

(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
2024 年 9 月 6 日 (06.09.2024)



(10) 国际公布号
WO 2024/178581 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01)

(21) 国际申请号: PCT/CN2023/078600

(22) 国际申请日: 2023 年 2 月 28 日 (28.02.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 侯硕 (**HOU, Shuo**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。岳青伦 (**YUE, Qinglun**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。李廷森 (**LI, Tingsen**); 中

国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (**TDIP & PARTNERS**); 中国北京市西城区西城区裕民路 18 号北环中心 A 座 2002, Beijing 100029 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) **Title:** DATA PROCESSING METHOD AND APPARATUS, AND STORAGE MEDIUM AND PROGRAM PRODUCT

(54) 发明名称: 一种数据处理方法、装置、存储介质及程序产品

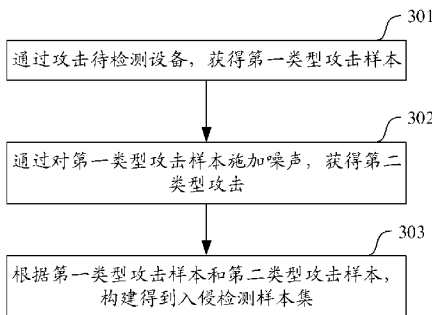


图 3

- 301 Obtain first-type attack samples by means of attacking a device to be tested
302 Obtain second-type attack samples by means of applying noise to the first-type attack samples
303 On the basis of the first-type attack samples and the second-type attack samples, perform construction to obtain an intrusion detection sample set

(57) **Abstract:** A data processing method and apparatus, and a storage medium and a program product, which are applicable to the technical field of network security and are used for constructing a more comprehensive intrusion detection sample set. The method comprises: obtaining first-type attack samples by means of attacking a device to be tested; obtaining second-type attack samples by means of applying noise to the first-type attack samples; and on the basis of the first-type attack samples and the second-type attack samples, performing construction to obtain an intrusion detection sample set. By means of the method, an intrusion detection sample set can cover both attack samples in a known intrusion scenario and attack samples in an unknown intrusion scenario, and intrusion detection samples in the intrusion detection sample set are more comprehensive; furthermore, using the more comprehensive intrusion detection sample set to evaluate a device to be tested can also improve the accuracy of security assessment on the device to be tested.

(57) **摘要:** 一种数据处理方法、装置、存储介质及程序产品, 适用于网络安全技术领域, 用以构建更加全面的入侵检测样本集。其中, 方法包括: 通过攻击待检测设备, 获得第一类型攻击样本, 通过对第一类型攻击样本施加噪声, 获得第二类型攻击样本, 根据第一类型攻击样本和第二类型攻击样本, 构建得到入侵检测样本集。通过该方法, 入侵检测样本集中既能覆盖已知入侵场景下的攻击样本又能覆盖未知入侵场景下的攻击样本, 该入侵检测样本集中的入侵检测样本更加全面, 进而, 使用更加全面的入侵检测样本集测评待检测设备, 也能提高对待检测设备进行安全评估的准确性。

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

一种数据处理方法、装置、存储介质及程序产品

技术领域

本申请涉及网络安全技术领域，提供了一种数据处理方法、装置、存储介质及程序产品。

背景技术

近年来，汽车网络安全攻击事件频发。据了解，仅在 2021 年，全球范围内公开报道的汽车网络安全攻击事件就高达 256 件，相较 2018 年增加了 225%。面对如今智能汽车快速发展的大趋势，汽车网络安全问题也应同样被重视起来。

为了提高汽车的网络安全性，业界针对于某些典型的入侵场景构建了入侵检测样本，并在汽车出厂之前，使用这些入侵检测样本对汽车进行攻击测试，以评估汽车的防攻击性能。虽然这种方式能确保仅出厂防攻击性能较好的汽车，但由于入侵检测样本仅是针对于某些典型的入侵场景构建得到的，因此，该入侵检测样本显然并不全面，不利于提高对汽车进行网络安全评估的准确性。

因此，目前对于汽车入侵检测样本的构建方面，还有待进一步研究。

发明内容

本申请提供一种数据处理方法、装置、存储介质及程序产品，用以构建更加全面的入侵检测样本集，以提高对待检测设备（如车辆）进行网络安全评估的准确性。

第一方面，本申请提供一种数据处理方法，适用于数据处理装置，该数据处理装置可以是具有处理能力的任意设备，如服务器或由多个服务器构成的服务器集群。该方法包括：数据处理装置通过攻击待检测设备，获得第一类型攻击样本，通过对第一类型攻击样本施加噪声，获得第二类型攻击样本，进而根据第一类型攻击样本和第二类型攻击样本，构建得到入侵检测样本集。

在上述设计中，第一类型攻击样本是通过攻击待检测设备而得到的，属于已知入侵场景下的攻击样本，而第二类型攻击样本是通过通过对第一类型攻击样本施加噪声而得到的，可以认为是通过对已知入侵场景下的攻击样本进行一些变形而得到的未知入侵场景下的攻击样本，如此，结合第一类型攻击样本和第二类型攻击样本构建入侵检测样本集，使得入侵检测样本集中既能覆盖已知入侵场景下的攻击样本，又能覆盖未知入侵场景下的攻击样本，从而该入侵检测样本集中的入侵检测样本更加全面，进而，使用更加全面的入侵检测样本集评估待检测设备，也能提高对待检测设备进行网络安全评估的准确性。

一种可能的设计中，第一类型攻击样本可以包括真实攻击样本和模拟攻击样本，其中，真实攻击样本是通过人为攻击待检测设备而得到的，模拟攻击样本是通过攻击工具攻击待检测设备而得到的。

在上述设计中，人为攻击方式能用于构造隐蔽性较强的或依赖业务逻辑的攻击行为，以获取到易于在真实攻击环境中标记的攻击样本，而攻击工具攻击方式则能通过模拟攻击流量的产生，获取到不易在真实攻击环境中标记的攻击样本。如此，通过结合人为攻击方式和攻击工具攻击方式综合构建第一类型攻击样本，能使第一类型攻击样本充分覆盖真实攻击环境中可能存在的各种攻击类型的攻击样本，提高第一类型攻击样本的全面性。

进一步地设计中，真实攻击样本可以对应如下攻击类型中的一项或多项：身份标识号（identity document, ID）不存在攻击、重放攻击、篡改攻击、数据长度错误攻击、信号超出定义范围攻击、上下文错误攻击、ID 来源非指定电子控制单元（electronic control unit, ECU）攻击、出现相同 ID 攻击、控制器局域网络（controller area network, CAN）扫描攻击、统一诊断服务（unified diagnostic services, UDS）执行敏感操作攻击、消息认证错误攻击、ECU 身份欺骗攻击、中间人攻击、ECU 认证错误攻击、暴力破解攻击、应用层协议错误攻击、未知的出栈连接攻击、未知的入栈连接攻击。

在上述设计中，通过给出易于在真实攻击环境中进行标记的多种攻击类型，能便于用户根据实际需求选择其中一种或多种攻击类型来构建真实攻击样本，以适用于不同的真实攻击场景，提高构建真实攻击样本的灵活性和通用性。

进一步地设计中，模拟攻击样本可以对应如下攻击类型中的一项或多项：ID 模糊（Fuzz）攻击、数据 Fuzz 攻击、CAN 的拒绝服务（denial-of-service, Dos）攻击、以太网（ethernet, ETH）的 Dos 攻击、畸形包注入攻击、端口扫描攻击。

在上述设计中，通过给出不易在真实攻击环境中进行标记的多种攻击类型，能便于用户根据实际需求选择其中一种或多种攻击类型来构建模拟攻击样本，以适用于不同的模拟攻击场景，提高构建模拟攻击样本的灵活性和通用性。

一种可能的设计中，数据处理装置通过攻击待检测设备，获得第一类型攻击样本，包括：数据处理装置遍历预设的多种攻击类型中的每种攻击类型，在遍历每种攻击类型时：对待检测设备执行该种攻击类型对应的攻击行为，并获取待检测设备对于该攻击行为所产生的流量数据，进而，当确定该流量数据是攻击流量时，将该流量数据标记为一个第一类型攻击样本。

在上述设计中，预设的多种攻击类型例如可以是前述设计中所给出的易于在真实攻击环境中进行标记的多种攻击类型和不易在真实攻击环境中进行标记的多种攻击类型，如此，通过对已知的每种攻击类型都进行流量采集和标记，能使第一类型攻击样本充分覆盖到已知的各种攻击类型，提高第一类型攻击样本的丰富性和全面性。

进一步地设计中，数据处理装置在获取待检测设备对于任一攻击行为所产生的流量数据后，若确定该流量数据不是攻击流量，而是正常流量，则可以将该流量数据标记为一个非攻击样本，进而，在遍历完全部的攻击类型后，根据第一类型攻击样本、第二类型攻击样本和非攻击样本，一起构建得到入侵检测样本集。

在上述设计中，入侵检测样本集中既包含攻击样本（包括前述的第一类型攻击样本和第二类型攻击样本）又包含非攻击样本，如此，不仅能使入侵检测样本集中的样本信息更加完善，还能在利用入侵检测样本集对待检测设备进行攻击测试时，根据待检测设备是否能拦截攻击样本以及是否能不拦截非攻击样本，更为准确地定义待检测设备的防攻击效果。

进一步地设计中，数据处理装置在获取待检测设备对于任一攻击行为所产生的流量数据后，若确定该流量数据既不满足攻击流量的特征又不满足正常流量的特征，则可以将该流量数据确定为一个无标记样本。其中，无标记样本属于未知样本，即在当前技术手段下无法识别出是攻击样本还是非攻击样本的样本。一些场景中，无标记样本属于异常样本，比如，当数据处理装置的攻击测试造成待检测设备的软硬件系统故障时，待检测设备本身可能会产生一些异常数据，这些异常数据既不满足正常流量的特征，也不满足攻击流量的特征，但仍会被数据处理装置采集下来。进而，针对于无标记样本，数据处理装置可以直

接进行丢弃，以节省入侵检测样本集的数据量，也可以在遍历完全部的攻击类型后，根据攻击样本、无标记样本和非攻击样本，一起构建得到入侵检测样本集，以将攻击待检测设备时所真实存在的全部样本都添加在入侵检测样本集中，提高入侵检测样本集中的样本丰富性，也能便于后续通过其它分析对无标记样本进行标记或执行其它一些操作。

进一步地设计中，入侵检测样本集中的攻击样本和非攻击样本占据同一比例，比如，攻击样本和非攻击样本各占全部样本的 50%。如此，通过均分攻击样本和非攻击样本，能使入侵检测样本集中的攻击样本和非攻击样本维持平衡，便于后续取出相同比例的数据进行待检测设备的攻击测试，提高攻击测试结果的可信度。

进一步地设计中，数据处理装置在构建得到入侵检测样本集后，若确定入侵检测样本集中的攻击样本占据的比例和非攻击样本占据的比例不同，则可以通过对占据比例较多的样本进行裁剪，使得裁剪后的攻击样本占据的比例和非攻击样本占据的比例相同。其中，占据比例较多的样本通常为非攻击样本，也称为上下文数据，如此，通过裁剪非攻击样本，能维持入侵检测样本集中攻击样本和非攻击样本的平衡性。

一种可能的设计中，数据处理装置通过对第一类型攻击样本施加噪声，得到第二类型攻击样本，包括：数据处理装置先对第一类型攻击样本施加噪声以得到扰动样本，再将扰动样本输入攻击识别模型，并获得攻击识别模型输出的识别结果，当该识别结果指示无法确定扰动样本是否为攻击样本时，将扰动样本确定为第二类型攻击样本，否则，根据该识别结果调节扰动样本，并将调节后的扰动样本再次输入攻击识别模型，不断重复上述过程，直至调节后的扰动样本对应的识别结果指示无法确定调节后的扰动样本是否为攻击样本时，将调节后的扰动样本确定为第二类型攻击样本。

在上述设计中，第二类型攻击样本是在已知攻击类型的第一类型攻击样本的基础上，通过施加噪声而得到的无法被识别的样本，可以认为是在当前技术手段下无法确定攻击类型的攻击样本，也即是，未知攻击类型的攻击样本，如此，通过将该攻击样本添加在入侵检测样本集中，能在真实攻击测试场景中避免将这些未知攻击类型的攻击样本误报为非攻击样本的现象发生。

一种可能的设计中，数据处理装置根据第一类型攻击样本和第二类型攻击样本，构建得到入侵检测样本集之后，还可以通过对入侵检测样本集进行特征提取，获得离线检测样本集，该离线检测样本集用于输入至入侵检测模型，以根据入侵检测模型输出的检测结果测评入侵检测模型的检测性能。比如，当离线检测样本集中属于攻击样本的离线检测样本越多地被入侵检测模型检测为攻击样本，同时属于非攻击样本的离线检测样本越多地被入侵检测模型检测为非攻击样本，则意味着入侵检测模型的检测效果较好。反之，当离线检测样本集中属于攻击样本的离线检测样本越多地被入侵检测模型检测为非攻击样本，而属于非攻击样本的离线检测样本越多地被入侵检测模型检测为攻击样本，则意味着入侵检测模型的检测效果较差。进而，当检测效果较差时，数据处理装置还可以调节入侵检测模型的参数，并使用调节后的入侵检测模型重新检测离线检测样本集，重复上述过程，直至得到检测效果较好的入侵检测模型为止。

在上述设计中，入侵检测样本集能支持在离线状态下测评入侵检测模型的检测效果（简称为离线测评），以便于根据该检测效果不断优化入侵检测模型，得到检测效果较好的入侵检测模型，提高入侵检测模型在待检测设备上的落地效果。

进一步地设计中，数据处理装置对入侵检测样本集进行特征提取，获得离线检测样本

集,包括:数据处理装置先确定入侵检测样本集中的每个入侵检测样本的报文类型,进而,针对于报文类型为传输控制协议(transmission control protocol, TCP)报文的各个入侵检测样本,通过对属于同一TCP连接的全部入侵检测样本进行特征提取,获得一个离线检测样本,而针对于报文类型为可变数据速率的CAN(CAN with flexible data rate, CAN(FD))

5 报文或UDP报文的各个入侵检测样本,则通过对每个CAN(FD)报文或UDP报文的入侵检测样本进行特征提取,获得一个离线检测样本。

在上述设计中,通过对属于同一TCP连接的各个入侵检测样本进行联合的特征提取,能将一个TCP连接线上所采集到的全部入侵检测样本聚合为一个离线检测样本,有效减少离线检测样本的样本数量的同时,使每个离线检测样本所包含的特征更有关联性。此外,

10 通过对不属于TCP连接的入侵检测样本(诸如属于CAN(FD)报文和UDP报文的入侵检测样本)进行单独的特征分析,则还能不遗漏没有关联关系的每个入侵检测样本,确保离线检测样本集覆盖全部的入侵检测样本。

进一步地设计中,离线测评所提取的特征可以包括如下特征中的一项或多项:时间戳、频率特征、协议类型、内容特征、丢包率、错误包数量、连接持续时间、连接发起方、连接接收方。比如,对于属于TCP报文的入侵检测样本,所提取的特征可以包括此处所示出的全部特征,而对于属于CAN(FD)报文或UDP报文的入侵检测样本,则可以包括时间戳、

15 频率特征、协议类型、内容特征、丢包率和错误包数量。

在上述设计中,通过给出离线测评对应的多种可提取特征,能便于用户根据实际离线场景中的应用层需求选择其中的一项或多项特征进行入侵检测样本集到离线检测样本集的转化,以适用于不同的离线测评场景,提高入侵检测样本集在离线测评领域中的通用性。

20

进一步地设计中,为保持各个离线检测样本的格式一致性,数据处理装置可以对每个入侵检测样本都提取前述的所有特征,进而,在某一入侵检测样本的某一特征不存在时,将该入侵检测样本集的该特征配置为预设字符,预设字符比如可以为数字、字母、符号或者其中一项或多项的组合形式等。

一种可能的设计中,数据处理装置根据第一类型攻击样本和第二类型攻击样本,构建得到入侵检测样本集之后,还可以对入侵检测样本集进行格式转换,获得与测试工具格式相匹配的在线检测样本集,进而通过测试工具将在线检测样本集输入待检测设备,该在线检测样本集用于测评部署有入侵检测模型的待检测设备的检测性能。

25

在上述设计中,入侵检测样本集能支持在在线状态下测评部署有入侵检测模型的待检测设备的检测效果(简称为在线测评),以便于根据该检测效果确定待检测设备的防攻击性能,确保仅出厂防攻击效果较好的待检测设备。

30

进一步地设计中,测试工具可以为CANoe、PCAN、Technica或其它能实现在线测评的工具,而格式转换后的入侵检测样本集可以为.PCAP、.ASC、.BLF或其它在线测试工具所对应的格式。

在上述设计中,通过使入侵检测样本支持转换为多种测试工具所对应的格式,能便于用户根据实际在线场景中的测试工具选择所对应的格式进行转换,以适用于不同的在线测评场景,提高入侵检测样本集在在线测评领域中的通用性。

35

一种可能的设计中,数据处理装置根据第一类型攻击样本和第二类型攻击样本,构建得到入侵检测样本集之后,还可以根据入侵检测样本集在各个预设指标下的值,确定入侵检测样本集对应的评估值,当评估值低于预设阈值时,调节入侵检测样本集。

40

在上述设计中, 预设指标例如可以是根据待检测设备所属的体系架构的特性而设置的, 通过参照预设指标对已构建的入侵检测样本集进行评估, 能根据评估结果有效优化入侵检测样本集, 使优化后的入侵检测样本集更加适用于待检测设备所属的体系架构。

