计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(3):316−321 [doi: 10.15888/j.cnki.csa.009007]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于随机域名检测和主动防御的用户站安全防护①

任小康[1,2], 向　勇[1], 李中伟[3], 常　星[1], 常　昱[1,2]

[1](中国科学院 沈阳计算技术研究所, 沈阳 110168)
[2](中国科学院大学, 北京 101408)
[3](哈尔滨工业大学 电气工程及自动化学院, 哈尔滨 150001)
通信作者: 任小康, E-mail: renxiaokang19@mails.ucas.ac.cn

摘　要: 电力监控系统是电力行业最重要的生产管理系统. 作为电力监控系统的重要组成部分, 缺少电网约束力的用户站将会成为网络攻击的重要目标. 为及时感知用户站侧网络攻击事件, 提出了一种结合用户站侧随机域名实时检测和主动防御的方法. 使用胶囊网络 (CapsNet) 结合长短期记忆网络 (LSTM) 对流量数据中提取的域名进行二分类, 当检测到随机域名时, 通过远程终端协议 (Telnet) 对路由器和交换机下发指令更新其安全策略或关闭路由器和交换机的业务接口以阻断网络攻击. 实验结果表明, 使用 CapsNet 结合 LSTM 分类算法在随机域名检测中准确率达到 99.16%, 召回率达到 98%, 通过 Telnet 协议可以联动路由器和交换机在不中断业务的情况下做出主动防御.

关键词: 用户站; 随机域名检测; 胶囊网络; 主动防御; 长短期记忆网络

引用格式: 任小康,向勇,李中伟,常星,常昱.基于随机域名检测和主动防御的用户站安全防护.计算机系统应用,2023,32(3):316–321. http://www.c-s-a.org.cn/1003-3254/9007.html

Security Protection of User Station Based on Random Domain Name Detection and Active Defense

REN Xiao-Kang[1,2], XIANG Yong[1], LI Zhong-Wei[3], CHANG Xing[1], CHANG Yu[1,2]

[1](Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110168 , China)
[2](University of Chinese Academy of Sciences, Beijing 101408, China)
[3](School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin 150001, China)

Abstract: The power monitoring system is the most important production management system in the power industry. As an important part of the power monitoring system, the user station will become the main target of network attacks if it lacks grid binding. In order to perceive the network attack events on the subscriber station side in time, a method combining real-time detection and active defense of random domain names on the subscriber station side is proposed. A capsule network (CapsNet) combined with a long short-term memory (LSTM) network is used to classify the domain names extracted from the traffic data. When a random domain name is detected, instructions are sent to routers and switches to update their security policies or shut down the service interfaces of routers and switches to block network attacks through the remote terminal protocol (Telnet). The experimental results show that the use of the CapsNet combined with the LSTM classification algorithm can achieve an accuracy of 99.16% and a recall of 98% in random domain name detection. Through the Telnet, routers and switches can be linked to make active defense without interrupting services.

Key words: user station; random domain name detection; capsule network (CapsNet); active defense; long short-term memory (LSTM)

① 收稿时间: 2022-07-29; 修改时间: 2022-09-07; 采用时间: 2022-09-30; csa 在线出版时间: 2022-12-23
CNKI 网络首发时间: 2022-12-27

© 中国科学院软件研究所 http://www.c-s-a.org.cn

电力监控系统正面临信息化、数字化和智能化变革, 利用信息系统和物理系统的高度融合, 带来了“电力-信息-业务”的发展模式, 同时也为电力监控系统安全带来了新的挑战[1]. 由于用户站安全防护意识薄弱, 其安全防护能力主要依赖于专用的安防设备, 并且用户站安防人员多以运行和检修人员为主缺乏专业的安全防护技能. 目前, 影响能源行业的安全攻击事件和漏洞事件频繁出现, 大量针对能源行业的勒索病毒、蠕虫病毒等现代恶意代码为了躲避安全人员的审查多采用随机域名与命令和控制服务器 (command and control server, C&C) 进行通信, 这种通信方式可以有效对抗域名黑名单屏蔽和特征码检测. 这些问题使电力监控系统用户站处于巨大安全风险之中, 并且针对用户站的网络攻击事件甚至可以通过调度数据网从用户站蔓延至主站和其他用户站, 从而对整个电力监控系统造成巨大安全威胁. 为了解决用户站的安全防护问题, 有研究人员通过对网络流量进行检测来发现异常行为[2−6], 但是电力系统中海量的异构终端为流量数据的检测与分析带来巨大困难. 如何有效检测电力监控系统中面临的安全风险是很多研究人员都在思考的问题[7−9].

