



基于 LightGBM 算法的网络战仿真与效能评估

陈晓楠¹, 胡建敏^{1*}, 陈茜², 张威³

(1. 国防大学联合勤务学院, 北京 100089; 2. 国防大学政治学院, 上海 201600; 3. 92354 部队, 北京 102202)

(* 通信作者电子邮箱 ugjrl@163.com)

摘要:为解决信息化条件下的网络战抽象程度过高、网络战的仿真和效能评估手段不够丰富的问题,提出了一种融合攻防双方多种指标的网络战仿真和效能评估的方法。首先,对于网络战攻击方,引入4类攻击方式对网络进行打击;对于网络防御方,引入网络节点结构、内容重要程度和应急反应能力作为网络的防御指标;然后,通过将 PageRank 算法和模糊综合评价法融入到 LightGBM 算法中,建立了网络战效能评估模型;最后,通过定义节点毁伤效能曲线,得到整个网络战攻防体系中的剩余效能和毁伤效能评估结果。仿真实验表明:网络战效能评估模型可以对网络战攻防双方的作战效能进行有效的评估,验证了网络战效能评估方法的合理性和可行性。

关键词: 网络战; 效能评估; LightGBM; 模糊综合评价; PageRank

中图分类号: TN915.08 **文献标志码:** A

Simulation and effectiveness evaluation of network warfare based on LightGBM algorithm

CHEN Xiaonan¹, HU Jianmin^{1*}, CHEN Xi², ZHANG Wei³

(1. Joint Logistics College, National Defense University, Beijing 100089, China;

2. Political College, National Defense University, Shanghai 201600, China; 3. Unit 92354, Beijing 102202, China)

Abstract: In order to solve the problems of high abstraction degree of network warfare and insufficient means of simulation and effectiveness evaluation of network warfare under the condition of informationization, a method of network warfare simulation and effectiveness evaluation integrating multiple indexes of both attack and defense sides was proposed. Firstly, for the network warfare attacker, four kinds of attack methods were introduced to attack the network; and for the network defender, the network node structure, content importance and emergency response ability were introduced as the defense indicators of the network. Then, the network warfare effectiveness evaluation model was established by integrating PageRank algorithm and fuzzy comprehensive evaluation method into Light Gradient Boosting Machine (LightGBM) algorithm. Finally, by defining the node damage effectiveness curve, the evaluation results of residual effectiveness and damage effectiveness in the whole network warfare attack and defense system were obtained. The simulation results show that the effectiveness evaluation model of network warfare can effectively evaluate the operational effectiveness of both attack and defense sides of network warfare, which verifies the rationality and feasibility of the effectiveness evaluation method of network warfare.

Key words: network warfare; effectiveness evaluation; Light Gradient Boosting Machine (LightGBM); fuzzy comprehensive evaluation; PageRank

0 引言

网络战是攻击、渗透敌方的计算机网络体系,并保证我方计算机网络安全稳定而采用的一系列网络攻击与防御策略。网络战已经成为现代化战争体系中一种独特的表现形式,不仅仅能够破坏和渗透敌方的军用网络,也可以攻击、渗透敌方的政府、商业、教育等民用网络,达到不战而屈人之兵的效果。

互联网的迅速发展给人们的生活带来了翻天覆地的变化,但也由此带来了日趋严峻的网络安全问题,高度透明的互联网使得网络战的表现形式更为复杂。随着计算机网络的高速发展,计算机网络安全防护愈发重要,网络攻击与防御、

渗透与反渗透的对抗将不断升级。并且互联网的数据的来源广泛、真假难辨,导致了网络战等非实体的对抗越来越频繁,网络战在军事行动中所占的比重越来越突出,所带来的正面和负面影响也日益显著。2013年6月发生的“棱镜门”事件,使各国之间日益激烈的计算机网络战对抗浮出水面。2014年2月,我国成立了网络安全和信息化中央领导小组,对“没有网络安全就没有国家安全”这一论断进行了深刻阐述^[1]。2018年4月,全国网络安全和信息化工作会议中指出,加强互联网内容建设、完善网络综合治理体系、营造清朗的网络空间,从而将网络安全提升到了一个更广泛的层次^[2]。

