(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 19 日 (19.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/100153 A1

(51) 国际专利分类号:
*H04L 29/06* (2006.01) *H04W 12/06* (2021.01)

(21) 国际申请号: PCT/CN2021/109153

(22) 国际申请日: 2021 年 7 月 29 日 (29.07.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011256559.2 2020年11月11日 (11.11.2020) 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: 许燕平 (**XU, Yanping**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 夏靓 (**XIA, Liang**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 佟晓惠 (**TONG, Xiaohui**); 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, 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,

(54) **Title:** PACKET PROCESSING METHOD AND APPARATUS

(54) 发明名称: 一种报文处理方法及装置

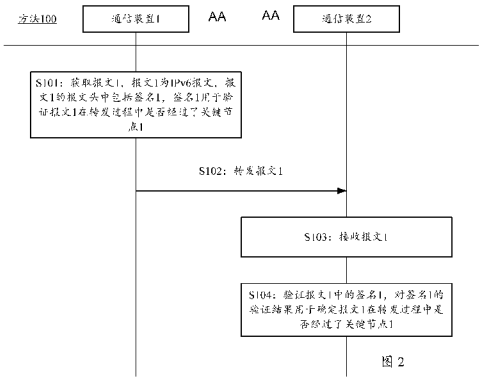



图 2

100 Method
S101 Acquire a packet 1, wherein the packet 1 is an IPv6 packet; a packet header of the packet 1 comprises a signature 1; the signature 1 is used for verifying whether the packet 1 passes through a key node 1 during a forwarding process
S102 Forward the packet 1
S103 Receive the packet 1
S104 Verify the signature 1 of the packet 1, wherein a verification result for the signature 1 is used for determining whether the packet 1 passes through the key node 1 during the forwarding process
AA Communication apparatus

(57) **Abstract:** Disclosed is a packet processing method. The method comprises: on a forwarding path of an IPv6 packet, a key node (e.g. a firewall) signing the packet; and an apparatus downstream of the key node verifying the signature, thereby determining whether the packet passes through the key node during a forwarding process. It can be seen therefrom that the checking of a key node can be executed by using this solution, such that an attacker can be effectively prevented from enabling a packet to bypass a key node by modifying a packet header.

(57) 摘要: 本申请实施例公开了一种报文处理方法。该方法包括：在IPv6报文的转发路径上，关键节点(例如防火墙)对报文进行签名，关键节点下游的装置通过对所述签名进行验证，从而确定报文在转发过程中是否经过了该关键节点。由此可见，利用本方案，可以执行关键节点校验，从而有效避免攻击者通过修改报文头使得报文绕过关键节点。

[见续页]

WO 2022/100153 A1

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))。

# 一种报文处理方法及装置

本申请要求于2020年11月11日递交中国国家知识产权局、申请号为202011256559.2，发明名称为“一种报文处理方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

## 技术领域

本申请涉及通信领域，尤其涉及一种报文处理方法及装置。

## 背景技术

在因特网协议第六版（internet protocol version 6，IPv6）网络中传输的报文，可以被称为IPv6报文。在一些场景中，为保证网络安全，要求IPv6报文在转发的过程中经过特定的关键节点，例如防火墙节点。

IPv6在转发的过程中有可能被恶意篡改，使得该IPv6报文绕过前述关键节点转发，从而带来一定的安全隐患。如何确定IPv6报文在转发过程中是否经过了前述关键节点，是目前尚待解决的问题。

## 发明内容

本申请实施例提供了一种报文处理方法及装置，可以确定IPv6报文在转发过程中是否经过了特定的关键节点。

第一方面，本申请实施例提供了一种报文处理方法，该方法可以由第一通信装置执行。在一个示例中，第一通信装置可以获取第一IPv6报文，该第一IPv6报文的报文头中包括第一签名，通过对第一签名进行验证，可以确定所述第一IPv6报文在转发过程中是否经过了第二通信装置。此处提及的第二通信装置是第一IPv6报文在转发过程中需要经过的关键节点。第一通信装置获取第一IPv6报文之后，可以转发所述第一IPv6报文。由于第一IPv6报文中包括能够验证该第一IPv6报文在转发过程中是否经过了关键节点的第一签名，因此，接收到所述第一IPv6报文的通信装置即可利用该第一签名确定第一IPv6报文在转发过程中是否经过了关键节点。由此可见，利用本方案，可以确定第一IPv6报文在转发过程中是否经过了关键节点。

