基于端信息完全跳扩混合技术的多用户接入机制研究

张祚铭[1,2]，李方晓[2]，罗胜瀚[2]，石乐义[1,2]
（1. 中国石油大学（华东）海洋与空间信息学院，山东 青岛 266580；
2. 中国石油大学（华东）计算机科学与技术学院，山东 青岛 266580）

摘　要：随着网络攻击日益频繁，传统网络防御技术已经无法满足当前需求。主动防御凭借其动态随机的特性，成为当前应对网络攻击的有效方法之一。端信息完全跳扩混合技术是一种主动防御技术，通过动态随机地调整端信息，使系统在端口关闭的情况下仍能保持通信，从而具有良好的隐蔽性和安全性。然而，该技术在传输速率和用户容量方面存在不足，仅支持一对一通信。为了解决上述问题，提出了一种新的网络通信策略，即将端信息完全跳扩混合技术和稀疏码分多址接入（sparse code multiple access，SCMA）相结合，以提高系统的接入用户容量和整体传输速率。理论分析和实验结果表明，在保证良好的隐蔽性和安全性情况下，该策略提高了系统的用户数量和传输速率。

关键词：网络安全；端信息完全跳扩混合技术；主动网络防御；稀疏码分多址接入
中图分类号：TN915.08
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025104

Research on multi-user access mechanism based on end-point information hopping and spreading hybrid technology

ZHANG Zuoming[1,2], LI Fangxiao[2], LUO Shenghan[2], SHI Leyi[1,2]
1. College of Oceanography and Space Informatics, China University of Petroleum (East China), Qingdao 266580, China
2. College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266580, China

Abstract: As network attacks become increasingly frequent, traditional network defense technologies can no longer meet current demands. Active defense, relying on its dynamic and random characteristics, has become one of the effective methods to counter network attacks. The end-point information hopping and spreading hybrid technology is a type of active defense that, based on dynamically and randomly changing end-point information, allows the system to maintain communication even when ports are closed, thus providing excellent concealment and security. However, it has limitations in terms of transmission rate and user capacity, supporting only one-to-one communication. To address these issues, a new network communication strategy was proposed, which combined the end-point information hopping and spreading hybrid technology with sparse code multiple access (SCMA) to enhance the number of system-

收稿日期：2025−01−07；修回日期：2025−03−29
通信作者：石乐义，shileyi@upc.edu.cn
基金项目：国家自然科学基金资助项目（No.62111530052）
Foundation Item: The National Natural Science Foundation of China (No.62111530052)

accessible users and overall transmission rate. Theoretical analysis and experimental results show that the system's user capacity and transmission rate have been improved while ensuring good concealment and security.

Key words: network security, end-point information hopping and spreading hybrid technology, active network defense, sparse code multiple access

0 引言

随着通信技术的飞速发展，互联网已经成为人们日常生活中不可或缺的一部分。同时，网络安全也成了人们关注的焦点[1-2]。犯罪分子利用网络拦截信息、攻击设备，不仅对个人信息安全造成威胁，也对国家安全和社会稳定构成重大挑战。网络安全已成为当今社会亟待解决的问题。

端信息跳变借鉴了军事通信中跳频技术的概念[3]。通过动态变化端信息（如IP地址、端口号等），端信息跳变能够有效缓解多种攻击的威胁。作为一种主动防御技术，端信息跳变能够迷惑攻击者，增加其识别目标的难度。端信息跳变的安全程度与端信息跳变的速度有关[4]，但跳变速度受限于同步机制的性能。为了克服这一限制，研究者提出了端信息扩展的概念。

端信息扩展将同步信息分散到多个端信息包中，减少了对单一同步方式（如时间戳）的依赖，从而提高了同步的鲁棒性。即使攻击者获取了部分同步信息，也无法还原完整的通信内容。端信息完全跳扩混合技术是在端信息跳变和扩展的基础上，关闭所有端口并将所有的信息嵌入端信息中，进而达到提升系统隐蔽性、安全性的效果。端信息完全跳扩混合技术尽管提高了系统的安全性，但在多用户通信场景中仍存在扩展性限制，且由于同步开销和信息嵌入的复杂性，系统的整体传输速率较传统通信方法有所下降。针对端信息完全跳扩混合技术的缺陷，石乐义等[5]将稀疏码分多址接入（sparse code multiple access，SCMA）与之结合，通过码本解决了多用户接入的问题。但是端信息完全跳扩混合技术依然存在着以下局限性：接入用户数量较少且受到码本的限制；减少了端信息的多样性，也降低了系统的安全性。

本文提出一种结合端信息完全跳扩混合技术和SCMA的改进方法，解决这些缺陷。在改进时，有两个挑战需要面对。第一个挑战是，计算机网络和现实通信环境不同，如何让SCMA与端信息完全跳扩混合技术相结合，使得经过码本编码的信息更加适合在计算机网络传输。第二个挑战是，如何在增加用户数量的同时不降低端信息跳变的性能。

面对这两个挑战，首先，本文创新性地通过对码本的重构和端口聚合，将主动防御中的端信息完全跳扩混合技术与SCMA进一步相结合，使之更好地适应计算机网络，以增加通信中的用户数量，并提高传输速率。其次，本文利用哈希（Hash）函数压缩端口映射范围和动态随机划分通信组，在保持端信息完全跳扩混合性能的同时增加用户数量。通信组的动态随机变化让系统在通信时可以通过设置时隙实现端信息的动态变化，通信双方在编码规则、身份信息、传输的端信息进行动态变化，进一步提高了系统的安全性。

1 相关工作

相较于被动防御技术，网络主动防御是指在攻击者发起攻击之前，主动采取防范措施。其目的是在进攻和防守过程中将防守方从被动和不利的位置转变为更主动的立场。目前，国内外学者已经对网络主动防御进行了广泛的研究，主要研

究方向包括拟态防御、动态目标防御（moving target defense，MTD）、端信息跳变技术等。

网络空间拟态防御（cyber mimic defense，CMD）是在拟态防御的基础上发展而来的，采用动态异构冗余（dynamic heterogeneous redundancy，DHR）来增强系统的安全性。为在CMD中选择适当的执行模块，目前已有学者提出如博弈论[5]和基于反馈控制的动态轮换算法[6]等方法。为了解决调度器可能受到攻击的情况，也有学者提出了基于共识协议的去中心化方法[7]。

MTD通过增加网络和系统的不确定性、随机性和动态性来抵御攻击。通过有效地降低确定性、相似性和静态，MTD增强了网络空间的防御能力[8]。MTD的变化方式主要有3种：冗余、变换、突变[9]。目前，MTD已在多个领域得到应用，例如基于软件定义网络（software defined network，SDN）的动态网络重构[10-11]、利用深度神经网络（deep neural network，DNN）的智能攻击面调整[12]、结合联邦学习（federated learning）的分布式安全策略优化[13-14]等。

