

[19] 中华人民共和国国家知识产权局



## [12] 发明专利申请公布说明书

[21] 申请号 200710065443.9

[51] Int. Cl.

H04L 29/02 (2006.01)

H04L 29/06 (2006.01)

H04L 12/26 (2006.01)

H04L 12/24 (2006.01)

H04L 12/56 (2006.01)

[43] 公开日 2007 年 9 月 12 日

[11] 公开号 CN 101035111A

[22] 申请日 2007.4.13

[21] 申请号 200710065443.9

[71] 申请人 北京启明星辰信息技术有限公司

地址 100094 北京市海淀区东北旺西路 8 号  
中关村软件园 21 号启明星辰大厦

[72] 发明人 孙海波 骆拥政 龚 晟 叶润国

[74] 专利代理机构 北京市商泰律师事务所

代理人 毛燕生

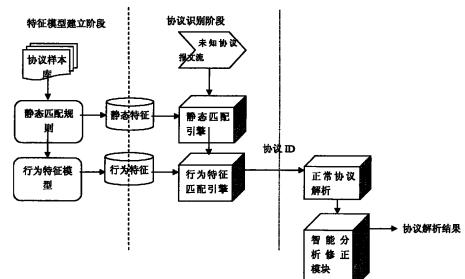
权利要求书 2 页 说明书 12 页 附图 3 页

### [54] 发明名称

一种智能协议解析方法及装置

### [57] 摘要

本发明一种智能协议解析方法及装置涉及可用于入侵检测防御( IDS/IPS )及审计产品中的一种智能协议分析方法及装置。本发明的目的是提供一种使用不单纯依赖于协议端口和静态协议特征字段匹配的智能协议分析技术，并在软件的不同版本使用时能够自动调整解析格式给出准确的协议分析结果，提高了协议分析的准确性。本发明包括三个主要步骤：建立协议特征模型；协议识别；协议智能分析修正。本发明解决了传统 IDS/IPS 产品中对于非标准端口或不具备静态数据包特征字段的网络协议的识别问题，同时对于某些应用软件或协议不同的版本等原因产生的解析结果错误可以提供自动化的修正工作。



1. 一种智能协议分析方法，其特征在于所述的步骤：

建立协议特征模型步骤；

协议识别步骤；

协议智能分析修正步骤。

2. 根据权利要求 1 所述的一种智能协议分析方法，其特征在于所述的建立协议特征模型步骤的子步骤：

协议静态字段匹配子步骤；

相应协议运行时行为特征模型的建立子步骤。

3. 根据权利要求 2 所述的一种智能协议分析方法，其特征在于所述的相应协议运行时行为特征模型的建立子步骤中分别运行的分步骤：

对于能够准确提取静态匹配模式的协议，直接提取协议样本当中的命令或静态标识字段作为匹配规则的分步骤；所述的协议静态特征提取方法是：针对单独的数据包，提取其中可以单独标识协议使用的特征作为匹配规则，如命令、状态码、固定报头中连续字段中独有的协议格式及描述；

对于无法准确提取匹配特征的协议，建立协议运行期间行为状态模型作为识别标准，以此建立特定的行为特征序列作为行为特征序列模型的分步骤；所述的协议行为特征序列模型提取规则建立方法是：依赖于一系列信息交互过程使用数据挖掘关联技术提取相关联的协议运行行为特征，并依靠自学习方法提取相对应的一个或多个特征序列；其行为特征包括协议交互逻辑顺序、相关命令、特定协议动作的操作过程及其它可以唯一标识该协议行为的特征规则。

4. 根据权利要求 1 所述的一种智能协议分析方法，其特征在于所述的协议识别步骤的子步骤：

协议静态字段快速匹配子步骤；

协议行为特征序列模型的匹配子步骤。

5. 根据权利要求 4 所述的一种智能协议分析方法，其特征在于所述的协议识别步骤的协议静态字段快速匹配子步骤中的分步骤：

将 IP 报文应用层数据作为文本输入的分步骤；

将所有协议静态特征作为模式集合，采用多模式配算法找到 IP 报文所属的可能协议集合的分步骤。

6. 根据权利要求 4 所述的一种智能协议分析方法，其特征在于所述的协议识别步骤的协议行为特征序列模型的匹配子步骤中的分步骤：

将协议静态特征匹配结果作为输入分步骤；

将所有协议运行行为特征序列作为模式集合，采用多模式配算法找到 IP 报文所属的可能协议集合分步骤。

7. 根据权利要求 5 或 6 所述的一种智能协议分析方法，其特征在于所述的协议识别步骤的相应协议运行时行为特征模型的建立子步骤中所述的协议静态特征匹配规则及行为特征匹配规则建立方法：采用控制流图的步骤，控制流图有一个假节点，有多个真节点；除真和假节点外，控制流图中每一个节点表示一条协议静态特征匹配规则布尔逻辑，其执行结果为真或假；从根节点开始执行，直到遇到真或假节点为止。

