DOI:10.13718/j.cnki.xsxb.2023.03.001

智能电网专题

智能化是电网的发展方向，智能电网将会给人们的工作和生活方式带来极大的变革，但是智能电网的开放性和包容性也决定了它必须应对各种网络安全挑战。智能电网的安全性一旦受到威胁，很有可能造成整个电力系统失控，不仅会带来信息和经济上的损失，而且会危及人身和社会安全。本期刊出智能电网专题，分别从密钥认证网络安全、密钥管理方案和数据安全防护等角度探讨智能电网的网络安全问题，提出相应的管理方案和防护技术，以期为决策者和科研人员提供参考。

基于交叉组合运算的密钥认证网络安全研究①

杨云帆[1]， 黄浩[1]， 古振威[1]， 马腾腾[1]， 王依云[2]

1. 广东电网有限责任公司 电力调度控制中心，广州 510000；
2. 南方电网数字电网研究院有限公司 平台安全分公司，广州 510000

摘要：针对当前多服务器网络安全性低和通信开销大的问题，提出了一种基于交叉组合运算的密钥认证网络安全研究方法. 该方法通过蝙蝠算法优化后的随机森林算法提取数据的有效特征，然后基于交叉组合运算建立协议模型完成数据判别，最后利用该协议模型对不同类型的网络攻击进行检测. 实验结果显示，该交叉组合运算方法能有效地减少网络中的通信开销并提升网络安全水平，所建立的协议模型可以有效减少网络攻击的危害，且在召回率和查准率方面都有较好的效果，具有一定可行性.

关 键 词：交叉组合运算；蝙蝠算法；随机森林算法；协议模型；网络安全

中图分类号：TN915.853 **文献标志码**：A **文章编号**：1000-5471(2023)03-0001-08

Research on the Security of Key Authentication Network Based on Cross-Combination Operation

YANG Yunfan[1], HUANG Hao[1],
GU Zhenwei[1], MA Tengteng[1], WANG Yiyun[2]

1. *SPower Dispatch Control Center, Guangdong Power Grid Co., Ltd., Guangzhou 510000, China*;
2. *China Southern Power Grid Digital Power Grid Research Institute Co., LTD. Platform Security Branch, Guangzhou 510000, China*

Abstract: For the current problems of low security and high communication overhead of multi-server networks, this paper proposed a research method of key authentication network security based on cross-combination operation. The method extracted the effective features of data through the random forest algorithm optimized by the bat algorithm, then built a protocol model based on the cross-combination operation to complete the data discrimination, and finally used the protocol model to detect different types of

① 收稿日期：2022-09-22
基金项目：广东电网有限责任公司资助项目(GDKJXM20198529).
作者简介：杨云帆，高级工程师，主要从事通信和网络安全研究.

network attacks. The experimental results showed that the proposed cross-combination operation method can effectively reduce the communication overhead in the network and improve the network security, and the established protocol model can effectively reduce the harm of network attacks and has certain feasibility.

Key words: cross-combinatorial operations; bat algorithm; random forest algorithm; protocol model; network security

随着信息技术的快速发展，信息网络在各行各业中已经实现了全覆盖、全普及和全应用，大数据已经成为了一种新兴资源. 然而，数据增长也会带来一些问题，在电力信息系统中[1]，各个设备之间形成了高度互联的智能网络信息系统，但人为的网络攻击，会严重影响电力信息网络的完整性[2]，网络安全问题也有愈演愈烈之势. 网络信息系统一旦出现病毒，就会使网络系统遭到恶意的访问[3]，不仅会导致资金的浪费，而且还会影响用户的隐私信息，造成一系列的负面效果，最终会威胁到用户网络数据的安全，造成不同程度的损害[4].

