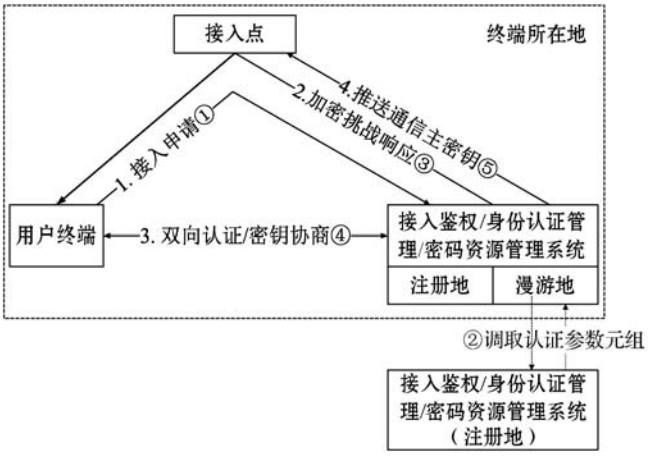

图 1 接入认证密码服务架构

步骤 1 用户终端将受保护的身份信息发送至接入鉴权系统,申请接入一体化网络。

步骤 2 接入鉴权系统将身份信息发送至身份认证管理系统,后者生成挑战信息,并利用从密码资源管理系统调取的用户终端根密钥对其进行加密并派生认证参数元组,对用户终端发送挑战响应。

步骤 3 用户终端利用自身根密钥将挑战信息解密,并利用认证参数元组完成和接入网络的双向认证。

步骤 4 用户终端和接入鉴权系统利用认证参数元组和交换的随机数生成通信主密钥,可衍生出接入网业务信息传输保护密钥和信令保护密钥。接入鉴权系统将通信主密钥推送至接入点。

