



(10) 授权公告号 CN 114208116 B

(45) 授权公告日 2024. 12. 03

(21) 申请号 202080055847.3

(22) 申请日 2020.07.31

(65) 同一申请的已公布的文献号

申请公布号 CN 114208116 A

(43) 申请公布日 2022.03.18

(30) 优先权数据

10-2019-0093503 2019.07.31 KR

10-2020-0095519 2020.07.30 KR

(85) PCT国际申请进入国家阶段日

2022.01.30

(86) PCT国际申请的申请数据

PCT/KR2020/010142 2020.07.31

(87) PCT国际申请的公布数据

W02021/020935 KO 2021.02.04

(73) 专利权人 现代自动车株式会社

地址 韩国首尔

专利权人 起亚株式会社

高丽大学校产学协力团

(72) 发明人 金辉刚 郑成薰 朴胜煜 林和平

(74) 专利代理机构 北京路浩知识产权代理有限公司 11002

专利代理师 张晶 赵赫

(51) Int.Cl.

H04L 9/40 (2022.01)

H04W 12/121 (2021.01)

H04W 4/48 (2018.01)

(56) 对比文件

CN 107770174 A, 2018.03.06

CN 109274673 A, 2019.01.25

审查员 周秋爽

权利要求书2页 说明书9页 附图8页

(54) 发明名称

入侵应对系统和方法

(57) 摘要

本公开提供一种入侵应对系统和方法,用于通过搭载在车载网络 (IVN) 中的SDN支持交换机和与SDN支持交换机进行通信的SDN控制器来检测和应对车辆入侵,在该方法中SDN控制器从SDN支持交换机接收流表,使入侵检测系统 (IDS) 执行入侵检测,并根据执行入侵检测的结果更新流表。



1. 一种入侵应对系统,其为用于车辆的车载网络即IVN的入侵应对系统,其特征在于,所述入侵应对系统包括:

软件定义网络支持交换机,即SDN支持交换机,安装在IVN中,通过参照来自流表的流条目来控制流入的数据包的流;以及

SDN控制器,设置在车辆外部,与所述SDN支持交换机进行通信,

其中所述SDN控制器从所述SDN支持交换机接收流统计数据,将所述流统计数据传送到入侵检测系统即IDS以便所述IDS执行入侵检测,当检测到入侵时,从所述IDS接收入侵检测的监控结果,并将所述监控结果传送到所述SDN支持交换机,

所述流条目包括规则字段、动作字段和统计字段,所述统计字段包括匹配计数器字段和字节计数器字段,并且

所述SDN支持交换机进一步将所述流入的数据包与所述流表的每个流条目的规则字段进行比较,当所述流入的数据包与所述流表的流条目的规则字段的匹配在预设范围内或预设数量以上时,更新所述匹配计数器字段,并且通过计算匹配数据包的每秒字节数来更新所述字节计数器字段。

2. 根据权利要求1所述的入侵应对系统,其特征在于,

所述SDN控制器从所述SDN支持交换机接收所述流统计数据的时间间隔T基于所述车辆的内部或外部环境、所述车辆的驾驶环境、所述IDS所采用的入侵检测方法和执行入侵检测的结果中的全部或部分来设置或重置。

3. 根据权利要求1所述的入侵应对系统,其特征在于,

所述SDN控制器与多个SDN支持交换机基于各自接口进行通信并从多个所述SDN支持交换机接收各自流统计数据,并且所述SDN控制器接收所述流统计数据的时间间隔T针对多个所述SDN支持交换机中的每一个单独地设置。

4. 根据权利要求3所述的入侵应对系统,其特征在于,

所述流条目包括一个或多个字段,并且所述一个或多个字段根据多个所述SDN支持交换机中的每一个所采用的接口来确定。

5. 根据权利要求1所述的入侵应对系统,其特征在于,

所述SDN支持交换机在接收到所述监控结果时更新所述流表。

6. 一种入侵应对方法,其为使用搭载在车载网络即IVN中的软件定义网络支持交换机即SDN支持交换机和设置在车辆外部的SDN控制器检测和应对车辆入侵的方法,所述SDN支持交换机通过参照来自流表的流条目来控制流入的数据包的数据包流,其特征在于,所述方法包括:

由所述SDN支持交换机将流统计数据传送到所述SDN控制器;

由所述SDN控制器接收所述流统计数据,并将所述流统计数据传送到入侵检测系统即IDS;

当检测到入侵时,由所述SDN控制器从所述IDS接收入侵检测的监控结果;

由所述SDN控制器将所述监控结果传送到所述SDN支持交换机;以及

由所述SDN支持交换机基于所述监控结果更新所述流表,

其中所述流条目包括规则字段、动作字段和统计字段,所述统计字段包括匹配计数器字段和字节计数器字段,并且

所述方法进一步包括：

由所述SDN支持交换机将所述流入的数据包与所述流表的每个流条目的规则字段进行比较,当所述流入的数据包与所述流表的流条目的规则字段的匹配在预设范围内或预设数量以上时,更新所述匹配计数器字段,并且通过计算匹配数据包的每秒字节数来更新所述字节计数器字段。

7. 根据权利要求6所述的方法,其特征在于,

所述SDN控制器从所述SDN支持交换机接收所述流统计数据的时间间隔T基于所述车辆的内部或外部环境、所述车辆的驾驶环境、所述IDS所采用的入侵检测方法和执行入侵检测的结果中的全部或部分来设置或重置。

8. 根据权利要求6所述的方法,其特征在于,进一步包括:

由所述SDN支持交换机将包括从IVN流入的数据包的数据包输入消息传送到所述SDN控制器;以及

由所述SDN控制器将包括所述流入的数据包和转发动作的数据包输出消息传送到所述SDN支持交换机。

9. 根据权利要求8所述的方法,其特征在于,

当所述流表中不存在与所述流入的数据包匹配的流条目时或者当匹配的流表到期时,执行将数据包输入消息传送到所述SDN控制器。

10. 根据权利要求6所述的方法,其特征在于,

所述SDN控制器与多个SDN支持交换机基于各自接口进行通信并从多个所述SDN支持交换机接收各自流统计数据,并且所述SDN控制器接收所述流统计数据的时间间隔T针对多个所述SDN支持交换机单独地设置。

11. 根据权利要求10所述的方法,其特征在于,

所述流条目包括一个或多个字段,并且所述一个或多个字段根据多个所述SDN支持交换机中的每一个所采用的接口来确定。

入侵应对系统和方法

技术领域

[0001] 本公开涉及一种用于检测和阻止对车载网络 (IVN) 的入侵或攻击的技术。

背景技术

[0002] 本部分所描述的内容仅为本实施例提供背景信息,并且不构成现有技术。

[0003] 已经开发出应用车辆到一切事物 (V2X) 通信和基于网络的自动驾驶相关技术的商用车辆。然而,应用V2X通信和车载网络的商用车辆容易受到入侵通信网络或网络通信的攻击。图1是示出车辆的安全威胁类型的分类的示图。威胁车辆安全的攻击包括特权窃取攻击和非特权窃取攻击、基于攻击源的外部攻击以及针对车辆内部元件的内部攻击。内部攻击通常由攻击者通过物理访问目标车辆来造成明显的破坏,而外部攻击主要使用诸如短距离射频通信、无钥匙进入系统或轮胎压力监测系统的基于传感器的系统,因此其影响力是有限的。然而,随着IVN环境中的车辆内连接性和V2X环境中的车辆间连接性的增加,车辆外部攻击的影响力预计会增加。

[0004] 即使在恰当地检测到攻击或入侵时,如何应对地缓解攻击或入侵也一直是一个问题。先前提出的缓解方法并不是对IVN车辆攻击的恰当的替代方案。

[0005] 换言之,缺乏用于检测和恰当地应对支持V2X和IVN的车辆风险的技术框架的开发。目前,由于车辆系统的计算能力的限制,搭载在车辆中的入侵检测系统 (Intrusion Detection System, IDS) 仅有限地支持轻量级算法。因此,需要设计一种克服这种计算能力的限制的用于检测入侵并进行应对的入侵应对系统 (Intrusion Response System, IRS)。

发明内容

[0006] 技术问题

[0007] 本公开提供一种使用软件定义网络 (Software-Defined Networking, SDN) 技术来检测和应对对基于以太网的车载网络 (IVN) 的攻击的方法和使用该方法的系统。