在应对复杂多样的攻击形式和海量数据的时候，传统网络入侵检测技术和手段就显得力不从心，所以需要更有效的手段来进行对抗，文献[5]使用基于机器学习的电力信息网络的入侵检测方法研究了4类子集，采用随机森林分类器达到分类目标，但是采用单一的随机森林分类器选择，其结果具有较强的随机性，容易陷入局部最优；文献[6]提出通过加权策略对过采样和随机森林进行改进的算法，使得随机森林算法在不平衡数据上的整体分类有更好的效果，但是由于未对随机森林进行改进，因此仍然存在随机性问题；文献[7]为了减少抽样对非平衡性的影响，在Bootstrap重抽样的基础上进行改进，使得对非平衡数据整体算法的分类性能有所提高，但是并未在分类方法上有明显突破；文献[8]提出了一种在线分布式安全特征选择方法，根据电网特征量的相关性强弱来划分，相比传统方法在计算准确性和计算速度方面更具优势，然而并未从根本上解决多服务器网络的安全性低的问题. 文献[5-8]尽管都提出了一些针对网络攻击的应对方法，重点解决了重抽样的问题，但是在面对多服务器网络时其分类方法仍然难以满足实际应用时的随机性问题，使得多服务器网络安全性和通信开销难以保证.

因此针对多服务器网络安全性低和通信开销大的问题，本研究提出一种基于交叉组合运算的密钥认证网络安全研究方法，实验结果显示使用交叉组合运算方法能有效地减少网络中的通信开销，并提升网络安全水平，减少网络攻击的危害，具有一定可行性. 在考虑了多服务器网络特性的基础上，引入交叉组合运算方法实现样本多次交叉验证，在保证了抽样效果的同时确保了样本的有效性. 同时，针对随机森林算法的局限性，采用蝙蝠算法对随机森林的参数进行优化，降低了分类的随机性，并且在交叉验证的前置条件下，优化算法的效率得到显著提升，能高效精准地完成有效样本特征选择.

1 多服务器交叉组合运算方法

1.1 交叉组合算法

交叉验证是一种用来评价一个统计分析的结果是否可以推广到一个独立的数据集上的技术，主要用于预测，即：想要估计一个预测模型在实际应用中的准确度. 它是一种统计学上将数据样本切割成较小子集的实用方法，也即是先在一个子集上做分析，而其他子集则用作后续对此分析的确认及验证.

交叉验证的理论是由Seymour Geisser所开始的. 它对于防范数据的检验假设(testing hypothess suggested by the data)非常重要，特别是当后续的样本是危险的、成本过高的或不可能(uncomfortable science)去搜集的[9]. 利用测试集来测试训练得到的分类器或模型，以此作为分类器或模型的性能指标. 得到高度预测精确度和低的预测误差是研究的期望. 为了减少交叉验证结果的可变性[10]，对一个样本数据集进行多次不同的划分，得到不同的互补子集，进行多次交叉验证，取多次验证的平均值作为验证结果.

1.2 多服务器身份认证

传统的单服务器网络架构已不适用于当前大多数的实际环境. 移动云计算环境中存在着不同的云服务器为用户提供不同类型的移动云服务[11]. 由于互联网的开放性，为了阻止非法用户获取网络服务，保障多服务器网络环境安全，需要建立一个高效安全的身份认证机制. 多服务器网络环境的身份认证协议便是一

种行之有效的方法，以此来保障网络活动参与者的通信安全. 多服务器网络环境的身份认证[12]协议通常包含 3 个参与方，即用户、服务提供者和注册中心 RC(可信的第三方). 根据服务提供者计算能力的强弱、硬件资源是否充足，多服务器网络环境身份认证过程通常有两种模型[13]，即两方参与认证的认证模型和三方参与认证的认证模型. 对于计算能力较强、硬件资源丰富的多服务器网络环境，用户与服务提供者的相互认证无需第三方的帮助(图 1). 而对于计算能力较弱、硬件资源有限的多服务器网络环境，与服务提供者的相互认证需要可信第三方的帮助. 三方参与认证的认证模型见图 2[14]，其计算能力和通信传输能力(以无线传感器网络为例)都是非常有限的，需要网关节点 GWN(注册中心)的参与，来完成与用户的相互认证.