石乐义等[3]从军事跳频通信中得到启发，提出端信息跳变的概念，并建立了端信息跳变主动防护模型。端信息跳变技术是MTD的一种，通过在数据传输过程中不断改变通信协议、端口、IP地址等终端信息，实现网络主动防御。端信息跳变技术的核心组成部分是跳变策略和同步策略。然而，同步会限制跳变的速度。为了解决这一问题，李方晓等[15]建立了基于密码基础逻辑（cryptography fundamental logics）的快速交换MTD（fast switching MTD，CMTD）模型。该模型将MTD切换速率提高到秒级，解决了具有高隐蔽性要求的高速跳频中的同步问题。同时，石乐义等[4]提出了端信息跳扩技术，通过将认证信息扩展成多个端信息发送给接收方，舍弃了第三方，缩减了同步所需的时间，将跳变速度也提高到秒级。后续研究对端信息跳扩的多个方面进行分析，以提高其性能。例如，在端信息跳扩混合传输文件过程中[16]，解决大文件传输问题。和SDN相结合，提高端信息跳扩混合机制的安全性[17]。利用端信息跳扩建立隐蔽通信[18]，实现高速跳变的隐蔽通信。再就是和本文密切相关的基于SCMA的端信息扩展序列研究，通过和SCMA相结合，提高接入用户数量。本文和现有研究的不同之处在于：（1）系统容纳的用户数量不受码本限制，可以同时应用多个码本增加接入用户数量；（2）系统可以随机组合不同码本和随机分配用户，增加端信息的多样性和变化，提高传输的安全性。

SCMA是一种新型的非正交多址接入（non-orthogonal multiple access，NOMA）技术。在众多NOMA方案中，SCMA因其支持过载传输的能力而脱颖而出，即在用户数量超过可用资源数量的情况下仍能实现高效通信。这一特性显著提高了频谱利用率，使其能够很好地满足5G[20]网络对海量连接的需求。在SCMA系统中，调制和扩频操作通过码本映射同时完成：输入数据直接映射到预先设计的码本中码字，而码本的设计则基于多维星座图优化[21-23]。目前，SCMA已在多个领域得到应用，例如，在物联网中，SCMA用于支持大规模设备连接[24]；在计算机网络中，它被用来提升系统的用户容量。然而，现有的SCMA方案仍存在一些局限性：一方面，它主要服务于少量用户的场景；另一方面，其码本设计通常是静态的，难以适应动态变化的网络环境。

2　基于端信息完全跳扩混合技术的多用户接入模型

2.1　通信模型

将端信息完全跳扩混合技术与SCMA结合，系统能利用主动防御动态、随机的特性来快速和随机地调整端信息，这使得攻击者很难准确地识

别和监控目标。此外，系统还允许多个客户端和服务器之间的通信。并且，这种通信方式可以选择性地关闭防火墙中的特定或全部端口，有效地抵御了大多数网络攻击。

整体通信模型如图1所示。该模型包括1个服务器和多个客户端。服务器可以在通信过程中关闭特定的端口，这个做法虽然提高了系统的安全性，但也使得系统无法使用传统的通信方法传输信息。对此，系统采用了端信息作为信息的载体，通过相关设置，服务器在端口关闭的情况下依然能获取到信息。

系统中的服务器端由动态码本生成、消息预处理、身份验证、端信息流生成与解析、通信组的动态变化这5个模块组成。这5个模块分别对应于码本生成、加密、认证、传输和动态变化。客户端的模块与服务器类似，但有2个地方不一样：一是身份认证，客户端需要生成认证信息的扩展端信息流；二是端信息的动态变化，客户端会根据设置的时隙，动态、随机地变化除了端口之外的端信息。

通信的整体流程如图2所示。在通信系统中，服务器和客户端都进行初始准备，配置IP地址和基础码本。随后，客户端生成端信息序列形式的认证数据包，并发送给服务器。服务器一旦收到认证信息，就开始验证这些数据包。认证成功的客户端被分配到空余的通信位置，未认证成功的数据包则被丢弃。在通信过程中，客户端可以在指定的时间动态调整端信息包的IP地址等端信息。同时，服务器可以为每个客户端调整通信参数，增加变化。服务器调整完成后，会将新的参数发往客户端进行参数的更新。

2.1.1 重构码本

在通信开始之前，服务器和客户端必须配置一些基本的码本。在SCMA中是通过增加欧几里得距离来设计码本，提升其在实际信道中的性能。但是，由于计算机网络不同于物理通道，因此需要对码本进行重新设计。

一台计算机通常有65 536个端口，为了减少干扰和降低解码的负担，避免使用常用端口来接收端信息包，因此，星座图将64 516个点均匀分布在x轴和y轴上，如图3所示。图3上的x和y坐标范围为−127到127，每个点对应一个端口。每个端口由一个16位二进制数表示，其中高8位表示x坐标，低8位表示y坐标。8位中的最高位作为符号位，负的设置为1，正的设置为0。然后通过分割星座图生成码本，在生成码本时要确保每个码本中的点是唯一的，没有重复。

