DOI:10.19651/j.cnki.emt.1802240

一种 Modbus TCP 模糊测试中畸形数据过滤方法*

任蒲军 付敬奇
(上海大学 机电工程与自动化学院 上海 200444)

摘 要：工业网络控制系统安全问题受到广泛重视,本文针对 Modbus TCP 协议模糊测试过程中,由于缓冲区设置难以与实际情况吻合进而导致经常出现的溢出漏洞,提出了一种改进的应用数据单元(IADU)格式,避免了报文长度变化导致的长度信息丢失,并采用主成分分析(PCA)方法处理数据相关性导致重复信息大量出现问题,降低了维数爆炸的风险。进一步采用概率神经网络(PNN)对待输入畸形数据引发漏洞可能性进行匹配和判断,从而提高模糊测试的效率。实验分析结果表明,本文方法能减少 8.6%的畸形数据输入量。

关键词：Modbus TCP;模糊测试;概率神经网络;主成分分析
中图分类号：TN918.91 **文献标识码**：A **国家标准学科分类代码**：510.5099

A malformed data filtering method in Modbus TCP fuzzing test

Ren Pujun Fu Jingqi
(School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China)

Abstract: The security of network control system has captured worldwide attention. For the frequent overflow caused by the disparity between buffer setting and practical requirement in the Modbus TCP protocol fuzzing test, a new data structure of improved application data unit capable to preventing the message length information from being lost is presented in this paper. Then principal component analysis (PCA) is used to reduce the dimensionality explosion risk aroused by the massive identical information which comes from the data relativity. At last, a probabilistic neural network (PNN) is deployed to estimate the vulnerabilities detecting possibility of the malformed data to be input, which makes the fuzzing test more efficient. The analysis and comparison to the experiment result denote that the input data is reduced by 8.60% via using the method presented in this paper.

Keywords: Modbus TCP; fuzzing test; probabilistic neural network (PNN); principal component analysis (PCA)

0 引 言

随着信息技术的快速发展,网络控制系统已成为自动控制系统的主导结构形式,并在油气、冶金、化工、电力等诸多行业得到广泛运用。但工业控制协议因自身存在的漏洞产生了一系列安全问题,例如,2010 年,伊朗的布什尔核电站受到“震网”病毒[1]的攻击,至少有 1/5 的离心机因此被关闭;2014 年,欧美地区的一千多家能源企业受到了“Havex”病毒[2]攻击等。上述攻击大都利用了工业控制系统中存在的漏洞,因此及时发现工业控制网络协议中存在的漏洞对工业网络控制安全具有重要的意义。

模糊测试[3]是指向待测目标输入畸形的测试数据来发现目标中存在的非法错误,常用于检测网络协议和存在输入合法性检验的程序的健壮性,模糊测试已经成为漏洞挖掘中行之有效的方法之一。由于工业控制网络设备通信能力在负载承受上与商业 IT 中的通信设备有较大差距[4],难以对工控设备进行高速率模糊测试,从而导致测试过程变慢、测试效率降低。因此,如何在畸形输入测试数据速率受限的条件下,对输入畸形数据队列中发现漏洞可能性较小的数据进行有效过滤,而保留漏洞可能性较大的数据,以提高模糊测试的效率。

Modbus 协议是 Modicon 公司 1979 年提出的一种工业控制协议,具有协议标准开放、支持范围广和实时性好等特点[5],Modbus 在工业控制系统中应用十分广泛[6]。Modbus TCP 协议是运行在 TCP/IP 协议上的 Modbus 协议,Modbus 协议数据单元作为传输层负载进行传播[7],因此 Modbus TCP 协议也继承了 TCP/IP 协议的漏洞;此外,Modbus 协议本身存在如明文传输、缺乏认证机制等问

收稿日期:2018-11-01
* 基金项目:上海市科委项目(17511107002)资助

题，以及实现过程中程序存在的不足也会产生一系列安全漏洞。针对 TCP/IP 协议的漏洞挖掘，文献[8]提出了一种改进的 Fuzzing 架构，将发现漏洞的置信度作为分类器的输入，预先筛选出可能有效的测试用例，从而达到减少输入和提高命中率的目的。文献[9]针对协议的特殊性，提出了一种自适应算法，能根据待测目标的状态反馈生成测试用例，有效地提高了测试效率，增加了测试用例的覆盖能力。文献[10]提出了将测试用例变异因子和协议特征结合生成测试用例的方法，根据协议特征和旁路监听相结合确定测试用例是否有效，实现了协议漏洞的有效检测。

