

(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



(10) 国际公布号
WO 2013/152672 A1

(43) 国际公布日
2013年10月17日 (17.10.2013)

- (51) 国际专利分类号:
H04L 12/26 (2006.01) H04L 9/00 (2006.01)
G06F 21/00 (2013.01)
- (21) 国际申请号: PCT/CN2013/073357
- (22) 国际申请日: 2013年3月28日 (28.03.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210101792.2 2012年4月9日 (09.04.2012) CN
- (71) 申请人: 腾讯科技(深圳)有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园2栋东403室, Guangdong 518000 (CN)。
- (72) 发明人: 吴家旭 (WU, Jiayu); 中国广东省深圳市福田区振兴路赛格科技园2栋东403室, Guangdong 518000 (CN)。 于涛 (YU, Tao); 中国广东省深圳市福田区振兴路赛格科技园2栋东403室, Guangdong 518000 (CN)。
- (74) 代理人: 深圳翼盛智成知识产权事务所(普通合伙) (ESSEN PATENT & TRADEMARK AGENCY);

中国广东省深圳市福田区天安数码城数码时代大厦A座1409, Guangdong 518040 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, RW, SD, SL, 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, 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))。

(54) Title: METHOD AND DEVICE FOR MONITORING VIRUS TREND ABNORMALITY

(54) 发明名称: 病毒趋势异常的监控方法及装置

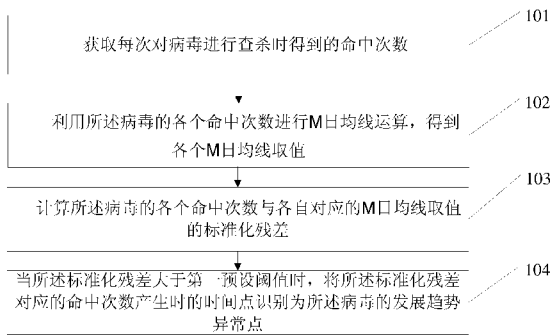


图1 / Fig. 1

101 ACQUIRE THE NUMBER OF HITS THAT IS OBTAINED WHEN A VIRUS IS SCANNED AND REMOVED EACH TIME
 102 PERFORM M-DAY MOVING AVERAGE CALCULATION BY USING EACH NUMBER OF HITS OF THE VIRUS, SO AS TO OBTAIN EACH M-DAY MOVING AVERAGE VALUE
 103 CALCULATE A STANDARDIZED RESIDUAL BETWEEN EACH NUMBER OF HITS OF THE VIRUS AND A CORRESPONDING M-DAY MOVING AVERAGE VALUE
 104 WHEN THE STANDARDIZED RESIDUAL IS LARGER THAN A FIRST PRESET THRESHOLD, IDENTIFY A TIME POINT OF GENERATING THE NUMBER OF HITS THAT IS CORRESPONDING TO THE STANDARDIZED RESIDUAL AS A GROWING TREND ABNORMALITY POINT OF THE VIRUS

(57) Abstract: A method and device for monitoring virus trend abnormality are used for timely and effectively monitoring various viruses. The method comprises: acquiring the number of hits that is obtained when a virus is scanned and removed; calculating each M-day moving average value of the number of hits; calculating a standardized residual of the number of hits; and when the standardized residual is larger than a first preset threshold, identifying time of the number of hits as a growing trend abnormality point of the virus.

(57) 摘要: 一种病毒趋势异常的监控方法及装置, 用于对各种病毒进行及时有效的监控。该方法包括: 获取查杀病毒时得到的命中次数; 计算所述命中次数的各个M日均线取值; 计算所述命中次数的标准化残差; 当所述标准化残差大于第一预设阈值时, 将所述命中次数的时间识别为所述病毒的发展趋势异常点。



WO 2013/152672 A1

说明书

病毒趋势异常的监控方法及装置

技术领域

本发明涉及计算机技术领域，尤其涉及一种病毒趋势异常的监控方法及装置。

背景技术

目前，通过杀毒引擎对计算机病毒进行定期查杀，可以在一定程度上制约病毒的增长。当杀毒引擎对某一种病毒的查杀能力在一个很短时间内严重偏离原先的趋势时，则说明可能存在如下异常状况：如果查杀出这种病毒的数量剧增，说明短时间内这种病毒可能会大规模爆发；如果查杀出这种病毒的数量锐减，说明杀毒引擎对这种病毒的识别能力可能降低甚至丧失、抑或这种病毒开始变种。因此，对病毒发展趋势是否存在异常进行有效监控，并在监控到病毒发展趋势存在异常时，及时进行预警，对防止病毒的大规模爆发具有重要意义。

现有技术中，当病毒种类很少的时候，可以通过技术人员的经验来主观判断病毒的发展趋势是否存在异常。但随着病毒种类成千上万的猛增，通过人工对病毒发展趋势是否存在异常进行监控，将会耗费大量的人力，并且也难以满足有效监控的需求。

于是，现有技术出现了一种基于病毒样本数量或病毒样本增长幅度的监控方法，对每个病毒设定对应的阈值，通过监控病毒样本数量是否大于一个阈值，或者监控病毒样本增长幅度是否大于一个阈值，来判断病毒发展趋势是否存在异常。然而，对新病毒或变种病毒无法实现及时有效的监控。

发明内容

本发明的实施例提供一种病毒趋势异常的监控方法及装置，实现对各种病毒进行及时有效的监控。

为达到上述目的，本发明的实施例采用如下技术方案：

一方面，提供一种病毒趋势异常的监控方法，包括：

获取每次对病毒进行查杀时得到的命中次数；

利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，所述 M 为正整数；

计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差；

当所述标准化残差大于第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

另一方面，提供一种病毒趋势异常的监控装置，包括：

获取模块，用于获取每次对病毒进行查杀时得到的命中次数；

运算模块，用于利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，所述 M 为正整数；

所述运算模块，还用于计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差；

识别模块，用于当所述标准化残差大于第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

由上述技术方案所描述的本发明实施例中，通过利用所述病毒的各个命中次数进行 7 日均线运算，得到各个 7 日均线取值，并计算所述病毒的各个命中次数与各自对应的 7 日均线取值的标准化残差，由于上述结合 7 日均线

运算所得到的各个标准化残差符合正态分布，因而采用置信区间可以准确判断出每次对病毒进行查杀时得到的命中次数是否存在异常，进而判断出病毒趋势是否存在异常。例如，将上述第一预设阈值设置为置信区间 95%对应的 1.96，即可在所述标准化残差大于所述第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

可见，本发明实施例中在监控病毒趋势是否存在异常时，上述第一预设阈值可根据不同的置信区间进行确定，与现有技术相比，本发明实施例不需要大量的历史数据来确定上述第一预设阈值，因而对新病毒和变种病毒也可以进行准确的监控。并且，每当获取到对病毒进行查杀时得到的最新命中次数时，即可采用本发明提供的方法进行判断，如果计算出所述病毒的最新命中次数与对应的 7 日均线取值的标准化残差大于第一预设阈值时，即说明所述病毒的最新的命中次数存在异常，因而，可实现对各种病毒进行及时有效的监控。

附图说明

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一些实施例，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，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例 1 提供一种病毒趋势异常的监控方法的流程图；

图 2 为本发明实施例 1 提供一种病毒趋势异常的监控方法中步骤 103 的实现流程图；

图 3 为本发明实施例 1 提供另一种病毒趋势异常的监控方法的流程图；

图 4 为本发明实施例 1 提供又一种病毒趋势异常的监控方法的流程图；

图 5 为采用本发明实施例提供的监控方法对病毒的趋势进行监控，没有监控到异常的效果示意图；

图 6 为采用本发明实施例提供的监控方法对病毒的趋势进行监控，监控到异常并报警的效果示意图；

图 7 为采用本发明实施例提供的监控方法对病毒的趋势进行监控，监控到异常并报警的另一效果示意图；

图 8 为采用本发明实施例提供的图 4 所示的监控方法对病毒的趋势进行监控，由于不满足条件 $C_{N+1} > \lambda$ 而没有进行过报警的效果示意图；

图 9 为验证采用本发明实施例提供的方法计算出的标准化残差符合正态分布的结果示意图；

图 10 为本发明实施例 2 提供一种病毒趋势异常的监控装置的结构图；

图 11 为本发明实施例 2 提供一种病毒趋势异常的监控装置的另一结构图；

图 12 为本发明实施例 2 提供一种病毒趋势异常的监控装置的又一结构图。

具体实施方式

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作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。

采用病毒引擎周期性地对病毒进行查杀时，不同的病毒引擎可以查杀的

病毒种类也不相同。对于每一种病毒，无论是已有病毒，或者变种病毒、或者新增病毒，均可以采用本发明实施例提供的如下方法来监控每一种病毒的发展趋势。下文中，以一种病毒为例，来详细说明病毒趋势异常的监控方法。

如图 1 所示，本发明实施例提供一种病毒趋势异常的监控方法，包括：

101、获取每次对病毒进行查杀时得到的命中次数。

需要说明的是，当病毒引擎每次对病毒进行查杀后，可将获得的该病毒的各个命中次数按照查杀时间由早到晚的次序存放在数据库中。该病毒的每个命中次数可按照“病毒引擎标识-病毒标识-日期-时间点-命中次数”的格式进行存放。

例如，采用病毒引擎 A 在 2012 年 2 月 21 日的 12:08 分对病毒 B 进行查杀后，得到该病毒 B 的最新命中次数为 3354，假设之前在数据库中已经存放的该病毒 B 的命中次数的总数为 N，且前 N 个命中次数已按照查杀时间由早到晚的次序进行存放，那么可知该病毒的最新命中次数为第 N+1 个，此时，可将该病毒的第 N+1 个命中次数按照“病毒引擎 A-病毒 B-2012 年 2 月 21 日-12:08 -3354”的格式，并存放在数据库中记录有该病毒引擎 A 对病毒 B 进行上一次查杀时得到的第 N 个命中次数之后。

具体地，在对病毒的趋势进行监控时，可以从数据库中获取一定周期内每次对病毒进行查杀时得到的命中次数，或者获取所有周期内每次对病毒进行查杀时得到的命中次数。

可选的，为了可以对病毒的趋势进行及时有效的监控，本发明实施例从数据库中获取病毒最新的前 N+1 个命中次数，其中第 N+1 个命中次数表示最新一次对病毒进行查杀后得到的命中次数。N 的取值可以为大于 90 的正整数。

102、利用所述病毒的各个命中次数进行 M 日（例如，7 日）均线运算，

得到各个 M 日均线取值。其中，M 为正整数。本发明的实施例中，以 M=7 来举例说明，当然，M 也可以取值为 4、5、6、8、9、10、11 等等数值。

具体地，根据 $B_i = \frac{1}{M} \sum_{j=0}^M A_{i-j}$ 计算各个 M 日均线取值，其中， B_i 为利用所述病毒的第 i 个命中次数到第 i-M+1 个命中次数计算得到的 M 日均线取值， $i \in [MK N+1]$ 且 i 为正整数，N+1 为所述病毒的命中次数的总数， A_{i-j} 为所述病毒的第 i-j 个命中次数。

103、计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差。

具体地，如图 2 所示，本步骤通过如下子步骤实现：

103-1、根据 $C_i = A_i - B_i$ 计算残差。

其中， C_i 为所述病毒的第 i 个命中次数与利用所述病毒的第 i 个命中次数到第 i-M+1 个命中次数计算得到的 M 日均线取值的残差， A_i 为所述病毒的第 i 个命中次数， B_i 为利用所述病毒的第 i 个命中次数到第 i-M+1 个命中次数计算得到的 M 日均线取值， $i \in [MK N+1]$ 且 i 为正整数，N+1 为所述病毒的命中次数的总数。

