计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.241200158

电力监控系统网络空间客体协同防御方法

李晓耕[1]　韩　校[1]　肖海怡[2]
1 云南电网有限责任公司云南电力调度控制中心　昆明 650000
2 云南电网有限责任公司楚雄供电局　云南 楚雄 675000

摘　要　电力监控系统是确保电力稳定供应的核心基础设施，当前电力监控系统网络空间客体安全防御手段大多基于固定策略，往往缺少对当前系统环境与安全事件的针对性，且执行这种防御策略也会对系统业务的正常运行产生较大影响。为解决此问题，提出了一种网络空间客体协同防御方法。首先，针对网络威胁阻断，使用IP溯源技术对攻击路径进行重绘，考虑节点与受攻击客体在攻击路径中的跳数以及节点处的网络流量，构造适应度函数，基于改进遗传算法思想确定最优阻断位置；其次，根据网络空间客体类型，制定网络空间客体分类防御策略，引入防御动作关联度计算模型，确定具体的防御动作。仿真实验证明，所提出的网络空间客体协同防御方法在防御动作选取与执行、防御效果等方面均有显著优势，可最大程度降低防御动作对系统正常业务的影响。

关键词：电力监控系统；网络空间；协同防御；遗传算法；关联分析
中图分类号　TM933

Cooperative Defense Method for Network Space Object of Power Monitoring System

LI Xiaogeng[1], HAN Xiao[1] and XIAO Haiyi[2]
1 Yunnan Power Grid Corporation Yunnan Power Dispatch Control Centre, Kunming 650000, China
2. Chuxiong Electric Power Supply Bureau, Yunnan Power Grid, Chuxiong, Yunnan 675000, China

Abstract　The power monitoring system is the core facility for ensuring stable power supply. Currently, most of the network security defense measures for power monitoring systems are based on fixed strategies, which often lack specificity for the current system environment and security events. Moreover, implementing such defense strategies can also have a significant impact on the normal operation of system business. To solve the above problem, a cooperative defense method for network space object is proposed. Firstly, in order to block network threats, IP tracing technology is used to redraw the attack path, taking into account the number of hops between nodes and the attacked object in the attack path, as well as the network traffic at nodes. A fitness function is constructed, and the optimal blocking position is determined based on the idea of improved genetic algorithm. Secondly, based on the types of objects, it formulates defense strategies for classifying objects, introduces a defense action correlation calculation model, and determines specific defense actions. Simulation experiments show that the proposed network space object cooperative defense method has significant advantages in selecting and executing defense actions, as well as defense effectiveness, which can minimize the impact of defense actions on normal system operations.

Keywords　Power monitoring system, Network space, Cooperative defense, Genetic algorithm, Correlation analysis

1　引言

网络空间客体是指一切可能被潜在攻击者利用的设备、信息、应用等数字资产，概括来说，只要是可操作的对象，不管是实体还是属性，都可以称为“网络空间客体”。随着电网朝着数字化、智能化的方向发展，电力系统面临着比以往更加复杂多样的网络攻击威胁，由于其自身的重要地位，如何协同环境内不同客体共同抵御网络攻击是提升网络空间客体安全性的重要研究方向。

当前，电力监控系统网络空间客体防御手段较为单一固化，所采取的安防手段大多基于设备或固定策略，容易因为设备失效、流量堵塞等因素导致防御策略可靠性较差，且往往会由于执行不当的防御策略而对系统当前运行状态产生较大影响。

针对上述问题，综合考虑各类因素，本文提出一种电力监控系统网络空间客体协同防御方法。该方法旨在实现电力监控系统内安防资源的互补，首先研究基于改进遗传算法的阻断位置选取方法，综合考虑执行防御措施的代价与收益，选取最适合执行防御措施的位置；然后定义分级防御策略及其触发机制进行威胁防御，并引入关联度计算选取具体的防御动作；最后在所搭建的仿真环境中验证协同防御策略的可靠性。

2　研究背景

传统网络安全威胁防御手段在面对新型网络攻击时面临

基金项目：中国南方电网有限责任公司科技项目(0500002023030301XT00152)
This work was supported by the China Southern Power Grid Co., Ltd. (0500002023030301XT00152).
通信作者：李晓耕(1067688698@qq.com)

