(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
2020 年 7 月 2 日 (02.07.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/135755 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *G06F 21/60* (2013.01)
G06F 21/55 (2013.01) *H04L 12/40* (2006.01)

(21) 国际申请号: PCT/CN2019/129315

(22) 国际申请日: 2019 年 12 月 27 日 (27.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811639337.1 2018年12月29日 (29.12.2018) CN

(71) 申请人: 北 京 奇 虎 科 技 有 限 公 司 **(BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。

(72) 发明人: 刘健皓 **(LIU, Jianhao)**; 中国北京市西城区新街口外大街28号D座112室 (德胜园区), Beijing (CN)。 曹明革**(CAO, Mingge)**; 中国北京市西城区新街口外大街28号D座112室 (德胜园区), Beijing (CN)。

(74) 代理人: 北京市浩天知识产权代理事务所 (普通合伙) **(HYLANDS LAW FIRM)**; 中国北京市朝阳区朝阳门外大街18号丰联广场A座15层1511, Beijing 100020 (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, JO, JP, KE, KG, KH, 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,

(54) **Title:** VEHICLE ATTACK DETECTION METHOD AND APPARATUS

(54) **发明名称**: 车辆攻击检测方法及装置

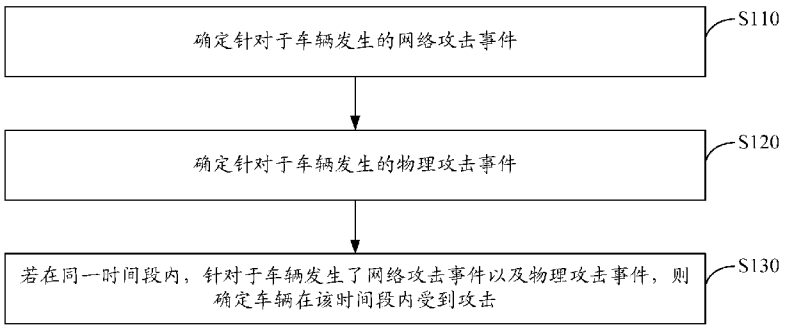

图 1

S110 Determine a network attack event occurring to a vehicle
S120 Determine a physical attack event occurring to the vehicle
S130 If the network attack event and the physical attack event occur to the vehicle in the same time period, determine that the vehicle is attacked in this time period

(57) **Abstract:** Disclosed are a vehicle attack detection method and apparatus. The method comprises: determining a network attack event occurring to a vehicle; determining a physical attack event occurring to the vehicle; and if the network attack event and the physical attack event occur to the vehicle in the same time period, determining that the vehicle is attacked in this time period.

(57) **摘要**: 本公开公开了一种车辆攻击检测方法及装置。其中，方法包括：确定针对于车辆发生的网络攻击事件；以及，确定针对于车辆发生的物理攻击事件；若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。

WO 2020/135755 A1

[见续页]

NA, 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))。

车辆攻击检测方法及装置

相关申请的交叉参考

本申请要求于 2018 年 12 月 29 日提交中国专利局、申请号为 201811639337.1、名称为“车辆攻击检测方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本公开涉及车辆安全技术领域，具体涉及一种车辆攻击检测方法及装置。

背景技术

随着科技及社会的不断发展，各类智能化、自动化车辆的出现极大地方便了人们的工作与生活，但同时也催生了许多针对车辆的安全威胁。例如，车辆中的可编程化或可远程控制化的智能单元为非法入侵者提供了新的入侵渠道，从而对人们的财产及生命安全造成极大威胁。

为保障车辆安全，实现对车辆的安全防护，首先需通过相应的检测方法检测车辆受到的攻击。目前，针对车辆的攻击检测仅仅局限于，在网络空间中检测是否存在针对车辆的攻击行为，若网络空间中存在针对车辆的攻击行为，则确定车辆受到攻击。然而，该检测方法检测到的车辆攻击误报率较高，检测准确度低，不利于对车辆的安全防护。

发明内容

鉴于上述问题，提出了本公开以便提供一种克服上述问题或者至少部分地解决上述问题的车辆攻击检测方法及装置。

根据本公开的一个方面，提供了一种车辆攻击检测方法，包括:

确定针对于车辆发生的网络攻击事件；以及，

确定针对于车辆发生的物理攻击事件;

若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。

根据本公开的另一方面，提供了一种车辆攻击检测装置，包括：

网络攻击检测单元，适于确定针对于车辆发生的网络攻击事件；

物理攻击检测单元，适于确定针对于车辆发生的物理攻击事件；

确定单元，适于若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。

根据本公开的又一方面，提供了一种计算设备，包括：处理器、存储器、通信接口和通信总线，处理器、存储器和通信接口通过通信总线完成相互间的通信；

存储器用于存放至少一可执行指令，可执行指令使处理器执行上述车辆攻击检测方法对应的操作。

根据本公开的再一方面，提供了一种非易失性计算机可读存储介质，该非易失性计算机可读存储介质中存储有至少一可执行指令，可执行指令使处理器执行如上述车辆攻击检测方法对应的操作。

根据本公开的再又一方面，还提供了一种计算机程序产品，该计算机程序产品包括存储在上述非易失性计算机可读存储介质上的计算程序。

根据本公开提供的车辆攻击检测方法及装置，确定针对于车辆发生的网络攻击事件；以及，确定针对于车辆发生的物理攻击事件；若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。本方案根据车辆在网络空间以及物理空间受到的攻击事件，多维度地对车辆进行攻击检测，从而可以大幅降低误报率，提升攻击检测的准确度，为实现车辆的安全防护提供基础；并且，本方案简单易行，易于大规模实施与应用。

