ISSN 1000-3428
CN 31-1289/TP
CODEN JISGEV

计算机工程

Computer Engineering

www.ecice06.com | 2021 7

■北大中文核心期刊 ■中科院CSCD核心期刊 ■中国科技核心期刊 ■RCCSE中国核心学术期刊 ■工业和信息化部精品期刊

华东计算技术研究所
上海市计算机学会 主办

计 算 机 工 程（月刊）

Jisuanji Gongcheng

第47卷　第7期　2021年7月15日

目　次

第47卷 第7期 计 算 机 工 程 2021年7月
Vol.47 No.7 Computer Engineering July 2021

·体系结构与软件技术· 文章编号：1000-3428(2021)07-0183-06 文献标志码：A 中图分类号：TP391.1

基于LSTM的S7协议模糊测试用例生成方法

姜亚光[1]，陈 曦[1,2]，李建彬[3]，闫靖晨[3]，刘曙元[4]，李坤昌[3]

（1.中国软件评测中心，北京 100044；2.北京大学 软件与微电子学院，北京 102600；
3.华北电力大学 控制与计算机工程学院，北京 100026；4.国能信控互联技术有限公司，北京 100039）

摘 要：基于传统模糊测试框架的S7协议模糊测试技术存在构造困难和代码覆盖率低的问题，对测试效率和质量产生很大影响。借助神经网络模型对数据较强的学习能力和预测能力，提出一种基于长短期记忆（LSTM）神经网络的S7协议模糊测试用例生成方法。将S7协议中的特征值字段分为可变字段和不可变字段，对可变字段进行模糊处理，对不可变字段做固定值操作，进而利用局部模糊实现对S7协议帧各字段的模糊分析，生成有效的测试用例。经过学习，模型可以提取到西门子S7协议的特征，自动产生满足协议结构的测试用例。实验对不同字段进行局部模糊，结果表明，该方法预测出的数据具备真实测试用例的特征，可生成大量对特征字段关联性较大的有效测试用例，提高代码覆盖率。

关键词：长短期记忆神经网络；S7协议；模糊测试；测试用例；字段

开放科学（资源服务）标志码（OSID）：

中文引用格式：姜亚光，陈曦，李建彬，等.基于LSTM的S7协议模糊测试用例生成方法[J].计算机工程，2021，47(7)：183-188.

英文引用格式：JIANG Y G，CHEN X，LI J B，et al.LSTM-based uzzy test case generation method for S7 protocol[J].Computer Engineering，2021，47(7)：183-188.

LSTM-based Fuzzy Test Case Generation Method for S7 Protocol

JIANG Yaguang[1]，CHEN Xi[1,2]，LI Jianbin[3]，YAN Jingchen[3]，LIU Shuyuan[4]，LI Kunchang[3]

（1. China Software Testing Center，Beijing 100044，China；2. School of Software and Microelectronics，Peking University，Beijing 102600，China；3. School of Control and Computer Engineering，North China Electric Power University，Beijing 100026，China；4. China Energy Information & Control Co.，Ltd.，Beijing 100039，China）

【Abstract】The fuzzy test technology for S7 protocol based on the traditional fuzzy test framework is limited by the difficulty in construction and low code coverage，which has a great impact on the test efficiency and quality.Exploiting the strong learning and prediction ability of the neural network model，a Long Short-Term Memory（LSTM）neural network-based method of generating fuzzy test cases for S7 protocol is proposed.The feature value fields in the S7 protocol are categorized into the mutable fields and the immutable fields.The mutable fields are blurred，and the immutable fields are specified with fixed values.And then local fuzzy is used to perform fuzzy analysis on each field of the S7 protocol frame to generate effective test cases.The learned model can extract the features of the Siemens S7 protocol and automatically generate test cases conforming to the protocol structure.Local fuzzy is performed on different fields for experiments，and the results show that the generated data has the features of real test cases.The method can provide a large number of effective test cases with strong correlation with the feature fields，improving the code coverage.

