

新型电力系统的物联网终端传输 无线协议安全检测模型

徐思尧[†], 李妍, 周刚, 占聪聪, 张子瑛, 张凯

(广东电网有限责任公司电力科学研究院, 广东 广州 510080)

摘 要:研究了新型电力系统的物联网终端传输无线协议安全检测模型,提升协议安全检测效果。通过分析基于物联网的新型电力系统,确定常见的物联网终端传输无线协议攻击类型;以确定的攻击类型为基础,针对新型电力系统内的物联网终端,建立物联网终端传输无线协议安全检测模型。该模型中传输无线协议分析器通过 Sketch 方法,分析物联网终端传输无线协议;特征提取算法选择器,依据协议分析结果,选择主成分分析法或独立成分分析法,提取传输无线协议入侵特征;安全检测引擎利用最小二乘支持向量机,结合提取的入侵特征,输出传输无线协议攻击类型,完成传输无线协议安全检测结果。实验证明:该模型可有效提取物联网终端传输无线协议入侵特征,实现协议安全检测;对于不同物联网终端类型,该模型安全检测的 Kappa 系数均较高,即安全检测精度较高。

关键词:新型电力系统;物联网终端;传输无线协议;安全检测模型;主成分分析;支持向量机

中图分类号:TP309

文献标识码:A

Internet of Things Terminal Transmission Wireless Protocol Security Detection Model for New Power System

XU Siyao[†], LI Yan, ZHOU Gang, ZHAN Congcong, ZHANG Ziyang, ZHANG Kai

(Electric Power Research Institute, Guangdong Power Grid Co., Ltd., Guangzhou, Guangdong 510080, China)

Abstract: Research on the wireless protocol security detection model of Internet of Things terminal transmission in new power system to improve the effectiveness of protocol security detection. By analyzing the new power system based on Internet of Things, the common wireless protocol attack types of Internet of Things terminal transmission are determined. Based on the identified attack types, a wireless protocol security detection model for Internet of Things terminals in the new power system is established. In this model, the transmission wireless protocol analyzer analyzes the transmission wireless protocol of Internet of Things terminal through Sketch method. Feature extraction algorithm selector, according to the protocol analysis results, choose principal component analysis or independent component analysis, extract transmission wireless protocol intrusion characteristics. The security detection engine uses the least square support vector machine and the extracted intrusion features to output the attack type of the transmission wireless protocol and complete the detection result of the transmission wireless protocol security. Experiments show that this model can effectively extract the wireless protocol intrusion characteristics of network terminal transmission and implement protocol security detection. For different types of Internet of Things terminal, the Kappa coefficient of security detection of this model is high, that is, the security detection accuracy is high.

Key words: new power system; Internet of Things terminal; transmission wireless protocol; security detection model; principal component analysis; support vector machine

新型电力系统包含的物联网终端设备较多^[1-3],且各物联网终端设备的工作模式均不相同,为此,新型电力系统中物联网终端的传输无线协议也不相同^[4]。大量物联网终端传输无线协议接入互联网后,会降低新型电力系统物联网终端信息传输的安全性,为此,需研究物联网终端传输无线协议安全检测模型,提升信息传输的安全性^[5]。例如,肖勇等^[6]以真、伪电力物联网终端信号强度变化的差异性作为物联网终端传输无线协议的特征指纹,利用密度聚类算法,对特征指纹进行聚类,得到入侵检测结果,实现物联网终端传输无线协议安全检测。该模型可有效检测到传输无线协议是否存在入侵情况,具备较优的安全检测效果,提升电力物联网终端的安全防护水平。朱新兵等^[7]以新攻击面形成的攻击数据为历史数据,通过分析攻击数据在通信协议中的传播路径与交互过程,建立物联网终端无线传输协议安全检测模型,得到安全检测结果。该模型具备较优的安全检测结果,为电力物联网终端传输无线协议安全检测提供新的理论指导。但这两种模型仅能检测到物联网终端无线传输协议是否存在攻击,无法检测到攻击类型。为解决该问题,本文研究新型电力系统的物联网终端传输无线协议安全检测模型,确保新型电力系统信息传输的安全性。

