一种多机制融合的可信网络探测认证技术*

王　斌，李　琪，张　宇，史建焘，朱国普
（哈尔滨工业大学　网络空间安全学院，黑龙江　哈尔滨　150001）

摘　要：为了在确保网络拓扑信息安全的同时，保留网络的灵活性和可调性，提出了一种多机制融合的可信探测认证技术，旨在对类 Traceroute 的拓扑探测流量进行认证。该技术通过基于 IP 地址的可信认证、基于令牌的可信认证以及基于哈希链的可信认证三种机制融合，实现了效率与安全的平衡。通过这种方法，网络管理员可以在不阻断合法拓扑探测的前提下，保护网络拓扑信息。开发了一种支持该技术的拓扑探测工具，并利用 Netfilter 技术在 Linux 主机上实现了该技术。实验结果表明，该技术能够有效识别可信探测，其延迟相比传统 Traceroute 略有提升。

关键词：可信探测认证；哈希链；网络拓扑；Traceroute
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.06.004
引用格式：王斌，李琪，张宇，等. 一种多机制融合的可信网络探测认证技术[J]. 网络安全与数据治理，2024，43(6)：23-32.

An authentication scheme for trusted network probing based on multiple mechanisms integrating

Wang Bin, Li Qi, Zhang Yu, Shi Jiantao, Zhu Guopu
(School of Cyberspace Science, Harbin Institute of Technology, Harbin 150001, China)

Abstract: To ensure the security of network topology information while maintaining the network's flexibility and tunability, this paper introduced an authentication technology for trusted network probing that integrates multiple mechanisms. This technology combines trusted authentication based on IP addresses, token-based authentication, and hash chain-based authentication, balancing efficiency and security. Through this method, network administrators can protect network topology information without blocking legitimate topology probing. A topology probing tool supporting this technology was developed, and the technique was implemented on Linux hosts using Netfilter technology. Experimental results demonstrated that this technology can effectively identify trusted probes, with a slight increase in latency compared to traditional Traceroute.

Key words: trusted probe authentication; hash chain; network topology; Traceroute

0　引言

在现代计算机网络中，网络拓扑结构描述了设备间的逻辑和物理连接，是网络的关键资产之一。泄露的网络拓扑信息可能被攻击者利用，以发起更为精准的 APT（Advanced Persistent Threat）攻击。为了防止网络拓扑信息泄露，网络管理员通常会采取一些预防措施，如丢弃具有较小 TTL（Time to Live）值的数据包或禁用 ICMP（Internet Control Message Protocol）数据包。这些措施虽然在提升网络安全性方面起到了积极作用，但同时也可能带来一些负面影响，比如降低网络的灵活性和妨碍与合作伙伴或其他组织的通信，从而影响网络的可调性和可用性。

目前，已有多种基于 IP 地址[1-4]、令牌[5-11]以及哈希链[12-22]的可信认证技术被提出，用于增强网络安全。然而，针对类 Traceroute 网络拓扑探测流量可信认证的研究尚处于起步阶段。

为了在确保网络拓扑信息安全的同时，最大限度地保持网络的灵活性和可调性，本文提出了一种多机制融合的可信探测认证技术，旨在对类 Traceroute 的拓扑探测流量进行认证。该技术通过基于 IP 地址的可信认证、基于令牌的可信认证以及基于哈希链的可信认证三种机制融合，实现了效率与安全的平衡。通过这种方法，网络

*基金项目：国家重点研发计划（2022YFB3102903）

管理员可以在不阻断合法拓扑探测的前提下，保护网络拓扑信息，并保留网络可调性。

本文基于 Traceroute 工具的原理，开发了一种支持该可信探测认证技术的拓扑探测工具，并利用 Netfilter 技术在 Linux 主机上以防火墙的形式实现了这一技术。此外，本文对该技术的功能和性能进行了验证，实验结果表明，该技术可有效识别可信探测，与传统的 Traceroute 工具相比，延迟略有提升。

1 相关工作

基于 IP 地址的白名单认证是一种简单且高效的认证方案，在防火墙等应用场景中广泛使用。鲁剑等人[1]提出了一种改进的基于白名单的深度包检测防火墙方法。该方法允许白名单中的可信流量在完成状态检测或协议分析后即可通过防火墙，不再需要进行完整的深度检测，从而减轻了防火墙的负荷。Yoon[2]提出了一种基于白名单的 DDoS（Distributed Denial-of-Service）缓解方案，该方案收集并标记已成功登录的 IP 地址以建立 VIP 名单，在网络遭受攻击时，优先放行来自 VIP 名单的流量，能够使关键网络设施在严重的网络攻击场景下继续正常工作。Tyou 等人[3]提出了一个控制异常流量的物联网安全系统，该系统引入基于 IP 地址等字段的白名单机制，可以在白名单条件下控制网关中的流量，从而防止异常流量。李大勇[4]提出了一种操作系统防火墙白名单技术，该技术可以在应用系统存在无法修复的安全隐患时，限制访问的 IP 地址与端口，从而大幅降低应用系统对外暴露风险，提升系统安全。

相较于基于 IP 的认证，基于令牌的方法展现出更高的灵活性，尤其在 Web 中得到广泛应用。Cheong 等人[5]提出了一种可增强 Web 服务安全性的新安全令牌，引入了五个安全令牌配置，实现了对远程客户端的位置验证。Huang 等人[6]提出了一种基于 HTTP 协议的 RESTful API 令牌认证机制，该机制在每次通信时生成一次性令牌，并由服务器进行验证，使得所有合法通信仅在固定的时间段内有效，降低了合法身份被盗的风险。Dammak 等人[7]提出了一种新的基于令牌的轻量级用户身份验证方案，该方案采用令牌技术增强身份验证的鲁棒性，具有较高的令牌安全性和完美的前向保密性。Ahmed 和 Mahmood[8]提出了一种基于真正随机时间戳值的身份认证技术，利用 JSON Web Token 增强服务器上客户端标识的安全性，加强令牌的安全性。Chen 等人[9]提出了一种基于量子令牌的网络认证协议，该协议要求用户在有效期内出示量子令牌以访问服务器，可以实现身份认证和窃听检测，提供更高的安全性和保密性。Mohanty 等人[10]提出一种基于令牌的认证方法，用于在物联网设备与云服务器之间建立安全通信，通过增强的散列算法提高数据传输的效率和安全性。Haggag 等人[11]提出了一种面向 Hadoop 平台的基于令牌的身份认证方法，通过灵活的令牌认证机制、哈希算法以及分层组结构，实现了更高的安全性、抗攻击性和可扩展性。