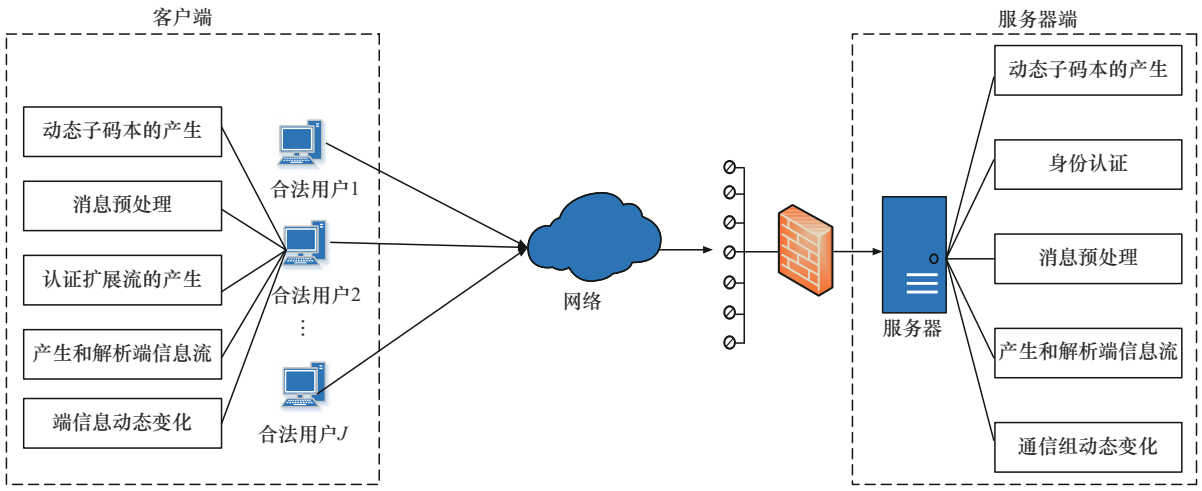

图1 整体通信模型

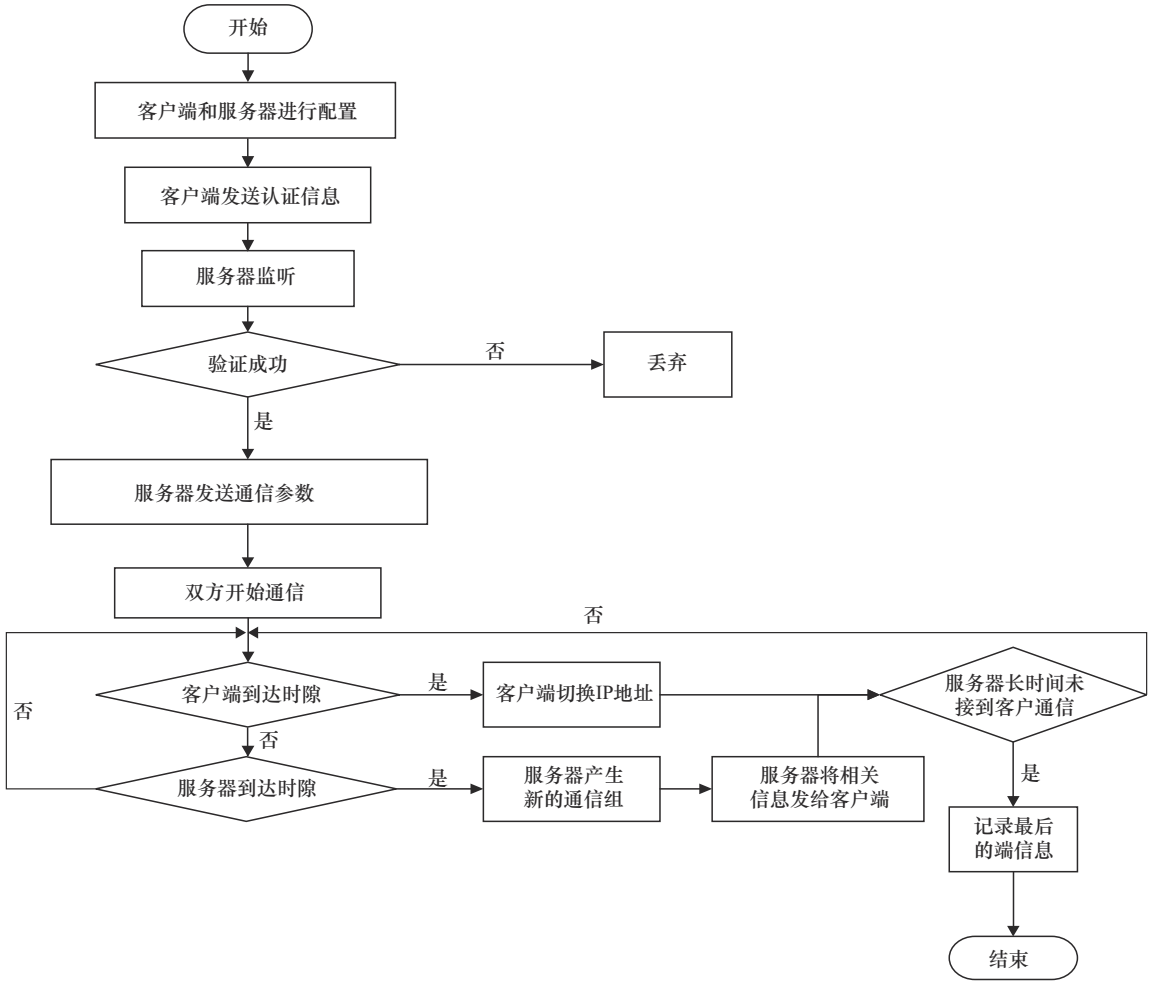

图2　通信的整体流程

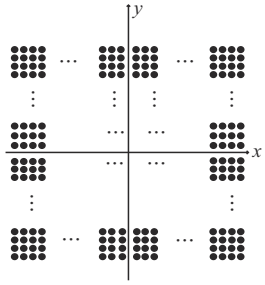

图3　星座图

2.1.2　通信组

在SCMA中，码本虽然使系统能够为多个客户端提供服务，但也会影响系统容量。为了克服这一限制并适应更多的用户，可利用通信组来分配端口资源。根据分配的码本大小和配置，这些组可以服务不同数量的客户端。这种方法可以更灵活地进行网络管理，满足不同的客户端需求，并保证可用端口资源的高效使用。

系统将端口划分为不同的通信组，并选择一组端口来组成4个通信组。通信组的构成如图4所示。这种划分可以根据不同组的容量进行组合，以有效分配端口资源。每个通信组都有不同的最大容量，这决定了它所包含的端口数量。例如，通信组2配置了4个通道，每个通道包含4个端口，该组使用的端口总共有16个。

每个通信组都有4个参数：用户标识（User_ID）、子码本、通道端口和通道宽度。通道宽度是一个固定的参数，用来平衡可用的端口资源和效率。当用户被分配到不同的组时，他们有2个参数用来作为身份的标志：User_ID和通道

端口。User_ID来源于码本。服务器从稀疏矩阵中选择User_ID并使用它来检索相应的子码本。码本的稀疏矩阵如图5所示。例如，客户端A被随机分配{0011}作为其User_ID。通道端口则是通道的第一个端口。这2个参数在身份识别上各有作用，User_ID是用来进行组内区分，通道端口用来区分不同的组。

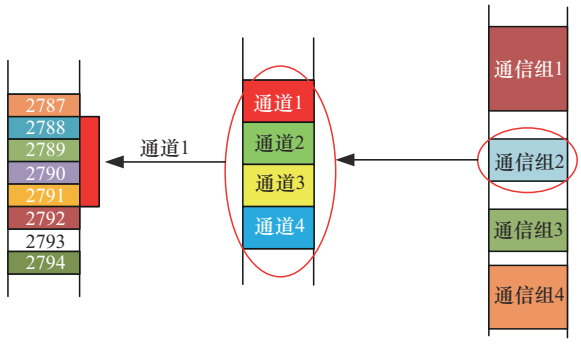

图4　通信组的构成

$$\boldsymbol{F}_{6\text{-}4}=\begin{bmatrix}0&1&0&1&0&1\\0&0&1&1&1&0\\1&0&1&0&0&1\\1&1&0&0&1&0\end{bmatrix}_{4\times6}$$

