(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
2022 年 5 月 27 日 (27.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/105703 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2021/130551

(22) 国际申请日: 2021 年 11 月 15 日 (15.11.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011313900.3 2020年11月20日 (20.11.2020) CN

(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: 吴迪(**WU, Di**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 曹斌(**CAO, Bin**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 潘伟(**PAN, Wei**); 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: 深圳市深佳知识产权代理事务所（普通合伙）(**SHENPAT INTELLECTUAL PROPERTY AGENCY**); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦B座18C2、18D、18E、18E2, Guangdong 518001 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

(54) **Title:** INTEGRITY VERIFICATION METHOD AND RELATED DEVICE

(54) 发明名称: 一种完整性校验方法及相关设备

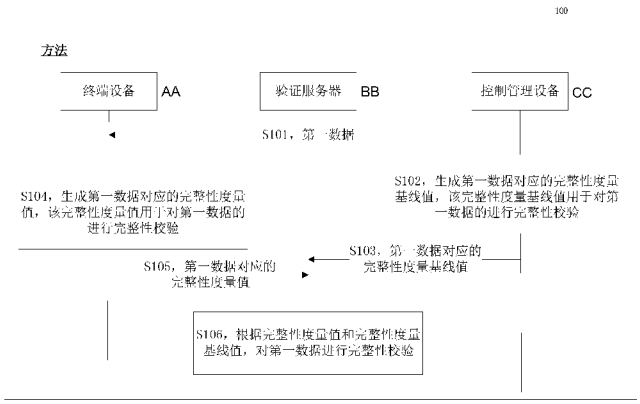

图 2

S101 First data
S102 Generate an integrity measurement baseline value corresponding to the first data, the integrity measurement baseline value being used for performing integrity verification on the first data
S103 Integrity measurement baseline value corresponding to the first data
S104 Generate an integrity measurement value corresponding to the first data, the integrity measurement value being used for performing integrity verification on the first data
S105 Integrity measurement value corresponding to the first data
S106 Perform integrity verification on the first data according to the integrity measurement value and the integrity measurement baseline value
AA Terminal device
BB Verification server
CC Control management device

(57) **Abstract:** Disclosed in the embodiments of the present application are an integrity verification method and a related device, the method comprising: a first device sends first data to a second device; the first device sends to a verification server an integrity measurement baseline value corresponding to the first data; the second device sends to the verification server an integrity measurement value corresponding to the first data; and then the verification server performs integrity verification on the first data according to the integrity measurement value and the integrity measurement baseline value, such that only the integrity measurement value and the

WO 2022/105703 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

integrity measurement baseline value corresponding to the first data need to be interacted, and the interaction of all the first data is no longer necessary, thereby reducing the amount of data required to be interacted for verification, and saving resources occupied by a verification process. In addition, the integrity verification is performed by a trusted verification server, rather than by directly comparing the first data by the first device, such that the security and reliability of the verification process are ensured, thus providing a guarantee for normal operation of services on the second device.

(57) 摘要：本申请实施例公开了一种完整性校验方法及相关设备，包括：第一设备向第二设备发送第一数据，第一设备向验证服务器发送该第一数据对应的完整性度量基线值，第二设备向验证服务器发送第一数据对应的完整性度量值；验证服务器即可根据完整性度量值和完整性度量基线值对第一数据进行完整性校验。如此，需要交互的仅是第一数据对应的完整性度量值和完整性度量基线值，无需交互全量的第一数据，减少了校验所需交互的数据量，节约了校验过程所占用的资源，而且，由可信的验证服务器进行完整性校验，而不是由第一设备直接对第一数据进行比对，确保该校验过程更加安全和可靠，从而为第二设备上业务的正常运行提供了保障。

一种完整性校验方法及相关设备

本申请要求于2020年11月20日提交中国国家知识产权局、申请号为202011313900.3、申请名称为“一种完整性校验方法及相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及一种完整性校验方法及相关设备。

背景技术

通常，设备之间会交互一些数据，指导接收端对待传输数据的处理，为了保证业务的正常运行，要求设备之间交互的数据在发送端和接收端保持一致，这就需要对发送端和接收端上保存的数据进行校验，例如，控制管理设备会向终端设备发送一些数据，这些数据指导该终端设备完成对报文的处理，要求终端设备上指导报文处理的数据来自控制管理设备且与控制管理设备下发的数据保持一致，一旦不一致，说明该终端设备上指导报文处理所依据的数据可能是不可靠的，基于此，需要对终端设备上用于指导报文处理的数据和控制管理设备上对应的数据进行校验。

目前，以控制管理设备向终端设备发送的数据的校验为例，终端设备会将从控制管理设备接收的数据全量上报给控制管理设备，由控制管理设备对所接收的数据和本地保存的数据进行比对，如果一致，则表示该终端设备中用于指导报文处理的数据准确，如果不一致，则表示该终端设备中用于指导报文处理的数据不准确。但是，该实现方式中，对终端设备和控制管理设备上数据的校验，需要两者之间交互的信息量较大，需要占用的网络资源较多，而且，通过全量数据的交互和对比进行校验，校验结果也不够安全和准确。

发明内容

本申请实施例提供了一种完整性校验方法及相关设备，数据的发送端和接收端分别将数据的完整性度量值和完整性度量基线值发送给可信的验证服务器，由该验证服务器对该数据的完整性进行校验，确保高效、可靠的完成对发送端和接收端上数据的完整性校验，从而为业务的正常运行提供了保障。

第一方面，本申请实施例提供了一种完整性校验方法，该方法可以包括：第一设备向第二设备发送第一数据之后，第一设备向验证服务器发送该第一数据对应的完整性度量基线值，第二设备向验证服务器发送第一数据对应的完整性度量值；这样，验证服务器即可根据完整性度量值和完整性度量基线值对第一数据进行完整性校验。如此，由可信的验证服务器对第一设备和第二设备分别发送的相同的第一数据对应的完整性度量值和完整性度量基线值进行完整性校验，需要交互的仅是第一数据对应的完整性度量值和完整性度量基线值，无需交互全量的第一数据，有效的减少了校验所需交互的数据量，大大的节约了校验过程所占用的资源，而且，通过引入可信的验证服务器，由验证服务器对完整性度量值和完整性度量基线值进行完整性校验，而不是由第一设备直接对第一数据进行比对，能够

确保该校验过程更加安全和可靠，从而为第二设备上业务的正常运行提供了保障。

其中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

作为一个示例，第一数据可以包括下述至少一个：分段路由流量工程（英文：Segment Routing Traffic Engineering，简称：SR TE）配置信息、分段路由流量工程的策略（英文：Segment Routing Traffic Engineering policy，简称：SR TE-policy）配置信息、访问控制列表（英文：Access Control Lists，简称：ACL）配置信息或流规则（英文：Flow Specification，简称：FlowSpec）配置信息。

其中，完整性度量基线值可以为经过哈希计算得到的哈希值，那么， 完整性度量值为经过哈希计算得到的哈希值。或者，完整性度量基线值也可以为数字签名，那么，完整性度量值为数字签名。又或者，完整性度量基线值还可以为经过加密处理得到的加密值，那么，完整性度量值为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据，例如，第一设备待校验的数据为数据 a 和数据 b，第二设备待检验的数据也为数据 a 和数据 b。

在一种可能的实现方式中，在第一设备向验证服务器发送第一数据的完整性度量基线值之前，第一设备还可以计算第一数据对应的完整性度量基线值；在第二设备向验证服务器发送第一数据的完整性度量值之前，第二设备还可以计算第一数据对应的完整性度量值。作为一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的全部内容确定所述完整性度量基线值；那么，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的全部内容确定完整性度量值。其中，第一设备和第二设备上对第一数据按照相同的顺序保存，可以确保根据第一数据的全部内容计算的校验值是对应的，为完整性校验的准确执行提供了保障。作为另一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的部分内容确定所述完整性度量基线值；那么，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的部分内容确定完整性度量值。其中，第一设备和第二设备上获取该第一数据的部分内容的规则相同，可以确保根据第一数据的部分内容计算的校验值是对应的，为完整性校验的准确执行提供了保障。作为又一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据发送第一数据对应的第一操作日志确定所述完整性度量基线值；那么，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据接收所述第一数据对应的第二操作日志确定所述完整性度量值。其中，第一设备和第二设备上对接收和发送数据生成操作日志的规则可以相同，可以确保根据第一数据对应的第一操作日志和第二操作日志得到的校验值是对应的，为完整性校验的准确执行提供了保障。

在一种可能的实现方式中，第二设备向验证服务器发送第一数据对应的完整性度量值，

可以是基于所接收的第一指示触发的，也可以是满足本地预设条件后触发的。作为一个示例，在第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以接收第一指示，该第一指示用于指示第二设备对第一数据进行完整性校验。其中，第一指示可以由第一设备发送给第二设备，或者，该第一指示也可以由验证服务器发送给第二设备。作为另一个示例，第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以在确定满足预设条件时，生成所述完整性度量值。其中，预设条件包括下述至少一种：条件一、接收到的第一数据的总长度达到预设长度阈值；条件二、接收到的第一数据包含的表项的数量达到预设数量阈值；条件三、接收第一数据的累计时长达到预设时长；或者，条件四、第一数据为增量数据。如此，第二设备可以被触发计算第一数据对应的完整性度量值并向验证服务器发送该完整性度量值，以便验证服务器对第一数据的完整性进行校验。

第二方面，本申请实施例还提供了一种完整性校验方法，该方法应用于第一设备，该方法例如可以包括：第一设备向第二设备发送第一数据后，第一设备向验证服务器发送第一数据对应的完整性度量基线值，该完整性度量基线值用于对第一数据的进行完整性校验。其中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

作为一个示例，第一数据可以包括下述至少一个：SR TE 配置信息、SR TE-policy 配置信息、ACL 配置信息或 FlowSpec 配置信息。

其中，完整性度量基线值可以为经过哈希计算得到的哈希值，或者，完整性度量基线值也可以为数字签名，又或者，完整性度量基线值还可以为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据。

在一种可能的实现方式中，在第一设备向验证服务器发送第一数据的完整性度量基线值之前，第一设备还可以计算第一数据对应的完整性度量基线值。作为一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的全部内容确定所述完整性度量基线值。作为另一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的部分内容确定所述完整性度量基线值。作为又一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据发送第一数据对应的第一操作日志确定所述完整性度量基线值。

在一种可能的实现方式中，第一设备可以向第二设备发送第一指示，该第一指示用于指示第二设备对第一数据进行完整性校验。其中，第一指示可以是第一设备直接发送给第二设备的，或者，该第一指示也可以是第一设备经过验证服务器发送给第二设备的。

需要说明的是，第二方面提供的方法中，第一设备可以是第一方面提供的方法中的第一设备，所以，第二方面提供的方法的具体实现方式以及达到的效果，可以参见第一方面的相关说明。

第三方面，本申请实施例还提供了一种完整性校验方法，该方法应用于第二设备，该方法例如可以包括：第二设备接收第一设备发送的第一数据后，该第二设备向验证服务器发送所述第一数据对应的完整性度量值，该完整性度量值用于对第一数据的进行完整性校验。

其中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

作为一个示例，第一数据可以包括下述至少一个：SR TE 配置信息、SR TE-policy 配置信息、ACL 配置信息或 FlowSpec 配置信息。

其中， 完整性度量值可以为经过哈希计算得到的哈希值，或者，完整性度量值也可以为数字签名，又或者，完整性度量值还可以为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据。

在一种可能的实现方式中，在第二设备向验证服务器发送第一数据的完整性度量值之前，第二设备还可以计算第一数据对应的完整性度量值。作为一个示例，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的全部内容确定完整性度量值。作为另一个示例，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的部分内容确定完整性度量值。作为又一个示例，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据接收所述第一数据对应的第二操作日志确定所述完整性度量值。

在一种可能的实现方式中，第二设备向验证服务器发送第一数据对应的完整性度量值，可以是基于所接收的第一指示触发的，也可以是满足本地预设条件后触发的。作为一个示例，在第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以接收第一指示，该第一指示用于指示第二设备对第一数据进行完整性校验。其中，第一指示可以由第一设备发送给第二设备，或者，该第一指示也可以由验证服务器发送给第二设备。作为另一个示例，第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以在确定满足预设条件时，生成所述完整性度量值。其中，预设条件包括下述至少一种：条件一、接收到的第一数据的总长度达到预设长度阈值；条件二、接收到的第一数据包含的表项的数量达到预设数量阈值；条件三、接收第一数据的累计时长达到预设时长；或者，条件四、第一数据为增量数据。如此，第二设备可以被触发计算第一数据对应的完整性度量值并向验证服务器发送该完整性度量值，以便验证服务器对第一数据的完整性进行校验。

需要说明的是，第三方面提供的方法中，第二设备可以是第一方面提供的方法中的第二设备，所以，第三方面提供的方法的具体实现方式以及达到的效果，可以参见第一方面的相关说明。

第四方面，本申请实施例还提供了一种完整性校验方法，该方法应用于验证服务器，

该方法例如可以包括：验证服务器接收第一设备发送的第一数据对应的完整性度量基线值和第二设备发送的第一数据对应的完整性度量值，该第一数据由第一设备发送给第二设备，那么，验证服务器根据完整性度量基线值和完整性度量值，对该第一数据的进行完整性校验。

其中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

作为一个示例，第一数据可以包括下述至少一个：SR TE 配置信息、SR TE-policy 配置信息、ACL 配置信息或 FlowSpec 配置信息。

其中，完整性度量基线值可以为经过哈希计算得到的哈希值，那么， 完整性度量值为经过哈希计算得到的哈希值。或者，完整性度量基线值也可以为数字签名，那么，完整性度量值为数字签名。又或者，完整性度量基线值还可以为经过加密处理得到的加密值，那么，完整性度量值为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据。

在一种可能的实现方式中，第二设备向验证服务器发送第一数据对应的完整性度量值，可以是基于所接收的指示触发的。作为一个示例，验证服务器可以接收第一设备发送的第一指示，该第一指示用于指示验证服务器对第一数据进行完整性校验。那么，响应于所述第一指示，验证服务器还可以向第二设备发送第二指示，该第二指示用于指示对第一数据进行完整性验证。这样，第二设备即可基于第二指示计算并向验证服务器发送第一数据对应的完整性度量值。

在一些可能的实现方式中，验证服务器根据完整性度量基线值和完整性度量值对第一数据的进行完整性校验，可以包括：验证服务器确定完整性度量值和完整性度量基线值匹配，从而，验证服务器确定对第一数据的完整性校验通过。

作为一个示例，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一哈希算法计算得到的第一哈希值，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第一哈希算法计算得到的第二哈希值，那么，验证服务器可以判断第一哈希值和第二哈希值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。

作为又一个示例，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一私钥对第一哈希值进行签名操作得到的第一签名，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第二私钥对第二哈希值进行签名操作得到的第二签名，那么，一种情况下，验证服务器可以先判断第一私钥对应的第一公钥和第二私钥对应的第二公钥是否相同，如果相同，再判断第一签名和第二签名是否一致，如果一致，则，确定

对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过；另一种情况下，验证服务器可以先采用第一私钥对应的第一公钥对第一签名进行处理得到第一还哈希值，采用第二私钥对应的第二公钥对第二签名进行处理得到第二哈希值，再判断第一哈希值和第二哈希值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。其中，第一公钥可以是控制管理设备对应的第一私钥对应的公钥，该公钥可以预先保存在验证服务器本地，也可以是控制管理设备向验证服务器发送第一数据的完整性度量基线值时发送给验证服务器的。同理，第二公钥可以是终端设备对应的第二私钥对应的公钥，该公钥可以预先保存在验证服务器本地，也可以是终端设备向验证服务器发送第一数据的完整性度量值时发送给验证服务器的。

