(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105721230 A
(43)申请公布日 2016.06.29

(21)申请号 201410713390.7

(22)申请日 2014.11.30

(71)申请人 中国科学院沈阳自动化研究所
地址 110016 辽宁省沈阳市南塔街114号

(72)发明人 于海斌 曾鹏 尚文利 万明
赵剑明

(74)专利代理机构 沈阳科苑专利商标代理有限公司 21002
代理人 徐丽 周秀梅

(51)Int.Cl.
H04L 12/26(2006.01)

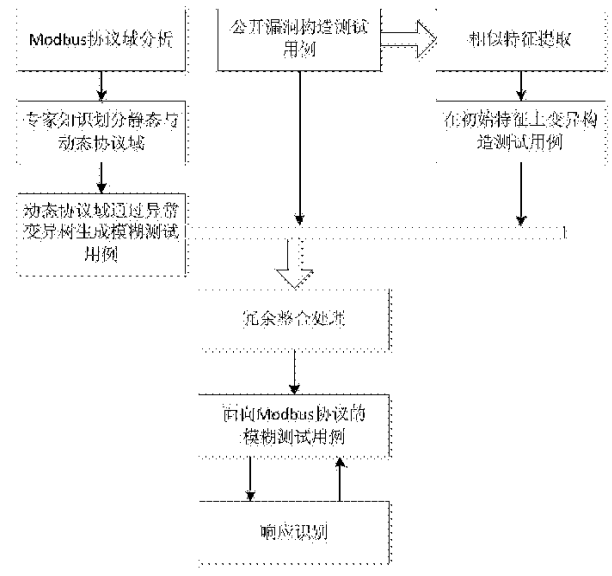
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种面向Modbus协议的模糊测试方法

(57)摘要

本发明提供了一种面向Modbus协议的模糊测试方法，能够发现工业控制系统的现场设备对Modbus协议数据的处理缺陷。该方法先通过专家知识划分Modbus协议域为静态与动态部分，动态部分通过异常变异树方法构造测试数据集合，大幅度过滤不易引发故障的模糊测试用例；之后整合已公开的漏洞信息构造测试用例，融合到模糊测试用例；再之后基于公开漏洞信息的相似特征通过遗传算法变异出一个或多个测试用例，融合到模糊测试用例，最终生成面向Modbus协议的模糊测试用例，最后设计模糊测试用例的响应信息识别方法，判断缺陷是否存在。该方法实现的装置工作于Modbus TCP/IP层，只需简单点对点的网络配置，即能有效地发现现场设备对Modbus协议数据的处理缺陷。



CN 105721230 A

1. 一种面向 Modbus 协议的模糊测试方法，其特征在于，包括以下步骤：

1) 生成三种测试用例：由异常变异树生成的模糊测试用例、基于公开漏洞信息生成的测试用例、基于公开漏洞信息的相似特征生成的测试用例；

2) 将三种测试用例进行冗余整合处理，最终生成面向 Modbus 协议的模糊测试用例；

3) 对发送的模糊测试用例，针对响应信息进行判断是否存在缺陷。

2. 根据权利要求 1 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述异常变异树生成的模糊测试用例的生成方法为：

Modbus 协议域分析：将 Modbus 请求与响应报文划分为 26 类模糊测试用例；

专家知识划分静态与动态协议域：将 Modbus 协议域分析结果划分为动态与静态部分，所述静态部分不需要组合变异，通过每个类型的模板库生成固定常亮的测试用例；所述动态部分需要组合变异，根据异常变异树的每个属性的变异规定进行每个部分的变异；

协议域通过异常变异树生成模糊测试用例：针对每类功能码确定一个模板报文，静态与动态部分基于模板报文进行模糊测试用例生成。

3. 根据权利要求 2 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述动态部分协议域采用异常变异树方式产生模糊测试用例，其中变异技术产生模糊测试用例中域变化的情况，基于污点数据区域进行裁剪，大大缩减测试用例规模；树形方式对协议域变化情况与协议域格式进行管理，组合生成模糊测试用例。

4. 根据权利要求 1 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述基于公开漏洞信息生成的测试用例给出的具体协议域异常变异特征的描述，生成测试用例，融合到模糊测试用例中，并设置最高优先级。