图5　码本的稀疏矩阵

2.2　服务器模块

服务器流程如图6所示。在通信开始之前，服务器必须做一定的准备工作。服务器端配置了多个IP地址，这增加了攻击者定位目标的难度。然后，系统会划分一个通信组作为准备。一旦准备工作完成，服务器就开始通过配置的IP地址侦听所有传入的数据包。当数据包从未记录的IP地址到达特定端口时，服务器便会验证数据包的发送者。如果客户端被识别为非法用户，这些数据包将被丢弃。相反，如果客户端被验证为合法，则服务器会分配参数并发送给客户端。与此同时，服务器还会不断地侦听所有传入的数据包，并评估其有效性。正确的数据包会被存储在缓冲区中，而不正确的数据包则被丢弃。此外，在通信过程中，服务器会在到达指定的时隙时调整通信组的参数。

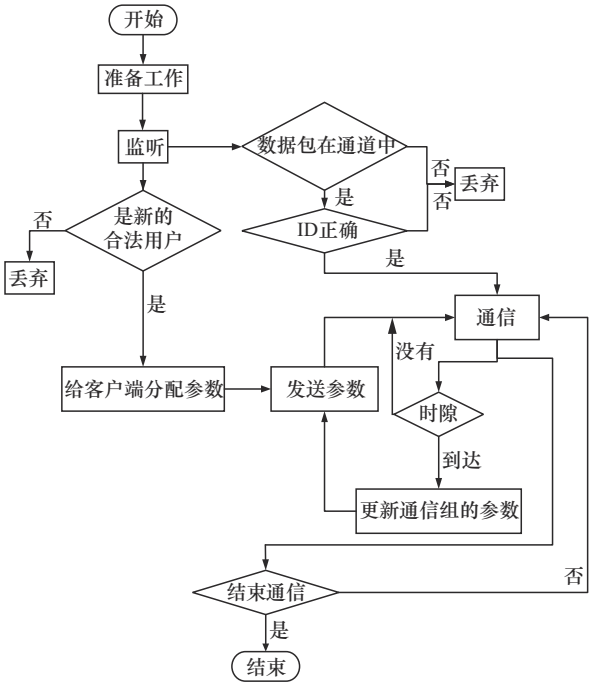

图6　服务器流程

服务器模块由6个部分组成：准备工作、认证扩展流的验证、动态子码本、信息预处理、端信息生成与解析和通信组动态变化。

2.2.1　认证扩展流的验证

当一个新的客户端试图与服务器建立连接时，它首先发送一个身份验证序列。服务器不断地侦听传入的数据包，获取这个序列并进行验证。首先，服务器从特定的、预先商定的端口接收数据包，先查看IP地址。如果该IP地址已经在服务器的记录中，则使用解码规则验证其合法性。对于新的IP地址，服务器先检查源端口以确定接收到的数据包是否确实是身份验证数据包。如果数据包包含身份信息，服务器将开始计数，累计从该客户端正确接收的数据包。一旦从客户端正确接收到的数据包数量超过预定的阈值，则这个客户就会被识别为合法用户，从而允许它们继续进行进一步的通信活动。这个过程确保只有经过验证的用户才能与服务器建立连接。在成功完成身份验证过程之后，服务器将客户随机分配到空余的通信组内，然后向客户端分发通信组参数。

2.2.2　动态子码本

服务器的基础码本作为创建动态子码本的基础模板，在客户端通过身份验证后，会生成一个随机数，即新的子码本。通过引入随机变量增加码本的变化，从而增强安全性。随机数的取值范围为−127 ~ 127，分为2个8位段：高8位和低8位。最高位作为符号位，表示该值是正还是负，其余的位表示该值的大小。使用这些值，服务器调整为用户指定的子码本中的x和y值。

2.2.3　端信息生成与解析

当服务器打算向客户端发送信息时，系统使用经过信息预处理生成的二进制序列进行编码。由于星座图上的星座点是分散的，因此映射的端口范围也是离散的，这就导致了端口资源的浪费，而且码本很容易被破解。为了优化端口利用率和提高安全性，系统采用了Hash函数。这有助于压缩端口范围，将编码映射到更小、更易于管理的范围来提高效率，然后将信息调制到不同的信道。系统利用Hash函数和调制技术来进一步增加客户端数量。Hash函数缩小了最大端口和最小端口之间的范围，从而增加了攻击者攻击的难度，而调制技术增加了端信息的变化范围。

对于接收方来说，其主要目标是从由端信息数据包、其他正常通信数据包、攻击数据包、噪声数据包等多种类型数据包组成的数据流中提取准确的端信息。当服务器接收到来自网络的数据包时，它首先检查源端口，以确定它是否是身份验证序列的一部分。如果不是，则服务器检查目的端口号。如果这个端口属于一个有效的通道，服务器将检查下一个参数；如果不是，则立即丢弃该报文。接下来，服务器读取数据包的源端口，获取User_ID。如果与通道关联的User_ID不匹配，就丢弃数据包。一旦所有检查通过，系统则将端信息存储在缓冲区中。考虑到数据包使用用户数据报协议（user datagram protocol，UDP），这可能导致传输混乱，系统会在缓冲区内按照正确的顺序重新排列数据包。最后，服务器按正确的顺序解码。

2.2.4　通信组动态变化

为了提高信息传输的安全性，服务器采用动态变化参数的方式。在每个时隙，服务器都会更新通信组的参数，并将其重新分配给客户端。服务器会根据当前客户端数量，随机生成不同的通信组，而且要有空闲的冗余，来承接后面新建立连接的客户端。在分配的过程中，客户的身份信息和编码用的码本都会重新生成、更新。这样，一个客户端在通信过程中用于表明身份的信息是在变化的，即使攻击者掌握了当前的身份信息，在下一个时隙到达，当前的身份信息便会失效，码本也是。

2.3　客户端模块

在通信过程中，每个客户端从IP地址池中分配多个唯一的IP地址，以确保不会与其他客户端的IP地址重叠。当客户端希望向服务器传输信息时，它从其IP地址池中选择一个IP地址。然后，将嵌入端信息包中的身份验证序列发送给服务器，并侦听来自服务器的数据包。客户端接收到参数后，使用新的码本生成端信息流，与服务器建立通信。在整个通信过程中，客户端可以在时隙到达时动态更改其IP地址。它对服务器传输的任何参数变化保持关注，并在收到这些数据包后相应地更新其通信参数。客户端的运行流程如图7所示。最后，如果客户端和服务器没有通信，客户端将记录最后的参数，用于后续通信。

该客户端由5个部分组成：信息预处理、子码本生成、认证流生成、终端信息流传输、时隙。其中，信息预处理过程、新码本生成、编码和解码功能与服务器的相同，但是扩展身份验证流的生成和端信息动态变化则与服务器不同。