极大挑战，近年来，随着攻击手段逐步朝着针对性强、威胁系数高的方向发展，国内外研究人员依托于传统的网络安全防御方法，针对电力监控系统安全防御技术开展了一些研究。

现有的电力监控系统安全协同防御方案通过进行动态资源分配来提高检测性能，但大多都没有考虑资源受限条件下的资源配置优化问题。Xia 等考虑了资源限制的影响，提出了一种基于共享策略的两级协同防御资源分配方案，该方案能更快地实现防御方与攻击者之间的纳什均衡，进而促进检测资源的更新，实现在资源受限的情况下获得最优的检测策略[1]。为了更好地抵御洪泛攻击，Saraswathi 提出了一种多级协同防御机制，该机制由两级缓解机制构成，通过协同源端和目的端进行洪泛攻击的识别与阻断，并将其引导到更接近攻击起点的地方[2]。Li 等提出了一种基于异常驱动的动态协同防御模型（ADCD），该模型能够将异常作为防御驱动因素，用来识别攻击行为并评估系统的安全状态。此外，该模型可以将网络协同防御（NCD）和移动目标防御（MTD）相结合来防御已知或未知的网络攻击[3]。Wei 等基于主次设备一体化思想，提出了分布式变电站区域保护一体化设备框架，采用点对点模型和基于 VLAN 的网络对网络模型，并提出了一种基于分布式协同一体化设备集群的变电站区域协同防御保护策略[4]。Zhu 等提出了一种针对协同防御战略的冲突检测方法，该方法在对协同防御策略进行形式化描述的基础上，根据防御动作与系统状态的关系，分析了策略冲突的类型，并通过建立防御动作之间的时间关系来模拟策略执行从而检测冲突[5]。传统电力监控系统安防手段不足以应对新型网络攻击，对此，Cai 提出了一种协同防御方法，构建了信息物理协同的纵深防御体系来应对网络攻击[6]。Li 等提出了一种多级后备自动阻断系统，该系统能够通过入侵检测、路径重构、策略下发以及分布式阻断等措施对网络攻击进行阻断[7]。文献[8]基于软件定义安全架构，将传统硬件或虚拟化安全设备的控制层和安全层分离，由安全资源池提供安全防护，安全控制平台负责管理和策略下发，根据不同防护需求编排安全业务，构建多种安全防护机制，实现内外协同、上下联动的网络安全协同防御能力。

网络空间客体的安防要求与传统信息安全系统存在差异性，现有的防御手段并不能完全满足电力监控系统网络空间客体安全防御的需求[9-11]，且现有的安全防御措施大多是基于各类安防措施的累加、安防设备的杂糅，存在单一、固化、系统性低的缺点，已很难满足现阶段网络空间客体安全发展的需求[12]。

3 协同防御总体机制

本文提出的电力监控系统网络空间客体协同防御方法的流程图如图 1 所示。

网络空间客体遭遇网络攻击时，会产生海量的告警和审计日志数据，对数据中包含的的告警信息数量、频发程度、告警事件类型、来源等安防信息进行收集，并将这些威胁信息及安全事件数据经统一标准化处理后进行上报。随后引入改进遗传算法，选取最适合执行阻断动作的位置，基于所选取的网络空间客体的类型，并结合关联度计算的方法，选取适当的防御动作进行下发，网络空间客体执行防御动作，防止威胁事件的进一步扩散。

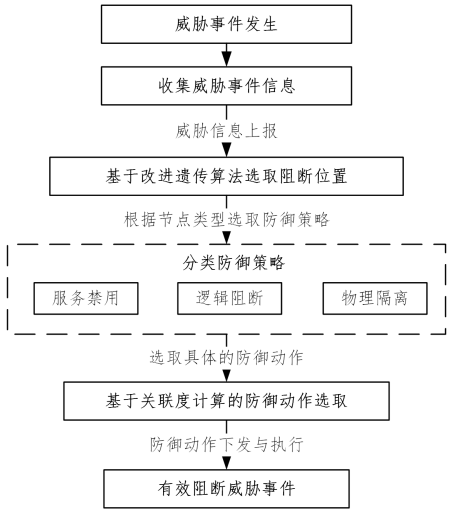

图 1 总体工作流程图

Fig. 1 Overall workflow diagram

4 阻断位置选择策略

网络威胁阻断是研究电力监控系统网络空间客体安全防御的重要环节[13]，现有的威胁阻断方法大多基于固定的对象划分级别并执行防御措施，其机制较为固化，且未考虑执行防御措施对系统业务的影响程度[14]。遗传算法通过模拟自然生物进化的过程来搜索最优解，将最优值的求解过程用生物进化中选择、交叉、变异的过程模拟出来。针对阻断节点的选取这一问题，通过遗传算法的选择、交叉、变异等步骤，综合考虑执行防御措施的代价与收益，能够快速得到不同的阻断节点集合，实现对最优阻断位置的快速搜索。

阻断节点集合的选择是通过对节点执行防御策略后的防御效果进行预估来实现的，而防御效果可以看作是由防御收益和防御代价决定的[15]。其中，防御收益是指对威胁事件的阻断与控制效果；而防御代价是指对客体执行防御措施时，可能产生的性能开销和误报开销；性能开销指的是在执行防御策略的过程中可能会对网络环境造成的负面影响，例如报文匹配造成的报文传输延迟或计算存储开销，执行某一防御措施的性能开销可近似看作与执行防御策略的客体节点数量成正比[16]；误报开销是指在区分攻击流量和正常流量的过程中由于区分度太小，造成流量类型的误判，从而将正常流量阻挡隔绝所产生的开销。

针对某一节点是否适合执行防御策略，通过从途经该节点的正常、异常流量数据和当前阻断节点与受感染客体之间的距离 3 个方面出发，构造适应度函数。其中，正常流量数据能够反映该节点所处位置在整体环境中的重要程度以及对系统正常业务的影响程度；异常流量数据表示通过该节点的异常流量，该指标越高则代表当前节点需要阻断的优先级更大；而对于安防环境中出现的威胁事件，将其遏制在更小的范围内会大大缩小对系统的负面影响，因此需要对当前阻断节点与受感染客体之间的距离加以考虑。基于改进遗传算法选取阻断节点集合，在交叉概率和变异概率的选择方面，考虑当前个体适应度值的变化趋势，自适应改变交叉概率和变异概率。相比于将交叉概率和变异概率设为定值，该方法能够在增加种群多样性、避免陷入局部最优的同时，最大程度地保护已获得的优良基因型不被破坏，工作流程图如图 2 所示。

