网络空间安全学院（密码学院）

2023-2024 学年度第 1 学期

Y03296 博弈论 课程论文

论文题目：**GTM-CSec：基于 IDS 和蜜罐的云安全博弈论模型**

学生学号及姓名：**20213006525** 梁浩哲

20213007015 刘涛、**20213006839** 甄五四

学生所在班级：**2021** 级信息安全实验班

论文提交时间：**2024** 年 **1** 月 **2** 日

授课教师：高扬

教师评阅：

成绩：_____

教师签名：_____

一、摘要

云计算可以提供存储、处理、共享以及其他服务等，现已被广泛应用。但是云计算也面临着来自其周围环境的一系列安全挑战，例如简单常规攻击、复杂攻击等。当物联网（IoT）设备连接到云计算时，由于这些设备具有较低的安全性，云计算所面临的挑战变得更加严峻。为应对这些威胁，通常采用入侵检测系统（IDS）、蜜罐、防火墙等技术来防御攻击。然而为了确定在这些技术中最佳的防御策略，则需要进一步深入研究。因此，在本文中，我们提出了一种名为 GTM-CSec 的博弈论模型。该模型以智能的方式选择基于签名、异常和蜜罐的检测模块，以便更有效地检测防御攻击。与同时使用所有模块相比，选择特定的检测模块不仅有助于降低能耗，还能提高整体防御系统的效率。模型对防御者和攻击者策略进行了全面评估，并使用纳什均衡（NE）确定了最佳策略。最后，我们引入该模型进行仿真实验，结果证明防御系统在抵御攻击方面取得显著成就。

关键词：博弈论，云计算，物联网，入侵检测系统，蜜罐

目录

一、前言

随着数字化时代的到来，越来越多的企业、个人等倾向于使用云计算及其多样化的服务。现阶段云服务已被大量运用到各行各业，包括教育、医疗、银行、工业以及物联网、大数据等领域。通过使用云服务，我们可以很方便的实现大量数据的存储和处理，极大的方便了我们的工作和生活。但是，云服务在为我们带来便利的同时，其安全问题也随之而来。比如供应商为了在功耗、产品寿命周期、整体效率等多方面实现更高的效益，会把像摄像头、社交媒体组件等智能设备暴露在公共场所，导致这些设备容易被访问且易受攻击。特别是物联网设备，由于这些设备不断地从云端发送和收集数据，因此他们很容易遭受安全攻击。这些攻击行为无疑对云服务器和其他资源构成了巨大的威胁。面对这些攻击行为，现如今我们已经运用防火墙技术、入侵检测系统（IDS）、蜜罐等防御工具来预防。其中入侵检测系统是一款基于签名检测功能异常检测功能的软件系统，其作用是监测网络流量并检测网络上的恶意活动。而蜜罐则是一种用于吸引和监测攻击者活动的安全工具，它可以通过向攻击者提供虚假数据来诱捕攻击者，当攻击者尝试去获取蜜罐提供的虚假数据时，它会被阻止进入网络。为了让防御机制更加高效，我们需要定期监测网络流量。因此，我们基于非零和非合作博弈提出了博弈论模型 GTM-Csec。该模型利用博弈论智能监控网络中的流量并通过不断调整 IDS 和蜜罐的相关配置以获得高效的防御效果。在该模型中，防御者和攻击者可以采取不同的策略，然后对攻击者和防御者采用不同策略的概率值进行更新，最后通过纳什均衡预测最佳策略。

二、相关工作

Shigeng Shen 等人在《Multistage Signaling Game-Based Optimal Detection Strategies for Suppressing Malware Diffusion in Fog-Cloud-Based IoT Networks》一文中给出了用于抑制扩散恶意软件的异构 WSNs 博弈论模型，文中设计了一个非零和博弈的马尔可夫链模型，其结果可用于任何相关的理论工作。 Liang Xiao 等人在《Cloud-based malware detection game for mobile devices with offloading》一文中为基于云的移动设备设计了一个恶意软件检测博弈，提出了一种基于后学习的方案，进一步提高了系统的学习能力。Rashvand 等人回顾了分布式安全在多

代理系统及其应用中的情况，为了解决其中提出的问题，针对 ICT 进行了跨层优化，以提高对环境感知安全性的分析和信任因素的防御效率，增强了 MAS 的自我管理能力，并改进了它们的对策技术，以保护系统免受攻击。Guisheng Fan 等人在《A game theoretic method to model and analyze at- tack-defense strategy of resource service in cloud application》一文中提出了一种模型，使用博弈论方法分析云应用中资源服务的攻击和防御策略。值得注意的是，这里的博弈模型是基于随机 Petri 网的，定义了攻击者和防御者的行为，并且设计了一种执行算法，用于发现攻击的可能路径并根据该路径执行策略。实验的仿真结果也验证了防御者选择的防御策略能够迅速应对攻击者。Calyam 等人在《Vdc-analyst: design and verification of virtual desktop cloud resource allocations》一文中为云服务提供商设计了一种名为 VDC-Analyst 的新工具，以最大化体验质量（QoE）。VD-Analyst 在仿真和模拟模式下工作，用于设计和验证资源分配方案。Fadlullah 等人在《A game-theoretic joint optimization of qos and security for differentiated services in next generation heterogeneous networks》一文中提出了一个 GT-QoSec 模型，使用博弈论优化了下一代异构网络中的服务质量（QoS）和安全性。该模型旨在平衡安全性和 QoS 参数，考虑了过渡矩阵，并在预期的步数中获得了纳什均衡（NE）。Zhi Li 等人在《A differential game model of intrusion detection system in cloud computing》一文中设计了一个云计算中 IDS 的微分博弈模型。这项工作通过博弈论的理论基础，决定了 IDS 为防御云资源的最优策略。Dazhi Li《A dynamic multiple-keys game-based industrial wireless sensor-cloud authentication scheme》为传感器云通信设计了基于博弈论的认证框架，因为这些设备部署在无人值守的环境中，更容易受到安全攻击。因此，在认证方案中增加了一个信任值。通过仿真实验的结果表明，所提出的方法可以提高网络和设备的安全性。Khaled Salah 等人在《Using cloud computing to implement a security overlay network》一文中提出了一种安全覆盖系统，用于增加云环境中的弹性和安全性，所提出的模型已经通过性能、成本、灵活性和控制等多个参数的测试。Yongkai Fan 在《One secure data integrity verification scheme for cloud storage》一文中确定了将数据传送到未知云服务器所引起的完整性问题。为了检查数据完整性并实现安全密钥管理，提出了一种基于身份的聚合签名安全方案。结果表明，所提出的方案是可行和高效的。

F. Al-Haidari 等人在《Impact of CPU Utilization Thresholds and Scaling Size on Autoscaling Cloud Resources》一文中调查了成本和性能对自动扩展操作的影响，并且进行了 CPU 上限阈值的调整，以优化问题。Liang Xiao 等人在《Attacker-Centric View of a Detection Game against Advanced Persistent Threats》一文中应用交换前景理论来解释网络系统与 APT 攻击者之间的关系，并且使用博弈论模型来提高检测性能，结果显示它比 Q 学习策略更有效。Ahmad Hammoud 等人在《On the detection of passive malicious providers in cloud federations》一文中确定了云联盟形成的最佳问题以及恶意内部人员的问题。提出了一个博弈模型，帮助经纪人管理联盟，并最大化检测内部恶意活动的率。该解决方案不仅将检测率提高到 92%，而且通过降低延迟，改善了联盟的服务质量，还进行了 IDS 的优化，以减少误报和降低功耗。