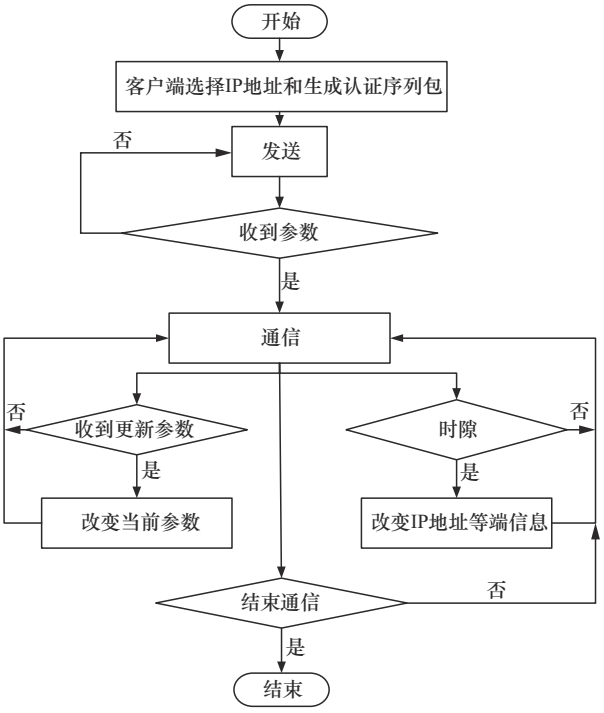

图7　客户端的运行流程

2.3.1　扩展身份验证流的生成

扩展身份验证流是通过生成一系列分散的二进制数据包来创建的，这些数据包用于在与服务器通信期间验证客户端的身份。通信双方在通信前约定好相应的生成方式，以保证验证的安全性。

2.3.2　端信息动态变化

客户端的时隙决定了何时更改其IP地址。在指定时间，客户端在部分端信息不变的情况下，从其IP地址池中随机选择一个IP地址。服务器端和客户端都可以在通信过程中修改终端信息的IP地址，增强了系统的整体安全性。

3　实验与分析

本文提出的方案主要是为了增加系统的用户数量，提高系统的总体传输速率。本节测试系统的安全性和多用户下的传输速率。

3.1　系统设置

基于端信息完全跳扩混合技术主动防御的多用户接入机制的原型系统分为客户端、服务器端和攻击者，均使用Linux操作系统，系统版本为Ubuntu 18.04，编程语言为C。原型系统使用Socket实现发送端和接收端之间的信息传输。系统配置见表1。

表1　系统配置

设备	内存	操作系统	处理器
服务器	4 GB	Ubuntu22.04	Intel® Core™ i5
攻击者	2 GB	Kali	Intel® Core™ i5
客户端(1～6)	2 GB	Ubuntu22.04	Intel® Core™ i5

本文采用以下方法获取所用码本：分割星座图获取码本示意图如图8所示。在图2的星座图上画一个圆圈，再将圆圈平均分成12份，选取分割点相近的星座点作为码元，共计12个点，见表2。然后映射到端口，见表3，所有的星座点转换为端口，最后得到3个基础码本。

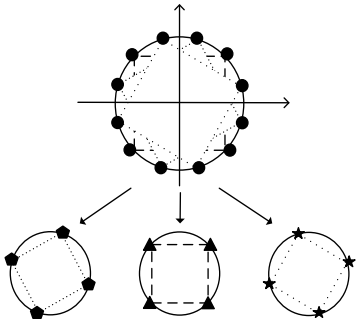

图8　分割星座图获取码本示意图

表2　星座图上的点

码元	00	01	10	11
Sub-codebook1	(−120,0)	(0,120)	(120,0)	(0,−120)
Sub-codebook2	(−104,60)	(60,104)	(104,−60)	(−60,−104)
Sub-codebook3	(−60,104)	(104,60)	(104,60)	(−104,−60)

表3　映射的端口

码元	00	01	10	11
Sub-codebook1	63 488	120	30 720	248
Sub-codebook2	59 452	15 464	26 812	48 360
Sub-codebook3	48 232	26 684	15 592	59 580

3.2　模型的性能验证与分析

3.2.1　抗攻击性

在实验中，使用拒绝服务攻击TCP通信、基于SCMA的端信息完全跳扩混合模型、MTD和本文提出的模型。由于传统通信端口是开放的，因此当有大量的报文访问时，服务器很容易崩溃，本文的模型在实验中表现更好的抗攻击性能。

本次服务器攻击实验使用的是hping3。配置攻击强度范围为0～20 Mbit/s的TCP洪泛攻击。攻击包被设计为空，完成信息传输时间以端信息被成功解码的时间为标准。传输的数据都是1 000 bit。不同TCP洪泛攻击速率下各模型完成信息传输的时间如图9所示。

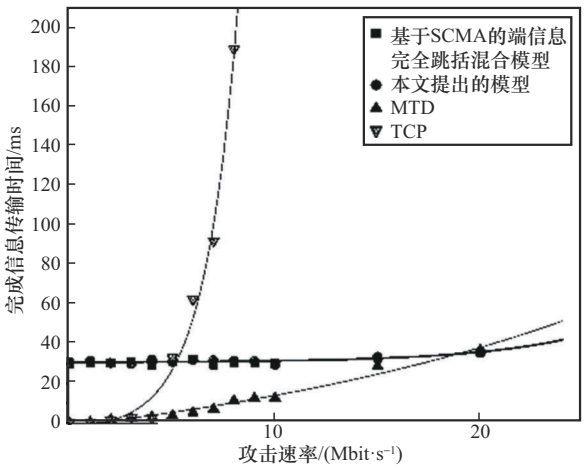

图9　不同TCP洪泛攻击速率下各模型完成信息传输的时间

由图9可知，当攻击速率在5 Mbit/s以下时，TCP很快就完成了信息传输，但是本文的模型花费更多的时间来完成同样的工作。然而，随着攻击速率的增加，TCP传输时间也在增加，而本文提出的模型完成信息传输的时间却很稳定。当攻击速率达到5 Mbit/s时，TCP发送1 000 bit的时间急剧增加。当攻击速率超过6.3 Mbit/s后，TCP完成信息传输的时间开始超过本文提出的模型。当速率达到7 Mbit/s时，TCP出现通信失败，而本文提出的模型仍保持正常的通信。MTD在3 Mbit/s之前和TCP相近，表现比本文模型要好，但随着攻击速率增加，MTD完成的时间也在增加，逐渐接近于本文提出的模型，这是因为MTD在传输时并不关闭端口，随着攻击强度的增加性能会逐渐下降。基于SCMA的端信息完全跳扩混合模型表现和本文模型差不多，只是时间略有减少，这是因为SCMA的码本是预先分配好的。

系统在不同UDP洪泛攻击速率下的传输完成时间见表4。由于此次采用盲目攻击，攻击者的目标端口不一定是通信端口，因此时间花费小于TCP时间。只有在30 Mbit/s时，部分端口在短时间内被攻击到，时间有所上升。