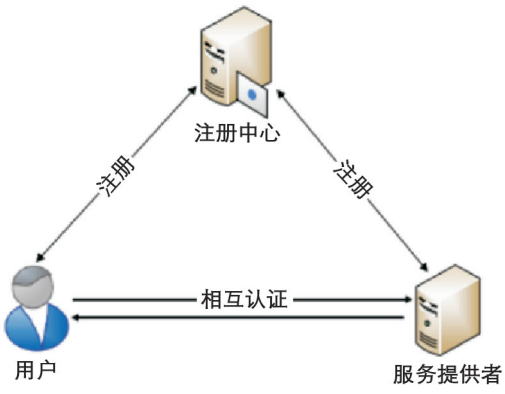

图 1　多服务器网络环境

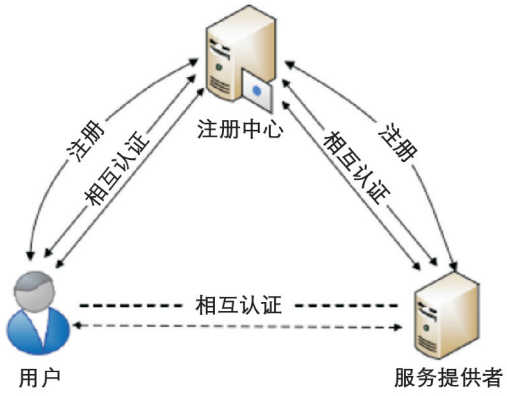

图 2　三方参与认证的认证模型

1.3　多服务器交叉组合运算

交叉验证(cross validation，CV)也叫做循环估计，其基本思想是对于训练样本集，分割为 K 个小的子集，将其中的 1 个子集拿出来作为测试集，其余的 $K-1$ 个子集当做实验的训练集，直到迭代完成. 这里的交叉验证方法与常见的不同，它不是将不同的行组合然后求平均值，而是将不同的列组合得到最优的特征数集，当减少特征会导致性能损失时，就不会再删除任何特征. 对整个信息网络数据集进行分析，其含有大量数据和较多的特征集，包含了许多冗余数据和无关特征，也会让整个模型处理数据的运算时长变多，此时就需要特征降维和变量选择，这也是在数据处理中普遍所使用的相关技术. 所以就要进行特征选择，所以在这里使用随机森林(random forest，RF)来进行特征的选择.

2　特征选择优化方法研究

2.1　RF 算法

RF 算法的最基本单位是决策树，利用多个决策树的结合能够科学地提升分类与预测的精确度，而各个树所映射的数据集的生成与特征子集的筛选呈现出明显的随机性. RF 算法首先基于 Bagging 算法产生得到决策树所对应的训练集，然后再筛选得到 CART 决策树的特征子集[15].

1) CART 决策树

CART 决策树的本质是一种二分递归分割的方法，在叶节点之外的其余的任意 1 个节点对现有的数据样本集合开展二分割，主要是将基尼指数当作属性筛选的度量指标，其计算公式为

$$Gi_D = 1 - \sum_{j=1}^{M} P_i^2 \tag{1}$$

式中：Gi_D 为基尼系数；P_i 为 i 类元素产生的概率；D 为数据集；M 为数据集中含有的类型.

若数据集依照属性 X 开展二元分类，那么相应的基尼系数为

$$Gi_{D,X} = \sum_{i=1}^{2} \frac{|D_i|}{D} Gi_{D_i}(D_i) \tag{2}$$

2) Bagging 算法

Bagging 算法主要是对样本数据集完成部分随机抽样从而获取决策树，有效提升算法泛化能力.

尽管随机森林算法具有较好的特征选择性能，但是在实际运算过程中往往存在随机性不可控的问题而

导致选择随机性强，结果容易陷入局部最优，因此本研究采用蝙蝠算法(bat algorithm，BA)对随机森林算法进行优化.

2.2 BA算法

BA算法的机理主要是源自蝙蝠的回声定位，其原理源自于粒子群算法的延展，该智能算法可以实现自身参数的动态调控，故而有着寻优效率高、鲁棒性强的优点. BA算法的核心参数分别是搜索脉冲响度 A_m，脉冲发生频率 f_m 以及脉冲频度 R_m，由此给出3个假设条件分别为[16]：

1) 根据科学研究表明，蝙蝠的觅食特性表现在其在随机飞行觅食过程中释放脉冲，通过对脉冲回声进行定位从而获知猎物距离自身的距离，并且可以通过对回声的变化对辨别猎物与障碍物进行分别.

