计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2021.20210615
58(11):2444-2455,2021

基于 SCMA 的端信息扩展多用户安全通信系统研究

石乐义[1,2] 兰 茹[1] 段鹏飞[1] 韩 强[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)
(shileyi@upc.edu.cn)

End Spreading Multi-User Secure Communication System Based on SCMA

Shi Leyi[1,2], Lan Ru[1], Duan Pengfei[1], and Han Qiang[2]
[1](*College of Oceanography and Space Informatics, China University of Petroleum, Qingdao, Shandong* 266580)
[2](*College of Computer Science and Technology, China University of Petroleum, Qingdao, Shandong* 266580)

Abstract End spreading technology uses a sequence of multiple end information to represent the identity information, and each piece of end information was irrelevant to the information it conveys. Thus it can hide the real information of the user. However, the end spreading sequence has the problems of low resource utilization, poor autocorrelation and unable to realize secure communication among multiple users. The sparse code multiple access (SCMA) technology is introduced into the generation process of end spreading sequence, establish the system model of end spreading multi-user secure communication system based on SCMA, and elaborating on the codebook design allocation strategy and code-word loading and sending strategy designed in the model. After that, the prototype system is analyzed and experimentally verified from two aspects of security capability and quality of communication service. The experiment result shows that, end spreading multi-user secure communication system based on SCMA realizes the covert transmission of user information, and the receiver can correctly distinguish user information. With sparse coding, the system has a low error rate and good transmission performance under certain overload conditions.

Key words sparse code multiple access (SCMA); end spreading technology; network security; resource utilization rate; multi-user communication

摘 要 端信息扩展技术使用多项端信息组成的扩展序列来表示身份信息,各项端信息与所传递的数据本身无关,从而隐藏用户的真实信息.然而,端信息扩展序列资源利用率低、自相关性弱,无法实现多用户并发安全通信.对此,将稀疏码多址接入(sparse code multiple access, SCMA)技术引入端信息扩展序列生成过程中,提出基于 SCMA 的端信息扩展多用户安全通信系统模型,详细阐述了模型中的码本设计分配、码字加载发送策略.进一步,从安全性能和通信服务质量 2 方面对原型系统进行理论分析和实验验证.实验结果表明:基于 SCMA 的端信息扩展多用户安全通信系统可实现用户信息的隐蔽传输,服务器端能够正确区分用户信息.采用稀疏编码后,系统具有较低误比特率,且在一定过载条件下,仍具有良好的传输性能.

收稿日期:2021-06-10;**修回日期**:2021-07-29
基金项目:国家自然科学基金项目(61772551);山东省自然科学基金项目(ZR2019MF034)
This work was supported by the National Natural Science Foundation of China (61772551) and the Natural Science Foundation of Shandong Province (ZR2019MF034).

关键词 稀疏码多址接入;端信息扩展技术;网络安全;资源利用率;多用户通信

中图法分类号 TP393

在通信网络的建设中,提高信息传输的可靠性和安全性是研究领域的研究重点[1].近年来,传统的网络防御技术包括防火墙技术、入侵检测技术、数据灾备技术等,虽然在一定程度上提供了安全保障,但由于其静态、被动的特点,无法更好地应对自动化和多样化的网络攻击,在安全防护方面显得越来越"心余力绌"[2].

面对互联网通信中的安全问题,课题团队在2008年提出了端信息跳变[3](end hopping)概念,通过动态地、伪随机地改变通信过程中的端口、IP 地址、跳变算法、时隙来迷惑攻击者,实现主动网络防御.随后提出了端信息扩展[4](end spreading)的概念,将数据通过端信息扩展算法进行转换,用多项端信息(IP 地址、端口、协议等)组成序列的方式来表示一条数据,各项端信息与所表示的数据本身没有关系,达到隐藏真实信息的目的.进而在此基础上提出端信息跳扩(end hopping and spreading)混合技术[5].利用端信息扩展序列进行同步认证,实现高隐蔽性要求下的高速跳变同步.

目前,针对端信息扩展技术的研究大多关注于利用端信息扩展技术提高系统的隐蔽性和在复杂网络环境中的抗攻击性能,而忽略了各类端信息的资源利用率低、自相关性弱,无法实现多用户并发通信等问题.因此,在万物互联的时代,除了关注如何提高信息的隐蔽性还需要关注隐蔽信息传输的效率问题.本文结合稀疏码多址接入(sparse code multiple access, SCMA)技术来保证用户利用端信息扩展序列进行高隐蔽通信的同时,实现多用户并发通信,降低系统误码率,提高系统传输效率和资源利用率.

1 相关工作

安全性和高效性是通信领域关注的 2 个重要指标,也是研究领域的研究重点.

在保障信息传输安全性方面,主动网络防御技术成为研究领域的热点.相关研究工作包括移动目标防御(moving target defense, MTD)[6]技术、拟态安全防御(mimic security defense, MSD)[7]技术及端信息跳变技术.其中,端信息跳变技术灵感来源于军事跳频通信对抗技术.文献[8]从攻击面动态转移角度剖析了移动目标防御技术,并将端信息跳变技术归类为移动目标防御网络中的动态转移技术.近年来,端信息跳变技术在研究领域受到广泛的关注,分别与 P2P(peer to peer),SDN(software defined network),IPv6 等相结合得到了应用[9-10].

端信息跳变系统抗攻击性能的优劣与跳变速率密切相关,而跳变速率与所采用的同步方案密切相关[11-12].然而,传统的严格时间同步方案[11]和时间戳同步方案[12]受分组网络异步、乱序和网络时延的影响较大,无法支持高速率跳变.因此,文献[5]创新性地提出利用端信息扩展技术进行同步认证,实现跳变与同步分离,保证信息传输完整性的同时兼顾了高速率的跳变,实验证明,结合端信息扩展技术系统具有更好的网络防御效果.端信息扩展技术的应用提高了信息传输的安全性,保护了用户隐私.但存在着资源利用率低、传输效率低、误码率高等问题.

在提高信息传输效率、突破系统容量方面,作为未来 5G 多址接入候选方案的非正交多址接入技术(non-orthogonal multiple access, NOMA)成为当下的研究热点.相关研究工作主要包括功率域非正交多址接入技术[13]以及码域非正交多址接入技术[14].其中,码域非正交多址接入技术以稀疏码多址接入为代表,信息在发送端经过编码后,编码比特被映射为复数域的多维码字,不同用户的发送码字在相同时频资源上非正交叠加,服务器端利用码字的稀疏性实现用户身份的识别.