5. 根据权利要求 4 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述公开漏洞构造测试用例包括：

通过 NVD、CVE、中国国家信息安全漏洞库的公开内容，构造 Modbus 相关的已知漏洞库；

构造已知漏洞特征码为核心的一组交互数据流。

6. 根据权利要求 1 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述基于公开漏洞信息的相似特征生成的测试用例的生成方法为：

相似特征提取：基于协议域分析公开漏洞信息引起故障的特征，提取多个公开漏洞具有相似特征的部分；

在初始特征上变异构造测试用例：规定生成的测试用例的上限，基于遗传算法或第三方工具生成符合上限数量的测试用例。

7. 根据权利要求 1 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述冗余整合处理包括：将模糊测试用例、基于公开漏洞信息的相似特征生成的测试用例、基于公开漏洞信息生成的测试用例进行冗余处理，并设置有效的优先级。

8. 根据权利要求 1 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述响应识别包括：针对以太网信号、工业电平信号，判断响应信号属于哪个测试用例，进而判断漏洞是否存在。

9. 根据权利要求 8 所述的一种面向 Modbus 协议的模糊测试方法，其特征在于，所述判断漏洞存在的方法基于校正模型，实现精确的漏洞识别。

一种面向 Modbus 协议的模糊测试方法

技术领域

[0001] 本文发明属于工业控制系统的安全技术领域，具体的说是一种面向 Modbus 协议的模糊测方法。

背景技术

[0002] 工业控制系统 (Industry Control System，ICS) 进入电力行业较早，发展时间最长，采用的协议也最多，主要包括 :Modbus、DNP3.0、IEC 60870-5-101/104、ICCP(即 IEC 60870-6 或者 TASE.2) 和 IEC 61850 等 ;其它行业的 ICS 发展相对滞后，使用情况比较类似，主要包括 Modbus、OPC 等，所以 Modbus 协议是目前国内工业控制系统采用最多的协议之一，目前 Modbus 协议已经在石油、电力、能源、冶金等行业的工业控制系统或 SCADA 系统中进行了广泛应用。

[0003] 工业控制系统的系统正面临新的安全威胁，针对工控系统的传统简单攻击手段已经演变为高级可持续性威胁 (Advanced Persistent Threat，APT)。APT 攻击范围广、针对性强，对能源、军工、金融、制造等国家重大基础设施将造成灾难性破坏，已经关系到国家的战略安全。由于目前 APT 攻击采用了“0-day”漏洞，所以针对 APT 攻击，没有有效的防御手段，唯一的方式就是在攻击者掌握“0-day”漏洞之前，发现“0-day”漏洞，对现场设备漏洞进行补丁升级。

[0004] 正由于国内工业控制系统中 Modbus 协议应用广，且高级可持续性威胁的出现，已经关系到国家的战略安全，目前需要针对 Modbus 协议进行有效的模糊测试，发现现场设备中关于处理 Modbus 协议的缺陷，测试设备中关于 Modbus 的“0-day”漏洞，给出详细出错信息，有利于设备开发人员进行修复或补丁升级。

[0005] 由于工业现场设备的安全测试与 IT 系统的安全测试在工业通信协议、工业控制系统漏洞库、测试反馈结果要支持嵌入式电子设备的特殊输出方式等方面存在着不同之处，需要对传统 IT 系统的模糊测试在以上三方面进行改进，并且要提出更有效的、符合工业专有协议的模糊测试方法。

[0006] 综上，为了解决面向 Modbus 协议的模糊测试技术，本文提出了三方面构造模糊测试用例，并通过异常变异树减小冗余测试用例的情况，能智能、高效的发现现场设备中存在的 Modbus 协议处理缺陷。

发明内容

[0007] 有鉴于此，本发明的目的是提供一种面向 Modbus 协议的模糊测试方法，基于人工分析与异常变异树技术，生成模糊测试用例，并设计响应识别模型，发现工业控制系统的现场设备对 Modbus 协议数据的处理缺陷。

[0008] 本发明提供了一种面向 Modbus 协议的模糊测试方法，包括以下步骤 :

[0009] 1) 生成三种测试用例 :由异常变异树生成的模糊测试用例、基于公开漏洞信息生成的测试用例、基于公开漏洞信息的相似特征生成的测试用例 ;