作为再一个示例，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一加密算法计算得到的第一加密值，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第一加密算法计算得到的第二加密值，那么，一种情况下，验证服务器可以判断第一加密值和第二加密值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过；另一种情况下，验证服务器也可以先采用第一加密算法对应的第一解密算法对第一加密值进行解密得到第一解密值，采用第一加密算法对应的第一解密算法对第二加密值进行解密得到第二解密值再判断第一解密值和第二解密值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。

当对第一数据的完整性校验未通过时，为了让控制管理设备感知到该控制管理设备和终端设备之间关于第一数据的一致性问题，验证服务器可以向控制管理设备发送告警消息，用于告知该终端设备上的第一数据存在异常。当控制管理设备接收到告警消息后，为了确保终端设备能够继续正常运行，还可以重新向终端设备发送第一数据，指示终端设备用新接收的第一数据替换本地保存的第一数据，或者，指示终端设备保存新接收的第一数据并将之前保存的第一数据添加老化标记，添加老化标记的第一数据不能再指导该终端设备对报文的处理，而是以新接收的第一数据指导该终端设备对报文进行处理。

需要说明的是，第四方面提供的方法中，验证服务器可以是第一方面提供的方法中的验证服务器，所以，第四方面提供的方法的具体实现方式以及达到的效果，可以参见第一方面的相关说明。

需要说明的是，对于批量发送的数据，为了确保安全和准确的校验，可以是周期性执行完整性校验；对于增量发送的数据，可以即时对增量数据进行完整性校验。

第五方面，本申请还提供了网络系统，包括第一设备、第二设备和验证服务器。其中，第一设备用于执行上述第二方面或第二方面任意一种可能的实现方式提供的方法，或者，执行第一方面、第一方面任意一种可能的实现方式提供的方法中第一设备所执行的操作；第二设备用于执行上述第三方面或第三方面任意一种可能的实现方式提供的方法，或者，执行第一方面、第一方面任意一种可能的实现方式提供的方法中第二设备所执行的操作；验证服务器用于执行上述第四方面或第四方面任意一种可能的实现方式提供的方法，或者，

执行第一方面、第一方面任意一种可能的实现方式提供的方法中验证服务器所执行的操作。

第六方面，本申请实施例还提供了一种第一设备，包括收发单元和处理单元。其中，收发单元用于执行上述第一方面、第一方面任意一种可能的实现方式、第二方面或第二方面任意一种可能的实现方式提供的方法中所述第一设备所执行的收发操作；处理单元用于执行上述第一方面、第一方面任意一种可能的实现方式、第二方面或第二方面任意一种可能的实现方式提供的方法中所述第一设备所执行的除了收发操作以外的其他操作。例如：当所述第一设备执行所述第二方面所述的方法时，所述收发单元用于向第二设备发送第一数据，以及向验证服务器发送所述第一数据对应的完整性度量基线值；所述处理单元用于根据所述第一数据的全部内容确定所述完整性度量基线值。

第七方面，本申请实施例还提供了一种第二设备，包括收发单元和处理单元。其中，收发单元用于执行上述第一方面、第一方面任意一种可能的实现方式、第三方面或第三方面任意一种可能的实现方式提供的方法中所述第二设备所执行的收发操作；处理单元用于执行上述第一方面、第一方面任意一种可能的实现方式、第三方面或第三方面任意一种可能的实现方式提供的方法中所述第二设备所执行的除了收发操作以外的其他操作。例如：当所述第二设备执行所述第三方面所述的方法时，所述收发单元用于接收第一设备发送的第一数据，以及向验证服务器发送所述第一数据对应的完整性度量值；所述处理单元用于根据所述第一数据的全部内容确定所述完整性度量值。

第八方面，本申请实施例还提供了一种验证服务器，包括收发单元和处理单元。其中，收发单元用于执行上述第一方面、第一方面任意一种可能的实现方式、第四方面或第四方面任意一种可能的实现方式提供的方法中所述验证服务器所执行的收发操作；处理单元用于执行上述第一方面、第一方面任意一种可能的实现方式、第四方面或第四方面任意一种可能的实现方式提供的方法中所述验证服务器所执行的除了收发操作以外的其他操作。例如：当所述验证服务器执行所述第四方面所述的方法时，所述收发单元用于接收第一设备发送的第一数据对应的完整性度量基线值，以及接收所述第二设备发送的所述第一数据对应的完整性度量值；所述处理单元用于根据所述完整性度量基线值和所述完整性度量值，对所述第一数据的进行完整性校验。

第九方面，本申请实施例还提供了一种第一设备，包括第一通信接口和处理器。其中，第一通信接口用于执行前述第一方面、第一方面任意一种可能的实现方式、第二方面或第二方面任意一种可能的实现方式提供的方法中所述第一设备所执行的发送操作；处理器，用于执行前述第一方面、第一方面任意一种可能的实现方式、第二方面或第二方面任意一种可能的实现方式提供的方法中所述第一设备所执行的除所述接收和发送操作以外的其他操作。该第一设备还可以包括第二通信接口，第二通信接口用于执行前述第一设备的接收操作。

第十方面，本申请实施例还提供了一种第二设备，包括第一通信接口和第二通信接口。其中，第一通信接口用于执行前述第一方面、第一方面任意一种可能的实现方式、第三方面或第三方面任意一种可能的实现方式提供的方法中所述第二设备所执行的发送操作，第二通信接口用于执行前述第一方面、第一方面任意一种可能的实现方式、第三方面或第三

方面任意一种可能的实现方式提供的方法中所述第二设备所执行的接收操作。此外，该第二设备还可以包括处理器，用于执行前述第一方面、第一方面任意一种可能的实现方式、第三方面或第三方面任意一种可能的实现方式提供的方法中所述第二设备所执行的除所述接收和发送操作以外的其他操作。

第十一方面，本申请实施例还提供了一种验证服务器，包括第一通信接口和处理器。其中，第一通信接口用于执行前述第一方面、第一方面任意一种可能的实现方式、第四方面或第四方面任意一种可能的实现方式提供的方法中所述验证服务器所执行的接收操作；处理器，用于执行前述第一方面、第一方面任意一种可能的实现方式、第四方面或第四方面任意一种可能的实现方式提供的方法中所述验证服务器所执行的除所述接收和发送操作以外的其他操作。该验证服务器还可以包括第二通信接口，第二通信接口用于执行前述第一设备的发送操作。

第十二方面，本申请实施例还提供了一种第一设备，该第一设备包括存储器和处理器。其中，该存储器包括计算机可读指令；与该存储器通信的处理器用于执行所述计算机可读指令，使得所述第一设备用于执行以上第一方面、第一方面任意一种可能的实现方式、第二方面或第二方面任意一种可能的实现方式提供的方法中所述第一设备对应的部分。

第十三方面，本申请实施例还提供了一种第二设备，该第二设备包括存储器和处理器。其中，该存储器包括计算机可读指令；与该存储器通信的处理器用于执行所述计算机可读指令，使得所述第二设备用于执行以上第一方面、第一方面任意一种可能的实现方式、第三方面或第三方面任意一种可能的实现方式提供的方法中所述第二设备对应的部分。

第十四方面，本申请实施例还提供了一种验证服务器，该验证服务器包括存储器和处理器。其中，该存储器包括计算机可读指令；与该存储器通信的处理器用于执行所述计算机可读指令，使得所述验证服务器用于执行以上第一方面、第一方面任意一种可能的实现方式、第四方面或第四方面任意一种可能的实现方式提供的方法中所述验证服务器对应的部分。

第十五方面，本申请实施例还提供了一种通信系统，该通信系统包括：第六方面、第九方面或第十二方面提供的所述第一设备，第七方面、第十方面或第十三方面提供的所述第二设备，以及第八方面、第十一方面或第十四方面提供的验证服务器。

第十六方面，本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得所述计算机执行以上第一方面、第一方面任意一种可能的实现方式、第二方面、第二方面任意一种可能的实现方式、第三方面、第三方面任意一种可能的实现方式、第四方面或第四方面任意一种可能的实现方式提供的方法。

第十七方面，本申请实施例还提供了计算机程序产品，包括计算机程序或计算机可读指令，当所述计算机程序或所述计算机可读指令在计算机上运行时，使得计算机执行前述第一方面、第一方面任意一种可能的实现方式、第二方面、第二方面任意一种可能的实现方式、第三方面、第三方面任意一种可能的实现方式、第四方面或第四方面任意一种可能的实现方式提供的方法。

需要说明的是，上述实施例中的第一设备、第二设备以及验证服务器，可以是用于执行上述方法的网络设备，也可以是指用于执行上述方法的单板、线卡、芯片等。

附图说明

图 1 为本申请实施例所适用的网络 10 的结构示意图；

图 2 为本申请实施例中一种完整性校验方法 100 的流程示意图；

图 3 为本申请实施例中一种完整性校验方法 200 的流程示意图；

图 4 为本申请实施例中一种完整性校验方法 300 的流程示意图；

图 5 为本申请实施例中一种完整性校验方法 400 的流程示意图；

图 6 为本申请实施例中一种完整性校验方法 500 的流程示意图；

图 7 为本申请实施例中一种第一设备 300 的结构示意图；

图 8 为本申请实施例中一种第二设备 400 的结构示意图；

图 9 为本申请实施例中一种验证服务器 500 的结构示意图；

图 10 为本申请实施例中一种第一设备 600 的结构示意图；

图 11 为本申请实施例中一种第二设备 700 的结构示意图；

图 12 为本申请实施例中一种验证服务器 800 的结构示意图；

图 13 为本申请实施例中一种第一设备 900 的结构示意图；

图 14 为本申请实施例中一种第二设备 1000 的结构示意图；

图 15 为本申请实施例中一种验证服务器 1100 的结构示意图；

图 16 为本申请实施例中一种通信系统 1200 的结构示意图。

具体实施方式

下面将结合附图，对本申请实施例中的技术方案进行描述。本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

本申请中的“1”、“2”、“3”、“第一”、“第二”以及“第三”等序数词用于对多个对象进行区分，不用于限定多个对象的顺序。

本申请中提及的“A 和/或 B”，应该理解为包括以下情形：仅包括 A，仅包括 B，或者同时包括 A 和 B。

第一设备可以向第二设备发送数据，这些数据可以作为第二设备对报文等待传输数据的处理依据。为了确保第二设备上业务的正常运行，需要保证第二设备从第一设备接收到的数据和第一设备发送给第二设备的数据，即，需要对第二设备和第一设备上保存的数据进行校验。第一设备和第二设备可以是任意需要保持数据一致的设备，例如，第一设备可以是控制管理设备，第二设备可以是终端设备；又例如，第一设备可以是终端设备，第二设备可以是控制管理设备；再例如，第一设备和第二设备均可以是终端设备。本申请实施例中以第一设备为控制管理设备，第二设备为终端设备为例进行说明。

终端设备对待传输数据的处理，可以以控制管理设备发送的一些数据作为依据，这些数据例如可以包括分段路由流量工程（英文：Segment Routing Traffic Engineering，简称：SR TE）配置信息、分段路由流量工程的策略（英文：Segment Routing Traffic Engineering policy，简称：SR TE-policy）配置信息、访问控制列表（英文：Access Control Lists，简称：ACL）配置信息或流规则（英文：Flow Specification，简称：FlowSpec）配置信息等。终端设备接收控制管理设备发送的数据之后，如果这些数据在存储、使用等过程中发生错误或被篡改，会使得指导报文处理的数据与控制管理设备发送的数据不一致，导致终端设备对报文的处理不够可靠，影响业务的正常运行。基于此，为了保证业务的正常运行，需要确保终端设备从控制管理设备上接收的、指导报文处理的数据与控制管理设备向该终端设备发送的数据是一致的。

目前，通常由控制管理设备对账的方式对终端设备上的数据和控制管理设备上的数据的一致性进行校验。对账方式，可以是指终端设备定期将指导报文处理的数据发送给控制管理设备，由控制管理设备对所接收的数据和自身发送给该终端设备的对应数据进行比对，以确定该周期内终端设备上指导报文处理的数据是否还是可靠的。

举例来说，以图 1 所示的网络 10 为例，假设该网络 10 中至少可以包括：控制管理设备 100 和终端设备 200 和终端设备 300。其中，各终端设备至少具有报文的处理能力；控制管理设备 100 可以能够和各个终端设备进行数据交互，例如，向终端设备 200 和终端设备 300 分别发送用于指导报文处理的数据，实现对终端设备 200 和终端设备 300 的管控。需要说明的是，该网络 10 中包括的终端设备的数量在本申请实施例中不作具体限定，例如终端设备可以多于 2 个，即，除了上述终端设备 200 和终端设备 300 以外，还包括其他的终端设备；或者，网络 10 中包括的终端设备数量也可以小于 2。

作为一个示例，控制管理设备 100 向终端设备 200 发送数据 1，终端设备 200 可以保存该数据 1，并基于本地保存的数据 1 指导对报文的处理。假设预设的对账周期为 1 小时，那么，每隔 1 小时，终端设备 200 将本地保存的数据 1’（如果终端设备 200 上的数据未被篡改或未发生错误，则数据 1’与数据 1 相同）发送给控制管理设备 100，由控制管理设备 100 对本地保存的数据 1 和数据 1’进行比对，如果比对结果表示数据 1 和数据 1’一致，则，确定该周期内终端设备 200 对从控制管理设备 100 接收的数据 1 没有进行篡改也没有发生错误，终端设备 200 在该周期内可靠，即，终端设备 200 在该周期内基于数据 1’进行报文的处理能够确保业务的正常运行；反之，如果比对结果表示数据 1 和数据 1’不一致，则，确定该周期内终端设备 200 对从控制管理设备 100 接收的数据 1 进行了篡改或发生了错误，此时，终端设备 200 在该周期内基于数据 1’进行报文的处理无法保证业务的正常运行。

但是，上述由控制管理设备对账的方式实现终端设备上的数据和控制管理设备上的数据的校验，一方面，终端设备需要每个周期均将本地保存的、来自控制管理设备的全量数据上报给控制管理设备，每次交互的数据量大且交互频繁，占用了较多的资源；另一方面，通过全量数据的对比进行校验，校验结果不够安全和可靠。

基于此，本申请实施例提供了一种完整性校验方法，引入可信的验证服务器对控制管

理设备向终端设备发送的数据进行远程完整性校验，过程例如可以包括：控制管理设备向终端设备发送第一数据后，该控制管理设备生成并向验证服务器发送该第一数据对应的完整性度量基线值；接收第一数据的终端设备也可以生成并向该验证服务器发送第一数据对应的完整性度量值；该可信的验证服务器即可对来自终端设备的完整性度量值和来自控制管理设备的完整性度量基线值，对该第一数据进行完整性校验。当对第一数据的完整性校验通过时，表明该终端设备上保存的第一数据和控制管理设备上保存的第一数据一致；否则，当对第一数据的完整性校验不通过时，表明该终端设备上保存的第一数据和控制管理设备上保存的第一数据不一致。如此，由可信的验证服务器对终端设备和控制管理设备分别发送的相同的第一数据对应的完整性度量值和完整性度量基线值进行完整性校验，需要交互的仅是第一数据对应的完整性度量值和完整性度量基线值，无需交互全量的第一数据，有效的减少了校验所需交互的数据量，大大的节约了校验过程所占用的资源，而且，通过引入可信的验证服务器，由验证服务器对完整性度量值和完整性度量基线值进行完整性校验，而不是由控制管理设备直接对第一数据进行比对，能够确保该校验过程更加安全和可靠，从而为终端设备上业务的正常运行提供了保障。