对稀疏码多址技术的研究,Wu 等人[15]结合 Turbo 信道编码设计出采用迭代结构的 SCMA 接收机;Xiao 等人[16]将 LDPC 信道译码与 SCMA 译码相结合设计出采用 LDPC 信道编码的 SCMA 迭代接收机结构,仿真结果表明采用该结构的迭代译码算法的接收机相比于原始 SCMA 接收机可以在保证计算复杂度不变的条件下获得较高的迭代增益;Xiao 等人[17]提出了 2 种基于边缘概率的译码简化算法,来降低接收机的复杂度,仿真结果表明简化算法可以在一定程度上以牺牲系统性能来换取译码复杂度.

本文兼顾信息传输的安全性和高效性,将稀疏码多址接入技术的思想与端信息扩展技术相结合,研究了基于 SCMA 的端信息扩展多用户安全通信系统,保证用户通信内容安全传输的同时,降低系统误码率,提高信息传输效率.对于将端信息扩展序列应用于未来海量接入场景中具有重要意义.

2 基于 SCMA 的端信息扩展多用户安全通信系统研究

2.1 系统模型

基于 SCMA 的端信息扩展多用户安全通信系统通过结合稀疏码多址接入技术使并发通信的各用户具有彼此唯一的身份标识,接收端通过标识区分用户信息.从系统的安全性和效率出发,设计基于 SCMA 的端信息扩展多用户安全通信系统模型,如图 1 所示.

对于某一用户来说,系统可分为客户端和服务器端,客户端主要负责机密信息的编码与端信息扩展流的生成,包括码本设计模块、码字加载发送模块.码本设计模块确保各用户之间不会产生干扰,服务器端能够通过码本中码字的稀疏性区分用户;码字加载发送模块是指将代表用户信息的码字通过一定的规则加载到端信息上,扩展为多条端信息的组合序列,保证信息传输的机密性.服务器端负责合法端信息扩展序列的识别和机密信息的解码,包括合法端信息扩展序列识别模块和端信息扩展序列解析模块.

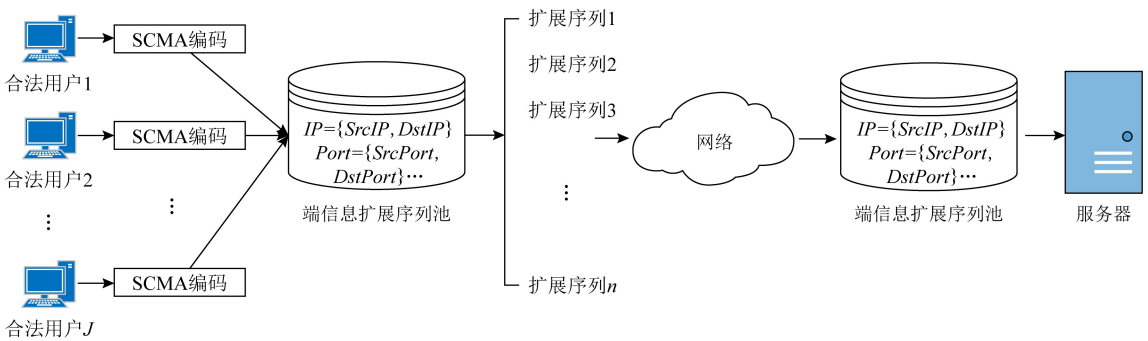

Fig. 1 End spreading multi-user secure communication system model based on SCMA

图 1 基于 SCMA 的端信息扩展多用户安全通信系统模型

用户采用公私钥数字签名验证口令的方式进行身份认证,认证成功后与服务器建立连接并随机选择一个码本进行机密信息调制.本文使用端口号、IP 地址等数据包中必备的端信息来加载调制后的信息,实现端信息的复用.由于将用户信息扩展为多条端信息组合序列,相当于利用端信息稀释了原始数据的信息量,并且传输过程中各项端信息是分散的,所以,攻击者难以通过截获的部分数据包分析出原始信息,增加了攻击者的难度.

2.2 关键策略

基于 SCMA 的端信息扩展多用户安全通信系统关键策略主要包括身份认证策略、码本设计分配策略、码字加载发送策略以及端信息解析策略.身份认证策略是保证系统安全的第一道防线,对接入用户进行身份核验,保证接入用户真实可信;码本设计分配策略关系到系统承载的最大并发用户数,以及资源块最大利用情况;码字加载发送策略保证用户信息传输的安全性,服务器端信息解析策略保证用户信息的正确解析,完成机密信息的完整传输.

2.2.1 身份认证策略

为阻止恶意用户接入系统,本文采用公私钥数字签名验证口令的方式进行接入用户的身份认证.每位用户在接入系统之前将用户公钥 K_{ei} 提交给服务器端,同时服务器为用户建立时间标志 T_i(访问次数计数器).

用户每次访问服务器时首先用私钥进行签名,然后提交给服务器 $ID_i \parallel D((ID_i, N_i), K_{di})$.其中,$K_{di}$ 为用户保密的私钥,N_i 表示用户访问第 N_i 次,ID_i 是明文形式的标识符.

服务器根据明文标识符 ID_i 找到存储的用户公钥 K_{ei},接着计算提交的签名,$E(D((ID_i, N_i), K_{di}), K_{ei}) = \langle ID_{i'}, N_{i'} \rangle$.

当且仅当 $ID_i = ID_{i'}$,$N_{i'} = T_i + 1$ 时,用户身份才能得到确认.

2.2.2 码本设计分配策略

采用子集分割法进行码本的设计[18],过程包括:1)构造映射矩阵;2)设计每个资源块星座图,并采用子集分割法为每位用户生成对应的星座图;3)将星座图与映射矩阵联合分析,生成用户星座矩阵;4)为每个用户生成对应码本.

1) 构造映射矩阵

映射矩阵 $\boldsymbol{F}$ 是反映系统对资源块的利用情况以及每个资源块上所要承载用户情况的.规则的映射矩阵每一行、每一列非 0 元素的数目是相同的.假设

系统的资源块个数为 N,非 0 元素个数为 R,那么该系统最大用户承载数为

$$J_{\max}=C_N^R, \tag{1}$$

每个资源块实际承载用户数为

$$M=\frac{JR}{N}, \tag{2}$$

过载率为

$$\lambda=\frac{J}{N}. \tag{3}$$

码本中非 0 元素项越少,服务器端解码越容易,由于映射矩阵 $\boldsymbol{F}$ 的构建过程与低密度奇偶校验码(low density parity check code, LDPC)中的校验矩阵类似,所以,当确定系统资源块个数、用户数以及各个资源块承载的用户数时,就可以参照 LDPC 校验矩阵设计一个具有良好特性的映射矩阵.例如,一个 6 用户、4 资源块($J=6,N=4,R=2$)的映射矩阵 $\boldsymbol{F}$ 可以设计为

$$\boldsymbol{F}=\begin{pmatrix}0&1&0&1&0&1\\0&0&1&1&1&0\\1&0&1&0&0&1\\1&1&0&0&1&0\end{pmatrix}_{4\times 6}. \tag{4}$$

2) 设计资源块总的星座图

为保证同一资源块上各个用户之间能够获得彼此唯一的标识,就需要使承载在同一资源块上的各个用户拥有彼此不重合的星座点数.设用户每次传输比特数为 b,则该用户需要占用的星座点数为

$$B=2^b, \tag{5}$$

联合式(2)可计算得到每个资源块上用户总的星座点数为

$$P=B\times M. \tag{6}$$

P 点星座对应的星座图可以采用现有数字调制技术中的星座图表示,如正交振幅调制(quadrature amplitude modulation, QAM)星座图、相移键控调制(phase-shift keying, PSK)星座图.最后,采用子集分割法为资源块上的每个用户分配不同的星座图.

