智能系统学报
CAAI TRANSACTIONS ON INTELLIGENT SYSTEMS

基于博弈论的预警卫星系统抗毁性研究

齐小刚，陈春绮，熊伟，刘立芳

引用本文:
齐小刚, 陈春绮, 熊伟, 等. 基于博弈论的预警卫星系统抗毁性研究[J]. 智能系统学报, 2021, 16(2): 338–345.
QI Xiaogang, CHEN Chunqi, XIONG Wei, et al. Research on the invulnerability of an early warning satellite system based on game theory[J]. *CAAI Transactions on Intelligent Systems*, 2021, 16(2): 338–345.

在线阅读 View online: https://dx.doi.org/10.11992/tis.202002017

DOI: 10.11992/tis.202002017
网络出版地址: https://kns.cnki.net/kcms/detail/23.1538.TP.20201115.1732.002.html

基于博弈论的预警卫星系统抗毁性研究

齐小刚[1], 陈春绮[1], 熊伟[2], 刘立芳[3]
（1. 西安电子科技大学 数学与统计学院, 陕西 西安 710071; 2. 航天工程大学 复杂电子系统仿真技术国防科技重点实验室, 北京 101416; 3. 西安电子科技大学 计算机学院, 陕西 西安 710071）

摘　要: 预警卫星系统在弹道导弹预警方面发挥着重要的作用, 一旦受到攻击, 将造成重大损失。针对这一实际情况, 利用博弈论知识, 将预警卫星系统的攻防过程构建为静态博弈模型。提出攻防状态下刻画系统抗毁性的方法, 将其分为防御者抗毁性和攻击者抗毁性, 在完全信息和不完全信息情况下, 分析双方应采取的策略, 用仿真得到的容量数据刻画节点受攻击后的失效概率, 提出基于仿真数据的攻防策略。并根据仿真数据分析提出不完全信息下模型的优化方向。

关键词: 预警卫星; 攻防博弈论; 博弈模型; 系统抗毁性; 防御者抗毁性; 攻击者抗毁性; 攻击策略; 防御策略
中图分类号: TP39; TJ861　　**文献标志码**: A　　**文章编号**: 1673−4785(2021)02−0338−08

中文引用格式: 齐小刚, 陈春绮, 熊伟, 等. 基于博弈论的预警卫星系统抗毁性研究 [J]. 智能系统学报, 2021, 16(2): 338–345.
英文引用格式: QI Xiaogang, CHEN Chunqi, XIONG Wei, et al. Research on the invulnerability of an early warning satellite system based on game theory[J]. CAAI transactions on intelligent systems, 2021, 16(2): 338–345.

Research on the invulnerability of an early warning satellite system based on game theory

QI Xiaogang[1], CHEN Chunqi[1], XIONG Wei[2], LIU Lifang[3]
(1. School of Mathematics and Statistics, Xidian University, Xi'an 710071, China; 2. Science and Technology on Complex Electronic System Simulation Laboratory, Space Engineering University, Beijing 101416, China; 3. School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: Satellite systems play an important role in the early warning of ballistic missile attacks, which may cause heavy losses. In view of this actual situation, using the knowledge of game theory, the attack and defense processes of the early warning satellite system are constructed as a static game model. A method is proposed to characterize the invulnerability of the system in the attack and defense states, and then it is divided into defender invulnerability and attacker indestructibility. In the case of complete information and incomplete information, the strategies that both sides should adopt are analyzed. The capacity data obtained from simulations is used to characterize the failure probability of the node under attack, and the attack and defense strategies are proposed based on the simulation data. The optimization direction of the model under incomplete information is proposed according to the analysis of simulation data.

Keywords: early warning satellite; attack and defense game theory; game model; system invulnerability; defender invulnerability; attacker invulnerability; attack strategy; defensive strategy

自 1957 年苏联成功发射第一颗人造地球卫星以来, 人类进入航天时代, 卫星被广泛应用于科学探测和研究、天气预报、通信、导航、军事等领域。预警卫星, 又称为导弹预警卫星, 是天基预警系统的核心组成部分, 主要利用星上红外探测器和可见光探测器, 探测导弹尾焰及弹体辐射, 跟踪、识别导弹从发射到助推段、自由段和再入段的过程, 测量来袭导弹的发射时间、发射地点、攻击目标、飞行方向等参数, 提供给地面拦截

收稿日期: 2020−02−25.　**网络出版日期**: 2020−11−16.
基金项目: 国家自然科学基金项目 (61877067); 装备领域基金项目 (61420100201162010002-2).
通信作者: 陈春绮. E-mail: 1098356554@qq.com.