在哈希链技术提出后，基于哈希链的可信认证技术成为一种新兴的更加安全的认证方法。Lamport[12]首次提出了一种基于哈希链的签名认证机制，通过单向哈希函数构建哈希链，实现了有效的身份认证，并能够防止窃听和重放攻击。针对哈希链签名方与认证过程中的计算负荷和存储限制问题，Jakobsson[13]提出了低成本的哈希链摊销技术，Coppersmith 等人[14]提出了一种优化的哈希序列计算技术，解决了计算负荷和空间复杂度问题。为了应对因数据包丢失而引起的断链问题，Zhang 等人[15]提出了一种蝶形哈希链结构，能够容忍数据包丢失，从而解决断链问题。对于现有哈希链仅支持单向认证的不足，Alshahrani 和 Traore[16]提出了一种基于哈希链的轻量级双向认证协议，而 Varsha 等人[17]提出了基于 Keyed – hash 链的双向认证协议，使通信双方能够互相认证，克服了单向认证的局限性。针对哈希块数量有限的问题，Goyal[18]提出了可重新初始化的哈希链技术 RHC，Zhang 等人[19-20]提出了自更新哈希链技术 SUHC 和新型自更新哈希链 SRHC，Park[21]则提出了由多个“短”反向哈希链组成的自更新哈希链，这些自更新哈希链技术通过一次注册生成和验证无限数量的哈希块，避免了重复初始化的开销。针对大多数相关研究未将网络层数据包作为研究对象的问题，Han 和 Jiang[22]提出了一种基于报文哈希链的签名认证方法，通过签名验证报文序列的哈希链，以确保报文的完整性、真实性和可靠性。

在类 Traceroute 的网络拓扑探测领域，针对可信探测认证的研究尚处于起步阶段。本研究将现有的可信认证技术——包括基于 IP 地址的认证、基于令牌的认证以及基于哈希链的认证——迁移到类 Traceroute 的网络拓扑探测中，并针对该应用场景下存在的具体问题进行改进。鉴于不同的可信认证方案各有局限，本文融合这三种技术，提出了一种多机制融合的可信探测认证技术，以实现在多样化的安全场景下的高效和安全认证。

2 多机制融合的可信探测认证

本文利用 Netfilter 技术，在 Linux 系统中以防火墙的形式实施了这一多机制融合的可信探测认证技术。在防火墙接收数据包后的处理逻辑如下：首先，防火墙将验证数据包是否为探测包。若确认为探测包，防火墙进一

步判断其是否为可信探测包。对于非可信探测包，防火墙将其直接丢弃；对于可信探测包，防火墙会根据数据包所采用的子认证技术，将其转交给相应的处理子程序。

2.1 基于 IP 地址的可信认证技术

基于 IP 地址的可信认证技术通过探测包头部的源 IP 字段来识别和过滤可信探测流量。具体实施过程如图 1 所示：在对内部网络进行探测之前，探测方需要将探测主机的 IP 地址报备给防火墙。防火墙会将这些 IP 地址标记为可信。当防火墙收到基于 IP 地址的可信认证技术的数据包时，会进一步验证探测包是否来自预先报备的可信 IP 地址。若确认来自可信 IP 地址，则允许其通过并返回内部网络的真实拓扑信息；否则，将对其进行阻断。

基于 IP 地址的可信认证技术仅利用探测包头部的源 IP 字段进行可信判别，能够简单且高效地识别可信探测方，从而减少判别时间并提升防火墙性能。然而，这种方案的灵活性相对较低。若可信探测方的网络环境频繁变化，例如从 Wi-Fi 切换至 5G，防火墙需不断更新标记同一可信端的不同可信 IP 地址。这会导致可信配置的效率降低，管理工作变得繁琐，同时维护和更新可信源 IP 地址的成本也会提高。

2.2 基于令牌的可信认证技术

针对基于 IP 地址的可信认证技术灵活性不足的问题，本文继而提出了基于令牌的可信认证技术。具体实施过程如图 2 所示。在进行内部网络探测之前，防火墙通过随机数生成算法为可信探测方生成随机令牌，并进行分发。令牌中引入了时间戳机制以限制其有效期，从而在一定程度上抵御重放攻击。当防火墙收到基于令牌的可信认证技术的数据包时，会检查该令牌是否存在于可信令牌集合中。如果令牌不在集合中，则阻断该数据包；如果令牌在集合中，防火墙将进一步检查令牌是否过期：若令牌未过期，探测包将被直接放行；若令牌已过期，防火墙将生成新的令牌，并随应答包一同发送给探测方，同时更新可信令牌集合中的该探测方令牌。

基于令牌的可信探测认证技术通过令牌进行可信认证，允许同一可信探测方使用不同的源 IP 地址对内部网络进行探测。这一特性为网络环境不固定的可信探测方提供了便利，提升了可信认证技术的灵活性。然而，由于取消了对 IP 地址的限制，该方案面临重放攻击的风险。例如，攻击者可能截获可信探测方与防火墙之间的通信数据包，获取携带令牌的 Traceroute 探测包，并将其源 IP 地址替换为攻击者自身的 IP 地址，从而获取目标网络的拓扑信息。

2.3 基于哈希链的可信认证技术

针对源 IP 地址配置效率低、管理复杂，以及令牌认证难以抵御重放攻击的问题，本文提出基于哈希链的可信认证技术。其大致过程如图 3 所示：在探测开始之前，防火墙和可信探测方通过协商配置哈希链的基础信息进行初始化。在探测过程中，双方各自迭代生成哈希链块序列。可信探测方根据哈希链序列，将哈希链块嵌入到 Traceroute 探测数据包中，并将其发送至目标网络。防火墙通过比较数据包中包含的哈希链块信息与自身生成的哈希链块信息是否匹配，从而实现可信认证。

该方案通过在探测包中嵌入动态更新的哈希链块，能够有效防止攻击者劫持数据包进行重放攻击。防火墙通过验证哈希链块信息来识别可信探测方，允许同一可信探测方使用不同的源 IP 地址进行网络探测，从而解决了源 IP 地址配置效率低下和管理复杂的问题。

