(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101388010 B
(45)授权公告日 2010.09.15

(21)申请号 200710121667.7

(22)申请日 2007.09.12

(73)专利权人 北京启明星辰信息技术股份有限公司
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 李新鹏 刘晖 张辉

(74)专利代理机构 北京市商泰律师事务所 11255
代理人 毛燕生

(51)Int.Cl.
G06F 17/30(2006.01)
H04L 12/26(2006.01)
H04L 29/08(2006.01)

(56)对比文件
US 6442541 B1,2002.08.27, 全文.
CN 1360261 A,2002.07.24, 说明书第5页第2行-第7页第20行、图1-2.

审查员 唐楹琰

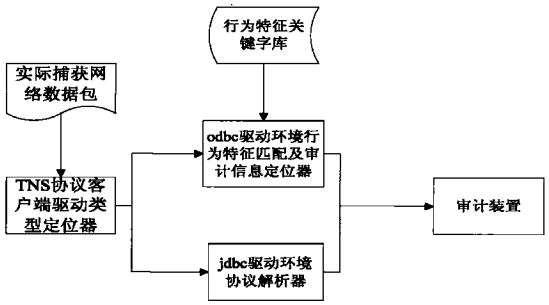
权利要求书 2 页 说明书 6 页 附图 2 页

(54)发明名称

一种Oracle数据库审计方法及系统

(57)摘要

一种Oracle数据库审计方法及系统，包括客户端驱动类型定位器、jdbc驱动环境协议解析器、行为特征关键字库、odbc驱动环境行为特征匹配及审计信息定位器、审计装置，有客户端驱动类型定位步骤；行为特征关键字库的建立步骤；odbc驱动环境行为特征匹配及审计信息定位的步骤；jdbc驱动环境协议解析的步骤；审计的步骤。解决传统审计产品中对于Oracle数据库操作行为的审计仅仅依赖协议解析带来的不准确性或仅仅依赖特征匹配带来的系统性能问题。对于Oracle数据库版本有灵活的可扩展性，扩大审计的范围，具有有针对不同版本的审计高效率和准确性，应用于网络业务审计产品。



CN 101388010 B

1. 一种 Oracle 数据库审计方法，其特征在于包含以下步骤：

TNS 协议客户端驱动类型定位步骤，以 Oracle 数据库客户端与服务器初始连接交互过程中交换的一些系统信息判断当前客户端所使用的驱动类型为 jdbc 驱动还是 odbc 驱动；并以此阶段的输出作为下一阶段按照 jdbc 驱动解析还是按照 odbc 驱动进行特征匹配的标准；

jdbc 驱动环境协议解析的步骤，在 jdbc 驱动环境下按照统一设定的数据报文解析格式对 oracle 数据库客户端与服务器之间交互信息进行解析并提取相关审计信息以供审计阶段使用；

行为特征关键字库的建立步骤，在 odbc 驱动环境下，由实际交互数据包中提取不受数据库版本影响的可标识数据库操作行为的特征关键字或匹配模式；并将所提取的特征关键字或匹配模式与包含该特征关键字或匹配模式的数据包类型进行关联建立索引，将该索引存储到行为特征关键字库中；

odbc 驱动环境行为特征匹配及审计信息定位的步骤，在 odbc 驱动环境下以实际捕获的数据库操作数据包为样本，以行为特征关键字库存储的特征关键字或匹配模式为模式进行多模式匹配并提取相关审计信息以供审计阶段使用；

审计的步骤，以 jdbc 驱动环境协议解析阶段或 odbc 驱动环境行为特征匹配及审计信息定位阶段输出的审计信息为依据对该环境下的 oracle 数据库的操作进行网络业务审计，同时将审计结果返回给管理系统进行实时显示同时将审计结果存储于事件库或系统日志当中。

