



(12)发明专利申请

(10)申请公布号 CN 110784431 A

(43)申请公布日 2020.02.11

(21)申请号 201810852175.3

(22)申请日 2018.07.30

(71)申请人 比亚迪股份有限公司

地址 518118 广东省深圳市坪山新区比亚迪路3009号

(72)发明人 磨俊生 曾文晓 赵龙 何蕾莉

(51)Int.Cl.

H04L 29/06(2006.01)

H04L 29/08(2006.01)

H04L 12/66(2006.01)

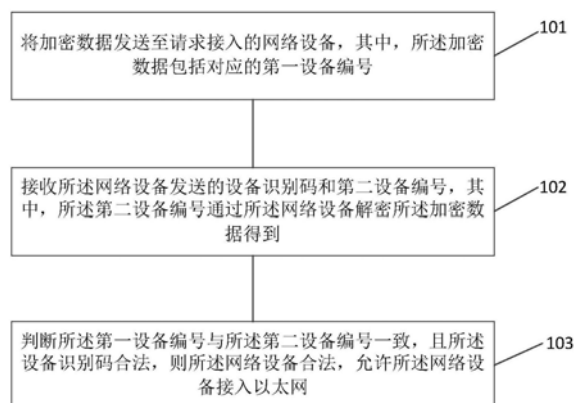
权利要求书4页 说明书18页 附图3页

(54)发明名称

车载以太网安全接入方法、系统、车载网关和网络设备

(57)摘要

本发明提出一种车载以太网安全接入方法、系统、车载网关和网络设备,其中方法包括:车载网关将包括第一设备编号的加密数据发送至网络设备;所述网络设备将设备识别码和解密得到的第二设备编号发送至所述车载网关;若所述第一设备编号与所述第二设备编号不一致,则所述网络设备不合法,不允许所述网络设备接入以太网;若所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网;若所述第一设备编号与所述第二设备编号一致,且所述设备识别码不合法,则所述网络设备不合法,不允许所述网络设备接入以太网,从而有效阻止了不合法网络设备的入侵。



1. 一种车载以太网安全接入方法,应用于车载网关,其特征在于,包括以下步骤:
将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号;
接收所述网络设备发送的设备识别码和第二设备编号,其中,所述第二设备编号由所述网络设备解密所述加密数据得到;
判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网。
2. 根据权利要求1所述的方法,其特征在于,还包括:
判断所述第一设备编号与所述第二设备编号不一致,则所述网络设备不合法,不允许所述网络设备接入以太网;
判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码不合法,则所述网络设备不合法,不允许所述网络设备接入以太网。
3. 根据权利要求1或2所述的方法,其特征在于,
所述车载网关存储有预先设定的关系对应表,所述关系对应表包括所有允许接入以太网的网络设备的设备识别码和第一设备编号,其中,关系对应信息包括:连接端口号、第一设备编号、设备识别码、MAC地址或IP 地址。
4. 根据权利要求3所述的方法,其特征在于,所述将加密数据发送至请求接入的网络设备之前,还包括:
所述车载网关通过预先设定的关系对应表,获取的一个未使用的第一设备编号,并对所述第一设备编号进行加密,得到所述加密数据。
5. 根据权利要求3所述的方法,其特征在于,
若所述设备识别码在所述车载网关预先设定的关系对应表中,且与所述设备识别码对应的网络设备未与所述车载网关连接,则所述设备识别码合法;
若所述设备识别码未在所述车载网关预先设定的关系对应表中,或者所述设备识别码在所述车载网关预先设定的关系对应表中,且与所述设备识别码对应的网络设备与所述车载网关连接,则所述网络设备不合法,不允许所述网络设备接入以太网。
6. 根据权利要求3所述的方法,其特征在于,所述允许所述网络设备接入以太网之后,还包括以下步骤:
所述车载网关向上一层级的车载网关发送所述网络设备上线的信息和所述网络设备的设备识别码和第一设备编号,直至最上层的车载网关获取所述网络设备上线的信息和所述网络设备的设备识别码和第一设备编号,
所有接收到所述网络设备上线的信息的车载网关建立相应的信息通道,所述网络设备通过所述信息通道发送或接收信息。
7. 根据权利要求3所述的方法,其特征在于,所述允许所述网络设备接入以太网之后,还包括以下步骤:
若所述网络设备下线,则所述车载网关依次向上一层级的车载网关发送所述网络设备下线的信息和所述网络设备的设备识别码和第一设备编号,直至最上层的车载网关获取所述网络设备下线的信息和所述网络设备的设备识别码和第一设备编号,
所有接收到所述网络设备下线的信息的车载网关关闭相应的信息通道。
8. 根据权利要求3所述的方法,其特征在于,若所述网络设备第一次接入以太网,则所

述将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号,具体包括:

获取所述网络设备的MAC地址或IP地址进行通信,

为所述网络设备随机分配一个未使用的第一设备编号,

根据所述网络设备的MAC地址或IP地址将加密数据发送至所述网络设备,所述加密数据包括所述未使用的第一设备编号。

9. 根据权利要求3所述的方法,其特征在于,若所述网络设备接入以太网后,下线再接入,所述将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号,具体包括以下步骤:

通过所述网络设备连接的端口对应的连接端口号,获取关系对应表中对应的MAC地址或IP地址,并通过该MAC地址或IP地址与网络设备进行通信,

若所述车载网关与所述网络设备可以正常通信,则所述车载网关通过所述MAC地址或IP地址将加密数据发送至所述网络设备,其中,所述加密数据包括关系对应表中对应的第一设备编号。

10. 根据权利要求3所述的方法,其特征在于,若所述网络设备接入以太网后,下线再接入,所述将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号,具体包括以下步骤:

通过所述网络设备连接的端口对应的连接端口号,获取关系对应表中对应的MAC地址或IP地址,并通过该MAC地址或IP地址与网络设备进行通信,

若所述车载网关与所述网络设备不可以正常通信,

则所述车载网关通过地址解析协议发送请求,所述网络设备根据收到的请求将所述网络设备的MAC地址或IP地址发送至车载网关,所述车载网关通过所述网络设备的MAC地址或IP地址进行与所述网络设备通信,所述车载网关随机为所述网络设备分配一个未使用的第一设备编号,所述车载网关通过所述网络设备的MAC地址或IP地址将加密数据发送至所述网络设备,其中,所述加密数据包括所述未使用的第一设备编号。

11. 根据权利要求3所述的方法,其特征在于,所述允许所述网络设备接入以太网之后,还包括:

将所述网络设备的信息存储到车载网关的关系对应表中。

12. 根据权利要求3所述的方法,其特征在于,若所述网络设备请求接入所述车载网关预留的端口,所述判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网,具体包括:

判断所述第一设备编号与所述第二设备编号一致,所述设备识别码未在所述车载网关预先设定的关系对应表中,则逐级向上层的车载网关发送请求信息,其中,所述请求信息包括所述设备识别码;

所述上层的车载网关接收到请求信息,若请求信息中的所述设备识别码在所述上层的车载网关预先设定的关系对应表中,且所述设备识别码对应的网络设备未与所述车载网关连接,则所述网络设备合法,允许所述网络设备接入以太网。

13. 根据权利要求12所述的方法,其特征在于,还包括:

若所述网络设备合法,则所述上层的车载网关逐级向下层的车载网关发送所述网络设

备合法的信息、所述网络设备的关系对应信息；

所述车载网关直至最上层的车载网关共同建立起相应的信息通道，以由所述网络设备通过所述信息通道发送或接收信息。

14. 根据权利要求3所述的方法，其特征在于，若所述网络设备请求接入所述车载网关预留的端口，所述判断所述第一设备编号与所述第二设备编号一致，且所述设备识别码不合法，则所述网络设备不合法，不允许所述网络设备接入以太网，具体包括：

判断所述第一设备编号与所述第二设备编号一致，所述设备识别码未在所述车载网关预先设定的关系对应表中，则逐级向上层的车载网关发送请求信息，其中，所述请求信息包括所述设备识别码；

所述上层的车载网关接收到请求信息，若请求信息中的所述设备识别码在所述上层的车载网关预先设定的关系对应表中，且所述设备识别码对应的网络设备与对应的车载网关连接，则所述网络设备不合法，不允许所述网络设备接入以太网；或者