[0008] 技术方案

[0009] 根据本公开的一个方面,提供一种用于车载网络 (IVN) 的入侵应对系统。该入侵应对系统的特征在于,包括:软件定义网络 (SDN) 支持交换机,安装在车辆的IVN中并且通过参照来自流表的流条目 (flow entry) 来控制流入的数据包的流;以及SDN控制器,与SDN支持交换机进行通信,以一定的时间间隔T从SDN支持交换机接收流表以执行监控,并将监控结果传送到SDN支持交换机。SDN控制器将流表传送到入侵检测系统 (IDS) 以便IDS执行入侵检测,并从IDS接收作为监控结果的执行入侵检测的结果。

[0010] 根据本公开的另一方面,提供一种使用搭载在车辆的车载网络 (IVN) 中的软件定义网络 (SDN) 支持交换机和设置在车辆外部的SDN控制器检测和应对车辆入侵的方法。该方法的特征在于,包括:由SDN支持交换机以一定的时间间隔T将流表传送到SDN控制器;由SDN控制器接收流表,并将接收到的流表传送到入侵检测系统 (IDS);由SDN控制器使IDS基于包括在流表中的每个流条目的全部或部分字段执行入侵检测,并且由SDN控制器从IDS接收入

入侵检测的结果;由SDN控制器将包括入侵检测的结果的数据包输出消息(packet-out message)传送到SDN支持交换机;以及由SDN支持交换机基于该数据包输出消息更新流表。

[0011] 有益效果

[0012] 本公开的SDN支持交换机可以同时监控和阻止流入IVN的流量。也就是说,SDN支持交换机在基于流表监控流入车辆的流量的同时,可以选择性地阻止被识别为攻击的流量。

[0013] 根据本公开,判断流入车辆的数据包是否是入侵数据包以及执行流控制动作是远程确定而不是在IVN中确定,从而可以基于例如深度学习或人工智能方法的要求高计算性能的高性能检测技术来检测入侵数据包,而不管车辆的内部环境如何,并且可以根据检测结果给出恰当的应对命令。此外,设置在车辆外部的入侵检测系统能够实时更改或更新检测算法或模型,而不管车辆环境如何。

[0014] 此外,根据本公开,可以在一个地方同时且全面地监控发生在多个车辆中的内部流量。这可以通过收集难以从单个车辆检测到的模糊异常并将收集的异常与其他车辆的正常流量进行比较,实现更精确的攻击检测。

[0015] 本公开的技术还可以通过将SDN设备添加到设置在现有的基于以太网的车辆中的普通交换机来应用。因此,可以在尽可能减少基于以太网的IVN的拓扑结构的变化的同时应用本公开的技术。

附图说明

[0016] 图1是示出车辆的安全威胁类型的分类的示意图。

[0017] 图2是示出典型的软件定义网络(SDN)的架构的概念图。

[0018] 图3示出构成SDN系统的SDN控制器和SDN设备以及构成搭载在SDN设备中的流表(flow table)的流条目的构成字段。

[0019] 图4是示意性地示出根据本公开的实施例的入侵应对系统的结构的概念图。

[0020] 图5A和图5B是示出根据本公开的实施例的车载网络(IVN)的示例性拓扑结构的示意图。

[0021] 图6A和图6B是示出根据本公开的实施例的入侵应对系统的集中式结构和分布式结构的控制平面拓扑结构的示意图。

[0022] 图7A和图7B是示出根据本公开的实施例的可应用于入侵应对系统的入侵检测系统(IDS)的拓扑结构的示意图。

[0023] 图8是示出支持根据本公开的入侵应对系统的有用性的用例场景的示意图。

[0024] 图9A和图9B是示出根据本实施例的数据驱动入侵检测和应对方法的流程图。

具体实施方式

[0025] 在下文中,将参照附图详细描述本公开的一些实施例。应当注意的是,在对各个附图中的组件添加附图标记时,相同的附图标记表示相同的组件,尽管这些组件在不同的附图中示出。此外,在本公开的以下描述中,将省略对相关的已知功能和配置的详细描述以免使得本公开的要旨不清楚。

[0026] 此外,诸如第一、第二、A、B、(a)、(b)等的各种术语仅用于区分一个组件与另一组件,而不是用于暗示或指示组件的本质、顺序或次序。在整个本说明书中,当一个部件“包

括”或“包括有”组件时,除非另有明确说明,否则意味着该部件进一步包括其他组件,而不排除包括其他组件。此外,说明书中记载的“单元”、“模块”等术语是指用于处理至少一种功能或操作的一个或多个单元,其可以通过硬件、软件或硬件和软件的组合来实现。

[0027] 下面参照附图给出的详细描述旨在解释本发明的示例性实施例,而不仅是示出可以根据本发明实施的实施例。

[0028] 本公开涉及一种使用软件定义网络 (SDN) 技术来检测和应对对基于以太网的车载网络 (IVN) 的攻击的入侵应对方法和入侵应对系统。

[0029] SDN是一种技术,其将诸如交换机和路由器的网络设备的控制部分与网络设备的数据传送部分分离,向外部提供可以定义网络设备的功能的开放接口,并通过开放接口利用编程的软件设置、控制和管理各种网络路径。

[0030] 图2是示出典型的SDN的架构的概念图。SDN架构被定义为三层,包括应用层、控制层和基础结构层 (infrastructure layer)。应用层、控制层和基础结构层也分别称为应用平面、控制平面和基础结构平面 (或数据平面)。各层通过开放接口 (open interface) 相互通信。被称为“北向API (northbound API)”的应用层和控制层之间的开放接口是能够开发具有各种功能的应用并与其他运行工具通信的API,北向API中一般使用Restful API。被称为“南向API (southbound API)”的控制层和基础结构层之间的开放接口是用于转发控制、信息收集等的接口,并且可以包括例如OpenFlow、OF-config、Netconf等。

[0031] 图3示出包括SDN控制器和SDN设备的SDN系统,以及包括在搭载在SDN设备中的流表中的流条目的字段。SDN控制器是逻辑实体 (entity),设置在SDN系统的控制平面上,并且SDN设备是硬件设备,设置在数据平面上。搭载在SDN设备中的流表包括以下三个主要字段以处理SDN设备接收到的数据包。主要字段包括定义流的包头信息 (packet header information) (规则 (RULE) 字段)、指示如何处理数据包的动作 (ACTION) 字段以及表示每个流的统计数据的STATS字段。控制器可以使用包括注册新流或删除流的功能的南向API在交换机中创建流表。

[0032] 图4是示意性地示出根据本公开的实施例的入侵应对系统 (IRS) 的结构的概念图。

[0033] 如上所述,本公开的入侵应对系统400利用SDN技术。由于SDN是一种虚拟化架构,因此不需要在物理上将其部件设置在相同的位置。根据本公开的入侵应对系统400,将具有SDN支持交换机 (简称为SDN交换机 (SDN Switch)) 410的车载网络 (IVN) 设置在SDN系统的数据平面上,将SDN控制器420设置在SDN系统的控制平面上,并且将入侵检测系统 (IDS) 430设置在SDN系统的应用平面上。

[0034] 入侵应对系统400从IVN中分离出逻辑或物理实体,该逻辑或物理实体通过分析发生流量的车辆和流量的统计数据来判断是否存在入侵,并根据判断结果确定应对。IDS430的操作主体可以不同于SDN控制器420的操作主体。

[0035] 设置在IVN中的SDN支持交换机410基于流表来控制发生在IVN中的流量或流入IVN的流量。设置在车辆外部通过V2I通信与车辆连接的SDN控制器420以一定的时间间隔周期性地从SDN支持交换机410接收流表,并从IDS接收作为对接收到的流表的监控结果的执行入侵检测的结果以使SDN支持交换机410更新流表。

[0036] 在下文中,将详细描述所提出的入侵应对系统400中的SDN支持交换机410、SDN控制器420和IDS430的功能和操作。

[0037] SDN支持交换机410搭载在车辆中并且控制流入车辆的IVN或V2X通信的所有流量或数据包(下文统称为“数据包”)的流。SDN支持交换机410可以是SDN交换机或与SDN设备组合以在SDN环境中操作的普通交换机,然而其不限于此。例如,根据本实施例的SDN支持交换机410可以是任何交换机,只要该交换机能够控制在车辆的IVN中或在V2X环境中生成的数据包的流并且能够与控制平面的SDN控制器420进行通信即可。

