移动边缘计算网络下基于静态贝叶斯博弈的入侵响应策略研究

范伟[1,2]，彭诚[1,2]，朱大立[1,2]，王雨晴[1,2]
（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学网络空间安全学院，北京 100049）

摘 要：针对移动边缘计算环境下边缘节点资源受限、入侵过程难以被准确检测且缺乏有效应对外部入侵的入侵响应策略的问题，提出了一种适用于移动边缘计算环境的入侵检测网络结构，建立了基于静态贝叶斯博弈的入侵响应决策模型，模拟边缘节点与外部入侵者的网络交互行为，并对博弈过程中攻击者和防御者选择不同行为的概率进行了预测。入侵响应决策模型综合考虑系统资源、响应成本以及检测率、误报率和漏报率等因素，在兼顾入侵检测系统资源消耗及边缘节点隐私保护的基础上，对入侵检测系统的响应决策进行优化。实验分析了影响入侵响应决策的因素，为具体应用提供了实验依据。

关键词：移动边缘计算；静态贝叶斯博弈；贝叶斯纳什均衡
中图分类号：TP309
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023040

Research on intrusion response strategy based on static Bayesian game in mobile edge computing network

FAN Wei[1,2], PENG Cheng[1,2], ZHU Dali[1,2], WANG Yuqing[1,2]
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: In the mobile edge computing (MEC) environment, the resources of edge nodes are limited. It is difficult to detect the intrusion process accurately, and there is no effective intrusion response strategy to deal with external intrusions. An intrusion detection network structure suitable for mobile edge computing environment was proposed and an intrusion response decision model based on static Bayesian game was established to simulate the network interaction behavior between edge nodes and external intruders. The probability of attackers and defenders in the game process was predicted respectively. The influence of the system resource, the cost of intrusion response, the detection rate and false alarm rate were considered comprehensively by the intrusion response decision model. The response decision of the intrusion detection system was optimized on the basis of the considering both resource consumption of the intrusion detection and the privacy protection of the edge nodes. The factors that affected the decision-making of intrusion response were analyzed, and the experimental basis for the specific application was provided.

Keywords: mobile edge computing, static Bayesian game, Bayesian-Nash equilibrium

0 引言

近年来，5G 移动网络技术日渐成熟，网络设备智能化程度不断加深，网络中用户设备的数量和设备产生的数据量呈几何式增长，以云计算[1]为核心的集中式服务模式逐渐难以满足终端智能化和海量数据实时处理的需求，移动边缘计算（MEC, mobile edge computing）[2]应运而生。其具有如图 1 所示的基于“云–边–端”的三层分布式体系架构[3]。其中，“端”指终端层，既是数据的消费者又是数据的生产者，包括传感器、个人计算机、车辆等各类移动和固定的终端设备，负责与用户直接交互或

收稿日期：2022–10–22；**修回日期：**2023–01–10
基金项目：国家重点研发计划基金资助项目（No.2019YFB1005204）
Foundation Item: The National Key Research and Development Program of China (No.2019YFB1005204)

收集各类原始数据并报告给边缘计算层。“边”指边缘计算层，位于靠近数据源头的网络边缘，由众多边缘节点构成，负责接收、存储和计算终端层上传的数据并有选择地交付给云计算层。“云”指云计算层，位于网络的中心，是距离终端层最远的一层，能够为整个网络提供更强的计算分析能力、更多的计算资源和全局分析服务。

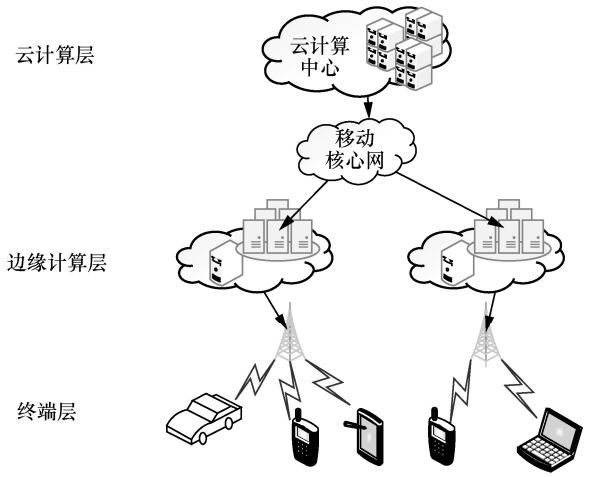

图 1　MEC 基于“云–边–端”的三层分布式体系架构

MEC 通过将计算与存储资源迁移到网络边缘，使计算任务可以在靠近数据源头的边缘节点运行，有效地减小了数据的传输时延和带宽，缓解了云计算中心的压力，使实时性和时延敏感型应用得以更好地实现，但也带来了新的安全挑战。以拒绝服务（DoS, denial of service）攻击为例，云计算中心的 DoS 攻击较集中，且一般的 DoS 攻击难以攻破。而在移动边缘计算架构下，攻击主要是针对分布式的边缘节点进行的，由于其计算和存储资源相对较少，当攻击强度增大时，节点被攻陷的可能性极大。因此，与云计算中的攻击相比，针对移动边缘计算的攻击可通过提高攻击强度来获得成功。

移动边缘计算所面临的安全问题与云计算大同小异，主要是结构上的差异。一方面，边缘节点通常部署在距离终端用户较近的网络边缘，地理分布广泛且网络环境复杂，容易遭到恶意攻击者的攻击威胁；另一方面，在移动边缘计算环境下，由于设备结构、协议、服务提供商的不同，导致发生在边缘节点上的攻击过程难以被准确地检测[4]。此外，传统的入侵检测系统通常很少考虑系统资源状态的影响，可能出现系统响应攻击的损失大于真实攻击引起的损失的情况，无法适用于计算和存储资源有限的边缘节点。因此，需要引入一种新的入侵响应决策模型，使边缘节点能够有效地应对入侵者的入侵行为。

由于 MEC 模式兴起的时间不长，目前，MEC 入侵检测的研究不多，可分为基于边缘智能和其他方法两大类。基于边缘智能的方法主要包括基于机器学习[5]和基于深度学习[6]2 种，其他方法则包括基于博弈论、基于生物免疫原理等方法。

在基于机器学习的入侵检测方法研究中，主要采用随机森林、XGBoost、高斯朴素贝叶斯、k 近邻（KNN, k-nearest neighbor）等算法。Lee 等[7]考虑边缘节点计算资源受限的缺点，提出在边缘节点部署一种基于稀疏自编码器和支持向量机的轻量级入侵检测系统（IDS, intrusion detection system），实验结果表明，该 IDS 可以获得 98.22%的准确度。李忠成等[8]根据边缘计算网络开放、异构和资源受限的特点，设计通用的边缘计算 IDS，并提出一种基于改进的训练样本筛选–极限学习机（TSS-ELM）的边缘计算入侵检测算法。相较于其他算法，该算法具有更优的准确性、时间依赖性、稳健性和误报率。基于机器学习的入侵检测方法具有训练和检测时间短、所需内存等资源较少的优点，但可构造的特征有限、检测率和准确率较低、缺乏可拓展性和稳健性。