103-2、根据 $E = \frac{1}{N - \max(M, N - L)} \sum_{i=\max(M, N-L)}^N C_i$ 计算残差的均值。

其中，E 为所述病毒的各个命中次数对应的残差的均值， $L \in [1K N]$ 且 L 为正整数。

实际应用时，该 L 的取值可以为 90，亦即使用最新的前 N 个命中次数中的前 90 个命中次数计算得到的残差作为标准数据，来对第 N+1 个命中次数是否存在异常进行监控。

103-3、根据 $S = \frac{1}{N - \max(M, N - L) - 1} \sum_{i=\max(M, N-L)}^N (C_i - E)^2$ 计算残差的标准差。

其中， S 为所述病毒的各个命中次数对应的残差的标准差。

103-4、根据 $D_{N+1} = \frac{C_{N+1} - E}{S}$ 计算所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差。

其中， D_{N+1} 为所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差， C_{N+1} 为所述病毒的第 $N+1$ 个命中次数与利用所述病毒的第 $N+1$ 个命中次数到第 $N-M+2$ 个命中次数计算得到的 M 日均线取值的残差。

104、当所述标准化残差大于第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

具体地，当 $D_{N+1} > \omega_1$ 时，将所述病毒的第 $N+1$ 个命中次数产生时的时间点识别为所述病毒的发展趋势异常点，其中， ω_1 为第一预设阈值。

可选的，上述 ω_1 的取值可以为置信区间 95% 对应的 2.58，也可以为置信区间 99% 对应的 1.96。

本发明实施例中，通过利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，并计算所述病毒各个命中次数与各自对应的 M 日均线取值的标准化残差，由于上述结合 M 日均线运算所得到的各个标准化残差符合正态分布（验证上述结合 M 日均线运算所得到的各个标准化残差符合正态分布的实例见下文），因而采用置信区间可以准确判断出每次对病毒进行查杀时得到的命中次数是否存在异常，进而判断出病毒趋势是否存在异常。例如，将上述第一预设阈值设置为置信区间 95% 对应的 1.96，即可在所述标准化残差大于所述第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

可见，本发明实施例中在监控病毒趋势是否存在异常时，上述第一预设阈值可根据不同的置信区间进行确定，在进行 M 日均线运算时，最少需要 M 个数据即可，而现有技术中的阈值需要对大量的历史数据进行学习和分析才能得到，对于新病毒或变种病毒，由于短时间内难以提供大量的历史数据，导致对新病毒或变种病毒无法实现及时有效的监控，与现有技术相比，本发明实施例不需要大量的历史数据来确定上述第一预设阈值，因而对新病毒和变种病毒也可以进行准确的监控。并且，每当获取到对病毒进行查杀时得到的最新命中次数时，即可采用本发明提供的方法进行判断，如果计算出所述病毒的最新命中次数与对应的 M 日均线取值的标准化残差大于第一预设阈值时，即说明所述病毒的最新命中次数存在异常，因而，可实现对各种病毒进行及时有效的监控。

可选的，如图 3 所示，上述方法还包括：

105、当 $\omega_2 \geq D_{N+1} > \omega_1$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第一级预警，其中， ω_1 为所述第一预设阈值， ω_2 为第二预设阈值；

可选的，上述 ω_1 的取值为置信区间 99% 对应的 1.96，上述 ω_2 的取值为置信区间 95% 对应的 2.58。

当利用第 N+1 个命中次数计算得到的标准化残差落在 [1.96, 2.58) 区间中时，则说明病毒的发展趋势存在异常的概率为 95%，则对所述病毒的第 N+1 个命中次数产生时的时间点进行第一级预警，例如，进行蓝色预警，以通知技术人员进行相关处理。

106、当 $D_{N+1} > \omega_2$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第二级预警。

当利用第 $N+1$ 个命中次数计算得到的标准化残差落在 $[2.58, \infty)$ 区间中时, 则说明病毒的发展趋势存在异常的概率为 99%, 则对所述病毒的第 $N+1$ 个命中次数产生时的时间点进行第二级预警, 例如, 进行红色预警, 以通知技术人员进行相关处理。

可选的, 如图 4 所示, 上述方法还包括:

107、当 $\omega_2 \geq D_{N+1} > \omega_1$ 且 $C_{N+1} > \lambda$ 时, 对所述病毒的第 $N+1$ 个命中次数产生时的时间点进行第一级预警, 其中, ω_1 为所述第一预设阈值, ω_2 为第二预设阈值, λ 为预设幅度。

可选的, 上述 ω_1 的取值为置信区间 99% 对应的 1.96, 上述 ω_2 的取值为置信区间 95% 对应的 2.58。

需要说明的是, 本步骤是在上述步骤 105 的基础上, 进一步地对第一级预警增加了前提条件 $C_{N+1} > \lambda$, 上述 λ 的取值可以为 500。由于 C_{N+1} 是所述病毒的第 $N+1$ 个命中次数与利用所述病毒的第 $N+1$ 个命中次数到第 $N-M+2$ 个命中次数计算得到的 M 日均线取值的残差, 也就是说, C_{N+1} 表示第 $N+1$ 个命中次数相对于利用所述病毒的第 $N+1$ 个命中次数到第 $N-M+2$ 个命中次数计算得到的 M 日均线取值的变化幅度, 在实际应用时, 当 C_{N+1} 小于 500 时, 说明第 $N+1$ 个命中次数的变化幅度较小, 对于病毒趋势异常的监控, 能提供的参考价值较小, 而当 C_{N+1} 大于 500 时, 说明第 $N+1$ 个命中次数的变化幅度较大, 对于病毒趋势异常的监控, 能提供的参考价值较大, 越能准确反映病毒的发展趋势。

108、当 $D_{N+1} > \omega_2$ 且 $C_{N+1} > \lambda$ 时, 对所述病毒的第 $N+1$ 个命中次数产生时的时间点进行第二级预警。

需要说明的是, 本步骤是在上述步骤 105 的基础上, 进一步地对第二级

预警增加了前提条件 $C_{N+1} > \lambda$ ，上述 λ 的取值可以为 500。具体参见上述步骤 107 中的相关描述。

下面给出一些采用本发明实施例提供的上述方法对病毒趋势进行监控时，得到的一些监控效果示意图。

图 5 为采用本发明实施例提供的监控方法，对病毒标识为 Virus.Win32.Loader.b[1023] 的趋势进行监控，没有监控到异常的效果示意图。其中，横坐标表示对病毒的查杀时间，纵坐标表示对病毒进行查杀时得到的命中次数。

图 6 为采用本发明实施例提供的方法对病毒 Virus.Win32.ICE.a[1040] 趋势进行监控，监控到异常并报警的效果示意图；图 7 为采用本发明实施例提供的方法对病毒 Trojan.Win32.BH0.ds[1408] 的趋势进行监控，监控到异常并报警的效果示意图。其中，横坐标表示对病毒的查杀时间，纵坐标表示对病毒进行查杀时得到的命中次数。三角形代表蓝色预警，圆形代表红色预警。

图 8 为采用本发明实施例提供的图 4 所示的监控方法，对病毒标识为 Trojan.Win32.Pasta.ghc[1291] 的趋势进行监控，由于不满足条件 $C_{N+1} > \lambda$ 而没有进行过报警的示意图。其中，横坐标表示对病毒的查杀时间，纵坐标表示对病毒进行查杀时得到的命中次数。

需要说明的是，本发明实施例中的监控方法是基于拉依达准则，其原理为：符合正态分布的数据，可以根据置信区间准确的判断出是否存在异常点。而本发明实施例中提供的上述结合 M 日均线运算所得到的各个标准化残差是符合正态分布的。特别地，下面将详细描述结合 M 日均线运算所得到的各个标准化残差是符合正态分布的验证过程：

针对某个病毒引擎，将该病毒引擎查杀出的每个病毒的命中次数均按照查杀时间从先向后的顺序归为一组数据。每个病毒均会对应一组数据。

首先，随机抽取 10 组的样本数据，分别为表 1 中第 1-2 列所示的病毒 D1000 的样本数据，表 1 中第 4-5 列所示的病毒 D1003 的样本数据，表 1 中第 7-8 列所示的病毒 D1021 的样本数据，表 2 中第 1-2 列所示的病毒 D1022 的样本数据，表 2 中第 4-5 列所示的病毒 D1026 的样本数据，表 2 中第 7-8 列所示的病毒 D1070 的样本数据，表 3 中第 1-2 列所示的病毒 D100000 的样本数据，表 3 中第 4-5 列所示的病毒 D200000 的样本数据，表 4 中第 1-2 列所示的病毒 D400015 的样本数据，表 4 中第 4-5 列所示的病毒 D500003 的样本数据。

其次，对于每组的样本数据均采用本发明实施例提供的上述方法中步骤 102 进行 M 日均线运算得到 M 日均线取值，并采用上述方法中步骤 103 基于 M 日均线取值计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差。

表 1-2 中的第 3、6、9 列为病毒的命中次数与对应的 M 日均线取值的标准化残差；表 3-4 中的第 3、6 列为病毒的命中次数与对应的 M 日均线取值的标准化残差。

最后，将每组样本数据计算得到的标准化残差导入 SPSS 软件进行 K-S 检验，结果示意图如图 9 所示，可见每组样本数据得到的标准化残差均满足正态分布的特性。采用 SPSS 软件进行 K-S 检验以验证数据是否满足正态分布的特性属于现有技术，在此不再赘述。

表 1

D1000	D1003	D1021
-------	-------	-------

查杀时间	命中次数	标准化残差	查杀时间	命中次数	标准化残差	查杀时间	命中次数	标准化残差
201107052155	1895		201107052155	43		201107052155	18005	
201107062002	2222		201107062002	70		201107062002	24150	
201107070112	2108		201107070112	42		201107070112	21124	
201107091516	2016		201107091516	37		201107091516	21236	
201107101803	1537		201107101803	52		201107101803	22956	
201107112201	2068		201107112201	75		201107112201	21388	
201107121230	2105	1.328076819	201107121230	36	-1.177678718	201107121230	22610	0.676634367
201107131230	1487	-2.817030456	201107131230	39	-0.849222794	201107131230	16610	-2.484412126
201107141230	1694	-0.725433447	201107141230	27	-1.38789051	201107141230	22899	1.040109951
201107151230	1553	-1.182474371	201107151230	40	-0.16603447	201107151230	23467	1.167236879
201107161230	1334	-2.082802674	201107161230	27	-1.230231666	201107161230	22874	0.716570751
201107181230	1488	-0.890476003	201107181230	48	0.753642119	201107181230	15126	-2.896076055
201107191058	1314	-1.381371811	201107191058	41	0.556568565	201107191058	13962	-2.952282817
201107191701	1312	-0.557216995	201107191701	41	0.49087738	201107191701	21239	1.119982718
201107201100	1304	-0.422855427	201107201100	36	0.070453796	201107201100	25376	2.691981532
201107211214	1250	-0.35302973	201107211214	22	-1.151402244	201107211214	26306	2.93354605
201107220859	1102	-0.971939316	201107220859	18	-1.230231666	201107220859	26693	2.893298272
201107230853	956	-1.653268842	201107230853	8	-1.900281753	201107230853	23434	1.07374059
201107240849	808	-2.029904419	201107240849	19	-0.507628632	201107240849	22550	0.014064076
201107250856	1067	0.149503694	201107250856	24	0.175559692	201107250856	21278	-1.24864185
201107261323	1034	0.199228054	201107261323	11	-0.625872765	201107261323	21255	-1.26242107
201107270854	1070	0.713399094	201107270854	12	-0.218587418	201107270854	21346	-0.899101184
201107280836	931	0.021489916	201107280836	14	0.070453796	201107280836	19533	-1.359809795
201107281427	931	0.202401949	201107281427	14	0.123006744	201107281427	19530	-0.803814374
201107290840	963	0.431980376	201107290840	10	-0.271140366	201107290840	24643	1.888349394
201107300841	822	-0.627042692	201107300841	7	-0.389384499	201107300841	22932	0.926217302
201107310839	746	-0.850273329	201107310839	4	-0.402522736	201107310839	23522	1.073039951
201107311623	746	-0.545579379	201107311623	4	-0.310555077	201107311623	23439	0.857788294
201107311810	746	-0.202798686	201107311810	4	-0.205449181	201107311810	23439	0.694850963
201107312014	746	-0.007075142	201107312014	4	-0.074066811	201107312014	23522	0.429542591
201108010900	985	1.70577036	201108010900	7	0.293803825	201108010900	21573	-0.791592128
201108011242	985	1.682495128	201108011242	7	0.333218536	201108011242	21368	-0.648350519
201108011440	985	1.510046816	201108011440	7	0.333218536	201108011440	21578	-0.428505788
201108100931	0	-4.995380603	201108100931	0	-0.258002129	201108020913	21320	-0.397677703
201108110917	829	1.056179787	201108110917	9	0.504015617	201108030922	20743	-0.502228508
201108120903	780	0.657326943	201108120903	7	0.280665588	201108041329	22002	0.295720675
201108130851	731	0.310314389	201108130851	26	1.739009894	201108051239	19897	-0.56917839
201108140835	562	-0.493739089	201108140835	9	0.149283218	201108061540	20041	-0.37144269
201108150839	793	1.420119783	201108150839	32	1.936083449	201108071734	18265	-1.09769322
201108161313	753	1.369337458	201108161313	8	-0.284278603	201108080908	19282	-0.364747702
201108170843	737	0.471125085	201108170843	24	0.871886252	201108090903	20241	0.241849374
201108171943	738	0.574805665	201108171943	24	0.674812697	201108100931	18908	-0.341704487