在一种实现方式中，所述第一IPv6报文是SRv6报文。对于这种情况，即使被配置进行HMAC校验的节点被网络黑客从SRH的SID list中删除，利用本方案也可以确定第一IPv6报文在转发过程中是否经过了第二通信装置，进而有效识别绕过关键节点的攻击报文

在一种实现方式中，当第一IPv6报文为SRv6报文时，第一签名可以携带在第一IPv6报文的SRH中。

在一种实现方式中，所述SRH包括可以包括扩展的TLV字段，所述第一签名可以携带在所述扩展的TLV字段中。

在一种实现方式中，根据所述第一IPv6报文中的第一内容进行哈希计算，将计算结果与第一签名进行比较。在一个示例中，当第一签名是第二通信装置计算的合法签名时，所

述第一签名可以是所述第二通信装置对上文中所述的第一内容进行哈希计算得到的，即第二通信装置在转发第一IPv6报文时，将第一签名添加到第一IPv6报文中，从而使得下游节点可以根据同样的内容进行计算，将计算结果与所述第一签名进行比较，从而验证所述第一IPv6报文在转发过程中是否经过了关键节点。一种示例中，当第一签名的内容和计算结果不一致时，将报文丢弃。

在一种实现方式中，为了降低第一签名被破解的可能性，所述第一内容可以包括所述第一IPv6报文的净荷中固定长度的数据。因为不同的IPv6报文，其报文净荷对应的数据也不同，因此，利用报文的净荷中固定长度的数据计算签名，可以使得不同IPv6报文所携带的签名不同，从而降低IPv6报文中携带的签名被破解的可能性。另外，为了防止重放攻击，所述第一内容还可以包括防重放攻击校验信息。在又一个示例中，第一内容还可以既包括第一IPv6报文的净荷中固定长度的数据，又包括防重放攻击校验信息。

在一种实现方式中，若所述第一内容包括所述防重放攻击校验信息，为了使得接收到第一IPv6报文的通信装置对第一签名进行验证，所述第一IPv6报文的报文头中还可以包括所述防重放攻击校验信息。所述报文头中携带的防重放攻击校验信息，一方面可以用于使得接收到第一IPv6报文的通信装置对第一签名进行验证，另一方面可以用于使得接收到第一IPv6报文的通信装置验证第一IPv6报文是否为重放报文。

在一种实现方式中，为了使得接收到第一IPv6报文的通信装置确定第一内容所包括的防重放攻击校验信息的具体类型，以便于接收到第一IPv6报文的通信装置验证第一IPv6报文是否为重放报文。所述第一IPv6报文的报文头中还可以包括第一指示信息，第一指示信息用于指示所述第一内容所包括的至少一种防重放攻击校验信息

在一种实现方式中，考虑到报文序列号、时间戳以及随机数均可以达到防止重放攻击的效果，因此，所述防重放攻击校验信息可以包括报文序列号、时间戳以及随机数中的其中一种或者多种。其中，报文序列号可以是第二通信装置为第一IPv6报文分配的报文序列号，时间戳可以是第二通信装置获取第一IPv6报文时第二通信装置本地的时间戳，随机数可以是第二通信装置生成的随机数。

在一种实现方式中，考虑到对于一个通信装置例如通信装置2而言，其转发的IPv6报文的数量有很多。对于其转发的IPv6报文，其中一些报文在转发过程中需要经过的关键节点为防火墙设备，另外一些IPv6报文需要经过的关键节点为其它类型的设备。对于不同类型的关键节点，通信装置2对IPv6报文中的签名进行验证所使用的密钥和/或哈希算法可能各不相同。在一个示例中，通信装置2可以根据关键节点的类型，确定对IPv6报文中携带的签名进行验证所使用的密钥和/或哈希算法。对于这种情况，所述第一IPv6报文的报文头中还可以包括第二指示信息，第二指示信息用于指示第一IPv6报文转发过程中需要经过的第二通信装置的类型。