子集分割方案如图 2 所示,这里以 16QAM 星座图分割过程为例.

如图 2 所示,设 16QAM 最大振幅为 $A_{\max}$,则相邻星座点的欧氏距离为

$$d_1=\frac{\sqrt{2}}{3}A_{\max}=0.471A_{\max}. \tag{7}$$

进行第 1 次子集分割后,每个子集由 8 个信号点组成,一次子集分割后,星座点间的欧氏距离 $d_2=\sqrt{2}d_1=0.667A_{\max}$.再次进行子集分割后,形成 2 个二次子集 $C1,C2$ 和 $C3,C4$,每个二次子集由 4 个信号点组成,进行二次分割后,子集星座点之间的欧氏距离 $d_3=2d_1=0.942A_{\max}$.由此可见,采用子集分割法,每次分割后子集内星座点间的欧氏距离会不断增加.

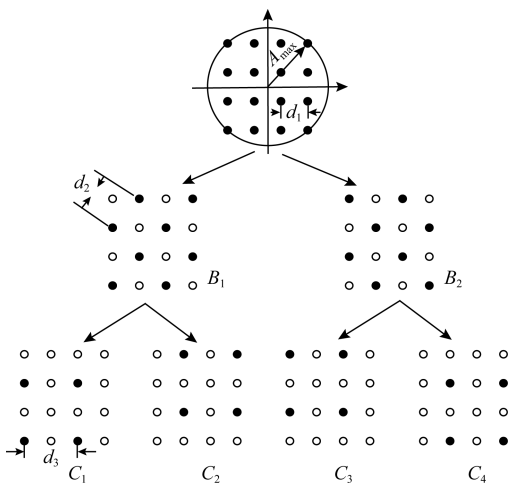

Fig. 2 Constellation subset segmentation of 16QAM

图 2 16QAM 星座子集分割图

若以子集星座点间的欧氏距离来表示用户之间的干扰程度,则采用子集分割法可以增大用户星座点间的欧氏距离,即用户之间的干扰会越来越小.

3) 设计星座矩阵

星座矩阵(constellation matrix, CM)是通过每个资源块上承载的用户星座结合映射矩阵 $\boldsymbol{F}$ 产生的.星座矩阵可以表示为

$$CM_{n,k}=\begin{cases}0, & F_{n,k}=0,\\ C_{n,rand(r)}, & F_{n,k}=1,\end{cases} \tag{8}$$

其中,n 代表资源块,对应星座矩阵的行;k 代表用户,对应星座矩阵的列.星座矩阵由 0 和用户星座图 $C_{n,rand(r)}$ 组成,其中,用户星座图 $C_{n,rand(r)}$ 表示分割子集进行不重复排列的所有可能取值的集合.

4) 生成码本

将星座矩阵 $CM_{n,k}$ 中每一列展开成 $N\times M$ 矩阵,构成三维矩阵,n 表示资源块,m 表示码字,k 表示用户.由此得到用户的码本为

$$CB_{n,k}(m_k)=\begin{cases}0, & F_{n,k}=0\\ C_{n,rand(r)}(m_k), & F_{n,k}=1\end{cases} \tag{9}$$

其中,$CB_{n,k}(m_k)$表示用户 k 使用码字 m_k 时,该码字的第 n 个值.

至此,系统中每个用户获得彼此相互独立的码本,即获得了唯一的用户标识.接下来给出 6 用户 4 资源块($J=6,N=4,R=2$)系统的用户码本.构造

的映射矩阵 $\boldsymbol{F}$ 如式(4)所示.采用基于 12PSK 星座图进行子集分割,分割子集如图 3 所示:

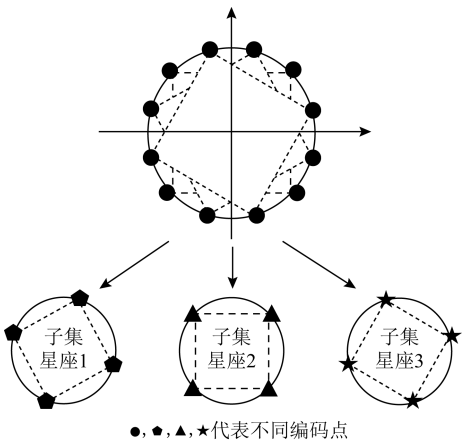

Fig. 3 Constellation subset segmentation of 12PSK

图 3 12PSK 星座子集分割

结合式(8)得到系统资源块星座矩阵如图 4 所示:

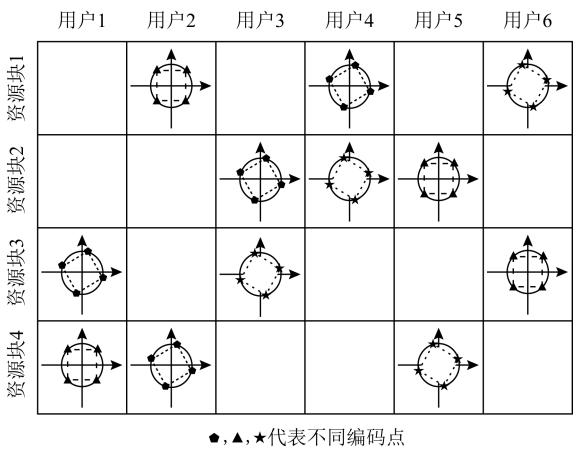

Fig. 4 User-resource block constellation matrix

图 4 用户-资源块星座矩阵图

最后得到系统中每个用户的码本如附录 A 所示.