2. 一种 Oracle 数据库审计系统，其特征在于包括：

对 Oracle 数据库实际使用驱动类型进行判断的 TNS 协议客户端驱动类型定位器，用于以 Oracle 数据库客户端与服务器初始连接交互过程中交换的一些系统信息判断当前客户端所使用的驱动类型为 jdbc 驱动还是 odbc 驱动；并以此阶段的输出作为下一阶段按照 jdbc 驱动解析还是按照 odbc 驱动进行特征匹配的标准；

对 jdbc 类型驱动环境下 TNS 协议数据包进行解析的 jdbc 驱动环境协议解析器，用于在 jdbc 驱动环境下按照统一设定的数据报文解析格式对 oracle 数据库客户端与服务器之间交互信息进行解析并提取相关审计信息以供审计阶段使用；

存储了 odbc 驱动环境下进行特征匹配并实现审计信息提取的行为特征关键字库，用于在 odbc 驱动环境下，由实际交互数据包中提取不受数据库版本影响的可标识数据库操作行为的特征关键字或匹配模式；并将所提取的特征关键字或匹配模式与包含该特征关键字或匹配模式的数据包类型进行关联建立索引，将该索引存储到行为特征关键字库中；

对 odbc 类型驱动环境下 TNS 协议数据包进行多模式匹配提取审计信息的 odbc 驱动环境行为特征匹配及审计信息定位器，用于在 odbc 驱动环境下以实际捕获的数据库操作数据包为样本，以行为特征关键字库存储的特征关键字或匹配模式为模式进行多模式匹配并提取相关审计信息以供审计阶段使用；

最终通过提取的信息进行网络业务行为审计并进行实时显示或日志保存的审计装置，用于以 jdbc 驱动环境协议解析阶段或 odbc 驱动环境行为特征匹配及审计信息定位阶段输出的审计信息为依据对该环境下的 oracle 数据库的操作进行网络业务审计，同时将审计结果返回给管理系统进行实时显示同时将审计结果存储于事件库或系统日志当中；

其中，所述的 TNS 协议客户端驱动类型定位器与 jdbc 驱动环境协议解析器和 odbc 驱动环境行为特征匹配及审计信息定位器连接；所述的行为特征关键字库与 odbc 驱动环境行为特征匹配及审计信息定位器连接；jdbc 驱动环境协议解析器和 odbc 驱动环境行为特征匹配及审计信息定位器与审计装置连接。

一种 Oracle 数据库审计方法及系统

技术领域

[0001] 本发明涉及可用于网络业务审计产品中的一种 Oracle 数据库审计方法及系统，它依据网络数据流中报文具有的特征对各种版本 oracle 数据库客户端使用的 TNS 协议进行解析，属于网络技术领域。

背景技术

[0002] 网络业务审计系统是目前应用日益广泛的作为网络安全防护的重要手段，它通过对业务系统中可信人员的网络活动进行解析、记录、分析以帮助管理人员事前规划预防、事中实时监控、违规行为阻止和事后追查网络运营事故，从而帮助用户加强内外部网络行为监管、避免核心资产（数据库、服务器、网络设备）损失、保障客户业务系统的正常运营，是企业实现 IT 管理和控制的最佳实践。其中在金融、电信等行业当中大量使用的数据库系统对于审计的要求尤为重要，行业内部经常需要对于业务系统当中的用户对于数据库的操作进行准确详细的审计。目前常用的几种数据库 (mysql、sql server、DB2、Oracle 等等）是网络业务审计系统最为重要的审计对象。其中以 Oracle 数据库最为复杂。对于常用的数据库来说，绝大多数的网络业务审计系统采用的是对数据包首先进行协议解析，然后根据解析后的协议格式提取相应的数据信息。例如 :用户登录时使用的用户名、用户对数据库进行的一些操作等等。此时对于数据库业务的准确审计完全依赖于对该数据库所使用协议的准确解析。而目前这些常用的数据库通常是由各大网络公司（如 Oracle、IBM) 自主研发的，其使用的具体协议各不相同。其中以 Oracle 公司开发的数据库使用的 TNS 协议最为复杂。并且对于 Oracle 数据库不同的环境当中使用的协议驱动类型也是不相同的，在其所使用的驱动类型当中以 jdbc 和 odbc 两种类型的驱动使用最为广泛，其中的 jdbc 版本驱动下的各版本遵照固定的数据格式进行消息的封装但是 odbc 驱动环境下的数据封装格式是随着具体的版本号的变化而变化的，这些都给准确的协议解析带来了非常大的困难。

