doi:10.11835/j.issn.1000-582X.2021.07.007

# 面向智能变电站的威胁与风险评价模型研究与实现

刘元生[1],王 胜[2],白云鹏[3],夏晓峰[3]

(1. 国网甘孜供电公司,四川 甘孜 626700;2.国网四川省电力科学研究院,成都 610072;
3. 重庆大学 大数据与软件学院,重庆 400044)

**摘要**:针对传统入侵检测系统在资源受限的工业网络中部署时效率和稳定性表现不足的问题,首先提出了面向智能变电站的入侵检测系统,以及工业设备安全风险评估方法,建立了针对智能变电站结构的威胁风险评价模型,引入基于灰色模型的网络脆弱性节点主动预测方法用以平衡威胁来源的权重;其次提出基于信息安全三维度风险值计算算法,引入模糊一致判断矩阵进行风险值参数计算,最终实现可以直观判断攻击对系统的影响范围和程度的风险评价。通过相关实验,系统在部署环境中满足被动性、低负荷、实时性以及可靠性要求的同时,能够有效地检测工业网络面临的入侵威胁。

**关键词**:智能变电站;入侵攻击;网络检测

**中图分类号**:TN914 **文献标志码**:A **文章编号**:1000-582X(2021)07-064-11

# Research and development of threat and risk evaluation model for smart substation

*LIU Yuansheng*[1], *WANG Sheng*[2], *BAI Yunpeng*[3], *XIA Xiaofeng*[3]

(1. State Grid Ganzi Power Supply Company, Ganzi, Sichuan 626700, P. R. China;2. Sichuan Electric Power Research Institute, Chengdu 610072, P. R. China;3. School of Bigdata and Software Engineering, Chongqing University, Chongqing 400044, P. R. China)

**Abstract**: Due to the lack of efficiency and stability in the deployment of traditional intrusion detection systems in resource-limited industrial equipment, an intrusion detection system for intelligent substations was proposed to supplement the evaluation model of industrial equipment security risks. The system used a gray model-based network vulnerability node active prediction method to balance the weight of threat sources in the established threats and risk assessment model. A risk value calculation algorithm based on the three-dimensionality of information security is proposed. The algorithm used a fuzzy consistent judgment matrix to calculate the risk value parameters. Therefore, a risk evaluation that can intuitively determine the scope and extent of the attack on the system was completed. Through relevant experiments, the system can effectively detect intrusion attacks and have good performance while satisfying the passive,

**收稿日期**:2021-02-12

**基金项目**:国网四川省电力公司科技资助项目(52199717001P);国网四川省电力公司电力科学研究院项目(SGSCDK00XTJS1800093)。

Supported by Research program of State Grid Corporation of Sichuan(52199717001P) and Research program of Sichuan Electric Power Research Institute (SGSCDK00XTJS1800093).

**作者简介**:刘元生(1977—),男,硕士,高级工程师,主要从事电力信息安全研究。

**通讯作者**:夏晓峰(1980—),男,副教授,(E-mail)xiaxiaofeng@cqu.edu.cn。

low load, real-time and reliability in the deployment environment.

**Keywords**: Intelligent substation; intrusion attack; network detection

## 1　智能变电站网络中的入侵检测

随着网络技术的发展，未来的网络通信将为自动化技术提供坚实的互联基础。智能变电站是典型的电力自动化控制系统，在中国电力网络发展中占据重要地位，其产生的数据具有规模大、复杂性高特点，对数据处理过程和方法有较高要求，同时，对系统的安全防护也提升到更复杂维度上。入侵检测系统作为安全防护的重要组成部分，也是智能变电站安全防护的关键环节。

目前的入侵检测系统是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。近年来国内外对入侵检测的研究集中在精确性中，在机器学习分类算法的提升上有很多应用[1-10]，这种方法要求首先对捕获的数据进行预处理并且引入参数[11-17]，在牺牲计算资源的同时可以在一定程度上提高检测系统的精度。另外在建立威胁模型方面，各类相关研究都专注于对特定的网络结构有效获取威胁来源[18-21]，并且平衡各威胁源对安全的权重也是研究的方向之一。在威胁分析后建立风险模型时，如何使得风险模型有效的反映出系统的安全状态[22-25]，近年来相关研究以引入机器学习与神经网络方法为主，在消耗运算资源的同时可以得出具有代表性的数值。

将入侵检测系统应用于智能变电站，需要结合智能变电站的运行特征[26-29]，例如变电站的报文捕获必须采用被动获取的方式，并且不能给变电站施加过多的系统负荷以至影响变电站的运行状态。另外智能变电站需要实时处理大量信息，并且对系统的可靠性要求极高，在任何数据量和运行状态下必须首先满足系统的平稳性要求。所以基于智能变电站的入侵检测系统需考虑系统在被动性、低负荷、实时性以及可靠性方面的影响。基于以上特点，面向智能变电站的入侵检测采用网络式结构设计，以被动式监听工具为载体并优化数据存储结构，使得系统在实际环境中的负载更小。

