基于模糊证据推理的智能变电站多源告警数据的攻击取证方法

王继业[1] 杨 军[2] 韩丽芳[1] 周 亮[1] 周纯杰[2]

[1](中国电力科学研究院有限公司 北京 100192)

[2](华中科技大学人工智能与自动化学院 湖北 武汉 430072)

摘 要 针对智能变电站的多源异构告警数据,提出一种基于模糊证据推理的多源告警数据攻击取证方法。根据设备告警信息分析其对不同类型攻击的支持度,利用模糊理论将告警信息模糊化;计算各设备告警信息模糊隶属度,并结合余弦相似度算法计算各告警设备之间的告警证据相似度,剔除无关、错误等告警证据;以不同类型的攻击场景为例,验证所提方法的有效性。实验结果表明,该方法能够在减少告警信息数量的基础上,解决单个设备的误报问题,提高电力工控系统设备告警信息的可信度。

关键词 智能变电站 攻击取证 模糊推理 相似度分析

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.12.045

ATTACK FORENSIC METHOD OF MULTI-SOURCE ALARM DATA IN SMART SUBSTATION BASED ON FUZZY EVIDENCE REASONING

Wang Jiye[1] Yang Jun[2] Han Lifang[1] Zhou Liang[1] Zhou Chunjie[2]

[1](*China Electric Power Research Institute*, *Beijing 100192*, *China*)

[2](*School of Artificial Intelligence and Automation*, *Huazhong University of Science and Technology*, *Wuhan 430072*, *Hubei*, *China*)

Abstract This paper proposes a method of attack forensics based on fuzzy evidence reasoning for multi-source heterogeneous alarm data of smart substations. According to the alarm information of the device, its support degree to different types of attacks was analyzed, and the alarm information was blurred by fuzzy theory; the fuzzy membership degree of alarm information of each device was calculated, and the similarity degree of alarm evidence among each device was calculated with cosine similarity algorithm, irrelevant, erroneous and other alarm evidences was eliminated; the effectiveness of the proposed method was verified by taking different types of attack scenarios as examples. Experimental results show that the proposed method can effectively solve the problem of false alarm of single equipment and improve the reliability of alarm information of power industry control system equipment on the basis of significantly reducing the number of alarm information.

Keywords Smart substation Attack forensics Fuzzy reasoning Similarity analysis

0 引 言

随着智能电网建设的全面展开,我国电力系统飞速发展,自动化水平不断提高,人们对电力的需求和依赖日渐增加。近些年,一些黑客或不法分子通过网络攻击手段侵入电力系统内部实施破坏的事件频频发生,给电力系统的稳定运行敲响了警钟。智能变电站作为智能电网的重要组成部分,承载了变电设备状态监测、电网运行数据、相关信息实时采集和发布等任

收稿日期:2019-03-09。国家自然科学基金重点项目(61433006);国家电网公司科技项目"面向电力工控的攻击仿真验证技术研究"(52110417001B);中国电力科学研究院有限公司创新基金项目"电力工控网络安全靶场技术研究"(XX83-19-003)。

王继业,教授级高工,主研领域:电力系统信息安全,大数据。**杨军**,博士生。**韩丽芳**,高工。**周亮**,高工。**周纯杰**,教授。

务。智能变电站的运行状态影响着电力系统的稳定运行,而智能变电站系统的通信协议标准化、数字化模式使其极易遭到攻击,变电站系统稳定性面临严峻的挑战[1]。

随着大量电网安全事件的发生,在对安全事件还原的过程中暴露出了告警数据量庞大、误报现象严重等问题。茹蓓等[2]提出一种海量数据干扰下冗余数据高性能消除方法,引入均值漂移传递函数对冗余数据进行分类,并通过获取其活跃程度实现高性能消除。刘自力等[3]提出了一种能够处理大数据的频繁项集挖掘算法,将海量复杂度高的多源异构数据转化为知识。文献[4]利用基于特征重叠的告警去冗模块,有效地去掉了海量告警日志中重复以及冗余的告警信息。

目前告警信息冗余处理大多是针对通信网络的,而面向电力工控系统的告警信息处理的研究较少。针对智能变电站,本文提出基于模糊证据推理的智能变电站多源告警数据的攻击取证方法。首先对数据进行预处理达到统一数据类型减少数据量的目的,再通过特征匹配、模糊化、归一化、相似度匹配等方法去掉智能变电站告警证据中的误报。这样,能够在显著减少告警信息数量的基础上,有效解决单个设备的误报问题,在提高智能变电站数据可靠性、还原攻击场景等方面具有积极意义。