8. 根据权利要求 1 所述的一种智能协议分析方法，其特征在于所述的协议智能分析修正步骤，对于无法准确解析协议数据包进行协议智能分析修正尝试准确解析的子步骤：

分析字段大小的变更子步骤；

分析字段偏移量的改变子步骤；

分析字段顺序的变化子步骤。

9. 一种智能协议分析装置，其特征在于：包括协议静态规则库、协议行为特征模型库、协议静态规则匹配引擎、协议行为特征匹配引擎、协议解析引擎和自动化调整解析尝试模块；所述的协议静态规则库与协议静态匹配引擎连接；所述的协议行为特征模型库与协议行为特征匹配引擎连接；协议静态匹配引擎与协议静态规则库连接；协议解析引擎与智能分析修正尝试模块连接。

## 一种智能协议解析方法及装置

### 技术领域

本发明一种智能协议解析方法及装置涉及以交换为功能的网络，是一种以协议为特征的，防止未经允许从数据传输信道取数据的通信控制/处理的方法和装置。是一种入侵检测/防御(Intrusion Detection/Protection System, IDS/IPS)及审计产品中的智能协议解析方法及装置。

### 背景技术

入侵检测/防御系统 (IDS/IPS) 作为网络安全防护的重要手段，通常部署在关键网络内部/网络边界入口处，实时捕获网络内或进出网络的报文数据流并进行智能综合分析，发现可能的入侵行为并进行实时阻断。应用层协议深层解析技术在当前主流 IDS/IPS 产品中被广泛采用，可用来实现基于协议攻击特征和协议异常的入侵检测。目前多数 IDS/IPS 产品都基于端口映射表或静态的报文特征来判别网络报文所属协议类型，比如，如发现捕获的网络报文中源/目端口为 80，则认为它为 HTTP(Hypertext Transfer Protocol) 协议报文，将该报文交给 HTTP 协议分析引擎进行协议解码和入侵检测；又如在数据包中发现“%13BitTorrent%20Protocol”则认定为 BitTorrent(常用 P2P 软件) 协议数据包。通常这种端口映射表及特征字段匹配模式在 IDS/IPS 产品出厂时已确定，但允许管理员修改以适应实际环境的需要。但是近年来，随着网络协议的发展出现了一批新型的网络应用协议，包括 SIP(Session Initiation Protocol) 和 P2P(Peer to peer protocol) 协议等，它们并不采用固定协议端口，而是在协议运行过程中动态协商端口；此外，目前各种木马、P2P 软件为躲避 IDS/IPS 产品的入侵检测或审计都采用了一些特殊的处理方式，主要表现

为：1) 不使用固定通信端口进行通信；2) 复用公开端口进行私有协议通信(比如某些P2P软件使用已知公开协议端口)；3) 采用已知公开协议的传输工具；4) 不同版本的应用软件采用不同的数据封装格式。在这种情况下，IDS/IPS产品无法根据端口映射表或特定的字段模式匹配来正确识别报文所属协议类型或具体的软件使用情况，给某些特定的需求带来了很大的麻烦，这就需要根据网络协议运行行为特征智能识别报文所属协议类别，否则对于协议的深入分析将造成很多的错误。此外，对于某些私有的软件使用的协议在不同的驱动版本当中会出现不同的封装格式和命令（字段长度调整或偏移量的改变），这就给协议的准确解析带来了额外的难度，必须针对不同版本进行不同的解析实现。

## 发明内容

为了克服现有技术的不足，本发明的目的是提供一种智能协议修正分析方法及装置。所述方法和装置使用不单纯依赖于协议端口和静态协议特征字段匹配的智能协议分析技术，并在软件的不同版本使用时能够自动调整解析格式给出准确的协议分析结果，提高了协议分析的准确性。该智能协议分析技术可以满足以下要求：

结合传统的协议识别方法，智能地根据实际协议运行行为特征判断报文所使用的协议类型及版本号等相关信息；对于某些具体协议版本变动带来的格式变化采用自动调整解析方式给出不同版本的协议解析方法，以尽可能提高入侵检测及审计的准确性；具有非常高的协议识别效率，算法实现尽可能简单；方法通用性强，并要求协议解析结果准确率高。

本发明解决其技术问题所采用的技术方案是：一种智能协议分析方法，其特征在于所述的步骤：

建立协议特征模型步骤；

协议识别步骤；

协议智能分析修正步骤。

所述的建立协议特征模型步骤的子步骤：

协议静态字段匹配子步骤；

相应协议运行时行为特征模型的建立子步骤。

所述的相应协议运行时行为特征模型的建立子步骤中分别运行的分步骤：

对于能够准确提取静态匹配模式的协议，直接提取协议样本当中的命令或静态标识字段作为匹配规则的分步骤；所述的协议静态特征提取方法是：针对单独的数据包，提取其中可以单独标识协议使用的特征作为匹配规则，如命令、状态码、固定报头中连续字段中独有的协议格式及描述；