201108180938	751	0.701761478	201108180938	3	-1.203955192	201108110917	18383	-0.346064014
201108181308	751	0.680602175	201108181308	3	-0.901775742	201108120903	18420	-0.21091867
201108181453	751	0.480646771	201108181453	3	-0.82294632	201108130851	17925	-0.315936567
201108181759	751	0.525081305	201108181759	3	-0.441937447	201108140835	15802	-1.281104758
201108190849	655	-0.082190664	201108190849	8	0.017900848	201108150839	17039	-0.432398223
201108200852	570	-0.534999728	201108200852	6	0.070453796	201108161313	17239	-0.089708243
201108210855	478	-0.941258328	201108210855	5	0.22811264	201108170843	17357	0.095338119
201108220841	627	0.293386948	201108220841	38	2.80320709	201108171943	17352	0.172875425
201108230905	439	-0.768810016	201108230905	46	2.974004171	201108180938	17967	0.543279543
201108231309	439	-0.438724904	201108231309	46	2.40905998	201108181308	17967	0.540009898
201108231831	439	-0.108639792	201108231831	46	1.84411579	201108181453	17967	0.371467461
201108240837	462	0.265879855	201108240837	4	-1.965972938	201108181759	17967	0.299223866
201108241631	462	0.380140086	201108241631	4	-1.939696464	201108190849	18767	0.616223776
201108250911	497	0.619240199	201108250911	6	-1.768899383	201108200852	15847	-0.857452129
201108260841	479	0.642515432	201108260841	15	-0.639011002	201108210855	15388	-0.954685156
201108270841	356	-0.180581419	201108270841	5	-1.020019874	201108220841	16897	-0.049071221
201108271532	356	-0.092770315	201108271532	5	-0.481352158	201108230905	16329	-0.231081483
201108280851	315	-0.265218627	201108280851	1	-0.258002129	201108231309	16325	-0.10543368
201108281238	315	-0.109697757	201108281238	1	-0.218587418	201108231831	16330	0.024729348
201108290920	359	0.325125901	201108290920	8	0.372633247	201108240837	17871	0.934235718
201108291222	359	0.471125085	201108291222	8	0.346356773	201108241631	17869	0.775735763
201108300841	316	0.325125901	201108300841	1	-0.113481522	201108250911	16771	0.069725897
201108301851	316	0.367444505	201108301851	1	-0.060928574	201108260841	16329	-0.126919922
201108310852	368	0.739848221	201108310852	3	0.149283218	201108270841	16082	-0.242291696
201108311700	368	0.683776071	201108311700	3	0.123006744	201108271532	16083	-0.22290737
201109011158	378	0.691181827	201109011158	14	0.963853911	201108280851	13940	-1.204657334
201109021211	293	0.131518287	201109021211	2	-0.060928574	201108281238	13940	-0.898634092
201109031504	183	-0.496912984	201109031504	3	0.09673027	201108290920	16421	0.566089212
201109041542	158	-0.514898391	201109041542	1	-0.087205048	201108291222	16419	0.592402073
201109041700	158	-0.347739905	201109041700	1	-0.087205048	201108300841	15302	0.063653698
201109050848	195	0.10930102	201109050848	29	2.146295241	201108301851	15368	0.15520377
201109051321	195	0.292328983	201109051321	29	1.804701079	201108310852	14833	-0.039028738
201109051827	195	0.485936596	201109051827	29	1.607627524	201108311700	14888	-0.082857557
201109060932	187	0.538834852	201109060932	9	-0.323693314	201109011158	12459	-1.29122509
201109061224	187	0.534602991	201109061224	9	-0.402522736	201109021211	13549	-0.473658035
201109061949	187	0.503922003	201109061949	9	-0.507628632	201109031504	15538	0.678814131
201109062121	187	0.473241015	201109062121	9	-0.612734528	201109041542	13558	-0.264400727
201109071244	235	0.786398686	201109071244	3	-0.82294632	201109041700	13560	-0.122560394
201109071502	235	0.744080082	201109071502	3	-0.481352158	201109050848	12797	-0.37985035
201109081134	191	0.42245869	201109081134	2	-0.218587418	201109051321	12792	-0.219404178
201109090918	172	0.297618808	201109090918	8	0.346356773	201109051827	12792	-0.245327795
201109100928	182	0.376966191	201109100928	2	-0.113481522	201109060932	13516	0.151778427
201109110917	138	0.102953229	201109110917	1	-0.100343285	201109061224	13516	0.3091885
201109120830	94	-0.124509268	201109120830	9	0.635397987	201109061949	13518	0.31339233

						201109062121	13518	0.316661975
						201109071244	14946	0.92754073
						201109071502	14946	0.759854628
						201109081134	12401	-0.596581133
						201109090918	12045	-0.676064656
						201109100928	16002	1.286734635
						201109110917	13852	0.089110223
						201109120830	13700	-0.007889258

表 2

D1022			D1026			D1070		
查杀时间	命中次数	标准化残差	查杀时间	命中次数	标准化残差	查杀时间	命中次数	标准化残差
201107052155	25475		201107052155	27313		201107112201	60997	
201107062002	38796		201107062002	46585		201107121230	73607	
201107070112	30555		201107070112	25112		201107131230	50082	
201107091516	20901		201107091516	46338		201107141230	64657	
201107101803	17781		201107101803	24895		201107151230	67143	
201107112201	14802		201107112201	25152		201107161230	60570	
201107121230	16964	-0.234138052	201107121230	32267	0.006325427	201107181230	50154	-1.184141483
201107131230	38402	0.304906424	201107131230	27968	-0.122270621	201107191058	50540	-0.933472986
201107141230	72207	1.103707454	201107141230	21081	-0.217228773	201107191701	50334	-0.517609778
201107151230	90849	1.379638606	201107151230	30552	0.03729086	201107201100	61431	0.745924032
201107161230	101604	1.358342381	201107161230	27535	0.027604752	201107211214	75280	2.390251462
201107181230	68861	0.256657779	201107181230	9021	-0.448018277	201107220859	63509	0.889878879
201107191058	74471	0.176476588	201107191058	8122	-0.40311338	201107230853	65829	1.099058206
201107191701	74170	-0.056661651	201107191701	8096	-0.30278521	201107240849	63865	0.575986069
201107201100	122514	0.942885189	201107201100	24444	0.19055386	201107250856	61315	0.030702557
201107211214	187754	2.28375729	201107211214	34484	0.428428108	201107261323	64780	0.217556215
201107220859	191758	1.997288084	201107220859	36393	0.459887048	201107270854	57899	-0.632705078
201107230853	197955	1.789074053	201107230853	38082	0.465223608	201107280836	60763	0.025730715
201107240849	202890	1.398037947	201107240849	39368	0.375953326	201107281427	60767	0.078497014
201107250856	218393	1.258889247	201107250856	44591	0.376338094	201107290840	67903	0.990534882
201107261323	241846	1.245112343	201107261323	47645	0.300342297	201107300841	73749	1.581784126
201107270854	219267	0.243560876	201107270854	48748	0.230987924	201107310839	77833	1.811708038
201107280836	223486	0.219194819	201107280836	27872	-0.352520614	201107311623	77838	1.563630233
201107281427	223495	0.094695626	201107281427	27874	-0.316833412	201107311810	77838	1.183808122
201107290840	280277	1.333445687	201107290840	55163	0.410636786	201107312014	77832	0.857857164
201107300841	258646	0.519122547	201107300841	88620	1.184132726	201108010900	81971	1.005850443
201107310839	270050	0.629852696	201107310839	95392	1.169925597	201108011242	81958	0.73638038
201107311623	270051	0.519016419	201107311623	95393	0.970260452	201108011440	81976	0.582062765
201107311810	270050	0.319379052	201107311810	95392	0.775153967	201108020913	85530	0.909347167
201107312014	270052	0.13639975	201107312014	95392	0.492767955	201108030922	75655	-0.365844757
201108010900	267638	-0.10353064	201108010900	77511	-0.238307349	201108041329	64935	-1.549505247