### 1.1　入侵检测系统结构

入侵检测系统在工业领域主要检测的威胁包括：利用系统权限进行非法操控，对设备参数的恶意篡改，通信协议的异常和攻击等。检测系统通过收集系统日志，网络报文，用户行为来判断是否产生告警信息，它有 3 种体系结构：主机入侵检测、网络入侵检测和分布式入侵检测。其中主机入侵检测是检测对主机或服务器的入侵与攻击，具有部署成本低，准确度高，可以应用在加密场景中并且检测出攻击造成的影响，但是主机入侵检测对系统资源占用较多，并且检测方法依赖系统记录文件，对入侵攻击存在一定的时差并且可能出现漏判的情况。

分布式入侵检测是由多个组成部分构成，并部署在网络中的各个设备中，每个设备将各自监听采集到的信息汇总到系统控制中心进行处理，但是这种方式对大型网络部署与维护代价高，并且同样会对系统资源大量占用。网络入侵检测是将系统的监听模块部署在设备的网卡中从而监听整个网络中的报文，从而使得系统的实时性响应度高，能够在收到威胁报文时迅速做出告警动作，并且系统在部署中对资源的需求低，对系统的正常功能影响低，这对设备运行稳定性要求高的设备十分重要；虽然这种模式只能检测到单独网卡中的报文信息，但是由于智能变电站的站控层中，监控主机具有集中收发报文的功能，所以在智能变电站中部署不受影响，适合在智能变电站中使用。

基于以上分析，在资源受限并且对运行稳定性要求高的环境中，使用网络入侵检测是可行且必要的选择。

### 1.2　智能变电站网络与部署

根据 IEC-61850 智能变电站通信结构被分为“三层两网”，如图 1 所示。

以上结构组成了智能变电站二次通信网络。其中站控层与间隔层的网络为站控层网络，间隔层与过程层中的网络为过程层网络。在站控层网络中，间隔层向上发送 MMS(manufacturing message specification)，

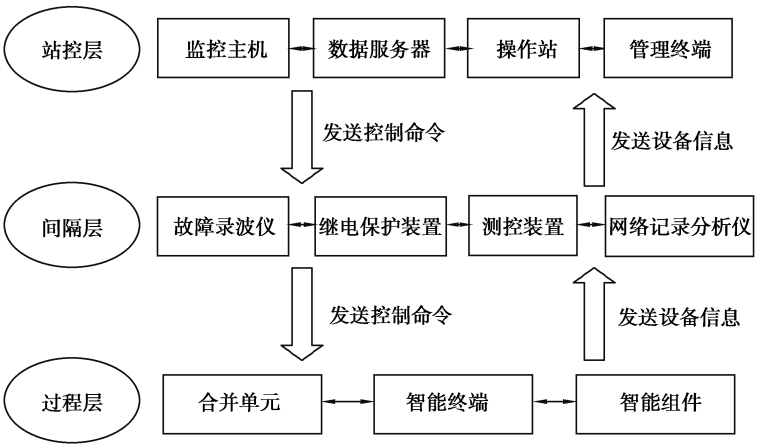


**图1 智能变电站网络**

**Fig. 1 The substation network**

GOOSE(generic object oriented substation event)和SNTP(simple network time protocol)报文格式的设备信息,站控层向下发送一样格式的控制命令;在过程层网络中过程层向上发送SV(Sampled Value)报文传输设备状态信息,间隔层向过程层发送GOOSE报文。

根据智能变电站中网络结构,入侵检测系统部署在站控层时可以更有效的检测报文,并且将系统界面实时更新在监控主机中;另一方面,来自外部的攻击是以与站控层设备通信为主,通过攻击操作平台来向网络中的设备发送恶意指令,因此系统部署在站控层主机可以更有效及时地应对威胁。

## 2 面向智能变电站的威胁与风险评价模型

### 2.1 面向工业设备的威胁分析模型

在网络威胁分析中,部署在网络中的各式安全防护系统所产生数据具有多样化和复杂化的特点,各类威胁分析模型被提出并应用于此类问题,并且在一定程度上对系统整合威胁分析提供了有效的帮助。

对于工业设备中常用威胁分析模型存在3点问题:1)所需系统资源高,威胁分析需要对系统日志,网络报文和数据库进行实时扫描,这对许多工业设备来说容易造成系统过载;2)传统威胁分析对各类数据进行格式统一时会遇到对报文有效信息的误裁剪,尤其是对存在特殊通信协议的系统;3)由于设计和算法的复杂性,系统对攻击的响应滞后,这对安全性要求高的工业设备来说同样是不可接受的。基于以上问题,研究提出面向工业设备的威胁分析模型,模型结构如图2所示。

模型将信息安全领域划分为3个功能域,功能域之间相互关联,相互传输数据,完成系统整体的安全防护。其中数据功能域负责收集并提供对安全防护有价值的信息;设备功能域用于获取设备信息并评估系统安全风险值;威胁分析功能域是模型中的关键域,负责处理系统日志中的安全信息,入侵检测产生的安全信息,并将所需的数据综合分析后得到设备的风险值,其功能结构如图3所示。

威胁分析功能域将不同来源的安全特征参数进行汇总,目的是将整个系统中提供的安全计算数据一起纳入风险模型的考量范围。但是风险模型输入的各安全特征对网络的影响参数不同,在优化威胁分析模型时,参考了专利[30]提出的基于灰色模型的网络脆弱性节点的主动预测方法的权重评估内容计算安全特征对网络全局的影响权重。