2.2.3 码字加载发送策略

码字加载发送策略,是在用户根据所传信息选择对应码字后,再以扩展的方式将码字加载于端信息上传输到服务器端.类比于 SCMA 系统并发传输 J 个用户信息所需的资源块个数,本文通过划分端口号范围来区分各个资源块,为防止端口号与其他通信连接所使用的端口号发生冲突,这里排除常用端口号,即规定本系统所使用的端口号范围是[1 024,65 535].其中,源端口表示码字的实数部分,目的端口表示码字的虚数部分;源 IP、目的 IP 组成的象限阵表示用户码字实部与虚部的正负情况;IDE(IP 报头标识符)前 k($k=length(bin(N))$,N 为资源块个数)位表示非 0 码字所处的行标,后$(16-k)$位由源端口号与密钥 key(密钥为收发双方共享的秘密)进行异或得到,用于服务器端对数据包的过滤,各端信息的使用情况如表 1 所示:

Table 1 Endinformation Distribution Table

表 1 端信息分布情况表

端信息		端信息范围	说明
IP 地址	*SrcIP*	192.168.2.41～192.168.2.50	组成 IP 象限阵,表示码字实部与虚部的正负情况
	DstIP	192.168.1.41～192.168.1.50	
端口号	*SrcPort*/*DstPort*	1 500～15 000	资源块 1
		16 000～30 000	资源块 2
		31 000～5 000	资源块 3
		46 000～60 000	资源块 4
IDE(IP 报头标识符)		$0\sim2^{16}$	前 k 位表示非 0 码字所处的行标,后$(16-k)$位由源 IP 与共享密钥异或得到,用于数据包的识别

具体码字加载发送策略步骤为:

1) 将用户输入的明文信息以字符为单位进行分割,通过 ASCII 编码将明文序列转换为 8 位二进制序列,不足位最高位补 0;

2) 从最低位开始每 2 b 为一组在对应码本中选择用户码字;

3) 将用户码字按行展开,为了提高系统的通信效率,只需要将码字中的非 0 元素加载到端信息上发送即可.按照非 0 元素实数域和负数域的正负情况,从通信双方共享的 IP 地址象限阵 IP_{array} 中通过地址选择算法(见式(10))选取 L 个源/目的 IP 对

$$IP_L=AddSelect(IP_{\text{array}},L) \tag{10}$$

组成长度为 L 的 IP 地址序列

$$IP=((SrcIP_1,DstIP_1),(SrcIP_2,DstIP_3),\cdots,(SrcIP_L,DstIP_L)),$$

其中,L 为端信息扩展序列的长度.

4) 根据码字非 0 元素所处的行标确定信息所要加载的资源块,即确定对应资源块端口号的范围.码字的实数域和虚数域分别用 *key-real* 和 *key-imag* 表示,并计算对应的端口号:

$$SrcPort=[key\text{-}real\times10^3]\%port_r+port_l, \tag{11}$$

$$DstPort=[key\text{-}imag\times10^3]\%port_r+port_l, \tag{12}$$

其中,$port_l$ 和 $port_r$ 分别代表所处资源块的左右边界,其目的是使生成的源端口号和目的端口号能够落在对应的资源块上,消除系统中各用户之间干扰.

步骤 3)中 IP 地址对作离散卷积处理生成 L 个对应端口号,最后 L 个端口号与计算得到的端口号进行异或处理得到长度为 L 的端口号序列:

$$Port=((SrcPort_1,DstPort_1),(SrcPort_2,DstPort_2),\cdots,(SrcPort_L,DstPort_L)).$$

5) 计算生成 IDE 报头标识符,前 $k(k=length(bin(N))$,N 为资源块个数)位表示非 0 元素所处的行标,后$(16-k)$位由源端口号和收发双方共享密钥 key 异或产生,用于服务器端对数据包的识别;

6) 用户将五元组$(SrcIP_1,DstIP_1,SrcPort_1,DstPort_1,IDE_1),(SrcIP_2,DstIP_2,SrcPort_2,DstPort_2,IDE_2),\cdots,(SrcIP_L,DstIP_L,SrcPort_L,DstPort_L,IDE_L)$依次封装为数据包;

7) 以用户字符为单位,每封装完成一个字符的数据包,用户将所有的数据包发送至网络,否则重复步骤 1)~6).码字加载发送策略算法如算法 1 所示.

算法 1. 码字加载发送策略算法.

输入:用户明文 Msg、用户码本 $codebook$、共享密钥 Key;

输出:端信息扩展序列;

① $CodewordConversion(Msg,codebook,Key)$;

② $m\_bin\leftarrow f\_1(Msg)$; /* 将明文信息转换为 8 位二进制 */

③ for i in m_bin

④ $SrcIP,DstIP\leftarrow f\_2(m\_i)$; /* 根据码字非 0 元素实数域和复数域的正负情况生成源 IP、目的 IP 地址序列 */

⑤ $SrcPort,DstPort\leftarrow f\_3(m\_i)$; /* 根据码字的值生成源端口、目的端口序列 */

⑥ $m\_enc\leftarrow f\_4(length(bin(N))$ concat $SrcIP\oplus key)$; /* 生成 IDE 报头标识符 */

⑦ $msg=f\_5(SrcIP,DstIP,SrcPort,DstPort,IDE)$; /* 封装数据包,形成端信息扩展序列 */

⑧ end for

2.2.4 端信息解析策略

客户端以端信息扩展的方式将携带不同信息的大量数据包通过 socket 套接字发送至服务器端,服务器端不断监听捕获网络中的数据包.捕获数据包后,首先用共享密钥与源端口异或,对照 IDE 后$(16-k)$位进行无效数据包的过滤,接收有用的数据包,单个数据包判断合法后,判断通过判断的合法数据包是否能够组成端信扩展序列以及判断扩展序列所属用户,具体验证算法:

$$IsSeqence=check(IP,Port,L,\tau),\quad(13)$$

其中,L 为端信息扩展序列的长度,τ 为序列的容错率,允许端信息扩展序列中一定数量的端信息未通过验证,即满足数量为 $L(1-\tau)$端信息认证通过即为端信息扩展序列认证成功.

接着解析五元组信息,按照端信息加载逆过程解析出用户码字,与所存储的码本进行比对,得到用户所传输的比特信息,最后对应 ASCII 编码还原用户的明文.具体的端信息扩展序列解析策略步骤为:

1) 服务器端持续监听信道中的数据包,提取数据包源端口并与收发双方共享秘钥 Key 进行异或,结果记为 xor;

2) 判断收到的数据包是否为合法端信息扩展序列,具体的方法是 xor 与该数据包报头标识符 IDE 的后$(16-k)$位进行一致性比较;

3) 取合法端信息扩展序列报头标识符 IDE 的前 k 位,确定非 0 元素的行标,确定该信息所承载的资源块;

4) 取合法端信息扩展序列的源 IP、目的 IP,确定非 0 元素实部和虚部的正负情况,与存储的各用户码本对应,完成对用户身份的确认;

5) 取合法端信息扩展序列源端口、目的端口,结合各资源块端口号范围,确定用户发送的具体比特信息;

6) 将每组比特信息按顺序拼接,以字符为单位还原用户明文.端信息解析策略算法如算法 2 所示.

