零信任体系架构的可跨域连续身份认证

李益发，孔雪曼，耿　宇，薛梦阳，陈　铎

(郑州大学 网络空间安全学院　河南 郑州 450002)

摘要：连续身份认证是零信任架构的核心，旨在确保通信和资源访问的安全性。传统身份认证方案存在一系列问题，比如依赖可信第三方、普适性差、中心化管理、高成本、低效率和缺乏隐私保护等。为了满足当前网络发展的需求，遵循“永不信任，始终验证”的零信任原则，提出了一种可跨域连续身份认证方案，利用统一多域标识和信道状态信息实现轻量级的连续认证和可跨域认证。通过安全协议分析本征逻辑方法对所提方案进行了正式分析，证明了其安全性，并展示了在零信任应用场景中的强大潜力。

关键词：连续身份认证；零信任；跨域认证；统一多域标识；信道状态信息

中图分类号：TN918　　**文献标志码**：A　　**文章编号**：1671-6841(2024)04-0041-07

DOI：10.13705/j.issn.1671-6841.2023035

Cross-domain Continuous Identity Authentication of Zero Trust Architecture

LI Yifa, KONG Xueman, GENG Yu, XUE Mengyang, CHEN Duo

(*School of Cyber Science and Engineering*, *Zhengzhou University*, *Zhengzhou* 450002, *China*)

Abstract: As the core of zero-trust architecture, continuous identity authentication aimed at ensuring the security of communication and resource access. There were series of problems with by traditional identity authentication schemes, such as reliance on trusted third parties, poor universality, centralized management, high costs, low efficiency, and lack of privacy protection. To meet the needs of current network development, a lightweight cross-domain continuous identity authentication scheme was proposed, with the principle of "never trust, always verify" of zero-trust. It utilizeal unified multi-domain identities and channel status information to achieve continuous and cross-domain authentication. The security of this scheme was formally analyzed through a secure protocol analysis intrinsic logic method. Results proved its security and its strong potential in zero-trust application scenarios.

Key words: continuous identity authentication; zero trust; cross-domain authentication; unified multi-domain identifty; channel state information

0　引言

零信任安全的理念基于重新构建访问控制的信任基础，这一基础依赖于身份认证和授权。该理念的目标是确保终端安全、链路安全和访问控制安全[1]。为了保证合法性，网络需要对所有发起访问请求的终端进行动态、连续的身份认证[2]。连续认证是指在一定时间段内建立安全通信会话，它是相互认证的补充，以确保在会话开始时被认证的设备始终保持不变[3]。由于异构应用系统使多样设备处在复杂的多域环境下，终端进行跨域认证的情况是不可忽略的。

密码技术是零信任安全体系建设中不可替代的

收稿日期：2023-02-08
基金项目：保密通信重点实验室基金项目(61421030107012102)。
第一作者：孔雪曼(1998—)，女，硕士研究生，主要从事物联网安全研究，E-mail：kongxm0115@163.com。
通信作者：李益发(1964—)，男，教授，主要从事物联网安全研究，E-mail：alphalyf@163.com。

核心技术,主要用于身份认证和加密通信。传统的静态身份认证难以满足零信任网络的需求。PKI/CA 体系[4-5]和基于身份的密码体制(IBC)[6-7]都存在一定的问题。近年来,许多研究致力于解决跨域认证[8-10]和连续认证[11-13]的问题,但同时满足轻量级可跨域和连续认证需求的研究较少。文献[13]提出的体系结构是目前很大程度上实现零信任架构中设备到设备(device-to-device,D2D)的连续认证协议,它主要应用于计算能力有限的物联网设备,可以很好地实现 D2D 的连续认证,但在跨域认证方面受到了应用场景的限制。

本文提出了一种基于统一多域标识[14](unified multi-domain identity, UMI)和信道状态信息[15](channel state information,CSI)的轻量级可跨域的连续认证协议,该协议实现了低时延跨域认证,并在相互认证阶段结束后使用由 CSI 生成的动态会话密钥进行连续认证,并结合动态函数定期更新密钥,确保连续身份验证的动态功能,满足零信任架构中身份认证的要求。最后,采用基于数理逻辑的本征逻辑分析方法对本文提出的协议进行正式分析,并证明了协议的安全性。