1 智能变电站网络架构

基于 IEC61850 标准的智能变电站从逻辑结构上分为站控层、间隔层和过程层[2-3]。其中过程层设备包括变压器、断路器、隔离开关、电流电压互感器、合并单元、智能终端、独立的智能电子装置等,主要完成开关量、模拟量采样和控制命令的执行等与一次设备相关的功能;间隔层设备包括继电保护装置、系统测控装置、在线监测装置等二次设备,主要完成对一次设备进行测量、控制、保护的功能;站控层通信设备包括监控主机、数据通信网关机、数据服务器、PMU 数据集中器、综合应用服务器、对时系统等,实现面向全站设备的监视、控制、告警和信息交互功能[5]。

智能变电站网络化的成功应用使其以功能、信息的冗余代替了常规变电站装置的冗余。智能变电站网络架构[6]如图 1 所示,其采用“三层两网”分层分布的结构,这使其站内数据流传递方向具有“纵横交错”的特点,即不仅保持了同一层次内的横向传送,还具有不同层次间的纵向交换。

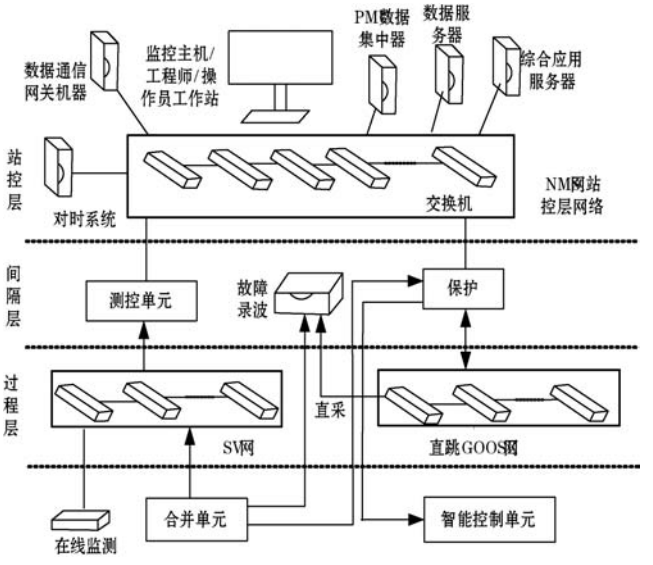

图 1 智能变电站网络架构

2 典型攻击与告警证据

2.1 网络攻击特征描述

智能变电站的典型安全攻击包括远程攻击、本地提权(获取超级权限)、系统数据窃取、伪造控制指令、篡改数据(包括篡改网络数据和本地系统数据等)等。典型攻击过程常常是这些安全攻击的组合,例如首先通过远程攻击获取本地访问权限,然后采用数据窃取获得关键用户的口令、关键系统配置、关键控制组件的控制逻辑。获得并分析电力控制系统的运行逻辑后,通过发送伪造的控制指令,破坏电力控制系统的正常运行。同时,攻击者可以利用篡改数据攻击,替换监控数据,使之符合控制逻辑,并达到隐蔽攻击行为的效果。

因此在攻击取证时要考虑攻击的多种攻击特征。攻击特征主要从攻击目的、攻击机理、攻击后果三个方面进行考虑。针对收集到的攻击种类,首先将攻击进行分类,然后针对每一种攻击类型,从上述三个方面选取相应的特征,以此构建攻击特征库。智能变电站常见网络攻击[7-8]如表 1 所示。

表 1 常见网络攻击

攻击分类	典型攻击
攻击目的	拒绝服务攻击(DoS)、获取系统权限的攻击、获取敏感信息的攻击
攻击切入点	缓冲区溢出攻击、系统设置漏洞的攻击等
攻击的纵向实施过程	获取初级权限攻击、提升最高权限的攻击、后门攻击、跳板攻击等
攻击对象	对操作系统的攻击、对网络设备的攻击、对特定应用系统的攻击等