在基于深度学习的入侵检测方法研究中，主要采用卷积神经网络（CNN）、循环神经网络（RNN）、长短期记忆网络（LSTM）等算法。由于深度学习算法的网络结构复杂、参数众多、训练需要海量的数据以及大量的计算和内存资源，需要设计轻量级的深度学习算法或将传统的深度学习算法进行轻量化才能应用于边缘计算环境。Sudqi 等[9]提出一种基于多层感知机模型向量空间表示形式的轻量级 IDS，以解决边缘设备资源受限且容易遭受安全攻击的问题，该方法相比于同类入侵检测算法有更高的检测率和更低的计算复杂度。Souza 等[10]提出了一种可以在网络边缘运行的入侵检测架构，它采用基于深度神经网络（DNN, deep neural network）和 KNN 的混合二元分类方法将事件分类为攻击和非攻击 2 种，可应用多种机器学习方法对分类为攻击的事件进行检测，实验结果表明，该方法能够在经典机器学习方法中实现较高的精确度，并在内存和处理成本方面具有较低的开销。

基于深度学习的入侵检测方法可以获得较高的检测率，但训练过程复杂、训练速度较低且需要强大的计算资源。

在基于博弈论的入侵检测方法研究中，研究目的不是求得对某种具体入侵行为的防御措施，而是寻求一种针对多种入侵行为的通用防御机制[11]，以有效地对非法入侵者及入侵检测系统之间的攻击与检测过程进行预测和分析[12]。An 等[13]将边缘网络中的攻击防御视作动态博弈过程，运用基于微分博弈论的入侵检测方法对边缘网络的入侵过程进行模拟，研究边缘节点的最优入侵策略及对应的最优响应策略。苗莉[14]利用平均场博弈和随机微分博弈等数学理论，在考虑边缘节点资源有限特征和恶意节点的攻击强度的基础上，对边缘计算环境下边缘用户数据、边缘节点和边缘网络的安全防御等问题进行了研究。基于博弈论的入侵检测方法采用不同的视角看待安全，即安全不是没有威胁，而是攻击系统比不攻击系统更加昂贵。相较于单纯对防御资源配置优化，它具有明显的优势：一是明确了模型中攻防双方行为的影响，而简单的优化公式只关注防御资源的优化，不考虑攻击者；二是博弈论具有内在的多玩家属性，不仅为防御算法的开发提供了基础，而且可以用来预测攻击者的行为[15]。

本文基于博弈论的入侵检测方法提出一种基于静态贝叶斯博弈的 MEC 入侵响应决策模型。该模型可以对边缘节点的网络行为进行分析和预测，使 MEC 系统在最小化节点资源消耗的前提下最大化抑制入侵者的入侵行为。本文的主要研究内容如下。

1) 将网络攻防过程映射到博弈过程中，建立基于静态贝叶斯博弈的 MEC 入侵响应决策模型，并通过求解模型的贝叶斯纳什均衡，确定攻防双方的最优响应策略。

2) 针对 MEC 实时性和可靠性要求高及边缘节点的能量与计算、存储、网络等资源受限的特点，考虑多种因素对攻防双方策略选取的影响，包括防御节点的资源、损失代价、防御成本，恶意节点的攻击类型、攻击成本以及防御系统的检测率和漏报率等，针对不同的安全目标采取不同的防御措施，使 MEC 系统在面临外部攻击时可以实现入侵损害与防御成本之间的平衡。

3) 设计模型算法并进行数值分析。实验结果证明了模型的有效性，可以对攻击者和防御者的策略选择进行理性的预测，并抑制恶意节点的攻击行为。

1　模型设计与形式化描述

本文基于图 1 提出一种与传统模式不同的入侵响应决策模型，如图 2 所示。在所有的边缘节点中部署入侵检测代理，主要负责收集监测数据，而入侵检测这项耗费大量计算和能量资源的工作则由云计算中心完成。需要注意的是，不是所有监测到的行为数据都要提交到云计算中心，只有被入侵响应决策模型确定为采取检测策略的边缘节点上的入侵检测代理才会被触发并上传数据。

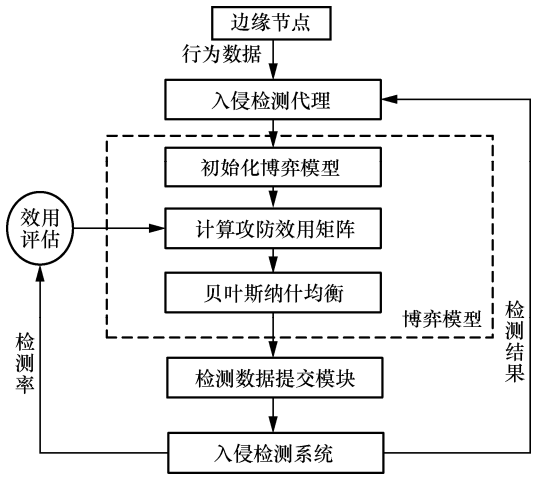

图 2　入侵响应决策模型

边缘节点上的入侵检测代理在收集到监测数据后，面临是否将监测数据提交至云计算中心并启动入侵检测系统的问题。一方面，入侵检测代理只有提交监测数据才可能检测到恶意攻击者的攻击威胁；另一方面，入侵检测代理在提交监测数据时将消耗用于数据发送的能量和带宽，同时泄露包含在监测数据中的隐私数据（如边缘节点的位置信息等）。因此，需要建立 MEC 入侵检测系统的最优响应决策模型，以在考虑 MEC 系统入侵检测代理监测数据发送能耗和带宽等资源及边缘计算节点隐私保护因素的基础上，最优化入侵检测系统的响应决策。

1.1　模型设计

边缘节点包括恶意节点与防御节点。恶意节点的目的是破坏 MEC 网络的安全，使边缘节点彻底瘫痪，而防御节点可以利用入侵检测系统对接收的信息进行检测。恶意节点为了掩饰自己的攻击行为也会给防御节点发送正常信息。防御节点对收到的信息进行检测需要消耗一定的能量，由于边缘节点的资源和能量有限，如果防御节点对收到的所有信

息都进行检测，则很快会因能量耗尽而无法工作。因此，防御节点在决定是否进行检测时需要综合考虑其付出的能耗代价及被攻击的可能性，即恶意节点和防御节点的攻防行为其实就是一个博弈过程，攻防双方会在分析博弈局势的基础上采取对自己最有利的策略。因此，本节用博弈论的方法对攻防双方的策略进行分析。

定义 1　MEC 入侵响应决策模型。在考虑 MEC 入侵检测代理监测数据发送能耗和边缘节点隐私保护的基础上，将 MEC 入侵响应决策模型表示为一个五元组[16] $G=(N,\theta,P,S,U)$，其含义如下。

1) $N=\{i,j\}$ 是博弈参与人的集合。其中，参与人 i 代表可能会对其他节点或设备发动攻击的边缘节点或终端设备，参与人 j 代表部署了入侵检测代理的边缘节点。

2) $\theta=\{\theta_i,\theta_j\}$ 是博弈参与人的类型空间。在博弈过程中，恶意节点 i 和防御节点 j 无法确定对方的策略收益，但可以将策略收益的不确定性转换为类型的不确定性，并通过概率分布对对方的类型进行判断。MEC 网络中可能既存在正常类型的边缘节点也存在恶意类型的边缘节点，因此假设 $\theta_i=\{\theta_i^m,\theta_i^n\}$ 是边缘节点 i 的类型空间，分为正常类型 θ_i^n 和恶意类型 θ_i^m。恶意类型的边缘节点 i 可能选择不攻击策略以混淆防御节点 j 的判断，而其最终目的是选择攻击策略以破坏 MEC 网络的安全，使边缘节点彻底瘫痪；而正常类型的边缘节点 i 不会发动攻击，可用于感知信息、转发数据等。$\theta_j=\{\theta_j^n\}$ 是部署了入侵检测代理的边缘节点 j 的类型空间，可以选择检测策略将监测数据提交到云计算中心进行入侵检测，也可能因为考虑资源消耗和隐私保护的需要选择不检测策略。由于恶意节点的伪装以及无线信道噪声的影响，入侵检测系统在检测前无法确定节点 i 的类型是正常还是恶意，而防御节点 j 是已知的。按博弈论的说法，其身份信息对入侵检测系统的防御节点 j 而言属于私有信息，而防御节点 j 的类型对参与人双方而言是公共信息。

