基于威胁情报的网络安全态势感知模型

张红斌[1,2]，尹彦[1]，赵冬梅[2]，刘滨[3,4]

（1. 河北科技大学信息科学与工程学院，河北 石家庄 050018；2. 河北师范大学河北省网络与信息安全重点实验室，河北 石家庄 050024；
3. 河北科技大学经济管理学院，河北 石家庄 050018；4. 河北科技大学大数据与社会计算研究中心，河北 石家庄 050018）

摘 要：为了解决现实环境中网络规模日益扩大导致网络攻击持续高发的现状，将威胁情报应用到态势感知，构建基于随机博弈的态势感知模型。将外源威胁情报与系统内部安全事件之间的相似度进行比较，对目标系统进行威胁察觉，根据系统内部的威胁信息生成内源威胁情报；在此过程中，利用博弈论的思想量化系统当前的网络安全态势，评估网络的安全状况，最终实现对网络安全态势的预测。实验结果表明，基于威胁情报的网络安全态势感知模型能正确地反映网络安全状态的变化，对攻击行为进行准确的预测。

关键词：威胁情报；态势感知；网络安全；博弈论；纳什均衡

中图分类号：TP393.08

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021106

Network security situational awareness model based on threat intelligence

ZHANG Hongbin[1,2], YIN Yan[1], ZHAO Dongmei[2], LIU Bin[3,4]

1. School of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050018, China
2. Hebei Key Laboratory of Network and Information Security, Hebei Normal University, Shijiazhuang 050024, China
3. School of Economics and Management, Hebei University of Science and Technology, Shijiazhuang 050018, China
4. Research Center of Big Data and Social Computing, Hebei University of Science and Technology, Shijiazhuang 050018, China

Abstract: In order to deal with the problems that the increasing scale of the network in the real environment leads to the continuous high incidence of network attacks, the threat intelligence was applied to situational awareness, and the situational awareness model based on random game was constructed. Threat perception of the target system was performed by comparing the similarity between the exogenous threat intelligence and the internal security events of the system. At the same time, internal threat intelligence was generated based on the threat information inside the system. In this process, game theory was used to quantify the current network security situation of the system, evaluate the security status of the network. Finally, the prediction of the network security situation was realized. The experimental results show that the network security situation awareness method based on threat intelligence can reflect the changes in the network security situation and predict attack behaviors accurately.

Keywords: threat intelligence, situational awareness, network security, game theory, Nash equilibrium

收稿日期：2020−11−13；**修回日期**：2021−04−09

基金项目：国家自然科学基金资助项目（No.61672206, No.61572170）；河北省省级科技计划基金资助项目（No.18210109D, No.20310701D, No.20310802D）；河北省高层次人才基金资助项目（No.A2016002015）；石家庄市科学技术研究与发展计划基金资助项目（No.19SCX01006, No.191130591A）

Foundation Items: The National Natural Science Foundation of China (No.61672206, No.61572170), S&T Program of Hebei (No.18210109D, No.20310701D, No.20310802D), High-Level Talents Subsidy Project in Hebei Province (No.A2016002015), S&T Research and Development Program of Shijiazhuang (No.19SCX01006, No.191130591A)

1　引言

随着网络规模和用户数量的不断增加，网络朝着大规模、多业务、大数据化的方向发展，网络的体系结构也随之日趋复杂化。在这种背景下，计算机病毒、恶意软件、信息泄露等网络攻击越来越严重，多层次的安全威胁和风险也在持续地增加。高级持续威胁（APT, advanced persistent threat）成为目前网络攻击的新趋势[1]，尤其是 APT 使用高级的攻击手段对某一指定目标进行长期、持续的网络攻击，具有高度的隐蔽性和危害性[2]。近年来，网络威胁情报（CTI, cyber threat intelligence）的出现为态势感知的研究带来了新思路。CTI 描述了攻击行为，提供了网络攻击的上下文数据，并指导了网络攻击和防御，利用威胁情报收集大量数据，通过有效的数据共享和确保信息交换的安全和质量，分析恶意行为，可发现和预防 APT[3]。

然而，目前对于 CTI 的研究仍处于初始阶段，相关研究成果较少，在使用 CTI 进行态势感知研究方面，如何合理规范地使用威胁情报也是亟待解决的关键问题。针对这一问题，本文提出了一种基于威胁情报的网络安全态势感知模型，对网络资产状态、风险状态、日志警告进行态势要素采集，将采集到的数据信息在外源威胁情报指导下进行数据筛选、清洗以及关联分析，通过攻防之间的博弈过程对处理后的数据进行态势量化及预测。在此过程中，利用外源威胁情报指导内源威胁信息，并与态势感知预测结果对比分析后，生成内源威胁情报。

2　相关工作

态势感知是指在特定的时间和空间内提取系统的要素，理解其含义并预测其可能产生的影响。Endsley[4]将态势感知分为 3 个层面：态势要素提取、态势理解、态势投射。之后 Bass[5]提出了网络态势感知的概念，即在大型网络环境中，获取、理解、评估和显示可能导致网络状态发生变化的要素，并预测未来的发展趋势。

在态势感知模型的研究方面，文献[6]针对物联网防御复杂的问题，提出了基于随机 C-Petri 网的安全态势感知博弈模型，动态地考虑攻防两者的对抗行为，发现潜在的攻击行为，做出有效的防御；但在具有大量 IoT 节点的复杂网络环境下，该模型的计算面临很大的困难，还需引入云计算的方法降低计算复杂性。文献[7]提出了一种基于随机博弈的网络安全态势评估模型，综合分析了攻击方、防御方和环境信息三者对安全态势的影响；然而在考虑攻防双方策略选择时仅考虑简单的策略集合，而在真实的攻击场景中策略选择要复杂得多。文献[8]提出了基于拓扑漏洞分析的态势感知模型，通过网络安全态势要素的获取、分析，计算网络安全态势值，实现态势感知；但当网络环境更改时，它需要再次对环境建模，不能很好地适应网络更改，还需建立模型参数自适应理解机制。文献[9]针对电子渗透 APT 攻击提出了马尔可夫多阶段可转移信念模型，将杀伤链模型与攻击树结合，利用冲突作为识别悖论的指标，能够为复杂的多阶段攻击进行态势感知；但该模型在选取最有效的方式优化资源分配以及改善决策制定方面也需要进行改进。

威胁情报主要是利用大数据的收集方法获取，能够提供最全、最新的安全事件数据，极大提高了网络安全态势感知工作中对新型和高级危险的察觉能力。文献[10]针对 APT 攻击链进行研究，选取域名系统（DNS, domain name system）流量作为 APT 整体检测的原始数据，采用多种不同检测特征，结合最新的威胁情报和大数据技术，对 APT 攻击检测具有一定的意义。文献[11]以威胁情报为切入点，设计安全威胁情报共享系统，通过第三方共享的威胁情报数据对电网安全的安全态势进行评估，并及时发现异常行为，利用威胁情报实现入侵意图识别，大大提升了系统安全态势感知的能力。威胁情报具有强大的更新能力，通过威胁情报的共享技术，情报库不断更新，因此威胁情报的共享技术是实现攻击溯源的重要手段。文献[12]为实现有效的攻击溯源，基于 STIX 提出了一种精简模式的威胁情报共享利用框架，以有关 C2 信息为例描述了威胁情报的共享利用表达方式，实验结果表明利用威胁情报进行攻击溯源具有实用性。

通过对上述文献进行分析可知，威胁情报在提高网络安全态势感知的准确性方面具有很大的影响，因此本文提出基于 CTI 和攻防博弈的态势感知模型，通过攻防之间的博弈过程量化网络态势，结合 CTI 和纳什均衡进行网络安全态势预测。