漫游接入认证是在本地接入认证的基础上增加了接入鉴权系统根据身份信息寻址用户注册地网络,并从注册地网络身份认证管理系统调取受用户终端认证

密钥保护的挑战信息以及派生的认证参数元组,对用户终端发送挑战响应。

3　方案设计

3.1　加密接入全认证

基于 AKA 协议的加密接入全认证过程如图 2 所示,包括接入申请、用户认证、认证响应、网络认证四个环节。

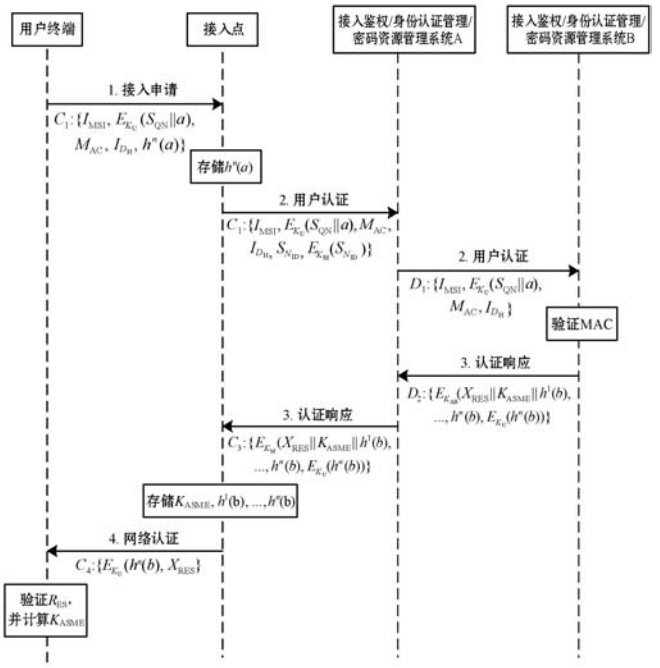

图 2　基于 AKA 协议的接入认证方案流程

步骤 1　接入申请。用户终端向接入点发送接入认证申请消息 $C_1=\{I_{\mathrm{MSI}},E_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a,M_{\mathrm{AC}},I_{D_{\mathrm{H}}},h^n(a)\}$,请求接入。其中:$I_{\mathrm{MSI}}$为用户识别码;$S_{\mathrm{QN}}$为认证序列号,用于避免重放攻击;$a$ 为随机数,用于密钥协商;K_{U}为用户终端根密钥,是用户终端和注册地接入鉴权系统/身份认证管理系统/密码资源管理系统(UIAM/PMS)共享秘密;M_{AC}为认证信息;$I_{D_{\mathrm{H}}}$为注册地 UIAM/PMS 的 ID;h 表示 Hash 运算,$h^n(a)$为随机数 a 经过 n 次哈希运算生成的哈希链 $h^1(a),h^2(a),\cdots,h^n(a)$的第 n 个哈希值,用于接入点对用户端的重认证。

(1) 生成随机数 a、S_{QN}。

(2) 计算 $E_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a)=ZUK_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a)$与 $M_{\mathrm{AC}}=f^1_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a\|A_{\mathrm{MF}})$,其中 A_{MF}为配置时保存的认证管理域参数。

(3) 随机数 a 做 n 次哈希运算得哈希链 $h^1(a),h^2(a),\cdots,h^n(a)$。

(4) 发送$\{I_{\mathrm{MSI}},E_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a,M_{\mathrm{AC}},I_{D_{\mathrm{H}}},h^n(a)\}$至接入点。

步骤 2　用户认证。接入点接收 C_1并存储用户终端发来的哈希值 $h^n(a)$,为重认证做准备;接入点向 UIAM/PMS 发送用户认证消息 $C_2=\{I_{\mathrm{MSI}},E_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a),M_{\mathrm{AC}},{}_{ID_{\mathrm{H}}},S_{N_{\mathrm{ID}}},E_{K_{\mathrm{M}}}(S_{N_{\mathrm{ID}}})\}$,其中:$S_{N_{\mathrm{ID}}}$为服务网络 ID;$K_{\mathrm{M}}$为接入点和注册地 UIAM/PMS 共享秘密。

步骤 3　认证响应。$(\mathrm{UIAM/PMS})_{\mathrm{A}}$ 接收 C_2并进行接入验证,若验证不通过,则向接入点发送验证失败消息;否则,发送认证响应消息 $C_3=\{E_{K_{\mathrm{M}}}(X_{\mathrm{RES}}\|K_{\mathrm{ASME}}\|h^1(b),h^2(b),\cdots,h^n(b)),E_{K_{\mathrm{U}}}(h^n(b))\}$至接入点。其中:$X_{\mathrm{RES}}$为认证信息;$K_{\mathrm{ASME}}$为通信主密钥;$b$ 为随机数,$h^1(b),h^2(b),\cdots,h^n(b)$为重认证中的接入点的哈希链。

(1) $(\mathrm{UIAM/PMS})_{\mathrm{A}}$ 接收 C_2并提取 $I_{D_{\mathrm{H}}}$,判断是否为自身 ID,若是,则在数据库中查找 I_{MSI},否则进入步骤(7)。

(2) $(\mathrm{UIAM/PMS})_{\mathrm{A}}$ 由 $S_{N_{\mathrm{ID}}}$获得 K_{M},解密 $E_{K_{\mathrm{M}}}(S_{N_{\mathrm{ID}}})$,并由解密出的 $S_{N_{\mathrm{ID}}}$验证接入点身份。

(3) $(\mathrm{UIAM/PMS})_{\mathrm{A}}$ 根据 I_{MSI}获得 K_{U},解密 $E_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a)$获得 $S_{\mathrm{QN}}\|a$。

(4) 计算 $X_{\mathrm{MAC}}=f^1_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|\alpha\|A_{\mathrm{MF}})$,验证 $X_{\mathrm{MAC}}?=M_{\mathrm{AC}}$,若相等,则用户认证通过,否则向接入点发送验证失败消息。

(5) $(\mathrm{UIAM/PMS})_{\mathrm{A}}$ 生成随机数 b,经过 n 次哈希运算得哈希链 $h^1(b),h^2(b),\cdots,h^n(b)$。