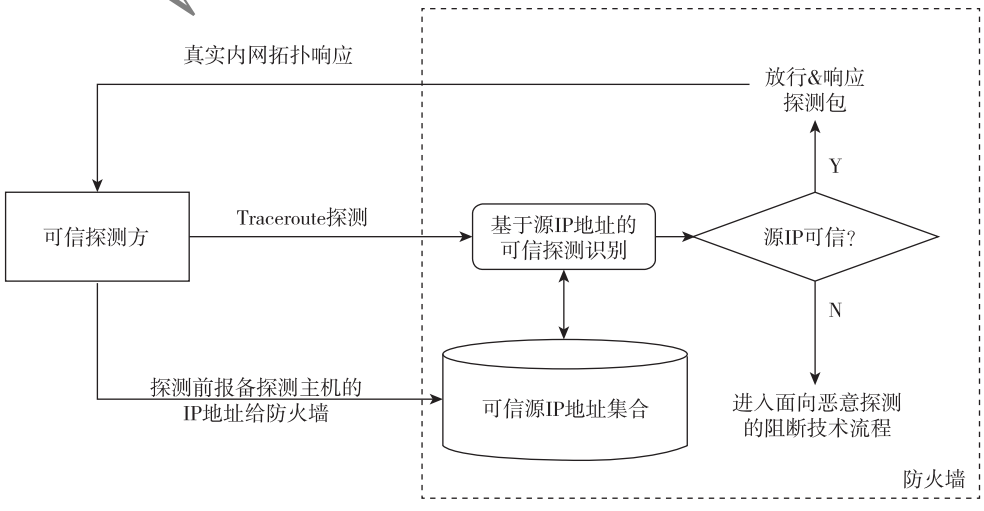

图 1 基于 IP 地址的可信认证技术原理图

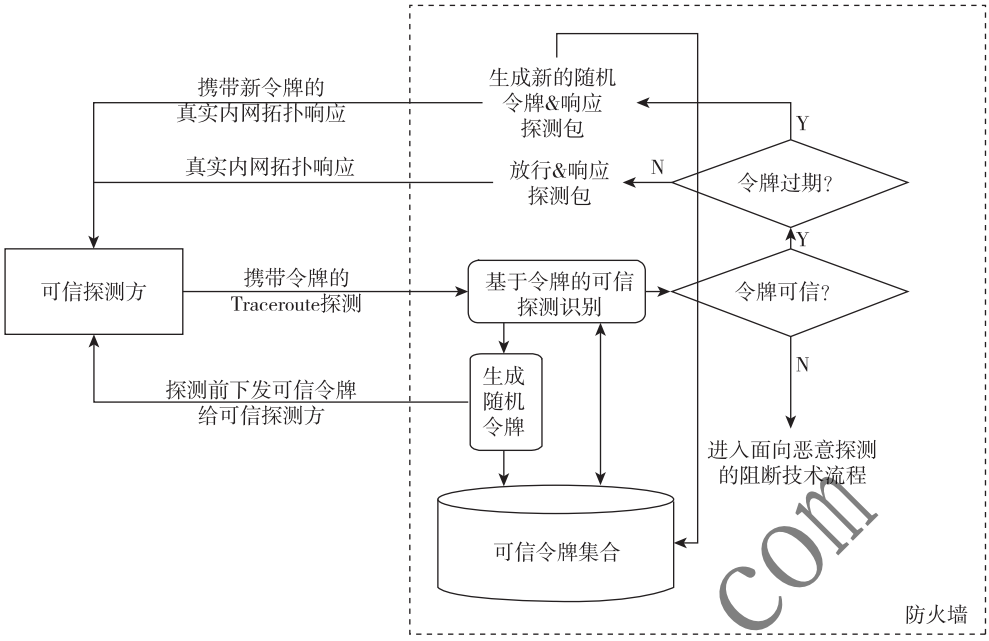

图 2　基于令牌的可信认证技术原理图

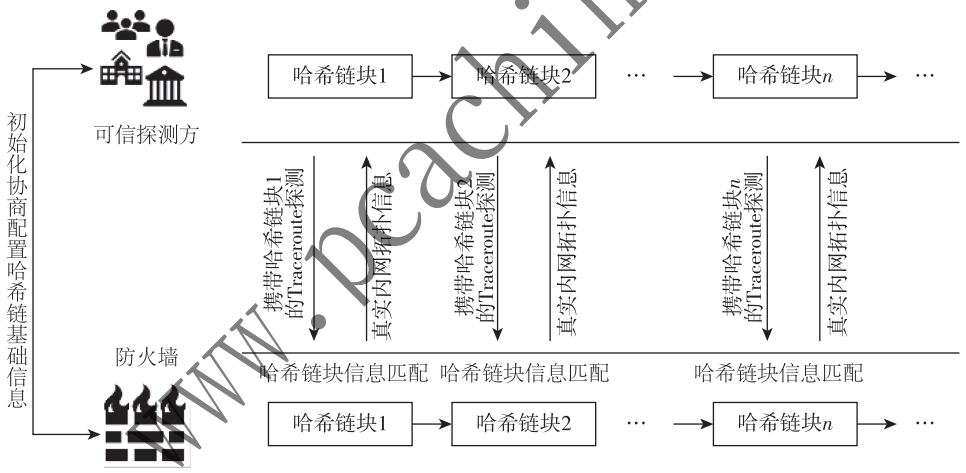

图 3　基于哈希链的可信认证技术示意图

2.3.1　签名和认证过程

基于哈希链的可信认证技术的签名和认证过程如图 4 所示。可信探测方与防火墙在正式通信前，需协商好初始序号 BASE_ID 与种子信息，BASE_ID 作为序号机制的初始化序号 ID_1，以防范中间人攻击；SEED 作为可信端首个探测包的正文消息 m_1，是开启防火墙认证的“敲门砖”。序号机制的引入，可防止攻击者根据旧的哈希链块信息推导后续哈希链块，从而避免中间人攻击。在初始化阶段，防火墙会记录不同可信方的种子信息 SEED，并通过可信端发送的第一个探测包的载荷识别其身份。

可信探测方签名阶段的基本流程如下：

（1）可信端配置已协商好的初始序号 BASE_ID 与种子信息 SEED，即令 ID_1 = BASE_ID，m_1 = SEED，并初始化报文计数下标 $i = 1$；