仍然以图 1 所示的网络 10 为例，该网络 10 还可以包括验证服务器 400，该验证服务器 400 能够和控制管理设备 100 以及各终端设备进行数据交互，且用于对控制管理设备 100 和各终端设备进行本申请实施例提供的完整性校验的过程例如可以包括：S11，控制管理设备 100 向终端设备 200 发送数据 a；S12，控制管理设备 100 根据私钥 1 生成数据 a 对应的签名 1，并将作为数据 a 对应的完整性度量基线值的签名 1 向验证服务器 400 发送；S13，终端设备 200 根据私钥 2 生成数据 a 对应的签名 2，并将作为数据 a 对应的完整性度量值的签名 2 向验证服务器 400 发送；S14，验证服务器 400 根据公钥 1 对接收的签名 1 进行处理，得到摘要 1，根据公钥 2 对接收的签名 2 进行处理，得到摘要 2，其中，公钥 1 与私钥 1 对应，公钥 2 与私钥 2 对应；S15，验证服务器 400 判断摘要 1 和摘要 2 是否一致，如果一致，则表示对该数据 a 的完整性校验通过；如果不一致，则表示对该数据 a 的完整性校验未通过。如果验证服务器 400 确定该数据 a 的完整性校验未通过，则，还可以向控制管理设备 100 发送告警消息，用于告知终端设备 200 上的数据 a 存在异常，以便控制管理设备 100 可以基于稿告警消息的指示，重新向终端设备 200 发送该数据 a；从而，终端设备 200 可以用新接收到的数据 a 替换本地保存的数据 a，以提供更加可靠的报文处理功能。

可以理解的是，上述场景仅是本申请实施例提供的一个场景示例，本申请实施例并不限于此场景。

本申请实施例中，终端设备，是指能够实现对待传输数据处理功能的任意设备，例如，可以是交换机、路由器等网络设备，又例如，也可以手机、电脑等用户设备。控制管理设备，是指对终端设备具有管理和/或控制功能的任意设备，例如，可以是网络云化引擎（英文：Network Cloud Engine，简称：NCE）、服务器、网管或者路由器等；或者，控制管理实体也可以是任意一个设备内集成的功能实体，该功能实体可以通过硬件形式体现也可以通过软件形式体现，例如，也可以是设备内的 Telnet（一种应用层协议）控制台或安全外壳协议（英文：Secure Shell Protocol，简称：SSH）控制台，其中，Telnet 控制台可以使用

于互联网及局域网中，使用虚拟终端的形式提供双向、以文字字符串为主的命令行接口交互功能；SSH 控制台是一种建立在应用层和传输层基于上的安全协议。验证服务器可以是可信的远程证明服务器，该验证服务器可以和控制管理设备合设于同一实体设备，作为该实体设备中两个功能单元；或者，该验证服务器也可以是一个独立的、可信的第三方实体设备，例如可以是证书授权（英文：Certificate Authority，简称：CA）服务器。需要说明的是，本申请实施例中的各种设备，在本申请实施例中不作具体限定。

下面结合附图，通过实施例来详细说明本申请实施例中一种完整性校验方法的具体实现方式。

图 2 为本申请实施例中一种完整性校验方法 100 的流程示意图。该方法 100 以终端设备、控制管理设备和验证服务器三者之间的交互进行说明，其中，终端设备可以是图 1 中的终端设备 200 或终端设备 300，控制管理设备可以是图 1 中的控制管理设备 100，验证服务器可以是图 1 中的验证服务器 400。参见图 2，该方法 100 例如可以包括下述 S101~S106：

S101，控制管理设备向终端设备发送第一数据。

第一数据可以为控制管理设备向终端设备发送的任何数据。该第一数据可以被终端设备直接或间接的用于指导报文的处理。例如，第一数据可以包括下述类型的数据中至少一种：SR TE 配置信息、SR TE-policy 配置信息、ACL 配置信息或 FlowSpec 配置信息。

如果第一数据包括 SR TE 配置信息，一种情况下，S101 例如可以是：控制管理设备向终端设备发送路径计算单元通信协议（英文：Path Computation Element Communication Protocol，简称：PCEP）报文，该 PCEP 报文中携带 SR TE 配置信息可以包括对应的 SR 标签。另一种情况下，S101 例如可以是：控制管理设备向终端设备发送网络配置协议（英文：Network Configuration Protocol，简称：NETCONF）报文或 YANG 模型报文，该 NETCONF 报文或 YANG 模型报文中携带的 SR TE 配置信息可以包括对应的 SR 标签。该场景中，第一数据中对应的 SR 标签，与多协议标签交换（英文：Multi-Protocol Label Switching，简称：MPLS）TE 场景中的 MPLS 标签类似，本申请实施例不再赘述。

如果第一数据包括 SR TE-policy 配置信息，一种情况下，S101 例如可以是：控制管理设备向终端设备静态下发命令行，命令行中携带 SR TE-policy 配置信息；另一种情况下，S101 例如可以是：控制管理设备向终端设备发送边界网关协议（英文：Border Gateway Protocol，简称：BGP）报文，该 BGP 报文中可以携带 SR TE-policy 配置信息。其中，SR TE-policy 配置信息可以包括：三元组标识、至少一条候选路径（英文：Candidate Path）、各候选路径的优先级（英文：Preference）属性、各候选路径下至少一个权重（英文：Weight）和该权重对应的段标识列表（英文：Segment Identification List，简称：SID List），三元组标识用于唯一标识 SR TE-policy 配置信息，例如，三元组标识可以包括：头端（英文：Headend），用于指示 SR TE-policy 生成或实现的节点；颜色（英文：Color），用于区分同一头端和尾端之间的多条 SR TE-policy；尾端（英文：Endpoint），用于指示 SR Policy 的尾端，可以是一个第四版互联网协议（英文：Internet Protocol version 4，简称：IPv4）地址或第六版互联网协议（英文：Internet Protocol version 6，简称：IPv6）地址。候选路径（英文：Candidate Path）可以由发起协议（英文：protocol-origin），发起者标识（originator）以及鉴

别器（英文：discriminator）唯一标识。例如，SR TE-policy 配置信息具体形式可以如下：

SR policy POL1 <headend, color, endpoint> //POL1 的 SR policy 的名称和标识

Candidate-path CP1 <protocol-origin, originator, discriminator> //该 SR policy 的候选路径 CP1

Preference 200 //CP 1 对应的候选路径的优先级属性为 200

weight W1, SID-List1 <SID11...SID1i> //权重为 W1 的 SID List

weight W2, SID-List2 <SID21...SID2j> //权重为 W2 的 SID List

Candidate-path CP2 <protocol-origin, originator, discriminator> //该 SR policy 的候选路径 CP2

Preference 100 //CP 2 对应的候选路径的优先级属性为 100

weight W3, SID-List3 <SID31...SID3i> //权重为 W3 的 SID List

weight W4, SID-List4 <SID41...SID4j> //权重为 W4 的 SID List

其中，每个 SID List 中均可以包括对应的多个 SID，每个 SID 可以为一个节点对应的 SR 标签。

如果第一数据包括 ACL 配置信息，一种情况下，S101 例如可以是：S101 例如可以是：控制管理设备向终端设备静态下发命令行，命令行中携带 ACL 配置信息。另一种情况下，S101 例如可以是：控制管理设备向终端设备发送 NETCONF 报文或 YANG 模型报文，该 NETCONF 报文或 YANG 模型报文中携带 ACL 配置信息。

如果第一数据包括 FlowSpec 配置信息，那么，S101 例如可以是：控制管理设备向终端设备发送 BGP 报文，该 BGP 报文中可以携带 FlowSpec 配置信息。

需要说明的是，上述四种可能的数据类型仅是举例说明，本申请实施例中的第一数据还可以是其他的表项或配置信息，不作具体限定。

对于控制管理设备，S101 之后可以保存该第一数据。对于终端设备，S101 之后不仅可以基于第一数据生成用于指导报文处理的表项，而且可以保存该第一数据。终端设备上用于指导报文处理的表项可以和本地保存的第一数据匹配。而且，控制管理设备上保存的第一数据的顺序可以和终端设备上保存的第一数据的顺序一致，以保证对第一数据的完整性进行校验时不会因为保存数据的顺序而影响校验结果，例如，可以均按照字典序排序和保存，又例如，也可以均按照数据对应的时间戳排序和保存。

需要说明的是，在完整性校验时，要求终端设备和控制管理设备上的校验对象是相同的，即，终端设备上参与校验的数据和控制管理设备上参与校验的数据是相同的。作为一个示例，如果终端设备和控制管理设备保持时钟同步，则可以满足校验对象一致的要求。作为另一个示例，如果终端设备和控制管理设备未设置时钟同步的功能，那么，S101 中的第一数据还可以携带发送时间戳，这样，可以将发送时间戳相同的数据作为参与校验的数据，按照本申请实施例提供的完整性校验方法进行校验，也可以满足校验对象一致的要求。

S102，控制管理设备生成第一数据对应的完整性度量基线值，该完整性度量基线值用于对第一数据的进行完整性校验。

S103，控制管理设备向验证服务器发送该第一数据对应的完整性度量基线值。

其中，第一数据对应的完整性度量基线值，可以作为验证服务器对该第一数据的完整性验证的基准值，将第一数据对应的完整性度量值与该完整性度量基线值进行匹配，如果与该完整性度量基线值匹配，则，确定该第一数据的完整性校验通过，否则，确定该第一数据的完整性校验不通过。该第一数据对应的完整性度量基线值例如可以为：经过哈希计算得到的哈希值、数字签名或经过加密处理得到的加密值。

在一些可能的实现方式中，S102 可以是控制管理设备根据第一数据生成该第一数据对应的完整性度量基线值。

作为一个示例，控制管理设备可以根据第一数据的全部内容确定第一数据对应的完整性度量基线值。例如，控制管理设备可以将本地保存的第一数据的全部内容经过哈希计算得到的哈希值，并将所得的该哈希值作为第一数据对应的完整性度量基线值；又例如，控制管理设备也可以将本地保存的第一数据的全部内容进行数字签名操作得到签名，并将所得的该签名作为第一数据对应的完整性度量基线值；再例如，控制管理设备可以将本地保存的第一数据的全部内容经过加密处理得到的加密值，并将所得的该加密值作为第一数据对应的完整性度量基线值。

作为另一个示例，控制管理设备可以根据第一数据的部分内容确定该第一数据对应的完整性度量基线值。其中，所述第一数据的部分内容可以是第一数据中参与校验的数据，S102 例如可以包括：控制管理设备基于预设规则从第一数据中确定所述第一数据的部分内容，从而，根据所确定的所述第一数据的部分内容确定该第一数据对应的完整性度量基线值，预设规则可以根据实际需求进行灵活设置，例如，可以为第一数据中的每个内容设置对应的权重并设置权重阈值，那么，预设规则可以包括：选择权重不小于所述权重阈值的内容，并将选中内容按照本地保存的顺序（或权重的大小顺序）排序后得到所述第一数据的部分内容；又例如，预设规则可以包括：选择某些预设位置的内容，并将选中内容按照本地保存的顺序（或权重的大小顺序）排序后得到所述第一数据的部分内容。该示例下，S102 的实现方式可以包括但不限于：方式一，控制管理设备可以将本地保存的第一数据的部分内容经过哈希计算得到的哈希值，并将所得的该哈希值作为第一数据对应的完整性度量基线值；方式二，控制管理设备也可以将本地保存的第一数据的部分内容进行数字签名操作得到签名，并将所得的该签名作为第一数据对应的完整性度量基线值；再例如，控制管理设备可以将本地保存的第一数据的部分内容经过加密处理得到的加密值，并将所得的该加密值作为第一数据对应的完整性度量基线值。

在一些可能的实现方式中，S102 可以是控制管理设备根据发送第一数据对应的第一操作日志生成该第一数据对应的完整性度量基线值。需要说明的是，控制管理设备为了记录自身执行的操作，控制管理设备可以将每次向终端设备发送数据的行为记录在第一操作日志中，作为该第一操作日志的一条内容。如果第一数据仅是控制管理设备向终端设备执行的一次发送数据的行为，则，控制管理设备可以根据第一操作日志中与发送该第一数据对应的一条内容确定第一数据对应的完整性度量基线值。如果第一数据包括控制管理设备向终端设备执行的多次发送数据的行为，则，控制管理设备可以根据第一操作日志中发送该第一数据对应的多条内容的全部确定第一数据对应的完整性度量基线值；或者，控制管理

设备也可以根据第一操作日志中发送该第一数据对应的多条内容的部分确定第一数据对应的完整性度量基线值，其中，多条内容中的部分例如可以是所述多条内容中某种操作类型对应的内容，操作类型可以包括增加、删除和修改等，或者，多条内容中的部分例如也可以是所述多条内容中生成时间相隔预设时长对应的内容。其中，该完整性度量基线值，例如可以是经过哈希计算得到的哈希值、经过数字签名操作得到签名或者经过加密处理得到的加密值。

具体实现时，对于S102执行的时机，一种情况下，可以是在网络部署初期，控制管理设备批量向终端设备发送数据时，控制管理设备执行该方法100对批量发送的第一数据进行完整性校验；另一种情况下，可以终端设备运行的过程中，控制管理设备在有需求时向终端设备发送数据时，控制管理设备执行该方法100对增量发送的第一数据进行完整性校验。其中，批量发送的数据也可以称为基本数据，是终端设备运行必备的数据；增量发送的数据，可以是指在批量发送的数据发送完成之后，超过预设时长（如1分钟）又发送的数据。需要说明的是，控制管理设备向终端设备发送增量数据，例如可以是该终端设备的远端设备的路由信息发生变化。

该实现方式中，第一操作日志中可以保存操作类型和操作数据。如果第一数据是批量发送的数据，则，既可以根据第一数据的全部或部分内容生成第一数据对应的完整性度量基线值，也可以根据发送第一数据对应的第一操作日志生成第一数据对应的完整性度量基线值。如果第一数据是增量数据，则，可以优选根据发送第一数据对应的第一操作日志生成第一数据对应的完整性度量基线值。

在S102之后或S102执行的同时，控制管理设备还可以直接或间接的向终端设备发送第一指示，该第一指示用于指示终端设备对第一数据进行完整性校验，该第一指示可以作为下述S104执行的一种可能的触发条件。其中，控制管理设备可以间接的向终端设备发送第一指示，例如可以是：控制管理设备通过验证服务器向终端设备发送所述第一指示。控制管理设备可以将第一指示携带在任何报文中向终端设备发送，只要该报文为终端设备可以识别并处理的报文类型即可。

对于S103，控制管理设备可以将第一数据对应的完整性度量基线值携带在任何报文中向验证服务器发送，例如，控制管理设备可以将第一数据对应的完整性度量基线值携带在BGP报文中发送给验证服务器，又例如，控制管理设备可以将第一数据对应的完整性度量基线值携带在PCEP报文中发送给验证服务器。本申请实施例对携带第一数据的完整性度量基线值的报文类型不作具体限定，只要是验证服务器能够识别并处理的报文即可。

作为一个示例，为了更加安全和可信的完成该完整性校验，控制管理设备还可以将该第一数据的完整性度量基线值携带在证书中，并将该证书发送给验证服务器。

需要说明的是，经过上述S102~S103，为后续验证服务器对第一数据的完整性校验提供了校验的标准，使得完成可靠、安全和准确的完整性校验成为了可能。

需要说明的是，上述S101~S103，可以单独作为控制管理设备执行的一个完整的实施例，该方法100只是为了方便描述，从终端设备、控制管理设备和验证服务器三者的交互作为一个整体进行说明。