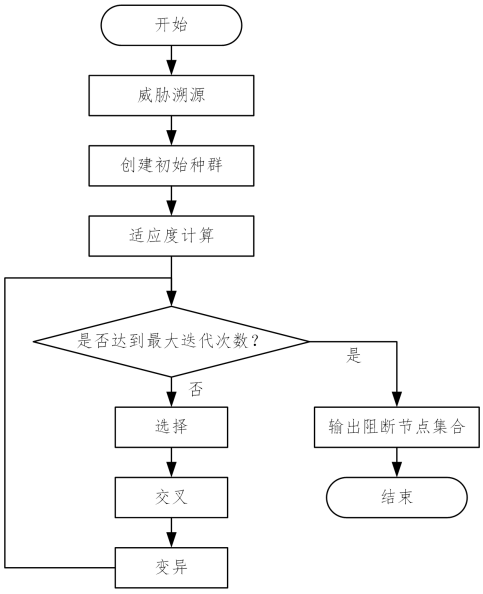

图 2 遗传算法选取阻断节点集合的流程图

Fig. 2 Flowchart of genetic algorithm to select the set of blocking nodes

4.1 威胁溯源

针对电力监控系统安防环境特点,将电力监控系统网络空间客体设备看作是攻击者执行攻击行为的节点与防御方进行威胁阻断的节点。使用 IP 溯源技术对攻击路径进行重绘,综合考虑基于概率性标记的溯源方法和基于包摘要的溯源方法,在实现单包溯源的同时,路由开销也较少[17-18]。具体来说,该方法通过包标记和包摘要的交替工作实现,将电力监控系统中的路由器看作是攻击路径的每一跳,包标记方法的标记信息通常可以保存三跳,因此设定在溯源过程中,每隔两次包标记动作后执行一次包摘要动作[19]。

4.2 初始化种群

针对当前电力监控系统安防环境内的客体节点是否需要被阻断的问题,将电力监控系统安防环境中所有节点的集合记作 $Nlist$,表示为 $Nlist=\langle N_1,N_2,\cdots,N_n\rangle$,其中,$n$ 为当前环境内有能力执行防御策略的客体总数。对于集合中的每个元素 $N_k(k=1,2,\cdots,n)$,其代表了环境中第 k 个客体节点是否需要被阻断,即 $N_k\in\{$'无需阻断','需要阻断'$\}$。

随后,对 $Nlist$ 进行二进制编码,将其转化为一个 n 位的二进制编码串 C,表示为 $C=\langle c_1,c_2,\cdots,c_n\rangle$,对于 C 中的每一位 $c_k(k=1,2,\cdots,n)$,其二进制编码的方式如式(1)所示:

$$\begin{cases} N_k=\text{'无需阻断'},c_k=0 \\ N_k=\text{'需要阻断'},c_k=1 \end{cases} \tag{1}$$

C 中的每一位同 $Nlist$ 中的元素一一对应,将 C 看作是遗传算法中的个体。接下来确定遗传算法的种群规模 NUM,即确定种群中个体的数量。设置遗传算法种群规模 $NUM=30$,也就是初始化生成 30 个随机个体,其含义为生成 30 种不同的客体节点阻断策略集合,表示为 $G=\{C_1,C_2,\cdots,C_{\mathrm{NUM}}\}$,G 表示当前种群,用 $C_l(l=1,2,\cdots,NUM)$ 表示该种群中的个体。

4.3 适应度评判因素的选取与归一化计算

针对个体 $C_l(l=1,2,\cdots,NUM)$ 中所有值为 1 的基因位所对应的客体节点,从该节点与受攻击设备在攻击路径中的距离以及该节点处正常和异常网络流量多少这 3 个因素入手构造适应度函数。这 3 个适应度评判因素是完全不同的属性,具有不同的量纲,无法直接对它们进行加权求和,因此需要对其进行归一化处理。对于当前个体中值为 1 的基因位数量 m,其代表当前被认为需要在此处执行防御动作的客体节点个数。将每个客体节点对应各个适应度评判因素的取值构建矩阵 $\boldsymbol{F}$:

$$\boldsymbol{F}=\begin{bmatrix} A_1 & D_1 & N_1 \\ A_2 & D_2 & N_2 \\ \vdots & \vdots & \vdots \\ A_m & D_m & N_m \end{bmatrix} \tag{2}$$

其中,矩阵第一列元素 A_i 代表个体 C_l 中第 i 个需要被阻断的客体节点在异常流量因素方面的赋值,矩阵第二列的元素 D_i 代表个体 C_l 中第 i 个需要被阻断的客体节点在与攻击源头距离因素方面的赋值,矩阵第三列的元素 N_i 代表个体 C_l 中第 i 个需要被阻断的客体节点在正常流量因素方面的赋值。对矩阵的每一列元素按照式(3)进行归一化操作:

$$\begin{cases} A_i'=\dfrac{A_i-A_{\min}}{A_{\max}-A_{\min}} \\ D_i'=\dfrac{D_i-D_{\min}}{D_{\max}-D_{\min}} \\ N_i'=\dfrac{N_i-N_{\min}}{N_{\max}-N_{\min}} \end{cases} \tag{3}$$

其中,$A_{\max}$ 和 $A_{\min}$ 分别代表异常流量因素的最大、最小取值;$D_{\max}$ 和 $D_{\min}$ 分别代表与攻击源头距离因素的最大、最小取值;$N_{\max}$ 和 $N_{\min}$ 分别代表正常流量因素的最大、最小取值;A_i',D_i',N_i' 代表矩阵 $\boldsymbol{F}$ 中元素的归一化结果。