对于无法准确提取匹配特征的协议，建立协议运行期间行为状态模型作为识别标准，以此建立特定的行为特征序列作为行为特征序列模型的分步骤；所述的协议行为特征序列模型提取规则建立方法是：依赖于一系列信息交互过程使用数据挖掘关联技术提取相关联的协议运行行为特征，并依靠自学习方法提取相对应的一个或多个特征序列；其行为特征包括协议交互逻辑顺序、相关命令、特定协议动作的操作过程及其它可以唯一标识该协议行为的特征规则。

所述的协议识别步骤的子步骤：

协议静态字段快速匹配子步骤；

协议行为特征序列模型的匹配子步骤。

所述的协议识别步骤的协议静态字段快速匹配子步骤中的分步骤：

将 IP 报文应用层数据作为文本输入的分步骤；

将所有协议静态特征作为模式集合，采用多模式配算法找到 IP 报文所属的可能协议集合的分步骤。

所述的协议识别步骤的协议行为特征序列模型的匹配子步骤中的分步骤：

将协议静态特征匹配结果集作为输入分步骤（当静态特征匹配无法唯一的识别协议）；

---

将所有协议运行行为特征序列作为模式集合，采用多模式配算法找到 IP 报文所属的可能协议集合分步骤。

所述的协议识别步骤的相应协议运行时行为特征模型的建立子步骤中所述的协议静态特征匹配规则及行为特征匹配规则建立方法：采用控制流图的步骤，控制流图有一个假节点，有多个真节点；除真和假节点外，控制流图中每一个节点表示一条协议静态特征匹配规则布尔逻辑，其执行结果为真或假；从根节点开始执行，直到遇到真或假节点为止。

所述的协议智能分析修正步骤，对于无法准确解析协议数据包进行自动化解析格式调整尝试准确解析的子步骤：

分析字段大小的变更子步骤；

分析字段偏移量的改变子步骤；

分析字段顺序的变化子步骤。

一种智能协议分析装置，其特征在于：包括协议静态规则库、协议行为特征模型库、协议静态规则匹配引擎、协议行为特征匹配引擎、协议解析引擎和智能分析修正尝试模块；所述的协议静态规则库与协议静态匹配引擎连接；所述的协议行为特征模型库与协议行为特征匹配引擎连接；协议行为特征匹配引擎与协议解析引擎连接；协议解析引擎与智能分析修正尝试模块连接。

本发明的有益效果是，本发明解决了传统 IDS/IPS 产品中对于非标准端口或不具备静态数据包特征字段的网络协议的识别问题，同时对于某些应用软件或协议不同的版本等原因产生的解析结果错误可以提供自动化的修正工作。本发明能够在网络协议通信过程中根据报文当中携带的协议行为特征准确识别所属协议类型及版本，并对于未知版本和命令采用智能分析修正尝试方法对协议进行深入解析。与已有方法相比，本发明可以基于网络协议通信过程中的协议行为特征识别出所属协议类别及版本，而不单纯依赖于固定端口和静态的字段特征匹配，可以对所有无固定端口及静态字段特征的协议进行识别，同时对于某些未知的版本等原因带来的协议解析错误进行智能分析修正得到更准确

的解析结果，并且具有协议分析速度快和准确率高等优点，可广泛应用于IDS/IPS、审计等所有需要协议分析的网络安全产品中。

## 附图说明

下面结合附图和实施例对本发明作进一步叙述。

图1为本发明的协议分析方法装置工作流程图；

图2为智能分析修正尝试模块工作流程图。

图3为BITTORRENT协议行为特征匹配规则提取举例；

图4为智能协议分析装置的原理示意图。

## 具体实施方式

本发明所述协议分析过程主要包括三个工作阶段，也就是三个重要步骤：建立协议特征模型步骤；协议识别步骤；协议智能分析修正步骤。

协议特征模型建立阶段、协议识别阶段和智能协议分析阶段，各阶段步骤如下（见图1）：

### A. 建立协议特征模型步骤

本步骤是协议样本特征提取阶段。依据协议静态特征提取方法从协议类型样本中提取该类协议的协议静态特征。依据协议实际运行过程从中提取协议行为特征并建立该类协议相应的行为特征序列规则集。

将提取的协议静态特征和相应协议运行行为特征序列规则集分别存储到协议静态特征库和协议行为特征序列规则库中，供协议识别阶段静态特征匹配引擎和协议行为特征序列匹配引擎使用。

对于能够准确提取静态匹配模式的协议，直接提取协议样本当中的命令或静态标识字段作为匹配规则的分步骤；所述的协议静态特征提取方法是：针对单独的数据包，提取其中可以单独标识协议使用的特征作为匹配规则，如命令、状态码、固定报头中连续字段中独有的协议格式及描述；