进一步地设计中, 预设指标可以包括如下指标中的一项或多项: 数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标、数据标记指标、平衡性指标、特征独立性指标、易用性指标。其中, 数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标、数据标记指标和衡性指标属于定量指标, 而特征独立性指标和易用性指标属于定性指标, 通过结合定量指标和定性指标综合评判入侵检测样本集的构建质量, 能使评判结果更加全面, 且更具有说服力。

进一步地设计中, 为使各个预设指标的度量具有可比性, 各个预设指标的取值范围可以配置成同一范围, 比如[0,1]。

进一步地设计中, 入侵检测样本集对应的评估值可以是入侵检测样本集在各个预设指标下的值的加权平均值, 其中, 各个预设指标对应的权重可以相同也可以不同, 比如, 一个具体的示例中, 可以配置各个定量的预设指标均对应第一权重, 各个定性的预设指标均对应第二权重, 且第一权重大于第二权重。

在上述设计中, 通过减小定性的预设指标的权重, 能降低需要通过人为经验判断的预设指标对评估值的影响, 使得评估过程更加关注理性的评判标准, 同时也不放弃需要人为经验的评判标准。

一种可能的设计中, 第一类型攻击样本可以通过攻击如下任一区域得到的: 整个待检测设备; 待检测设备的一个或多个物理区域; 或者, 待检测设备的一个或多个功能区域。示例性地, 当待检测设备为车辆时, 一个或多个物理区域可以包括车载主干区域、左前车身区域、右前车身区域、左后车身区域或右后车身区域中的一个或多个, 一个或多个功能区域可以包括车载中控网关区域、车身控制区域、座舱控制区域、动力控制区域、底盘控制区域或信息娱乐区域等中的一个或多个。

在上述设计中, 数据处理装置可以针对于整个待检测设备构建一个入侵检测样本集, 也可以针对于待检测设备中的一个或多个物理区域构建一个入侵检测样本集, 也可以针对于待检测设备中的一个或多个功能区域构建一个入侵检测样本集, 或者, 还可以针对于一个或多个物理区域和一个或多个功能区域组合构建一个入侵检测样本集, 可见, 该入侵检测样本集的构建方法可以适用于各种不同的构建场景, 有助于提高入侵检测样本集的灵活性、通用性和易用性。

第二方面, 本申请提供一种数据处理装置, 该数据处理装置可以为具有处理能力的任意设备, 如服务器或由服务器构成的服务器集群。该数据处理装置包括: 攻击单元, 用于通过攻击待检测设备, 获得第一类型攻击样本; 扰动单元, 用于通过对第一类型攻击样本施加噪声, 获得第二类型攻击样本; 构建单元, 用于根据第一类型攻击样本和第二类型攻击样本, 构建得到入侵检测样本集。

一种可能的设计中, 第一类型攻击样本可以包括真实攻击样本和模拟攻击样本, 真实攻击样本是通过人为攻击待检测设备得到的, 模拟攻击样本是通过攻击工具攻击待检测设备得到的。

一种可能的设计中, 真实攻击样本可以对应如下攻击类型中的一项或多项: ID 不存在攻击、重放攻击、篡改攻击、数据长度错误攻击、信号超出定义范围攻击、上下文错误攻

击、ID 来源非指定 ECU 攻击、出现相同 ID 攻击、CAN 扫描攻击、UDS 执行敏感操作攻击、消息认证错误攻击、ECU 身份欺骗攻击、中间人攻击、ECU 认证错误攻击、暴力破解攻击、应用层协议错误攻击、未知的出栈连接攻击、未知的入栈连接攻击。

一种可能的设计中，模拟攻击样本可以对应如下攻击类型中的一项或多项：ID Fuzz 攻击、数据 Fuzz 攻击、CAN 的 Dos 攻击、ETH 的 Dos 攻击、畸形包注入攻击、端口扫描攻击。

一种可能的设计中，攻击单元具体用于：遍历预设的多种攻击类型中的每种攻击类型，在遍历每种攻击类型时：对待检测设备执行该种攻击类型对应的攻击行为，并获取待检测设备对于该攻击行为所产生的流量数据，若该流量数据是攻击流量，则将该流量数据标记为一个第一类型攻击样本。

一种可能的设计中，攻击单元在获取待检测设备对于攻击行为所产生的流量数据之后，还用于：若流量数据是正常流量，则将流量数据标记为一个非攻击样本；对应的，构建单元具体用于：根据第一类型攻击样本、第二类型攻击样本和非攻击样本，构建得到入侵检测样本集。

一种可能的设计中，扰动单元具体用于：对第一类型攻击样本施加噪声，得到扰动样本，将扰动样本输入攻击识别模型，获得攻击识别模型输出的识别结果，根据识别结果调节扰动样本，直至调节后的扰动样本对应的识别结果指示无法确定扰动样本是否为攻击样本时，将调节后的扰动样本确定为第二类型攻击样本。其中，攻击识别模型输出的识别结果用于指示扰动样本是否属于攻击样本。

一种可能的设计中，数据处理装置还可以包括特征提取单元，特征提取单元用于：对入侵检测样本集进行特征提取，获得离线检测样本集，该离线检测样本集用于测评入侵检测模型的检测效果。

一种可能的设计中，特征提取单元具体用于：确定入侵检测样本集中的每个入侵检测样本的报文类型，对于报文类型为 TCP 报文的各个入侵检测样本，通过对属于同一 TCP 连接的全部入侵检测样本进行特征提取，获得一个离线检测样本，而对于报文类型为 CAN(FD)报文或 UDP 报文的各个入侵检测样本，通过对每个 CAN(FD)报文或 UDP 报文的入侵检测样本进行特征提取，获得一个离线检测样本。

一种可能的设计中，前述特征提取的特征包括如下特征中的一项或多项：时间戳、频率特征、协议类型、内容特征、丢包率、错误包数量、连接持续时间、连接发起方、连接接收方。

一种可能的设计中，数据处理装置还可以包括格式转换单元，格式转换单元用于：对入侵检测样本集进行格式转换，获得与测试工具格式相匹配的在线检测样本集，并通过测试工具将在线检测样本集输入待检测设备，其中，在线检测样本集用于测评部署有入侵检测模型的待检测设备的检测性能。

一种可能的设计中，数据处理装置还可以包括调节单元，调节单元用于：根据入侵检测样本集在各个预设指标下的值，确定入侵检测样本集对应的评估值，当评估值低于预设阈值时，调节入侵检测样本集。

一种可能的设计中，预设指标包括如下指标中的一项或多项：数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标、数据标记指标、平衡性指标、特征独立性指标、易用性指标。

一种可能的设计中，第一类型攻击样本可以通过攻击如下任一区域得到的：整个待检测设备；待检测设备的一个或多个物理区域；或者，待检测设备的一个或多个功能区域。

第三方面，本申请提供一种数据处理装置，包括处理器，处理器与存储器相连，存储器用于存储计算机程序，处理器用于执行存储器中存储的计算机程序，以使得数据处理装置执行如上述第一方面中任一项设计所述的方法。

第四方面，本申请提供一种数据处理装置，包括处理器和存储器，存储器存储计算机程序指令，处理器运行计算机程序指令以实现如上述第一方面中任一项设计所述的方法。

第五方面，本申请提供一种数据处理装置，包括处理器、存储器和收发器，存储器存储计算机程序指令，处理器运行计算机程序指令，以调用收发器实现如上述第一方面中任一项设计所述的方法。

第六方面，本申请提供一种芯片，该芯片可以包括处理器和接口，处理器用于通过接口读取指令，以执行如上述第一方面中任一项设计所述的方法。

第七方面，本申请提供一种数据处理系统，该数据处理系统可以包括待检测设备和数据处理装置，数据处理装置用于执行如上述第一方面中任一项设计所述的方法。

第八方面，本申请提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，当计算机程序被运行时，实现如上述第一方面中任一项所述的方法。

第九方面，本申请提供一种计算机程序产品，当该计算机程序产品在处理器上运行时，实现如上述第一方面中任一项所述的方法。

上述第二方面至第九方面的有益效果，具体请参照上述第一方面中相应设计可以达到技术效果，这里不再重复赘述。

附图说明

图 1 示例性示出本申请实施例提供的一种可能的系统架构示意图；

图 2 示例性示出本申请实施例提供的一种车辆的分区架构示意图；

图 3 示例性示出本申请实施例提供的一种数据处理方法的流程示意图；

图 4 示例性示出本申请实施例提供的一种第一类型攻击样本的获取流程示意图；

图 5 示例性示出本申请实施例提供的一种入侵检测样本集的应用场景示意图；

图 6 示例性示出本申请实施例提供的一种评估入侵检测样本集的流程示意图；

图 7 示例性示意出本申请实施例提供的一种开发数据处理方案的设计架构图；

图 8 示例性示出本申请实施例提供的一种数据处理装置的结构示意图；

图 9 示例性示出本申请实施例提供的另一种数据处理装置的结构示意图。

具体实施方式

本申请所公开的数据处理方法可以用于构建入侵检测样本集，该入侵检测样本集可以用于训练入侵检测模型，也可以用于检测入侵检测模型或部署有入侵检测模型的待检测设备的检测效果。其中，待检测设备可以是具有通信能力的任意终端设备，尤其可以是对网络安全具有一定需求的终端设备。一些示例中，该终端设备可以包括但不限于：智能运输设备，诸如汽车、轮船、无人机、火车、货车、卡车、飞行汽车等；智能家居设备，诸如电视、扫地机器人、智能台灯、音响系统、智能照明系统、电器控制系统、家庭背景音乐、家庭影院系统、对讲系统、视频监控等；智能制造设备，

诸如机器人、工业设备、工控机、智能物流、智能工厂等。或者，该终端设备也可以是计算机设备，例如台式机、个人计算机、服务器等。还应当理解的是，该终端设备也可以是便携式电子设备，诸如手机、平板电脑、掌上电脑、耳机、音响、穿戴设备（如智能手表）、车载设备、虚拟现实设备、增强现实设备等。便携式电子设备的示例包括但不限于搭载 iOS®、android®、microsoft®、Harmony® 或者其它操作系统的便携式电子设备。上述便携式电子设备也可以是诸如具有触敏表面（例如触控面板）的膝上型计算机（Laptop）等。

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。

需要说明的是，本申请实施例中的术语“系统”和“网络”可被互换使用。“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 的情况，其中 A，B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a,b,或 c 中的至少一项(个)，可以表示：a,b,c,a-b,a-c,b-c,或 a-b-c，其中 a,b,c 可以是单个，也可以是多个。

以及，除非有特别说明，本申请实施例提及“第一”、“第二”等序数词是用于对多个对象进行区分，不用于限定多个对象的优先级或者重要程度。例如，第一类型攻击样本和第二类型攻击样本，只是为了区分不同类型的攻击样本，而并不是表示这两种攻击样本的优先级或者重要程度等的不同。

另外，本申请实施例中“连接”可以理解为电连接，两个电学元件连接可以是两个电学元件之间的直接或间接连接。例如，A 与 B 连接，既可以是 A 与 B 直接连接，也可以是 A 与 B 之间通过一个或多个其它电学元件间接连接，例如 A 与 B 连接，也可以是 A 与 C 直接连接，C 与 B 直接连接，A 与 B 之间通过 C 实现了连接。在一些场景下，“连接”也可以理解为耦合，如两个电感之间的电磁耦合。总之，A 与 B 之间连接，可以使 A 与 B 之间能够传输电能。

图 1 示例性示出本申请实施例提供的一种可能的系统架构示意图，如图 1 所示，该系统架构中包括待检测设备 100 和数据处理装置 200。其中，待检测设备 100 可以是对网络安全具有一定要求的设备，比如车辆。数据处理装置 200 可以是具有数据处理能力的任意装置，比如服务器或者由多个服务器所构成的服务器集群，或者还可以是芯片或电路，比如设置在服务器或服务器集群中的芯片或电路。一个具体的示例中，该数据处理装置 200 可以是云服务器，云服务器可以通过无线方式连接待检测设备 100。应理解，本申请实施例对该系统架构中的待检测设备 100 的数量和数据处理装置 200 的数量不作限定，例如，一个数据处理装置 200 可以如图 1 所示意的只连接一个待检测设备 100，也可以同时连接多个待检测设备 100。以及，本申请实施例中的数据处理装置 200 可以将所有的功能集成在一个独立的物理设备上，也可以将功能分布在多个独立的物理设备上，对此本申请实施例也不作具体限定。

进一步示例性地，继续参照图 1 所示，该系统架构中还可以包括数据库 300、模型训练装置 400 和测试工具 500 中的一项或多项，或者还可以包括其它设备，如路由设备、无线中继设备、无线回传设备及操作管理维护设备等。其中，数据库 300 可以

用于存储数据处理装置 200 所构建的入侵检测样本集，该数据库 300 可以是独立于数据处理装置 200 以外的存储单元，比如数据库服务器，也可以是数据处理装置 200 的内部存储单元，如高速缓存存储器、随机存储器、寄存器、主存储器或只读存储器等。模型训练装置 400 可以是具有算法开发和验证能力的任意设备，如模型训练服务器。

5 该模型训练装置 400 中部署有入侵检测系统 (intrusion detection system, IDS)，该 IDS 是汽车开放系统架构 (automotive open system architecture, AUTOSAR) 针对于汽车网络安全所发布的一种测试系统，属于目前最主流的车载测试系统之一，能在有限的车载硬件资源和车载存储资源的基础上结合规则和机器学习的方式训练出高准确性、高时效性和高鲁棒性的入侵检测模型。测试工具 500 是指能向待检测设备 100 注入测试
10 流量的工具，比如可以是 CAN 测试工具、TCP 测试工具或 UDP 测试工具等。且，该测试工具 500 对外可呈现用户界面，用户通过在用户界面上点击相应的测试命令（比如流量注入类型、流量注入数量及流量注入频率等），可驱动测试工具 500 按照对应的测试命令自动向待检测设备 100 注入测试流量。

进一步示例性地，当包括待检测设备 100、数据处理装置 200、数据库 300、模型
15 训练装置 400 和测试工具 500 时，数据处理装置 200 可以分别与待检测设备 100、数据库 300、模型训练装置 400 和测试工具 500 连接，待检测设备 100 还可以与模型训练装置 400 和测试工具 500 连接。在实施中，数据处理装置 200 可以针对于待检测设备 100 构建入侵检测样本集，并将该入侵检测样本集存储在数据库 300 中。之后，在使用时，数据处理装置 200 可以将数据库 300 中的入侵检测样本集转化为离线检测样
20 本集，并可以选取其中一部分离线检测样本发送给模型训练装置 400，由模型训练装置 400 使用该部分离线检测样本训练得到入侵检测模型后，将入侵检测模型部署在待检测设备 100 中，以便于待检测设备 100 利用入侵检测模型识别攻击流量。进而，在需要进行离线测评时，数据处理装置 200 还可以将转化得到的另一部分离线检测样本发送给模型训练装置 400，由模型训练装置 400 使用之前训练好的入侵检测模型检测
25 该部分离线检测样本以得到离线测评信息，数据处理装置 200 根据该离线测评信息测评模型训练装置 400 所训练的入侵检测模型的检测效果。相对应的，在需要进行在线测评时，数据处理装置 200 可以将数据库 300 中的入侵检测样本集转化为在线检测样本集，进而通过在线工具将部分或全部的在线检测样本输入待检测设备 100，并获取待检测设备 100 针对于该在线检测样本产生的在线测评信息，根据该在线测评信息测
30 评部署有入侵检测模型的待检测设备 100 的检测效果。

根据上述内容可知，入侵检测样本集不仅会用来训练入侵检测模型，还会作为测试样本用来测试入侵检测模型的质量和部署有入侵检测模型的待检测设备的质量。当该入侵检测样本集中的样本类型足够充分时，依据足够充分的入侵检测样本训练得到的入侵检测模型的检测效果也会更好，进而部署有入侵检测模型的待检测设备的防攻
35 击性能也会更好，相应地，依据足够充分的入侵检测样本测评入侵检测模型或待检测设备所得到的测评结果的可靠性也会更好。因此，如何构建样本类型足够充分的入侵检测样本集，对于提高入侵检测模型的检测效果、提高待检测设备的防攻击效果、提高测评入侵检测模型的可靠性以及提高测评待检测设备的可靠性至关重要。

然而，业界在构建入侵检测样本集时，仅仅只是会利用攻击工具模拟一些典型的
40 入侵场景来对待检测设备进行攻击，导致入侵检测样本集中也只会包含典型的入侵场

景所对应的入侵检测样本，该入侵检测样本集中的样本类型非常有限，不利于提高入侵检测模型的检测效果、提高待检测设备的防攻击效果、提高测评入侵检测模型的可靠性以及提高测评待检测设备的可靠性，进而也就不利于入侵检测技术在待检测设备上的落地。

有鉴于此，本申请实施例提供一种数据处理方法，用以构建样本类型更为丰富的入侵检测样本集，使其既能覆盖到已知入侵场景下的入侵检测样本，又能覆盖到未知入侵场景下的入侵检测样本，以提高使用该入侵检测样本集训练得到的入侵检测模型的检测效果，提高部署有入侵检测模型的待检测设备的防攻击效果，提高使用该入侵检测样本集测评入侵检测模型的可靠性，以及提高使用该入侵检测样本集测评待检测设备的可靠性。

需要说明的是，本申请实施例中的入侵检测样本集可以是针对于整个待检测设备构建得到的，也可以是针对于待检测设备中的一个或多个区域构建得到的。示例性地，当待检测设备为车辆时，图 2 示出了本申请实施例提供的一种车辆的分区架构示意图，其中：

图 2 中 (A) 示出的是车辆的物理分区架构图，该架构根据物理区域的不同将整个车辆划分为车载主干区域、右前车身区域、左前车身区域、右后车身区域和左后车身区域，右前车身区域、左前车身区域、右后车身区域和右后车身区域作为车载主干区域的分支区域而存在。其中，车载主干区域中部署有整车控制器 (vehicle control unit, VCU)，每个分支区域中部署有各自的控制节点 (即 Z_1 、 Z_2 、 Z_3 、 Z_4) 和与控制节点相连的若干 ECU，每个分支区域中的全部 ECU 通过 CAN (FD) 与控制节点相连，且每个分支区域中的控制节点通过 ETH 与车载主干区域中的 VCU 相连；