【Key words】Long Short-Term Memory（LSTM）neural network；S7 protocol；fuzzy test；test case；field

DOI：10.19678/j.issn.1000-3428.0058857

0 概述

随着互联网设备的全面普及，面向工业控制（工控）系统的网络威胁日益增多，并且呈高强度和批量化的态势[1-2]，因此，人们开始关注保护关键基础设施和制造工厂的重要性。互连和互操作性的发展扩大了工控系统的脆弱性，特别是在广泛应用和传播的背景下，数据被暴露给外部网络，在通过发动各种

基金项目：北京市科委计划项目（Z181100005118016）；国家电网公司工作部科技项目（5700-201914241A-0-0-00）。

作者简介：姜亚光（1985—），女，工程师、硕士研究生，主研方向为工业控制系统质量与安全测评；陈 曦，工程师、硕士研究生；李建彬（通信作者），教授；闫靖晨，博士；刘曙元，高级工程师；李坤昌，硕士。

收稿日期：2020-07-07 **修回日期：**2020-08-16 **E-mail：**lijb87@ncepu.edu.com

攻击获取系统数据后,入侵者的行为可能会对现有的工业过程造成严重损害[3]。2010年6月,一种复杂的网络武器——震网(Stuxnet)病毒肆虐全球[4],与传统网络病毒不同的是,震网病毒的攻击对象是国家重要基础设施,其本质是一种直接破坏现实世界中工业基础设施的恶意攻击代码。据赛门铁克公司统计,全球约有4.5万个网络被该病毒感染。目前,主流的工业控制系统有DCS、SCADA、PLC、远程终端设备等[5-6]。为实现系统中不同级设备间的数据通信,各类通信协议被不断革新,其中由Siemens公司基于ISO协议设计实现的S7通信协议在工业领域具有极其广泛的应用[7-9]。因此,S7协议的安全性测试成为研究热点[10]。

目前,研究者针对工控系统的安全防护已经开展了一些研究工作。文献[11]通过分析S7协议的内容与帧格式,使客户能够自己编写程序并用自己的socket程序通过以太网读写西门子S200 PLC区数据。文献[12]介绍网络协议的识别方法和测试用例生成技术,根据启发式搜索算法和概率权重,提出一种基于参数权重的启发式模糊测试框架。文献[13]使用基于规则的状态机和有状态规则树来指导模糊测试数据的生成,提高了有状态网络协议模糊化的效率和覆盖率,同时提高了测试效率。总体而言,针对工控网络协议漏洞挖掘的研究仍处于探索阶段。

目前,模糊测试是最常用的软件漏洞挖掘方法,基于模糊测试的漏洞挖掘技术[14-16]可面向部分公有协议进行高效的漏洞挖掘,但由于该类技术针对性不强且内容覆盖率低,因此在私有协议领域尚未得到较好应用。考虑到知识获取难度大、描述建模成本高等因素的影响,研究者多采用专家分析方法人工编写测试脚本,此方式不仅费时费力,而且对研究人员专业能力要求较高,生成的测试用例通过率也无法得到有效保证。由此可见,传统的模糊测试方法已不能满足工控系统的安全性要求。

神经网络模型[17-19]善于从海量数据中挖掘规则和知识,因此,将神经网络技术与工业通信安全防护工作相结合,是保障工控系统安全的一种重要举措[20-21]。本文利用长短期记忆(Long Short-Term Memory,LSTM)[22]神经网络模型强大的数据学习能力和预测能力,提出一种基于LSTM的测试用例生成方法,通过不断学习提取西门子S7协议的特征,自动产生满足协议结构的测试用例。

1 S7协议与模糊测试

1.1 S7协议

1.1.1 S7协议结构

西门子S7协议的TCP/IP实现依赖于面向块的ISO传输服务,协议结构如图1所示。S7协议不仅允许协议数据单元(Protocol Data Unit,PDU)由TCP承载,而且协议还包含在TPKT和ISO-COTP协议中。ISO通过TCP通信在RFC1006中定义,ISO-COTP在基于ISO 8073协议(RFC905)的RFC2126中定义。ST协议结构如图1所示。