3) 信念 $P=\{p_j(\theta_i^m),p_j(\theta_i^n),p_i(\theta_j^n)\}$ 是恶意节点、正常节点与防御节点在博弈过程中对对方所属类型的估计。其中，$p_j(\theta_i^m)$ 和 $p_j(\theta_i^n)$ 分别表示防御节点 j 认为节点 i 是恶意节点和正常节点的概率，$p_j(\theta_i^n)=1-p_j(\theta_i^m)$；$p_i(\theta_j^n)$ 表示节点 i 认为防御节点 j 是正常节点的先验概率，由于防御节点 j 对节点 i 是已知信息，且部署了入侵检测代理的边缘节点 j 只有一种类型，因此 $p_i(\theta_j^n)=1$。

4) 策略空间 $S=\{S_i,S_j\}$ 是参与人在博弈过程中可以选择的策略。其中，$S_i(\theta_i^m)=\{\text{Attack, NotAttack}\}$ 表示恶意节点 i 有 2 个可选策略——攻击和不攻击；$S_i(\theta_i^n)=\{\text{NotAttack}\}$ 表示正常节点 i 有一个可选策略——不攻击；$S_j(\theta_j^n)=\{\text{Monitor, NotMonitor}\}$ 表示防御节点 j 有 2 个可选策略——防御和不防御。

5) 效用函数 $U=\{u_i,u_j\}$ 是参与人在博弈时可以获得的收益，由参与人类型和其选择的策略决定。其中，u_i 表示节点 i 在策略集 S_i 对应策略下进行博弈可得的收益，u_j 表示节点 j 在策略集 S_j 对应策略下进行博弈可得的收益。

在 MEC 网络中，节点 i 与节点 j 的效用函数与多方面的因素有关，如防御节点 j 的资源、损失代价、防御成本，恶意节点 i 的攻击收益、攻击成本以及入侵检测系统的检测率和误测率等。表 1 列出了参数及其含义，所有参数均为正值[17-19]。其中，防御节点 j 守护的资源的总价值为 ω，它包括节点的能量、网络带宽、存储和计算资源以及安全相关的因素。在假设不存在节点因自私而争用网络资源的情况下，MEC 入侵响应决策模型可以看作零和博弈，即恶意节点 i 发动攻击成功后，防御节点 j 的损失与恶意节点 i 的收益相同，均为 ω。此外，由于现有的入侵检测技术无法完全准确地区分系统的正常行为和攻击行为，导致不可避免地存在漏报和误报现象，因此将存在漏报和误报的概率定义为误测率 β。当节点 i 进行攻击时，入侵检测系统会以 α 的概率发出正确警报；当节点 j 没有受到攻击时，入侵检测系统会以 β 的概率发出错误警报。

表 1　　**参数及其含义**

参数	含义
α	入侵检测系统的检测率
β	入侵检测系统的误测率
c_a	节点 i 发动攻击的成本
c_d	防御节点 j 防御攻击的成本
b_n	网络正常运行时，防御节点 j 的收益
b_a	入侵检测系统检测到攻击时，恶意节点 i 受到的惩罚
b_d	入侵检测系统检测到攻击时，防御节点 j 的收益
ω	入侵检测系统未检测到攻击时，恶意节点 i 的收益及防御节点 j 的损失

边缘节点 i 和部署了入侵检测代理的边缘节点 j 在进行博弈时共有 6 组策略。对于策略组合 $\left\{S_i\left(\theta_i^m\right)=\text{Attack}, S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$，恶意节点 i 对部署了入侵检测代理的边缘节点 j 发动攻击，边缘节点 j 将收集到的监测数据提交至云计算中心并由云计算中心进行入侵检测。此时，防御节点 j 的收益等于检测到攻击时防御节点 j 的收益 αb_d 减去防御攻击的成本 c_d，还需减去未检测到攻击时防御节点的损失 $(1-\alpha)\omega$，因此防御节点 j 的收益为 $\alpha b_d-c_d-(1-\alpha)\omega$；恶意节点 i 的收益等于攻击未被检测到时恶意节点的收益 $(1-\alpha)\omega$ 减去攻击的成本 c_a，再减去攻击被检测到时恶意节点受到的惩罚 αb_a，因此恶意节点 i 的收益为 $(1-\alpha)\omega-c_a-\alpha b_a$。对于策略组合 $\left\{S_i\left(\theta_i^m\right)=\text{Attack}, S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$，恶意节点 i 对部署了入侵检测代理的边缘节点 j 发动攻击，边缘节点 j 不提交监测数据启动入侵检测。此时，防御节点 j 的收益等于攻击成功时防御节点 j 的损失，即 $-\omega$；恶意节点 i 的收益等于入侵成功的收益 ω 减去发动攻击的成本 c_a，即 $\omega-c_a$。对于策略组合 $\left\{S_i\left(\theta_i^m\right)=\text{NotAttack},\ \ S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 和 $\left\{S_i\left(\theta_i^m\right)=\text{NotAttack}, S_j\left(\theta_j^n\right)=\ \text{NotMonitor}\right\}$，虽然边缘节点 i 是恶意节点，但均采取不攻击的策略，所以 2 种策略组合下恶意节点 i 的收益均为 0。当防御节点 j 选择将监测数据提交并启动入侵检测时，节点 j 的收益包括防御的成本和因误测而导致的损失，即 $-\beta b_d-c_d$；当防御节点 j 不将监测数据提交时，节点 j 的收益等于边缘节点进行正常网络活动的收益 b_n。对于策略组合 $\left\{S_i\left(\theta_i^n\right)=\text{NotAttack}, S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 和 $\left\{S_i\left(\theta_i^n\right)=\ \text{NotAttack}, S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$，正常节点 i 只有不攻击一个可选策略，因此节点 i 的攻击收益总为 0。当防御节点 j 选择将监测数据提交并启动入侵检测时，其收益为 $-\beta b_d-c_d$；当防御节点 j 不将监测数据提交时，其收益为 b_n。

边缘节点 i 和部署了 MEC 入侵检测代理的防御节点 j 进行博弈的攻防效用矩阵如表 2 所示。效用表示部分（*, *）中，逗号左边代表节点 i 在相应攻防策略下的收益，逗号右边代表防御节点 j 在相应攻防策略下的收益。

表 2　　攻防效用矩阵

节点 i 类型	节点 i 策略	收益	
		节点 j 选择 Monitor	节点 j 选择 NotMonitor
恶意	Attack	$((1-\alpha)\omega-c_a-\alpha b_a,\ \alpha b_d-(1-\alpha)\omega-c_d)$	$(\omega-c_a,\ -\omega)$
恶意	NotAttack	$(0,\ -\beta b_d-c_d)$	$(0,\ b_n)$
正常	NotAttack	$(0,\ -\beta b_d-c_d)$	$(0,\ b_n)$

