

## (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局

(43) 国际公布日  
2017 年 6 月 22 日 (22.06.2017)



(10) 国际公布号  
WO 2017/101656 A1

- (51) 国际专利分类号:  
H04L 12/24 (2006.01) H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/107199
- (22) 国际申请日: 2016 年 11 月 25 日 (25.11.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201510946845.4 2015 年 12 月 16 日 (16.12.2015) CN
- (71) 申请人: 网宿科技股份有限公司 (WANGSU SCIENCE & TECHNOLOGY CO., LTD.) [CN/CN]; 中国上海市徐汇区斜土路 2899 号甲光启文化广场 A 幢 5 楼, Shanghai 200030 (CN)。
- (72) 发明人: 洪珂 (HONG, Ke); 中国上海市徐汇区斜土路 2899 号甲光启文化广场 A 幢 5 楼, Shanghai 200030 (CN)。 陈文生 (CHEN, Wensheng); 中国上海市徐汇区斜土路 2899 号甲光启文化广场 A 幢 5 楼, Shanghai 200030 (CN)。 郑斌斌 (ZHENG, Binbin); 中国上海市徐汇区斜土路 2899 号甲光启文化广场 A 幢 5 楼, Shanghai 200030 (CN)。 陈文娟

(CHEN, Wenjuan); 中国上海市徐汇区斜土路 2899 号甲光启文化广场 A 幢 5 楼, Shanghai 200030 (CN)。 陈建坤 (CHEN, Jiankun); 中国上海市徐汇区斜土路 2899 号甲光启文化广场 A 幢 5 楼, Shanghai 200030 (CN)。

(74) 代理人: 北京华智则铭知识产权代理有限公司 (BEIJING HUA-WISDOM INTELLECTUAL PROPERTY INC.); 中国北京市大兴区宏业路 9 号院 7 号楼 1307 室, Beijing 100162 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA,

[见续页]

(54) Title: GRAPHICAL ANALYSIS METHOD AND SYSTEM FOR TCP TRANSMISSION DATA

(54) 发明名称: TCP 传输数据的图形化分析方法和系统

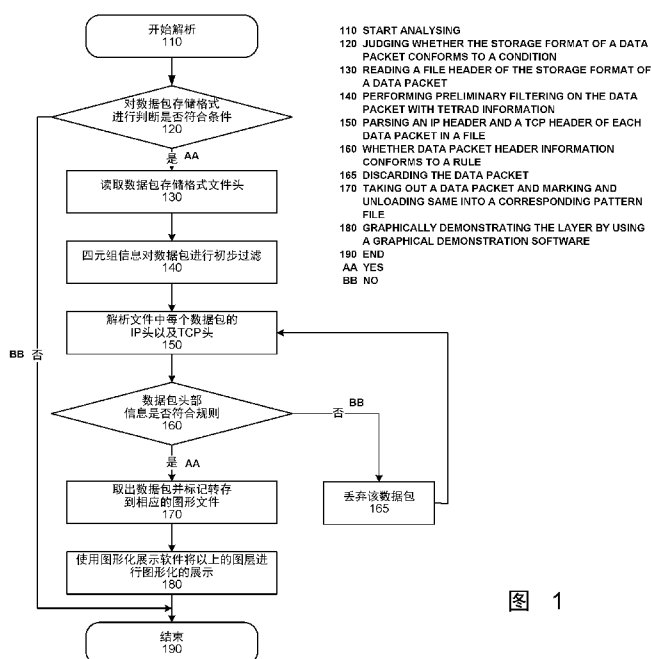


图 1

(57) Abstract: The present application relates to a graphical analysis method and system for a transport protocol data packet, especially for a TCP transport protocol data packet. The graphical analysis method comprises: judging the storage format of a transport protocol data packet to be analysed; if the storage format of the transport protocol data packet to be analysed is a supported storage format, extracting corresponding different data from the content of the read data packet and writing same into a corresponding graphic file; and graphically demonstrating the transmission process of the transport protocol data packet based on data read from the corresponding graphic file. Therefore, the graphical analysis method and system can demonstrate a data packet in as detailed a manner as possible by means of more steric graphical method, so that an analyser analyses an interaction process of a TCP protocol data packet in a segment of link more intuitively, thereby better discovering and solving the problem in a TCP protocol transmission process.

(57) 摘要: 本申请涉及一种用于传输协议数据包的数据包。所述图形化分析方法和系统, 特别针对 TCP 传输协议的数据包。所述图形化分析方法包括: 判断要分析的传输协议数据包的存储格式; 如果所述要分析的传输协议数据包的存储格式是支持的存储格式, 则从读取的数据包的内容中提取相应不同的

数据并将其写入到相应的图形文件中; 基于从相应的图形文件中读取的数据来图形化展示所述传输协议数据包的传输过程。因此, 所述图形化分析方法和系统能够尽可能地通过更加立体的图形化的方式将数据包尽可能详细的展示, 便于分析者更加直观的分析在一段链接之中 TCP 协议的数据包相互交互的过程, 更好发现和解决 TCP 协议传输过程中的问题。



RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG,

CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

## TCP 传输数据的图形化分析方法和系统

## 技术领域

本申请涉及对传输的数据包的分析，尤其涉及对基于 TCP 传输协议的数据包  
5 包的图形化分析。

## 背景技术

随着网络技术的高速发展，在计算机网络领域开发的网络应用软件也越来越多，在针对 TCP/IP 体系为核心的开发也逐渐成为热点，因此，在计算机网络  
10 络中传输的数据日趋呈现出多样性和复杂性，同时在网络中传输的数据中的某些问题也是日益的突出，网络传输中所出现的问题也是越来越复杂，但是目前对网络中的数据包的分析还是处于发展的阶段，相对于其他的数据分析技术来说还是比较落后的，尤其是对于特定的数据包，还无法提供比较令人满意的有针对性的专门性的分析工具以及方法。

其次，从产生和运用信息的载体来看，各种服务器对性能的不断追求造成服务器或软件架构多采用分布式、内容海量等特性，使得网络内部的数据量伴随着网络链接数量的增加而日趋复杂，因而针对复杂的网络环境以及巨大的网络数据量，各种越来越复杂的网络问题也是层出不穷。

虽然目前市场有很多相类似的分析基于网络传输协议的数据包中的问题  
20 的分析工具以及方法，例如最让我们熟悉的 wireshark 网络封包分析软件，虽然该工具很强大不仅能够捕获不同协议的数据包，同时能够应用各种的过滤规则过滤出不同类型的数据包，并呈现它们以让开发者进行分析，但是 wireshake 所呈现的数据包更加偏向于数据型的展示，它并不能很好地对经分析的数据进行图形化展示，例如将在一条 TCP 连接之中各种数据包的类型（例如重传包、  
25 ack 包、sack 包等）彼此之间区分开来。并且，由于 wireshake 是偏向数据型的展示，分析者只能通过复杂的过滤规则，过滤出相应的数据包，然后查看数据包挨个进行分析，这种分析不仅耗时而且容易造成视觉上的疲劳以及混乱，况且过滤规则较为复杂而且繁多，不利于初学者使用及分析。同时，针对 TCP 协议而言，过滤规则虽然能过滤出哪些数据包为客户端发送，哪些数据包为服务端发送，但是其过程比较繁琐，在对 TCP 链接重传分析时不能很直观地分辨  
30 出重传的数据包、ack 包以及 sack 包等，不能很直观地看出在 TCP 连接的各个阶段客户端与服务端的数据包的交互过程，对于由于 TCP 连接所出现的问题不能进行很直观地分析。

因此，需要一种能够解决上述各种问题以便提供更加直观、方便以及简洁的网络数据包的分析方法。

## 发明内容

5 本申请的目的在于解决在分析 TCP 传输协议的数据包时使用其他分析工具以及分析方法时所带来的各种不便利。

本申请是一种关于传输协议数据包的分析方法，特别针对 TCP 传输协议的数据包，能够尽可能地通过更加立体的图形化的方式将数据包尽可能详细的展示，便于分析者更加直观的分析在一段链接之中 TCP 协议的数据包相互交互的过程，更好发现和解决 TCP 协议传输过程中的问题。

10 根据本申请的一方面，提供了一种使用图形化分析工具对传输协议数据包进行图形化分析的方法，包括：

判断要分析的传输协议数据包的存储格式；

15 如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则执行下述步骤：

根据所述图形化分析工具所定义的数据包的存储格式的文件形式从文件读取相应数据包中的内容，其中所述读取包括：

通过在所述图形化分析工具所提供的用户界面中设置提取数据条件来允许开发者选择所想生成的数据包的类型；

20 根据所述开发者在所述用户界面中所设置的提取数据条件的不同，从读取的数据包的内容中提取相应不同的数据；

将所提取到的不同的数据写入到相应的图形文件中；

基于从相应的图形文件中读取的数据来图形化展示所述传输协议数据包的传输过程；

25 如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则结束所述方法。

根据本发明的另一方面，提供了一种使用图形化分析工具对传输协议数据包进行图形化分析的系统，包括：

用于判断要分析的传输协议数据包的存储格式的装置；

30 用于如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则执行下述处理的装置：

根据所述图形化分析工具所定义的数据包的存储格式的文件形式从文件读取相应数据包中的内容，其中所述读取包括：

通过在所述图形化分析工具所提供的用户界面中设置提取数据条件来允许开发者选择所想生成的数据包的类型；

5 根据所述开发者在所述用户界面中所设置的提取数据条件的不同，从读取的数据包的内容中提取相应不同的数据；

将所提取到的不同的数据写入到相应的图形文件中；

基于从相应的图形文件中读取的数据来图形化展示所述传输协议数据包的传输过程；

10 用于如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则结束所述方法的装置。

#### 附图说明

15 为了描述可获得本发明的上述和其它优点和特征的方式，将通过参考附图中示出的本发明的具体实施例来呈现以上简要描述的本发明的更具体描述。可以理解，这些附图只描绘了本发明的各典型实施例，并且因此不被认为是对其范围的限制，将通过使用附图并利用附加特征和细节来描述和解释本发明，在附图中：