上述说明仅是本公开技术方案的概述，为了能够更清楚了解本公开的技术手段，而可依照说明书的内容予以实施，并且为了让本公开的上述和其它目的、特征和优点能够更明显易懂，以下特举本公开的具体实施方式。

附图概述

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，

而并不认为是对本公开的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本公开一个实施例提供的一种车辆攻击检测方法的流程示意图；

图 2 示出了根据本公开另一个实施例提供的一种车辆攻击检测方法的流程示意图；

图 3 示出了根据本公开的又一个实施例提供的一种车辆攻击检测方法的流程示意图；

图 4 示出了根据本公开一个实施例提供的一种车辆攻击检测装置的结构示意图；

图 5 示出了根据本公开一个实施例提供的一种计算设备的结构示意图。

本公开的较佳实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

本公开所提供的车辆攻击检测方法及装置具体可用于，基于 CAN（Controller Area Network，控制器局域网络）总线结构的车辆的攻击检测。

图 1 示出了根据本公开一个实施例提供的一种车辆攻击检测方法的流程示意图。如图 1 所示，该方法包括：

步骤 S110，确定针对于车辆发生的网络攻击事件。

其中，本步骤可由车辆中的联网单元（如车载路由设备、车载娱乐单元等等）来执行；或者，本步骤也可由云端服务器执行，并由云端服务器下发确定结果至车辆，由车辆中的联网单元接收确定结果。

在实际的实施过程中，可确定车辆在网络空间中所受到的网络攻击事件。其中，本实施例对车辆受到的网络攻击事件的具体确定方法不做限定，例如，可利用白名单、沙箱、行为检测、和/或特征检测技术，确定针对于车

辆发生的网络攻击事件，如可通过指令白名单的方式，判断下发至车辆的网络指令是否位于预设的指令白名单中，若否，则确定针对于车辆发生了网络攻击事件。

步骤 S120，确定针对于车辆发生的物理攻击事件。

与现有技术不同的是，本实施例除了确定针对于车辆发生的网络攻击事件之外，还进一步确定针对于车辆发生的物理攻击事件。其中，在确定针对于车辆发生的物理攻击事件时，具体是根据车辆总线中的模拟信号进行确定，例如，可通过对车辆总线中模拟信号的来源合法性，判断是否发生针对车辆的物理攻击事件。本实施例对确定针对于车辆发生的物理攻击事件的具体实施方式不做限定。

其中，本步骤可由设置于车辆中的物理攻击检测单元执行，该物理攻击检测检测单元可搭载于车辆 CAN 总线中。可选地，为降低攻击检测的漏报率，可在每一路 CAN 总线中均搭载一物理攻击检测单元，也可以将物理攻击检测单元设置于各路 CAN 总线共同连接的网关中，并由设置于网关中的物理攻击检测单元监控每一路 CAN 总线发生的物理攻击事件，该设置方式可较大程度地降低成本。

本实施例对步骤 S110 以及步骤 S120 的具体执行顺序不做限定，两者可以顺序或并行执行。

步骤 S130，若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。

本实施例通过网络空间以及物理空间两个维度来对车辆进行攻击检测，可大幅降低攻击检测的误报率，提升攻击检测的准确率。

具体地，本实施例在确定车辆发生网络攻击事件以及物理攻击事件时，分别记录有网络攻击事件以及物理攻击事各自对应的攻击时间，当确定在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。

其中，本实施对该同一时间段的时间段长度不做限定。本领域技术人员可根据攻击检测的精度需求设置相应的时间段长度；和/或，基于对历史的攻

击事件的大数据分析，确定时间段长度；和/或，可根据确定的网络攻击事件以及物理攻击事件的攻击事件的类型，确定相应的时间段长度，即本实施例可预先为不同的攻击事件类型配置对应的时间段长度。

由此可见，本实施例中从网络空间以及物理空间两个维度来对车辆进行攻击检测，当在同一时间段内，针对于车辆既发生了网络攻击事件，又发生了物理攻击事件时，确定车辆在该时间段内受到攻击，从而可大幅降低攻击误报率，提升车辆攻击检测精度，从而为实现车辆的安全防护提供基础；并且，本方案简单易行，易于大规模实施与应用。

图 2 示出了根据本公开另一个实施例提供的一种车辆攻击检测方法的流程示意图。如图 2 所示，该方法包括：

步骤 S210，确定是否针对于车辆发生了网络攻击事件；若是，则确定该网络攻击事件对应的时间段。

其中，本实施例对确定车辆发生网络攻击事件的具体方法不做限定，例如，可采用以下实施方式中的一种或多种的结合来确定是否针对于车辆发生了网络攻击事件：

在一种实施方式中，可在车辆的联网单元中配置相应的指令白名单，当车辆中的联网单元接收到网络指令时，判断接收到的网络指令是否位于指令白名单中，若否，则确定车辆发生了网络攻击事件；或者，也可在车辆的联网单元中配置相应的指令黑名单，当车辆中的联网单元接收到网络指令时，判断接收到的网络指令是否位于指令黑名单中，若是，则确定车辆发生了网络攻击事件。可选地，指令白名单和/或指令黑名单可根据云端服务器中的数据进行动态更新。云端服务器可根据车联网系统中车辆数据的分析，确定出相应的指令白名单或指令黑名单，并下发至车辆，从而车辆可根据云端服务器下发的指令白名单和/或指令黑名单进行减量或增量更新。可选地，为进一步地提升车辆的攻击检测精度，以及减少车辆联网单元的存储压力，云端服务器可进一步对指令白名单和/或指令黑名单进行细粒度的划分，为不同类型的车辆或不同的车辆个体，配置相应的指令白名单和/或指令黑名单，从而实现针对于车辆的指令白名单或指令黑名单的定制化，提高车辆的攻击检测效果。