1 物联网终端传输无线协议安全检测模型

1.1 基于物联网的新型电力系统

以物联网的技术架构为基础,建立基于物联网的新型电力系统,该系统的基本结构如图 1 所示。



图 1 新型电力系统结构图

感知层内的设备均属于物联网终端,利用传感器与射频设备等物联网终端采集电力信息。其中,网关负责将物联网终端接入网络层内。

网络层包括窄带物联网与无线局域网等^[8]。在传输电力信息过程中,各物联网终端采用的传输无线协议各不相同。

应用层根据接收的电力信息,通过分析基于物联网的新型电力系统,确定常见的物联网终端传输无线协议攻击类型,如表 1 所示。

表 1 物联网终端传输无线协议攻击类型

攻击类型	描述
女巫攻击	以虚假身份冒充其他节点,结合其余攻击手段达到攻击目的,包含直接通信与间接通信、伪造与窃取身份、同时攻击与非同时攻击三种形式。
流量嗅探攻击	攻击者可被动分析数据流,得到新型电力系统的机密信息。
节点仿冒攻击	攻击者模仿合法的射频设备信号在电力设备电子标签上采集机密信息。
幅值攻击	攻击者由一个电子标签幅值数据至另一个电子标签内,篡改机密信息。
水坑攻击	攻击者引诱传输无线协议内的全部数据流,同时删除该数据流,达到拒绝服务的目的。
中间人攻击	攻击者可监视与控制物联网终端间的通信,访问受限制信息。
拒绝服务攻击	攻击者可操控海量节点形成流量攻击某个物联网终端传输无线协议,令其信息传输失败。
路由攻击	以伪造合法理由信息的方式,在合法传输无线协议内形成错误路由表项,延长信息传输时间,破坏合法路由信息。

依据物联网终端传输无线协议攻击类型,建立物联网终端传输无线协议安全检测模型。

1.2 无线传输协议安全检测模型构建

在上述场景下,物联网终端设备可以通过 Wi-Fi、ZigBee 等无线协议进行通信。攻击者利用漏洞或其他手段,对物联网终端设备的无线协议进行攻击,从而窃取用户的隐私信息或控制设备。针对这种情况,构建物联网终端传输无线协议安全检测模型进行安全检测。该模型的技术架构如图 2 所示。

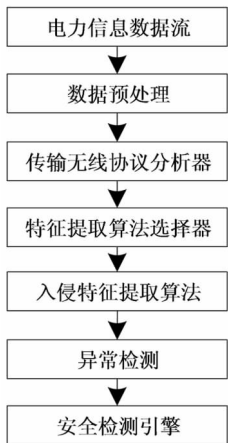


图 2 物联网终端传输无线协议安全检测模型技术架构

对采集到的数据进行去噪、归一化等预处理操

作,提高模型的准确性和鲁棒性。传输无线协议分析器通过 Sketch 方法,分析新型电力系统中物联网终端传输电力信息数据流时的传输无线协议。特征提取算法选择器依据传输无线协议分析结果,选择物联网终端传输无线协议入侵特征提取算法,并利用选择的特征提取算法,在电力信息数据流内提取传输无线协议入侵特征。通过异常检测,对异常数据进行识别和处理,降低误报率和漏报率。安全检测引擎利用最小二乘支持向量机(Least Squares Support Vector Machine, LSSVM),结合提取的入侵特征,输出传输无线协议安全检测结果,确定物联网终端传输无线协议攻击类型。

通过以上的构建过程,可以建立一个较为完整的物联网终端传输无线协议安全检测模型,实现对智能家居设备的无线协议进行安全检测。

1.2.1 物联网终端传输无线协议分析

安全检测模型中,利用传输无线协议分析器,分析物联网终端传输电力信息数据流时的传输无线协议。物联网终端传输无线协议分析即物联网终端传输电力信息数据流分析^[9,10]。在新型电力系统中,物联网终端传输的电力信息数据流是一个二元组 (i, v) , 电力信息数据流的索引是 i , 包含电力信息数据流的源地址与端口号等信息^[11]; 电力信息数据流的关键信息是 v 。通过 Sketch 方法分析电力信息数据流^[12]。依次传输的电力信息数据流是 $X = x_1, x_2, \dots, x_n$, 电力信息数据流数量是 n ; 第 j 项电力信息数据流是 $x_j(p_j, u_j)$; 其中, 电力信息数据流的传输无线协议类型是 p_j , 电力信息数据流的字节数是 u_j 。利用 Sketch 方法, 分析传输无线协议的具体步骤如下:

步骤 1: 对比分析连续的两个电力信息数据流 x_{new} 、 x 的索引项, 得到返回值 $\hat{p} = p - p_{\text{new}}$, 其中, x, x_{new} 的传输无线协议类型是 p, p_{new} 。如果 $\hat{p} \neq 0$, 那么电力信息数据流进入特征提取算法选择器, 并依据 $\hat{p}$ 对应的电力信息数据流分布情况, 选择特征提取算法; 如果 $\hat{p} = 0$, 那么继续步骤 2。