S104，终端设备生成第一数据对应的完整性度量值，该完整性度量值用于对第一数据的进行完整性校验。

S105，终端设备向验证服务器发送第一数据对应的完整性度量值。

其中，第一数据对应的完整性度量值，可以作为参与完整性校验的一个待校验值，将该第一数据对应的完整性度量值与该第一数据对应的完整性度量基线值进行匹配，如果与完整性度量基线值匹配，则，确定该第一数据的完整性度量值通过了完整性校验，即，第一数据的完整性校验通过，否则，确定该第一数据的完整性度量值未通过完整性校验，即，第一数据的完整性校验未通过。该第一数据对应的完整性度量值例如可以为：经过哈希计算得到的哈希值、数字签名或经过加密处理得到的加密值。

在一些可能的实现方式中，如果 S102 中是控制管理设备根据第一数据生成第一数据对应的完整性度量基线值，那么，S104 可以是终端设备根据第一数据生成该第一数据对应的完整性度量值。

作为一个示例，如果 S102 是控制管理设备根据第一数据的全部内容确定第一数据对应的完整性度量基线值，那么，S104 也可以是终端设备根据第一数据的全部内容确定第一数据对应的完整性度量值。例如，终端设备可以将本地保存的第一数据的全部内容经过哈希计算得到的哈希值，并将所得的该哈希值作为第一数据对应的完整性度量值；又例如，终端设备也可以将本地保存的第一数据的全部内容进行数字签名操作得到签名，并将所得的该签名作为第一数据对应的完整性度量值；再例如，终端设备可以将本地保存的第一数据的全部内容经过加密处理得到的加密值，并将所得的该加密值作为第一数据对应的完整性度量值。

作为另一个示例，如果 S102 是控制管理设备根据第一数据的部分内容确定该第一数据对应的完整性度量基线值，那么，S104 也可以是终端设备根据第一数据的部分内容确定第一数据对应的完整性度量值。其中，所述第一数据的部分内容可以是第一数据中参与校验的数据，S104 例如可以包括：终端设备基于预设规则从第一数据中确定所述第一数据的部分内容，从而，根据所确定的所述第一数据的部分内容确定该第一数据对应的完整性度量值，该预设规则可以与 S102 中选择第一数据的部分内容所遵循的预设规则一致。该示例下，S104 的实现方式可以包括但不限于：方式一，终端设备可以将本地保存的第一数据的部分内容经过哈希计算得到的哈希值，并将所得的该哈希值作为第一数据对应的完整性度量值；方式二，终端设备也可以将本地保存的第一数据的部分内容进行数字签名操作得到签名，并将所得的该签名作为第一数据对应的完整性度量值；再例如，终端设备可以将本地保存的第一数据的部分内容经过加密处理得到的加密值，并将所得的该加密值作为第一数据对应的完整性度量值。

在一些可能的实现方式中，如果 S102 中是控制管理设备根据发送第一数据对应的第一操作日志生成该第一数据对应的完整性度量基线值，那么，S104 中可以是终端设备根据接收第一数据对应的第二操作日志生成该第一数据对应的完整性度量值。需要说明的是，终端设备为了记录自身执行的操作，可以将每次从控制管理设备接收数据的行为记录在第二操作日志中，作为该第二操作日志的一条内容。如果第一数据仅是终端设备从控制管理设

备执行的一次接收数据的行为，则，终端设备可以根据第二操作日志中与接收该第一数据对应的一条内容确定第一数据对应的完整性度量值。如果第一数据包括终端设备从控制管理设备执行的多次接收数据的行为，则，终端设备可以根据第二操作日志中发送该第一数据对应的多条内容的全部确定第一数据对应的完整性度量值；或者，终端设备也可以根据第二操作日志中发送该第一数据对应的多条内容的部分确定第一数据对应的完整性度量值，其中，多条内容中的部分的选择规则可以与控制管理设备从第一操作日志的多条内容中选择部分的选择规则一致。其中，该完整性度量值，例如可以是经过哈希计算得到的哈希值、经过数字签名操作得到签名或者经过加密处理得到的加密值。

该实现方式中，第二操作日志中可以保存操作类型和操作数据。如果第一数据是批量发送的数据，则，既可以根据第一数据的全部或部分内容生成第一数据对应的完整性度量值，也可以根据接收第一数据对应的第二操作日志生成第一数据对应的完整性度量值。如果第一数据是增量数据，则，可以优选根据接收第一数据对应的第二操作日志生成第一数据对应的完整性度量值。

需要说明的是，S104 生成完整性度量值的方式需要与 S102 生成完整性度量基线值的方式对应，例如，S102 中控制管理设备将本地保存的第一数据的全部内容经过哈希计算得到的哈希值，并将所得的该哈希值作为第一数据对应的完整性度量基线值，那么，S104 中终端设备将本地保存的第一数据的全部内容经过哈希计算得到的哈希值，并将所得的该哈希值作为第一数据对应的完整性度量值，这样，为后续验证服务器基于该对应的方式，准确的完成完整性校验提供了可能，如果终端设备生成完整性度量值的方式和控制管理设备生成完整性度量基线值的方式不对应，例如，S102 中控制管理设备将本地保存的第一数据的全部内容经过哈希计算得到的哈希值，并将所得的该哈希值作为第一数据对应的完整性度量基线值，而 S104 中终端设备将接收第一数据对应的第二操作日志经过数字签名操作得到签名，并将所得的该签名作为第一数据对应的完整性度量值，则，验证服务器很可能无法完成对第一数据的完整性校验。

具体实现时，对于 S104 执行的时机，一种情况下，可以在终端设备接收到用于指示对第一数据进行完整性校验的第一指示时，触发终端设备执行 S104，其中，第一指示可以是控制管理设备直接向终端设备发送的，或者，第一指示也可以是控制管理设备通过验证服务器间接的向终端设备发送的，或者，第一指示也可以是验证服务器接收到控制管理设备发送的校验请求或第一数据对应的完整性度量基线值时，生成并向终端设备发送的。另一种情况下，也可以在终端设备确定满足预设条件时，触发终端设备执行 S104，其中，预设条件可以是控制管理设备和终端设备约定好的执行该方法 100 以进行完整性校验的条件。

其中，预设条件例如可以是：接收到的所述第一数据的总长度达到预设长度阈值，如，终端设备从接收控制管理设备发送的第一个数据开始（或从某个时刻开始），记录从控制管理设备接收的数据的总长度，如果该总长度等于预设长度阈值，则，确定满足预设条件，触发执行 S104；同理，对于控制管理设备，从向终端设备发送的第一个数据开始（或从某个时刻开始），记录向终端设备发送的数据的总长度，如果该总长度等于预设长度阈值，则，确定满足预设条件，触发执行 S102；该情况下，第一数据的总长度可以为预设长度阈值。

或者，预设条件例如也可以是：接收到的所述第一数据包含的表项的数量达到预设数量阈值，如，终端设备从接收控制管理设备发送的第一个数据开始（或从某个时刻开始），记录从控制管理设备接收的数据包含表项的总数量，如果该总数量等于预设数量阈值，则，确定满足预设条件，触发执行 S104；同理，对于控制管理设备，从向终端设备发送的第一个数据开始（或从某个时刻开始），记录向终端设备发送的数据包含表项的总数量，如果该总数量等于预设数量阈值，则，确定满足预设条件，触发执行 S102；该情况下，第一数据包含的表项的总数量可以为预设数量阈值。又或者，预设条件例如也可以是：接收到的所述第一数据的累计时长达到预设时长，如，终端设备从接收控制管理设备发送的第一个数据开始（或从某个时刻开始），记录从控制管理设备接收的数据的累计时长，如果该累计时长等于预设时长，则，确定满足预设条件，触发执行 S104；同理，对于控制管理设备，从向终端设备发送的第一个数据开始（或从某个时刻开始），记录向终端设备发送的数据的累计时长，如果该累计时长等于预设时长，则，确定满足预设条件，触发执行 S102；该情况下，第一数据可以为预设时长内控制管理设备向终端设备发送的所有数据。再或者，预设条件例如也可以是：接收到的属性为增量数据的第一数据，如，在开始接收所述第一数据之前的预设时长内没有接收到控制管理设备发送的数据，那么，认为该第一数据为增量数据，则，确定满足预设条件，触发执行 S104；同理，对于控制管理设备，发送属性为增量数据的第一数据，如，在开始发送所述第一数据之前的预设时长内没有向终端设备发送数据，那么，认为该第一数据为增量数据，则，确定满足预设条件，触发执行 S102。

对于 S105，终端设备可以将第一数据对应的完整性度量值携带在任何报文中向验证服务器发送，例如，终端设备可以将第一数据对应的完整性度量值携带在 BGP 报文中发送给验证服务器，又例如，终端设备可以将第一数据对应的完整性度量值携带在 PCEP 报文中发送给验证服务器。本申请实施例对携带第一数据的完整性度量值的报文类型不作具体限定，只要是验证服务器能够识别并处理的报文即可。

作为一个示例，为了更加安全和可信的完成该完整性校验，终端设备还可以将该第一数据的完整性度量值携带在证书中，并将该证书发送给验证服务器。

需要说明的是，经过上述 S104~S105，为后续验证服务器对第一数据的完整性校验提供了校验的对象，使得完成可靠、安全和准确的完整性校验成为了可能。

需要说明的是，上述 S101、S104~S105，可以单独作为终端设备执行的一个完整的实施例，该方法 100 只是为了方便描述，从终端设备、控制管理设备和验证服务器三者的交互作为一个整体进行说明。

S106，验证服务器根据完整性度量值和完整性度量基线值，对第一数据进行完整性校验。

具体实现时，S106 例如可以包括：验证服务器确定完整性度量值和完整性度量基线值匹配，那么，该验证服务器确定对第一数据的完整性校验通过；反之，验证服务器确定完整性度量值和完整性度量基线值不匹配；那么，该验证服务器确定对第一数据的完整性校验未通过。

例如，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发

送第一数据对应的第一操作日志）经过第一哈希算法计算得到的第一哈希值，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第一哈希算法计算得到的第二哈希值，那么，S106 例如可以是验证服务器判断第一哈希值和第二哈希值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。

又例如，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一私钥对第一哈希值进行签名操作得到的第一签名，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第二私钥对第二哈希值进行签名操作得到的第二签名，那么，一种情况下，S106 中验证服务器可以先判断第一私钥对应的第一公钥和第二私钥对应的第二公钥是否相同，如果相同，再判断第一签名和第二签名是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过；另一种情况下，S106 中验证服务器可以先采用第一私钥对应的第一公钥对第一签名进行处理得到第一还哈希值，采用第二私钥对应的第二公钥对第二签名进行处理得到第二哈希值，再判断第一哈希值和第二哈希值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。其中，第一公钥可以是控制管理设备对应的第一私钥对应的公钥，该公钥可以预先保存在验证服务器本地，也可以是控制管理设备向验证服务器发送第一数据的完整性度量基线值时发送给验证服务器的。同理，第二公钥可以是终端设备对应的第二私钥对应的公钥，该公钥可以预先保存在验证服务器本地，也可以是终端设备向验证服务器发送第一数据的完整性度量值时发送给验证服务器的。

再例如，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一加密算法计算得到的第一加密值，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第一加密算法计算得到的第二加密值，那么，一种情况下，S106 例如可以是验证服务器判断第一加密值和第二加密值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过；另一种情况下，S106 例如可以是验证服务器先采用第一加密算法对应的第一解密算法对第一加密值进行解密得到第一解密值，采用第一加密算法对应的第一解密算法对第二加密值进行解密得到第二解密值再判断第一解密值和第二解密值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。

当对第一数据的完整性校验未通过时，为了让控制管理设备感知到该控制管理设备和终端设备之间关于第一数据的一致性问题，验证服务器可以向控制管理设备发送告警消息，用于告知该终端设备上的第一数据存在异常。当控制管理设备接收到告警消息后，为了确保终端设备能够继续正常运行，还可以重新向终端设备发送第一数据，指示终端设备用新接收的第一数据替换本地保存的第一数据，或者，指示终端设备保存新接收的第一数据并将之前保存的第一数据添加老化标记，添加老化标记的第一数据不能再指导该终端设备对报文的处理，而是以新接收的第一数据指导该终端设备对报文进行处理。

需要说明的是，对于批量发送的数据，为了确保安全和准确的校验，可以是周期性执行完整性校验；对于增量发送的数据，可以即时对增量数据进行完整性校验。

需要说明的是，上述 S103 对应的验证服务器接收控制管理设备发送的第一数据的完整性度量基线值、S105 对应的验证服务器接收终端设备发送的第一数据的完整性度量值以及该 S106，可以单独作为验证服务器执行的一个完整的实施例，该方法 100 只是为了方便描述，从终端设备、控制管理设备和验证服务器三者的交互作为一个整体进行说明。

可见，通过本申请实施例提供的方法 100，由可信的验证服务器对终端设备和控制管理设备分别发送的第一数据对应的完整性度量值和完整性度量基线值进行完整性校验，需要交互的仅是第一数据对应的完整性度量值和完整性度量基线值，无需交互全量的第一数据，有效的减少了校验所需交互的数据量，大大的节约了校验过程所占用的资源，而且，通过引入可信的验证服务器，由验证服务器根据第一数据对应的完整性度量值和完整性度量基线值即可完成对第一数据的完整性校验，而不是由控制管理设备直接对第一数据的全量数据进行比对，能够确保该校验过程更加安全和可靠，从而为终端设备上业务的正常运行提供了保障。

上述方法 100 以可信的验证服务器对控制管理设备向终端设备发送的第一数据的完整性校验为例进行说明，本申请实施例提供的方法还可以用于对终端设备向控制管理设备发送的第二数据的完整性校验，或者，用于对终端设备之间交互的第三数据的完整性校验，完整性校验的流程可以参见上述方法 100 中的相关描述。

本申请实施例提供了一种完整性校验方法 200，如图 3 所示，该方法 200 以交互的方式描述对第一数据的完整性校验。该方法 200 例如可以包括：

S201，第一设备向第二设备发送第一数据。

S202，第一设备向验证服务器发送该第一数据对应的完整性度量基线值。

S203，第二设备向验证服务器发送第一数据对应的完整性度量值。

S204，验证服务器根据完整性度量值和完整性度量基线值对第一数据进行完整性校验。

该方法 200 中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

以该方法 200 中的第一设备是控制管理设备且第二设备是终端设备为例，那么，该方法 200 中的第一设备可以是上述方法 100 中的控制管理设备，相关操作具体可以参见方法 100 中控制管理设备执行的操作；该方法 200 中的第二设备可以是上述方法 100 中的终端设备，相关操作具体可以参见方法 100 中终端设备执行的操作；该方法 200 中的验证服务器可以是上述方法 100 中的验证服务器，相关操作具体可以参见方法 100 中验证服务器执行的操作。具体而言，S201 的相关描述可以参见方法 100 中的 S101，S202 的相关描述可以参见方法 100 中的 S103，S203 的相关描述可以参见方法 100 中的 S105，S204 的相关描述可以参见方法 100 中的 S106。其中，第一数据可以是方法 100 中的第一数据，第一数据对应的完整性度量值可以是方法 100 中的第一数据对应的完整性度量值，第一数据对应的

完整性度量基线值可以是方法 100 中的第一数据对应的完整性度量基线值。

作为一个示例，第一数据可以包括下述至少一个：SR TE 配置信息、SR TE-policy 配置信息、ACL 配置信息或 FlowSpec 配置信息。

其中，完整性度量基线值可以为经过哈希计算得到的哈希值，那么， 完整性度量值为经过哈希计算得到的哈希值。或者，完整性度量基线值也可以为数字签名，那么，完整性度量值为数字签名。又或者，完整性度量基线值还可以为经过加密处理得到的加密值，那么，完整性度量值为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据，例如，第一设备待校验的数据为数据 a 和数据 b，第二设备待检验的数据也为数据 a 和数据 b。