博弈过程中，防御节点 j 知道自己所属的类型 θ_j，但不知道节点 i 的类型 θ_i。为了表现这种不确定性，使用 Harsanyi 转换引入一个虚拟的参与人——自然（N, Nature），由 N 首先采取行动，决定边缘节点 i 的类型[20-21]。节点 i 和节点 j 对 N 的行动拥有一个共同信念：N 以概率 μ（$0\leqslant\mu\leqslant1$）确定节点 i 的类型为恶意类型，以概率 $1-\mu$ 确定节点 i 的类型为正常类型，接着节点 i 和节点 j 开始行动，节点 i 首先选择是否采取攻击策略，然后防御节点 j 选择是否采取防御的策略。图 3 所示的贝叶斯博弈树详细地描述了这个过程。

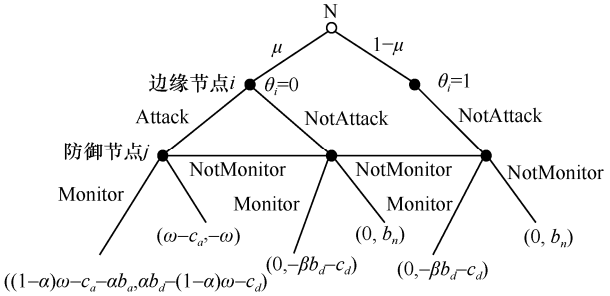

图 3　贝叶斯博弈树

1.2　贝叶斯纳什均衡分析

1.1 节给出的 MEC 入侵响应决策模型属于静态贝叶斯博弈类型，对应的均衡概念称为贝叶斯纳什均衡，它是纳什均衡概念在静态贝叶斯博弈（又称不完全信息静态博弈）上的扩展，最大的特点是参与人可以在不确定其他参与人类型的情况下得出博弈的最优策略。

定义 2　混合策略贝叶斯纳什均衡。在给定的 MEC 入侵响应决策模型 $G=(N, \theta, A, P, U)$ 中，边缘节点 i 的混合策略概率分布为 $p_i=\left\{p_i\left(\theta_j^n\right)\right\}$，边缘节点 j 的混合策略概率分布为 $p_j=\left\{p_j\left(\theta_i^m\right), p_j\left(\theta_i^n\right)\right\}$。混合策略 $\left(p_i, p_j\right)$ 为贝叶斯纳什均衡，当且仅当对 $\forall s_i\in S_i\left(\theta_i\right)$ 和 $\forall s_j\in S_j\left(\theta_j\right)$ 都满足

$$s_i^*(\theta_i)\in\arg\max\sum_{S_i}p_i(\theta_{-i}\mid\theta_i)u_i(s_i,s_{-i}^*,\theta_i,\theta_{-i}) \quad (1)$$

$$s_j^*(\theta_j)\in\arg\max\sum_{S_j}p_j(\theta_{-j}\mid\theta_j)u_j(s_j,s_{-j}^*,\theta_j,\theta_{-j}) \quad (2)$$

MEC 入侵响应决策模型中，恶意节点 i 与防御节点 j 的类型有限，且每种类型下攻防双方的行动组合也是有限的，即此博弈模型是一种有限的策略博弈。因此，根据纳什均衡的存在性定理[22]，在每个有限的策略博弈至少存在一个纯策略或混合策略纳什均衡。由于纯策略可以看作混合策略的特殊情况，则 MEC 入侵响应决策模型必然存在一个混合策略的贝叶斯纳什均衡。由混合策略贝叶斯纳什均衡的定义可知，在纳什均衡状态下存在一组混合策略或策略组合，相比其他策略，攻防双方的收益最大。在不清楚对方策略的情况下，攻防双方都倾向于选择这一组策略或策略组合，以使己方的收益最大，即通过对混合策略贝叶斯纳什均衡进行求解一定能够得到最优入侵响应策略。下面对 1.1 节给出的静态贝叶斯博弈模型的贝叶斯纳什均衡进行求解。

当边缘节点 i 选择纯策略 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack}\right\}$ 时，防御节点 j 选择纯策略 $\left\{S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 的期望效用为

$$\begin{aligned}&\text{Eu}_j(\text{Monitor})=\\&\mu\left[\alpha b_d-(1-\alpha)\omega-c_d\right]-(1-\mu)(\beta b_d+c_d)\end{aligned} \quad (3)$$

防御节点 j 选择纯策略 $\left\{S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$ 的期望效用为

$$\text{Eu}_j(\text{NotMonitor})=-\mu\omega+(1-\mu)b_n \quad (4)$$

因此，当满足 $\text{Eu}_j(\text{Monitor})>\text{Eu}_j(\text{NotMonitor})$，即 $\mu>\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}$ 时，防御节点 j 的最优策略是 $\left\{S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$。然而，当防御节点 j 选择策略 $\left\{S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 时，节点 i 的最优策略是 $\left\{S_i\left(\theta_i^m\right)=\text{NotAttack},\ S_i\left(\theta_i^n\right)=\text{NotAttack}\right\}$，而不是 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack}\right\}$。因此，$\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack},\ S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 不是 MEC 入侵响应决策模型的纯策略纳什均衡。

同理，当 $\text{Eu}_j(\text{Monitor})<\text{Eu}_j(\text{NotMonitor})$，即 $\mu<\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}$ 时，防御节点 j 的最优策略是 $\left\{S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$。此时，节点 i 的最优策略是 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack}\right\}$，与假设一致。因此，$\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)\text{NotAttack},\ S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$ 是 MEC 入侵响应决策模型的纯策略贝叶斯纳什均衡。

当边缘节点 i 选择策略 $\left\{S_i\left(\theta_i^m\right)=\text{NotAttack},\ S_i\left(\theta_i^n\right)=\text{NotAttack}\right\}$ 时，防御节点 j 选择纯策略 $\left\{S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 的期望效用为

$$\begin{aligned}&\text{Eu}_j(\text{Monitor})=-\mu(\beta b_d+c_d)-(1-\mu)(\beta b_d+c_d)=\\&-\beta b_d-c_d<0\end{aligned} \quad (5)$$

防御节点 j 选择纯策略 $\left\{S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$ 的期望效用为

$$\text{Eu}_j(\text{NotMonitor})=b_n>0 \quad (6)$$

此时，$\text{Eu}_j(\text{NotMonitor})$ 恒大于 $\text{Eu}_j(\text{Monitor})$，防御节点 j 的最优策略为 $\left\{S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$。然而，当防御节点 j 选择策略 $\left\{S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$ 时，节点 i 的最优策略是 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack}\right\}$。因此，$\left\{S_i\left(\theta_i^m\right)=\text{NotAttack},\ S_i\left(\theta_i^n\right)=\text{NotAttack},S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$ 和 $\left\{S_i\left(\theta_i^m\right)=\text{NotAttack},\ S_i\left(\theta_i^n\right)=\text{NotAttack},\ S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 都不是 MEC 入侵响应决策模型的纯策略贝叶斯纳什均衡。

综上，当 $\mu<\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}$ 时，此移动边缘计算入侵响应决策模型仅存在一个纯策略的贝叶斯纳什均衡；当 $\mu>\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}$ 时，此移动边缘计算入侵响应决策模型不存在任何纯策略的贝叶斯纳什均衡。

下面，求解 MEC 入侵响应决策模型的混合策略贝叶斯纳什均衡。假设恶意类型的节点 i 以概率 p 选择攻击策略，以概率 $1–p$ 选择不攻击策略，防御节点 j 以概率 q 选择检测策略，以概率 $1–q$ 选择不检测策略，且满足 $0\leqslant p,q\leqslant 1$。防御节点 j 选择检测策略 $\left\{S_j\left(\theta_j^n\right)=\text{Monitor}\right\}$ 的期望效用为

$$\begin{aligned}&\text{Eu}_j(\text{Monitor})=p\mu\left[\alpha b_d-(1-\alpha)\omega-c_d\right]-\\&(1-p)\mu(\beta b_d+c_d)-(1-\mu)(\beta b_d+c_d)\end{aligned} \quad (7)$$