对于无法准确提取匹配特征的协议，建立协议运行期间行为状态模型作为识别标准，以此建立特定的行为特征序列作为行为特征序列模型的分步骤；所

述的协议行为特征序列模型提取规则建立方法是：依赖于一系列信息交互过程使用数据挖掘关联技术提取相关联的协议运行行为特征，并依靠自学习方法提取相对应的一个或多个特征序列；其行为特征包括协议交互逻辑顺序、相关命令、特定协议动作的操作过程及其它可以唯一标识该协议行为的特征规则。

#### B. 协议识别阶段：

将 IP 报文应用层数据作为文本输入，首先将所有静态匹配特征作为模式集合，采用多模式配算法找到 IP 报文所属的可能协议集合。

对于可能的协议集合，如果结果不唯一，采用协议行为特征匹配，依靠建立的行为特征序列对于协议运行的数据包序列进行匹配。因为协议行为特征的独立性可唯一确定所使用的协议及其它相关信息（如版本号）。

捕获未知协议类型数据流 IP 报文，从应用层载荷中提取所有可能协议静态特征，采用多模式匹配算法与协议静态特征库中各特征进行匹配，识别出可能的协议集合。

对于上述可能协议集合中每一协议，调用相应的协议行为特征序列规则进行进一步的匹配，如果协议行为特征序列匹配通过，则识别出该 IP 报文所属正确协议类型，否则继续执行下一个候选协议相关验证规则，直到识别出正确协议为止。

当识别出 IP 报文所属协议类型并且经过智能分析修正得到正确解析格式之后，创建一个<源 IP，目 IP，源端口，目端口，协议 ID>五元组，从而使得属于该协议数据流的后续报文直接以正确解析方法进行解析，以减轻装置计算开销。

本方法当中除了传统的协议静态特征匹配之外添加了行为特征识别阶段和智能解析修正阶段，一般需要捕获到应用协议初期交互过程中 3—5 回合（以提取的行为特征序列长度为准）中带应用数据载荷的报文，而对于确定解析格

式及方法之后的报文无需进行重复的行为特征识别和修正，因此具有很好的协议解析速度。

本协议分析方法为每一类型协议建立一个协议静态特征集合和唯一的行为特征集合。其中的静态特征一般是一个有限长度的连续字节串；而行为特征一般是一个有限长度的特征字串序列。在协议运行过程中，首先使用静态特征匹配规则判断报文所属协议类型，限定可能使用的协议和软件的集合。在此基础上对于可能的协议类型进行行为特征检测就可以唯一的确定其所属协议类型。

实施例 1 (BitTorrent 协议静态特征)：

%13BitTorrent%20Protocol 可以标识 BitTorrent 协议或使用 BitTorrent 协议工作的软件通信过程中的 BitTorrent 消息类型，可以用它来作为 BitTorrent 协议静态识别规则；

建立 BITTORRENT 协议静态识别规则集：

文本中必须含有” Bittorrent” 字串；

等等，如实际数据包样本为：

```
GET /announce?info_hash=%0D%40_%F3%0A%269%81%94%B9/%B80%5EC%8A%8
A%9A%9C%E5&peer_id=Plus---tL315oWGtwZ9o&port=9096&uploaded=0&down-
loaded=0&left=28742712&event=started HTTP/1.0..Host: btfans.332
2.org:8000..Accept-encoding: gzip..User-agent: BitTorrent/Plus!
II 1.02 RC1....
```

但是某些情况下对于具体的软件或版本进行判断比较困难，例如发现某一 IP 报文携带协议静态特征 “HTTP”，则该 IP 报文所属协议类型为 HTTP 的可能性很大，但是无法唯一的确定是何种软件在使用。此时单纯基于协议静态匹配特征得到的协议分析或审计结果可能错误，因此需要进一步的使用行为特征匹配规则来确定协议识别结果正确性。本协议分析方法在使用静态特征匹配的

同时使用了协议行为特征识别方法。因为对于任何一种应用软件来说，无论使用何种协议必然有其特定的行为特征。依赖于具体的行为特征进行协议识别将大大提高识别的准确性。协议行为特征集与具体协议应用相关，集合中每一条规则包含一系列的行为特征，而这个行为特征序列唯一的标识了将一个 IP 报文判别为该类型协议时该 IP 报文必须满足的准则。因此，可以将为某一协议类型建立的协议行为特征集看作是该类型协议规范的一个必要条件集合。

实施例 2 (BitTorrent 协议行为特征):

首先使用与 tracker 服务器交互的 track HTTP 协议:

1) client 向 tracker 发一个 HTTP 的 GET 请求

该步骤特征为: GET /announce..... HTTP/1.0 发送给 Tracker 的 GET 请求，  
包含关键字 BitTorrent:

2) tracker 将同一个文件的下载者的信息返回给对方，该步骤特征为：用  
bencoded 编码的字典列表 Peers 地址和端口。

3) BitTorrent 客户端按照得到的 peer 列表以此发送连接请求。该步骤特征  
为：对于每个 peer 的连接请求都包括“BitTorrent”关键字。