表4　不同UDP洪泛攻击速率下传输完成时间

UDP洪泛攻击/(Mbit·s^{-1})	攻击包的数量	时间/ms
0	0	14.133 99
10	20 887.8	15.278 62
20	22 090	15.514 34
30	33 017.3	16.340 72
40	46 913.3	15.594 12
50	51 051.2	15.789 50

3.2.2　隐蔽性

不同通信模式的网络矩阵如图10所示。正常的通信通常是点对点的，如图10（a）所示。这种通信方式很容易被攻击者监控和攻击。端信息跳变通过跳变服务器改变连接的IP地址和端口，实现一对多通信，如图10（b）所示。然而，攻击者虽然无法验证变化端，却可以从固定端收集信息。在本文提出的模型中，通信两端都能动态地调整端信息。在生成扩展端信息序列数据包时，可以动态更改自己的IP地址，并随机选择目的IP地址。无论监控的是哪一端，攻击者都无法识别目标，如图10（c）所示。

TCP模型的通信方式是一对一的，攻击者很容易找到目标。端信息跳变增加目的地址以迷惑攻击者。本文的模型在通信方面有更多的变化。在此次测试实验中，客户端有2个IP地址：192.168.17.136和192.168.17.137。服务器有3个地址：192.168.17.138、

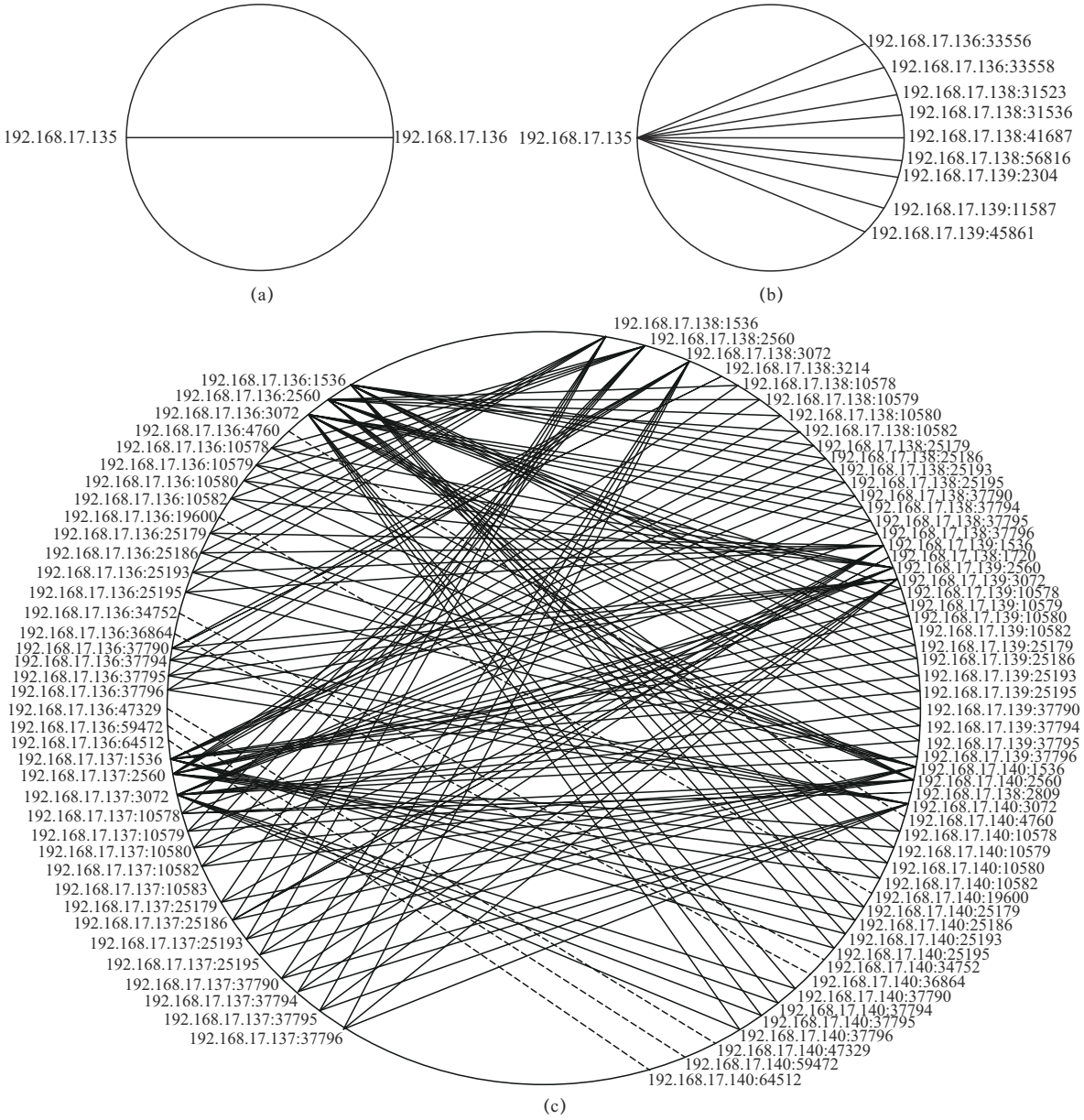

图10　不同通信模式的网络矩阵

192.168.17.139和192.168.17.140。通信组有2个时隙。图10（c）中实线表示双方通信传输的端信息包；虚线为客户端发送到服务器端的认证端信息包；点表示服务器发送通信组参数。在实验过程中，服务器只改变组参数2次，总共涉及大约70个端口。

在相同的IP地址资源、跳变次数下，不同模型的IP地址和端口数统计如图11所示。MTD、基于SCMA的端信息完全跳扩混合模型和本文提出的模型，其接收端都配置3个IP地址。不同之处在于对于端口的应用，MTD采用了TCP传输，其源端口和目的端口只有1个；基于SCMA的端信息完全跳扩混合模型通过码本编码，需要4个目的端口作为信息的载体，在通信过程中码本不变化，故整个通信过程中只有4个目的端口；本文提出的模型，由于添加了端口的动态变化，用到了12个目的端口。相比之下，本文模型在端信息上表现出更多的变化，有更强的隐蔽性。

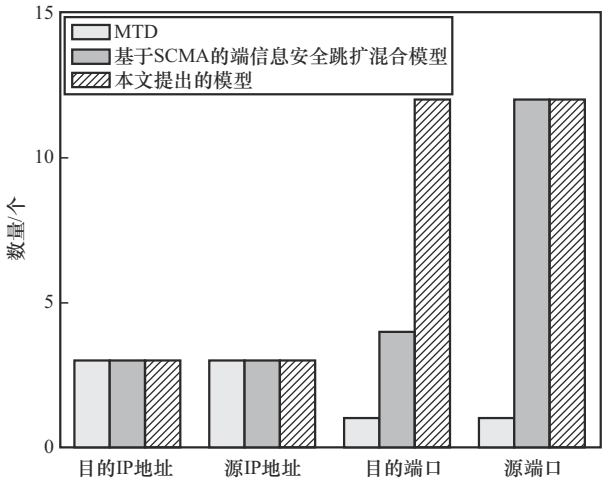

图 11　不同模型下的 IP 地址和端口数统计

3.2.3　对不同攻击的性能分析

在攻击时，攻击者通常通过发送过量的请求来耗尽服务器资源，进而使计算机崩溃。然而，模型可以在通信时关闭所有端口以拒绝其服务请求。但是系统从端信息包中获取信息，因此也会受到带宽攻击的影响。

