

基于多节点协同的电力网络靶场 混合入侵识别方法

郭舒扬[†], 王宁, 覃岩岩

(海南电网有限责任公司 信息通信分公司, 海南 海口 570203)

摘 要:研究了基于多节点协同的电力网络靶场混合入侵识别方法,提升电力网络对混合入侵行为的防御能力。依据多节点协同的分层协作结构,设置电力网络靶场训练平台内的通信节点作为感知节点,利用感知节点感知混合入侵数据,将感知结果传送到电力网络靶场训练平台的中心节点,利用中心节点融合混合入侵感知数据形成聚合节点。协同融合层的聚合节点将协同融合结果传送到识别层,识别层利用混合入侵识别模块,依据 K-means 聚类算法对混合入侵数据的聚类结果,构建 C4.5 决策树,利用决策树输出电力网络靶场混合入侵识别结果。实验结果表明,该方法可以精准识别电力网络靶场混合入侵行为,识别精度高于 98%。

关键词:多节点协同;电力网络靶场;混合入侵;识别方法;K-means 聚类;C4.5 决策树

中图分类号:TP309

文献标识码:A

Hybrid Intrusion Identification Method for Power Network Range Based on Multi-node Cooperation

GUO Shuyang[†], WANG Ning, QIN Yanyan

(Information and Communication Branch of Hainan Power Grid, Haikou, Hainan 570203, China)

Abstract: A hybrid intrusion identification method based on multi-node cooperation in power network shooting range is studied to improve the defense capability of power network against hybrid intrusion behavior. Based on hierarchical collaborative structure of multi-node cooperative, set up the electric power network as perception communication node within the range training platform, using the data from the mixed aware of node invasion will perceive the results sent to the center of the power network range training platform node, using data fusion hybrid intrusion awareness center node form aggregation node. The aggregation node of the collaborative fusion layer sends the collaborative fusion results to the recognition layer, which uses the hybrid intrusion recognition module to cluster the hybrid intrusion data according to the K-means clustering algorithm, constructs the C4.5 decision tree, and uses the decision tree to output the hybrid intrusion recognition results of the power network range. The experimental results show that the method can accurately identify the hybrid intrusion behavior of power network range, and the recognition accuracy is higher than 98%.

Key words: multi-node collaboration; power network range; hybrid intrusion; identification method; K-means clustering; C4.5 decision tree

电力网络安全是电力领域的研究重点,防火墙、数据加密等防护手段^[1]已无法满足电力网络的安全需求,无法应对电力网络的混合入侵行为。混合入侵识别是网络安全领域的重要技术,混合入侵识别需要精准识别电力网络是否存在入侵行为^[2],保护电力网络的资源完整性。电力网络安全是电力系统信息化发展的重要部分,电力网络节点容易受到攻击、窃取以及更改等入侵行为,威胁电力网络安全^[3]。电力网络是输送电力信息的网络,电力网络对电力系统的稳定运行具有重要意义。伴随智能电网高速发展,众多自动化设备应用于电力网络安全监控中。采用人工方式监控电力网络安全需要大量人力成本,同时存在无法精准识别电力网络入侵行为的缺陷^[4]。电力网络中包含众多的混合入侵行为,增加了入侵识别的难度。

电力网络靶场是电力网络的安全测试训练平台,精准识别电力网络靶场混合入侵行为,对于提升电力网络安全性具有重要意义^[5]。电力网络入侵行为主要包括选择转发攻击、黑洞攻击等众多入侵行为。利用电力网络靶场内的众多通信节点,通过多节点协同方法识别电力网络靶场的混合入侵行为。多节点协同方法具有灵活性高、不影响电力网络通信性能等优势^[6],应用于电力网络靶场混合入侵识别中,提升电力网络的运行可靠性。混合入侵行为识别可以有效应对不同类型的入侵行为,具有较高的高效性以及可用性,满足电力网络的通信需求。电力网络靶场混合入侵识别方法不仅需要具备较高的混合入侵识别性能,同时需要保障电力网络具有较高的吞吐量,缩短数据包传输时间间隔。