[0010] 2) 将三种测试用例进行冗余整合处理，最终生成面向 Modbus 协议的模糊测试用例；

[0011] 3) 对发送的模糊测试用例，针对响应信息进行判断是否存在缺陷。

[0012] 所述异常变异树生成的模糊测试用例的生成方法为：

[0013] Modbus 协议域分析：将 Modbus 请求与响应报文划分为 26 类模糊测试用例；

[0014] 专家知识划分静态与动态协议域：将 Modbus 协议域分析结果划分为动态与静态部分，所述静态部分不需要组合变异，通过每个类型的模板库生成固定常亮的测试用例；所述动态部分需要组合变异，根据异常变异树的每个属性的变异规定进行每个部分的变异；

[0015] 协议域通过异常变异树生成模糊测试用例：针对每类功能码确定一个模板报文，静态与动态部分基于模板报文进行模糊测试用例生成。

[0016] 所述动态部分协议域采用异常变异树方式产生模糊测试用例，其中变异技术产生模糊测试用例中域变化的情况，基于污点数据区域进行裁剪，大大缩减测试用例规模；树形方式对协议域变化情况与协议域格式进行管理，组合生成模糊测试用例。

[0017] 所述基于公开漏洞信息生成的测试用例给出的具体协议域异常变异特征的描述，生成测试用例，融合到模糊测试用例中，并设置最高优先级。

[0018] 所述公开漏洞构造测试用例包括：

[0019] 通过 NVD、CVE、中国国家信息安全漏洞库的公开内容，构造 Modbus 相关的已知漏洞库；

[0020] 构造已知漏洞特征码为核心的一组交互数据流.

[0021] 所述基于公开漏洞信息的相似特征生成的测试用例的生成方法为：

[0022] 相似特征提取：基于协议域分析公开漏洞信息引起故障的特征，提取多个公开漏洞具有相似特征的部分；

[0023] 在初始特征上变异构造测试用例：规定生成的测试用例的上限，基于遗传算法或第三方工具生成符合上限数量的测试用例。

[0024] 所述冗余整合处理包括：将模糊测试用例、基于公开漏洞信息的相似特征生成的测试用例、基于公开漏洞信息生成的测试用例进行冗余处理，并设置有效的优先级。

[0025] 所述响应识别包括：针对以太网信号、工业电平信号，判断响应信号属于哪个测试用例，进而判断漏洞是否存在。

[0026] 所述判断漏洞存在的方法基于校正模型，实现精确的漏洞识别。

[0027] 本发明在深入理解 Modbus 协议及模糊测试技术的基础上设计，有很好的全面性与实用性，能有效降低变异空间，使之能高效的发现现场设备中存在的 Modbus 缺陷。

附图说明

[0028] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图，均应落入本发明的保护范围。

[0029] 图 1 为本发明中模糊测方法整体流程图；

[0030] 图 2 为本发明中模糊测试方法的详细结构示意图；

[0031] 图 3 为本发明中异常变异树组织示意图；

[0032] 图 4 为本发明中基于 Modbus 协议的数据包格式域图。

具体实施方式

[0033] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0034] 考虑到工业现场设备的安全测试与 IT 系统的安全测试在工业通信协议、工业控制系统漏洞库、测试反馈结果要支持嵌入式电子设备的特殊输出方式等方面存在着缺陷，本发明提供了针对这些问题的解决方案，同时引入了异常变异树对协议域中动态与静态部分的不同处理方式，可以在保证测试报文能有效测试目标故障的同时，使模糊测试用例组合空间减少，加快测试效率。

[0035] 图 1 是本发明方法的整体测试流程，图 2 为方法的详细模块结构示意图，以下根据图 1 的具体实现及图 2 的具体模块功能，实现待测目标中 Modbus 协议缺陷的发现，其中待测目标将包含所有支持 Modbus 协议的嵌入式电子设备，如可编程逻辑控制器 (PLC)、分布式控制系统 (DCS)、智能嵌入式设备 (IED) 等。

[0036] 基于图 1，本发明测试用例包含异常变异树生成的模糊测试用例、基于公开漏洞信息生成的测试用例、基于公开漏洞信息的相似特征生成的测试用例三个部分，之后将三个部分进行冗余处理，发送最终的模糊测试用例，对测试数据的响应信息进行漏洞识别处理。