和反击的各种信息, 取得预警时间[1]。

目前空间领域竞争不断加剧, 以卫星为主体的航天系统将是一体化全球感知、全球交战系统的核心, 以美、俄为代表的国家已经认识到卫星系统特别是预警卫星系统在军事活动中起到的重大作用[2], 在大力发展卫星的同时, 也投入大量的精力研究反卫星武器, 从这一方面来说, 在保护己方卫星提高抗毁性的同时, 利用反卫星武器来干扰、破坏乃至摧毁敌方预警卫星系统具有巨大的军事价值和战略意义。

因此, 对于预警系统信息网络来说, 攻击通常是不可避免的, 考虑受到攻击情况下的系统抗毁性有着重大意义。本文以天基红外系统 (space-based infrared system, SBIRS) 为主要研究对象, 基于博弈论, 区别于传统的系统抗毁性, 在攻击/防御框架下将系统抗毁性分为攻击者抗毁性和防御者抗毁性进行研究。

1　研究现状

1.1　天基红外系统 (SBIRS)

天基红外系统 (SBIRS) 是美国建造的逐步取代原有 DSP 卫星系统的下一代导弹预警和跟踪系统, 是由地球同步轨道卫星 (GEO)、低轨道卫星 (LEO) 以及大椭圆轨道卫星 (HEO) 组成的复合型星座。SBIRS 用来执行 4 项任务: 导弹预警、导弹防御、技术情报和作战空间特征描述[3], 是目前技术最先进的军事红外探测卫星, 大大增强了美国的全球导弹预警能力。

SBIRS 系统可分为 3 部分, 即高轨道部分 (SBIRS-high), 低轨道部分 (SBIRS-low) 和地面支持部分。

SBIRS-high 由 4 颗 GEO 和 2 颗 HEO 卫星构成, SBIRS-GEO 卫星主要用于探测和发现处于助推段的弹道导弹, SBIRS-HEO 主要任务在于对北极地区的探测预警, 将 SBIRS 的预警能力扩展到两极地区。SBIRS 最大的改进是采用了双探测器方案, 每颗卫星载有一台高速扫描型探测器和高分辨率凝视型探测器。卫星工作时, 扫描型探测器先对地球进行快速扫描, 然后将探测到的数据提供给凝视型探测器。紧接着, 凝视型探测器将目标画面拉近放大, 获取详细信息, 进而确定是否发生导弹发射活动。双探测器协调工作, 共同完成任务, 有效增强了 SBIRS 探测弹道导弹的能力[4]。

SBIRS-low 后更名为空间跟踪和监视系统 (STSS), 设想由分布于 3 个高度为 1 600 km 轨道的 24 颗卫星组成, 卫星之间利用 60 GHz 的星间链路传递弹道导弹飞行中段的跟踪信息, 提供立体的探测, 实现对弹道导弹和洲际导弹飞行全过程的持续跟踪。通过与 SBIRS-high 的配合, 为拦截导弹提供飞行轨迹及坐标。

地面支持部分由控制站、国外中继地面站、可移动终端及相关的通信设备组成。

1.2　抗毁性

关于抗毁性一直以来并没有形成统一的定义, 抗毁性注重的是系统的关键部分遭受到攻击或摧毁, 系统的恢复性和适应性, 并在此情况下仍能完成关键服务的能力[5]。

目前, 针对预警卫星的抗毁性研究甚少, 针对卫星网络的抗毁性研究也局限于拓扑结构、路由方案、容量优化及星座架构等方面[6-9]。但是卫星网络工作在极其复杂的空间环境中, 卫星节点之间的星间链路在任意时刻都可能发生随机故障, 甚至遭受蓄意攻击, 从而导致性能下降甚至完全损坏, 这一情况下的抗毁性很少受到关注。

2　攻防博弈论

2.1　网络攻防博弈论

博弈论 (game theory) 是研究具有斗争或竞争性质现象的数学理论和方法, 其实质是从对抗双方的角度出发, 考虑各自的预期行为和实际行为, 并研究它们的优化策略。博弈过程中, 参与对抗的双方都试图寻找使得自己利益最大化的最合理的策略。

博弈论作为一种在竞争对抗环境下博弈参与方策略选择的理论, 其与网络攻防行为所具有的目标对立性、非合作性以及策略依存性高度契合[10]。攻防双方选择各自的策略进行攻击与防御, 在实际的攻防博弈场景中, 防御者采取的防御策略和攻击者使用的攻击策略, 双方均无法确定, 例如防御者知道攻击者可能的几种攻击类型但无法确定, 造成了信息的不完全性, 攻防双方选取策略的过程可以看作不完全信息博弈过程。博弈图如图 1 所示。