201108011242	267639	-0.053827657	201108011242	77510	-0.331797529	201108051239	61330	-1.71586196
201108011440	267639	-0.089175931	201108011440	77511	-0.285307557	201108061540	75566	0.304439642
201108020913	249593	-0.505293472	201108020913	12378	-1.8449424	201108071734	60669	-1.276453934
201108030922	211568	-1.321656616	201108030922	17796	-1.361795491	201108080908	59019	-1.059159645
201108041329	149049	-2.566224029	201108041329	46046	-0.328376442	201108090903	45574	-2.090845573
201108051239	148916	-2.093741065	201108051239	25939	-0.626554658	201108100931	48845	-1.143966708
201108061540	161778	-1.323751649	201108061540	57632	0.384422397	201108110917	48970	-0.823178085
201108071734	158222	-0.991514034	201108071734	58310	0.48457073	201108120903	49623	-0.513095116
201108080908	139819	-0.995448608	201108080908	50327	0.364552493	201108130851	43825	-0.68158534
201108090903	146887	-0.397275467	201108090903	66830	0.619958763	201108140835	42834	-0.473987097
201108100931	136254	-0.393804709	201108100931	63716	0.336744664	201108150839	41603	-0.306373137
201108110917	148280	-0.05989264	201108110917	43556	-0.243041665	201108161313	45116	0.170790415
201108120903	149564	-0.027111075	201108120903	17605	-0.967923045	201108170843	42232	-0.087802551
201108130851	158085	0.221855864	201108130851	14259	-0.88448283	201108171943	42241	0.041579654
201108140835	182168	0.790364441	201108140835	32181	-0.250523723	201108180938	43164	0.28769539
201108150839	171568	0.373916726	201108150839	21044	-0.454099279	201108181308	43163	0.30017262
201108161313	153767	-0.142911754	201108161313	13719	-0.446420655	201108181453	43163	0.293905431
201108170843	131536	-0.73604188	201108170843	6183	-0.426425282	201108181759	43163	0.264188671
201108171943	131578	-0.669236669	201108171943	6186	-0.2700465	201108190849	47762	0.82703555
201108180938	131863	-0.59181872	201108180938	3009	-0.302011492	201108200852	44805	0.383722436
201108181308	131864	-0.488725811	201108181308	3009	-0.254961098	201108210855	41524	-0.040122389
201108181453	131864	-0.290998736	201108181453	3009	-0.132956288	201108220841	42867	0.144616807
201108181759	131863	-0.134960063	201108181759	3009	-0.057529278	201108230905	48330	0.774650234
201108190849	159646	0.606367103	201108190849	60306	1.425047475	201108231309	48324	0.675537217
201108200852	210242	1.689125658	201108200852	116859	2.617806343	201108231831	48331	0.578024334
201108210855	219746	1.60406654	201108210855	131900	2.532375374	201108240837	42803	-0.064638717
201108220841	211268	1.058685867	201108220841	101924	1.241115981	201108241631	42803	-0.026502207
201108230905	200454	0.491541224	201108230905	87826	0.473659221	201108250911	44158	0.1040039
201108231309	200413	0.220971469	201108231309	87809	0.118506114	201108260841	43456	-0.000823878
201108231831	200454	-0.047507183	201108231831	87827	-0.235697621	201108270841	45323	0.305411152
201108240837	136879	-1.707252713	201108240837	18647	-2.086768881	201108271532	45324	0.362692113
201108241631	136879	-1.418888937	201108241631	18647	-1.676021028	201108280851	42132	0.055142688
201108250911	134639	-1.145996172	201108250911	15614	-1.278476561	201108281238	42132	0.067924705
201108260841	180533	0.237562714	201108260841	35523	-0.417918571	201108290920	45860	0.506799354
201108270841	245048	1.837377727	201108270841	159819	2.919853147	201108291222	45860	0.474377606
201108271532	245044	1.661839133	201108271532	159820	2.618713893	201108300841	45351	0.370407041
201108280851	266089	1.982894069	201108280851	174767	2.692693843	201108301851	45352	0.369987959
201108281238	266089	1.475015663	201108281238	174766	2.03973474	201108310852	40005	-0.241682034
201108290920	227585	0.059064346	201108290920	149330	0.748525535	201108311700	40006	-0.201050079
201108291222	227586	-0.306249632	201108291222	149328	0.189240632	201109011158	36208	-0.594644765
201108300841	199070	-1.163715512	201108300841	109464	-1.287050188	201109021211	35905	-0.445413288
201108301851	199070	-0.9829924	201108301851	109464	-1.076452622	201109031504	35841	-0.263093341
201108310852	192613	-0.954565988	201108310852	53516	-2.26978446	201109041542	48139	1.32366739
201108311700	192618	-0.66564013	201108311700	53516	-1.762681581	201109041700	48139	1.270577254

201109011158	139937	-1.619273126	201109011158	65958	-0.943369013	201109050848	36776	-0.183105727
201109021211	138255	-1.314428164	201109021211	42586	-1.181172163	201109051321	36775	-0.121691088
201109031504	150974	-0.663336773	201109031504	106226	0.86220347	201109051827	36775	-0.132491987
201109041542	128246	-1.010302508	201109041542	63273	-0.202097366	201109060932	33541	-0.518695583
201109041700	128247	-0.731895052	201109041700	63273	-0.008914719	201109061224	33540	-0.474996705
201109050848	97355	-1.207447848	201109050848	30433	-0.873792981	201109061949	33545	-0.196325876
201109051321	97354	-0.83302657	201109051321	30433	-0.777253935	201109062121	33544	0.081563936
201109051827	97355	-0.665624408	201109051827	30433	-0.628679245	201109071244	33786	0.170790415
201109060932	76077	-1.006678455	201109060932	20309	-0.831899309	201109071502	33787	0.227842786
201109061224	76077	-0.712285073	201109061224	20309	-0.472572309	201109081134	34367	0.351053048
201109061949	76077	-0.507227348	201109061949	20309	-0.292885807	201109090918	31504	0.00809115
201109062121	76077	-0.302165694	201109062121	20308	-0.113224398	201109100928	41393	1.1771409
201109071244	67021	-0.432104896	201109071244	12095	-0.276972318	201109110917	40673	0.945350166
201109071502	67020	-0.31290028	201109071502	12096	-0.20025299	201109120830	39532	0.679137517
201109081134	81116	0.138773859	201109081134	24175	0.179541977	201109081134	2695	-3.640612747
201109090918	87149	0.26124877	201109090918	31885	0.356844593	201109090918	1336	-3.203662068
201109100928	88500	0.249590482	201109100928	9678	-0.248821544	201109100928	2332	-2.460609703
201109110917	72714	-0.171534698	201109110917	15026	-0.070159695	201109110917	2714	-1.861245497
201109120830	65904	-0.318922025	201109120830	15956	-0.024732016	201109120830	2509	-1.147871795

表 3

D100000			D200000		
查杀时间	命中次数	标准化残差	查杀时间	命中次数	标准化残差
201107052155	4601		201107052155	1192	
201107062002	5749		201107062002	2020	
201107070112	5038		201107070112	1877	
201107091516	5500		201107091516	1354	
201107101803	5042		201107101803	1303	
201107112201	4752		201107112201	1722	
201107121230	5578	0.792694815	201107121230	2180	0.874004445
201107131230	4950	-0.542204571	201107131230	1478	-0.453100915
201107141230	6203	1.797596946	201107141230	2088	0.619302301
201107151230	6146	1.373636277	201107151230	1708	-0.016432209
201107161230	5481	0.069401597	201107161230	1451	-0.500315241
201107181230	6216	1.186553433	201107181230	1475	-0.501336091
201107191058	7384	2.746233559	201107191058	2486	1.109820859
201107191701	7380	2.23140408	201107191701	3003	1.823395203
201107201100	5845	-1.043248998	201107201100	1638	-0.655994908
201107211214	5912	-0.829440034	201107211214	2346	0.542993743
201107220859	5410	-1.610968063	201107220859	2021	-0.117496387
201107230853	5358	-1.678768011	201107230853	1583	-0.933666183
201107240849	4921	-2.175029869	201107240849	2128	-0.126684039
201107250856	5560	-0.403510072	201107250856	1622	-0.8101433

201107261323	5932	0.736429299	201107261323	2200	0.427382449
201107270854	5879	0.622491627	201107270854	1679	-0.513841507
201107280836	5429	-0.12780904	201107280836	1688	-0.329833244
201107281427	5430	-0.131466298	201107281427	3462	2.471635129
201107290840	5210	-0.523074295	201107290840	3528	2.093154888
201107300841	5499	-0.116555936	201107300841	3653	1.927266718
201107310839	5162	-0.668239329	201107310839	4542	2.770233835
201107311623	5174	-0.431361503	201107311623	4543	2.174057273
201107311810	5173	-0.234713522	201107311810	4543	1.443128475
201107312014	5161	-0.182949246	201107312014	4542	0.712965314
201108010900	5790	0.954458176	201108010900	4153	-0.158330398
201108011242	5647	0.54990911	201108011242	4153	-0.317838254
201108011440	5801	0.768219316	201108011440	4153	-0.445444538
201108020913	6404	1.606294189	201108020913	4511	0.20202975
201108030922	6385	1.228189916	201108030922	3393	-1.501769363
201108041329	6515	1.106656399	201108041329	3702	-0.735110804
201108051239	6286	0.33919475	201108051239	3042	-1.531374021
201108061540	6289	0.204720165	201108061540	2788	-1.636776812
201108071734	6346	0.12032189	201108071734	2232	-2.139800786
201108080908	6378	0.021013252	201108080908	2632	-1.037027274
201108090903	6181	-0.304201435	201108090903	2496	-0.765736313
201108100931	8228	3.20845478	201108100931	3315	0.717303927
201108110917	6502	-0.186887832	201108110917	1938	-1.292495056
201108120903	5603	-1.765135579	201108120903	2309	-0.4426372
201108130851	5759	-1.308822238	201108130851	1394	-1.721507385
201108140835	5333	-1.862756251	201108140835	2489	0.169107329
201108150839	5976	-0.483407106	201108150839	2351	-0.005713281
201108161313	5369	-1.450330012	201108161313	2574	0.372766959
201108170843	5817	0.110194097	201108170843	3597	2.128374223
201108171943	5819	0.306279423	201108171943	3597	1.704976571
201108180938	6574	1.51992662	201108180938	2439	-0.39695415
201108181308	6574	1.290644639	201108181308	2439	-0.663651285
201108181453	6572	0.938141176	201108181453	2439	-0.650890657
201108181759	6575	0.775533833	201108181759	2439	-0.673349363
201108190849	5964	-0.595094157	201108190849	1880	-1.494878623
201108200852	5709	-1.066880515	201108200852	2448	-0.186914206
201108210855	5401	-1.555827856	201108210855	2399	0.031292541
201108220841	5781	-0.584403709	201108220841	2682	0.474851987
201108230905	6449	0.766250023	201108230905	2114	-0.456929104
201108231309	6447	0.797477384	201108231309	2113	-0.375516294
201108231831	6450	0.838551212	201108231831	2114	-0.290785721
201108240837	6310	0.465510835	201108240837	1870	-0.724136664
201108241631	6311	0.298120923	201108241631	1870	-0.576623799
201108250911	6008	-0.469340727	201108250911	2016	-0.218050139

201108260841	5946	-0.63785595	201108260841	3127	1.653168419
201108270841	5634	-1.022993412	201108270841	1760	-0.698615407
201108271532	5634	-0.794274086	201108271532	1760	-0.60852537
201108280851	5548	-0.709875811	201108280851	2332	0.357709417
201108281238	5548	-0.495504192	201108281238	2332	0.23980121
201108290920	5732	0.029734407	201108290920	2260	0.011641173
201108291222	5732	0.107380821	201108291222	2260	-0.050630694
201108300841	5939	0.516993783	201108300841	1994	-0.236680657
201108301851	5938	0.429500904	201108301851	1994	-0.296400398
201108310852	4934	-1.350740048	201108310852	2789	0.861243817
201108311700	4935	-1.176316945	201108311700	2789	0.744611672
201109011158	5025	-0.851946241	201109011158	1852	-0.806825536
201109021211	4728	-1.154373394	201109021211	3413	1.687622116
201109031504	5440	0.32991094	201109031504	1821	-1.044428438
201109041542	4659	-0.848007655	201109041542	2221	-0.387766498
201109041700	4659	-0.488189675	201109041700	2221	-0.445699751
201109050848	4905	0.004414925	201109050848	1954	-0.709589547
201109051321	4902	0.007790856	201109051321	1954	-0.496487052
201109051827	4902	0.042394149	201109051827	1954	-0.522518734
201109060932	5122	0.36479556	201109060932	2462	0.627724316
201109061224	5122	0.454257732	201109061224	2462	0.464133059
201109061949	5122	0.32400306	201109061949	2462	0.402626829

表 4

D400015			D500003		
查杀时间	命中次数	标准化残差	查杀时间	命中次数	标准化残差
201109051827	259		201108110917	1483	
201109061224	284		201108120903	598	
201109061949	284		201108130851	1009	
201109062121	284		201108140835	2327	
201109071244	309		201108150839	1020	
201109071502	309		201108161313	1694	
201109081134	246	-1.364940734	201108170843	512	-1.245679866
201109090918	317	-0.347607997	201108171943	513	-0.961074186
201109100928	402	0.757785433	201108180938	953	-0.167266121
201109110917	452	1.179549803	201108181308	953	-0.150953001
201109120830	379	-0.224786505	201108181453	953	0.249301047
			201108181759	953	0.268818529
			201108190849	1923	2.180075304
			201108200852	1798	1.550563661
			201108210855	565	-0.978843834
			201108220841	414	-1.129740193
			201108230905	1190	0.38359298