[0037] 第一部分测试用例，具体地，异常变异树生成的模糊测试用例部分：如图 3 所示，首先 Modbus 协议域规定了请求与响应报文均封装为 IP 头、TCP 头、MBAP 头（包括事务处理标识符、协议标识符、长度、单元标识符）、功能码、数据；分类 Modbus 协议为标准协议规定的 21 类功能码 (1 ～ 21)、保留扩展功能码 (22 ～ 64)、保留以备用户所用功能码 (65 ～ 72)、非法功能功能码 (73 ～ 119)、内部作用 (120 ～ 127)、异常应答 (128 ～ 255)，共计 26 类模糊测试用例；之后确定各个分类中协议域规定的属性类型及范围，针对每个分类划分为静态与动态协议域，如事务处理标识符、协议标识符、单元标识符等划分为静态部分，寄存器地址、寄存器值、输出地址、输出值等划分为动态部分，不考虑功能码的变异情况；其中静态部分不需要组合变异，通过每个类型的模板库生成固定常亮的测试用例；动态部分需要组合变异，根据异常变异树的每个属性的变异规定进行每个部分的变异，如图 4 所示，常用的构造变异数据报文的依据有：针对缓冲区溢出漏洞主要考虑如“ABAB”“\A\”或“\..\”等污点数据；针对格式化字符串漏洞主要考虑如“% s% d”“% n% d”以及诸如此类的字符串；针对整数溢出主要考虑的方法往往是填充整数的边界值，如 -1、0、1、0xff、0x ffff、0x ffffffff 等；之后进行组合变异，静态部分与动态部分都能有效降低组合空间，提高测试效率。

[0038] 第二部分测试用例，具体地，首先根据 NVD（美国国家漏洞库）、CVE（公共漏洞和暴露）、中国国家信息安全漏洞库等公开内容，统计 Modbus 相关的已知漏洞，测试用例基于已知漏洞的特征码为核心，构造特定的测试用例报文。

[0039] 第三部分测试用例，具体地，基于第二部分分析的已知漏洞的特征码，提取同属于

一类的动态协议域之间相似内容或共同的行为特征的特征码，基于遗传算法或第三方工具等方式在提取的共同特征基础上，生成特定常量的测试用例；

[0040] 具体地，对三部分测试用例进行冗余处理，并设置优先级从高到底依次为基于公开漏洞信息生成的测试用例、基于公开漏洞信息的相似特征生成的测试用例、异常变异树生成的模糊测试用例。

[0041] 具体地，对已有的模糊测试用例的响应进行判断是否存在缺陷，这里针对以太网信号、工业电平信号，两个信号符合工业现场设备的特性，首先判断响应信号属于哪个测试用例，再之后根据返回信号的值，建立校正模型来精确判断是否存在缺陷，其中可采用非线性回归、多权重、自由定标等方法构造校正模型，实现精确的漏洞识别。