[0038] SDN支持交换机410使用流表控制流入SDN支持交换机410的数据包。根据本实施例的一个方面,SDN支持交换机410将诸如端口信息的数据包相关数据与流表中的每个流条目的规则字段进行匹配,并提取或引用与特定数据包匹配的流条目。这种匹配根据与SDN支持交换机410和SDN控制器420之间的通信协议相对应的南向API的规范(specification)而变化。例如,如图4所示,流条目的规则字段可以包括交换机端口(Switch port)、MAC源(Mac src)、以太网类型(Eth type)、VLAN ID、IP源(IP src)等。在这种情况下,可以通过相对于规则字段的规范的全部匹配、在预设范围内匹配或者预设数量以上的匹配来建立数据包数据和流条目之间的匹配。在这种情况下,可能有多条流条目与特定数据包匹配。

[0039] 当存在与流入的数据包匹配的流条目时,SDN支持交换机410提取流条目并执行流条目的动作字段的命令。根据本实施例的一个方面,当存在与流入的数据包匹配的多个流条目时,SDN支持交换机410可以利用包括在每个流条目中的优先级字段(priority field)在多个流条目中提取具有最高优先级的流条目。

[0040] 将流入SDN支持交换机410的所有数据包传送到SDN控制器420可能导致隐私侵犯和资源浪费。因此,根据本实施例的一个方面,当不能仅使用流表进行数据包控制时,例如不存在与流入的数据包匹配的流条目的情况以及匹配的流条目的有效期已到期(expire)的情况下,可以将包括流入的数据包的数据包输入消息传送到SDN控制器420。按照SDN支持交换机410和SDN控制器420所应用的接口生成数据包输入消息。SDN控制器420可以将包括数据包输入消息中包括的数据包和转发动作的数据包输出消息传送到SDN支持交换机410。SDN支持交换机410通过基于接收到的数据包输出消息更新流表来恰当地控制引入的数据包。

[0041] 可选地,SDN支持交换机410可以采用使用SDN支持交换机410的基于流表控制所有数据包数据的功能的数据驱动入侵检测方法。在该数据驱动入侵检测方法中,SDN支持交换机410以一定的时间间隔“T”或响应以一定的时间间隔“T”从SDN控制器420接收到的用于请求流表的查询而将流表传送到SDN控制器420,以便执行入侵检测,并且SDN支持交换机410从SDN控制器420接收入侵检测的结果并基于该入侵检测的结果更新流表。在该数据驱动入侵检测方法中,数据包控制和入侵检测分开进行。

[0042] 这里,SDN控制器420接收流表的时间间隔“T”可以基于车辆的内部或外部环境、驾驶环境、IDS430所采用的入侵检测方法和执行入侵检测的结果中的全部或部分来设置或重置。时间间隔“T”的设置或重置可以由SDN支持交换机410基于从SDN控制器420接收的数据包输出消息来确定,可以由SDN控制器420基于对接收到的数据包输入消息或数据包流的监控来确定,或者可以由IDS430确定。

[0043] 数据包输出消息可以包括入侵检测的结果。例如,当判断存在入侵时,数据包输出消息可以包括能够过滤掉入侵数据包或攻击的规则以及相应的应对(例如,数据包丢弃动作、数据包丢弃和源阻断动作、数据包丢弃和转发到控制器动作、时间间隔“T”的减少等)。

SDN支持交换机410可以基于数据包输出消息,通过将新的流条目添加到流表、更新现有流表或改变时间间隔“T”来响应入侵检测。确定这些规则和相应动作的主体可以是已经从SDN控制器420接收到请求的外部设备(例如,IDS430等)或SDN控制器420本身。稍后将参照图9A和图9B详细描述数据驱动入侵检测方法。

[0044] 流条目不仅包括上述的规则字段和动作字段,而且可以进一步包括统计字段(图4的STATS字段)。统计字段是收集或计算有关数据包的统计数据并存储的字段,并且可以包括计数器字段(counter field)。计数器字段记录流条目的规则字段与流入的数据包匹配的数量,在某些情况下,该数量可以累积增加或以预设周期初始化。计数器字段可以包括匹配计数器(match counter),该匹配计数器被设置为在预定参考值内计数与流入的数据包匹配的数量,或者计数器字段还可以包括字节计数器(bytes counter),该字节计数器被设置为计数匹配数据包的每秒字节数。

[0045] SDN支持交换机410可以仅在接收到来自SDN控制器420的消息时更新流表。在与SDN控制器420的通信(例如,基于南向API的通信)被断开时或直到在冷启动(例如,发动机启动)时恢复与SDN控制器420的连接,SDN支持交换机410在故障安全模式(fail-safe mode)下操作。SDN支持交换机410可以在故障安全模式下基于由车辆制造商设置为默认的流表来控制数据包流。在这种情况下,SDN支持交换机410作为普通交换机(common switch)来操作。

[0046] SDN控制器420从SDN支持交换机410接收数据包输入消息或流表。如上所述,当SDN控制器420接收到数据包输入消息时,SDN控制器420生成包括相应数据包和转发动作的数据包输出消息,并将该数据包输出消息传送到SDN支持交换机410。当SDN控制器420接收到流表时,SDN控制器420将流表传送到IDS430。然后,IDS430执行入侵检测,并且SDN控制器接收执行入侵检测的结果(例如,动作)。SDN控制器420将包括执行入侵检测的结果的数据包输出消息传送到SDN支持交换机410。

[0047] SDN控制器420可以是用于SDN的专用控制器或者是与SDN设备结合以在SDN环境中操作的通用控制器,然而其不限于此。例如,根据本实施例的SDN控制器420可以包括任何控制器,只要该控制器能够管理在IVN或V2X环境中生成的数据包并且能够与SDN支持交换机410或搭载有SDN支持交换机410的车辆进行通信即可。

[0048] SDN控制器420可以根据从IDS430接收到的执行入侵检测的结果生成能够过滤掉相应入侵的新规则(例如,时间间隔“T”的改变、流条目的规则字段的设置等),并且可以将新规则包括在数据包输出消息中。这样的新规则可以通过从IDS430或外部设备接收来生成。

[0049] 根据本实施例的另一方面,SDN控制器420可以使用搭载在一个或多个车辆中的一个或多个SDN支持交换机410来执行诸如OpenFlow的基于南向API的连接的维护、流表管理或数据包统计收集。SDN控制器420还可以使用一个或多个IDS(例如图4中的430)来执行诸如ad-hoc API、RESTful API或其他编程接口的基于北向API的连接的维护。

[0050] IDS430与SDN控制器420进行通信,从SDN控制器420接收流表,执行入侵检测,确定与执行入侵检测的结果相对应的动作,并将确定的动作传送到SDN控制器420。例如,根据本实施例的一个方面,IDS430监控流表中的每个流条目的每个字段,并且当计数器增量异常时或当未授权的源节点向要求授权的处理器发送数据包时,IDS430可以将该情况确定为攻

击,指定过滤掉相应流的规则,或者可以指定特定流条目的动作字段为数据包丢弃命令。根据本实施例的另一方面,IDS430可以将数据包丢弃命令和转发到控制器命令确定为动作。该动作使SDN支持交换机410丢弃IVN中的该数据包类型并将该数据包类型转发到SDN控制器420,使得SDN控制器420能够监控该数据包类型。对于这样的监控,SDN控制器420可以从另一设备或SDN支持交换机410接收流统计数据。

[0051] 在下文中,分别参照图5A、图5B、图6A、图6B、图7A和图7B、描述所提出的入侵应对系统的数据平面、控制平面和应用平面的示例性拓扑结构。

[0052] 图5A和图5B是示出根据本公开的实施例的IVN的示例性拓扑结构的示意图。

[0053] 图5A示出具有混合结构的IVN的示例性拓扑结构。示出的IVN包括各种以太网设备、信息娱乐(infortainment)设备、一个或多个电子控制单元(ECU)、以及包括连接到这些设备的SDN交换机的基于以太网的LAN。通常,诸如高级驾驶辅助系统(ADAS)和多媒体的高速数据应用可以通过基于以太网的LAN连接到SDN交换机。此外,示出的IVN包括用于诸如要求消息优先级的动力传动系统的不适合使用以太网的某些应用的传统CAN总线(legacy CAN bus)。传统CAN总线可以通过支持以太网和CAN总线之间的通信的ETH-CAN网关(ETH-CAN gateway)连接到SDN支持交换机。SDN交换机可以通过V2I通信调制解调器与包括位于远程的SDN控制器420的其他设备、服务器、系统等进行通信。