1 相关知识

1.1 基于统一多域标识(UMI)的认证

UMI 技术具有以下四个特点。

(1) 基于轻量级密码算法,适用面广。

(2) 不使用证书(方案中使用的公钥是无需证书的)。

(3) 用户(主机或实体)的公钥与其身份标识存在对应或绑定关系,但不同于基于身份的密码体制。

(4) 可实现多域的域内认证、跨域认证等,且认证时延较小,创新性地给出了新的公钥管理和全域认证方案。

UMI 技术可以通过基于标识映射公钥、标识绑定公钥和全域认证三个部分实现。

1.1.1 基于标识映射公钥技术 主要包含以下四个方面的内容。

(1) 提出统一多域标识,每个不同的标识可以拥有公、私钥对。标识至少包含两段:前段为域的标识;后段为域内实体(包括用户、设备等)的标识。

(2) 将公钥管理分为域内和域间两层架构,如图 1 所示。第一层实现根密钥管理中心(root key management center,RKMC)管理子域实体,域标识私钥由 RKMC 生成,第二层为子域密钥管理中心(domain key management center,DKMC),管理域内节点。

(3) 由 RKMC 生成一组公钥基(base consisting of PK factors,BPK),含有 r 个公钥,记 $BPK=\{bpk_1, bpk_2,\cdots,bpk_r\}$。与 BPK 对应的有一组私钥基(base consisting of SK factors, BSK),记 $BSK=\{bsk_1, bsk_2,\cdots,bsk_r\}$。这里 bpk_i 与 bsk_i 构成椭圆曲线加密算法中的密钥对,即 $bpk_i=bsk_iG$,其中 G 为椭圆曲线上的一个基点。私钥基是安全体系的核心敏感参数,公钥基是系统内的公开参数。

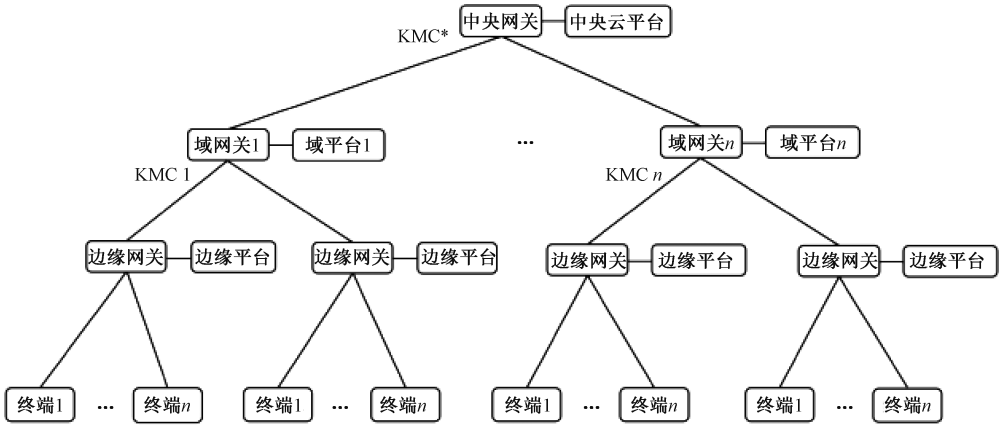

图 1 两层公钥管理架构

Figure 1 Two-tier public key management architecture

(4) 先由 RKMC 负责为每个域(包括根域)分发域私钥,域公钥可由公钥基和域的标识计算出来。在给定的公开公钥基下,域的公钥是唯一确定且在任一拥有公钥基的节点均可查询计算的。

1.1.2 标识绑定公钥技术 每个域对于其管辖内的所有节点,配合或代为生成公、私钥对。节点私钥既可由 DKMC 统一生成并分发,也可由节点和 DKMC 协同生成。协同生成时,终端私钥只有终端拥有。

1.1.3 全域认证技术 全域内节点均拥有唯一的

标识,即统一标识,并拥有自己的伴随公钥。统一标识至少包含域标识 k bit 和域内标识 l bit 两个部分,长度为($k+l$)bit。

设 A、B 为全域内的两个节点,A 与 B 的标识、伴随公钥和私钥分别是 ID_A、ID_B、apk_A、apk_B、sk_A 和 sk_B,则 A 与 B 间的双向统一强认证(指使用基于非对称算法的数字签名进行认证)协议如下:

$A \rightarrow B$: ID_B, M_A, ID_A, apk_A, $*ET_A$, S_A;

$B \rightarrow A$: ID_A, M_B, ID_B, apk_B, $*ET_B$, S_B。

$A \rightarrow B$ 表示 A 向 B 发送信息;$*ET_A$ 是有效期;M_A 是 A 发送给 B 需要认证的数据;$S_A = \mathrm{Sig}(sk_A, H(ID_B \| M_A))$ 是认证码,即使用数字签名 Sig 函数签名的值,签名内容为 ID_B 和 M_A 的哈希值,即 $H(ID_B \| M_A)$。