（2）利用 SHA256 哈希算法，分别计算 ID_i 与 m_i 的哈希值 h（ID_i）与 h（m_i）；

（3）利用哈希链迭代公式（见 2.3.2 节），计算构造本次报文的哈希链块 HC_i；

（4）构造 Traceroute 探测包 p_i =（m_i，HC_i），并将其发送到目标网络，其中（m_i，HC_i）为探测包的载荷字段；

（5）重新计算报文计数下标，令 $i = i + 1$，并利用迭代公式，计算更新 ID_i 与 m_i；

（6）利用更新后的 ID_i 与 m_i，重新计算下一个探测包的对应哈希值，继续进行新的 Traceroute 探测。

防火墙认证阶段的基本流程如下：

（1）防火墙端配置已经协商好的初始序号 BASE_ID，即令 $ID'_1 = BASE\_ID$，同时令 $HC'_0 = NULL$，并初始化报文计数下标 $i = 1$；

（2）收到 Traceroute 探测包 p_i =（m_i，HC_i）后，提取其载荷中的 m_i 与 HC_i；

（3）根据 m_i 与本端的 ID'_i、HC'_{i-1}，计算构造的防火墙端的哈希链块 HC'_i；

（4）对比可信探测方的哈希链块 HC_i 与防火墙端自行计算的哈希链块 HC'_i；

（5）若 HC_i 与 HC'_i 相同则通过验证，放行该探测包，并令报文计数下标 $i = i + 1$，同时计算更新 ID'_i；否则阻断丢弃该探测数据包。

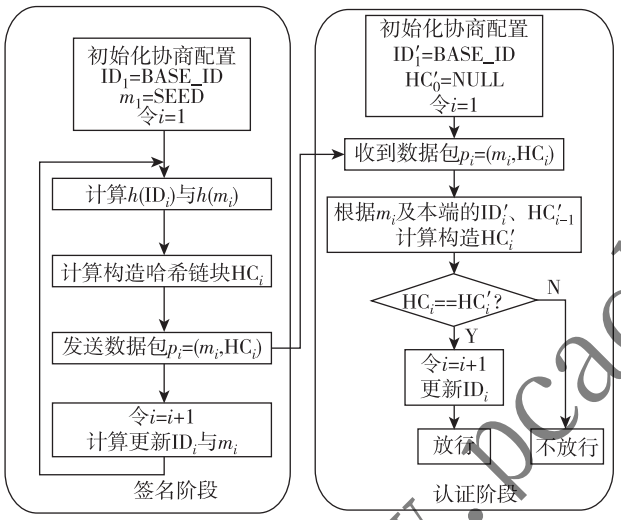

图 4　基于哈希链的可信认证技术的签名和认证过程

2.3.2　哈希链构建方案

通信双方在协商初始序号 BASE_ID 与种子信息 SEED 后，哈希链的构建方案如图 5 所示。

可信探测方令 $m_1 = SEED$，$ID_1 = BASE\_ID$，并用式（1）与式（2）确定需要发送的序号 ID、探测包的正文消息 m 的序列，利用 SHA256 哈希函数计算 m_i 和 ID_i 的哈希值 h（m_i）和 h（ID_i）。接着，如式（3）所示，将 h（m_i）和 h（ID_i）与上一个哈希链块 HC_{i-1}（如果存在）拼接，计算新的哈希链块 $HC_i = h(h(m_i) \| h(ID_i) \| HC_{i-1})$，形成一个连续的报文哈希链。

$$ID_i = \begin{cases} BASE\_ID, & i = 1 \\ ID_{i-1} + 1, & i > 1 \end{cases} \tag{1}$$

$$m_i = \begin{cases} SEED, & i = 1 \\ h(m_{i-1}), & i > 1 \end{cases} \tag{2}$$

$$HC_i = \begin{cases} h(h(m_1) \| h(ID_1)), & i = 1 \\ h(h(m_i) \| h(ID_i) \| HC_{i-1}), & i > 1 \end{cases} \tag{3}$$

防火墙收到可信探测方发送的 Traceroute 探测包后，提取其载荷中的 m_i 与 HC_i，利用式（4）和式（5）迭代计算本端序号 ID'_i 与本端哈希链块 HC'_i，对比 HC_i 与 HC'_i 是否相同。如果 HC_i 与 HC'_i 相同，则认为该数据包为可信探测包，否则为不可信探测包。

$$ID'_i = \begin{cases} BASE\_ID, & i = 1 \\ ID'_{i-1} + 1, & i > 1 \end{cases} \tag{4}$$

$$HC'_i = \begin{cases} h(h(m_1) \| h(ID'_1)), & i = 1 \\ h(h(m_i) \| h(ID'_i) \| HC'_{i-1}), & i > 1 \end{cases} \tag{5}$$

2.3.3　超时重传与哈希跳跃

为应对网络层数据包丢失问题，本文引入了超时重传和哈希跳跃机制，以解决由网络层数据包丢失导致的断链问题，增强系统的鲁棒性。为简化讨论，假设目标网络内部是可靠的，不会发生数据包丢失，只有可信方到防火墙之间的网络会发生丢包。根据丢包的数据包类型不同，可能会出现探测包丢失与响应包丢失两类情形：

（1）探测包丢失：设可信探测方向受保护的目标网络连续发送了 p_i、p_{i+1}、p_{i+2} 三个 Traceroute 探测包。其中，探测包 p_i 成功到达防火墙，并收到对应的响应包 r_i；而探测包 p_{i+1} 在途中丢失。