为了有效检测电力监控系统用户站面临的安全风险, 本文以随机域名为研究对象, 提出一种随机域名检测和主动防御技术相结合的方法, 用来提高用户站的安全防护能力. 本文提出的方法结合胶囊网络 (capsule network, CapsNet) 与长短期记忆网络 (long short-term memory, LSTM) 对随机域名进行检测, 同时使用主动防御技术对随机域名的恶意解析行为作出防御. 通过实验证明, 本文提出的 CapsNet 与 LSTM 融合的重建网络在随机域名检测的准确率上有明显提升, 达到 99.16%. 并且主动防御技术可以对域名恶意解析行为做出有效防御.

1 随机域名检测研究现状

目前, 对随即域名的检测方法以机器学习和深度学习为主流方法. 机器学习方法需要人工提取域名字符特征, 检测效果相对深度学习较差, 但是具有较强的可解释性; 深度学习无需人工提取特征, 检测效果好, 是目前域名检测领域应用最广泛的方法.

由于随机域名使用随机域名生成算法生成具有很大的随机性, 这很容易造成随机域名与正常域名存在统计差异, 因此使用机器学习传统方法从域名自身的角度出发进行分类检测可以有效检测出随机域名[10−13]. 郭向民等人以域名生成算法 (domain generation algorithm, DGA) 生成的域名为识别对象, 基于隐式马尔可夫模型对恶意域名进行聚类分析, 从而实现 DGA 域名判定[14]; 张洋等人提出一种基于多元属性特征的恶意域名检测方法, 该方法在词法特征方面提取更加细粒度的特征然后使用随机森林算法检测随机域名[15]. 于光喜等人设计了一种域名检测系统, 首先使用随机森林对域名进行分类分析, 然后使用聚类和集合分析方法对疑似恶意域名进一步检测, 降低系统误检率[16]. 机器学习虽然在随机域名检测方面取得令人满意的结果, 但是传统机器学习方法需要人工提取大量域名特征, 并且无法提取域名字符间的前后关系, 检测效果取决的特征工程的质量, 因此检测效率和检测精度较低.

从自然语言处理角度开展基于深度学习的 DGA 域名分类检测成为现在主流的解决方法[17]. Woodbridge 等人[18] 设计了一种专门面向恶意域名的 LSTM 模型, 实现了对恶意域名的实时预测, 无需上下文信息且不用手工提取特征[19]. 陈立国等人提出一种基于门控循环单元 (gate recurrent unit, GRU) 的随机域名检测模型, 借助 GRU 自动学习域名向量特征, 最后通过神经网络计算分类[20]. 陈立皇等人则在 GRU 循环神经网络的基础上引入注意力机制, 加强域名中部分高随机性特征[21] . 张斌等人提出一种基于卷积神经网络 (convolutional neural network, CNN) 与 LSTM 相结合的域名检测模型, 该模型通过提取域名字符串中不同长度字符组合的序列特征进行恶意域名检测, 同时引入注意力机制为填充字符所处位置的输出特征分配较小权重, 降低填充字符对特征提取的干扰, 增强对长距离序列特征的提取能力[22]. 基于 CNN 提取域名字符串的组合特征, 然后使用 LSTM 充分挖掘域名字符串中字符上下文信息比单纯使用 LSTM、GRU 或 CNN 取得了更高的检测准确率, 但是 CNN 在识别空间关系特征时存在很大的局限性并且 CNN 的池化操作会丢失大量有价值的信息. 基于此, 本文提出一种结合 CapsNet[23] 和 LSTM 融合的域名检测模型, 该模型通过检测用户站中的随机域名并结合主动防御技术实现用户站的安全防护.

2 随机域名检测模型

勒索病毒、蠕虫病毒等大量现代恶意代码为了保证与 C&C 服务器通信过程的隐蔽性和安全性使用 DGA 与 C&C 服务器建立通信. 为了隐藏真实的恶意域名,

© 中国科学院软件研究所 http://www.c-s-a.org.cn

恶意代码一次所产生的虚假域名数量高达上千. 为有效检测用户站中随机域名, 本文提出一种 CapsNet 和 LSTM 融合的域名检测模型检测随机域名, 模型结构示意图如图 1 所示. 模型分为输入层、特征提取层和输出层. 同时, 该模型结合主动防御技术对域名恶意解析行为做出防御.