在一种可能的实现方式中，在第一设备向验证服务器发送第一数据的完整性度量基线值之前，第一设备还可以计算第一数据对应的完整性度量基线值；在第二设备向验证服务器发送第一数据的完整性度量值之前，第二设备还可以计算第一数据对应的完整性度量值。

其中，以该方法 200 中的第一设备是控制管理设备且第二设备是终端设备为例，第一设备计算第一数据对应的完整性度量基线值可以参见方法 100 中的 S102 的相关说明，第二设备计算第一数据对应的完整性度量值可以参见方法 100 中的 S104 的相关说明。

作为一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的全部内容确定所述完整性度量基线值；那么，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的全部内容确定完整性度量值。其中，第一设备和第二设备上对第一数据按照相同的顺序保存，可以确保根据第一数据的全部内容计算的校验值是对应的，为完整性校验的准确执行提供了保障。

作为另一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的部分内容确定所述完整性度量基线值；那么，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的部分内容确定完整性度量值。其中，第一设备和第二设备上获取该第一数据的部分内容的规则相同，可以确保根据第一数据的部分内容计算的校验值是对应的，为完整性校验的准确执行提供了保障。

作为又一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据发送第一数据对应的第一操作日志确定所述完整性度量基线值；那么，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据接收所述第一数据对应的第二操作日志确定所述完整性度量值。其中，第一设备和第二设备上对接收和发送数据生成操作日志的规则可以相同，可以确保根据第一数据对应的第一操作日志和第二操作日志得到的校验值是对应的，为完整性校验的准确执行提供了保障。

在一种可能的实现方式中，第二设备向验证服务器发送第一数据对应的完整性度量值，可以是基于所接收的第一指示触发的，也可以是满足本地预设条件后触发的。

作为一个示例，在第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以接收第一指示，该第一指示用于指示第二设备对第一数据进行完整性校验。

其中，第一指示可以由第一设备发送给第二设备，或者，该第一指示也可以由验证服务器发送给第二设备。

作为另一个示例，第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以在确定满足预设条件时，生成所述完整性度量值。其中，预设条件包括下述至少一种：条件一、接收到的第一数据的总长度达到预设长度阈值；条件二、接收到的第一数据包含的表项的数量达到预设数量阈值；条件三、接收第一数据的累计时长达到预设时长；或者，条件四、第一数据为增量数据。如此，第二设备可以被触发计算第一数据对应的完整性度量值并向验证服务器发送该完整性度量值，以便验证服务器对第一数据的完整性进行校验。

需要说明的是，该方法200中，第一设备的相关描述以及达到的效果可以参见方法100中控制管理设备执行的相关操作和对应的效果描述，第二设备的相关描述以及达到的效果可以参见方法100中终端设备执行的相关操作和对应的效果描述，验证服务器的相关描述以及达到的效果可以参见方法100中验证服务器执行的相关操作和对应的效果描述。

本申请实施例还提供了一种完整性校验方法300，参见图4，该方法300应用于第一设备，该方法300例如可以包括：

S301，第一设备向第二设备发送第一数据。

S302，第一设备向验证服务器发送第一数据对应的完整性度量基线值，该完整性度量基线值用于对第一数据的进行完整性校验。

该方法300中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

以该方法300中的第一设备是控制管理设备且第二设备是终端设备为例，那么，该方法300中的第一设备可以是上述方法100中的控制管理设备，相关操作具体可以参见方法100中控制管理设备执行的操作。具体而言，S301的相关描述可以参见方法100中的S101，S302的相关描述可以参见方法100中的S103。其中，第一数据可以是方法100中的第一数据，第一数据对应的完整性度量基线值可以是方法100中的第一数据对应的完整性度量基线值。

作为一个示例，第一数据可以包括下述至少一个：SR TE配置信息、SR TE-policy配置信息、ACL配置信息或FlowSpec配置信息。

其中，完整性度量基线值可以为经过哈希计算得到的哈希值，或者，完整性度量基线值也可以为数字签名，又或者，完整性度量基线值还可以为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据。

在一种可能的实现方式中，在第一设备向验证服务器发送第一数据的完整性度量基线值之前，第一设备还可以计算第一数据对应的完整性度量基线值。

其中，以该方法300中的第一设备是控制管理设备且第二设备是终端设备为例，第一

设备计算第一数据对应的完整性度量基线值可以参见方法 100 中的 S102 的相关说明。

作为一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的全部内容确定所述完整性度量基线值。

作为另一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据第一数据的部分内容确定所述完整性度量基线值。

作为又一个示例，第一设备计算第一数据对应的完整性度量基线值，可以包括：第一设备根据发送第一数据对应的第一操作日志确定所述完整性度量基线值。

在一种可能的实现方式中，第一设备可以向第二设备发送第一指示，该第一指示用于指示第二设备对第一数据进行完整性校验。其中，第一指示可以是第一设备直接发送给第二设备的，或者，该第一指示也可以是第一设备经过验证服务器发送给第二设备的。

需要说明的是，该方法 300 中，第一设备的相关描述以及达到的效果可以参见方法 100 中控制管理设备执行的相关操作和对应的效果描述。

本申请实施例还提供了一种完整性校验方法 400，参见图 5，该方法 400 应用于第二设备，该方法 400 例如可以包括：

S401，第二设备接收第一设备发送的第一数据。

S402，第二设备向验证服务器发送所述第一数据对应的完整性度量值，该完整性度量值用于对第一数据的进行完整性校验。

该方法 400 中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

以该方法 400 中的第一设备是控制管理设备且第二设备是终端设备为例，那么，该方法 400 中的第二设备可以是上述方法 100 中的终端设备，相关操作具体可以参见方法 100 中终端设备执行的操作。具体而言，S401 的相关描述可以参见方法 100 中的 S101，S402 的相关描述可以参见方法 100 中的 S105。其中，第一数据可以是方法 100 中的第一数据，第一数据对应的完整性度量值可以是方法 100 中的第一数据对应的完整性度量值，第一数据对应的完整性度量基线值可以是方法 100 中的第一数据对应的完整性度量基线值。

作为一个示例，第一数据可以包括下述至少一个：SR TE 配置信息、SR TE-policy 配置信息、ACL 配置信息或 FlowSpec 配置信息。

其中，完整性度量值可以为经过哈希计算得到的哈希值，或者，完整性度量值也可以为数字签名，又或者，完整性度量值还可以为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据。

在一种可能的实现方式中，在第二设备向验证服务器发送第一数据的完整性度量值之前，第二设备还可以计算第一数据对应的完整性度量值。

其中，以该方法 400 中的第一设备是控制管理设备且第二设备是终端设备为例，第二设备计算第一数据对应的完整性度量值可以参见方法 100 中的 S104 的相关说明。

作为一个示例，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的全部内容确定完整性度量值。

作为另一个示例，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据所述第一数据的部分内容确定完整性度量值。

作为又一个示例，第二设备计算第一数据对应的完整性度量值，可以包括：第二设备根据接收所述第一数据对应的第二操作日志确定所述完整性度量值。

在一种可能的实现方式中，第二设备向验证服务器发送第一数据对应的完整性度量值，可以是基于所接收的第一指示触发的，也可以是满足本地预设条件后触发的。

作为一个示例，在第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以接收第一指示，该第一指示用于指示第二设备对第一数据进行完整性校验。其中，第一指示可以由第一设备发送给第二设备，或者，该第一指示也可以由验证服务器发送给第二设备。

作为另一个示例，第二设备向验证服务器发送第一数据对应的完整性度量值之前，第二设备还可以在确定满足预设条件时，生成所述完整性度量值。其中，预设条件包括下述至少一种：条件一、接收到的第一数据的总长度达到预设长度阈值；条件二、接收到的第一数据包含的表项的数量达到预设数量阈值；条件三、接收第一数据的累计时长达到预设时长；或者，条件四、第一数据为增量数据。如此，第二设备可以被触发计算第一数据对应的完整性度量值并向验证服务器发送该完整性度量值，以便验证服务器对第一数据的完整性进行校验。

需要说明的是，该方法 400 中，第二设备的相关描述以及达到的效果可以参见方法 100 中终端设备执行的相关操作和对应的效果描述。

本申请实施例还提供了一种完整性校验方法 500，参见图 6，该方法 500 应用于验证服务器，该方法 500 例如可以包括：

S501，验证服务器接收第一设备发送的第一数据对应的完整性度量基线值，该第一数据由第一设备发送给第二设备。

S502，验证服务器接收第二设备发送的第一数据对应的完整性度量值。

S503，验证服务器根据完整性度量基线值和完整性度量值，对该第一数据的进行完整性校验。

该方法 500 中，第一设备可以是控制管理设备，第二设备可以是终端设备。或者，第一设备可以是终端设备，第二设备可以是控制管理设备。又或者，第一设备和第二设备均可以是终端设备。

以该方法 500 中的第一设备是控制管理设备且第二设备是终端设备为例，那么，该方法 500 中的验证服务器可以是上述方法 100 中的验证服务器，相关操作具体可以参见方法 100 中验证服务器执行的操作。具体而言，S501 的相关描述可以参见方法 100 中的 S103，S502 的相关描述可以参见方法 100 中的 S105，S503 的相关描述可以参见方法 100 中的 S106。其中，第一数据可以是方法 100 中的第一数据，第一数据对应的完整性度量值可以是方法 100 中的第一数据对应的完整性度量值，第一数据对应的完整性度量基线值可以是

方法 100 中的第一数据对应的完整性度量基线值。

作为一个示例，第一数据可以包括下述至少一个：SR TE 配置信息、SR TE-policy 配置信息、ACL 配置信息或 FlowSpec 配置信息。

其中，完整性度量基线值可以为经过哈希计算得到的哈希值，那么， 完整性度量值为经过哈希计算得到的哈希值。或者，完整性度量基线值也可以为数字签名，那么，完整性度量值为数字签名。又或者，完整性度量基线值还可以为经过加密处理得到的加密值，那么，完整性度量值为经过加密处理得到的加密值。

需要说明的是，为了确保第一设备和第二设备对相同的对象进行完整性校验，第一设备和第二设备可以保持时钟同步，或者，在第一数据携带发送时间戳，这样，可以保障进行完整性校验的第一数据是相同的数据。

在一种可能的实现方式中，第二设备向验证服务器发送第一数据对应的完整性度量值，可以是基于所接收的指示触发的。作为一个示例，验证服务器可以接收第一设备发送的第一指示，该第一指示用于指示验证服务器对第一数据进行完整性校验。那么，响应于所述第一指示，验证服务器还可以向第二设备发送第二指示，该第二指示用于指示对第一数据进行完整性验证。这样，第二设备即可基于第二指示计算并向验证服务器发送第一数据对应的完整性度量值。

在一些可能的实现方式中，验证服务器根据完整性度量基线值和完整性度量值对第一数据的进行完整性校验，可以包括：验证服务器确定完整性度量值和完整性度量基线值匹配，从而，验证服务器确定对第一数据的完整性校验通过。

作为一个示例，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一哈希算法计算得到的第一哈希值，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第一哈希算法计算得到的第二哈希值，那么，验证服务器可以判断第一哈希值和第二哈希值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。

作为又一个示例，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一私钥对第一哈希值进行签名操作得到的第一签名，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第二私钥对第二哈希值进行签名操作得到的第二签名，那么，一种情况下，验证服务器可以先判断第一私钥对应的第一公钥和第二私钥对应的第二公钥是否相同，如果相同，再判断第一签名和第二签名是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过；另一种情况下，验证服务器可以先采用第一私钥对应的第一公钥对第一签名进行处理得到第一还哈希值，采用第二私钥对应的第二公钥对第二签名进行处理得到第二哈希值，再判断第一哈希值和第二哈希值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。其中，第一公钥可以是控制管理设备对应的第一私钥对应的公钥，该公钥可以预先保存在验证服务器本地，也可以是控制管理设备向验证服务

器发送第一数据的完整性度量基线值时发送给验证服务器的。同理，第二公钥可以是终端设备对应的第二私钥对应的公钥，该公钥可以预先保存在验证服务器本地，也可以是终端设备向验证服务器发送第一数据的完整性度量值时发送给验证服务器的。

作为再一个示例，第一数据的完整性度量基线值为第一数据的全部内容（或部分内容，又或者发送第一数据对应的第一操作日志）经过第一加密算法计算得到的第一加密值，第一数据的完整性度量值为第一数据的全部内容（或部分内容，又或者接收第一数据对应的第二操作日志）经过第一加密算法计算得到的第二加密值，那么，一种情况下，验证服务器可以判断第一加密值和第二加密值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过；另一种情况下，验证服务器也可以先采用第一加密算法对应的第一解密算法对第一加密值进行解密得到第一解密值，采用第一加密算法对应的第一解密算法对第二加密值进行解密得到第二解密值再判断第一解密值和第二解密值是否一致，如果一致，则，确定对第一数据的完整性校验通过，否则，确定对第一数据的完整性校验未通过。

当对第一数据的完整性校验未通过时，为了让控制管理设备感知到该控制管理设备和终端设备之间关于第一数据的一致性问题，验证服务器可以向控制管理设备发送告警消息，用于告知该终端设备上的第一数据存在异常。当控制管理设备接收到告警消息后，为了确保终端设备能够继续正常运行，还可以重新向终端设备发送第一数据，指示终端设备用新接收的第一数据替换本地保存的第一数据，或者，指示终端设备保存新接收的第一数据并将之前保存的第一数据添加老化标记，添加老化标记的第一数据不能再指导该终端设备对报文的处理，而是以新接收的第一数据指导该终端设备对报文进行处理。

需要说明的是，该方法 500 中，验证服务器的相关描述以及达到的效果可以参见方法 100 中验证服务器执行的相关操作和对应的效果描述。

此外，本申请实施例还提供了一种第一设备 300，参见图 7 所示。该第一设备 300 包括处理单元 301 和发送单元 302。其中，处理单元 301 用于执行上述图 2 所示实施例中控制管理设备执行的处理操作、以及图 1 所示实施例中控制管理设备 100 执行的处理操作；发送单元 302 用于执行上述图 2 所示实施例中控制管理设备执行的发送操作、以及图 1 所示实施例中控制管理设备 100 执行的发送操作。例如：处理单元 301 可以执行图 2 中实施例中的操作：生成第一数据对应的完整性度量基线值。例如：发送单元 302 可以执行图 2 中实施例中的操作：向终端设备发送第一数据，以及向验证服务器发送所述完整性度量基线值。

此外，本申请实施例还提供了一种第二设备 400，参见图 8 所示。该第二设备 400 包括接收单元 401、发送单元 402 和处理单元 403。其中，接收单元 401 用于执行上述图 2 所示实施例中终端设备执行的接收操作、以及图 1 所示实施例中终端设备 200 执行的接收操作；发送单元 402 用于执行上述图 2 所示实施例中终端设备执行的发送操作、以及图 1 所示实施例中终端设备 200 执行的发送操作；处理单元 403 用于执行上述图 2 所示实施例中终端设备执行的处理操作、以及图 1 所示实施例中终端设备 200 执行的处理操作。例如：

接收单元 401 可以执行图 2 中实施例中的操作：接收控制管理设备发送的第一数据；发送单元 402 可以执行图 2 中实施例中的操作：向验证服务器发送第一数据对应的完整性度量值；处理单元 403 可以执行图 2 中实施例中的操作：生成第一数据对应的完整性度量值。