本文针对 Modbus TCP 协议模糊测试过程中，由于缓冲区设置难以与实际情况吻合进而导致经常出现的溢出漏洞，首先，提出了一种改进的应用数据单元（improvecl application data unit，IADU）格式，通过对原有的 Modbus TCP 报文的应用数据单元（application data unit，ADU）中添加一个新的字段来构造 IADU，其字段值为长度字段后所有字段的总字节数，防止了后续处理中报文长度发生变化导致长度信息的丢失，确保了训练数据的原始长度信息不丢失并用于判定机制的构建；其次，针对 Modbus TCP 协议中不同位置数据之间的相关性导致重复信息大量出现的情况，采用主成分分析（principal compinent analysis，PCA）方法减少维数爆炸的风险，降低计算量；最后，构造了基于 IADU 和 PCA 的概率神经网络（probabilstic neural network，PNN）模型，通过计算被判断畸形数据与训练数据中产生各种通信结果的 Modus TCP 报文的匹配程度，实现对待输入畸形数据能引发漏洞可能性进行判断，从而提高模糊测试的效率。针对某公司生产的 Modbus TCP 协议产品仿真实验和对比分析结果表明，本文方法能减少 8.6%的畸形数据输入量。

1　改进的 IADU 实现方法

1.1　ADU 单元存在的问题

缓冲区漏洞是一类重要的安全漏洞，是 C 程序中众多安全问题的根源之一。当写入数据长度大于缓冲区长度时，则会发生缓冲区溢出[G]，进而引发缓冲区漏洞。当漏洞是由于缓冲区溢出引起时，则发现该漏洞的 Modbus 报文中包含了引起待测设备缓冲区漏洞的条件，其中 Modbus TCP 报文长度不但直接反映了写入数据的长度，而且与产生漏洞的条件密切相关，因此 Modbus TCP 报文长度是反映该类型漏洞是否存在的重要信息。Modbus TCP 应用数据单元（ADU）如图 1 所示。

事物处理标识符TID	协议标识符PID	长度 *LEN*	单元标识符UID	功能码FCODE	数据DATA
2 Bytes	2 Bytes	2 Bytes	1 Byte	1 Byte	*n* Bytes

图 1　Modbus TCP 应用数据单元格式

由图 1 可知，ADU 作为一个整体位于 TCP/IP 报文的帧负载中。其中正常的 Modbus 报文中满足 $LEN=n+2$，因此 *LEN* 可以表示 ADU 的长度信息。而训练样本中的数据中主要为已有的畸形数据，它往往无法满足 $LEN=n+2$，因此此时 LEN 字段无法准确表示 ADU 长度信息，从而导致反映存在漏洞信息中的长度信息的丢失，因此，如何在测试中将畸形数据的长度信息有效准确表达是进一步处理需要解决的重要问题。

1.2　IADU 的实现

改进的应用数据单元格式的构造方法为在原有的 ADU 格式基础上，插入一个新的字段$\overline{\text{LEN}}$，其值为从 LEN 字段开始所有字段的总字节数，得到 IADU。IADU 格式如图 2 所示。

事物处理标识符TID	协议标识符PID	$\overline{\text{LEN}}$	长度 *LEN*	单元标识符UID	功能码FCODE	数据DATA
2 Bytes	2 Bytes	2 Bytes	2 Bytes	1 Byte	1 Byte	*n* Bytes

图 2　IADU 格式

对于每一个改进的 ADU 可以使用一个 IADU 向量 $\boldsymbol{A}$ 来表示：

$$\boldsymbol{A}=(\text{TID},\text{PID},\overline{\text{LEN}},\text{LEN},\text{UID},\text{FCODE},\text{DATA}[0],\text{DATA}[1],\cdots,\text{DATA}[\text{n}-1])^{\text{T}} \tag{1}$$