Jianhua Liu 等人在《Energy-Efficient Two-Layer Cooperative Defense Scheme to Secure Sensor-Clouds》通过博弈论解决了检测攻击的动态方程，并提出了一个合作防御系统，模拟结果证明了能耗更低和误报更少。Agnieszka Jakóbik 等人在《Stackelberg games for modeling defense scenarios against cloud security threats》一文中检查了数据中心的脆弱性，并提出了一个博弈理论模型，用于衡量数据中心的脆弱程度。结果证明，尽管使用了 IDS 来保护虚拟机（VM），所提出的模型仍有助于提高云的安全性。通过在攻击者和防御者之间设计了一个非零和的 Stackelberg 博弈，以最大化增加防御者的收益。同时计算出的方程和收益也被进一步用来预测攻击。

在对相关研究背景的文献调查进行严谨的分析后，发现大多数相关工作都是只考虑了单一的一般防御者系统。在本文的这项工作中，使用了基于签名、基于异常和蜜罐的检测系统，这些被认为是最先进的检测系统。此外，所提出的模型根据攻击类型智能地选择最合适的工具或这些工具的组合。虽然 IoT 和云之间有着非常紧密的关系，但在这种合作的安全方面还没有进行太多的研究。本文考虑到这两个范式之间安全通信的需求，攻击时刻的时间因素非常关键，攻击时间越长，对云的破坏就越大。因此，明确考虑了时间参数。同时本文也考虑到提出的模型应具有灵活性，可以顺利地应用于现有的防御系统，或者可以通过小的更新扩展到其他范式。在考虑到所有这些约束的情况下，本文设计了 GTM-CSec 模

型，它通过结合基于 IDS 和蜜罐的方法，帮助实时选择最佳防御策略。

三、系统框架

3.1 理论模型架构图

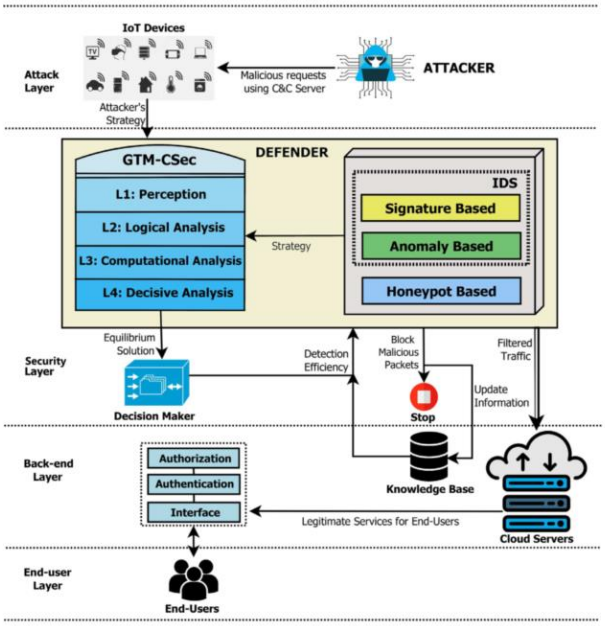

图 1 理论模型框架图

3.2GTM-CSec 模型概述

GTM-CSec 模型是一个非合作博弈模型，其中包括两个主要博弈方：防御者（Defender, D）和攻击者（Attacker, A）。这个模型的核心在于通过分析这两方的策略和潜在的收益，来制定最有效的云安全策略。

3.3 模型结构和组成

1.非合作博弈:

GTM-CSec 采用非合作博弈的形式。在这个博弈中，攻击者和防御者各自有不同的目标和策略，他们互不合作，各自寻求最大化自己的利益。

2.玩家角色:

防御者: 通常是云服务提供商，负责保护云环境免受攻击。

攻击者: 尝试通过各种手段攻击云环境，以窃取数据、破坏服务等。

3.策略空间:

防御者策略: 包括使用基于签名的入侵检测系统（IDS）、基于异常的 IDS 和蜜罐技术等。

攻击者策略: 包括常规攻击、等待特定时间后攻击、采用新型或复杂的攻击手段等。

4.收益函数:

防御者收益: 取决于成功防御攻击的能力。

攻击者收益: 取决于攻击的成功与否。

3.4 模型的运作机制

提出工作的部署架构被划分为四层：攻击层、安全层、后端层和终端用户层。

在攻击层中，攻击者或僵尸网络控制者向 IoT 设备发送恶意请求，并从命令和控制（C&C）服务器控制这些设备。攻击者根据其最佳策略来实现最大收益。攻击者的策略主要有定期攻击云服务器、等待特定时间段(t)、使用新的或复杂的攻击方式攻击云。

为了防御攻击者的攻击，安全层开始行动。这一层包括入侵检测系统（IDS），包括基于签名的检测模块和基于异常的检测模块、基于蜜罐的检测模块以及提出的 GTM-CSec 模型和决策者。IDS 有两个不同的模块：签名检测（SD）和异常检测（AD）模块。已知或常规攻击最好由 SD 防御，因为这些攻击已经在数据库中。SD 与数据库核对，并以更高效和快速的方式给出结果。另一方面，AD 最适合处理未知或复杂的攻击。如果进入流量或数据包的行为发生偏差，AD 技术会发出真正积极的信号，表明存在攻击。蜜罐位于网络上，包含虚拟数据以诱捕攻击者。在检测系统验证合法流量后，将其发送到云中进行安全网络。防御者采用其最佳策略来防御攻击者的攻击。防御者的策略集主要有使用基于签名的 IDS 进行监控、使用基于异常的 IDS 进行监控、蜜罐监测。

GTM-CSec 模型进一步扩展为四层：感知层、逻辑分析层、计算分析层和决策分析层。

感知层：这一层主要负责识别和分析攻击者和防御者的策略。它对当前环境中的行为模式进行监测，以识别潜在的攻击或防御行动。

逻辑分析层：在这一层，基于感知层收集的信息，进行策略的逻辑评估。这包括分析攻击者可能采取的策略和防御者的最佳响应策略。

计算分析层：这一层对攻击者的潜在策略进行更深入的分析，并计算确定防御者的最佳响应策略。这涉及对各种可能的攻击和防御动作进行成本效益分析。

决策分析层：最后一层负责制定最终的防御策略。它结合了前三层的信息和分析，制定出最适合当前威胁环境的防御策略。

接下来的后端层通常处理云服务的核心功能和资源，比如服务器、存储、网络资源和计算能力。它负责维护和管理云环境的基础设施，以及提供必要的支持和资源以保证云服务的连续性和可靠性。后端层也可能涉及数据处理和存储操作，确保数据的安全和高效管理。