步骤 2: 对比分析 x_{new} 与 x 的数据项, 得到返回值 $\hat{u} = u - u_{\text{new}}$, 其中, x_{new}, x 的字节数是 u_{new}, u 。如果 $\hat{u} \neq 0$, 那么电力信息数据流进入特征提取算法选择器。

1.2.2 物联网终端传输无线协议入侵特征提取

特征提取算法选择器依据 2.2.1 小节确定的物联网终端传输无线协议类型, 选择合适的特征提

取算法。

当物联网终端传输无线协议传输的电力信息数据流是高斯分布时, 利用主成分分析法, 降维处理电力信息数据流^[13], 提取物联网终端传输无线协议入侵特征, 具体步骤如下:

步骤 1: 标准化处理 $X = x_1, x_2, \dots, x_n$, 公式如下:

$$\hat{x}_j = \frac{x_j - \bar{X}}{\sqrt{\varphi(X)}} \quad (1)$$

其中, X 的均值是 $\bar{X}$; 标准差函数是 $\varphi(X)$; 标准化处理后的电力信息数据流是 $\hat{x}_j$ 。

步骤 2: 求解 X 的协方差矩阵 Σ , 公式如下:

$$\Sigma = \frac{\theta \sum_{j=1}^n x_j x_j^T}{n} \quad (2)$$

其中, 修正系数是 θ ; 转置符号是 T 。

步骤 3: 计算 Σ 的特征值 $\lambda = \lambda_1, \lambda_2, \dots, \lambda_m$ 与特征向量 $z = z_1, z_2, \dots, z_m$ 。

步骤 4: 由大到小排列 λ , 选择前 k 个值为主要成分, 同时求解主成分贡献率, 公式如下:

$$\xi = \frac{\sum_{l=1}^k \lambda_l}{\sum_{l=1}^m \lambda_l} \quad (3)$$

其中, 第 l 个特征值是 λ_l 。 ξ 可呈现物联网终端传输无线协议入侵特征的重要性。

步骤 5: 依据 k 个特征值对应的特征向量 z_k 获取降维后的物联网终端传输无线协议入侵特征^[14], 公式如下:

$$y_j = \hat{x}_j z_k \quad (4)$$

其中, 第 j 个电力信息数据流的传输无线协议入侵特征是 y_j 。

当物联网终端传输无线协议传输的电力信息数据流不是高斯分布时, 利用独立成分分析法(Independent Components Analysis, ICA), 提取物联网终端传输无线协议入侵特征, 具体步骤如下:

步骤 1: 白化处理 $X = x_1, x_2, \dots, x_n$, 公式如下:

$$X'' = \hat{\lambda}^{-\frac{1}{2}} Z^T X \quad (5)$$

其中, 白化后的电力信息数据流是 X'' ; 电力信息数据流协方差矩阵内特征值矩阵是 $\hat{\lambda}$; 特征向量矩阵是 Z 。

步骤 2: 依据负熵 $E(X'')$ 确定电力信息数据流的随机程度, 并提取独立分量^[15], 即物联网终端传

输无线协议入侵特征 Y , $E(X'')$ 越大, 电力信息数据流的随机程度越大。 $E(X'')$ 的计算公式如下:

$$X'' = \hat{\lambda}^{-\frac{1}{2}} Z^T X \quad (5)$$

其中, 白化后的电力信息数据流是 X'' ; 电力信息数据流协方差矩阵内特征值矩阵是 $\hat{\lambda}$; 特征向量矩阵是 Z 。

步骤 2: 依据负熵 $E(X'')$ 确定电力信息数据流的随机程度, 并提取独立分量^[15], 即物联网终端传输无线协议入侵特征 Y , $E(X'')$ 越大, 电力信息数据流的随机程度越大。 $E(X'')$ 的计算公式如下:

$$E(X'') = H(\hat{X}'') - H(X'') \quad (6)$$

其中, 与 X'' 存在一致方差的高斯随机变量是 $\hat{X}''$; X'' 与 $\hat{X}''$ 的微分熵是 $H(X'')$ 、 $H(\hat{X}'')$ 。