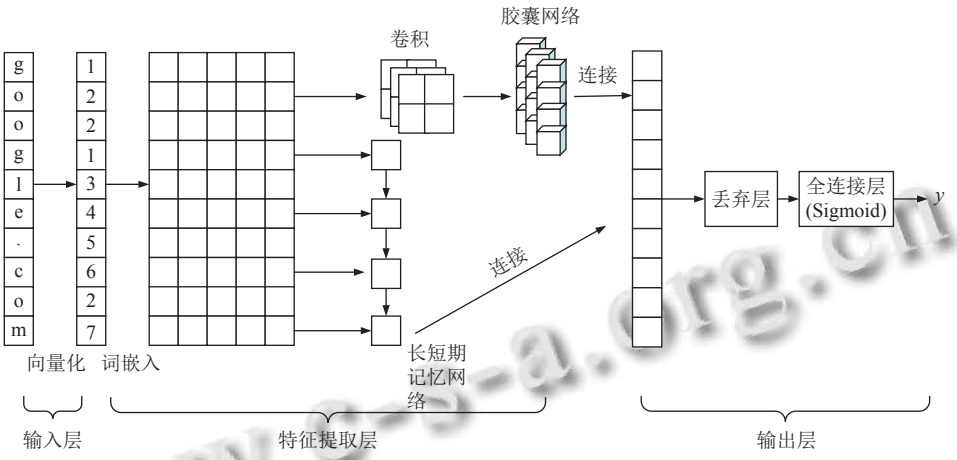

图 1 CapsNet+LSTM 模型结构示意图

本文随机域名检测模型使用的数据集中随机域名为 26 个恶意样本实际产生的随机域名, 正常域名为 Alex 网站排名前 100 万域名. 本文对域名的检测仅针对域名的二级域名, 例如 google.com 其二级域名为 google.

2.1 输入层

为了使神经网络能够处理域名数据需要首先将域名转换成向量. 本文中, 首先统计数据集中出现的所有字符形成字典, 然后对字典中的所有字符分配唯一索引. 对任意域名D (c_1, c_2, c_3, ⋯, c_L), 使用长度为 L 的向量表示, L 为数据集中最长域名的长度, 在本文数据集中 L 的值为 63, D中的值为字符 c_i (i=1, 2, 3,⋯, L) 在字典中的索引值.

2.2 特征提取层

特征提取层使用深度学习网络提取域名的字符组合和序列特征. 该层由词嵌入层、CapsNet 和 LSTM 组成.

本文采用词嵌入方式将域名转换成向量, 与独热表示、矩阵表示等相比具有维度低、语义可计算等优势[24]. 经过向量化后的域名经过词嵌入层转换为一个向量序列 (w_1, w_2, w_3, ⋯, w_L), $w_i \in \mathbb{R}^d$, d 为嵌入层向量维度, d 在本文中取 128, 可以保留足够的上下文信息.

CapsNet 用于提取域名字符串的空间特征, 将域名向量输入 CapsNet, CapsNet 首先使用一维卷积提取域名字符串中 n-gram 语法信息. 一维卷积通过尺寸为 k, $k \in \{2, 3, 5\}$的卷积核 ω, $\omega \in \mathbb{R}^{k \times d}$ 进行特征提取, 卷积操作使用 0 填充法. 卷积提取特征包括两个步骤, 卷积计算和卷积核移动. 卷积计算使用尺寸为 k 的卷积核在序列向量上平移, 每次对 k 个输入序列执行卷积计算, 计算公式如式 (1) 和式 (2) 所示:

$$x_i = \oplus(w_{i:i+k-1}) \tag{1}$$

$$c_i = g(x_i \cdot u + b) \tag{2}$$

$$x_i, u \in \mathbb{R}^{k \times d}$$

其中, $\oplus$表示向量拼接, u为权重矩阵, b 为偏置量, 卷积计算将权重矩阵u与拼接向量 b 做内积运算, 加上偏置 b 以后由非线性函数 g 处理后输出, 这里非线性函数 g 采用 ReLU 函数. 卷积核移动在序列向量上平移, 每次移动步长为 1. 经过卷积操作形成 3 个 63×64 的二维张量. 将 3 个二维张量进行拼接后形成一个 63×192 的二维张量, CapsNet 使用动态路由替代池化操作对输入的 63×192 张量进行特征提取, 最终输出 64×128 的二维张量. 动态路由过程如下所示, u^1, u^2是输入向量, c_1^r, c_2^r是动态更新的参数.