在实际计算中首先对图3中威胁分析功能域中安全分析与其他功能域的9项安全特征参数建立观测矩阵

$$\boldsymbol{A}=\begin{pmatrix} f_1(1)f_1(2) & \cdots & f_1(9) \\ f_2(1)f_2(2) & \cdots & f_2(9) \\ \cdots & \cdots & \cdots \\ f_t(1)f_t(2) & \cdots & f_t(9) \end{pmatrix}, \tag{1}$$

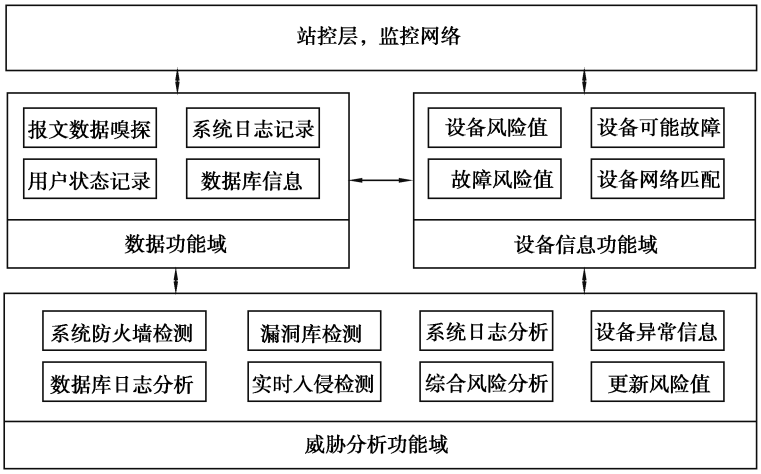


**图 2　面向工业设备的威胁分析模型结构**

**Fig. 2　The threat analysis model structure of industrial devices**

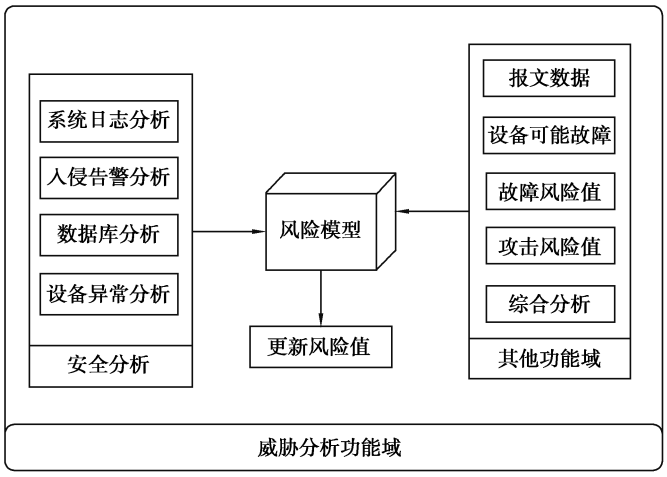


**图 3　威胁分析功能域结构**

**Fig. 3　The functional domain structure of threat analysis**

其中:$t$ 代表时刻,$f_t(1)$代表第 $t$ 时刻第 1 个安全特征参数的影响值,并且按照公式(2)对观测矩阵进行无量纲处理得到矩阵 $\boldsymbol{A}_1$。

$$f'_t(i)=\frac{f_t(i)}{f_1(i)}, \tag{2}$$

$$\boldsymbol{A}_1=\begin{pmatrix}1 & \cdots & 1\\ f'_2(1)f'_2(2) & \cdots & f'_2(9)\\ \cdots & \cdots & \cdots\\ f'_t(1)f'_t(2) & \cdots & f'_t(9)\end{pmatrix}, \tag{3}$$

此时矩阵 $\boldsymbol{A}_1$的第一列向量为观测向量,其他列为比较向量,通过公式(4)计算得到各子项的关联系数并构成关联矩阵 $\boldsymbol{M}$。

$$\varepsilon_t(j)=\frac{\min_t(\min_j|f'_t(j)-f'_t(1)|)+0.5\max_t(\max_j|f'_t(j)-f'_t(1)|)}{|f'_t(j)-f'_t(1)|+0.5\max_t(\max_j|f'_t(j)-f'_t(1)|)}。 \tag{4}$$

$$\boldsymbol{M}=\begin{bmatrix}1 & 1 & \cdots & 1\\ \varepsilon_2(1) & \varepsilon_2(2) & \cdots & \varepsilon_2(9)\\ \cdots & \cdots & \cdots & \cdots\\ \varepsilon_t(1) & \varepsilon_t(2) & \cdots & \varepsilon_t(9)\end{bmatrix}, \tag{5}$$