[0054] 图5B示出基于以太网的IVN的示例性拓扑结构。示出的IVN包括3个交换机(即交换机1、交换机2和基础交换机3)以及九个ECU。应注意的是,交换机的数量或ECU设备的数量可以根据配置拓扑结构的方法而变化。为了保证ECU生成的所有数据包都通过交换机传送到最终目的地节点,每个ECU必须单独连接到交换机,并且多个ECU不占用一条总线路径。

[0055] 交换机1和交换机2是具有激活的SDN功能的SDN支持交换机。这两个交换机通过负责车辆与外部基础设施之间的通信(即V2I通信)的无线调制解调器(wireless modem)连接到SDN控制器。当与SDN控制器建立连接时,交换机1和交换机2根据从SDN控制器接收到的动作处理ECU1至ECU6的数据包,并且不能自行确定每个数据包的动作。然而,当与SDN控制器的连接由于无线调制解调器故障而被断开时,交换机1和交换机2像稍后将描述的基础交换机3一样工作。因此,基于根据本实施例的入侵应对系统400的车辆即使在紧急情况下也可以保持正常操作(例如,故障安全操作),并且允许选择性地应用入侵应对系统400的每个功能。

[0056] 根据从SDN控制器接收到的命令或动作,交换机1和交换机2可以阻止被认为是攻击的数据包,而不将该数据包转发到其他ECU,此外,交换机1或交换机2可以将该数据包传送到SDN控制器进行后期分析。由外部入侵检测系统来执行判断数据包是否对应于攻击者的入侵。

[0057] 基础交换机3不是根据本实施例的SDN支持交换机,而是已被现有车辆应用的执行MAC地址学习(MAC address learning)的传统交换机。当基础交换机3知道由ECU7至ECU9传送的数据包的目的地时,基础交换机3将数据包转发到特定端口,并且当基础交换机3不知道目的地时,基础交换机3将数据包广播(broadcast)到所有端口。基础交换机3不支持用于入侵检测/应对的数据包信息收集功能,并且不从诸如SDN控制器的外部设备接收指定用于控制数据包流的动作。

[0058] 图6A和图6B是示出根据本公开的实施例的入侵应对系统的集中式结构和分布式

结构的控制平面拓扑结构的示意图。

[0059] 通常,设置在控制平面上的SDN控制器可以向多个车辆内的SDN交换机传送数据以及从多个车辆内的SDN交换机接收数据。图6A示出一种集中式结构,其中单个SDN控制器管理所有车辆数据包。本公开的IDS可以只用一个SDN控制器就可以实现预期的目的,但考虑到时延(latency)和负载均衡(load balancing),也可以安装并操作多个SDN控制器。图6B示出一种分布式结构,其中若干基地SDN控制器中的每一个都管理物理上或逻辑上靠近该SDN控制器的一个或多个车辆。例如,SDN控制器可以在每个基地的边缘云服务器(Edge cloud server)或雾服务器(fog server)中实现。每个基地的SDN控制器可以与物理上或逻辑上靠近SDN控制器的车辆进行主要通信,并将其结果传送给集中式SDN控制器。在集中式架构中,单个SDN控制器使用北向API执行与IDS430的通信,而在分布式架构中,集中式SDN控制器使用北向API执行与IDS430的通信。

[0060] 图7A和图7B是示出根据本公开的实施例的可应用于入侵应对系统的IDS的拓扑结构的示意图。

[0061] 最近提出的基于深度学习的IDS需要更多例如GPU的资源来获得精确的检测结果。搭载在车辆中的计算系统具有驾驶所需的最低性能,因此该计算系统不适合操作基于深度学习的IDS。设置在车辆外部的IDS在计算入侵检测算法时不再需要考虑车载性能问题。因此,所提出的入侵应对系统可以采用操作诸如图7A中所示的深度学习算法的需要高计算能力的精确入侵检测算法的IDS。

[0062] 在所提出的入侵应对系统中,可以同时操作多个IDS。每个IDS负责针对特定协议的入侵检测(例如,针对SSH的IDS1、针对AVTP的IDS2、针对UDP的IDS3),可选地,如图7B所示,可以使用利用操作不同的检测算法的若干IDS的检测结果的集成(Ensemble)方法。

[0063] 将IDS设置在车辆外部而不是设置在IVN内部在入侵应对系统的操作中提供了很大的灵活性。无论被分析车辆的位置或状态如何,IDS都可以被实时更新。例如,即使待分析的车辆正在行驶,IDS也可以动态地添加、重新配置或删除入侵检测模型或算法。此外,如果在单个车辆中引入新功能或发现针对单个车辆的新攻击模式,操作员(或服务提供商)可以使用相关的数据更新检测模型。

[0064] 图8是示出支持根据本公开的入侵应对系统的有用性的用例场景的示意图。

[0065] (1) 每当检测到攻击时,所有车辆通过云服务器或雾服务器上的SDN控制器将检测到的攻击信息传送到IDS。在这种情况下,路侧单元(RSU)可以中继相邻车辆和每个服务器之间的通信。RSU的通信方法可以基于近场通信(NFC)、低功率蓝牙(BLE)、无线局域网(WIFI)、超宽带(UWB)、射频、红外数据通讯(IrDA)、Zigbee、LTE,或5G来实现。

[0066] (2) 当作为应用本公开的入侵应对系统或方法的车辆之一的某个车辆受到攻击时,搭载在该车辆(a)中的IDS将攻击流量信息或疑似攻击的数据包传送到云服务器或雾服务器。

[0067] (3) 云服务器或雾服务器上的SDN控制器将攻击流量信息或数据包传送到IDS,并且IDS对数据进行分析。如果判断为存在攻击,则IDS通过SDN控制器将绕行该车辆(a)的警告命令传送到附近的每个车辆。

[0068] (4) 当车辆对车辆(V2V)通信被激活时,该车辆(a)可以与相邻车辆共享其状态。

[0069] (5) 当允许外部设备进行远程控制时,外部设备可以根据云服务器或雾服务器的

请求控制该车辆(a)减速和牵引行驶。

[0070] 图9A和图9B是示出根据本实施例的数据驱动入侵检测和应对方法的流程图。

[0071] 图9A示出SDN支持交换机410和SDN控制器420执行数据驱动入侵检测的过程。

[0072] 当应用根据本实施例的入侵应对系统400的车辆(例如,CAV)开始行驶时,数据包从IVN或V2X环境流入SDN支持交换机410(S900)。

[0073] SDN支持交换机410判断是否在搭载的流表中存在具有与流入的数据包匹配的规则字段的流条目(S902)。

[0074] 当存在匹配的流条目时,SDN支持交换机410判断是否在匹配的流条目的动作字段命令中包括数据包丢弃命令(S904),当不存在数据包丢弃命令时,SDN支持交换机410执行动作字段的命令而不丢弃数据包(S906)。

[0075] 当存在数据包丢弃命令时,SDN支持交换机410丢弃相应数据包并阻止来自相应源的流量(S912)。

[0076] 当不存在与流入的数据包匹配的流条目时或当匹配的流条目到期而最终不存在匹配的流条目时,SDN支持交换机410将包括诸如端口编号的事件信息和包括相应数据包的数据包输入消息传送到设置在车辆外部的SDN控制器420(S910),丢弃相应数据包,并阻止相应流量(S912)。

[0077] SDN控制器420接收数据包输入消息(S920),指定转发动作(S922),生成包括该转发动作的数据包输出消息,并将该数据包输出消息传送到SDN支持交换机410(S992)。

[0078] SDN控制器420从IDS430接收请求流表的查询(S940),并将该查询传送到SDN支持交换机410。

[0079] SDN支持交换机410从SDN控制器420接收请求流表的查询并将流表传送到SDN控制器420(S950和S952)。

[0080] 在从SDN支持交换机410接收到流表时,SDN控制器420将流表传送到IDS430(S960)。

[0081] SDN控制器420从IDS430接收基于流表执行入侵检测的结果(S990),生成包括执行入侵检测的结果的数据包输出消息,并将该数据包输出消息传送到SDN支持交换机410(S992)。

[0082] SDN支持交换机410从SDN控制器420接收数据包输出消息(S996)并更新流表(S998)。这种更新可以包括添加新的流条目,更新到期流条目的到期信息或流条目的每个字段,或者如果没有要更新的新内容,则保持流表不变。