所述上层的车载网关接收到请求信息，若请求信息中的所述设备识别码不在所述上层的车载网关预先设定的关系对应表中，则所述网络设备不合法，不允许所述网络设备接入以太网。

15. 根据权利要求1所述的方法，其特征在于，

同一种类型的所述网络设备的设备识别码相同，不同类型的所述网络设备的设备识别码不同。

16. 一种车载以太网安全接入方法，应用于网络设备，其特征在于，包括以下步骤：

接收车载网关发送的加密数据，并对所述加密数据进行解密得到第二设备编号，所述加密数据包括第一设备编号；

向车载网关发送第二设备编号和设备识别码，以由所述车载网关判断，当所述第一设备编号与所述第二设备编号一致，且所述设备识别码合法时，则请求接入的网络设备合法，允许所述网络设备接入以太网。

17. 一种车载以太网安全接入方法，其特征在于，包括以下步骤：

车载网关将加密数据发送至请求接入的网络设备，其中，所述加密数据包括第一设备编号；

所述网络设备接收所述加密数据，并对所述加密数据进行解密，所述网络设备将解密得到的第二设备编号和设备识别码发送至所述车载网关；

所述车载网关根据所述第二设备编号、所述设备识别码和所述第一设备编号，判断是否允许所述网络设备接入以太网，若判断所述第一设备编号与所述第二设备编号一致，且所述设备识别码合法，则所述网络设备合法，允许所述网络设备接入以太网。

18. 一种车载网关，其特征在于，包括：

第一发送模块，用于将加密数据发送至请求接入的网络设备，其中，所述加密数据包括第一设备编号；

第一接收模块，用于接收所述网络设备发送的设备识别码和第二设备编号，其中，所述第二设备编号由所述网络设备解密所述加密数据得到，

判断模块，用于判断所述第一设备编号与所述第二设备编号一致，且所述设备识别码合法，则所述网络设备合法，允许所述网络设备接入以太网。

19. 一种网络设备, 其特征在于, 包括:

第二接收模块, 用于接收车载网关发送的加密数据, 并对所述加密数据进行解密得到第二设备编号, 所述加密数据包括第一设备编号;

第二发送模块, 用于向车载网关发送第二设备编号和设备识别码, 以由所述车载网关判断, 当所述第一设备编号与所述第二设备编号一致, 且所述设备识别码合法时, 则请求接入的网络设备合法, 允许所述网络设备接入以太网。

20. 一种车载以太网安全接入系统, 其特征在于, 包括车载网关和网络设备,

所述车载网关将加密数据发送至请求接入的网络设备, 其中, 所述加密数据包括第一设备编号;

所述网络设备接收所述加密数据, 并对所述加密数据进行解密, 所述网络设备将解密得到的第二设备编号和设备识别码发送至所述车载网关;

所述车载网关根据所述第二设备编号、所述设备识别码和所述第一设备编号, 判断是否允许所述网络设备接入以太网, 若判断所述第一设备编号与所述第二设备编号一致, 且所述设备识别码合法, 则所述网络设备合法, 允许所述网络设备接入以太网。

车载以太网安全接入方法、系统、车载网关和网络设备

技术领域

[0001] 本发明涉车载通信技术领域,尤其涉及一种车载以太网安全接入方法、系统、车载网关和网络设备。

背景技术

[0002] 随着车载通信领域的发展需求,许多车载通信网络都引入了以太网技术,以太网可提供高速的网络带宽,提高了人们工作效率,丰富了人们日常生活,极大地满足大数据分析及应用的发展需求。另外,以太网在当今最热门的无人驾驶技术应用当中也是起了不小的作用。由于以太网如此普及,其所引申出来的网络安全问题让人重视,例如,一些不法人员利用网络黑客技术劫持并控制车辆,不仅仅获取车辆上的信息,还可以控制车辆行驶,严重影响乘客的人身财产安全。

[0003] 现有技术对于以太网网络安全分三方面做防范,一方面,对于一些带有恶意网络攻击性质的病毒、木马采用加装专门的防火墙;另一方面,对于一些关键性的网络,所有网络设备在接入网络时,需要通过预先申请安全证书,由预定的以太网主机进行认证其安全证书,以决定是否让设备接入网络;再一方面,对于一些关键性的通信数据,在数据传输时通过加密方式打包。

[0004] 防火墙只能防范一些已知的带有恶意网络攻击性质的病毒、木马,由于在工业上各类网络设备MAC地址(物理地址,Media Access Control)与IP地址(互联网协议地址,Internet Protocol Address)的公开性与可变性,非法入侵者可以先截获当前网络中任一合法设备的MAC地址与IP地址,然后再进行伪造对应地址信息就可以成功进入网络,截获并破坏网络通信。

[0005] 安全证书是目前已知安全性最高的网络安全防范措施,但由于安全证书申请及校验过程较为繁杂,应用在车辆等车载通信领域上,将带来很多不便。由于车辆等车载设备运行环境的不确定性,车辆上设备不可避免会产生耗损的情况,例如车辆网络上某一设备损坏,需要替换时,新替换的设备还需申请与当前以太网主机配套使用的安全证书才能接入网络使用,如果是以太网主机损坏,则整个网络的设备都需要重新申请与主机配套使用的安全证书,才能正常通信。此过程过于麻烦,因此使用安全证书对于车载通信领域长时间持续通信的网络环境具有一定的局限性。

[0006] 通信数据加密传输也是一种必备的安全防范措施,不管是何种网络,对于关键性数据保护,都必须采用加密传输。但是,数据加密解密的过程会损耗一定的时间,这种时间损耗会导致操作执行上有延迟,如果控制部件发送的控制指令不能及时传达到车辆的执行部件处,或者车辆的执行部件接收到指令不能及时执行动作,那么会产生一定不可预估的后果。例如,一辆无人驾驶的车辆,若是刹车信号不能及时传达到执行刹车部件,势必会威胁到车辆上人员的人身安全,因此加密传输在车载通信网络上使用,只能应用在一些关键性的数据,对于实时传输的控制类信息,不能适用。

发明内容

[0007] 本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

[0008] 为此,本发明的第一个目的在于提出一种车载以太网安全接入方法。

[0009] 本发明的第二个目的在于提出另一种车载以太网安全接入方法。

[0010] 本发明的第三个目的在于提出又一种车载以太网安全接入方法。

[0011] 本发明的第四个目的在于提出一种车载网关。

[0012] 本发明的第五个目的在于提出一种网络设备。

[0013] 本发明的第六个目的在于提出一种车载以太网安全接入系统。

[0014] 为达上述目的,本发明第一方面实施例提出了一种车载以太网安全接入方法,应用于车载网关,包括以下步骤:

[0015] 将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号;

[0016] 接收所述网络设备发送的设备识别码和第二设备编号,其中,所述第二设备编号由所述网络设备解密所述加密数据得到;

[0017] 判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网。

[0018] 本发明实施例的车载以太网安全接入方法,判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0019] 为达上述目的,本发明第二方面实施例提出了另一种车载以太网安全接入方法,应用于网络设备,包括以下步骤:

[0020] 接收车载网关发送的加密数据,并对所述加密数据进行解密得到第二设备编号,所述加密数据包括第一设备编号;

[0021] 向车载网关发送第二设备编号和设备识别码,以由所述车载网关判断,当所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法时,则请求接入的网络设备合法,允许所述网络设备接入以太网。

[0022] 本发明实施例的车载以太网安全接入方法,向车载网关发送第二设备编号和设备识别码,以由所述车载网关判断,当所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法时,则请求接入的网络设备合法,允许所述网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0023] 为达上述目的,本发明第三方面实施例提出了又一种车载以太网安全接入方法,包括以下步骤:

[0024] 车载网关将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号;

[0025] 所述网络设备接收所述加密数据,并对所述加密数据进行解密,所述网络设备将解密得到的第二设备编号和设备识别码发送至所述车载网关;

[0026] 所述车载网关根据所述第二设备编号、所述设备识别码和所述第一设备编号,判断是否允许所述网络设备接入以太网,若判断所述第一设备编号与所述第二设备编号一

致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网。

[0027] 本发明实施例的车载以太网安全接入方法,车载网关判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0028] 为达上述目的,本发明第四方面实施例提出了一种车载网关,包括:

[0029] 第一发送模块,用于将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号;

[0030] 第一接收模块,用于接收所述网络设备发送的设备识别码和第二设备编号,其中,所述第二设备编号通过所述网络设备解密所述加密数据得到,

[0031] 判断模块,用于判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网。

[0032] 本发明实施例的车载网关,车载网关判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0033] 为达上述目的,本发明第五方面实施例提出了一种网络设备,包括:

[0034] 第二接收模块,用于接收车载网关发送的加密数据,并对所述加密数据进行解密得到第二设备编号,所述加密数据包括第一设备编号;

[0035] 第二发送模块,用于向车载网关发送第二设备编号和设备识别码,以由所述车载网关判断,当所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法时,则请求接入的网络设备合法,允许所述网络设备接入以太网。

[0036] 本发明实施例的网络设备,所述网络设备将解密得到的第二设备编号和设备识别码发送至所述车载网关;所述车载网关判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0037] 为达上述目的,本发明第六方面实施例提出了一种车载以太网安全接入系统,包括:

[0038] 所述车载网关将加密数据发送至请求接入的网络设备,其中,所述加密数据包括第一设备编号;

[0039] 所述网络设备接收所述加密数据,并对所述加密数据进行解密,所述网络设备将解密得到的第二设备编号和设备识别码发送至所述车载网关;

[0040] 所述车载网关根据所述第二设备编号、所述设备识别码和所述第一设备编号,判断是否允许所述网络设备接入以太网,若判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合法,允许所述网络设备接入以太网。

[0041] 本发明实施例的车载以太网安全接入系统,所述车载网关根据所述第二设备编号、所述设备识别码和所述第一设备编号,判断是否允许所述网络设备接入以太网,若判断所述第一设备编号与所述第二设备编号一致,且所述设备识别码合法,则所述网络设备合

法,允许所述网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0042] 本发明附加的方面和优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本发明的实践了解到。

附图说明

[0043] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解,其中:

[0044] 图1为本发明实施例提供的一种车载以太网安全接入方法的流程示意图;

[0045] 图2为本发明实施例提供的另一种车载以太网安全接入方法的流程示意图;

[0046] 图3为本发明实施例提供的又一种车载以太网安全接入方法的流程示意图;

[0047] 图4为本发明实施例提供的一种车载以太网的结构示意图;

[0048] 图5为本发明实施例提供的一种车载网关的结构示意图;

[0049] 图6为本发明实施例提供的一种网络设备的结构示意图;

[0050] 图7为本发明实施例提供的一种车载以太网安全接入系统的结构示意图。

具体实施方式

[0051] 下面详细描述本发明的实施例,实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0052] 下面参考附图描述本发明实施例的车载以太网安全接入方法及系统。

[0053] 图1为本发明实施例提供的一种车载以太网安全接入方法的流程示意图,执行主体为车载网关。如图1所示,该车载以太网安全接入方法包括以下步骤:

[0054] S101、将加密数据发送至请求接入的网络设备,其中,加密数据包括第一设备编号。

[0055] 本发明提供的车载以太网安全接入方法,车载网关具体可以为安装在车辆上的网关、交换机或路由器等,或者,网关、交换机或路由器上安装的软件等。本实施例中,车载网关,加密数据包括第一设备编号,第一设备编号为车载网关管理的数据。网络设备为网卡、交换机、路由器或网关等,或者,网卡、交换机、路由器或网关安装的软件等。其中,车载网关要求是高安全级别的,具备一定强度的防火墙,可防止不合法网络设备入侵。

[0056] 车载网关存储一个由网络管理员预先设定好的关系对应表,关系对应表中包括连接端口号、第一设备编号、设备识别码、MAC地址、IP地址。

[0057] 其中,第一设备编号与设备识别码相互配合构成允许接入当前通信网络的设备的唯一身份识别标识。在定义网络通信架构时为各个类型的网络设备分配相对应的设备识别码,各个设备的MAC地址、IP地址以及接入车载网关的连接端口号都可以变化,但是设备识别码是固定不变的,车载网关在初始状态时,其存储的关系对应表中只记录了第一设备编号与设备识别码。车载网关与对应的网络设备正常通信且网络设备合法之后才把网络设备的MAC地址、IP地址、连接端口号补充到关系对应表中,第一设备编号、设备识别码、MAC地址、IP地址、连接端口号组成了网络设备的不关系对应信息。其中,同一种类型的网络设备的

设备识别码相同,不同类型的网络设备的设备识别码不同。例如,若两个网络设备均为显示屏,则两个网络设备的设备识别码相同;若三个网络设备分别为显示屏、交换机和门控器,则显示屏、交换机和门控器的设备识别码不同。车载网关将第一设备编号预先设置并存储在关系对应表中,且关系对应表中第一设备编号的个数与允许接入的网络设备的个数相同,第一设备编号可以是车载网关随机设置,关系对应表中第一设备编号互不相同。

[0058] 当有网络设备接入时,车载网关通过一定加密的算法将一个未使用的第一设备编号加密后发送到接入的网络设备,加密算法可预定义为多个,车载网关发送的加密数据中还包括当前使用的是第几个加密算法,以供网络设备解密。

[0059] S102、接收网络设备发送的设备识别码和第二设备编号,其中,第二设备编号通过网络设备解密加密数据得到。

[0060] 本实施例中,当网络设备收到加密数据后,通过识别车载网关当前使用的是第几个加密算法,并选择相应的解密算法进行解密,进而把解密后的第二设备编号与网络设备的设备识别码一起发送至车载网关。

[0061] S103、判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网。

[0062] 本实施例中,设备识别码合法,即网络设备能够对车载网关发送至网络设备的加密数据进行解密,且网络设备的设备识别码在车载网关预先设定的关系对应表中。此时,允许网络设备接入以太网,即网络设备通过车载网关接入以太网。车载网关则允许该网络设备接入以太网,为其建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。

[0063] 进一步的,判断第一设备编号与第二设备编号不一致,则网络设备不合法,不允许网络设备接入以太网。

[0064] 本实施例中,判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0065] 进一步的,判断第一设备编号与第二设备编号一致,且设备识别码不合法,则网络设备不合法,不允许网络设备接入以太网。

[0066] 本实施例中,若第一设备编号与第二设备编号一致,且设备识别码不合法,即网络设备能够对车载网关发送至网络设备的加密数据进行解密,但是,网络设备的设备识别码不在车载网关预先设定的关系对应表中,则网络设备不合法,不允许网络设备接入以太网,车载网关自动强制让该网络设备下线,在软件层停止该网络设备连接端口的使用,防止其进一步非法侵入,进而阻止网络设备接入以太网。

[0067] 进一步的,还可以包括:若车载网关和网络设备第一次上电,车载网关与网络设备通过获取对方的MAC地址或IP地址进行通信,或者,车载网关获取网络设备的MAC地址或IP地址向述网络设备发送信息,网络设备通过广播的方式向车载网关发送信息。具体地,车载网关通过地址解析协议发送请求,网络设备根据收到的请求将网络设备的MAC地址或IP地址发送至车载网关,车载网关通过网络设备的MAC地址或IP地址进行与网络设备通信,网络设备通过广播的方式与车载网关进行通信。其中,网络设备的IP地址为预先配置的。车载网关随机为网络设备分配一个未使用的第一设备编号,车载网关根据网络设备的MAC地址或

IP地址将加密数据发送至网络设备,其中,加密数据包括第一设备编号。

[0068] 车载网关上电后,首先检测各个端口的连接状态,即识别当前网络设备的连接状态,网络设备上电后首先是与车载网关进行通信。由于刚上电运行,车载网关未能确定网络设备的MAC地址或IP地址,因此,车载网关发起获取网络设备MAC地址的操作。若网络设备具有IP地址,则车载网关再通过MAC地址获取网络设备对应的IP地址。同时,在此过程中网络设备也将获取到车载网关的MAC地址或IP地址。

[0069] 车载网关获取网络设备的IP地址后,根据预先定义的通信协议发送获取网络设备识别码的请求,该请求包含两部分信息:第一设备编号(取值范围为1-n,n为正整数)、当前使用的加密算法(取值范围为1-m,m为正整数)。

[0070] 其中,由于网络设备第一次连接车载网关,车载网关无法确定网络设备对应的第一设备编号,因此在车载网关所记录的关系对应表中的设备编号处于未确定状态,由车载网关自行随机为网络设备分配一个未使用过的第一设备编号。该请求的信息中,定义第一设备编号的数据经过加密的,定义加密算法的数据是明码,不需要解密,直接提供给网络设备识别。其中,加密算法可预定义为多个,车载网关选择其中一个对第一设备编号进行加密。

[0071] 网络设备接收到请求,首先,识别请求信息中的加密数据使用的是第几个加密算法,之后再运行对应的解密程序,解密获取第二设备编号,最后,使用车载网关发送数据所用的同一个加密算法把该网络设备的设备识别码与解密所得的第二设备编号打包加密后发送至车载网关。