20 图 1 示出根据实施例的 TCP 传输数据的图形化分析方法。

图 2 示出根据实施例的 TCP 传输图形化分析工具中用于选择想要生成的数据包类型的用户界面。

图 3 是经根据实施例的 TCP 传输数据的图形化分析方法处理过的不同类型的数据包的按照用户设置的条件的图形化分解展示图。

25

#### 具体实施方式

此处用细节来描述本申请的主题以满足法定要求。然而，该描述本身并非旨在限制本专利的范围。相反，发明人设想所要求保护的所针对的还可结合其他当前或未来技术按照其他方式来具体化，以包括不同的步骤或类似于本文中所描述的步骤的步骤组合。此外，尽管术语“步骤”和/或“框”可在此处用于指示所采用的方法的不同元素，但除非而且仅当明确描述了各个步骤的顺序

30 时，该术语不应被解释为意味着此处公开的各个步骤之中或之间的任何特定顺

序。

在本申请的一个实施例中，提供了一种 TCP 传输数据的图形化分析方法。通过该方法，一方面让开发者能够更好分析所抓取的数据包，以帮助问题的排查以及解决，另外一方面能够使初学者更容易上手，无需花费大量的时间去学习分析工具的使用。

具体而言，由于 TCP 协议是目前一种主流的协议，提供的是一种可靠的数据流服务，采用“带重传的肯定确认”技术来实现传输的可靠性。目前网络中数据包之间相互的发送基本使用 TCP 协议，还采用一种称为“滑动窗口”的方式进行流量控制，所谓窗口实际表示接收能力，用以限制发送方的发送速度。因而 TCP 协议会更加的复杂，分析问题会更加的困难，因此，需要一种更加直观，简便又能完美解决问题的协议分析工具。同时，为了能够更好的面对网络所层出不穷的复杂的问题，同时也为了帮助人们更好的强化了解 TCP 传输协议，利用该方法对 TCP 协议进行分析，将能够很好的展现数据包的整体传输过程，让开发者能够更加直观的了解整体网络的工作原理。应对基于 TCP 协议体系中所发生的各种问题，本申请所研发的 TCP 传输图形化分析方法能够很好地弥补上述缺点，帮助开发者在工作过程中对问题的分析和解决。但需要理解的是本申请的方案并不局限于使用 TCP 传输协议传输数据，实际上任何其它合适的数据通信协议都可以应用于本申请的图形化方案中。

首先，参见图 1，在图 1 中示出了根据实施例的 TCP 传输数据的图形化分析方法 100。所述方法在步骤 110 开始解析。在步骤 120 处，所述方法在分析基于 TCP 传输协议的数据包之前首先对该数据包的存储格式进行判断。目前主流的 TCP 协议的数据包的存储格式为 .pcap .cap，甚至可以支持 .log 日志类型的数据包的存储格式。在本申请中主要是以 pcap 格式的数据包作为示例来进行具体说明，但应该理解的是其它数据存储格式也同样可以应用于本申请。使用 pcap 的数据包的格式原因在于抓取该种格式的数据包的抓取工具能够从网卡中捕获原始数据包，这些数据包包括共享网络上的各主机所发送/接收的以及相互之间交换的数据包。同时在数据包发往应用程序之前，可以按照自定义的规则将某些特殊的数据包过滤掉，基于其灵活的规则可以更有针对性地将涉及网络问题的数据包进行抓包，以配合该 TCP 图形化的分析方法，使问题的分析更加具有针对性。同时，目前大多数从 TCP 链接所抓取的数据包也几乎都是 pcap 格式的。本申请的抓取工具支持使用 wireshark, tcpdump 等这些主流的抓包软件来抓取有关于 TCP 协议的数据包。因此，接下去的步骤中的所有代码文件都是根据 pcap 的文件头的形式去读取。在步骤 120 中，如果抓取的数据包的格式是分析工具所支持的存储格式，例如 pcap 格式，则方法行

进到步骤 130, 否则, 所述方法到达结束 190 处, 整个流程结束。在步骤 130-170 中, 根据所述分析工具中预定义的数据包的存储格式的文件形式从文件读取相应数据包中的数据, 为后续的 TCP 传输协议的数据包分析和图形化展示做准备。如上所述, 由于所述数据包是 pcap 这种格式的数据包, 所以在读取该数据包的内容时所述方法是严格按照 pcap 数据包中所拥有的格式去读取相应的数据。

为了便于技术人员更好地理解所述数据包的数据提取和解析处理, 下面以 pcap 文件格式的数据包为例进行详细举例说明。

pcap 文件的格式为:

文件头      24 字节

10      数据包头 + 数据包    (数据包头为 16 字节, 后面紧跟数包)

数据包头 + 数据包    .....