2.2　多源异构告警证据

现今,通信网络报文已成为智能变电站设备间信息交互和共享的主要方式,可将智能变电站系统的信息流主要分为 GOOSE 报文信息流、MMS 报文信息流、SV 报文信息流[9]。为了记录报文事件,智能变电站新配置了网络报文记录分析装置,除此之外,智能变电站还配置了记录电压电流发生突变、开关量变化引起的保护动作波形的故障录波装置,在智能变电站遭到攻击时,服务器中的系统日志及登录日志文件可以提供大量有用的告警信息。不同层次的不同设备都会产生告警数据,它们的来源不同,而且格式多样,如报文数据、日志文件等,由此可见告警数据具有多源异构的特性。正是由于告警数据数量庞大且多源异构,无法将告警数据直接进行告警关联以还原攻击场景。因此,本文先对多源异构的告警数据进行预处理,再将智能变电站的多源告警数据与攻击特征库进行特征匹配,并通过模糊隶属度以及归一化处理得到相同数据格式的告警证据,最终利用余弦相似度算法分析设备之间的证据相似度,得到有效的证据集,解决告警数据量庞大且格式不统一的问题。

3　基于模糊证据推理的攻击取证方法

面对形式各异和不断发展的网络攻击手段,传统的安全事件检测手段日益不能满足变电站安全管理的需求。入侵攻击场景还原可以从整体上反映攻击者攻击意图,为增强网络安全管理效率、制定有效的安全规划和监管策略提供科学依据。然而由于变电站通信链路、设备状态等问题,各设备产生的告警不能保证其正确性,难免会发生误报、漏报等现象。

为了避免过多的错误信息影响攻击场景的还原效率[10],本文提出基于模糊证据推理的智能变电站多源告警数据的攻击取证方法,从实现规则上讲,用模糊证据推理确定目标所属类型的过程共分三步:(1)确定目标信息的模糊隶属函数。(2)用证据理论对目标信息隶属函数进行合成。(3)判决准则选取。此方法在减少误报的同时降低了告警数据的数量,考虑到变电站各设备之间的关联性,应用于变电站的攻击取证方法总体实现思路为:采集智能变电站各个设备的告警证据,经过数据预处理后将其与攻击特征库进行攻击特征匹配,然后通过隶属度函数对告警证据进行模糊隶属度计算,再对每个设备的模糊隶属度进行归一化处理,此时对于各个设备的告警证据具有相同的数据格式。格式统一后,还需利用余弦相似度算法分析设备之间的证据相似度,得到符合要求的攻击证据集,最后通过分析证据集判断其属于哪种类型的攻击。基于模糊证据推理的攻击取证过程示意图如图 2 所示。

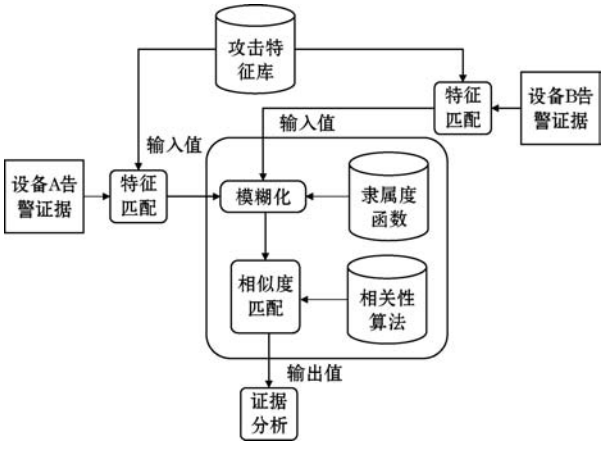

图 2　基于模糊证据推理的攻击取证过程示意图

3.1　告警信息预处理

在对智能变电站多源告警数据的攻击取证过程中,一般要保存所有相关信息。由于告警信息数目庞大,因此在取证前需要对数据进行预处理,这样可以节约时间和空间,降低后续成本。预处理分为两个方面,一是减小数据量,二是统一数据类型。由于在数据采集过程中存在数据采集的非同步性、数据来源的不一致性、数据采集的时效性等问题,不可避免会出现数据缺失、冗余、格式不符、含义不明等多种情况,这些不符合分类模型处理规范的数据在攻击取证过程中十分棘手。因此,需要对变电站各类信息(量测信息、状态信息、通信信息、事务日志等)进行预处理,形成可以方便分析处理的数据集。