假设 A、B 不在同一子域内,A 位于域 D_1,A 标识的前 k 位是域 D_1 的标识 ID_{D_1}。B 位于域 D_N 内,B 标识的前 k 位是域 D_N 的标识 ID_{D_N}。而 A 与 B 都在本地存储着全域相同的公钥基 $BPK = \{bpk_1, bpk_2, \cdots, bpk_r\}$。当 B 收到 A 发送的消息 ID_B、M_A、ID_A、apk_A、$*ET_A$、S_A 时,B 先通过存储在本地的公钥基来计算域 D_1 的公钥 pk_1[14]。然后,B 再用 pk_1、ID_A、apk_A、$*ET_A$ 计算 A 的公钥 pk_A,用 pk_A 验证 A 的签名 S_A,若验证通过,表示 A 合法,反之,A 不合法;同理,A 使用同样的方法验证 B 的身份。

A 与 B 之所以能跨域认证,其重要的创新性基于全域有相同的公钥基,尽管 A 与 B 不在同一个域,但却可以用公钥基计算对方域的域公钥,并计算出对方的公钥进行身份认证。同一域的两个节点之间认证更加简单,利用自身的域公钥计算对方公钥即可进行身份认证。

1.2　信道状态信息(CSI)

安全协议需要前向保密和抵御设备模拟攻击。使用安全密钥并确保其始终安全更改是关键。此外,不可复制的独特设备功能对安全身份验证至关重要。设备指纹识别方法[16-17]可实现设备的连续认证,但大多需要额外硬件或容易受到攻击。基于通道状态信息(channel state information,CSI)的设备指纹识别方法,无需额外硬件且安全,取得了可喜成果[18-19]。

CSI 以精细的粒度(子载波级别)指示通信信道特性,包括多径传播、散射和衰落等,其值受到通信路径上各种障碍物和物体的影响,为不同位置生成唯一值。CSI 计算无需其他硬件,只需商用硬件中的网络接口卡 NIC。使用 CSI 生成动态会话密钥有几个优点:测量值会随着通信路径的变化而变化;不能预测并仅取决于信道物理特性,且无需额外硬件。

可跨域的连续身份认证协议利用 CSI 制作会话密钥进行有效连续身份验证,相较其他方法,计算成本低且无需第三方应用支持。

2　可跨域的连续身份认证协议

2.1　协议基础和符号

可跨域的连续身份认证协议在以下基础上实现:假设初始化阶段在安全环境下完成,并且通过交换的密钥和标识符被视为安全的;可以在零信任网络中的任何设备之间发生通信。最后,协议可针对企业、医院等场景进行定制。表 1 中给出了用于该协议的符号说明。

表 1　协议符号说明

Table 1　Protocol symbol description

符号	说明
A、B	终端设备
ID_A	A 的标识 ID
apk_A	A 的伴随公钥
S_A	A 的认证码
r	随机数
C_i	从设备发送的数据包中测量的通道状态信息
$\oplus$	按位异或运算符
$H(\cdot)$	单向哈希函数
T	设置的会话连续时间
M_i	第 i 个中间消息
t_m	相互认证阶段结束时的时间戳
t_c	连续认证阶段的时间戳
Ctr_e、Ctr_g	计数器值
f	用于连续认证阶段线性或非线性函数
SN_{key}	用于连续认证的会话密钥

2.2　协议的可行性分析

相互认证和连续认证的联合被视为当前零信任架构概念的重要组成部分[20]。一般来说,相互认证阶段容易实现,但随着网络环境不断变化并更为复杂,网络交流也变得错综复杂,因此在相互认证过程中,跨域认证功能显得不可或缺。然而,大多数连续身份认证协议并没有考虑跨域身份认证需求。有希望解决主体之间跨域认证问题的 UMI 技术已经问世,为零信任架构带来了新的可能。

连续性意味着在某一时间段内建立安全通信会话(会话连续时间为 T)。原则上它补充了相互认证阶段,以确保会话开始时被认证的设备始终保持不变,称其为连续认证。利用函数动态变化的功能和

上下文 CSI 制作的密钥进行保护。采用 $f=t^a+t^b$ 函数形式,其中:t 是时间戳的差异;a 和 b 是设备设置的指数。此函数满足连续验证的要求,因为它可以通过 a、b 的变化来改变,且对于一组固定的 a 和 b,其值会随时间变化而改变。

会话连续时间 T 表示系统设置的会话密钥只在 T 秒内有效。T 值可根据实际需求设置。当然,T 值越小,安全性越高,代价越大;相反,T 值越大,安全性会降低,代价越小。