4.4 适应度计算

基于得到的适应度评判因素归一化结果,对 C_l 中所有值为 1 的位所对应的阻断节点,从该节点与受攻击客体在攻击路径中的跳数以及该节点处的网络流量等方面入手,构造适应度函数:

$$f(x)=\frac{1}{m}\sum_{i=1}^{m}(\alpha\times A_i'-\beta\times D_i'-\gamma\times N_i') \tag{4}$$

适应度的值越大,代表当前个体对应的阻断方案越优,即同时考虑对系统业务的影响度和对威胁阻断的效果,并实现了二者之间的最优平衡。A_i' 与适应度函数的值正相关,而 D_i' 和 N_i' 与适应度函数的值负相关。3 个适应度评判因素在适应度计算中所占权重默认取 $\alpha=\beta=\gamma=1/3$。

4.5 选择策略

选择操作是建立在种群中个体适应度评估基础上的,采用轮盘赌选择法计算种群中各个个体的适应度值,每个个体进入下一代的概率等于它的适应度值与整个种群中个体适应度值和的比例。针对个体 C_l,计算其被选择进入下一代的概率 $P_S(C_l)$:

$$P_S(C_l)=\frac{f(C_l)}{\sum_{l=1}^{NUM}f(C_l)} \tag{5}$$

通过计算个体被选择进入下一代的概率 $P_S(C_l)$,该概率值可看作是每个个体在轮盘中的占比,基于此概率值进行选择操作,选取父代和母代进入交配池,能够使选取更优个体的概率增加。由于种群规模 $NUM=30$,因此对初始化种群执行 30 次选择操作,得到选择操作的结果表示为 $G'=\{C_1',C_2',\cdots,C'_{\mathrm{NUM}}\}$,$G'$ 表示选择操作得到的种群,用 $C_l'(l=1,2,\cdots,NUM)$ 表示该种群中的个体。此外,对于当前种群中已

获得的优良基因型，为避免其在接下来的交叉、变异操作中遭到破坏，本文引入最优选择法，将当前种群中适应度最高的个体完整复制到下一代种群中，在增加种群多样性的同时，更大程度地保留优秀个体的结构。

4.6 交叉策略

交叉操作即按照交叉概率判断两个父代和母代是否会发生交叉。令交叉概率根据当前选择的父代、母代的适应度大小自适应变化，自适应交叉概率$P_C(C_l)$的计算式为：

$$P_C(C_l)=\begin{cases}P_C^{\max}-\dfrac{f_C^{\max}-f_{\text{avg}}}{f_{\max}-f_{\text{avg}}}(P_C^{\max}-P_C^{\min}), & f_C^{\max}>f_{\text{avg}}\\ P_C^{\max}, & f_C^{\max}\leqslant f_{\text{avg}}\end{cases} \tag{6}$$

其中，$P_C(C_l)$表示个体C_l的自适应交叉概率；$P_C^{\max}$和$P_C^{\min}$分别表示自适应交叉概率$P_C(C_l)$的取值上界和下界，本文取$P_C^{\max}=0.9$，$P_C^{\min}=0.5$；$f_C^{\max}$表示参与交叉操作的父代、母代中适应度值较大一方的适应度值，f_{avg}表示当前种群适应度值的平均值，$f_{\max}$表示当前种群中适应度值的最大值。

随后，生成一个 0～1 之间的随机数 $Rand$，若 $Rand\leqslant P_C(C_l)$，则对当前父代和母代执行交叉操作，否则不执行交叉操作。由于遗传算法的个体由二进制编码串组成，且该编码串在电力监控系统网络空间客体安全防御背景下具备一定的内在含义，单点交叉法在交叉的过程中能够将个体受到的破坏最小化，故单点交叉法是最适合本文的交叉算子。具体来说，通过随机选取一个大于 1、小于种群规模 NUM 的整数作为发生交叉的位置，并在该位置上同时对父代子代个体的序列进行分割并交换序列右侧的部分。得到交叉操作的结果表示为 $G''=\{C_1'',C_2'',\cdots,C''_{\text{NUM}}\}$，$G''$表示交叉操作得到的种群，$C_l''(l=1,2,\cdots,NUM)$表示该种群中的个体。

4.7 变异策略

变异操作即按照变异概率判断当前个体的某个基因位是否会发生变异，变异概率可以根据当前个体的适应度大小而自适应变化，自适应变异概率$P_M(C_l)$的计算式为：

$$P_M(C_l)=\begin{cases}P_M^{\max}-\dfrac{f_M-f_{\text{avg}}}{f_{\max}-f_{\text{avg}}}(P_M^{\max}-P_M^{\min}), & f_M>f_{\text{avg}}\\ P_M^{\max}, & f_M\leqslant f_{\text{avg}}\end{cases} \tag{7}$$

其中，$P_M(C_l)$表示个体C_l的自适应变异概率；$P_M^{\max}$和$P_M^{\min}$分别表示自适应变异概率$P_M(C_l)$的取值上界和下界，本文取$P_M^{\max}=0.005$，$P_M^{\min}=0.001$；f_M表示变异个体的适应度值，f_{avg}表示当前种群适应度值的平均值，$f_{\max}$表示当前种群中适应度值的最大值。

随后，生成一个 0～1 之间的随机数 $Rand'$，若 $Rand'\leqslant P_M(C_l)$，则继续随机选取一个大于 1、小于 n 的整数作为发生变异的位置，对该基因位执行 0→1 或 1→0 的变异操作，否则不进行变异操作。得到变异操作的结果表示为 $G'''=\{C_1''',C_2''',\cdots,C_{\text{NUM}}'''\}$，$G'''$表示经变异操作后得到的种群，$C_l(l=1,2,\cdots,NUM)$表示该种群中的个体。