收稿日期:2019-12-19;修回日期:2020-02-23;录用日期:2020-03-03。

作者简介:陈晓楠(1991—),男,山东烟台人,硕士研究生,主要研究方向:联合勤务指挥、管理与训练; 胡建敏(1964—),男,河北吴桥人,教授,博士生导师,主要研究方向:军事管理学; 陈茜(1990—),女,内蒙古鄂伦春人,讲师,博士,主要研究方向:舆论战、军事外宣; 张威(1989—),男,河北秦皇岛人,主要研究方向:信息安全、后勤管理。



网络战效能评估的研究方法很多,文献[3]中将网络战分为功能模型、物理模型以及信息模型,采用服务到节点、链路到网络系统的自底向上的层次效能评估方法;文献[4]从网络战装备入手,从技术、战术、战役、战略4个层次进行网络战效能评估,除此之外,更多的研究是针对网络入侵检测方面,例如文献[5-8],通过贝叶斯算法、支持向量机、神经网络、聚类分析等不同算法进行网络入侵检测研究,这些研究和算法各有特点,但主要是针对攻击策略的研究与评估,且实时性较差,不能从全局的角度分析和评估整个网络攻防态势,也不能体现出网络战双方互相对抗这一过程。

对网络战的作战效能进行科学合理的分析与评估,是研究网络战乃至信息化作战的前沿课题。网络战的效能评估就是在互联网基础上,对网络攻击方和网络防御方的作战效能做出定量的论断。研究网络战效能评估方法,可以了解敌人的网络攻击策略,完善我方网络防护方案,可以更加有效地保证我方网络安全稳定运行,有助于我国在未来的信息化战争中取得主动。

1 网络战攻防指标体系的建立

在进行网络战效能评估时,首要是要确立网络战攻防指标体系,如何建立网络战攻防指标体系将直接影响网络战效能评估的结果。

这里将网络战指标体系分为攻击效能指标和防御效能指标两部分。其中,攻击效能指标是根据KDDCUP99数据集的分类标识进行建立的,由于KDDCUP99数据集是根据模拟美国空军局域网的一个网络环境而收集到的信息,KDDCUP99数据集是通过仿真真实的攻击手段而采集的,所以数据的收集更贴近真实的网络环境^[9]。目前关于网络入侵的文献中相当数量都是以KDDCUP99数据集为基础进行研究的,并且网络入侵的种类离不开KDDCUP99数据集中的4种攻击标识。这里根据按照KDDCUP99数据集中的攻击标识,将攻击指标分为四大类:拒绝服务攻击(Denial Of Service, DOS)、监视和其他探测活动(Probing)、来自远程机器的非法访问(Remote to Local, R2L)、普通用户对本地超级用户特权的非法访问(User to Root, U2R)四大类^[10-11]。

防御效能指标则主要反映在对应的网络节点的防御能力上,网络战中网络节点的防御能力在于节点本身的功能,假设一个网络节点没有采取任何防御措施,那么此节点的防御能力就为零,而节点防御措施是如何设定的?在网络战中,防御方的每一个节点防御措施有高有低,越重要的节点的防御措施就越高。节点的重要性主要在两个方面:一个是网络节点的结构重要性;一个是节点的内容重要性。

节点的结构重要性即网络节点的脆弱性研究,研究网络节点的脆弱性的文献数不胜数,脆弱性研究主要有两种方法:一种是通过节点在网络中的中心性程度进行评估,即节点的中心性越强,节点就越重要,可以通过度中心、介数、紧密性等指标进行评判;另一种是除掉节点后观察对网络的毁伤程度,即除掉该节点后,网络性能下降得越多,节点就越重要^[12-13]。节点的结构重要性越大,则应该采取越强的防御措施。节点的内容重要性是节点自身的价值,一个网络节点所存储的信息或者自身的功能越重要,则遭受攻击的可能性和攻击强度就越大,就要采取更加严密的防御措施。

接下来需要根据节点的结构重要程度和内容重要程度来设定节点的防御能力,即节点的应急反应能力。这里举个例子,网络入侵检测系统是通过匹配自身的特征库来进行入侵检测,特征库越全面、特征数量越多,那么入侵检测的能力就越强。这里为了更好地反映节点的防御能力,将节点的结构重要程度和内容重要程度量化后之积作为特征库的特征数量,可以采用支持向量机、神经网络、聚类分析等不同的算法,来对攻击方的攻击行为进行检测,能够更贴近网络战的攻防实际,更好地体现双方互相对抗这一过程。因此这里将节点的防御效能指标设定为节点结构重要性、节点内容的重要性和节点的应急反应能力三大类。