在一种实现方式中，所述第一通信装置和所述第二通信装置是同一个装置，即第一通信装置是关键节点。此时，所述第一IPv6报文可以是第一通信装置生成的，换言之，关键节点生成所述第一签名，获得包括有所述第一签名的所述第一IPv6报文。在一个示例中，第一通信装置可以根据所述第二通信装置的第一私钥和第一哈希算法，生成所述第一签名。进一步地，生成包括所述第一签名的第一IPv6报文。

在一种实现方式中，所述第一通信装置为所述第二通信装置在所述第一IPv6报文的转发路径上的下游装置，对于这种情况，第一通信装置在转发所述第一IPv6报文之前，可以根据所述第二通信装置的第一公钥和第一哈希算法，对所述第一签名进行验证。在一个示例中，第一通信装置可以在第一签名通过验证的情况下，转发所述第一IPv6报文，从而避免非法报文在网络中继续传输。在另一个示例中，当对所述第一签名验证失败时，丢弃所述第一IPv6报文，避免可能的攻击报文在网络中继续传输，占用网络资源。

在一种实现方式中，第一通信装置可以利用第一公钥和第一哈希算法对第一签名进行验证，其中，所述第一公钥和/或所述第一哈希算法可以是控制管理实体发送给第一通信装置的。对于这种情况，第一通信装置在对第一签名进行验证之前，还可以接收控制管理实体发送的所述第一公钥和/或所述第一哈希算法。

第二方面，本申请实施例提供了一种报文处理方法，该方法可以由第一通信装置执行。在一个示例中，第一通信装置可以接收第一IPv6报文，对所述接收到的第一IPv6报文进行验证，确定所述第一IPv6报文是否包括第二通信装置的第一签名，根据验证结果验证所述第一IPv6报文在转发过程中是否经过了第二通信装置。一个示例中，该第一IPv6报文的报文头中包括所述第一签名，该第一签名可以用于验证所述第一IPv6报文在转发过程中是否经过了第二通信装置。此处提及的第二通信装置，可以是第一IPv6报文在转发过程中需要经过的关键节点。第一通信装置接收第一IPv6报文之后，可以验证所述第一签名，对第一签名的验证结果用于确定所述第一IPv6报文在转发过程中是否经过了第二通信装置。由此可见，利用本方案，第一通信装置可以确定第一IPv6报文在转发过程中是否经过了关键节点。

在一种实现方式中，若第一通信装置对第一签名进行验证之后，确定第一签名未通过验证，则第一通信装置可以丢弃所述第一IPv6报文，从而避免非法报文在网络中继续传输。

在一种实现方式中，所述第一IPv6报文是因特网协议第6版分段路由SRv6报文。

在一种实现方式中，所述第一签名包含在分段路由头SRH中。

在一种实现方式中，所述SRH包括扩展的类型长度值TLV字段，所述扩展的TLV字段包括所述第一签名。

在一种实现方式中，所述第一签名是根据所述第一IPv6报文中的第一内容进行哈希计算所得。

在一种实现方式中，所述第一内容包括以下任意一项或者多项：净荷中固定长度的数据和防重放攻击校验信息。

在一种实现方式中，所述报文头中还包括防重放攻击校验信息。

在一种实现方式中，所述报文头中还包括第一指示信息，所述第一指示信息用于指示所述第一内容包括的至少一种防重放攻击校验信息。

在一种实现方式中，所述防重放攻击校验信息包括以下一种或多种：报文序列号，时间戳以及随机数。

在一种实现方式中，所述报文头还包括第二指示信息，所述第二指示信息用于指示所述第二通信装置的类型。

在一种实现方式中，若第一IPv6报文的报文头中包括第一指示信息，则第一通信装置

可以根据该第一指示信息确定所述第一内容所包括的至少一种防重放攻击校验信息。进一步地，根据所述至少一种防重放攻击校验信息，进行防重放攻击校验，即验证第一IPv6报文是否为重放报文。