本文协议使用设备的 CSI 和动态变化的共享密钥来实现连续身份认证。在连续认证阶段开始时,两个设备安全地交换相同的值,并使用线性或非线性函数,该函数的指数被限制在特定范围内,以确保其可以在受约束的设备上进行计算。针对每个新会话,指数会动态变化以使功能不受损害,且取值与设备资源限制一致。在连续认证阶段,指数和函数值使用基于每个设备的 CSI 动态会话密钥 SN_{key} 安全交换,从而使其不被妥协。最后,该协议还使用时间戳和本地计数器在两个设备上提高协议的安全性。

2.3 详细设计

协议包括三个阶段,以主体 A 和 B 之间的通信认证为例描述协议的过程(此时假设主体 A、B 不在一个域内,若 A、B 在一个域内,忽略计算对方域公钥步骤即可),这里的主体 A 和 B 可以是需要通信的用户、访问主体与网关或需要通信的设备等,协议可以广泛地应用于需要零信任网络的场景,比如医院、企业、国家保密单位等。

(1) 初始化阶段。在系统初始化阶段,会进行以下步骤。首先,注册设备并将系统的公钥基存储到设备中。该公钥基与系统的私钥基相对应,后者是系统的私密参数,由根密钥管理中心安全地存储和使用,禁止外部访问。接着,系统根据 UMI 技术原则为每个设备生成全域唯一的标识、公私钥对及节点的伴随公钥,这些信息用于相互认证。这些唯一的标识和公私钥对可以确保设备之间的身份验证和数据传输的安全性。同时,节点的伴随公钥也可以用于相互认证,确保系统中的通信是双向认证的。

(2) 相互认证阶段。① $A\rightarrow B:ID_A,ID_B,apk_A,S_A,r_A$;② $B\rightarrow A:ID_B,ID_A,apk_B,S_B,r_B$;③ $A\rightarrow B:M_1$;④ $B\rightarrow A:M_2$。

在上述场景中,ID_A 和 ID_B 分别代表主体 A 和 B 的标识,$S_A=\text{Sig}(sk_A,H(ID_B\parallel r_A))$ 表示 A 的数字签名值,其中:sk_A 为 A 的私钥;H 为哈希函数;r_A 为 A 生成的随机数。同理,$S_B=\text{Sig}(sk_B,H(ID_A\parallel r_B))$ 表示 B 的数字签名值,其中:sk_B 为 B 的私钥;r_B 为 B 生成的随机数。

$M_1=pk_B(C_r,r_B)$ 表示 A 向 B 发送的数据包,其中 C_r 为 A 测量的从 B 发送的数据包中的信道状态信息。$M_2=pk_A(C_i,r_A))$ 表示 B 向 A 发送的数据包,其中 C_i 为 B 测量的从 A 发送的数据包中的信道状态信息。

A 和 B 使用强认证方式(使用非对称密钥算法认证)确认对方身份。首先,A 生成随机数 r_A,并将 r_A、ID_A、ID_B、apk_A 和 S_A 发送给 B,B 收到信息后验证 S_A 的签名值,根据 A 的标识求出 A 所在域的公钥 pk_1,用 pk_1 求出 A 的公钥 pk_A,并用 pk_A 解密 S_A 进行验证($ID_B\parallel r_A$)的哈希值,验证通过则证明 A 身份合法。接着,B 生成随机数 r_B,并将 r_B、ID_B、ID_A、apk_B 和 S_B 发送给 A,A 收到信息后对数字签名值进行验证,验证过程与 B 验证 A 相同。

若认证成功,主体 A 生成从主体 B 发送的数据包中测量的信道状态信息 C_r,主体 B 生成从主体 A 发送的数据包中测量的信道状态信息 C_i。双方使用公私钥对将 C_i 和 C_r 进行安全交换。主体 A 计算 $M_1=pk_B(C_r,r_B)$,并将其发送给主体 B。主体 B 收到 M_1 后,使用私钥 sk_B 解密,得到 C_i 和 r_B,若 r_B 正确,则证明消息在传输过程中没有被篡改,得到的信道状态信息 C_i 准确无误,此时设置主体 A 的计数器 $Ctr_g=1$。接着主体 B 计算 $M_2=pk_A(C_i,r_A)$,并将其发送给主体 A,主体 A 收到 M_2 后,使用私钥 sk_A 解密,得到 C_r 和 r_A。同样,若 r_A 正确,则证明消息在传输过程中没有被篡改,得到的信道状态信息 C_r 准确无误,此时设置主体 B 的计数器 $Ctr_e=1$,并为了避免重放攻击,设置一个用于表示协议传输中确认收到正确的标识 A_K,$A_K=1$ 表示确认收到数据。会话密钥 $SN_{\text{key}}=C_i\oplus C_r$。主体 A 设置会话连续时间 T 和时间戳 t_m。

