

引用格式: 兰茹, 段鹏飞, 石乐义. 基于 m 序列的端信息扩展序列生成机制研究[J]. 微电子学与计算机, 2022, 39(3): 65-70.
[LAN R, DUAN P F, SHI L Y. Research on generation mechanism of End Spreading based on m-sequence[J]. Microelectronics & Computer, 2022, 39(3): 65-70.] DOI: 10. 19304/J. ISSN1000-7180. 2021. 0767

基于 m 序列的端信息扩展序列生成机制研究

兰 茹¹, 段鹏飞¹, 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: 端信息扩展被用来解决高速端信息跳变系统中同步认证难的问题. 其使用多项端信息组成的扩展序列来表征身份信息并使得各项端信息与所表示数据本身无关, 达到隐藏真实信息的目的. 然而, 现有算法生成的端信息扩展序列存在伪随机性差、抗分析能力弱等弊端, 不利于保障原始数据的安全与隐私. 针对上述问题, 首先将 m 序列引入端信息扩展序列的生成过程中, 提出了基于 m 序列的端信息扩展序列生成机制, 使其具有良好的机密性与伪随机性; 其次, 详细介绍了基于 m 序列的端信息扩展序列生成机制中包含的消息预处理、m 序列生成与调制、端信息扩展序列生成等模块; 随后, 对其所具有的机密性、容失性及抗截获性等特性进行了理论分析; 最后, 对所提出机制生成的端信息扩展序列进行了性能测试实验并以现有端信息扩展序列生成算法作为对比方案. 实验结果表明基于 m 序列生成的端信息扩展序列具有更好的伪随机性及鲁棒性, 对保障秘密信息的安全可靠传输具有重要意义.

关键词: 端信息扩展; m 序列; 伪随机性; 鲁棒性

中图分类号: TP393. 08

文献标识码: A

文章编号: 1000-7180(2022)03-0065-06

Research on generation mechanism of end spreading based on m-sequence

LAN Ru¹, DUAN Pengfei¹, SHI Leyi^{1,2}

(1 College of Oceanography and Space Informatics, China University of Petroleum, Qingdao 266580 China;

2 College of Computer Science and Technology, China University of Petroleum, Qingdao 266580, China)

Abstract: End Spreading is proposed to solve the problem of synchronization authentication in high-speed End Hopping system, which expresses the identity information as the extended sequence composed of several independent end information and protects the security and privacy of identity information well. However, the End Spreading sequence generated by the existing algorithm has poor pseudo-randomness and weak anti-analysis ability, which is not conducive to ensuring the security and privacy of the original data. Therefore, the m-sequence was introduced into the generation process for the first time and proposes the generation mechanism of End Spreading based on m-sequence, making it have great confidentiality and pseudo-randomness. Secondly, the modules involved in this mechanism are discussed in detail, such as message preprocessing, m-sequence generation and modulation, and End Spreading sequence generation. Then, the characteristics equipped by the End Spreading sequence generated by the generation mechanism based on m-sequence are analyzed theoretically, like concealment, loss-tolerance, and anti-interference. Finally, the performance tests are conducted and the existing algorithm is regarded as the comparison scheme. The test results show that the End Spreading sequence generated by the

收稿日期: 2021-05-24; 修回日期: 2021-06-30

基金项目: 国家自然科学基金(61772551); 山东省自然科学基金项目(ZR2019MF034)

generation mechanism based on m-sequence has better pseudo-randomness and robustness, which is of great significance to guarantee the security and reliable transmission of secret information.

Key words: endspreading; m-sequence; pseudo-randomness; robustness

1 引言

如今,社会经济与科学技术快速发展,网络服务与网络应用日趋渐盛.但与此同时,网络安全形势日益严峻,数据失窃等网络安全事件频发.防火墙、入侵检测、身份认证等传统网络防御机制无法彻底消除被保护系统中存在的安全漏洞且无法有效应对来自攻击者自动且多样的网络攻击手段.

移动目标防御(moving target defense, MTD)通过先于敌手建立动态防御体系,来避免、迁移或减弱被保护系统所面临的安全威胁^[1].现有的 MTD 技术主要分为三种类型:系统级、应用级、网络级^[2].系统级 MTD 技术专注于动态切换被保护主机的操作系统、内存上下文及指令集合等^[3].应用级 MTD 技术涉及借助应用软件层面的动态变化来实现主动网络防御^[4].网络级 MTD 指的是动态地改变网络配置及网络拓扑从而实现主动防御,其代表性技术有 MT6D^[5]、SDN-based MTD^[6]、端信息跳变(End Hopping, EH)等.