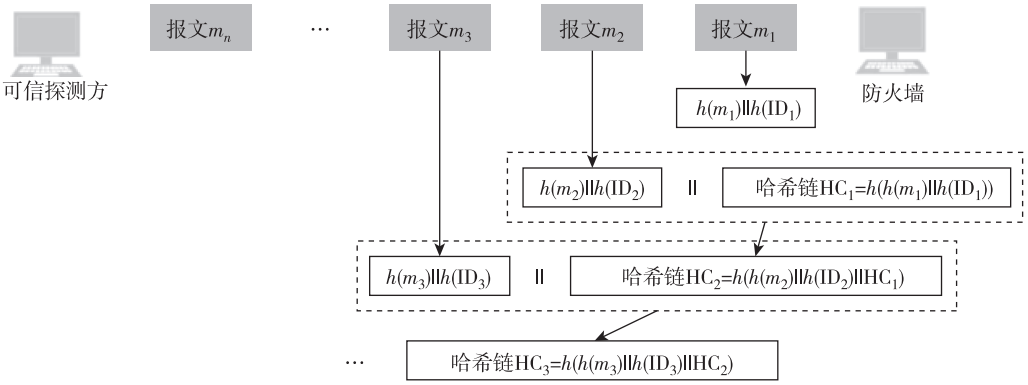

图 5　哈希链构建方案图

如图6所示，在引入超时重传机制之前，可信探测方无法感知探测包的丢失，会继续发送第三个探测包 p_{i+2}。由于探测包 p_{i+1} 的丢失，可信探测方更新了哈希链块信息，而防火墙端未能同步更新。当防火墙收到探测包 p_{i+2} 时，检测到其携带的哈希链块 HC_{i+2} 与防火墙维护的哈希链块 HC'_{i+1} 不匹配，将探测包 p_{i+2} 判定为攻击流量并予以丢弃。探测包 p_{i+1} 的丢失导致可信探测方与防火墙之间的哈希链块信息不一致，进而引发哈希链断裂，导致可信探测方无法接收到后续的任何响应包。

针对探测包丢失的情景，本文引入了超时重传机制，以解决可信探测方无法感知探测包丢失的问题。超时重传机制在可信探测方增加了超时计时器（timer），并调整了哈希链块信息更新的时机。具体过程如图 7 所示，可信探测方在发送 Traceroute 探测包的同时启动一个 timer。只有当可信探测方在 timer 超时之前收到该探测包对应的响应包，才会更新哈希链块及相关信息，并发送下一个探测包；反之，若 timer 超时且未收到响应包，可信探测方会立即重传当前探测包，同时保持原有的哈希链块相关信息和 TTL 值不变。

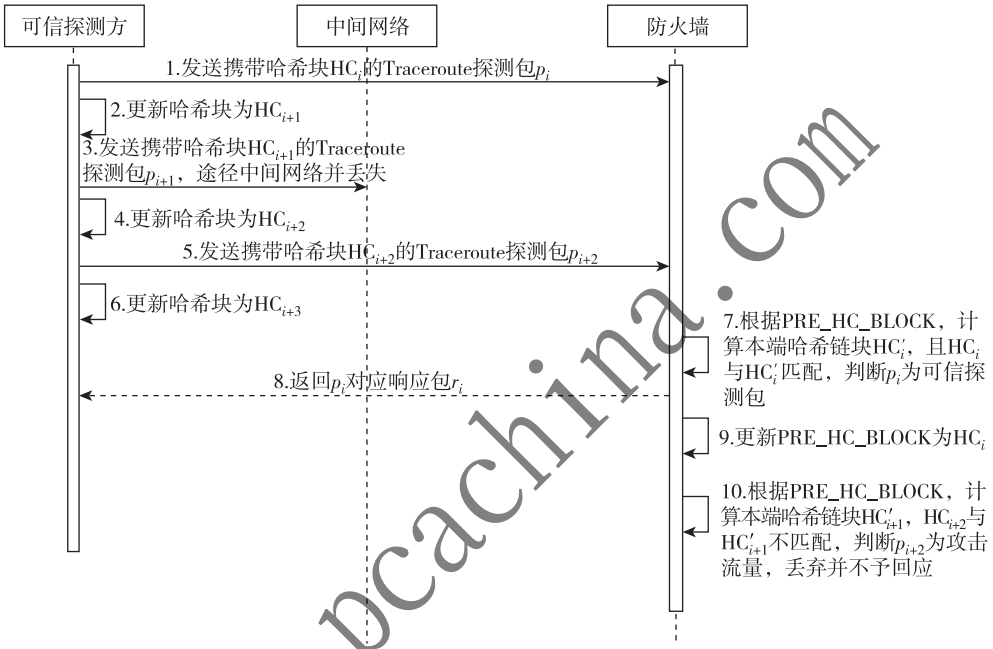

图 6　探测包丢失时序图

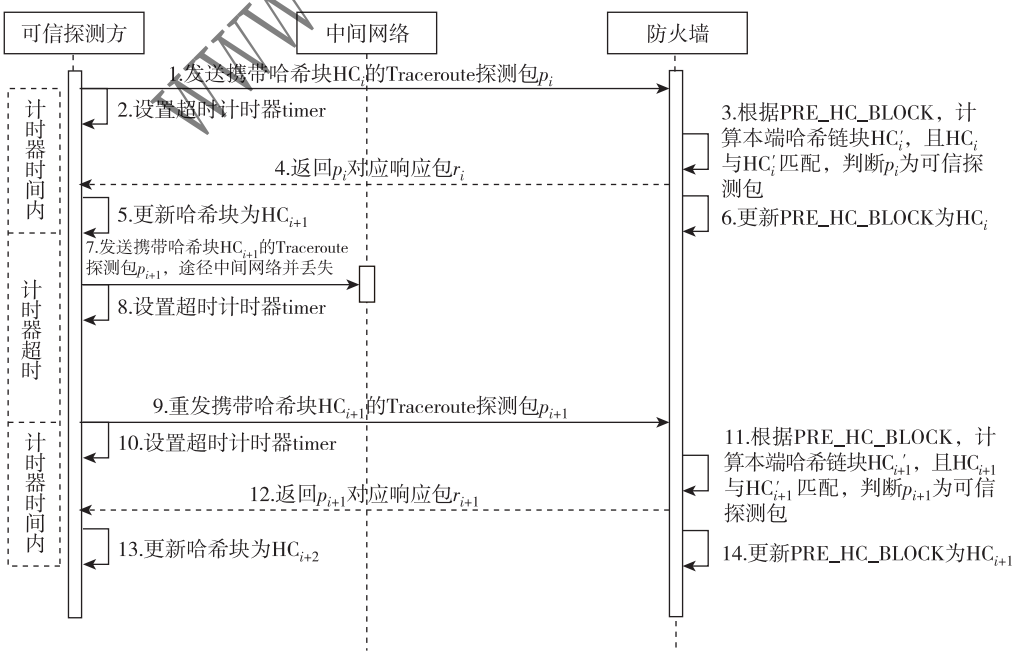

图 7　超时重传机制时序图

（2）响应包丢失：设可信探测方向受保护的目标网络连续发送了 p_i、p_{i+1}、p_{i+2} 三个 Traceroute 探测包。其中，探测包 p_i 成功到达防火墙，但其响应包 r_i 在传输过程中丢失。