针对变电站数据本身不符合分析规范的情况进行处理,主要包括数据清洗、数据集成、数值化处理几个方面。

数据清洗主要负责处理数据缺失及噪声问题。对于数据缺失可以采用剔除法或替代法,剔除法虽实现容易但可能造成其他关键数据的缺失,而替代法可以采用均值填补,或用回归、贝叶斯等算法结合一些固定约束估计缺失值。噪声数据则可以采用分箱、聚类、回归、计算机与人工相结合的方法剔除。

数据集成主要负责将要进行综合分析计算的不同格式的数据合并成可用的数据集。

数值化处理将变电站数据中非数值型转化为数值型,例如通信报文所用的协议类型 MMS 和 SV 分别用标号“0”和“1”代替。

为了提高告警信息的通用性和扩展性,选取入侵检测信息交换格式(IDMEF)中权重比较大的属性将告警信息格式标准化,即可以将告警信息的格式表示

为 Alarm(Alarm_ID,Alarm_Type,Alarm_Source,Alarm_Dest,Alarm_Time,Alarm_Port)。

获取的告警信息中可能包含大量无关告警,通过各类安全设备从网络中采集主机、服务、漏洞等告警校验所需信息判断目标系统与告警信息的相关性,以此去掉无关的告警信息。在告警校验中,需要根据攻击行为的类型,相应地调整元素内容。以拒绝服务攻击为例,给出告警校验函数:

```
Function DoS-Verification{
alarm:{
  Dest : DestIP                    /* 告警的目的 IP 集合 */
  Port: DestPort                   /* 目的端口号集合 */
  Vulnerability: CVEID             /* 告警的漏洞信息 */
  Source: SrcIP                    /* 告警的源 IP 地址 */
  }
Target:{
  Active: Hosts                    /* 活跃主机地址集 */
  Ports: ports                     /* 主机开放端口 */
  Vul: CVEID                       /* 漏洞信息集合 */
  RA: RAccessed /* 主机访问控制策略中被访问关系 */
}
Verification:{
If (alarm.Dest ∈ Target.Active & alarm.Port ∈ Target.Ports
& alarm.Vulnerability ∈ Target.Vul & alarm.Source ∈ Target.
RA)
  Result = 1;
Else
  Resut = 0;          /* 校验未通过,将告警信息滤除 */
}
}
```

虽然去除掉了告警中的无关告警信息,但是同一攻击在某一瞬时可能在某一设备产生重复的原始告警,因此,在分析告警数据之前还要去除这些冗余的告警。本文采用滑动窗口来消除重复告警,实现如下:

(1) 产生新的告警 NewAlarm 时,从时间窗口中移除开始时间差值大于窗口值的告警,即若存在(NewAlarm.starttime—DeAlarm.starttime) > WindowSize,则将 DeAlarm 从时间窗口中移除;

(2) 按时间顺序匹配新告警 NewAlarm 与时间窗口中的告警 $Alarm_i$;

(3) 若两个告警的类型、源 IP 地址和目的 IP 地址均相同则将两个告警合并,即若存在(NewAlarm.Alarm_type == $Alarm_i$.Alarm_type) && (NewAlarm.source == $Alarm_i$.source) && (NewAlarm.dest == $Alarm_i$.dest),则合并两个告警。

3.2 单一告警证据的模糊化处理

模糊理论是指用到了模糊集合的基本概念或隶属度函数的理论,其应用范围广泛,从工程科技到人文科学都可以发现它的研究踪迹与成果。针对电力系统,在模拟人脑对电力系统进行运行控制时,由于人脑存在识别、推理等模糊性的特点,在采用专家系统、模式识别等技术时均用到了模糊集方法。

当智能变电站某部分运行异常时,可能引发与其相关联的部分发生运行错误,产生大量告警信息。通常情况下,依据 0 和 1 来判断某件事情是否发生。然而,针对本文这种情况即告警信息与其产生的根源是一种模糊的、一对多的关系,采用 1 或者 0 来判断比较片面和绝对,由此用 0 到 1 之间的任意数来表示[11]。本文结合最大隶属法,对告警进行模糊相关性分析,实现告警的精确描述与定位,以解决单个设备误报问题。