4.8 迭代结束条件判定

将算法的结束条件定义为：已满足最大迭代次数且最终输出的适应度值最大的个体已持续 20 代未发生改变，将最大迭代次数设置为 180。若已满足上述结束条件，则输出适应度值最大的个体 Best；若未达到最大迭代次数，则重复上述选择、交叉、变异的过程。最优个体 Best 的定义如式(8)所示：

$$Best=\{C_b\mid f(C_b)=MAX\{f(C_1),f(C_2),\cdots,f(C_{\text{NUM}})\}\},b=1,2,\cdots,NUM \tag{8}$$

最终得到最优个体 Best 的表示形式为一组由“0”和“1”组成的二进制编码串，其中，值为 1 的位所对应的客体节点为最终确定需要被阻断的客体节点。将 Best 解码为$Nlist_{\text{Best}}$：

$$Nlist_{\text{Best}}=\{N'_1,N'_2,\cdots,N'_n\} \tag{9}$$

其中，对于集合中的每个元素$N'_k(k=1,2,\cdots,n)$，$N'_k\in\{$‘无需阻断’,‘需要阻断’$\}$。

对于集合中的元素N_k'，若$N_k'=$‘需要阻断’，则对于电力监控系统中的客体节点 k，选定该客体节点作为执行防御手段的位置，随后基于其客体类型，选取防御策略大类，再结合当前的威胁事件相关信息进行具体防御动作的选取，并在该节点处执行所选取的防御动作，对威胁进行阻断。

5 分类防御策略制定

收集电力监控系统网络空间客体上报的安防信息，包括异常事件、告警信息、威胁来源、攻击目标等。当所上报信息满足一定条件时，按照表 1 所列情况执行对应的防御策略。所执行的防御策略按照所针对客体类型的不同以及执行策略的触发条件，可分为服务禁用、逻辑阻断和物理禁用三大类。

表 1 网络空间客体分类防御策略

Table 1 Defence strategies for object classification in cyberspace

防御策略	对象	防御动作
服务禁用	主机设备	USB 外设禁用、串/并口禁用、网卡禁用、用户强制登出、限制外部连接、结束异常应用进程
逻辑阻断	安防设备	关闭安防设备端口、增加安防设备访问控制策略、关闭/删除纵向加密装置的隧道、修改/删除纵向加密装置的策略
物理隔离	网络设备	关闭网络设备端口、增加网络设备访问控制策略、去除网络设备 MAC 地址绑定

5.1 服务禁用

服务禁用策略主要用于解决单台主机类型客体中出现的异常事件，用于禁用该客体上的服务或直接将该客体隔离。一旦发现未授权 USB 接入、串/并口接入、非法用户登录、用户违规操作、不安全的外部连接或登录会话等操作事件发生，则针对环境中的主机类型客体下发服务禁用的防御策略，由 Agent 程序执行。

5.2 逻辑阻断

逻辑阻断策略主要针对站内的防火墙、纵向加密装置等安防类型客体，通过软件或配置在逻辑层面将受到威胁的区域进行隔离。一旦发现诸如非法的外部连接或远程登录操作等异常事件，或是在服务禁用防御策略失效的情况下，通过对安防设备下发逻辑阻断策略的方式进行连接限制。

5.3 物理隔离

当服务禁用、逻辑阻断策略防御效果不佳，且经分析判定电力监控系统环境内某一个或多个不同区域的客体存在多重安全隐患，则采取具备更高层次安全防护能力的物理隔离策略，将受到威胁的区域内所有客体的网络隔离。

6 基于关联度计算的网络空间客体防御动作选取方法

在确定了防御策略后，针对服务禁用、逻辑阻断、物理隔

离三大类防御策略，进行防御策略下具体防御动作的选取。引入关联规则分析法，结合安全特征参数与防御动作进行关联度计算，选取关联度值最高的防御动作作为优先级最高的防御动作，并执行该防御动作。

6.1 构造观测矩阵并初始化

针对所确定的客体节点防御策略，构造防御动作集合，分析并计算安全特征参数与防御动作之间的关联性，所需考虑的安全特征参数共 5 项：执行防御动作对系统业务的影响程度、防御动作的可靠性、防御动作的时效性、该防御动作执行所需频次/时长、该防御动作与当前威胁事件的适配性。

防御动作集合中包含 n 项可行的防御动作，n 的取值按照不同的防御策略大类取值如下：当防御策略为服务禁用时，$n=6$；当防御策略为逻辑阻断时，$n=4$；当防御策略为物理隔离时，$n=3$。构造观测矩阵 $\boldsymbol{A}$：

$$\boldsymbol{A}=[x_i(j)]=\begin{bmatrix} x_1(1) & x_2(1) & \cdots & x_5(1) \\ x_1(2) & x_2(2) & \cdots & x_5(2) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(n) & x_2(n) & \cdots & x_5(n) \end{bmatrix},$$

$$i=1,2,\cdots,5;j=1,2,\cdots,n \tag{10}$$

其中，矩阵 $\boldsymbol{A}$ 的每一列代表 n 项可行的防御动作对应某项安全特征参数的适配性集合，而矩阵元素 $x_i(j)$ 代表第 j 种防御动作对于第 i 项安全特征参数的适配性，在对观测矩阵进行初始化指标赋值方面，赋值越高，代表防御动作对安全特征参数的适配性更好。