如图 8 所示，在仅使用超时重传机制的情况下，可信探测方无法区分是探测包丢失还是响应包丢失。当 timer 超时后，可信探测方会重复发送探测包 p_i。而防火墙端则在返回响应包 r_i 后已经更新了哈希链块信息，这导致通信双方维护的哈希链块信息不匹配，从而使可信探测方陷入一个无限重发的循环中。

针对响应包丢失的情景，本文引入哈希跳跃机制，以解决可信探测方无法感知响应包丢失的问题。具体过程如图 9 所示，当防火墙收到非预期的 Traceroute 探测流量时，会丢弃该数据包并主动返回一个带有特殊标记的 ICMP 主机不可达报文。如果可信探测方接收到带有特殊标记的 ICMP 主机不可达报文，则判定前序探测包的响应包在传输途中丢失。此时，可信探测方会立即采用“跳跃”策略放弃当前探测包，并更新哈希块信息，与防火墙端的哈希链块保持同步。同时，它还将确保下一个 Traceroute 探测包的 TTL 值与前序探测包保持一致，以获取完整的内网拓扑链路信息，并继续发送下一探测包。

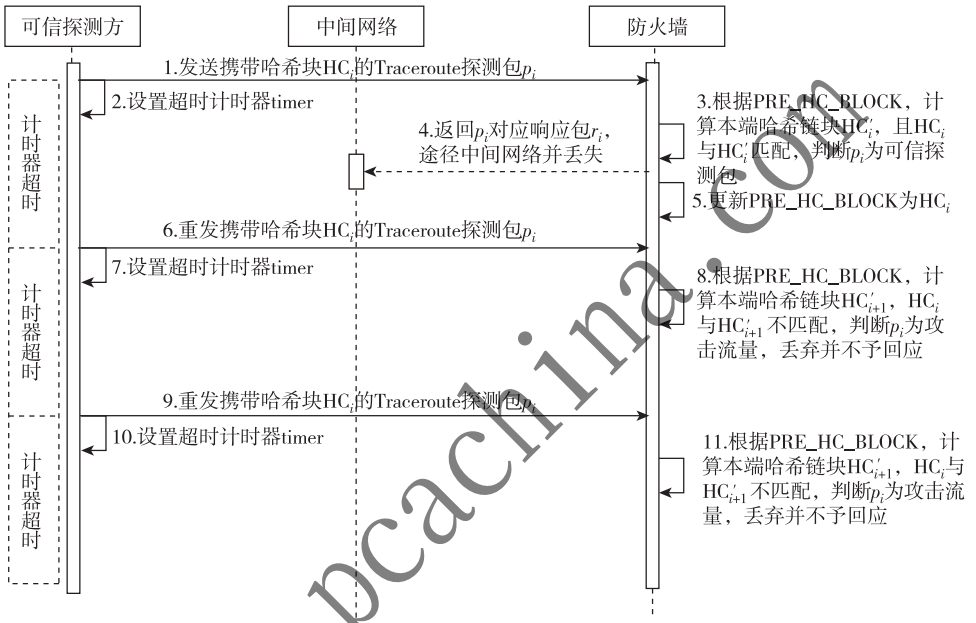

图 8　响应包丢失时序图

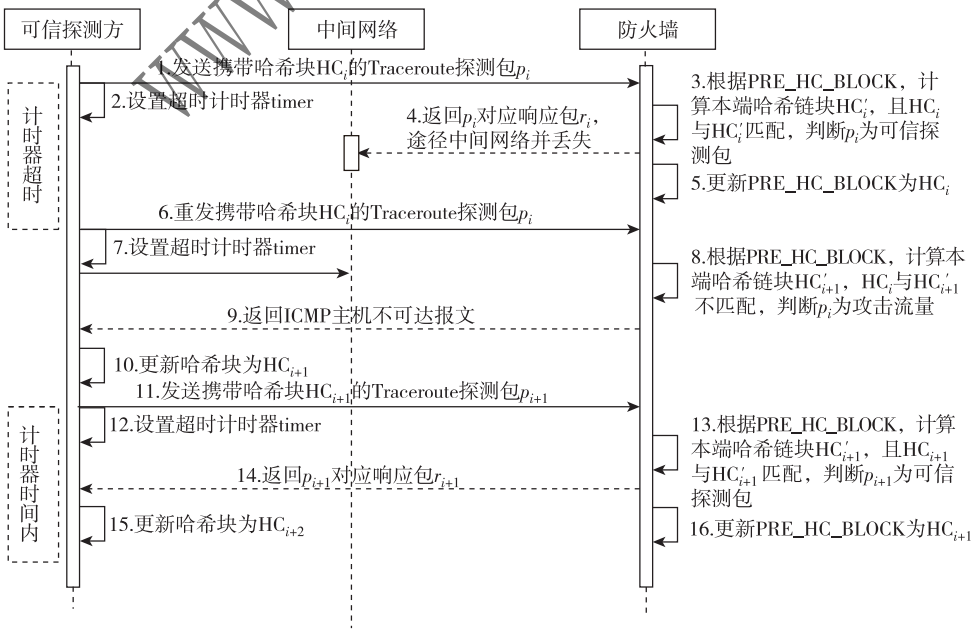

图 9　哈希跳跃机制时序图

3 实验结果与分析

本文对提出的三种可信认证技术进行了功能和性能测试，以验证其在实际应用中的有效性和可行性。

3.1 功能测试

在功能测试中，本文对提出的多机制融合的可信探测认证技术的有效性进行了完整测试，其主要的测试项与测试结果如表 1 所示。

在对基于 IP 地址的可信认证技术的功能测试中，将外网主机的 IP 地址在防火墙处标记为可信地址，随后利用外网主机对内网主机进行基于源 IP 地址的可信探测，测试结果表明探测成功，功能正常；在对基于令牌的可信认证技术的功能测试中，利用外网主机对内网主机进行了 5 次基于令牌的可信探测识别，所有探测均成功，外部节点可以成功获取到内网主机的信息，且第 2 次探测与第 3 次探测的令牌值相同，但由于令牌的有效期为 2 h，因此第 5 次探测时发现令牌值已发生变化；在对基于哈希链的可信认证技术的功能测试中，首先让外网主机在防火墙上初始化协商注册哈希链信息，然后对内网主机进行基于报文哈希链签名认证的可信探测，测试结果表明探测成功，其功能正常。