最后的终端用户层这一层面向最终用户，是用户与云服务交互的界面。它提供用户访问云资源的门户和应用程序界面，使用户能够使用和管理云服务。终端用户层也关注用户体验和访问控制，确保用户可以安全、便捷地访问所需的云服务和资源。

3.5 个人理解

GTM-CSec 模型的创新之处在于它提供了一种动态和灵活的方式来分析和应对云环境中的安全威胁。通过将传统的安全措施（如 IDS 和蜜罐）与先进的博弈论分析相结合，使这个模型能够针对不断变化的攻击模式提出有效的防御策略。这种方法不仅提高了防御策略的有效性，还增加了对新兴威胁的适应能力，比单一的安全措施或静态防御策略更为有效，同时也减少了不必要的能耗。此外，模型的多层结构提供了全面的安全分析，从感知攻击到做出最终决策的每个阶段都经过精细考量。

GTM-CSec 模型体现了现代网络安全领域对博弈论方法的深入应用，特别是在处理云计算环境中的安全问题时，展示了其独特的价值和潜力。通过考虑攻击者和防御者的不同策略和动机，该模型为云安全提供了一个更灵活、更全面、更有效的解决方案。

四、博弈论技术分析

4.1 博弈论基础知识

博弈论是一种研究决策和策略的数学理论，它涉及多方参与者在制定决策时如何相互影响和相互作用的问题。博弈论中假设在博弈过程中所有的参与者都是理性的，即总是会根据对方的选择而选择最好的策略以获得最大的收益。在博弈论中包含如下几种基本要素：

1、博弈方（P）：博弈的参与者，即在博弈过程中独立决策、独立承担结果的个人或组织。一组博弈方可以表示为（$P_1,P_2,...,P_a$）,$a>2$。在本文的博弈模型中，存在两博弈方，分别为防御者和攻击者；

2、行为（A）：博弈方选择的有最大收益的行为。博弈方P_i的动作集合可以表示为（$A_1,A_2,...,A_b$）。

3、策略（S）：博弈中各博弈方的决策内容，即规定每个博弈方可以选择的行为等。博弈方的策略组合可以表示为（$S_1,S_2,...,S_c$）;在此博弈模型中，防御者的策略组合为（$S_{A1},S_{A2},...,S_{Ac}$），攻击者的策略组合为（$S_{D1},S_{D2},...,S_{Dc}$）；

4、得益（U）：即博弈方从博弈中获得的利益，也是博弈方决策行为的主要依据。对应策略的得益集可表示为（$U_1,U_2,...,U_d$）。在此博弈模型中，防御者的得益为U_D，攻击者的得益为U_A；

5、均衡：博弈的均衡是指在给定的策略下，没有玩家有动机单独改变他们的策略来获得更高的收益。在纳什均衡中，每个博弈方都采取相对于其他博弈方策略的最优策略。均衡状态下的策略可以是纯策略，也可以是混合策略。因此，策略博弈可以表示为：

$$G=(P,(S_j)_{i\in P},(U_j)_{i\in P}) \quad (1)$$

其中P表示所有参与博弈的博弈方集合，$(S_j)_{i\in P}$表示博弈方i可能采取的不同策略集合,$(U_j)_{i\in P}$表示博弈方i在不同策略下可能获得的得益集合。

4.2GTM-CSec 博弈模型分析

4.2.1 确定博弈双方得益矩阵

以其中一种情况为例，当攻击者使用防御者已知的常规技术进行攻击时，防御者使用基于签名的方法进行监测，此时防御者将成功监视攻击。防御者的总得益取决于消耗的能量和成功监视所获得的收益。防御者得益函数如下：

$$U_{11}(D)=B_{ds}(t)-E_{ids}(t) \quad (2)$$

而对于攻击者，由于此次攻击未成功，故将丢失使用的资源，攻击者的得益函数为：

$$U_{11}(A)=-R_{at}(t) \quad (3)$$

对于其他情况，根据本文第三节中对攻防双方策略的描述，便可得到双方的

得益结果，在此处将不再赘述，直接给出攻击者和防御者的得益函数如下：

防御者得益矩阵：

$$M_D=\begin{bmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \\ d_{31} & d_{32} & d_{33} \end{bmatrix}=\begin{bmatrix} B_{ds}(t)-E_{ids}(t) & -E_{ids}(t) & -E_{ids}(t)-V(t) \\ -E_{ids}(t) & -E_{ids}(t) & B_{ds}(t)-E_{ids}(t) \\ B_{ds}(t)-H_{hp}(t) & -E_{ids}(t) & -H_{hp}(t)-V(t) \end{bmatrix} \quad (4)$$

攻击者得益矩阵：

$$M_A=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}=\begin{bmatrix} -R_{at}(t) & -W_{at}(t) & G_{at}(t)-R_{at}(t) \\ G_{at}(t)-R_{at}(t) & -W_{at}(t) & -R_{at}(t) \\ -R_{at}(t) & -W_{at}(t) & G_{at}(t)-R_{at}(t) \end{bmatrix} \quad (5)$$

（注：其中 d_{ij} 是策略矩阵中 m_{11} 对应防御者的得益函数，a_{11} 是策略矩阵中 m_{11} 对应防御者的得益函数）

4.3GTM-CSec 博弈模型纯策略纳什均衡

本文使用划线法寻找本博弈的纯策略纳什均衡，结果如下所示：

$$M_D=\begin{bmatrix} \underline{d_{11}} & d_{12} & d_{13} \\ d_{21} & d_{22} & \underline{d_{23}} \\ \underline{d_{31}} & d_{32} & d_{33} \end{bmatrix}=\begin{bmatrix} \underline{B_{ds}(t)-E_{ids}(t)} & -E_{ids}(t) & -E_{ids}(t)-V(t) \\ -E_{ids}(t) & -E_{ids}(t) & \underline{B_{ds}(t)-E_{ids}(t)} \\ \underline{B_{ds}(t)-H_{hp}(t)} & -E_{ids}(t) & -H_{hp}(t)-V(t) \end{bmatrix} \quad (6)$$

$$M_A=\begin{bmatrix} a_{11} & a_{12} & \underline{a_{13}} \\ \underline{a_{21}} & a_{22} & a_{23} \\ a_{31} & a_{32} & \underline{a_{33}} \end{bmatrix}=\begin{bmatrix} -R_{at}(t) & -W_{at}(t) & \underline{G_{at}(t)-R_{at}(t)} \\ \underline{G_{at}(t)-R_{at}(t)} & -W_{at}(t) & -R_{at}(t) \\ -R_{at}(t) & -W_{at}(t) & \underline{G_{at}(t)-R_{at}(t)} \end{bmatrix} \quad (7)$$

对于攻击方，最大的收益策略是 a_{13},a_{21},a_{33}，对于防御一方，最大收益策略是 d_{11},d_{23},d_{31}。

根据上述结果可以得到以下两条结论：

1、该博弈模型中不存在纯策略纳什均衡。从划线的结果中可以看到，防御者和攻击者的最大收益对应的矩阵元素不匹配。攻击者的最大收益是采用复杂的攻击方式攻击云端，但是复杂的攻击方式意味着消耗更多资源。因此，防御者将选择基于异常检测的方法进行检测，从而阻止攻击者的攻击。然后，由于防御者选择了基于异常监测的策略，攻击者将尝试使用常规方式进行攻击。同样的，防御者可以选择蜜罐或者基于签名检测的策略来阻止攻击者的攻击。由此可见系统无法达到稳定状态，也就不存在纯策略纳什均衡。