定义 1 设 U 为论域,一个模糊集合 A 在 U 上的一个映射 u_A 表示为:

$$u_A: U \rightarrow [0,1]$$
$$u \rightarrow u_A(u) \tag{1}$$

对于 $u \in U$,函数 $u_A(u)$ 称为模糊集合 A 的隶属度函数即表示 u 对 A 的隶属度。通常结合实际选取隶属度函数 u_A。

将理论应用于智能变电站,告警信息经过预处理后,要确定目标信息的模糊隶属度函数。隶属度函数的确定有多种方法,例如:模糊统计法、例证法、专家经验法、指派方法等。本文采用指派方法,根据问题的性质主观地选用某些形式的模糊分布。

针对不同的变电站设备有不同的模糊集合,隶属度函数有不同的选择,比较典型的隶属度函数包括三角形、梯形、S 型等。可以将三角形、梯形的隶属度函数表示为:

$$u_A(x) = triangular(x,a,b,c) = \begin{cases} 0 & x \leqslant a \\ \dfrac{(x-a)}{(b-a)} & a \leqslant x \leqslant b \\ \dfrac{(c-x)}{(c-b)} & b \leqslant x \leqslant c \\ 0 & \text{其他} \end{cases} \tag{2}$$

式中:a 和 c 为确定三角形“脚”的参数; b 为确定三角形“峰”的参数。

$$u_A(x) = trapezoid(x,a,b,c,d) = \begin{cases} 0 & x \leqslant a \\ \dfrac{(x-a)}{(b-a)} & a \leqslant x \leqslant b \\ 1 & b \leqslant x \leqslant c \\ \dfrac{(d-x)}{(d-c)} & c \leqslant x \leqslant d \\ 0 & \text{其他} \end{cases} \tag{3}$$

式中:a 和 d 为确定梯形“脚”的参数;b 和 c 为确定梯

形“肩膀”的参数。

将攻击特征库中的攻击类型集合假设为 $\Theta=\{\theta_1,\theta_2,\cdots,\theta_n\}$,并将某一节点设备 A 的告警证据集表示为 $e^A=\{e_1,e_2,\cdots,e_{N_A}\}$,则设备告警对攻击 θ_i 的支持度表示为:

$$u_A(\theta_i)=\frac{N_{A,\theta_i}}{N_A} \tag{4}$$

式中:N_{A,θ_i} 代表符合攻击特征的异常告警数量;N_A 代表该设备异常告警的总数量。则该设备对攻击的支持度为:$u_A=\{u_A(\theta_1),u_A(\theta_2),\cdots,u_A(\theta_n)\}$。

本文采用偏大型上升函数 S 型隶属函数[12],即将攻击 θ_i 的告警证据的隶属度函数表示为:

$$f_A(\theta_i)=\begin{cases}0 & 0\leqslant u_A(\theta_i)\leqslant a\\ 2\left(\dfrac{u_A(\theta_i)-a}{b-a}\right)^2 & a<u_A(\theta_i)\leqslant\dfrac{a+b}{2}\\ 1-2\left(\dfrac{u_A(\theta_i)-b}{b-a}\right)^2 & \dfrac{a+b}{2}<u_A(\theta_i)\leqslant b\\ 1 & b<u_A(\theta_i)\leqslant 1\end{cases} \tag{5}$$

式中:a、b 的值需要自定义。通过隶属度函数计算设备对各不同攻击支持度的模糊隶属度,得到的结果为 $f_A=\{f_A(\theta_1),f_A(\theta_2),\cdots,f_A(\theta_n)\}$。

为了让数据尺度统一将上述结果作归一化处理,即将有量纲的表达式经过变换化为无量纲的表达式,其目的是可以用数值来直接进行比较。归一化后的形式如下:

$$m(f_A(\theta_i))=\frac{f_A(\theta_i)}{\sum f_A} \tag{6}$$

3.3　多源告警证据相似度分析

通过对单一告警证据的模糊化处理,得到某个设备可能遭受的攻击情况,由于智能变电站各设备模块间有信息传递,若仅凭某一个设备遭到攻击的情况就下定论可能不符合实际。由此,可以通过判断智能变电站各设备间告警信息的相似程度以得到有效的告警证据集。