DoS 攻击：对攻击者而言，攻击者不知道跳变图案，只是随机选择一个端口进行攻击，其所有的攻击都是盲目攻击。对系统来说，当攻击的端口与通信组中端口无关时，系统会丢弃，这样不会消耗很多资源。但如果端口正好是通信组的端口，则需要花费更多的时间和资源进行判断。假设可用 IP 地址数为 m，可用端口数为 n，通信端口数为 x，协议数为 I，时隙周期为 t，通信时间为 s，在一段时间内，攻击者的攻击成功率为：$P=\left(\frac{x}{mnI}\right)^{\frac{s}{t}}$。在通信中，$mn$ 显示的是地址，它的范围比较大，一般情况下，$n>50\,000$，且 $m\geqslant 3$。s/t 为通信组参数变化的次数。因此，攻击者的成功概率较低，且攻击者在一段时间内连续攻击成功的概率会随着时隙变化次数的增加而降低。

跟随攻击：此时系统的安全性取决于通信组的变化速率。假设通信中相邻 2 次变化之间的时间为 $T1$，从获得最终信息到攻击的总时间是 $T2$。当 $T1<T2$ 时，攻击者很难确定动态服务器的结束信息。在这种情况下，攻击者在发起攻击之前已经改变了活动端口。因此，攻击无效。即使攻击者发起攻击时，端口不跳。当攻击到达系统时，由于网络延迟，端信息很可能已经发生了变化。攻击者的推断可以忽略不计。因此，可以认为当 $T1<T2$ 时，攻击者对系统成功发起后续攻击的概率为 0。

当 $T1\geqslant T2$ 时，系统可以提高组参数变化的速度。变化周期 $T1$ 越小，攻击者成功的概率越低。在系统中，$T1$ 包括传输端信息时间和参数变化时间。服务器在通信期间先配置好参数，并在时隙到达时更新，然后发送到客户端。客户端收到后进行解析和更新。由于变化的参数只有 2 个，这个过程的时间可以忽略不计，变化周期的大部分时间花在传输上。在局域网中，客户端和攻击者距客户端的距离不会相差太多，因此即使 $T1\geqslant T2$，攻击者造成的影响也是比较小的。

3.2.4　不同攻击速率下的误码率

误码率是通信性能的一个重要指标。此次实验测试了本文模型和其他类似的通信模型在不同 UDP 洪泛攻击速率下的误码率，如图 12 所示，由于最终会将传输的比特转为字符，所以统计的误码率是 SER（symbol error rate）。

模型 1 由 Gimbi 提出，它将信息加载到源端口进行传输。服务器端使用源端口的差异进行解码，但是解码时会产生连锁反应，误码率随着错误的增加而急剧上升。在模型 2 中，原始信息被加载到源 IP 地址进行传输，并且每个 IP 地址之间是相互独立的。虽然不会对服务器的解调产生连锁反应，但错误也会直接导致原始信息的丢失，因此模型 2 的解码精度略好于模型 1。在本文提出的模型中，将某一原始信息扩展为由不同的数据包表示，这些数据包相互独立，因此系统可以在一定范围内承受丢包对系统的影响，同时本身的安全性减缓了攻击的影响，在高攻击速率下的表现要远好于其他两种模型。

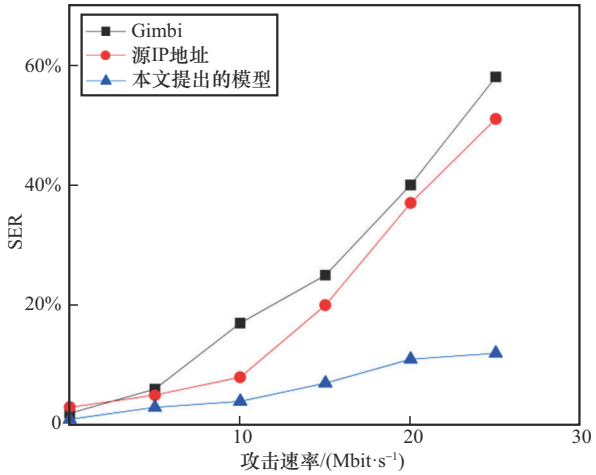

图12　不同UDP洪泛攻击速率下的SER

3.2.5　多用户的传输速度

服务器获取端信息并对序列进行解码的速率取决于数据包的数量和传输时间。当网络环境稳定时，速率随客户端数量的增加而降低。因为更多的客户端会发送更多的端信息包，而系统也会花费更多的时间。

为测试本文提出的模型在多用户中的传输速率，设置单个用户在通信用户数量为0~20个时，完成1 000 bit的传输时间。多用户的传输时间如图13所示。

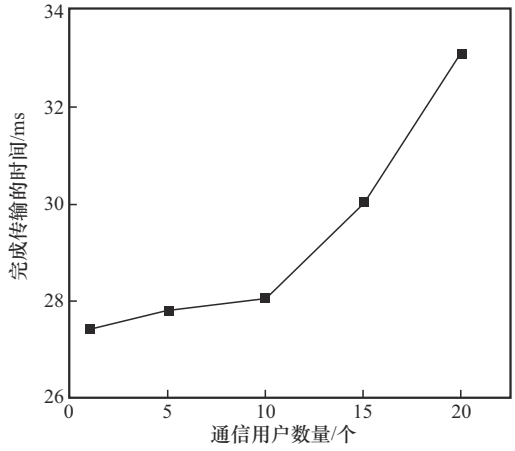

图13　多用户的传输时间

由图13可知，用户越多，系统花费时间也越长。一个用户的时候只需花费27.417 ms就可以完成1 000 bit信息的传输。当系统有20个用户时，时间将超过33 ms。

4　结束语

本文针对端信息完全跳扩混合技术中存在的传输效率低及不支持一对多通信的问题，提出了一种基于稀疏码多址接入技术的多用户接入机制。将稀疏码多址接入技术和端信息完全跳扩技术结合，提高端信息的利用率，实现信道复用，增加系统的用户数量，进而提高整体的传输效率。经过实验和性能分析，本机制增加了系统的接入用户数量，提高了系统的整体传输速率。同时，在面对攻击时，系统有着良好的表现，可以抵御大部分的攻击，并缓解带宽攻击的影响。未来，研究将进一步和人工智能相结合，提高动态变化的效率，提升机制的适应性与可扩展性。

参考文献：

[1] AGGARWAL N, ALBERT L J, HILL T R, et al. Risk knowledge and concern as influences of purchase intention for Internet of things devices[J]. Technology in Society, 2020(62) 101311.