协议特征提取；主要将特征提取分为两个步骤，首先是协议数据包静态特  
征提取。这部分主要依赖于单个数据包即可对协议进行初步判断，包括文本命  
令格式协议；固定报头格式协议和无固定格式协议。在此步骤中，尽可能多的  
提取协议数据包当中携带的特征字段以缩小行为特征匹配的范围。接下来是协  
议运行行为特征的提取，这部分针对单个数据包无法有效标识协议类型或版本  
等信息，需要对实际的运行过程进行监控加以提取以进一步准确的判断使用的  
协议类型及版本号等具体特征。行为特征的匹配针对的是一阶段内协议运行的

详细行为和动作，因此准确性更高。

协议行为特征规则集与具体协议类型及版本等信息相关，为各种类型协议建立协议行为特征规则集目的主要有以下 3 个：

- 1) 通过协议行为特征规则集可以检验静态协议规则匹配结果正确性，即在静态协议规则匹配之后产生的可能协议类型或软件使用集中唯一的标识出具体的识别结果。
- 2) 在静态协议规则匹配之后判断的协议类型基础上能够识别具体的协议运行版本等细节，保证接下来的协议解析结果的正确性。
- 3) 对于协议行为特征的匹配可以深入检查或审计特定协议或软件运行事件和动作，只有在通过静态规则匹配和行为特征匹配之后的报文才能准确的定位该通信使用的协议或软件的具体信息。

为某一类型协议建立的协议行为特征规则集为一个规则集合，采用控制流图(CFG)模型来描述协议行为特征规则集。如图 3 所示，在 CFG 模型表示方法中，每一步协议运行行为特征用一个椭圆节点表示，这里除 TRUE 和 FALSE 两条用于返回协议匹配结果的特殊规则外，其余验证规则都是一个布尔逻辑，其执行结果只能为真或假。这个协议验证规则集合从根节点开始执行，如果当前协议验证规则执行结果为真，则执行其左侧的验证规则树，如果为假，则执行其右侧的验证规则树，直到执行到 TRUE 或 FALSE 节点为止。图 3 为 BitTorrent 协议行为特征规则集例子：定义了 BitTorrent 协议运行行为特征规则集，该协议行为匹配规则集的执行从根节点开始，某一 IP 报文只有全部通过了行为特征序列的匹配，才可能返回 BitTorrent 协议 ID，否则返回 FALSE。为某一协议特征模型建立的行为特征序列的大小直接影响到协议识别结果准确

性和效率：当为某一类型协议静态特征和行为特征序列建立的条目越多，则协议识别结果的准确性就越高，但是协议识别效率会较低；当为某一类型协议静态特征和行为特征序列建立的条目越少，则协议识别效率会很高，但可能会降低协议识别结果准确性，因此，应根据需要合理定义协议验证规则集。

### C 协议智能分析修正阶段，见图 2：

对于已确定的协议类型采用相应的解析方法进行解析，如果出现解析格式结果错误，使用智能分析修正方法进行解析尝试，直至得到更加准确的解析结果。在实际的网络通信环境中，尤其是在某些私有协议的使用当中，软件版本的升级或改变通常会带来解析格式和方式上的变化。在这种情况下希望建立统一适用的解析格式和方法是不现实的。在前面的模块当中即使确定了协议的使用类型和相关的版本的信息，实际上也是针对目前已有的软件使用版本而言的。而对于很多软件，版本升级工作进行的是非常频繁的。因此对于已有版本的解析速度往往跟不上软件的更新速度。这种情况下对于每一个新的或未知版本都需要进行全面解析的话，工作量非常之大并且重复的工作很多。实际上对于这种变更所使用协议的结构变化是非常小的，本装置当中使用了智能分析修正的方法来不必要的重复工作。

在实际的解析过程中，对于协议变动的主要包括以下几个方面：

1. 字段大小的变更
2. 字段偏移量的改变
3. 字段顺序的变化

协议智能分析修正尝试模块实现的目的主要是针对目前某些私有软件使用的协议在版本变更或某些特定行为当中对于数据包格式部分所做出的改变

---

进行自动化的解析实现，这样在遇到这类问题所引起的解析错误情况下大大降低了重新解析的工作量，使得对于协议相关性的把握，对于协议类型确定情况下的具体解析提供了更大的准确性和灵活性。

为某一确定协议无法进行准确解析的时候采用的智能分析修正尝试时尝试范围的选取将影响到协议解析的准确性和效率：当尝试的范围选取越多，覆盖的可正确解析的软件或协议的类型和版本越多，同时效率也会降低。当尝试的范围选取较少时，对于某一特定类型或版本深入解析的结果的准确性会比较差，但此时效率较高。建议使用者根据对特定解析协议的了解程度，可能出现的变化情况制定合适的修正范围。