$b_1^0=0, b_2^0=0$
For r=1 to T do
$c_1^r, c_2^r = Softmax(b_1^{r-1}, b_2^{r-1})$
$s^r = c_1^r u^1 + c_2^r u^2$
$a^r = Squash(s^r)$
$b_i^r = b_i^{r-1} + a^r \cdot u^i$

© 中国科学院软件研究所 http://www.c-s-a.org.cn

T 取值为 3, u^1, u^2分别与 c_1^r, c_2^r加权求和得到 s^r, 经过 *Squash* 挤压函数得到a^r, a^r 与 u^i (i=1, 2) 做点乘运算加上得到b_i^r. 循环 T (T=3) 次得到最终更新的参数 c_1^r, c_2^r, 完成动态路由.

LSTM 层用于提取域名字符串的单字符序列特征, 将经过词嵌入层的域名向量序列拼接成单个向量 $e=\oplus(w_{1:L}), e\in^{L\times d}$ 输入到 LSTM 网络.

2.3 输出层

最后, 本文将 CapsNet 的输出与 LSTM 的输出拼接输入到全连接层进行分类, 使用 Sigmoid 函数作为分类函数, 二元交叉熵作为损失函数, 使用 Adam 优化器最小化损失函数. 输出结果记作 y, 其中 $y\in[0, 1]$. 损失函数计算公式为:

$$L(\hat{y},y)=-\frac{\sum_{i}^{N}[\hat{y}_i\log\hat{y}_i+(1-y_i)\log(1-\hat{y}_i)]}{N} \tag{3}$$

其中, $\hat{y}$为 Sigmoid 函数得到的预测概率, y 为实际目标值, DGA 域名值为 1, 正常域名值为 0.

同时为了验证 CapsNet 的实际效果, 本文设计了消融实验即仅使用 LSTM 模型对随机域名进行检测, 将检测结果与 CapsNet 加 LSTM 模型的结果做对比, 来验证 CapsNet 对模型的实际贡献, LSTM 模型结构如图 2 所示, 与 CapsNet 加 LSTM 模型结构相比, LSTM 去除了卷积操作和胶囊神经网络. 经过向量化和词嵌入操作后仅使用 LSTM 对域名特征进行提取, 然后经过输出层以后输出检测结果.

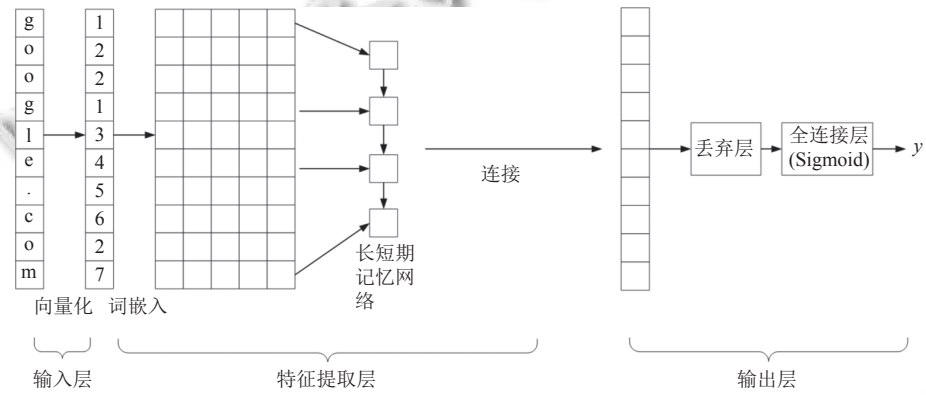

图 2 LSTM 模型结构图

3 实验及模型评估

3.1 数据源及数据预处理

本文实验所使用数据集由正常域名和随机域名两类域名组成, 其中随机域名来自 26 个恶意样本随机生成的域名共 100 万条, 类别标记为 1; 正常域名来自 Alex 网站排名前 70 万域名, 类别标记为 0. 本文首先统计域名中出现的所有唯一字符形成字典, 使用字典将域名向量化, 域名向量经过 Keras 中的词嵌入层形成 63×128 的张量作为神经网络的输入. 本文中数据集的 80% 用于训练, 20% 用于测试.