1.2.3 基于 LSSVM 的终端传输无线协议安全检测

安全检测引擎利用 LSSVM, 结合 1.2.2 小节提取的物联网终端传输无线协议入侵特征输出传输无线协议攻击类型, 完成物联网终端传输无线协议安全检测。

令物联网终端传输无线协议入侵特征样本是 $Y = \{y_1, y_2, \dots, y_k\}$, LSSVM 的训练样本集是 $D = \{y_i', s_i'\}$, 其中, $i' = 1, 2, \dots, k$, 样本数量是 k ; 第 i' 个物联网终端传输无线协议入侵特征样本是 y_i' , 即输入数据; 第 i' 个传输无线协议安全检测结果是输出数据 s_i' 。按照 Mercer 定理可知, LSSVM 内存在核函数 $K(\cdot)$ 与映射函数 $\phi(\cdot)$ 、 $K(\cdot)$ 、 $\phi(\cdot)$ 之间的关系为:

$$K(y_i', y_j') = \langle \phi(y_i'), \phi(y_j') \rangle \quad (7)$$

其中, 第 j' 个物联网终端传输无线协议入侵特征样本是 y_j' 。

利用 LSSVM 进行物联网终端传输无线协议安全检测过程中的优化问题, 公式如下:

$$\min R(w, b, y) = \frac{w^T w}{2} + \frac{\sigma \sum_{i=1}^k y_i'^2}{2} \quad (8)$$

$$\text{s. t. } s_i' = w^T \phi(y_i') + b + y_i'$$

其中, 权值是 w ; 偏置是 b ; 正则化参数是 σ ; 损失函数是 R 。

通过定义拉格朗日函数 F , 求解式(8), F 的表达公式如下:

$$F(w, b, y, \alpha) = R(w, y) - \sum_{i=1}^k \alpha_i' \{ [w^T \phi(y_i')] + b + y_i' - s_i' \} \quad (9)$$

其中, 拉格朗日乘子是 α_i' 。按照最优性条件, 计算式(9)的偏导, 并令其等于 0, 获取:

$$\begin{cases} \frac{\partial F}{\partial w} = 0 \rightarrow w = \sum_{i=1}^k \alpha_i' \phi(y_i') \\ \frac{\partial F}{\partial b} = 0 \rightarrow \sum_{i=1}^k \alpha_i' = 0 \\ \frac{\partial F}{\partial \alpha_i'} = 0 \rightarrow w^T \phi(y_i') + b + y_i' - s_i' = 0 \end{cases} \quad (10)$$

在式(9)内引入式(10), 可剔除 w , 获取式(8)的对偶问题:

$$\begin{bmatrix} 0 & 1^T \\ 1 & K + \sigma^{-1} I \end{bmatrix} \begin{bmatrix} b \\ \alpha \end{bmatrix} = \begin{bmatrix} 0 \\ s \end{bmatrix} \quad (11)$$

其中, 常数矩阵是 I ; 求解式(11)便可获取 b 与 α 的值。

最终, 获取物联网终端传输无线协议安全检测的判别结果, 公式如下:

$$s(y) = \text{sign}(\sum_{i=1}^k \sum_{j=1}^k \alpha_i' K(y_i', y_j') + b) \quad (12)$$

物联网终端传输无线协议安全检测判别结果对应的攻击类型如表 2 所示。

表 2 安全检测判别结果对应的攻击类型

判别结果	攻击类型
0	无攻击
1	女巫攻击
2	流量嗅探攻击
3	节点假冒攻击
4	复制攻击
5	水坑攻击
6	中间人攻击
7	拒绝服务攻击
8	路由攻击

2 实验分析

以某新型电力系统为实验对象, 利用本文模型对该新型电力系统物联网终端传输无线协议进行安全检测, 提升电力信息传输的安全性。该新型电力系统中包含 7 种类型物联网终端, 这 7 种物联网终端产生的电力信息将近 15 万条, 其中, 正常电力信息数量为 81959 条, 包含攻击的电力信息数量

为 67998 条,每条电力信息内均包含 70 维特征,在 7 种类型物联网终端产生的电力信息内,各抽取 2000 条数据作为实验数据集,实验数据集如表 3 所示。

表 3 实验数据集		
物联网终端名称	攻击数据/条	正常数据/条
温度传感器	1000	1000
湿度传感器	1000	1000
电流/电压传感器	1000	1000
射频设备	1000	1000
摄像机	1000	1000
电表	1000	1000
巡检设备	1000	1000