[0072] 车载网关接收网络设备发送的数据并进行解密,首先,比对第二设备编号与第一设备编号,如果两个编号的数据一致,则说明网络设备使用了正确的解密算法,第一次设备校验合格;如果两个编号数据不一致,则说明网络设备无法使用正确的算法,第一次设备校验失败,即当前的网络设备不在允许接入网络的设备范围中,车载网关自动强制让该网络设备下线,在软件层停止该网络设备连接端口的使用。

[0073] 第一次设备校验合格,即第一设备编号与第二设备编号一致,车载网关把解密获取的设备识别码与预先设定好的关系对应表进行比对,进行第二次设备校验。如果当前连接的网络设备的设备识别码不在预先设定好的关系对应表中,或者,该设备识别码对应的网络设备已与车载网关连接,即该设备识别码对应的网络设备已上线,则车载网关停止与该网络设备的通信,自动关闭与该网络设备连接的端口,达到强制让该网络设备下线目的。如果当前连接的网络设备的设备识别码在预先设定好的关系对应表中,且该设备识别码对应的网络设备未与车载网关连接,即该设备识别码对应的网络设备下线,车载网关则允许该网络设备接入以太网,为其建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。同时,车载网关把当前网络设备的连接端口号、第一设备编号、MAC地址、设备识别码或IP地址存储记录到关系对应表中。

[0074] 进一步的,还可以包括:网络设备下线后重新上线,网络设备连接到车载网关的一个端口,车载网关重新对该网络设备进行身份校验,车载网关通过关系对应表获取该网络设备连接的端口对应的连接端口号,进而通过关系对应表获取对应的MAC地址或IP地址,并通过该MAC地址或IP地址尝试与网络设备建立通信,若网络设备的MAC地址或IP地址与车载网关的关系对应表中对应的MAC地址或IP地址一致,则车载网关可通过关系对应表中对应

的MAC地址或IP地址直接与网络设备进行通信,并根据预先定义的通信协议发送获取网络设备识别码的请求,即车载网关通过网络设备的MAC地址或IP地址将加密数据发送至网络设备,其中,加密数据包括关系对应表中对应的第一设备编号。其中,加密算法可预定义为多个,车载网关选择其中一个对第一设备编号进行加密。

[0075] 进一步的,还可以包括:网络设备下线后重新上线,网络设备连接到车载网关的一个端口,车载网关重新对该网络设备进行身份校验,车载网关通过关系对应表获取该网络设备连接的端口对应的连接端口号,进而通过关系对应表获取对应的MAC地址或IP地址,并通过该MAC地址或IP地址尝试与网络设备建立通信,若车载网关不能通过关系对应表中对应的MAC地址或IP地址直接与网络设备进行通信,则车载网关通过地址解析协议发送请求,网络设备根据收到的请求将网络设备的MAC地址或IP地址发送至车载网关,车载网关通过网络设备的MAC地址或IP地址进行与网络设备通信,车载网关随机为网络设备分配一个未使用的第一设备编号,车载网关根据网络设备的MAC地址或IP地址将加密数据发送至网络设备,其中,加密数据包括第一设备编号。其中,加密算法可预定义为多个,车载网关选择其中一个对第一设备编号进行加密。

[0076] 进一步的,还可以包括:若网络设备接入车载网关预留的端口,第一次设备校验合格,即第一设备编号与第二设备编号一致,设备识别码在车载网关预先设定的关系对应表中。车载网关进一步判定该网络设备是否正常连接,即车载网关通过关系对应表获取该设备识别码的对应的连接端口号,进而判断连接端口号对应的网络设备上线或者下线。若设备识别码对应的网络设备未与车载网关连接,即设备识别码对应的网络设备下线,则网络设备合法,车载网关则允许该网络设备接入以太网,为其建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。同时,车载网关将网络设备的信息存储到车载网关的关系对应表中,其中,该信息包括网络设备的连接端口号、第一设备编号、MAC地址、设备识别码或IP地址。

[0077] 进一步的,还可以包括:若网络设备接入车载网关预留的端口,第一设备编号与第二设备编号一致,设备识别码在车载网关预先设定的关系对应表中。车载网关进一步判定该网络设备是否正常连接,即车载网关通过关系对应表获取该设备识别码的对应的连接端口号,进而判断连接端口号对应的网络设备上线或者下线。若设备识别码对应的网络设备与车载网关连接,即设备识别码对应的网络设备已上线,则网络设备不合法,不允许网络设备接入以太网。车载网关停止与该网络设备的通信,自动关闭与该网络设备连接的端口,使该网络设备断开与车载网关的连接,达到强制让该网络设备下线目的。

[0078] 本发明实施例的车载以太网安全接入方法,判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0079] 另外,若网络设备发生损坏,只要替换的网络设备与之前的网络设备为同一类型的网络设备,网络设备重新接入后即可正常使用,操作简单。

[0080] 在上述实施例的基础上,若车载以太网为多层网络(大于等于3层),由于多层网络之间的车载网关需要交互信息,且一个车载网关管理的网络设备可连接到另一个车载网关,因此,针对多层网络的情形,说明车载以太网安全接入方法。允许网络设备接入以太网

之后,还包括以下步骤:

[0081] 若车载网关不是最上层的车载网关,则车载网关向上一层级的车载网关发送网络设备上线的信息,直至最上层的车载网关获取网络设备上线的信息,其中,网络设备上线的信息包括网络设备的关系对应信息。

[0082] 所有接收到网络设备上线的信息的车载网关建立信息通道,网络设备通过信息通道发送或接收信息。

[0083] 本实施例中,各层级的车载网关维护各网络层级的网络设备的关系对应表。最上层的车载网关通过关系对应表存储着整个网络所有网络设备的信息,包括网络设备的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址。下层各级的车载网关都要配置一个合法有效的设备识别码,以供校验。下层各级车载网关获取该层级所有网络设备、车载网关以及其下属各级车载网关所连接的网络设备的信息,其中,该信息包括网络设备或车载网关的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址。

[0084] 具体地,若车载网关接入以太网,且车载网关不是最上层的车载网关,则需做两方面工作,一方面需与上一层级的车载网关进行身份校验,即该车载网关向上一层级的车载网关发送包括第一设备编号的加密数据,其中,加密数据包括通过加密算法加密的第一设备编号,加密算法可预定义为多个,车载网关发送的加密数据中还包括当前使用的是第几个加密算法,以供上一层级的车载网关解密。当车载网关收到加密数据后,通过识别上一层级的车载网关当前使用的是第几个加密算法,并选择相应的解密算法进行解密,进而把解密后的第二设备编号与车载网关的设备识别码一起加密并打包发送至上一层级的车载网关。

[0085] 上一层级的车载网关接收车载网关发送的设备识别码和第二设备编号,若第一设备编号与第二设备编号不一致,即车载网关无法对上一层级的车载网关发送至车载网关的加密数据进行解密,则车载网关不合法,不允许车载网关接入以太网,上一层级的车载网关自动强制让该车载网关下线,在软件层停止车载网关连接端口的使用,防止其进一步非法侵入,进而阻止车载网关接入以太网。若第一设备编号与第二设备编号一致,且设备识别码合法,即车载网关能够对上一层级的车载网关发送至车载网关的加密数据进行解密,且车载网关的设备识别码在上一层级的车载网关预先设定的关系对应表中,则车载网关合法,允许车载网关接入以太网,即车载网关通过上一层级的车载网关接入以太网。上一层级的车载网关直至最上层的车载网关为车载网关建立相应的信息通道,车载网关通过信息通道发送或接收预先设定的信息。若第一设备编号与第二设备编号一致,且设备识别码不合法,即车载网关能够对上一层级的车载网关发送至车载网关的加密数据进行解密,但是,车载网关的设备识别码不在上一层级的车载网关预先设定的关系对应表中,则车载网关不合法,不允许车载网关接入以太网,上一层级的车载网关自动强制让车载网关下线,在软件层停止车载网关连接的端口的使用,防止其进一步非法侵入,进而阻止车载网关接入以太网。

[0086] 另一方面,该车载网关对下挂的所有网络设备进行身份校验,同时在校验完所有网络设备后,把校验结果传输至上一层级的车载网关,让上一层级的车载网关了解车载网关下属网络设备的情况,共同建立起相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。直至各层级的车载网关分别获取该层级所有网络设备、车载网关以及其下属各级车载网关所连接的网络设备的信息,其中,信息还包括其该层级所有网络设备、车