3　态势感知模型基础

本文提出的基于威胁情报的态势感知模型分

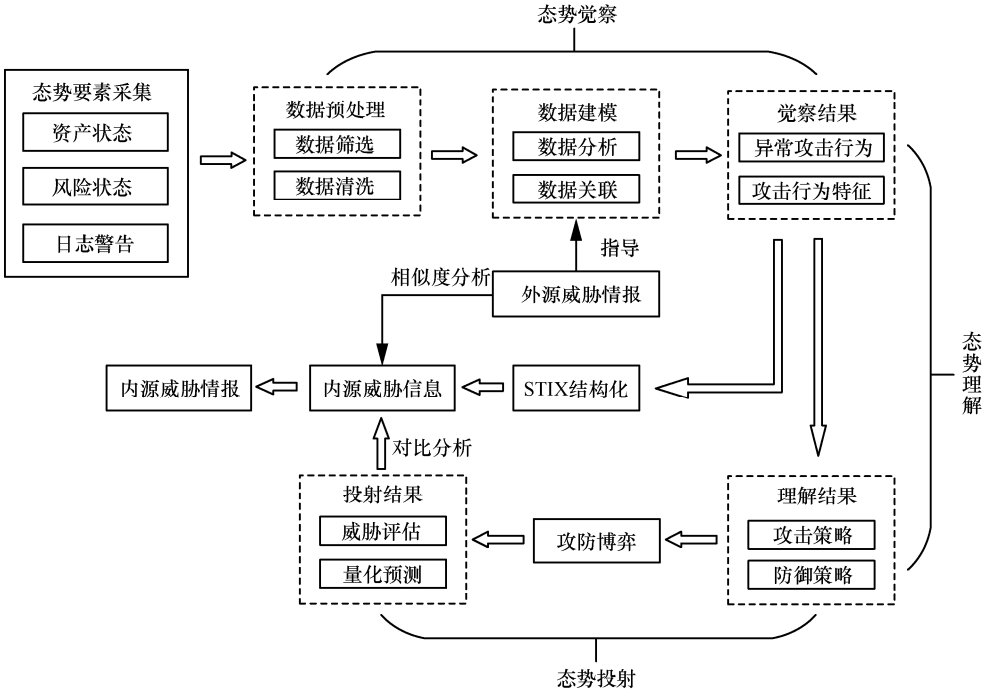


图 1　态势感知模型

为 3 个部分：态势觉察、态势理解和态势投射，如图 1 所示。

1) 态势觉察的主要目的是通过对采集到的要素（主要包含目标网络的资产状态信息、风险状态信息及日志警告信息）在外源威胁情报的指导下进行数据预处理及关联分析，找出系统中的异常攻击行为及其特征，确定攻击的意图、方式以及产生的影响，然后对攻击信息进行 STIX 结构化，生成具有威胁性的内源威胁信息。

2) 态势理解是在态势觉察的基础上对攻击行为进行理解，确定攻击者的攻击策略，针对攻击策略选取合适的防御策略。

3) 态势投射在前两步的基础上分析攻击行为对网络中对象的威胁情况，引入攻防博弈的思想，对网络整体的安全态势进行量化及预测，将预测结果与之后网络态势感知的结果进行对比分析。若结果一致，说明通过该方法进行预测分析是可行的，同时将态势觉察部分生成的内源威胁信息定义为系统内源威胁情报。生成的内源威胁情报通过威胁情报的共享技术，能够提高整体网络空间的安全性。

本文对一般态势感知模型的改进主要表现为两点，一方面在态势觉察部分，通过外源威胁情报的指导，对系统内部的安全事件进行分析和理解，觉察系统内部的威胁。经过态势觉察生成的内源威胁信息可以准确地发现攻击，并能对攻击的意图、方式及攻击进行精准描述。另一方面在态势投射部分，通过攻击者、防御者之间的博弈过程，定义相关变量，并对目标系统的安全态势进行量化，从而评估网络的安全状态；通过纳什均衡存在定理，对目标网络的未来安全态势进行预测，预测攻击者可能采取的攻击策略，促使防御者提前采取合适的措施进行防御，使网络免受攻击。

4　基于相似度的态势觉察方法

本节介绍了威胁情报的定义、表达格式等相关概念，提出基于外源威胁情报与安全事件相似度比较的威胁信息察觉方法，通过比较两者之间的相似度，判断内部安全事件是否具有威胁性，发现系统内部的威胁信息。最后将态势预测结果对内源威胁信息进行反馈，确定内源威胁情报。

4.1　威胁情报的定义

Gartner 对威胁情报的定义为：威胁情报是关于 IT、信息资产面临现有或酝酿中的威胁的证据性知识，包括可实施上下文、机制、标示、含义和能够执行的建议，这些知识可以为威胁的响应、处理决策提供技术支持[13]。本文根据威胁情报的来源将其分为内源威胁情报和外源威胁情报，具体内容如以

下定义所示。

定义 1　外源威胁情报（ECTI, external cyber threat intelligence）。通常源于情报提供者提供的开源威胁情报（OSINT, open source intelligence），如互联网公开的漏洞信息、安全事件信息、网络安全预警信息等。

定义 2　内源威胁情报（ICTI, internal cyber threat intelligence）。企业或机构产生的威胁情报数据，用于保护内部信息资产和业务流程。通常是目标系统受到攻击后，通过相应的安全信息与时间管理入侵检测系统等安全设备获取的相关数据集，进行数据分析、融合后，与态势感知的结果进行对比分析证明正确性，最后生成系统内源威胁情报。

在进行威胁情报数据的预处理前，有必要统一内外源威胁情报的格式，本文采用结构化威胁信息表达式 STIX[14]作为威胁情报的格式。STIX 提供一种以标准 XML 为基础的语法，用于描述威胁情报的详细信息、内容和威胁情报各个方面的特点。本文首先对 ECTI 进行 STIX2.0 结构化，选取威胁指标（Indicator）、攻击模式（Attack Pattern）、工具（Tool）、漏洞（Vulnerability）、可观测数据（Observed Data）这 5 类对象作为分析要素，其中每个对象包含了若干的威胁属性，如表 1 所示；然后将这些对象及属性作为 ICTI 的收集依据，发现系统内部的攻击行为。威胁对象的具体描述如下。

表 1　　**对象及其属性**

对象	属性	相关描述
Indicator	Name	用于标识威胁指标的名称
	Labels	用于指定指标的类型
	Pattern	指示器的检测模式
Attack Pattern	Description	描述攻击模式的详细信息、上下文
	Name	用于标识攻击模式的名称
Tool	Labels	所描述的工具类型
	Name	用于标识工具的名称
Vulnerability	CVE-id	漏洞标识符
Observed Data	Objects	观测到的数据
	First_observed	观察数据的时间窗口开始
	Last_observed	观察数据的时间窗口结束

1) Indicator：威胁的指标点，包含攻击时间、工具、恶意软件所在的僵尸网络信息等特征参数。

2) Attack Pattern：描述攻击者试图破坏目标的方式，实际是 TTP（tactic、technique and procedure）类型，通常使用通用攻击模式枚举和分类（CAPEC）标准来结构化描述攻击模式。

3) Tool：威胁者可以用来执行攻击的合法软件。

4) Vulnerability：软件中的错误，黑客可以直接利用该错误来访问系统或网络。

5) Observed Data：在系统和网络上观察到的传输信息，例如 IP 地址等。

4.2　针对威胁的态势觉察方法

威胁觉察过程为通过对目标系统攻击数据的处理，明确攻击的目的、攻击工具及产生的影响等；利用 STIX2.0 提取上述相关对象及威胁属性，生成安全事件（SI, security incident）；对安全事件进行权重的计算，得到具有威胁价值的信息，将其定义为内源威胁信息。图 2 描述了相似度分析的过程。