式中：$\boldsymbol{A}$ 中的各个字段所占的字节数存在差异，字段值的上限随着字节数的增加而增加。为消除特定字段值变化范围过大对判定结果带来的影响，根据 $\boldsymbol{A}$ 中各个字段能取到的最大值进行归一化处理，使各个字段变化的范围趋于一致。归一化处理的实现方法如式(2)所示。

$$\boldsymbol{A}=\left(\frac{\text{TID}}{65\ 535},\frac{\text{PID}}{65\ 535},\frac{\overline{\text{LEN}}}{\text{MSS}},\frac{\text{LEN}}{65\ 535},\frac{\text{UID}}{255},\frac{\text{FCODE}}{255},\frac{\text{DATA}[0]}{255},\frac{\text{DATA}[1]}{255},\cdots,\frac{\text{DATA}[n-1]}{255}\right)^{\text{T}} \tag{2}$$

其中 *MSS*（maximum segment size）为 TCP 3 次握手过程中双方约定的最大应用数据段最大长度，TCP/IP 协议中 *MSS* 默认取值为 536。由于 Modbus TCP 是运行与 TCP/IP 之上的 Modbus 协议，畸形数据的长度上限为 *MSS*。

显然，经过归一化处理的 IADU 向量中既保留了原有报文的长度信息，又使各个字段的变化范围趋于一致，从而保证判定机制能更加准确地判定待输入畸形数据能否引发缓冲区漏洞。

2　模糊测试过滤方法

2.1　过滤机制

模糊测试中过滤机制流程如图 3 所示。

由图 3 可知，模糊测试过滤机制主要由数据输入、畸形数据过滤和测试记录分类 3 部分组成。其中数据输入部分主要进行训练数据导入、训练数据解析，并对其进行数据单

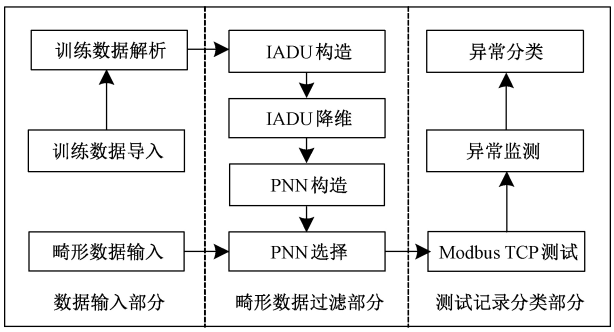

图 3 Modbus TCP 模糊测试中过滤机制流程

元格式改进,同时,将得到的畸形数据进行畸形数据过滤处理。畸形数据过滤主要实现畸形数据的选择,保留发现待测目标漏洞可能性较高的畸形数据,舍弃发现待测目标漏洞可能性较低的数据。

训练数据导入主要提供给用户导入存有训练样本数据的图形用户界面。图形用户界面设计与开发的相关技术已经比计较完善。训练样本可以包括对产品或者同类型产品进行初步测试时的抓包文件以及测试结果。通过解析导入的训练数据,获得其中的 Modbus TCP 测试报文。畸形数据输入可以使用第 3 模糊数据产生器,例如 Peach Fuzzer。对模糊数据产生器的研究与应用[11]也已有学者进行了大量工作;抓包文件解析可以使用 python3 的 scapy 模块简化实现过程;Modbus 数据具体的发送使用的 Socket 编程技术也很成熟。

畸形数据过滤部分主要进行 IADU 构造、IADU 降维、PNN 构造和 PNN 选择。通过在训练数据解析后得到的 Modbus TCP 原报文数据的基础上添加一个新的字段,其值为原长度字段 LEN 后所有字段的总字节数,防止在后续处理中数据处理中原有的长度信息丢失。对由多个 IADU 构成的矩阵,针对 Modbus TCP 协议中不同位置数据之间的相关性导致重复信息大量出现的情况,采用 PCA 方法进行降维,从而过滤携带重复信息的字段,减少维数爆炸的风险。基于降维处理得到的训练数据构造 PNN,实现对待输入的畸形数据的判断,保留发现设备漏洞可能性较高的畸形数据。

测试记录分类部分主要将经过 PNN 判定保留的畸形数据输入待测设备,并对监测设备的工作状态是否因为畸形数据的输入而产生异常。异常信息将根据其产生的原因被分类,最终与引发异常的相应畸形数据一起存储。