目前众多研究学者针对网络入侵行为进行研究,陈霖等将动态增量聚类算法应用于电力网络攻击模式识别中^[7],有效识别电力网络中的信息泄露入侵行为;王洋等将贝叶斯方法应用于网络入侵识别中^[8],该方法可以精准识别网络中的拒绝服务入侵行为。以上两种方法虽然具有较高的入侵识别性能,但是对于混合入侵行为的识别性能较差,识别电力网络靶场混合入侵行为时,容易出现误识别情况,影响电力系统的可靠运行。针对以上方法在入侵行为识别时存在的缺陷,研究基于多节点协同的电力网络靶场混合入侵识别方法。利用多节点协同方法实现电力网络靶场混合入侵识别,精准识别电力网络靶场的混合入侵行为,构建一个应用于电力网络靶场的安全防护体系。通过实验验证该方法可以精准识别电力网络靶场混合入侵行为,电

力网络的吞吐量高,有效提升电力网络的安全性,保障电力网络可靠运行。

1 电力网络靶场混合入侵识别方法

1.1 电力网络靶场训练平台

电力网络靶场是电力网络的安全攻击训练平台,电力网络靶场结合了安全测试、安全态势分析、大数据分析技术以及安全培训技术等众多技术,电力网络靶场是保护网络安全的重要部分。搭建电力网络靶场为电力网络的攻防演练提供一个测试平台,利用所搭建电力网络靶场,跟踪电力网络的攻防演练过程,评估电力网络受到入侵时的具体情况,提升电力网络受到入侵时的防御性能。搭建电力网络靶场时需要重点考虑为训练参与者提供丰富的入侵防御演练内容^[9]。电力网络靶场的入侵方,需要考虑网络、数据库等存在于电力网络中的主流入侵方式,细分到不同入侵类型的各种入侵手段。电力网络靶场内的防御方式应该包含网络安全监测中的众多防护策略,需要及时对安全防护策略升级,利用主流的防护策略应对电力网络中的混合入侵行为。电力网络靶场应该具备易于扩展的环境结构,便于实时添加电力网络入侵以及防御演练内容。电力网络靶场训练平台的基本结构图如图 1 所示。

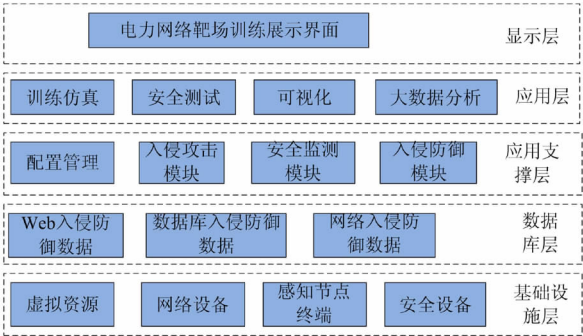


图 1 电力网络靶场训练平台结构图

通过图 1 电力网络靶场训练平台结构图可以看出,电力网络靶场训练平台主要包含基础设施层、数据库层、应用支撑层、应用层以及显示层。电力网络靶场训练平台的训练人员登录电力网络靶场训练平台,选择入侵与防御的演练项目。电力网络靶场训练平台利用单独的物理机服务器承载,众多物理机作为电力网络靶场的通信节点,各节点为网络联通状态^[10-12]。设置电力网络靶场连接的物理机作为虚拟机,为电力网络靶场的入侵与防御训

练提供环境。

1.2 基于多节点协同的混合入侵识别方法

利用多节点协同的分层协作结构,作为电力网络靶场混合入侵识别方法。多节点协同方法识别电力网络靶场混合入侵行为的结构如图 2 所示。

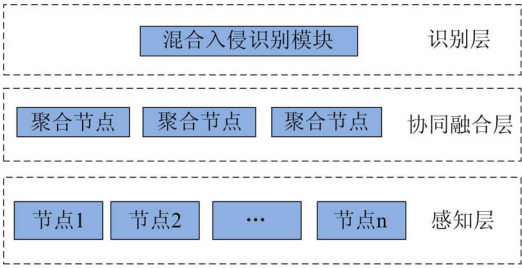


图 2 多节点协同的混合入侵识别结构图

将电力网络靶场训练平台内的众多通信节点作为感知节点,利用感知节点感知电力网络靶场内的混合入侵数据,将混合入侵数据传送至电力网络靶场内的中心节点,利用电力网络靶场的中心节点融合各个感知节点的数据^[13],组成聚合节点。聚合节点将数据传送至识别层,识别层的混合入侵识别模块结合 K-means 聚类算法和 C4.5 决策树算法,利用所构建决策树,输出电力网络靶场混合入侵识别结果。