作为网络级 MTD 技术的一种,端信息跳变通过在端对端数据传输过程中伪随机地改变端信息(如通信协议、通信端口、IP 地址等)来迷惑攻击者,起到保护主机系统的作用^[7].随着网络技术的快速发展,高对抗强度的相关场景对端信息跳变提出了高速率跳变与高隐蔽性的技术要求.然而,传统的跟踪式同步机制无法实现高速端信息跳变系统中的同步认证.石乐义等人创新性地提出了端信息扩展的概念,利用端信息扩展算法计算得出表征用户身份信息的端信息扩展序列解决了上述问题^[8].然而,现有算法生成的端信息扩展序列伪随机性差,导致其易被攻击者截获并破解,不利于保障通信内容的安全与隐私.

针对上述问题,本文在端信息扩展序列的生成过程中引入 m 序列并设计了新的端信息扩展序列生成算法,从而使其具有良好的伪随机性.同时,由于 m 序列所具有的加密作用,本文生成的端信息扩展序列不易被攻击者截获并破解,对保护数据隐私具有重要意义.

2 基于 m 序列的端信息扩展序列生成机制

基于 m 序列的端信息扩展序列生成机制包括

消息预处理、m 序列生成与调制、端信息扩展序列生成等模块.

2.1 消息预处理模块

消息预处理指原始消息 M 被编码算法 F_1 转换为编码消息 M' 的过程,如式(1)所示:

$$F_1(M, n) \Leftrightarrow M \rightarrow M' \Leftrightarrow M \rightarrow \{m'_1, \dots, m'_k, \dots, m'_t\} \quad (1)$$

式中, n 为生成 m 序列的本原多项式阶数, m'_k 为编码消息 M' 中的消息分组,其数量为 t 且二进制长度为 b .该模块中使用的编码算法 F_1 可描述如下.

算法 1: 原始消息编码算法

输入: M, n ;

输出: M' ;

- 1 假设原始消息 M 的字符长度 l ;
- 2 取 M 中的第 i 个字符,记为 chr_i ;
- 3 依据 ASCII 码,将 chr_i 转换为二进制格式 bin_i ;
- 4 若 bin_i 的长度不足 7,则对其左补零处理;
- 5 将 M 中的所有字符依次进行上述格式转换操作,得 $M_{\text{bin}} = \{\text{bin}_1, \text{bin}_2, \dots, \text{bin}_l\}$;
- 6 若 $7x \leq n \leq 7x+6, (x \geq 1 \text{ 且 } x \in N_1)$,则将 M_{bin} 合并 t 个消息分组,每个消息分组的二进制长度为 $7x$,不足
- 7 x 的消息分组则右补零,得 M' ;

在算法 1 中,由于 ASCII 码表的可打印字符范围是 $[32, 126]$,字符转换后的最大二进制为“0b1111110”,其长度为 7;最小二进制为“0b100000”,其长度为 6.因此为了统一格式,将各字符格式转换后的二进制长度设定为 7,不足部分则在其左侧补 0 处理.

2.2 m 序列生成与调制模块

m 序列是指带线性反馈的移位寄存器产生的周期最长序列^[9].一般的线性反馈移位寄存器原理方框图如图 1 所示.

在图 1 中, a_i 表示各级移位寄存器的状态, g_i 表示反馈线的连接状态,其取值决定了移位寄存器的序列结构.线性反馈移位寄存器可被表示为:

$$\begin{aligned} f(x) &= g_0 + g_1x + g_2x^2 + \dots + g_nx^n \\ &= \sum_{i=0}^n g_ix^i \end{aligned} \quad (2)$$

其能产生 m 序列的充要条件是特征多项式 $f(x)$ 为本原多项式,即 $f(x)$ 是既约的; $f(x)$ 可整除 $(x^m + 1)$, $m = 2^n - 1$; $f(x)$ 除不尽 $(x^q + 1)$, $q < m$.常用的