图 2 中 (B) 示出的是车辆的功能分区架构图，该架构根据实现功能的不同将整个车辆划分为车载中控网关功能区域和 K 个其它功能区域，K 个其它功能区域作为车载中控网关功能区域的分支区域而存在，各自实现不同的功能，比如，一些场景中，K 个其它功能区域可以包括车身控制域、座舱控制域、动力控制域、底盘控制域或信息娱乐域等中的一项或多项，K 为正整数。其中，车载中控网关功能区域中部署有 GateWay 网关，每个其它功能区域中部署有各自的域控制器 (即 D_1 、 D_2 、...、 D_{4K}) 和与域控制器相连的若干 ECU，每个其它功能区域中的全部 ECU 通过 CAN (FD) 与域控制器相连，且每个其它功能区域中的域控制器通过 ETH 与车载中控网关功能区域中的 GateWay 相连。

基于图 2 中 (A) 或图 2 中 (B) 所示意的车载分区架构，本申请实施例中可以针对于整个车辆构建一个入侵检测样本集，也可以针对于车辆中的一个或多个物理区域构建一个入侵检测样本集，还可以针对于车辆中的一个或多个功能区域构建一个入侵检测样本集，或者，还可以针对于一个或多个物理区域以及一个或多个功能区域的组合构建一个入侵检测样本集等。其中，物理区域可以是车载主干区域，也可以是右前车身区域、左前车身区域、右后车身区域或左后车身区域，功能区域可以是车载中控网关功能区域，也可以是其它功能区域，具体不作限定。

需要说明的是，具体针对于哪些区域构建入侵检测样本集，可以根据数据处理装置的处理能力和用户的实际需求进行设置。比如，当数据处理装置的处理能力较强时，可以选择针对于整个车辆构建入侵检测样本集，以利用高效的处理能力构建得到比较完整的全局

入侵检测样本集。其中，该全局入侵检测样本集可以适用于全局攻击场景，也可以适用于局部攻击场景，通用性较好。反之，当数据处理装置的处理能力不强时，可以根据实际业务所涉及到的区域，针对性地选取这些区域来构建局部的入侵检测样本集。其中，该局部的入侵检测样本集属于全局的入侵检测样本集的一个子集，虽然仅可以适用于局部攻击场景，但其需要处理的区域规模变小，因此能较好地降低构建入侵检测样本集的难度，降低入侵检测样本集的复杂程度。

下面以构建整个待检测设备对应的入侵检测模型为例，通过具体的实施例来介绍上述技术问题是如何被解决的。需要说明的是，在下文的描述中，数据处理装置可以是图 1 所示意的数据处理装置 200，也可以是能够支持数据处理装置实现所需功能的其它通信节点、通信装置或通信系统，例如芯片、芯片系统、电路或电路系统，具体不作限定。

基于图 1 所示意的系统架构，图 3 示例性示出本申请实施例提供的一种数据处理方法的流程示意图，该数据处理方法可以由数据处理装置执行，比如图 1 所示意的数据处理装置 200。如图 3 所示，该方法包括：

步骤 301，数据处理装置通过攻击待检测设备，获得第一类型攻击样本。

其中，当针对于整个待检测设备构建全局入侵检测样本集，数据处理装置可以针对于整个待检测设备发起攻击行为，以获得整个待检测设备对应的第一类型攻击样本。反之，当针对于一个或多个区域构建局部入侵检测样本集时，数据处理装置可以仅针对于该一个或多个区域发起攻击行为，以获得该一个或多个区域对应的第一类型攻击样本。

一个示例中，待检测设备为车辆，该车辆可以是分布式电子电气架构、域集中式电子电气架构、车辆集中式电子电气架构或未来可能出现的任一车载架构下的车辆。如此，数据处理装置通过对属于每种车载架构的车辆进行攻击，能构建出每种车载架构所对应的入侵检测样本集，进而能便于用户根据实际需求选择其中一种或多种车载架构所对应的入侵检测样本集进行使用，提高用户的使用体验。

进一步地示例中，为了提高任一车载架构所对应的入侵检测样本集的准确性，数据处理装置还可以针对于属于该车载架构的多台车辆一起进行攻击，以使第一类型攻击样本能覆盖到该车载架构下的多台车辆，避免只攻击一台车辆时由于该车辆出现问题而导致的样本采集不准确的问题。

进一步地示例中，当针对于属于一个车载架构的多台车辆进行攻击时，数据处理装置在获取到多台车辆对应的大量的第一类型攻击样本后，还可以通过聚类或模型识别等手段对这些第一类型攻击样本进行筛选，比如筛除其中与其它的第一类型攻击样本差异较大的第一类型攻击样本，而仅保留比较相似的第一类型攻击样本。如此，通过提前清理明显存在问题的第一类型攻击样本，能避免后续对明显存在问题的第一类型攻击样本进行无意义地处理，有效节省数据处理装置的计算资源。

本申请实施例中，第一类型攻击样本可以包括真实攻击样本和模拟攻击样本。其中，真实攻击样本是通过人为攻击待检测设备而得到的，例如可以是在渗透测试的过程中采集得到的。其中，渗透测试过程是指攻击人员站在黑客的角度以攻破待检测设备为目的真实地对车辆进行攻击，这种攻击方式能够构造出隐蔽性较强的攻击行为和依赖业务逻辑的攻击行为，能获取到易于在真实攻击环境中标记的攻击样本。相应地，模拟攻击样本是通过攻击工具攻击待检测设备而得到的，例如可以是利用攻击工具模拟产生攻击流量并将该攻击流量自动地注入到待检测设备后从待检测设备中采集的，该种攻击方式能够获取到不易

在真实攻击环境中标记的攻击样本。如此，通过结合人为攻击方式和攻击工具攻击方式综合构建第一类型攻击样本，能使第一类型攻击样本充分覆盖到真实攻击环境中可能存在的各种攻击类型的攻击样本，提高第一类型攻击样本的全面性。

5 一种可选地实施方式中，第一类型攻击样本可以是在现阶段已知的入侵场景中根据已知的各种攻击类型攻击待检测设备而得到的。其中，已知的各种攻击类型包括易于在真实攻击环境中进行采集和标注的攻击类型（简称为第一种攻击类型）和不易在真实攻击环境中进行采集和标注的攻击类型（简称为第二种攻击类型），因此，通过采用人为方式按照第一种攻击类型真实地攻击待检测设备，可以采集得到上述真实攻击样本，通过采用攻击工具按照第二种攻击类型模拟地攻击待检测设备，可以集中采集得到上述模拟攻击样本。

10 举例来说，假设待检测设备为车辆，且车辆中的各个 ECU 通过 CAN（FD）总线和 ETH 总线进行通信，则，请参照表 1，其示出了待检测设备中可能存在的攻击类型以及每种攻击样本所对应的攻击类型的对应关系表。

表 1

攻击类型		第一类型攻击样本		第二类型攻击样本
		真实攻击样本	模拟攻击样本	
CAN（FD）	ID Fuzz	×	✓	×
	数据 Fuzz	×	✓	×
	DoS 攻击	×	✓	×
	ID 不存在	✓	×	×
	重放	✓	×	×
	篡改	✓	×	×
	数据长度错误	✓	×	×
	信号超出定义范围	✓	×	×
	上下文错误	✓	×	✓
	ID 来源非指定 ECU	✓	×	✓
	出现相同 ID	✓	×	×
	CAN 网络扫描	✓	×	✓
	UDS 执行敏感操作	✓	×	×
	消息认证错误	✓	×	×
ETH	DoS 攻击	×	✓	×
	协议 Fuzz	×	✓	×
	ECU 身份欺骗	✓	×	✓
	中间人攻击	✓	×	✓
	ECU 认证错误	✓	×	×
	暴力破解	✓	×	×
	畸形包注入	×	✓	✓
	端口扫描攻击	×	✓	✓
	应用层协议错误	✓	×	✓
	未知的出栈连接	✓	×	×

	未知的入栈连接	✓	×	×
--	---------	---	---	---

参照表 1 所示，第一种攻击类型可以包括如下攻击类型中的一项或多项：

ID 不存在攻击，是指通过将 CAN 报文中的 ID 修改为某个不存在的 ID 来攻击车辆；

重放攻击，是指通过发送车辆之前已接收过的 CAN 报文来欺骗车辆；

5 篡改攻击，是指通过篡改 CAN 报文中携带的数据来攻击车辆；

数据长度错误攻击，是指通过修改 CAN 报文的数据长度来攻击车辆；

信号超出定义范围攻击，是指通过将 CAN 报文中的信号数值修改为大于最大规定值的值或小于最小规定值的值来攻击车辆；

10 上下文错误攻击，是指通过在 CAN 网络上发布不适合某种状态的特定消息或信号来攻击车辆，比如在刹车状态下发出加速信号；

ID 来源非指定 ECU 攻击，是指通过非指定的 ECU 发布理应由指定 ECU 发布的 CAN 报文来攻击车辆；

出现相同 ID 攻击，是指通过在两个 ECU 发布的 CAN 报文中携带相同的 ID 来攻击车

15 辆；CAN 扫描攻击，是指通过发送 CAN 扫描消息来侵入车辆；

UDS 执行敏感操作攻击，是指通过在 UDS 报文中携带敏感信息来攻击车辆；

消息认证错误攻击，是指通过修改 CAN 总线的消息认证流程使得车辆无法成功认证消息；

ECU 身份欺骗攻击，是指通过更改 ETH 消息中的 ECU 身份来欺骗车辆；

20 中间人攻击，是指通过将一台受入侵者控制的设备虚拟放置在 ETH 连接的两个 ECU 之间来攻击车辆；

ECU 认证错误攻击，是指通过修改 ETH 的 ECU 认证流程使得车辆无法成功 ECU；

暴力破解攻击，是指通过穷举的方式破译 ETH 密钥来攻击车辆；

25 应用层协议错误攻击，是指通过修改应用层协议使得车辆无法获取正确的应用层协议进行消息交互来攻击车辆；

未知的出栈连接攻击，是指通过给定一个虚假的出栈连接来攻击车辆；

未知的入栈连接攻击，是指通过给定一个虚假的入栈连接来攻击车辆。

在上述第一种攻击类型中，ID 不存在攻击、重放攻击、篡改攻击、数据长度错误攻击、信号超出定义范围攻击、上下文错误攻击、ID 来源非指定 ECU 攻击、出现相同 ID 攻击、CAN 扫描攻击、UDS 执行敏感操作攻击和消息认证错误攻击属于 CAN (FD) 通信方式下存在的攻击类型，而 ECU 身份欺骗攻击、中间人攻击、ECU 认证错误攻击、暴力破解攻击、应用层协议错误攻击、未知的出栈连接攻击和未知的入栈连接攻击属于 ETH 通信方式下存在的攻击类型。

继续参照表 1 所示，第二种攻击类型可以包括如下攻击类型中的一项或多项：

35 ID 模糊 (Fuzz) 攻击，是指通过模糊处理 CAN 报文中的 ID 来攻击车辆；

数据 Fuzz 攻击，是指通过模糊处理 CAN 报文中的数据来攻击车辆；

CAN 的 Dos 攻击，是指通过停止某部分 CAN 总线的收发服务来攻击车辆；

ETH 的 Dos 攻击，是指通过停止某部分 ETH 总线的收发服务来攻击车辆；

畸形包注入攻击，是指通过注入畸形包来攻击车辆；

端口扫描攻击，是指通过发送端口扫描消息来侵入车辆。

在上述第二种攻击类型中，ID 模糊（Fuzz）攻击、数据 Fuzz 攻击和 CAN 的 Dos 攻击属于 CAN（FD）通信方式下存在的攻击类型，而 ETH 的 Dos 攻击、畸形包注入攻击和端口扫描攻击属于 ETH 通信方式下存在的攻击类型。

在上述实施方式中，通过给出已知入侵场景中可能存在的各种攻击类型，能便于用户根据实际需求选择其中一种或多种攻击类型来构建第一类型攻击样本，且还可以采用真实攻击或模拟攻击的方式获取所需要的真实攻击样本或模拟攻击样本，以适用于不同的攻击场景，提高构建第一类型攻击样本的灵活性和通用性。

进一步地示例中，数据处理装置可以通过多种方式攻击待检测设备来获取第一类型攻击样本，比如，请参照图 4，其示出了本申请实施例提供的一种获取第一类型攻击样本的具体流程示意图，该流程包括：

步骤 401，数据处理装置获取预设的多种攻击类型。

其中，预设的多种攻击类型示例性地可以包括上述表 1 所示意的全部攻击类型，以便使第一类型攻击样本能充分覆盖到已知的各种攻击类型，提高第一类型攻击样本的丰富性和全面性。

步骤 402，数据处理装置确定预设的多种攻击类型中是否存在未被遍历过的攻击类型，若是，则执行步骤 403，若否，则执行步骤 409。

步骤 403，数据处理装置对待检测设备执行未被遍历过的攻击类型所对应的攻击行为，并获取待检测设备对于该攻击行为产生的流量数据。

示例性地，针对于第一种攻击类型，可以通过人为方式提前编写好所需要的攻击代码，并将该攻击代码与所对应的第一种攻击类型映射存储在数据处理装置中。如此，数据处理装置在获取到未被遍历过的攻击类型后，如果确定该攻击类型属于第一种攻击类型，则可以从本地直接获取该第一种攻击类型对应的攻击代码，并自动按照该攻击代码生成对应的攻击行为后攻击待检测设备。反之，如果确定该攻击类型属于第二种攻击类型，则数据处理装置可以调用攻击工具，通过攻击工具生成该第二种攻击类型所对应的攻击行为后攻击对待检测设备。如此，整个攻击流程可以由数据处理装置自动实现，有助于提高对整个攻击流程的统一管理，且还不需要等待人为现场编程，有助于节省样本采集的时延。

进一步地示例中，当待检测设备为车辆时，数据处理装置可以通过数据线接入待检测设备的车载诊断（on-board diagnostics，OBD）接口，该 OBD 接口示例性地可以是 II 型车载诊断系统的接口，即 OBD-II 接口。最初时，由于全部的攻击类型都还未被遍历过，因此数据处理装置可以从全部的攻击类型中按照随机方式、或者按照顺序方式、或者按照其它方式选取一种攻击类型，然后按照该种攻击类型攻击待检测设备，并通过 OBD 接口获取待检测设备针对于该种攻击类型所产生的流量数据。进而，在分析完该流量数据后，数据处理装置可以再从未被遍历过的攻击类型中选取一种攻击类型继续攻击待检测设备，重复上述过程，直至全部的攻击类型都被遍历过为止。

进一步示例性地，上述整个攻击过程的流量采集操作可以通过数据处理装置自动实现。具体的，可以是在数据处理装置中配置采集时长，数据处理装置在开始执行攻击行为后，即可启动计时，在计时时间内，数不断从待检测设备的 OBD 接口处采集待检测设备输出的流量数据，直至计时到所配置的采集时长时，结束采集。其中，采集时长可以为几个小时、几天、几个星期甚至几个月，具体的，可以由本领域技术人员根据实际需求进行配置。

比如，当预设的攻击类型的数量较多时，攻击待检测设备所需的时间较长，采集时长也可以配置的越长，如数周。反之，当预设的攻击类型的数量较少时，攻击待检测设备所需的时间较短，采集时长也可以配置的越短，如数天。

步骤 404，数据处理装置判断流量数据是否为攻击流量，若是，则执行步骤 405，若否，则执行步骤 406。

步骤 405，数据处理装置将流量数据标记为一个第一类型攻击样本，之后执行步骤 402。

示例性地，在确定某一流量的数据满足攻击流量的特征后，若该流量数据是在第一种攻击类型下采集得到的，则数据处理装置可以将该攻击流量标记为真实攻击样本，反之，若该流量数据是在第二种攻击类型下采集得到的，则数据处理装置可以将该攻击流量标记为模拟攻击样本。

步骤 406，数据处理装置判断流量数据是否为正常流量，若是，则执行步骤 407，若否，则执行步骤 408。

步骤 407，数据处理装置将流量数据标记为一个非攻击样本，之后执行步骤 402。

一些场景中，非攻击样本也称为上下文数据或上下文样本。

步骤 408，数据处理装置确定流量数据为一个无标记样本，之后执行步骤 402。

示例性地，当流量数据既不满足攻击流量的特征，也不满足正常流量的特征时，意味着该流量数据在当前的技术手段下无法识别其样本类型，该情况下，数据处理装置可以不对该流量数据进行标记，而是将其作为一个无标记样本。一些场景中，该无标记样本属于异常样本，比如，当数据处理装置的攻击测试造成待检测设备的软硬件系统故障时，待检测设备本身可能会产生一些异常数据，这些异常数据既不满足正常流量的特征，也不满足攻击流量的特征，但仍会被数据处理装置采集下来。

步骤 409，数据处理装置结束攻击流程。

在上述示例中，数据处理装置通过攻击待检测设备，既能获取到攻击样本，如真实攻击样本和模拟攻击样本，又能获取到非攻击样本，甚至还能获取到无标记样本，这种获取方式能够获取到多种类型的样本，便于提高后续构建入侵检测样本集的样本丰富性。

需要说明的是，图 4 只是示例性介绍一种获取第一类型攻击样本的可能方式，本申请实施例并不限定只能采用这种方式获取第一类型攻击样本。比如，另一种可能的获取方式中，数据处理装置还可以组合预设的多种攻击类型中的至少两种攻击类型，一次性地对待检测设备执行至少两种攻击类型所对应的攻击行为，进而获取待检测设备生成的流量数据后，从该流量数据中分离出至少两种攻击类型各自对应的流量数据，根据至少两种流量数据获得第一类型攻击样本。应理解，可能的获取方式还有很多，此处不再进行一一列举。