在另一种实施方式中，可利用沙箱检测技术来确定针对于车辆发生的网络攻击事件。在具体的实施过程中，可将网络指令置于沙箱环境中，根据网络指令在沙箱中的执行结果来确定车辆是否发生网络攻击事件。可选地，本实施方式可具体与指令白名单和/或指令黑名单结合使用，即当网络指令未位于指令白名单时，进一步将该网络指令置于沙箱环境中，进而确定车辆是否发生网络攻击事件。

在此，本领域技术人员应当理解的是，确定是否针对于车辆发生了网络攻击事件的方法不仅仅包含以上两种方式或两种方式的组合，例如，还可根据行为检测技术和/或特征检测技术确定针对于车辆发生的网络攻击事件。本领域技术人员可根据实际情况选择相应的检测方法，本实施例在此不做限定。

若通过相应的检测方法确定针对于车辆发生了网络攻击事件，则进一步确定发生的网络攻击事件对应的时间段。在确定网络攻击事件对应的时间段时，可首先确定网络攻击事件对应的时间点以及预设的时间段长度，并进一步根据网络攻击事件对应的时间点以及预设的时间段长度，确定网络攻击事件对应的时间段。其中，在根据网络攻击事件对应的时间点以及预设的时间段长度，确定网络攻击事件对应的时间段过程中，可以以网络攻击事件对应的时间点为该时间段的起点，以网络攻击事件对应的时间点与预设的时间段长度之和作为该时间段的终点；又或者，以网络攻击事件对应的时间点与预设的时间段长度的一半的差值作为该时间段的起点，以网络攻击事件对应的时间点与预设的时间段长度的一半的和作为该时间段的终点，例如，若网络攻击事件对应的时间点为 a，而预设的时间段长度为 b，则网络攻击事件对应的时间段可以为（a，a+b），或者，（a-b/2，a+b/2）。

步骤 S220，判断在该时间段内，是否发生了针对于车辆的物理攻击事件；若是，则确定在该时间段内车辆受到攻击。

判断在步骤 S210 中确定的时间段内，是否发生了针对于车辆的物理攻击事件。其中，在确定针对于车辆发生的物理攻击事件时，可由搭载于车辆总线中的物理攻击检测检测单元对车辆总线中的数据报文进行监测，根据监测结果确定在该时间段内是否发生了针对于车辆的物理攻击事件。

在一种可选的实施方式中，可监测车辆总线中的数据报文，判断数据报文是否来自于合法的电子控制单元（ECU，Electronic Control Unit）；若否，则确定针对于车辆发生了物理攻击事件。其中，在判断数据报文是否来自于合法的电子控制单元时，需先确定发出数据报文的电子控制单元，车辆中不同的电子控制单元发出同一数据报文所对应的模拟信号声纹不同（该模拟信号声纹具体是指模拟信号的特征数据，例如可将模拟信号进行相应的数学转换后获得的数据作为模拟信号声纹，如模拟信号的差分信号电压等等。其中，可通过机器学习等方法预先确定出至少一个电子控制单元发出的至少一条数据报文的模拟信号声纹）。所以，可对数据报文进行解析，获得与数据报文对应的模拟信号声纹，并根据模拟信号声纹确定发出数据报文的电子控制单元。进一步地，车辆中的电子控制单元仅可发出某类或某几类数据报文，例如，车辆中的转向控制报文仅能由转向控制单元发出。因此，在确定发出数据报文的电子控制单元之后，判断发出数据报文的电子控制单元是否位于该数据报文对应的电子控制单元白名单中；若否，则确定针对于车辆发生了物理攻击事件。

在又一种实施方式中，可监测车辆总线中的数据报文，对数据报文进行解析，获得与数据报文对应的模拟信号声纹；并判断与数据报文对应的模拟信号声纹是否与该数据报文对应的标准模拟信号声纹相匹配；若否，则确定针对于车辆发生了物理攻击事件。在具体的实施过程中，针对于同一数据报文，不同的电子控制单元发出同一数据报文所解析出的模拟信号不同，而不同的模拟信号所对应的模拟信号声纹不同，则表明不同的电子控制单元发出同一数据报文所对应的模拟信号声纹不同。因此，针对于数据报文，可预先确定出合法的电子控制单元发出该数据报文的模拟信号，进而将合法的电子控制单元发出的该数据报文的模拟信号声纹作为与该数据报文对应的标准模拟信号声纹，从而，在确定针对于车辆发生的物理攻击事件过程中，可判断与数据报文对应的模拟信号声纹是否与该数据报文对应的标准模拟信号声纹相匹配；若否，则确定针对于车辆发生了物理攻击事件。

若在确定的时间段内，发生了针对于车辆的物理攻击事件，则确定在该确定的时间段内车辆受到攻击。

可选地，在确定车辆受到攻击之后，可进一步地发出相应的告警信息，从而可供对攻击行为进行快速阻断。

由此可见，本实施例从网络空间以及物理空间两个维度来对车辆进行攻击检测，当确定针对于车辆发生了网络攻击事件后，判断在与该网络攻击事件对应的时间段，进而当在确定的时间段内，发生了针对于车辆的物理攻击事件时，确定车辆受到攻击，从而可大幅降低攻击误报率，提升车辆攻击检测精度，从而为实现车辆的安全防护提供基础；并且，本实施例通过确定车辆总线中数据报文是否来源于合法的电子控制单元，和/或，确定数据报文对应的模拟信号声纹是否与数据报文对应的标准模拟信号声纹相匹配，来确定针对于车辆发生的物理攻击事件，可大幅提升物理攻击事件的检测效率及检测精度。

图 3 示出了根据本公开又一个实施例提供的一种车辆攻击检测方法的流程示意图。如图 3 所示，该方法包括:

步骤 S310，确定是否针对于车辆发生了物理攻击事件；若是，则确定该物理攻击事件对应的时间段。

步骤 S320，判断在该时间段内，是否发生了针对于车辆的网络攻击事件；若是，则确定在该时间段内车辆受到攻击。

其中，步骤 S310 及步骤 S320 的具体实施方式可参照步骤 S210 及步骤 S220 中相应描述，本实施例在此不做赘述。

由此可见，本实施例从网络空间以及物理空间两个维度来对车辆进行攻击检测，当确定针对于车辆发生了物理攻击事件后，判断在与该物理攻击事件对应的时间段，进而当在确定的时间段内，发生了针对于车辆的网络攻击事件时，确定车辆受到攻击，从而可大幅降低攻击误报率，提升车辆攻击检测精度，从而为实现车辆的安全防护提供基础；并且，本实施例通过确定车辆总线中数据报文是否来源于合法的电子控制单元，和/或，确定数据报文对应的模拟信号声纹是否与数据报文对应的标准模拟信号声纹相匹配，来确定针对于车辆发生的物理攻击事件，可大幅提升物理攻击事件的检测效率及检测精度。

图 4 示出了根据本公开一个实施例提供的一种车辆攻击检测装置的结构

示意图。如图 4 所示，该装置包括：网络攻击检测单元 41、物理攻击检测单元 42 以及确定单元 43。

网络攻击检测单元 41，适于确定针对于车辆发生的网络攻击事件。可选的，网络攻击检测单元 41 可以为车辆中的联网单元。

物理攻击检测单元 42，适于确定针对于车辆发生的物理攻击事件。其中，物理攻击检测单元 42 可搭载于车辆总线中。可选地，可将物理攻击检测单元 42 设置于各路车辆总线共同连接的网关中，并由设置于网关中的物理攻击检测单元 42 监控每一路车辆总线发生的物理攻击事件，从而可较大程度地降低成本；又或者，可在每一路车辆总线中均搭载一物理攻击检测单元 42，从而避免当网关受到入侵时导致整个车辆中的物理攻击事件无法监控的弊端。

确定单元 43，适于若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。其中，该模块可由搭载于车辆总线中专门的处理单元执行，也可以集成于网络攻击检测单元 41 或物理攻击检测单元 42 中。

可选地，物理攻击检测单元 42 进一步适于：监测车辆总线中的数据报文，判断数据报文是否来自于合法的电子控制单元；若否，则确定针对于车辆发生了物理攻击事件。

可选地，物理攻击检测单元 42 进一步适于：确定发出数据报文的电子控制单元，并判断发出数据报文的电子控制单元是否位于数据报文对应的电子控制单元白名单中；若否，则确定针对于车辆发生了物理攻击事件。

可选地，物理攻击检测单元 42 进一步适于：对数据报文进行解析，获得与数据报文对应的模拟信号声纹；根据模拟信号声纹确定发出数据报文的电子控制单元。

可选地，物理攻击检测单元 42 进一步适于：监测车辆总线中的数据报文，对数据报文进行解析，获得与数据报文对应的模拟信号声纹；判断与数据报文对应的模拟信号声纹是否与数据报文对应的标准模拟信号声纹相匹配；若否，则确定针对于车辆发生了物理攻击事件。

可选地，不同的电子控制单元发出同一数据报文所对应的模拟信号声纹不同。

可选地，网络攻击检测单元 41 进一步适于：利用白名单、沙箱、行为检测、和/或特征检测技术，确定针对于车辆发生的网络攻击事件。

可选地，网络攻击检测单元 41 进一步适于：确定是否针对于车辆发生了网络攻击事件；若是，则确定网络攻击事件对应的时间段；

物理攻击检测单元 42 进一步适于：判断在确定的时间段内，是否发生了针对于车辆的物理攻击事件；

确定单元 43 进一步适于：若在确定的时间段内，发生了针对于车辆的物理攻击事件，则确定在确定的时间段内车辆受到攻击。

可选地，物理攻击检测单元 42 进一步适于：确定是否针对于车辆发生了物理攻击事件；若是，则确定物理攻击事件对应的时间段；

网络攻击检测单元 41 进一步适于：判断在确定的时间段内，是否发生了针对于车辆的网络攻击事件；

确定单元 43 进一步适于：若在确定的时间段内，发生了针对于车辆的网络攻击事件，则确定在确定的时间段内车辆受到攻击。

其中，本装置中各单元的具体实施过程可参照图 1、图 2、和/或图 3 方法实施例中相应步骤的描述，本实施例在此不做赘述。

由此可见，本实施例中从网络空间以及物理空间两个维度来对车辆进行攻击检测，当在同一时间段内，针对于车辆既发生了网络攻击事件，又发生了物理攻击事件时，确定车辆在该时间段内受到攻击，从而可大幅降低攻击误报率，提升车辆攻击检测精度，从而为实现车辆的安全防护提供基础；并且，本方案简单易行，易于大规模实施与应用。

根据本公开一个实施例提供了一种非易失性计算机可读存储介质，该非易失性计算机可读存储介质存储有至少一可执行指令，该计算机可执行指令可执行上述任意方法实施例中的车辆攻击检测方法。

图 5 示出了根据本公开一个实施例提供的一种计算设备的结构示意图，本公开具体实施例并不对计算设备的具体实现做限定。

如图 5 所示，该计算设备可以包括：处理器(processor)502、通信接口(Communications Interface)504、存储器(memory)506、以及通信总线 508。