2) 当蝙蝠觅食时，蝙蝠在位置 X_bi 以速率 V_{xi} 完成随机飞行，在对 F_m 与 A_m 进行调节来完成觅食搜索行为. 另外，蝙蝠可以通过对于自身发出的回声分析估算猎物与自身的距离进而调节自身射出的脉冲频率，然后在接近猎物时主动调整脉冲频度.

3) 在觅食过程中，随着蝙蝠逐渐接近猎物时，其所发出的脉冲响度从最大值 A_{m_max} 渐次降到最小值 A_{m_min}，而脉冲发射率 f_m 则逐渐上升. 在 d 维的搜索域中，第 i 只蝙蝠在 t 时刻的位置为 X_i^t，速率时 V_i^t，而种群中的最优位置可以定义为 X^*，那么在 $t+1$ 时进行全局搜索时，第 i 只蝙蝠的位置和速率应当被更新为

$$f_{mi} = f_{i\_min} + (f_{m\_max} - f_{m\_min})\varphi \tag{3}$$

$$V_i^{t+1} = V_i^t + f_{mi} \cdot (X_i^t - X^*) \tag{4}$$

$$X_i^{t+1} = X_i^t + V_i^{t+1} \tag{5}$$

式中：φ 为[0，1]范围内服从均匀分布的随机数；f_{mi} 为第 i 只蝙蝠的频率，在[f_{m_min}，f_{m_max}]范围内随机生成.

当对局部进行搜索时，必须从现有的最优解的集合中，随机筛选出一个优异的个体 X_i^t，则每个个体的新位置 X_i^{t+1} 在旧有位置附近随机生成，则

$$X_i^{t+1} = X_i^t + eA_m(t) \tag{6}$$

式中：e 为[-1，1]范围内的随机变量；$A_m(t)$ 为全部个体在 t 时刻的平均脉冲响度.

在迭代运算时，$A_m(t)$ 和 R_m 要动态即时更新，以保证算法有效平衡全局与局部搜索，其更新公式为

$$A_i^{t+1} = \mu A_i^t \tag{7}$$

$$R_i^{t+1} = R_i^0[1 - exp^{(-\eta t)}] \tag{8}$$

其中 $\mu \in (0, 1)$ 和 $\eta \in (0, +\infty)$ 均为常数.

BA优化后的RF算法中，将RF中的参数当作BA个体的2个位置，每个个体在搜索域中单独搜索，最优解记作当前极值，并确定为局部最优. 等到下次迭代时，与其他个体分享，并基于个体与种群经验，完成比较后调节自身定位与速率，从而得到全局最优解. BA-RF流程见图3.

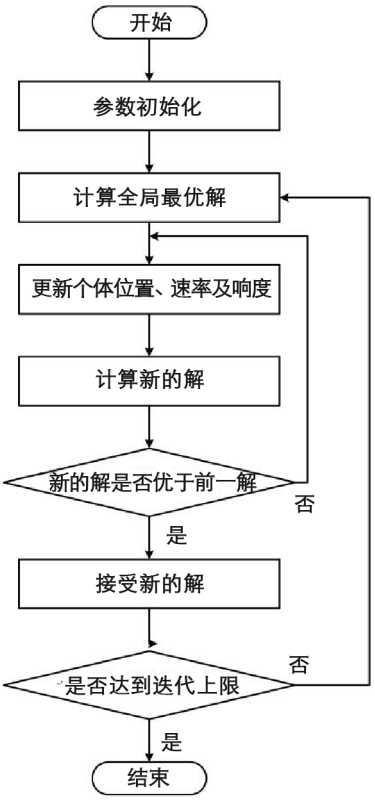

图3 BA-RF流程

2.3 特征选择流程

采用BA-RF算法完成特征选择流程如下所示：

1) 首先需要计算每个特征的重要性，并对计算出的结果进行大小排序，这样就可以根据得到各个特征值的大小来选择出特征的重要程度，其计算公式为

$$I = \frac{1}{N}\sum_{i=1}^{N} |E_2 - E_1| \tag{9}$$

式中：I 表示的是特征的重要性，E_1 表示的是决策树所相对应的袋外数据计算误差，E_2 为对所有的袋外数

据样本特征加入噪声后再次计算后的袋外数据误差，而加入随机噪声后会影响 E_2 大小，使整体数值变化，这样就能说明该特征的重要程度.