2、攻击者在等待攻击的过程中不会获得任何收益，所以攻击者总是会选择

攻击。从攻击方最大收益策略中可以看出，策略 SA2 从未被考虑过。为了获得最大的收益，攻击者将在 SA1、SA3 之间做出选择，即攻击者总会选择实施攻击。所以在后续的讨论中，本模型将忽略攻击者的策略 SA2，仅考虑攻击者在策略 SA1 和 SA3 间做选择。更新后博弈双方得益矩阵如下所示：

$$M_D=\begin{bmatrix} d_{11} & d_{21} & d_{31} \\ d_{13} & d_{23} & d_{33} \end{bmatrix}=\begin{bmatrix} B_{ds}(t)-E_{ids}(t) & -E_{ids}(t) & B_{ds}(t)-H_{hp}(t) \\ -E_{ids}(t)-V(t) & B_{ds}(t)-E_{ids}(t) & -H_{hp}(t)-V(t) \end{bmatrix} \quad \textbf{(8)}$$

$$M_A=\begin{bmatrix} a_{11} & a_{21} & a_{31} \\ a_{13} & a_{23} & a_{33} \end{bmatrix}=\begin{bmatrix} -R_{at}(t) & G_{at}(t)-R_{at}(t) & -R_{at}(t) \\ G_{at}(t)-R_{at}(t) & -R_{at}(t) & G_{at}(t)-R_{at}(t) \end{bmatrix} \quad \textbf{(9)}$$

4.4GTM-CSec 博弈模型混合策略纳什均衡

上述所得到的得益矩阵是假设 IDS 和蜜罐的检测及防御效率达到 100%，但考虑到实际的防御效率，在这里需要再次更新博弈双方的得益矩阵：

以策略组合（S_{D1},S_{A1}）为例来分析攻防双方实际的得益函数。此种情况下，由于攻击者选择常规攻击策略，而防御者选择基于签名的检测策略，那么此时攻击方实施的攻击将被成功检测，但由于防御方此策略的检测率为 μ，所以在（$1-\mu$）的概率下，攻击方将攻击成功。因此对于攻击方，其收益函数为：

$$U_{11}(A)=(1-\mu)G_{at}(t)-R_{at}(t) \quad \textbf{（10）}$$

对于防御方，其收益函数应为：

$$U_{11}(D)=\mu B_{ds}(t)-(1-\mu)V(t)-E_{ids}(t) \quad \textbf{（11）}$$

对于其他策略组合的收益函数，均可根据上述分析方法得到，此处将不再赘述，而直接给出更新后的得益矩阵如下所示：

$$M'_D=\begin{bmatrix} \mu B_{ds}(t)-(1-\mu)V(t)-E_{ids}(t) & -E_{ids}(t)-V(t) & \gamma B_{ds}(t)-(1-\gamma)V(t)-H_{hp}(t) \\ -E_{ids}(t)-V(t) & \alpha B_{ds}(t)-(1-\alpha)V(t)-E_{ids}(t) & -H_{hp}(t)-V(t) \end{bmatrix} \quad \textbf{(12)}$$

$$M'_A=\begin{bmatrix} (1-\mu)G_{at}(t)-R_{at}(t) & G_{at}(t)-R_{at}(t) & (1-\gamma)G_{at}(t)-R_{at}(t) \\ G_{at}(t)-R_{at}(t) & (1-\alpha)G_{at}(t)-R_{at}(t) & G_{at}(t)-R_{at}(t) \end{bmatrix} \quad \textbf{(13)}$$

（注：其中 M'_D、M'_A 分别表示防御者和攻击者的得益矩阵。得益矩阵中各得益函数所对应的策略与（8）、（9）式相同）

其中 α、μ、γ、B_{ds}、E_{ids}、H_{hp}、V 均是常数。为了找出防御者针对攻击的最佳防御策略，本文将防御方的防御策略组合分为七种情况如下表所示：

表 1 防御者的不同策略组合

序号	防御者的策略组合
情况 1	基于签名的 IDS、基于异常的 IDS 和蜜罐三种协同工作策略
情况 2	基于签名的 IDS 策略或基于异常的 IDS 和蜜罐协同工作策略
情况 3	基于异常的 IDS 策略或基于签名的 IDS 和蜜罐协同工作策略
情况 4	蜜罐防御策略或基于签名的 IDS 和基于异常的 IDS 协同工作策略
情况 5	基于签名的 IDS 策略或基于异常的 IDS 策略
情况 6	基于签名的 IDS 策略或基于蜜罐的防御策略
情况 7	基于异常的 IDS 策略或基于蜜罐的防御策略

下面将详细分析以上七种情况下博弈双方的收益函数并求出其最佳混合策略纳什均衡。

4.4.1 情况 1

假设防御者以 $\frac{2p}{5},\frac{2p}{5},\frac{p}{5}$ 的概率实施基于签名的 IDS、基于异常的 IDS 和蜜罐防御策略；攻击者以 f 和（$1-f$ ）的概率执行常规攻击和复杂攻击。

防御者收益函数：

$$\begin{aligned}U_{Dsah}=&\left(\frac{2p}{5}\right)(f)U_{11}(D)+\left(\frac{2p}{5}\right)(f)U_{12}(D)+\left(\frac{p}{5}\right)(f)U_{13}(D)\\&+\left(\frac{2p}{5}\right)(1-f)U_{21}(D)+\left(\frac{2p}{5}\right)(1-f)U_{22}(D)+\left(\frac{p}{5}\right)(1-f)U_{23}(D)\end{aligned}\tag{14}$$

(注：$U_{ij}(D)$ 表示防御者得益矩阵式（12）中第 i 行第 j 列对应的得益函数)

攻击者收益函数：

$$\begin{aligned}U_{Asah}=&\left(\frac{2p}{5}\right)(f)U_{11}(A)+\left(\frac{2p}{5}\right)(f)U_{12}(A)+\left(\frac{p}{5}\right)(f)U_{13}(A)\\&+\left(\frac{2p}{5}\right)(1-f)U_{21}(A)+\left(\frac{2p}{5}\right)(1-f)U_{22}(A)+\left(\frac{p}{5}\right)(1-f)U_{23}(A)\end{aligned}\tag{15}$$

(注：$U_{ij}(A)$ 表示攻击者得益矩阵式（13）中第 i 行第 j 列对应的得益函数)

为了最大化收益，需将防御方的收益函数对 p 求偏导，将攻击方的收益函数对 f 求偏导并令它们为 0，求出 p 和 f ：

$$\frac{\partial U_{Dsah}}{\partial p}=\frac{pf}{5}\left[B_{ds}(t)+V(t)\right]\left[2\mu-2\alpha+\gamma\right]+\frac{2p\alpha}{5}\left[B_{ds}(t)+V(t)\right]$$
$$-4pE_{ids}(t)-pV(t)-\frac{p}{5}H_{hp}(t)=0 \quad (16)$$

$$\frac{\partial U_{Asah}}{\partial f}=\frac{pf}{5}G_{at}(t)\left[2\mu-2\alpha+\gamma\right]+pG_{at}(t)-pR_{at}(t)\frac{2p\alpha}{5}G_{at}(t)=0 \quad (17)$$