			201108231309	1190	0.314553526
			201108231831	1190	0.245514072
			201108240837	800	-0.222614207
			201108241631	801	0.069856728
			201108250911	1113	0.546432873
			201108260841	2027	1.940330704
			201108270841	1001	-0.096770139
			201108271532	1001	-0.04171336
			201108280851	1228	0.410101799
			201108281238	1228	0.285422955
			201108291222	1718	1.017474209
			201108300841	1327	0.157831053
			201108301851	1324	0.356501548
			201108310852	607	-0.990787369
			201108311700	605	-0.879508587
			201109011158	1421	0.728207637
			201109021211	758	-0.486828487
			201109031504	304	-1.000691763
			201109041700	2242	2.684616797
			201109050848	1039	0.314553526
			201109060932	58	-1.525915961
			201109061224	58	-1.366571737
			201109061949	58	-0.969522052
			201109062121	58	-0.765608053
			201109110917	41	-0.723660031

实施例 2:

本发明实施例提供一种病毒趋势异常的监控装置，如 10 所示，包括：

获取模块 11，用于获取每次对病毒进行查杀时得到的命中次数；

运算模块 12，用于利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，其中，M 为正整数。本发明的实施例中，以 M=7 来举例说明，当然，M 也可以取值为 4、5、6、8、9、10、11 等等数值；

所述运算模块 12，还用于计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差；

识别模块 13，用于当所述标准化残差大于第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

本发明实施例提供的装置，通过利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，并计算所述病毒各个命中次数与各自对应的 M 日均线取值的标准化残差，由于上述结合 M 日均线运算所得到的各个标准化残差符合正态分布，因而采用置信区间可以准确判断出每次对病毒进行查杀时得到的命中次数是否存在异常，进而判断出病毒趋势是否存在异常。例如，将上述第一预设阈值设置为置信区间 95% 对应的 1.96，即可在所述标准化残差大于所述第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

可见，本发明实施例中在监控病毒趋势是否存在异常时，上述第一预设阈值可根据不同的置信区间进行确定，与现有技术相比，本发明实施例不需要大量的历史数据来确定上述第一预设阈值，因而对新病毒和变种病毒也可以进行准确的监控。并且，每当获取到对病毒进行查杀时得到的最新命中次数时，即可采用本发明提供的方法进行判断，如果计算出所述病毒的最新命中次数与对应的 M 日均线取值的标准化残差大于第一预设阈值时，即说明所述病毒的最新命中次数存在异常，因而，可实现对各种病毒进行及时有效的监控。

具体地，所述运算模块 12，具体用于根据 $B_i = \frac{1}{M} \sum_{j=0}^{M-1} A_{i-j}$ 计算各个 M 日均线取值，其中， B_i 为利用所述病毒的第 i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值， $i \in [MK, N+1]$ 且 i 为正整数， $N+1$ 为所述病毒的命中次数的总数， A_{i-j} 为所述病毒的第 $i-j$ 个命中次数。

具体地，所述运算模块 12，还具体用于根据 $C_i = A_i - B_i$ 计算残差，其中， C_i 为所述病毒的第 i 个命中次数与利用所述病毒的第 i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值的残差， A_i 为所述病毒的第 i 个命中次数， B_i 为利用所述病毒的第 i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值， $i \in [MK N+1]$ 且 i 为正整数， $N+1$ 为所述病毒的命中次数的总数；

并根据 $E = \frac{1}{N - \max(M, N-L)} \sum_{i=\max(M, N-L)}^N C_i$ 计算残差的均值，其中， E 为所述病毒

的各个命中次数对应的残差的均值， $L \in [1K N]$ 且 L 为正整数；

并根据 $S = \frac{1}{N - \max(M, N-L) - 1} \sum_{i=\max(M, N-L)}^N (C_i - E)^2$ 计算残差的标准差，其中， S 为

所述病毒的各个命中次数对应的残差的标准差；

并根据 $D_{N+1} = \frac{C_{N+1} - E}{S}$ 计算所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差，其中， D_{N+1} 为所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差， C_{N+1} 为所述病毒的第 $N+1$ 个命中次数与利用所述病毒的第 $N+1$ 个命中次数到第 $N-M+2$ 个命中次数计算得到的 M 日均线取值的残差。

具体地，所述识别模块 13，具体用于当 $D_{N+1} > \omega_1$ 时，将所述病毒的第 $N+1$ 个命中次数产生时的时间点识别为所述病毒的发展趋势异常点，其中， ω_1 为第一预设阈值。

可选的，如图 11 所示，所述的装置还包括：

第一预警模块 14，用于当 $\omega_2 \geq D_{N+1} > \omega_1$ 时，对所述病毒的第 $N+1$ 个命中次数产生时的时间点进行第一级预警，其中， ω_1 为所述第一预设阈值， ω_2 为第二预设阈值；

所述第一预警模块 14, 还用于当 $D_{N+1} > \omega_2$ 时, 对所述病毒的第 N+1 个命中次数产生时的时间点进行第二级预警。

可选的, 如图 12 所示, 所述的装置还包括:

第二预警模块 15, 用于当 $\omega_2 \geq D_{N+1} > \omega_1$ 且 $C_{N+1} > \lambda$ 时, 对所述病毒的第 N+1 个命中次数产生时的时间点进行第一级预警, 其中, ω_1 为所述第一预设阈值, ω_2 为第二预设阈值, λ 为预设幅度;

所述第二预警模块 15, 还用于当 $D_{N+1} > \omega_2$ 且 $C_{N+1} > \lambda$ 时, 对所述病毒的第 N+1 个命中次数产生时的时间点进行第二级预警。

本装置的功能实现过程可参见上述实施例 1 中的方法的相关描述。

以上所述, 仅为本发明的具体实施方式, 但本发明的保护范围并不局限于此, 任何熟悉本技术领域的技术人员在本发明揭露的技术范围内, 可轻易想到变化或替换, 都应涵盖在本发明的保护范围之内。因此, 本发明的保护范围应以所述权利要求的保护范围为准。

权利要求书

1、一种病毒趋势异常的监控方法，其包括：

获取每次对病毒进行查杀时得到的命中次数；

利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，所述 M 为正整数；

计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差；

当所述标准化残差大于第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

2、根据权利要求 1 所述的方法，其中

所述利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，包括：

根据 $B_i = \frac{1}{M} \sum_{j=0}^M A_{i-j}$ 计算各个 M 日均线取值，其中， B_i 为利用所述病毒的第

i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值， $i \in [M, N+1]$ 且 i 为正整数， $N+1$ 为所述病毒的命中次数的总数， A_{i-j} 为所述病毒的第 $i-j$ 个命中次数。

3、根据权利要求 2 所述的方法，其中

所述计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差，包括：

根据 $C_i = A_i - B_i$ 计算残差，其中， C_i 为所述病毒的第 i 个命中次数与利用所述病毒的第 i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值

的残差, A_i 为所述病毒的第 i 个命中次数, B_i 为利用所述病毒的第 i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值, $i \in [MK N+1]$ 且 i 为正整数, $N+1$ 为所述病毒的命中次数的总数;

根据 $E = \frac{1}{N - \max(M, N-L)} \sum_{i=\max(M, N-L)}^N C_i$ 计算残差的均值, 其中, E 为所述病毒

的各个命中次数对应的残差的均值, $L \in [1K N]$ 且 L 为正整数;

根据 $S = \frac{1}{N - \max(M, N-L) - 1} \sum_{i=\max(M, N-L)}^N (C_i - E)^2$ 计算残差的标准差, 其中, S 为

所述病毒各个命中次数对应的残差的标准差;

根据 $D_{N+1} = \frac{C_{N+1} - E}{S}$ 计算所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差, 其中, D_{N+1} 为所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差, C_{N+1} 为所述病毒的第 $N+1$ 个命中次数与利用所述病毒的第 $N+1$ 个命中次数到第 $N-M+2$ 个命中次数计算得到的 M 日均线取值的残差。

4、根据权利要求 3 所述的方法, 其中

当所述标准化残差大于第一预设阈值时, 将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点包括:

当 $D_{N+1} > \omega_1$ 时, 将所述病毒的第 $N+1$ 个命中次数产生时的时间点识别为所述病毒的发展趋势异常点, 其中, ω_1 为第一预设阈值。

5、根据权利要求 2 至 4 中任意一项所述的方法, 其包括:

当 $\omega_2 \geq D_{N+1} > \omega_1$ 时, 对所述病毒的第 $N+1$ 个命中次数产生时的时间点进行第一级预警, 其中, ω_1 为所述第一预设阈值, ω_2 为第二预设阈值;

当 $D_{N+1} > \omega_2$ 时, 对所述病毒的第 $N+1$ 个命中次数产生时的时间点进行第二

级预警。

6、根据权利要求 2 至 4 中任意一项所述的方法，其包括：

当 $\omega_2 \geq D_{N+1} > \omega_1$ 且 $C_{N+1} > \lambda$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第一级预警，其中， ω_1 为所述第一预设阈值， ω_2 为第二预设阈值， λ 为预设幅度；

当 $D_{N+1} > \omega_2$ 且 $C_{N+1} > \lambda$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第二级预警。

7、根据权利要求 1 所述的方法，其中

所述命中次数按照“病毒引擎标识-病毒标识-日期-时间点-命中次数”的格式存放于数据库中，并且所述命中次数按照查杀时间由早到晚的次序存放于所述数据库中。

8、一种病毒趋势异常的监控装置，其包括：

获取模块，用于获取每次对病毒进行查杀时得到的命中次数；

运算模块，用于利用所述病毒的各个命中次数进行 M 日均线运算，得到各个 M 日均线取值，所述 M 为正整数；

所述运算模块，还用于计算所述病毒的各个命中次数与各自对应的 M 日均线取值的标准化残差；

识别模块，用于当所述标准化残差大于第一预设阈值时，将所述标准化残差对应的命中次数产生时的时间点识别为所述病毒的发展趋势异常点。

9、根据权利要求 8 所述的装置，其中

所述运算模块，用于根据 $B_i = \frac{1}{M} \sum_{j=0}^{M-1} A_{i-j}$ 计算各个 M 日均线取值，其中， B_i

为利用所述病毒的第 i 个命中次数到第 i-M+1 个命中次数计算得到的 M 日均

线取值, $i \in [MK N + 1]$ 且 i 为正整数, $N+1$ 为所述病毒的命中次数的总数, A_{i-j} 为所述病毒的第 $i-j$ 个命中次数。

10、根据权利要求 9 所述的装置, 其中

所述运算模块, 还用于根据 $C_i = A_i - B_i$ 计算残差, 其中, C_i 为所述病毒的第 i 个命中次数与利用所述病毒的第 i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值的残差, A_i 为所述病毒的第 i 个命中次数, B_i 为利用所述病毒的第 i 个命中次数到第 $i-M+1$ 个命中次数计算得到的 M 日均线取值, $i \in [MK N + 1]$ 且 i 为正整数, $N+1$ 为所述病毒的命中次数的总数;

并根据 $E = \frac{1}{N - \max(M, N - L)} \sum_{i=\max(M, N-L)}^N C_i$ 计算残差的均值, 其中, E 为所述病

毒的各个命中次数对应的残差的均值, $L \in [IK N]$ 且 L 为正整数;

并根据 $S = \frac{1}{N - \max(M, N - L) - 1} \sum_{i=\max(M, N-L)}^N (C_i - E)^2$ 计算残差的标准差, 其中, S 为

所述病毒的各个命中次数对应的残差的标准差;

并根据 $D_{N+1} = \frac{C_{N+1} - E}{S}$ 计算所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差, 其中, D_{N+1} 为所述病毒的第 $N+1$ 个命中次数与对应的 M 日均线取值的标准化残差, C_{N+1} 为所述病毒的第 $N+1$ 个命中次数与利用所述病毒的第 $N+1$ 个命中次数到第 $N-M+2$ 个命中次数计算得到的 M 日均线取值的残差。