算法 2. 端信息解析策略算法.

输入:端信息扩展流数据包 DP,用户码本 $codebook$,共享密钥 Key;

输出:用户身份 ID 及用户明文 Msg;

① $CodewordResolution(DP,codebook,Key)$;

② $xor=DP.SrcPort\oplus Key$;

③ if $xor==bin(DP.IDE)[k:16]$ /* 判断数据包是否为合法扩展序列 */

④ for IP,IDE in DP

⑤ $ID\leftarrow f\_6(SrcIP,DstIP)$ & $f\_7(IDE[0:k])$; /* 合法数据包中的源 IP、目的 IP 确定码字实部虚部的正负情况;数据包标识符确定码字行标,二者结合确定用户 ID */

⑥ $Msg\leftarrow f\_8(SrcPort,DstPort)$; /* 合法数据包中的源端口、目的端口确定用户明文 */

⑦ end for

⑧ end if

3 系统性能分析

基于 SCMA 的端信息扩展多用户安全通信系统主要关注其能否在保证通信内容的安全传输的前提下提高系统资源的利用率、降低系统误码率、实现多用户并发通信.所以系统的性能分析主要涉及安全性分析和通信服务质量分析.

3.1 安全性分析

1) 抗重放攻击.由于本文采用公私钥数字签名验证口令进行接入用户的身份认证,这种方式中,系统为每个用户设置了时间标志 T_i,当且仅当客户端时间属性满足一定条件,即 $N_{i'}=T_i+1$ 时,客户端身份才可验证通过并与服务器进行数据传输.这种验证方式避免了直接重放攻击带来的威胁.除了直接重放攻击,攻击者还可能利用客户端发起反向的重放攻击[19],也就是本来发送给服务器的数据包被截获后反向发送给客户端的情况.面对此类反向重放攻击,规定客户端只在发送信息时开放相应的端口,其他时间关闭端口,所以面对攻击者反向发来的数据包,客户端也不会识别.

2) 抗丢失分析.抗丢失性是指客户端生成的端信息扩展序列即使在传输过程中发生丢失,服务器端仍能利用剩余的端信息扩展序列正确恢复原始消息的能力.假设当前网络环境中有 e 个分组,丢失其中的 k 个数据分组,端信息认证的数据分组为 m,序列的容错度为 τ,则抗丢失能力 β 为

$$\beta=\begin{cases}1, & k<m(1-\tau),\\ 1-\dfrac{1}{C_e^k}\displaystyle\sum_{i=0}^{m\tau}C_m^{m(1-\tau)+i}C_{e-m}^{k-m(1-\tau)-i}, & \\ & k\geqslant m(1-\tau),\end{cases} \tag{14}$$

其中,e,k 由当前网络复杂度决定,在 e 与 k 一定的情况下,分析 β 与 m 和 τ 有关.

当 m 一定时,β 随着 τ 的增大而减小.当 $\tau=0$ 时,

$$\beta=1-\frac{C_{e-m}^{k-m}}{C_e^k}=1-\prod_{i=1}^{m}\frac{k-i+1}{e-i+1},$$

另设 $m+\Delta m>m$ 时,

$$\beta_{m+\Delta m}-\beta_m=1-\frac{C_{e-m}^{k-m}}{C_e^k}=$$

$$\frac{e-k}{e-(m+\Delta m)+1}\prod_{i=1}^{m}\frac{k-i+1}{e-i+1}>0,$$

因此,β 随着 m 的增大而增大.

因此,当网络环境一定时,增加扩展序列的长度或者减小序列验证的容错率均可增加系统的抗丢失能力.

3.2 通信服务质量分析

本文设计实现的基于 SCMA 的端信息扩展多用户安全通信系统服务器端能够识别多个用户特征,满足多用户并发通信的需求.其中,码本的设计保证了并发用户具有唯一的身份特征,互相之间不产生干扰;端信息扩展技术保证了用户信息实现高可靠、高安全传输.为进一步提升系统传输效率,采用无连接的 UDP 协议,由此会带来 2 个问题:

1) 采用不可靠的 UPD 协议会导致数据包不是按序到达服务器端;

2) 由于 UDP 协议是尽最大可能交付,会导致出现数据包丢失的情况.

针对数据包乱序问题,客户端以字符为单位进行数据包的封装,待每个字符的数据包封装发送完毕后等待一定的时间阈值,在进行下一个字符数据包的封装发送,这样避免了字符间数据包乱序的影响.在字符数据包内部,设定端信息扩展序列的长度为 L,即 L 个数据包均表示一组数据信息,所以扩展序列的长度越大,数据包乱序对解码正确性的影响越小;针对数据包丢失问题,由 3.1 节分析,增加序列的长度或减小序列的容错率可增加系统的抗丢失能力,所以合适的参数设置能够弥补一定程度 UDP 协议带来的不可靠现象.

4 系统性能测试

本节对基于 SCMA 的端信息扩展多用户安全通信系统进行实验测试.实验设置最大用户数 $J=6$,资源块个数 $N=4$.分别从系统的抗攻击性能和系统传输性能 2 方面进行实验.具体测试的系统配置如表 2 所示.主机 A 作为端信息扩展的多用户安全通信系统的服务器,主机 B 作为攻击者,主机 $C1\sim C6$ 作为 6 个请求客户端.

Table 2 System Parameter Configuration Table

表 2 系统参数配置表

主机	处理器	操作系统	内存/GB	硬盘/GB
主机 A	Intel® Core™ i5-5200U	Ubuntu	8	512
主机 B	Intel® Core™ i7-7700	Ubuntu	8	1 024
主机 $C1\sim C6$	Intel® Core™ i7-5670	Ubuntu	8	512

4.1 系统安全性测试

4.1.1 抗攻击测试

对基于 SCMA 的端信息扩展多用户安全通信系统进行拒绝服务攻击实验.通过对比普通服务器

在 UDP Flood 攻击下信息传输完成所需的时间,验证系统的抗攻击性能.

在本次针对服务器的攻击实验中,假设攻击者已知端信息扩展地址池的范围,因此攻击者所选的 IP 地址和端口号是在端信息地址池中随机选取.设拒绝服务攻击强度范围是 0～50 Mb/s,传输的数据是大小为 15 KB 的电子文档.如图 5 所示为不同拒绝服务攻击速率下信息传输完成所需的时间.