[0003] 目前日益广泛使用的数据库应用成为了当前网络业务的重要组成部分，做为主流数据库之一的 Oracle 数据库得到了更加广泛的使用，越来越多的用户及企事业单位对于 Oracle 数据库业务的审计提出了很高的要求，这使得基于协议解析进行准确的业务审计变得非常困难。目前通常所使用的大多数网络业务审计系统当中对于 Oracle 数据库的审计都是基于对 TNS 协议的准确解析的，但是 TNS 协议本身具有的灵活性和数据字段的不确定性（主要体现在 odbc 驱动环境下不同的客户端版本使用不同的协议格式）给准确的业务审计带来了前所未有的困难，而具有准确灵活的能够实现对于 Oracle 数据库 TNS 协议跨版本解析并进一步进行业务审计的产品是非常缺乏的。注意到 Oracle 数据库使用 odbc 驱动的客户端每一个版本的变动都会带来数据包格式的变化，但是这种变化还是具有一定的特征，例如所有的数据库操作 SQL 语句都包含在特定类型的包当中，并且都以明文的形式出现，因此实现根据不同的驱动版本类型实现跨版本的 TNS 协议的解析及操作审计是可能的。从而有必要发展一种能够实现跨版本对于 Oracle 数据库 TNS 协议的解析用以提高网络业务审计系统的准确性、效率和审计范围。

发明内容

[0004] 为了克服现有对于Oracle数据库TNS协议无法提供统一准确的解析方法的不足，本发明提供一种Oracle数据库审计方法及系统。一种Oracle数据库审计方法含有TNS协议跨版本解析技术，TNS协议跨版本解析技术可以满足：尽可能多的准确解析Oracle数据库不同驱动环境下各个客户端版本所使用的TNS协议，对于不同类型驱动环境下的客户端版本都能够准确进行协议解析并提取相关数据以供审计；具有很好的可扩展性，对于某些新的Oracle数据库版本具有灵活的可扩展性以扩大审计的范围；具有非常高的针对不同版本的TNS协议解析效率，算法实现尽可能简单；

[0005] 本发明的目的是这样实现的：

[0006] 一种Oracle数据库审计系统（或称为：Oracle数据库TNS协议跨版本解析系统），包括有：

[0007] 负责通过捕获的报文当中包含的信息来判断当前数据库应用环境下客户端所使用的驱动类型的TNS协议客户端驱动类型定位器；

[0008] 根据驱动类型定位阶段的结果，如果是使用jdbc驱动的时候采用协议解析的方式实现对Oracle数据库操作过程中相关信息的提取的jdbc驱动环境协议解析器；

[0009] 存储了odbc驱动环境行为特征匹配阶段进行多模式匹配使用的特征模式的行为特征关键字库；

[0010] 在驱动类型定位阶段输出实际客户端使用odbc驱动的情况下根据实际捕获的数据报文使用多模式匹配的方式对需要审计的特定行为特征的匹配及相关信息的提取的odbc驱动环境行为特征匹配及审计信息定位器；

[0011] 根据上述提取的相关信息进行Oracle数据库业务的审计装置。

[0012] 所述的TNS协议客户端驱动类型定位器与jdbc驱动环境协议解析器和odbc驱动环境行为特征匹配及审计信息定位器连接；所述的行为特征关键字库与odbc驱动环境行为特征匹配及审计信息定位器连接；jdbc驱动环境协议解析器和odbc驱动环境行为特征匹配及审计信息定位器与审计装置连接。