2.2 IADU 降维处理

Modbus TCP 报文中不同字段代表着被控对象的各个物理量的值。各个物理量之间相关性导致了对应字段携带重复的引发漏洞信息,进而作为训练数据的 IADU 向量也包含重复信息。重复信息会给判定机制的训练和工作增加计算复杂度[12],进而影响判定的实时性。通过对多个 IADU 向量进行降维处理来减少 IADU 向量中携带重复信息的字段,从而减少训练和判定过程中的计算量,保证判定的实时性。PCA 是一种启发式的数据处理分析方法,能够大幅度减少数据的维数并且保持数据原有的信息[13]。

训练数据中,由 i 条训练数据可构造出 i 个 IADU 向量 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_i$。将 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_i$ 组合构造一个 IADU 矩阵 $\boldsymbol{S}_i$,如式(3)所示。

$$\boldsymbol{S}_i=(\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_i)^{\mathrm{T}} \tag{3}$$

在 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_i$ 维数不尽相同的情况下为确保成功构造 IADU 矩阵 $\boldsymbol{S}_i$,当向量 $\boldsymbol{A}_k$ 的维数 $d(\boldsymbol{A}_k)<\max(d(\boldsymbol{A}_m))(1\leqslant m\leqslant i)$ 时,则对 $\boldsymbol{A}_k$ 向量不足的维数补 0。

MSS 决定了 Modbus TCP 通信中 ADU 的最大长度,进而决定了 IADU 矩阵中最大列数 $\boldsymbol{S}_i$。*MSS* 取默认值时,$\boldsymbol{S}_i$ 列数最高可达 536。直接对 IADU 矩阵 $\boldsymbol{S}_i$ 使用 PCA 必然会导致维数爆炸。

由于 IADU 向量中反映训练数据实际长度信息在第 3 个字段就已经得到反映,因此通过保留 $\boldsymbol{S}_i$ 矩阵中前 $j(3<j<<MSS)$ 列可以在不丢失实际长度信息的前提下解决 *MSS* 带来的维数爆炸问题。

矩阵 $\boldsymbol{S}_{ij}$ 中一行数据反映的是一条 Modbus TCP 通信数据包含的信息。要过滤报文中字段与字段之间相互依赖关系以减少判定机制的计算量,则必须对 $\boldsymbol{S}_{ij}$ 行方向上的数据进行降维处理。

计算 $\boldsymbol{S}_{ij}$ 的协方差矩阵 $\boldsymbol{C}$ 如式(4)所示。

$$\boldsymbol{C}=\begin{bmatrix}\mathrm{cov}(s_1,s_1) & \mathrm{cov}(s_1,s_2) & \cdots & \mathrm{cov}(s_1,s_j)\\ \mathrm{cov}(s_2,s_1) & \mathrm{cov}(s_2,s_2) & \cdots & \mathrm{cov}(s_2,s_j)\\ \vdots & \vdots & \ddots & \vdots\\ \mathrm{cov}(s_j,s_1) & \mathrm{cov}(s_j,s_2) & \cdots & \mathrm{cov}(s_j,s_j)\end{bmatrix} \tag{4}$$

求 $\boldsymbol{C}$ 的特征值和特征向量,对特征值进行降序排序,选择前第 1 到 $m(m<<j)$ 个特征值 $\lambda_1,\lambda_2,\cdots,\lambda_m$ 对应的特征向量 $\boldsymbol{p}_1,\boldsymbol{p}_2,\cdots,\boldsymbol{p}_m$ 组成特征向量矩阵 $\boldsymbol{T}$。

$$\boldsymbol{T}=(\boldsymbol{p}_1,\boldsymbol{p}_2,\cdots,\boldsymbol{p}_m) \tag{5}$$

将 $\boldsymbol{S}_{ij}$ 投影到特征向量矩阵 $\boldsymbol{T}$ 上即可得到 PNN 构造样本的数据集 $\overline{\boldsymbol{S}}_{im}$。

$$\overline{\boldsymbol{S}}_{im}=\boldsymbol{S}_{ij}\boldsymbol{T} \tag{6}$$

$\overline{\boldsymbol{S}}_{im}$ 中的每一行都表示一个报文中最基本的 m 个单元特征。至此,原始报文的基本信息得到了保留,训练数据维数得到降低。