11、根据权利要求 10 所述的装置, 其中

所述识别模块, 用于当 $D_{N+1} > \omega_1$ 时, 将所述病毒的第 $N+1$ 个命中次数产生时的时间点识别为所述病毒的发展趋势异常点, 其中, ω_1 为第一预设阈值。

12、根据权利要求 9 至 11 中任意一项所述的装置, 其包括:

第一预警模块，用于当 $\omega_2 \geq D_{N+1} > \omega_1$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第一级预警，其中， ω_1 为所述第一预设阈值， ω_2 为第二预设阈值；

所述第一预警模块，还用于当 $D_{N+1} > \omega_2$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第二级预警。

13、根据权利要求 9 至 11 中任意一项所述的装置，其包括：

第二预警模块，用于当 $\omega_2 \geq D_{N+1} > \omega_1$ 且 $C_{N+1} > \lambda$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第一级预警，其中， ω_1 为所述第一预设阈值， ω_2 为第二预设阈值， λ 为预设幅度；

所述第二预警模块，还用于当 $D_{N+1} > \omega_2$ 且 $C_{N+1} > \lambda$ 时，对所述病毒的第 N+1 个命中次数产生时的时间点进行第二级预警。

14、根据权利要求 8 所述的装置，其中

所述命中次数按照“病毒引擎标识-病毒标识-日期-时间点-命中次数”的格式存放于数据库中，并且所述命中次数按照查杀时间由早到晚的次序存放于所述数据库中。

说明书附图

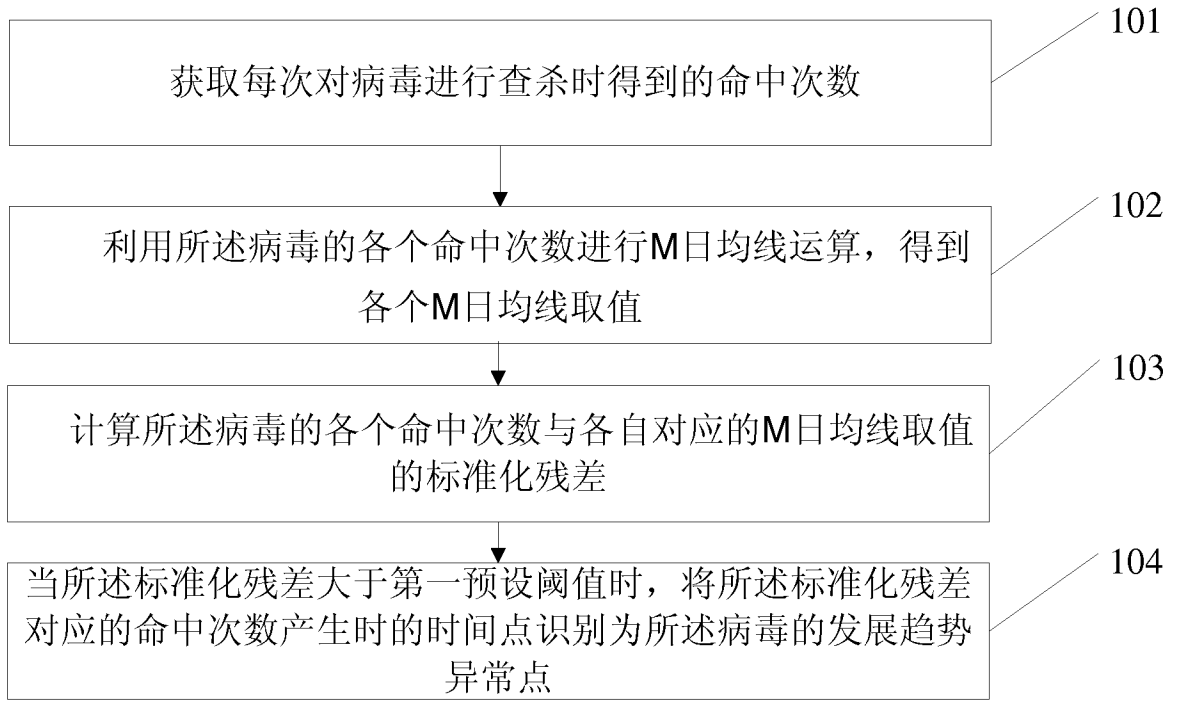


图 1

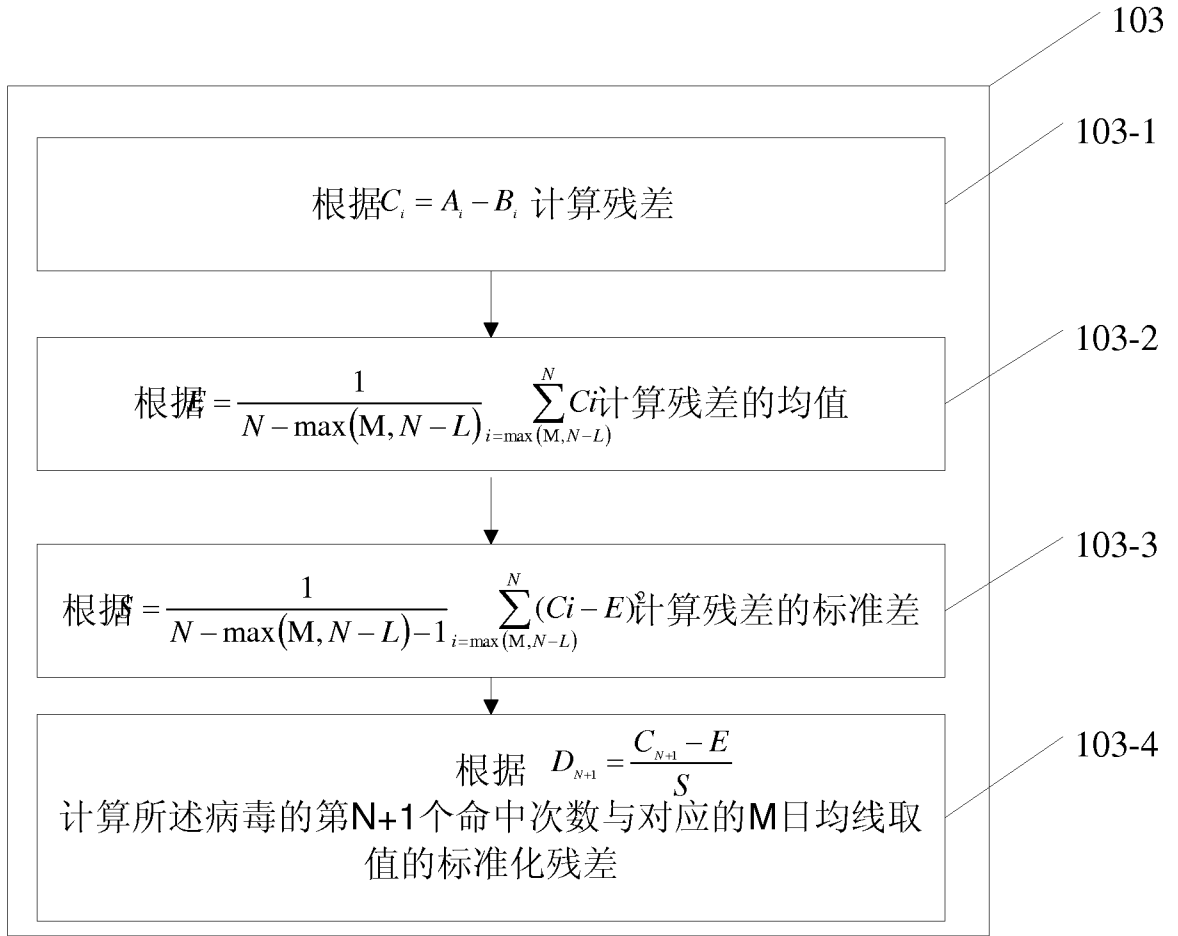


图 2

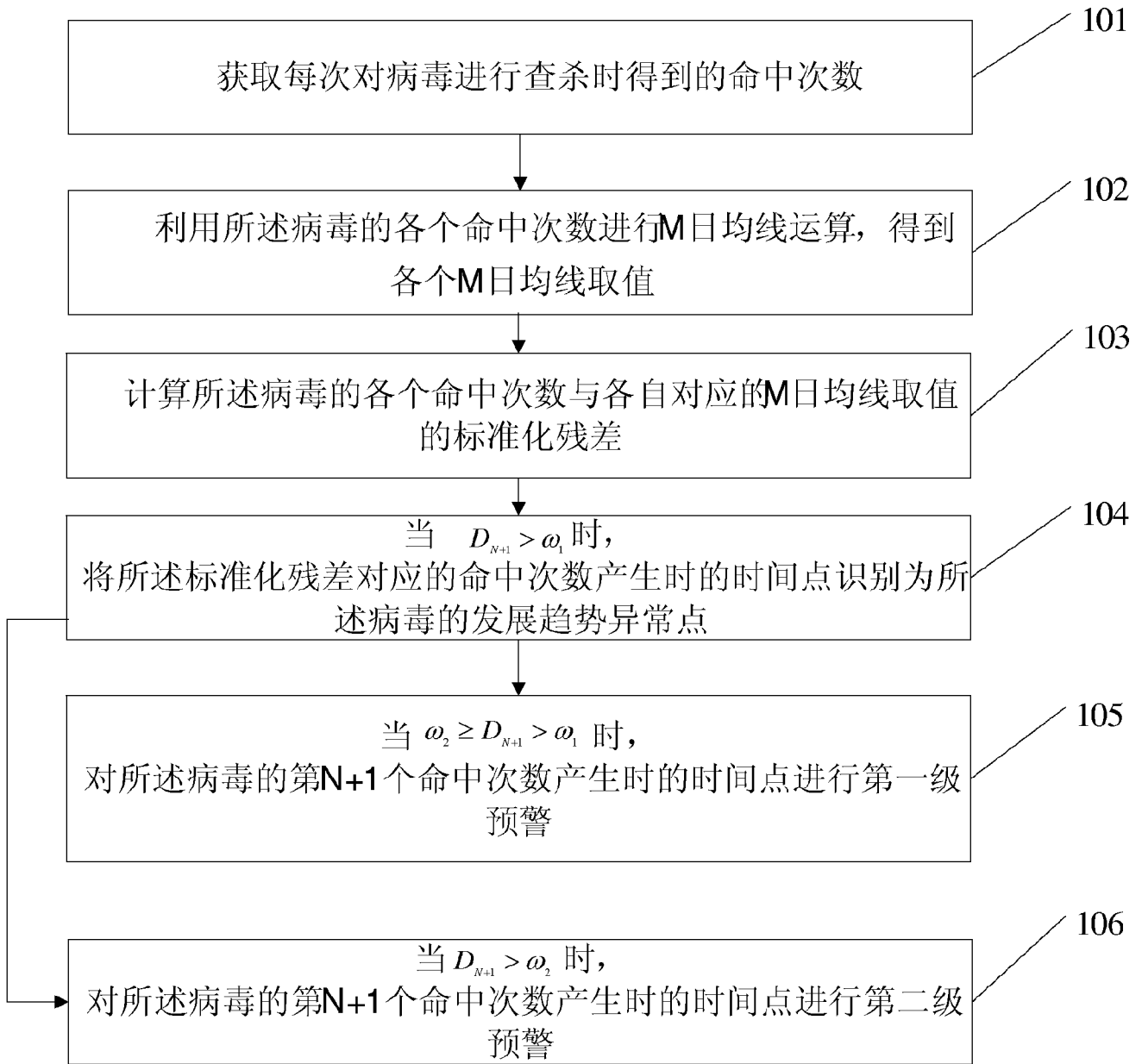


图 3

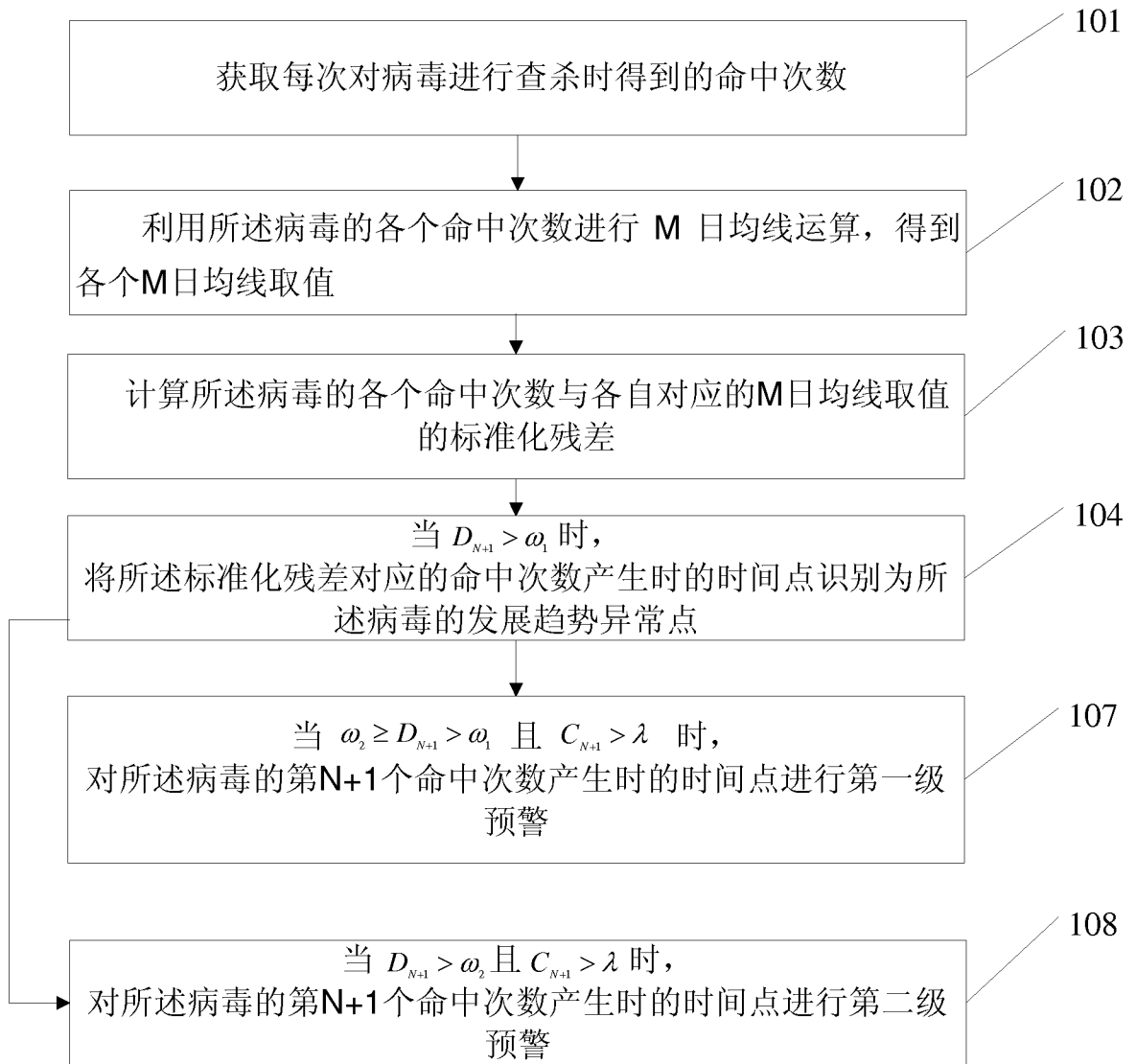