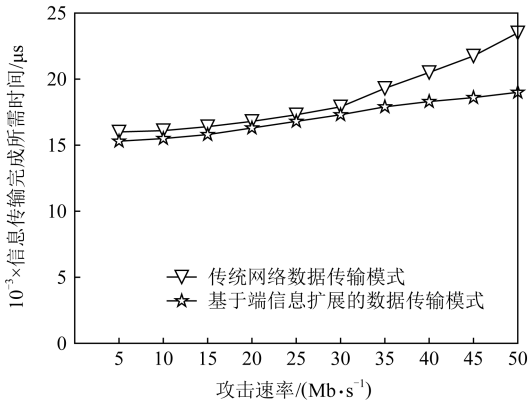

Fig. 5 Service response time under UDP Flood

图 5 不同攻击速率下传输时间比较

由图 5 可以看出,传统网络中,随着攻击速率增大,信息传输完成所需的时间明显增加;采用端信息扩展模式,随着攻击速率的增加,信息传输完成所需的时间没有明显变化.这是因为本系统的服务器通过监听扫描数据包来解析用户信息,其端口始终处于关闭状态,所以,基于 SCMA 的端信息扩展多用户安全通信系统可以有效抵御一定程度的拒绝服务攻击.

本文还对拒绝服务攻击的不同攻击类型做了分析比较.测试了基于 TCP 协议拒绝服务攻击下的系统性能.表 3 给出了端信息扩展多用户安全通信系统在不同攻击(攻击速率为 50 Mb/s,每位用户传输数据大小为 20 KB)下完成信息传输所需的时间.

Table 3 Data Transmission Schedule Under Different Attacks

表 3 不同攻击下信息传输时间表

拒绝服务攻击类型	信息传输完成所需时间/ms
SYN Flood	17.96
ACK Flood	18.30
UDP Flood	19.65
No Attack	17.53

基于 SCMA 的端信息扩展多用户安全通信系统在不同类型的拒绝服务攻击下均可实现信息的完整传输,系统受拒绝服务攻击的影响不明显.

4.1.2 隐蔽性测试

对于隐蔽性的测试是对通信过程中的数据包进行抓包分析,通过地址选取的随机性证明端信息扩展多用户通信系统具有良好的隐蔽性.

用 SnifferV4.7.5 抓包工具对系统进行连续 1 000 次抓包统计,对服务器端配置的 10 个 IP 地址(包括源 IP 和目的 IP)使用情况进行统计如图 6 所示:

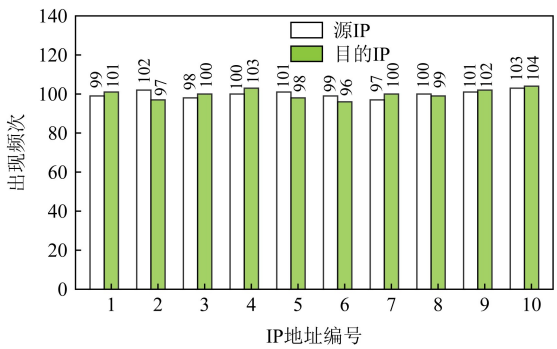

Fig. 6 IP address usage

图 6 IP 地址使用情况

从图 6 可以看出,10 个 IP 地址使用情况基本平均,证明本文设计的模型系统在端信息选取上具有随机性,不易被攻击者扫描分析.因此,基于 SCMA 的端信息扩展多用户安全通信系统能够实现信息的隐蔽传输,保证信息传输的可靠性.

4.2 系统传输性能测试

为验证基于 SCMA 的端信息扩展多用户安全通信系统的传输性能,探究了数据包数量、过载率以及不同接入用户数量对系统传输性能的影响.定义比特率为单位时间服务器端成功接收数据包占客户端发送数据包的百分比,用 δ 表示.设客户端发送的端信息扩展数据包总数为 n,服务器端接收数据包数为 m.那么,$\delta=m/n$,$\delta'=1-\delta$ 表示信息的损失率.

1) 数据包数量对系统传输性能的影响.设置数据包数量依次为 2^8,2^9,2^{10},2^{11},2^{12}.统计用户 1,3,5 的平均信息损失率如图 7 所示.

由于采用了不可靠的 UDP 协议,且不同时间段内,受网络信道的干扰强度不同,不可避免的出现了丢包现象.从图 7 可以得出,各用户发送不同数量数据包的信息损失率范围是[0.78%,15.87%].但仍无法确认一定信息的损失对服务器端解码准确率的影响.因此,接下来通过 Linux 系统中的网络模拟功能模块 Netem 来模拟网络丢包现象.在上述实验的基础上,设置网络丢包范围是[0%,40%],记录不同方案对应的解码准确率如图 8 所示.

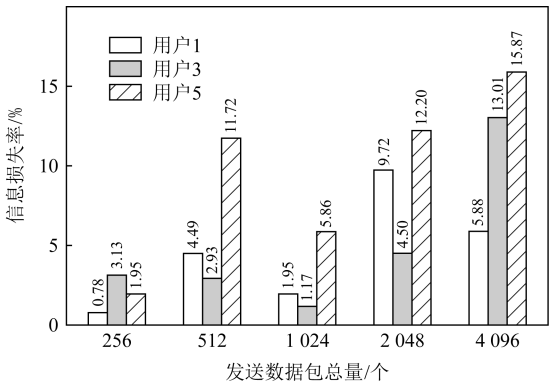

Fig. 7 Data loss statistics for different users

图 7 不同用户信息损失统计图

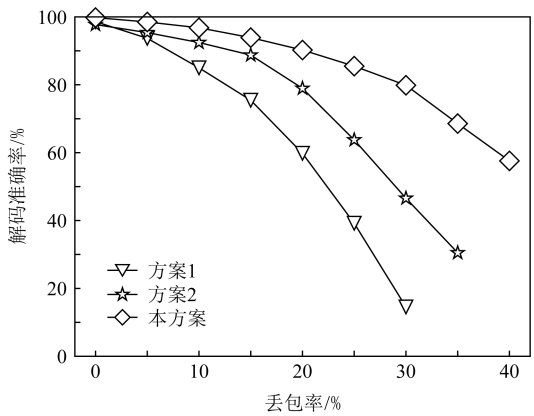

Fig. 8 The decoding accuracy of different schemes

图 8 不同方案的解码准确率

图 8 中,方案 1 是 Gimbi 等人[20]提出的将用户信息加载到源端口进行传输,服务器端利用源端口的差值进行解码.由于没有鲁棒性保障机制,数据包丢失在解码时会产生连锁反应.因此,其解码准确率随着丢包率的增加而急剧下降.方案 2 是将原始信息加载于源 IP 进行传输,各 IP 之间相互独立,虽然丢包对服务器端解调不会产生连锁反应,但数据包的丢失会直接导致原始信息丢失,所以方案 2 解码准确率较方案 1 略好一些.本方案中,某一原始信息扩展为由不同的数据包表示,各数据包之间相互独立,所以一定范围内数据包的丢失不会对解码产生太大的影响.