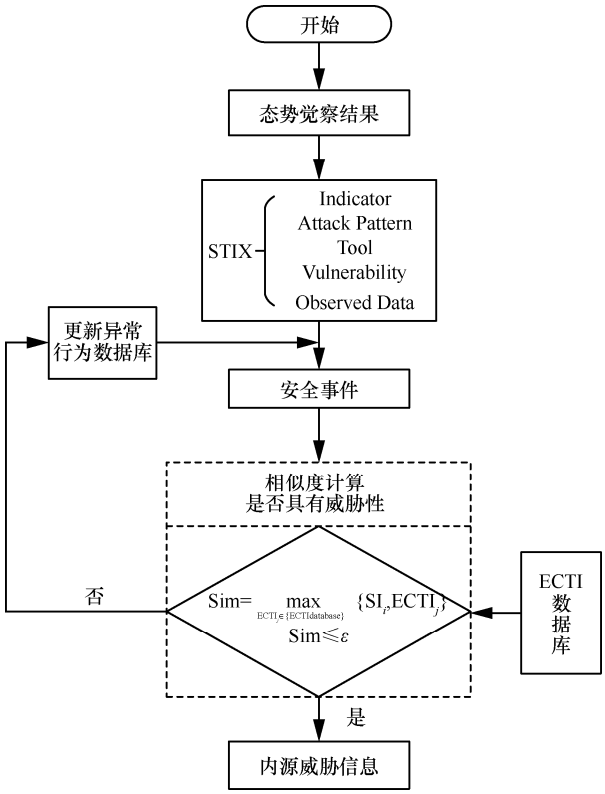


图 2　相似度分析的过程

1) 获取相关对象及属性

安全事件 SI 是一个 5 元组，对应上述的 5 个对象，每个对象都代表一个分系统，每个分系统下又有若干的威胁属性，即

$$SI = (Ind, AP, Tool, Vul, OD)$$

其中，每个对象的权重用 ω_i 表示，所有对象的权重

值满足 $\sum_{i=1}^{5}\omega_i=1$，每个对象下威胁属性的权重用 ω_{ij} 表示，权重值满足 $\sum_{i=1,j=1}^{i,j}\omega_{ij}=1$。

2) 权重计算

开源的威胁情报库过于庞大，系统内部 SI 与其完全匹配成功的可能性极低，因此，使用与安全事件相同类型的威胁情报来分析后续的安全事件。本文利用攻击方式的 CAPEC-id 进行 ECTI 的分类，统计每种类型威胁情报中具有 SI 特性的威胁数据。

本文以分系统 Indicator 为例进行描述。对象 Indicator 的 3 个属性在外源威胁情报中出现的次数如表 2 所示，其中，x_{ij} 表示威胁属性在外源威胁情报中出现的次数。

表 2 Indicator 的属性在 ECTI 中出现的次数

属性	出现次数				
	id_1	id_2	id_3	…	id_n
Name	x_{11}	x_{12}	x_{13}	…	x_{1n}
Labels	x_{21}	x_{22}	x_{23}	…	x_{2n}
Pattem	x_{31}	x_{32}	x_{33}	…	x_{3n}

计算 Indicator 分系统中各个属性在 ECTI 中出现的频率，即

$$P_{kj}=\frac{x_{kj}}{\sum_{k=1,j=1}^{k=3,j=n}x_{kj}},j=1,2,3,\cdots,n \tag{1}$$

建立目标对象的相对优越度矩阵 $\boldsymbol{R}_{m\times n}$ 为

$$\boldsymbol{R}_{m\times n}=\begin{bmatrix}r_{11}&r_{12}&r_{13}\\r_{21}&r_{22}&r_{23}\\r_{31}&r_{32}&r_{33}\end{bmatrix} \tag{2}$$

对象的属性出现频次越多，在威胁情报中越具有代表性，利用该属性进行威胁情报生成越能准确反映目标系统的安全状态。根据文献[15]，利用式(3)求取相对优越值 r_{ij}，通过式(4)计算 ECTI 中每个属性的权重 $\omega_{ij}^{'}$。

$$r_{ij}=\frac{p_{ij}-\hat{j}p_{ij}}{\overset{\vee}{j}p_{ij}-\hat{j}p_{ij}} \tag{3}$$

$$\omega_{ij}^{'}=\frac{\sum_{j=1}^{j=n}r_{kj}}{\sum r_{ij}} \tag{4}$$

其中，∧、∨分别表示取小、取大符，即 $\hat{j}p_{ij}$、$\overset{\vee}{j}p_{ij}$ 分别表示目标属性中的最小、最大的概率值。通过上述计算，可以得到对象 Indicator 的权重为 $\omega_1^{'}=(\omega_{11}^{'},\omega_{12}^{'},\omega_{13}^{'})$，同理可求得 SI 中其他元组 $(\mathrm{AP},\mathrm{Tool},\mathrm{Vul},\mathrm{OD})$ 属性权重 $\omega_{ij}^{'}$。

通过对系统内部安全数据的收集、整理，可以得到内部安全事件 SI 中每个元组的权重 ω_i，以及每个元组下属性的权重 ω_{ij}，计算式为

$$\omega_{ij}=\frac{y_{ij}}{\sum_{j=1}^{n}y_{ij}} \tag{5}$$

其中，y_{ij} 表示威胁属性在内部安全事件 SI 中出现的频次，则 $\omega_i=\{\omega_{i1},\omega_{i2},\cdots,\omega_{ij}\}$，$i=1,2,\cdots,5$，$j=1,2,\cdots,n$。

比较 ω_{ij} 与 $\omega_{ij}^{'}$ 之间的差值，差值越小，说明安全事件中这一对象与同类 ECTI 的相似性越大。通过比较可以得到内外源安全数据 Indicator 对象中差值最大的属性，将该差值作为 SI 与 ECTI 中 Indicator 之间的相似度 sim_1，即

$$\mathrm{sim}_1=\max_{\mathrm{ECTI}_j\in\{\mathrm{ECTIdatabase}\}}\{\mathrm{SI}_1,\mathrm{Indicator}\in\mathrm{ECTI}_j\} \tag{6}$$

同理，能够求得 SI 中其余元组与 ECTI 的相似度，选择这些 sim_i 中的最大值作为内部安全事件与外源威胁情报之间的相似度 Sim，即

$$\mathrm{Sim}=\max\{\mathrm{sim}_i\},i=1,2,\cdots,5 \tag{7}$$

设置阈值 ε，当 $\mathrm{Sim}\leqslant\varepsilon$ 时，则该安全事件可以作为目标系统内源的威胁信息；否则，将此安全事件进行存储。

得到系统内源的威胁信息后，对攻防策略建立博弈模型，进行态势预测，得到预测结果，将威胁信息与预测结果进行对比分析，判断是否一致，若一致，将此内源威胁信息定义为 ICTI。图 3 为 ICTI 生成过程，在此过程中 ECTI 指导信息收集，规范了 ICTI 信息的格式。

5 攻防博弈模型

5.1 攻防模型的建立

在网络攻防过程中，攻防双方采取的攻击与防御措施会对整个目标系统网络状态的转移产生影响，使系统的网络状态进行更新，导致攻防双方根据新的网络状态选择新的行动策略，并反复进行该

行为。此过程符合博弈的思想，因此，本文采用随机博弈的思想对网络攻防过程进行建模。

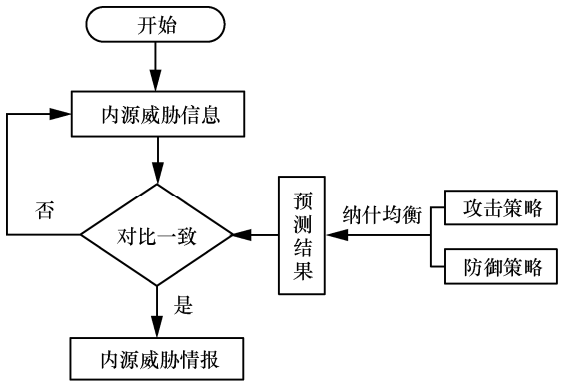


图 3　内源威胁情报生成过程

在攻防博弈中，参与者不论采用何种策略都会产生相应的成本和收益，定义两者之间的差值为效用，利用效用来量化网络安全态势值。假设网络攻防双方收益相等，本文将攻防过程描述为一个非合作零和攻防博弈模型。

网络安全博弈模型定义如下。

定义 3　基于随机博弈的网络安全感知模型（NSAM-SG, network security awareness model-stochastic game）描述了网络攻击与防御行为，包含博弈的参与者、目标网络的安全状态、攻防双方的策略集合、博弈双方的效用函数，即 NSAM-SG = (P, S, T_{a}, T_{d}, U)。