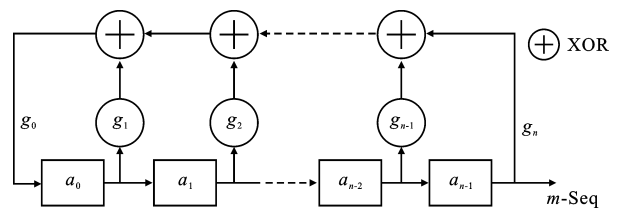


图 1 线性反馈移位寄存器原理图

Fig. 1 The principle diagram of linear feedback shift register

本原多项式如表 1 所示。

表 1 常用本原多项式

Tab. 1 The commonly used primitive polynomial	
<i>n</i>	本原多项式
7	$f(x) = x^7 + x^3 + 1$
9	$f(x) = x^9 + x^4 + 1$
14	$f(x) = x^{14} + x^{10} + x^6 + x + 1$
16	$f(x) = x^{16} + x^{12} + x^3 + x + 1$
17	$f(x) = x^{17} + x^3 + 1$

本模块将移位寄存器的初始状态 $\{a_{n-1}, a_{n-2}, \dots, a_0\}$ 用作 m 序列生成密钥(记为 key_m) 且将生成的 m 序列记作 $m\text{-Seq}$ 。

m 序列调制指的是由 m 序列生成器生成的 m 序列 $m\text{-Seq}$ 被编码消息中 M' 的消息分组 m'_k 依次调制的过程,如式(3) 所示:

$$F_2(M', m\text{-Seq}) \Leftrightarrow m\text{-Seq} \rightarrow m\text{-Seq}_M \Leftrightarrow m\text{-Seq} \rightarrow \{(m\text{-Seq})_{m'_1}, (m\text{-Seq})_{m'_2}, \dots, (m\text{-Seq})_{m'_k}\}$$
 (3)

式中,调制函数 F_2 指将编码消息 M' 中各消息分组 m'_k 用于调制上述生成的 $m\text{-Seq}$,从而得到调制后的 m 序列 $m\text{-Seq}_M$ 。本模块使用二进制位异或作为调制方法,具体调制过程如图 2 所示。

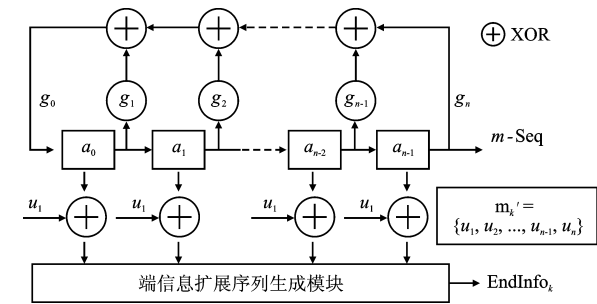


图 2 m 序列调制示意图

Fig. 2 The schematic diagram of m -sequence modulation

2.3 端信息扩展序列生成模块

端信息扩展序列生成指将经过编码消息 M' 中各消息分组 m'_k 调制后的 m 序列 $m\text{-Seq}_M$ 转换为各

类端信息序列并加载到数据包中形成端信息扩展序列的过程,如式(4) 所示。

$$F_3(m\text{-Seq}_M) = \{\text{EndInfo}_1, \text{EndInfo}_2 \dots \text{EndInfo}_k\}$$
 (4)

式中,端信息扩展序列生成算法 F_3 的作用是将 $m\text{-Seq}_M$ 转换为各类端信息序列。本机制选用目的端口 DstPort 作为 $m\text{-Seq}_M$ 的载体,其序列生成算法如下所示。其中, p 表示调制后的 m 序列 $m\text{-Seq}_M$ 中各分组的二进制长度, n 为生成 m 序列的本原多项式阶数。

算法 2: 目的端口序列生成算法

输入: $m\text{-Seq}_M, p, n$;

输出: DstPortSeq ;

- 1 取 $m\text{-Seq}_M$ 中的第 i 个元素,记为 $(m\text{-Seq})_i$;
- 2 以 n 为单位长度,将 $(m\text{-Seq})_i$ 划分为 num 个子小组,其中 $\text{num} = p/n$;
- 3 将上述 num 个子小组由二进制转换为十进制,得到 $(m\text{-Seq})_i$ 对应的 DstPortSeq_i ;
- 4 将 $m\text{-Seq}_M$ 中的所有元素依次进行上述操作,得到 DstPortSeq ;