相似度度量即计算个体间的相似程度,相似度度量的值越小则说明个体间相似度越小,反之说明个体相似度越大。典型的相似度算法包括欧几里得距离、Jaccard 相似系数、余弦相似度等。欧几里得距离的计算是基于各维度特征的绝对数值,指的是在 m 维空间中两个点之间的真实距离。Jaccard 相似系数主要用于计算符号度量或布尔值度量的个体间的相似度,其无法衡量差异具体值的大小,只关心个体间共同具有的特征是否一致。余弦相似度算法则用向量空间中两个向量夹角的余弦值作为衡量两个个体间差异的大小的度量,其更加注重两个向量在方向上的不同,相比于其他算法更适合应用在智能变电站的各设备间多源告警证据的相似度的衡量上。因而,本文用余弦相似度算法[13]衡量智能变电站任意两个节点设备间的相似度:

$$d_{AB}=\frac{\sum m(f_A(\theta_i))\cdot m(f_B(\theta_j))}{\sqrt{\sum m^2(f_A(\theta_i))}\cdot\sqrt{\sum m^2(f_B(\theta_j))}} \tag{7}$$

d_{AB} 越高则智能变电站中设备 A、B 发生相同攻击的概率越大。计算完成后,将所有符合要求的告警证据集表示为:

$$E=\{(e^i,e^j)\mid d_{ij}\geqslant\delta,\forall i,j,i\neq j\} \tag{8}$$

式中:δ 表示证据相似度阈值。进一步,假设智能变电站中有 k 个设备符合要求,通过分析证据集 $E=\{e^1,e^2,\cdots,e^k\}$ 中的证据,可以得到证据集隶属于某种攻击 θ_i 的概率:

$$p(\theta_i)=\frac{\sum u(\theta_i)}{\sum u} \tag{9}$$

通过将单一告警证据模糊化处理,分析不同设备告警证据的相似度,得到有效的攻击证据集,避免因错误告警过多而影响攻击取证的有效性,最后通过分析有效证据集判断其属于不同类型攻击的概率。

4　案例分析

4.1　智能变电站多源告警数据

以图 1 所示智能变电站网络架构来说明本文所提方法的可行性和有效性。实验以 UDP Flood 攻击[14-15]为例。当间隔层设备收到 UDP 数据包时,检测目的端口是否有正在等待的应用程序,若不存在,其会给该伪造的源地址发送 ICMP 数据包。随着不断向间隔层设备的开放端口发送 UDP 数据包,导致整个系统负担过重,通信缓慢甚至崩溃,不能处理合法的传输任务。具体流程如下:

(1) 构造 UDP 数据包。构建与间隔层各类 UDP 数据包具体内容相似的 UDP 数据包,以确保实验的有效性;

(2) 检测间隔层设备端口的开放性,为 UDP 攻击作准备;

(3) 向间隔层设备的开放端口发送大量 UDP 报文,占用网络资源,导致无法正常通信;

(4) 监控主机抓取数据包。

当实际系统遭到攻击时,首先从智能变电站的各层设备中得到多源异构的告警数据,对智能变电站而

言,同一设备产生的告警类型可能不同,通过分析智能变电站不同设备的告警信息,我们将告警类型分为事故告警、异常告警、变位告警、越限告警、告知告警,某一时间段内,变电站的部分告警信息如表 2 所示。

表 2 变电站的部分告警信息

告警来源	告警时间	告警信息	告警类型
断路器保护	2018 - 03 - 22 15:23:19	第一套开关保护出口	事故告警
测控装置	2018 - 03 - 22 15:23:20	测控 GOOSE 总告警	异常告警
	2018 - 03 - 22 15:23:22	测控 SV 总告警	异常告警
	2018 - 03 - 22 15:23:23	测控检修状态投入	告知告警
主变保护装置	2018 - 03 - 22 15:23:41	主变温度高跳闸	变位告警
	2018 - 03 - 22 15:24:03	主变本体油温过高告警	越限告警
⋮	⋮	⋮	⋮

攻击实施后,先对多源异构的告警数据进行预处理,再截取某段时间内智能变电站各设备的告警信息如表 3 所示。

表 3 某段时间内智能变电站各设备告警信息统计表

设备名称	总数	事故告警数	变位告警数	越限告警数	异常告警数	告知告警数
监控主机	217	70	41	22	61	23
在线监测装置	191	66	32	15	57	21
报文记录分析装置	226	73	43	26	62	22
电流电压互感器	223	32	28	63	51	49
合并单元	198	11	24	98	29	36
⋮	⋮	⋮	⋮	⋮	⋮	⋮