2）确定需要剔除的比例，依据上一步中所得出的特征重要性大小值来剔除掉相应比例的特征，去除掉多余的特征后，所得到特征数据集就是一个我们所需要的新的特征集.

3）在上两步的基础上，使用新的特征集来重复上述的两个过程，直到剩下需要的 m 个特征[17]（m 为提前设定的值，一般根据自己需要来定，如果不设置的话，一般会默认设置为 10 个）.

4）根据上述过程中得到的各个特征集和特征集对应的袋外误差率，选择袋外误差率最低的特征集.

3　协议模型的训练

在选择完特征后，需要通过协议模型对训练集进行训练(图 4)，为了使得最后的运算效果较好，一般把全部样本集分为 2 个部分，也就是训练集和测试集. 可以通过 K 次交叉验证使得实验效果更好，降低仅一次运算产生的过度拟合问题，可以在处理实际数据时，避免只对数据集中训练集有很高检测率而对数据集以外的数据检测效果一般，更加有效地反映实验结果，所以在运算模型时，仅仅分出一部分来对模型的参数进行调试，将其余部分作为模型的测试集，也可以从另一个角度分析是否调节的最优参数符合其他数据集. 其流程见图 4.

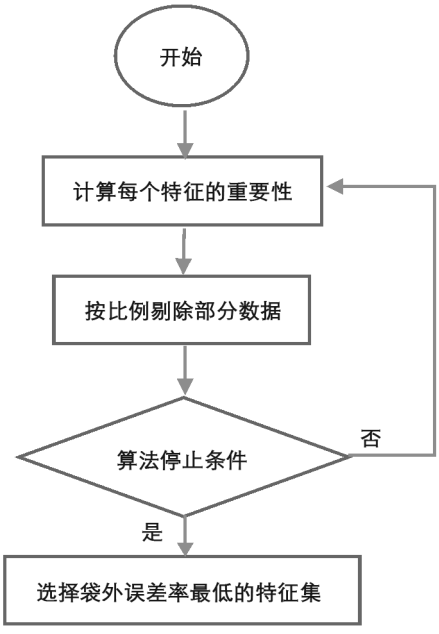

图 4　训练流程

在本研究的实验中，将采用 10 次交叉验证进行数据筛选，将冗余数据和无效数据剔除出样本，使得样本的有效性大大提升，确保了后续分类模型对于样本的敏感性并且避免了过拟合问题，从而保证基于 BA-RF 的电力信息网络的入侵检测方法研究实验效果的稳定. 考虑到数据检验实验的合理性和模型测试的科学性，将数据集分为 10 份，仅将 1 份作为测试集，其余 9 份拿来训练，10 次交叉验证的原理图见图 5.

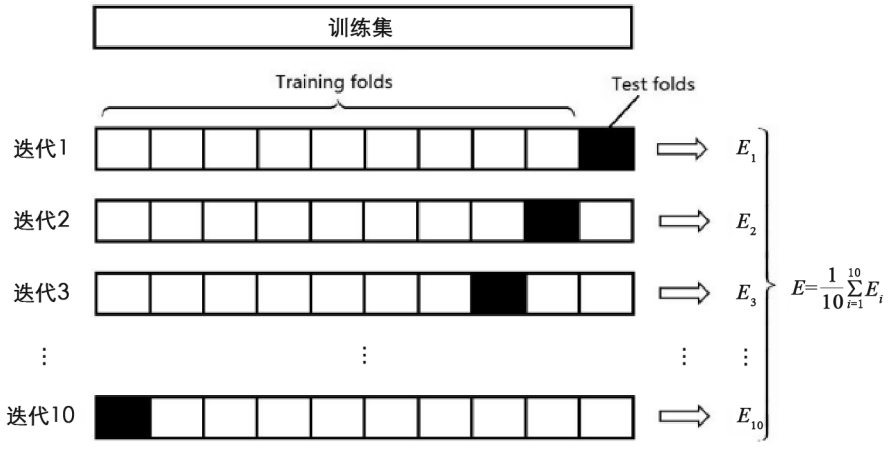

图 5　10 次交叉验证的原理图

具体模型的训练流程分为 8 个步骤.