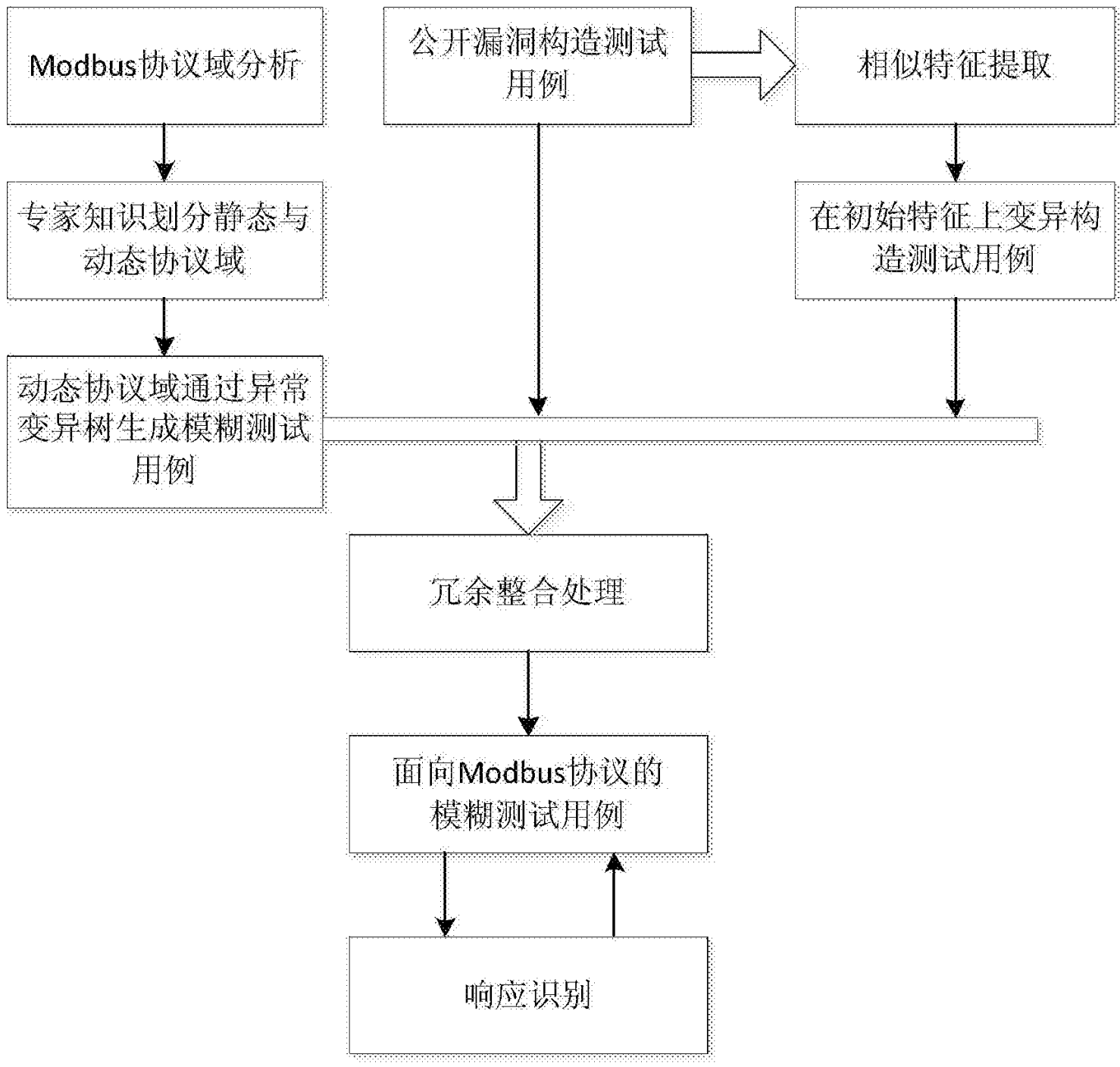

Modbus协议域分析
公开漏洞构造测试用例
相似特征提取
专家知识划分静态与动态协议域
在初始特征上变异构造测试用例
动态协议域通过异常变异树生成模糊测试用例
冗余整合处理
面向Modbus协议的模糊测试用例
响应识别

