

基于移动目标防御的卫星互联网防御系统设计

徐瑞荣

(中国石化胜利油田电力分公司, 山东 东营 257087)

摘 要: 卫星互联网在促进信息互联互通的同时, 也引发了日益复杂的安全性问题。将作为主动防御手段的移动目标防御技术引入卫星互联网的安全防护中, 通过将卫星互联网的IP地址、协议端口等端址信息进行伪随机变化, 增强系统的抗截获攻击和拒绝服务攻击性能, 从而实现主动防御。在此基础上, 设计基于移动目标防御的卫星互联网原型系统, 解决跳变同步、跳变传输等关键问题, 验证原型系统的可行性和有效性。

关键词: 移动目标防御; 卫星互联网; 主动网络防御; 同步

中图分类号: TN927

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2024043

Design of Satellite Internet Defense System Based on Mobile Target Defense

XU Ruirong

SINOPEC Shengli Oil-Field Electric Power Branch, Dongying 257087, China

Abstract: While satellite Internet promote information inter connectivity, they also raise increasingly complex security issues. This article introduced mobile target defense as proactive defense measure into the cyber protection of satellite Internet. By changing the IP address, protocol port information of satellite Internet pseudo-randomly, the system's resistance to interception attacks and denial of service attacks was enhanced, thereby achieving active defense. On this basis, a prototype system of satellite Internet based on mobile target defense was designed, which solved some key problems such as synchronization scheme, hopping data transmission, and verified the feasibility and effectiveness of the prototype system.

Keywords: mobile target defense, satellite Internet, proactive cyber defense, synchronization

0 引言

卫星互联网是近年来受到广泛关注的信息基础设施^[1]。卫星互联网包括了地球静止轨道 (Geostationary Orbit Satellite, GEO) 卫星、中轨 (Medium Earth Orbit, MEO) 卫星和低轨 (Low Earth Orbit, LEO) 互联网星座^[2]。近年来, 随着万物互联的快速发展, 卫星互联网, 特别是以“星链”为代表的低轨卫星网络受到了广泛关注, 能够为全球人类的工作、研究和生活提供便捷的网络服务。2022年12月, SpaceX公布了专门为军事目的设计的“星盾”计划^[3]。2023年8月, 在拉斯维加斯DEFCON会议上, 5个黑客团队对一颗名为“MoonLighter (月光者)”的低

轨卫星发起了持续数小时的攻击比赛^[4]。可见, 卫星互联网已成为网络攻防的新战场和新焦点。

与传统的计算机网络类似, 卫星互联网同样面临DoS拒绝服务、截获嗅探等攻击和威胁。因此, 现阶段很多研究者与科研机构将传统网络防御技术如加密流量监测、入侵检测技术以及深度学习等应用到了卫星互联网中。针对跨域安全攻击的应对方法, 也可以通过跨域攻击溯源法^[5]解决。通过针对组网架构的特点同时考虑切换预留时间和影响切换的相关属性值, 提出一种基于接收信号强度预测的多属性权重优化的自适应安全切换决策算法^[6], 确保整个系统中用户节点发生网络切换的安全性和高效性。这些传统防护技术在本质上都是被动式防御, 因此对于人工干

预困难的卫星互联网来讲是十分不利的。

1 移动目标防御

移动目标防御 (Moving Target Defense, MTD)^[7]是由美国国防部于2011年提出的一种“改变游戏规则”的主动网络防御技术。移动目标防御借鉴了移动靶射击训练的思想,通过将目标靶快速、伪随机地移动,从而干扰射击者,增加射击者难度,降低目标靶遭受射击后被命中的概率。