表 1 面向可信探测的识别技术主要测试项与结果

功能	操作描述	预期结果	测试结果
基于 IP 地址的可信认证技术	把 IP 地址为 192. 168. 9. 100 的外网主机标记为可信源 IP 地址，后该主机对 IP 地址为 192. 168. 5. 3 的内网主机进行基于 IP 地址的可信探测	探测成功，外部节点获取到内网信息	与预期结果一致
基于令牌的可信认证技术	IP 地址为 192. 168. 9. 100 的外网主机对 IP 地址为 192. 168. 5. 3 的内网主机进行 5 次基于令牌的可信探测，第 1 次探测和第 2 次探测无间隔，第 2 次探测与第 3 次探测间隔 0. 5 h，第 3 次探测与第 4 次探测间隔 3 h，第 4 次探测和第 5 次探测无间隔	所有探测均成功，外部节点可以获取到内网信息，且第 2 次探测与第 3 次探测的令牌值相同，但由于令牌的有效期为 2 h，因此第 5 次探测到令牌值发生变化	与预期结果一致
基于哈希链的可信认证技术	IP 地址为 192. 168. 9. 100 的外网主机初始化协商注册哈希链信息（BASE_ID、SEED）到防火墙上，后该主机对 IP 地址为 192. 168. 5. 3 的内网主机进行基于报文哈希链签名认证的可信探测	探测成功，外部节点获取到内网信息	与预期结果一致

3.2 性能测试

在性能测试部分，本文首先对传统的 Traceroute 探测技术进行了基准延迟测试，以建立性能基准。随后，对本文提出的三种可信认证技术进行了延迟测试，在测试过程中，三种技术分别加载不同数量的可信探测规则，以测试其性能随可信探测规则数量的变化。最后，比较分析了传统 Traceroute 探测与三种不同的可信认证技术的延迟差异，同时还对三种不同的可信认证技术间的延迟差异进行了对比分析。

在进行传统 Traceroute 探测技术的延迟基准测试时，本文利用 Linux 系统中的 Traceroute 工具从外网主机向内网主机连续发送 100 个 Traceroute 探测包，然后收集并统计探测结果中的往返时间值，计算其最高延迟、最低延迟和平均延迟，实验结果如图 10 所示。

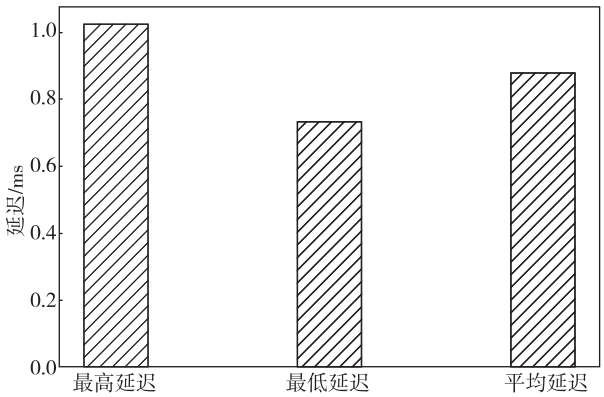

图 10 传统 Traceroute 探测延迟测试结果

在进行可信认证技术的延迟测试时，本文首先在防火墙以及可信探测方的主机上配置了必要的可信探测认证信息。随后，在载入不同数量的可信探测规则的情况下，分别利用基于 IP 地址、基于令牌和基于哈希链的三种可信认证技术从外网主机向内网主机连续发送 100 个可信 Traceroute 探测包，然后收集并统计探测结果中的往返时间值，从最高延迟、最低延迟和平均延迟三个指标对上述三种可信认证技术进行了评估，实验结果如图 11 ~ 图 13 所示。

在延迟基准测试中，传统 Traceroute 探测技术的最高、最低和平均延迟分别为 1. 022 ms、0. 732 ms 与 0. 878 ms。

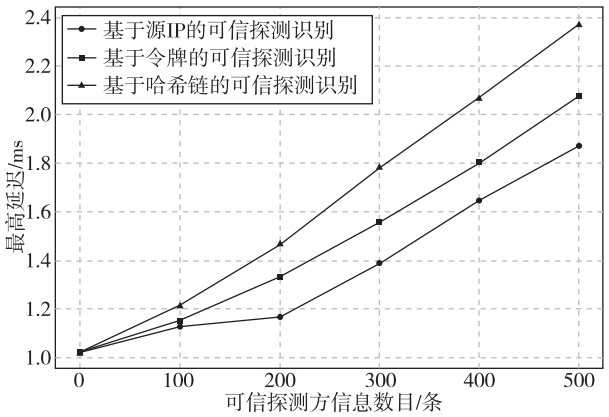

图 11　三种可信认证技术的最高延迟测试结果

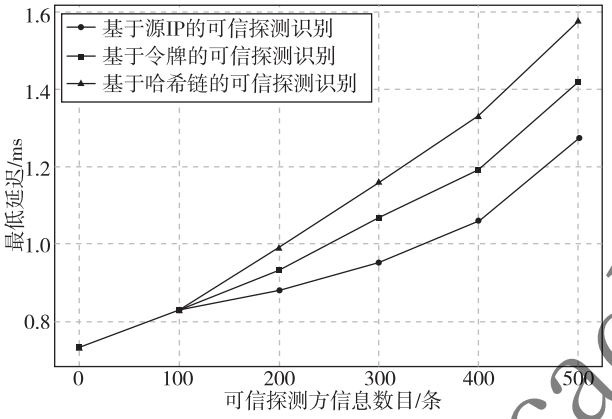

图 12　三种可信认证技术的最低延迟测试结果

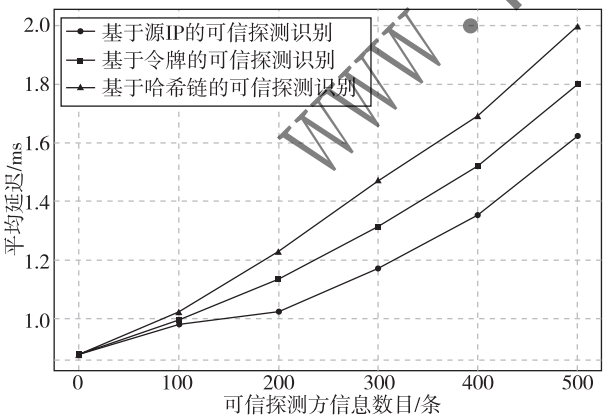

图 13　三种可信认证技术的平均延迟测试结果

随着可信探测规则数量的增加，本文提出的可信探测识别技术的延迟会略高于传统 Traceroute 探测技术，但其总体也处于较低延迟的水平。具体来说，当可信探测方信息数目为 500 条时，基于报文哈希链签名认证的可信探测识别的平均延迟为 1.998 ms，相较于传统 Traceroute 探测技术的平均延迟 0.878 ms 仅增加 1.12 ms。