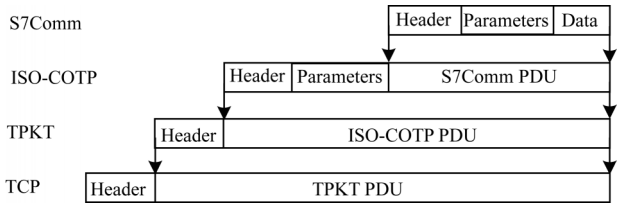

图1 S7协议结构

Fig.1 Structure of S7 protocol

1.1.2 S7协议漏洞

当工控协议栈的程序中有漏洞时,其相应报文中的数据与协议中的规约会出现不同,这会引起上位机获取异常数据,进而导致组态界面与实际运行状态存在差异,使得现场工作人员无法正常工作。在工控系统行业漏洞库平台检索S7协议,截止至2019年11月15日检索到相关漏洞77条,其中仅2019年就有5个漏洞。因此,对于模糊测试,本文提出通过学习得到S7协议报文作为测试数据,用于发现协议中不符合协议规约的情况。

1.2 模糊测试

模糊测试可以将非预期的输入传送到目标系统,同时监视该系统的异常情况进而发现软件的漏洞[23-24]。为提高测试用例的代码覆盖度,在进行模糊时需要考虑输入向量的特征,例如协议测试时需要通过网络协议解析获得协议特征,根据已获得的协议特征进一步生成测试用例。此外,在实时监控传输测试用例进行模糊测试的过程中,根据被测对象的状态可以及时检测出异常情况。模糊测试流程如图2所示。依据不同的产生模式,网络协议模糊测试方法主要有基于变异的方法和基于生成的方法[25]2种。

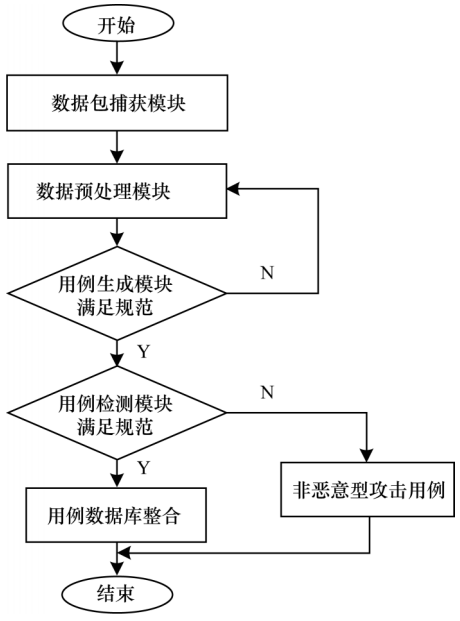

图2 模糊测试流程

Fig.2 Procedure of fuzzy test

1.2.1　基于生成的模糊测试方法

基于生成的模糊测试方法需要根据已知网络协议的协议特征和测试用例生成策略，从而建立网络协议数据模型，并根据协议模型构造测试用例生成器，生成畸形的网络报文作为测试用例发送给被测对象。这种方法可以保证较高的测试用例接收率，但用例的异常程度不高，非法数据的覆盖程度相对较低，导致生成的用例在测试时效率低下，因此，为达到预计的测试效果，需要花费更多的时间和更多的用例数据进行测试。此外，这种基于生成的模糊测试方法一般需要根据协议特征来构建测试用例生成器，而满足这方面的需求不仅要做大量的网络协议相关的调研，而且还要求开发人员对关于网络协议的专业知识有相当的储备。

1.2.2　基于变异的模糊测试方法

基于变异的模糊测试方法首先捕获网络中正常通信的网络报文，然后依据制定的模糊策略将报文中的某些字段更改为非法的字段，在生成变异的测试用例后，再对被测对象进行模糊测试。该测试方法不要求提前对被测的网络协议进行深入了解学习，只需要针对特定的网络通信，截取通信过程中的数据包，根据指定的模糊策略对数据包进行模糊修改。这种测试方法能够给研究人员带来极大的便利。测试用例经过变异策略更改数据值之后都包含了一些不合法数据值，因此，该方法的不合法数据覆盖率较高，但是测试对象协议栈程序可能会拒绝接受包含不合法数据值的测试用例，最终导致基于变异的模糊测试方法生成的测试用例被接受的数量较少，降低了模糊测试的效率。