移动目标防御将自身看作动态变化的靶标,这里所包括的动态变化有着丰富的层次和种类。从攻击面转移的角度分析,移动目标防御技术可以分为数据攻击面、软件攻击面、网络攻击面和平台攻击面等4种类型的技术^[8]。其中,数据攻击面的移动目标防御包括数据随机化、数据多样化等技术。软件攻击面的移动目标防御包括地址空间布局随机化、代码随机化、软件多态化等技术。网络攻击面包括动态网络架构、网络地址随机化和端信息随机跳变技术。平台攻击面的移动目标防御包括平台动态迁移、虚拟化技术、Web应用动态防御和移动平台动态防御^[9]。

本文针对卫星互联网所面临的安全问题展开研究,重点分析网络攻击面的网络地址和端口信息随机化在卫星互联网中的原型实现和测试。本文主要贡献如下。

(1) 构建了基于移动目标防御的卫星互联网安全防护系统模型。

(2) 研究了移动目标防御中的跳变同步策略等关键策略,通过对多种同步方法进行细致的比对分析,选定了一种适合卫星互联网环境的优化同步解决方案。

(3) 探讨了一种针对卫星互联网特性的时间基数据传输策略,确保了在卫星与地面间数据传输的持续性、完整性。

2 相关工作

国际空间数据系统咨询委员会等权威机构在近年来不断完善空间网络安全标准体系,制定了一系列的标准和规范。这些标准涵盖空间网络安全的基本框架、通信协议、加密算法等多个方面,为保障空间数据的安全传输提供了坚实的理论基础。同时,也有不少学者开展了卫星互联网的攻防策略研究。

Rosenberg等^[10]提出了一组卫星互联网安全协议,具有高比特、低成本以及数据保护能力强的特点。然而,由于它在安全服务方面较为固定,因此无法充分满足空

间网络对于多样化安全的需求。

Fischer等^[11]进行了卫星互联网中的通信链路监听、嗅探、拒绝服务等攻击的防护策略研究,用以增强卫星互联网链路数据传输的可靠性。

Maple等^[12]研究了卫星互联网远程任务操作中的消息加密对于远程安全控制的时延影响,从而使得任务规划者能够综合考虑安全漏洞风险和威胁。

Liu等^[13]总结了卫星互联网安全防护的关键技术,重点分析了卫星互联网的形式化认证、访问验证以及加密协议等关键策略。

She等^[14]提出了一种针对卫星互联网的异常流量检测方法,对卫星互联网中的攻击行为方式及所产生的攻击流量进行了分析和建模。

在空间网络的主动防御研究方面,参考文献[15]从可信、行为安全、情报威胁以及智能化态势感知等方面,提出了卫星互联网的主动防御框架。该框架综合包括了安全审计、认证、密码计算、入侵检测、攻击容忍等各项传统的网络安全技术,不仅框架庞大复杂,而且没有使用移动目标防御等主动网络对抗新技术。

参考文献[16-17]提出了一种卫星互联网安全动态赋能架构,进行了形式化描述和建模,并给出了一种适用于卫星互联网的双重判定威胁处置方法。该动态赋能架构针对空间卫星网络面临的安全需求动态变化、威胁动态变化和防护技术动态变化的基本特征,提出了融合安全服务能力编排、安全态势分析、安全威胁处置指挥等于一体的防护架构,并进行了形式化的描述和推理证明。同样,该方案中也没有提及移动目标防御等主动防御技术在卫星互联网中的赋能研究。

根据卫星互联网中存在的DoS攻击、远程安全控制的时延问题、截获嗅探等攻击和威胁,本文提出基于移动目标防御的卫星互联网防御系统,通过制定跳变策略等关键策略,与多种同步方法进行细致的对比分析,验证本文所提系统在不显著增加通信时间的情况下,能够有效地为卫星互联网保障通信安全,可有效解决DoS攻击、Replay攻击、跟随攻击、远程安全控制的时延过大的问题以及防止截获嗅探等攻击的威胁;确保可以将卫星通信收发系统的通信地址、传输端口等信息进行伪随机动态变化,并为合法客户端提供同步接入,避免攻击者访问卫星通信系统,最终增强了系统的抗截获攻击和拒绝攻击的性能,能够有效抵抗DoS攻击、Replay攻击以及跟随攻击等,最终有效提升了卫星互联网的抗攻击性能。