NSAM-SG 各个元组的含义表示如下。

P 表示参与攻防博弈的参与者集合，P_{a} 为攻击者，P_{d} 为防御者，即 $P=(P_{\mathrm{a}},P_{\mathrm{d}})$。

S 表示目标网络的安全状态构成的集合，$S=(S_0,S_1,S_2,\cdots,S_n)$，$S_i$ 表示目标网络在 i（$1\leqslant i\leqslant n$）时刻所处的安全状态。

$T_{\mathrm{a}}=\{T_{\mathrm{a}}^1,T_{\mathrm{a}}^2,T_{\mathrm{a}}^3,\cdots,T_{\mathrm{a}}^i\},i=1,2,3,\cdots,n$，$T_{\mathrm{a}}^i$ 表示在安全状态 S_i 下的攻击策略。

$T_{\mathrm{d}}=\{T_{\mathrm{d}}^1,T_{\mathrm{d}}^2,T_{\mathrm{d}}^3,\cdots,T_{\mathrm{d}}^j\},i=1,2,3,\cdots,m$，$T_{\mathrm{d}}^j$ 表示在安全状态 S_j 下的防御策略。

U 表示博弈双方的效用函数集合，$U=\{U_{\mathrm{a}}^i,U_{\mathrm{d}}^j\}$，$U_{\mathrm{a}}^i$ 表示攻击者在状态 S_i 下的效用函数，U_{d}^j 表示防御者在状态 S_i 下的效用函数。

5.2　态势量化

当攻击方 τ 对目标系统进行攻击后，$U(\tau)_{\mathrm{a}}$、$\mathrm{profit}(\tau)_{\mathrm{a}}$ 和 $\mathrm{cost}(\tau)_{\mathrm{a}}$ 分别表示攻击方的效用、收益和成本，则防御方采取防御措施防御后的效用、收益和成本定义为 $U(\tau)_{\mathrm{d}}$、$\mathrm{profit}(\tau)_{\mathrm{d}}$ 和 $\mathrm{cost}(\tau)_{\mathrm{d}}$。相关定义如下。

1) 攻击方效用。攻击方的效用 $U(\tau)_{\mathrm{a}}$ 等于攻击方的收益与成本的差值，即

$$U(\tau)_{\mathrm{a}}=\mathrm{profit}(\tau)_{\mathrm{a}}-\mathrm{cost}(\tau)_{\mathrm{a}}+\mathrm{cost}(\tau)_{\mathrm{d}} \tag{8}$$

2) 防御方效用。根据博弈双方对立的关系，防御方的效用为

$$U(\tau)_{\mathrm{d}}=\mathrm{profit}(\tau)_{\mathrm{d}}-\mathrm{cost}(\tau)_{\mathrm{d}}+\mathrm{cost}(\tau)_{\mathrm{a}} \tag{9}$$

3) 攻击成本。攻击成本可以理解为与攻击者被发现进行法律制裁的风险有关[16]，事实上，被发现进行法律诉讼的情况很少，因此本文认为攻击成本与其对应威胁情报的威胁度（TL, threat level）成正比，威胁程度越高，攻击成本越大，则

$$\mathrm{cost}(\tau)_{\mathrm{a}}=\mathrm{TL} \tag{10}$$

参考 MIT 林肯实验室对攻击的分类[17]，根据威胁行为的攻击意图，威胁情报可分为 6 类，同种类型的威胁情报具有相同的威胁度，具体分类说明和 TL 值如表 3 所示。

表 3　**威胁情报分类与威胁度**

分类	描述	TL
Root	获取管理员权限	10
User	获取普通用户权限	5
Data	非授权访问或读写数据	3
DoS	拒绝服务攻击	2
Probe	扫描攻击	0.5
Other	其他	—

4) 防御成本。防御成本指攻击发生后，防御方采取防御措施付出的操作代价。结合文献[18]对防御类别的分类，根据外源威胁情报中处置方法（course of action）的复杂程度对防御成本进行分类，可以分为以下 4 个级别。

DC_1：未采取防御措施，操作代价为零。

DC_2：抵御攻击付出的操作成本很小，如对攻击行为进行监测。

DC_3：对攻击行为进行阻止，防御的操作成本较大。

DC_4：修复攻击对系统造成的损害，此时付出的操作成本很大。

对操作代价进行量化，对应的防御成本为 $\mathrm{DC}=(0,4,8,10)$。

5) 攻击方收益。攻击方的收益通常用攻击对网络系统造成的损害来表示，在本文中，攻击收益主要从威胁攻击成功率、利用威胁情报中脆弱性（Vulnerability）产生的危害这 2 个方面进行量化。

根据 CVSS 评级标准，利用 Vulnerability 产生的危害 Impact 为

$$\text{Impact}=\lambda \text{VL}\left[1-\left(1-\text{Con}_{\text{a}}\right)\left(1-\text{Int}_{\text{a}}\right)\left(1-\text{Ava}_{\text{a}}\right)\right] \tag{11}$$

其中，λ 为修正因子，取值为 10.41；VL 为脆弱性利用的难易程度，分为严重（Critical）、高（High）、中（Medium）、低（Low）4 个等级，评分范围如表 4 所示；$\text{CIA}=(\text{Con}_{\text{a}},\text{Int}_{\text{a}},\text{Ava}_{\text{a}})$ 表示该脆弱性对系统造成的机密性、完整性、可用性危害，根据 CVSS 评分标准，$\text{Con}_{\text{a}},\text{Int}_{\text{a}},\text{Ava}_{\text{a}}$ 的取值如表 5 所示。最终可以得到攻击方的收益为

$$\text{profit}(\tau)_{\text{a}}=\beta\text{Impact} \tag{12}$$

其中，β 为攻击成功率，来自系统的历史信息。

表 4 Vulnerability 等级与评分标准

等级	VL
Critical	9.0～10.0
High	7.0～8.9
Medium	4.0～6.9
Low	0～3.9

表 5 CIA 要素取值范围

要素	可选值	分值
$\text{Con}_{\text{a}},\text{Int}_{\text{a}},\text{Ava}_{\text{a}}$	无（None）	0
	低（Low）	0.22
	高（High）	0.56

6) 防御方收益。防御方的收益与防御者采取防御措施后使系统免受的损害有关，在数值上与攻击造成的收益相等，因此，防御收益为

$$\text{profit}(\tau)_{\text{d}}=-\text{profit}(\tau)_{\text{a}} \tag{13}$$

通过上述的量化方法，将式(12)和式(13)代入式(8)中，可以得到攻击方的效用函数$U(\tau)_{\text{a}}$，即

$$U(\tau)_{\text{a}}=\beta\text{Impact}-\text{TL}+\text{DC} \tag{14}$$

同理，可以求得防御方的效用函数$U(\tau)_{\text{d}}$，即

$$U(\tau)_{\text{d}}=-\beta\text{Impact}+\text{TL}-\text{DC} \tag{15}$$

双方的效用函数分别代表了攻防双方采取策略行动的收益程度，根据博弈双方的效用函数，计算得到目标网络的安全态势值 S 为

$$S=U(\tau)_{\text{d}}-U(\tau)_{\text{a}} \tag{16}$$

$|S|$ 的大小反映了目标系统当前网络的安全状态或者危险状态的程度。当 $S>0$ 时，当前网络处于安全状态，$|S|$ 越大，网络越安全。当 $S<0$ 时，当前网络处于危险状态，$|S|$ 越大，网络越危险。

5.3 攻击预测

在博弈中，纳什均衡指参与博弈的任一方选择的策略针对其他人的策略选择都是最优方案。网络攻防的过程中，攻击者与防御者都希望能够以最小的攻击或防御成本，收获最大的利益，在这种情况下，攻防双方会根据彼此的策略选择最佳策略。根据纳什均衡，NSAM-SG 必然存在均衡点。因此，本文利用纳什均衡对攻击行为进行预测。