此外，本申请实施例还提供了一种验证服务器 500，参见图 9 所示。该验证服务器 500 包括接收单元 501 和处理单元 502。其中，接收单元 501 用于执行上述图 2 所示实施例中验证服务器执行的接收操作、以及图 1 所示实施例中验证服务器 400 执行的接收操作；处理单元 502 用于执行上述图 2 所示实施例中验证服务器执行的处理操作、以及图 1 所示实施例中验证服务器 400 执行的处理操作。例如：接收单元 501 可以执行图 2 中实施例中的操作：接收控制管理设备发送的第一数据对应的完整性度量基线值，以及接收终端设备发送的第一数据对应的完整性度量值；处理单元 502 可以执行图 2 中实施例中的操作：根据所述完整性度量基线值和所述完整性度量值，对所述第一数据的进行完整性校验。

此外，本申请实施例还提供了一种第一设备 600，参见图 10 所示。该第一设备 600 包括第一通信接口 601 和处理器 603。其中，第一通信接口 601 用于执行前述用于执行上述图 2 所示实施例中控制管理设备、以及图 1 所示实施例中控制管理设备 100 执行的发送操作；处理器 603 用于执行上述图 2 所示实施例中控制管理设备、以及图 1 所示实施例中控制管理设备 100 执行的除了接收操作和发送操作之外的其他操作。例如：第一通信接口 601 可以执行图 2 中实施例中的操作：向终端设备发送第一数据，以及向验证服务器发送所述第一数据对应的完整性度量基线值；处理器 603 可以执行图 2 中实施例中的操作：根据所述第一数据的全部内容确定所述完整性度量基线值。此外，该第一设备 600 还可以包括第二通信接口 602。其中，第二通信接口 602 用于执行前述用于执行上述图 2 所示实施例中控制管理设备、以及图 1 所示实施例中控制管理设备 100 执行的接收操作。

此外，本申请实施例还提供了一种第二设备 700，参见图 11 所示。该第二设备 700 包括第一通信接口 701 和第二通信接口 702。其中，第一通信接口 701 用于执行前述用于执行上述图 2 所示实施例中终端设备、以及图 1 所示实施例中终端设备 200 执行的发送操作；第二通信接口 702 用于执行前述用于执行上述图 2 所示实施例中终端设备、以及图 1 所示实施例中终端设备 200 执行的接收操作。例如：第一通信接口 701 可以执行图 2 中实施例中的操作：向验证服务器发送第一数据对应的完整性度量值；第二通信接口 702 可以执行图 2 中实施例中的操作：接收控制管理设备发送的第一数据。此外，该第二设备 700 还可以包括处理器 703。其中，处理器 703 用于执行前述用于执行上述图 2 所示实施例中终端设备、以及图 1 所示实施例中终端设备 200 执行的除了接收操作和发送操作之外的其他操作。

此外，本申请实施例还提供了一种验证服务器 800，参见图 12 所示。该验证服务器 800 包括第一通信接口 801 和处理器 803。其中，第一通信接口 801 用于执行前述用于执行上述图 2 所示实施例中验证服务器、以及图 1 所示实施例中验证服务器 400 执行的接收操作；处理器 803 用于执行上述图 2 所示实施例中验证服务器、以及图 1 所示实施例中验证服务器 400 执行的除了接收操作和发送操作之外的其他操作。例如：第一通信接口 801 可以执行图 2 中实施例中的操作：接收第一设备发送的第一数据对应的完整性度量基线值，以及

接收所述第二设备发送的所述第一数据对应的完整性度量值；处理器 803 可以执行图 2 中实施例中的操作：根据所述完整性度量基线值和所述完整性度量值，对所述第一数据的进行完整性校验。此外，该验证服务器 800 还可以包括第二通信接口 802。其中，第二通信接口 802 用于执行前述用于执行上述图 2 所示实施例中验证服务器、以及图 1 所示实施例中验证服务器 400 执行的发送操作。

此外，本申请实施例还提供了一种第一设备 900，参见图 13 所示。该第一设备 900 包括存储器 901 和与存储器 901 通信的处理器 902。其中，存储器 901 包括计算机可读指令；处理器 902 用于执行所述计算机可读指令，使得该第一设备 900 执行以上图 2 所示实施例中控制管理设备侧执行的方法，以及图 1 所示实施例中控制管理设备 100 执行的方法。

此外，本申请实施例还提供了一种第二设备 1000，参见图 14 所示。该第二设备 1000 包括存储器 1001 和与存储器 1001 通信的处理器 1002。其中，存储器 1001 包括计算机可读指令；处理器 1002 用于执行所述计算机可读指令，使得该第二设备 1000 执行以上图 2 所示实施例中终端设备侧执行的方法，以及图 1 所示实施例中终端设备 200 执行的方法。

此外，本申请实施例还提供了一种验证服务器 1100，参见图 15 所示。该验证服务器 1100 包括存储器 1101 和与存储器 1101 通信的处理器 1102。其中，存储器 1101 包括计算机可读指令；处理器 1102 用于执行所述计算机可读指令，使得该验证服务器 1100 执行以上图 2 所示实施例中验证服务器侧执行的方法，以及图 1 所示实施例中验证服务器 400 执行的方法。

可以理解的是，上述实施例中，处理器可以是中央处理器（英文：central processing unit，缩写：CPU），网络处理器（英文：network processor，缩写：NP）或者 CPU 和 NP 的组合。处理器还可以是专用集成电路（英文：application-specific integrated circuit，缩写：ASIC），可编程逻辑器件（英文：programmable logic device，缩写：PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（英文：complex programmable logic device，缩写：CPLD），现场可编程逻辑门阵列（英文：field-programmable gate array，缩写：FPGA），通用阵列逻辑（英文：generic array logic，缩写：GAL）或其任意组合。处理器可以是指一个处理器，也可以包括多个处理器。存储器可以包括易失性存储器（英文：volatile memory），例如随机存取存储器（英文：random-access memory，缩写：RAM）；存储器也可以包括非易失性存储器（英文：non-volatile memory），例如只读存储器（英文：read-only memory，缩写：ROM），快闪存储器（英文：flash memory），硬盘（英文：hard disk drive，缩写：HDD）或固态硬盘（英文：solid-state drive，缩写：SSD）；存储器还可以包括上述种类的存储器的组合。存储器可以是指一个存储器，也可以包括多个存储器。在一个具体实施方式中，存储器中存储有计算机可读指令，所述计算机可读指令包括多个软件模块，例如发送模块，处理模块和接收模块。处理器执行各个软件模块后可以按照各个软件模块的指示进行相应的操作。在本实施例中，一个软件模块所执行的操作实际上是指处理器根据所述软件模块的指示而执行的操作。处理器执行存储器中的计算机可读指令后，可以按照所述计算机可读指令的指示，执行完整性校验中各设备或服务器可以执行的全部操作。

可以理解的是，上述实施例中，第一设备 600 的第一通信接口 601，具体可以被用作

第一设备 300 中的发送单元 302，实现第一设备到第二设备或验证服务器之间的数据通信；第一设备 600 的处理器 603，具体可以被用作第一设备 300 中的处理单元 301，例如可以用于根据所述第一数据的全部内容确定所述完整性度量基线值。同理，第二设备 700 的第一通信接口 701，具体可以被用作第二设备 400 中的发送单元 402，实现第二设备到验证服务器的数据通信；第二设备 700 的第二通信接口 702，具体可以被用作第二设备 400 中的接收单元 401，实现第一设备到第二设备的数据通信。同理，验证服务器 800 的第一通信接口 801，具体可以被用作验证服务器 500 中的接收单元 501，实现第一设备或第二设备到验证服务器的数据通信；验证服务器 800 的处理器 803，具体可以被用作验证服务器 500 中的处理单元 502，例如可以用于根据所述完整性度量基线值和所述完整性度量值，对所述第一数据的进行完整性校验。

此外，本申请实施例还提供了一种通信系统 1200，参见图 16 所示。该通信系统 1200 包括第一设备 1201、第二设备 1202 以及验证服务器 1203，其中，第一设备 1201 具体可以是上述第一设备 300、第一设备 600 或第一设备 900，第二设备 1202 具体可以是上述第二设备 400、第二设备 700 或第二设备 1000，验证服务器 1203 具体可以是上述验证服务器 500、验证服务器 800 或验证服务器 1100。

需要说明的是，上述实施例中的各个设备或服务器，可以是用于执行上述方法的网络设备，也可以是指用于执行上述方法的单板、线卡、芯片等。

此外，本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得所述计算机执行以上图 1 或图 2 所示实施例中的所述完整性校验方法。

此外，本申请实施例还提供了计算机程序产品，包括计算机程序或计算机可读指令，当所述计算机程序或所述计算机可读指令在计算机上运行时，使得计算机执行前述图 1 或图 2 所示实施例中的所述完整性校验方法。

通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到上述实施例方法中的全部或部分步骤可借助软件加通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如只读存储器（英文：read-only memory，ROM）/RAM、磁碟、光盘等，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，或者诸如路由器等网络通信设备）执行本申请各个实施例或者实施例的某些部分所述的方法。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例和设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的设备及系统实施例仅仅是示意性的，其中作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，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模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

以上所述仅是本申请的优选实施方式，并非用于限定本申请的保护范围。应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本申请的保护范围。

5

权 利 要 求

1.一种完整性校验方法，其特征在于，包括：

第一设备向第二设备发送第一数据；

所述第一设备向验证服务器发送所述第一数据对应的完整性度量基线值，所述第二设备向所述验证服务器发送所述第一数据对应的完整性度量值；

所述验证服务器根据所述完整性度量值和所述完整性度量基线值，对所述第一数据进行完整性校验。

2.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述第一设备根据所述第一数据的全部内容确定所述完整性度量基线值；

所述第二设备根据所述第一数据的全部内容确定所述完整性度量值。

3.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述第一设备根据所述第一数据的部分内容确定所述完整性度量基线值；

所述第二设备根据所述第一数据的所述部分内容确定所述完整性度量值。

4.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述第一设备根据发送所述第一数据对应的第一操作日志，获得所述完整性度量基线值；

所述第二设备根据接收所述第一数据对应的第二操作日志，获得所述完整性度量值。

5.根据权利要求 1-4 任一项所述的方法，其特征在于，所述第二设备向所述验证服务器发送所述第一数据对应的完整性度量值之前，所述方法还包括：

所述第二设备接收第一指示，所述第一指示用于指示所述第二设备对所述第一数据进行完整性校验。

6.根据权利要求 5 所述的方法，其特征在于，所述第一指示由所述第一设备发送。

7.根据权利要求 5 所述的方法，其特征在于，所述第一指示由所述验证服务器发送。

8.根据权利要求 1-4 任一项所述的方法，其特征在于，所述第二设备向所述验证服务器发送所述第一数据对应的完整性度量值之前，所述方法包括：

在满足预设条件时，所述第二设备生成所述完整性度量值。

9.根据权利要求 8 所述的方法，其特征在于，所述预设条件包括下述至少一种：

接收到的所述第一数据的总长度达到预设长度阈值；

接收到的所述第一数据包含的表项的数量达到预设数量阈值；

接收所述第一数据的累计时长达到预设时长；或者

所述第一数据为增量数据。

10.一种完整性校验方法，其特征在于，包括：

第一设备向第二设备发送第一数据；

所述第一设备向验证服务器发送所述第一数据对应的完整性度量基线值，所述完整性度量基线值用于对所述第一数据的进行完整性校验。

11.根据权利要求 10 所述的方法，其特征在于，所述方法还包括：

所述第一设备根据所述第一数据的全部内容确定所述完整性度量基线值。

12.根据权利要求 10 所述的方法，其特征在于，所述方法还包括：

所述第一设备根据所述第一数据的部分内容确定所述完整性度量基线值。

13.根据权利要求 10 所述的方法，其特征在于，所述方法还包括：

所述第一设备根据发送所述第一数据对应的第一操作日志，确定所述完整性度量基线值。

14.根据权利要求 10-13 任一项所述的方法，其特征在于，所述方法还包括：

所述第一设备向所述第二设备发送第一指示，所述第一指示用于指示所述第二设备对所述第一数据进行完整性校验。

15.根据权利要求 14 所述的方法，其特征在于，所述第一设备通过所述验证服务器向所述第二设备发送所述第一指示。

16.一种完整性校验方法，其特征在于，包括：

第二设备接收第一设备发送的第一数据；

所述第二设备向验证服务器发送所述第一数据对应的完整性度量值，所述完整性度量值用于对所述第一数据的进行完整性校验。

17.根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

所述第二设备根据所述第一数据的全部内容确定所述完整性度量值。

18.根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

所述第二设备根据所述第一数据的所述部分内容确定所述完整性度量值。

19.根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

所述第二设备根据接收所述第一数据对应的第二操作日志，获得所述完整性度量值。

20.根据权利要求 16-19 任一项所述的方法，其特征在于，所述第二设备向验证服务器发送所述第一数据对应的完整性度量值之前，所述方法还包括：

所述第二设备接收第一指示，所述第一指示用于指示所述第二设备对所述第一数据进行完整性校验。

21.根据权利要求 20 所述的方法，其特征在于，所述第一指示由所述第一设备发送。

22.根据权利要求 20 所述的方法，其特征在于，所述第一指示由所述验证服务器发送。

23.根据权利要求 16-19 任一项所述的方法，其特征在于，所述第二设备向验证服务器发送所述第一数据对应的完整性度量值之前，所述方法包括：

在满足预设条件时，所述第二设备生成所述完整性度量值。

24.根据权利要求 23 所述的方法，其特征在于，所述预设条件包括下述至少一种：

接收到的所述第一数据的总长度达到预设长度阈值；

接收到的所述第一数据包含的表项的数量达到预设数量阈值；

接收所述第一数据的累计时长达到预设时长；或者

所述第一数据为增量数据。

25.一种完整性校验方法，其特征在于，包括：

验证服务器接收第一设备发送的第一数据对应的完整性度量基线值，所述第一数据由所述第一设备发送给第二设备；

所述验证服务器接收所述第二设备发送的所述第一数据对应的完整性度量值；

所述验证服务器根据所述完整性度量基线值和所述完整性度量值，对所述第一数据的进行完整性校验。

26.根据权利要求 25 所述的方法，其特征在于，所述方法还包括：

所述验证服务器接收所述第一设备发送的第一指示，所述第一指示用于指示所述验证服务器对所述第一数据进行完整性校验。

27.根据权利要求 26 所述的方法，其特征在于，所述方法还包括：

响应于所述第一指示，所述验证服务器向所述第二设备发送第二指示，所述第二指示用于指示对所述第一数据进行完整性验证。

28.根据权利要求 25-27 任一项所述的方法，其特征在于，所述验证服务器根据所述完整性度量基线值和所述完整性度量值，对所述第一数据的进行完整性校验，包括：

所述验证服务器确定所述完整性度量值和所述完整性度量基线值匹配；

所述验证服务器确定对所述第一数据的完整性校验通过。

29.根据权利要求 1-28 任一项所述的方法，其特征在于，所述第一数据包括下述至少一个：

分段路由流量工程 SR TE 配置信息、分段路由流量工程的策略 SR TE-policy 配置信息、访问控制列表 ACL 配置信息或流规则 FlowSpec 配置信息。