6.2 参考序列确定

从观测矩阵 $\boldsymbol{A}$ 中提取每一列的最大值组成参考序列 LIST，如式(11)和式(12)所示：

$$LIST=\{x_1,x_2,x_3,x_4,x_5\} \tag{11}$$

$$x_i=\max\{x_i(1),x_i(2),\cdots,x_i(n)\},i=1,2,\cdots,5 \tag{12}$$

6.3 关联度系数计算

逐一计算防御动作集合中每项安全特征参数对应参考序列的绝对值后，计算得到最大-最小标准化参数，随后通过式(13)进行关联系数的计算：

$$\xi_i(j)=\frac{\min_i\min_j|x_i(j)-x_i|+\rho\times\min_i\min_j|x_i(j)-x_i|}{|x_i(j)-x_i|+\rho\times\min_i\min_j|x_i(j)-x_i|} \tag{13}$$

其中，ρ 表示分辨系数，此处取 $\rho=0.5$；$\xi_i(j)$ 表示第 i 个安全特征参数与第 j 个防御动作间的关联系数值。

6.4 加权关联度计算

不同的安全特征参数在对网络安全事件的影响方面占不同的权重，故需要进行加权计算，如式(14)所示，通过计算加权关联度并取均值，能够反映不同防御动作与参考序列间的关联关系，从而得到整个网络安全事件与各个防御动作间的关联度，选取最合适的防御动作。

$$S_j=\frac{1}{5}\sum_{i=1}^{5}W_i\cdot\xi_i(j),i=1,2,\cdots,5;j=1,2,\cdots,n \tag{14}$$

其中，W_i 表示第 i 个安全特征参数在整个网络安全事件影响中所占权重，S_j 表示第 j 个防御动作最终的关联度值。

得到关联度值的结果序列 $S=\{S_1,S_2,\cdots,S_n\}$，将序列 S 中的关联度值由大到小进行排列，选择关联度最大的防御动作执行。

6.5 防御动作的执行

对于式(9)得到的集合 $Nlist_{\text{Best}}$，针对集合中的元素 N_k' $(k=1,2,\cdots,n)$，若 $N_{k'}=$‘需要阻断’，则对于客体节点 k，选定该客体节点作为执行防御动作的位置，并选取本节计算得到的结果序列 S 中关联度最大的防御动作，对客体节点 k 执行该防御动作。同理，对于集合 $Nlist_{\text{Best}}$ 中被认为需要阻断的其余客体节点同样经关联度计算，选取在该节点处最适合执行的防御动作。

7 仿真实验

7.1 实验环境

本文搭建如图 3 所示的仿真环境用于模拟电力监控系统网络空间客体安防环境，分为主站域和厂站域。

7.2 防御动作的选取与执行

经由威胁溯源重构攻击路径，并经由遗传算法选取最适合执行防御动作的客体集合后，进行防御动作的执行。在仿真环境中，模拟业务主机 A 发生 USB 无线网卡非法接入事件，依照网络空间客体分级防御策略，基于业务主机 A 的客体类型判断，应对其执行“服务禁用”防御策略。在确定防御策略大类后，进行关联度计算选取具体的防御动作。

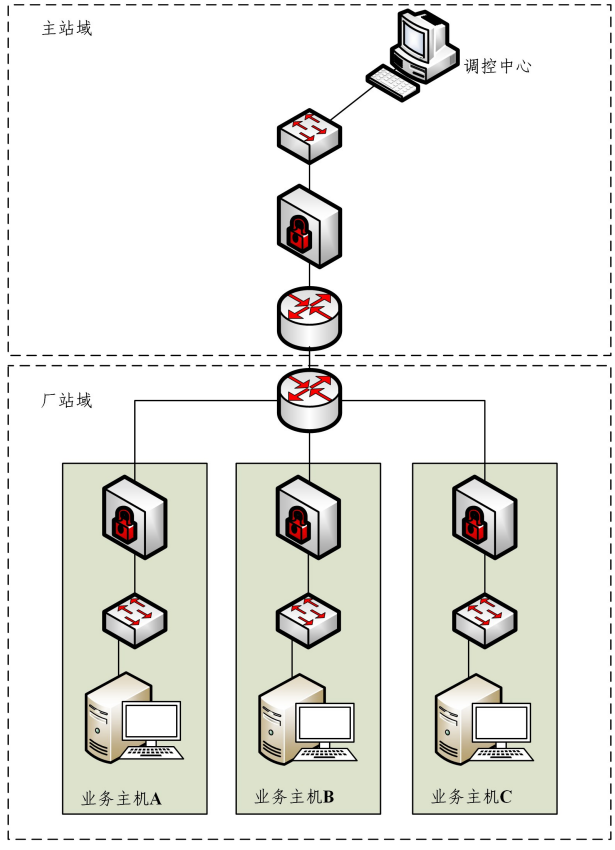

图 3 仿真环境拓扑

Fig. 3 Simulation environment topology

针对 USB 无线网卡非法接入事件，选取网卡禁用、USB 外设禁用、上端交换机端口关闭、纵向隧道阻断和主站域路由端口阻断 5 项待选防御动作进行关联度的计算，随后对上文提到的 5 项安全特征参数与上述防御动作进行关联程度的评分并构造观测矩阵，如表 2 所列。其中，权重 W_i 是根据所针对的安防环境拓扑以及安防需求来进行赋值的，表 2 中的取