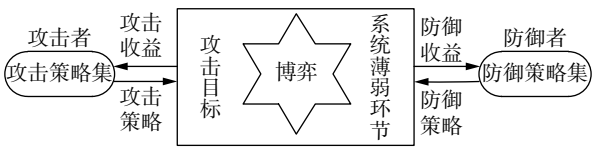


图 1　博弈图

Fig. 1　Game diagram

网络攻防对抗过程, 即是攻击方对网络系统中存在的脆弱性加以利用, 为达到某种损害网络

系统的目标而采取一系列的攻击行动；防御方针对网络系统的性能要求及所遭受的攻击而采取一系列的防御行动，整个对抗过程的实质就是博弈的过程[11]。在这一过程中，攻击者的收益即为目标网络的破坏程度，而防御者的收益为网络正常运行满足需求。网络攻防博弈过程与传统博弈过程的对应关系如图 2 所示。

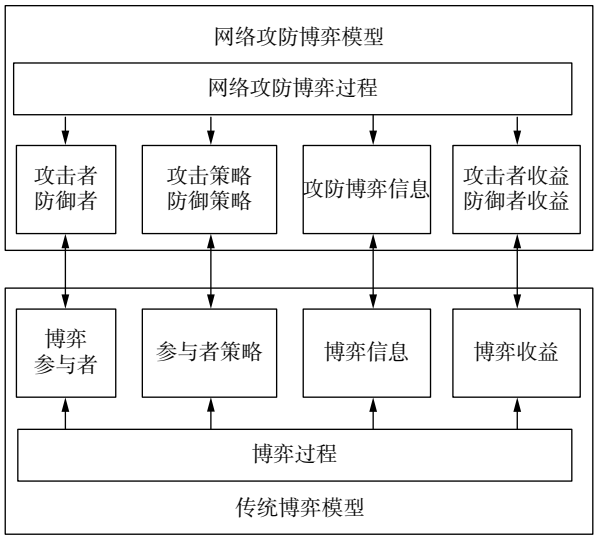


图 2　博弈要素对应关系

Fig. 2　Correspondence between game elements

2.2　预警卫星薄弱环节

卫星本身的一些特性使卫星比地面系统更容易遭受攻击，且难以修复。

1) 卫星轨道固定，易被探测。人造卫星是环绕地球在空间轨道上运行的无人航天器，一旦发射，只能沿着预定的轨道飞行，仅仅为躲避反卫星武器攻击做微小变动都很困难，变轨更是需要付出极大代价。同时，卫星最主要的特点就是覆盖面广，但也使得地面上很容易观测到卫星，通过雷达等探测仪器可以很轻易地获得卫星的轨道参数。尤其是低轨预警卫星，轨道高度仅为 1 600 km，一旦进入监视范围，会被立刻探测。因此，会受到反卫星及动能反卫星武器的攻击，被直接摧毁。

2) 在激光武器攻击下卫星的组件性能下降乃至失效。使用激光武器可以使得卫星的一些部件性能受损，当能量密度达到一定阈值时，能对卫星造成更迅速的破坏，导致卫星中高压容器破裂、摧毁太阳能电池板、破坏表面热控制材料、损毁卫星天线等。对于光电探测器，当照射激光超过最大负载值时，将发生饱和现象，无法正常工作，尤其是预警卫星搭载的探测器，为了探测到导弹尾焰，灵敏度极高，使得饱和所需的功率更低。

3) 上下行及星间链路实时性要求高，易受干扰。预警卫星在探测到导弹的相关参数后，通过下行链路传送给地面控制站，同时卫星也需要通过上行链路获取指挥信息。在卫星工作时，星上数据处理系统会接收到大量数据并进行预处理，为了确保预警信息的实时性，必须建立高效的通信链路。正常情况下，由于无线通信易受干扰，链路会采用编码、加密等技术来抵抗干扰与欺骗。但是，攻击者利用与实际信号相同的频率但功率较大的干扰信号来扰乱卫星通信，或者加大功率并模仿真实信号的特征，使得地面无法接受信息或接收到虚假信息，星间和星地间无法正常通信，从而影响预警性能。

4) 低轨卫星需要组网才能完成全球覆盖。SBIRS-low 轨道高度仅为 1 600 km，运行周期短。为了更好地全程持续跟踪导弹飞行，必须组网才能实现对全球的覆盖监视。SBIRS-low 协同工作，才能进行对导弹的监视跟踪，若对其中某些卫星实施攻击导致其失效，将会破坏整个系统的预警能力。

3　系统抗毁性

3.1　影响抗毁性的因素

系统的可靠性一般被认为是：在规定的条件下，系统在给定时间段内执行所需功能的概率。因此，在条件相同时，两个系统如果各方面均相同，则其有着相同的可靠性，即可靠性是静态的。抗毁性与其看似十分相似但却大有不同，抗毁性关注的是系统在受攻击后继续正常运行的概率，在攻击/防御框架下，这一概率会受到以下几个因素的影响：