[0083] 图9B示出IDS430执行数据驱动入侵检测的过程。

[0084] IDS430等待用于请求流表的时间间隔(S930中的“T”)(S930),并向SDN控制器420查询(S932)。

[0085] 当从SDN控制器420接收到流表(S970)时,IDS430基于流表中的每个流条目的每个字段和流统计数据来执行入侵检测(S972)。

[0086] 当IDS430判断为存在入侵时(S974),IDS430确定丢弃与入侵相关联的数据包(S980)。该确定还可以通过将丢弃命令包括在和与入侵相关联的数据包匹配的流条目的动作字段中来执行。IDS430将包括丢弃动作的检测结果显示到SDN控制器420(S982)。

[0087] 然而,如果判断为不存在入侵,则IDS430不传送检测结果(S976)。

[0088] 尽管图9A和图9B中描述了顺序地执行每个过程,但这仅仅是说明本公开的实施例的技术思想。换言之,在不脱离本公开的实施例的本质特征的情况下,本公开的实施例所属领域的技术人员可以进行各种修改和变化以便应用,例如通过改变在图9A和图9B中描述的顺序来执行过程或者并行执行每个过程的一个或多个过程,并且因此,本公开不限于图9A和图9B的时序顺序。

[0089] 本文所述的系统和方法的各种实施方式可以通过数字电子电路、集成电路、现场可编程门阵列(FPGA)、专用集成电路(ASIC)、计算机硬件、固件、软件和/或其组合来实现。这些各种实施方式可以包括作为在可编程系统上可运行的一个或多个计算机程序的实施方式。可编程系统包括至少一个可编程处理器(其可以是专用处理器或通用处理器),其被联接以从存储系统、至少一个输入设备以及至少一个输出设备接收数据和指令,并向存储系统、至少一个输入设备以及至少一个输出设备传送数据和指令。计算机程序(也称为程序、软件、软件应用或代码)包括用于可编程处理器的指令并存储在“计算机可读介质”中。

[0090] 计算机可读记录介质包括由存储计算机系统可读的数据的所有类型的记录设备。计算机可读记录介质可以是诸如ROM、CD-ROM、磁带、软盘、存储卡、硬盘、磁光盘和存储设备的非易失性或非暂时性介质,并且可以进一步包括诸如数据传送介质的暂时性介质。此外,计算机可读记录介质可以分布在连接网络的计算机系统中,并且计算机可读代码可以以分布式方式存储和运行。

[0091] 本文描述的系统和技术各种实施方式可以由可编程计算机实现。这里,计算机包括可编程处理器、数据存储系统(包括易失性存储器、非易失性存储器或其他类型的存储系统,或其组合)以及至少一个通信接口。例如,可编程计算机可以是服务器、网络设备、机顶盒、嵌入式设备、计算机扩展模块、个人计算机、便携式计算机、个人数据助理(PDA)、云计算系统和移动设备中的一种。

[0092] 以上描述仅是描述本实施例的技术思想,本实施例所属领域的技术人员能够在不超出本实施例的基本特征的情况下进行各种修改和变化。因此,本实施例旨在描述而不是限制本实施例的技术思想,并且本实施例的技术思想的范围不受这些实施例的限制。本实施例的保护范围应由所附权利要求书来解释,在其等同范围内的技术思想均应理解为包含在本实施例的权利范围内。

[0093] 附图标记说明

[0094] 400:入侵应对系统

[0095] 410:SDN支持交换机

[0096] 420:SDN控制器

[0097] 430:入侵检测系统(IDS)

[0098] 相关申请的交叉引用

[0099] 本申请要求于2019年7月31日提交的申请号为10-2019-0093503的韩国专利申请以及于2020年7月30日提交的申请号为10-2020-0095519的韩国专利申请的优先权的权益,这些韩国专利申请的全部内容通过引用并入本文。