30.根据权利要求 1-15、25-29 任意一项所述的方法，其特征在于，所述完整性度量基线值为：经过哈希计算得到的哈希值、数字签名或经过加密处理得到的加密值。

31.根据权利要求 1-9、16-29 任意一项所述的方法，其特征在于，所述完整性度量值为：经过哈希计算得到的哈希值、数字签名或经过加密处理得到的加密值。

32.据权利要求 1-31 任意一项所述的方法，其特征在于，所述第一设备和所述第二设备保持时钟同步。

33.根据权利要求 1-31 任意一项所述的方法，其特征在于，所述第一数据携带发送时间戳。

34.根据权利要求 1-33 任一项所述的方法，其特征在于，所述第一设备是控制管理设备，所述第二设备是终端设备。

35.一种网络系统，其特征在于，包括：第一设备，第二设备和验证服务器，所述网络系统用于执行权利要求 1-9 以及 29-34 任一项所述的方法。

36.一种第一设备，其特征在于，包括：

收发单元，用于向第二设备发送第一数据；

所述收发单元，还用于向验证服务器发送所述第一数据对应的完整性度量基线值，所述完整性度量基线值用于对所述第一数据的进行完整性校验。

37.根据权利要求 36 所述的第一设备，其特征在于，所述第一设备还包括：

处理单元，用于根据所述第一数据的全部内容确定所述完整性度量基线值。

38.根据权利要求 36 所述的第一设备，其特征在于，所述第一设备还包括：

处理单元，用于根据所述第一数据的部分内容确定所述完整性度量基线值。

39.根据权利要求 36 所述的第一设备，其特征在于，所述第一设备还包括：

处理单元，用于根据发送所述第一数据对应的第一操作日志，确定所述完整性度量基线值。

40.根据权利要求 36-39 任一项所述的第一设备，其特征在于，

所述收发单元，还用于向所述第二设备发送第一指示，所述第一指示用于指示所述第二设备对所述第一数据进行完整性校验。

41.根据权利要求 40 所述的第一设备，其特征在于，所述收发单元，具体用于：

通过所述验证服务器向所述第二设备发送所述第一指示。

42.一种第二设备，其特征在于，包括：

收发单元，用于接收第一设备发送的第一数据；

所述收发单元，还用于向验证服务器发送所述第一数据对应的完整性度量值，所述完整性度量值用于对所述第一数据的进行完整性校验。

43.根据权利要求 42 所述的第二设备，其特征在于，所述第二设备还包括：

处理单元，用于根据所述第一数据的全部内容确定所述完整性度量值。

44.根据权利要求 42 所述的第二设备，其特征在于，所述第二设备还包括：

处理单元，用于根据所述第一数据的所述部分内容确定所述完整性度量值。

45.根据权利要求 42 所述的第二设备，其特征在于，所述第二设备还包括：

处理单元，用于根据接收所述第一数据对应的第二操作日志，获得所述完整性度量值。

46.根据权利要求 42-45 任一项所述的第二设备，其特征在于，

所述收发单元，还用于在向所述验证服务器发送所述第一数据对应的完整性度量值之前，接收第一指示，所述第一指示用于指示所述第二设备对所述第一数据进行完整性校验。

47.根据权利要求 46 所述的第二设备，其特征在于，所述第一指示由所述第一设备发送。

48.根据权利要求 46 所述的第二设备，其特征在于，所述第一指示由所述验证服务器发送。

49.根据权利要求 42-45 任一项所述的第二设备，其特征在于，

所述处理单元，还用于在向所述验证服务器发送所述第一数据对应的完整性度量值之前，在满足预设条件时，生成所述完整性度量值。

50.根据权利要求 49 所述的第二设备，其特征在于，所述预设条件包括下述至少一种：

接收到的所述第一数据的总长度达到预设长度阈值；

接收到的所述第一数据包含的表项的数量达到预设数量阈值；

接收所述第一数据的累计时长达到预设时长；或者

所述第一数据为增量数据。

51.一种验证服务器，其特征在于，包括：

收发单元，用于接收第一设备发送的第一数据对应的完整性度量基线值，所述第一数据由所述第一设备发送给第二设备；

所述收发单元，还用于接收所述第二设备发送的所述第一数据对应的完整性度量值；

处理单元，用于根据所述完整性度量基线值和所述完整性度量值，对所述第一数据的进行完整性校验。

52.根据权利要求 51 所述的验证服务器，其特征在于，

所述收发单元，还用于接收所述第一设备发送的第一指示，所述第一指示用于指示所述验证服务器对所述第一数据进行完整性校验。

53.根据权利要求 52 所述的验证服务器，其特征在于，

所述收发单元，还用于响应于所述第一指示，所述验证服务器向所述第二设备发送第二指示，所述第二指示用于指示对所述第一数据进行完整性验证。

54.根据权利要求 51-53 任一项所述的验证服务器，其特征在于，所述处理单元，具体用于：

确定所述完整性度量值和所述完整性度量基线值匹配；

确定对所述第一数据的完整性校验通过。

55.一种第一设备，包括：

存储器，所述存储器包括计算机可读指令；

与所述存储器通信的处理器，所述处理器用于执行所述计算机可读指令，使得所述第一设备执行权利要求 10-15 以及 29-34 任一项所述的方法。

56.一种第二设备，其特征在于，包括：

存储器，所述存储器包括计算机可读指令；

与所述存储器通信的处理器，所述处理器用于执行所述计算机可读指令，使得所述第二设备执行权利要求 16-24 以及 29-34 任一项所述的方法。

57.一种验证服务器，其特征在于，包括：

存储器，所述存储器包括计算机可读指令；

与所述存储器通信的处理器，所述处理器用于执行所述计算机可读指令，使得所述验证服务器执行权利要求 25-34 任一项所述的方法。

58.一种通信系统，其特征在于，所述通信系统包括：权利要求 55 对应的所述第一设备、权利要求 56 对应的所述第二设备、以及权利要求 57 对应的所述验证服务器；

或者，所述通信系统包括：权利要求 36-41 任一项对应的所述第一设备、权利要求 42-50 任一项对应的所述第二设备、以及权利要求 51-54 任一项对应的所述验证服务器。

59.一种计算机可读存储介质，其特征在于，包括程序或指令，当其被处理器执行时实现如权利要求 1-34 任一项所述的方法。

60.一种计算机程序产品，其特征在于，包括计算机程序，所述计算机程序被处理器执行时实现权利要求 1-34 任一项所述的方法。

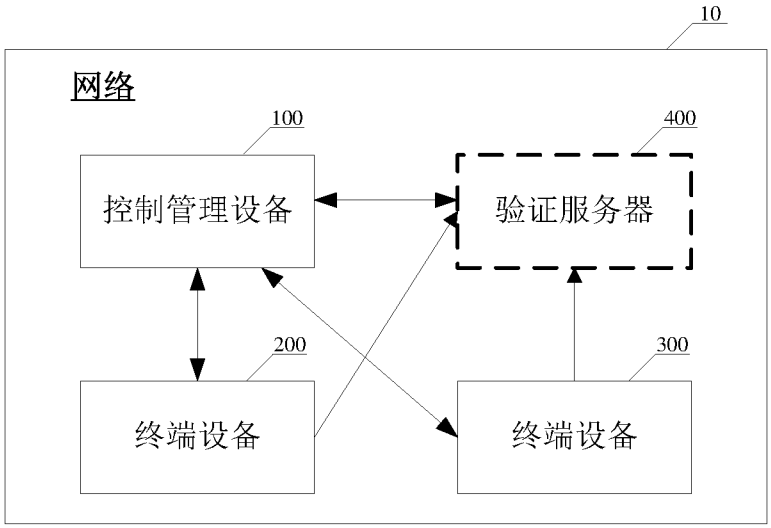

图 1

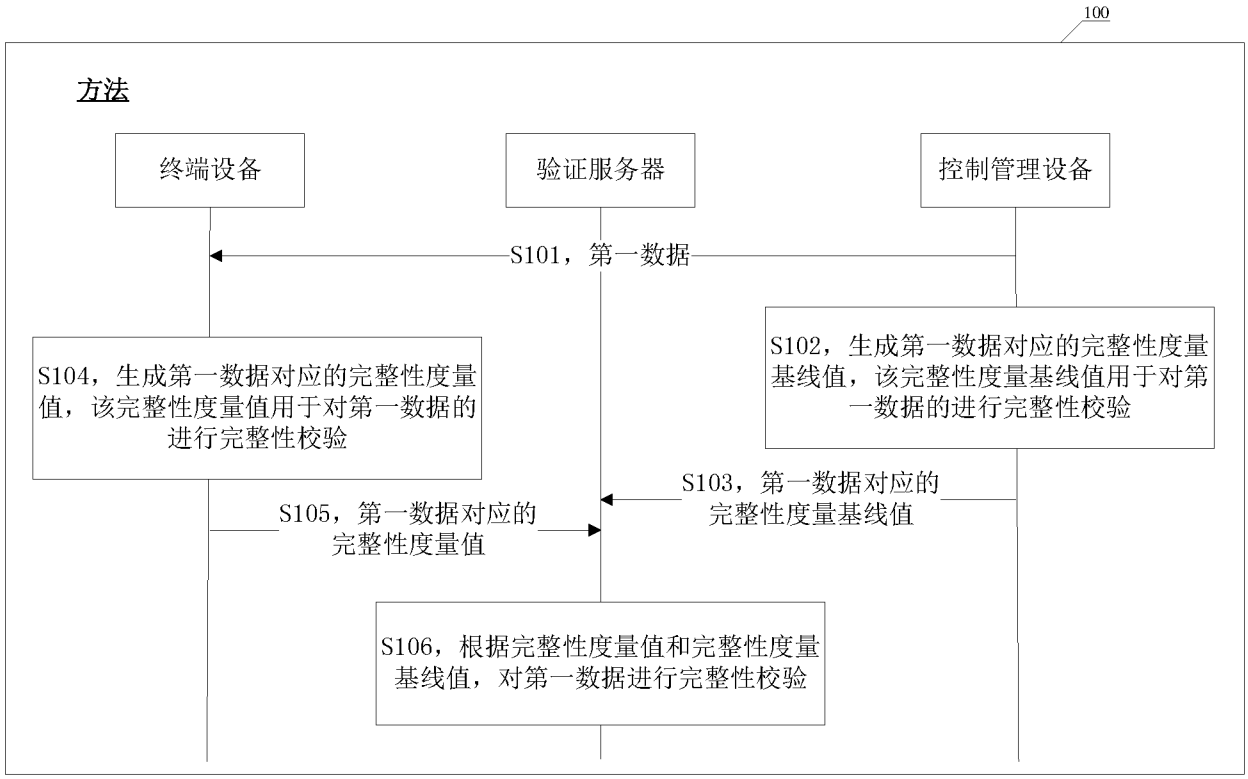
100
方法
终端设备
验证服务器
控制管理设备
S101，第一数据
S104，生成第一数据对应的完整性度量值，该完整性度量值用于对第一数据的进行完整性校验
S102，生成第一数据对应的完整性度量基线值，该完整性度量基线值用于对第一数据的进行完整性校验
S103，第一数据对应的完整性度量基线值
S105，第一数据对应的完整性度量值
S106，根据完整性度量值和完整性度量基线值，对第一数据进行完整性校验

图 2

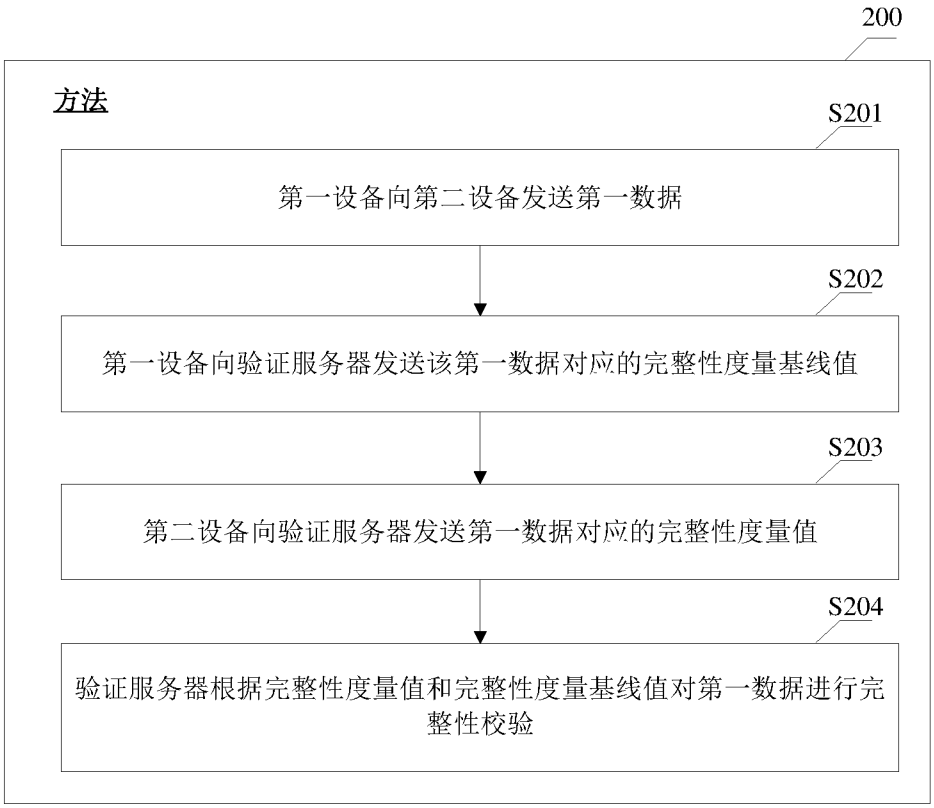
200
方法
S201
第一设备向第二设备发送第一数据
S202
第一设备向验证服务器发送该第一数据对应的完整性度量基线值
S203
第二设备向验证服务器发送第一数据对应的完整性度量值
S204
验证服务器根据完整性度量值和完整性度量基线值对第一数据进行完整性校验

图 3

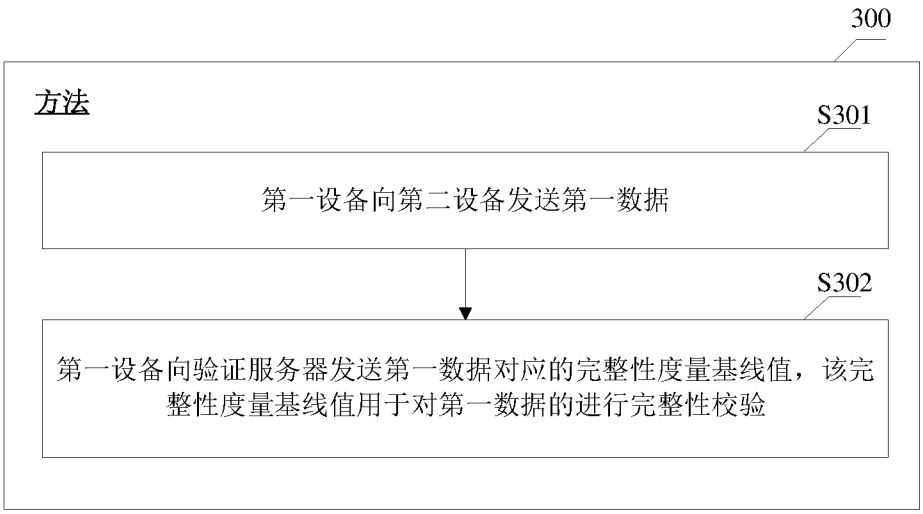
300
方法
S301
第一设备向第二设备发送第一数据
S302
第一设备向验证服务器发送第一数据对应的完整性度量基线值，该完整性度量基线值用于对第一数据的进行完整性校验