3.2 模型参数设置

本文提出的模型分为输入层、特征提取层和输出层. 输入层选用顺序结构, 将神经网络中神经元以顺序方式进行连接. 特征提取层首先使用 embedding 层进行字符级别的词嵌入, 嵌入维度 d 选择为 128. 接着使用 3 个尺寸为 k, $k\in\{2, 3, 5\}$的卷积核进行卷积操作, 神经元个数设置为 64. 然后使用胶囊网络进行特征提取, 胶囊网络个数设置为 64, 路由次数设置为 3, 输出维度为 128. 同时在特征提取层并行一个 LSTM 网络用于提取域名字符串中字符的上下文信息, 神经元个数设置为 64, 为防止 LSTM 过拟合, 设置丢弃层, 丢弃率设置为 0.5. 训练过程中 batch_size 和 epochs 分别设定为 128 和 10.

3.3 模型评估

为了评估本文提出的融合 CapsNet 和 LSTM 域名检测模型的效果, 将 CNN 模型、LSTM 模型、CNN+LSTM 模型与之做对比, 并使用传统机器学习分类方法 K 最近邻 (K-nearest neighbor, KNN)、逻辑回归 (logistic regression, LR)、决策树 (decision tree, DT) 等模型做参照.

从表 1 可以看出, 基于深度学习的分类模型性能要优于基于传统机器学习的分类方法. CNN 检测模型通过卷积操作可以提取域名的 n-gram 语法信息, 但是需要设计更深层次的卷积网络提取更长距离的语法信

© 中国科学院软件研究所 http://www.c-s-a.org.cn

息来提高准确率; LSTM 检测模型可以提取域名字符串的序列特征, LSTM 的 *F*1-score 比 CNN 提升了 1 个百分点, 准确率提升 1 个百分点, 说明通过提取域名字符串的序列特征可以提高准确率, 融合 CNN 和 LSTM 的模型相比较 CNN 模型和 LSTM 模型在准确率分别提升一个百分点和两个百分点. 同时对比 CapsNet+LSTM 与 LSTM 发现 CapsNet+LSTM 比单纯使用 LSTM 在召回率、精确率、准确率分别提高 1, 2, 3 个百分点. 表明 CapsNet 对模型提升效果明显.

为了更加直观的衡量不同模型的分类性能, 本文给出了不同模型的接收者操作特征 (receiver operating characteristic, ROC) 曲线, 如图 3 所示, ROC 曲线下面积 (area under ROC curve, AUC) 越接近 1 代表检测模型的真实性越高.

表 1 模型检测性能对比

模型	Recall (%)	Precision (%)	Accuracy (%)	*F*1-score
CapsNet+LSTM	98	98	99	0.98
CNN	95	96	96	0.97
LSTM	97	96	96	0.98
CNN-LSTM	98	97	98	0.98
LR	92	90	89	0.91
KNN	95	93	92	0.94
DT	92	91	90	0.92

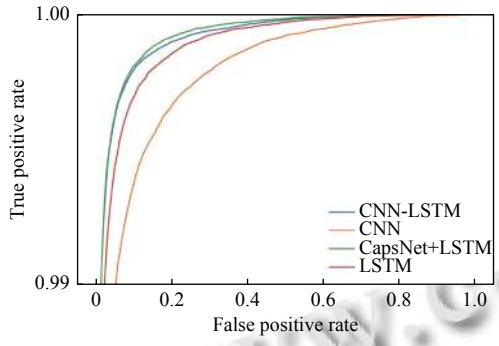

图 3 ROC 曲线对比图

由表 1 和图 2 可得, 本文提出的 CapsNet 结合 LSTM 的检测模型具有最高的检测准确率 99%, 说明使用胶囊网络的动态路由替换 CNN 的池化操作可以有效减少信息的丢失达到较高的准确率; 同时本文提出的模型 AUC 面积达到 0.999 具有最高的检测真实性.