防御节点 j 选择不防御策略 $\left\{S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$ 的期望效用为

$$\text{Eu}_j(\text{NotMonitor})=-p\mu\omega+(1-p)\mu b_n+(1-\mu)b_n \quad (8)$$

根据博弈论中求解混合策略纳什均衡的支付等值法可知，当 $\text{Eu}_j(\text{Monitor})=\text{Eu}_j(\text{NotMonitor})$，即 $p^*=\dfrac{\beta b_d+\text{c}_d+b_n}{\mu(\alpha b_d+\beta b_d+\alpha\omega+b_n)}$ 时，防御节点 j 是否将收集到的监测数据提交至云计算中心启动入侵检测是没有区别的，所以恶意节点 i 的贝叶斯纳什均衡是以概率 p^* 采取攻击策略，以概率 $1-p^*$ 采取不攻击策略。恶意节点 i 选择攻击策略 $\left\{S_i\left(\theta_i^m\right)=\text{Attack}\right\}$ 的期望效用为

$$\text{Eu}_i(\text{Attack})=q[(1-\alpha)\omega-c_a-\alpha b_a]+(1-q)(\omega-c_a) \quad (9)$$

恶意节点 i 选择不攻击策略 $\left\{S_i\left(\theta_i^n\right)=\text{NotAttack}\right\}$ 的期望效用为

$$\text{Eu}_i(\text{NotAttack})=0 \quad (10)$$

根据支付等值法，当 $\text{Eu}_i(\text{Attack})=\text{Eu}_i(\text{NotAttack})$，即 $q^*=\dfrac{\omega-c_a}{\alpha(\omega+b_a)}$ 时，恶意节点 i 选择攻击策略或不攻击策略没有区别，所以防御节点 j 的混合策略贝叶斯纳什均衡是以概率 q^* 采取检测策略，以概率 $1-q^*$ 采取不检测策略。因此 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack},\ S_j\left(\theta_j^n\right)=\text{Monitor},\ q^*=\dfrac{\omega-c_a}{\alpha(\omega+b_a)}\right),\ p^*=\dfrac{\beta b_d+\text{c}_d+b_n}{\mu(\alpha b_d+\beta b_d+\alpha\omega+b_n)}\right\}$ 是 MEC 入侵响应决策模型的混合策略贝叶斯纳什均衡。

表 3 展示了入侵响应决策模型的贝叶斯纳什均衡。当防御节点 j 认为节点 i 是恶意节点的先验概率很低 $\left(\mu<\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}\right)$ 时，博弈存在纯策略的贝叶斯纳什均衡 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack},\ S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$，即如果节点 i 是恶意节点就采取攻击策略，如果节点 i 是正常节点就采取不攻击策略，防御节点 j 采取不检测策略。反之，当防御节点 j 认为节点 i 是恶意节点的先验概率很高 $\left(\mu>\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}\right)$ 时，博弈只有混合策略的贝叶斯纳什均衡 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},S_i\left(\theta_i^n\right)=\text{NotAttack},S_j\left(\theta_j^n\right)=\text{Monitor},\ p^*=\dfrac{\beta b_d+c_d+b_n}{\mu(\alpha b_d+\beta b_d+\alpha\omega+b_n)},q^*=\dfrac{\omega-c_a}{\alpha(\omega+b_a)}\right\}$，即如果节点 i 是恶意节点就以概率 p^* 采取攻击策略，以概率 $1-p^*$ 采取不攻击策略；如果节点 i 是正常节点就采取不攻击策略，防御节点 j 以概率 q^* 采取检测策略，以概率 $1-q^*$ 采取不检测策略。

2 算法步骤

在运用 1.2 节得到的结果时，首先依据 1.1 节设置移动边缘计算入侵响应决策模型的博弈参数，然后依据表 2 初始化博弈模型的攻防效用矩阵，一旦部署在边缘节点上的入侵检测代理监测到其他节点发出的行为数据后，就依据表 3 计算最优的响应策略，根据响应策略决定是否将监测数据发送到云计算中心并采取入侵检测，实现最大化抑制入侵节点的入侵行为。具体算法如算法 1 所示。

算法 1 最优响应策略求解算法

输入 静态贝叶斯博弈模型

输出 防御节点的最优响应策略

1) 根据网络收集的数据，初始化博弈模型 $G=(N, P, S, U)$；
2) 循环每对攻防策略，计算攻防效用矩阵；
3) 求解纳什均衡，计算贝叶斯纳什均衡；
4) 确定恶意节点采取攻击策略的概率

表 3 入侵响应决策博弈的贝叶斯纳什均衡

μ	纳什均衡
$\mu<\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}$	存在纯策略的贝叶斯纳什均衡 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack},S_j\left(\theta_j^n\right)=\text{NotMonitor}\right\}$
$\mu>\dfrac{\beta b_d+c_d+b_n}{\alpha b_d+\beta b_d+\alpha\omega+b_n}$	只有混合策略的贝叶斯纳什均衡 $\left\{S_i\left(\theta_i^m\right)=\text{Attack},\ S_i\left(\theta_i^n\right)=\text{NotAttack},\ S_j\left(\theta_j^n\right)=\text{Monitor},\ p^*=\dfrac{\beta b_d+c_d+b_n}{\mu(\alpha b_d+\beta b_d+\alpha\omega+b_n)},q^*=\dfrac{\omega-c_a}{\alpha(\omega+b_a)}\right\}$

$$p^* = \frac{\beta b_d + c_d + b_n}{\mu(\alpha b_d + \beta b_d + \alpha\omega + b_n)};$$