在一种实现方式中，若第一指示信息指示所述第一内容包括报文序列号，则第一通信装置可以从第一IPv6报文的报文头中获取序列号1，并确定在一定时间段内第一通信装置是否接收到报文序列号为序列号1的其它IPv6报文。若第一通信装置在一定时间段内未接收到报文序列号为序列号1的其它IPv6报文，则说明第一IPv6报文不是重放报文。若第一通信装置在一定时间段内曾接收到报文序列号为序列号1的其它IPv6报文，则说明第一IPv6报文为重放报文。若第一Pv6报文为重放报文，则第一通信装置可以不必第一签名进行验证，从而节省对第一签名进行验证的资源开销。

在一种实现方式中，若第一指示信息指示所述第一内容包括时间戳，则第一通信装置可以从第一IPv6报文的报文头中获取时间戳1，并确定第一通信装置接收第一IPv6报文的时间戳2，而后计算时间戳2和时间戳1之间的差值。考虑到若第一IPv6报文不是重放报文，则时间戳2和时间戳1之间的差值应当小于或者等于第一阈值，即第一IPv6报文在关键节点1和第一通信装置之间的传输时延小于或者等于第一阈值。而若第一IPv6报文是重放报文，则时间戳2和时间戳1之间的差值则可能大于第一阈值。因此，若所述时间戳2和时间戳1的差值小于或者等于第一阈值，第一通信装置可以确定第一IPv6报文不是重放报文，若所述时间戳2和时间戳1的差值大于第一阈值，第一通信装置可以确定第一IPv6报文为重放报文。若第一Pv6报文为重放报文，则第一通信装置可以不必第一签名进行验证，从而节省对第一签名进行验证的资源开销。

在一种实现方式中，若第一指示信息指示所述第一内容包括随机数，则第一通信装置可以从第一IPv6报文的报文头中获取随机数1，并确定在一定时间段内第一通信装置是否接收到携带随机数为随机数1的其它IPv6报文。若第一通信装置在一定时间段内未接收到携带随机数为随机数1的其它IPv6报文，则说明第一IPv6报文不是重放报文。若第一通信装置在一定时间段内曾接收到携带随机数为随机数1的其它IPv6报文，则说明第一IPv6报文为重放报文。若第一Pv6报文为重放报文，则第一通信装置可以不必第一签名进行验证，从而节省对第一签名进行验证的资源开销。

在一种实现方式中，所述第一签名是利用所述第二通信装置的第一私钥和第一哈希算法生成的。

在一种实现方式中，第一通信装置验证所述第一签名在具体实现时，可以根据所述第二通信装置的第一公钥和第一哈希算法，对所述第一签名进行验证。

在一种实现方式中，所述方法还包括：接收控制管理实体发送的所述第一公钥和/或所述第一哈希算法。

在一种实现方式中，第一通信装置可以基于控制管理实体的指示，对第一签名进行验证。对于这种情况，第一通信装置还可以接收控制管理实体发送的第三指示信息，所述第三指示信息用于指示所述第一通信装置对所述第一签名进行验证。

在一种实现方式中，所述第一通信装置为所述第二通信装置在所述第一IPv6报文的转发路径上的下游装置。

在一种实现方式中，所述第一通信装置是所述第一IPv6报文的SRH中的SID list所指示的尾节点。

第三方面，本申请提供了一种第一通信装置，包括：收发单元和处理单元。所述收发单元用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的收发操作，所述处理单元用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的除收发操作之外的其它操作。

第四方面，本申请提供了一种第一通信装置，所述第一通信装置包括存储器和处理器；所述存储器，用于存储程序代码；所述处理器，用于运行所述程序代码中的指令，使得所述第一通信装置执行以上第一方面以及第一方面任意一项所述的方法。

第五方面，本申请提供了一种第一通信装置，所述第一通信装置包括通信接口和处理器，所述通信接口用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的收发操作，所述处理器用于执行以上第一方面以及第一方面任意一项所述的第一通信装置执行的除收发操作之外的其它操作。