步骤 1　划分样本集分为训练集和测试集，并采用 10 次交叉验证提取有效数据，避免过拟合问题的出现，并设定标签；

步骤 2　初始化 RF-BA 分类模型参数，设定模型迭代上限、种群规模、个体初始位置和个体速率等；

步骤3 设定BA算法个体最优位置并代入RF中，计算个体适应度值并随机选择当前全局极值；

步骤4 比较当前个体适应度值与当前全局极值，取高者为当前个体极值；

步骤5 迭代计算并更新个体位置与速率，输出RF分类结果到BA中更新适应度值；

步骤6 将更新的适应度值与当前全局极值比较，取高者为更新后个体极值；

步骤7 判定是否达到迭代上限或者全局极值不再更新，若是则终止运算至步骤8，反之返回步骤5；

步骤8 输出最优参数和分类结果.

4 实验结果及分析

4.1 安全性评价

为了更加直观地观测结果，通过以召回率、查准率和F1_score这3个指标与Wazid等[19]所提协议、Lu等[20]所提协议以及Ali等[21]所提协议进行对比，通过对比分析，查看模型效果.

检测各协议对DOS类攻击的效果，由表1的结果可以看出，各个协议的3项评价指标都很高，所有协议的检测率都在99%之上，本研究提出协议的检测效果和其他3类协议相差不大，在召回率和查准率上略高于其他3类协议，可以说明本研究的协议对于DOS攻击的防御效果比其他方法更好.

表1 对DOS类攻击的检测效果

协议	召回率	查准率	F1_score
文献[19]	0.999 987	0.999 910	0.999 948
文献[20]	0.999 965	0.999 988	0.999 977
文献[21]	0.999 974	0.999 986	0.999 980
本研究	0.999 991	0.999 993	0.999 992

对NORMAL类样本的检测(表2)，从整体上看所有的协议都有不错的效果. 由于训练样本相对较大，各协议的检测数值也都在99%以上，但本研究提出的协议在召回率上具有优势，高于其余协议，而在查准率上率略低于文献[21]的协议，与文献[20]的查准率相等且略高于文献[19]，最终F1_score与文献[21]相等并略高于其他协议. 综合来讲，本研究提出的协议效果与其他各个协议之间的差别不算太大，这是由于NORMAL类样本内部的特征区分不显著，使得本研究提出的特征分类方法的优势表现得并不是特别明显，但可以说明本研究的协议对于NORMAL类攻击的检测准确率仍然相对较高.

表2 对NORMAL类样本的检测效果

协议	召回率	查准率	F1_score
文献[19]	0.999 977	0.999 910	0.999 943
文献[20]	0.999 969	0.999 994	0.999 982
文献[21]	0.999 979	0.999 996	0.999 987
本研究	0.999 980	0.999 994	0.999 987

检测各协议对PROBE类攻击的效果(表3)，与前两类数据样本相比，各个协议对此类攻击的检测效果已经有轻微下降了，其他3类协议相对来讲比较稳定，其检测整体数值也都在99.9%以上，本研究的协议检测率是最高的，其召回率和查准率效果最好，F1_score的数值也高于其他3类协议，说明对此类攻击的检测具有良好的效果.