其中：

处理器 502、通信接口 504、以及存储器 506 通过通信总线 508 完成相互间的通信。

通信接口 504，用于与其它设备比如客户端或其它服务器等的网元通信。

处理器 502，用于执行程序 510，具体可以执行上述车辆攻击检测方法实施例中的相关步骤。

具体地，程序 510 可以包括程序代码，该程序代码包括计算机操作指令。

处理器 502 可能是中央处理器 CPU，或者是特定集成电路 ASIC（Application Specific Integrated Circuit），或者是被配置成实施本公开实施例的一个或多个集成电路。计算设备包括的一个或多个处理器，可以是同一类型的处理器，如一个或多个 CPU；也可以是不同类型的处理器，如一个或多个 CPU 以及一个或多个 ASIC。

存储器 506，用于存放程序 510。存储器 506 可能包含高速 RAM 存储器，也可能还包括非易失性存储器（non-volatile memory），例如至少一个磁盘存储器。

程序 510 具体可以用于使得处理器 502 执行以下操作：

确定针对于车辆发生的网络攻击事件；以及，

确定针对于车辆发生的物理攻击事件；

若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击。

在一种可选的实施方式中，程序 510 具体可以用于使得处理器 502 执行以下操作：

监测车辆总线中的数据报文，判断数据报文是否来自于合法的电子控制单元；

若否，则确定针对于车辆发生了物理攻击事件。

在一种可选的实施方式中，程序 510 具体可以用于使得处理器 502 执行以下操作:

确定发出数据报文的电子控制单元，并判断发出数据报文的电子控制单元是否位于数据报文对应的电子控制单元白名单中;

若否，则确定针对于车辆发生了物理攻击事件。

在一种可选的实施方式中，程序 510 具体可以用于使得处理器 502 执行以下操作:

对数据报文进行解析，获得与数据报文对应的模拟信号声纹;

根据模拟信号声纹确定发出数据报文的电子控制单元。

在一种可选的实施方式中，程序 510 具体可以用于使得处理器 502 执行以下操作:

监测车辆总线中的数据报文，对数据报文进行解析，获得与数据报文对应的模拟信号声纹;

判断与数据报文对应的模拟信号声纹是否与数据报文对应的标准模拟信号声纹相匹配;

若否，则确定针对于车辆发生了物理攻击事件。

在一种可选的实施方式中，不同的电子控制单元发出同一数据报文所对应的模拟信号声纹不同。

在一种可选的实施方式中，程序 510 具体可以用于使得处理器 502 执行以下操作:

利用白名单、沙箱、行为检测、和/或特征检测技术，确定针对于车辆发生的网络攻击事件。

在一种可选的实施方式中，程序 510 具体可以用于使得处理器 502 执行以下操作:

确定是否针对于车辆发生了网络攻击事件;

若是，则确定网络攻击事件对应的时间段;

判断在确定的时间段内，是否发生了针对于车辆的物理攻击事件;

若在确定的时间段内，发生了针对于车辆的物理攻击事件，则确定在确定的时间段内车辆受到攻击。

在一种可选的实施方式中，程序 510 具体可以用于使得处理器 502 执行以下操作：

确定是否针对于车辆发生了物理攻击事件；

若是，则确定物理攻击事件对应的时间段；

判断在确定的时间段内，是否发生了针对于车辆的网络攻击事件；

若在确定的时间段内，发生了针对于车辆的网络攻击事件，则确定在确定的时间段内车辆受到攻击。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本公开也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本公开的内容，并且上面对特定语言所做的描述是为了披露本公开的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本公开的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个公开方面中的一个或多个，在上面对本公开的示例性实施例的描述中，本公开的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本公开要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，公开方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本公开的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可

以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本公开的范围之内并且形成不同的实施例。例如，在权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本公开的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本公开实施例中车辆攻击检测装置中的一些或者全部部件的一些或者全部功能。本公开还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本公开的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

应该注意的是上述实施例对本公开进行说明而不是对本公开进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本公开可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

权 利 要 求 书

1. 一种车辆攻击检测方法，包括:

确定针对于车辆发生的网络攻击事件；以及，

确定针对于车辆发生的物理攻击事件;

若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定所述车辆在所述时间段内受到攻击。

2. 根据权利要求 1 所述的方法，其中，所述确定针对于车辆发生的物理攻击事件进一步包括:

监测车辆总线中的数据报文，判断所述数据报文是否来自于合法的电子控制单元;

若否，则确定针对于车辆发生了物理攻击事件。

3. 根据权利要求 2 所述的方法，其中，所述判断所述数据报文是否来自于合法的电子控制单元；若否，则确定针对于车辆发生了物理攻击事件进一步包括:

确定发出所述数据报文的电子控制单元，并判断发出所述数据报文的电子控制单元是否位于所述数据报文对应的电子控制单元白名单中;

若否，则确定针对于车辆发生了物理攻击事件。

4. 根据权利要求 3 所述的方法，其中，所述确定发出所述数据报文的电子控制单元进一步包括:

对所述数据报文进行解析，获得与所述数据报文对应的模拟信号声纹;

根据所述模拟信号声纹确定发出所述数据报文的电子控制单元。

5. 根据权利要求 1-4 中任一项所述的方法，其中，所述确定针对于车辆发生的物理攻击事件进一步包括:

监测车辆总线中的数据报文，对所述数据报文进行解析，获得与所述数据报文对应的模拟信号声纹;

判断与所述数据报文对应的模拟信号声纹是否与所述数据报文对应的标准模拟信号声纹相匹配;

若否，则确定针对于车辆发生了物理攻击事件。

6. 根据权利要求 4 或 5 所述的方法，其中，不同的电子控制单元发出同一数据报文所对应的模拟信号声纹不同。

7. 根据权利要求 1-6 中任一项所述的方法，其中，所述确定针对于车辆发生的网络攻击事件进一步包括:

利用白名单、沙箱、行为检测、和/或特征检测技术，确定针对于车辆发生的网络攻击事件。

8. 根据权利要求 1-7 中任一项所述的方法，其中，所述确定针对于车辆发生的网络攻击事件；以及，确定针对于车辆发生的物理攻击事件；若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定所述车辆在所述时间段内受到攻击进一步包括:

确定是否针对于车辆发生了网络攻击事件;

若是，则确定所述网络攻击事件对应的时间段;

判断在确定的时间段内，是否发生了针对于所述车辆的物理攻击事件;

若在确定的时间段内，发生了针对于所述车辆的物理攻击事件，则确定在所述确定的时间段内车辆受到攻击。

9. 根据权利要求 1-7 中任一项所述的方法，其中，所述确定针对于车辆发生的网络攻击事件；以及，确定针对于车辆发生的物理攻击事件；若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定所述车辆在所述时间段内受到攻击进一步包括:

确定是否针对于车辆发生了物理攻击事件;

若是，则确定所述物理攻击事件对应的时间段;

判断在确定的时间段内，是否发生了针对于所述车辆的网络攻击事件;

若在确定的时间段内，发生了针对于所述车辆的网络攻击事件，则确定在所述确定的时间段内车辆受到攻击。

10. 一种车辆攻击检测装置，包括:

网络攻击检测单元，适于确定针对于车辆发生的网络攻击事件;

物理攻击检测单元，适于确定针对于车辆发生的物理攻击事件;

确定单元，适于若在同一时间段内，针对于车辆发生了网络攻击事件以

及物理攻击事件，则确定所述车辆在所述时间段内受到攻击。

11. 根据权利要求 10 所述的装置，其中，所述物理攻击检测单元进一步适于：

监测车辆总线中的数据报文，判断所述数据报文是否来自于合法的电子控制单元；

若否，则确定针对于车辆发生了物理攻击事件。

12. 根据权利要求 11 所述的装置，其中，所述物理攻击检测单元进一步适于：

确定发出所述数据报文的电子控制单元，并判断发出所述数据报文的电子控制单元是否位于所述数据报文对应的电子控制单元白名单中；

若否，则确定针对于车辆发生了物理攻击事件。

13. 根据权利要求 12 所述的装置，其中，所述物理攻击检测单元进一步适于：

对所述数据报文进行解析，获得与所述数据报文对应的模拟信号声纹；

根据所述模拟信号声纹确定发出所述数据报文的电子控制单元。

14. 根据权利要求 10-13 中任一项所述的装置，其中，所述物理攻击检测单元进一步适于：

监测车辆总线中的数据报文，对所述数据报文进行解析，获得与所述数据报文对应的模拟信号声纹；

判断与所述数据报文对应的模拟信号声纹是否与所述数据报文对应的标准模拟信号声纹相匹配；

若否，则确定针对于车辆发生了物理攻击事件。

15. 根据权利要求 13 或 14 所述的装置，其中，不同的电子控制单元发出同一数据报文所对应的模拟信号声纹不同。

16. 根据权利要求 10-15 中任一项所述的装置，其中，所述网络攻击检测单元进一步适于：

利用白名单、沙箱、行为检测、和/或特征检测技术，确定针对于车辆发生的网络攻击事件。

17. 根据权利要求 10-16 中任一项所述的装置，其中，所述网络攻击检测单元进一步适于：确定是否针对于车辆发生了网络攻击事件；若是，则确定所述网络攻击事件对应的时间段；

所述物理攻击检测单元进一步适于：判断在确定的时间段内，是否发生了针对于所述车辆的物理攻击事件；

所述确定单元进一步适于：若在确定的时间段内，发生了针对于所述车辆的物理攻击事件，则确定在所述确定的时间段内车辆受到攻击。

18. 根据权利要求 10-16 中任一项所述的装置，其中，

所述物理攻击检测单元进一步适于：确定是否针对于车辆发生了物理攻击事件；若是，则确定所述物理攻击事件对应的时间段；

所述网络攻击检测单元进一步适于：判断在确定的时间段内，是否发生了针对于所述车辆的网络攻击事件；

所述确定单元进一步适于：若在确定的时间段内，发生了针对于所述车辆的网络攻击事件，则确定在所述确定的时间段内车辆受到攻击。

19. 一种计算设备，包括：处理器、存储器、通信接口和通信总线，所述处理器、所述存储器和所述通信接口通过所述通信总线完成相互间的通信；

所述存储器用于存放至少一可执行指令，所述可执行指令使所述处理器执行如权利要求 1-9 中任一项所述的车辆攻击检测方法对应的操作。

20. 一种非易失性计算机可读存储介质，所述非易失性计算机存储介质中存储有至少一可执行指令，所述可执行指令使处理器执行如权利要求 1-9 中任一项所述的车辆攻击检测方法对应的操作。

21. 一种计算机程序产品，该计算机程序产品包括存储在非易失性计算机可读存储介质上的计算机程序，该计算机程序包括程序指令，当该程序指令被处理器执行时，使该处理器执行如权利要求 1-9 中任一项所述的车辆攻击检测方法对应的操作。