第六方面，本申请提供了一种第一通信装置，包括：收发单元和处理单元。所述收发单元用于执行以上第二方面以及第二方面任意一项所述的第一通信装置执行的收发操作，所述处理单元用于执行以上第二方面以及第二方面任意一项所述的第一通信装置执行的除收发操作之外的其它操作。

第七方面，本申请提供了一种第一通信装置，所述第一通信装置包括存储器和处理器；所述存储器，用于存储程序代码；所述处理器，用于运行所述程序代码中的指令，使得所述第一通信装置执行以上第二方面以及第二方面任意一项所述的方法。

第八方面，本申请提供了一种第一通信装置，所述第一通信装置包括通信接口和处理器，所述通信接口用于执行以上第二方面以及第二方面任意一项所述的第一通信装置执行的收发操作，所述处理器用于执行以上第二方面以及第二方面任意一项所述的第一通信装置执行的除收发操作之外的其它操作。

第九方面，本申请提供了一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有指令，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以及第一方面任意一项所述的方法，或者，使得所述计算机执行以上第二方面以及第二方面任意一项所述的方法。

第十方面，本申请提供了一种通信系统，该通信系统包括以上第三方面或者第四方面或者第五方面所述的第一通信装置，以及以上第六方面或者第七方面或者第八方面所述的第一通信装置。

## 附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图1为一种示例性应用场景示意图；

图2为本申请实施例提供的一种报文处理方法的信令交互图；
图3为本申请实施例提供的一种扩展的TLV字段的示意图；
图4为本申请实施例提供的一种报文处理方法的流程示意图；
图5为本申请实施例提供的一种报文处理方法的流程示意图；
图6为本申请实施例提供的一种通信装置的结构示意图；
图7为本申请实施例提供的一种通信装置的结构示意图；
图8为本申请实施例提供的一种通信装置的结构示意图。

## 具体实施方式

本申请实施例提供了一种报文处理方法及装置，可以确定IPv6报文在转发过程中是否经过了关键节点。

为方便理解，首先对本申请实施例可能的应用场景进行介绍。

因特网协议第6版段路由（Segment Routing Internet Protocol Version 6，SRv6）技术，可以将分段路由（segment routing，SR）技术应用于因特网协议第六版（internet protocol version 6，IPv6）报文的转发。其中，利用SRv6技术转发的报文，可以称为SRv6报文。

SRv6报文的报文头包括分段路由头（segment routing header，SRH）。SRH包括段标识列表（segment identifier list，SID list），该SID list用于指示SRv6报文的转发路径。因此，对于SRv6报文而言，可以通过SRH中的SID list确定其在转发过程中是否经过了关键节点。

但是，SRv6报文在转发过程中可能被篡改，换言之，SRv6报文的SID list在转发过程中也可能会被篡改。若SID list被篡改，则根据该SID list则不能准确的确定SRv6报文在转发过程中是否经过了关键节点。

本申请的发明人发现，目前，可以通过密钥相关的哈希运算消息认证码（hashed-based message authentication code，HMAC）校验，来确定SRv6报文的SRH是否被篡改。相应的，在SRH没有被篡改的情况下，根据SRH中的SID list确定其在转发过程中是否经过了关键节点。关于HMAC校验，可以参考因特网工程任务组（internet engineering task framework，IETF）制定的征求意见稿RFC8754中的相关描述，此处不做详细描述。

但是，这种方式也会存在一些问题。例如，网络黑客将被配置进行HMAC校验的节点从该SRv6报文的SID list删除，则该SRv6报文在转发过程中不再经过该被配置进行HMAC校验的节点。相应的，该被配置进行HMAC校验的节点也不能再对该SRv6报文进行HMAC校验。这就导致该SRv6报文的SID list的合法性无法确定，进一步的也无法根据该SID list确定该SRv6报文在转发过程中是否经过了关键节点。