多节点协同的分层协作技术,利用多代理技术,将电力网络靶场内的各个节点设置为 Agent,利用多个 Agent 组成高层次的识别结构。将多节点协同技术,应用于电力网络靶场中,利用每个 Agent 通过电力网络靶场训练平台的数据库,保存该 Agent 的节点状态。由于电力网络靶场内的节点分布较为分散^[14],混合入侵行为攻击电力网络靶场时,需要多个节点协同处理入侵行为,采用多节点协同的分层协作技术具有较高的识别性能。多节点协同的分层协作技术中,最底层设置了众多的感知节点,利用感知节点搜集电力网络靶场内的信息,最底层具有速度快、数据处理量大、处理效率高的特点。第二层节点是聚合节点,协同融合层的聚合节点具有承上启下的作用,各节点连接一个下级节点链表,利用下级节点链表接收子节点传送数据^[15],通过聚合节点协同多节点采集的电力网络靶场感知信息。设置聚合节点于感知节点和识别层中,降低混合入侵识别方法的识别运算量,提升电力网络靶场混合入侵识别的可伸缩性。

1.3 基于 K-means 聚类与决策树的混合入侵识别

将 C4.5 决策树算法与 K-means 聚类算法结合,作为多节点协同的电力网络靶场混合入侵的识

别方法。C4.5 决策树算法选取信息增益比作为电力网络靶场混合入侵识别的属性选择依据,C4.5 决策树算法获取的混合入侵行为的信息增益比存在明显差异时,决策树算法的工作水平较高;信息增益比差异较小时,所生成的决策树识别电力网络靶场混合入侵行为,可能存在明显的误识别情况。

K-means 聚类算法是适用于电力网络靶场内海量大数据划分的聚类算法,K-means 聚类算法的聚类初始时,需要给出所需划分电力网络靶场混合入侵数据的聚类簇数量以及聚类中心。通过重复迭代,实现电力网络靶场混合入侵数据聚类中心更新,所获取聚类的最优解,即电力网络靶场混合入侵数据的聚类结果。利用 K-means 聚类算法对电力网络靶场混合入侵数据进行聚类的目标函数表达式如下:

$$J = \sum_{j=1}^k \sum_{i=1}^m \text{dist}(p_i, c_j) \tag{1}$$

公式(1)中, m 与 p_i 分别表示电力网络靶场混合入侵数据的属性数量以及聚类中心 c_j 的对应数据, dist 表示混合入侵数据的欧式距离,混合入侵数据的欧式距离计算公式如下:

$$\text{dist}_{ij} = \sqrt{\sum_{k=1}^p |x_{ik} - x_{jk}|^2} \tag{2}$$

公式(2)中, p 表示电力网络靶场混合入侵数据的属性数量。

利用 K-means 聚类算法划分电力网络靶场内的混合入侵数据属性的流程如下:

- (1)设定电力网络靶场混合入侵数据的聚类簇数 K ;
 - (2)从电力网络靶场混合入侵数据样本中,随机选取 K 个数据,作为 K-means 聚类算法的初始聚类中心;
 - (3)计算电力网络靶场混合入侵数据中的数据与所设置聚类中心的欧式距离。依据最近邻原则,将数据划分至与该数据距离最小的聚类中心中;
 - (4)更新 K-means 聚类算法的聚类中心;
 - (5)计算此时电力网络靶场混合入侵数据聚类的目标函数值;
 - (6)重复以上过程,直至混合入侵数据聚类的目标函数不再变化,或满足最大迭代次数为止。输出此时的电力网络靶场混合入侵数据划分结果。
- 利用 K-means 聚类算法对电力网络靶场混合入侵行为进行聚类时,所划分簇的数量以及初始聚类中心的设置极为重要。选取合适的初始聚类中心,有助于后续的聚类结果,提升聚类的收敛速度。