此时由关联矩阵 $\boldsymbol{M}$，再通过公式(6)、(7)、(8)得出任意2个安全特征参数的关联度，并形成新矩阵 $\boldsymbol{M}'$。

$$\nu(f(i),f(1))=\frac{1}{T}\sum\nolimits_t\varepsilon_t(i), \tag{6}$$

$$\nu(f(k),f(1))=\frac{1}{T}\sum\nolimits_t\varepsilon_t(k), \tag{7}$$

$$\nu(f(i),f(k))=\frac{\nu(f(i),f(1))}{\nu(f(k),f(1))}, \tag{8}$$

$$\boldsymbol{M}'=\begin{bmatrix}1 & \nu(f(1),f(2)) & \cdots & \nu(f(1),f(9))\\ \nu(f(2),f(1)) & 1 & \cdots & \nu(f(2),f(9))\\ \cdots & \cdots & \cdots & \cdots\\ \nu(f(i),f(1)) & \nu(f(i),f(2)) & \cdots & 1\end{bmatrix}, \tag{9}$$

因为 $\boldsymbol{M}'$ 是非负对称矩阵，$\boldsymbol{M}'$ 存在最大模特征值 $\lambda$，设特征向量为 $\boldsymbol{P}$，存在 $\lambda\boldsymbol{P}=\boldsymbol{M}'\boldsymbol{P}$，此时该特征向量 $\boldsymbol{P}$ 即表示第 $i$ 个安全特征参数在全局中的影响。

计算后可以根据9个安全特征参数在网络中的不同影响加以权值分析，使得模型计算出的风险值更具有说明性。

### 2.2 风险数值计算系统模型

在对威胁分析功能域模型中的9个影响参数进行计算后，系统在面临威胁攻击时主要产生影响的安全风险参数为以下5类，攻击风险，故障风险，报文数据，入侵告警以及设备可能故障，其中后三者为前两者的计算提供依据。所以攻击与故障的风险对整个系统的安全分析具有重要价值，为了进一步使计算出的安全风险具有代表性和说服力，系统将攻击与故障造成的风险进行分类。系统使用 $C$(confidentiality)，$I$(integrity)，$A$(Availability)3个维度的安全风险因素作为分析元组，结合入侵检测中识别到威胁报文的攻击动态计算风险数值，最后将计算结果输入到威胁分析功能域中，通过功能模型对系统设备风险值实时更新。

在计算风险元组的参数数值时参考层次分析法(AHP)计算模型，考虑到该方法在一致性比较中一致性检验的代价不确定，并且存在主观性判断影响，为了优化参数生成，文献[31]中提出的攻击模型与文献[32]中提出的模糊一致判断矩阵实现对风险值参数的优化。

算法首先对某次入侵攻击 $R$ 在机密性方面对下层传播层次元组中的 $a_1,a_2,\cdots,a_n$ 进行重要程度比较，按照表1中的0.1～0.9标度的九标度法，从而生成模糊矩阵 $\boldsymbol{C}$。

**表1 0.1～0.9标度表**

**Table 1 0.1～0.9 elements scale**

| 标度 | 定义 |
|---|---|
| 0.9 | 两元素重要性相差极多 |
| 0.8 | 两元素重要性相差很多 |
| 0.7 | 两元素重要性明显不同 |
| 0.6 | 两元素重要性略微不同 |
| 0.5 | 两元素重要性相同 |

$$\boldsymbol{C}=\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix},$$

矩阵 $\boldsymbol{C}$ 满足：$r_{ii}=0.5, i=1,2,\cdots,n$；$r_{ij}=1-r_{ji}, i=1,2,\cdots,n$；$r_{ij}=r_{ik}-r_{jk}, i, j, k=1,2,\cdots,n$。

接着对矩阵判断是否满足一致性，如果不满足则对矩阵进行一致化处理：以 1,2 行为例，$r_{11}+r_{22}=r_{12}+r_{21}=1$；$r_{11}-r_{21}=r_{12}-r_{22}=a$，$r_{2k}=r_{1k}-a$；同理推出，$r_{11}-r_{31}=r_{13}-r_{33}=b$，$r_{32}=r_{12}-b$，进一步得出 $r_{kj}=r_{1j}-\boldsymbol{C}(j=2,3,\cdots,n, k\neq j)$；

根据公式(10)计算得出新矩阵，最后按照公式(11)进行归一化处理后得到参数值。

$$r'_{ij}=\frac{1}{2n}\sum_{k=1}^{n}(r_{ik}-r_{jk})+0.5; \tag{10}$$

$$\boldsymbol{W}_i=\frac{1}{n}-\frac{1}{2a}+\frac{1}{na}\sum_{k=1}^{n}r'_{ik}, \tag{11}$$

在完整性、可用性方面同理，经计算得到攻击在机密性、完整性、可用性 3 个方面的评价指数。

在得到了攻击在 3 个维度的评分后对风险值进行进一步计算，公式如下

$$f_c(x)=[\sum_{i=1}(C\cdot TC_i)]/N, \tag{12}$$

$$f_i(x)=[\sum_{i=1}(I\cdot TI_i)]/N, \tag{13}$$

$$f_a(x)=[\sum_{i=1}(A\cdot TA_i)]/N, \tag{14}$$

其中：$f_c(x)$，$f_i(x)$，$f_a(x)$ 分别表示攻击在机密性，完整性，可用性方面所造成影响与范围的评价指数；$i$ 代表第 $i$ 个攻击可能引起的故障；$C$，$I$，$A$ 分别代表该攻击在机密性、完整性，可用性方面的评价指数；$TC_i$，$TI_i$，$TA_i$ 分别代表当前故障在机密性、完整性、可用性方面的评价指数；$N$ 代表可能引起故障的总数。