2　基于LSTM的S7协议模糊测试方法

2.1　LSTM模型

LSTM内部状态主要通过3个不同作用的控制开关进行改变和更新，LSTM模型结构如图3所示，其中一个开关的作用是保存长期状态c，另一个负责对即时状态向长期状态c的传递，最后一个开关用于把控当前时刻的输出受长期状态c的影响程度。门是神经网络中的一层全连接层，输入向量经过门之后输出0到1之间的实数向量，3个开关都与门有关，分别对应遗忘门、输入门和输出门。以下公式表示了LSTM的前向计算过程，通过加法和乘法运算修改信息用以更新当前状态。

若W表示权重，b表示偏置，$\delta(x)$表示激活函数，则门函数表示为：

$$G(x)=\delta(Wx+b) \tag{1}$$

f_t表示若遗忘门函数，W_f表示遗忘门函数侧权重，h_{t-1}表示上一时刻LSTM的输出值，b_f表示遗忘门侧偏置，则遗忘门函数表示为：

$$f_t=\delta(W_f\cdot[h_{t-1},x_t]+b_f) \tag{2}$$

若W_c表示单元状态的权重，x_t表示t时刻的输入，b_c表示单元状态的偏置值，则候选向量表示为：

$$c'_t=\tanh(W_c\cdot[h_{t-1},x_t]+b_c \tag{3}$$

若c_t表示更新状态，i_t表示输入门的向量值，c_{t-1}表示上一时刻的状态，则更新状态为：

$$c_t=f_t\times c_{t-1}+i_t\times c_t \tag{4}$$

Sigmoid门函数表示为：

$$o_t=\delta(W_o\cdot[h_{t-1},x_t]+b_o) \tag{5}$$

若h_t表示当前输出值，则：

$$h_t=o_t\times\tanh(c_t) \tag{6}$$

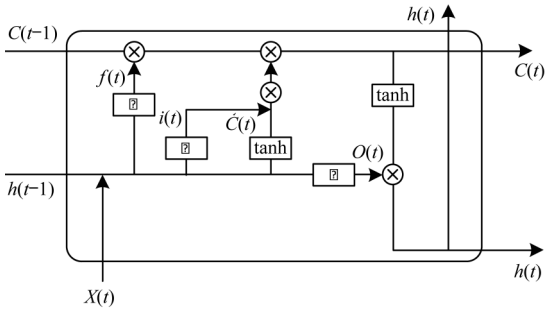

图3　LSTM模型结构

Fig.3　Structure of LSTM model

2.2　模型构建

2.2.1　数据采集

本文在S7模拟器传输过程中使用Wireshark收集实验数据。S7模拟器模拟测试基本情况如下：

一台装有WIN10操作系统的笔记本，在该笔记本中安装S7模拟器，以及虚拟环境下的WIN10操作系统，同样安装S7模拟器，打开笔记本上的S7模拟器上的Server服务器作为上位机，打开虚拟环境下的S7模拟器中的Client客户端作为下位机，例如PLC，然后在下位机上执行相应的控制操作，在笔记本上打开Wireshark来实时抓取模拟器通信协议包，获取实验数据集。

模拟环境配置如下：1）WIN10（本机）S7模拟器Server，IP地址为192.168.0.100；2）虚拟环境下的WIN10 S7模拟器客户端，IP地址为0.0.0.0；3）Wireshark_3.0.6，将IP地址192.168.0.100作为上位机，将IP地址0.0.0.0作为下位机。

2.2.2　数据预处理

上述帧需要经过有效的预处理之后才能构造数据集，预处理过程主要包含3步，分别是分析帧数据格式、数据进制转换和数据归一化处理。

1)分析帧数据的格式。使用网络抓包工具Wireshark分析可知,S7协议的数据帧是十六进制的字符串数据。

2)数据进制转换。笔者通过分析发现,十六进制的字母无法直接用于模糊测试用例的生成,即无法用作测试用例生成模型的输入,因此,将数据由十六进制转换为十进制数字来表示。此处主要考虑将一维十六进制转换为一维十进制。转换公式为$H(\text{data})\rightarrow D(\text{data})$。