利用本文模型提取新型电力系统物联网终端传输无线协议入侵特征,提取的入侵特征维度如图 3 所示。

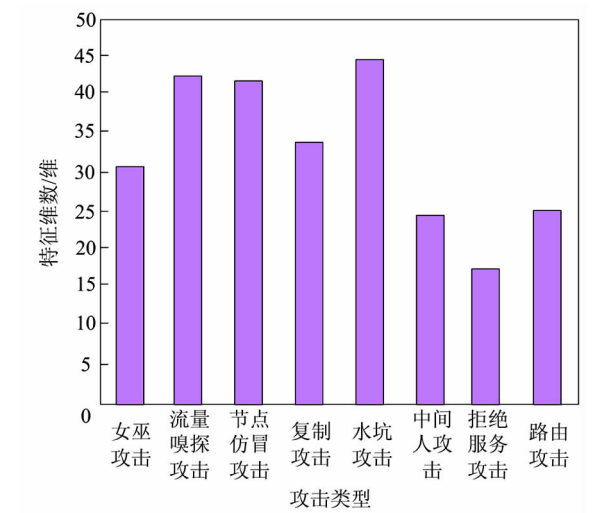


图 3 本文模型提取的入侵特征维度

根据图 3 可知,本文方法可有效提取不同攻击类型的入侵特征,其中,水坑攻击的入侵特征维度最高,在 45 维左右,但也明显低于原始电力信息数据维度。实验结果表明,本文模型可有效降维处理物联网终端传输的电力信息数据流维度,并有效提取物联网终端传输无线协议入侵特征。

利用汉明损失衡量本文模型物联网终端传输无线协议入侵特征提取效果,其值与入侵特征提取精度具有负相关关系,分析不同电力信息数量时,本文模型物联网终端传输无线协议入侵特征提取的汉明损失,分析结果如图 4 所示,汉明损失阈值是 0.5。

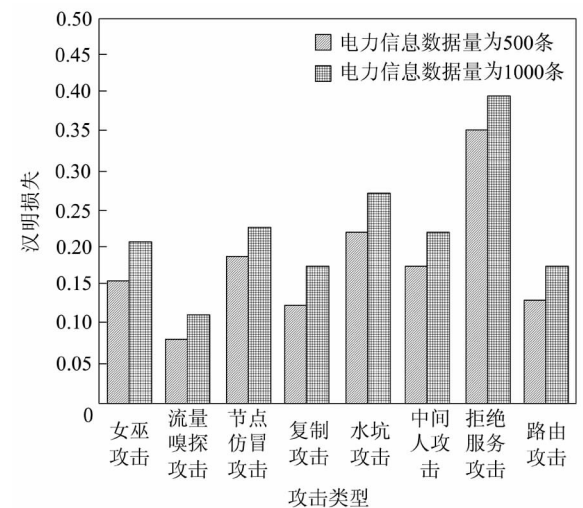


图 4 本文模型的汉明损失分析结果

由图 4 可知,对于不同攻击类型,本文模型提取物联网终端传输无线协议入侵特征时,电力信息数据量越大,汉明损失越高。其中,不同数据量下,拒绝服务攻击入侵特征的汉明损失均明显高于其余攻击类型,最高汉明损失在 0.40 左右,并未超过汉明损失阈值。实验结果表明,对于不同攻击类型,本文模型提取物联网终端传输无线协议入侵特征的汉明损失均较低,即特征提取精度较高。

利用本文模型对该新型电力系统物联网终端传输无线协议进行安全检测,安全检测结果如表 4 所示。

表 4 物联网终端传输无线协议安全检测结果		
物联网终端名称	安全检测结果	实际结果
温度传感器	8	路由攻击
湿度传感器	6	中间人攻击
电流/电压传感器	1	女巫攻击
射频设备	4	复制攻击
摄像机	3	节点仿冒攻击
电表	7	拒绝服务攻击
巡检设备	0	无攻击

由表 4 可知,本文模型可有效完成物联网终端传输无线协议安全检测,对比表 2 可知,本文模型的安全检测结果与实际结果完全相同,说明本文模型具备较高的物联网终端传输无线协议安全检测精度。

为进一步分析本文模型的物联网终端传输无线协议安全检测效果,利用 Kappa 系数衡量不同数据量时的安全检测效果,Kappa 系数越接近 1,说明安全检测精度越高。以温度传感器、射频设备