5) 恶意节点以概率 p^*选择攻击策略，以概率 $1-p^*$选择非攻击策略；

6) 确定防御节点启动防御机制的概率 $q^* = \frac{\omega - c_a}{\alpha(\omega + b_a)}$；

7) 对入侵检测系统的检测结果进行判断，若判断结果是攻击，则防御节点以 q^*的概率启动防御机制，否则防御节点以 $1-q^*$的概率不启动防御机制；

8) 判断是否已检测网络中的全部节点，若是则结束博弈，否则返回步骤 2)。

最优防御策略选取算法流程如图 4 所示。

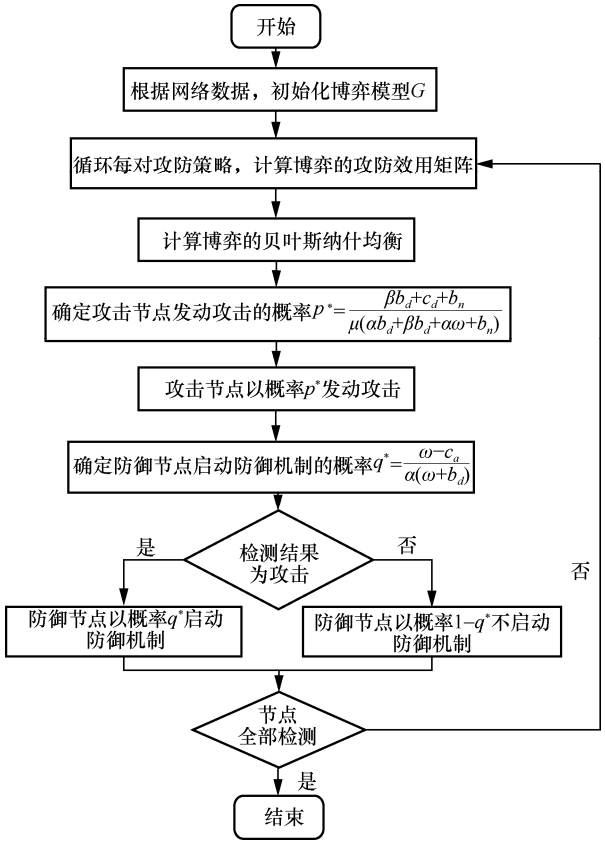

图 4　最优防御策略选取算法流程

算法 1 的复杂度取决于贝叶斯均衡的求解和攻防策略的规模。时间复杂度是由调用的攻防策略决定的，即调用纳什均衡的次数。由于纳什均衡算法的时间复杂度是多项式级别的[23]，即在策略规模为常数的模型中时间复杂度是多项式级别，满足移动边缘计算网络对实时性的要求。一次纳什均衡操作涉及确定攻击策略的概率以及选择攻击策略。设$|A|$为参与人边缘节点 i 空间的大小，$|B|$为参与人防御节点 j 空间的大小，则防御节点 j 要遍历边缘节点 i 空间$|A|^2$ 次。全部节点需要进行 n 次检测才能得到最终的结果，因此整个算法的时间复杂度为 $O(n|A|^2|B|)$。

存储空间消耗主要集中在策略防御成本和均衡求解中间值的存储上，符合移动边缘计算节点资源受限的特点。防御节点选择防御策略的成本为c_d，类型空间包含恶意节点和正常节点两类，所有节点空间要遍历$|AB|^2$ 次，则每个贝叶斯纳什均衡的空间消耗为 $O(c_d|AB|^2)$。全部节点需要进行 n 次检测才能得到最终的结果，因此整个算法的空间复杂度为 $O(nc_d|AB|^2)$。

3　数值分析

采用数值分析的方法计算基于静态贝叶斯博弈模型的最优响应策略，分析入侵检测系统的检测率、误报率、检测次数、恶意节点的攻击成本与攻击收益的比值和防御节点的防御代价与不防御损失的比值对恶意节点选择攻击策略的概率和防御节点选择防御策略的概率的影响。考虑移动边缘计算的实际情况，攻防双方效用参数及取值如表 4 所示。虽然这些参数设置了选定的值，但合理改变这些参数值也能得到类似的实验结果变化趋势。

表 4　　攻防双方效用参数及取值

参数	取值
攻击成本 c_a	5
防御成本 c_d	10
网络正常工作收益 b_n	10
攻击失败代价 b_a	120
防御成功收益 b_d	80
攻击成功收益（或防御失败被攻击代价） ω	100
防御节点 j 认为节点 i 是恶意节点的概率 μ	0.5

图 5 和图 6 分别展示了入侵检测系统的检测率 α 对恶意节点和防御节点策略选择的影响。从图 5 和图 6 可以看出，随着 α 的增大，恶意节点 i 选择攻击策略的概率变小且与 β 的取值有关，防御节点 j 选择防御策略的概率也变小且与 β 的值无关。这是因为当入侵检测系统的检测率 α 增大时，恶意节点的攻击行为被系统检测出的概率会变大，而被检测出攻击行为的节点损失势必增大，因此恶意节点选择攻击策略的概率会降低，

进而导致防御节点的检测率变低。如果防御节点继续保持当前的检测率和检测能耗不变，则防御节点的整体收益就会降低，因此防御节点也会降低检测率。

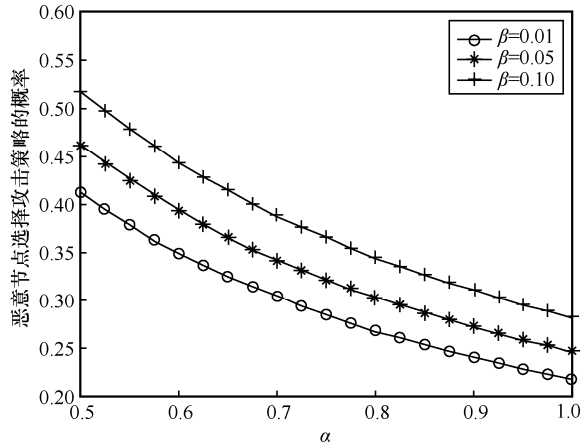

图 5　α 对恶意节点选择攻击策略的影响

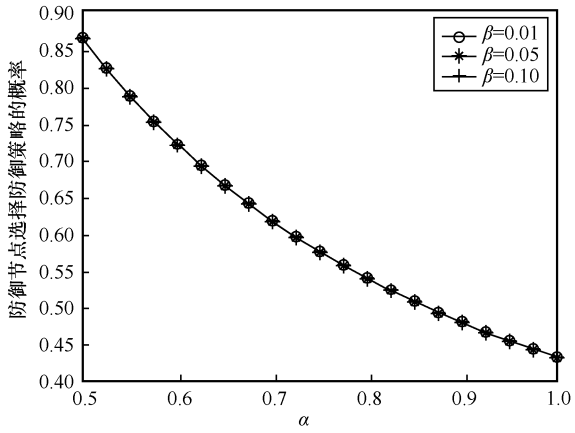

图 6　α 对防御节点选择防御策略的影响

由图 5 和图 6 所示的概率变化可知，如果期望保持当前的概率不变，同时避免过高的检测次数导致整体的收益降低，也可以通过减少检测的次数，以达到高效检测的目的，进而节省边缘节点的能量。图 7 展示了保持防御成功收益不变的情况下，检测次数对防御节点选择防御策略的影响。从图 7 可以看出，防御节点 j 选择防御策略的概率随着 b_d 值的增大而增大，防御成功收益对节点选择防御策略具有正向的刺激作用。同时，随着检测次数的增大，防御节点选择防御策略的概率不会持续增加，而是会在增加到某一个值之后趋于平稳。如果想在保持当前的防御成功收益的同时节省边缘节点的能量，那么检测次数就不能过高，否则防御节点也会降低选择防御策略的概率。

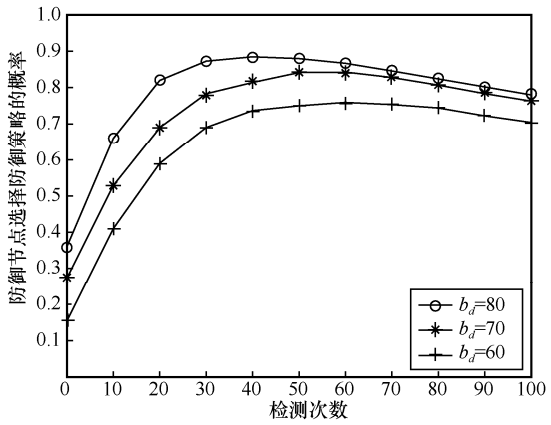

图 7　检测次数对防御节点选择防御策略的影响

图 8 和图 9 分别展示了入侵检测系统的误测率 β 对恶意节点和防御节点策略选择的影响。不难看出，入侵检测系统误测率 β 越大，恶意节点 i 选择攻击策略的概率越大，而防御节点选择防御策略的概率不随 β 值的变化而变化。这是因为当入侵检测系统的误测率 β 增大时，防御节点被攻击的损失增大，因此防御节点会增大选择防御策略的概率。而防御节点选择防御策略的概率增加时，势必会使恶意节点的攻击成功率降低，如果恶意节点继续保持选择攻击策略的概率不变（攻击能耗不变），那么恶意节点的整体收益就会降低，因此恶意节点会降低选择攻击策略的概率。