为降低无关流量对端信息扩展序列在解调时的干扰程度,选用目的地址 DstIP 作为筛选合法端信息扩展序列的验证域。为避免 $m\text{-Seq}_M$ 中各分组所对应的目的端口序列 DstPortSeq_k 在被解调时出现分组错乱从而导致错误解调的情况,本机制选用源端口 SrcPort 作为分帧标志。两种端信息序列的生成算法如算法 3 所示。其中, $\text{DstIP}_{\text{pool}}$ 表示的是目的地址池,其长度为 len_{pool} ; key_{xor} 表示的是求目的地址时使用的异或密钥; len_{bin} 表示的是求随机值 random 时使用的 $m\text{-Seq}_M$ 中各分组的比特数。

算法 3: 目的地址与源端口序列生成算法

输入: $m\text{-Seq}_M, \text{DstPortSeq}, \text{DstIP}_{\text{pool}}, \text{key}_{\text{xor}}, \text{len}_{\text{bin}}$;

输出: DstIPSeq 与 SrcPortSeq ;

- 1 取 DstPortSeq 中 $(m\text{-Seq})_i$ 对应的目的端口序列,即 DstPortSeq_i ;
- 2 DstPortSeq_i 中的第 j 个目的端口,记为 dstport_j ;
- 3 计算 dstport_j 与 key_{xor} 的异或值,记为 xor ;
- 4 计算 xor 对 len_{pool} 的模值,记为 index ;
- 5 从 $\text{DstIP}_{\text{pool}}$ 中取第 index 个目的地址,记作 dstIP_j ;
- 6 遍历 DstPortSeq_i 中的所有目的端口执行上述异或及取模运算,最终得到 DstIPSeq_i ;
- 7 取 $m\text{-Seq}_M$ 中的第 i 个元素,记作 $(m\text{-Seq})_i$;
- 8 取 $(m\text{-Seq})_i$ 中的前 len_{bin} 位二进制并转为十进制,记为 random ;
- 9 计算 random 与 dstport_j 的和值并对 65535 取模,记模值为 srcport_j ;
- 10 遍历 DstPortSeq_i 中的所有目的端口执行上述格式转换

及取模运算,最终得到 SrcPortSeq_i ;

- 11 对 DstPortSeq 中所有 $(m\text{-Seq})_k$ 对应 DstPortSeq_k 执行上述操作,得到目的地址序列 DstIPSeq 与源端口序列 SrcPortSeq ;

至此,客户端将上述 3 类端信息序列加载于数据包中,即可得到端信息扩展序列.在实际操作中,客户端无需发送全部的端信息扩展序列至服务器端,仅需发送编码消息 M' 中各消息分组 m'_k 对应的连续一部分序列即可.本文将这一连续端信息扩展序列的长度称为端信息扩展度,表示为 e .基于 m 序列的端信息扩展序列生成机制流程如图 3 所示.

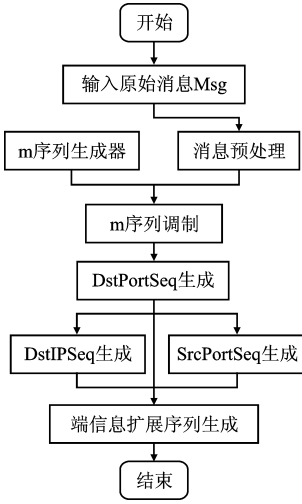


图 3 基于 m 序列的端信息扩展序列生成机制流程图

Fig. 3 The flowchart of generation mechanism of End Spreading sequence based on m -sequence

3 特性分析

端信息扩展序列特性分析涉及机密性分析、容失性分析以及抗截获性分析.

3.1 机密性分析

在基于 m 序列的端信息扩展序列生成过程中,将具有编码消息特征的 m 序列进行格式转换,获得伪随机性良好的端信息扩展序列.由于原始消息被表示为多条端信息扩展序列,窃听者在缺少解密参数及相应算法的情况下,无法实现对端信息扩展序列的破解,从而有效保护消息的安全性与隐私性.由于文献[8]并未对原始消息作加密处理,其生成的端信息扩展序列易被攻击者截获并破解,从而对消息的机密性造成威胁.相比之下,本文所提机制有效提高了序列的机密性.