步骤 302，数据处理装置通过对第一类型攻击样本施加噪声，获得第二类型攻击样本。

示例性地，数据处理装置在获取到第一类型攻击样本后，可以对第一类型攻击样本进行格式转换，获得文本格式或二进制格式的第一类型攻击样本，并将文本格式或二进制格式的第一类型攻击样本存储在原始数据库中。

进一步示例性地，数据处理装置可以遍历原始数据库中的全部第一类型攻击样本，在遍历每个第一类型攻击样本时：对该第一类型攻击样本施加噪声以得到扰动样本，再将扰动样本输入攻击识别模型，并获得攻击识别模型输出的识别结果，当该识别结果指示无法确定扰动样本是否为攻击样本时，将扰动样本确定为一个第二类型攻击样本，否则，根据该识别结果调节扰动样本，并将调节后的扰动样本再次输入攻击识别模型，不断重复上述

过程，直至调节后的扰动样本对应的识别结果指示无法确定调节后的扰动样本是否为攻击样本时，将调节后的扰动样本确定为一个第二类型攻击样本。

其中，攻击识别模型可以是具有识别能力的任意模型，具体的，可以是采用人工智能（artificial intelligence, AI）算法训练得到的神经网络模型，该 AI 算法比如可以是生成对抗网络（generative adversarial networks, GAN）算法。GAN 算法可以学习已知的一些攻击样本和非攻击样本的特征，并根据学习到的特征构建攻击识别模型，使攻击识别模型能够识别出输入样本属于攻击样本的概率。具体的，攻击识别模型中可以包含生成器和鉴别器，输入至攻击识别模型的任一第一类型攻击样本首先由生成器所接收。当该第一类型攻击样本具有 N 维特征空间（N 为正整数）时，生成器可以通过对该第一类型攻击样本施加与 N 维特征空间一一对应的 N 维噪声向量，生成扰动样本，进而将扰动样本输入鉴别器。鉴别器鉴别出扰动样本属于攻击样本的概率后，如果该概率大于 50%，则通知生成器按照第一方向调节 N 维噪声向量，如果该概率小于 50%，则通知生成器按照第二方向调节 N 维噪声向量。进而，生成器使用调节后的 N 维噪声向量重新加扰第一类型攻击样本生成新的扰动样本，并发送给鉴别器，由鉴别器重新鉴别新的扰动样本属于攻击样本的概率，若该概率为 50%，则可以将该新的扰动样本作为一个第二类型攻击样本，否则，重复执行上述过程，直至获得属于攻击样本的概率为 50%的扰动样本为止。

如此，通过生成器和鉴别器的博弈，攻击识别模型可以生成无法识别样本类型的样本，但由于该样本是对真实攻击待检测设备所得到的攻击样本（即真实攻击样本和模拟攻击样本）进行加扰得到的，大概率属于攻击样本，因此，该样本可以认为是在当前技术手段下无法确定攻击类型的攻击样本，该攻击样本在真实识别过程中容易被误报。基于此，数据处理装置可以将该样本作为第二类型攻击样本，后续存入入侵检测样本集，以便于能在真实攻击测试场景中避免将这些未知攻击类型的攻击样本误报为非攻击样本的现象发生。

此外，由于第二类型攻击样本是通过 AI 算法中的生成器和鉴别器对抗而生成的，因此，第二类型样本也可以称为 AI 对抗样本，或者也可以具有其它名称，本申请实施例对此不作具体限定。

步骤 303，数据处理装置根据第一类型攻击样本和第二类型攻击样本，构建得到入侵检测样本集。

示例性地，数据处理装置根据上述步骤 301 获得第一类型攻击样本（包括真实攻击样本和模拟攻击样本）和非攻击样本，以及根据上述步骤 302 中获得第二类型攻击样本后，可以将这些样本统一保存为 .pcap 格式，进而根据 .pcap 格式的全部样本构建得到入侵检测样本集。其中，.pcap 格式是与现有的 IDS 系统相对接的格式，如果是对接其它系统，则数据处理装置也可以将这些样本保存为其它系统所对接的格式，本申请实施例对此不作具体限定。

进一步示例性地，针对于上述步骤 301 中获取的无标记样本，数据处理装置可以直接进行丢弃，以节省入侵检测样本集的数据量，也可以在遍历完全部的攻击类型后，根据攻击样本、无标记样本和非攻击样本，一起构建得到入侵检测样本集，以将攻击待检测设备时所真实存在的全部样本都添加在入侵检测样本集中，提高入侵检测样本集中的样本丰富性，也能便于后续通过其它分析对无标记样本进行标记或执行其它一些操作，或者一些特例中，还可以将其标记为异常样本后添加在入侵检测样本集中，具体不作限定。

进一步示例性地，数据处理装置在构建得到入侵检测样本集后，若确定入侵检测样本

集中的攻击样本（包括第一类型攻击样本和第二类型攻击样本）占据的比例和非攻击样本占据的比例不同，则可以通过对占据比例较多的样本进行裁剪，使得裁剪后的攻击样本占据的比例和非攻击样本占据同一比例，如攻击样本和非攻击样本各占全部样本的 50%。其中，占据比例较多的样本通常为非攻击样本，在某些特殊情况下也可能是攻击样本，通过裁剪占据比例较多的样本，能使入侵检测样本集中的攻击样本和非攻击样本维持平衡，便于后续取出相同比例的数据进行攻击测试，提高攻击测试结果的可信度。

在上述构建方式中，入侵检测样本集中既能覆盖已知入侵场景下的第一类型攻击样本，又能覆盖未知入侵场景下的第二类型攻击样本，还能覆盖非攻击样本，如此，不仅能使入侵检测样本集中的样本信息更加完善，还能在利用入侵检测样本集对待检测设备进行攻击测试时，根据待检测设备是否能拦截攻击样本以及是否能不拦截非攻击样本，更为准确地定义待检测设备的防攻击效果。

上述内容介绍了入侵检测样本集的具体构建过程，下面再对已构建的入侵检测样本集的应用进行详细介绍。

图 5 示例性示出本申请实施例提供的一种入侵检测样本集的应用场景示意图，如图 5 所示，该入侵检测样本集可以应用于模型训练场景、离线测评场景或在线测评场景中的一个或多个场景。其中，图示实线示出的是模型训练场景的应用流程，图示虚线示出的是离线测评场景的应用流程，图示双节点线示出的是在线测评场景的应用流程。下面参照图 5 分别对这三个应用场景进行详细介绍。

模型训练场景

参照图 5 所示意的实线部分，模型训练是指在早期算法开发和验证中，使用入侵检测样本集训练得到入侵检测模型。由于入侵检测模型所需的训练样本具有自己的特征格式，而入侵检测样本集中的入侵检测样本未必与该特征格式相匹配，因此在训练入侵检测模型之前，数据处理装置还可以先对入侵检测样本集进行特征提取，并根据提取得到的特征构建得到离线检测样本集。如此，在需要训练入侵检测模型时，数据处理装置即可直接从离线检测样本集中选取部分离线检测样本作为训练集数据，输入至模型训练装置，由模型训练装置利用训练集数据训练入侵检测模型。其中，训练集数据中可以包括攻击类型的离线检测样本和正常类型的离线检测样本，攻击类型的离线检测样本是通过对入侵检测样本集中的第一类型攻击样本和/或第二类型攻击样本进行特征提取而得到的，正常类型的离线检测样本是对入侵检测样本集中的非攻击样本进行特征提取而得到的，且攻击类型的离线检测样本和正常类型的离线检测样本还可以保持数量的一致性，以便于能基于均衡的数据训练得到效果较好的入侵检测模型。

需要说明的是，离线检测样本集中的各个离线检测样本可以保存为文本格式，如.csv。其中，该.csv 格式是与现有的 IDS 系统中的模型训练装置相对接的格式，如果对接的是其它类型的模型训练装置，则可以保存为其它系统所适配的格式，具体不作限定。

本申请实施例中，在进行特征提取时，数据处理装置可以孤立地分析每个入侵检测样本，也即是对每个入侵检测样本进行特征提取后得到一个离线检测样本，也可以联合多个入侵检测样本进行集中分析，比如对具有关联关系的多个入侵检测样本进行特征提取后得到一个离线检测样本。其中，具有关联关系的多个入侵检测样本比如可以是属于同一个连接的多个入侵检测样本、流量数据来自于同一个 ECU 的多个入侵检测样本或者流量数据

发送至同一个 ECU 的多个入侵检测样本等。

进一步示例性地，以具有关联关系的多个入侵检测样本为属于同一个连接的多个入侵检测样本为例，当待检测设备为车辆时，车辆中的报文类型通常可以包括 TCP 报文、CAN (FD)报文和 UDP 报文，其中，TCP 报文是在至少两个 ECU 之间建立连接后在该连接上传输的报文，而 CAN(FD)报文和 UDP 报文则是通过广播的方式发送在对应的总线上后由所需的 ECU 节点从总线中获取的报文，这三种报文的内容中既包含源互联网协议（internet protocol, IP）地址又包含目的 IP 地址。可见，TCP 报文具有连接的概念，而 CAN(FD)报文和 UDP 报文不具有连接的概念，因此，数据处理装置在构建得到入侵检测样本集后，可以先确定入侵检测样本集中的每个入侵检测样本的报文类型，进而，针对于报文类型为 TCP 报文的各个入侵检测样本，根据报文内容中包含的源 IP 地址和目的 IP 地址，获取属于同一 TCP 连接的全部入侵检测样本，并对这些入侵检测样本进行特征提取后得到一个离线检测样本。反之，针对于报文类型为 CAN (FD)报文和 UDP 报文的每个入侵检测样本，单独地对每个入侵检测样本进行特征提取后得到一个离线检测样本。如此，通过联合一个 TCP 连接线上的全部入侵检测样本聚合得到一个离线检测样本，能在有效减少离线检测样本集中的样本数量的同时，使每个离线检测样本所包含的特征更有关联性，而通过对不具有连接概念的每个入侵检测样本进行单独的特征分析，则还能不遗漏没有关联关系的每个入侵检测样本，确保离线检测样本集能覆盖到全部入侵检测样本。

进一步示例性地，上述特征提取所提取的特征可以包括如下特征中的一项或多项：时间戳、频率特征、协议类型、内容特征、丢包率、错误包数量、连接持续时间、连接发起方、连接接收方。其中，时间戳是指采集到报文的时间，包括日期和时刻等。频率特征是指在源 IP 和目的 IP 之间收发报文的通信频率。协议类型是指报文所适配的协议，比如上表 3 中的任一种协议类型。内容特征是指报文中携带的实质内容，比如数据或指令等。丢包率是指在源 IP 和目的 IP 之间收发报文时的报文丢失比例。错误包数量是指在源 IP 和目的 IP 之间收发报文时出现的错误报文的数量。连接持续时间是指一个连接自开始建立至断开之间的时间间隔。连接发起方是指请求建立连接的 ECU。连接接收方是指接收连接发起方所发送请求的 ECU。

进一步示例性地，为保持各个离线检测样本的格式一致性，数据处理装置还可以针对于每类入侵检测样本都提取上述的全部特征。具体的，对于属于 TCP 报文的入侵检测样本，由于其存在连接的概念，因此可以提取到上述的全部特征。而对于属于 CAN (FND) 报文或 UDP 报文的入侵检测样本，由于其不存在连接的概念，因此仅可以提取到上述特征中的时间戳、频率特征、协议类型、内容特征、丢包率和错误包数量，而无法提取到连接持续时间、连接发起方和连接接收方。该情况下，为了保持离线检测样本的格式一致性，数据处理装置还可以将无法提取到的特征配置为预设字符，该预设字符比如可以为数字、字母、符号或者其中一项或多项的组合形式等。

需要说明的是，上述内容只是给出一种特征提取的示例，至于实际应用时需要提取哪些特征，则可以由本领域技术人员根据经验进行设置，本申请实施例对此不作限定。

在模型训练场景中，通过给出多种可提取的特征，能便于用户根据实际模型训练场景中的应用层需求选择其中的一项或多项特征进行入侵检测样本集到离线检测样本集的转化，以适用于不同的模型训练场景，提高入侵检测样本集在模型训练领域中的通用性。

离线测评场景

参照图 5 所示意的虚线部分，离线测评是指在早期算法开发和验证中，使用入侵检测样本集测试在模型训练场景中训练得到的入侵检测模型的检测效果。由于已经在模型训练场景中提取得到了离线检测样本集，因此，在使用该离线检测样本集中的部分离线检测样本训练得到入侵检测模型后，数据处理装置还可以从离线检测样本集中选取另一部分离线检测样本作为测试集数据，输入至模型训练装置，由模型训练装置利用该测试集数据测试入侵检测模型得到离线测评信息，进而将离线测评信息发送给数据处理装置，由数据处理装置根据离线测评信息评估入侵检测模型的检测效果。

其中，测试集数据中也可以包括攻击类型的离线检测样本和正常类型的离线检测样本，且攻击类型的离线检测样本和正常类型的离线检测样本还可以保持数量的一致性。如此，模型训练装置获取到入侵检测模型针对于每个离线检测样本的检测结果后，结合其中将攻击类型的离线检测样本识别为攻击样本的数量以及将正常类型的离线检测样本识别为非攻击样本的数量得到识别正确的离线检测样本的总数量，以及结合其中将攻击类型的离线检测样本识别为非攻击样本的数量以及将正常类型的离线检测样本识别为攻击样本的数量得到识别错误的离线检测样本的总数量，进而将识别正确的离线检测样本的总数量和识别错误的离线检测样本的总数量携带在离线测评信息中发送给数据处理装置。进而，若识别正确的离线检测样本的总数量越多，识别错误的离线检测样本的总数量越少，则数据处理装置可以确定入侵检测模型的检测效果越好，反之，则检测效果越差。

需要说明的是，上述离线测评的具体实现过程仅是一个示例，实际操作中还可能存在其它的实现方式，比如模型训练装置也可以直接将每个离线检测样本的检测结果作为离线测评信息发送给数据处理装置，由数据处理装置自行统计识别正确的离线检测样本的总数量和识别错误的离线检测样本的总数量后完成离线测评，可能的实现方式有很多，此处不再一一进行列举。

在离线测评场景中，入侵检测样本集能支持在离线状态下测评入侵检测模型的检测效果，如此，能便于模型训练装置根据该检测效果不断优化入侵检测模型，得到检测效果更好的入侵检测模型，为入侵检测模型在待检测设备上的落地提供依据。

在线测评场景

参照图 5 所示意的双节点线部分，在线测评是指在后期算法部署中，使用入侵检测样本集测试部署有入侵检测模型的待检测设备的检测效果。经过上述模型训练和离线测评后，入侵检测模型能具有较好的检测效果，但该检测效果只是在脱离待检测设备的基础上测得的，无法表征真实应用在待检测设备后的实际效果。因此，还需要将入侵检测模型部署在待检测设备上，并对部署有入侵检测模型的待检测设备进行真实地攻击后，根据待检测设备的反应确定在待检测设备中应用入侵检测模型的实际检测效果。

具体实施中，数据处理装置可以对入侵检测样本集中的入侵检测样本进行格式转换，获得与测试工具格式相匹配的在线检测样本，进而通过测试工具将在线检测样本输入至待检测设备，并获得待检测设备中部署的入侵检测模型对于在线检测样本所产生的在线测评信息，根据该在线测评信息测评部署有入侵检测模型的待检测设备的检测性能。其中，格式转换也可以以连接为单元进行，比如针对于属于同一 TCP 连接的各个入侵检测样本，首先聚合这些入侵检测样本得到一个初步的在线检测样本后，再将该初步的在线检测样本的格式转换为当前场景下的测试工具所适配的格式，得到一个在线检测样本。而针对于属于 CAN(FD)报文或 UDP 报文的各个入侵检测样本，则可以直接将每个入侵检测样本的格式

转换为当前场景下的测试工具所适配的格式，得到对应的一个在线检测样本。

举例来说，当待检测设备为车辆时，测试工具可以通过车辆的 OBD 接口实时地将不同的在线检测样本依次注入至车辆，针对于每个在线检测样本，若车辆识别其为攻击样本，则可以通过 VCU 向云端的安全运营中心（security operations center，SOC）进行报警。进而，在全部的在线检测样本都注入完成后，SOC 结合全部的在线检测样本的数量和在此期间车辆的报警记录信息，确定其中识别正确的在线检测样本的总数量和识别错误的在线检测样本的总数量，然后根据这两个总数量生成在线测评信息后发送给数据处理装置。进而，若识别正确的在线检测样本的总数量越多，识别错误的在线检测样本的总数量越少，则数据处理装置可以确定部署有入侵检测模型的待检测设备的检测效果越好，反之，则检测效果越差。

进一步地, 考虑到 CAN(FD)报文类型的测试注入需要 CANoe 或 PCAN 等测试工具, 而一台数据的测试注入需要 CANoe 或 Technica 等测试工具, 因此, 本申请实施例中的测试工具具体可以为 CANoe、PCAN、Technica 或其它能实现在线测评的工具, 与此对应的, 格式转换后的在线检测样本可以为 .PCAP、.ASC、.BLF 或其它能实现在线测试的工具所对应的格式, 数据处理装置将 .pcap 格式的入侵检测样本转换为测试工具所对应的格式的在线检测样本后, 通过测试工具将该在线检测样本注入待检测设备。如此, 通过使入侵检测样本集支持转换为多种测试工具所对应的格式, 能便于用户根据实际在线场景中的测试工具选择所对应的格式进行转换, 以适用于不同的在线测评场景, 提高入侵检测样本集在在线测评领域中的通用性。