3)数据归一化。数据归一化过程包括去除数据中的无效数据、空缺数据和不完整数据的处理,将所得数据归一化。去冗操作主要是去除数据集databegin中的空值,归一化处理主要是将数据归一化到0.0~0.5之间。

2.2.3 构建方法

为实现对S7协议的模糊测试,本文使用LSTM神经网络对S7协议数据进行预测。该模型主要包括数据预处理模块、测试用例生成模型搭建模块和测试用例检测模块。

1)数据预处理模块主要包括数据格式分析、数据进制转换和数据归一化处理。程序实现时的伪代码如下:

```
//数据预处理模块
Begin
def dataprocess(databegin):
去除数据集databegin中的空值
数据归一化到0.0~0.5之间
将数据分成训练集和测试集
预测部分每条两位数据,标签为一位数据
End
```

2)测试用例生成模型搭建模块主要包括LSTM数据输入、前向计算和训练输出。在实现设计程序时,利用局部模糊来对S7协议帧各字段进行模糊分析,其伪代码如下:

```
//测试用例生成模型搭建模块
Begin
class lstm_reg(nn.Module):
definit__(self, input_size, hidden_size, output_size=1,
num_layers=2):
调用父类(超类)的初始化方法
搭建LSTM网络
用Linear函数继承nn.Module
def forward(self,x): //定义model类的forward函数
得到矩阵从外到里的维数
转换size大小使输出变为(s×b)×h的二维
卷积的输出从外到里的维数为s,b,一列
return x
End
```

3)测试用例检测模块主要包括检测将特征值字段修改为边界值、字段置为空、变更字段长度引起溢出。程序实现时的伪代码如下:

```
//测试用例检测模块
Begin
if特征值字段={边界值}
test(测试用例)
if特征值字段 == Null
test(测试用例)
if特征值字段.length() > Maxlength
溢出无效
End
```

通过上述3个模块的实现,可以完成数据预处理且归一化,用处理过后的数据作为模型输入能够生成测试用例并检测出测试用例是否有效。

3 实验验证

实验的模型主要采用LSTM来对S7协议样本数据进行训练,进而生成更多的有效测试用例。在实验中,S7协议中的特征值字段分为可变字段和不可变字段,对可变字段进行模糊,对不可变字段做固定值操作,进而局部模糊生成测试用例。

3.1 数据采集和预处理

本文根据S7模拟器模拟实际上位机和下位机的通信过程,获取到138 481条数据帧,这些数据帧类型很多,也存在重复问题。因此,对获取的样本集合进行分类、整合、去重,得到99 289个有效的数据帧样本。在此基础上,对这些数据帧做进制转换处理,对转换后的十进制数据做归一化处理,得到0.0~0.5之间的数作为模型的输入,形成23.03 MB大小的训练数据集。

3.2 模型参数训练和硬件配置

LSTM模型按Batch-size为31和61形成2组参数,其他设置为序列长度为2、1层、4个隐藏节点、0.01学习率和100轮次训练。

硬件配置为Intel® Core i7-8750 CPU,8 GB内存的服务器。训练时间约为40 h。

3.3 测试用例集的生成

测试所用数据包括数据生成和数据帧组装两部分。通过LSTM模型生成99 289个模糊测试数据,然后和物理层到传输层的数据组装在一起,形成完整的测试数据帧。

3.4 测试用例执行

为保证生成数据有效,使用脚本语言Python编写测试用例的执行脚本。本地服务端存放组装后的S7协议数据帧,虚拟机模拟下位机,与上位机通信获取组装后的S7协议数据帧。首先启动snap7服务器端,启动服务,然后把生成的测试用例放入脚本中,再运行脚本程序,即可将测试用例发送到服务器上,如图4所示。