在攻防进行时，双方采取的策略对彼此来说都是不明确的，因此不存在纯策略的纳什均衡。本文使用混合策略对 NSAM-SG 进行博弈均衡分析。

设攻击者与防御者分别依据概率向量 $\boldsymbol{P}_{\text{a}}=(x_1,x_2,x_3,\cdots,x_m)$、$\boldsymbol{P}_{\text{d}}=(y_1,y_2,y_3,\cdots,y_n)$ 选择攻击策略与防御策略，则攻防双方的混合策略为

$$X=\{x=(x_1,x_2,x_3,\cdots,x_m)\,|\,\sum_{i=1}^{m}x_i=1,x_i\geqslant 0\} \tag{17}$$

$$Y=\{y=(y_1,y_2,y_3,\cdots,y_n)\,|\,\sum_{j=1}^{n}y_j=1,y_j\geqslant 0\} \tag{18}$$

定义攻击者的效益期望为 E_{a}，防御者的效益期望为 E_{d}，即

$$\text{E}_{\text{a}}=\sum_{i=1}^{m}\sum_{j=1}^{n}x_iy_jU_{\text{a}}(T_{\text{a}}^i,T_{\text{d}}^j) \tag{19}$$

$$\text{E}_{\text{d}}=\sum_{i=1}^{m}\sum_{j=1}^{n}x_iy_jU_{\text{d}}(T_{\text{a}}^i,T_{\text{d}}^j) \tag{20}$$

根据博弈均衡定义，在 NSAM-SG 里，混合策略 (x_i^*,y_j^*) 的均衡效用期望 E_{a} 和 E_{d} 具有最优性，且 (x_i^*,y_j^*) 满足如下条件

$$\begin{cases}\forall x_i,\sum_{i=1}^{m}\sum_{j=1}^{n}x_i^*y_j^*U_{\text{a}}(T_{\text{a}}^i,T_{\text{d}}^j)\geqslant\sum_{i=1}^{m}\sum_{j=1}^{n}x_iy_j^*U_{\text{a}}(T_{\text{a}}^i,T_{\text{d}}^j)\\ \forall y_j,\sum_{i=1}^{m}\sum_{j=1}^{n}x_i^*y_j^*U_{\text{a}}(T_{\text{a}}^i,T_{\text{d}}^j)\geqslant\sum_{i=1}^{m}\sum_{j=1}^{n}x_i^*y_jU_{\text{d}}(T_{\text{a}}^i,T_{\text{d}}^j)\\ \sum_{i=1}^{m}x_i=1,x_i\geqslant 0\\ \sum_{j=1}^{n}y_j=1,y_j\geqslant 0\end{cases} \tag{21}$$

其中，混合策略 $x^* = (x_1^*, x_2^*, \cdots, x_m^*)$ 是攻击者最优策略，　$y^* = (y_1^*, y_2^*, \cdots, y_n^*)$ 是防御者最优策略。

6　实验结果与分析

6.1　实验环境

本文实验利用加拿大网络安全研究院提出的 CICIDS2017 入侵检测数据集进行基于相似度生成 ICTI 方法的验证，根据 NSAM-SG 验证利用纳什均衡预测攻击行动方法的有效性与准确性，该数据集拓扑结构如图 4 所示。

由图 4 可以看出，网络结构被划分成 2 个分离的网络，即攻击者网络与受害者网络。该数据集[19]提供了广泛的攻击多样性，包含了良性流量和最新的攻击流量，数据捕获期从 2017 年 7 月 3 日上午开始，到 2017 年 7 月 7 日下午结束，实施的攻击包括暴力 FTP、暴力 SSH、DoS、Heartbleed、Web 攻击、渗透等，具体的攻击种类及时间如表 6 所示。

6.2　威胁觉察

实验选取 CAPEC-24、CAPEC-47、CAPEC-185、CAPEC-122 作为 ECTI，指导内部威胁的觉察。分析该数据集的攻击行为，将其制成具有 STIX2.0 格式的攻击信息，分析该攻击信息与外源威胁情报之间的相似度，判断该信息是否为内源威胁信息。通过实验，得到 SI 分系统 Indicator 相关属性的频次如表 7 所示。

表 6　CICIDS2017 攻击种类及时间

时间	标签
Monday	Benign
Tuesday	FTP-Patator(9:20-10:20), SSH-Patator(14:00-15:00)
Wednesday	DoS Slowloris(9:47-10:10), DoS slowhttptest (10:14-10:35), DoSHulk(10:43-11:00), DoSGoldenEye (11:10-12:23), Heartbleed Attack(15:12-15:23)
Thursday	Web BForce(9:20-10:00), XSS(10:15-10:35), Sql Injection(10:40-10:42), Web and Infiltration Attacks (14:19-15:45)
Friday	Botnet(10:02-11:02), PortScans(13:55-15:23), DDoS (15:57-16:16)

表 7　Indicator 的属性在 ECTI 中出现的频次

属性	出现频次			
	24	47	185	122
Name	2	1	0	0
Labels	9	6	0	8
Pattern	2	3	1	2

建立目标 Indicator 的相对优越度矩阵 $\boldsymbol{R}_1$ 为

$$\boldsymbol{R}_1 = \begin{bmatrix} 1 & 0.49 & 0 & 0 \\ 1 & 0.67 & 0 & 0.69 \\ 0.5 & 1 & 0 & 0.5 \end{bmatrix}$$

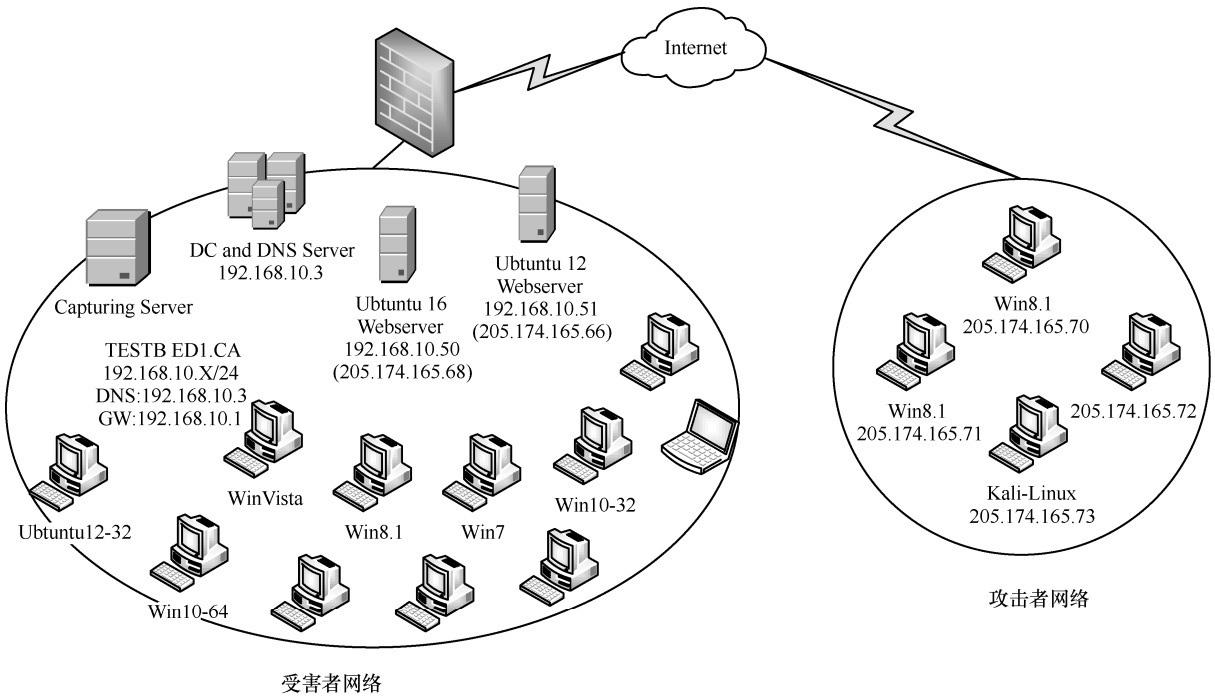


图 4　CICIDS2017 数据集拓扑结构

计算外源威胁情报中 Indicator 的权重 ω_1' 为

$$\omega_1' = (0.25, 0.42, 0.33)$$

同理，求得 ECTI 中其他元组 (AP, Tool, Vul, OD) 属性权重分别为 $\omega_2' = (0.58, 0.42)$，$\omega_3' = (0.33, 0.67)$，$\omega_4' = (1)$，$\omega_5' = (0.35, 0.325, 0.325)$。