[0013] 一种Oracle数据库审计方法（或称为：Oracle数据库TNS协议跨版本解析方法），包括有：

[0014] TNS协议客户端驱动类型定位步骤；

[0015] 行为特征关键字库的建立步骤；

[0016] odbc驱动环境行为特征匹配及审计信息定位的步骤；

[0017] jdbc驱动环境协议解析的步骤；

[0018] 审计的步骤。

[0019] 本发明的有益效果是，本发明解决了传统审计产品中对于Oracle数据库仅仅依赖于TNS协议解析带来的版本性解析错误问题。对于可以按照统一解析格式的部分采用协议解析技术（jdbc驱动环境），而对于不能使用精确解析的odbc环境采用了特征关键字匹配技术进行信息提取。在保证效率的同时，实现了对于Oracle数据库TNS协议跨版本的审计。此外在系统实现的过程当中充分考虑了扩展性问题，使得对于将来出现的新的数据库版本只需要补充新的特征关键字，进行扩展相当的简单和方便无需对系统进行大的改动，

可广泛应用于网络业务审计产品中。

附图说明

[0020] 下面结合附图和实施例对本发明进一步说明。

[0021] 图 1 为本发明的 Oracle 数据库审计系统结构图；

[0022] 图 2 为 Oracle 数据库审计方法程序流程图；

[0023] 图 3 为行为关键字库建立关联例图。

具体实施方式

[0024] 实施例 1：

[0025] 本实施例为 Oracle 数据库 TNS 协议跨版本解析方法的基本模式。所使用的系统如图 1 所示。包括 TNS 协议客户端驱动类型定位器、jdbc 驱动环境协议解析器、行为特征关键字库、odbc 驱动环境行为特征匹配及审计信息定位器、审计装置，运行流程如图 2 所示。

[0026] ① TNS 协议客户端驱动类型定位步骤：不同版本客户端环境下在客户端与服务器连接交互的过程中首先会交换彼此的一些系统信息，如服务器与客户端的操作系统、当前使用的版本等等。这些信息是不随着版本的变化而变化的。因此在客户端与服务器初始连接交互的过程当中可以在数据包当中捕获相应的系统信息，以此可以准确的判断当前客户端所使用的驱动类型（主要是 jdbc 和 odbc 的区分）。此阶段的输出将作为下一阶段按照 jdbc 驱动解析还是按照 odbc 驱动进行特征匹配的标准。

[0027] ② jdbc 驱动环境协议解析步骤：在 jdbc 驱动类型的环境当中，所有的数据包格式是固定的，并不随着具体的客户端版本的不同而变化。因此这里采用通用的协议解析方式给出所有数据包的组装格式，并且按照不同类型的命令区分不同目的的数据包并从中提取相应的有用的信息。

[0028] ③行为特征关键字库的建立步骤：此阶段主要针对 odbc 驱动环境下的客户端与服务器交互过程当中特定的 Oracle 数据库操作具有的报文特征进行提取。在 Oracle 数据库的操作过程当中，客户端与服务器的信息交互是以 SQL 语句传递的，通常在数据包中以明文出现。因为在 odbc 驱动环境当中，这些交互的信息封装的报文格式是随着版本的不同而变化的，即 SQL 语句在数据包当中所处位置并不是固定的，因此无法采用通用的解析方式进行提取。但是所有的 SQL 语句开头都包含一定的特征关键字，因此本阶段主要负责将所有这类可以标识 Oracle 数据库相关操作的特征关键字进行汇总并储存到行为特征关键字库中作为 odbc 驱动环境行为特征匹配及信息提取阶段进行多模式匹配的标准，同时与包含相应 SQL 语句或其他审计信息的特征关键字与对应的数据包类型进行关联。