2) 过载率对系统传输性能的影响.根据式(3)过载率的计算,实验选取实际用户数为 3,4,6 三种情况,则对应的过载率为 75%,100%,150%.图 9 是系统用户传输 1 000 b 信息时,在不同过载条件下测得的系统误比特率对比图,其中横坐标代表端信息扩展序列的长度.

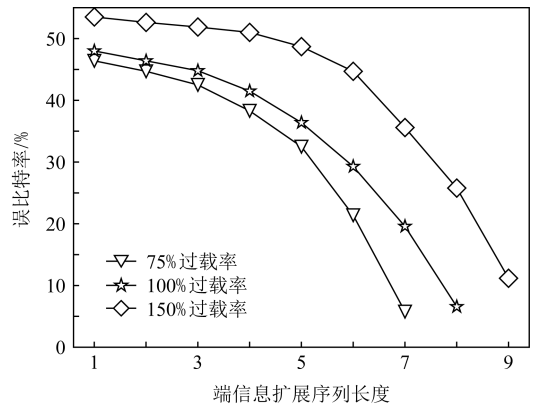

Fig. 9 Bit error rate under different overload

图 9 不同过载下的误比特率

由图 9 得到,当过载率一定时,系统误比特率随着端信息扩展序列长度的增加而逐渐减小;当端信息扩展序列的长度一定时,系统未达到过载,即 $\lambda=75\%$ 或者 $\lambda=100\%$,系统的误比特率较低;达到过载后,随着过载率的增加,系统的误比特率有明显的增加.端信息扩展序列长度越大,过载率对系统误比特率的影响越明显.因此,合理选择过载率对提高系统的误比特率,提升系统传输性能有至关重要的作用.

3) 不同接入用户数对系统性能的影响.本文选取了 2 类码本,一种是文献[21]中为解决相同场景下不同用户的不同业务需求基于度分布理论而设计的非规则码本,另一种是基于本文码本设计方法设计的规则码本.统计在相同的网络环境下(丢包率为 5%,端信息扩展序列长度 $L=8$)不同接入用户数的情况下系统的解码准确率,结果如图 10 所示:

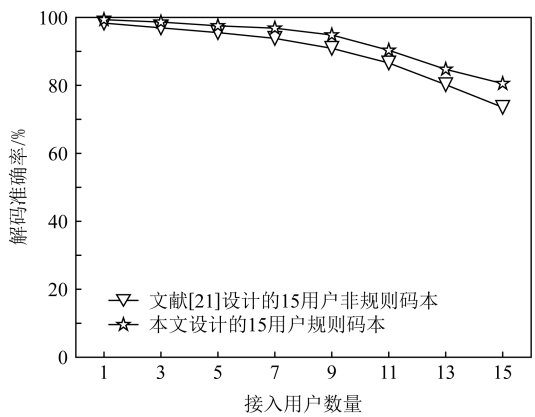

Fig. 10 The decoding accuracy of different number users

图 10 不同接入用户数的解码准确率

由图 10 得到,系统的解码准确率会随着接入用

户数量的增加而降低,因为接入用户数越多,单位资源块所承受的用户数就越大,彼此之间的竞争越大,解码也因此变得越困难.其中,比较规则码本和非规则码本,由于非规则码本考虑了用户传输信息的急切程度,对应于码本中每一列的非 0 码字是不一样多的,因此,随着接入用户数的增加,对于优先级比较低的用户来说,其对应非 0 元素就越少,客户端形成的端信息扩展流就越少,系统丢包率对其影响就越大,表现为非规则码本的解码准确率较规则码本来说就越低.但从图 10 中可以看到,即使用户数量对服务器端解码准确率存在一定的影响,但在一个可接受的范围内.

5 总 结

本文将稀疏编码引入端信息扩展序列的生成过程中,设计实现基于 SCMA 的端信息扩展多用户安全通信系统,对系统中的关键策略进行分析研究.提出用户码本设计分配策略,保证各用户具有唯一的用户特征,服务器端能够正确区分用户;提出码字加载发送策略,以端信息扩展的方式实现信息安全传输.

最后对系统进行理论分析和实验验证,结果表明:基于 SCMA 的端信息扩展多用户安全通信系统具有良好的抗攻击性能和较好的传输性能,保证用户信息传输完整性和可靠性的同时,提高了系统资源利用率,降低了系统误比特率.这对于将端信息扩展技术应用于未来大规模接入场景具有重要意义.

参 考 文 献

[1] Xin Ai, Chen Honglong, Lin Kai, et al. Nowhere to hide: Efficiently identifying probabilistic cloning attacks in large-scale RFID systems [J]. IEEE Transactions on Information Forensics and Security, 2020, 7(4): 714-727

[2] Fan Linna, Ma Yufeng, Huang He, et al. The research summary of moving target defense technology [J]. Journal of China Academy of Electronics and Information Technology, 2017, 12(2): 209-214 (in Chinese)
(樊琳娜, 马宇峰, 黄河, 等. 移动目标防御技术研究综述[J]. 中国电子科学研究院学报, 2017, 12(2): 209-214)

[3] Shi Leyi, Jia Chunfu, Lv Shuwang. Research on hopping for active network confrontation [J]. Journal on Communications, 2008, 29(2): 106-110 (in Chinese)
(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)

[4] Wen Xiao. Research on hybrid of hopping and spreading for active cyber defense [D]. Qingdao: China University of Petroleum, 2018 (in Chinese)
(温晓. 基于端信息跳扩混合的主动网络防御研究[D]. 青岛: 中国石油大学(华东), 2018)

[5] Hou Bowen, Shi Leyi, Guo Hongbin. et al. File covert transfer strategy based on end hopping and spreading [J]. Journal of Computer Research and Development, 2020, 57(11): 2283-2293 (in Chinese)
(侯博文, 石乐义, 郭宏彬, 等. 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)

[6] Jajodia S, Ghost A K, Swarup V, et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats [M]. Berlin: Springer, 2011

[7] Hu Hongchao, Wu Jiangxing, Wang Zhenpeng, et al. Mimic defense: A designed-in cyber security defense framework [J]. IET Information Security, 2017, 12(3): 226-237

[8] Zhou Yuyang, Cheng Guang, Guo Chunsheng. et al. Survey on attack surface dynamic transfer technology based on moving target defense [J]. Journal of Software, 2018, 29(9): 2799-2820 (in Chinese)
(周余阳, 程光, 郭春生, 等. 移动目标防御的攻击面动态转移技术研究综述[J]. 软件学报, 2018, 29(9): 2799-2820)