K-means 聚类算法对电力网络靶场混合入侵行为聚类,将相似的类聚集在相同空间范围内,设置欧式距离作为函数聚类的测试属性,构建决策树。利用聚类算法将待识别的电力网络靶场混合入侵数据划分为不同类别,分别构造不同类别的决策树。对 K-means 聚类算法通过聚类获取的距离公式基础上,将权值添加于不同属性中,设置 C4.5 决策树算法生成的信息增益比作为 K-means 聚类算法聚类的权值。

结合 K-means 聚类算法与 C4.5 决策树算法,实现多节点协同的电力网络靶场混合入侵识别,总体结构图如图 3 所示。

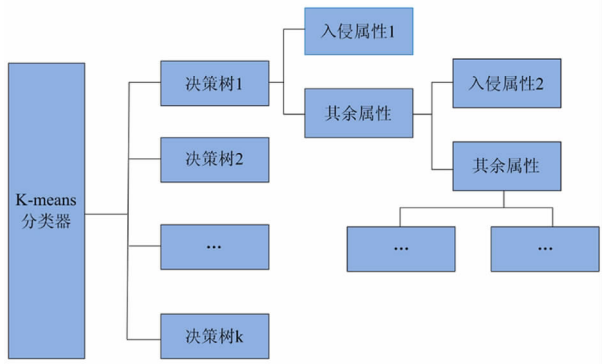


图 3 电力网络靶场混合入侵识别结构图

依据图 3 获取电力网络靶场混合入侵识别的流程如下：

(1)设置电力网络靶场混合入侵的数据集合用 S 表示,其中包含属性 a_i 数量为 n ,聚类数量为 k 。

(2)利用 C4.5 决策树算法,计算不同类别电力网络靶场混合入侵行为的信息增益比用 b_k 表示。

(3)依据 K-means 聚类算法,将电力网络靶场混合入侵行为的数据集,划分为 k 份。引入 C4.5 决策树算法,获取电力网络靶场混合入侵行为数据的相似目标函数表达式如下：

$$O = \sqrt{\sum_{k=1}^n b_k (x_{ik} - x_{jk})^2}$$

(3)

(4)对利用 K-means 聚类算法划分的不同的数据集,构建决策树。

所构建决策树中,信息增益比是选择测试属性的重要依据,将信息增益比设置为聚类算法距离公式中的权重,依据不同属性的信息增益比,划分混合入侵数据。

(5)通过以上过程完成电力网络靶场混合入侵识别方法的训练,计算待识别电力网络靶场混合入侵样本点与全部 k 类中心点的相似目标函数,将测

试样本划分至具有最小相似目标函数值的类别中；

(6)利用所构建的决策树分类器,将所划分类型输入决策树中,输出电力网络靶场混合入侵识别结果。

2 实例分析

为了验证所研究基于多节点协同的电力网络靶场混合入侵识别方法识别电力网络靶场有效性,将该方法应用于某电力企业的电力网络靶场训练平台,通过电力网络靶场的混合入侵识别性能,验证该方法的混合入侵识别性能。电力网络靶场训练平台内包含感知节点数量为 5846 个,聚合节点数量为 584 个,利用多节点协同,实现电力网络靶场混合入侵识别结果。电力网络靶场内设置了入侵攻击数据库,利用入侵攻击数据库内的数据进行电力网络靶场的混合入侵识别训练。电力网络靶场的混合入侵数据设置情况如表 1 所示。

表 1 电力网络靶场混合入侵数据设置

入侵类型	属性维度	入侵样本数量/个
拒绝服务攻击 DOS	3	25846
未授权本地用户访问 U2R	7	52312
未授权远程用户访问 R2L	5	28456
端口监视	8	58464
虚假路由信息攻击	5	25645
选择转发攻击	8	25456
方向误导入侵	7	38845
黑洞攻击	6	48561
虫洞攻击	5	59652
确认欺骗攻击	8	84561