通过求解方程得到 $p=\infty$，

$$f=\frac{2\alpha}{5(2\mu-2\alpha-\gamma)}+\frac{1}{\left[2\mu-2\alpha+\gamma\right]\left[Bds(t)+V(t)\right]}\left[4Eids(t)+Hhp(t)+5V(t)\right] \quad (18)$$

4.4.2 情况 2

假设防御者以概率 s 执行基于签名的 IDS 策略，以（$1-s$）的概率执行基于异常的 IDS 和蜜罐协同工作策略；攻击者以 g 和（$1-g$）的概率执行常规攻击和复杂攻击。

防御者收益函数：

$$U_{DS}=(s)(g)U_{11}(D)+(s)(1-g)U_{21}(D)+(1-s)(g)\left[U_{13}(D)+U_{12}(D)\right]$$
$$+(1-s)(1-g)\left[U_{23}(D)+U_{22}(D)\right] \quad (19)$$

攻击者收益函数：

$$U_{AS}=(s)(g)U_{11}(A)+(s)(1-g)U_{21}(A)+(1-s)(g)\left[U_{13}(A)+U_{12}(A)\right]$$
$$+(1-s)(1-g)\left[U_{23}(A)+U_{22}(A)\right] \quad (20)$$

同样的，为了最大化收益，需对两收益函数求偏导：

$$\frac{\partial U_{DS}}{\partial s}=sg\mu B_{ds}(t)+sg\mu V(t)+sV(t)+g\gamma B_{ds}(t)+g\gamma V(t)$$
$$-sg\gamma B_{ds}(t)-sg\gamma V(t)-s\alpha B_{ds}(t)-s\alpha V(t)+sH_{hp}(t)-g\alpha B_{ds}(t)$$
$$-g\alpha V(t)+sg\alpha B_{ds}(t)+sg\alpha V(t)=0 \quad (21)$$

$$\frac{\partial U_{AS}}{\partial g}=4G_{at}(t)-s\mu G_{at}(t)+s\alpha G_{at}(t)-2sG_{at}(t)-g\gamma G_{at}(t)$$
$$-g\alpha G_{at}(t)-sg\mu G_{at}(t)+sg\gamma G_{at}(t)-sg\alpha G_{at}(t)$$
$$-\alpha G_{at}(t)-2R_{at}(t)=0 \quad (22)$$

令导数为 0 求解 s 和 g：

$$s=\frac{\gamma-\alpha}{\gamma-\alpha-\mu} \quad (23)$$

$$g=\frac{\mu-\gamma-2\alpha}{\mu-\gamma-\alpha}-\frac{V(t)+H_{hp}(t)}{(\mu-\gamma-\alpha)(B_{ds}(t)+V(t))} \quad (24)$$

当防御方以（s，1-s）的概率随机选择（基于签名的 IDS 策略，基于异常的 IDS 和蜜罐协同工作策略），攻击方以（g，1-g）的概率随机选择（常规攻击，复杂攻击）时，此混合策略组合便达到了一个稳定状态，即为此博弈的混合策略纳什均衡。

4.4.3 情况 3

假设防御者以概率r执行基于异常的 IDS 策略，以（$1-r$）的概率执行基于签名的 IDS 和蜜罐协同工作策略；攻击者以q和（$1-q$）的概率执行常规攻击和复杂攻击。

防御者收益函数：

$$\begin{aligned}U_{DA}=&(r)(q)U_{12}(D)+(r)(1-q)U_{22}(D)+(1-r)(q)[U_{11}(D)+U_{13}(D)]\\&+(1-r)(1-q)[U_{21}(D)+U_{23}(D)]\end{aligned} \quad (25)$$

攻击者收益函数：

$$\begin{aligned}U_{AA}=&(r)(q)U_{12}(A)+(r)(1-q)U_{22}(A)+(1-r)(q)[U_{11}(A)+U_{13}(A)]\\&+(1-r)(1-q)[U_{21}(A)+U_{23}(A)]\end{aligned} \quad (26)$$

求两收益函数对概率r或q的偏导：

$$\begin{aligned}\frac{\partial U_{DA}}{\partial r}=&r\alpha B_{ds}(t)-rV(t)+r\alpha V(t)-rq\alpha B_{ds}(t)-rq\alpha V(t)+r\mu B_{ds}(t)\\&-2qV(t)-q\gamma B_{ds}(t)+q\gamma V(t)-qH_{hp}(t)-rq\mu B_{ds}(t)-rq\mu V(t)\\&-rq\gamma B_{ds}(t)-rq\gamma V(t)+rH_{hp}(t)+qE_{ids}(t)+2qV(t)+qH_{hp}(t)=0\end{aligned} \quad (27)$$

$$\begin{aligned}\frac{\partial U_{AA}}{\partial q}=&rG_{at}(t)-r\alpha G_{at}(t)-rR_{at}(t)+rq\alpha G_{at}(t)-\mu qG_{at}(t)\\&-q\alpha G_{at}(t)+rq\mu G_{at}(t)+rq\gamma G_{at}(t)+2G_{at}(t)-2R_{at}(t)\\&-2rG_{at}(t)+2rR_{at}(t)=0\end{aligned} \quad (28)$$

令导数为 0 求得r和q：

$$r=\frac{\mu+\alpha}{\alpha+\mu+\gamma} \quad (29)$$

$$q=\frac{\mu+\gamma}{\mu+\gamma+\alpha}+\frac{V(t)+H_{hp}(t)}{(\mu+\gamma+\alpha)(B_{ds}(t)+V(t))} \quad (30)$$

当防御方以（r，1-r）的概率随机选择（基于异常的 IDS 策略，基于签名

的 IDS 和蜜罐协同工作策略），攻击方以（q，1-q）的概率随机选择（常规攻击，复杂攻击）时，此混合策略组合便达到了一个稳定状态，即为此博弈的混合策略纳什均衡。

4.4.4 情况 4

假设防御者以概率 x 执行蜜罐防御策略，以（$1-x$）的概率执行基于签名的 IDS 和基于异常的 IDS 协同工作策略；攻击者以 y 和（$1-y$）的概率执行常规攻击和复杂攻击。

防御者收益函数：

$$\begin{aligned}U_{DH}=&(x)(y)U_{13}(D)+(x)(1-y)U_{23}(D)+(1-x)(y)\left[U_{11}(D)+U_{12}(D)\right]\\&+(1-x)(1-y)\left[U_{21}(D)+U_{22}(D)\right]\end{aligned}\tag{31}$$

攻击者收益函数：

$$\begin{aligned}U_{AH}=&(x)(y)U_{13}(A)+(x)(1-y)U_{23}(A)+(1-x)(y)\left[U_{11}(A)+U_{12}(A)\right]\\&+(1-x)(1-y)\left[U_{21}(A)+U_{22}(A)\right]\end{aligned}\tag{32}$$