[0029] ④ odbc 驱动环境行为特征匹配及审计信息定位步骤：此阶段的进入前提条件是 TNS 协议客户端驱动类型定位阶段判断当前实际网络客户环境使用的是 odbc 类型的驱动。然后以实际捕获的数据库操作数据包为样本，以行为特征关键字库存储的特征关键字为模式进行匹配并将匹配到的位置作为待审计的信息起始位置输出。

[0030] ⑤审计步骤：以 jdbc 驱动环境协议解析阶段或 odbc 驱动环境行为特征匹配及审计信息定位阶段的输出做为审计的内容，记录网络业务特定行为的一些相关信息。

[0031] 实施例 2：

[0032] 本实施例为实施例 1 中的 TNS 协议客户端驱动类型定位步骤的优选方案。

[0033] 本实施例的基本思路是：首先在 Oracle 数据库客户端和服务器进行连接的过程当中尽可能多的寻找能够标识驱动类型和主机状态的信息，包括主机操作系统、操作系统版本，所使用的 Oracle 数据库版本等等。因为这些信息是不随着版本的变化而变化的，因此是可行的。在本实施例当中选取了交互过程当中的 01 和 02 号数据包，这里 01 和 02 是在数据报文当中消息类型字段标识的。主要是依赖于 02 相应报文当中的明文特征。如在 jdbc 驱动类型环境下数据报文中包含“Java_TTC”的明文特征，在 odbc 驱动类型环境下可能包含“IBMPC/WIN_NT”等等。以此来唯一的确定当前客户环境下所使用的驱动类型并作为下一阶段按照 jdbc 驱动解析还是按照 odbc 驱动进行特征匹配的标准。

[0034] 实施例 3：

[0035] 本实施例为实施例 1 中的 jdbc 驱动环境协议解析步骤的优选方案。

[0036] 本实施例是在 TNS 协议客户端驱动类型定位阶段确定当前客户环境使用 jdbc 驱动类型的前提下进行的。因为在 jdbc 驱动环境下 oracle 数据库所有版本使用相同的协议封装格式对数据进行封装，因此可以采用统一的协议解析方法对数据进行提取。例如可以在包类型字段标识为 033b 的数据包当中跳过固定的偏移位置在 ReqrVN 字段当中提取当前使用的客户端具体的版本号；同样在包类型字段标识为 0351 的数据包当中跳过固定的偏移位置在固定字段 userN 当中可以提取到当前对数据库进行操作的用户名。以此方式通过对 jdbc 类型驱动的详细解析可以提取出任何在此驱动类型环境下客户端和数据库交互操作的所有需要审计的内容。

[0037] 实施例 4：

[0038] 本实施例为实施例 1 中的行为特征关键字库的建立步骤的优选方案，其实现如图 3 所示。

[0039] 本实施例是在 TNS 协议客户端驱动类型定位阶段确定当前客户环境使用 odbc 驱动类型的前提下进行的。因为在 odbc 类型驱动环境下客户端与服务器交互操作过程的数据信息封装格式是随着版本的不同而变化的，因此以统一的解析方式对信息进行提取必然带来准确性的问题。在 oracle 数据库的操作过程当中，所有客户端与服务器之间的信息交互都是以 SQL 语句的形式在数据包文中明文传输的。而所有的 SQL 语句都是包含一定明文特征的，本实施例实现的思路就是提取相应数据库操作的所有 SQL 语句的明文特征，以及其它信息的匹配特征或规则。并且按照包含该信息的数据包类型建立索引并入库。如在包类型为 0376 数据包当中建立用户名提取的匹配规则为：“从数据包末尾向前进行搜索，因为在出现用户名之后不会出现连续的两个不可见字符，因此可以进行由后向前进行匹配找到第一处连续两个不可见字符，之后作为用户名提取直至遇到下一个不可见字符提取结束。”又如对于所有的 SQL 语句标识的数据库操作提取如下的特征字段：对数据库中建立新表的操作 SQL 语句会以“add...”开头并且只出现在 03** 类型的数据包当中。因此将 add 作为该数据库操作的特征关键字提取并与 03** 类型的数据包进行关联入库。