3.4 主动防御

主动防御模块的作用是当随机域名检测模块检测到随机域名时根据随机域名解析结果作出主动防御以防止网络攻击事件进一步蔓延. 随机域名检测模型依次提取 DNS 流量中的域名, 使用白名单进行过滤, 接着随机域名检测模型对域名进行分类, 如果检测模型判定为随机域名则提取该域名对应的 IP 地址, 然后主动防御模块根据该 IP 地址通过 Telnet 协议更新交换机的访问控制列表 (ACL), 阻止与该 IP 地址建立连接; 如果该域名被判定为正常域名继续分析下一条域名. 主动防御流程如图 4 所示.

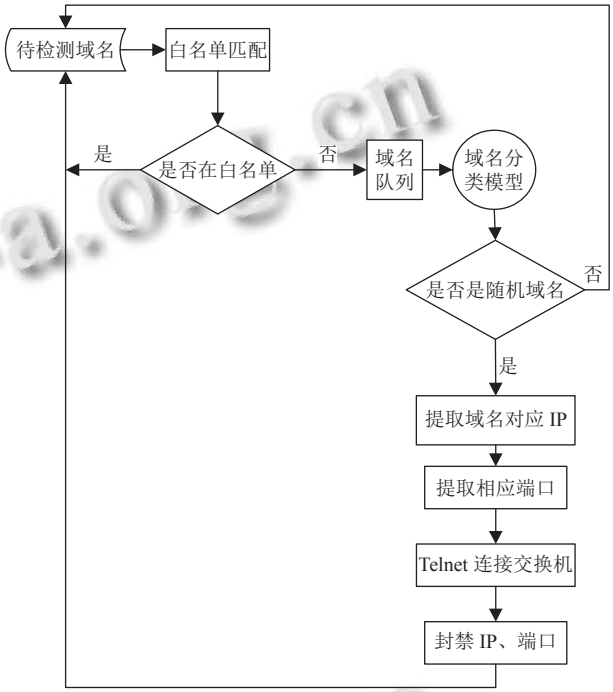

图 4 主动防御流程图

4 结语

本文提出了一种结合随机域名检测和主动防御技术的电力监控系统用户站安全防护方法. 本文提出的方法可以从用户站 DNS 流量中检测出随机域名, 然后根据随机域名的解析结果利用主动防御技术进行恶意连接的阻断. 在随机域名检测阶段, 本文提出的检测模型首先将域名进行向量化处理然后对域名进行分类; 主动防御则根据随机域名检测的结果提取域名对应的网际协议 (IP) 地址并完成相对应 IP 地址恶意连接的阻断. 本文最后以用户站 DNS 流量数据对本文提出的方法进行验证, 实验结果表明, 使用 CapsNet+LSTM 模型成功在连续 30 天的 DNS 流量中检测出 304 条随机域名, 并成功更新 2 条交换机的 ACL 阻止了 2 次恶意连接, 检测效果最好; 单纯 LSTM 模型只检测出了 268 条随机域名, 效果次之; 而使用机器学习方法最好情况下也只检测出 158 条随机域名. 经过实际验证,

© 中国科学院软件研究所 http://www.c-s-a.org.cn

CapsNet+LSTM 的模型能够满足实际使用需求.

本文提出的方法可以在用户站不中断业务的情况下通过随机域名检测和主动防御技术解决其安全防护问题. 该方法与现有的用户站防护方案相比主要有以下优点: (1) 针对用户站的安全防护现状提出了一种基于随机域名检测和主动防御结合的防护思路; (2) 当发现用户站存在随机域名解析行为时可以做出主动防御措施来阻止恶意连接而不需要中断业务. 未来主要的工作为: 进一步提高现有检测引擎的准确性; 进一步缩短随即域名检测模型的训练时间.

参考文献

1 张露. 电力监控系统网络安全威胁溯源技术分析. 通信电源技术, 2020, 37(20): 48–49, 52.

2 杜浩良, 孔飘红, 金学奇, 等. 基于深度学习的电力信息网络流量异常检测. 浙江电力, 2021, 40(12): 117–123. [doi: 10.19585/j.zjdl.202112016]

3 刘栋, 蒋正威, 朱英伟, 等. 基于 LDSAD 的电力监控系统网络流量异常检测. 浙江电力, 2022, 41(3): 87–92. [doi: 10.19585/j.zjdl.202203011]

4 杨航, 刘益松, 刘贵恒, 等. 基于网络流量异常检测的电网工控系统安全监测技术. 电子技术与软件工程, 2020, (22): 259–260.