3 基于移动目标防御的卫星互联网防护模型

3.1 卫星互联网系统

卫星互联网系统示意如图1所示,由不同类别的人造地球卫星、地面站构成^[18]。

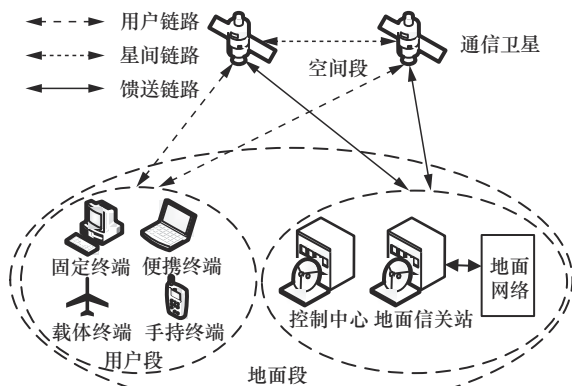


图1 卫星互联网系统示意

在卫星互联网架构中,地面站扮演着操控卫星通信并支撑用户终端设备服务的核心地面设施的角色,主要由地面信关站和地面卫星控制中心(GSCC)等关键组件构成。用户端方面,则包含了一系列具备卫星通信接口功能的用户终端设备(UTE)。这些终端设备不仅负责上行链路信号的发送,将信息传递给卫星及地面站,同时承担着下行链路信号的接收任务,即从轨道上的卫星中接收信号的任务。

3.2 移动目标防御空间网络模型

本文将卫星互联网与网络层面的移动目标防御技术相融合,建立相应的空间网络安全防御系统模型,并设计实现一套基于移动目标防御的空间网络防护体系原型系统。基于移动目标防御的空间网络安全防御模型如图2所示。

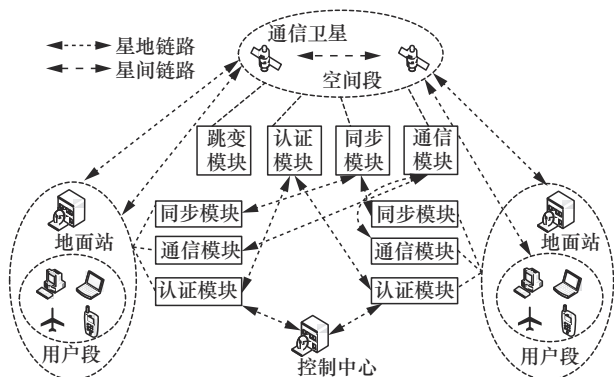


图2 基于移动目标防御的空间网络安全防御模型

基于移动目标防御的空间网络安全防御模型由同步模块和通信模块等组成,形式化描述如下。

同步模块负责与跳变卫星建立连接:

Information(EI)→{Succ, Fail}

其中,若输出Succ则表明网络层面端址跳变的空间网络安全防御模型中的同步模块与跳变卫星同步成功,若输出Fail则表示同步模块与跳变卫星同步失败。

跳变卫星由认证模块、同步模块、跳变模块、通信模块组成。同步模块负责通过特定的算法和协议保持通信各方的跳变策略一致,保持通信的连续性和可用性。通信模块负责通过选择的协议类型与地面控制中心以及其他卫星之间进行数据传输。

4 关键策略

4.1 同步策略

设卫星跳变周期为 T ,若用户端能在 T 时间内完成与通信卫星同步,即判定为同步成功;反之,若未能在此周期内完成同步,则判定为同步失败。具体而言,同步成功的判定需满足以下条件:接收到连接请求的时间点减去关键参数的初始化时刻要小于或等于周期 T 。