然后进行攻击类型匹配。具体流程如下:先逐条分析设备告警信息判断是否属于某种攻击特征,如果属于,则将对应的 $N_{A,\theta}$ 数量增加 1。以典型的两种攻击为例,其在攻击特征库中的表现形式如表 4 所示,如果告警信息中出现表 4 所示情况,则可以判断其隶属的攻击类型。另外,由于不同攻击类型的攻击特征可能具有相似性,例如“安全日志异常”均符合两种示例攻击的特征,因此某一设备攻击支持度之和可能不为 1,即 $\sum \mu_A(\theta) \neq 1$。

表 4 变电站的部分告警信息

攻击类型	告警设备	告警信息
UDP Flood	监控主机	安全日志异常,如:529、532 等
	网络报文记录分析装置	SV 采样数据异常,GOOSE 数据异常
	在线监测装置	断路器动作、变压器过热等
重放攻击	监控主机	安全日志异常
	网络报文记录分析装置	SV 采样数据异常,GOOSE 数据异常

4.2 取证分析

攻击特征库中包含 UDP Flood 和重放攻击两种攻击类型,即表示为 $\Theta = \{\theta_1, \theta_2\}$。统计表中的五个节点设备用 A、B、C、D、E 来表示,并将设备 A 的告警证据集表示为 $e^A = \{e_1, e_2, \cdots, e_{N_A}\}$,以此类推。将节点设备的告警证据集与攻击特征库相匹配,得到的统计结果如表 5 所示。

表 5 攻击特征匹配结果

设备名称	计算结果			
	θ_1	θ_2	$u(\theta_1)$	$u(\theta_2)$
A	172	83	0.79	0.38
B	155	72	0.81	0.38
C	178	88	0.79	0.39
D	111	114	0.50	0.51
E	64	127	0.32	0.64

表 5 中,$u(\theta_1)$、$u(\theta_2)$ 代表各设备对攻击 θ_1、θ_2 的支持度。将隶属度函数 a、b 的值设为 0.3 和 0.7。即可以将攻击 θ_i 的告警证据的隶属度函数表示为:

$$f_A(\theta_i) = \begin{cases} 0 & 0.0 \leqslant u_A(\theta_i) \leqslant 0.3 \\ 2\left(\dfrac{u_A(\theta_i) - 0.3}{0.4}\right)^2 & 0.3 < u_A(\theta_i) \leqslant 0.5 \\ 1 - 2\left(\dfrac{u_A(\theta_i) - 0.7}{0.4}\right)^2 & 0.5 < u_A(\theta_i) \leqslant 0.7 \\ 1 & 0.7 < u_A(\theta_i) \leqslant 1 \end{cases} \tag{10}$$

通过隶属度函数分别计算各设备对不同攻击类型支持度的模糊隶属度并进行归一化处理,得到的结果如表 6 所示。

表 6 支持度的模糊隶属度以及归一化结果

设备名称	计算结果		
	f	$m(f(\theta_1))$	$m(f(\theta_2))$
A	{1,0.08}	0.930	0.070
B	{1,0.08}	0.930	0.070
C	{1,0.10}	0.910	0.090
D	{0.5,0.56}	0.470	0.530
E	{0,0.96}	0.006	0.994

采用余弦相似度算法计算任意两节点设备间的相似度即[AB,AC,AD,AE,BC,BD,BE,CD,CE,DE],其结果为[1,1,0.72,0.09,1,0.72,0.08,0.73,0.11,0.71]。

将相似度阈值 δ 置为 0.8,由此可见,设备 A、B、C 相似度比较高,即智能变电站的这三个设备发生相同攻击的概率比较大。现智能变电站中有三个设备符合 $E=\{(e^i,e^j)\mid d_{ij}>\delta,\forall i,j,i\neq j\}$,通过分析告警证据集 $E=\{e^A,e^B,e^C\}$ 中的证据,计算出证据集隶属于攻击 θ_1、θ_2 的概率,即 $p(\theta_1)=0.68$、$p(\theta_2)=0.32$。

若考虑到设备 D、E,则可以将告警证据集表示为 $E=\{e^A,e^B,e^C,e^D,e^E\}$。分别计算出证据集隶属于攻击 θ_1、θ_2 的概率:$p'(\theta_1)=0.58$、$p'(\theta_2)=0.42$。本次实验采用的 UDP Flood 攻击,依据本文方法将攻击隶属于 UDP Flood 攻击的概率由 0.58 提升至 0.68,可见通过将证据模糊化的取证方法可以有效去掉误报。为了验证此方法对不同攻击的有效性,分别采用 UDP Flood、SYN Flood、重放攻击、中间人攻击、错误数据注入攻击[8-9,14]进行测试,实验结果如图 3 所示。