在在线测评场景中，入侵检测样本集能支持在在线状态下测评部署有入侵检测模型的待检测设备的检测效果，如此，能便于用户根据该检测效果确定待检测设备的防攻击性能，确保仅出厂防攻击效果较好的待检测设备。

上述内容详细介绍了数据处理装置如何构建和应用入侵检测样本集，除此之外，一些场景中，数据处理装置还可以评估所构建的入侵检测样本集的质量，下面示例性地介绍一种具体的评估过程。

请参照图 6 所示, 其为本申请实施例提供的一种评估入侵检测样本集的流程示意图, 该流程包括:

步骤 601, 数据处理装置获取入侵检测样本集。

步骤 602, 数据处理装置计算入侵检测样本集在每个预设指标下的值, 并根据入侵检测样本集在各个预设指标下的值, 计算得到入侵检测样本集对应的评估值。

其中，各个预设指标可以是根据待检测设备所属的体系架构的特性而设置的，示例性地可以包括定量指标和定性指标，定量指标是指可以通过准确的数量进行定义的评估指标，定性指标是指不能直接量化而需要通过其它途径实现量化的评估指标。

举例来说,表2示出了本申请实施例提供的一种可能的预设指标的示意表:

表 2

[illegible]

参照表 2 所示, 该示例中, 各个预设指标可以包括数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标、平衡性指标、特征独立性指标和易用性指标中的一项或多项。其中, 数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标和平衡性指标属于定量指标, 特征独立性指标和易用性指标属于定性指标。且, 为了保持各个预设指标衡量的一致性, 各个预设指标的取值范围还可以保持一致, 比如均设置为 $[0,1]$, 也即是, 每个预设指标的值可以为 0 至 1 中的任一实数, 且包括 0 和 1。

下面先对表 2 所列出的各个预设指标进行详细介绍。

数据冗余指标

数据冗余指标用于指示入侵检测样本集的非冗余程度, 示例性地可以表示为入侵检测样本集中的非冗余的入侵检测样本的数量和全部的入侵检测样本的数量的比值。比如, 当入侵检测样本集中共存在 100 个入侵检测样本时, 如果其中的 5 个入侵检测样本均对应同一 ID, 剩余的 95 个入侵检测样本对应不同的 ID, 则该入侵检测样本集在数据冗余指标下的值为 95/100。

需要说明的是, 数据冗余指标也可以表示为其它形式, 只要能保证与冗余的入侵检测样本的数量和全部的入侵检测样本的数量的比值呈负相关即可。如此, 当全部的入侵检测样本都不同时, 数据冗余指标的值最大, 入侵检测样本集中的有效样本的数量最多, 样本的充足性最好。随着相同的入侵检测样本的数量增大, 数据冗余指标的值逐渐变小, 入侵检测样本集中的有效样本的数量逐渐变少, 样本的充足性逐渐变差。直至全部的入侵检测样本都相同时, 数据冗余指标的值最小, 入侵检测样本集中的有效样本的数量最少, 样本的充足性最差。

攻击覆盖指标

攻击覆盖指标用于指示入侵检测样本集中已包含的攻击类型的覆盖程度, 示例性地可以表示为入侵检测样本集所覆盖的攻击类型的数量与待检测设备中可能存在的全部攻击类型的数量的比值。比如, 假设待检测设备中可能存在的全部攻击类型为表 1 中所示意的 25 种攻击类型, 而入侵检测样本集中的第一类型攻击样本是按照其中的 10 种攻击类型攻击待检测设备得到的, 则该入侵检测样本集在攻击覆盖指标下的值为 10/25。

需要说明的是, 攻击覆盖指标也可以表示为其它形式, 只要能保证与所覆盖的攻击类型的数量与全部可能的攻击类型的数量的比值呈正相关即可。如此, 当入侵检测样本集覆盖全部可能的攻击类型时, 攻击覆盖指标的值最大, 入侵检测样本集中的样本类型最多, 样本的多样性最好。随着所覆盖的攻击类型的数量变少, 攻击覆盖指标的值逐渐变小, 入侵检测样本集中的样本类型逐渐变少, 样本的多样性逐渐变差。直至未覆盖任一攻击类型时, 攻击覆盖指标的值最小, 入侵检测样本集中的样本类型最少, 样本的多样性最差。

协议覆盖指标

协议覆盖指标用于指示入侵检测样本集中已包含的通信协议的覆盖程度, 示例性地可以表示为入侵检测样本集所覆盖的通信协议的数量与待检测设备中可能存在的全部通信协议的数量的比值。示例性地, 请参照表 3 所示, 其为本申请实施例提供的一种车联网领域中可能存在的通信协议的示意表, 应理解, 随着车联网技术的发展, 未来还可能会出现新的通信协议, 因此表 3 中的通信协议还可以随之更新, 本申请实施例对此不作具体限定。

表 3

协议名称	协议说明	连接类型
CAN (FD)	基于信号的通信	CAN (FD)
DoCAN	基于 CAN (FD)的诊断	CAN (FD)
DoIP	基于 IP 的诊断	TCP
SOME/IP	面向服务的通信	TCP
SOME/IP-SD	面向服务的通信, 服务发现	UDP
DDS	数据分发服务	TCP
MQTT	消息队列遥测传输协议	TCP
HTTP(S)	超文本传输协议	TCP

假设待检测设备为车辆,车辆中可能存在的全部通信协议为表 3 中所示意的 8 种协议,而入侵检测样本集所覆盖的通信协议包括 CAN (FD)、DoCAN、DDS、MQTT 和 HTTP(S),则该入侵检测样本集在协议覆盖指标下的值为 5/8。

需要说明的是,协议覆盖指标也可以表示为其它形式,只要能保证与所覆盖的通信协议的数量与全部可能的通信协议的数量比值呈正相关即可。如此,当入侵检测样本集覆盖全部可能的通信协议时,协议覆盖指标的值最大,该入侵检测样本集中的样本是通过对全部的通信协议消息都进行攻击而得到的,该入侵检测样本集的样本来源最多,样本的丰富性最好。随着所覆盖的协议的数量变少,协议覆盖指标的值逐渐变小,入侵检测样本集中的样本来源逐渐变少,样本的丰富性逐渐变差。直至未覆盖任一协议时,协议覆盖指标的值最小,入侵检测样本集中的样本来源最少,样本的丰富性最差。

业务覆盖指标

业务覆盖指标用于指示入侵检测样本集中已包含的业务覆盖程度,示例性地可以表示为入侵检测样本集所包含的业务的数量与待检测设备中可能存在的全部业务的数量比值。比如,假设待检测设备中可能存在的全部业务包括远程控制、日志传输、空中 (over-the-air, OTA) 更新、诊断服务、视频传输和网络管理这 6 种业务,而入侵检测样本集所包含的业务为远程控制、OTA 更新和诊断服务,则该入侵检测样本集在业务覆盖指标下的值为 3/6。

需要说明的是,业务覆盖指标也可以表示为其它形式,只要能保证与所覆盖的业务的数量与全部可能的业务的数量比值呈正相关即可。如此,当入侵检测样本集覆盖待检测设备中的全量业务时,业务覆盖指标的值最大,样本的业务适用性最好。随着所覆盖的业务的数量变少,业务覆盖指标的值逐渐变小,入侵检测样本集的业务适用性逐渐变差,直至未覆盖任一业务时,协议覆盖指标的值最小,入侵检测样本集的业务适用性最差。

数据标记指标

数据标记指标用于指示入侵检测样本集中的入侵检测样本的可标记程度,示例性地可以表示为入侵检测样本集中已标记的入侵检测样本的数量与全部的入侵检测样本的数量比值。其中,已标记的入侵检测样本可以包括上述步骤 301 中获得的真实攻击样本、模拟攻击样本和非攻击样本以及上述步骤 302 中获得的第二类型攻击样本,未标记的入侵检测样本包括上述步骤 301 中获得的无标记样本。举例来说,当入侵检测样本集中共存在 100 个入侵检测样本时,如果其中的 20 个入侵检测样本为第一类型攻击样本,20 个入侵检测样本为第二类型攻击样本,55 个入侵检测样本为非攻击样本,5 个入侵检测样本为无标记

样本, 则该入侵检测样本集中已标记的入侵检测样本的数量为 95, 因此, 该入侵检测样本集在数据标记指标下的值为 95/100。

需要说明的是, 数据标记指标也可以表示为其它形式, 只要能保证与已标记的入侵检测样本的数量与全部的入侵检测样本的总数量的比值呈正相关即可。如此, 当入侵检测样本集中的全部的入侵检测样本都已标记时, 意味着全部的入侵检测样本都已明确划分为非攻击样本和攻击样本, 而不包含不确定的样本, 该入侵检测样本集中的样本清晰度最高。随着已标记的入侵检测样本的数量变少, 入侵检测样本集中包含的不确定的样本逐渐变多, 样本的清晰度逐渐变差, 直至全部的入侵检测样本都未标记时, 入侵检测样本集中包含最多的不确定样本, 样本的清晰度最差。

平衡性指标

平衡性指标用于指示入侵检测样本集中的攻击样本和非攻击样本的均衡程度, 示例性地可以表示为入侵检测样本集中的全部入侵检测样本的总数量与攻击样本和非攻击样本的数量差的差值与全部的入侵检测样本的总数量的比值。比如, 当入侵检测样本集中共存在 100 个入侵检测样本时, 如果其中的 45 个入侵检测样本为攻击样本, 55 个入侵检测样本为非攻击样本, 则该入侵检测样本集中的攻击样本和非攻击样本的数量差为 10, 因此, 该入侵检测样本集在平衡性指标下的值可以为 $(100-10)/100$ 。

需要说明的是, 平衡性指标也可以表示为其它形式, 只要能保证与攻击样本和非攻击样本的数量差呈负相关即可。如此, 当入侵检测样本集中的攻击样本和非攻击样本各占 50% 时, 平衡性指标的值最大, 入侵检测样本集中的样本均衡性最好, 后续更容易从入侵检测样本集中取出等量的攻击样本和非攻击样本进行测试。随着攻击样本和非攻击样本的数量差变大, 入侵检测样本集中的样本均衡性逐渐变差, 越不容易从入侵检测样本集中取出等量的攻击样本和非攻击样本进行测试。直至入侵检测样本集中全部为攻击样本或全部为非攻击样本时, 入侵检测样本集中的样本均衡性最差, 无法从入侵检测样本集中取出等量的攻击样本和非攻击样本进行测试。

特征独立性指标

特征独立性指标用于指示使用入侵检测样本集进行离线测评时所提取的特征的独立性, 相互独立的特征越多, 则特征独立性指标的取值越大, 相互独立的特征越少, 则特征独立性指标的取值越小。

需要说明的是, 特征是否独立可以由本领域技术人员根据经验进行判断, 比如可以由工程师、专家或者第三方机构中的至少两者进行判断, 以综合各方经验得到较为准确的评估结果。

易用性指标

易用性指标用于指示入侵检测样本集所能兼容的应用场景的通用性, 该应用场景示例性地可以是使用入侵检测样本集进行在线测评时所能支持的测试工具的格式, 所能支持的测试工具的格式越多, 则易用性指标的取值越大, 所能支持的测试工具的格式越少, 则易用性指标的取值越小。

需要说明的是, 入侵检测样本集所能兼容的应用场景也可以由本领域技术人员根据经验进行判断, 比如可以由工程师、专家或者第三方机构中的至少两者进行判断, 以综合各方经验得到较为准确的评估结果。

进一步地, 按照上述表 2 所示意的各个预设指标, 在计算得到入侵检测样本集在每个

预设指标下的值之后，数据处理装置还可以根据各个预设指标对应的权重对入侵检测样本集在各个预设指标下的值进行加权平均，并将计算得到的加权平均值作为入侵检测样本集的评估值。其中，各个预设指标对应的权重可以相同，也可以不同，比如，一个示例中，可以配置各个定量的预设指标均对应第一权重，各个定性的预设指标均对应第二权重，且第一权重大于第二权重。如此，通过减小定性的预设指标的权重，能降低需要通过人为经验判断的预设指标对入侵检测样本对应的评估值的影响，使得评估过程更加关注理性的评判标准。

步骤 603，数据处理装置判断入侵检测样本集对应的评估值是否低于预设阈值，若是，则执行步骤 604，若否，则执行步骤 605。

步骤 604，数据处理装置调节入侵检测样本集，之后执行步骤 602。

示例性地，当入侵检测样本集对应的评估值低于预设阈值时，意味着入侵检测样本集的质量不能满足要求，此时，数据处理装置可以根据入侵检测样本集在各个预设指标下的值调节入侵检测样本集，使得调节后的入侵检测样本集在一个或多个预设指标下的值变大，进而增大入侵检测样本集对应的评估值。比如，当入侵检测样本集在平衡性指标下的值较低时，数据处理装置可以通过裁剪数量较多的样本，使得攻击样本和非攻击样本趋近于一致，以提高入侵检测样本集在平衡性指标下的值。或者，当入侵检测样本集在数据冗余指标下的值较低时，数据处理装置可以通过删除冗余的入侵检测样本，使得冗余的入侵检测样本的数量和全部的入侵检测样本的数量的比值减小，以提高入侵检测样本集在数据冗余指标下的值。

需要说明的是，上述内容只是示例性地给出一种可能的调节方式，在实际操作中，还可以由本领域技术人员根据经验选择其它方式调节入侵检测样本集，本申请实施例对此不作具体限定。

步骤 605，数据处理装置存储入侵检测样本集。

示例性地，当入侵检测样本集对应的评估值不低于预设阈值时，意味着入侵检测样本集的质量能够满足需求，该情况下，数据处理装置可以以文本格式将入侵检测样本集存储在数据库中。其中，文本格式示例性地可以是 .cpap 或者其它 IDS 所支持的格式。

在上述实施方式中，通过参照预设指标对已构建的入侵检测样本集进行评估，能根据评估结果不断优化入侵检测样本集，使优化后的入侵检测样本集更加适用于待检测设备所属的体系架构。且，通过结合定量指标和定性指标综合评判入侵检测样本集的构建质量，还能使评判结果更加全面，且更具有说服力。

应理解，通过预设指标评估入侵检测样本集的质量，这只是一种可选地评估方式，实际操作中还可能存在其它的评估方式，比如也可以通过人为经验直接评估，或者通过第三方机构间接评估，或者通过对比历史入侵检测样本集进行评估等，本申请实施例对此不作具体限定。

基于上述内容，图 7 示例性示意出本申请实施例提供的一种开发上述数据处理方案的设计架构图，该设计架构图示例性地可以是呈现给开发测试人员或运维人员的界面，由开发测试人员或运维人员根据该界面中需要实现的各个功能编写相应的程序代码。具体的，如图 7 所示，该设计架构中包括硬件工具层、数据生成层、调用接口层和应用场景层，下面针对每个层的内容进行详细地介绍。

硬件工具层负责提供硬件接口工具，该硬件接口工具用于接入待检测设备，为采集待检测设备的流量数据提供支撑。示例性地，当待检测设备为车辆时，硬件工具层主要可以包括面向信号的 CAN(FD)工具和面向服务的 ETH 工具，这两个工具可以接入在车辆的 OBD 接口上，以支持数据采集模块采集车辆针对于攻击行为所产生的流量数据。

5 数据生成层负责构建和查看入侵检测样本集，主要包括数据采集模块、AI 生成样本模块、特征提取模块、格式转换模块、样本集评估模块和数据查看模块，还可以包括数据库。实施中，数据采集模块可以通过硬件工具层采集待检测设备对于攻击行为所产生的流量数据，通过分析该流量数据，标记得到其中的第一类型攻击样本和非攻击样本，并将第一类型攻击样本和非攻击样本存入数据库。AI 生成样本模块可以对数据采集模块标记的第一类型攻击样本添加噪声，通过 AI 对抗算法处理得到容易被误报的第二类型攻击样本后，将第二类型攻击样本存入数据库。如此，数据库中的第一类型攻击样本、第二类型攻击样本和非攻击样本构成了入侵检测样本集。进而，特征提取模块可以对数据库中的入侵检测样本集进行特征提取后构成离线检测样本集，格式转换模块可以对数据库中的入侵检测样本集进行格式转换后构成在线检测样本集。样本集评估模块可以计算入侵检测样本集在各个预设指标下的评估值，并在评估值低于预设阈值时，调节入侵检测样本集，直至调节到入侵检测样本集对应的评估值不低于预设阈值为止。数据查看模块可以根据开发测试人员或运维人员的命令向其显示部分或全部入侵检测样本。

调用接口层负责提供应用编程接口 (application programming interface, API), 具体的，可以根据上层应用的使用需求，通过 API 从数据生成层中调用相应的数据提供给上层应用。比如，调用接口层可以通过 API 将数据生成层中的离线检测样本集中的部分离线检测样本提供给上层应用以训练入侵检测模型，也可以通过 API 将数据生成层中的离线检测样本集中的另一部分离线检测样本提供给上层应用以实现入侵检测模型的离线测评，还可以通过 API 将数据生成层中的在线检测样本提供给上层应用以实现部署有入侵检测模型的待检测设备的在线测评。

25 应用场景层负责与外界设备交互，以将入侵检测样本集应用到各种可能的应用场景中。一些典型的应用场景中，应用场景层可以利用调用接口层提供的离线检测样本在 IDS 开发中训练入侵检测模型，也可以利用调用接口层提供的在线检测样本在车云运维中测评部署有入侵检测模型的待检测设备的检测效果，也可以利用调用接口层提供的离线检测样本在 IDS 测试中测评入侵检测模型的检测效果，还可以将调用接口层提供的入侵检测样本集提供给第三方检测认证机构，以便于使待检测设备获得第三方认证机构的认证后顺利出厂，等等。