经过公式(12)、(13)、(14)计算出的对应风险值可以将攻击对系统风险影响的范围进行较好的定义，从而对后续系统安全防护提供重要依据。得到攻击在不同维度造成的风险评估后，系统需要将风险值更新至设备列表中，具体可以依据的函数为

$$F_c(x)=f_C(x)\cdot T(y), \tag{15}$$

$$F_I(x)=f_i(x)\cdot T(y), \tag{16}$$

$$F_a(x)=f_a(x)\cdot T(y), \tag{17}$$

其中 $y$ 代表该攻击来源攻击的次数，$T(y)$ 函数为

$$T(y)=\begin{cases} 100, & y\geqslant 20 \\ 50, & 0\leqslant y<20 \\ 20, & 5\leqslant y<10 \\ 10, & 1<y<5 \\ 1, & \mathrm{y}=1 \end{cases}, \tag{18}$$

$T(y)$ 函数根据不同攻击次数设定不同的参数以提高风险值，将最终的风险值更新到系统中。

在威胁与风险评价模型实际部署在入侵检测系统中时，系统执行流程将分为 3 步：1)每当系统受到威胁攻击，系统将首先通过威胁分析模型把 9 条关键参数传入到威胁分析功能域中，该域通过基于灰色模型的网络脆弱性节点主动预测的方法将 9 条参数的权重计算出来；2)系统将作用于攻击与故障的 5 条加权后的参数传入风险数值计算系统模型中，经过模糊一致矩阵和相应算法得出攻击在 3 个安全维度中的评估；3)将得出的评估数值传回威胁分析功能域，以经过三维风险计算的 5 条高权重安全影响因素为主体，加上 4 条低权重安全影响因素综合得出系统的安全风险，并实时更新。

# 3 系统实现

## 3.1 系统网络结构设计

为了将系统网络部署在智能变电站站控层设备中，本系统首先部署在与站控层设备具有相同内核的CentOS云服务器中，并且对系统的相关实验也在相同环境中建立并进行测试，服务器中的系统部署如图4所示，其中系统的重点功能是根据检测出的数据对告警终端信息的后续处理以及设备风险值的同步更新。

对告警信息提供了下载与查看攻击详情的同时，可以联合查询，如来自同一攻击源发送的其他攻击信息等。对设备风险值的同步更新通过对数据库的低耦合性设计，使得在交互过程中可以保证良好的数据独立性。

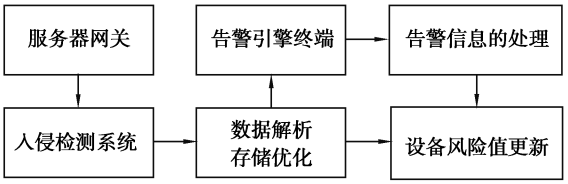


**图4 服务器中的系统结构**

**Fig. 4 The system structure in servers**

## 3.2 数据库与交互设计

系统在实现风险值更新模块设计时采用了共享数据表的方法，通过数据访问实现入侵检测系统与风险计算关联交互，对数据库要进行相应的优化设计。

系统告警信息通过风险数值计算模型得出的三维度风险值，将分别存储在两张表中，第一张表在攻击发生后的初次计算后写入，第二张表在写入后通过更新算法继续写入，系统只从第二张表中获得更新后的数据，第一张表只用于数据计算，表示结构如表2所示，并且单独列出数据表表示更新后的系统风险值表结构所示，这样降低数据耦合度可以使得数据访问效率和数据安全性提升。

**表2 风险值更新数据表设计**

**Table 2 The updating data of risk values**

| 字段名 | 类型 | 定义 |
|---|---|---|
| FID | Int | 攻击编号 |
| PID | Int | 目标设备 |
| C_score | Double | 机密性风险值 |
| I_score | Double | 完整性风险值 |
| A_score | Double | 可用性风险值 |

通过对数据表的共享处理实现了入侵检测系统对安全分析风险值更新，另外在系统交互方面，为了更好地适应智能变电站网络，对入侵检测系统采用模块化分析，通过优化存储连接的方法优化性能表现。入侵检测系统结构分为：数据嗅探，威胁分析，响应处理和数据存储模块。模块之间的关系如图5所示，其中数据嗅探器为被动式嗅探工具；威胁分析使用了官方数据漏洞库并提供更新漏洞库版本接口，并增加自定义威胁来源功能；在响应处理中对识别的威胁报文提供下载，查看详细信息和攻击类别的功能；最后优化存储结构，使得风险分析系统可以有效更新被攻击设备的风险值。

经过对各功能和效率的比较，嗅探器部分功能实现选择Snort，使得系统在满足被动式报文获取的同时可以匹配官方Snort漏洞库进行威胁分析，这样使得系统在入侵检测中更加适配，执行效率更高。Snort威胁分析是一种基于特征的入侵检测系统，入侵检测的关键模块在于威胁分析模块，其处理逻辑如图6所示，其中报文解码与预处理对报文进行格式处理并先后交由2次匹配判断是否为威胁报文并存储，其数据可以为后续进行数值分析提供依据。