计算安全事件 SI 中每个元组的权重为 $\omega_1 = (0.5, 0.33, 0.17)$，$\omega_2 = (0.44, 0.56)$，$\omega_3 = (0.43, 0.57)$，$\omega_4 = (1)$，$\omega_5 = (0.5, 0.25, 0.25)$。得到安全事件与外源威胁情报之间的相似度 $\mathrm{Sim} = 0.25$。根据模糊优选模型物理含义的分析[20]，设置模糊阈值 $\varepsilon = 0.5$，当 $\mathrm{Sim} \leqslant 0.5$ 时，则该安全事件具有威胁价值，作为系统内源的威胁信息，与之后态势预测的结果进行对比分析。

根据 6.4 节的结果可知，攻击者最有可能采取的攻击策略是利用拒绝服务漏洞发起攻击。因此，所有安全事件 SI 中的 Tool、Vulnerability 对象及其属性可以定义为目标系统的内源威胁情报。由此可知，本文提出基于相似度分析的威胁察觉方法可以较准确地发现威胁行为。

6.3 态势评估

本文在林肯实验室的 DARPA2000-LLDoS1.0 数据集上进行对比实验，验证本文提出基于攻防博弈的态势评估的准确性，在 CICIDS2017 入侵检测数据集上验证该方法的普适性。由于实验数据集中仅包含攻击信息，没有防御信息，因此假设防御者未采取防御措施。

1) 准确性的验证

DARPA2000-LLDoS1.0 数据集拓扑结构如图 5 所示，该数据集描述了一个完整的分布式拒绝服务攻击场景，分为 5 个攻击阶段，即扫描、探测、登录、安装 DDoS 软件、发动 DDoS 攻击。

各主机在攻击过程中所占的权重如表 8 所示。

表 8　　主机所占权重

主机	权重
Mill	0.34
Locke	0.18
Pascal	0.18
Hume	0.2
Robin	0.05
www.af.mil	0.05

对目标系统的主机资产进行权重的分配，即 $\mathrm{CIA_M} = (5,5,5)$，$\mathrm{CIA_L} = (1,5,10)$，$\mathrm{CIA_P} = (5,5,10)$，$\mathrm{CIA_H} = (5,5,1)$，$\mathrm{CIA_R} = (5,5,1)$，$\mathrm{CIA_{www}} = (5,5,10)$。各主机在攻击阶段以相同的方式受到攻击，因此各阶段对目标系统资产的攻击影响按照等级划分为 $N = (1,2,3,3,2)$。通过计算，得到整个网络环境的安全态势变化趋势，变化曲线如图 6 所示，此时网络处于危险状态，且安全态势值越大，网络越危险。

从图 6 中可以看出，攻击者在探测阶段对网络的影响小，之后的缓冲区溢出攻击使网络的危险状态进一步加强，当攻击者获取主机的 Root 权限并安装 DDoS 工具后，网络的安全面临进一步的威胁。

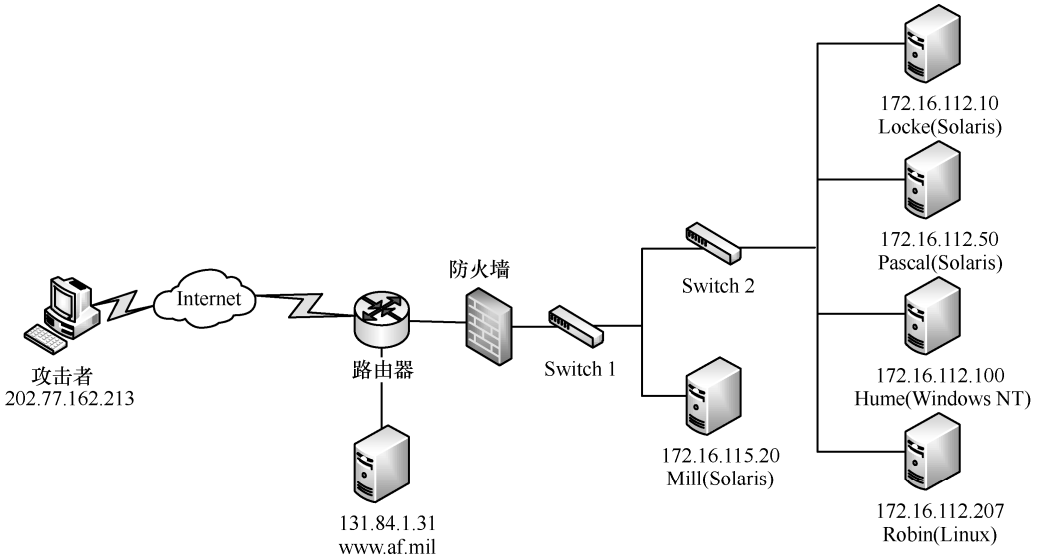


图 5　LLDoS1.0 数据集拓扑结构

攻击者手动启动 DDoS，威胁仍未解除，整个网络的态势值进一步提高。

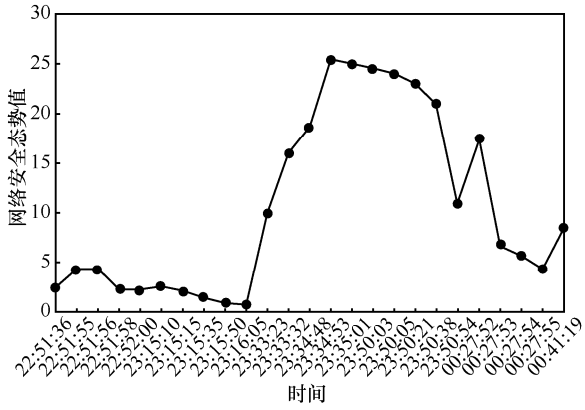


图 6　安全态势曲线

为了探究本文方法的特性，将应用集对分析方法[21]、HMM 方法[22]、层次化分析方法[23]与本文基于攻防博弈的态势评估方法进行比较，对比结果如表 9 所示。

表 9　　与其他方法的比较

评估方法	低风险的灵敏度	高风险的灵敏度	风险值累积	实现复杂度
攻防博弈方法	高	高	无	高
应用集对分析方法	低	低	无	低
HMM 方法	中	低	无	中
层次化分析方法	中	中	有	低

表 9 中，应用集对分析方法的原理融合了多个数据源的信息，对网络安全各要素展开了全面的分析，但在区分危险性不强的探测阶段，该方法的灵敏度不高；HMM 方法使用隐马尔可夫模型进行态势评估，采用威胁评估结果对告警分类，解决了观测事件分类问题，但模型参数的配置具有一定的主观性，准确性偏低；层次化分析方法在评估整个网络系统风险值时具有一定的优势，但风险计算的本质依旧为风险累计算法，利用风险累积进行态势评估，风险值只增不减，不能准确地反映网络态势的变化。

各方法的网络安全态势变化对比如图 7 所示。从图 7 中可以看出，基于攻防博弈的态势评估方法在区分危险性不强的探测阶段，态势值有了显著的变化，相对于应用集对分析方法更灵敏；在危险较大的权限提升阶段方面，基于攻防博弈的态势评估方法与 HMM 方法、应用集对分析方法相比，对网络态势的变化反应更强烈，更能引起网络安全管理员的警觉；同时，该方法解决了层次化分析法风险值只增不减的问题，反映了不同攻击方式对网络态势的影响不是一味地增长，而是具有一定的回复性。因此，本文提出的态势评估方法可以正确地反映网络态势值的变化。