对于网络战敌我双方来说,网络战包括我方的进攻、敌方的进攻、我方的防御和敌方的防御,对应的是我方攻击效能、敌方攻击效能、我方防御效能和敌方防御效能。敌方的攻击失败代表着我方的防御成功;同样地,敌方的进攻成功也代表我方的防御失败。因此,为了更好地对网络战整体作战效能进行评估和仿真,这里取蓝方攻击效能和红军防御效能两项指标作为二级指标,通过网络战的交战的攻防双方来确定最后的作战效能。

网络战攻防指标体系如图1所示。



图1 网络战攻防指标体系

Fig. 1 Attack and defense index system of network warfare

2 网络战攻击效能的评估模型

2.1 网络战攻击的定义

网络战的攻击是通过拒绝服务攻击、监视和其他探测活动、来自远程机器的非法访问、普通用户对本地超级用户特权的非法访问四类手段进行攻击的,在四类攻击手段之下还可以继续分为39个次一级的攻击类型,这里不再继续细分。

在网络战中,不可能每一次攻击都会成功,一次成功也不代表着完全控制或者瘫痪对应的目标节点,因此需要对网络战攻击的效能进行评估。

网络战是基于计算机网络实施的作战行动,研究网络战的第一步是要研究网络的拓扑结构。作战网络的邻接矩阵为:

$$C = [a_{ij}]_{N \times N} \quad (1)$$

式中 N 为网络中节点数量。

2.2 网络战攻击效能分析

无论是网络结构多么复杂,敌方的攻击都会作用在不同的网络节点上,网络战的攻击效能由攻击效果决定的,对不同的节点目标,采用不同的攻击策略,将直接影响网络战攻击的效能,因此对网络战的攻击效能 $A(p_i)$ 的定义如下:

$$A(p_i) \leftarrow ATTACK \{p_i, D_i, P_i, R_i, U_i\} \quad (2)$$

其中: $ATTACK$ 函数表示对节点 p_i 采用 D_i 次拒绝服务攻击、 P_i 次监视和其他探测活动攻击、 R_i 次来自远程机器非法访问攻



击和 U_i 次普通用户对本地超级用户特权非法访问攻击。

3 网络战防御效能的评估模型

3.1 节点结构重要程度

采用 PageRank 算法来判断在网络战的网络体系中节点结构的重要程度。PageRank 算法最早来源于搜索引擎的网页的重要性排序和评价,同样,对于网络中网络节点的重要性也可以通过 PageRank 算法来确定,网络中每一个节点的 PageRank 值等于与这个节点相连接的各个节点的 PageRank 值总和。

最初的 PageRank 算法是面向有向图的,其迭代方程为:

$$PR(p_i) = \frac{1-d}{N} + d \cdot \sum_{p_j \in M(p_i)} \frac{PR(p_j)}{L(p_j)} \quad (3)$$

其中: $L(p_j)$ 为节点 p_j 的出度; d 为阻尼因子; N 是节点总数; $(1-d)$ 为随机跳往任意一个节点的概率; $M(p_i)$ 为连接节点 p_j 的所有节点集合。

而在本文中,网络战的网络体系为无向图,因此可以得到 p_i 点的 PageRank 值 $PR(p_i)$, 其迭代方程^[14]为:

$$PR(p_i) = \frac{1-d}{N} + d \cdot \sum_{p_j \in M(p_i)} \frac{PR(p_j)}{degree(p_j)} \quad (4)$$

其中 $degree(p_j)$ 为节点 p_j 的度。

因此,节点 p_i 结构的重要程度可以用 $PR(p_i)$ 表示。

3.2 节点内容重要程度

网络战中每个被攻击节点都有着自身的价值,这些价值可能是包含重要的军事信息,也有可能是有着重要的功能等。网络节点的内容价值越大,作为目标被攻击的可能性越大,同时网络节点被攻击损毁后所造成的损失也越大,因此这里通过模糊评价法来综合评估节点的内容重要性^[15],层次图如图 2 所示。