载网关以及其下属各级车载网关的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址。

[0087] 进一步的,若网络设备下线,且车载网关不是最上层的车载网关,则车载网关向上一层级的车载网关发送网络设备下线的信息,上一层级的车载网关获取网络设备下线的信息,逐级发送,直至最上层的车载网关获取网络设备下线的信息,其中,网络设备下线的信息还包括该网络设备的连接端口号和设备识别码。车载网关、上一层级的车载网关直至最上层的车载网关关闭相应的信息通道。

[0088] 进一步的,网络设备下线后重新上线,若网络设备合法,且车载网关不是最上层的车载网关,则车载网关向上一层级的车载网关发送网络设备的信息,直至最上层的车载网关获取网络设备的信息。同时,车载网关、上一层级的车载网关直至最上层的车载网关分别将该网络设备的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址存储到各自的关系对应表中。车载网关、上一层级的车载网关直至最上层的车载网关建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。

[0089] 网络设备下线后重新上线,若网络设备不合法,不允许网络设备接入以太网,车载网关自动强制让网络设备下线,在软件层停止网络设备连接的端口的使用,防止其进一步非法侵入,进而阻止网络设备接入以太网。

[0090] 进一步的,若网络设备接入车载网关预留的端口,网络设备合法,且车载网关不是最上层的车载网关,则车载网关向上一层级的车载网关发送网络设备的信息,直至最上层的车载网关获取网络设备的信息。同时,车载网关、上一层级的车载网关直至最上层的车载网关分别将该网络设备的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址存储到各自的关系对应表中。车载网关、上一层级的车载网关直至最上层的车载网关建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。

[0091] 若网络设备接入车载网关预留的端口,且网络设备不合法,则不允许网络设备接入以太网,车载网关自动强制让网络设备下线,在软件层停止网络设备连接的端口的使用,防止其进一步非法侵入,进而阻止网络设备接入以太网。

[0092] 进一步的,若网络设备接入车载网关预留的端口,第一设备编号与第二设备编号一致,设备识别码未在车载网关预先设定的关系对应表中,且车载网关不是最上层的车载网关,则向上层的车载网关发送请求信息;上层的车载网关接收请求信息,并根据请求信息中的设备识别码判断网络设备是否合法。

[0093] 进一步的,网络设备接入车载网关预留的端口,若上层的车载网关接收到请求信息,请求信息中的设备识别码在上层的车载网关预先设定的关系对应表中,且设备识别码对应的网络设备未与上层的车载网关连接,即设备识别码对应的网络设备下线,则网络设备合法,上层的车载网关向下层的车载网关发送允许网络设备接入以太网的信息,允许网络设备通过车载网关接入以太网。车载网关直至最上层的车载网关建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。同时,车载网关直至最上层车载网关分别将该网络设备的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址存储到各自的关系对应表中。

[0094] 若请求信息中的设备识别码在上层的车载网关预先设定的关系对应表中,且设备识别码对应的网络设备与车载网关连接,即设备识别码对应的网络设备已上线,则网络设

备不合法,上层的车载网关向下层的车载网关发送不允许网络设备接入以太网的信息,不允许网络设备通过车载网关接入以太网。车载网关自动强制让网络设备下线,在软件层停止网络设备连接的端口的使用,防止其进一步非法侵入,进而阻止网络设备接入以太网。

[0095] 进一步的,网络设备接入车载网关预留的端口,最上层的车载网关接收到请求信息,请求信息中的设备识别码在最上层的车载网关预先设定的关系对应表中,且设备识别码对应的网络设备未与最上层的车载网关连接,即设备识别码对应的网络设备下线,则网络设备合法,最上层的车载网关逐级向下层的车载网关发送允许网络设备接入以太网的信息。同时,车载网关直至最上层的车载网关分别将该网络设备的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址存储到各自的关系对应表中。车载网关直至最上层的车载网关建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。否则,网络设备不合法,最上层的车载网关逐级向下层的车载网关不允许网络设备接入以太网的信息。车载网关自动强制让网络设备下线,在软件层停止网络设备连接的端口的使用,防止其进一步非法侵入,进而阻止网络设备接入以太网。

[0096] 本发明实施例的车载以太网安全接入方法,判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0097] 另外,若网络设备或者车载网关发生损坏,只要替换的网络设备或者车载网关与之前网络设备或者车载网关为同一类型的网络设备,网络设备或者车载网关重新接入后即可正常使用,操作简单。

[0098] 网络设备更改其在当前网络中的网络层级,无需再重新申请任何身份信息,只需通过上述方法进行身份校验,该网络设备的信息自动由原接入位置迁入到当前接入位置,并且各层级的车载网关为其建立相应的信息通道,网络设备通过信息通道发送或接收预先设定的信息。即,合法的设备在网络的任意一层级接入,都可正常进行通信,大大提高了网络架构的灵活性。

[0099] 图2为本发明实施例提供的另一种车载以太网安全接入方法的流程示意图,应用于网络设备。如图2所示,该车载以太网安全接入方法包括以下步骤:

[0100] S104、接收车载网关发送的加密数据,并对加密数据进行解密得到第二设备编号,加密数据包括第一设备编号。

[0101] S105、向车载网关发送第二设备编号和设备识别码,以由车载网关判断,当第一设备编号与第二设备编号一致,且设备识别码合法时,则请求接入的网络设备合法,允许网络设备接入以太网。

[0102] 需要说明的是,前述对车载以太网安全接入方法的解释说明,也适用于本发明实施例的车载以太网安全接入方法,本发明实施例中未公布的细节,在此不再赘述。

[0103] 本发明实施例的车载以太网安全接入方法,向车载网关发送第二设备编号和设备识别码,以由车载网关判断,当第一设备编号与第二设备编号一致,且设备识别码合法时,则请求接入的网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0104] 图3为本发明实施例提供的又一种车载以太网安全接入方法的流程示意图。如图3所示,该车载以太网安全接入方法包括以下步骤:

[0105] S106、车载网关将加密数据发送至请求接入的网络设备,其中,加密数据包括第一设备编号。

[0106] S107、网络设备接收加密数据,并对加密数据进行解密,网络设备将解密得到的第二设备编号和设备识别码发送至车载网关。

[0107] S108、车载网关根据第二设备编号、设备识别码和第一设备编号,判断是否允许网络设备接入以太网,若判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网。

[0108] 需要说明的是,前述对车载以太网安全接入方法的解释说明,也适用于本发明实施例的车载以太网安全接入方法,本发明实施例中未公布的细节,在此不再赘述。

[0109] 本发明实施例的车载以太网安全接入方法,车载网关判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0110] 作为一个示例,如图4所示,车载以太网络为一个三层级网络,最上层的车载网关为一个,即车载网关1,车载网关有4个端口(1-4),分别连接网络设备1、网络设备2和车载网关2、车载网关3。车载网关1存储的关系对应表如表1所示(需要说明的是,以下数据仅为示例):

[0111] 表1

[0112]

连接端口号	第一设备编号	设备识别码	MAC 地址	IP 地址
1	1	A01 (网络设备 1)	90-FA-A6-76-38-18	192. 168. 1. 2
2	2	A02 (网络设备 2)	90-FB-A6-76-38-18	192. 168. 1. 3
3	3	A03 (车载网关 2)	90-FC-A6-76-38-18	192. 168. 1. 4
4	4	A04 (车载网关 3)	90-FD-A6-76-38-18	192. 168. 1. 5
5	5	B01	90-FE-A6-76-38-18	192. 168. 1. 6

[0113]

		(网络设备 3)		
6	6	B02 (网络设备 4)	90-FF-A6-76-38-18	192. 168. 1. 7
7	7	B03 (网络设备 5)	91-F0-A6-76-38-18	192. 168. 1. 8
8	8	B04 (网络设备 6)	92-F0-A6-76-38-18	192. 168. 1. 9
9	9	B05 (车载网关 4)	93-F0-A6-76-38-18	192. 168. 1. 10
10	10	C01 (网络设备 7)	94-F0-A6-76-38-18	192. 168. 1. 11
11	11	C02 (网络设备 8)	95-F0-A6-76-38-18	192. 168. 1. 12
12	12	C03 (网络设备 9)	96-F0-A6-76-38-18	192. 168. 1. 13

[0114] 车载网关2有3个端口(5-7),分别连接网络设备3、网络设备4、网络设备5,车载网关2存储的关系对应表如表2所示(需要说明的是,以下数据仅为示例):

[0115] 表2

[0116]