本申请的上述实施例中，通过结合已知攻击类型的第一类型攻击样本、未知攻击类型的第二类型攻击样本和非攻击样本构建入侵检测样本集，能使入侵检测样本集中的样本类型更加丰富全面，如此，当应用在车联网领域时，即使不同车型的网络拓扑和流量特征存在显著差异，这种构建方式也能针对于每种类型的车型构建出适配且丰富的入侵检测样本，有效提高使用入侵检测样本评估车辆网络安全的准确性。

应理解，本申请提供的数据处理方法还可以推广至任意对网络安全有需求的信息系统中。比如，还可以应用在智能家居领域中，通过攻击智能家居产品并进行加扰以获得丰富的攻击样本，研究智能家居场景下的攻击者画像。或者，还可以应用在工业控制领域中，

通过在数字孪生模型中引入攻击样本研究入侵防御，增强工控系统的鲁棒性。具体的，可以通过云服务器虚拟地构建出一台车辆或者一台车辆上所需测试的部件，进而对这台虚拟的车辆或车辆部件进行上述数据处理操作以获得入侵检测样本集，如此，能在真实组装车辆之前提前获知该车辆的防攻击能力，以便于在确定车辆能较好地防攻击的情况下才实际去造车，有效地节省人力和物力成本。

此外，随着系统架构的演变和新场景的出现，本申请提供的数据处理方法对类似的技术问题，同样适用，本申请对此也不作具体限定。

需要说明的是，上述各个信息的名称仅仅是作为示例，随着通信技术的演变，上述任意信息均可能改变其名称，但不管其名称如何发生变化，只要其含义与本申请上述信息的含义相同，则均落入本申请的保护范围之内。

上述主要从各个网元之间交互的角度对本申请提供的方案进行了介绍。可以理解的是，上述实现各网元为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本发明能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

根据前述方法，图 8 为本申请实施例提供的一种数据处理装置的结构示意图，该数据处理装置可以为具有处理能力的任意设备，如服务器，或者也可以为芯片或电路，比如可设置于服务器中的芯片或电路，或者还可以为多个服务器构成的服务器集群。如图 8 所示，该数据处理装置 800 可以包括处理器 801、存储器 802 和收发器 803，还可以进一步包括总线系统，处理器 801、存储器 802 和收发器 803 可以通过总线系统相连。

在实现过程中，上述方法的各步骤可以通过处理器 801 中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器 801 中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 802，处理器 801 读取存储器 802 中的信息，结合其硬件完成上述方法的步骤。

应理解，上述处理器 801 可以是一个芯片。例如，该处理器 801 可以是现场可编程门阵列（field programmable gate array, FPGA），可以是专用集成芯片（application specific integrated circuit, ASIC），还可以是系统芯片（system on chip, SoC），还可以是中央处理器（central processor unit, CPU），还可以是网络处理器（network processor, NP），还可以是数字信号处理电路（digital signal processor, DSP），还可以是微控制器（micro controller unit, MCU），还可以是可编程控制器（programmable logic device, PLD）或其他集成芯片。

可以理解，本申请实施例中的存储器 802 可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory, ROM）、可编程只读存储器（programmable ROM, PROM）、可擦除可编程只读存储器（erasable PROM, EPROM）、电可擦除可编程只读存储器（electrically EPROM, EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory, RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态

随机存取存储器 (static RAM, SRAM)、动态随机存取存储器 (dynamic RAM, DRAM)、同步动态随机存取存储器 (synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器 (double data rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器 (enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器 (synchlink DRAM, SLD RAM) 和直接内存总线随机存取存储器 (direct rambus RAM, DR RAM)。应注意, 本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

本申请实施例中, 存储器 802 用于存储指令, 处理器 801 用于执行该存储器 802 存储的指令, 实现如上图 3、图 4 或图 6 中所示的任意一项或任意多项中数据处理装置所对应的方法。具体来说, 处理器 801 通过调用收发器 803 攻击待检测设备, 获得第一类型攻击样本, 通过对第一类型攻击样本施加噪声, 获得第二类型攻击样本, 进而根据第一类型攻击样本和第二类型攻击样本, 构建得到入侵检测样本集。

在一种可选地实施方式中, 第一类型攻击样本可以包括真实攻击样本和模拟攻击样本, 真实攻击样本是通过人为攻击待检测设备得到的, 模拟攻击样本是通过攻击工具攻击待检测设备得到的。

在一种可选地实施方式中, 真实攻击样本可以对应如下攻击类型中的一项或多项: 身份标识号 ID 不存在攻击、重放攻击、篡改攻击、数据长度错误攻击、信号超出定义范围攻击、上下文错误攻击、ID 来源非指定电子控制单元 ECU 攻击、出现相同 ID 攻击、控制器局域网络 CAN 扫描攻击、统一诊断服务 UDS 执行敏感操作攻击、消息认证错误攻击、ECU 身份欺骗攻击、中间人攻击、ECU 认证错误攻击、暴力破解攻击、应用层协议错误攻击、未知的出栈连接攻击、未知的入栈连接攻击。

在一种可选地实施方式中, 模拟攻击样本可以对应如下攻击类型中的一项或多项: ID Fuzz 攻击、数据 Fuzz 攻击、CAN 的 Dos 攻击、ETH 的 Dos 攻击、畸形包注入攻击、端口扫描攻击。

在一种可选地实施方式中, 处理器 801 具体用于: 遍历预设的多种攻击类型中的每种攻击类型, 在遍历每种攻击类型时: 通过调用收发器 803 对待检测设备执行攻击类型对应的攻击行为, 并获取待检测设备对于攻击行为所产生的流量数据, 若流量数据是攻击流量, 则将流量数据标记为一个第一类型攻击样本。

在一种可选地实施方式中, 处理器 801 在获取待检测设备对于攻击行为所产生的流量数据之后, 若确定该流量数据是正常流量, 则将该流量数据标记为一个非攻击样本, 进而根据第一类型攻击样本、第二类型攻击样本和非攻击样本, 构建得到入侵检测样本集。

在一种可选地实施方式中, 处理器 801 具体用于: 对第一类型攻击样本施加噪声, 得到扰动样本, 并将扰动样本输入攻击识别模型, 获得攻击识别模型输出的识别结果, 进而根据识别结果调节扰动样本, 直至调节后的扰动样本对应的识别结果指示无法确定调节后的扰动样本是否为攻击样本时, 将调节后的扰动样本确定为第二类型攻击样本。其中, 识别结果用于指示扰动样本是否属于攻击样本。

在一种可选地实施方式中, 处理器 801 在根据第一类型攻击样本和第二类型攻击样本, 构建得到入侵检测样本集之后, 还可以对入侵检测样本集进行特征提取, 获得离线检测样本集, 该离线检测样本集用于测评入侵检测模型的检测性能。

在一种可选地实施方式中, 处理器 801 具体用于: 确定入侵检测样本集中的每个入侵检测样本的报文类型, 对于报文类型为 TCP 报文的各个入侵检测样本, 通过对属于同一

TCP 连接的全部入侵检测样本进行特征提取, 获得一个离线检测样本, 对于报文类型为 CAN(FD)报文或 UDP 报文的各个入侵检测样本, 通过对每个 CAN(FD)报文或 UDP 报文的入侵检测样本进行特征提取, 获得一个离线检测样本。

在一种可选地实施方式中, 特征提取出的特征包括如下特征中的一项或多项: 时间戳、频率特征、协议类型、内容特征、丢包率、错误包数量、连接持续时间、连接发起方、连接接收方。

在一种可选地实施方式中, 处理器 801 在根据第一类型攻击样本和第二类型攻击样本, 构建得到入侵检测样本集之后, 还可以对入侵检测样本集进行格式转换, 获得与测试工具格式相匹配的在线检测样本集, 进而通过测试工具将在线检测样本集输入待检测设备, 该在线检测样本用于测评部署有入侵检测模型的待检测设备的检测性能。

在一种可选地实施方式中, 处理器 801 在根据第一类型攻击样本和第二类型攻击样本, 构建得到入侵检测样本集之后, 还可以根据入侵检测样本集在各个预设指标下的值, 确定入侵检测样本集对应的评估值, 当评估值低于预设阈值时, 调节入侵检测样本集。

在一种可选地实施方式中, 预设指标可以包括如下指标中的一项或多项: 数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标、数据标记指标、平衡性指标、特征独立性指标、易用性指标。

在一种可选地实施方式中, 第一类型攻击样本可以通过攻击如下任一区域得到的: 整个待检测设备; 待检测设备的一个或多个物理区域; 或者, 待检测设备的一个或多个功能区域。

该数据处理装置 800 所涉及的与本申请实施例提供的数据处理装置的技术方案相关的概念, 解释和详细说明及其他步骤请参见前述方法或其他实施例中关于这些内容的描述, 此处不做赘述。

基于以上实施例以及相同构思, 图 9 为本申请实施例提供的另一种数据处理装置的示意图, 该数据处理装置 900 示例性地可以为上述任一实施例中所述的数据处理装置, 也可以为芯片或电路, 比如可设置于数据处理装置中的芯片或电路。该数据处理装置 900 可以实现如上图 3、图 4 或图 6 中所示的任一项或任多项对应的方法中数据处理装置所执行的步骤。

如图 9 所示, 该数据处理装置 900 可以包括攻击单元 901、扰动单元 902 和构建单元 903, 示例性地还可以包括特征提取单元 904、格式转换单元 905 和调节单元 906 中的一项或多项。攻击单元 901 用于通过攻击待检测设备, 获得第一类型攻击样本; 扰动单元 902 用于通过对第一类型攻击样本施加噪声, 获得第二类型攻击样本; 构建单元 903 用于根据第一类型攻击样本和第二类型攻击样本, 构建得到入侵检测样本集。一些场景中, 特征提取单元 904 用于: 对入侵检测样本集进行特征提取, 获得离线检测样本集, 该离线检测样本集用于测评入侵检测模型的检测性能。另一些场景中, 格式转换单元 905 用于: 对入侵检测样本集进行格式转换, 获得与测试工具格式相匹配的在线检测样本集, 并通过测试工具将在线检测样本集输入待检测设备, 该在线检测样本集用于测评部署有入侵检测模型的待检测设备的检测性能。另一些场景中, 调节单元 906 用于根据入侵检测样本集在各个预设指标下的值, 确定入侵检测样本集对应的评估值, 当该评估值低于预设阈值时, 调节入侵检测样本集。

实施中, 攻击单元 901 通过向待检测设备注入流量, 以实现对待检测设备的攻击。该

攻击单元在诸如流量时可以为发送单元、发送器、输出接口、管脚或电路。当数据处理装置 900 包含存储单元时,该存储单元用于存储计算机指令,攻击单元 901、扰动单元 902、构建单元 903、特征提取单元 904、格式转换单元 905 和调节单元 906 分别与存储单元通信连接,分别执行存储单元存储的计算机指令,使数据处理装置 900 可以用于执行上述任一实施例中数据处理装置所执行的方法。其中,攻击单元 901、扰动单元 902、构建单元 903、特征提取单元 904、格式转换单元 905 和调节单元 906 可以是一个通用中央处理器 (CPU),微处理器,特定应用集成电路 (application specific intergrated circuit, ASIC)。存储单元为芯片内的存储单元,如寄存器、缓存等,存储单元还可以是数据处理装置 900 内的位于该芯片外部的存储单元,如只读存储器 (read only memory, ROM) 或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器 (random access memory, RAM) 等。

该数据处理装置 900 所涉及的与本申请实施例提供的技术方案相关的概念,解释和详细说明及其他步骤请参见前述方法或其他实施例中关于这些内容的描述,此处不做赘述。

应理解,以上数据处理装置 900 的单元的划分仅仅是一种逻辑功能的划分,实际实现时可以全部或部分集成到一个物理实体上,也可以物理上分开。本申请实施例中,攻击单元 901、扰动单元 902、构建单元 903、特征提取单元 904、格式转换单元 905 和调节单元 906 可以由上述图 8 的处理器 801 实现。

根据本申请实施例提供的数据处理方法,本申请还提供一种数据处理装置,该数据处理装置包括处理器,处理器与存储器相连,存储器用于存储计算机程序,处理器用于执行存储器中存储的计算机程序,以使得数据处理装置实现如图 3、图 4 或图 6 中任一实施例所述的方法。

根据本申请实施例提供的数据处理方法,本申请还提供一种数据处理装置,该数据处理装置包括处理器和存储器,存储器用于存储计算机程序指令,处理器用于运行计算机程序指令以实现如图 3、图 4 或图 6 中任一实施例所述的方法。

根据本申请实施例提供的数据处理方法,本申请还提供一种芯片,该芯片可以包括处理器和接口,处理器用于通过接口读取指令,以执行如图 3、图 4 或图 6 中任一实施例所述的方法。

根据本申请实施例提供的数据处理方法,本申请还提供一种数据处理系统,该数据处理系统可以包括前述的待检测设备和数据处理装置。

根据本申请实施例提供的数据处理方法,本申请还提供一种计算机可读存储介质,该计算机可读存储介质存储有计算机程序,当计算机程序被运行时,实现如图 3、图 4 或图 6 中任一实施例所述的方法。

根据本申请实施例提供的数据处理方法,本申请还提供一种计算机程序产品,当该计算机程序产品在处理器上运行时,实现如图 3、图 4 或图 6 中任一实施例所述的方法。

在本说明书中使用的术语“部件”、“单元”、“系统”等用于表示计算机相关的实体、硬件、固件、硬件和软件的组合、软件、或执行中的软件。例如,部件可以是但不限于,在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。通过图示,在计算设备上运行的应用和计算设备都可以是部件。一个或多个部件可驻留在进程和/或执行线程中,部件可位于一个计算机上和/或分布在两个或更多个计算机之间。此外,这些部件可从在上面存储有各种数据结构的各种计算机可读介质执行。部件可例如根据具有一个或多个数据分组 (例如来自与本地系统、分布式系统和/或网络间的另一部件交互的

二个部件的数据，例如通过信号与其它系统交互的互联网)的信号通过本地和/或远程进程来通信。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各种说明性逻辑块 (illustrative logical block) 和步骤 (step)，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备 (可以是个人计算机，服务器，或者网络设备等) 执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器 (read-only memory, ROM)、随机存取存储器 (random access memory, RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求

1.一种数据处理方法，其特征在于，包括：

通过攻击待检测设备，获得第一类型攻击样本；

通过对所述第一类型攻击样本施加噪声，获得第二类型攻击样本；

根据所述第一类型攻击样本和所述第二类型攻击样本，构建得到入侵检测样本集。

2.如权利要求1所述的方法，其特征在于，所述第一类型攻击样本包括真实攻击样本和模拟攻击样本，所述真实攻击样本是通过人为攻击所述待检测设备得到的，所述模拟攻击样本是通过攻击工具攻击所述待检测设备得到的。

3.如权利要求2所述的方法，其特征在于，所述真实攻击样本对应如下攻击类型中的一项或多项：

身份标识号ID不存在攻击、重放攻击、篡改攻击、数据长度错误攻击、信号超出定义范围攻击、上下文错误攻击、ID来源非指定电子控制单元ECU攻击、出现相同ID攻击、控制器局域网络CAN扫描攻击、统一诊断服务UDS执行敏感操作攻击、消息认证错误攻击、ECU身份欺骗攻击、中间人攻击、ECU认证错误攻击、暴力破解攻击、应用层协议错误攻击、未知的出栈连接攻击、未知的入栈连接攻击。

4.如权利要求2或3所述的方法，其特征在于，所述模拟攻击样本对应如下攻击类型中的一项或多项：

ID模糊Fuzz攻击、数据Fuzz攻击、CAN的拒绝服务Dos攻击、以太网的Dos攻击、畸形包注入攻击、端口扫描攻击。

5.如权利要求1至4中任一项所述的方法，其特征在于，所述通过攻击待检测设备，获得第一类型攻击样本，包括：

遍历预设的多种攻击类型中的每种攻击类型，在遍历所述每种攻击类型时：

对所述待检测设备执行所述攻击类型对应的攻击行为；

获取所述待检测设备对于所述攻击行为所产生的流量数据；

若所述流量数据是攻击流量，则将所述流量数据标记为一个所述第一类型攻击样本。

6.如权利要求5所述的方法，其特征在于，

所述获取所述待检测设备对于所述攻击行为所产生的流量数据之后，还包括：

若所述流量数据是正常流量，则将所述流量数据标记为一个非攻击样本；

所述根据所述第一类型攻击样本和所述第二类型攻击样本，构建得到入侵检测样本集，包括：

根据所述第一类型攻击样本、所述第二类型攻击样本和所述非攻击样本，构建得到所述入侵检测样本集。

7.如权利要求1至6中任一项所述的方法，其特征在于，所述通过对所述第一类型攻击样本施加噪声，得到第二类型攻击样本，包括：

对所述第一类型攻击样本施加噪声，得到扰动样本；

将所述扰动样本输入攻击识别模型，获得所述攻击识别模型输出的识别结果，所述识别结果用于指示所述扰动样本是否属于攻击样本；

根据所述识别结果调节所述扰动样本，直至调节后的所述扰动样本对应的识别结果指示无法确定调节后的所述扰动样本是否为所述攻击样本时，将调节后的所述扰动样本确定

为所述第二类型攻击样本。

8.如权利要求 1 至 7 中任一项所述的方法,其特征在于,所述根据所述第一类型攻击样本和所述第二类型攻击样本,构建得到入侵检测样本集之后,还包括:

对所述入侵检测样本集进行特征提取,获得离线检测样本集;

5 其中,所述离线检测样本集用于测评入侵检测模型的检测性能。

9.如权利要求 8 所述的方法,其特征在于,所述对所述入侵检测样本集进行特征提取,获得离线检测样本集,包括:

确定所述入侵检测样本集中的每个入侵检测样本的报文类型;

10 对于报文类型为传输控制协议 TCP 报文的各个入侵检测样本,通过对属于同一 TCP 连接的全部入侵检测样本进行特征提取,获得一个离线检测样本;