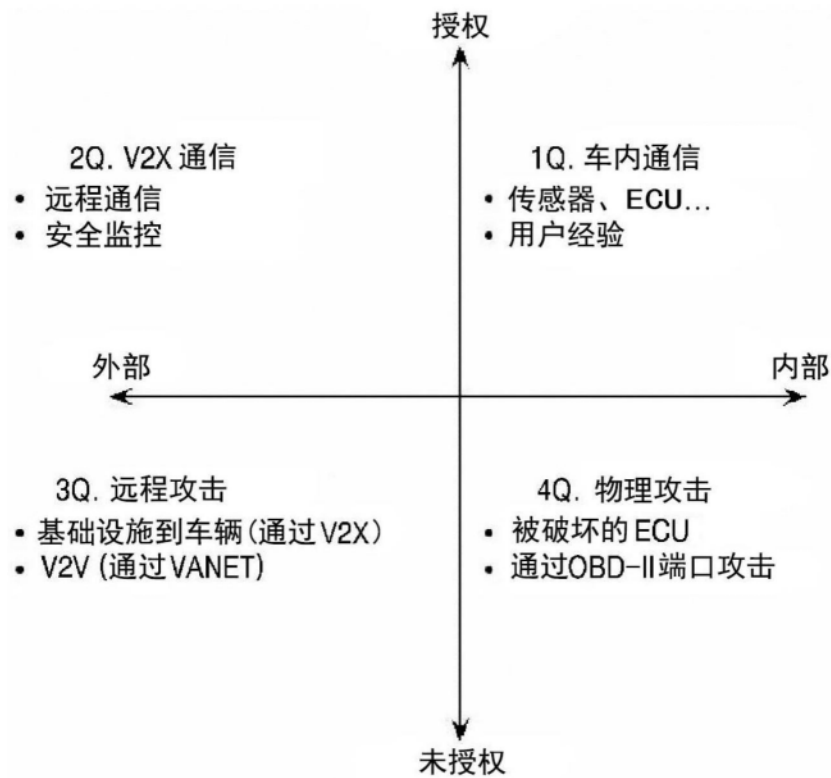


图1

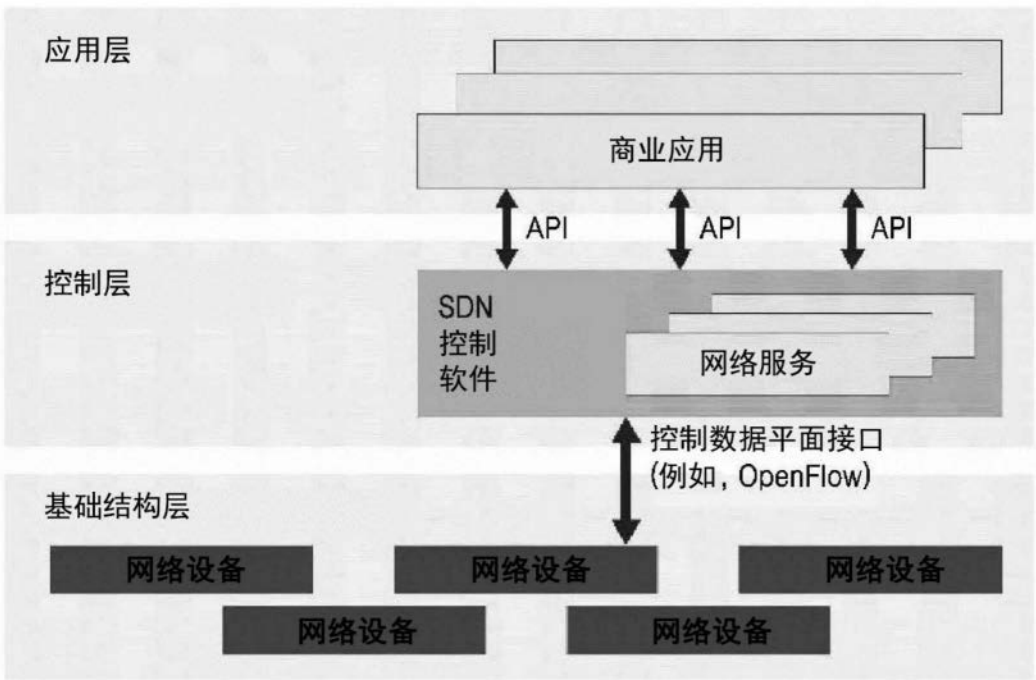


图2

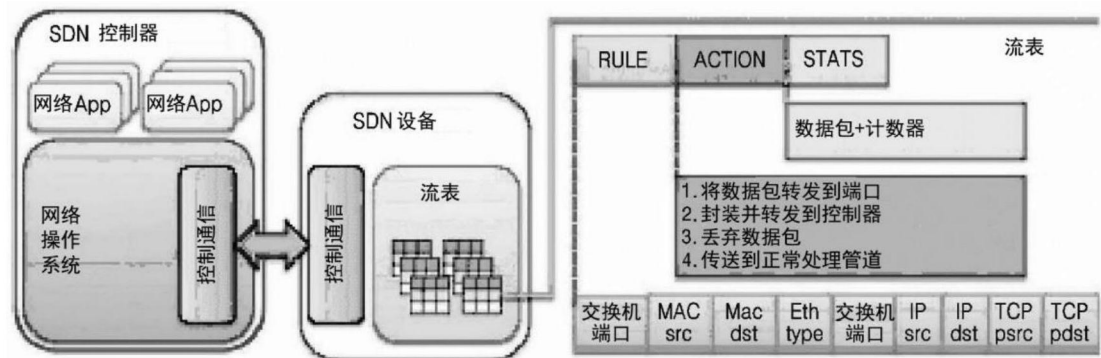


图3

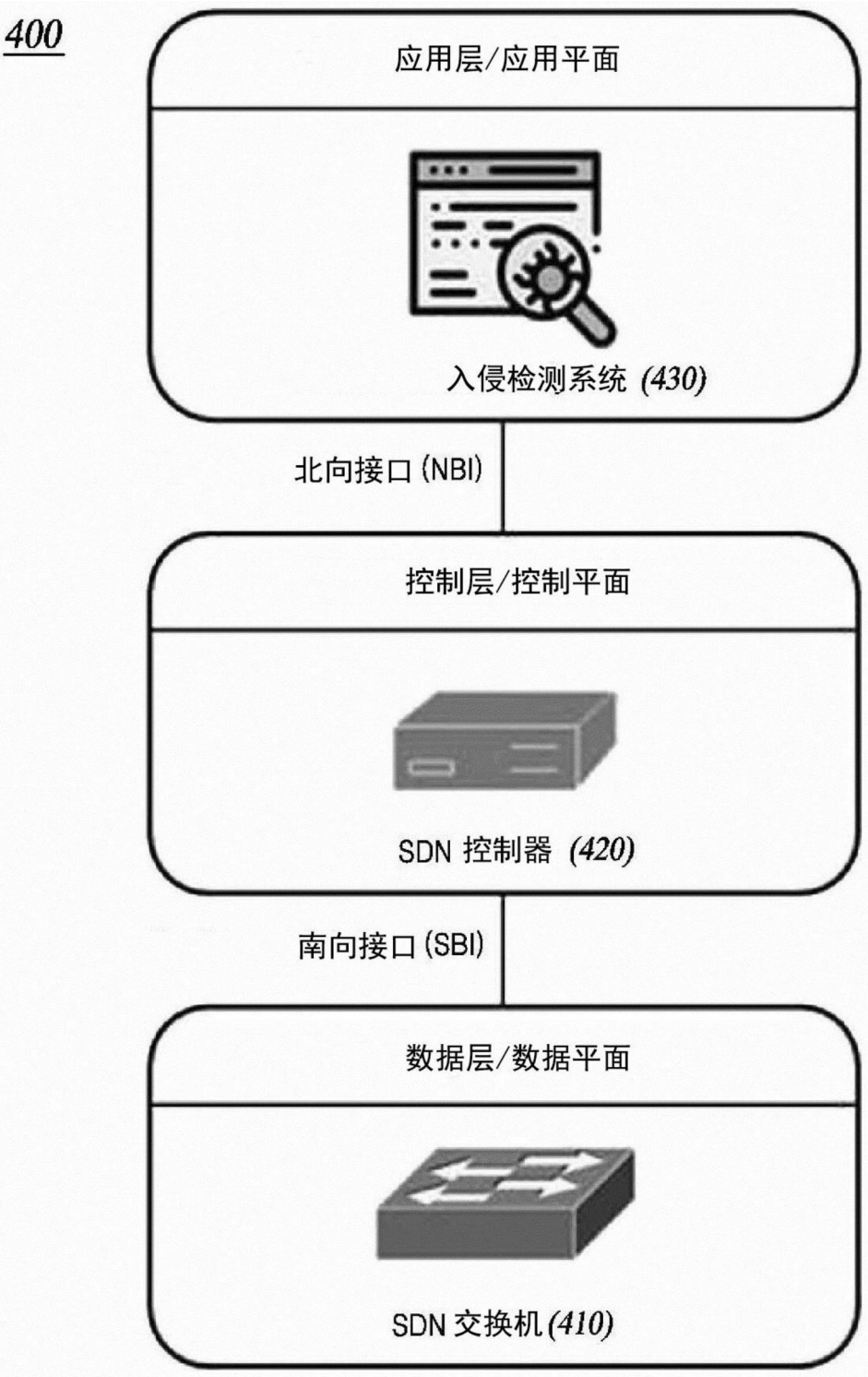


图4