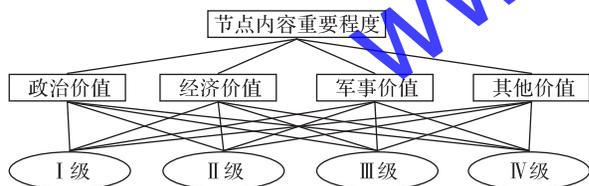


图 2 节点内容重要程度层次

Fig. 2 Hierarchy of node content importance

节点内容的重要程度主要体现在政治价值、军事价值、经济价值和其他价值四个方面,并且与涉密信息或者节点功能的重要性程度有关,信息的密级越高或者节点的功能越重要,其节点的内容重要程度就越大。

其中: I 级表示此节点内存有绝密级信息或者有着极度重要的功能; II 级表示此节点内存有机密级信息或者有着很重要的功能; III 级表示此节点内存有秘密级信息或者有着次重要功能; IV 级表示此节点内存有内部级信息或者有着普通功能。

这里按照 I 到 IV 四种不同级别的信息或者功能的重要程度进行分析,假设节点中存在一项 I 级的信息或者功能,其所影响的政治、军事、经济和其他方面价值为 $l_{11}, l_{12}, l_{13}, l_{14}$, 当有数量 N_1 的 I 级信息或者功能,则对应的价值总量为:

$$L_1 = \frac{1}{4} N_1 \sum_{i=1}^4 l_{1i} \quad (5)$$

同理,一项 II 级的信息或者功能,其所影响的政治、军事、经济和其他方面价值为 $l_{21}, l_{22}, l_{23}, l_{24}$, 一项 III 级的信息或者功能,其所影响的政治、军事、经济和其他方面价值为 $l_{31}, l_{32}, l_{33}, l_{34}$, 一项 IV 级的信息或者功能,其所影响的政治、军事、经济和其他方面价值为 $l_{41}, l_{42}, l_{43}, l_{44}$ 。三者对应数量为 N_2, N_3, N_4 , 对应的价值总量为:

$$\begin{cases} L_2 = \frac{1}{4} N_2 \sum_{i=1}^4 l_{2i} \\ L_3 = \frac{1}{4} N_3 \sum_{i=1}^4 l_{3i} \\ L_4 = \frac{1}{4} N_4 \sum_{i=1}^4 l_{4i} \end{cases} \quad (6)$$

对于 p_i 节点所持有全部涉密信息的内容重要程度 $L(p_i)$ 就等于各种级别的信息或者功能影响政治、军事、经济和其他的价值之和化,并进行归一化处理,即:

$$L(p_i) = (L_1 + L_2 + L_3 + L_4) / L_c \quad (7)$$

其中 L_c 为网络所有节点的内容重要程度之和。

这里对于每一项价值量都可以给出一个客观的评价,这里取评判集的量化值 $V \in [0, 100]$ 。

3.3 节点应急反应能力

如果说节点的结构和内容的重要程度是网络战的网络体系中节点所被动拥有的属性,那么节点的应急反应能力则是主动防御的属性,包括对攻击进行检测、拦截、修复等一系列措施。

节点的应急反应能力中,最主要的是对网络战攻击的入侵检测。关于入侵检测的研究有很多,这里将采取 LightGBM (Light Gradient Boosting Machine) 算法进行检测。

LightGBM 是一种基于决策树算法的梯度提升框架,它的主要特点是:分布式、快速、高效。LightGBM 主要使用了基于 Histogram 决策树算法进行学习^[16-17]。首先将特征值进行离散化,并生成一个宽为 k 的直方图。当对数据样本进行遍历时,将取离散后值作为索引值。直方图在完成一次遍历后就会累积了需要的统计量,然后通过直方图的离散值来寻找最优的分割点。采取这种方式能非常显著降低内存的使用,从而降低时间复杂度。

LightGBM 算法的另一个特点是采取了高效率的叶子生长策略,即带深度限制的叶子生长策略 (Leaf-wise)。Leaf-wise 精度高、误差低,并在 Leaf-wise 中加入了防止过拟合的最大深度限制。该策略在每一次分裂前都会遍历决策树中全部叶子,寻找到分裂增益最大的叶子来进行分裂,然后重复这一操作^[18]。