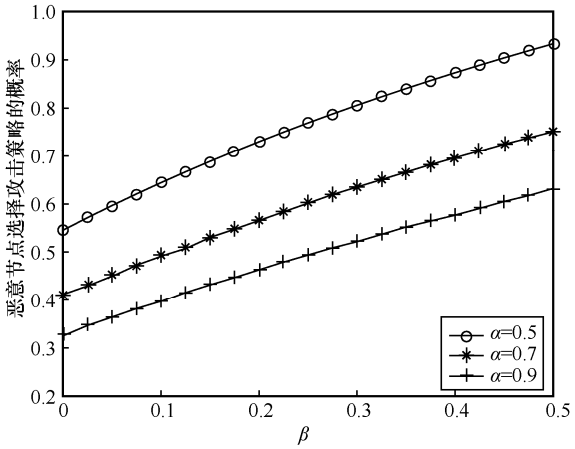

图 8　β 对恶意节点选择攻击策略的影响

由此可知，入侵检测系统的检测精度越高（即检测率 α 越大、误测率 β 越小），恶意节点采取攻击策略的可能性越低。因此，网络防御者可以通过提升入侵检测系统的检测精度来减少攻击事件的发生，从而节约防御攻击的成本。

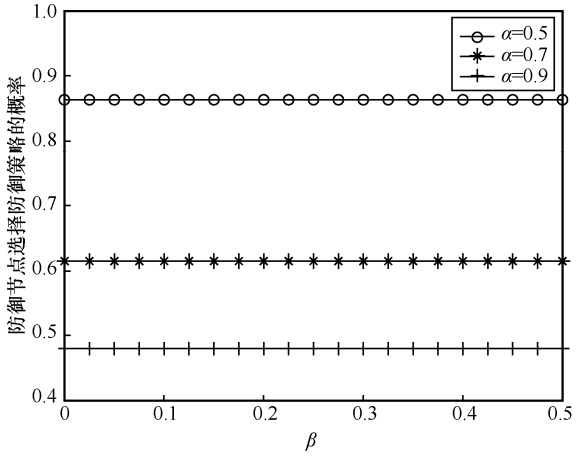

图 9　β 对防御节点选择防御策略的影响

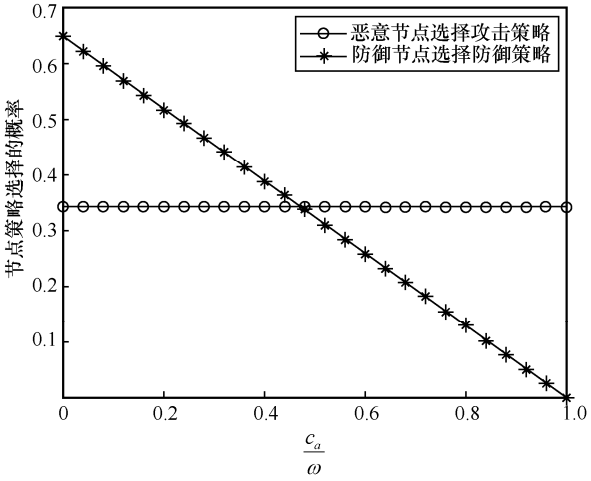

图 10　$\frac{c_a}{\omega}$ 对恶意节点和防御节点策略选择的影响

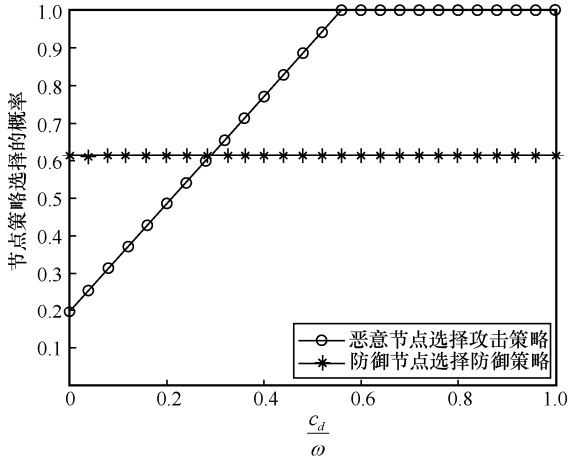

图 11　$\frac{c_d}{\omega}$ 对恶意节点和防御节点策略选择的影响

边缘节点资源受限使恶意节点可以通过增大攻击强度入侵边缘节点。恶意节点的攻击强度与节点的攻击成本和攻击收益有关。同等条件下节点的攻击强度越大，发动攻击的成本越高，在防御节点未检测到攻击时的收益也越多，同时防御节点防御攻击的成本增加，未能有效防御攻击时的系统损耗增高。图 10 和图 11 分别展示了 $\alpha=0.7$、$\beta=0.05$ 条件下恶意节点的攻击成本与攻击成功收益的比值 $\frac{c_a}{\omega}$ 和防御节点的防御成本与防御失败代价的比值 $\frac{c_d}{\omega}$ 对恶意节点和防御节点策略选择的影响。如果攻击成功收益大于攻击成本或防御成功收益大于防御成本，依据博弈参与者“唯利是图”的特性，攻击者没有攻击的动机，防御者也没有防御的理由，因此 $\frac{c_a}{\omega}<1$、$\frac{c_d}{\omega}<1$。当 $\frac{c_a}{\omega}<1$ 时，随着 $\frac{c_a}{\omega}$ 的不断增大，攻击成本与攻击成功收益之间的差距越来越小，导致恶意节点发动攻击的概率越来越小，因此防御节点选择防御策略的概率越来越小，而恶意节点选择攻击策略的概率不随 $\frac{c_a}{\omega}$ 值的变化而变化。当 $\frac{c_d}{\omega}<1$ 时，随着 $\frac{c_d}{\omega}$ 的增大，防御成本越来越大，导致恶意节点选择攻击策略的概率变大，直至恶意节点选择攻击策略的概率达到 1，随后不再增加，而防御节点选择防御策略的概率不变。这是因为在基于静态贝叶斯博弈的最优防御策略选择模型中，攻击者和防御者的选择依赖于对方而非自身的情况。因此，攻击者和防御者可以根据对方的情况，做出最理性的选择。

总结实验结果变化趋势可知，各种因素中对移动边缘计算入侵检测代理响应决策影响最大的是检测率 α，其次是 $\frac{c_a}{\omega}$ 和检测次数，最后是误测率 β 和 $\frac{c_d}{\omega}$。这与入侵响应决策的实际情况一致，当入侵检测系统的检测精度增大时，恶意节点选择攻击策略的概率降低，从而节约防御攻击的成本。另外，模型不仅能对恶意节点选择攻击策略以及防御节点选择防御策略的概率进行预测，还能在入侵检测系统检测精度不高的情况下，直接根据检测结果进行决策，并减少不必要的资源消耗。这对实际系统研发具有指导意义。

将本文所提基于静态贝叶斯博弈模型的最优响应策略与常用的入侵检测算法进行比较，应用效果对比如表 5 所示。从表 5 可以看出，本文基于静

态贝叶斯博弈的 MEC 入侵响应决策模型能在入侵检测系统中获得较高的检测率及较低的误报率和漏报率，优于具有最快检测时间的朴素贝叶斯算法，整体表现优于随机森林算法，检测时间明显低于 DNN 算法。同时，在时间成本、内存和处理成本方面相对具有更低的开销，在实时性上强于机器学习和深度学习算法，模型运算过程相对简单、节省有限的计算资源，更适用于计算和存储资源有限的边缘节点。