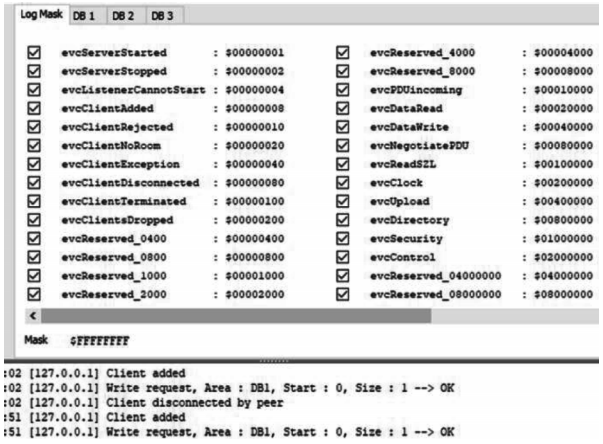

图4　测试用例发送至服务器的界面

Fig.4　Interface of sending test cases to server

判定1条测试用例是否有效,其原理是检测测试用例对应的协议控制操作是否会导致故障的发现,若发生故障,则测试用例有效,反之则无效。如图5所示,1条有效的测试用例主要包括9个特征值,分别为Type、Version、Header Length等字段。实验考虑空指针、溢出和数值边界这3种异常情况。

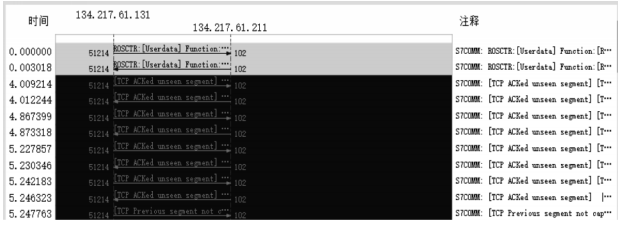

图5　判定1条测试用例是否有效的界面

Fig.5　Interface of judging validity of a test case

3.5　实验结果分析

本文所采用的算法为LSTM算法,利用局部模糊来对S7协议帧各字段进行模糊分析。由实验结果可知,模型生成的数据机构和训练集合中的数据帧很相似,可见循环神经网络模型对S7协议结构学习有较好的结果。图6为部分生成的测试数据结果。图中显示,LSTM模型预测出的数据已经具备真实测试用例的特征,可根据特征进行测试用例的预测。与Peach对特征字段关联性很小的方法相比,本文模型对特征字段关联性较大。实验结果显示本文方法所生成的测试用例代码覆盖度较高,验证了其有效性。