这里采用 KDDCUP99 作为训练集进行训练,来判断和识别网络战的攻击手段。当然,实际上,不同节点的应急反应能力各不相同,重要的节点应急反应能力强,次要的节点应急反应能力一般,体现应急反应能力大小的就是节点的入侵检测能力。这里为了更好地评估应急反应能力,没有简单地直接利用 LightGBM 算法进行分析,而是从 LightGBM 算法的训练集出发,通过设定训练集的数量来反映节点的入侵检测能力,即应急反应能力。

训练集的数量越多,入侵检测的准确率越大,成功拦截敌方网络攻击的概率就越大,节点的应急反应能力就越强大。



3.4 节点防御效能的分析

节点的防御效能与节点的结构重要程度、节点的内容重要程度和节点的应急反应能力有关。这里为了更好地评估节点的防御效能,对节点 p_i 防御效能 $D(p_i)$ 进行如下定义:

$$D(p_i) \leftarrow \text{LightGBM} \{ \alpha \cdot I \cdot PR(p_i) \cdot L(p_i) \} \quad (8)$$

其中: I 为训练集总量; α 为修正系数;函数 LightGBM 是对训练集进行训练后得出的训练模型。

节点 p_i 的防御效能 $D(p_i)$ 可以由训练集的数量反映出来,节点的结构重要程度越大,节点的内容重要程度越大,那么参与训练的训练集的数目就越大,训练出来的模型就越精确,入侵识别效果就越好,节点 p_i 的防御效能 $D(p_i)$ 就越大。

4 基于LightGBM的网络战效能评估模型

4.1 节点毁伤效能曲线

对网络传递的信息进行检测,通过 LightGBM 算法对信息进行判别,如果断定是攻击行为^[19],则进行拦截,若判断失误,则拦截失败,就会对节点造成一定的毁伤,节点因攻击带来的毁伤达到一定的程度,该节点则会瘫痪或者被摧毁。

根据网络战的性质可知,节点毁伤效果是趋大型的,即攻击效能越大对毁伤节点的满足程度越大,因此这里定义节点毁伤曲线来计算节点的毁伤情况^[20],当毁伤效能达到1时,节点则会瘫痪或者被摧毁,如图3所示。

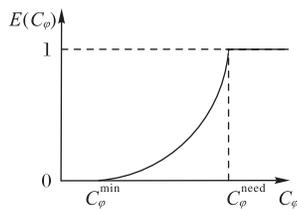


图3 节点毁伤效能曲线

Fig. 3 Node damage effectiveness curve

具体函数表达式为:

$$E(C_\varphi) = \begin{cases} 0, & C_\varphi < C_\varphi^{\min} \\ \left(\frac{C_\varphi - C_\varphi^{\min}}{C_\varphi^{\text{need}} - C_\varphi^{\min}} \right)^3, & C_\varphi^{\min} \leq C_\varphi \leq C_\varphi^{\text{need}} \\ 1, & C_\varphi > C_\varphi^{\text{need}} \end{cases} \quad (9)$$

其中: $\varphi \in \{D_i, P_i, R_i, U_i\}$, C_φ 为采用 D_i, P_i, R_i, U_i 进行攻击后突破节点防御的攻击数量; i 表示节点 p_i 的序号, $i = 1, 2, \dots, N$ 。

4.2 网络战效能计算

网络战的效能评估方法归根到底是判断网络节点的损毁程度,在网络战中,网络中节点数量的保存和损毁数量直接决定网络战的作战效果,则:对攻击方而言,损毁对方节点的重要性越高、数量越多,完成的作战效果越好,与之对应的作战效能就越高;对于防御方而言,成功抵御的攻击数量越多,保存的网络节点数量越多、完整程度越高,那么对应的作战效能就越高。

对于网络中每一个节点 p_i ,都需要计算出其结构重要程度和节点内容重要程度,然后结合训练集总量 I 和修正系数 α ,求得每一个节点的防御效能 $D(p_i)$,并与每一个节点受到的攻击效能 $A(p_i)$ 进行比较,从而得到每一个节点的毁伤情况,

得出网络战中网络体系的剩余效能总量和毁伤效能总量,即网络战的作战效能。

毁伤效能总量为:

$$E_1 = \sum_{i=1}^N \sum_{\varphi} E(C_\varphi) \quad (10)$$

剩余效能总量为:

$$E_2 = \sum_{i=1}^N \sum_{\varphi} [1 - E(C_\varphi)] \quad (11)$$

5 仿真实验与结果分析

5.1 仿真实验步骤

下面进行网络战的仿真实验,为简化计算,这里选取攻击类型为DOS,步骤如下:

- 1)随机生成一个100节点网络作为实验对象,通过计算,得到此网络各个节点的结构重要程度数值;
- 2)对每个节点的内容重要程度进行评估,通过计算,得到此网络各个节点的内容重要程度数值;
- 3)选取KDDCUP99的部分DOS和Normal数据作为训练总集 I ,对每个节点进行训练,对应的每个节点的训练集根据计算求得;
- 4)选取KDDCUP99的部分DOS和Normal数据作为攻击数据,按照设定的攻击策略进行攻击,攻击目标为100个网络节点;
- 5)使用 LightGBM 算法分别对100个网络节点进行判断,得到突破节点防御的攻击数量;
- 6)根据节点毁伤曲线计算每个节点的剩余效能和毁伤效能,并进行累加求和,得到最终的网络战作战效能。

5.2 结果分析

首先根据网络拓扑结构计算出每个节点的结构重要程度,再随机生成每个节点的I到IV四种重要程度的信息或者功能与其所影响的政治、军事、经济和其他方面的价值,得到节点的内容重要程度,如表1所示。

表1 节点重要程度
Tab. 1 Node importance

序号	节点结构重要程度	节点内容重要程度
1	0.0119	0.0126
2	0.0089	0.0079
3	0.0089	0.0055
4	0.0099	0.0112
5	0.0139	0.0142
⋮	⋮	⋮
96	0.0129	0.0130
97	0.0109	0.0129
98	0.0070	0.0127
99	0.0129	0.0087
100	0.0099	0.0099

接下来选取KDDCUP99数据总集合并进行数据集的分配,取KDDCUP99数据集的10%中的DOS和Normal类型共488736条作为数据总集合。这里根据情况调整修正系数 $\alpha = 0.1$, α 的大小会影响训练集的数量, α 取值过大或过小都会造成防御效能设定过强或者过弱,使得网络战攻防过程不平衡,导致网络战攻防双方对抗性将不能很好地展现出来。通过节



点的结构重要程度和节点的内容重要程度计算得到每个节点的训练集,如表2所示。

表2 训练集的分配
Tab. 2 Distribution of training sets

序号	Normal类型	DOS类型	训练集总数
1	146	587	733
2	68	275	344
3	105	422	526
4	108	434	542
5	192	773	965
⋮	⋮	⋮	⋮
96	163	656	820
97	137	550	687
98	86	348	434
99	109	439	549
100	95	384	479

按照得出的100种不同的训练集分别进行100次训练,得到100个网络节点的LightGBM训练参数。

下面设定攻击方的攻击策略,这里为了简化计算,设定攻击方对每一个节点采用同样的攻击策略,攻击数据采用KDDCUP99的测试数据集的10%共30000条DOS和Normal类型数据。

利用LightGBM算法对每个节点的面临的30000条模拟进攻的数据进行判别,得到突破每一个网络节点防御的攻击数量,如表3所示。

表3 突破防御的攻击数量
Tab. 3 Number of attacks breaking through defense

序号	DOS突破防御数量	突破防御比例/%
1	932	3.1
2	6316	21.05
3	3593	11.98
4	1453	4.84
5	579	1.93
⋮	⋮	⋮
96	440	1.47
97	1162	3.87
98	6259	20.86
99	5006	16.69
100	4592	15.31

接下来根据节点毁伤曲线计算每个节点的剩余效能和毁伤效能。节点毁伤曲线中 C_D^{min} 和 C_D^{need} 的取值决定了节点在遭受攻击后何时开始受到影响、何时完全损毁。这里举个例子,在真实的网络战环境某个节点遭受到DOS攻击,在受到强度为10的DOS攻击时,对节点完全没有影响,当受到强度为100的DOS攻击时,节点受到影响明显,当受到强度为1000的DOS攻击时,节点完全瘫痪。 C_D^{min} 和 C_D^{need} 的取值应该结合真实网络中节点实际承受能力进行测量,这里为了能够使网络战的对抗过程更好地展现出来,取 $C_D^{min} = 500, C_D^{need} = 4000$,最后得到每个节点的剩余效能和毁伤效能,如表4所示。

通过计算得到,100个网络节点中有12个节点完好无损,有35个网络节点完全损毁,网络剩余效能总量 $E_1 = 55.995$,攻击方造成的毁伤效能 $E_2 = 44.005$ 。