图 4

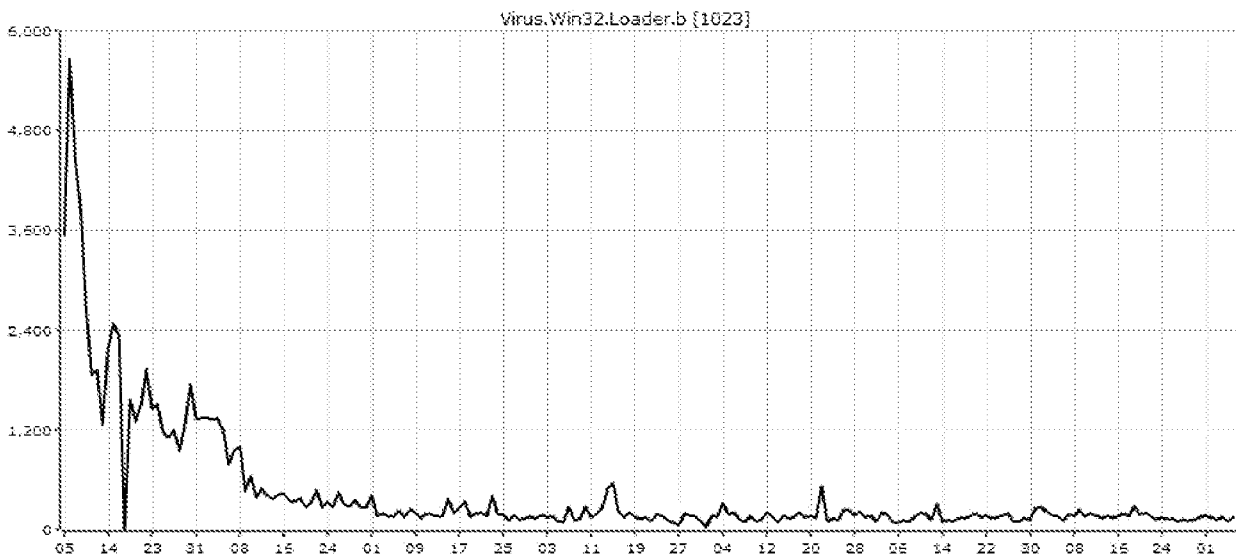


图 5

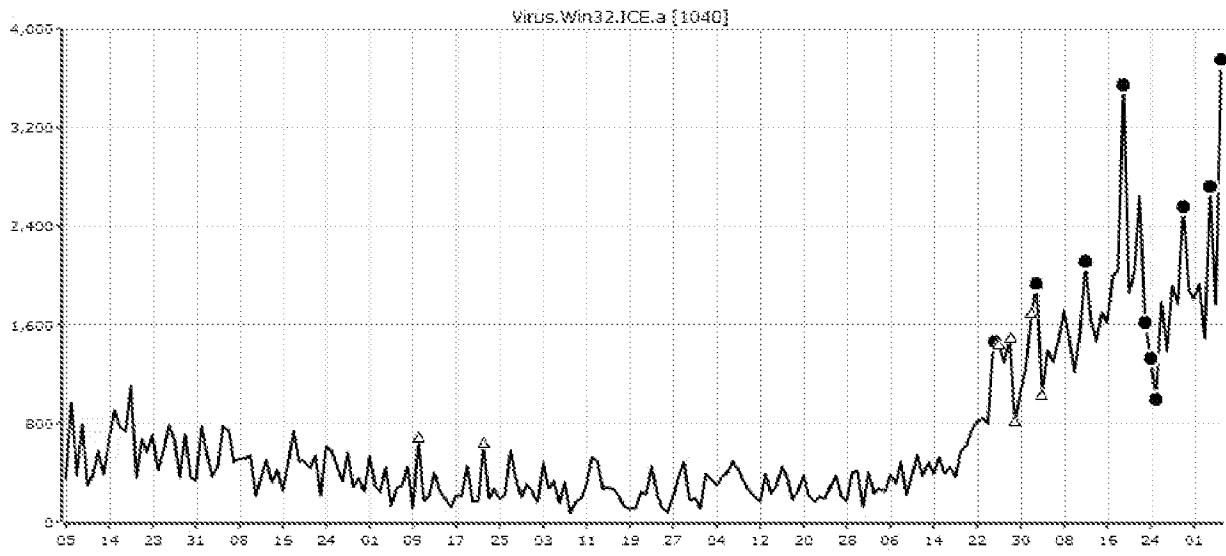


图 6

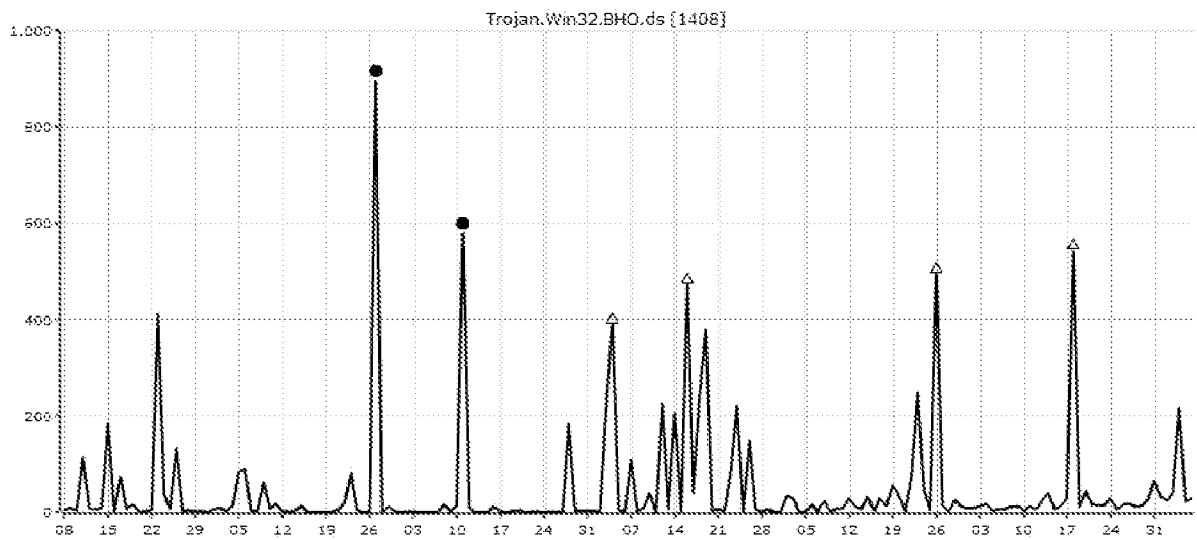


图 7

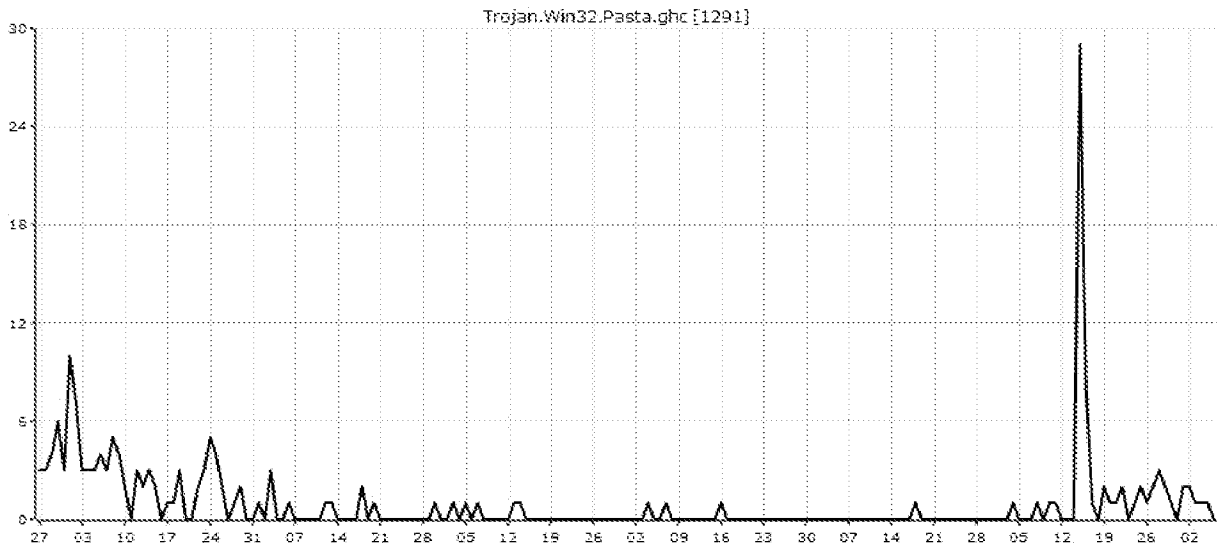


图 8

假设检验汇总				
	原假设	测试	sig.	决策者
1	D1000的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.143	保留原假设
2	D1003的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.079	保留原假设
3	D1021的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.584	保留原假设
4	D1022的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.465	保留原假设
5	D1026的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.062	保留原假设
6	D1070的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.207	保留原假设
7	D100000的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.965	保留原假设
8	D400000的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.329	保留原假设
9	D400014的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.994	保留原假设
10	D500003的分布为正态分布, 平均值为-0.00.标准差为1.00	单样本Kolmogorov - Smirnov 检测	.423	保留原假设
显示渐进显著性。显著性水平是.05				