值为针对图 3 所示拓扑的权重赋值情况。

表 2 观测矩阵赋值

Table 2 Observation matrix assignments

USB 无线网卡非法接入	业务影响度	可靠性	时效性	频次/时长	适配性
网卡禁用	100	80	70	100	100
USB 外设禁用	100	50	60	100	90
上端交换机端口关闭	90	80	70	80	90
纵向隧道阻断	70	90	80	60	80
主站域路由端口阻断	50	100	90	30	70
权重(W_i)	30	15	15	20	20

随后计算关联系数，关联系数计算结果矩阵如图 4 所示。

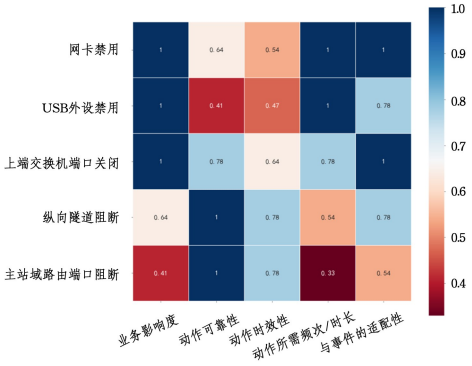

图 4 关联系数计算结果矩阵

Fig. 4 Matrix of results of linkage calculation

经由加权关联度计算后得到各个防御动作最终的关联度，S={87.7,78.8,86.9,72.3,56.4}，因此，选取关联度数值最大的“网卡禁用”作为当前选定客体的防御动作，并对业务主机 A 执行，若因某些因素导致“网卡禁用”动作失效，则按照关联度计算结果大小依次执行其余防御动作，直至消除受感染客体的威胁。

7.3 协同防御效果测试仿真实验

随后，对仿真环境中的业务节点进行协同防御效果测试，针对仿真环境中的不同客体模拟不同的安全事件，通过 3 个案例分别测试服务禁用、逻辑阻断、物理隔离防御策略的有效性。

对于上述 3 类威胁事件，各自进行 20 次仿真实验，用于测试协同防御机制对不同范围、不同程度威胁事件的威胁阻断成功率。下面对 3 种威胁事件各自选取一个典型攻击场景，对所选取的场景和协同防御机制的阻断效果进行说明。

1)针对单一客体、单一威胁的威胁防御：仿真环境中业务主机 A 发生违规外联行为。下发防御动作，阻断其 SSH 链路，成功阻止异常行为，在针对该类威胁事件进行的 20 次仿真实验中，协同防御机制实现了对威胁事件的 100%阻断成功率。

2)针对单一客体、多种威胁的威胁防御：仿真环境中业务主机 B 同时发生非法登录尝试、权限变更、文件篡改与销毁等一系列违规操作，“网卡禁用”动作失效，则下发防御动作，关闭该业务主机上联交换机端口，成功阻止威胁事件进一步扩大。在针对该类威胁事件进行的 20 次仿真实验中，协同防御机制同样实现了对威胁事件的 100%阻断成功率。

3)针对区域级、复合型威胁事件的威胁防御：仿真环境中业务主机 C 发生复合型威胁事件，“网卡禁用”“上联交换机端口关闭”动作失效，且威胁呈现逐步扩散的态势，下发防御动作执行纵向隧道的阻断，对业务主机 C 所在区域的网络进行切除，实现区域级隔离；若发现其余区域的客体已经受到威胁影响，则考虑针对其他区域站执行纵向隧道的阻断或是直接下发主站域路由端口阻断动作，隔离整个厂站域。在针对该类威胁事件进行的 20 次仿真实验中，协同防御机制实现了对威胁事件的 90%阻断成功率。协同防御机制失效的仿真案例，是因为在安防设备的阻断动作选取上出现了错误。对于此问题，将所选取的“增加安防设备访问控制策略”更改为“关闭安防设备端口”，最终实现了对威胁事件的阻断。

7.4 防御结果对比仿真实验

当前，电力监控系统广泛采用的网络空间客体威胁防御机制是基于网络攻击的影响范围和程度进行划分的，可分为 3 级：

1)单设备级(1 级)阻断：针对影响范围只是单台设备的事件、威胁，需要进行的阻断。

2)局部级(2 级)阻断：针对影响范围是局部的，一个网段内多台设备的事件、威胁，需要进行的阻断。

3)区域级(3 级)阻断：针对影响范围是区域中的多个网段、多台设备的事件、威胁，需要进行的阻断。

将所提出的协同防御机制和当前广泛采用的基于固定策略的三级阻断机制进行仿真比较，观察两种方案在执行阻断期间仿真环境中数据包传输成功率，能够比较执行两种阻断方案对系统正常业务的影响程度。具体来说，从仿真环境中最底层的客体设备发送数据包模拟系统正常业务，通过在模拟主站域的调控中心接收数据包判断系统业务的执行情况。

仿真环境中某台客体设备发生复合型网络威胁事件，且威胁沿横向、纵向的方向蔓延至厂站域内的不同区域，导致厂站域中大量设备感染，并呈现进一步扩散的态势。

将仿真环境中数据包传输成功率作为对比指标，观察模拟攻击行为前后 15 分钟内每分钟的数据包传输成功率，数据包传输成功率对比折线图如图 5 所示。在前 5 分钟，系统检测到攻击行为，攻击行为对数据包的传输造成了影响，导致传输成功率下降；随后，在第 6 分钟执行防御动作，使得环境内的一些客体设备被阻断，造成数据包传输成功率下降，而三级阻断方案直接断开厂站域路由器下联端口，导致厂站域整体与主站域断开，数据包传输成功率变为 0%；第 10 分钟，由于防御动作的执行，仿真环境内的客体设备逐渐恢复正常，并解除阻断，恢复正常状态，数据包传输成功率也恢复至正常数值。