表4 节点剩余效能和毁伤效能

Tab. 4 Node residual effectiveness and damage effectiveness

序号	剩余效能	毁伤效能
1	0.9965	0.0035
2	0.0000	1.0000
3	0.2407	0.7593
4	0.9728	0.0272
5	0.9999	0.0001
⋮	⋮	⋮
96	1.0000	0.0000
97	0.9897	0.0103
98	0.0000	1.0000
99	0.0000	1.0000
100	0.0000	1.0000
总量	55.995	44.005

6 结语

在复杂多变的网络环境中,存在来自国内外高频率的网络攻击和入侵,攻击层次由浅入深,攻击手段日益复杂,攻击危害性持续增长,网络安全形势日益严峻,对网络战效能进行评估对我国的网络安全有着重要而深远的意义。本文提出了一种可行的网络战效能评估的方法,通过构建红蓝双方的网络战攻防指标体系,引入四种不同攻击类型作为攻击指标,引入节点结构、内容重要程度和应急反应能力作为防御指标,提出了基于LightGBM的网络战效能评估模型,得到整个网络战攻防体系中的剩余效能和毁伤效能指标,综合两个指标分析网络战红蓝双方的作战效能。最后,利用仿真实验证明了模型的有效性和可行性。该方法对网络战效能评估问题提供了一种完整的评估和分析思路:一方面有利于网络战的攻击方确定攻击的正确性和可行性,同时可以让作战指挥员在网络战开始之前评估不同策略的网络战效能,从而进行相应的策略调整;另一方面,也有利于防御方提前做好防护措施,完善和丰富网络防护策略,可用于加强网络安全建设、维护国家利益。

参考文献(References)

[1] 杨光. 我国将出台网络安全审查制度[J]. 计算机与网络, 2014(10):6-6. (YANG G. China will introduce a network security review system[J]. Computer and Network, 2014(10):6-6.)

[2] 习近平. 没有网络安全就没有国家安全[EB/OL]. [2019-03-22]. http://www.cac.gov.cn/2018-12/27/c_1123907720.htm. (XI J P. No network security, no national security[EB/OL]. [2019-03-22]. http://www.cac.gov.cn/2018-12/27/c_1123907720.htm.)

[3] 杨艳萍,叶锡庆,张明安,等. 战场网络战基本模型研究[J]. 系统仿真学报, 2011, 23(5):1015-1020, 1038. (YANG Y P, YE X Q, ZHANG M A, et al. Research on basic models for battlefield network war[J]. Journal of System Simulation, 2011, 23(5):1015-1020, 1038.)

[4] 石磊,潘平俊,李铮,等. 网络战装备综合效能评估框架[J]. 现代防御技术, 2008, 36(4):1-5. (SHI L, PAN P J, LI Z, et al. Architecture of integrative effectiveness evaluation of equipments in net war environment[J]. Modern Defence Technology, 2008, 36(4):1-5.)