使用对 IADU 进行降维处理得到训练数据集的流程如图 4 所示。首先将 i 个 IADU 向量组合得到 IADU 矩阵 $\boldsymbol{S}_i$;其次提取 IADU 矩阵 $\boldsymbol{S}_i$ 的前 j 列得到 $\boldsymbol{S}_{ij}$,防止直接 PCA 造成维数爆炸;最后对 $\boldsymbol{S}_{ij}$ 进行 PCA 处理,得到训练数据集 $\overline{\boldsymbol{S}}_{im}$。

2.3 畸形数据过滤判断

通过训练数据构造的判定机制在对待输入畸形数据进行判定过程中必须有判定计算量少、速度快、判定准确的优

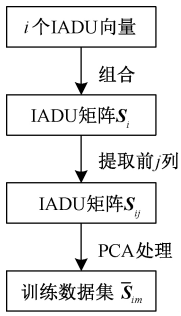

图 4　IADU 降维流程

点才能在保证实时通信的前提下减少发现待测目标漏洞可能性较低的畸形数据的输入，提高测试效率。

同时随着模糊测试的进行，不断会有新的测试数据发现已有的漏洞，甚至新的测试数据发现判别机制中未收录的漏洞。因此模糊测试过程中判定机制必须通过不断收录新的测试数据信息和漏洞信息来实现自我更新以提升自己的判定能力。为减少更新判定机制不对正常的判定带来的不利影响，判定机制必须具有训练时间短和易于自我更新的优势。

PNN 具有计算量小、训练速度快、分类准确等特点[14]。本文中使用 PNN 作为判定机制来实现对待输入畸形数据的判定。

3　PNN 的判定

对于样本中的 i 个报文可以得到训练数据集 $\overline{\boldsymbol{S}}_{im}$，记 $\overline{\boldsymbol{S}}_{im}=(\bar{s}_1,\bar{s}_2,\cdots,\bar{s}_i)^{\mathrm{T}}$。

根据是否引发测试目标异常和异常的类型，可以将样本中的报文分为 $Y-1$ 种异常类型报文和 1 种正常类型的报文，将正常报文类型记为第 1 种类型。此处将第 t 类报文包含的报文总数记为。记 r_{tw} 为 $\overline{\boldsymbol{S}}_{im}$ 中第 t 类中第 w 个报文对应的维数为 m 的由单元特征组成的行向量。

设计 PNN 如图 5 所示，从左至右分别为输入层、模式层、求和层和输出层。

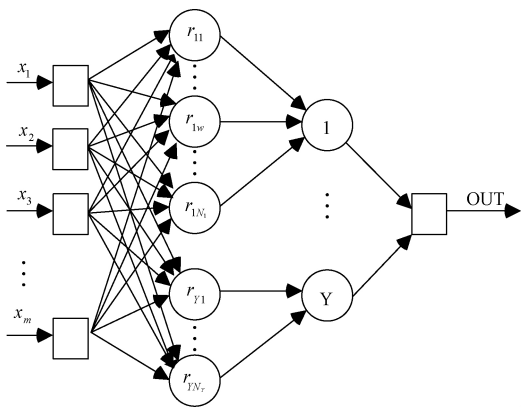

图 5　PNN 整体结构

模式层中的神经元是训练数据集 $\overline{\boldsymbol{S}}_{im}$ 中各个行向量，能计算输入向量 $\boldsymbol{X}$ 和各个训练数据的匹配程度。

求和层中各神经元表示 r_{tw} 向量所属的漏洞类别，能将模式层输出的且属于同一种漏洞类型的所有匹配程度进行求和。

输出层的输出为输入向量 $\boldsymbol{X}$ 匹配最大的漏洞类别号。

PNN 选择判定的目的是减少引发待测目标异常可能性较小的畸形数据向待测设备输入，从而提升测试效率，减少待测设备的测试负载。PNN 判定畸形数据的有效性流程如图 6 所示。

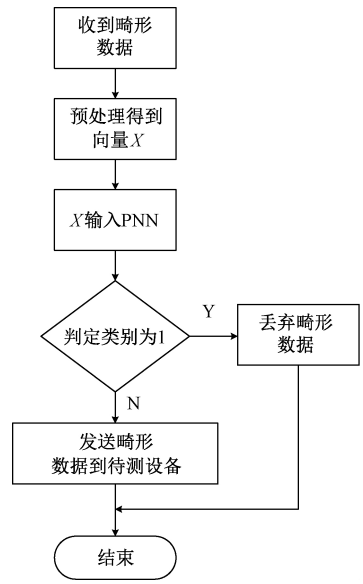

图 6　PNN 判定畸形数据的流程

PNN 判定主要是在接受到一条模糊数据后，先使用 PCA 降维，得到一个 m 维的向量 $\boldsymbol{X}$，再将 $\boldsymbol{X}$ 输入 PNN 进行判定。