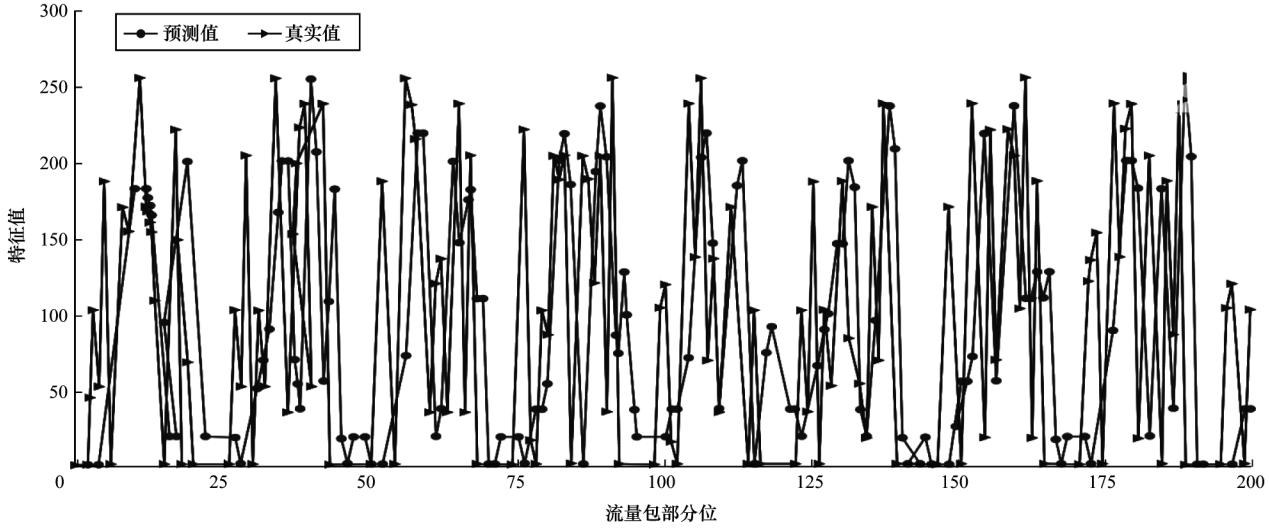

图6　部分测试数据预测结果

Fig.6　Partial prediction results of test data

4　结束语

本文提出一种基于神经网络的S7协议模糊测试用例生成方法。通过LSTM神经网络模型学习S7协议样本,得到协议的结构特征,预测生成符合结构特征的测试用例。仿真实验对不同字段进行局部模糊,结果表明,该模型生成了大量有效的测试用例,预测出的数据具备真实测试用例的特征,测试用例的代码覆盖度较高,从而验证了本文方法的有效性。然而本文所构建的模型数据来源类型单一,神经网络本身所带有的随机性导致用例生成时某些固定字段存在误差,并且脆弱性字段比较固定,而在实际应用中工控网络面临复杂的安全问题。因此,下一步将研究数据来源不同和字段值发生改变时如何生成更有效的测试用例,并进行对比实验。

参考文献

[1] 彭勇,江常青,谢丰,等. 工业控制系统信息安全研究进展[J]. 清华大学学报(自然科学版),2012,52(10):1396-1408.
PENG Y,JIANG C Q,XIE F,et al. Research progress on information security of industrial control systems[J]. Journal of Tsinghua University(Natural Science Edition),2012,52(10):1396-1408. (in Chinese)