[0040] 实施例 5：

[0041] 本实施例为实施例 1 中的 odbc 驱动环境行为特征匹配及审计信息定位步骤的优选方案。

[0042] 此阶段的进入前提条件是 TNS 协议客户端驱动类型定位阶段判断当前实际网络

客户环境使用的是odbc类型的驱动。然后以实际捕获的数据库操作数据包为样本，以行为特征关键字库存储的特征关键字为模式进行多模式匹配并将匹配到的位置作为待审计的信息起始位置输出。例如当实际捕获到包类型标识为0376数据包的时候，需要按照特征关键字库当中存储的与该类型数据包关联的所有特征关键字或匹配模式进行多模式匹配。本实施例当中对于0376数据包需要对于用户名进行提取，其匹配规则参照实施例4当中提取的用户名匹配规则，同时因为对所有03**类型的数据包需要进行SQL语句的提取，因此将以该数据包为样本，以所有SQL语句特征关键字（如add、delete等等）为模式使用多模式匹配算法进行信息的定位与提取以供审计阶段使用。

[0043] 本实施例中采用的算法；

[0044] 多模式匹配算法：以实际捕获的样本包数据作为匹配样本，以特征关键字库当中存储的与该类型数据包关联的所有特征关键字或匹配模式进行多模式匹配。本系统采用ACBM多模式匹配算法，对于每一个数据包样本只扫描一次，同时对于多个匹配模式进行匹配，可以输出所有的满足任意匹配模式的样本片段。在本实施例中采用多模式匹配算法可以准确的输出所有包含在特征关键字库中的特征关键字或匹配模式相对应的oracle数据库操作。

[0045] 实施例6：

[0046] 本实施例为实施例1中的odbc驱动环境行为特征匹配及审计信息定位步骤的优选方案。

[0047] 此阶段以jdbc驱动环境协议解析阶段或odbc驱动环境行为特征匹配及审计信息定位阶段的输出做为审计的内容，记录网络业务特定行为的一些相关信息。本实施例以相应提取的数据段内容如用户名、SQL语句内容等等作为输出信息。这些输出信息实际上标识了当前环境下当前用户对数据库的一些具体操作行为，如登录、创建、修改、删除数据库内容等等。本系统将这些输出信息传输到系统管理平台的显示装置上供管理员使用，同时将具体审计的网络业务事件存储到相应的事件库或系统日志当中以备后期追查、取证等使用。

[0048] 实施例7：

[0049] 本实施例是实现实施例1、2、3、4、5、6所述的方法的虚拟装置或者说系统。系统如图1所示，本实施例包括：对Oracle数据库实际使用驱动类型进行判断的TNS协议客户端驱动类型定位器、对jdbc类型驱动环境下TNS协议数据包进行解析的jdbc驱动环境协议解析器、存储了odbc驱动环境下进行特征匹配并实现审计信息提取的行为特征关键字库、对odbc类型驱动环境下TNS协议数据包进行多模式匹配提取审计信息的odbc驱动环境行为特征匹配及审计信息定位器、最终通过提取的信息进行网络业务行为审计并进行实时显示或日志保存的审计装置。

[0050] 其中，TNS协议客户端驱动类型定位器实现了如实施例2中所述的对实际客户环境使用的Oracle数据库驱动类型的判定功能；jdbc驱动环境协议解析器实现了如实施例3对于jdbc驱动环境下Oracle数据库客户端与服务器交互数据的准确解析功能；行为特征关键字库存储了odbc驱动环境行为特征匹配及审计信息定位器进行多模式匹配需要使用的特征关键字及匹配模式；odbc驱动环境行为特征匹配及审计信息定位器实现了如实施例5所述的对于odbc驱动环境下依据特征关键字及相应匹配模式对Oracle数据库客户端