PNN 中输入层和模式层之间的连接是通过一个高斯函数，求得模式层中每个神经元和输入层中每个神经元的匹配程度值，然后对每个类中各自的所有神经元匹配程度加权求平均。

输入向量 $\boldsymbol{X}=(x_1,x_2,\cdots,x_m)$ 对第 t 类的匹配程度可以表示为：

$$L_{N_t}(X,\sigma)=\frac{1}{N_t(2\pi)^{m/2}\sigma^m}\sum_{w=1}^{N_t}\exp\left(-\frac{|\boldsymbol{r}_{tw}-\boldsymbol{X}|^2}{2\sigma^2}\right) \tag{7}$$

式中：σ 为表示平滑参数，是唯一可以调整的量，可以通过调整 σ 的值来提高精确度，通常 $\sigma\in(0,1)$。

输出层输出匹配度最大的类别，若输出的类别号为 1，表示被判定的数据与无法引发漏洞的数据最相似，很有可能无法引发待测目标异常，此时丢弃该模糊数据。如果输出的类别号不为 1，则将改模糊数据发送到待测设备。

4 实验与结果分析

为验证本文研究方法的有效性,采用了某公司生产的 Modbus TCP 协议工业控制器,进行了 5 次测试。训练样本数据为该公司对此款产品进行初步测试的抓包文件。

由于使用的样本数据中 80%的报文长度超过 400 字节,构造 $\boldsymbol{S}_{ij}$ 中 j 取 40 以减少计算量。

使用 python 中的 sklearn 库对 $\boldsymbol{S}_{ij}$ 进行 PCA 分析,累积贡献率与保留的主成分分析的曲线如图 7 所示。

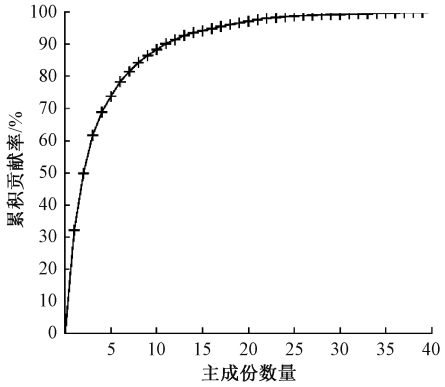

图 7 累积贡献率曲线

工程中一般选择累积贡献率达到 85%～95%[15]间的主要成分,本文中选择累积贡献率为 88.3%时对应的主成份数量 10 作为 m 的值。

测试的评价标准是引发待测目标 3 次异常所需要的实际向目标发送的数据次数,并与直接使用 Peach 对目标进行测试的传统方法进行比较。在 PNN 选择环节中平滑参数 σ 分别取 0.6、0.7 和 0.8 时,传统方法与本文方法的实验结果如表 1 所示。

表 1 数据发送次数比较

编号	传统方法/次	$\sigma=0.6$		$\sigma=0.7$		$\sigma=0.8$	
		次数	减少率/%	次数	减少率/%	次数	减少率/%
1	2 977	2 891	2.89	2 833	4.84	2 753	7.52
2	2 767	2 717	1.81	2 687	2.89	2 533	8.64
3	2 713	2 614	3.65	2 588	4.61	2 479	8.63
4	2 896	2 803	3.21	2 704	6.63	2 612	9.81
5	2 734	2 698	1.32	2 577	5.74	2 481	9.25
合计	14 087	13 723	2.58	13 389	4.95	12 876	8.60

表 1 结果表明,使用本文的方法进行模糊测试,平滑参数 $\sigma=0.8$ 时,引发目标产生 3 次异常所需要的实际测试数据最多可减少 8.6%。

5 结 论

针对 Modbus TCP 工业控制网络协议可承受负载低导致的模糊测试效率低的问题,本文通过建立 PNN 判定机制舍弃了待输入畸形数据队列中的发现待测设备漏洞可能性较低的数据,保留发现队列中发现待测设备能动可能性较高的数据,加速了整个模糊测试过程。