[2] 张环宇,陈凯. 基于零动态的工控系统攻击检测识别安全模型[J]. 计算机工程,2017,43(10):98-103.
ZHANG H Y,CHEN K. Industrial control system security model of attack detection and identification based on zero dynamics[J]. Computer Engineering,2017,43(10):98-103. (in Chinese)
[3] 杨国泰. 工业控制系统安全网络防护分析[J]. 电子世界,2019(16):70-71.
YANG G T. Analysis of security network protection of industrial control system[J]. Electronic World,2019(16):70-71. (in Chinese)
[4] 蒲石,陈周国,祝世雄. 震网病毒分析与防范[J]. 信息网络安全,2012(2):40-43.
PU S,CHEN Z G,ZHU S X. Analysis and prevention of Stuxnet virus[J]. Information Network Security,2012(2):40-43. (in Chinese)
[5] 邹颀伟. 基于Fuzzing测试的工控网络协议漏洞挖掘技术研究[D]. 西安:西安电子科技大学,2018.
ZOU Q W. Research on mining technology of industrial control network protocol vulnerabilities based on Fuzzing test[D]. Xi'an:Xidian University,2018. (in Chinese)
[6] 阮伟,黄光平,陈亮,等. 工业控制系统私有协议深度解析方法[J]. 电子技术与软件工程,2019(22):3-4.
RUAN W,HUANG G P,CHEN L,et al. In-depth analysis method of industrial control system private protocol[J]. Electronic Technology and Software Engineering,2019(22):3-4. (in Chinese)
[7] 马小荣,贺琴,马晟. 西门子工业控制的PLC应用及关键技术分析[J]. 中国新通信,2019,21(19):119.
MA X R,HE Q,MA S. PLC application and key technology analysis of Siemens industrial control[J]. China New Communications,2019,21(19):119. (in Chinese)
[8] 常焘. 关于西门子PLC控制系统工作原理及常见故障应用分析[J]. 山东工业技术,2018(20):155.
CHANG T. About the working principle of Siemens PLC control system and application analysis of common faults[J]. Shandong Industrial Technology,2018(20):155. (in Chinese)
[9] 赵国华. 西门子PLC在工厂应用中的问题及对策探讨[J]. 橡塑技术与装备,2016,42(10):97-98.
ZHAO G H. Discussion on the problems and countermeasures of Siemens PLC in factory application[J]. Rubber and Plastics Technology and Equipment,2016,42(10):97-98. (in Chinese)
[10] 李文轩. 工控系统网络协议安全测试方法研究综述[J]. 单片机与嵌入式系统应用,2019,19(9):18-21.
LI W X. Summary of research on security test methods of industrial control system network protocol[J]. Single Chip Microcomputer and Embedded System Applications,2019,19(9):18-21. (in Chinese)
[11] 贾涛. 西门子S7-200以太网通讯协议研究[J]. 电子技术与软件工程,2014(24):30-32.
JIA T. Research on Siemens S7-200 Ethernet communication protocol[J]. Electronic Technology and Software Engineering,2014(24):30-32. (in Chinese)
[12] LI M X,HE L,TENG Y X,et al. Research on network protocol vulnerability discovery based on fuzz testing[C]// Proceedings of 2017 IEEE Information Technology,Networking,Electronic and Automation Control Conference. Washington D. C.,USA:IEEE Press,2017:1354-1358.
[13] MA R,WANG D G,HU C Z,et al. Test data generation for stateful network protocol fuzzing using a rule-based state machine[J]. Tsinghua Science and Technology,2016,21(3):352-360.
[14] KIM S J,SHON T. Field classification-based novel fuzzing case generation for ICS protocols [J]. Journal of Supercomputing,2018,74(9):4434-4450.
[15] ZHOU B H,LI Q,SUN B W,et al. An improved fuzzy test of industrial control system[C]//Proceedings of the 10th International Conference on Computer and Automation Engineering. New York,USA:ACM Press,2018:233-237.
[16] MOUSAVI S M,TAVANA M,ALIKAR N,et al. A tuned hybrid intelligent fruit fly optimization algorithm for fuzzy rule generation and classification[J]. Neural Computing and Applications,2019,31(3):1-4.
[17] 张成彬,赵慧,曹宗钰. 基于深度学习的车身网络KWP2000协议漏洞挖掘[J]. 山东大学学报(工学版),2019,49(2):17-22.
ZHANG C B,ZHAO H,CAO Z Y. The vulnerability mining method for KWP2000 protocol based on deep learning and fuzzing[J]. Journal of Shandong University (Engineering Science),2019,49 (2):17-22. (in Chinese)
[18] LI Z H,ZHAO H,SHI J Q,et al. An intelligent fuzzing data generation method based on deep adversarial learning[J]. IEEE Access,2019,7:49327-49340.
[19] 吕佩吾,葛雅川,李楠,等. 基于卷积神经网络的工控协议Modbus TCP异常检测[J]. 信息安全研究,2019,5(7):635-638.
LÜ P W,GE Y C,LI N,et al. Anomaly detection of industrial control protocol Modbus TCP based on convolutional neural network [J]. Information Security Research,2019,5(7):635-638.
[20] DONG G F,SUN P,SHI W B,et al. A novel valuation pruning optimization fuzzing test model based on mutation tree for industrial control systems [J]. Applied Soft Computing,2018,70:896-902.
[21] 申莹珠. 基于模型学习的安全协议脆弱性分析关键技术研究[D]. 郑州:战略支援部队信息工程大学,2018.
SHEN Y Z. Research on key technologies for vulnerability analysis of security protocols based on model learning[D]. Zhengzhou:Strategic Support Force Information Engineering University,2018. (in Chinese)
[22] 钱忠,李培峰,周国栋,等. 基于双向LSTM网络的不确定和否定作用范围识别[J]. 软件学报,2018,29(8):2427-2447.
QIAN Z,LI P F,ZHOU G D,et al. Recognition of uncertain and negative scope based on two-way LSTM network[J]. Journal of Software,2018,29(8):2427-2447. (in Chinese)
[23] GAO J L,ZHANG H P,LU P,et al. An effective LSTM recurrent network to detect arrhythmia on imbalanced ECG dataset[J]. Journal of Healthcare Engineering,2019,2019:1-10.
[24] MA R,REN S M,MA K,et al. Semi-valid fuzz testing case generation for stateful network protocol [J]. Tsinghua Science and Technology,2017,22(5):458-468.
[25] 梁卓杰. 测试用例自动生成算法设计及自动化测试平台构建[D]. 北京:北京交通大学,2019.
LIANG Z J. Design of automatic test case generation algorithm and construction of automatic test platform[D]. Beijing:Beijing Jiaotong University,2019. (in Chinese)

编辑 金胡考