与服务器交互数据当中的审计信息进行准确提取的功能；审计装置实现了实施例 6 所述的对于 Oracle 数据库跨版本的网络业务行为审计功能。

[0051] 一种 Oracle 数据库审计系统（或称为：Oracle 数据库 TNS 协议跨版本解析系统），包括：TNS 协议客户端驱动类型定位器、jdbc 驱动环境协议解析器、行为特征关键字库、odbc 驱动环境行为特征匹配及审计信息定位器、审计装置。所述的 TNS 协议客户端驱动类型定位器与 jdbc 驱动环境协议解析器和 odbc 驱动环境行为特征匹配及审计信息定位器连接；所述的行为特征关键字库与 odbc 驱动环境行为特征匹配及审计信息定位器连接；jdbc 驱动环境协议解析器和 odbc 驱动环境行为特征匹配及审计信息定位器与审计装置连接。

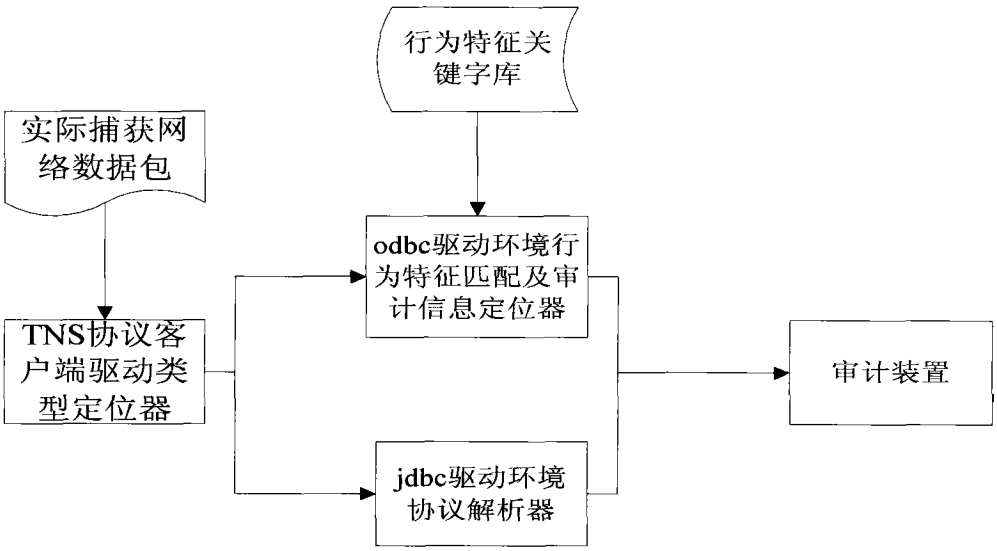