(3) 持续认证阶段。① $A\rightarrow B:M_3=SN_{\text{key}}(m_a,ID_A)$;② $B\rightarrow A:M_4=SN_{\text{key}}(A_K,f',a,t,m_b,Ctr_g)$;③ $A\rightarrow B:M_5=SN_{\text{key}}(f',Ctr_e)$。

第一步,A 会随机选择一个指数值 a,计算 $m_a=a\oplus(SN_{\text{key}}\oplus r_B)$,其中 SN_{key} 和 r_B 是通过安全通道交换的会话密钥和随机数。然后,A 使用会话密钥 SN_{key} 对 m_a 进行加密,并将 $M_3=SN_{\text{key}}(m_a,ID_A)$ 发送给 B。

在收到 M_3 消息后,B 使用 SN_{key} 对其进行解密,以获取 ID_A 和 m_a 的值。接下来,B 计算指数 a。同时,B 也会记录当前的时间戳 t_c,并将其与在相互身份验证阶段设置的时间戳 t_m 进行比较。如果时间戳的差值大于会话持续时间 T,B 将 ACK 值设置

为 0,以触发相互认证阶段。

第二步,若时间戳 t_c 和 t_m 之间的差异小于等于 T,则 B 继续随机生成第二个指数 b,计算 $m_b = b \oplus H(SN_{key} \oplus r_A)$,并计算出 $f = t^a + t^b$,将本地计数器 Ctr_g 的值加 1。随后,B 使用 SN_{key} 加密 A_K、f、t、a、m_b 和 Ctr_g,并将 M_4 发送回 A。A 解密 M_4 并查看 A_K 的值,如果值为 0,则表示双方身份已经互相认证,如果 A_K 值不为 0,则 A 检查 B 发回的指数 a 是否与之前发送的相同,这确保了消息 M_4 来自 A。通过使用动态上下文相关会话密钥 SN_{key} 交换指数 a 的 B。此外,A 还检查本地计数器的值以及 B 发送的值,以确保以正确的顺序接收消息。A 通过从接收到的消息 M_4 中检索 m_b 来获得指数 b,并通过检索 a 和 b 的值在本地计算 f 的值 f',然后将其与从接收到的值进行比较。这些值的正确匹配确保 A 正在与其安全交换指数 a 的同一 B 通信。

第三步,A 将 $M_5 = SN_{key}(f', Ctr_e)$ 发送给 B。B 收到 M_5 后进行解密,验证 f' 是否与 f 相同,并且与计数器值匹配。如果这些参数都被验证通过,则返回生成指数 a 点之后的时间戳 t_c。继续将 t_c 与 t_m 进行比较,以验证其差异是否在会话时间 T 内。

3　安全性分析

3.1　一般性分析

(1) 相互身份认证。相互认证指两个通信方的身份认证过程。在这个阶段,B 通过 A 发送的信息来验证 A 的身份。B 使用 A 的公钥来验证数字签名,如果验证通过,则表明数字签名的私钥属于 A。这足以证明数字签名是由 A 创建的,并且可以确认 A 的身份。同样地,A 也可以在此阶段确认 B 的身份。

在连续认证阶段,A 和 B 使用与时间相关的线性或非线性函数相互认证。这些函数的指数值是由两个设备使用新生成的动态会话密钥安全地设置,因此只有两个合法设备才能进行通信。此外,它们还利用计数器来验证从彼此接收到的消息的序列。因此,该协议实现了两个阶段的相互认证。

(2) 数据完整性。数据完整性确保发送的消息在传输过程中未被更改。我们的协议采用 UMI 认证方案,在相互认证阶段,CSI 由两个设备计算,使攻击者难以更改。此外,剩余的消息也使用安全的公私钥对进行加密,并使用从 CSI 生成的密钥 SN_{key} 加密。由于连续阶段的密钥在 T 时间后会发生变化,攻击者也难以成功更改传递的消息。因此,我们的协议满足数据完整性的属性。

(3) 重放攻击。重放攻击中,对手窃听并重放传输的消息,以冒充合法设备。在相互认证阶段,生成并采用新的随机数和 CSI 可保证先前记录的消息不违反安全属性。在连续认证阶段,时间相关的函数值和计数器值可抵抗重放攻击。由于使用了新的 SN_{key} 值,因此无法在其他设备上解密先前记录的消息 M_3 或 M_4。消息 M_4 和 M_5 只能在有效会话中重放,否则将没有匹配的计数器值,从而无法成功进行任何重放攻击。