在同步策略下,通过本地时间和跳变图案实现同步。该策略通过确定跳变图案中对应的端址信息,实现同步并建立通信连接,其工作原理示意如图3所示。

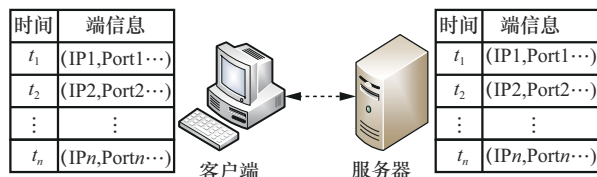


图3 严格时间同步工作原理

ACK应答同步工作原理如图4所示。

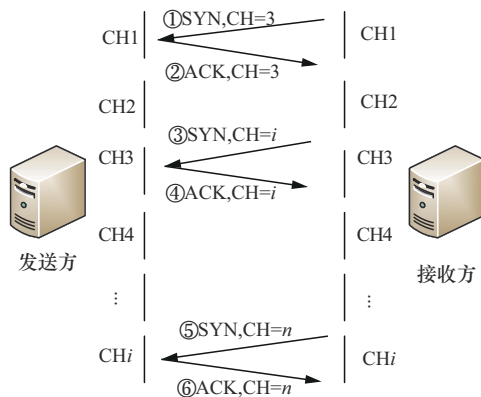


图4 ACK应答同步工作原理

空间网络环境中用户与卫星间的传输时延为 τ ，用户计算卫星端址信息的时间为 ε_1 ，因此整个同步流程的总耗时为 ε_1 加上 τ 。为了确保同步的顺利进行，跳变周期 T 必须大于 ε_1 与 τ 之和。然而，ACK应答同步存在一个显著的缺陷，即其对截获攻击的防御能力相对较弱。

时间戳同步技术原理如图5所示，客户端向服务器发送一个请求，目的是获取服务器生成的时间戳，在收到客户端发送的请求以后，根据请求服务器生成一个实时的时间戳再发送回客户端。接下来双方均运用同一个跳变算法，并依据这个请求通过服务器生成的时间戳来计算各自的端信息。

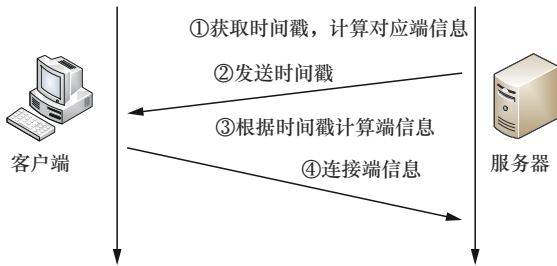


图5 时间戳同步技术原理

采用UDP发言人辅助的时间戳同步策略，会导致总体所需时间的增加，并且会提升遭受攻击的概率和风险。

若用户根据相同算法来计算卫星端址信息消耗的时间为 r ，则整个同步流程的总耗时将是 r 加上两倍传输时延 τ ，因此要求跳变周期 T 必须大于 r 与 2τ 之和。

4.2 跳变策略

本模型中的跳变算法采用了IP地址和端口号伪随机生成的方式，具体为：

$$(\text{IP}_{\text{key}}, \text{Port}_{\text{key}}) = \text{EndInfo}(\text{timestamp})$$

其中， IP_{key} 为跳变地址，范围为 $1 \leq \text{IP}_{\text{key}} \leq n$ ， n 表示地址池中的个数； Port_{key} 表示跳变端的输入端口号，用以计算当前端址信息 EndInfo ， EndInfo 则表示伪随机函数，通过本文涉及的跳变算法和时间戳信息计算得出。

4.3 数据传输策略

本文设计的数据传输策略如图6所示，流程如下。

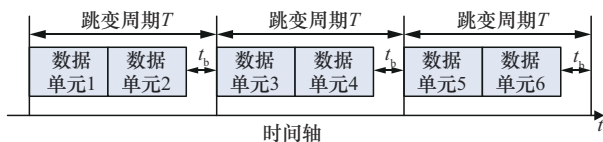


图6 数据传输策略

(1) 初始连接阶段：用户端与卫星建立连接。鉴于连接建立时可能处于任一跳变周期中，为确保数据传输的连续性，规定在当前跳变周期内不进行任何数据传输操作，以此避免数据传输因周期切换而中断。