1) 攻击者目标：干扰系统，完全禁用系统，对系统造成不可修复的最大损害等。

2) 攻击者资源：单次攻击或者可重复攻击，攻击所采用的技术手段等。

3) 攻击策略：系统禁用则停止攻击，攻击所有组件，攻击顺序等。

4) 防御者资源：第一次攻击后是否及时做出反应，拦截攻击的能力，虚假目标误导攻击等。

5) 防御策略：隐藏目标使攻击者无法接触，改变传输方式等。

3.2　抗毁性博弈模型

基于上述研究，在攻击/防御框架下，建立预警卫星的抗毁性问题博弈模型如下：

1) 参与者：预警卫星系统攻击者与防御者。①攻击者：攻击预警卫星系统，干扰、破坏和摧毁卫星节点，降低系统性能。如果预警系统无法完

成预警任务, 则认为攻击成功。②防御者: 保护预警卫星系统正常运行, 最小化系统失效概率, 完成既定的预警任务。

2) 攻击策略集: 攻击者选择攻击任意数量的卫星节点, 以及攻击顺序和攻击方式。

3) 防御策略集: 防御者采取最短路或者其他通信方式, 选择不同的预警模式。

4) 攻击者收益: 预警卫星系统被破坏的程度。

5) 防御者收益: 预警卫星系统维持正常的预警性能。

6) 攻击方式: 根据卫星受到攻击的实际情况, 将攻击方式分为两类: 一是直接摧毁, 卫星节点及相连的星间链路全部失效, 对应于卫星受到的硬杀伤攻击; 二是卫星受到干扰, 性能受到影响, 抽象为饱和攻击、篡改攻击、删除攻击, 对应于卫星受到的软杀伤攻击。

3.3　系统抗毁性

为了更好地从攻守双方刻画预警卫星系统抗毁性, 将其分为防御者抗毁性和攻击者抗毁性。定义如下:

定义 1　防御者抗毁性是系统在攻击下存活的概率。

定义 2　攻击者抗毁性是攻击失败的概率。

在 3.2 节博弈模型下, 防御者为提高自身收益, 会尽可能提升防御者抗毁性, 而攻击者为了最大可能禁用系统预警功能, 会选择合适的攻击策略, 提高攻击成功的概率, 降低攻击者抗毁性。

在完全信息的情况下, 防御者将采取最大化预警卫星系统预警能力的策略, 而攻击者也将针对这一策略进行攻击, 防御者抗毁性和攻击者抗毁性在这种情况下一致, 显然, 这是一种零和博弈, 其中防御者收益的任何增加都是以攻击者收益的减少为代价获得的, 反之亦然。因此, 防御者不会选择策略减少收益以使攻击者受益, 防御者没有动力在当前完全信息背景下采取误导攻击者的举动, 纳什均衡保持不变, 攻防双方坚持最佳策略。

但是预警卫星系统完全信息基本不可能实现, 在不完全信息的情况下, 防御者采取不同的通信方式使得最佳策略不同, 而攻击者不了解防御者策略, 双方均采取随机策略。此时防御者和攻击者的最佳收益不一致, 博弈被认为是不稳定的并且纳什均衡不适用。下面, 以 SBIRS-low 为例, 说明在不完全信息情况下, 攻防双方选择的策略, 以及防御者抗毁性和攻击者抗毁性的不同。

图 3 所示为 SBIRS-low 的网状拓扑结构, 3 条轨道, 每条轨道均匀分布 8 颗卫星, 协同工作完成预警任务。卫星暴露于外太空, 轨道及拓扑结构极易被攻击方获取, 但是防御方采取的通信策略则是保密的, 如路由算法、拥塞控制方案等, 在这种情况下, 可选择的攻防策略如下。

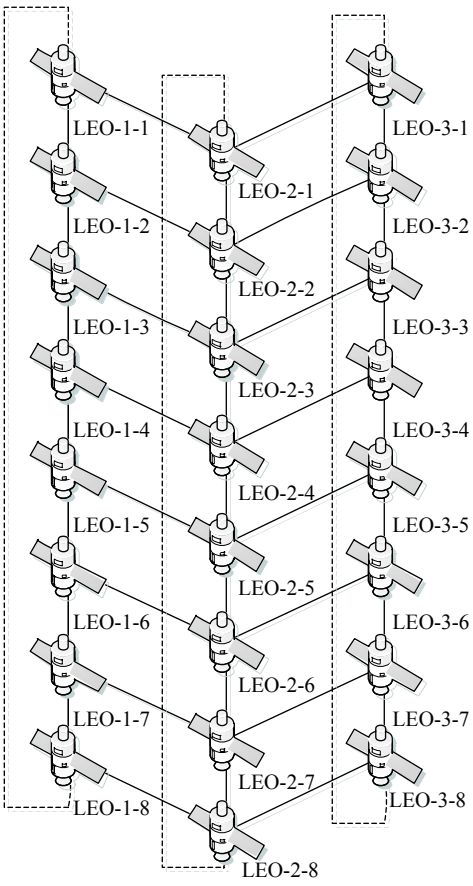


图 3　SBIRS-low 拓扑结构

Fig. 3　SBIRS-low topology

防御策略: 在博弈过程中, 防御方是率先做出决策的一方, 防御方所采取的通信方式和预警模式, 决定了每颗卫星在系统中的作用, 也就确定了其在受到攻击情况下失效的概率大小。防御者仍然选择最佳策略, 也就是使得攻击时系统失效概率最低的策略, 因为如果防御者网络的抗毁性降低, 将有利于攻击者, 与防御者的收益相矛盾。