与摄像机三个物联网终端为例,分析结果如图 5 所示。

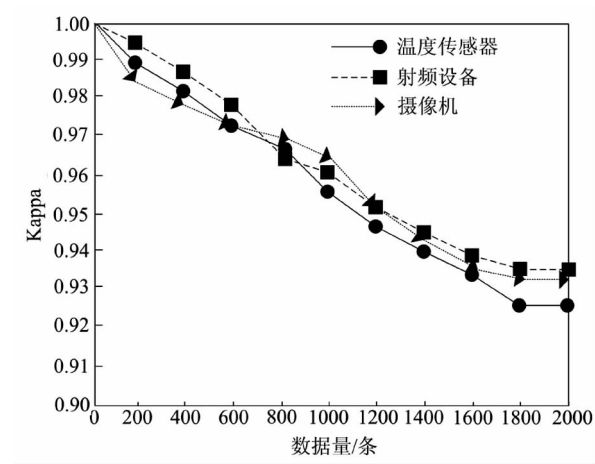


图 5 本文模型安全检测的 Kappa 系数分析结果

由图 5 可知,对于不同类型的物联网终端来说,随着数据量的提升,三种类型物联网终端传输无线协议安全检测的 Kappa 系数均呈下降趋势,当数据量为 1800 条时,三种类型物联网终端的 Kappa 系数均趋于稳定,分别稳定在 0.915、0.935、0.93,均与 1 较为接近,说明本文模型的传输无线协议安全检测精度较高。

3 结 论

本文提出了一种物联网终端传输无线协议安全检测模型,并在新型电力系统物联网场景下进行了实验验证。得出结论如下:

- (1)可以有效降低电力信息数据流的维度,并提取不同攻击类型的入侵特征。
- (2)可以有效完成物联网终端传输无线协议的安全检测,并且具有较高的检测精度和可靠性。
- (3)对于不同类型的物联网终端,本文模型的传输无线协议安全检测精度都较高,可以为电力系统的安全保障提供有力支持。

因此,本文提出的物联网终端传输无线协议安全检测模型在新型电力系统物联网场景下具有较高的实用价值,可为电力系统的安全保障提供有力支撑。

参考文献

[1] 刘伟,张雁丽,刘洁,等. 无线 LoRa 在全业务泛在电力物联网终端层的应用[J]. 电信科学,2020,36(9):94—101.

[2] 王晓楠,符劲轩,虞红芳,等. 基于抽象原则和模型检测的网络协议安全分析[J]. 北京邮电大学学报,2021,44(2):40—46.

[3] 程小辉,牛童,汪彦君. 基于序列模型的无线传感网入侵检测系统[J]. 计算机应用,2020,40(6):1680—1684.

[4] 廉文娟,赵朵朵,范修斌. 基于 CFL_BLP 模型的 CFL SSL 安全通信协议[J]. 计算机工程,2021,47(6):152—163.

[5] 夏锐,钱振江,刘苇. 一种基于 Isabelle/HOL 的安全通信协议验证方法[J]. 计算机工程,2021,47(1):146—153.

[6] 肖勇,钱斌,蔡梓文,等. 电力物联网终端非法无线通信链路检测方法[J]. 电工技术学报,2020,35(11):2319—2327.

[7] 彭鹏,薛东. 基于边缘代理的云边协同物联网框架设计及其应用研究[J]. 广东电力,2023,36(5):18—26.

[8] 朱俊翔,张翔. 基于 Event-B 对存在网络攻击的安全协议的改进研究[J]. 中国电子科学研究院学报,2020,15(6):530—538.

[9] 吴吉胜,洪征,马甜甜,等. 基于残差网络和循环神经网络混合模型的应用层协议识别方法[J]. 计算机科学,2022,49(11):293—301.

[10] 龚翔,冯涛,杜谨泽. 基于 CPN 的安全协议形式化建模及安全分析方法[J]. 通信学报,2021,42(9):240—253.

[11] 张杰,景雯,陈富. 基于被动分簇算法的即时通信网络协议漏洞检测[J]. 吉林大学学报(工学版),2021,51(6):2253—2258.

[12] 吴德鹏,柳毅. 基于可变网络结构自组织映射的入侵检测模型[J]. 计算机工程与应用,2020,56(12):81—86.

[13] 杨威超,郭渊博,李涛,等. 基于流量指纹的物联网设备识别方法和物联网安全模型[J]. 计算机科学,2020,47(7):299—306.

[14] 乔楠,李振兴,赵国生. XGBoost—RF 的物联网入侵检测模型[J]. 小型微型计算机系统,2022,43(1):152—158.

[15] 杨晗竹,完颜绍澎,胡光宇,等. 基于区块链的电力泛在业务接入网关的研究[J]. 广东电力,2020,33(8):54—61.