(2) 数据传输阶段：从紧接着的下一个跳变周期开始，通信双方正式进入数据传输环节。双方预确定每个跳变周期内应传输的固定数量数据单元，并在整个周期内持续、稳定地传输这些已确定的数据单元。

(3) 周期结束与重启：当双方在当前跳变周期内完成规定的单元传输任务后，会暂停该周期的数据传输活动。随着下一个跳变周期的到来，双方将重新启动数据传输流程，按照既定步骤继续传输数据，直至整个通信过程结束。

图6中的跳变周期均为 T 且固定， T 内传输固定大小的数据量， t_b 为一个 T 内的空余时间。

4.4 安全性分析

下文将从DoS攻击、Replay攻击和跟随攻击等方面进行安全性分析。

(1) DoS攻击。攻击者在某一时间段对目标主机集中、连续发送过量的访问请求，使合法用户无法正常访问目标主机，使攻击主机资源消耗殆尽。

设攻击者了解跳变通信卫星的跳变地址池和端口跳变范围，对跳变通信卫星进行DoS攻击。在某一时刻，若跳变通信卫星仅有一对地址、端口组合处于活动状态，那么此种情况下攻击者攻击成功所需要的时间 T' 为

$$T' = \left[\sum_{i=1}^{N-1} i \frac{C_{N-1}^i}{C_N^i C_{N-1}^1} + 1 \right] T \quad (1)$$

式中， $N=n \times P$ ， n 代表跳变地址池中地址个数， P 代表端口的选取范围。 T 代表的是非端信息跳变情况下攻击者从发起攻击到击中目标所耗费的时间。从式(1)中可以看出，在端信息跳变的情况下，攻击者击中目标的时间明显大于非端信息跳变的情况，而且随着 N 的增大， T' 也会随之增大。因此，证明了本文设计的系统可以增加攻击者的攻击耗费时间，达到网络防御的效果。

(2) Replay攻击。在本文设计的系统中，在同步策略中加上时间戳机制，把时间戳和其他参数一起进行签名处理后发给认证方。由于时间戳的新鲜性，攻击者将截获的端信息重放发给验证方时，验证不通过，因此攻击者无法假冒合法用户与通信卫星进行通信，也就无法利用Replay攻击对空间网络系统进行攻击。

(3) 跟随攻击。攻击者根据截获的信息判断端信息跳变规律,不断定位当前跳变节点的端信息进行精确攻击。假设跳变周期为 T ,攻击者定位当前端信息并发起攻击所需的时间为 t_A 。当 $T < t_A$ 时,攻击成功概率为0,即在攻击者发起攻击之时端信息已经跳变;当 $t_A \geq T$ 时, T 越小,攻击成功的概率越低。一般情况下,缩短跳变周期 T 或者增大攻击者攻击所需时间 t_A 可以有效抵御跟随攻击。

5 原型系统实现

5.1 系统模块设计

卫星互联网移动目标防御原型系统功能模块如图7所示。

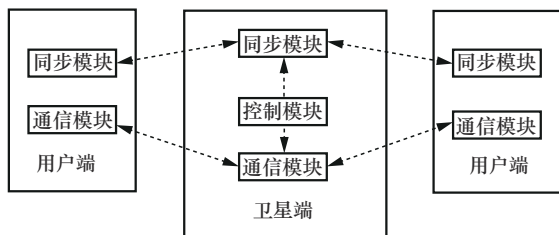


图7 卫星互联网移动目标防御原型系统功能模块

其中,用户端包含通信模块和同步模块两大核心组成部分。通信模块的作用是与卫星建立稳定的数据传输通道,使用户端与卫星能够进行连续、稳定的数据交换;同步模块通过特定的算法计算卫星的端址信息,使通信模块能够与正确的目标进行通信行为。