(4) 冒充攻击。在相互认证阶段,冒充设备无法生成密钥 SN_{key},因为只能根据对方发送的消息随机生成 C_i 和 C_r 值。在连续认证阶段,攻击者需要知道会话密钥 SN_{key} 和线性/非线性函数的指数,但由于这些都是动态变化的,攻击将被阻止。会话密钥和指数的有效期均有限,不会对整个设备生命周期内的安全属性构成威胁。

(5) 拒绝服务攻击。若入侵者成功拦截了合法主体发送的消息,同时阻止了发送者,使其消息无法到达预期的接收者。在相互认证阶段,入侵者无法成功进行拦截和阻止攻击,因为无法计算 C_i 和 C_r 的值完成认证。在连续认证阶段,攻击者拦截消息并发送给接收方,但无法解密响应消息 M_4,因为无法获取 SN_{key}。这种攻击不会导致任何与消息同步相关的安全漏洞。

3.2　形式化分析

使用安全协议分析本征逻辑(security protocol analysis latent logic,SPALL[21])方法对协议的安全性进行分析。首先,相互认证阶段的协议过程如下。

(1) $A \rightarrow B: ID_A, ID_B, apk_A, S_A, r_A$。

(2) $B \rightarrow A: ID_B, ID_A, apk_B, S_B, r_B$。

(3) $A \rightarrow B: M_1 = pk_B(C_r, r_B)$。

(4) $A \rightarrow B: M_2 = pk_A(C_i, r_A)$。

① 对协议的分析。协议消息可区分性分析,协议中只有几个极简单的消息,不存在不可区分的消息。用 SPALL 方法对本协议进行分析。记 $\Gamma = \{A, B\}$,A、$B \in \Omega$,Ω 是主机集合,协议的目标如下。

相互认证阶段的目的是 A、B 完成相互认证并生成会话密钥 SN_{key},故该阶段要保证 SN_{key} 的安全性。满足以下四个条件:第一,$\Gamma \mid \equiv SN_{key} \in \Sigma$,其中 Σ 表示密码系统中有意义的消息集合,当满足上述条件时说明 A、B 相信 SN_{key} 是有意义的消息;第二,$\Gamma \mid \equiv \#(SN_{key})$,$A$、$B$ 相信 SN_{key} 是新鲜的;第三,$\Gamma \mid \equiv \Diamond(SN_{key})$,$A$、$B$ 相信 SN_{key} 在传递过程中是双向可追溯的;第四,$\Gamma \mid \equiv \Gamma \mid \backsim SN_{key}$,$A$、$B$ 相信

有且仅有双方看到 SN_{key}。$SN_{key}=C_i \oplus C_r$，故 C_i 和 C_r 是生成会话密钥的关键参数，同时还要求 $\Gamma \mid \equiv \#(C_i)$，$\Gamma \mid \equiv \#(C_r)$，$\Gamma \mid \equiv \Diamond(C_i)$，$\Gamma \mid \equiv \Diamond(C_r)$。

由协议内容可知，协议消息集 $\Sigma^+=\{ID_A, ID_B, apk_A, apk_B, S_A, S_B, r_A, r_B, M_1, M_2\}$。

由协议背景可以设 $A \ni S_A$，$B \ni S_B$，$A \ni r_A$，$B \ni r_B$，$A \ni C_r$，$B \ni C_i$，$A \ni M_1$，$B \ni M_2$。即 A 生成了 S_A、r_A、C_r、M_1，r_A 是一个随机数，B 生成了 S_B、r_B、C_i、M_2，r_B 是一个随机数。$A \mid \equiv A \mid \trianglelefteq apk_A$，$B \mid \equiv B \mid \trianglelefteq apk_B$，$sk_A$、$sk_B$ 属于非对称密码体制中的私钥。此外，对 A 来说，C_i 为一个随机数，需假设 $A \lhd C_i \rightarrow A \mid \equiv C_i \in \Sigma$，即当 A 看见 C_i 时，把它当作有意义的消息；对 B 来说，C_r 形同一个随机数，需要假设 $B \lhd C_r \rightarrow B \mid \equiv C_r \in \Sigma$。

② 对协议的目标分析。使用 UMI 技术进行身份认证，apk_A、sk_A 和 apk_B、sk_B 分别属于 A 和 B 的私有资源。A 使用 apk_A 和 sk_A 进行签名后向 B 发送消息，B 可以通过验证签名确认该消息确实来自 A，而不是被其他人伪造的。此外，消息中还包含有 B 的标识，表明该消息是 A 发送给 B 的，因此 B 可以确认 A 是其意图的通信对象，从而确认 A 的身份合法。同样地，A 也可以通过验证消息中的 B 标识确认 B 的身份合法。