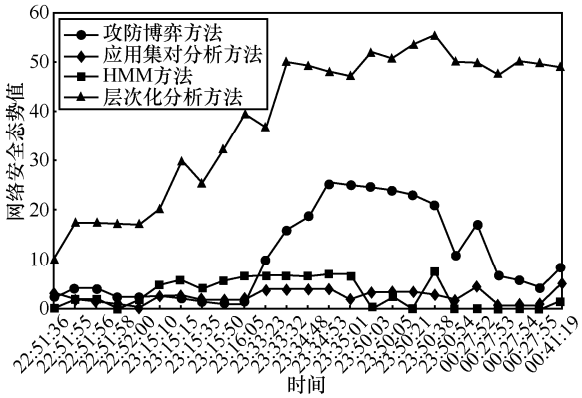


图 7　不同方法的网络安全态势变化对比

2) 普适性的验证

在 CICIDS2017 入侵检测数据集上验证本文提出方法的普适性。根据提出的 NSAM-SG 模型，量化数据捕获周期的安全态势值，由于星期一的数据都是正常流量，网络处于安全状态，态势值为 0，因此本文从星期二开始进行态势评估。CICIDS2017 数据集入侵类型的攻击成本如表 10 所示。

表 10　　CICIDS2017 数据集入侵类型的攻击成本

入侵组	攻击类型	TL
Normal	Benign	—
Probe	Port Scan	0.5
DoS	Botnet, DDoS, DoSGoldenEye, DoSHulk, DoSslow-loris, DoSslowhttp	2
Data	Web-Attack-XSS,Web-Attack-Sql-Injection, Heartbleed Attack	3
Root	FTP-Patator, SSH-Patator, Web-attack-Brute Force, Infiltration	10

通过计算，得到整个网络环境的安全态势值，态势变化曲线如图 8 所示，此时网络处于危险状态。从图 8 中可以看出，在每个攻击阶段中，随着攻击的深入，态势值呈上升趋势，整个网络面临的危险进一步加深。针对不同的攻击可以看出，当网络受到端口扫描攻击时，网络的安全态势值最低，网络受到的影响最小，当网络受到 SSH 暴力攻击、渗透攻击时，网络的安全态势值很高，网络受到的影响比较严重。

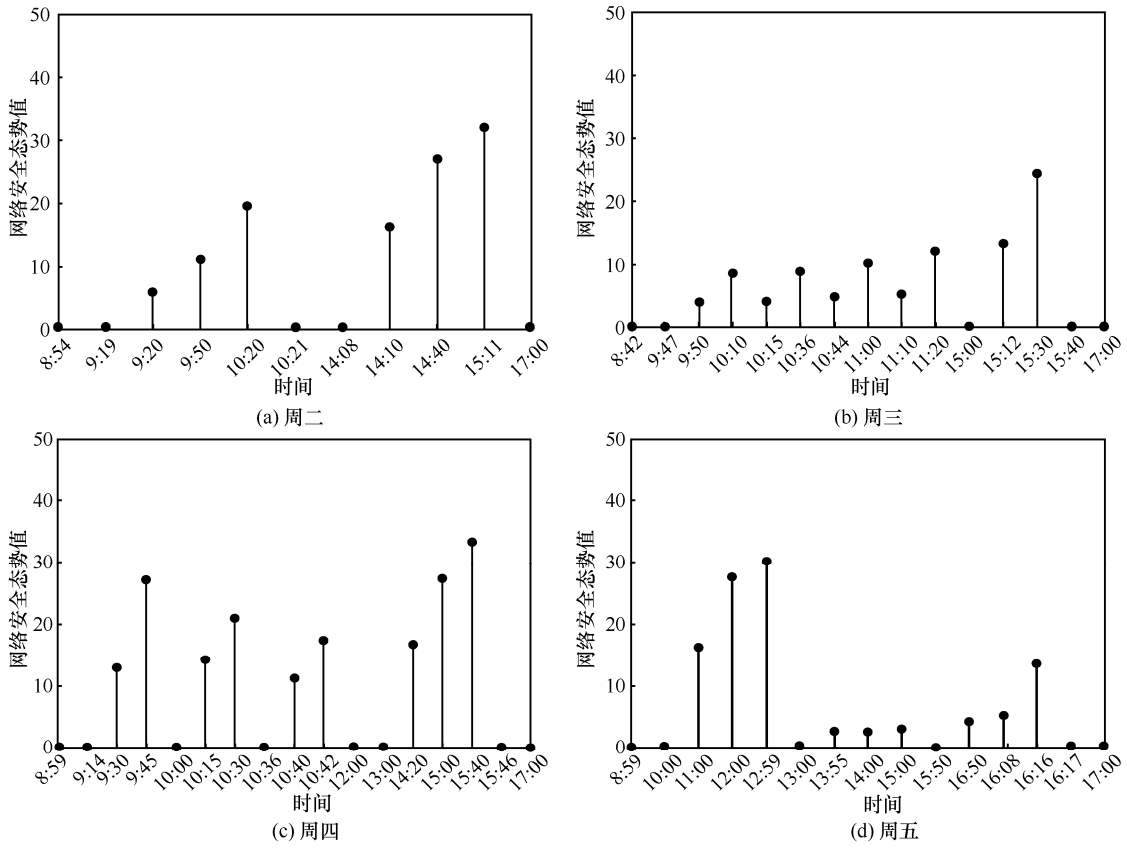


图 8　安全态势

从实验结果可以看出，本文提出的态势评估方法可以适用不同的数据集，能够正确地反映网络安全态势值的变化，具有一定的普适性。但不足之处表现在当网络受到像 DoS/DDoS 这样攻击过程不明显的攻击行为时，网络安全态势值的变化不明显，在攻击初期时可能无法引起安全管理员的注意，因此在接下来的工作中还需要进一步的改进。

6.4　攻击预测

在图 4 所示的网络拓扑结构中，选取 CICIDS2017 入侵检测数据集中受害主机 Ubuntu 16 WebServer、Ubuntu12 进行实验，选取的主机共有 5 处漏洞，具体的漏洞信息及防御者可采取的防御策略如表 11 所示。

表 11　　系统漏洞信息及防御措施

漏洞	影响	TL	防御措施	类别	DC
暴力破解漏洞	Root	10	应用防火墙	DC_3	8
			限制访问	DC_3	8
拒绝服务漏洞	DoS	2	修改服务器参数（如限制单机 IP 连接数）	DC_2	4
SQL 注入漏洞	Data	3	采用 sql 语句预编译，然后进行参数绑定	DC_3	8
跨站脚本（XSS）漏洞	Data	3	HTML 转义	DC_3	8
			验证用户输入	DC_3	8
Heartbleed 漏洞	Data	3	升级 OpenSSL	DC_4	10

根据攻防双方策略的选择，利用式(14)和式(15)计算双方的收益矩阵 $\boldsymbol{P}$ 为

$$\boldsymbol{P}=\begin{bmatrix} 4.58,-4.58 & 6.41,-6.41 & 14.27,-14.27 & 18.89,-18.89 & 34.98,-34.98 \\ 8.15,-8.15 & 4.58,-4.58 & 23.93,-23.93 & 26.44,-26.44 & 27.98,-27.98 \\ 20.51,-20.51 & 1.83,-1.83 & 27.35,-27.35 & 24.55,-24.55 & 29.74,-29.74 \\ 29.38,-29.38 & 16.32,-16.32 & 4.59,-4.59 & 12.84,-12.84 & 34.98,-34.98 \\ 37.78,-37.78 & 18.65,-18.65 & 27.34,-27.34 & 4.12,-4.12 & 31.48,-31.48 \\ 17.09,-17.09 & 17.49,-17.49 & 12.23,-12.23 & 3.60,-3.60 & 34.98,-34.98 \\ 29.38,-29.38 & 20.99,-20.99 & 37.78,-37.78 & 30.22,-30.22 & 2.50,-2.50 \end{bmatrix}$$

根据博弈论纳什均衡的满足条件，计算得到双方的混合策略为 $x^* = (0,0.71,0,0.12,0.17)$，$y^* = (0,0,0,0.31,0.22,0,0.47)$。

通过对原始数据集进行处理，合并 5 天的数据，删除无效的样本，将具有相似特征和行为的少数攻击进行合并，重新定义标签[24]。经过数据处理后，发现 DoS/DDoS 类攻击的样本数量最多，共 379 748 条记录，占全部样本的 36%，且 DoS/DDoS 类攻击付出的攻击成本较低，因此攻击者下一步最有可能进行 DoS 攻击。所以本文提出的纳什均衡进行态势预测方法是可行的。