本装置采用算法：

1. 协议静态特征规则快速匹配；

在协议样本提取阶段定义好各种类型协议静态特征规则后，采用了多模匹配算法进行静态特征规则的匹配，用于在协议识别阶段对 IP 报文应用数据进行协议静态特征的发现和快速匹配，从而找到该 IP 报文所属的可能协议类型集合。可以采用多模式匹配算法来执行这种协议静态特征快速匹配过程：将 IP 报文应用层载荷数据作为多模式匹配算法的 Text，所有提取的协议静态特征集合作为模式集合，使用多模式匹配算法找到所有可能的协议类型集合，然后调用协议行为特征匹配模块排除错误的协议类型，直到找到合适的协议类型为止。

2. 协议行为特征规则的建立与匹配；

在进行协议行为特征规则提取的过程当中，对于采集的大量协议样本进行数据挖掘，利用关联规则和自学习方法逐步提取并修正行为特征序列。出于效

率的考虑，不同的协议运行过程产生的协议行为特征序列的大小不同，可以根据具体的准确性需要制定行为特征序列的长度，必要时可针对特定协议的不同行为实现多行为特征序列匹配。在收到由协议静态特征匹配输出的协议集合当中，使用多模式匹配算法匹配所有的协议行为特征序列集合，直至确定具体的协议类型及版本等详细信息。

### 3. 智能协议解析修正算法：

通过协议静态特征匹配和行为特征匹配确定协议类型之后，如果遇到不能正确解析的数据包情况，将调用智能协议解析修正模块进行修正。这里主要采用循环遍历验证的方式，按照字段大小变更、字段偏移量变更和字段编码顺序的改变顺序逐一验证可能的情况直至得出更加详细的协议解析结果。由于采用循环遍历验证的方式工作，这部分模块对于效率的影响比较明显，需要适当的设定修正范围。

一种智能协议分析装置，如图 4 所示：包括协议静态规则库、协议行为特征模型库、协议静态规则匹配引擎、协议行为特征匹配引擎和自动化调整解析尝试模块；所述的协议静态规则库与协议静态匹配引擎连接；所述的协议行为特征模型库与协议行为特征匹配引擎连接；协议行为特征匹配引擎与协议解析引擎连接；协议解析引擎与智能分析修正尝试模块连接。

其中，协议静态规则库和协议行为特征模型库分别存储了协议特征模型阶段建立的静态匹配规则和根据协议或软件实际运行过程提取的行为特征序列。协议静态规则匹配引擎实现所有能够在单独数据包中匹配的数据字段特征的快速匹配算法，协议行为特征匹配引擎需要记录协议运行期间的一系列动作和状态，以此匹配已建立的行为特征序列。