连接端口号	第一设备编号	设备识别码	MAC 地址	IP 地址
5	5	B01 (网络设备 3)	90-FE-A6-76-38-18	192. 168. 1. 6
6	6	B02 (网络设备 4)	90-FF-A6-76-38-18	192. 168. 1. 7
7	7	B03 (网络设备 5)	91-F0-A6-76-38-18	192. 168. 1. 8

[0117] 车载网关3有3个端口(13、8、9),连接端口号为13对应的端口为预留端口,未定义连接的网络设备,其他两个端口分别连接了网络设备6、车载网关4,车载网关3存储的关系对应表如表3所示(需要说明的是,以下数据仅为示例):

[0118] 表3

[0119]

连接端口号	第一设备编号	设备识别码	MAC 地址	IP 地址
13	(空)	(空)	(空)	(空)
8	8	B04 (网络设备 6)	92-F0-A6-76-38-18	192. 168. 1. 9
9	9	B05 (车载网关 4)	93-F0-A6-76-38-18	192. 168. 1. 10
10	10	C01 (网络设备 7)	94-F0-A6-76-38-18	192. 168. 1. 11
11	11	C02 (网络设备 8)	95-F0-A6-76-38-18	192. 168. 1. 12
12	12	C03 (网络设备 9)	96-F0-A6-76-38-18	192. 168. 1. 13

[0120] 车载网关4有4个端口(10、11、12、14),连接端口号为14对应的端口为预留端口,未定义连接的网络设备,其他三个端口分别连接网络设备7、网络设备8、网络设备9,车载网关4存储的关系对应表如表4所示(需要说明的是,以下数据仅为示例):

[0121] 表4

[0122]

连接端口号	第一设备编号	设备识别码	MAC 地址	IP 地址
10	10	C01 (网络设备 7)	94-F0-A6-76-38-18	192. 168. 1. 11
11	11	C02 (网络设备 8)	95-F0-A6-76-38-18	192. 168. 1. 12
12	12	C03 (网络设备 9)	96-F0-A6-76-38-18	192. 168. 1. 13
14	(空)	(空)	(空)	(空)

[0123] 若该三层级网络上的网络设备和车载网关第一次上电,车载网关1、车载网关2、车

载网关3或车载网关4上电后分别检测各个端口的连接状态,即分别识别网络设备1、网络设备2、网络设备3、网络设备4、网络设备5、网络设备6、网络设备7、网络设备8、网络设备9或网络设备10的连接状态。网络设备1、网络设备2、网络设备3、网络设备4、网络设备5、网络设备6、网络设备7、网络设备8、网络设备9或网络设备10上电后首先与车载网关1、车载网关2、车载网关3或车载网关4进行通信。由于刚上电运行工作,车载网关1、车载网关2、车载网关3或车载网关4未能确定网络设备1、网络设备2、网络设备3、网络设备4、网络设备5、网络设备6、网络设备7、网络设备8、网络设备9或网络设备10的MAC地址与IP地址,因此,车载网关1获取网络设备1、网络设备2、车载网关2或车载网关3的MAC地址与IP地址。车载网关2获取网络设备3、网络设备4、网络设备5的MAC地址与IP地址,并把获取到的这些信息发送至车载网关1。车载网关3获取网络设备6、车载网关4的MAC地址与IP地址,并把获取到的这些信息发送至车载网关1。车载网关4获取网络设备7、网络设备8、网络设备9的MAC地址与IP地址,并把获取到的这些信息经由车载网关3发送至车载网关1。

[0124] 一级车载网关、二级车载网关1、二级车载网关2或三级车载网关分别获取网络设备1、网络设备2、网络设备3、网络设备4、网络设备5、网络设备6、网络设备7、网络设备8、网络设备9或网络设备10的MAC地址与IP地址后,分别根据预先定义的通信协议分别获取各个网络设备的设备识别码和第二设备编号。例如,一级车载网关通过一定加密的算法将网络设备1对应的第一设备编号加密后发送至网络设备1,加密算法可预定义为多个,一级车载网关发送的加密数据中还包括当前使用的是第几个加密算法,以供网络设备1解密。网络设备1接收到一级车载网关的请求,首先识别加密数据使用的是第几个加密算法,之后再运行相应的解密程序对该加密数据进行解密,获取第二设备编号,最后,网络设备1使用车载网关发送数据所用的加密算法把设备识别码与解密所得的第二设备编号打包发送至一级车载网关。一级车载网关接收并解密获取网络设备1的设备识别码和第二设备编号。

[0125] 车载网关1、车载网关2、车载网关3或车载网关4分别根据网络设备1、网络设备2、网络设备3、网络设备4、网络设备5、网络设备6、网络设备7、网络设备8、网络设备9或网络设备10的设备识别码和第二设备编号判断其合法或者不合法。例如,车载网关4对网络设备7进行第一次设备校验,对比网络设备7解密获取的第二设备编号与接收到的第一设备编号。若网络设备7解密获取的第二设备编号与接收到的第一设备编号一致,车载网关4把网络设备7的设备识别码与预先设定好的关系对应表进行比对,进行第二次设备校验,若网络设备7的设备识别码(C01)在预先设定好的关系对应表中,且设备识别码(C01)对应的网络设备未上线,即设备识别码(C01)对应的网络设备未与车载网关4连接,则网络设备7合法;否则,网络设备7不合法。

[0126] 若网络设备7合法,允许网络设备7接入以太网。车载网关4把网络设备7上线的信息发送至车载网关3,车载网关3把网络设备7上线的信息发送至车载网关1,其中,网络设备7上线的信息还包括连接端口号、第一设备编号、设备识别码、MAC地址或IP地址。车载网关1、车载网关3或车载网关4分别把网络设备7的连接端口号、第一设备编号、设备识别码、MAC地址或IP地址存储到所维护或管理的关系对应表中。车载网关1、车载网关2、车载网关3或车载网关4为网络设备7建立相应的信息通道,网络设备7通过相应的信息通道接收或发送预先设定的信息。

[0127] 若网络设备7不合法,不允许网络设备7接入以太网。车载网关4停止与该网络设备

的通信,自动关闭与该网络设备7连接的端口,使该网络设备7断开与车载网关4的连接,达到强制让该网络设备7下线目的。

[0128] 网络设备4下线后,车载网关2向车载网关1发送网络设备4下线已下线的信息,该下线的信息还包括网络设备4的设备识别码和连接端口号。车载网关2、车载网关1关闭网络设备4对应的信息通道。

[0129] 当网络设备4重新上线时,车载网关2重新对网络设备4进行身份校验。由于网络设备4的MAC地址与IP地址可能改变,车载网关2首先通过关系对应表获取网络设备4连接的端口对应的连接端口号,进而通过关系对应表获取对应的MAC地址与IP地址,并通过该MAC地址与IP地址尝试与网络设备4进行通信。若网络设备4的MAC地址或IP地址与车载网关2的关系对应表中对应的MAC地址与IP地址一致,则车载网关2通过关系对应表中对应的MAC地址与IP地址直接与网络设备4进行通信,车载网关2根据预先定义的通信协议发送获取网络设备4的设备识别码的请求信息,即车载网关2通过网络设备4或关系对应表中对应的MAC地址或IP地址将加密数据发送至网络设备4,其中,加密数据包括关系对应表中对应的第一设备编号,以获取网络设备4的设备识别码。若网络设备4的MAC地址或IP地址与车载网关2的关系对应表中对应的MAC地址或IP地址不一致,即车载网关2不能通过关系对应表中对应的MAC地址或IP地址直接与网络设备4进行通信,则车载网关2通过地址解析协议向网络设备4发送请求,网络设备4根据收到的请求将网络设备4的MAC地址或IP地址发送至车载网关2,车载网关2通过网络设备4的MAC地址或IP地址进行与网络设备4通信,网络设备4通过获取车载网关2的MAC地址或IP地址或者通过广播的方式,与车载网关2进行通信。车载网关2根据预先定义的通信协议发送获取网络设备4的设备识别码的请求信息,即车载网关2随机为网络设备4分配一个未使用的第一设备编号,车载网关2根据网络设备4的MAC地址或IP地址将加密数据发送至网络设备4,其中,加密数据包括该第一设备编号。网络设备4接收到该请求信息后,识别请求信息中的加密数据使用的是第几个加密算法,之后再运行对应的解密程序,获取第二设备编号,最后,使用车载网关2发送数据所用的同一个加密算法把该网络设备4的设备识别码与解密所得的第二设备编号打包加密后发送至车载网关2。