(6) 发送$\{E_{K_{\mathrm{M}}}(X_{\mathrm{RES}}\|K_{\mathrm{ASME}}\|h^1(b),h^2(b),\cdots,h^n(b)),E_{K_{\mathrm{U}}}(h^n(b))\}$至接入点。

$$X_{\mathrm{RES}}=f^2_{K_{\mathrm{U}}}(h^n(b)) \tag{1}$$

$$K_{\mathrm{ASME}}=KDF(f^3_{K_{\mathrm{U}}}(a\oplus h^n(b)),f^4_{K_{\mathrm{U}}}(a\oplus h^n(b))) \tag{2}$$

$$E_{K_{\mathrm{U}}}(h^n(b))=ZUK_{K_{\mathrm{U}}}(h^n(b)) \tag{3}$$

将通信主密钥 K_{ASME}和接入点在重认证中用于认证的哈希链 $h^1(b),h^2(b),\cdots,h^n(b)$加密发送是为了保护这两条信息不被除合法接入点之外的其他实体获取,给保密通信和本地重认证过程带来非法用户窃听消息、身份仿冒攻击等安全问题。X_{RES}为预期应答,用于用户验证接入点的合法性。$h^n(b)$由用户终端预置密钥加密,可以保证只有提出接入申请的用户终端才能解密获得 $h^n(b)$,以此来保证用于密钥协商的随机数 $h^n(b)$是安全有效的。

(7) $(\mathrm{UIAM/PMS})_{\mathrm{A}}$ 根据 $I_{D_{\mathrm{H}}}$,向用户终端本地 $(\mathrm{UIAM/PMS})_{\mathrm{B}}$ 发送漫游地用户认证消息 $D_1=\{I_{\mathrm{MSI}},E_{K_{\mathrm{U}}}(S_{\mathrm{QN}}\|a),M_{\mathrm{AC}},I_{D_{\mathrm{H}}}\}$。

(8) $(\mathrm{UIAM/PMS})_{\mathrm{B}}$ 验证 D_1中的认证信息 M_{AC},若验证不通过,则向 $(\mathrm{UIAM/PMS})_{\mathrm{A}}$ 发送认证失败消

息;否则,发送认证响应消息 $D_2=\{E_{K_{AB}}(X_{RES}\parallel K_{ASME}\parallel h^1(b),h^2(b),\cdots,h^n(b)),E_{K_U}(h^n(b))\}$。其中 K_{AB} 为$(UIAM/PMS)_A$ 和$(UIAM/PMS)_B$ 共享的密钥,用以保证认证信息 X_{RES} 和通信主密钥 K_{ASME} 的保密性。将随机数 b 经过用户终端预置密钥的加密,可以保证只有提出接入申请的用户终端才能解密获得随机数 b,以此来保证用于密钥协商的随机数 b 是安全有效的。

(9) $(UIAM/PMS)_A$ 解密 D_2 中的 $E_{K_{AB}}(X_{RES}\parallel K_{ASME}\parallel h^1(b),h^2(b),\cdots,h^n(b))$,进入步骤(6)。

步骤 4 网络认证。首先,接入点接收 C_3,在进行以下两步操作之后向用户终端发送网络认证信息 $C_4=\{E_{K_U}(h^n(b)),X_{RES}\}$。

(1) 对 $E_{K_M}(X_{RES}\parallel K_{ASME}\parallel h^1(b),h^2(b),\cdots,h^n(b))$ 进行解密,接入点存储用于重认证的哈希链 $h^1(b)$,$h^2(b),\cdots,h^n(b)$ 和通信主密钥 K_{ASME}。