设置固定的电力网络靶场入侵频率,电力网络靶场训练平台伴随时间不断变化,入侵数据传输频率变化如图 4 所示。

通过图 4 实验结果可以看出,采用本文方法对电力网络靶场的混合攻击入侵识别时,通过入侵数据传输频率变化,模拟电力网络靶场实际运行状态。电力网络靶场的入侵数据频率存在变化,与实际电力网络靶场训练情况相符。

采用本文方法利用多节点协同方法,对电力网络靶场混合攻击入侵行为进行识别。统计本文方法设置 K-means 聚类算法的不同 K 值时,电力网络靶场混合攻击入侵行为识别的精度变化,统计结果如图 5 所示。

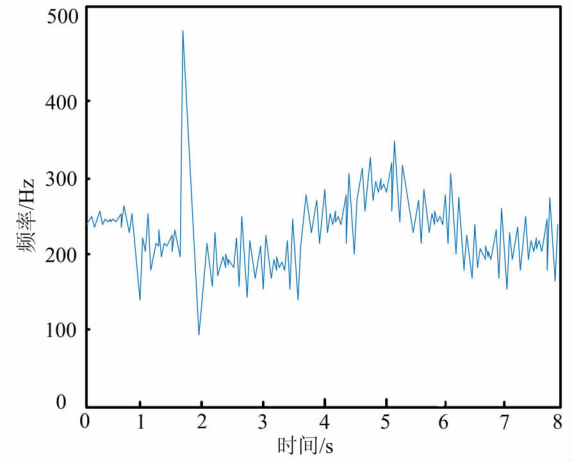


图 4 入侵数据传输频率变化

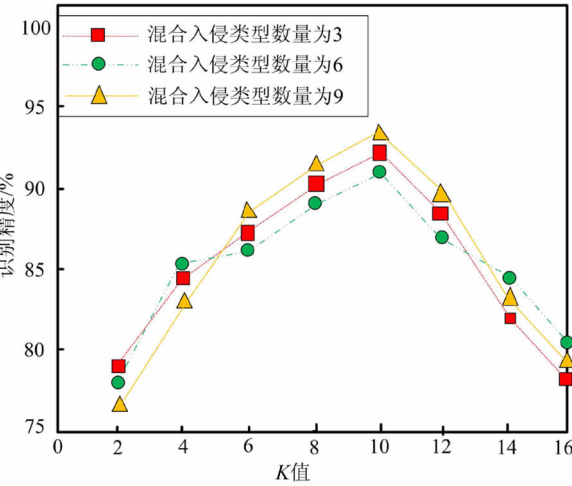


图 5 K 值对混合攻击入侵识别精度的影响

通过图 5 可以看出, K 值为 10 时, 采用本文方法识别电力网络靶场混合入侵行为的识别精度最高。聚类数量 K 为 10 时, 本文方法识别电力网络靶场混合入侵行为的性能最优, 采用本文方法识别电力网络靶场混合入侵行为时, 设置聚类数量为 10。

设置聚类数量为 10, 统计采用本文方法对电力网络靶场混合入侵行为的识别结果, 统计结果如表 2 所示。

通过表 2 可以看出, 采用本文方法可以有效识别电力网络靶场混合入侵行为。采用本文方法识别电力网络靶场混合入侵行为的结果与电力网络靶场混合入侵行为的实际数量相差极小, 验证本文方法具有较高的电力网络靶场混合入侵识别性能。本文方法可以精准识别电力网络靶场混合入侵行为, 适用于电力网络靶场的安全训练中。

表 2 混合入侵行为识别结果

入侵类型	总样本数量/个	训练样本/个	测试样本/个	识别结果/个
拒绝服务攻击 DOS	25846	15846	10000	9999
未授权本地用户访问 U2R	52312	42312	10000	9998
未授权远程用户访问 R2L	28456	18456	10000	9999
端口监视	58464	48464	10000	9997
虚假路由信息攻击	25645	15645	10000	9998
选择转发攻击	25456	15456	10000	9997
方向误导入侵	38845	28845	10000	9996
黑洞攻击	48561	38561	10000	9995
虫洞攻击	59652	49652	10000	9994
确认欺骗攻击	84561	74561	10000	9996