此时防御者抗毁性与防御者选取的最佳策略有关。防御者在受到攻击后, 应该如何应对以提高自身抗毁性, 是后续动态博弈的主要研究内容。

攻击策略: 考虑到有非常多的候选防御策略, 保险起见, 攻击者应该攻击卫星网络的点割集, 一旦完全禁用该点割集, 无论防御者采取何种策略, 网络将无法连通, 攻击成功。虽然这可以被视为攻击者采用的保守方法, 但当攻击者目标为完全禁用卫星网络时, 可以认为这是充分现实的。因此, 攻击者应该做出最佳的攻击选择。换句话说, 攻击者应该以攻击成功的概率来定位点

割集，并依据攻击时可以继续操作的概率来确定攻击顺序。

在 SBIRS-low 中，为了确保卫星网络不连通，应该分别在每条轨道上选择不相邻的两个卫星节点进行攻击，从而使得网络不连通。目前暂不考虑由于极地的存在导致在高纬度区域，卫星轨道间链路不存在的情况。

设 p_{ij}(i 为轨道编号，j 为轨道内卫星编号) 表示卫星 LEO-i-j 受到攻击时失效的概率，则系统的攻击者抗毁性为 $P_a = 1 - p_{1j_1}p_{1j_2}p_{2j_3}p_{2j_4}p_{3j_5}p_{3j_6}$，攻击者应该选择使得 P_a 值最小卫星节点集合进行攻击。同时在攻击不同卫星节点成本一致的情况下，按照节点攻击成功概率从小到大的顺序进行攻击，一旦某一个节点的攻击失败，则本次攻击失败并停止攻击，攻击者应该重新选择攻击策略，这一问题属于动态博弈，本文暂不考虑。

此外，SBIRS 系统主要依靠高轨卫星来探测导弹的发射，因此在攻击时可以首先考虑攻击所在地区上空的 GEO 卫星，例如欧洲国家应选择首先攻击欧洲地区上空的 GEO 卫星。

4　性能测试与分析

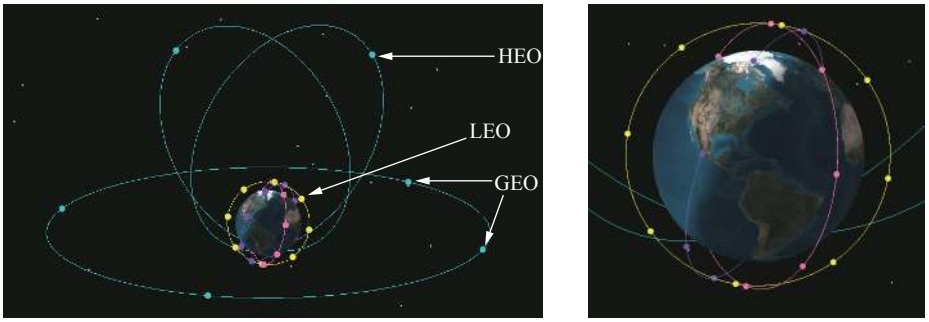
4.1　博弈策略分析

使用 STK 搭建 SBIRS 系统的轨道模型，相关参数如表 1 所示。图 4 展示了轨道模型的结果，图 4(a) 中展示了 SBIRS 系统 30 颗卫星的轨道模型，图 4(b) 是 SBIRS-low 的轨道模型，可以清楚地看到 3 个轨道面。在 OPNET 软件中导入 STK 生成的轨道模型，在全球范围内布置地面控制站。

表 1　SBIRS 轨道参数

Table 1　SBIRS orbital parameters

卫星	半长轴/km	轨道倾角	偏心率	近地点幅角/(°)
GEO卫星	42 164.2	0	0	0
HEO卫星	26 553.9	63.4	0.729 677	270
LEO卫星	7978.14	102.49	0	0



(a) SBIRS 轨道模型　　(b) SBIRS-low

图 4　轨道模型

Fig. 4　Track model

由于 SBIRS-low 卫星运行周期短，拓扑时变，采取时间片方法，认为在一定的时间内，拓扑固定。路由算法采取最短路算法。仿真运行得到节点容量，如表 2 所示。

表 2　卫星节点容量 (实验 1)