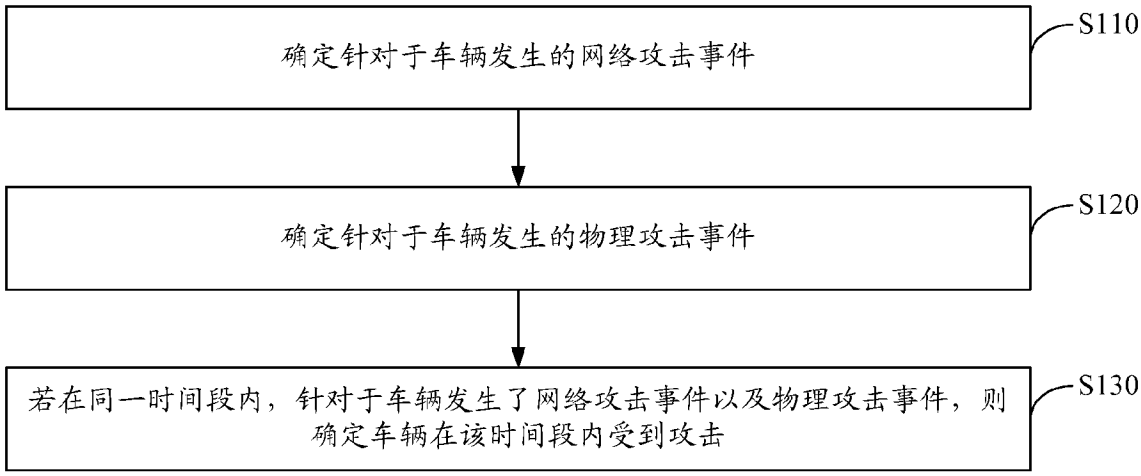
确定针对于车辆发生的网络攻击事件
S110
确定针对于车辆发生的物理攻击事件
S120
若在同一时间段内，针对于车辆发生了网络攻击事件以及物理攻击事件，则确定车辆在该时间段内受到攻击
S130

图 1

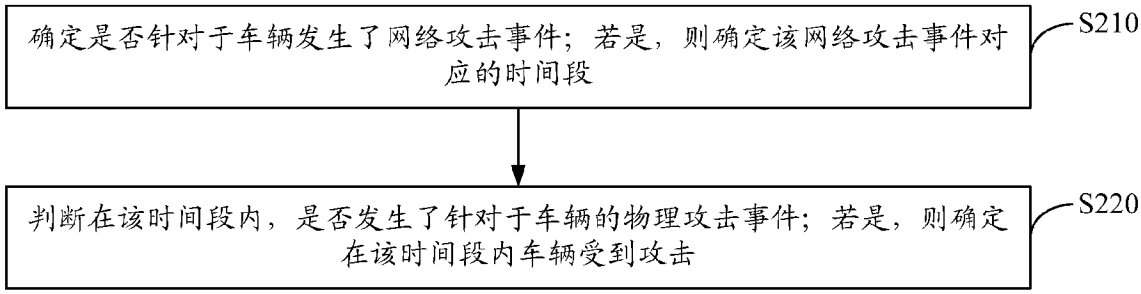
确定是否针对于车辆发生了网络攻击事件；若是，则确定该网络攻击事件对应的时间段
S210
判断在该时间段内，是否发生了针对于车辆的物理攻击事件；若是，则确定在该时间段内车辆受到攻击
S220

图 2

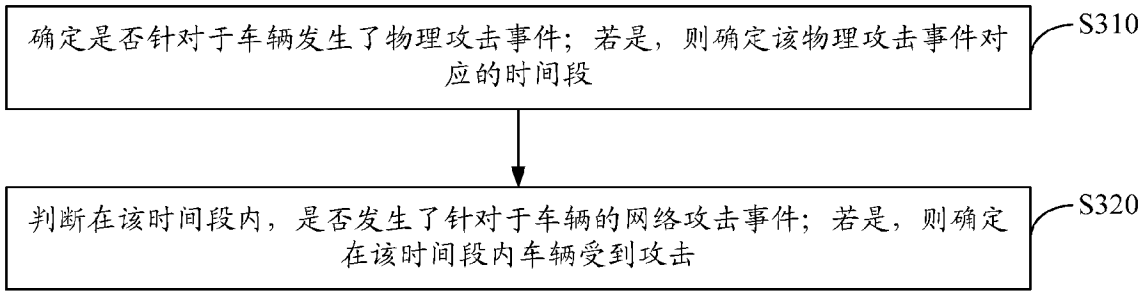
确定是否针对于车辆发生了物理攻击事件；若是，则确定该物理攻击事件对应的时间段
S310
判断在该时间段内，是否发生了针对于车辆的网络攻击事件；若是，则确定在该时间段内车辆受到攻击
S320