卫星端同样包含同步模块和通信模块,用于与用户端进行数据通信。为了有效进行跳变同步和通信,卫星端设置了控制模块,具有指令控制功能,用于根据预先

设计的跳变策略执行网络层面的端口、地址信息的伪随机切换,使卫星的端址信息能够产生高效和不可预测的变化;通信模块负责在用户端和卫星之间建立起可靠的信息交换的通道,进行卫星和用户端的数据交换。

5.2 系统通信过程

系统通信流程如图8所示,具体如下。

用户终端A与通信卫星C建立同步连接,实现数据传输。在单次转发的情况下,通信卫星C仅将数据转发至地面站或另一用户终端B。如需多次转发,数据首先由通信卫星C传至另一通信卫星D,随后由通信卫星D转发至地面站或用户终端B。

6 系统测试

6.1 系统性能测试

环节一是端址信息随机性测试,旨在验证系统的动态特性以及端址信息选择的随机程度,确保系统能够适应多变的环境并具备足够的安全性;环节二是数据传输时间测试,确认原型系统数据传输的可行性。这两项测试均在配置有Ubuntu操作系统和4 GB内存的硬件环境中执行,两台通信机、两台中继机的处理器均为Intel Core i5-4170,带宽为100 Mbit/s。

6.1.1 端址信息随机性测试

本节根据分析使用模式来检验动态随机性。实验对一台中继主机进行连续1 000次的数据包抓取操作,并随后对这些数据进行深入的统计分析。IP地址使用情况统计如图9所示。