求两收益函数对概率 x 或 y 的偏导：

$$\begin{aligned}\frac{\partial U_{DH}}{\partial x}=&xy\gamma B_{ds}(t)+xy\gamma V(t)-xH_{hp}(t)-xV(t)-xy\mu B_{ds}(t)-xy\mu V(t)\\&-x\alpha B_{ds}(t)+2xV(t)-x\alpha V(t)+2xE_{ids}(t)+xy\alpha B_{ds}(t)+xy\alpha V(t)=0\end{aligned}\tag{33}$$

$$\begin{aligned}\frac{\partial U_{AH}}{\partial y}=&xy\gamma G_{at}(t)+xG_{at}(t)-xR_{at}(t)-\mu yG_{at}(t)+xy\mu G_{at}(t)\\&+2G_{at}(t)-2R_{at}(t)-\alpha G_{at}(t)-2xG_{at}(t)+2xR_{at}(t)+x\alpha G_{at}(t)\\&+x\alpha G_{at}(t)+y\alpha G_{at}(t)-xy\alpha G_{at}(t)=0\end{aligned}\tag{34}$$

令偏导数等于 0 求解 x 和 y：

$$x=\frac{\mu-\alpha}{\mu-\gamma-\alpha}\tag{35}$$

$$y=\frac{\gamma-\mu-2\alpha}{\gamma-\mu-\alpha}+\frac{V(t)+H_{hp}(t)-2E_{ids}(t)}{(\gamma-\mu-\alpha)\left(B_{ds}(t)+V(t)\right)}\tag{36}$$

当防御方以（x，$1-x$）的概率随机选择（蜜罐防御策略，基于签名的 IDS 和基于异常的 IDS 协同工作策略），攻击方以（y，$1-y$）的概率随机选择（常规攻击，复杂攻击）时，此混合策略组合便达到了一个稳定状态，即为此博弈的混合策略纳什均衡。

4.4.5 情况 5

假设防御者以概率a执行基于签名的 IDS 策略，以（$1-a$）的概率执行基于异常的 IDS 策略；攻击者以b和（$1-b$）的概率执行常规攻击和复杂攻击。

防御者收益函数：

$$U_{Dsa}=(a)(b)U_{11}(D)+(a)(1-b)U_{21}(D)+(1-a)(b)U_{12}(D)+(1-a)(1-b)U_{22}(D) \quad \textbf{(37)}$$

攻击者收益函数：

$$U_{Asa}=(a)(b)U_{11}(A)+(a)(1-b)U_{21}(A)+(1-a)(b)U_{12}(A)+(1-a)(1-b)U_{22}(A) \quad \textbf{(38)}$$

求两收益函数对概率a或b的偏导：

$$\begin{aligned}&\frac{\partial U_{Dsa}}{\partial a}=ab\mu B_{ds}(t)+ab\alpha B_{ds}(t)+ab\mu V(t)+ab\alpha V(t)\\&-a\alpha B_{ds}(t)-a\alpha V(t)-b\alpha B_{ds}(t)-b\alpha V(t)=0\end{aligned} \quad \textbf{(39)}$$

$$\frac{\partial U_{Asa}}{\partial b}=-ab\mu G_{at}(t)+1-\alpha G_{at}(t)-R_{at}(t)+a\alpha G_{at}(t)+b\alpha G_{at}(t)-ab\alpha G_{at}(t)=0 \quad \textbf{(40)}$$

令偏导数等于 0 求解a和b：

$$a=\frac{\alpha}{\mu+\alpha} \quad \textbf{（41）}$$

$$b=\frac{\alpha}{\mu+\alpha} \quad \textbf{（42）}$$

当防御方以（a，$1-a$）的概率随机选择（基于签名的 IDS 策略，基于异常的 IDS 策略），攻击方以（b，$1-b$）的概率随机选择（常规攻击，复杂攻击）时，此混合策略组合便达到了一个稳定状态，即为此博弈的混合策略纳什均衡。

4.4.6 情况 6

假设防御者以概率j执行基于签名的 IDS 策略，以（$1-j$）的概率执行基于蜜罐的防御策略；攻击者以k和（$1-k$）的概率执行常规攻击和复杂攻击。

防御者收益函数：

$$U_{Dsh}=(j)(k)U_{11}(D)+(j)(1-k)U_{21}(D)+(1-j)(k)U_{13}(D)+(1-j)(1-k)U_{23}(D) \quad \textbf{(43)}$$

攻击者收益函数：

$$U_{Ash}=(j)(k)U_{11}(A)+(j)(1-k)U_{21}(A)+(1-j)(k)U_{13}(A)+(1-j)(1-k)U_{23}(A) \quad \textbf{(44)}$$

求两收益函数对概率j或k的偏导：

$$\begin{aligned}&\frac{\partial U_{Dsh}}{\partial j}=jk\mu B_{ds}(t)+jk\alpha B_{ds}(t)+k\gamma B_{ds}(t)+k\gamma V(t)-jk\gamma B_{ds}(t)\\&-jk\gamma V(t)-H_{hp}(t)-V(t)+jH_{hp}(t)-jE_{ids}(t)=0\end{aligned} \quad \textbf{(45)}$$

$$\frac{\partial U_{Ash}}{\partial k} = -jk\mu G_{at}(t) - k\gamma G_{at}(t) - jkG_{at}(t) + jk\alpha G_{at}(t) + jkR_{at}(t) + G_{at}(t) - R_{at}(t) + jkG_{at}(t) - jkR_{at}(t) = 0 \quad \textbf{(46)}$$

令偏导数等于 0 求解 j 和 k：

$$j = \frac{\gamma}{\gamma - \mu} \quad \textbf{（47）}$$

$$k = \frac{E_{ids}(t) - H_{hp}(t)}{\mu - \gamma} \quad \textbf{（48）}$$

4.4.7 情况 7

假设防御者以概率 u 执行基于异常的 IDS 策略，以（$1-u$）的概率执行蜜罐防御策略；攻击者以 v 和（$1-v$）的概率执行常规攻击和复杂攻击。

防御者收益函数：

$$U_{Dah} = (u)(v)U_{12}(D) + (u)(1-v)U_{22}(D) + (1-u)(v)U_{13}(D) + (1-u)(1-v)U_{23}(D) \quad \textbf{(49)}$$

攻击者收益函数：

$$U_{Aah} = (u)(v)U_{12}(A) + (u)(1-v)U_{22}(A) + (1-u)(v)U_{13}(A) + (1-u)(1-v)U_{23}(A) \quad \textbf{(50)}$$

求两收益函数对概率 u 或 v 的偏导：

$$\frac{\partial U_{Dah}}{\partial u} = v\gamma B_{ds}(t) + v\gamma V(t) - uv\gamma B_{ds}(t) - uv\alpha V(t) + u\alpha B_{ds}(t) - u\alpha V(t) - uv\alpha B_{ds}(t) - uv\alpha V(t) - H_{hp}(t) - V(t) = 0 \quad \textbf{(51)}$$

$$\frac{\partial U_{Dah}}{\partial v} = u\alpha G_{at}(t) + uv\alpha G_{at}(t) - u\gamma G_{at}(t) + uv\gamma G_{at}(t) + G_{at}(t) - R_{at}(t) = 0 \quad \textbf{(52)}$$