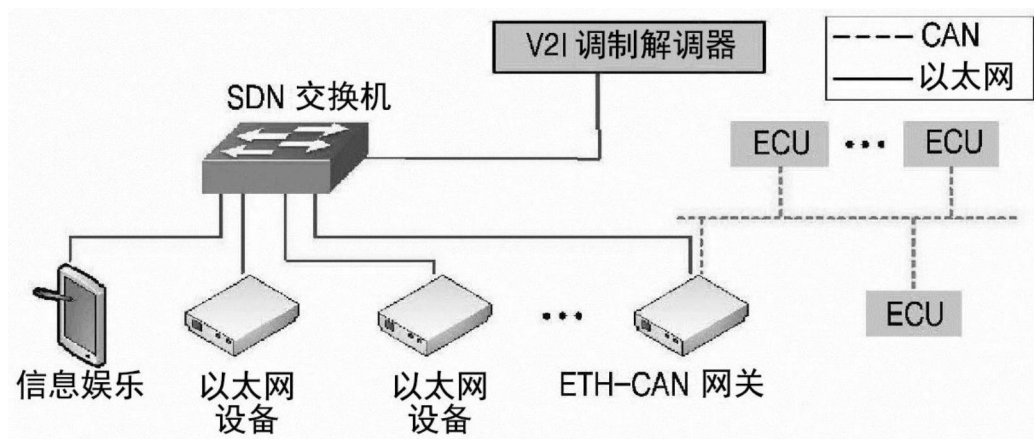


图5A

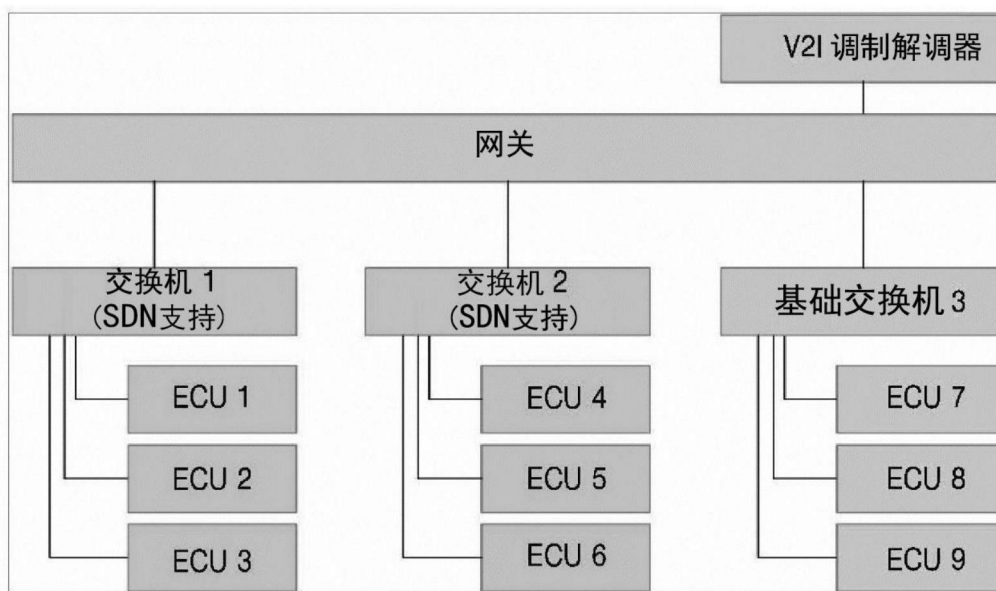


图5B

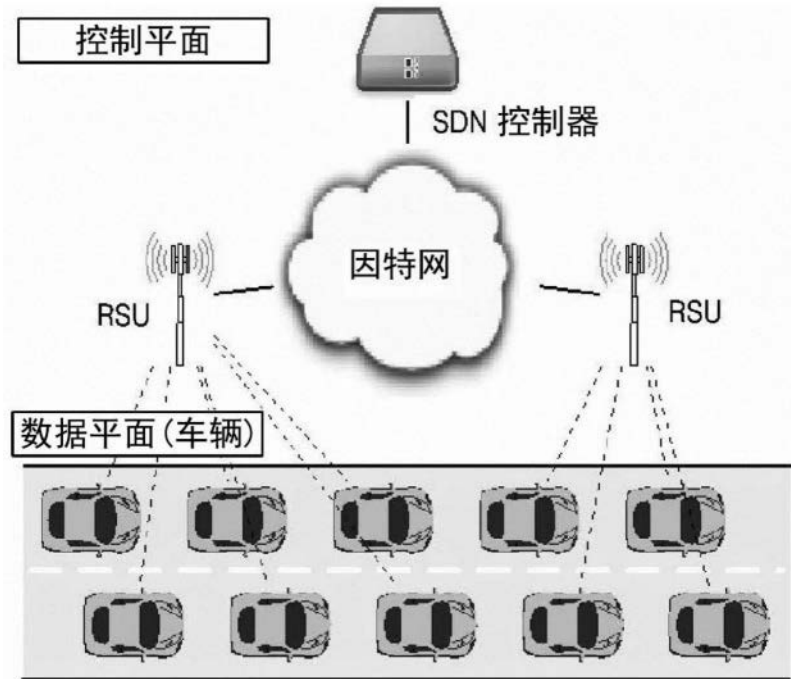


图6A

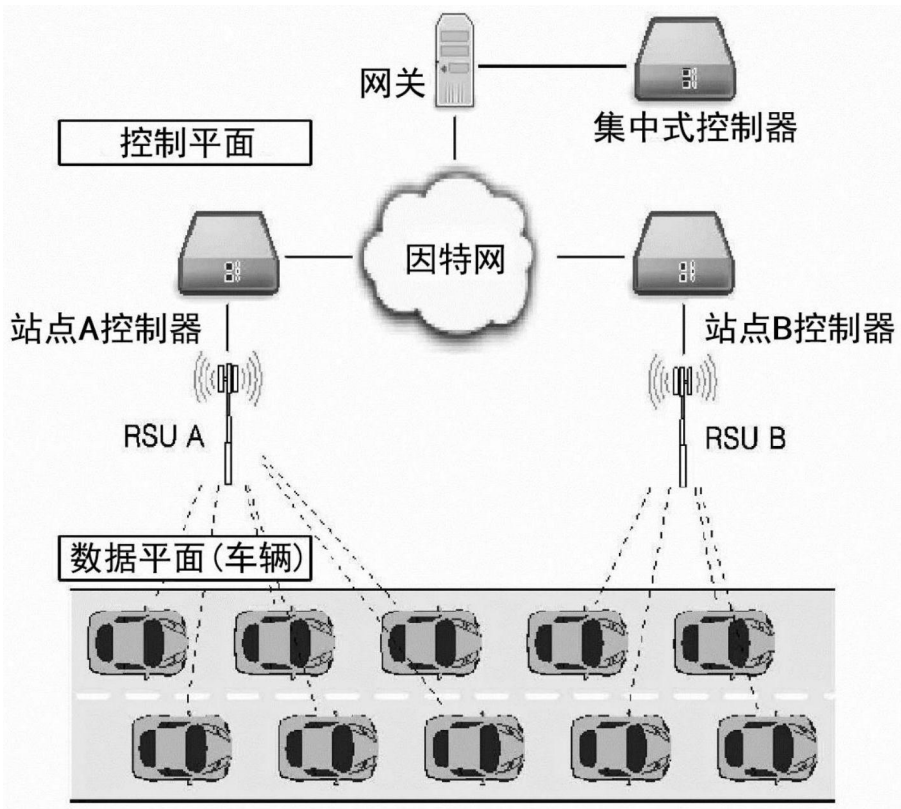


图6B

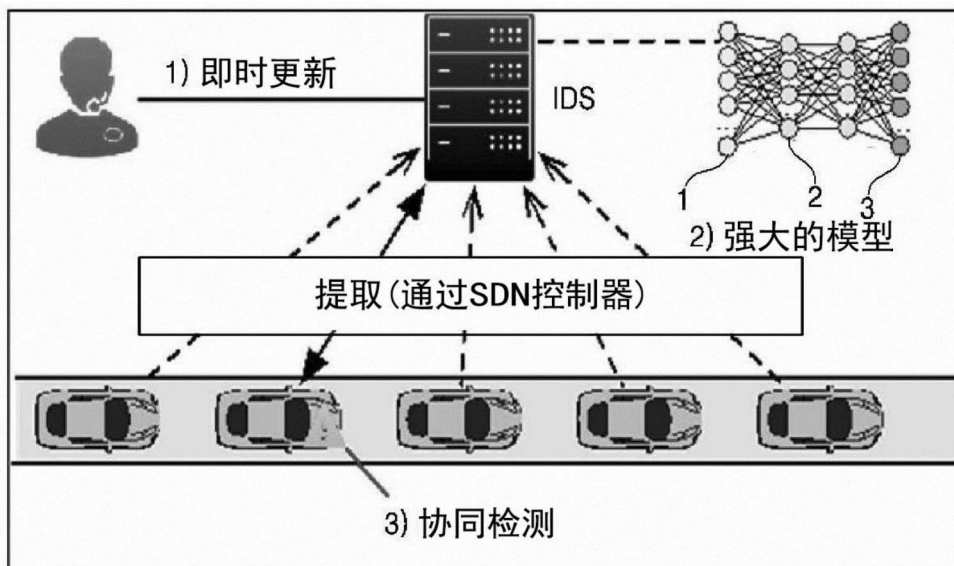