图 4

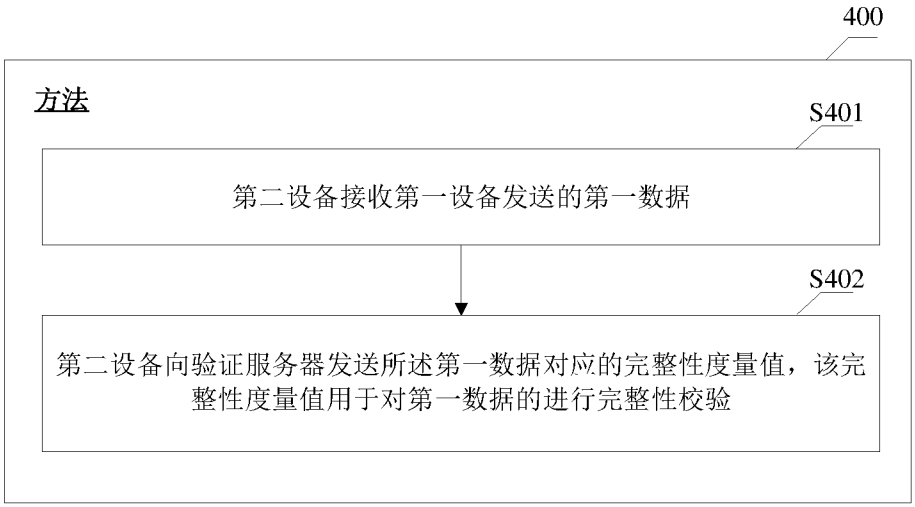
400
方法
S401
第二设备接收第一设备发送的第一数据
S402
第二设备向验证服务器发送所述第一数据对应的完整性度量值，该完整性度量值用于对第一数据的进行完整性校验

图 5

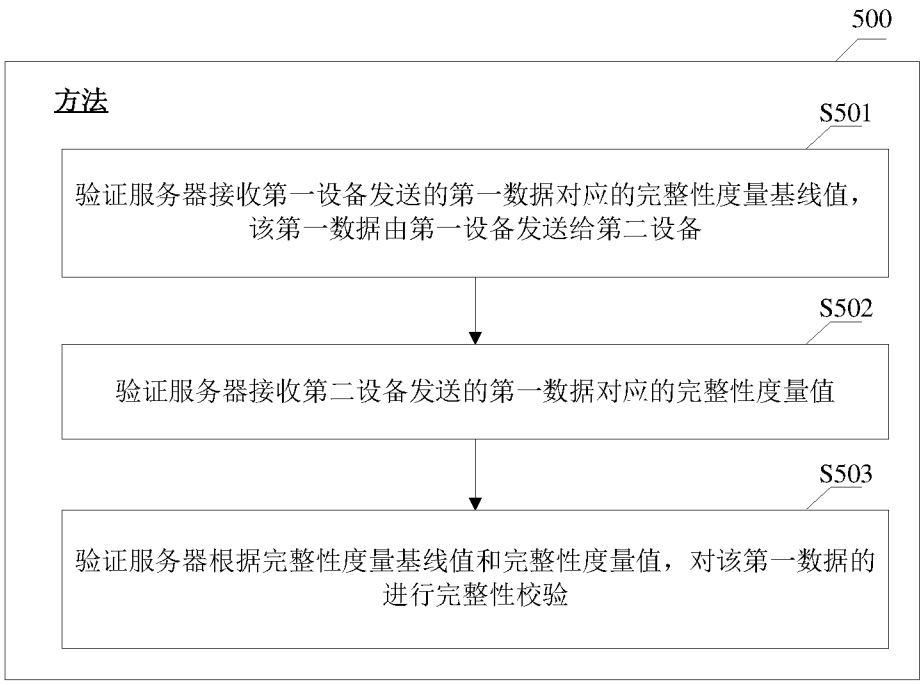
500
方法
S501
验证服务器接收第一设备发送的第一数据对应的完整性度量基线值，该第一数据由第一设备发送给第二设备
S502
验证服务器接收第二设备发送的第一数据对应的完整性度量值
S503
验证服务器根据完整性度量基线值和完整性度量值，对该第一数据的进行完整性校验

图 6

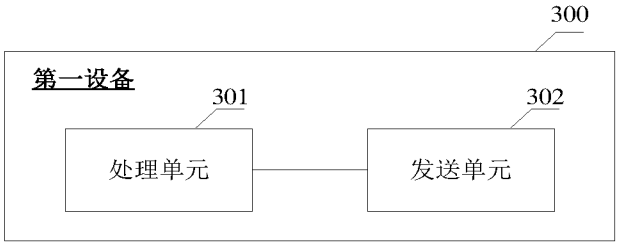
300
第一设备
301
302
处理单元
发送单元

图 7

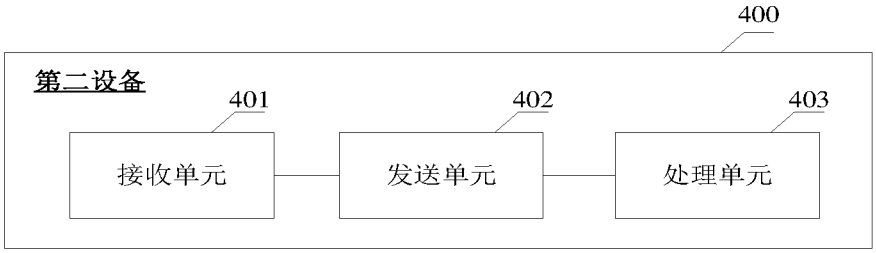
400
第二设备
401
402
403
接收单元
发送单元
处理单元

图 8

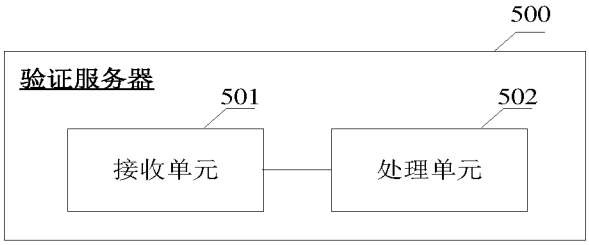
500
验证服务器
501
502
接收单元
处理单元

图 9

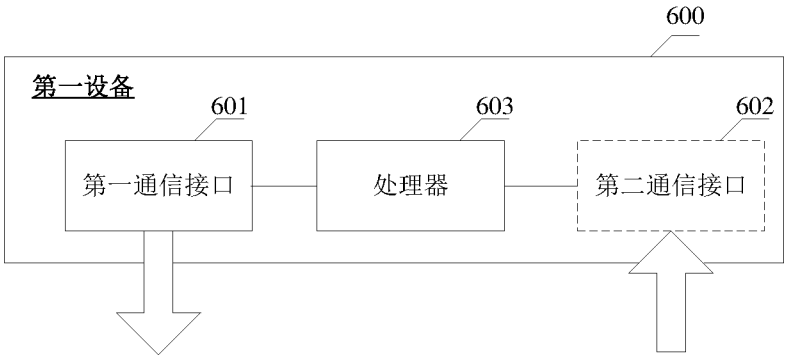
600
第一设备
601
603
602
第一通信接口
处理器
第二通信接口

图 10

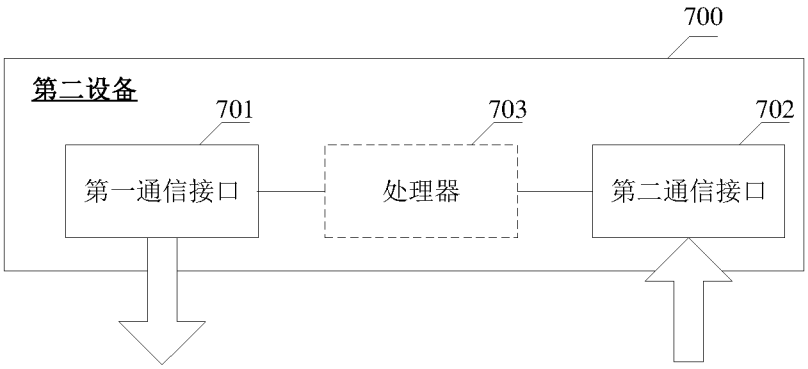
700
第二设备
701
703
702
第一通信接口
处理器
第二通信接口

图 11

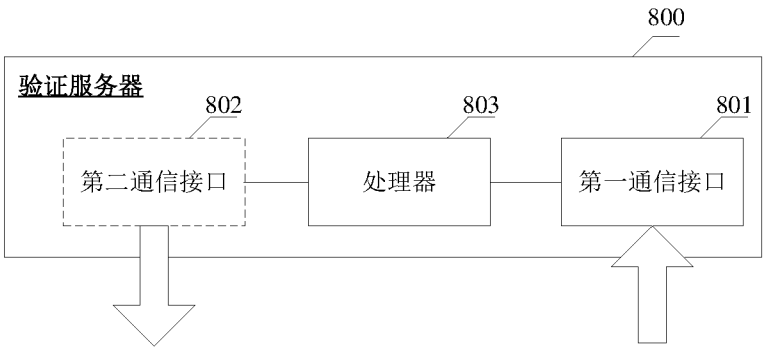
800
验证服务器
802
803
801
第二通信接口
处理器
第一通信接口

图 12

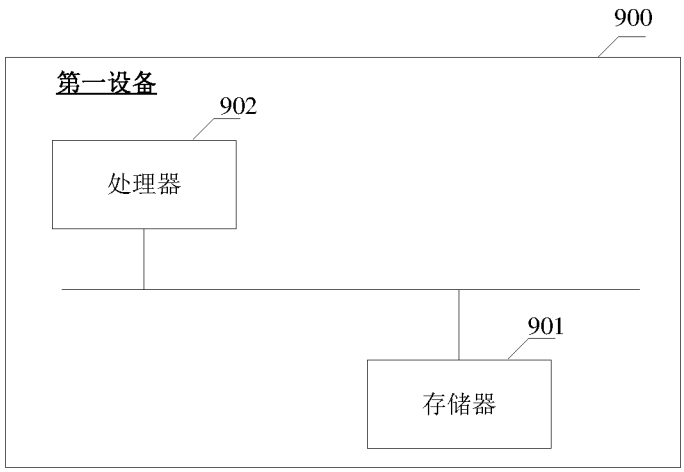
900
第一设备
902
处理器
901
存储器

图 13

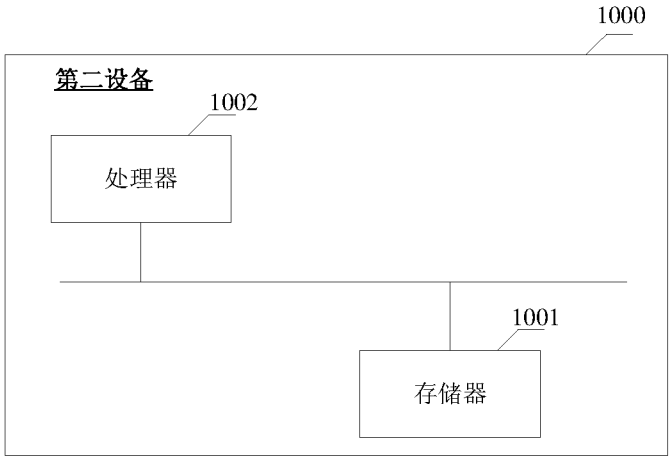
1000
第二设备
1002
处理器
1001
存储器

图 14

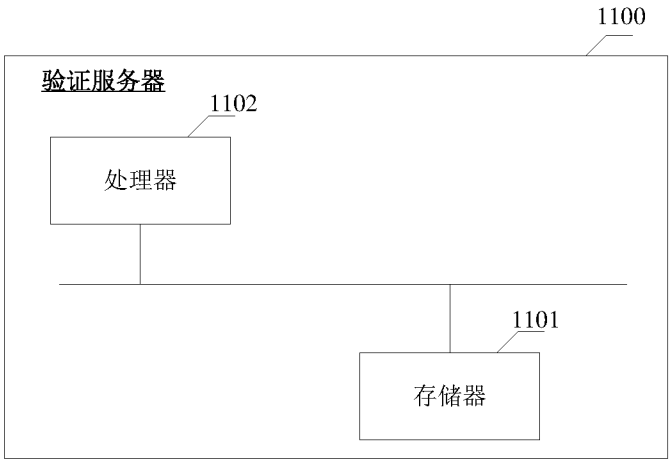
1100
验证服务器
1102
处理器
1101
存储器

图 15

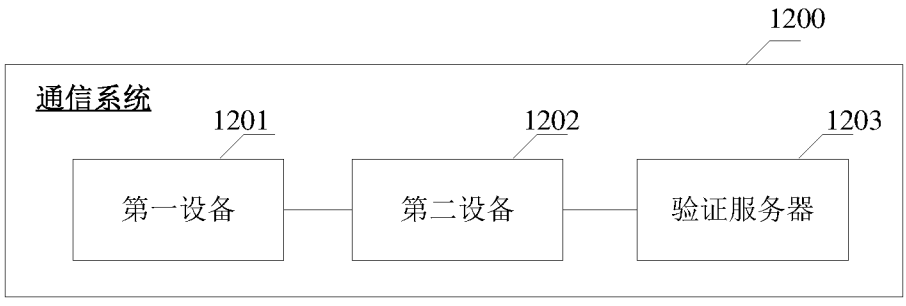
1200
通信系统
1201
1202
1203
第一设备
第二设备
验证服务器

图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/130551

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 完整性, 校验, 哈希, 签名, 加密, 验证, 第三方, 传输, 发送, integrity, check, hash, signature, encrypt, certificat+, third party, transmission, send

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111597590 A (CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 28 August 2020 (2020-08-28) description, paragraphs [0030]-[0060]	1-60
X	CN 104202168 A (LANGCHAO ELECTRONIC INFORMATION INDUSTRY CO., LTD.) 10 December 2014 (2014-12-10) description, paragraphs [0015]-[0032]	1-60
A	CN 108111464 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 01 June 2018 (2018-06-01) entire document	1-60
A	US 2018260583 A1 (QUANTUM CORP.) 13 September 2018 (2018-09-13) entire document	1-60

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 December 2021	**22 December 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/130551

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111597590 A	28 August 2020	None	
CN 104202168 A	10 December 2014	None	
CN 108111464 A	01 June 2018	CN 108111464 B	10 November 2020
US 2018260583 A1	13 September 2018	US 10552640 B2	04 February 2020

国际检索报告

国际申请号
PCT/CN2021/130551

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;CNKI;VEN;USTXT;EPTXT;WOTXT：完整性，校验，哈希，签名，加密，验证，第三方，传输，发送，integrity，check，hash，signature，encrypt，certificat+，third party，transmission，send

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 111597590 A (重庆邮电大学) 2020年8月28日 (2020-08-28) 说明书第[0030]-[0060]段	1-60
X	CN 104202168 A (浪潮电子信息产业股份有限公司) 2014年12月10日 (2014-12-10) 说明书第[0015]-[0032]段	1-60
A	CN 108111464 A (腾讯科技深圳有限公司) 2018年6月1日 (2018-06-01) 全文	1-60
A	US 2018260583 A1 (QUANTUM CORP) 2018年9月13日 (2018-09-13) 全文	1-60

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：
“A” 认为不特别相关的表示了现有技术一般状态的文件
“E” 在国际申请日的当天或之后公布的在先申请或专利
“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
“O” 涉及口头公开、使用、展览或其他方式公开的文件
“P” 公布日先于国际申请日但迟于所要求的优先权日的文件
“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年12月6日	2021年12月22日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 苏星晔 电话号码 86-(512)-88996074

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/130551

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 111597590 A	2020年8月28日	无	
CN 104202168 A	2014年12月10日	无	
CN 108111464 A	2018年6月1日	CN 108111464 B	2020年11月10日
US 2018260583 A1	2018年9月13日	US 10552640 B2	2020年2月4日