Table 2　Satellite node capacity (Experiment 1)

卫星编号	容量(数据包)/个	卫星编号	容量(数据包)/个	卫星编号	容量(数据包)/个
GEO-1	114 100	LEO-1-5	65 967	LEO-2-7	65 533
GEO-2	118 467	LEO-1-6	69 967	LEO-2-8	70 233
GEO-3	109 567	LEO-1-7	68 567	LEO-3-1	64 366
GEO-4	118 433	LEO-1-8	64 767	LEO-3-2	74 700
HEO-1	104 333	LEO-2-1	70 433	LEO-3-3	73 833
HEO-2	109 133	LEO-2-2	69 833	LEO-3-4	68 367
LEO-1-1	65 800	LEO-2-3	75 333	LEO-3-5	60 333
LEO-1-2	70 500	LEO-2-4	64 700	LEO-3-6	65 366
LEO-1-3	78 167	LEO-2-5	70 466	LEO-3-7	64 133
LEO-1-4	69 600	LEO-2-6	60 966	LEO-3-8	63 733

采用节点容量来刻画节点受到攻击时失效的概率, 节点容量越大, 受到攻击时更易造成拥塞和饱和现象, 失效的概率越大, 在系统中越重要。由表 2 中数据可知, SBIRS-high 中的 GEO 和 HEO 卫星承担着更加重要的作用, 其中 GEO 重要性更高。在 SBIRS-low 中, 由于卫星组网周期性运动, 重要程度差别不大, 但是仍然有着区别。轨道 1 中, LEO-1-2 和 LEO-1-3; 轨道 2 中, LEO-2-3 和 LEO-2-5; 轨道 3 中, LEO-3-2 和 LEO-3-3, 承载了更多的容量, 因此在受到攻击时更容易失效。

1) 如果完全信息情况下, 双方处于非合作博弈状态, 防御者采取最高效的路由方式传输数据, 而攻击者也根据该路由方式进行攻击。防御者不会降低自己的传输效率, 采取其余的路由方式来欺骗攻击者, 同时攻击者也不会选择攻击其余节点降低攻击成功的概率。

2) 在不完全信息情况下, 双方都将采取自身收益最大的策略, 无法达成纳什均衡。根据表 2 数据, 初步的攻防博弈策略如下:

防御者: 防御者应加强对 GEO 卫星的保护, 同时加大对 SBIRS-low 中承载容量更多节点的关注, 根据节点的组件性能以及在网络中的重要程度, 选择攻击下失效概率低的节点传输数据, 例如 LEO-1-8、LEO-2-6 和 LEO-3-5, 以提高系统防御者抗毁性。与此同时, 防御者可以采取迂回的路由方式, 改变节点受攻击时失效的概率, 设置虚假节点误导攻击者。

攻击者: 根据 3.3 节中描述, 在成本一致的情况下, 攻击者应该首先攻击 GEO 卫星。由于信息不完全, 攻击者无法得知防御者采取的路由方式, 因此只能选择使得 SBIRS-low 网络不连通的攻击策略。以实验 1 的数据来刻画失效概率, 应选择攻击节点 LEO-1-3、LEO-1-6、LEO-2-3、LEO-2-5、LEO-3-2 和 LEO-3-4 来断开 SBIRS-low 网络, 同时按照节点攻击成功概率从小到大的顺序进行攻击, 即最先攻击 LEO-3-4。其中为了满足不相邻节点, 轨道 1 和轨道 3 中的节点做了相应调整。攻击这些易于失效的节点, 攻击成功的概率变大, 使得攻击者抗毁性最小。

实验 1 的仿真时间较短, 得到的结果数据差异不显著, 实验 2 延长了仿真时间, 结果如表 3 所示。

表 3　卫星节点容量 (实验 2)

Table 3　Satellite node capacity (Experiment 2)

卫星编号	容量(数据包)/个	卫星编号	容量(数据包)/个	卫星编号	容量(数据包)/个
GEO-1	295 385	LEO-1-5	167 121	LEO-2-7	165 567
GEO-2	307 640	LEO-1-6	176 787	LEO-2-8	177 935
GEO-3	283 156	LEO-1-7	173 421	LEO-3-1	163 540
GEO-4	307 584	LEO-1-8	164 037	LEO-3-2	190 124
HEO-1	270 665	LEO-2-1	178 432	LEO-3-3	187 663
HEO-2	283 052	LEO-2-2	175 640	LEO-3-4	174 423
LEO-1-1	166 850	LEO-2-3	190 214	LEO-3-5	153 571
LEO-1-2	176 752	LEO-2-4	163 689	LEO-3-6	165 795
LEO-1-3	198 003	LEO-2-5	178 280	LEO-3-7	161 668
LEO-1-4	176 349	LEO-2-6	153 283	LEO-3-8	161 571