从图9中可以看出,纵坐标上下浮动较小并保持基本稳定。可以得出以下结论:本文所设计的卫星互联网安全防御模型的地址跳变空间是均匀的且具备伪随机性的。

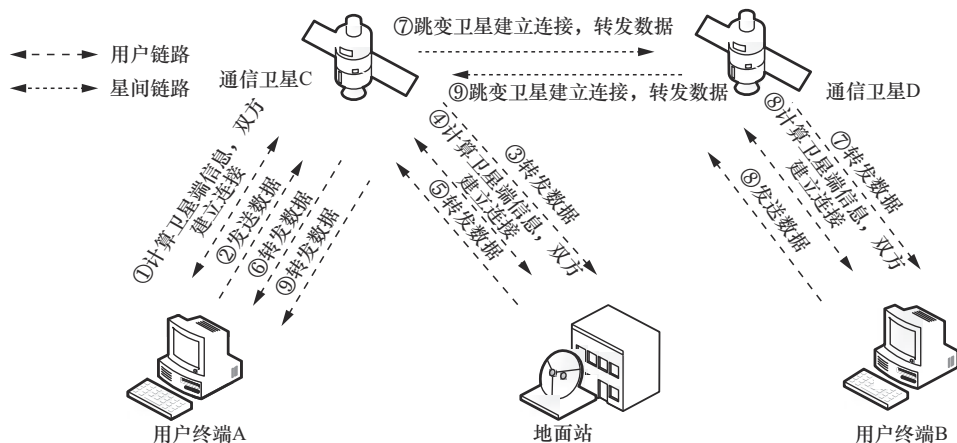


图8 系统通信流程

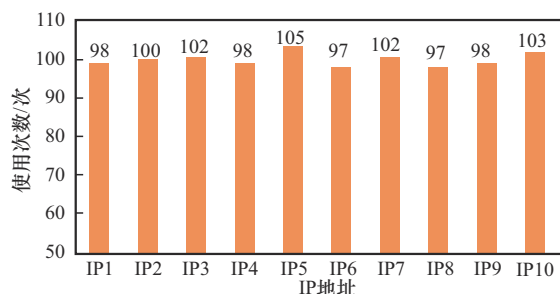


图9 IP地址使用情况统计

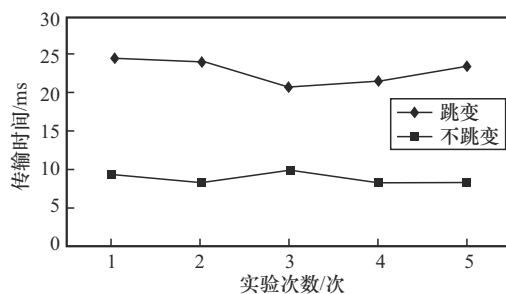


图11 时延比较结果

6.1.2 数据传输时间测试

本节实验设置情况与上节相同，通信机之间互发消息，执行的任务为20次消息互相的发送，详细记录了每次通信的耗时，并计算了平均值以便于分析。

传输时间比较结果如图10所示。在实验设置中，特意设定了30 ms的传输时延，并设置了每2 s发生一次的跳变频率。通过这一系列的实验设计，能够更加准确地评估端址信息跳变技术对通信时间的影响。

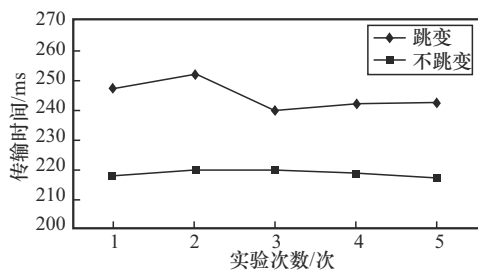


图10 传输时间比较结果

图10证明了原型系统能够很好地完成数据传输。

本文还设计了一项对比实验，目的是探究假设在无线条件下，对时间的影响，实验步骤和之前一样。

时延比较结果如图11所示，应用端址信息跳变技术所带来的时间开销相对较小。结果表明，在空间网络环境中，时延的增加主要是由空间网络本身固有的传输时延导致的。因此，经验证，端址信息跳变技术不增加显著时间开销，且能够有效地为卫星互联网中的通信提供安全保障。

综上所述，本文提出的系统的核心创新在于巧妙引入了基于端址信息跳变的移动目标防御技术，通过不断改变通信节点的端址信息，有效保障了数据传输过程中的安全性和可靠性。同时，经过深入分析与实验验证，发现端址信息跳变对传输时间的影响相对较小。因此，原型系统在实际应用中具备良好的可行性和实用性。

7 结束语

本文根据卫星互联网的特点，通过分析网络层面的移动目标防御技术，即端址跳变技术，并将其应用到卫星互联网防护中，构建了一个基于移动目标防御的空间网络安全防御系统模型，目前该模型仍有一些方面有待进一步完善和优化。

首先，实验是在模拟环境中进行的，结果存在偏差，为了克服此问题，在未来的研究中，可以考虑采用更加精确和复杂的模拟方法来逼近真实的空间网络环境。

其次，还可以进一步深入分析身份认证策略的实验结果，以验证其在空间网络环境中的有效性和可靠性。

最后，探索更加高效和优化的数据传输策略也是提升模型实用性和效能的重要途径，以期未来的空间网络安全提供更加坚实的保障。

参考文献

- [1] HE D J, LI X R, CHAN S, et al. Security analysis of a space-based wireless network[J]. IEEE Network, 2019, 33(1): 36-43.
- [2] 单超, 马少焯, 谷欣, 等. 卫星互联网应用与挑战[J]. 天地一体化信息网络, 2024, 5(3): 96-101.
- [3] SHAN C, MA S X, GU X, et al. Satellite Internet: application and development[J]. Space-Integrated-Ground Information Networks, 2024, 5(3): 96-101.
- [4] Space Exploration. SpaceX reveals 'Starshield' satellite project for national security use[R]. 2022.
- [5] 张睿健, 陈艺苑. 全球首颗太空网络安全测试卫星“月光者”影响分析[J]. 工业信息安全, 2023(5): 6-11.
- [6] ZHANG R J, CHEN Y Y. Analysis of the impact of world's first space cybersecurity test satellite moonlighter[J]. Industry Information Security, 2023(5): 6-11.
- [7] 邱涛, 张聚名. 基于5G技术的卫星空天地一体化网络安全研究[J]. 中国信息界, 2024(5): 35-36.
- [8] QIU T, ZHANG J M. Research on network security of satellite space-space integration based on 5G technology[J]. Information