[9] Wang Yuhang. Research and implementation of an active address jump defense technology based on SDN [D]. Hangzhou: Zhejiang University, 2017 (in Chinese)
(王宇航. 一种基于 SDN 的地址跳变主动防御技术的研究与实现[D]. 杭州: 浙江大学, 2017)

[10] Mei Zhifeng, Wang Zhenxing, Wang Yu, et al. An IPv6 MTD model based on subnet hopping [J]. Computer Applications and Software, 2016, 67(12): 301-304 (in Chinese)
(梅志锋, 王振兴, 王禹, 等. 一种基于子网跳变的 IPv6 MTD 模型[J]. 计算机应用与软件, 2016, 67(12): 301-304)

[11] Fan Xiaoshi, Li Chenghai, Wang Hao. Research on port jump technology based on variable time slot and dynamic synchronization [J]. Computer Engineering and Design, 2013, 44(10): 113-117 (in Chinese)
(范晓诗, 李成海, 王昊. 基于可变时隙与动态同步的端口跳变技术研究[J]. 计算机工程与设计, 2013, 44(10): 113-117)

[12] Liu Jiang, Zhang Hongqi, Dai Xiangdong, et al. A proactive network defense model based on self adaptive end hopping [J]. Journal of Electronics & Information Technology, 2015, 37(11): 2642-2649 (in Chinese)
(刘江, 张红旗, 代向东, 等. 基于端信息自适应跳变的主动网络防御模型[J]. 电子与信息学报, 2015, 37(11): 2642-2649)

[13] Wang Jiangtao, Zhou Mengyuan, Chen Dong. et al. Power allocation algorithm in NOMA-based cognitive radio networks [J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2020, 32(6): 945-953 (in Chinese)

(王江涛, 周梦园, 陈东, 等. 非正交多址认知无线电网功率分配算法[J]. 重庆邮电大学学报: 自然科学版, 2020, 32(6): 945-953)

[14] Yang Yifu, Wu Gang, Li Xinran. et al. A survey of non-orthogonal multiple access technology for Beyond-5G [J]. Radio Communication Technology, 2020, 46(1): 26-34 (in Chinese)
(杨一夫, 武刚, 李欣然, 等. 面向后 5G 的非正交多址技术综述[J]. 无线电通信技术, 2020, 46(1): 26-34)

[15] Wu Yiqun, Zhang Shunqing, Chen Yan. Iterative receiver in sparse code multiple access systems [C] //Proc of IEEE Int Conf on Communications (ICC). Piscataway, NJ: IEEE, 2015: 2918-2923

[16] Xiao Baichen, Xiao Kexin, Zhang Shutian, et al. Iterative detection and decoding for SCMA systems with LDPC codes [C] //Proc of Int Conf on Wireless Communications & Signal Processing(WCSP). Piscataway, NJ: IEEE, 2015: 1-5

[17] Xiao Baichen, Xiao Kexin, Zhang Shutian, et al. Simplified multiuser detection for SCMA with sum-product algorithm [C] //Proc of Int Conf on Wireless Communications & Signal Processing(WCSP), Piscataway, NJ: IEEE, 2015: 11-15

[18] Liang Yan, Yu Bei, Tong Kaimeng. Simple codebook design of SCMA in Gaussian channel [J]. Computer Application Research, 2017, 32(9): 190-193 (in Chinese)
(梁燕, 余贝, 童开蒙. 高斯信道下 SCMA 简易码本设计[J]. 计算机应用研究, 2017, 32(9): 190-193)

[19] Liu Meng, Wang Longbai, Dang Jiawu, et al. Replay attack detection using variable-frequency resolution phase and magnitude features [J]. Computer Speech & Language, 2020, 7(6): 66-78

[20] Gimbi J, Johnson D, Lutz P, et al. A covert channel over transport layer source ports [C] //Proc of Int Conf on Security & Management. New York: ACM, 2012: 56-76

[21] Zhang Shutian, Xiao Baicen, Xiao Kexin, et al. Design and analysis of irregular sparse code multiple access [C] //Proc of Int Conf on Wireless Communications & Signal Processing (WCSP). Piscataway, NJ: IEEE, 2015: 67-70

Shi Leyi, bron in 1975. PhD, professor, PhD supervisor. Senior member of CCF. His main research interests include cyber security, game theory, and trusted computing.
石乐义, 1975 年生. 博士, 教授, 博士生导师, CCF 高级会员. 主要研究方向为网络安全、博弈论和可信计算.

Lan Ru, born in 1996. Master candidate. Her main research interests include active network attack and defense, non-orthogonal multiple access.
兰 茹, 1996 年生. 硕士研究生. 主要研究方向为主动网络攻击与防御、非正交多址接入.

Duan Pengfei, born in 1995. Master candidate. His main research interests include active network attack and defense.
段鹏飞, 1995 年生. 硕士研究生. 主要研究方向为主动网络攻击和防御.

Han Qiang, born in 1999. Master candidate. His main research interests include network security and security of the blockchain.
韩 强, 1999 年生. 硕士研究生. 主要研究方向为网络安全、区块链安全.

附录 A:

表 A1 6-4 系统各用户码本

用户	码本
用户 1	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0.262+0.965i & -0.965+0.262i & -0.262-0.965i & 0.965-0.262i \\ 0.708+0.708i & -0.708+0.708i & -0.708-0.708i & 0.708-0.708i \end{bmatrix}$
用户 2	$\begin{bmatrix} 0.708+0.708i & -0.708+0.708i & -0.708-0.708i & 0.708-0.708i \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0.262+0.965i & -0.965+0.262i & -0.262-0.965i & 0.965-0.262i \end{bmatrix}$
用户 3	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0.262+0.965i & -0.965+0.262i & -0.262-0.965i & 0.965-0.262i \\ 0.965+0.262i & -0.262+0.965i & -0.965-0.262i & 0.262-0.965i \\ 0 & 0 & 0 & 0 \end{bmatrix}$
用户 4	$\begin{bmatrix} 0.262+0.965i & -0.965+0.262i & -0.262-0.965i & 0.965-0.262i \\ 0.965+0.262i & -0.262+0.965i & -0.965-0.262i & 0.262-0.965i \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
用户 5	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0.708+0.708i & -0.708+0.708i & -0.708-0.708i & 0.708-0.708i \\ 0 & 0 & 0 & 0 \\ 0.965+0.262i & -0.262+0.965i & -0.965-0.262i & 0.262-0.965i \end{bmatrix}$
用户 6	$\begin{bmatrix} 0.965+0.262i & -0.262+0.965i & -0.965-0.262i & 0.262-0.965i \\ 0 & 0 & 0 & 0 \\ 0.708+0.708i & -0.708+0.708i & -0.708-0.708i & 0.708-0.708i \\ 0 & 0 & 0 & 0 \end{bmatrix}$