5 李怡晨. 基于机器学习的电力工控网络流量异常检测技术研究 [硕士学位论文]. 上海: 上海交通大学, 2019. [doi: 10.27307/d.cnki.gsjtu.2019.001571]

6 刘亚丽, 孟令愚, 丁云峰. 电网工控系统流量异常检测的应用与算法改进. 计算机系统应用, 2018, 27(3): 173–178. [doi: 10.15888/j.cnki.csa.006267]

7 刘博, 李梁, 刘军娜, 等. 新能源场站电力监控系统网络安全薄弱环节分析. 电工技术, 2021, (18): 78–80. [doi: 10.19768/j.cnki.dgjs.2021.18.026]

8 金学奇, 苏达, 毛南平, 等. 面向新能源场站的主动监视与预警技术研究. 浙江电力, 2019, 38(6): 106–112. [doi: 10.19585/j.zjdl.201906018]

9 Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 2020, 169: 107094. [doi: 10.1016/j.comnet.2019.107094]

10 Yadav S, Reddy AKK, Reddy ALN, *et al*. Detecting algorithmically generated malicious domain names. Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement. Melbourne: Association for Computing Machinery, 2010. 48–61.

11 Schiavoni S, Maggi F, Cavallaro L, *et al*. Phoenix: DGA-based Botnet tracking and intelligence. Proceedings of the 11th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Egham: Springer, 2014. 192–211.

12 张维维, 龚俭, 刘茜, 等. 基于词素特征的轻量级域名检测算法. 软件学报, 2016, 27(9): 2348–2364. [doi: 10.13328/j.cnki.jos.004913]

13 Truong DT, Cheng G. Detecting domain-flux Botnet based on DNS traffic features in managed network. Security and Communication Networks, 2016, 9(14): 2338–2347. [doi: 10.1002/sec.1495]

14 郭向民, 梁广俊, 夏玲玲. 基于 HMM 的 Domain-Flux 恶意域名检测及分析. 信息网络安全, 2021, 21(12): 1–8. [doi: 10.3969/j.issn.1671-1122.2021.12.001]

15 张洋, 柳厅文, 沙泓州, 等. 基于多元属性特征的恶意域名检测. 计算机应用, 2016, 36(4): 941–944, 984. [doi: 10.11772/j.issn.1001-9081.2016.04.0941]

16 于光喜, 张棪, 崔华俊, 等. 基于机器学习的僵尸网络 DGA 域名检测系统设计与实现. 信息安全学报, 2020, 5(3): 35–47. [doi: 10.19363/J.cnki.cn10-1380/tn.2020.05.04]

17 刘洋, 赵科军, 葛连升, 等. 一种基于深度学习的快速 DGA 域名分类算法. 山东大学学报 (理学版), 2019, 54(7): 106–112.

18 Woodbridge J, Anderson HS, Ahuja A, *et al*. Predicting domain generation algorithms with long short-term memory networks. arXiv:1611.00791, 2016.

19 吴警. 基于深度学习的恶意域名检测技术研究 [硕士学位论文]. 北京: 中国人民公安大学, 2021. [doi: 10.27634/d.cnki.gzrgu.2021.000156]

20 陈立国, 张跃冬, 耿光刚, 等. 基于 GRU 型循环神经网络的随机域名检测. 计算机系统应用, 2018, 27(8): 198–202. [doi: 10.15888/j.cnki.csa.006466]

21 陈立皇, 程华, 房一泉. 基于注意力机制的 DGA 域名检测算法. 华东理工大学学报 (自然科学版), 2019, 45(3): 478–485. [doi: 10.14135/j.cnki.1006-3080.20180326002]

22 张斌, 廖仁杰. 基于 CNN 与 LSTM 相结合的恶意域名检测模型. 电子与信息学报, 2021, 43(10): 2944–2951. [doi: 10.11999/JEIT200679]

23 Sabour S, Frosst N, Hinton GE. Dynamic routing between capsules. Proceedings of the 31st International Conference on Neural Information Processing Systems. Long Beach: Curran Associates Inc., 2017. 3859–3869.

24 于政. 基于深度学习的文本向量化研究与应用 [博士学位论文]. 上海: 华东师范大学, 2016.

(校对责编: 孙君艳)

© 中国科学院软件研究所 http://www.c-s-a.org.cn