为验证本文提出的纳什均衡态势预测方法的准确精度，选取 CICIDS2017 数据集中周二的流量数据，分别使用 RBF 神经网络和 Verhulst 灰色模型进行预测，并与本文方法进行对比。使用均方根误差 RMSE 作为定量评价预测模型的预测精度的指标，计算方法为

$$\mathrm{RMSE} = \sqrt{\sum_{i=1}^{n} \frac{(S_i^{'} - S_i)^2}{n}} \tag{22}$$

其中，$S_i^{'}$ 为真实的态势值，S_i 为预测态势值。

3 种预测方法预测精度结果如表 12 所示。

表 12　　3 种预测方法预测精度结果

预测方法	RMSE
本文方法	0.042 5
RBF 神经网络	0.047 7
Verhulst 灰色模型	0.106 8

由表 12 可知，本文提出的基于纳什均衡的态势预测方法的预测精度优于其他方法，能取得良好的预测效果。

7　结束语

本文提出了基于威胁情报的网络态势感知模型，利用威胁情报进行态势感知，对网络进行态势觉察，发现内部威胁信息。对攻防博弈进行建模，通过定义模型的相关概念，量化双方成本和收益，评估当前网络的安全状态，最后利用纳什均衡预测攻击者可能采取的攻击行为。实验分析表明，该模型可以很好地发现未知攻击，对网络的安全态势进行准确的评估和预测。在下一步的工作中，要将所提出的方法应用到实际的网络环境中，改进实验中存在的不足，并在 ICTI 生成过程中引入预测攻击策略概率的思想，进一步规范 ICTI 的生成。

参考文献：

[1] ZHANG Q Y, LI H, HU J S. A study on security framework against advanced persistent threat[C]//2017 7th IEEE International Conference on Electronics Information and Emergency Communication. Piscataway: IEEE Press, 2017: 128-131.

[2] ÇıNAR C, ALKAN M, DÖRTERLER M, et al. A study on advanced persistent threat[C]//2018 3rd International Conference on Computer Science and Engineering. Piscataway: IEEE Press, 2018: 116-121.

[3] LI Y Q, DAI W K, BAI J, et al. An intelligence-driven security-aware defense mechanism for advanced persistent threats[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(3): 646-661.

[4] ENDSLEY M R. Toward a theory of situation awareness in dynamic systems[J]. Human Factors: the Journal of the Human Factors and Ergonomics Society, 1995, 37(1): 32-64.

[5] BASS T. Intrusion detection systems and multisensor data fusion[J]. Communications of the ACM, 2000, 43(4): 99-105.

[6] HE F N, ZHANG Y Q, LIU H Z, et al. SCPN-based game model for security situational awareness in the Intenet of things[C]//2018 IEEE Conference on Communications and Network Security. Piscataway: IEEE Press, 2018: 1-5.

[7] 翁芳雨. 基于随机博弈模型的网络安全态势评估与预测方法的研究与设计[D]. 北京: 北京邮电大学, 2018.
WENG F Y. Research and design of network security situation assessment and prediction method based on random game model[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.

[8] 李腾飞, 李强, 余祥, 等. 基于拓扑漏洞分析的网络安全态势感知模型[J]. 计算机应用, 2018, 38(S2): 157-163, 169.
LI T F, LI Q, YU X, et al. Network security situational awareness model based on topological vulnerability analysis[J]. Journal of Computer Applications, 2018, 38(S2): 157-163, 169.

[9] IOANNOU G, LOUVIERIS P, CLEWLEY N. A Markov multi-phase transferable belief model for cyber situational awareness[J]. IEEE Access, 2019, 7: 39305-39320.

[10] 李骏韬. 基于 DNS 流量和威胁情报的 APT 检测研究[D]. 上海: 上海交通大学, 2016.
LI J T. APT detection research based on DNS traffic and threat intelligence[D]. Shanghai: Shanghai JiaoTong University, 2016.

[11] 李炜键, 金倩倩, 郭靓. 基于威胁情报共享的安全态势感知和入侵意图识别技术研究[J]. 计算机与现代化, 2017(3): 65-70.
LI W J, JIN Q Q, GUO L. Research on security situation awareness and intrusion intention recognition based on threat intelligence sharing[J]. Computer and Modernization, 2017(3): 65-70.

[12] 杨泽明, 李强, 刘俊荣, 等. 面向攻击溯源的威胁情报共享利用研究[J]. 信息安全研究, 2015, 1(1): 31-36.
YANG Z M, LI Q, LIU J R, et al. Research of threat intelligence sharing and using for cyber attack attribution[J]. Journal of Information

Security Research, 2015, 1(1): 31-36.

[13] MAVROEIDIS V, BROMANDER S. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence[C]//2017 European Intelligence and Security Informatics Conference. Piscataway: IEEE Press, 2017: 91-98.

[14] SADIQUE F, CHEUNG S, VAKILINIA I, et al. Automated structured threat information expression (STIX) document generation with privacy preservation[C]//2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference. Piscataway: IEEE Press, 2018: 847-853.

[15] ZHANG H, YI Y, WANG J, et al. Network security situation awareness framework based on threat intelligence[J]. Computers, Materials and Continua, 2018, 56(3): 381-399.

[16] YANG S, WEI X. Research on optimization model of network attack-defense game[C]//2017 8th IEEE International Conference on Software Engineering and Service Science. Piscataway: IEEE Press, 2017: 426-429.

[17] LIPPMANN R P, FRIED D J, GRAF I, et al. Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation[J]. Proceedings DARPA Information Survivability Conference and Exposition DISCEX'00, 2000, 2(2): 12-26.

[18] 席荣荣, 云晓春, 张永铮, 等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报, 2015, 38(4): 749-758.
XI R R, YUN X C, ZHANG Y Z, et al. An improved quantitative evaluation method for network security[J]. Chinese Journal of Computers, 2015, 38(4): 749-758.

[19] SHARAFALDIN I, HABIBI LASHKARI A, GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]//Proceedings of the 4th International Conference on Information Systems Security and Privacy. Piscataway: IEEE Press, 2018: 108-116.

[20] 李希灿. 模糊数学方法及应用[M]. 北京: 化学工业出版社, 2016.
LI X C. Fuzzy mathematics method and application[M]. Beijing: Chemical Industry Press, 2016.

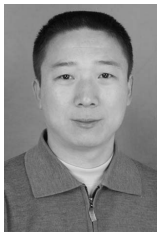
[21] 韩敏娜. 基于多传感器数据融合的网络安全态势评估及预测模型研究[D]. 无锡: 江南大学, 2013.
HAN M N. The research on the assessment and prediction model of network security situation based on multi-sensor data fusion[D]. Wuxi: Jiangnan University, 2013.

[22] 雷杰. 网络安全威胁与态势评估方法研究[D]. 武汉: 华中科技大学, 2008.
LEI J. Research on the network security threat and situation assessment[D]. Wuhan: Huazhong University of Science and Technology, 2008.

[23] 卢鹏. 网络安全态势量化评估方法研究与应用[D]. 成都: 电子科技大学, 2019.
LU P. Research and application of network security situation quantitative evaluation method[D]. Chengdu: University of Electronic Science and Technology of China, 2019.

[24] 赵迪. 面向佯攻的虚实攻击链构造及检测方法的研究与实现[D]. 北京: 北京交通大学, 2019.
ZHAO D. Research and implementation of construction and detection methods of virtual attack and real attack chains for feint attacks[D]. Beijing: Beijing Jiaotong University, 2019.

[作者简介]



张红斌（1976− ），男，河北赵县人，博士，河北科技大学教授，主要研究方向为网络安全与管理、社交物联网等。

尹彦（1997− ），女，山东德州人，河北科技大学硕士生，主要研究方向为网络安全与管理。

赵冬梅（1966− ），女，河北深州人，博士，河北师范大学教授，主要研究方向为网络空间安全、人工智能及应用等。

刘滨（1975− ），男，河北唐山人，博士，河北科技大学教授，主要研究方向为大数据、社会计算、人工智能等。