在 pcap 的文件头中包含了文件版本号, 文件长度等, 本申请的工具有会先读取 pcap 文件格式的文件头 (步骤 130) 以确定文件版本号, 文件长度等信息, 并判断是否为 pcap 格式的数据包以确定接下去对数据包的解析是否按照 pcap 文件的形式进行。

在读取文件头确定了使用 pcap 的文件格式之后, 读取数据包报头的信息, 数据包报头的信息包含抓取的时间和包的总长度以及抓取的长度等并作相应的记录以便最终在所呈现的图形化的界面之中进行展示

如图 2 所示, 开发者可以利用图形化分析方法所提供的用户界面来选择开发者所想生成的数据包的类型, 所述类型包括服务端发送的正常的数据包、重传包, 以及客户端所发送的诸如确认包和 sack 包之类的包。同时, 在此用户界面中, 开发者可以设置接下去所呈现的数据包的时间单位、发送 IP、发送端口、接收 IP、接收端口、速度等等与提取有关的参数。需要注意的是, 图 2 中的用户界面所示出的参数仅仅是用于说明性目的, 并非局限于此。本领域的技术人员完全可以根据提取数据的需求, 采用其它参数来过滤需要从数据包中提取的数据。当开发者在所述用户界面中设置完所述参数之后, 所述方法就根据开发者在用户界面中所设置的提取数据条件的不同, 从读取的数据包的内容中提取相应不同的数据。例如, 用户可以在 TCP 传输图形化分析工具的界面中选取工具从数据包之中所初步得到的源 IP 目的 IP, 源端口和目的端口, 选定之后根据所选定的四元组信息, 对 pcap 文件中的数据包进行初步过滤 (步骤 140), 选取符合以上选定的四元组的数据包进行再一次的加工和读取。

工具首先会对所选定的数据包进行一个初步解析的过程, 解析数据包之中所包含的 IP 头以及 TCP 头 (步骤 150), 并判断数据包中 IP 头以及 TCP 头中的信息是否符合服务端发送的正常的数据包, 重传包, 以及客户端所发送的 ack

包以及 sack 包的在工具中所设定的规则（步骤 160），若是判断符合某一类型的数据，就将该数据包取出并进行标记然后转存到相应的图形文件中（步骤 170）。目前将服务端所发送的正常的数据包以及重传包记录到同一个图形文件中，所述写入是例如严格按照 GIS 软件所能识别的文件格式写入的，并将提取的数据分别写入到不同的图层之中。例如，ack 包和 sack 包记录到另外一个图形文件中，并使用是 type 以及时间序列去打上标记，为接下去图形化界面的正确显示打下基础。而如果判断符合某一类型的数据，就将该数据包丢弃（步骤 165）。随后，方法前进到步骤 180，在此，所述 GIS 软件基于从特定文件中读取的内容来进行图形化展示以体现 TCP 传输数据包的过程以便于开发者的分析以及理解。

同时可以根据从文件中读取到相关信息，计算出在发包的速率，即在一定的时间段内能够在网络中发多少的数据包，并生成又一个图形文件，可以很好的展示网络的拥堵情况。在所述工具解析数据包生成以上相应的图形文件之后，使用图形化展示软件（例如 GIS 软件）将以上的图层进行图形化的展示。在完成所有以上操作之后，流程在步骤 190 结束。

当前示例中所使用的图形化的展示软件是以 GIS（地理信息系统）为基础所开发的软件。

地理信息系统（GIS, Geographic Information System）是一门综合性学科，结合地理学与地图学以及遥感和计算机科学，已经广泛地应用在不同的领域，是用于输入、存储、查询、分析和显示地理数据的计算机系统。随着 GIS 的发展，也称 GIS 为“地理信息科学”（Geographic Information Science），近年来，还称 GIS 为“地理信息服务”（Geographic Information service）。GIS 是一种基于计算机的工具，它可以对空间信息进行分析和处理（简而言之，是对地球上存在的现象和发生的事件进行成图和分析）。GIS 技术把地图这种独特的视觉化效果和地理分析功能与一般的数据库操作（例如查询和统计分析等）集成在一起。

目前 GIS 主要应用在环境监测，资源调查，监测预测，城市规划，军事，城市电网，金融业、保险业、公共事业、社会治安、运输导航、考古、医疗救护等领域得到了广泛的应用。所以，将 GIS 与网络数据包的分析结合在一起相互配合，也是一次很好的尝试。

在图 3 中，则展示了按照用户设置的条件的图形化分解展示图。在所述示图中，根据开发者在 GIS 软件中所设的过滤的条件不同，所述方法可以将一个 pcap 的数据包中 TCP 传输链接的情况分为不同的图层，在这些图层中我们重点关注的有两个图层。为了使得这两个图层中的不同类型的数据包更加容易



被区分开来，将图 3 中右下方进一步示出了其中的一部分的局部放大图，以方便进行说明。

第一个图层代表发送端发送数据包的情况为如何，如图 3 中所示的较深点线段 1 代表发送端正常发送的数据包，而图 3 中的深色实线段 2 表示发送端重传的数据包，具体的图形化的表示可以参照图 3。另外，在图 3 中横轴代表时间即图中从左至右的顺序表示时间从早到晚，竖轴代表数据包的时间序列号即图中从下至上的顺序表示时间序列号从小到大，使用者可以进行放大或者缩小来查看数据包的具体情况，若想查看具体的数据也可以使用相关的按钮进行查看每个数据包之中所包含的具体的数据。需要说明的是，图中的每一类型的数据包可以使用不同颜色的线状图形进行表示，图 3 中所示的仅仅是示例说明，具体而言，该工具可以将正常发送的数据包以及重传的数据包根据个人的意愿使用不同的颜色进行标记不是仅仅局限于上述所表明的两种颜色，这样可以让使用者更加一目了然地查看当时发送端发送数据的情况以及当时的网络情况等等。