在构建 PNN 的过程中,通过构造 IADU 数据格式,将原长度字段后的总字节数作为一个新的字段插入原来 ADU 的前部,防止了训练数据的原始长度信息因后续处理中对训练数据的降维而丢失,确保最终用于构造 PNN 的训练数据中包含训练数据的原始长度信息。保证了最终的 PNN 判定机制能根据待判定的畸形数据的长度判定其能否引发漏洞。通过只使用训练数据中 Modbus 报文中的前部,确保在不丢失训练数据的原始长度信息的条件下,降低 PCA 的计算复杂度。通过对训练数据的 PCA 处理,滤除了携带重复信息的字段,实现对训练数据的降维,确保了不影响 PNN 准确度的同时,减少了 PNN 的复杂程度,最终减少判定时的计算量。在实验中使用本文中的数据过滤方法,引发待测目标 3 次异常所要的实际测试数据的发送量比传统模糊测试最高可减少 8.6%,验证了本文提出过滤方法的有效性。

下一步的工作是研究在测试的过程中对新的漏洞和对应的测试数据进行分类和动态学习,在测试的过程中更新判定机制,进一步降低测试数据实际发送量,提高测试效率。

参考文献

[1] FENG X, YONG P, WEI Z, et al. Security evaluation for industrial control devices[J]. Journal of Tsinghua University, 2014,54(1):29-34.

[2] TAKAGI H, MORITA T, MATTA M, et al. Strategic security protection for industrial control systems [C]. Society of Instrument and Control Engineers of Japan, IEEE, 2015:2-7.

[3] 蔡军,邹鹏,沈弼龙,等.基于改进轮盘赌策略的反馈式模糊测试方法[J].四川大学学报(工程科学版),2016,48(2):132-138.

[4] XU Y, YANG Y, LI T, et al. Review on cyber vulnerabilities of communication protocols in industrial control systems [C]. IEEE Conference on Energy Internet and Energy System Integration, 2017:1-6.

[5] 秦天柱,张伟刚,瞿少成.基于 Modbus 协议的多路数据采集器[J].电子测量技术,2017,40(11):175-178.

[6] 孙彦赞,张瀚,吴雅婷,等.基于 Modbus 协议的 OBD 设备检测控制系统设计[J].电子测量技术,2018,41(3):102-106.

[7] AL-DALKY R, ABDULJALEEL O, SALAH K, et al. A Modbus traffic generator for evaluating the security of SCADA systems [C]. International Symposium on Communication Systems, Networks &

Digital Signal Processing, IEEE, 2014:809-814.

[8] 向騄,赵波,纪祥敏,等.一种基于改进 Fuzzing 架构的工业控制设备漏洞挖掘框架[J].武汉大学学报(理学版),2013,59(5):411-415.

[9] XIONG Q, LIU H, XU Y, et al. A vulnerability detecting method for Modbus-TCP based on smart fuzzing mechanism[C]. IEEE International Conference on Electro/information Technology, 2015:404-409.

[10] 赖英旭,杨凯翔,刘静.基于模糊测试的工控网络协议漏洞挖掘方法[J].计算机集成制造系统,2018(6):1-22.

[11] 伊胜伟,张翀斌,谢丰,等.基于 Peach 的工业控制网络协议安全分析[J].清华大学学报(自然科学版),2017,57(1):50-54.

[12] 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.

[13] 马峻,赵飞乐,徐潇,等.MRA-PCA-PSO 组合优化 BP 神经网络模拟电路故障诊断研究[J].电子测量与仪器学报,2018,32(3):73-79..

[14] 叶永伟,刘志浩,黄利群.基于 PCA 的汽车涂装线设备信号特征提取[J].仪器仪表学报,2011,32(10):2363-2370.

[15] 张阔,李国勇,韩方阵.故障树法和改进 PSO-PNN 网络的电梯故障诊断模型[J].中国安全生产科学技术,2017,13(9):175-179.

作者简介

任蒲军,硕士研究生,主要研究方向为工业控制网络漏洞挖掘。

E-mail: rpjshu@163.com

付敬奇(通信作者),教授、博士生导师,主要研究方向为无线传感器网络、仪表智能化、网络化等。

E-mail: jqfu@staff.shu.edu.cn