因为 sk_A 是一个私钥，且 $\Gamma \mid \equiv A \mid \trianglelefteq sk_A$，所以 $\Gamma \mid \equiv A \ni S_A$，而 $S_A=\mathrm{Sig}(sk_A, H(ID_B \parallel r_A))$，即 $A \mid \sim ID_B$，故 $B \mid \equiv A \Rightarrow B$。即 B 可以确认来自 A 的消息是双向可追溯的，用 A 的公钥 pk_A 验证签名确认 A 的身份；同理 A 也可确认 B 的身份。

因 $A \ni C_r$，$A \ni r_A$，$B \ni r_B$，所以 $A \mid \equiv \#C_r$，$B \mid \equiv \#r_B$，$M_1=pk_B(C_r, r_B)$，故 $\Gamma \mid \equiv \#(M_1)$，$\Gamma \mid \equiv \#(C_r)$。同理可证 $\Gamma \mid \equiv \#(M_2)$，$\Gamma \mid \equiv \#(C_i)$。

因 $A \ni C_r$，$B \ni C_i$，$A \mid \equiv A \mid \trianglelefteq sk_A$，$B \mid \equiv B \mid \trianglelefteq sk_B$，$M_1=pk_B(C_i, r_B)$，$M_2=pk_A(C_r, r_A)$，故 $A \mid \equiv \Gamma \mid \trianglelefteq C_r$，$B \mid \equiv \Gamma \mid \trianglelefteq C_i$，又因在 A 发送的消息中包含有随机数 r_B，$B \mid \equiv A \Rightarrow B$，所以 $B \mid \equiv \Gamma \mid \trianglelefteq C_r$，同理 $A \mid \equiv \Gamma \mid \trianglelefteq C_i$。

综上可知，$\Gamma \mid \equiv \#(C_r)$，$\Gamma \mid \equiv \#(Ci)$，$\Gamma \mid \equiv \Diamond C_r$，$\Gamma \mid \equiv \Diamond C_i$。

因 $A \lhd C_i \rightarrow A \mid \equiv C_i \in \Sigma$，故有 $A \mid \equiv C_i \in \Sigma$，$A \mid \equiv C_r \in \Sigma$，故 $A \mid \equiv SN_{key} \in \Sigma$；同理可得 $B \mid \equiv SN_{key} \in \Sigma$。

因 $A \ni C_r$，$A \mid \equiv \#C_r$，$SN_{key}=C_i \oplus C_r$，所以 $A \mid \equiv \#SN_{key}$；同理 $B \mid \equiv \#SN_{key}$。

因 $\Gamma \mid \equiv \Diamond C_r$，$\Gamma \mid \equiv \Diamond C_i$，所以 $\Gamma \mid \equiv \Diamond SN_{key}$，而且 $B \mid \equiv \Gamma \mid \trianglelefteq C_r$，$A \mid \equiv \Gamma \mid \trianglelefteq C_i$，故 $\Gamma \mid \equiv \Gamma \mid \trianglelefteq SN_{key}$。

综上所述，相互认证阶段，证明了会话密钥 SN_{key} 满足安全性的条件。连续认证阶段的协议是基于 SN_{key} 和动态变换函数 $f=t^a+t^b$ 的，即使是对于固定的指数 a、b，函数也会随着时间的变化而改变，所以攻击者不太可能会获得加密的过程信息 M_3、M_4 和 M_5，而且也不能轻易被冒充，所以连续认证阶段在 T 时间段内是安全的。

4 结语

本文基于一种连续身份验证协议，使用 UMI 技术实现了跨域认证功能，设计了一种轻量级的可跨域连续身份认证协议，旨在为企业、医院等大型通信系统提供一种身份认证方法，从传统的边界安全防护转变为零信任网络防护。该协议定义了相互认证和连续认证阶段，其中包括基于 UMI 的跨域认证和利用信道状态信息动态密钥刷新机制等。此外，采用轻量级可调线性或非线性函数来有效保护主体之间通信路径免受各种协议攻击。最后，本文使用 SPALL 方法对协议进行了形式化分析，证明了其安全性。

参考文献：

[1] SYED N F, SHAH S W, SHAGHAGHI A, et al. Zero trust architecture (ZTA): a comprehensive survey[J]. IEEE access, 2022, 10: 57143-57179.

[2] 诸葛程晨, 王群, 刘家银, 等. 零信任网络综述[J]. 计算机工程与应用, 2022, 58(22): 12-29.
ZHUGE C C, WANG Q, LIU J Y, et al. Survey of zero trust network[J]. Computer engineering and applications, 2022, 58(22): 12-29.

[3] 王凯, 宋礼鹏, 郑家杰. 融合击键内容和击键行为的持续身份认证[J]. 计算机工程与设计, 2020, 41(6): 1562-1567.
WANG K, SONG L P, ZHENG J J. Continuous authentication fusing keystroke behavior and keystroke content[J]. Computer engineering and design, 2020, 41(6): 1562-1567.