- China, 2024(5): 35-36.
- [6] 雷依翰, 曹利峰, 韩孟达, 等. 软件定义天地一体化网络安全切换架构与方法[J]. 计算机与现代化, 2023(8): 119-126.
- LEI Y H, CAO L F, HAN M D, et al. Security handover architecture and method for software defined space-ground integration network[J]. Computer and Modernization, 2023(8): 119-126.
- [7] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for cyber threats[M]. New York: Springer, 2011.
- [8] 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.
- ZHOU Y Y, CHENG G, GUO C S, et al. Survey on attack surface dynamic transfer technology based on moving target defense[J]. Journal of Software, 2018, 29(9): 2799-2820.
- [9] 陈廷政. 面向主干网的DDoS攻击检测及防御方法研究[D]. 南京: 东南大学, 2022.
- CHEN Y Z. Research on detection and defense methods of DDoS attacks for backbone network [D]. Nanjing: Southeast University, 2022.
- [10] ROSENBERG J, SCHULZRINNE H, Camarillo. RFC3261, SIP: Session Initiation Protocol[Z]. 2002.
- [11] FISCHER D, AGUILAR S I, KOISSER D, et al. Making space-link security work: auxiliary services to enable the CCSDS space data-link security protocol[C]//Proceedings of the AIAA SPACE 2016. Virginia: AIAA, 2016.
- [12] MAPLE C, EPIPHANIOU G, HATHAL W, et al. The impact of message encryption on teleoperation for space applications[C]//Proceedings of the 2022 IEEE Aerospace Conference (AERO). Piscataway: IEEE Press, 2022: 1-10.
- [13] LIU J W, LIU W R, WU Q H, et al. Survey on key security technologies for space information networks[J]. Journal of Communications and Information Networks, 2016, 1(1): 72-85.
- [14] SHE C D, MA Y Q, WANG J C, et al. An improved malicious code intrusion detection method based on target tree for space information network[J]. International Journal of Distributed Sensor Networks, 2017, 13(12).
- [15] 景文强, 余波, 李昂阳, 等. 天地一体化信息网络主动防御安全体系研究[J]. 信息技术与网络安全, 2019, 38(8): 17-21.
- JING W Q, YU B, LI A Y, et al. Research on active defense security system of space-ground information network[J]. Information Technology and Network Security, 2019, 38(8): 17-21.
- [16] 李凤华, 郭云川, 耿魁, 等. 天地一体化信息网络安全动态赋能研究[J]. 无线电通信技术, 2020, 46(5): 561-570.
- LI F H, GUO Y C, GENG K, et al. Dynamically empowering security for space-terrestrial integrated information network[J]. Radio Communications Technology, 2020, 46(5): 561-570.
- [17] 张玲翠, 许瑶冰, 李凤华, 等. 天地一体化信息网络安全动态赋能架构[J]. 通信学报, 2021, 42(9): 87-95.
- ZHANG L C, XU Y B, LI F H, et al. Dynamic security-empowering architecture for space-ground integration information network[J]. Journal on Communications, 2021, 42(9): 87-95.
- [18] XU S S, LIU X D, MA M M, et al. An improved mutual authentication protocol based on perfect forward secrecy for satellite communications[J]. International Journal of Satellite Communications and Networking, 2020, 38(1): 62-73.

[作者简介]

徐瑞荣 (1976-), 女, 硕士, 主要研究方向为网络安全、数字通信和数字油田。