现结合图1所示的场景进行介绍。图1为一种示例性应用场景示意图。

如图1所示，正常情况下，SRv6报文的转发路径为通信装置R1-通信装置R2-防火墙FW1-通信装置R3-通信装置R4-服务器S1。其中，防火墙FW1为SRv6报文转发过程中需要经过的关键节点。通信装置R2被配置进行HMAC校验，以验证该SRv6报文的SID list是否被篡改。但是，若网络黑客对该SRv6报文的SID list进行了修改，将通信装置R2的SID从该SID list中删除，则篡改后的SRv6报文的不再经过通信装置R2转发，因此，通信装置R2也不能对该SRv6报文进行HMAC校验。从而无法判断该SRv6报文的SID list是否被篡改。相应的，其它

通信装置也无法根据该SID list确定SRv6报文在转发过程中是否经过了关键节点。另外，在一些示例中，网络黑客除了将通信装置R2的SID从该SID list中删除之外，还可以将防火墙FW1的SID从该SID list中删除，从而使得该报文绕过关键节点（防火墙FW1）转发。

为了解决上述问题，本申请实施例提供了一种报文处理方法，以下结合附图介绍该方法。

在介绍本申请实施例提供的报文处理方法之前，需要说明的是，图1只是为了方便理解而示出，其并不构成对本申请实施例的限定。而且，被配置进行HMAC校验的节点除了是通信装置R2之外，还可以是通信装置R3、通信装置R4或者通信装置R5。SRv6报文转发过程中必须经过的关键节点，除了可以是图1所示的防火墙之外，还可以是其它类型设备，例如可以是防止拒绝服务（denial of service，DoS）攻击的服务器。

本申请实施例中提及的通信装置，可以是交换机、路由器等网络设备，也可以是网络设备上的一部分组件，例如是网络设备上的单板，线卡，还可以是网络设备上的一个功能模块，本申请实施例不做具体限定。通信装置之间例如可以通过以太网线或光缆直接连接。

图2为本申请实施例提供的一种报文处理方法的信令交互图。图2所示的报文处理方法100，例如可以包括如下S101-S104。

S101：通信装置1获取报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1。

此处提及的通信装置1，例如可以是图1所示的防火墙FW1、通信装置R3、通信装置R4或者服务器S1。此处提及的关键节点1，例如可以是图1所示的防火墙FW1。

在本申请实施例中，通信装置1获取报文1在具体实现时，可以有多种实现方式。

在一个示例中，通信装置1作为报文1的转发路径上、所述关键节点1的下游装置，则通信装置1可以接收上游装置发送的报文1。此处提及的上游装置，例如可以是所述关键节点1。

在一个示例中，通信装置1可以为所述关键节点1，即通信装置1和所述关键节点1是同一个通信装置。对于这种情况，通信装置1可以生成报文1。在一个示例中，通信装置1可以接收其它通信装置发送的报文2，对报文2进行重新封装，得到包括签名1的报文1。换言之，关键节点1接收到报文2之后，对报文2进行签名，以说明报文2在转发过程中经过了所述关键节点1。关键节点1对报文2进行签名之后得到包括签名1的报文1，报文1中的签名1可以用于确定报文1在转发过程中是否经过了所述关键节点1。此处提及的报文2，也可以是IPv6报文。在一些实施例中，所述签名1可以携带在报文1的报文的扩展的类型长度值（type length value，TLV）字段中。

在本申请实施例的一种实现方式中，签名1可以是关键节点1对报文1中的第一内容进行哈希计算得到的。在一个示例中，关键节点1可以对利用关键节点1自身的第一私钥和第一哈希算法对第一内容进行计算，从而得到所述签名1。例如，关键节点1可以利用第一哈希算法对第一内容进行计算，得到摘要1，而后利用第一私钥对所述摘要1进行加密，得到所述签名1。

本申请实施例不具体限定所述第一内容，在一个示例中，为了降低签名1被破解的可能性，所述第一内容可以包括所述报文1的净荷中固定长度的数据。因为不同的IPv6报文，其报文净荷对应的数据也不同，因此，利用报文的净荷中固定长度的数据计算签名，可以使