对比表 2、3 的数据, 可以发现, 在仿真时间增加后, GEO 和 HEO 承载的数据量明显区别于 LEO, 且 GEO-2 和 GEO-4 一直处于更加重要的位置。SBIRS-low 系统中差距显著, LEO-1-3 明显属于重要节点, 攻击时极易失效, 而 LEO-3-5 的失效概率则比较低。这些数据也进一步验证了上述提出的攻防策略。

4.2　模型分析

根据攻防对抗双方的攻击选择策略可以看出, 在非完全信息状态下存在 3 种博弈的收益:

1) 攻击方对于防御方 GEO、HEO 和 LEO 所构成的预警系统完全不知情, 因此在选择攻击位置时是完全随机的, 其收益为给防御方造成的损失在 3 种模式下的平均值。

根据实验 1 表 2 中 GEO、HEO 和 LEO 所有节点的容量 (数据包), 计算其平均值为 76 990。实验 2 表 3 中平均值为 196 273。

2) 攻击方对于防御方 GEO、HEO 和 LEO 所构成的预警系统而言, 其 GEO 和 HEO 的作用是部分知情的, 因此在选择攻击位置时不是完全随机的, 其收益为给防御方 GEO 和 HEO 造成的损失的平均值。

根据实验 1 表 2 中 GEO 和 HEO 节点的容量 (数据包), 计算其平均值为 112 339。实验 2 表 3 中平均值为 291 247。

3) 攻击方对于防御方 GEO、HEO 和 LEO 所构成的预警系统而言, 其 GEO 的作用是部分知情的, 因此在选择攻击位置时也不是完全随机的, 其收益为给防御方 GEO 造成的损失的平均值。

根据实验 1 表 2 中 GEO 节点的容量 (数据包), 计算其平均值为 115 142。实验 2 表 3 中平均值为 298 441。

进而, 可以获得 3 种模式下, 攻击者随机发起攻击造成防御方的损失最大值为第 3 种情形, 第 1 种情形最小。其中实验 1 为 115 142 和 76 990, 实验 2 为 298 441 和 196 273。

两种不完全信息下的网络攻击者对防御者攻击带来的攻击收益 (防御方损失) 的优化百分比计算如下: 实验 1 为 (115 142−76 990)/115 142= 33.13%, 实验 2 为 (298 441−196 273)/298 441= 34.23%。因此, 基于博弈论的网络抗毁性指标优化后, 可区别不同的不完全信息情况优化模型。

然而, 在攻击方对于防御方造成的攻击收益为防御方的数据损失量均值的计算方式也不完全符合实际的情况, 具体的损失还应该考虑攻击者的成本和实施难度。

5　结束语

本文针对预警卫星系统, 在攻击/防御框架下, 基于博弈论, 利用不完全信息静态博弈, 将 SBIRS 系统的抗毁性分为攻击者抗毁性和防御者抗毁性, 区别于传统仅对系统本身进行研究, 分别从攻击方和防御方对预警系统分析研究, 提出攻防状态下刻画系统抗毁性的方式, 并利用 OPNET 仿真平台模拟卫星工作状态, 用卫星节点的容量大小来刻画节点受攻击时干扰及失效概率, 提出了攻防双方的初步策略, 并分析了博弈模型, 可进行相应优化。但是攻击和防御并不是静止不变的, 双方都需要根据当前情况来修正自己的策略, 尤其是攻击者将根据已经攻击的结果结合攻击成本等来重新选择策略, 这将是一个动态博弈的过程, 如何准确的刻画这一过程, 并提出合理的攻防博弈策略是作者接下来的主要研究方向。

参考文献:

[1] 张东坡, 邵坤, 游敬云. 天基预警系统及其脆弱性分析 [J]. 通信对抗, 2017, 36(4): 34–36, 58.
ZHANG Dongpo, SHAO Kun, YOU Jingyun. Space-based early warning system and its vulnerability analysis[J]. Communication confrontation, 2017, 36(4): 34–36, 58.

[2] MAINI A K, AGRAWAL V. Satellite technology: principles and applications[M]. 2nd ed. Chichester: Wiley, 2011.

[3] LI Wenjie, YAN Shiqiang, WANG Chengliang, et al. SBIRS: missions, challenages and oppotunities[C]//Proceedings of 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis. Chengdu, China, 2019: 363−367.

[4] ANDREAS N S. Space-Based Infrared System (SBIRS) system of systems[C]//Proceedings of 1997 IEEE Aerospace Conference. Snowmass at Aspen, USA, 1997: 429−438.

[5] ELLISON R J, FISHER D A, LINGER R C, et al. Survivable network systems: an emerging discipline[R]. Pittsburgh: Carnegie Mellon University, 1997.