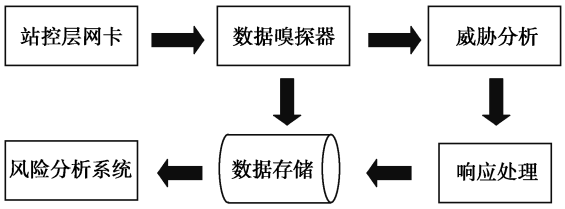


**图 5　入侵检测系统结构**

**Fig. 5　Intrusion detection system structure**

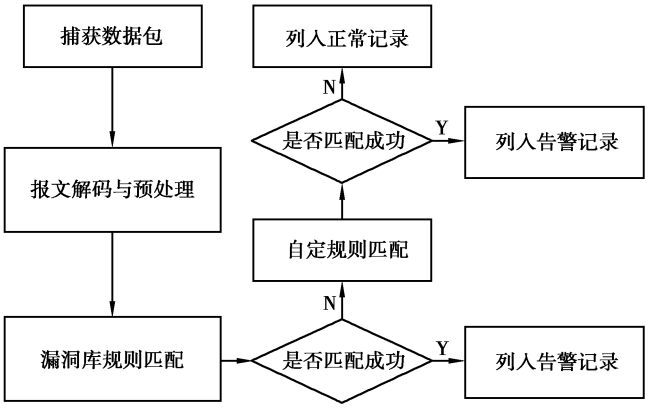


**图 6　威胁分析处理逻辑**

**Fig. 6　The logic of threat analysis and processing**

在按照上述结构完成系统搭建后,对系统交互逻辑实现了有效的优化。

## 4　实验与结果分析

系统在服务器中的部署后进行了运行效率以及模拟攻击测试的实验。其中运行效率分别考虑网络极限和处理器极限状态时的系统运行情况。

在网络测试中对 1 M 带宽的服务器中下载上传文件,使得网络带宽被占用的同时对服务器发送标记威胁报文,从而测试系统的有效性。结果如表 3 所示。

**表 3　网络极限测试**

**Table 3　Limit testing of network**

| 带宽占用比/% | 发送测试报文 | 接收率/% |
|---|---|---|
| 98 | 50 | 100 |
| 96 | 50 | 100 |

在处理器测试中对 1 核 1 G 内存的服务器中对文件,在处理器占用时对服务器发送标记威胁报文,从而测试系统的有效性。结果如表 4 所示。

**表 4　处理器极限测试**

**Table 4　Limit testing of CPU**

| 内存占用比/% | 发送测试报文 | 接收率/% |
|---|---|---|
| 92 | 50 | 100 |
| 86 | 50 | 100 |

如上述实验所示，在网络和处理器资源占用较大时系统依然具有良好的可靠性，并且证明了本系统对资源的占用低，不影响系统性能。

模拟攻击测试共分为5种类型的测试，包括更改权限，数据库访问，删除文件，虚假指令以及自定义威胁来源的测试。

测试结果使用混淆矩阵来评估表现，如表5所示。

**表5 混淆矩阵**

**Table 5 Confusion Matrix**

| 实际状态/预测状态 | 正常报文 | 攻击报文 |
|---|---|---|
| 正常报文 | $TP$ | $FN$ |
| 攻击报文 | $FP$ | $TN$ |

其中，$TP$(真阳性)表示正确预测的正常报文；$FN$(假阴性)表示错误预测的正常报文；$FP$(假阳性)表示错误预测的攻击报文；$TN$(真阴性)表示正确预测的攻击报文。其中预测正确的是 $TP$，$TN$，故攻击实验的系统精确值计算方法为

$$P=\frac{TP+TN}{TP+FP+TN+FN}, \tag{19}$$

分别对上述的5种攻击进行测试，将测试结果统计后如表6所示。

**表6 模拟攻击测试**

**Table 6 Testing of simulated attacks**

| 攻击种类 | 发送测试报文 | 精确值(P)/% |
|---|---|---|
| 更改权限 | 61 | 98.3 |
| 数据库访问 | 84 | 96.3 |
| 删除文件 | 72 | 86.1 |
| 虚假指令 | 62 | 67.7 |
| 自定义威胁来源 | 80 | 100 |

在系统的攻击测试中，虚假指令一项识别率较低，分析认为主要有以下3点原因：1)入侵检测的关键部分漏洞规则检测中对虚假指令的涵盖不足；2)单个服务器难以还原智能变电站网络结构，所发送的虚假指令不能向下传输；3)因为构造的模拟报文不能正确触发预警；这种情况可以通过自定义规则，或者在实际网络中测试优化。

通过上述实验结果，总体上入侵检测系统可以满足主要的攻击检测需求，并且对系统的资源需求较低，可以作为安全辅助系统部署在智能变电站中。

## 5 结 论

主要针对智能变电站中建立入侵检测系统进行研究，通过调整系统结构，存储方式，同时提出三维风险值更新算法，将入侵攻击的范围与影响直观的体现出来，实现了实时分析的被动式入侵检测系统，并且通过一系列实验证明了系统的有效性，为安全防护和后续研究提供了相关的依据和经验。

**参考文献：**

[1] Gaddam R, Nandhini M. An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment[C]// 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT). March 10-11, 2017. Coimbatore, India. IEEE, 2017: 10-15.