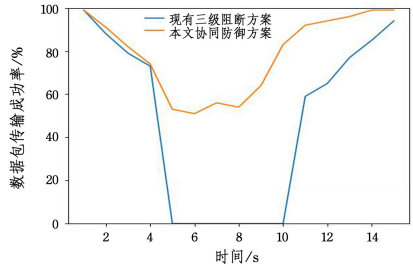

图 5 数据包传输成功率对比

Fig. 5 Comparison of packet transmission success rate

由上述对比实验可以看出，所提出的协同防御方案在执行期间相比现有的威胁防御机制能够自适应地选择阻断位置，使得其在维持电力监控系统系统业务完整性、稳定性方面得到了改进。

结束语 为解决当前电力监控系统网络空间客体防御手段较为单一固化的问题，本文在现有防御策略的基础上进行分级防御策略的研究。首先基于改进遗传算法进行阻断节点的选取，找到最适合执行防御动作的位置，同时自适应选择交叉、变异概率，相比现有方法，所提方法在增加种群多样性、避免陷入局部最优的同时，能最大程度地保护已获得的优良基因型不被破坏；其次，针对不同业务节点的类型，定义分类防御策略及其触发条件，给出了服务禁用、逻辑阻断、物理隔离三大类防御策略；随后基于关联度计算的方法选取具体的防御动作并执行，并在所搭建的电力监控系统仿真环境中进行了实验验证，结果表明所提出的方法细化了防御策略的执行条件，在阻断网络空间客体安全威胁的基础上，将防御动作的执行限制在尽可能小的范围内，最大程度降低防御动作对系统正常业务的影响。后续将进一步验证所提方法在电力监控系统的实际应用效果，并尝试进行分级分区自适应协同防御方面的研究。

参 考 文 献

[1] ZHOU Q X et al. Detection resource allocation scheme for two-layer cooperative IDSs in smartgrids[J]. Journal of Parallel and Distributed Computing, 2021, 147: 236-247.

[2] SARASWATHI S. Enforcing a source-end cooperative multilevel defense mechanism to counter floodingattack[J]. Computer Systems Science and Engineering, 2023, 44(1): 67-79.

[3] LI L X, ZHANG B, WU H M, et al. A novel network proactive defense model: anomaly driven dynamic cooperative defense model[C]// IOP Conference Series: Materials Science and Engineering. 2018.

[4] FANRONG W et al. Substation area joint defensive protection strategy based on distributed cooperative all-in-onedevice[J]. Journal of Modern Power Systems and Clean Energy, 2016, 4(3): 467-477.

[5] HONG Q Z, ZI W, WEI L, et al. A method of conflict detection for cooperative defense strategy in power industrial control system[J]. International Conference on Advanced Cloud and Big Data, 2020.

[6] CAI X P. Research on information-physical collaborativedefence methods for power system cyber attacks[D]. Najjing: Southeast University, 2021.

[7] LI W, HE H. Design and implementation of a multi-level backup automatic blocking system for source-network-load interaction [J]. Computer Applications and Software, 2020, 37(9): 302-309, 333.

[8] XIAO Y X, MU T, QIN Z Y, et al. Exploration of water resources network security collaborative defence system based on software defined security[J]. Pearl River, 2023, 44(2): 122-128, 133.

[9] TAN S S. Design and implementation of an attack blocking system for virtual-real networks[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[10] WANG Z, WANG Z H, HAN Y, et al. Research on multi-layer collaborativedefence model for power system network security [J]. Computer Engineering, 2021, 47(12): 131-140.

[11] SONG L, FAN Y, LIU M, et al. State estimation method of a new energy power system based on SC-DNN and multi-source datafusion[J]. Power System Protection and Control, 2023, 51: 177-187.

[12] LIU J Q, W R. An overview of new information transmission methods for powersystems[J]. Journal of Northeast Dianli University, 2024, 44(4): 1-8, 76.

[13] ZHANG D, ZHANG Y, ZANG X X. Anomalous Intrusion Detection Method for Surveillance Video Based on Self-Organising Mathematical Models[J]. Journal of Northeast Dianli University, 2022, 42(4): 63-69.

[14] HAN Y, WANG Y, CAO Y, et al. A novel wrapped feature selection framework for developing power system intrusion detection based on machine learning methods[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2023, 53(11): 7066-7076.

[15] YAN B, JIANG Z, YAO P, et al. Game Theory based optimal defensive resources allocation with incomplete information in cyber-physical power systems against false data injection attacks [J]. Protection and Control of Modern Power Systems, 2024, 9(2): 115-127.

[16] LIU C, ZHU H, ZHOU M, et al. Phase shiftingtransformer-based mitigation strategy for load redistribution attacks in power system optimal power flow[J]. IEEE Transactions on Smart Grid, 2024, 15(5): 5127-5138.

[17] CHANG Z, WU J, LIANG H, et al. A review of power system false data attack detection technology based on bigdata[J]. Information, 2024, 15(8): 439.

[18] ABDELKADER S, AMISSAH J, KINGA S, et al. Securing modern power systems: implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks[J]. Results in Engineering, 2024: 102647.

[19] ZHANG S, YANG Y, ZHOU Z, et al. DIBAD: A disentangled information bottleneck adversarial defense method using Hilbert-Schmidt independence criterion for spectrum security[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 3879-3891.

LI Xiaogeng, born in 1986, master of engineering. His main research interests include network security and power communication.