[0130] 车载网关2接收网络设备4发送的数据并进行解密,首先,比对第二设备编号与第一设备编号,如果两个编号的数据一致,则说明网络设备4使用了正确的解密算法,第一次设备校验合格;如果两个编号数据不一致,则说明网络设备4无法使用正确的算法,第一次设备校验失败,即当前的网络设备4不在允许接入网络的设备范围中,车载网关2自动强制让该网络设备4下线,在软件层停止该网络设备4连接端口的使用。

[0131] 第一次设备校验合格,即第一设备编号与第二设备编号一致,车载网关2把解密获取的设备识别码与预先设定好的关系对应表进行比对,进行第二次设备校验。如果当前连接的网络设备4的设备识别码不在预先设定好的关系对应表中,或者,该设备识别码对应的网络设备4已与车载网关2连接,即该设备识别码对应的网络设备4已上线,则车载网关2停止与该网络设备4的通信,自动关闭与该网络设备4连接的端口,使该网络设备4断开与车载网关2的连接,达到强制让该网络设备4下线目的。如果当前连接的网络设备4的设备识别码在预先设定好的关系对应表中,且该设备识别码对应的网络设备4未与车载网关2连接,即该设备识别码对应的网络设备4下线,车载网关2则允许该网络设备4接入以太网。车载网关2向车载网关1发送网络设备上线的信息。车载网关2、车载网关1为其建立相应的信息通

道,网络设备4通过信息通道发送或接收预先设定的信息。同时,车载网关2、车载网关1把当前网络设备4的连接端口号、第一设备编号、MAC地址、设备识别码或IP地址存储到各自的关系对应表中。

[0132] 若网络设备1通过车载网关4预留的端口接入以太网,该预留的端口的连接端口号为14,车载网关4将加密数据发送至网络设备1,其中,加密数据包括关系对应表中一个未使用的第一设备编号,以获取网络设备1的设备识别码。网络设备1接收到该加密数据后,识别该加密数据使用的是第几个加密算法,之后再运行对应的解密程序,获取第二设备编号,最后,使用车载网关4发送数据所用的同一个加密算法把网络设备1的设备识别码与解密所得的第二设备编号打包加密后发送至车载网关4。第一设备编号与第二设备编号一致,网络设备1的设备识别码不在车载网关4预先设定的关系对应表中。车载网关4向上层的车载网关3发送请求信息,上层的车载网关3接收该请求信息,请求信息中,网络设备1的设备识别码不在车载网关3预先设定的关系对应表中。车载网关3向车载网关1发送请求信息,车载网关1接收该请求信息,请求信息中,网络设备1的设备识别码在车载网关1预先设定的关系对应表中。若网络设备1的设备识别码对应的网络设备未与车载网关1连接,即网络设备1的设备识别码对应的网络设备下线,则网络设备1的设备识别码合法,允许网络设备1的设备识别码接入以太网。车载网关4、车载网关3或车载网关1为其建立相应的信息通道,网络设备1通过信息通道发送或接收预先设定的信息。同时,车载网关4、车载网关3或车载网关1分别把当前网络设备1的连接端口号、第一设备编号、MAC地址、设备识别码或IP地址存储到各自的关系对应表中。若网络设备1的设备识别码对应的网络设备与车载网关1连接,即网络设备1的设备识别码对应的网络设备上线,网络设备1不合法,不允许网络设备1接入以太网。车载网关4自动强制让该网络设备1下线,在软件层停止该网络设备1连接的端口的使用。

[0133] 图5为本发明实施例提供的一种车载网关的结构示意图。如图5所示,包括:第一发送模块201、第一接收模块202和判断模块203。

[0134] 第一发送模块201,用于将加密数据发送至请求接入的网络设备,其中,加密数据包括第一设备编号。

[0135] 第一接收模块202,用于接收网络设备发送的设备识别码和第二设备编号,其中,第二设备编号通过网络设备解密加密数据得到。

[0136] 判断模块203,用于判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网。

[0137] 需要说明的是,前述对车载以太网安全接入方法的解释说明,也适用于本发明实施例的车载网关,本发明实施例中未公布的细节,在此不再赘述。

[0138] 本发明实施例的车载网关,车载网关判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0139] 图6为本发明实施例提供的一种网络设备的结构示意图。如图6所示,包括:第二接收模块301和第二发送模块302。

[0140] 第二接收模块301,用于接收车载网关发送的加密数据,并对加密数据进行解密得到第二设备编号,加密数据包括第一设备编号。

[0141] 第二发送模块302,用于向车载网关发送第二设备编号和设备识别码,以由车载网关判断,当第一设备编号与第二设备编号一致,且设备识别码合法时,则请求接入的网络设备合法,允许网络设备接入以太网。

[0142] 需要说明的是,前述对车载以太网安全接入方法的解释说明,也适用于本发明实施例的网络设备,本发明实施例中未公布的细节,在此不再赘述。

[0143] 本发明实施例的网络设备,网络设备将解密得到的第二设备编号和设备识别码发送至车载网关;车载网关判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0144] 图7为本发明实施例提供的一种车载以太网安全接入系统的结构示意图。如图7所示,包括:车载网关401和网络设备402。

[0145] 车载网关401将加密数据发送至请求接入的网络设备402,其中,加密数据包括第一设备编号;网络设备402接收加密数据,并对加密数据进行解密,网络设备402将解密得到的第二设备编号和设备识别码发送至车载网关401;车载网关401根据第二设备编号、设备识别码和第一设备编号,判断是否允许网络设备402接入以太网,若判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备402合法,允许网络设备402接入以太网。

[0146] 需要说明的是,前述对车载以太网安全接入方法的解释说明,也适用于本发明实施例的网络设备,本发明实施例中未公布的细节,在此不再赘述。

[0147] 本发明实施例的车载以太网安全接入系统,车载网关根据第二设备编号、设备识别码和第一设备编号,判断是否允许网络设备接入以太网,若判断第一设备编号与第二设备编号一致,且设备识别码合法,则网络设备合法,允许网络设备接入以太网,建立了完善的网络设备的身份验证体系,身份验证过程简单,方便更换或维护网络设备,有效阻止了不合法网络设备的入侵。

[0148] 本实施例还提供一种非临时性计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如上的车载以太网安全接入方法。

[0149] 本实施例还提供一种计算机程序产品,当计算机程序产品中的指令处理器执行时,实现如上的车载以太网安全接入方法。

[0150] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0151] 此外,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中,“多个”的含义是至少两个,例如两个,三个等,除非另有明确具体的限定。

[0152] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为,表示包括

一个或更多个用于实现定制逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分,并且本发明的优选实施方式的范围包括另外的实现,其中可以不按所示出或讨论的顺序,包括根据所涉及的功能按基本同时的方式或按相反的顺序,来执行功能,这应被本发明的实施例所属技术领域的技术人员所理解。

[0153] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤,例如,可以被认为用于实现逻辑功能的可执行指令的定序列列表,可以具体实现在任何计算机可读介质中,以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用,或结合这些指令执行系统、装置或设备而使用。就本说明书而言,“计算机可读介质”可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例(非穷尽性列表)包括以下:具有一个或多个布线的电连接部(电子装置),便携式计算机盘盒(磁装置),随机存取存储器(RAM),只读存储器(ROM),可擦除可编程只读存储器(EPROM或闪速存储器),光纤装置,以及便携式光盘只读存储器(CDROM)。另外,计算机可读介质甚至可以是可在其上打印程序的纸或其他合适的介质,因为可以例如通过对纸或其他介质进行光学扫描,接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得程序,然后将其存储在计算机存储器中。

[0154] 应当理解,本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中,多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。如,如果用硬件来实现和在另一实施方式中一样,可用本领域公知的下列技术中的任一项或它们的组合来实现:具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路,具有合适的组合逻辑门电路的专用集成电路,可编程门阵列(PGA),现场可编程门阵列(FPGA)等。

[0155] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通程序来指令相关的硬件完成,的程序可以存储于一种计算机可读存储介质中,该程序在执行时,包括方法实施例的步骤之一或其组合。

[0156] 此外,在本发明各个实施例中的各功能单元可以集成在一个处理模块中,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模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也可以存储在一个计算机可读存储介质中。

[0157] 上述提到的存储介质可以是只读存储器,磁盘或光盘等。尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