[2] 肖静. 基于IEC 61850规约的智能变电站在线监测系统设计[J]. 自动化应用, 2015(9): 107-108.

Xiao J. Design of intelligent substation online monitoring system based on IEC 61850[J]. Automation Application, 2015 (9): 107-108. (in Chinese)

[3] Kimura S, Rotta A, Abboud R, et al. Applying IEC 61850 to real life: modernization project for 30 electrical substations [C]// Proceedings of the 10th Annual Western Power Delivery Automation Conference. Spokane: WA, 2008: 1-18.

[4] Janssen M C, Apostolov A. IEC 61850 impact on substation design[C]// 2008 IEEE/PES Transmission and Distribution Conference and Exposition. April 21-24, 2008, Chicago, IL, USA. IEEE, 2008: 1-7.

[5] 王明俊. 智能电网热点问题探讨[J]. 电网技术, 2009, 33(18): 9-16.
Wang M J. Some highlights in relation to smart grid[J]. Power System Technology, 2009, 33(18): 9-16. (in Chinese)

[6] 刘昊昱, 左群业, 张保善. 智能变电站过程层网络性能测试与分析[J]. 电力系统保护与控制, 2012, 40(18): 112-116.
Liu H Y, Zuo Q Y, Zhang B S. Process level network performance testing and analysis in smart substation[J]. Power System Protection and Control, 2012, 40(18): 112-116. (in Chinese)

[7] 刘姗梅, 王胜, 柴继文, 等. 智能变电站安全脆弱性评估方法[J]. 重庆大学学报, 2017, 40(7): 52-62.
Liu S M, Wang S, Chai J W, et al. The assessment method of cyber-security vulnerability for smart substation[J]. Journal of Chongqing University, 2017, 40(7): 52-62. (in Chinese)

[8] 焦建林, 韩盟, 刘少波. SCD 图形化技术在网络报文记录分析装置中的应用[J]. 华北电力技术, 2016(4): 28-32.
Jiao J L, Han M, Liu S B. Application of SCD graphic technology in message recording and analysis device[J]. North China Electric Power, 2016(4): 28-32. (in Chinese)

[9] Rashid M T A, Yussof S, Yusoff Y, et al. A review of security attacks on IEC61850 substation automation system network[C]// Proceedings of the 6th International Conference on Information Technology and Multimedia. November 18-20, 2014, Putrajaya, Malaysia. IEEE, 2014: 5-10.

[10] 王松, 陆承宇. 数字化变电站继电保护的 GOOSE 网络方案[J]. 电力系统自动化, 2009, 33(3): 51-54,103.
Wang S, Lu C Y. A GOOSE network scheme for relay protection in digitized substations[J]. Automation of Electric Power Systems, 2009, 33(3): 51-54,103. (in Chinese)

[11] Sidhu T S, Gangadharan P K. Control and automation of power system substation using IEC61850 communication[C]// Proceedings of 2005 IEEE Conference on Control Applications, 2005. CCA 2005. August 28-31, 2005, Toronto, Canada: IEEE, 2005: 1331-1336.

[12] Baker W H, Wallace L. Is information security under control?: investigating quality in information security management [J]. IEEE Security & Privacy, 2007, 5(1): 36-44.

[13] Grinstein U M F G G, Wierse A. Information visualization in data mining and knowledge discovery[M]. US: Morgan Kaufmann, 2002.

[14] 王志勇. 基于 k 近邻密度峰值聚类混合算法的网络入侵检测[J]. 自动化技术与应用, 2019, 38(12): 48-52.
Wang Z Y. Network intrusion detection based on K nearest neighbor density peak clustering hybrid algorithm [J]. Techniques of Automation and Applications, 2019, 38(12): 48-52. (in Chinese)

[15] 张玲, 张建伟, 桑永宣, 等. 基于随机森林与人工免疫的入侵检测算法[J]. 计算机工程, 2020, 46(8): 146-152.
Zhang L, Zhang J W, Sang Y X, et al. Intrusion detection algorithm based on random forest and artificial immunity [J]. Computer Engineering, 2020, 46(8): 146-152. (in Chinese)

[16] 池亚平, 凌志婷, 王志强, 等. 基于支持向量机与 Adaboost 的入侵检测系统[J]. 计算机工程, 2019, 45(10): 183-188,202.
Chi Y P, Ling Z T, Wang Z Q, et al. Intrusion detection system based on support vector machine and adaboost[J]. Computer Engineering, 2019, 45(10): 183-188,202. (in Chinese)

[17] 王丽媛, 李晓风, 李玉洁, 等. 基于系统调用的交互式入侵检测系统设计与实现[J]. 仪表技术, 2020(3): 1-5,11.
Wang L Y, Li X F, Li Y J, et al. Design and implementation of interactive intrusion detection system based on the system call[J]. Instrumentation Technology, 2020(3): 1-5,11. (in Chinese)

[18] 张泽, 樊江伟, 周南. 基于 MEA-LVQ 的网络态势预测模型[J]. 信息安全研究, 2020, 6(6): 499-505.
Zhang Z, Fan J W, Zhou N. Network situation prediction model based on MEA-LVQ[J]. Journal of Information Security Research, 2020, 6(6): 499-505. (in Chinese)

[19] 李渤, 徐伟光, 张涛. 基于攻击面的通用系统安全统一建模研究[J]. 信息系统工程, 2019(1): 18-20.
Li B, Xu W G, Zhang T. Research on universal system security unified modeling based on attack surface[J]. Information Systems Engineering, 2019(1): 18-20.