对于报文类型为 CAN(FD)报文或 UDP 报文的各个入侵检测样本,通过对每个所述 CAN(FD) 报文或 UDP 报文的入侵检测样本进行特征提取,获得一个所述离线检测样本。

10.如权利要求 8 或 9 所述的方法,其特征在于,所述特征提取出的特征包括如下特征中的一项或多项:

15 时间戳、频率特征、协议类型、内容特征、丢包率、错误包数量、连接持续时间、连接发起方、连接接收方。

11.如权利要求 1 至 10 中任一项所述的方法,其特征在于,所述根据所述第一类型攻击样本和所述第二类型攻击样本,构建得到入侵检测样本集之后,还包括:

对所述入侵检测样本集进行格式转换,获得与测试工具格式相匹配的在线检测样本集;

20 通过所述测试工具将所述在线检测样本集输入所述待检测设备;

其中,所述在线检测样本集用于测评部署有入侵检测模型的所述待检测设备的检测性能。

12.如权利要求 1 至 11 中任一项所述的方法,其特征在于,所述根据所述第一类型攻击样本和所述第二类型攻击样本,构建得到入侵检测样本集之后,还包括:

25 根据所述入侵检测样本集在各个预设指标下的值,确定所述入侵检测样本集对应的评估值,当所述评估值低于预设阈值时,调节所述入侵检测样本集。

13.如权利要求 12 所述的方法,其特征在于,所述预设指标包括如下指标中的一项或多项:

30 数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标、数据标记指标、平衡性指标、特征独立性指标、易用性指标。

14.如权利要求 1 至 13 中任一项所述的方法,其特征在于,所述第一类型攻击样本是通过攻击如下任一区域得到的:

整个所述待检测设备;

所述待检测设备的一个或多个物理区域;

35 或者,

所述待检测设备的一个或多个功能区域。

15.一种数据处理装置,其特征在于,包括:

攻击单元,用于通过攻击待检测设备,获得第一类型攻击样本;

扰动单元,用于通过对所述第一类型攻击样本施加噪声,获得第二类型攻击样本;

40 构建单元,用于根据所述第一类型攻击样本和所述第二类型攻击样本,构建得到入侵

检测样本集。

16.如权利要求 15 所述的装置,其特征在于,所述第一类型攻击样本包括真实攻击样本和模拟攻击样本,所述真实攻击样本是通过人为攻击所述待检测设备得到的,所述模拟攻击样本是通过攻击工具攻击所述待检测设备得到的。

17.如权利要求 16 所述的装置,其特征在于,所述真实攻击样本对应如下攻击类型中的一项或多项:

身份标识 ID 不存在攻击、重放攻击、篡改攻击、数据长度错误攻击、信号超出定义范围攻击、上下文错误攻击、ID 来源非指定电子控制单元 ECU 攻击、出现相同 ID 攻击、控制器局域网络 CAN 扫描攻击、统一诊断服务 UDS 执行敏感操作攻击、消息认证错误攻击、ECU 身份欺骗攻击、中间人攻击、ECU 认证错误攻击、暴力破解攻击、应用层协议错误攻击、未知的出栈连接攻击、未知的入栈连接攻击。

18.如权利要求 16 或 17 所述的装置,其特征在于,所述模拟攻击样本对应如下攻击类型中的一项或多项:

ID 模糊 Fuzz 攻击、数据 Fuzz 攻击、CAN 的拒绝服务 Dos 攻击、以太网的 Dos 攻击、畸形包注入攻击、端口扫描攻击。

19.如权利要求 15 至 18 中任一项所述的装置,其特征在于,所述攻击单元具体用于:遍历预设的多种攻击类型中的每种攻击类型,在遍历所述每种攻击类型时:

对所述待检测设备执行所述攻击类型对应的攻击行为;

获取所述待检测设备对于所述攻击行为所产生的流量数据;

若所述流量数据是攻击流量,则将所述流量数据标记为一个所述第一类型攻击样本。

20.如权利要求 19 所述的装置,其特征在于,

所述攻击单元在获取所述待检测设备对于所述攻击行为所产生的流量数据之后,还用于:若所述流量数据是正常流量,则将所述流量数据标记为一个非攻击样本;

所述构建单元具体用于:根据所述第一类型攻击样本、所述第二类型攻击样本和所述非攻击样本,构建得到所述入侵检测样本集。

21.如权利要求 15 至 20 中任一项所述的装置,其特征在于,所述扰动单元具体用于:对所述第一类型攻击样本施加噪声,得到扰动样本;

将所述扰动样本输入攻击识别模型,获得所述攻击识别模型输出的识别结果,所述识别结果用于指示所述扰动样本是否属于攻击样本;

根据所述识别结果调节所述扰动样本,直至调节后的所述扰动样本对应的识别结果指示无法确定所述扰动样本是否为所述攻击样本时,将调节后的所述扰动样本确定为所述第二类型攻击样本。

22.如权利要求 15 至 21 中任一项所述的装置,其特征在于,还包括特征提取单元;所述特征提取单元用于:

对所述入侵检测样本集进行特征提取,获得离线检测样本集;

其中,所述离线检测样本集输用于测评入侵检测模型的检测效果。

23.如权利要求 22 所述的装置,其特征在于,所述特征提取单元具体用于:

确定所述入侵检测样本集中的每个入侵检测样本的报文类型;

对于报文类型为传输控制协议 TCP 报文的各个入侵检测样本,通过对属于同一 TCP 连接的全部入侵检测样本进行特征提取,获得一个离线检测样本;

对于报文类型为 CAN(FD)报文或 UDP 报文的各个入侵检测样本,通过对每个所述 CAN(FD)报文或 UDP 报文的入侵检测样本进行特征提取,获得一个所述离线检测样本。

24.如权利要求 22 或 23 所述的装置,其特征在于,所述特征提取出的特征包括如下特征中的一项或多项:

时间戳、频率特征、协议类型、内容特征、丢包率、错误包数量、连接持续时间、连接发起方、连接接收方。

25.如权利要求 15 至 24 中任一项所述的装置,其特征在于,还包括格式转换单元;所述格式转换单元用于:

对所述入侵检测样本集进行格式转换,获得与测试工具格式相匹配的在线检测样本集;

通过所述测试工具将所述在线检测样本集输入所述待检测设备;

其中,所述在线检测样本集用于测评部署有入侵检测模型的所述待检测设备的检测性能。

26.如权利要求 15 至 25 中任一项所述的装置,其特征在于,还包括调节单元;所述调节单元用于:

根据所述入侵检测样本集在各个预设指标下的值,确定所述入侵检测样本集对应的评估值,当所述评估值低于预设阈值时,调节所述入侵检测样本集。

27.如权利要求 26 所述的装置,其特征在于,所述预设指标包括如下指标中的一项或多项:

数据冗余指标、攻击覆盖指标、协议覆盖指标、业务覆盖指标、数据标记指标、平衡性指标、特征独立性指标、易用性指标。

28.如权利要求 15 至 27 中任一项所述的装置,其特征在于,所述第一类型攻击样本是通过攻击如下任一区域得到的:

整个所述待检测设备;

所述待检测设备的一个或多个物理区域;

或者,

所述待检测设备的一个或多个功能区域。

29.一种数据处理装置,其特征在于,包括处理器和存储器,所述存储器存储计算机程序指令,所述处理器运行所述计算机程序指令以实现如权利要求 1 至权利要求 14 中任一项所述的方法。

30.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有计算机程序,当所述计算机程序被运行时,实现如权利要求 1 至权利要求 14 中任一项所述的方法。