[5] 王辉,陈泓予,刘淑芬. 基于改进朴素贝叶斯算法的入侵检测系统[J]. 计算机科学, 2014, 41(4):111-115, 119. (WANG H,



- CHEN H Y, LIU S F. Intrusion detection system based on improved naive Bayesian algorithm [J]. *Computer Science*, 2014, 41(4): 111-115, 119.)
- [6] 谭爱平,陈浩,吴伯桥. 基于SVM的网络入侵检测集成学习算法[J]. *计算机科学*, 2014, 41(2):197-200. (TAN A P, CHEN H, WU B Q. Network intrusion intelligent detection algorithm based on AdaBoost[J]. *Computer Science*, 2014, 41(2): 197-200.)
- [7] 杨宏宇,王峰岩. 基于改进卷积神经网络的网络入侵检测模型[J]. *计算机应用*, 2019, 39(9): 2604-2610. (YANG H Y, WANG F Y. Network intrusion detection model based on improved convolutional neural network [J]. *Journal of Computer Applications*, 2019, 39(9): 2604-2610.)
- [8] 陈万志,徐东升,张静,等. 结合优化支持向量机与K-means++的工控系统入侵检测方法[J]. *计算机应用*, 2019, 39(4):1089-1094. (CHEN W Z, XU D S, ZHANG J, et al. Intrusion detection method for industrial control system with optimized support vector machine and K-means ++ [J]. *Journal of Computer Applications*, 2019, 39(4): 1089-1094.)
- [9] 张新有,曾华荣,贾磊. 入侵检测数据集KDD CUP99研究[J]. *计算机工程与设计*, 2010, 31(22):4809-4812, 4816. (ZHANG X Y, ZENG H S, JIA L. Research of intrusion detection system dataset-KDD CUP99 [J]. *Computer Engineering and Design*, 2010, 31(22): 4809-4812, 4816.)
- [10] 池亚平,莫崇维,杨垠坦,等. 面向软件定义网络架构的入侵检测模型设计与实现[J]. *计算机应用*, 2020, 40(1): 116-122. (CHI Y P, MO C W, YANG Y T, et al. Design and implementation of intrusion detection model for software defined network architecture [J]. *Journal of Computer Applications*, 2020, 40(1): 116-122.)
- [11] FRANK A, ASUNCION A. UC Irvine machine learning repository [DB/OL]. [2019-08-19]. <http://archive.ics.uci.edu/ml>.
- [12] 程光权,陆永中,张明星,等. 复杂网络节点重要度评估及网络脆弱性分析[J]. *国防科技大学学报*, 2017, 39(1):120-127. (CHENG G Q, LU Y Z, ZHANG M X, et al. Node importance evaluation and network vulnerability analysis on complex network [J]. *Journal of National University of Defense Technology*, 2017, 39(1): 120-127.)
- [13] 刘建国,任卓明,郭强,等. 复杂网络中节点重要性排序的研究进展[J]. *物理学报*, 2013, 62(17):No. 178901. (LIU J G, REN Z M, GUO Q, et al. Node importance ranking of complex networks[J]. *Acta Physica Sinica*, 2013, 62(17):No. 178901.)
- [14] 高建召. PageRank 用在无向图上[EB/OL]. [2019-03-22]. <http://wap.sciencenet.cn/blog-468005-1051894.html>. (GAO J Z. PageRank for undirected graphs [EB/OL]. [2019-03-22]. <http://wap.sciencenet.cn/blog-468005-1051894.html>.)
- [15] 崔良中,郭福亮,杨光明. 军队保密工作风险评估模型研究[J]. *网络空间安全*, 2016, 7(5):15-19, 31. (CUI L Z, GUO F L, YANG G M. Research on the risk assessment model of military confidential work [J]. *Cyberspace Security*, 2016, 7(5): 15-19, 31.)
- [16] XIA Y, YANG X, ZHANG Y. A rejection inference technique based on contrastive pessimistic likelihood estimation for P2P lending [J]. *Electronic Commerce Research and Applications*, 2018, 30:111-124.
- [17] SARKAR T K, JI Z, KIM K, et al. A survey of various propagation models for mobile communication [J]. *IEEE Antennas and Propagation Magazine*, 2003, 45(3): 51-82.
- [18] 王思宇,陈建平. 基于LightGBM算法的信用风险评估模型研究[J]. *软件导刊*, 2019, 18(10):19-22. (WANG S Y, CHEN J P. Research on credit risk assessment model based on lightGBM algorithm[J]. *Software Guide*, 2019, 18(10):19-22.)
- [19] 莫坤,王娜,李恒吉,等. 基于LightGBM的网络入侵检测系统[J]. *信息安全研究*, 2019, 5(2):152-156. (MO K, WANG N, LI H J, et al. Network intrusion detection system based on lightGBM [J]. *Research on Information Security*, 2019, 5(2): 152-156.)
- [20] 赵厚玲,谭跃进,李际超,等. 基于作战环的武器装备体系贡献度评估[J]. *系统工程与电子技术*, 2017, 39(10):2239-2247. (ZHAO D L, TAN Y J, LI J C, et al. Armament system of systems contribution evaluation based on operation loop [J]. *Systems Engineering and Electronics*, 2017, 39(10): 2239-2247.)
- CHEN Xiaonan**, born in 1991, M. S. candidate. His research interests include joint service command, management and training.
- HU Jianmin**, born in 1964, Ph. D., professor. His research interests include military management.
- CHEN Xi**, born in 1990, Ph. D., lecturer. Her research interests include public opinion warfare, military publicity.
- ZHANG Wei**, born in 1988. His research interests include information security, logistics management.