[2] 张同须, 余立. 信息通信技术若干发展趋势[J]. 电信科学, 2024, 40(4): 151-159.
ZHANG T X, YU L. Development trends of information and communication technology[J]. Telecommunications Science, 2024, 40(4): 151-159.

[3] 石乐义, 贾春福, 吕述望. 基于端信息跳变的主动网络防护研究[J]. 通信学报, 2008, 29(2): 106-110.
SHI L Y, JIA C F, LYU S W. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29 (2): 106-110.

[4] 石乐义, 郭宏彬, 温晓, 等. 端信息跳扩混合的主动网络防御技术研究[J]. 通信学报, 2019, 40(5): 125-135.
SHI L Y, GUO H B, WEN X, et al. Research on end hopping and spreading for active cyber defense[J]. Journal on Communications, 2019, 40(5): 125-135.

[5] CHEN Z Q, CUI G, ZHANG L, et al. Optimal strategy for cyberspace mimic defense based on game theory[J]. IEEE Access, 2021(9) 68376-68386.

[6] 陈福才, 周梦丽, 刘文彦, 等. 云环境下面向拟态防御的反馈控制方法[J]. 信息网络安全, 2021, 21(1): 49-56.
CHEN F C, ZHOU M L, LIU W Y, et al. Feedback control method for mimic defense in cloud environment[J]. Netinfo Security, 2021, 21(1): 49-56.

[7] MENG Z, DU J Y, GUO W, et al. A decentralized cyber mimic defense architecture based on consensus protocol[C]//Proceedings of the 2023 4th Information Communication Technologies Conference (ICTC). Piscataway: IEEE Press, 2023: 143-150.

[8] ZHENG Y, LI Z, XU X L, et al. Dynamic defenses in cyber security: techniques, methods and challenges[J]. Digital Communications and Networks, 2022, 8(4): 422-435.

[9] HONG J B, KIM D S. Assessing the effectiveness of moving target defenses using security models[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 163-177.

[10] GAO C G, WANG Y J, XIONG X L, et al. MTDCD: an MTD enhanced cyber deception defense system[C]//Proceedings of the 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). Piscataway: IEEE Press, 2021: 1412-1417.

[11] MARTÍNEZ BELTRÁN E T, SÁNCHEZ SÁNCHEZ P M, LÓPEZ BERNAL S, et al. Mitigating communications threats in decentralized federated learning through moving target defense[J]. Wireless Networks, 2024, 30(9): 7407-7421.

[12] HYDER M F, FATIMA T, ARSHAD S. Towards adding digital forensics capabilities in software defined networking based moving target defense[J]. Cluster Computing, 2024, 27(1): 893-912.

[13] QIU Y H, WU J, MUMTAZ S, et al. MT-MTD: muti-training based moving target defense trojaning attack in edged-AI network[C]//Proceedings of the ICC 2021 - IEEE International Conference on Communications. Piscataway: IEEE Press, 2021: 1-6.

[14] FENG C, CELDRÁN A H, VUONG M, et al. Voyager: MTD-based aggregation protocol for mitigating poisoning attacks on DFL[C]//Proceedings of the NOMS 2024-2024 IEEE Network Operations and Management Symposium. Piscataway: IEEE Press, 2024: 1-9.

[15] LI F X, SHI L Y, ZHAO Y C, et al. CMTD: a fast moving target defense scheme based on CFL authentication[J]. IEEE Internet of Things Journal, 2025, 12(1): 822-833.

[16] 侯博文, 郭宏彬, 石乐义. 基于端信息跳扩混合的文件隐蔽传输策略[J]. 计算机研究与发展, 2020, 57(11): 2283-2293.
HOU B W, GUO H B, SHI L Y. File covert transfer strategy based on end hopping and spreading[J]. Journal of Computer Research and Development, 2020, 57(11): 2283-2293.

[17] 宋煜枭. 基于SDN的端信息跳扩混合技术研究[D]. 东营: 中国石油大学(华东), 2021.
SONG Y X. Research on hybrid technology of end information hopping and spreading based on SDN[D]. Dongying: China University of Petroleum (East China), 2021.

[18] 马荣. 基于端信息完全跳扩混合的隐蔽通信研究[D]. 东营: 中国石油大学(华东), 2021.
MA R. Research on covert communication based on complete hopping and spreading of end information[D]. Dongying: China University of Petroleum (East China), 2021.

[19] 石乐义, 兰茹, 段鹏飞, 等. 基于SCMA的端信息扩展多用户安全通信系统研究[J]. 计算机研究与发展, 2021, 58(11): 2444-2455.
SHI L Y, LAN R, DUAN P F, et al. End spreading multi-user secure communication system based on SCMA[J]. Journal of Computer Research and Development, 2021, 58(11): 2444-2455.

[20] 周立, 刘喜庆. 基于CP-free OFDM的上行SCMA收发机设计和性能分析[J]. 电信科学, 2021, 37(6): 23-32.
ZHOU L, LIU X Q. Transceiver design and performance analysis for uplink SCMA based on CP-free OFDM[J]. Telecommunications Science, 2021, 37(6): 23-32.

[21] MERIEM A, ANAS H, ADNANE L, et al. Design of SCMA codebook based on QAM segmentation constellation[M]// International Conference on Advanced Intelligent Systems for Sustainable Development. Cham: Springer, 2023: 320-327.

[22] ZHANG X W, ZHANG D L, YANG L Q, et al. SCMA codebook design based on uniquely decomposable constellation groups[J]. IEEE Transactions on Wireless Communications, 2021, 20(8): 4828-4842.

[23] MADHURA K, RUKMINI M S S, RAUT R. Irregular SCMA codebook design approaches[J]. Wireless Personal Communications, 2023, 131(3): 2019-2037.

[24] LIU P T, AN K, LEI J, et al. Computation rate maximization for SCMA-aided edge computing in IoT networks: a multi-agent reinforcement learning approach[J]. IEEE Transactions on Wireless Communications, 2024, 23(8): 10414-10429.

[作者简介]

张祚铭（1998- ），男，中国石油大学（华东）海洋与空间信息学院硕士生，主要研究方向为网络安全。

罗胜瀚（2001- ），男，中国石油大学（华东）计算机科学与技术学院硕士生，主要研究方向为信息安全、软件定义网络。

李方晓（1999- ），男，中国石油大学（华东）计算机科学与技术学院博士生，主要研究方向为信息安全、认证。

石乐义（1975- ），男，博士，中国石油大学（华东）海洋与空间信息学院教授、博士生导师，主要研究方向为信息安全、主动防御、博弈理论。