表3 对PROBE类攻击的检测效果

协议	召回率	查准率	F1_score
文献[19]	0.999 589	0.999 186	0.999 387
文献[20]	0.999 659	0.999 259	0.999 459
文献[21]	0.999 689	0.999 445	0.999 567
本研究	0.999 725	0.999 790	0.999 757

在对 R2L 类攻击的检测中(表 4)，相比较于前 3 类攻击，各个协议检测的检测度进一步地下降了，不过所有的协议都保持在 99%以上，从结果上看，本研究提出的协议其召回率与查准率在几种协议中最好，其 F1_score 也显著高于其他协议，表明本研究提出的协议对 R2L 类攻击的检测效果较好.

表 4　对 R2L 类攻击的检测效果

协议	召回率	查准率	F1_score
文献[19]	0.998 987	0.999 001	0.998 994
文献[20]	0.998 887	0.998 995	0.998 941
文献[21]	0.999 012	0.998 956	0.998 984
本研究	0.999 050	0.999 005	0.999 027

在对 U2R 类攻击的检测中，从表 5 的数值可以看出，各个协议的召回率和查准率数值都有了明显的下降，文献[20]和文献[21]召回率、查准率与 F1_score 数值都降到 98%左右，而本研究提出的协议在 4 类协议中检测效果最好，其召回率、查准率和 F1_score 在 99.1%左右，比文献[19]提出的协议的 F1_score 值高 2‰左右，较文献[20]协议高 3‰左右，较文献[21]的协议高 3‰左右，召回率和查准率与 F1_score 数值已具有较高的水平.

表 5　对 U2R 类攻击的检测效果

协议	召回率	查准率	F1_score
文献[19]	0.989 994	0.990 056	0.990 025
文献[20]	0.988 956	0.988 966	0.988 961
文献[21]	0.988 947	0.988 915	0.988 931
本研究	0.991 287	0.991 323	0.991 305

通过对检测数值之间的比较，说明了本研究提出的协议模型的有效性. 由于选择的数据集、数据量和特征集都比较多，其中包含了大量的冗余和相关性不大的特征，造成数据的检测出现了很大的误判，本研究对数据集进行特征提取对减少误判起到了作用，特别是将查准率和召回率结合，取代了原算法以准确率评估去除特征的指标，考虑到了对少部分攻击的忽略，使得最终取得了好的运算效果，这一点也可以通过 F1_score 这个综合指标可以看出. 但是，从整体上看，对 R2L 和 U2R 类攻击的效果较对 DOS 类攻击的效果更差，本研究提出协议模型在查准率和召回率上都有较好的效果，能够有效地防范 R2L 和 U2R 类网络攻击，为网络提供适当的网络防护，提升网络安全水平，减少因网络攻击而造成的损失.

4.2　效率评价

对协议获取用户生物特征的操作不进行比较. 根据文献[18]的实验数据，$T_h \approx 0.32$ ms，$T_E \approx 5.6$ ms，得到本研究所提新协议与文献[19－20]所提协议的计算开销对比(表 6). 其中，T_h 表示执行一次单向 Hash 函数所需时间，T_E 表示执行一次对称加/解密运算所需时间. 通过表 6 的对比结果可发现，本研究所提新协议的计算开销与同类协议相比也具有一定的优势.

表 6　计算开销对比

协议	用户	传感器节点	GWN
文献[19]	$13T_h+2T_E \approx 15.36$	$5T_h+2\ T_E \approx 12.8$	$5T_h+4\ T_E \approx 24$
文献[20]	$7T_h+2\ T_E \approx 13.44$	$4T_h+2\ T_E \approx 12.48$	$8T_h+4\ T_E \approx 24.96$
文献[21]	$6T_h+2\ T_E \approx 13.12$	$4T_h+\ T_E \approx 6.88$	$5T_h+3\ T_E \approx 18.4$
本研究	$12T_h+2\ T_E \approx 15.04$	$8T_h \approx 2.56$	$13T_h+2\ T_E \approx 15.36$

5　总结

为了解决针对多服务器网络安全性低和通信开销大的问题，本研究提出了多服务器交叉组合运算方法，首先通过蝙蝠算法优化的随机森林算法提取权重特征，减少无用特征，对于数据结果的影响，之后用交叉组合的方法，对数据进行比对判别，提升实验的输出结果，通过实验结果表明，本研究提出协议模型

在召回率和查准率上都有着较好的效果，能够有效地防范R2L和U2R类网络攻击，同时其计算开销与同类协议相比也具有一定的优势，说明使用交叉组合运算方法能有效地减少网络中的通信开销，并提升网络安全水平，减少网络攻击的危害，具有一定可行性.