(2) 提取 $E_{K_U}(h^n(b))$ 和 X_{RES},并发送至用户终端。

其次,用户终端接收 C_4 并进行以下 3 步完成网络认证。

(1) 解密 $E_{K_U}(h^n(b))$,获得并存储 $h^n(b)$。

(2) 计算 R_{ES}。

$$R_{ES}=f_{K_U}^2(h^n(b)) \tag{4}$$

判断 X_{RES} 是否等于 R_{ES}。若相等,则网络认证通过,进入下一步;若不相等则发送认证失败消息。

(3) 计算通信主密钥 $K_{ASME}=KDF(f_{K_U}^3(a\oplus h^n(b)),f_{K_U}^4(a\oplus h^n(b)))$ 该密钥与接入点保存的 K_{ASME} 一致,用户终端与接入点即可进行后续的保密通信。

3.2 接入重认证

基于 AKA 协议的加密接入认证方案实现了漫游接入重认证的本地化,本地/漫游接入重认证流程如图 3 所示。

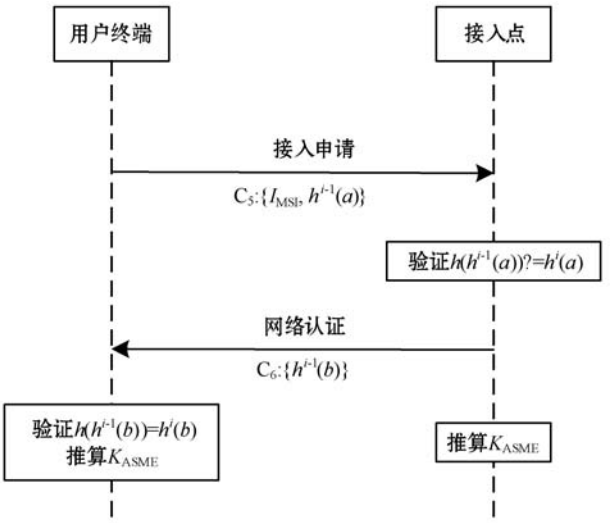

图 3 基于 AKA 协议加密接入重认证流程

步骤 1 用户终端向接入点发送接入申请信息 $C_5=\{I_{MSI},h^{i-1}(a)\}$,其中 $h^{i-1}(a)$ 为用户终端哈希链的第 $i-1$ 个哈希值,哈希值用于接入点对用户终端的认证。

步骤 2 接入点利用全认证过程中保存的 $h^i(a)$ 对用户终端接入申请中的 $h^{i-1}(a)$ 进行认证,若 $h(h^{i-1}(a))=h^i(a)$,认证成功,接入点向用户终端发送网络认证消息 $C_6=\{h^{i-1}(b)\}$;否则认证失败。

步骤 3 用户终端利用全认证过程中保存的 $h^i(b)$ 对接入点发送的 $h^i(b)$ 进行认证,若 $h(h^{i-1}(b))=h^i(b)$,认证成功;否则认证失败。

用户端和接入点分别计算获得通信主密钥 K_{ASME},通信主密钥由重认证哈希值和原通信主密钥生成,即:

$$K_{ASME}=KDF(K'_{ASME},h^{i-1}(a)\oplus h^{i-1}(b)) \tag{5}$$

4 性能分析

4.1 安全性分析

(1) 保护认证参数信息。在本加密接入认证方案中,用户接入端对用于计算消息认证码 M_{AC} 和通信主密钥 K_{ASME} 的随机数 a 进行了加密,同时 UIAM/PMS 将认证响应消息中的信息利用 ZUC 加密算法进行了加密,其中,R_{ES}、K_{ASME} 和重认证中接入点使用的哈希链使用接入点的密钥 K_M 进行加密,用于计算 R_{ES} 和通信主密钥 K_{ASME} 的随机数 b 利用用户的根密钥 K_U 进行加密,再由接入点将加密的随机数 b 传给用户。将认证参数信息进行加密,可以保证只有合法的用户才能将认证参数信息解密,完成双向认证。而非法用户无法将加密的认证参数信息解密,不能得到认证相关信息,就无法仿冒用户或接入点来进行接入认证。