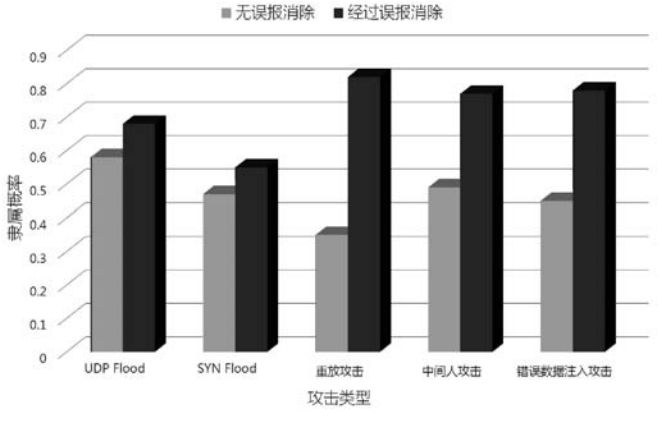

图 3　误报消除效果对比实验

由此可见,本文提出的基于模糊证据推理的智能变电站多源告警数据的攻击取证方法可有效减少不同攻击对智能变电站产生的误报。

5　结　语

本文提出基于模糊证据推理的智能变电站多源告警数据的攻击取证方法。首先介绍智能变电站的网络架构、告警数据的多源异构特性,以及常见的攻击。通过对智能变电站各个设备的告警证据进行预处理和模糊化处理,将多源异构的告警证据统一化,再利用余弦相似度算法分析设备之间的证据相似度,得到符合要求的攻击证据集以减少误报。最后以 UDP Flood 攻击为例,对方法的有效性进行验证。

本文方法能够有效解决单个设备无法解决的误报问题,对提高工控系统的数据可靠性、还原攻击场景等方面具有积极意义。

参　考　文　献

[1] 翟峰,岑伟,赵兵,等. 智能变电站系统安全防护技术研究[J]. 自动化与仪表,2015,30(3):6-9.

[2] 茹蓓,李虹. 海量数据干扰下冗余数据高性能消除方法[J]. 沈阳工业大学学报,2017,39(6):686-690.

[3] 刘自力,范军丽,陈文伟,等. 面向多源异构信息的频繁项集挖掘算法[J]. 计算机技术与发展,2017,27(6):76-80.

[4] Hong J, Liu C C. Intelligent electronic devices with collaborative intrusion detection systems[J]. IEEE Transactions on Smart Grid,2019,10(1):271-281.

[5] Hong J, Liu C C, Govindarasu M. Detection of cyber intrusions using network-based multicast messages for substation automation[C]//Innovative Smart Grid Technologies Conference, 2014.

[6] 李圆智. 智能变电站网络系统性能测试技术研究[D]. 北京:华北电力大学,2016.

[7] 张道银. 智能变电站信息安全技术研究[J]. 电力信息与通信技术,2015,13(1):108-111.

[8] 汤奕,陈倩,李梦雅,等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化,2016,40(17):59-69.

[9] 黄新庭. 智能变电站数据流分析及其网络通信性能研究[D]. 广州:广东工业大学,2016.

[10] Elshoush H T, Osman I M. Intrusion alert correlation framework: an innovative approach[J]. Lecture Notes in Electrical Engineering,2013, 229:405-420.

[11] 段锁林,杨可,毛丹,等. 基于模糊证据理论算法在火灾检测中的应用[J]. 计算机工程与应用,2017,53(5):231-235.

[12] 黄洋,鲁海燕,许凯波,等. 基于 S 型函数的自适应粒子群优化算法[J]. 计算机科学,2019,46(1):245-250.

[13] 陈大力,沈岩涛,谢槟竹,等. 基于余弦相似度模型的最佳教练遴选算法[J]. 东北大学学报(自然科学版),2014,35(12):1697-1700.

[14] 朱玛,李勇,章坚民,等. 基于 OPNET 的数字化变电站 DoS 攻击建模与仿真研究[J]. 机电工程,2017,34(3):304-309.

[15] 凌光,王志亮,吕建龙,等. 基于 OPNET 的智能变电站过程层网络建模方法[J]. 中国电力,2017,50(1):79-84.