令偏导数等于 0 求解 u 和 v：

$$u = \frac{\gamma}{\gamma + \alpha} \quad \textbf{（53）}$$

$$v = \frac{\alpha}{\alpha + \gamma} \quad \textbf{（54）}$$

当防御方以（u，$1-u$）的概率随机选择（基于异常的 IDS 策略，蜜罐防御策略），攻击方以（v，$1-v$）的概率随机选择（常规攻击，复杂攻击）时，此混合策略组合便达到了一个稳定状态，即为此博弈的混合策略纳什均衡。

除以上七种情况外，还可能存在防御方只有三种防御策略中的一种处于工作状态，且防御方处于休眠状态，但攻击方总是会选择攻击，所以这种情况下将会对云服务安全造成巨大的威胁。因此，本文从以上七种情况中找到稳定的解决方

案并计算了纳什均衡。通过博弈模型的分析将有助于检测系统以有效的方式保护云服务器等云端设备和数据的安全。

五、实验

5.1 实验环境

Windows10，python=3.10.0，您可以通过 pip install -r requirements.txt(文件在我们所给的代码链接中)安装其他依赖项。

5.2 实验设置

所提出的算法已与收益函数和概率一起设置。表 2 中讨论了模拟所考虑的参数。

表 2 仿真参数

描述	范围
E_{ids}	[0,0.99]
H_{hp}	[0,0.99]
B_{ds}	$\{-5,0,5\}$
V	[1,5]
R_{at}	[0,0.99]
G_{at}	$\{-5,0,5\}$
μ	[0,0.99]
α	[0,0.99]
γ	[0,0.99]

防御系统的检测率（μ、α、γ）取值范围为 0 到 0.99（即 0%－100%）。防御者和攻击者的增益被取为-5、0 或 5。博弈方要么输掉并获得-5，要么获胜并获得 5，要么保持静止并获得 0 增益。资产的价值范围为 1 到 5。该值应等于或小于收益。否则，防御资产就没有意义，因为防御者获得的收益将小于资产的价值。

5.3 实验结果分析

我们的仿真实验运行 175 秒以捕获一个实例，并已在情况 2,3,4,5,6,7 上进行了仿真测试（情况 1 和情况 6 无法达到纳什均衡）。图 2 中的趋势表明，情况 2 对于攻击者非常有效。在情况 2 中防守方的收益高于攻击方，这意味着防守方赢得了比赛。因此，对于这个特定情况，防御系统将自动启动基于签名的 IDS 策略或基于异常的 IDS 和蜜罐协同工作。同样，对于其他实例，GTM-CSec 模型