31.一种计算机程序产品,其特征在于,当所述计算机程序产品在处理器上运行时,实现如权利要求 1 至权利要求 14 中任一项所述的方法。

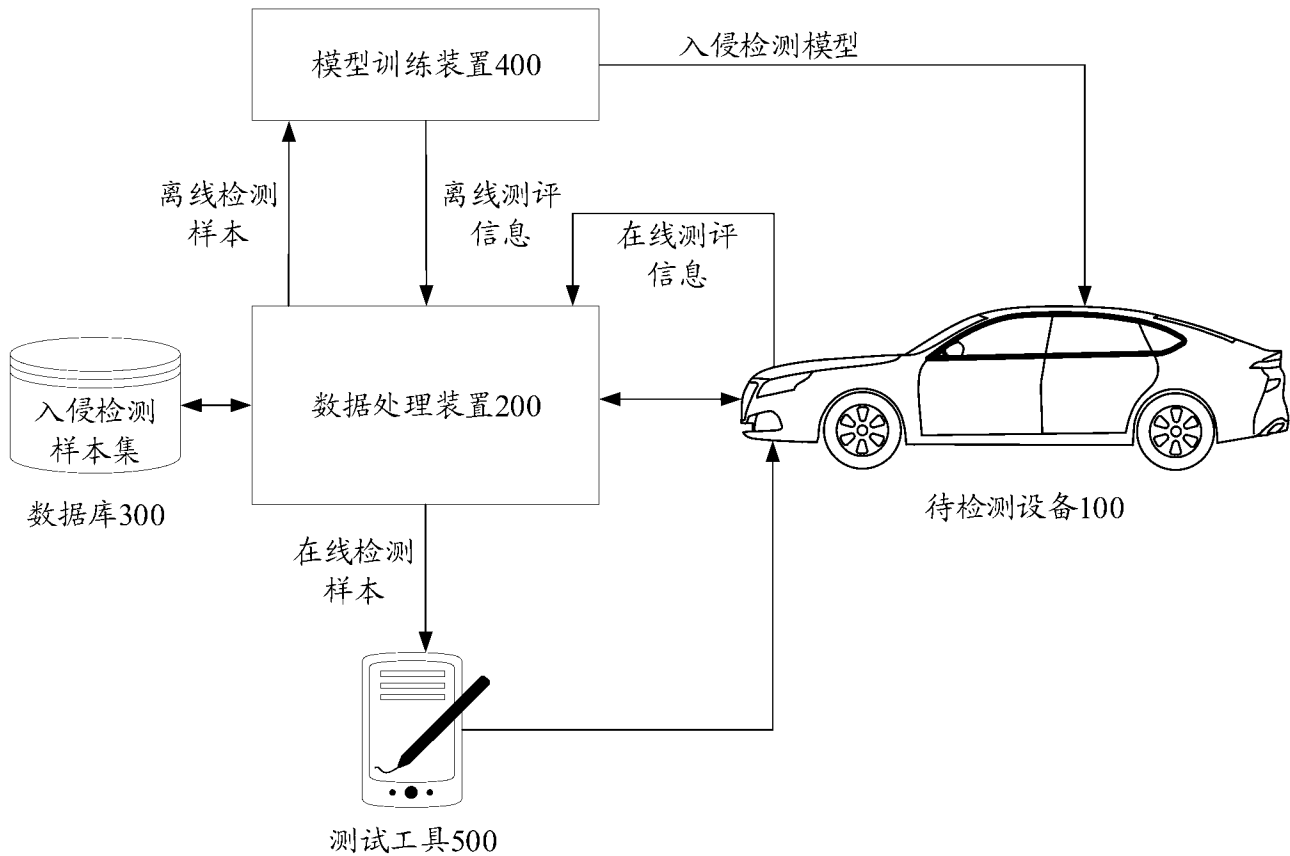


图 1

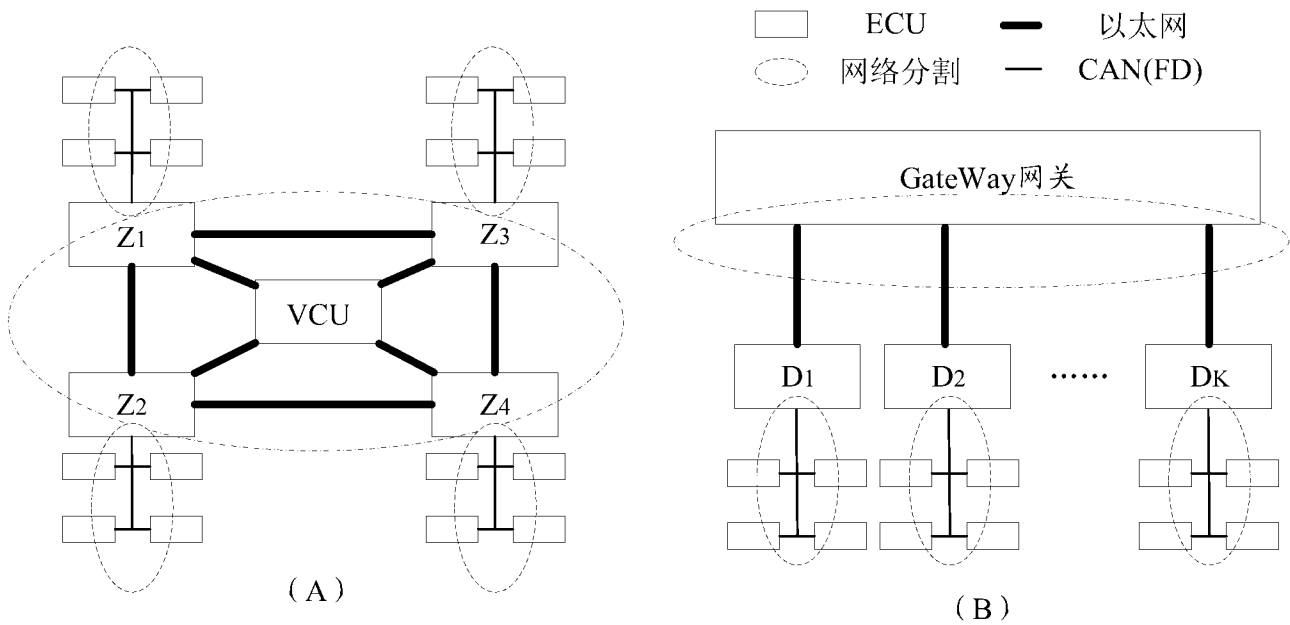


图 2

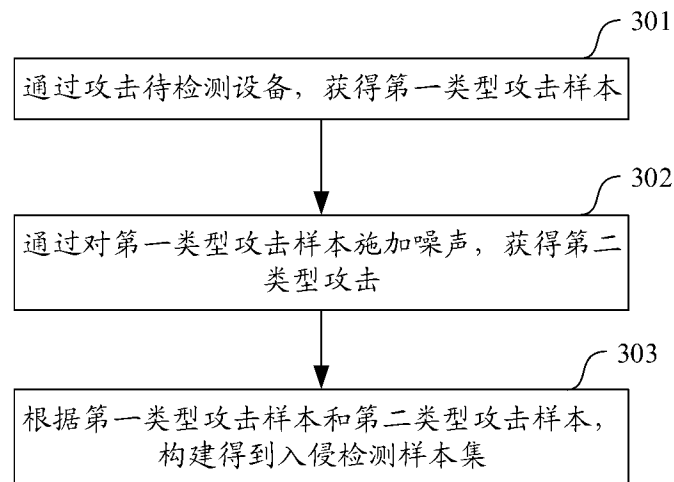


图 3

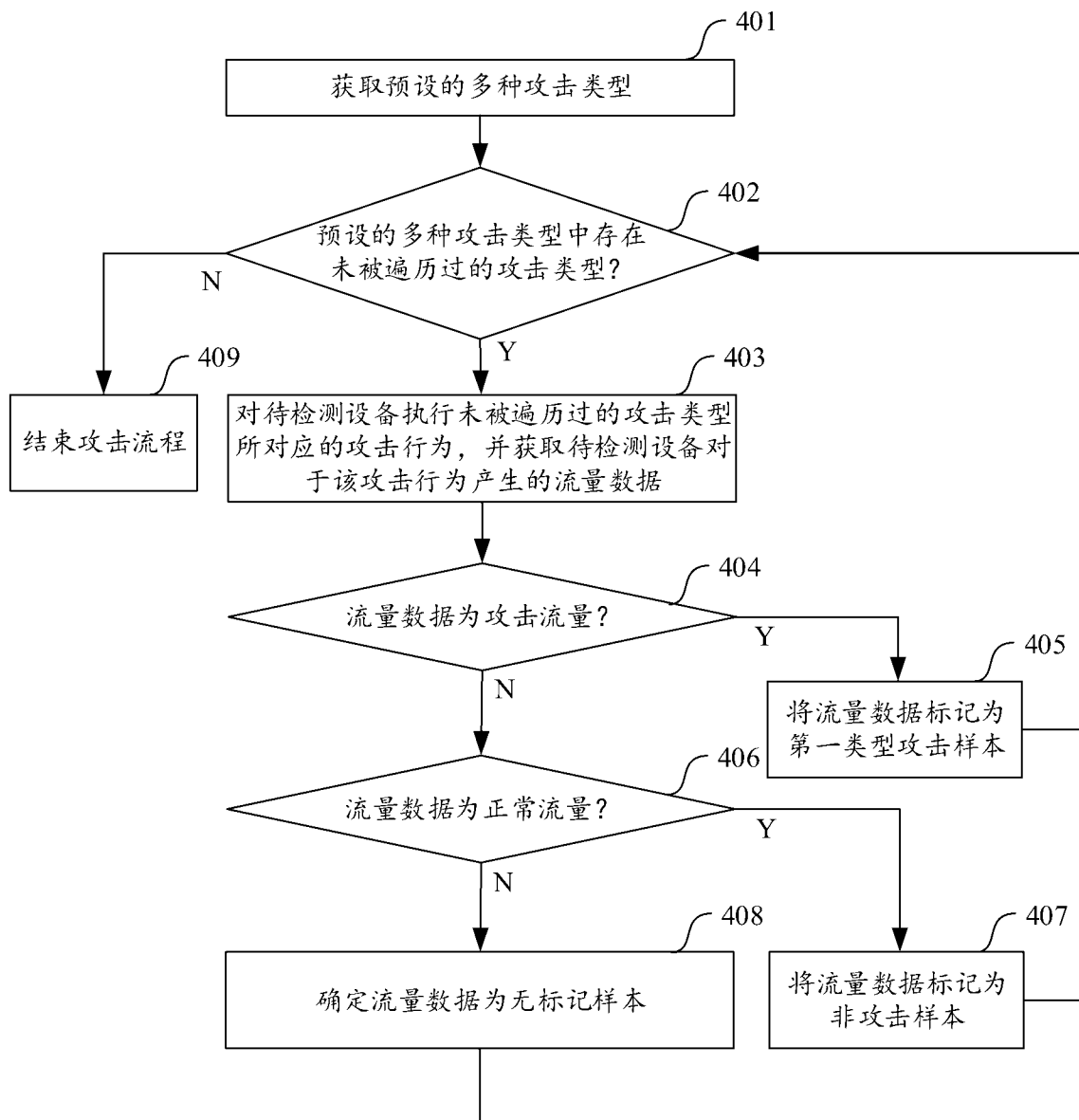


图 4

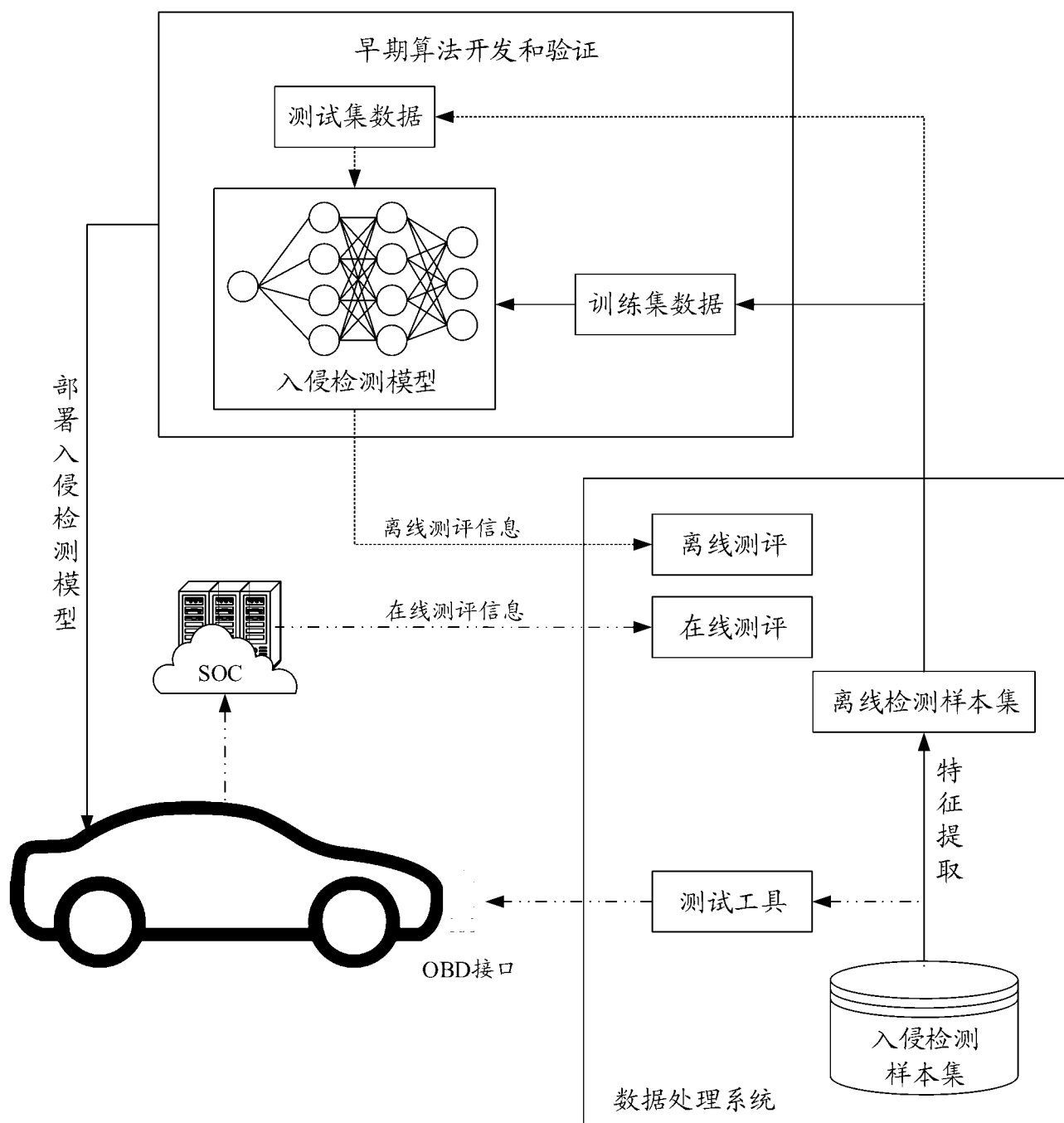


图 5

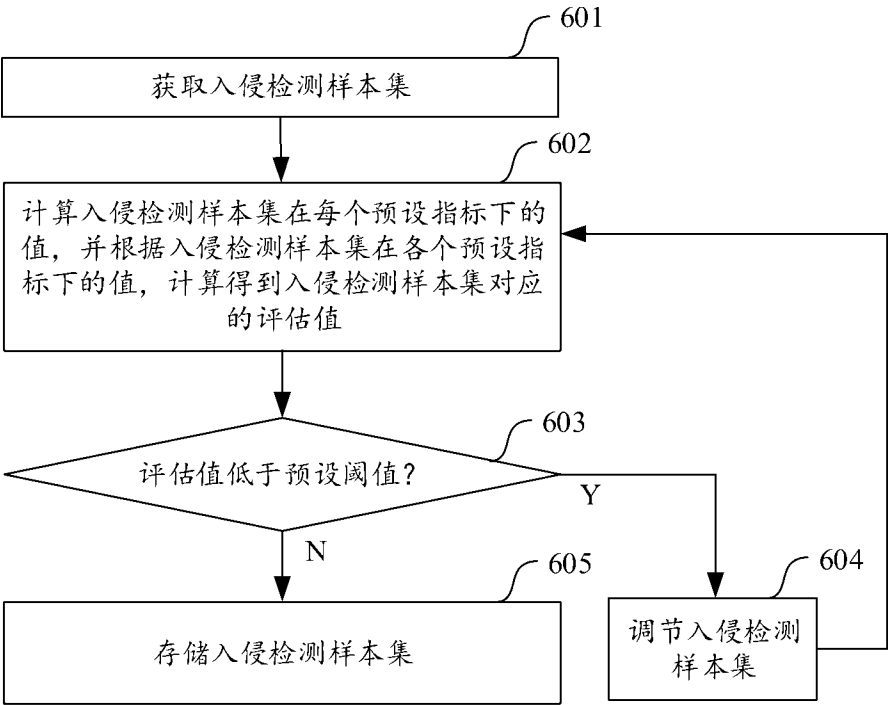


图 6

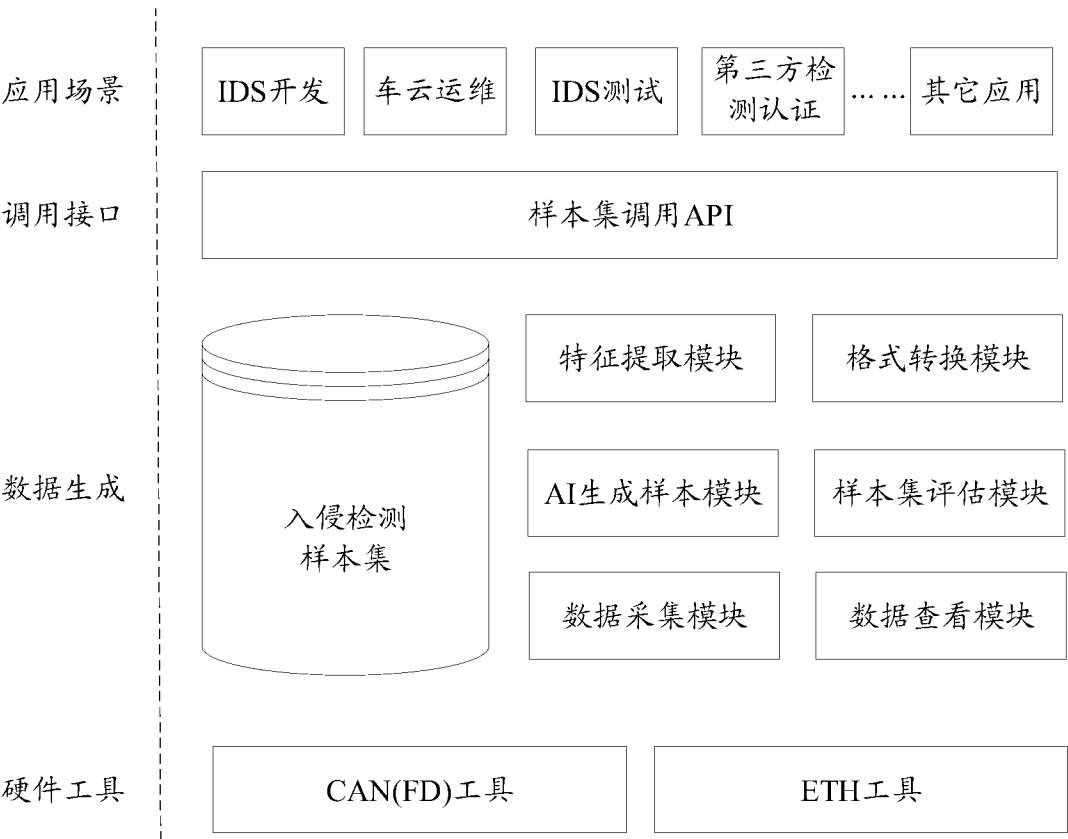


图 7

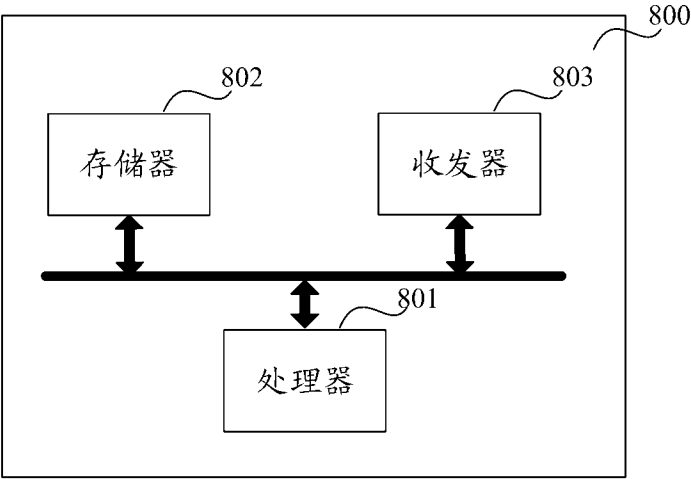


图 8

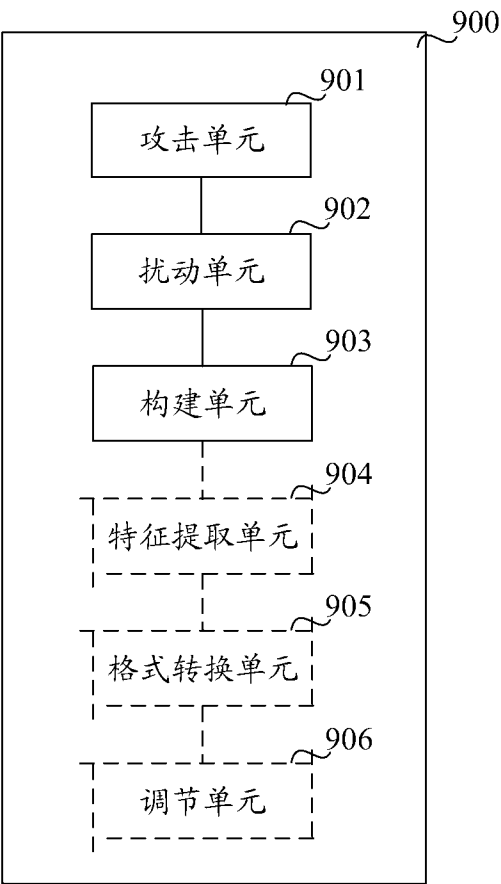


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/078600

A. CLASSIFICATION OF SUBJECT MATTER H04L9/40(2022.01)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) IPC: 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) CNTXT; CNABS; CNKI; VEN; WOTXT; USTXT; EPTXT: 侯硕; 岳青伦; 李廷森, 华为, 样本, 攻击, 噪声, 扰动, 控制器局域网网络, 统一诊断服务, attack, sample, noise, distribute, CAN, UDS, ECU, Fuzz, Dos																				
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 106656981 A (NEUSOFT CORP.) 10 May 2017 (2017-05-10) description, paragraphs [0022]-[0078] and [0085]-[0087]</td> <td>1-31</td> </tr> <tr> <td>X</td> <td>CN 114707572 A (ZHEJIANG UNIVERSITY OF TECHNOLOGY) 05 July 2022 (2022-07-05) description, paragraphs [0044]-[0065] and [0087]-[0092]</td> <td>1-31</td> </tr> <tr> <td>A</td> <td>CN 115129607 A (CHINA ELECTRIC POWER RESEARCH INSTITUTE CO., LTD. et al.) 30 September 2022 (2022-09-30) entire document</td> <td>1-31</td> </tr> <tr> <td>A</td> <td>CN 115712893 A (HUAWEI TECHNOLOGIES CO., LTD.) 24 February 2023 (2023-02-24) entire document</td> <td>1-31</td> </tr> <tr> <td>A</td> <td>JP 2022163431 A (HITACHI, LTD.) 26 October 2022 (2022-10-26) entire document</td> <td>1-31</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	CN 106656981 A (NEUSOFT CORP.) 10 May 2017 (2017-05-10) description, paragraphs [0022]-[0078] and [0085]-[0087]	1-31	X	CN 114707572 A (ZHEJIANG UNIVERSITY OF TECHNOLOGY) 05 July 2022 (2022-07-05) description, paragraphs [0044]-[0065] and [0087]-[0092]	1-31	A	CN 115129607 A (CHINA ELECTRIC POWER RESEARCH INSTITUTE CO., LTD. et al.) 30 September 2022 (2022-09-30) entire document	1-31	A	CN 115712893 A (HUAWEI TECHNOLOGIES CO., LTD.) 24 February 2023 (2023-02-24) entire document	1-31	A	JP 2022163431 A (HITACHI, LTD.) 26 October 2022 (2022-10-26) entire document	1-31
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																		
X	CN 106656981 A (NEUSOFT CORP.) 10 May 2017 (2017-05-10) description, paragraphs [0022]-[0078] and [0085]-[0087]	1-31																		
X	CN 114707572 A (ZHEJIANG UNIVERSITY OF TECHNOLOGY) 05 July 2022 (2022-07-05) description, paragraphs [0044]-[0065] and [0087]-[0092]	1-31																		
A	CN 115129607 A (CHINA ELECTRIC POWER RESEARCH INSTITUTE CO., LTD. et al.) 30 September 2022 (2022-09-30) entire document	1-31																		
A	CN 115712893 A (HUAWEI TECHNOLOGIES CO., LTD.) 24 February 2023 (2023-02-24) entire document	1-31																		
A	JP 2022163431 A (HITACHI, LTD.) 26 October 2022 (2022-10-26) entire document	1-31																		
☐ 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 “D” document cited by the applicant in the international application “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 01 November 2023		Date of mailing of the international search report 07 November 2023																		
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/CN) China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088		Authorized officer Telephone No.																		

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/078600

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106656981	A	10 May 2017	JP	2018067304	A	26 April 2018
				JP	6534712	B2	26 June 2019
				US	2018115568	A1	26 April 2018
				US	10237289	B2	19 March 2019
CN	114707572	A	05 July 2022	None			
CN	115129607	A	30 September 2022	None			
CN	115712893	A	24 February 2023	WO	2023019970	A1	23 February 2023
JP	2022163431	A	26 October 2022	None			

A. 主题的分类 H04L9/40(2022.01)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) IPC: H04L 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)) CNTXT;CNABS;CNKI;VEN;WOTXT;USTXT;EPTXT: 侯硕; 岳青伦; 李廷森, 华为, 样本, 攻击, 噪声, 扰动, 控制器局域网络, 统一诊断服务, attack, sample, noise, distribute, CAN, UDS, ECU, Fuzz, Dos		
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	CN 106656981 A (东软集团股份有限公司) 2017年5月10日 (2017 - 05 - 10) 说明书第[0022]-[0078]、[0085]-[0087]段	1-31
X	CN 114707572 A (浙江工业大学) 2022年7月5日 (2022 - 07 - 05) 说明书第[0044]-[0065]、[0087]-[0092]段	1-31
A	CN 115129607 A (中国电力科学研究院有限公司等) 2022年9月30日 (2022 - 09 - 30) 全文	1-31
A	CN 115712893 A (华为技术有限公司) 2023年2月24日 (2023 - 02 - 24) 全文	1-31
A	JP 2022163431 A (HITACHI LTD) 2022年10月26日 (2022 - 10 - 26) 全文	1-31
☐ 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 “D” 申请人在国际申请中引证的文件 “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 2023年11月1日		国际检索报告邮寄日期 2023年11月7日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088		授权官员 周萍 电话号码 (+86) 020-28958637

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/078600

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	106656981	A	2017年5月10日	JP	2018067304	A	2018年4月26日
				JP	6534712	B2	2019年6月26日
				US	2018115568	A1	2018年4月26日
				US	10237289	B2	2019年3月19日
CN	114707572	A	2022年7月5日	无			
CN	115129607	A	2022年9月30日	无			
CN	115712893	A	2023年2月24日	WO	2023019970	A1	2023年2月23日
JP	2022163431	A	2022年10月26日	无			