(2) 用户与接入点实现双重认证。基于 AKA 协议的加密接入认证方案中对用户的认证是通过消息认证码 M_{AC} 完成的。UIAM/PMS 通过接入点发送给用户终端的随机数 b 是使用用户的根密钥 K_U 进行加密的,而随机数 b 是计算通信主密钥 K_{ASME} 的重要参数,因此只要用户可以计算出正确的通信主密钥,即代表用户成功解密加密后的随机数 b。由于只有合法的用户才有正确的 K_U,才可以成功解密利用 K_U 加密的信息,因此,只要可以成功计算出通信主密钥 K_{ASME} 就说明用户有正确的密钥,就可以再次认证用户身份的合法性。

接入鉴权/身份认证管理/密码资源管理系统发送给接入点的认证响应消息中的相关认证信息是经过接入点的密钥加密的,只要用户可以接收到接入点发送的正确的 X_{RES},即代表接入点成功解密认证响应消息。由于只有合法的接入点才有正确的 K_M,才可以成功解密

由 K_M 加密的信息,因此,只要用户收到正确的 X_{RES} 就代表接入点有正确的密钥,再次认证接入点的合法身份。

4.2　存储资源消耗分析

标准 AKA 协议加密认证方案中,接入点需要存储 n 组有序认证向量 $\boldsymbol{A}_V(1,2,\cdots,n)$,存储认证向量组所消耗的存储资源为 $576n$(bit)。基于 AKA 协议的加密接入认证方案中,接入点只需要存储自己用于重认证的哈希链 $h^1(a),h^2(a),\cdots,h^n(a)$ 和用户用于重认证的哈希链的第 n 个哈希值 $h^n(a)$,消耗的存储资源为 $160(n+1)$(bit)。存储资源消耗对比如图 4 所示。随着 n 的增大,基于 AKA 协议的加密接入认证方案在存储资源占有率方面的优势愈加明显,适用于更多用户的接入认证服务。

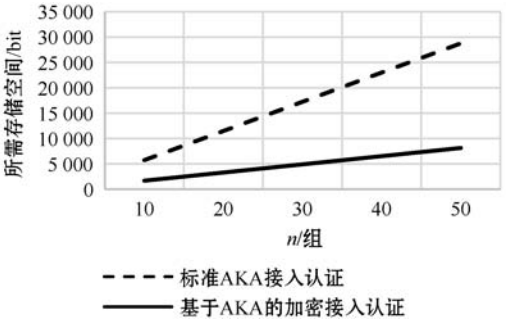

图 4　存储资源消耗对比

4.3　消息通信量分析

标准 AKA 协议接入认证方案中本地接入全认证需要进行 5 次信息传输,重认证需要进行 3 次信息传输,因此,进行 M 次认证的消息通信量为:

$$S(M,n)_A=\left\lceil\frac{M}{n}\right\rceil\times 5+\left(M-\left\lceil\frac{M}{n}\right\rceil\right)\times 3 \tag{6}$$

基于 AKA 协议的加密接入认证方案中本地接入全认证需要进行 4 次信息传输,重认证进行 2 次信息传输,因此,进行 M 次认证的消息通信量为:

$$S(M,n)_C=\left\lceil\frac{M}{n}\right\rceil\times 4+\left(M-\left\lceil\frac{M}{n}\right\rceil\right)\times 2 \tag{7}$$

可见基于 AKA 协议的加密接入认证方案的消息通信量小于标准 AKA 协议接入认证方案。在天地一体化网络环境中,减少消息通信量可以有效减少认证过程所占用的传输资源,将更多的传输资源用于其他密码服务工作。

4.4　比特通信量分析

标准 AKA 协议本地接入认证方案中传输消息的长度为:

$$|A_1|=|I_{MSI}|=128\ \text{bit} \tag{8}$$

$$|A_2|=|I_{MSI}|+|S_{N_{id}}|+\text{网络类型}=384\ \text{bit} \tag{9}$$

$$|A_3|=n\times|\boldsymbol{A}_V|=n\times(|R_{AND}|+|A_{UTN}|+|K_{ASME}|+|X_{RES}|)=576n\ \text{bit} \tag{10}$$