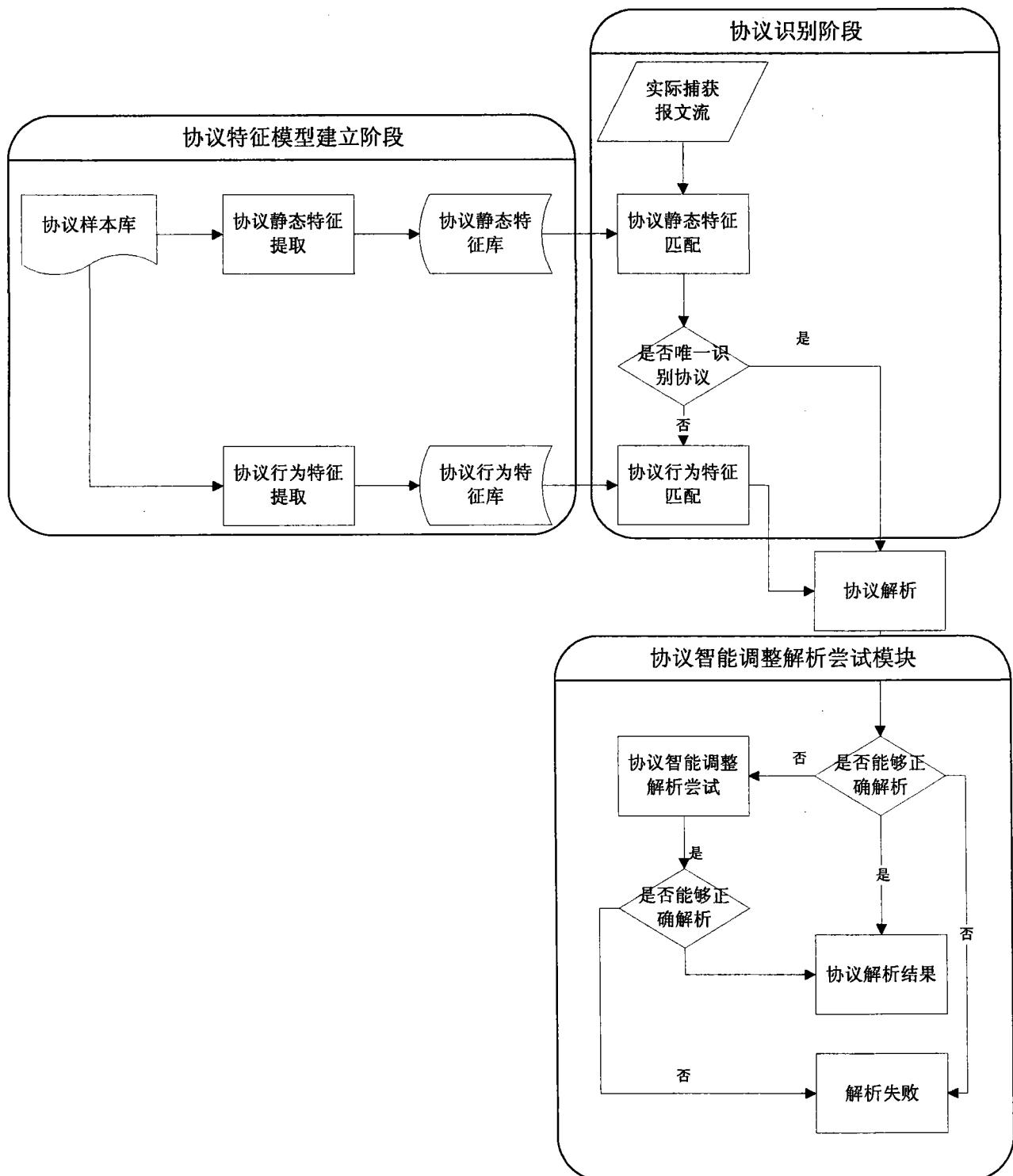


图 1

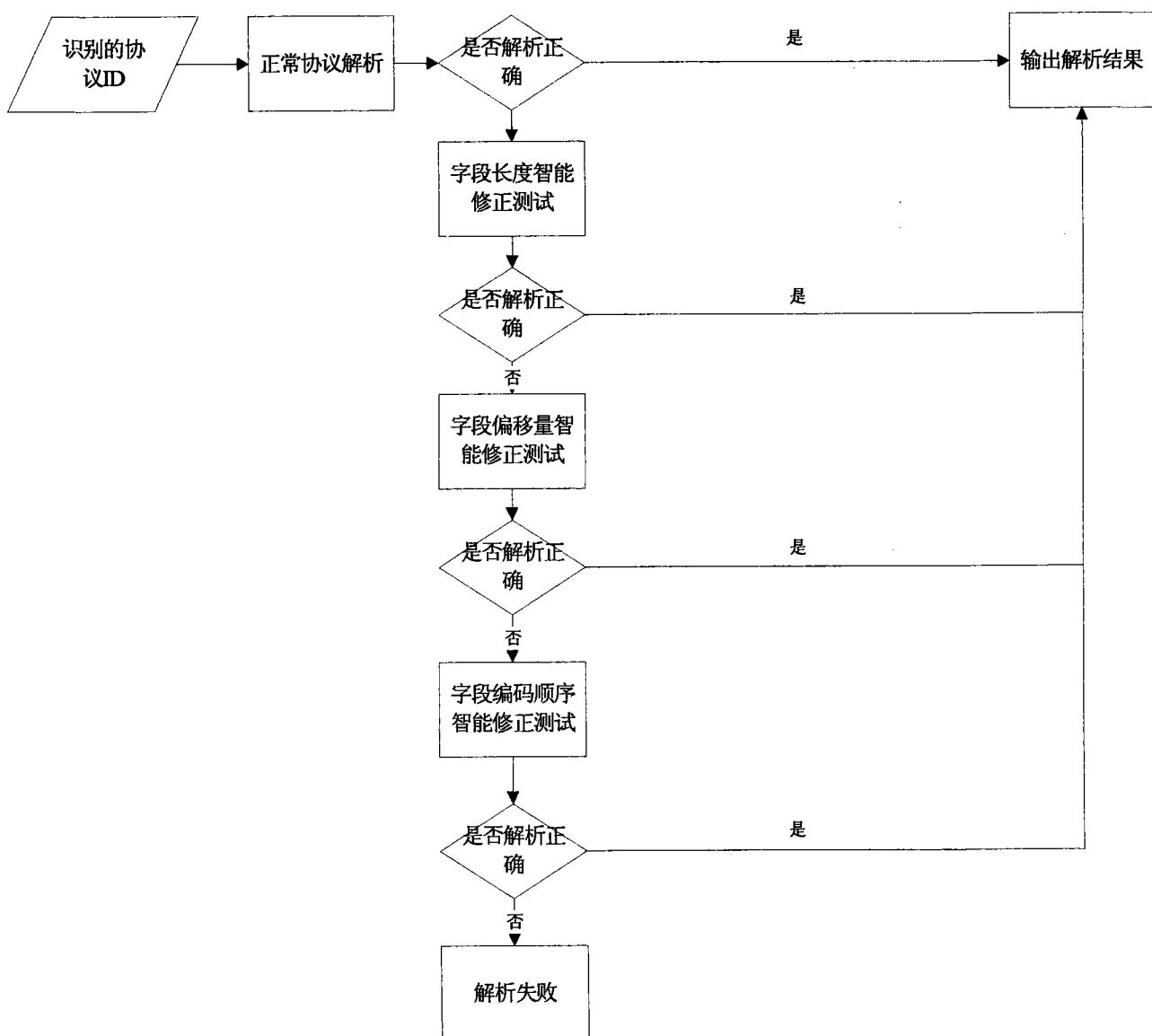


图 2