[20] 赵凯，辛阳，杨义先，等. 下一代网络安全脆弱性分析及威胁模型的建立[C]//第十一届全国青年通信学术会议论文集. 绵阳，2006：664-668.
Zhao K，Xin Y，Yang Y X，et al. Vulnerability analysis and threat model establishment of next generation network security[C]// Proceedings of the 11th National Youth Communication Academic Conference. China，Mianyang：Beijing University of Posts and Telecommunications Press，2006：664-668.

[21] 谭大礼，王明政，王璇. 面向服务的信息安全威胁分析模型[J]. 信息安全与通信保密，2011，9(9)：97-99，104.
Tan D L，Wang M Z，Wang X. Service-oriented threat analysis model for information security[J]. Information Security and Communications Privacy，2011，9(9)：97-99，104. (in Chinese)

[22] 王赛娥，刘彩霞，刘树新，等. 一种基于攻击树的4G网络安全风险评估方法[J]. 计算机工程，2021，47(3)：139-146，154.
Wang S E，Liu C X，Liu S X，et al. A method of 4G network security risk assessment based on attack tree[J]. Computer Engineering，2021，47(3)：139-146，154. (in Chinese)

[23] 王皓然，严彬元. 依赖小波神经网络算法的信息安全风险评估方法[J]. 信息技术，2018，42(12)：93-96.
Wang H R，Yan B Y. Information security risk assessment method based on wavelet neural network algorithm[J]. Information Technology，2018，42(12)：93-96. (in Chinese)

[24] 郭威，邬江兴，张帆，等. 基于自动机理论的网络攻防模型与安全性能分析[J]. 信息安全学报，2016，1(4)：29-39.
Guo W，Wu J X，Zhang F，et al. A cyberspace attack and defense model with security performance analysis based on automata theory[J]. Journal of Cyber Security，2016，1(4)：29-39. (in Chinese)

[25] 赵志岩，纪小默. 智能化网络安全威胁感知融合模型研究[J]. 信息网络安全，2020，20(4)：87-93.
Zhao Z Y，Ji X M. Research on the intelligent fusion model of network security situation awareness[J]. Netinfo Security，2020，20(4)：87-93. (in Chinese)

[26] Tawde R，Nivangune A，Sankhe M. Cyber security in smart grid SCADA automation systems[C]// 2015 International Conference on Innovations in Information，Embedded and Communication Systems (ICIIECS). March 19-20，2015，Coimbatore，India：IEEE，2015：1-5.

[27] Yang Y，Jiang H T，McLaughlin K，et al. Cybersecurity test-bed for IEC 61850 based smart substations[C]// 2015 IEEE Power & Energy Society General Meeting. July 26-30，2015，Denver，CO，USA：IEEE，2015：1-5.

[28] Drias Z，Serhrouchni A，Vogel O. Analysis of cyber security for industrial control systems[C]// 2015 International Conference on Cyber Security of Smart Cities，Industrial Control System and Communications (SSIC). August 5-7，2015，Shanghai，China：IEEE，2015：1-8.

[29] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. 中华人民共和国推荐性国家标准：工业通信网络，网络和系统安全，系统安全要求和安全等级 GB/T 35673—2017[S]. 北京：中国标准出版社.
General Administration of Quality Supervision，Inspection and Quarantine of the People's Republic of China，Standardization Administration of the People's Republic of China. National standard (recommended) of the People's Republic of China：industrial communication networks，network and system security，system security requirements and security levels. GB/T 35673—2017[S]. Beijing：Standards Press of China. (in Chinese)

[30] 胡昌振，吕坤，高程昕. 基于灰色模型的网络脆弱性节点的主动预测方法：CN109040027A[P]. 2018-12-18.
Hu C Z，Lv K，Gao C X. Active prediction method of network vulnerability nodes based on grey model：CN109040027A[P]. 2018-12-18. (in Chinese)

[31] 何明亮，陈泽茂，龙小东. 一种基于层次分析法的攻击树模型改进[J]. 计算机应用研究，2016，33(12)：3755-3758.
He M L，Chen Z M，Long X D. Improvement of attack tree model based on analytic hierarchy process[J]. Application Research of Computers，2016，33(12)：3755-3758. (in Chinese)

[32] 陶余会，刘家才，张吉军. 如何构造模糊层次分析法中模糊一致判断矩阵[C]//中国系统工程学会第12届年会论文集. 北京：海洋出版社，2002：460-464.
Tao Y H，Liu J C，Zhang J J. How to construct fuzzy consistent judgment matrix in fuzzy analytic hierarchy process[C]// Proceedings of the 12th annual meeting of Chinese Society for Systems Engineering. Beijing：China Ocean Press，2002：460-464. (in Chinese)

(编辑 侯 湘)