图 3

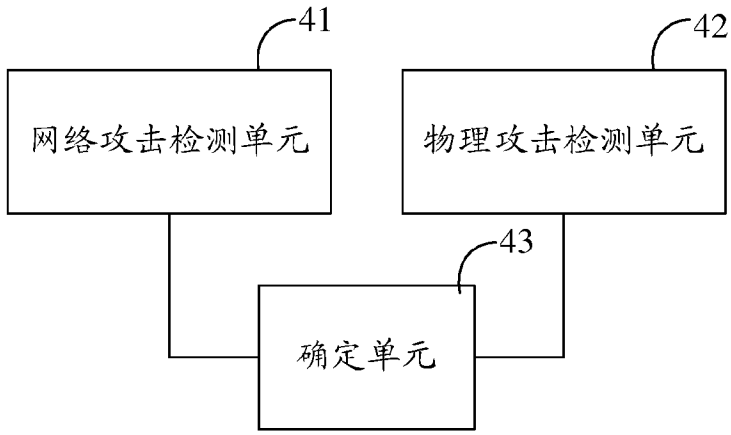
41
网络攻击检测单元
42
物理攻击检测单元
43
确定单元

图 4

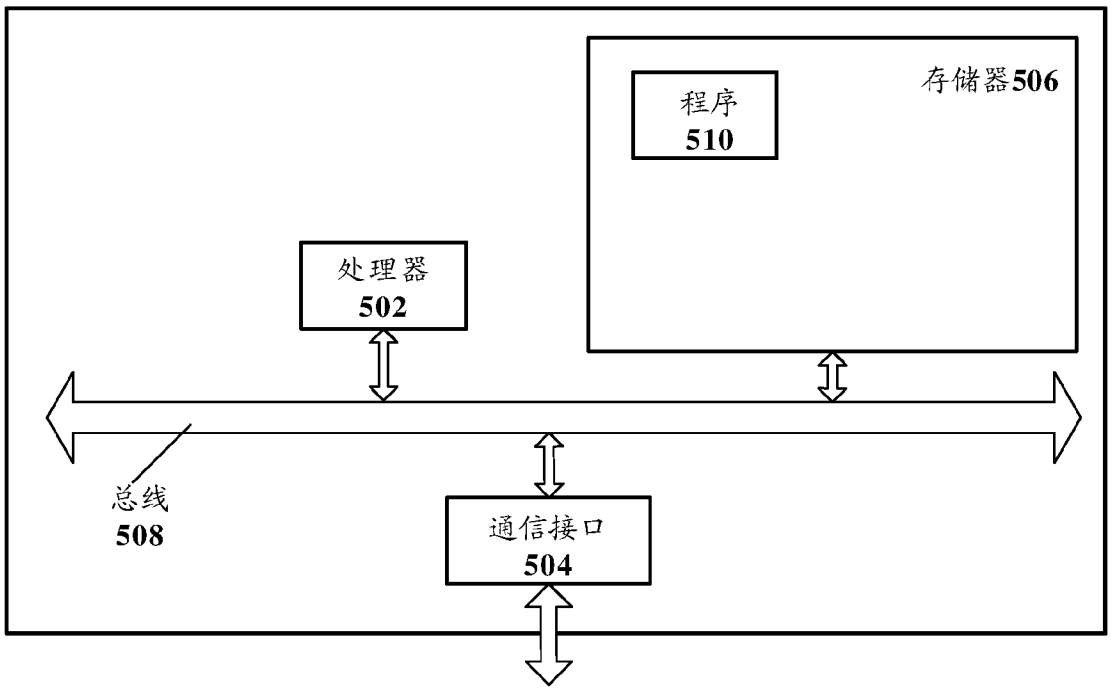

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/129315

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; G06F 21/55(2013.01)i; G06F 21/60(2013.01)i; H04L 12/40(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; G06F

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)

CNABS; CNTXT; CNKI; VEN; USTXT; WOTXT; EPTXT; PATENTICS: 奇虎, 车辆, 汽车, 车联网, 车载, 检测, 辨别, 识别, 监测, 网络, 物理, 总线, 攻击, 异常, 安全, 风险, 入侵, 威胁, 事件, 误报, 时间, 相关性, 时间段, 同时, Vehicle, internet, cyber, network, physical, CAN, Controller area network, bus, attack+, security, threat, intrusion, detect+, monitor+, discern+, notif+, period, event

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 106790153 A (BEIJING TOPSEC NETWORK SECURITY TECHNOLOGY CO., LTD. et al.) 31 May 2017 (2017-05-31) description, paragraphs [0049]-[0097]	1-21
A	US 2013347060 A1 (VERINT SYSTEMS LTD) 26 December 2013 (2013-12-26) entire document	1-21
A	CN 109033829 A (BEIJING BANGCLE SAFETY TECHNOLOGY CO., LTD.) 18 December 2018 (2018-12-18) entire document	1-21
A	CN 105357179 A (SANGFOR NETWORK TECHNOLOGY (SHENZHEN) CO., LTD.) 24 February 2016 (2016-02-24) entire document	1-21

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 2020	**16 March 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/129315

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106790153	A	31 May 2017	CN	106790153	B	28 June 2019
US	2013347060	A1	26 December 2013	EP	2657880	A1	30 October 2013
				US	9767279	B2	19 September 2017
				IL	219361	A	28 September 2017
CN	109033829	A	18 December 2018		None		
CN	105357179	A	24 February 2016	CN	105357179	B	30 October 2018

国际检索报告

国际申请号
PCT/CN2019/129315

A. 主题的分类

H04L 29/06(2006.01)i; G06F 21/55(2013.01)i; G06F 21/60(2013.01)i; H04L 12/40(2006.01)i

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)

H04L; G06F

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）)

CNABS;CNTXT;CNKI;VEN;USTXT;WOTXT;EPTXT;PATENTICS：奇虎，车辆，汽车，车联网，车载，检测，辨别，识别，监测，网络，物理，总线，攻击，异常，安全，风险，入侵，威胁，事件，误报，时间，相关性，时间段，同时，Vehicle，internet，cyber，network，physical，CAN，Controller area network，bus，attack+，security，threat，intrusion，detect+，monitor+，discern+，notif+，period，event

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
A	CN 106790153 A (北京天融信网络安全技术有限公司 等) 2017年 5月 31日 (2017-05-31) 说明书第[0049]-[0097]段	1-21
A	US 2013347060 A1 (VERINT SYSTEMS LTD) 2013年 12月 26日 (2013-12-26) 全文	1-21
A	CN 109033829 A (北京梆梆安全科技有限公司) 2018年 12月 18日 (2018-12-18) 全文	1-21
A	CN 105357179 A (深信服网络科技深圳有限公司) 2016年 2月 24日 (2016-02-24) 全文	1-21

☐ 其余文件在C栏的续页中列出。

☑ 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

“E” 在国际申请日的当天或之后公布的在先申请或专利

“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）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“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

“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

“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

“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

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 2月 14日	2020年 3月 16日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 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 顾莹莹 电话号码 (86-512)88996427

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/129315

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106790153	A	2017年 5月 31日	CN	106790153	B	2019年 6月 28日
US	2013347060	A1	2013年 12月 26日	EP	2657880	A1	2013年 10月 30日
				US	9767279	B2	2017年 9月 19日
				IL	219361	A	2017年 9月 28日
CN	109033829	A	2018年 12月 18日		无		
CN	105357179	A	2016年 2月 24日	CN	105357179	B	2018年 10月 30日