第二个图层代表了接收端所发送的 ack 以及 sack 包的情况，如图 3 所示的较浅实线段 10 代表接收端所发送的正常的 ack 包，而较浅点线段 11 代表了接收端发送的 sack 包。同理具体想选用什么颜色以及怎样的线条来进行表示可以根据使用者个人的意愿进行自主的选择，在分析 tcp 连接的传输情况时，可以将几个图层进行全部的勾选进行分析，同时亦可单独分开勾选图层以分别显示来进行分析，这个根据使用者的具体情况而定。

通过观看上述图形化展示，使得开发者可以很容易地掌控数据包在 TCP 传输过程中的情况，发现当中可能存在的问题并加以解决。

综上所述，本申请提供了一种新颖的 TCP 传输数据的图形化分析方法，所述方法针对目前市场所存在数据包的分析方法做了一些改进，主要的改进点在于：

以一种更加直观的图形化的方式，将 TCP 协议中客户端与服务端的数据包的相互的交互过程体现出来，使人能够对所述过程更加一目了然以便于分析；

将所抓取的某条 TCP 链接的数据包中的数据进行分类拆分，统计记录统计出各中数据包的传输情况，并将这条链接之中各种数据包换成 GIS 地图软件所能识别并读取的文件，然后使用 GIS 地图软件将不同连接的传输情况使用不同的图层表示，并且可以根据自主的意愿将不同类型的数据包标记为不同的颜色、阴影线、网格、形状或线条等进行表示，这样不仅能够更清楚地明白不同链接的传输情况便于分析各个链接中所出

现的问题，同时也增加了自主的选择性，更加便于人们的理解。

尽管用结构特征和/或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于上述特征或动作或上述动作的次序。更具体而言，所描述的特征和动作是作为实现权利要求书的示例形式而公开的。

- 5 本申请可具体化为其它具体形式而不背离其精神或本质特征。所描述的实施例在所有方面都应被认为仅是说明性而非限制性的。因此，本申请的范围由所附权利要求书而非前述描述指示。落入权利要求书的等效方案的含义和范围内的所有改变都被权利要求书的范围所涵盖。

# 权 利 要 求 书

1. 一种使用图形化分析工具对传输协议数据包进行图形化分析的方法，其特征在于，包括：

判断要分析的传输协议数据包的存储格式；

5 如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则执行下述步骤：

根据所述图形化分析工具所定义的数据包的存储格式的文件形式从文件读取相应数据包中的内容，其中所述读取包括：

10 通过在所述图形化分析工具所提供的用户界面中设置提取数据条件来允许开发者选择所想生成的数据包的类型；

根据所述开发者在所述用户界面中所设置的提取数据条件的不同，从读取的数据包的内容中提取相应不同的数据；

将所提取到的不同的数据写入到相应的图形文件中；

15 基于从相应的图形文件中读取的数据来图形化展示所述传输协议数据包的传输过程；

如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则结束所述方法。

2. 如权利要求 1 所述的方法，其特征在于，所述传输协议数据包是基于 TCP 传输协议的数据包。

20 3. 如权利要求 2 所述的方法，其特征在于，所述基于各种传输协议的数据包的存储格式为 .pcap、.cap，甚至可以支持 .log 日志类型的数据包的存储格式。

4. 如权利要求 1 所述的方法，其特征在于，所述要分析的传输协议数据包是由抓包软件从各种的网络环境中抓取，其中所述抓包软件是 wireshark，  
25 tcpdump 等。

5. 如权利要求 1 所述的方法，其特征在于，所述数据包的类型包括服务端发送的正常的数据包、重传包，以及客户端所发送的诸如 ACK 包和 sack 包之类的包。

6. 如权利要求 1 所述的方法，其特征在于，所述将所提取到的符合不同条

件的数据包取出并进行标记然后转存到相应的图形文件中，其中转存到相应的图形文件中是按照 GIS 软件所能识别的文件格式写入的，并将提取到的不同的数据分别写入到不同的图层之中并打上相应的 type 的标志。

7. 如权利要求 3 所述的方法，其特征在于，所述基于从相应的图形文件中读取的数据来图形化展示所述传输协议数据包的传输过程的步骤包括：根据使用者所设的过滤的条件不同，所述图形化分析工具可以将某一类型数据包的存储格式的数据包中 TCP 传输链接的情况分为不同的图层来显示。