表 5　　入侵检测算法应用效果对比

算法	检测率	误报率	漏报率	检测时间/s
静态贝叶斯博弈模型	94.5%	5.82%	5.07%	8.4
朴素贝叶斯	80.3%	19.56%	20.14%	2.7
随机森林	90.2%	10.41%	9.43%	23.6
DNN	95.4%	5.24%	4.31%	65.1

基于本文的研究成果，可以制定以下措施来降低恶意节点发动攻击的概率，从根源上保障 MEC 网络的安全。1) 加大对发动攻击行为的恶意节点的惩罚，促使防御节点积极地应对恶意节点的攻击，提高检测率；2) 通过优化入侵检测算法来降低防御节点的检测能耗，从而降低恶意节点发动攻击的概率；3) 适当减小边缘节点的通信半径，这一方面可以降低通信范围内恶意节点的数量，另一方面也可以节约边缘节点的能耗，延长其使用寿命。

4　结束语

本文提出了一种适用于移动边缘计算环境的入侵响应决策模型。模型通过深入研究边缘节点和攻击者之间的交互行为，并结合边缘节点地理分布广泛、网络环境复杂、资源受限等特点，建立了基于静态贝叶斯博弈的入侵响应决策模型，模拟攻防双方在单次博弈中的行为选择，预测出博弈过程中攻击者选择攻击行为和防御者选择防御行为的概率。模型综合考虑系统的资源状态、入侵响应的成本以及入侵检测系统的检测率、误报率和漏报率等因素对防御策略选取的影响，使移动边缘计算系统在面临外部入侵时遭受的损失最低，且对整个网络的时延影响较小，满足移动边缘计算网络对实时性和可靠性的要求。仿真结果表明，该模型为防御者产生了更节能的防御策略，同时提高了系统的整体检测能力。

参考文献：

[1] ARMBRUST M, FOX A, GRIFFITH R, et al. A view of cloud computing[J]. Communications of the ACM, 2010, 53(4): 50-58.

[2] HU Y C, PATEL M, SABELLA D, et al. Mobile edge computing-a key technology towards 5G[R]. 2015.

[3] LUAN T H, GAO L X, LI Z, et al. Fog computing: focusing on mobile users at the edge[J]. arXiv Preprint, arXiv: 1502.01815, 2015.

[4] PRABAVATHY S, SUNDARAKANTHAM K, SHALINIE S M. Design of cognitive fog computing for intrusion detection in Internet of things[J]. Journal of Communications and Networks, 2018, 20(3): 291-298.

[5] 李韵, 黄辰林, 王中锋, 等. 基于机器学习的软件漏洞挖掘方法综述[J]. 软件学报, 2020, 31(7): 2040-2061.
LI Y, HUANG C L, WANG Z F, et al. Survey of software vulnerability mining methods based on machine learning[J]. Journal of Software, 2020, 31(7): 2040-2061.

[6] 张玉清, 董颖, 柳彩云, 等. 深度学习应用于网络空间安全的现状、趋势与展望[J]. 计算机研究与发展, 2018, 55(6): 1117-1142.
ZHANG Y Q, DONG Y, LIU C Y, et al. Situation, trends and prospects of deep learning applied to cyberspace security[J]. Journal of Computer Research and Development, 2018, 55(6): 1117-1142.

[7] LEE S J, YOO P D, ASYHARI A T, et al. IMPACT: impersonation attack detection via edge computing using deep autoencoder and feature abstraction[J]. IEEE Access, 2020, 8: 65520-65529.

[8] 李忠成, 高惠燕, 张文祥. 边缘计算中改进 ELM 的高效入侵检测算法[J]. 计算机测量与控制, 2021, 29(7): 223-228, 234.
LI Z C, GAO H Y, ZHANG W X. An efficient edge computing intrusion detection algorithm based on improved ELM[J]. Computer Measurement & Control, 2021, 29(7): 223-228, 234.

[9] SUDQI K B, ABDUL W A W B, IDRIS M Y I B, et al. A lightweight perceptron-based intrusion detection system for fog computing[J]. Applied Sciences, 2019, 9(1): 178.

[10] SOUZA C A D, WESTPHALL C B, MACHADO R B, et al. Hybrid approach to intrusion detection in fog-based IoT environments[J]. Computer Networks, 2020, 180: 107417.

[11] SYVERSON P F. A different look at secure distributed computation[C]//Proceedings of the 10th IEEE Workshop on Computer Security Foundations. Piscataway: IEEE Press, 1997: 109-115.

[12] 陈赵懿, 高秀峰, 王帅. 攻防博弈下的 Ad hoc 网络风险预测[J]. 火力与指挥控制, 2020, 45(8): 16-21.
CHEN Z Y, GAO X F, WANG S. Risk prediction of ad hoc network based on game[J]. Fire Control & Command Control, 2020, 45(8): 16-21.

[13] AN X S, LIN F H, XU S G, et al. A novel differential game model-based intrusion response strategy in fog computing[J]. Security and Communication Networks, 2018, 2018: 1-9.

[14] 苗莉. 边缘计算环境下安全防御模型及算法研究[D]. 北京: 北京科技大学, 2019.
MIAO L. Research on security defense model and algorithm in edge computing[D]. Beijing: University of Science and Technology Beijing, 2019.

[15] ALPCAN T, BAŞAR T. Network security a decision and game-theoretic approach[M]. Cambridge: Cambridge University Press, 2010.

[16] 石进, 陆音, 谢立. 基于博弈理论的动态入侵响应[J]. 计算机研究与发展, 2008, 45(5): 747-757.
SHI J, LU Y, XIE L. Dynamic intrusion response based on game theory[J]. Journal of Computer Research and Development, 2008, 45(5): 747-757.

[17] 姜伟, 方滨兴, 田志宏, 等. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展, 2010, 47(10): 1714-1723.
JIANG W, FANG B X, TIAN Z H, et al. Research on defense strategies selection based on attack-defense stochastic game model[J]. Journal of Computer Research and Development, 2010, 47(10): 1714-1723.

[18] 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 Y Z, YU J Y, QIU W, et al. Evolutionary game model and analysis methods for network group behavior[J]. Chinese Journal of Computers, 2015, 38(2): 282-300.

[19] BABAR S D, PRASAD N R, PRASAD R. Game theoretic modelling of WSN jamming attack and detection mechanism[C]//Proceedings of 2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC). Piscataway: IEEE Press, 2013: 1-5.

[20] HARSANYI J C. Games with incomplete information played by “Bayesian” players, I-III[J]. Management Science, 2004, 50(12): 1804-1817.

[21] KANTZAVELOU I, KATSIKAS S. A generic intrusion detection game model in IT security[C]//Proceedings of the 5th International Conference on Trust, Privacy and Security in Digital Business. New York: ACM Press, 2008: 151-162.

[22] NASH J F. Equilibrium points in N-person games[J]. Proceedings of the National Academy of Sciences of the United States of America, 1950, 36(1): 48-49.

[23] DU S G, LI X L, DU J B, et al. An attack-and-defence game for security assessment in vehicular ad hoc networks[J]. Peer-to-Peer Networking and Applications, 2014, 7(3): 215-228.

[作者简介]

范伟（1984− ），男，北京人，博士，中国科学院信息工程研究所高级工程师、硕士生导师，主要研究方向为移动通信安全、云计算安全、虚拟化安全等。

彭诚（1994− ），男，北京人，中国科学院信息工程研究所博士生，主要研究方向为移动通信安全、通信协议分析等。

朱大立（1972− ），男，北京人，博士，中国科学院信息工程研究所正高级工程师、博士生导师，主要研究方向为移动互联网安全等。

王雨晴（1995− ），女，天津人，中国科学院信息工程研究所硕士生，主要研究方向为边缘计算安全等。