图7A

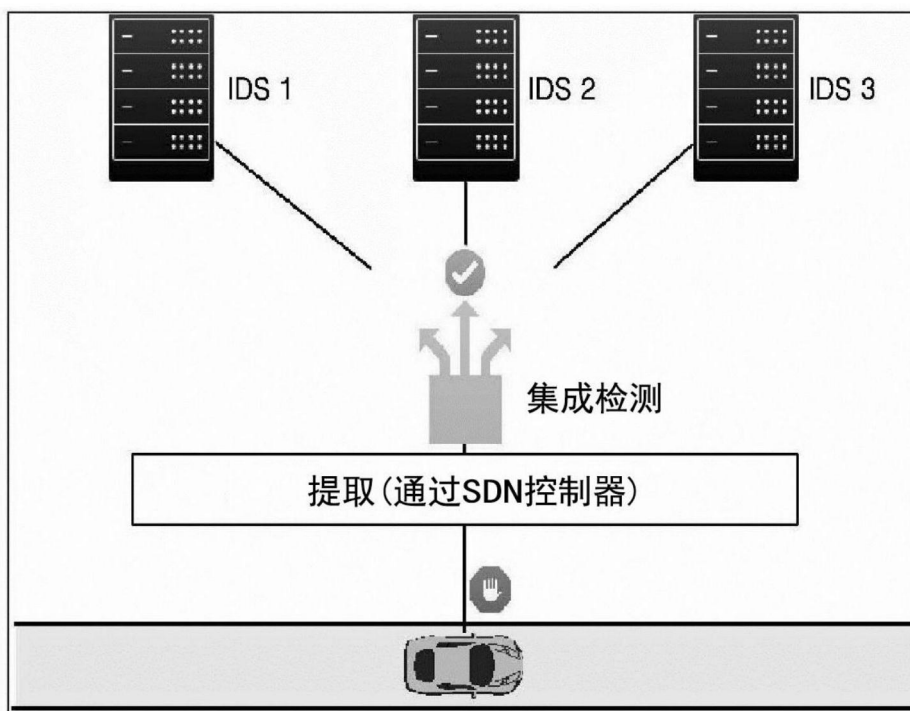


图7B

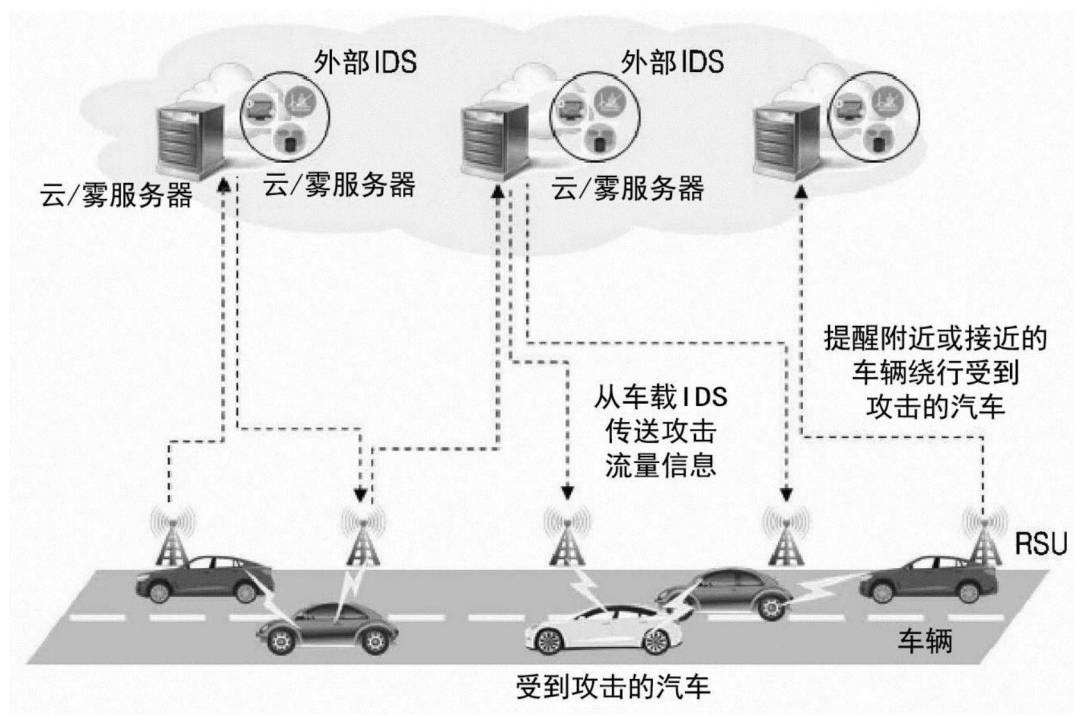


图8

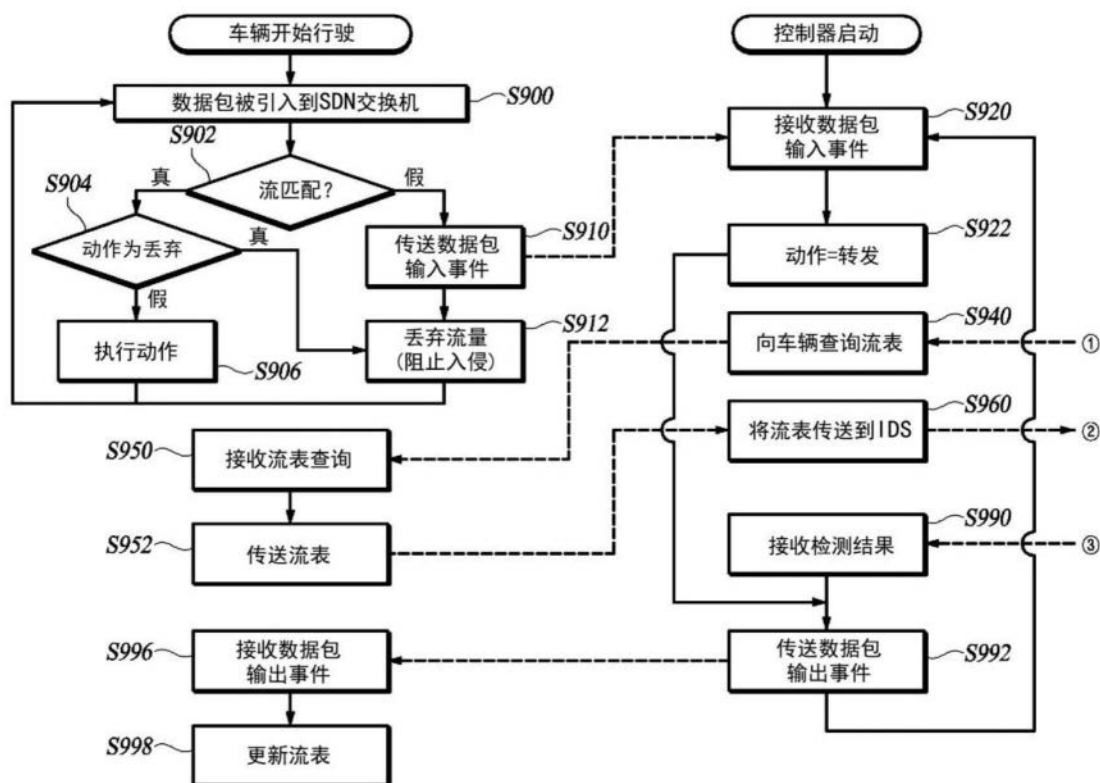


图9A

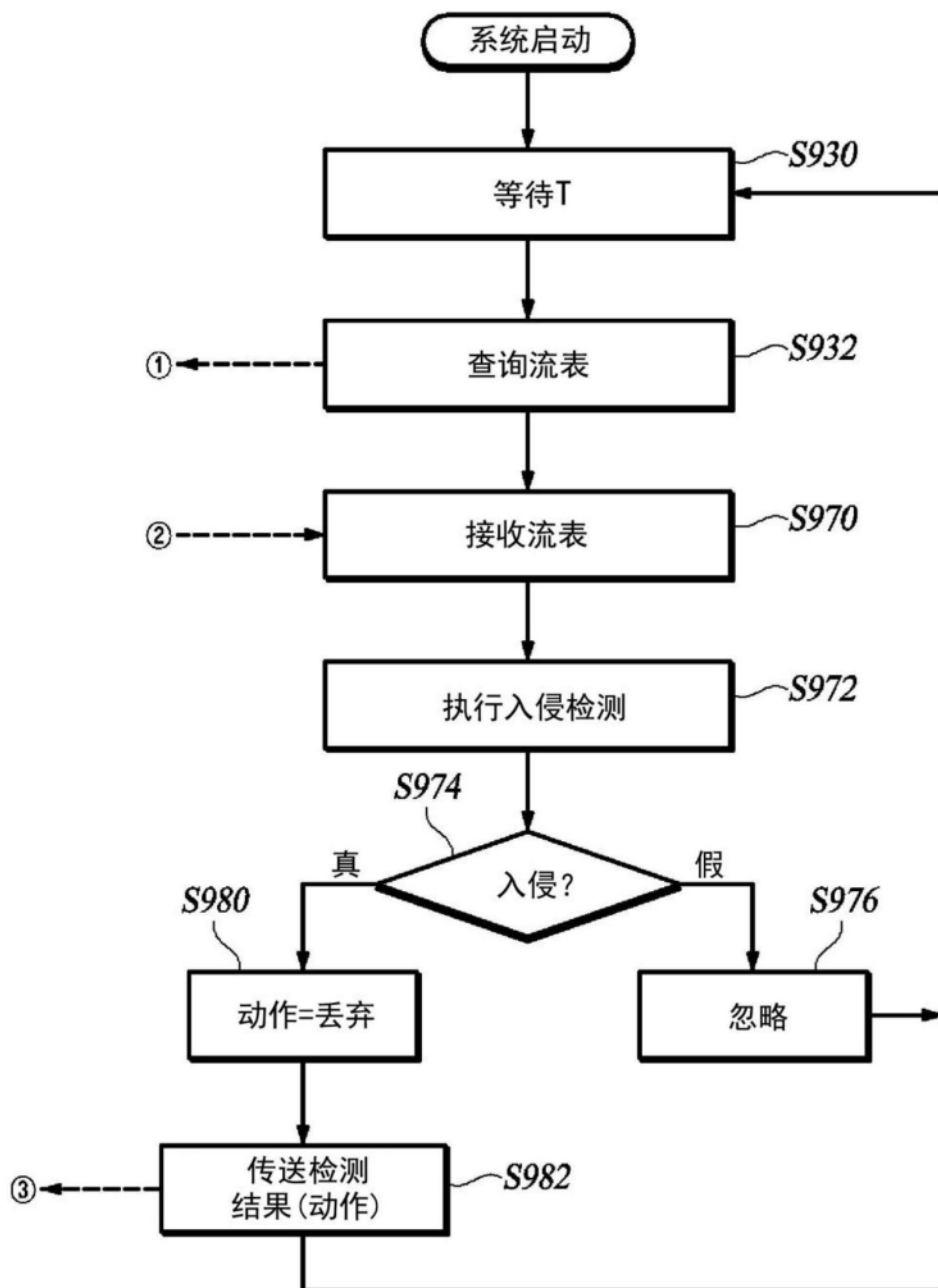


图9B