8. 一种使用图形化分析工具对传输协议数据包进行图形化分析的系统，其特征在于，包括：

10 用于判断要分析的传输协议数据包的存储格式的装置；

用于如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则执行下述处理的装置：

根据所述图形化分析工具所定义的数据包的存储格式的文件形式从文件读取相应数据包中的内容，其中所述读取包括：

15 通过在所述图形化分析工具所提供的用户界面中设置提取数据条件来允许开发者选择所想生成的数据包的类型；

根据所述开发者在所述用户界面中所设置的提取数据条件的不同，从读取的数据包的内容中提取相应不同的数据；

将所提取到的不同的数据写入到相应的图形文件中；

20 基于从相应的图形文件中读取的数据来图形化展示所述传输协议数据包的传输过程；

用于如果所述要分析的传输协议数据包的存储格式是支持的存储格式，则结束所述方法的装置。

25

## 说明书附图

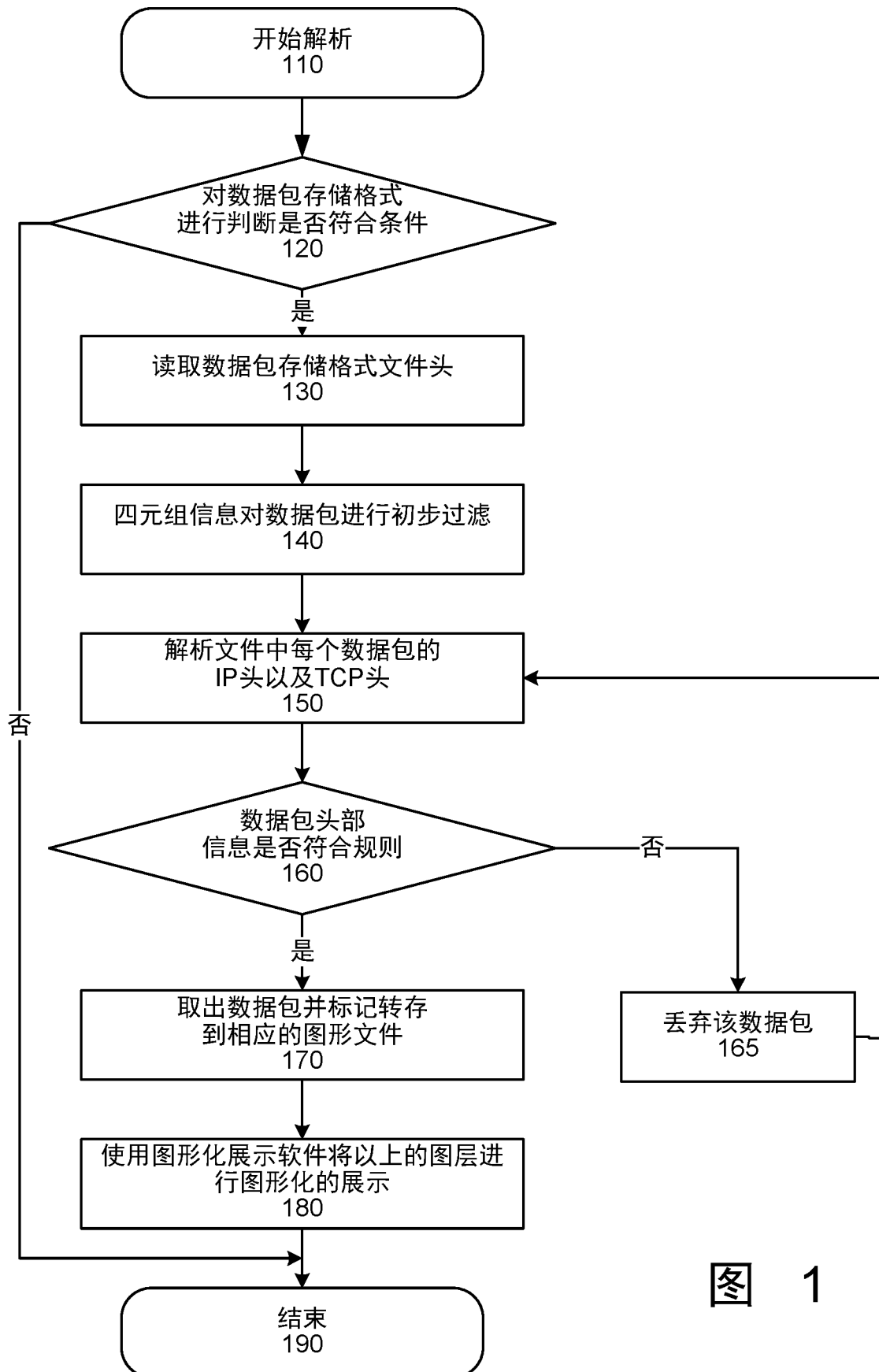


图 1

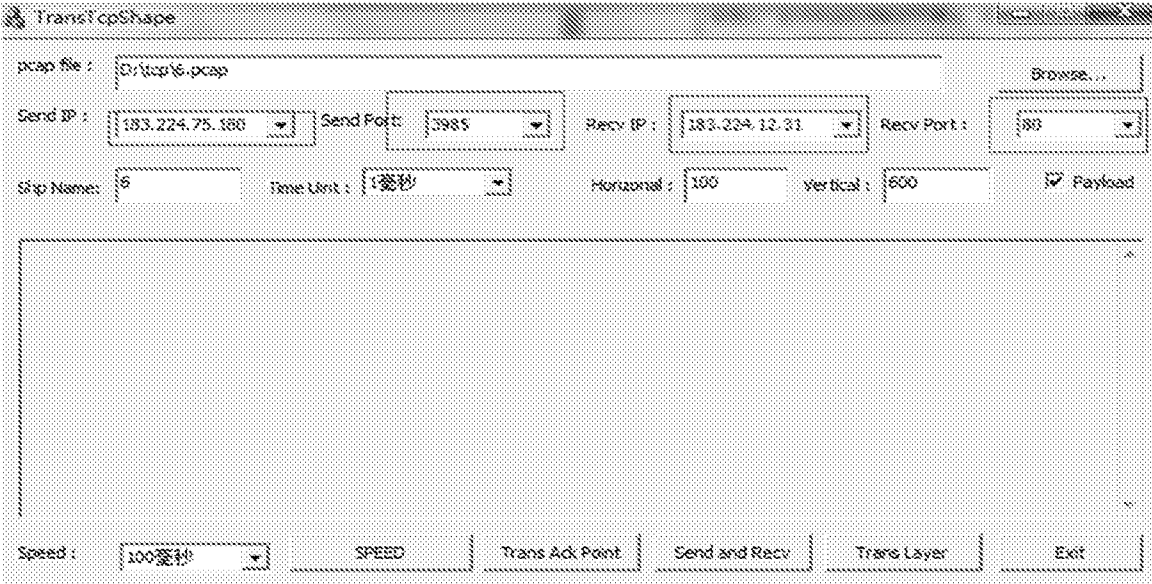


图 2

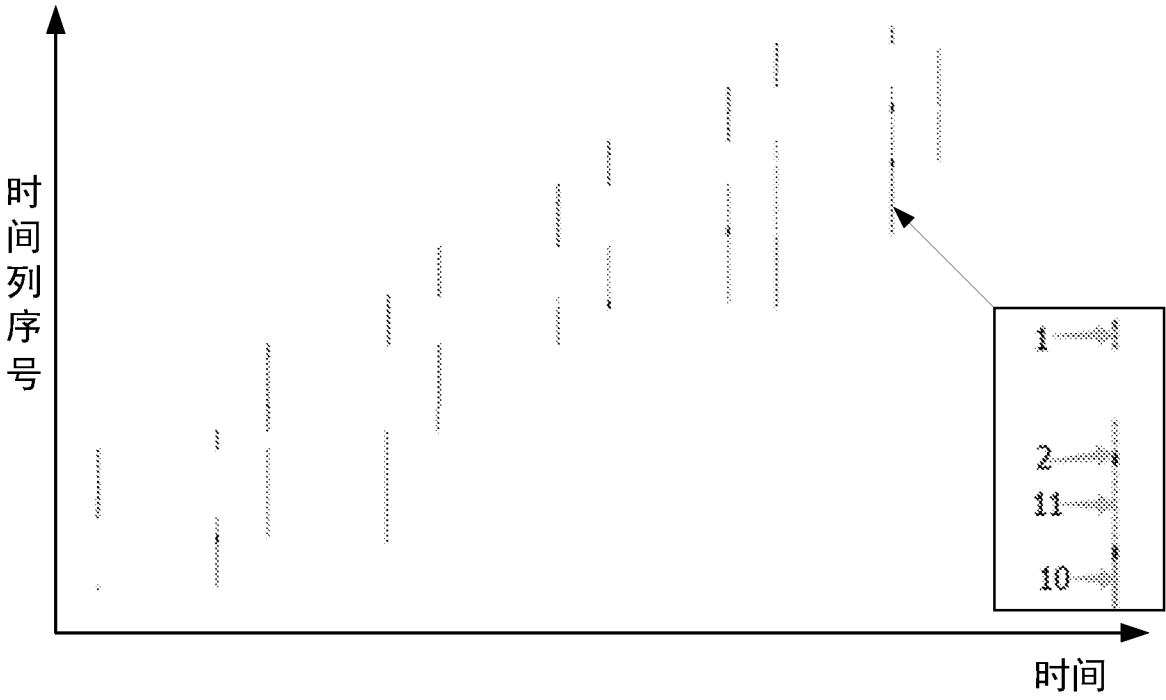


图 3

# INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CN2016/107199**

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (2006.01) i; H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNTXT; VEN; CNKI: imaging, colour, virtualized, graphical, data, transmit, analyze, filter, color

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                             | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | CN 102970189 A (BEIJING RUN TECHNOLOGY CO., LTD.), 13 March 2013 (13.03.2013), description, paragraphs [0006]-[0012]                           | 1-8                   |
| PX        | CN 105610604 A (SHANGHAI CHINANETCENTER TECHNOLOGY CO., LTD.), 25 May 2016 (25.05.2016), claims 1-8, and description, paragraphs [0006]-[0053] | 1-8                   |
| A         | CN 102244610 A (CSS & JLU INFO-TECH CO., LTD.), 16 November 2011 (16.11.2011), the whole document                                              | 1-8                   |
| A         | CN 104394021 A (CENTRAL SOUTH UNIVERSITY), 04 March 2015 (04.03.2015), the whole document                                                      | 1-8                   |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

|                                                                                                                                                                         |                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * Special categories of cited documents:                                                                                                                                | “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention                                              |
| “A” document defining the general state of the art which is not considered to be of particular relevance                                                                | “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone                                                                     |
| “E” earlier application or patent but published on or after the international filing date                                                                               | “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | “&” document member of the same patent family                                                                                                                                                                                                    |
| “O” document referring to an oral disclosure, use, exhibition or other means                                                                                            |                                                                                                                                                                                                                                                  |
| “P” document published prior to the international filing date but later than the priority date claimed                                                                  |                                                                                                                                                                                                                                                  |

|                                                                                                                                                                                                                    |                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Date of the actual completion of the international search<br>06 February 2017 (06.02.2017)                                                                                                                         | Date of mailing of the international search report<br><b>02 March 2017 (02.03.2017)</b> |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br><b>BAI, Tan</b><br>Telephone No.: (86-10) <b>62411245</b>         |