[6] 史春辉. 复杂网络拓扑结构抗毁性研究 [D]. 成都: 电子科技大学, 2012.
SHI Chunhui. Research on the invulnerability of complex network topology[D]. Chengdu: University of Electronic Science and Technology of China, 2012.

[7] 刘立芳, 吴丹, 郎晓光, 等. GEO/LEO 卫星网络的数据传输与抗毁性技术 [J]. 西安电子科技大学学报(自然科学版), 2018, 45(1): 1–5, 54.
LIU Lifang, WU Dan, LANG Xiaoguang, et al. Research on data transmission and survivability technology of the GEO/LEO satellite network[J]. Journal of Xidian University (natural science edition), 2018, 45(1): 1–5, 54.

[8] 王雅慧, 况鸿凤, 朱立东. 中轨卫星星座系统容量分析 [J]. 通信学报, 2017, 38(S1): 193–199.
WANG Yahui, KUANG Hongfeng, ZHU Lidong. Capacity analysis of the MEO satellite constellation[J]. Journal on communications, 2017, 38(S1): 193–199.

[9] 董飞鸿, 吕晶, 巩向武. 空间信息网络结构抗毁性优化设计 [J]. 通信学报, 2014, 35(10): 50–58.
DONG Feihong, LV Jing, GONG Xiangwu. Optimization design of structure invulnerability in space information net-

work[J]. Journal on communications, 2014, 35(10): 50–58.

[10] 王元卓, 于建业, 邱雯, 等. 网络群体行为的演化博弈模型与分析方法 [J]. 计算机学报, 2015, 38(2): 282–300.
WANG Yuanzhuo, YU Jianye, QIU Wen, et al. Evolutionary game model and analysis methods for network group behavior[J]. Chinese journal of computers, 2015, 38(2): 282–300.

[11] 刘妮, 周海平, 王波. 面向多种攻击的无线传感器网络攻防博弈模型 [J]. 计算机应用研究, 2020, 37(8): 2491–2495.
LIU Ni, ZHOU Haiping, WANG Bo. Attack and defense game model of wireless sensor networks facing multiple attacks[J]. Application research of computers, 2020, 37(8): 2491–2495.

作者简介:

齐小刚, 教授, 博士生导师, 主要研究方向为复杂系统建模与仿真、网络算法设计与应用。申请专利 47 项 (授权 19 项), 登记软件著作权 4 项。发表学术论文 100 余篇。

陈春绮, 硕士研究生, 主要研究方向为多层卫星网络建模与抗毁性。

生物信息学与智能信息处理 2021 年学术会议（BIIP2021）

由中国人工智能学会主办的 “生物信息学与智能信息处理 2021 年学术会议 (BIIP2021)” 将于 2021 年 5 月 21 日—23 日在湖北省武汉市召开。 2020 年是不平凡的一年, 武汉经受了新冠疫情的严峻考验, 中国向全球展示了中国速度和抗疫经验。 后疫情时代, 如何运用人工智能技术推动与人类健康相关的研究, 具有重要的现实意义。本次大会的主题: 人工智能+健康, 旨在为广大从事生物信息学、合成生物学、人工生命及其它与生命科学相关的智能信息处理研究的专家、学者和学生提供一个学术交流的平台, 推动人工智能与生命科学的深度融合, 促进我国生物信息学、合成生物学等学科的发展。本次会议将开设生物信息学教育论坛, 交流生物信息学人才培养、课程体系建设等方面的经验。

本次会议由中国人工智能学会主办, 中国人工智能学会生物信息学与人工生命专委会及华中农业大学信息学院承办, 并由湖北省农业大数据工程技术研究中心协办。会议将邀请信息科学和生命学科领域著名的国内外专家做大会特邀报告, 并分多个主题对相关领域的最新研究进展和动向进行大会报告、分会报告和张贴报告交流。

本次会议从即日起接收中英文摘要投稿 (截至日期 4 月 21 日), 经组委会评议和筛选, 符合要求的摘要将收录到会议摘要集, 优秀摘要的提交人将受邀做大会口头报告或海报展讲。接收两类论文的中英文摘要: (1) 已发表论文: 近三年在重要学术期刊上发表的研究成果; (2) 未发表论文: 尚未正式发表的原创性研究成果。 详细信息查看: 会议征文, 投稿模板下载: 摘要模板, 邮件中请注明已发表论文/未发表论文。投稿邮箱:biip2021@126.com。

会议简要日程安排

- 5 月 21 日 (周五): 下午报到, 晚上 19: 30 专委会会议
- 5 月 22 日 (周六): 上午主旨报告, 下午分会场报告, 晚宴
- 5 月 23 日 (周日): 上午主旨报告, 下午分会场报告 (4: 30 闭幕)