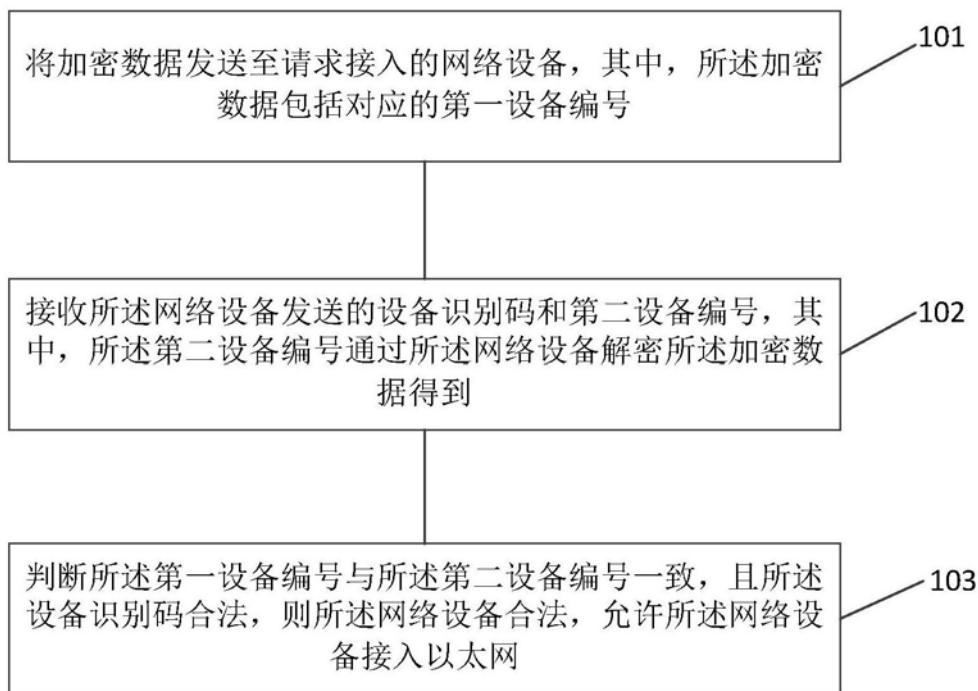


图1

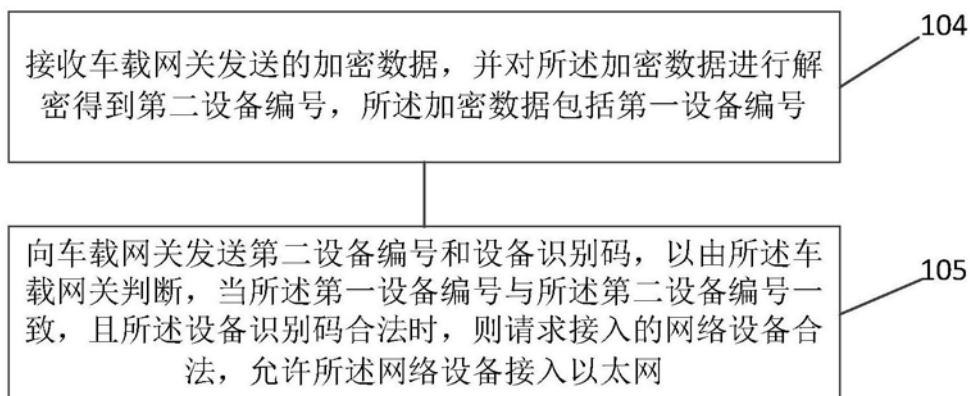


图2

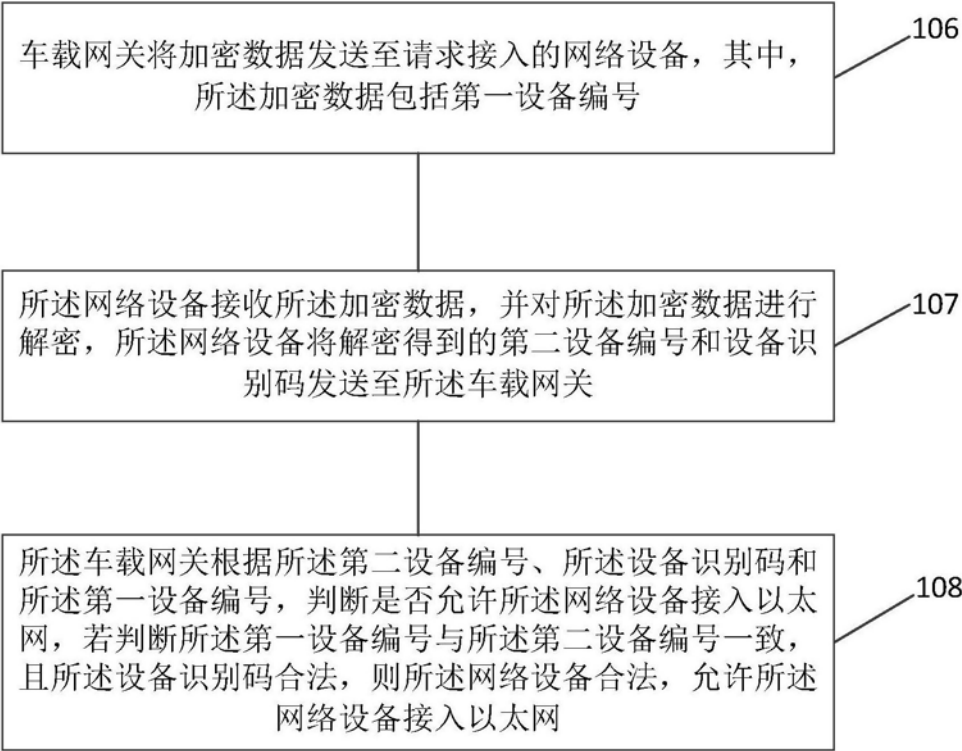


图3

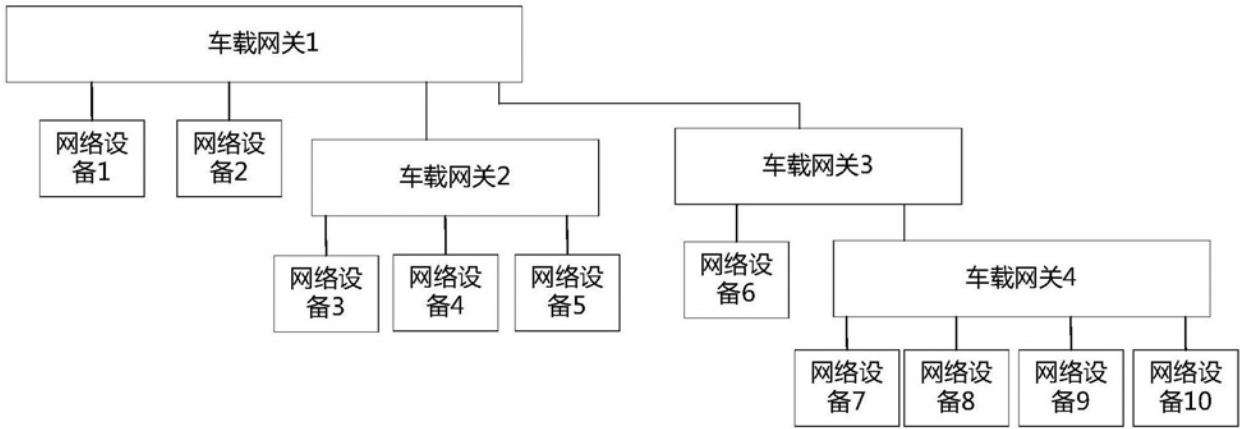


图4

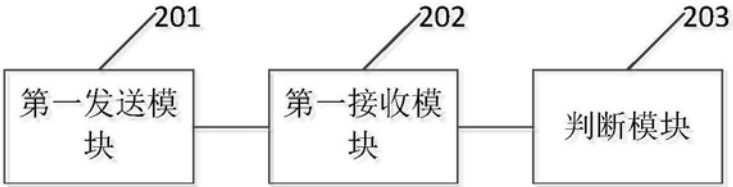


图5

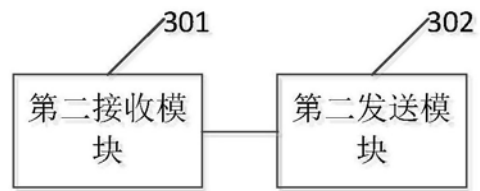


图6

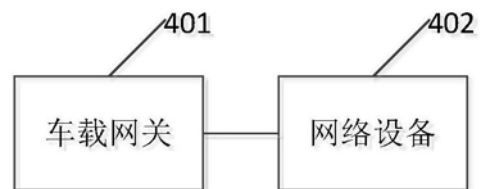


图7