电力网络运行实际过程中, 容易受到外界环境干扰, 在电力网络靶场的训练测试平台中, 加入单音干扰、多音干扰、宽带干扰三种干扰噪声, 所加入干扰噪声的幅度谱如图 6 所示。

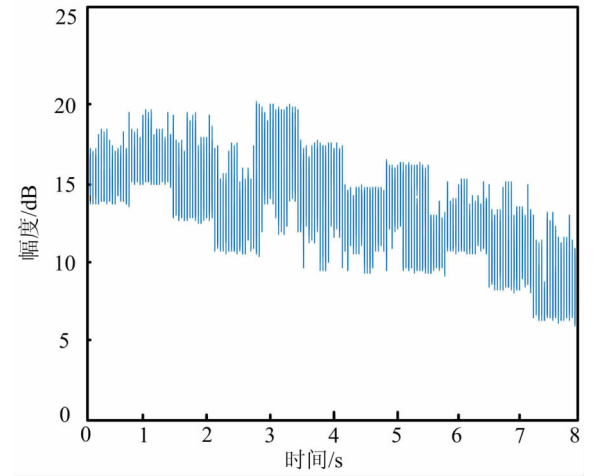


图 6 电力网络靶场干扰的幅度谱

依据图 6 的干扰噪声幅度谱, 在电力网络靶场训练平台中设置干扰噪声。统计不同干扰噪声时, 采用本文方法识别电力网络靶场混合入侵行为的识别精度, 统计结果如图 7 所示。

通过图 7 可以看出, 采用本文方法识别电力网络靶场混合入侵行为, 不同类型干扰环境下, 识别精度均高于 98%。图 7 实验结果验证, 本文方法在干扰环境下, 仍然可以精准识别电力网络靶场的混合入侵行为, 验证本文方法仍然具有较高的混合入侵识别精度, 应用性能较高。