3.2 容失性分析

在端信息跳变客户端,原始消息被表示为多条端信息扩展序列(其数量称为端信息扩展度),且其

具有良好的容失性,即使在传输过程中发生序列丢失,剩余序列仍能被接收端正确解调.不难想象,较小的端信息扩展度限制了端信息扩展序列的丢失数量,一旦发生丢失就会对序列辨识度产生较大影响,从而发生错误解码.当使用较大端信息扩展度时,部分序列的丢失并不影响其序列辨识度,因而具有良好的容失性.本文所提机制可依据网络环境的恶劣程度对端信息扩展度作灵活调整,从而保证服务器端能够正确解调扩展序列.而文献[8]扩展序列生成算法中的端信息扩展度固定不变且数值较小,这使得客户端无法依据实际的网络状况有效调整端信息扩展序列的生成数量,从而易造成错误解码,不利于保障原始消息的完整性和可用性.

3.3 抗截获性分析

在基于 m 序列的端信息扩展序列生成过程中,客户端将原始消息 M 表示为多条端信息扩展序列.由于这些序列在外观上与 M 不具有明显的相关性,因此攻击者很难由监听到的端信息扩展序列推导出原始消息.假设攻击者从网络中窃取的数据包数量为 α (其中合法端信息扩展序列的数量为 β)、攻击者每次抽取分析的数据包数量为 η 、端信息扩展度为 e 、序列容失度为 τ ,则其在破解原始消息时能够抽取到合适数量的端信息扩展序列的概率 P 符合超几何分布,如式(5)所示:

$$P = \begin{cases} 0, & 0 < \eta < (e - \tau) \cup e < \eta < \alpha. \\ \frac{\sum_{i=0}^{\tau} C_{\beta}^{e-i} C_{\alpha-\beta}^{\tau-e+i}}{C_{\alpha}^{\tau}}, & (e - \tau) \leq \eta \leq e. \end{cases} \quad (5)$$

攻击者在未知伪随机序列生成密钥 key_{xor} 的情况下,需尝试的 key_{xor} 数量为 2^n .因此攻击者的成功破解出原始消息的概率 Q 为:

$$Q = \frac{1}{2^{n+b}} P = \frac{\sum_{i=0}^{\tau} C_{\beta}^{e-i} C_{\alpha-\beta}^{\tau-e+i}}{2^{n+b} C_{\alpha}^{\tau}}, (e - \tau) \leq \eta \leq e \quad (6)$$

从式(6)可以看出, Q 与 n, b 呈负相关,即随着 n, b 的增长,攻击者的成功概率 Q 呈现出指数级下降.在上述假设中,合法端信息扩展序列的占比为 e/α .因此,当客户端在发送端信息扩展序列时选择常规端信息跳变流量作为掩护流量,则攻击者能够成功破解出原始消息的概率 Q 将大幅下降,即 $e \ll \alpha$ 时, $Q \approx 0$.

4 实验测试与分析

本节将对基于 m 序列生成的端信息扩展序列进行性能测试,同时将文献[8]中现有端信息扩展序列生成算法作为本文所提机制的对比方案. 在本实验中,两种方案均采用大小为 15 kB 的电子文档作为原始消息,并依据各自的生成算法生成相应的端信息扩展序列. 随后,对上述两类序列分别进行性能测试,包括伪随机性、容失性、抗干扰性等方面.

4.1 伪随机性测试

为比较文献[8]中的现有生成算法与本方案所生成的端信息扩展序列的伪随机性,本文采用信息熵来对其进行定量分析并比较. 信息熵在信息论中是对不确定性的一种度量且熵值越大,系统的不确定性越高,系统越混乱. 本测试实验选用 4 种不同的 m 序列(其中, $n \in \{7, 9, 14, 16\}$)来生成端信息扩展序列并分别计算其在不同端信息扩展度下的熵值. 最终的熵值测试结果如图 4 所示.