[4] 徐辉, 张莹, 步晓亮, 等. 结合生物特征的 PKI/CA 认证系统设计[J]. 通信技术, 2018, 51(7): 1684-1688.
XU H, ZHANG Y, BU X L, et al. Design of PKI/CA certification system combined with biometrics[J]. Communications technology, 2018, 51(7): 1684-1688.

[5] 周加法, 马涛, 李益发. PKI、CPK、IBC 性能浅析[J].

信息工程大学学报, 2005, 6(3): 26-31.
ZHOU J F, MA T, LI Y F. Comparison and analysis of PKI, CPK and IBC[J]. Journal of information engineering university, 2005, 6(3): 26-31.

[6] 刘学. 基于身份的密码体制密钥管理研究[D]. 济南: 山东大学, 2012.
LIU X. Research on identity based cryptosystem public key management scheme[D]. Jinan: Shandong University, 2012.

[7] 王真, 马兆丰, 罗守山. 基于身份的移动互联网高效认证密钥协商协议[J]. 通信学报, 2017, 38(8): 19-27.
WANG Z, MA Z F, LUO S S. Identity-based efficient authentication and key agreement protocol for mobile Internet[J]. Journal on communications, 2017, 38(8): 19-27.

[8] ZHANG H X, CHEN X S, LAN X, et al. BTCAS: a blockchain-based thoroughly cross-domain authentication scheme[J]. Journal of information security and applications, 2020, 55: 102538.

[9] XIA T, HE J, LIU H F. Cross-domain authentication technology of UAV based on alliance chain[J]. Mobile information systems, 2022, 2022: 1-8.

[10] 高阳,马文平,刘小雪. 基于信任的服务实体跨域认证方案[J]. 系统工程与电子技术, 2019,41(2):439-444.
GAO Y,MA W P,LIU X X. Cross-domain authentication scheme based on trust for service entity[J]. Systems engineering and electronics,2019,41(2):439-444.

[11] CHUANG Y H, LO N W, YANG C Y, et al. A lightweight continuous authentication protocol for the Internet of Things[J]. Sensors, 2018, 18(4): 1104.

[12] BAMASAG O O, YOUCEF-TOUMI K. Towards continuous authentication in Internet of Things based on secret sharing scheme [C]// Proceedings of the WESS' 15: Workshop on Embedded Systems Security. New York: ACM Press, 2015: 1-8.

[13] SHAH S W, SYED N F, SHAGHAGHI A, et al. LCDA: lightweight continuous device-to-device authentication for a zero trust architecture (ZTA)[J]. Computers & security, 2021, 108: 102351.

[14] 孔雪曼, 薛梦阳. 基于统一多域标识的密钥处理方法、装置及系统: 中国,CN115001673A[P]. 2022-09-02.
KONG X M, XUE M Y. Secret key processing method, device and system based on unified multi-domain identifier: PRC Patent,CN115001673A[P]. 2022-09-02.

[15] HUA J Y, SUN H Y, SHEN Z Y, et al. Accurate and efficient wireless device fingerprinting using channel state information[C]//IEEE INFOCOM 2018-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2018: 1700-1708.

[16] CHEN D J, ZHANG N, QIN Z, et al. S2M: a lightweight acoustic fingerprints-based wireless device authentication protocol[J]. IEEE Internet of Things journal, 2017, 4(1): 88-100.

[17] SATHYADEVAN S, ACHUTHAN K, DOSS R, et al. Protean authentication scheme-A time-bound dynamic KeyGen authentication technique for IoT edge nodes in outdoor deployments[J]. IEEE access, 2019, 7: 92419-92435.

[18] YU B Y, YANG C, MA J F. Continuous authentication for the Internet of Things using channel state information [C]// 2019 IEEE Global Communications Conference (GLOBECOM). Piscataway:IEEE Press, 2020: 1-6.

[19] HSIEH C H, CHEN J Y, NIEN B H. Deep learning-based indoor localization using received signal strength and channel state information[J]. IEEE access, 2019, 7: 33256-33267.

[20] YAN X S, WANG H J. Survey on zero-trust network security[C]//International Conference on Artificial Intelligence and Security. Berlin: Springer Press, 2020: 50-60.

[21] 张文政, 王立斌, 李益发. 安全协议设计与分析[M]. 北京: 国防工业出版社, 2015: 33-60.
ZHANG W Z, WANG L B, LI Y F. Design and analysis of security protocols[M]. Beijing: National Defense Industry Press, 2015: 33-60.