网络吞吐量是衡量电力网络应用性能的重要指标, 统计采用本文方法识别电力网络靶场混合入

侵行为时,电力网络的吞吐量变化情况,统计结果如图 8 所示。

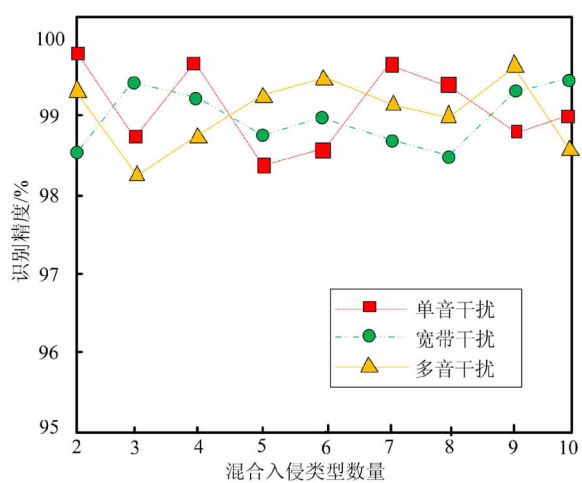


图 7 干扰环境下混合入侵识别精度

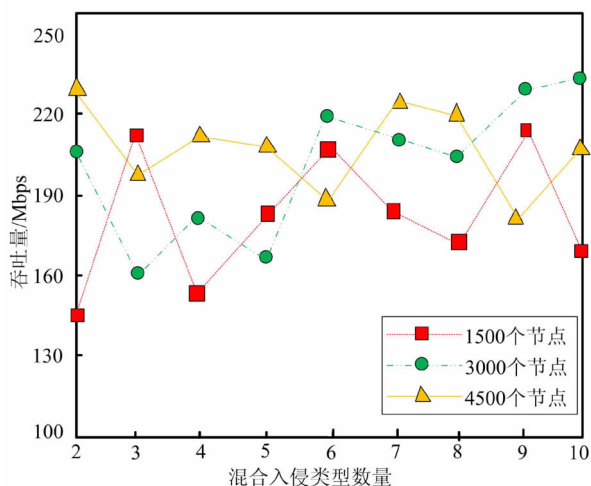


图 8 电力网络吞吐量变化

通过图 8 可以看出,采用本文方法识别电力网络靶场混合攻击行为,电力网络的吞吐量均高于 140Mbps,实验结果验证采用本文方法识别电力网络靶场混合攻击行为,可以提升电力网络的通信性能。电力网络具有较高的吞吐量时,表示电力网络具有良好的通信性能,电力系统可以利用电力网络具备的良好通信性能,维持可靠的运行状态。

3 结 论

针对电力网络的安全靶场攻击测试平台的攻防训练对电力网络安全的重要性,研究了多节点协同的混合攻击入侵识别方法。电力网络靶场以多节点协同的入侵识别方法作为攻防训练的重要方法,支撑电力网络的空间安全。充分考虑电力网络

的安全防护需求,利用电力网络靶场的模拟性能,保障电力网络安全运行。通过实验验证,该方法可以精准识别电力网络靶场混合入侵行为,对电力网络运行状态影响较小,识别正确率高,具有较高的识别性能,为电力网络靶场的攻防训练提供理论及实践依据。

参考文献

- [1] 樊冰,郑陈熹,唐良瑞,等. 基于多属性决策的电力通信网的节点重要度计算方法[J]. 电力系统保护与控制, 2020, 48(9):68—76.
- [2] 张红旗,黄睿,常德显. 一种基于匹配博弈的服务链协同映射方法[J]. 电子与信息学报, 2019, 41(2):385—393.
- [3] 石刘强,石顾禹,杨明,等. 协同调制识别算法在电力线通信网络中的设计与实现[J]. 计算机工程, 2019, 45(8):159—164.
- [4] 李群,王超,任天宇. 基于渗透测试的多层次网络安全入侵检测方法[J]. 沈阳工业大学学报, 2022, 44(4):372—377.
- [5] 李昌超,康忠健,于洪国,等. 考虑电力业务重要性的电力通信网关键节点识别[J]. 电工技术学报, 2019, 34(11):2384—2394.
- [6] 任家东,张亚飞,张炳,等. 基于特征选择的工业互联网入侵检测分类方法[J]. 计算机研究与发展, 2022, 59(5):1148—1159.
- [7] 陈霖,许爱东,蒋屹新,等. 基于动态增量聚类分析的电力信息网络攻击模式识别算法[J]. 南方电网技术, 2020, 14(8):25—32.
- [8] 王洋,吴建英,黄金全,等. 基于贝叶斯攻击图的网络入侵意图识别方法[J]. 计算机工程与应用, 2019, 55(22):73—79.
- [9] 刘阳,夏添,汪旸. 区域电网内多输电断面有功协同控制策略在线生成方法[J]. 电力自动化设备, 2020, 40(7):204—210.
- [10] 戚振彪,凌松,刘文烨,等. 基于高频测试信号注入的配电网故障节点在线识别方法[J]. 电力系统保护与控制, 2020, 48(4):110—117.
- [11] 余学兵,占清华,鄢昌兴. 基于协同过滤的多节点信息资源分配推荐算法[J]. 计算机仿真, 2021, 38(6):419—423.
- [12] 巩磊,司瑞彬,田宇. 基于本体论的网络靶场威胁建模关键技术研究[J]. 中国电子科学研究院学报, 2020, 15(12):1139—1144+1162.
- [13] 戚元星,崔双喜. 集成学习在电网假数据入侵检测中的应用[J]. 河北大学学报(自然科学版), 2022, 42(1):105—112.
- [14] 任志航. 面向电力客户侧终端网络的高效入侵检测模型研究[J]. 电测与仪表, 2022, 59(5):149—157.
- [15] 冯小伟,胡聪,许畅,等. 基于网络效率最优的关键节点识别方法[J]. 计算机工程与设计, 2019, 40(2):328—335.