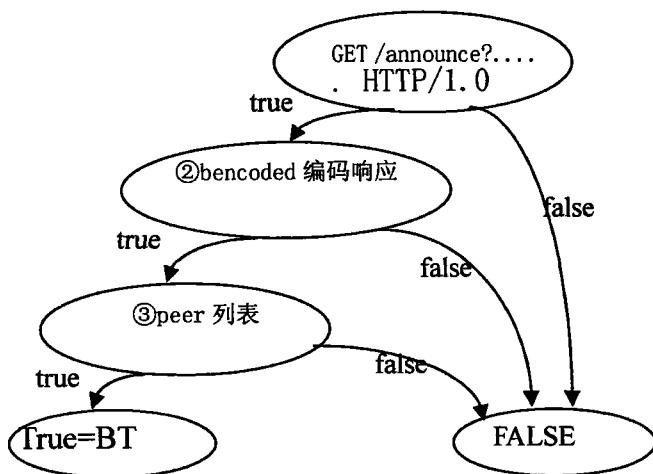


图 3

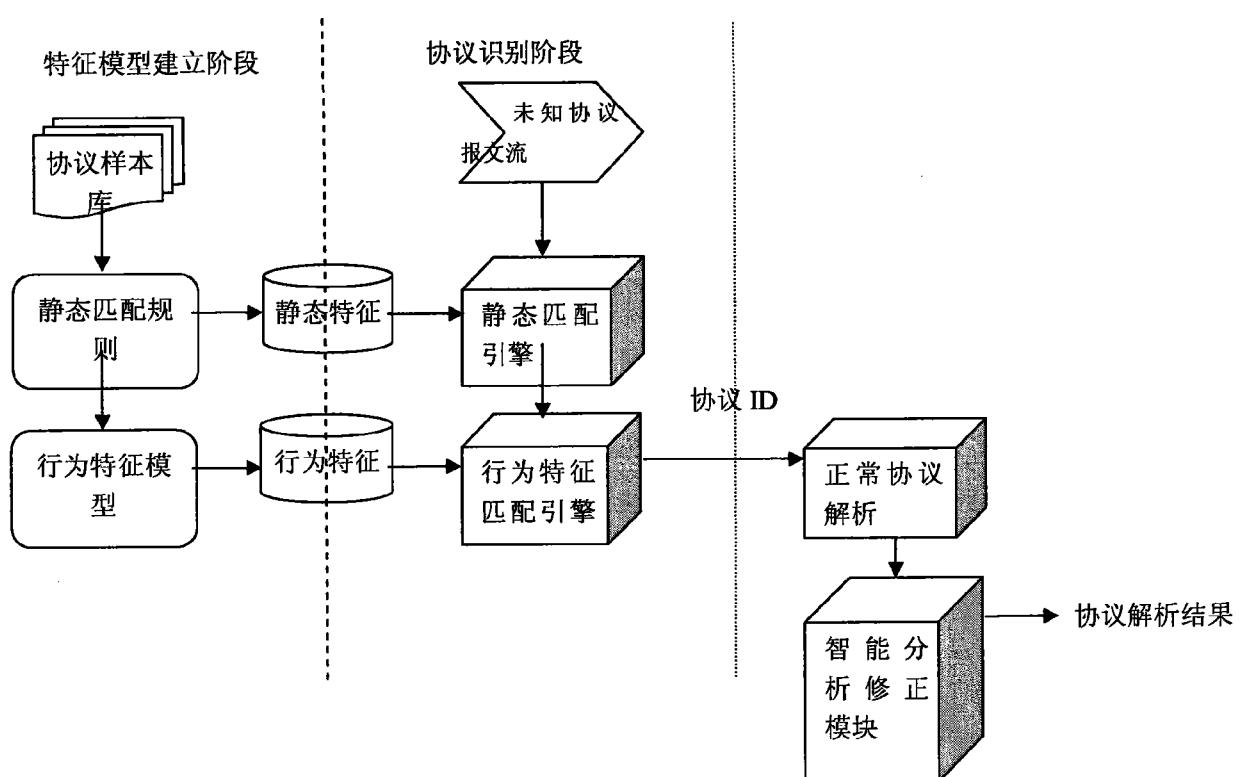


图 4