将计算收益并启动最佳的策略。

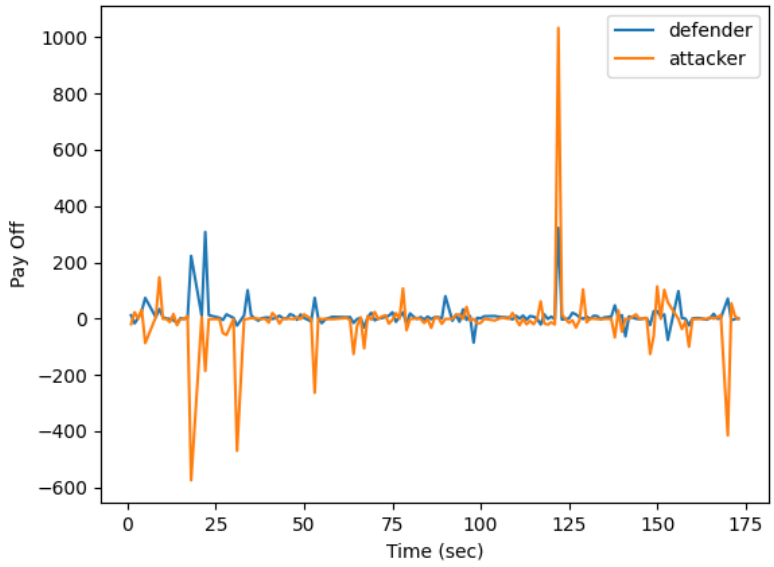

图 2 情况 2 防御者和攻击者的收益

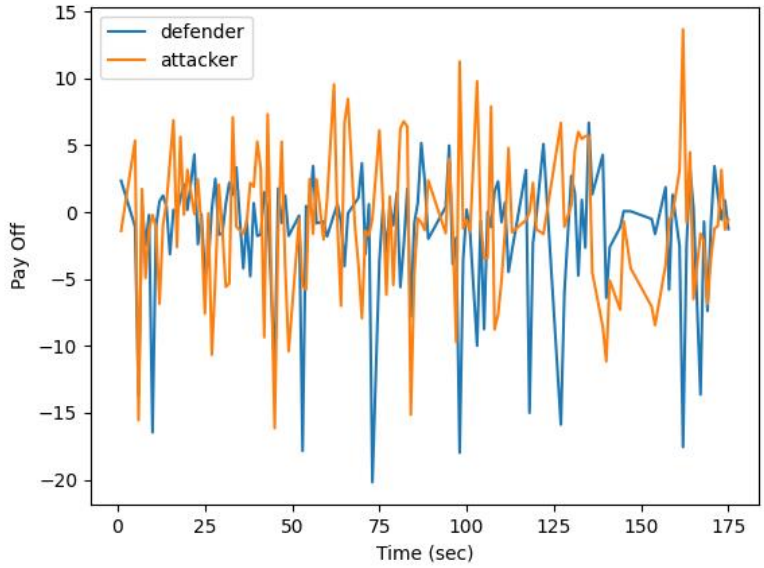

图 3 情况 3 防御者和攻击者的收益

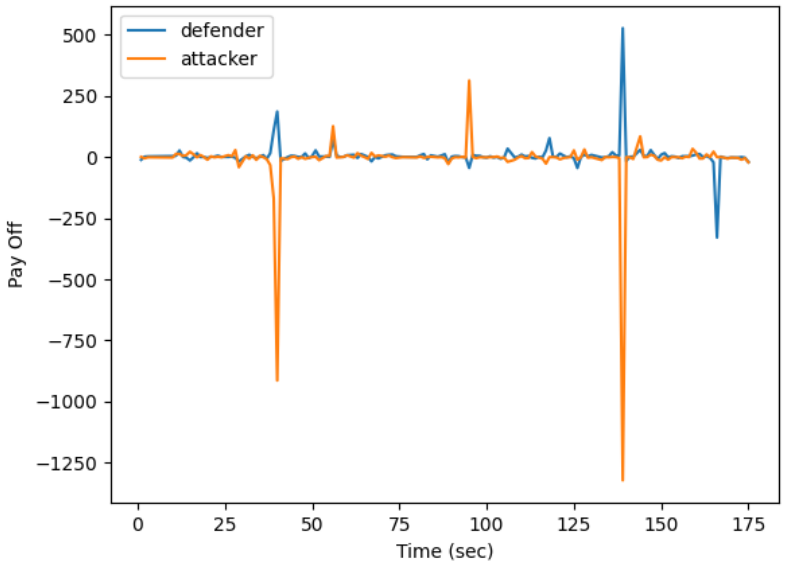

图 4 情况 4 防御者和攻击者的收益

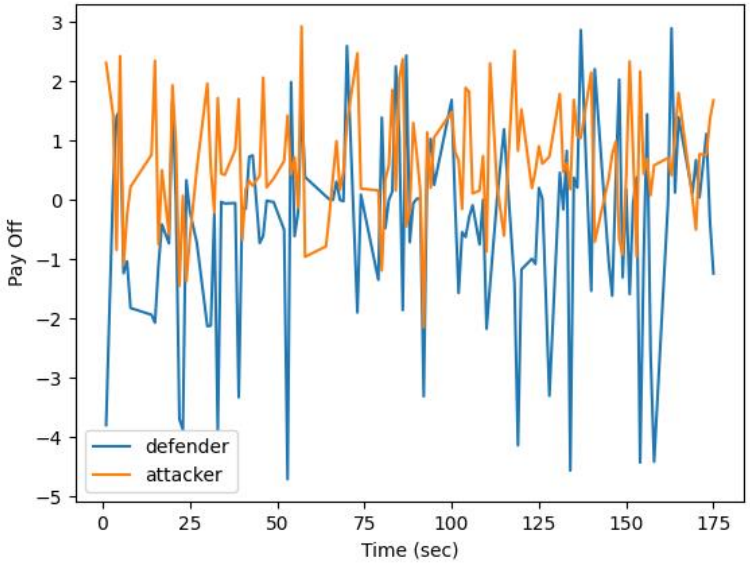

图 5 情况 5 防御者和攻击者的收益

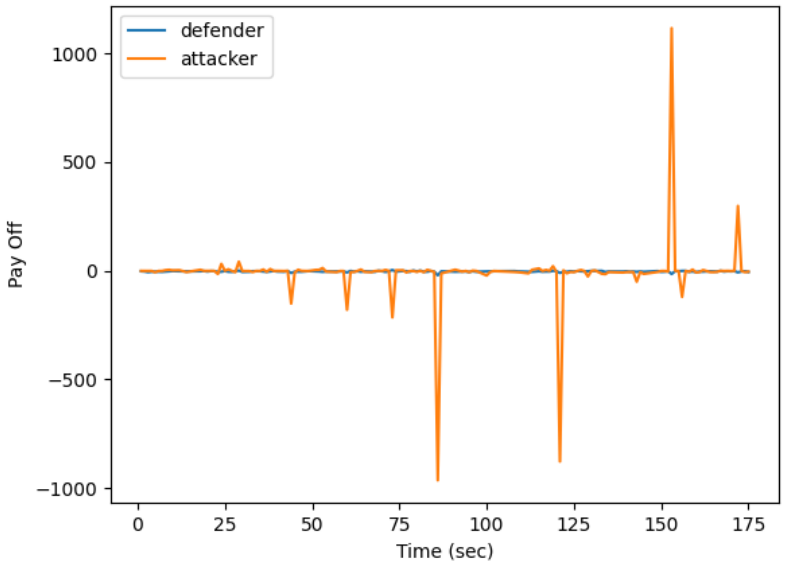

图 6 情况 6 防御者和攻击者的收益

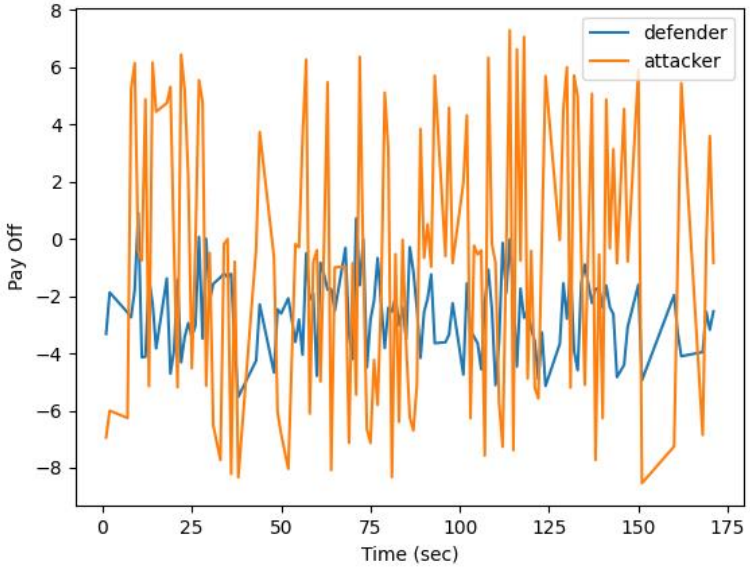

图 7 情况 7 防御者和攻击者的收益

六、结论

为了解决云安全问题，本文提出了一种非合作博弈模型 (GTM-CSec)，并在 Python 环境中实现了仿真实验，并在其中说明了攻击防御场景。攻击者有两种策略即简单常规攻击和复杂攻击。同样，防御者也有三种策略即基于签名、基于异常和基于蜜罐的检测方法。博弈模型根据场景寻找纯策略或混合策略纳什均衡。本文第四部分中针对 1-7 每种情况计算了混合策略纳什均衡。最后的仿真结果表

明，本文所提出的模型对于防御攻击者的攻击是非常有效的。该模型没有同时使用所有三个检测模块，而是选择最佳的攻击检测模块。这可以减少防御系统的能耗，并能够最有效、最智能地应对攻击。另外，本文的模型存在两个限制，一是是该模型基于一些假设，例如基于签名的 IDS 和基于异常的 IDS 在给定时间内消耗相同数量的能量；在这个博弈模型中，双方的行为都是理性的。另一个限制是每个参数的初始化。一旦实例开始，建议的模型就开始实时计算收益。因此，在实际系统中实现该模型时，初始值是已知的，并且可以通过这些值来初始化模型。GTM-CSec 模型是一个独立的模块，因此，通过将博弈论与现有的 IDS 和蜜罐相结合，即可以在实际系统中轻松实现，而无需对现有 IDS 或蜜罐进行更改。

七、参考文献

[1] Komal Singh Gill, Sharad Saxena, Anju Sharma,GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot, Computers & Security,Volume 92,2020,101732.

[2] Calyam, P. , Rajagopalan, S. , Seetharam, S. , Selvadhurai, A. , Salah, K. , Ramnath, R. ,2014. Vdc-analyst: design and verification of virtual desktop cloud resource al-locations. Comput. Netw. 68, 110–122 .

[3] Gartner. Gartner survey says cloud computing remains top emerging business risk.2018.

[4] Han, L. , Zhou, M. , Jia, W. , Dalil, Z. , Xu, X. , 2019. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. Inf. Sci. 476, 491–504 .

[5] Xiao, L. , Xu, D. , Mandayam, N.B. , Poor, H.V. , 2018. Attacker-centric view of a detec-tion game against advanced persistent threats. IEEE Trans. Mobile Comput. 17,2512–2523 .

八、仿真实验代码

代码链接：https://github.com/ZhenWusi/Game-Theory-Course-Project

（此链接包含了仿真实验的使用方法以及源码，请老师查看！）