随着可信探测规则数目的增加，各可信认证技术的最高延迟、最低延迟和平均延迟均呈线性增加的趋势。当可信探测方信息数目从 0 条增加到 500 条时，基于哈希链的可信认证技术的平均延迟从 0.878 ms 增加到 1.998 ms，为原来的 2.28 倍，这表明可信探测规则数目越多，可信认证技术的性能越差。

在可信探测规则数量相同的情况下，基于 IP 地址的可信认证技术展现出最低的延迟，其次是基于令牌的技术，而基于哈希链的技术则表现出最高的延迟。随着可信探测方信息数目的增加，这三种技术之间的延迟差异变得更加显著。这是由于三种技术实现背后的复杂度不同，导致三者之间的性能差距越来越明显。

4　结论

本文提出了一种多机制融合的可信探测认证技术，整合了基于 IP 地址、基于令牌以及基于哈希链的多种可信认证机制。该技术的引入使得在保护网络拓扑信息安全性的同时，保持了网络的灵活性和可调性。实验结果显示，尽管相较于传统的 Traceroute 工具，延迟略有提升，但该技术在整体上实现了效率与安全的平衡。三种认证机制各有其优势和局限，通过有效融合能够适应不同场景下的安全策略，提升认证效率。本文所提出的可信探测认证技术为需要同时保护和探测网络拓扑的场景提供了一个高效的解决方案，展现出在关键基础设施等重要网络领域应用的广泛前景。

参考文献

[1] 鲁剑，杨树堂，倪佑生. 基于白名单的深度包检测防火墙的改进方法 [J]. 信息安全与通信保密，2005 (2)：137－139.

[2] YOON M K. Using whitelisting to mitigate DDoS attacks on critical Internet sites [J]. IEEE Communications Magazine, 2010, 48 (7): 110－115.

[3] TYOU I, NAGAYAMA H, SAEKI T, et al. Decentralized IoT security gateway [C]//2018 3rd Cloudification of the Internet of Things (CIoT). IEEE, 2018: 1－6.

[4] 李大勇. 操作系统防火墙白名单技术的应用 [J]. 信息系统工程，2019 (1)：108－110.

[5] CHEONG C P, CHATWIN C, YOUNG R. A new secure token for enhancing web service security [C]//2011 IEEE International Conference on Computer Science and Automation Engineering. IEEE, 2011, 1: 45－48.

[6] HUANG X W, HSIEH C Y, WU C H, et al. A token-based user authentication mechanism for data exchange in RESTful API [C]// 2015 18th International Conference on Network-Based Information Systems. IEEE, 2015: 601－606.

[7] DAMMAK M, BOUDIA O R M, MESSOUS M A, et al. Token-

based lightweight authentication to secure IoT networks [C]// 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2019: 1 - 4.

[8] AHMED S, MAHMOOD Q. An authentication based scheme for applications using JSON web token [C]//2019 22nd International Multitopic Conference (INMIC). IEEE, 2019: 1 - 6.

[9] CHEN H, JIA H, WU X, et al. Quantum token for network authentication [C]//2021 IEEE International Conference on Web Services (ICWS). IEEE, 2021: 688 - 692.

[10] MOHANTY J R, MOHAPATRA M R, MISHRA S, et al. Token based authentication and modified hashing approach to improve the security of internet of things enabled wireless networks [J]. Journal of Survey in Fisheries Sciences, 2023, 10 (2S): 3879 - 3892.

[11] HAGGAG M, TANTAWY M M, EL-SOUDANI M M S. Token-based authentication for Hadoop platform [J]. Ain Shams Engineering Journal, 2023, 14 (4): 101921.

[12] LAMPORT L. Password authentication with insecure communication [J]. Communications of the ACM, 1981, 24 (11): 770 - 772.

[13] JAKOBSSON M. Fractal hash sequence representation and traversal [C]//Proceedings IEEE International Symposium on Information Theory. IEEE, 2002: 437.

[14] COPPERSMITH D, JAKOBSSON M. Almost optimal hash sequence traversal [C]//Financial Cryptography: 6th International Conference, 2002. Springer Berlin Heidelberg, 2003: 102 - 119.

[15] ZHANG Z S, SUN Q B, WONG W C. A proposal of butterfly-graph based stream authentication over lossy networks [C] // 2005 IEEE International Conference on Multimedia and Expo. IEEE, 2005: 784 - 787.

[16] ALSHAHRANI M, TRAORE I. Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain [J]. Journal of Information Security and Applications, 2019, 45: 156 - 175.

[17] VARSHA P, HEMANTH K, RAUT A. Modified protocol for secure mutual authentication in IoT smart homes [C]//2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2021: 398 - 405.

[18] GOYAL V. How to re-initialize a hash chain [EB/OL]. (2006 - 12 - 30) [2023 - 04 - 01]. https: //eprint. iacr. org/2004/097. pdf.

[19] ZHANG H J, ZHU Y F. Self-updating hash chains and their implementations [J]. IEEE Lecture Notes in Computer Science, 2006, 42 (55): 387 - 397.

[20] ZHANG H J, LI X X, Ren R. A novel self-renewal hash chain and its implementation [C]//2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. IEEE, 2008, 2: 144 - 149.

[21] PARK C S. One-time password based on hash chain without shared secret and re-registration [J]. Computers & Security, 2018, 75: 138 - 146.

[22] HAN M, JIANG W. A secure communication method based on message hash chain [J]. Applied Sciences, 2022, 12 (9): 4505.

（收稿日期：2024 - 05 - 05）

作者简介：

王斌（2001 - ），男，本科，主要研究方向：抗网络空间测绘。

李琪（1998 - ），女，硕士，主要研究方向：防火墙、抗网络空间测绘。

张宇（1979 - ），通信作者，男，博士，教授，主要研究方向：互联网安全、互联网体系、互联网测量。E-mail: yuzhang @ hit. edu. cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部