图 1

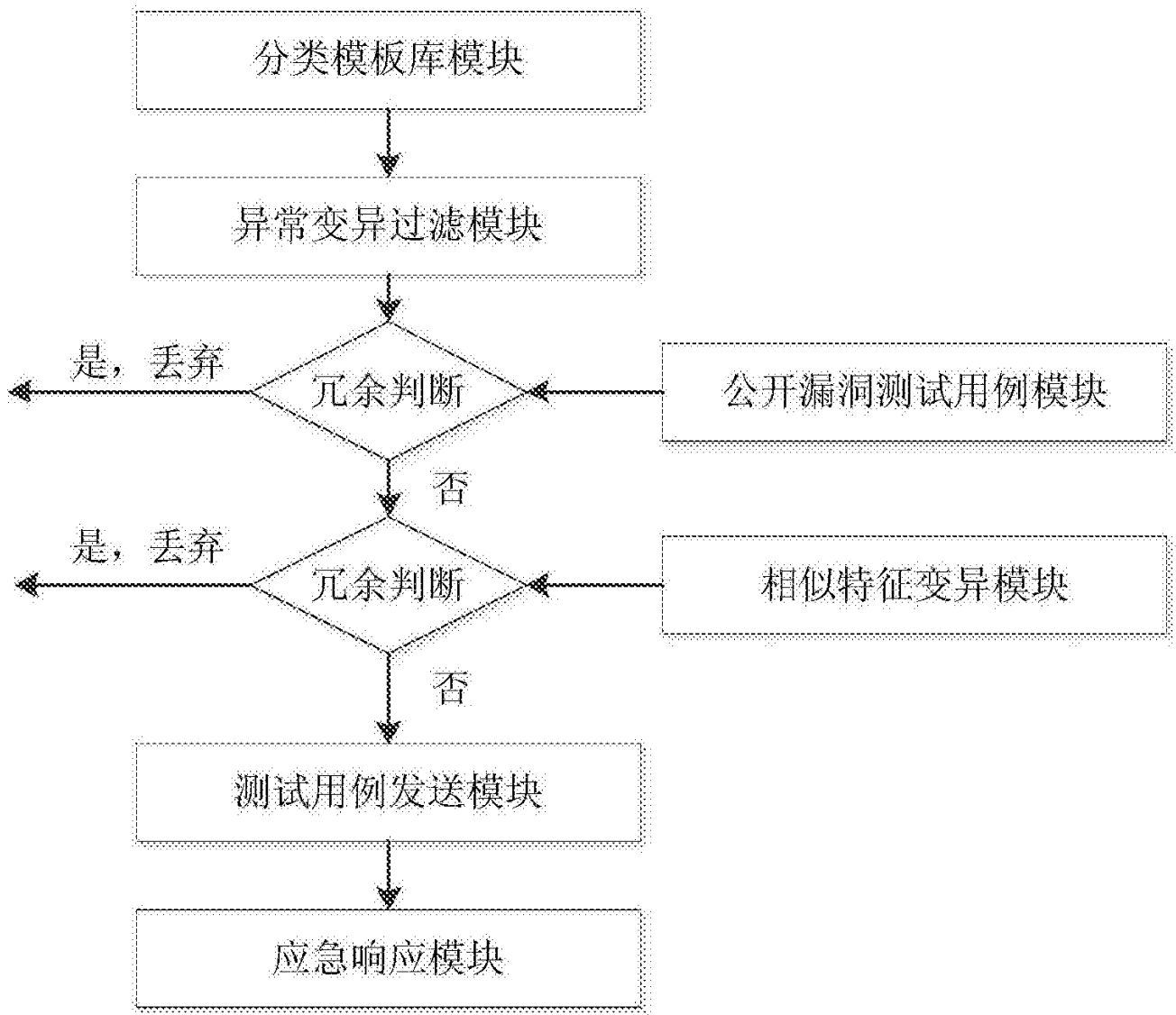

分类模板库模块
异常变异过滤模块
是，丢弃
冗余判断
公开漏洞测试用例模块
否
是，丢弃
冗余判断
相似特征变异模块
否
测试用例发送模块
应急响应模块

图 2

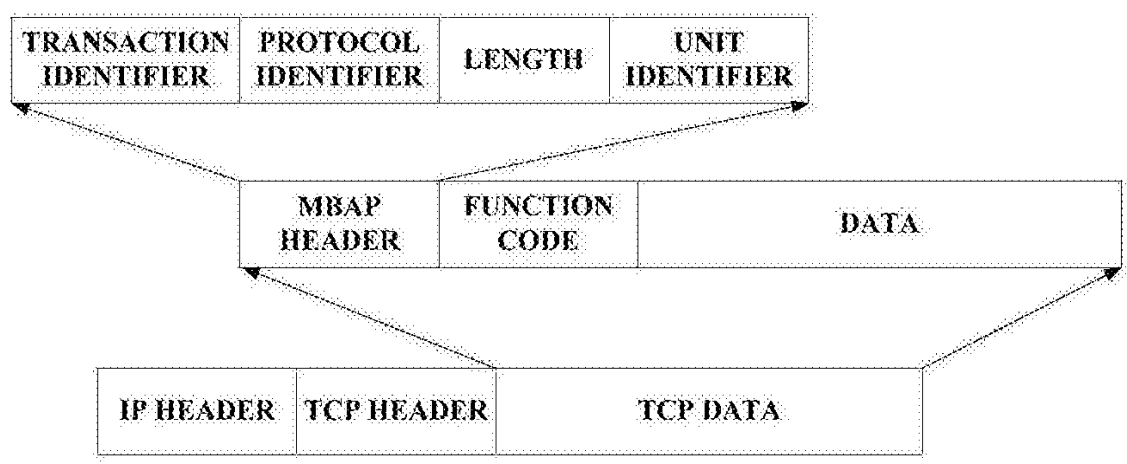

TRANSACTION IDENTIFIER
PROTOCOL IDENTIFIER
LENGTH
UNIT IDENTIFIER
MBAP HEADER
FUNCTION CODE
DATA
IP HEADER
TCP HEADER
TCP DATA