图 9

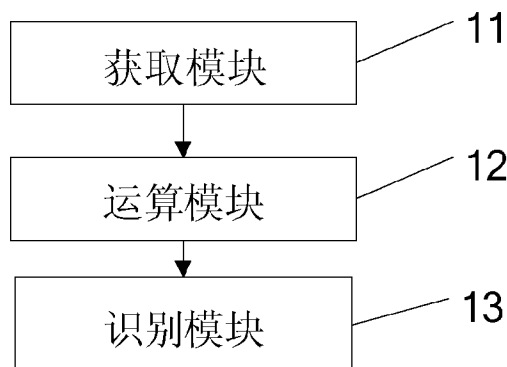


图 10

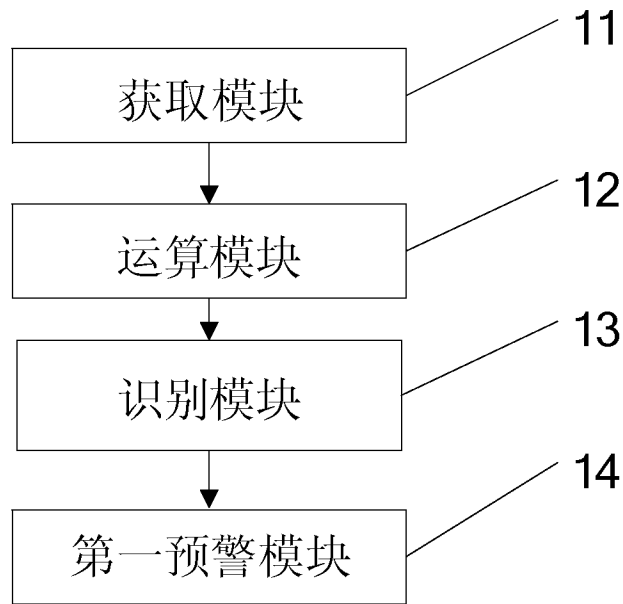


图 11

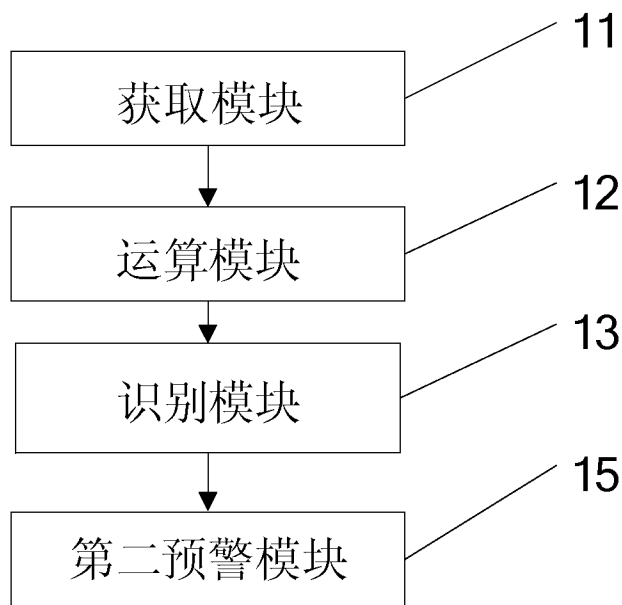


图 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/073357

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

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)

IPC: H04L 12/-; G06F 21/-; H04L 9/-

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)

CNKI; CNPAT; WPI; EPODOC: monitor, moving average, residual, standardization, virus??, trend, uptrend, abnormal, average, mean, deviation, standard, threshold

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 4156540 B2 (KDDI CORP.), 24 September 2008 (24.09.2008), description, paragraphs 0002-0054, and figures 1-5	1-4, 7-11, 14
A	EP 1995929 A2 (DEUTSCHE TELEKOM AG), 26 November 2008 (26.11.2008), the whole document	1-14
A	JP 4723466 B2 (MITSUBISHI ELECTRIC CORPORATION), 13 July 2011 (13.07.2011), the whole document	1-14
A	JP 2009-15427A (NIPPON TELEGRAPH AND TELEPHONE CORP.), 22 January 2009 (22.01.2009), the whole document	1-14
A	US 7936682 B2 (CISCO TECHNOLOGY INC.), 03 May 2011 (03.05.2011), the whole document	1-14
A	US 8112801 B2 (ALCATEL LUCENT), 07 February 2012 (07.02.2012), the whole document	1-14
A	WO 2009/083022 A1 (TELECOM ITALIA S.P.A.), 09 July 2009 (09.07.2009), the whole document	1-14
A	CN 1848745 A (INTERNET SECURITY ONE (CHINA) LTD.), 18 October 2006 (18.10.2006), the whole document	1-14

Further documents are listed in the continuation of Box C.

See patent family annex.

<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“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)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“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</p> <p>“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</p> <p>“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</p> <p>“&” document member of the same patent family</p>
---	---

Date of the actual completion of the international search
13 June 2013 (13.06.2013)

Date of mailing of the international search report
04 July 2013 (04.07.2013)

Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer
SONG, Jie
Telephone No.: (86-10) **82245961**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/073357

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 4156540 B2	24.09.2008	JP 2005-236863 A	02.09.2005
EP 1995929 A2	26.11.2008	US 2008/0313734 A1	18.12.2008
		US 7941853 B2	10.05.2011
		EP 1995929 A3	06.03.2013
JP 4723466 B2	13.07.2011	JP 2008-154010 A	03.07.2008
JP 2009-15427 A	22.01.2009	JP 4945344 B2	06.06.2012
US 7936682 B2	03.05.2011	US 2006/098585 A1	11.05.2006
		US 2006/098687 A1	11.05.2006
		US 7535909 B2	19.05.2009
		US 2006/0161986 A1	20.07.2006
		US 8010685 B2	30.08.2011
US 8112801 B2	07.02.2012	US 2009/0044276 A1	12.02.2009
		WO 2008/090531 A2	31.07.2008
		WO 2008/090531 A3	08.01.2009
		WO 2008/142666 A2	27.11.2008
		WO 2008/142666 A3	11.06.2009
		US 2008/0301812 A1	04.12.2008
		US 7917957 B2	29.03.2011
		CN 101589595 A	25.11.2009
		CN 101589595 B	24.04.2013
		EP 2127313 A2	02.12.2009
		US 2009/0328220 A1	31.12.2009
		US 8250645 B2	21.08.2012
		US 2011/0197278 A1	11.08.2011
		US 8020207 B2	13.09.2011
		US 8095981 B2	10.01.2012
WO 2009/083022 A1	09.07.2009	EP 2241072 A1	20.10.2010
		EP 2241072 B1	25.05.2011
		US 2010/0284283 A1	11.11.2010
		AT 511296 T	15.06.2011
CN 1848745 A	18.10.2006	None	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/073357

CLASSIFICATION OF SUBJECT MATTER:

H04L 12/26 (2006.01) i

G06F 21/00 (2013.01) i

H04L 9/00 (2006.01) n

国际检索报告

国际申请号
PCT/CN2013/073357

A. 主题的分类		
参见附加页		
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. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
IPC: H04L12/-; G06F21/-; H04L9/-		
包含在检索领域中的除最低限度文献以外的检索文献		
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))		
CNKI; CNPAT; WPI; EPODOC; 病毒, 趋势, 监控, 异常, 均线, 残差, 标准化, 阈值, virus??, trend, uptrend, abnormal, average, mean, deviation, standard, threshold		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	JP 特许第 4156540 B2 (KDDI 株式会社)24.9 月 2008(24.09.2008) 说明书第 0002-0054 段以及图 1-5	1-4,7-11,14
A	EP1995929 A2 (DEUTSCHE TELEKOM AG)26.11 月 2008 (26.11.2008) 全文	1-14
A	JP 特许第 4723466 B2 (三菱電機株式会社)13.7 月 2011(13.07.2011) 全文	1-14
A	JP 特开 2009-15427A (日本電信電話株式会社)22.1 月 2009(22.01.2009) 全文	1-14
A	US7936682 B2 (CISCO TECHNOLOGY INC.)3.5 月 2011(03.05.2011) 全文	1-14
A	US8112801 B2 (ALCATEL LUCENT)7.2 月 2012 (07.02.2012) 全文	1-14
A	WO2009/083022 A1 (TELECOM ITALIA S.P.A.)9.7 月 2009 (09.07.2009) 全文	1-14
A	CN1848745 A (安氏互联网安全系统(中国)有限公司)18.10 月 2006(18.10.2006) 全文	1-14
<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:		
“A” 认为不特别相关的表示了现有技术一般状态的文件		“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
“E” 在国际申请日的当天或之后公布的在先申请或专利		“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
“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)		“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
“O” 涉及口头公开、使用、展览或其他方式公开的文件		“&” 同族专利的文件
“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		
国际检索实际完成的日期	13.6 月 2013(13.06.2013)	国际检索报告邮寄日期 04.7 月 2013 (04.07.2013)
ISA/CN 的名称和邮寄地址:	中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451	受权官员 宋洁 电话号码: (86-10) 82245961

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/073357

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
JP 特许第 4156540 B2	24.09.2008	JP 特开 2005-236863A	02.09.2005
EP1995929 A2	26.11.2008	US2008/0313734A1	18.12.2008
		US7941853B2	10.05.2011
		EP1995929 A3	06.03.2013
JP 特许第 4723466 B2	13.07.2011	JP 特开 2008-154010A	03.07.2008
JP 特开 2009-15427A	22.01.2009	JP 特许第 4945344B2	06.06.2012
US7936682 B2	03.05.2011	US2006/098585A1	11.05.2006
		US2006/098687A1	11.05.2006
		US7535909B2	19.05.2009
		US2006/0161986A1	20.07.206
		US8010685B2	30.08.2011
US8112801 B2	07.02.2012	US2009/0044276A1	12.02.2009
		WO2008/090531A2	31.07.2008
		WO2008/090531A3	08.01.2009
		WO2008/142666A2	27.11.2008
		WO2008/142666A3	11.06.2009
		US2008/0301812A1	04.12.2008
		US7917957B2	29.03.2011
		CN101589595A	25.11.2009
		CN101589595B	24.04.2013
		EP2127313A2	02.12.2009
		US2009/0328220A1	31.12.2009
		US8250645B2	21.08.2012
		US2011/0197278A1	11.08.2011
		US8020207B2	13.09.2011
		US8095981B2	10.01.2012
WO2009/083022 A1	09.07.2009	EP2241072A1	20.10.2010
		EP2241072B1	25.05.2011
		US2010/0284283A1	11.11.2010
		AT511296T	15.06.2011
CN1848745 A	18.10.2006	无	

主题的分类:

H04L12/26 (2006.01) i

G06F21/00 (2013.01) i

H04L9/00 (2006.01) n