$$|A_4|=|R_{AND}|+|A_{UTN}|+|K_{SI_{ASME}}|=259\ \text{bit} \tag{11}$$

$$|A_5|=|X_{RES}|=64\ \text{bit} \tag{12}$$

式中:R_{AND} 为 128 bit 随机数;A_{UTN} 为 128 bit 认证令牌。

本地接入全认证的比特通信量 W_{A1} 为 5 条消息的总长度,即:

$$W_{A1}=\sum_{i=1}^{5}A_i=835+576n\ \text{bit} \tag{13}$$

重认证的比特通信量 W_{A2} 为 3 条消息的总长度,即:

$$W_{A2}=|A_1|+|A_4|+|A_5|=451\ \text{bit} \tag{14}$$

进行 M 次认证的比特通信量 $W_A(M,n)$:

$$W_A(M,n)=\left\lceil\frac{M}{n}\right\rceil\times W_{A1}+\left(M-\left\lceil\frac{M}{n}\right\rceil\right)\times W_{A2} \tag{15}$$

基于 AKA 协议的加密本地接入认证方案中传输的消息的长度为:

$$|C_1|=|I_{MSI}|+|a|+|S_{QN}|+|M_{AC}|+|I_{D_H}|+|h^n(a)|=656\ \text{bit} \tag{16}$$

$$|C_2|=|I_{MSI}|+|a|+|S_{QN}|+|M_{AC}|+|I_{D_H}|+2\times|S_{N_{ID}}|=752\ \text{bit} \tag{17}$$

$$|C_3|=|R_{ES}|+|K_{ASME}|+n\times|h^n(b)|=320+160n\ \text{bit} \tag{18}$$

$$|C_4|=|R_{ES}|+n\times|h^n(b)|=64+160n\ \text{bit} \tag{19}$$

$$|C_5|=|I_{MSI}|+|h^{i-1}(a)|=288\ \text{bit} \tag{20}$$

$$|C_6|=|h^{i-1}(b)|=160\ \text{bit} \tag{21}$$

本地接入全认证的比特通信量 W_{C1} 为:

$$W_{C1}=\sum_{i=1}^{4}C_i=1\ 792+320n\ \text{bit} \tag{22}$$

重认证的比特通信量 W_{C2} 为:

$$W_{C2}=|C_5|+|C_6|=448\ \text{bit} \tag{23}$$

进行 M 次认证的比特通信量 $W_C(M,n)$:

$$W_C(M,n)=\left\lceil\frac{M}{n}\right\rceil\times W_{C1}+\left(M-\left\lceil\frac{M}{n}\right\rceil\right)\times W_{C2} \tag{24}$$

$n=100$ 时,两种方案的本地接入认证比特通信量对比如图 5 所示,可见基于 AKA 的加密接入认证比特通信量少于标准 AKA 接入认证比特通信量,且随着认证次数的增加,优势逐渐加大。

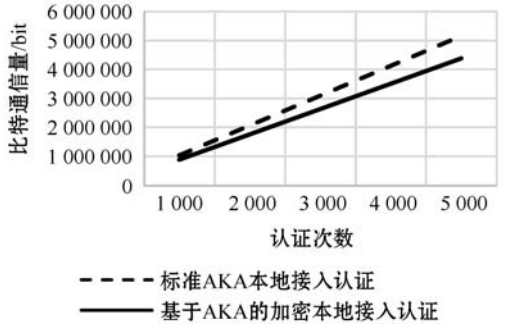

图 5　本地接入认证比特通信量对比

5 结 语

基于 AKA 协议的加密接入认证方案,通过用轻量级的密码算法加密需要传输的信息,调整信息传输的次序,减少通信次数来改进接入认证的全认证方案,用哈希链技术改进接入认证的重认证方案,减少了通信次数和接入点信息存储量,提高了本地接入认证全认证方案的安全性和效率。本方案能够更好地适用于终端计算能力、存储空间、电功率等属性受限、信道带宽受限的工作环境。

参 考 文 献

[1] 刘立祥. 天地一体化网络[M]. 北京:科学出版社,2015:2-3.