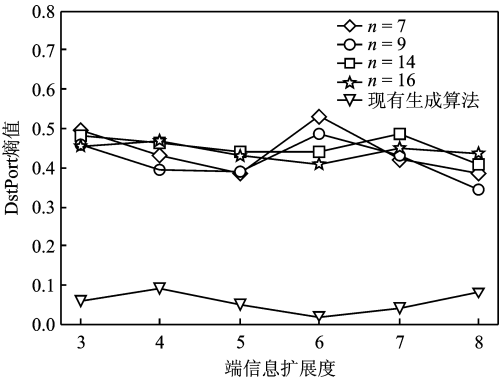


图 4 各方案在不同端信息扩展度下的熵值
Fig. 4 The entropy value under different e

可以看出,现有算法生成的端信息扩展序列的熵值处于 $[0.1, 0.2]$ 之间,这说明上述序列不确定性较低,易被攻击者分析出序列规律从而威胁所传信息的安全与隐私. 而本文方案生成的端信息扩展序列熵值较现有生成算法有明显提升,其熵值均处于 0.3 以上. 由此可得出结论,基于 m 序列的端信息扩展序列生成机制改善了现有端信息扩展序列的伪随机性,对保护数据的安全与隐私具有重要意义.

4.2 容失性测试

容失性指端信息扩展序列在发生序列丢失后,剩余序列仍能被服务器端准确解调的能力. 本文使用误码率(bit error rate, BER)来衡量其抗丢失能力并使用 Linux 系统中网络模拟功能模块 netem 来模拟网络丢包现象. 本文设计了如下 4 种方案:现有

生成算法、 $e=4$ 、 $e=6$ 、 $e=8$. 假设网络丢包率(packet loss rate, PLR)范围为 $(0\%, 40\%)$,测试结果如图 5 所示.

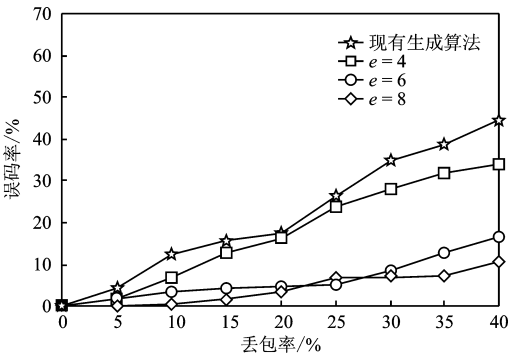


图 5 各方案在不同丢包率下的误码率
Fig. 5 The BER under different PLR

从图 5 中可以看出,现有生成算法的误码率随着丢包率的提高而显著升高,当丢包率达到 40% 时,其误码率达到了 40%. 这是由于现有生成算法未进行序列分帧从而导致在解码时易发生连锁误码反应. 相比之下,本文方案的误码率均低于现有生成算法且随着端信息扩展度的提高,误码率有明显下降. 当丢包率为 40% 时, $e=6$ 或 $e=8$ 方案的误码率均低于 10%. 这是由于较大的端信息扩展度能够使得端信息扩展序列具有良好的容失性.

4.3 抗干扰性测试

为降低无关流量对端信息扩展序列在解调时的干扰程度,基于 m 序列生成的端信息扩展序列使用目的地址 DstIP 作为筛选合法端信息扩展序列的验证域. 本文使用 Hping3 来生成大量干扰流量并对如下四种方案进行抗干扰性测试,即现有生成算法、 $e=4$ 、 $e=6$ 、 $e=8$. 最终的测试结果如图 6 所示.

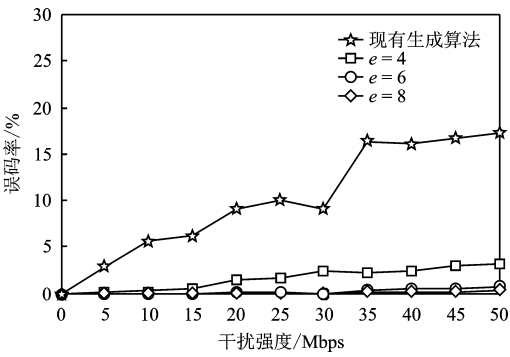


图 6 各方案在不同干扰强度下的误码率
Fig. 6 The BER under different disturbance intensity

从图 6 中可以看出,由于缺少合法端信息扩展序列验证机制,现有生成算法的误码率随着攻击强

度的提高而急剧升高. 在攻击强度为 50 Mbps 时, 其误码率达到了 15% 以上. 相比之下, 本文方案由于使用了目的地址 DstIP 作为筛选合法端信息扩展序列的验证域, 其误码率并没有随着攻击强度的提高出现明显变化. 由此可得出结论, 本文方案生成的端信息扩展序列具有良好的抗干扰能力.