参考文献：

[1] 张翼英，阮元龙，尚静，等. 面向不完备信息的网络入侵检测方法 [J]. 计算机工程与设计，2022，43(5)：1224-1231.

[2] 陈晨，刘曙，王艺菲，等. 基于PSOGWO-SVM的网络入侵检测方法 [J]. 空军工程大学学报(自然科学版)，2022，23(2)：97-105.

[3] 孙海丽，龙翔，韩兰胜，等. 工业物联网异常检测技术综述 [J]. 通信学报，2022，43(3)：196-210.

[4] 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.

[5] XU Z Q，HE D B，HUANG X Y. Secure and Efficient Two-Factor Authentication Protocol Using RSA Signature for Multi-Server Environments [M]//International Conference on Information and Communications Security. Cham：Springer International Publishing，2018：595-605.

[6] AMIN R. Cryptanalysis and Efficient Dynamic 1D Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card [J]. International Journal of Network Security，2016，18：172-181.

[7] LEE C C，LIN T H，CHANG R X. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment Using Smart Cards [J]. Expert Systems with Applications，2011，38(11)：13863-13870.

[8] LI X，MA J，WANG W，et al. A Novel Smart Card and Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environments [J]. Mathematical and Computer Modelling，2013，58(1/2)：85-95.

[9] WANG B，MA M D. A Smart Card Based Efficient and Secured Multi-Server Authentication Scheme [J]. Wireless Personal Communications an International Journal，2013，68(2)：361-378.

[10] LU Y R，LI L X，PENG H P，et al. Cryptanalysis and Improvement of a Chaotic Maps-Based Anonymous Authenticated Key Agreement Protocol for Multiserver Architecture [J]. Security and Communication Networks，2016，9(11)：1321-1330.

[11] 李梦菲，毛莺池，屠子健，等. 基于深度确定性策略梯度的服务器可靠性任务卸载策略 [J]. 计算机科学，2022，49(7)：271-279.

[12] 路亚. MEC多服务器启发式联合任务卸载和资源分配策略 [J]. 计算机应用与软件，2020，37(10)：77-84.

[13] 任仪. 基于区块链与人工智能的网络多服务器SIP信息加密系统设计 [J]. 计算机科学，2020，47(S1)：634-638.

[14] 余宜诚，胡亮，迟令，等. 一种改进的适用于多服务器架构的匿名认证协议 [J]. 吉林大学学报(工学版)，2018，48(5)：1586-1592.

[15] 陈跃，王丽雅，李国富，张林，杨甫，马卓远，高正. 基于随机森林算法的低煤阶煤层气开发选区预测 [J]. 油气藏评价与开发，2022，12(4)：596-603,616.

[16] 何新佳，马中亮，代淑兰. 基于多目标蝙蝠算法的加农炮内弹道性能优化研究 [J]. 弹箭与制导学报，2022，42(1)：71-76,81.

[17] HSIANG H C，SHIH W K. Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment [J]. Computer Standards&Interfaces，2009，31(6)：1118-1123.

[18] WANG D，LI W T，WANG P. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks [J]. IEEE Transactions on Industrial Informatics，2018，14(9)：4081-4092.

[19] WAZID M，DAS A K，ODELU V，et al Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks [J]. IEEE Internet of Things Journal，2018，5(1)：269-282.

[20] LU Y，LI L，PENG H，et al. An Energy Efficient Mutual Authentication and Key Agreement Scheme Preserving Anonymity for Wireless Sensor Networks [J]. Sensors(Basel，Switzerland)，2016，16(6)：E837.

[21] ALI R，PAL A K，KUMARI S，et al. A secure User Authentication and Key-Agreement Scheme Using Wireless Sensor Networks for Agriculture Monitoring [J]. Future Generation Computer Systems，2018，84(C)：200-215.

责任编辑 潘春燕