图 3

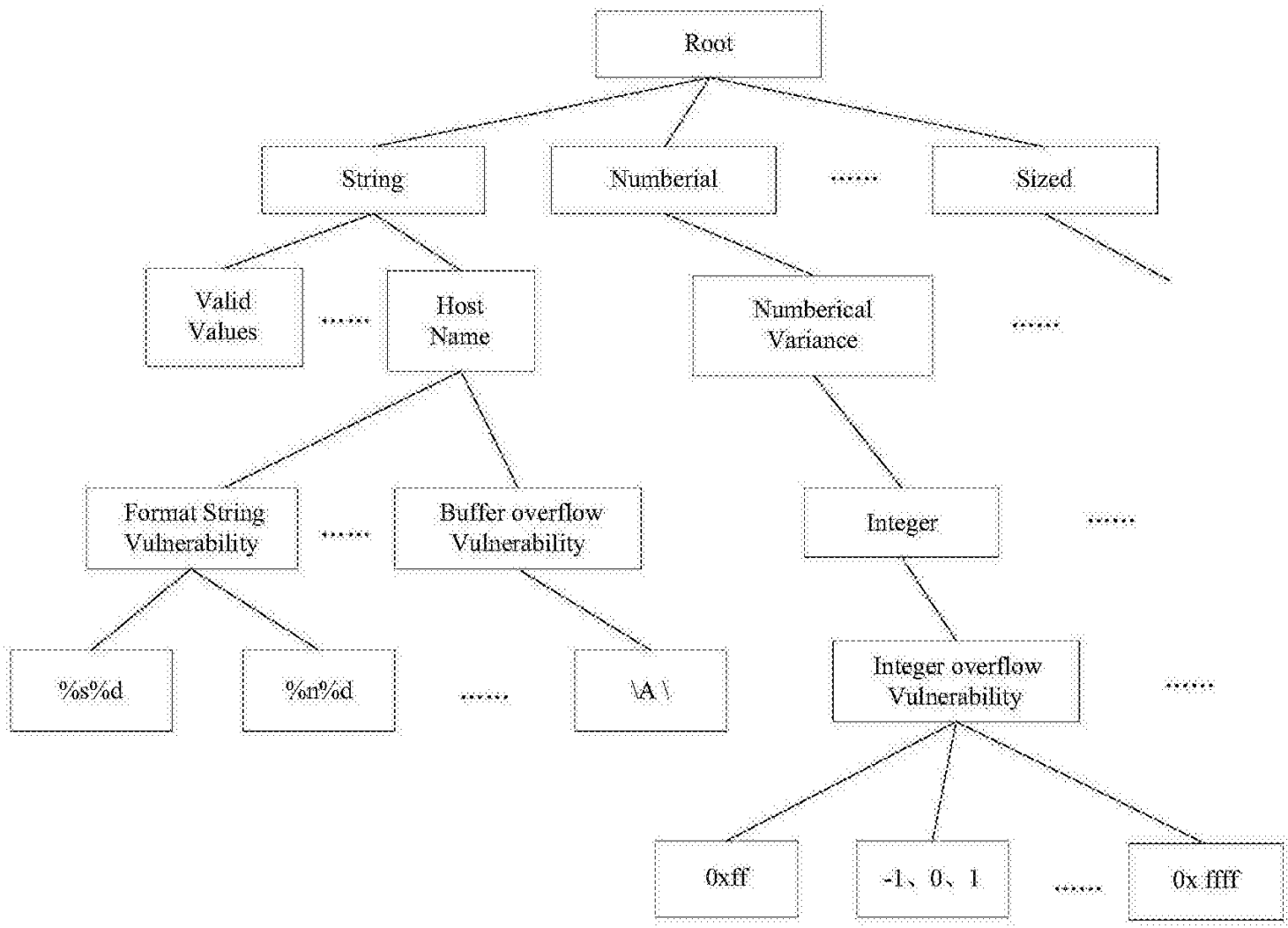

Root
String
Numberial
……
Sized
Valid Values
……
Host Name
Numberical Variance
……
Format String Vulnerability
……
Buffer overflow Vulnerability
Integer
……
%s%d
%n%d
……
\A \
Integer overflow Vulnerability
……
0xff
-1、0、1
……
0x ffff

图 4