International application No.  
**PCT/CN2016/107199**

Form PCT/ISA/210 (patent family annex) (July 2009)

| <b>A. 主题的分类</b><br>H04L 12/24(2006.01)i; H04L 29/06(2006.01)i<br><br>按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                          |                                            |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------|------|-------------------|---------|---|---------------------------------------------------------------------------------|-----|----|------------------------------------------------------------------------------------------|-----|---|----------------------------------------------------------------------|-----|---|----------------------------------------------------------|-----|
| <b>B. 检索领域</b><br>检索的最低限度文献(标明分类系统和分类号)<br>H04L<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))<br>CPRSABS;CNTXT;VEN;CNKI:图形化, 图像化, 可视化, 数据, 传输, 分析, 过滤, 颜色, 着色, virtualized, graphical, data, transmit, analyze, filter, color                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                          |                                            |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| <b>C. 相关文件</b> <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 102970189 A (北京锐安科技有限公司) 2013年 3月 13日 (2013 - 03 - 13)<br/>说明书第[0006]-[0012]段</td> <td>1-8</td> </tr> <tr> <td>PX</td> <td>CN 105610604 A (网宿科技股份有限公司) 2016年 5月 25日 (2016 - 05 - 25)<br/>权利要求1-8, 说明书第[0006]-[0053]段</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 102244610 A (吉林中软吉大信息技术有限公司) 2011年 11月 16日 (2011 - 11 - 16)<br/>全文</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 104394021 A (中南大学) 2015年 3月 4日 (2015 - 03 - 04)<br/>全文</td> <td>1-8</td> </tr> </tbody> </table> |                                                                                          |                                            | 类 型* | 引用文件, 必要时, 指明相关段落 | 相关的权利要求 | X | CN 102970189 A (北京锐安科技有限公司) 2013年 3月 13日 (2013 - 03 - 13)<br>说明书第[0006]-[0012]段 | 1-8 | PX | CN 105610604 A (网宿科技股份有限公司) 2016年 5月 25日 (2016 - 05 - 25)<br>权利要求1-8, 说明书第[0006]-[0053]段 | 1-8 | A | CN 102244610 A (吉林中软吉大信息技术有限公司) 2011年 11月 16日 (2011 - 11 - 16)<br>全文 | 1-8 | A | CN 104394021 A (中南大学) 2015年 3月 4日 (2015 - 03 - 04)<br>全文 | 1-8 |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 引用文件, 必要时, 指明相关段落                                                                        | 相关的权利要求                                    |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CN 102970189 A (北京锐安科技有限公司) 2013年 3月 13日 (2013 - 03 - 13)<br>说明书第[0006]-[0012]段          | 1-8                                        |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| PX                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | CN 105610604 A (网宿科技股份有限公司) 2016年 5月 25日 (2016 - 05 - 25)<br>权利要求1-8, 说明书第[0006]-[0053]段 | 1-8                                        |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CN 102244610 A (吉林中软吉大信息技术有限公司) 2011年 11月 16日 (2011 - 11 - 16)<br>全文                     | 1-8                                        |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CN 104394021 A (中南大学) 2015年 3月 4日 (2015 - 03 - 04)<br>全文                                 | 1-8                                        |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                          |                                            |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“P” 公布日先于国际申请日但迟于所要求的优先权日的文件<br>“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件<br>“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性<br>“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性<br>“&” 同族专利的文件                                                                                                                                                                                                                                              |                                                                                          |                                            |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| 国际检索实际完成的日期<br><br>2017年 2月 6日                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                          | 国际检索报告邮寄日期<br><br>2017年 3月 2日              |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |
| ISA/CN的名称和邮寄地址<br>中华人民共和国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                          | 受权官员<br><br>白坦<br><br>电话号码 (86-10)62411245 |      |                   |         |   |                                                                                 |     |    |                                                                                          |     |   |                                                                      |     |   |                                                          |     |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2016/107199

| 检索报告引用的专利文件 |           |   | 公布日<br>(年/月/日) | 同族专利           | 公布日<br>(年/月/日) |
|-------------|-----------|---|----------------|----------------|----------------|
| CN          | 102970189 | A | 2013年 3月 13日   | CN 102970189 B | 2016年 6月 29日   |
| CN          | 105610604 | A | 2016年 5月 25日   | 无              |                |
| CN          | 102244610 | A | 2011年 11月 16日  | 无              |                |
| CN          | 104394021 | A | 2015年 3月 4日    | 无              |                |