行为特征关键字库
实际捕获网络数据包
odbc驱动环境行为特征匹配及审计信息定位器
TNS协议客户端驱动类型定位器
审计装置
jdbc驱动环境协议解析器

图 1

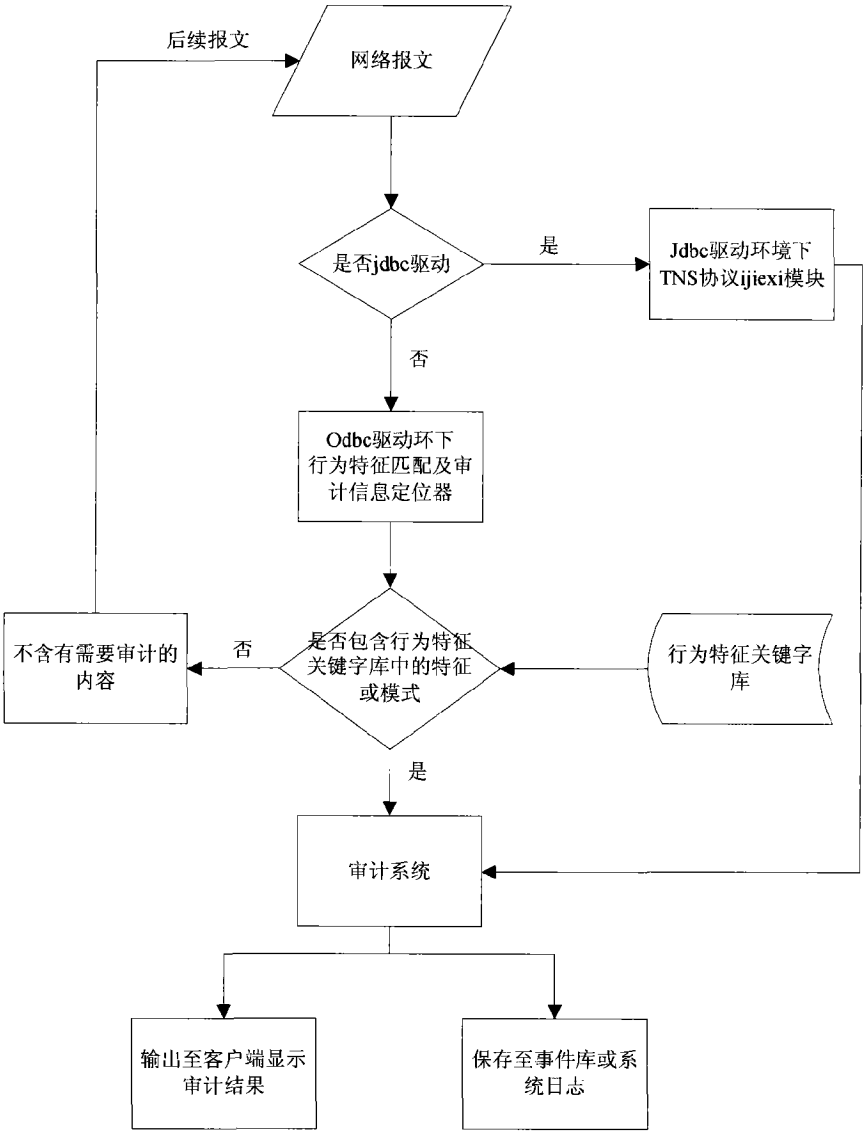

后续报文
网络报文
是否jdbc驱动
是
Jdbc驱动环境下TNS协议ijiexi模块
否
Odbc驱动环下行为特征匹配及审计信息定位器
不含有需要审计的内容
否
是否包含行为特征关键字库中的特征或模式
行为特征关键字库
是
审计系统
输出至客户端显示审计结果
保存至事件库或系统日志

图 2

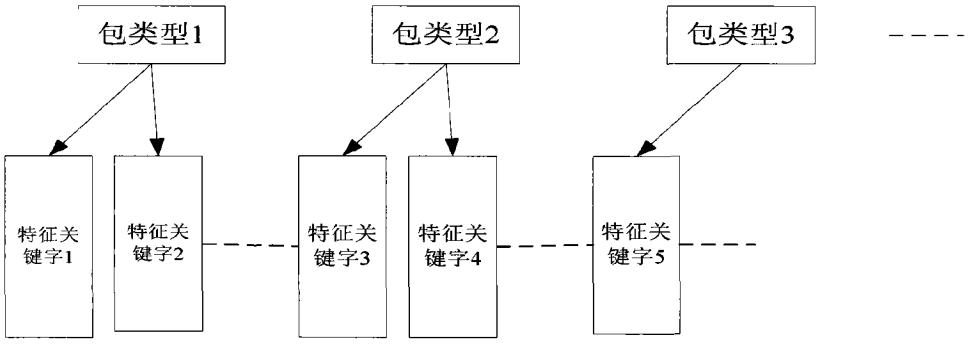

包类型1
包类型2
包类型3
特征关键字1
特征关键字2
特征关键字3
特征关键字4
特征关键字5

图 3