5 结束语

移动目标防御通过先于敌手建立动态防御体系, 来避免、迁移或减弱被保护系统所面临的安全威胁并使得攻击者无法轻易对其展开攻击. 为解决高速端信息跳变系统中的同步认证, 端信息扩展的概念被提出. 本文在其生成过程中引入 m 序列并给出新的端信息扩展序列生成算法. 理论分析与实验结果均表明, 本文方案较现有算法生成的端信息扩展序列具有良好的机密性、伪随机性与鲁棒性, 这对于将端信息扩展序列应用于信息的隐蔽传输或其他领域具有重要意义. 在下一步的研究工作中, 应关注如何实现多用户端信息跳变系统中的身份认证及提高端信息扩展序列的信息传输速率等方面.

参考文献:

- [1] PISKOZUB M, SPOLAOR R, CONTI M, et al. On the resilience of network-based moving target defense techniques against host profiling attacks[C]//Proceedings of the 6th ACM Workshop on Moving Target Defense. London: ACM, 2019: 1-12. DOI: 10.1145/3338468.3356825.
- [2] STEINBERGER J, KUHNERT B, DIETZ C, et al. DDoS defense using MTD and SDN[C]//Proceedings of 2018 IEEE/IFIP Network Operations and Management Symposium. Taipei, China: IEEE, 2018: 1-9. DOI: 10.1109/NOMS.2018.8406221.
- [3] 谭韧, 殷肖川, 焦贤龙, 等. 一种软件定义 APT 攻击移动目标防御网络架构[J]. 山东大学学报(理学版), 2018, 53(1): 38-45. DOI: 10.6040/j.issn.1671-9352.2.2017.196.
- TAN R, YIN X C, JIAO X L, et al. Software defined APT attack moving target defense network architecture[J]. Journal of Shandong University(Natural Science), 2018, 53(1): 38-45. DOI: 10.6040/j.issn.1671-9352.2.2017.196.
- [4] 全青, 张铮, 张为华, 等. 拟态防御 Web 服务器设计与实现[J]. 软件学报, 2017, 28(4): 883-897. DOI:

10.13328/j.cnki.jos.005192.

- TONG Q, ZHANG Z, ZHANG W H, et al. Design and implementation of mimic defense web server[J]. Journal of Software, 2017, 28(4): 883-897. DOI: 10.13328/j.cnki.jos.005192.
- [5] DUNLOP M, GROAT S, URBANSKI W, et al. MT6D: a moving target IPv6 defense[C]//Proceedings of MILCOM 2011 Military Communications Conference. Baltimore: IEEE, 2011: 1321-1326. DOI: 10.1109/MILCOM.2011.6127486.
- [6] SHARMA D, KIM DS, YOON S, et al. FRVM: flexible random virtual IP multiplexing in software-defined networks[C]//12th IEEE International Conference on Big Data Science and Engineering. New York: IEEE, 2018: 579-587. DOI: 10.1109/TrustCom/BigDataSE.2018.00088.
- [7] 石乐义, 贾春福, 吕述望, 等. 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. DOI: 10.3321/j.issn:1000-436X.2008.02.016.
- SHI L Y, JIA C F, LV S W, et al. Research on End Hopping for active network confrontation[J]. Journal on Communications, 2008, 29(2): 106-110. DOI: 10.3321/j.issn:1000-436X.2008.02.016.
- [8] 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. DOI: 10.11959/j.issn.1000-436x.2019071.
- 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. DOI: 10.11959/j.issn.1000-436x.2019071.
- [9] 冯建利. 跳频保密通信中跳频序列的设计与实现[J]. 四川兵工学报, 2011, 32(3): 56-58. DOI: 10.3969/j.issn.1006-0707.2011.03.018.
- FENG J L. Design and implementation of frequency hopping sequence in frequency hopping secure communication[J]. Sichuan Ordnance Journal, 2011, 32(3): 56-58. DOI: 10.3969/j.issn.1006-0707.2011.03.018.

作者简介:

兰茹女, (1996-), 硕士. 研究方向为主动网络防御、网络隐蔽信道.

段鹏飞男, (1995-), 硕士. 研究方向为主动网络防御、区块链.

石乐义(通讯作者)男, (1975-), 博士, 教授. 研究方向为信息安全、博弈论. E-mail: shileyi@upc.edu.cn.