[2] 李凤华,殷丽华,吴巍,等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报,2016,37(11):156-168.

[3] 胡志言. 天地一体化网络统一接入认证关键技术研究[D]. 洛阳:战略支援部队信息工程大学,2018.

[4] Park K, Kim Y, Kim J. Security enhanced IEEE 802.1x authentication method for WLAN mobile router[C]//2012 14th International Conference on Advanced Communication Technology,2012:549-553.

[5] 蒋华,张乐乾,阮玲玲. 基于公钥密码体制的 802.1x 双向认证研究[J]. 计算机应用与软件,2016,33(2):290-293.

[6] Potthast M, Forler C, List E, et al. PASSPHONE: Outsourcing phone-based web authentication while protecting user privacy[C]//Nordic Conference on Secure IT Systems, 2016:235-255.

[7] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//International Conference on the Theory and Applications of Cryptographic Techniques,2003:416-432.

[8] Zheng G, Ma H, Cheng C, et al. Design and logical analysis on the access authentication scheme for satellite mobile communication networks[J]. IET Information Security,2012,6(1):6-13.

[9] 胡志言,杜学绘,曹利峰. 软件定义天地一体化网络接入认证架构与方法[J]. 计算机应用研究,2019,36(3):873-877.

[10] 薛开平,周焕城,孟薇,等. 天地一体化网络无缝切换和跨域漫游场景下的安全认证增强方案[J]. 通信学报,2019,40(6):138-147.

[11] 赵国锋,周文涛,徐川,等. 一种基于双线性配对的天地一体化网络安全身份认证方案[J]. 信息网络安全,2020,20(12):33-39.

[12] Hojjati M, Shafieinejad A, Yanikomeroglu H. A Blockchain-based authentication and key agreement (AKA) protocol for 5G networks[J]. IEEE Access,2020,8:216461-216476.

[13] 李晓红,刘福文,齐旻鹏,等. 基于 PKI 的 5G-DHAKA 协议安全性分析[J]. 网络空间安全,2019,10(11):64-73.

[14] Gupta S, Parne B, Chaudhari N. PSEH: A provably secure and efficient handover AKA protocol in LTE/LTE-A network[J]. Peer-to-Peer Networking and Applications,2019,12(4):989-1011.

[15] 许名松,李谢华,曹基宏,等. 一种安全增强型无线认证与密钥协商协议[J]. 计算机工程,2011,37(17):116-118,135.

[16] Purkhiabani M, Salahi A. Enhanced authentication and key agreement procedure of next generation evolved mobile networks[C]//2011 IEEE 3rd International Conference on Communication Software and Networks,2011:557-563.

[17] Hamandi K, Sarji I, Chehab A, et al. Privacy enhanced and computationally efficient HSK-AKA LTE scheme[C]//2013 27th International Conference on Advanced Information Networking and Applications Workshops,2013:929-934.

[18] Lu Y, Zhang Q, Li J. A certificate-based AKA protocol secure against public key replacement attacks[J]. International Arab Journal of Information Technology,2019,16(4):754-765.

(上接第 301 页)

[14] Moustafa N, Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)[C]//2015 Military Communications and Information Systems Conference,2015:1-6.

[15] Gregorio M, Giordano M. An experimental evaluation of weightless neural networks for multi-class classification[J]. Applied Soft Computing,2018,72:338-354.

[16] Moustafa N, Slay J. RCNF: Real-time collaborative network forensic scheme for evidence analysis[EB]. arXiv:1711.02824,2017.

[17] Khan F, Gumaei A, Derhab A, et al. A novel two-stage deep learning model for efficient network intrusion detection[J]. IEEE Access,2019,7:30373-30385.

[18] Yang Y, Zheng K, Wu C, et al. Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network[J]. Sensors,2019,19(11):2528.

[19] Binbusayyis A, Vaiyapuri T. Identifying and benchmarking key features for cyber intrusion detection: An ensemble approach[J]. IEEE Access,2019,7:106495-106513.