得不同IPv6报文所携带的签名不同，从而降低IPv6报文中携带的签名被破解的可能性。在另一个示例中，为了防止重放攻击，所述第一内容还可以包括防重放攻击校验信息。在又一个示例中，第一内容还可以既包括报文1的净荷中固定长度的数据，又包括防重放攻击校验信息。

本申请实施例不具体限定所述防重放攻击校验信息，考虑到报文序列号、时间戳以及随机数均可以达到防止重放攻击的效果，因此，所述防重放攻击校验信息可以包括报文序列号、时间戳以及随机数中的其中一种或者多种。其中，报文序列号可以是关键节点1为报文1分配的报文序列号，时间戳可以是关键节点1获取报文1时关键节点1本地的时间戳，随机数可以是关键节点1生成的随机数。

在本申请实施例的一种实现方式中，若所述第一内容包括所述防重放攻击校验信息，为了使得接收到报文1的通信装置对签名1进行验证，所述报文1的报文头中还可以包括所述防重放攻击校验信息。所述报文头中携带的防重放攻击校验信息，一方面可以用于使得接收到报文1的通信装置对签名1进行验证，另一方面可以用于使得接收到报文1的通信装置验证报文1是否为重放报文。在一个示例中，所述防重放攻击校验信息和所述签名1可以携带在同一个扩展的TLV字段中。在又一个示例中，所述防重放攻击校验信息可以携带在一个单独的扩展的TLV字段中。

在本申请实施例的一种实现方式中，为了使得接收到报文1的通信装置确定第一内容所包括的防重放攻击校验信息具体是哪一种或者哪几种防重放攻击校验信息，以便于接收到报文1的通信装置验证报文1是否为重放报文。所述报文1的报文头中还可以包括指示信息1，指示信息1用于指示所述第一内容所包括的至少一种防重放攻击校验信息。在一个示例中，报文1的报文头中包括第一指示位，第二指示位和第三指示位，第一指示位，第二指示位和第三指示位用于携带所述指示信息1。其中，第一指示位用于指示第一内容包括的防重放攻击校验信息是否包括报文序列号，第二指示位用于指示第一内容包括的防重放攻击校验信息是否包括时间戳，第三指示位用于指示第一内容包括的防重放攻击校验信息是否包括随机数。

举例说明，第一指示位、第二指示位和第三指示位各占1比特。当第一指示位的值为1时，说明第一内容包括的防重放攻击校验信息包括报文序列号，当第一指示位的值为0时，说明第一内容包括的防重放攻击校验信息不包括报文序列号；当第二指示位的值为1时，说明第一内容包括的防重放攻击校验信息包括时间戳，当第二指示位的值为0时，说明第一内容包括的防重放攻击校验信息不包括报文时间戳；当第三指示位的值为1时，说明第一内容包括的防重放攻击校验信息包括随机数，当第三指示位的值为0时，说明第一内容包括的防重放攻击校验信息不包括报文随机数。

在一个示例中，所述防重放攻击校验信息和所述指示信息1可以携带在同一个扩展的TLV字段中。在又一个示例中，所述指示信息1可以携带在一个单独的扩展的TLV字段中。

在一种实现方式中，考虑到对于一个通信装置例如通信装置2而言，其转发的IPv6报文的数量有很多。对于其转发的IPv6报文，其中一些报文在转发过程中需要经过的关键节点为防火墙设备，另外一些IPv6报文需要经过的关键节点为其它类型的设备，例如防止DoS攻击的服务器。对于不同类型的关键节点，通信装置2对IPv6报文中的签名进行验证所使用

的密钥和/或哈希算法可能各不相同。在一个示例中，通信装置2可以根据关键节点的类型，确定对IPv6报文中携带的签名进行验证所使用的密钥和/或哈希算法。对于这种情况，所述报文1的报文头中还可以包括指示信息2，指示信息2用于指示报文1转发过程中需要经过的关键节点1的类型。在一个示例中，所述指示信息2和所述签名1可以携带在同一个扩展的TLV字段中。在又一个示例中，所述指示信息2可以携带在一个单独的扩展的TLV字段中。

在本申请实施例的一种实现方式中，所述报文1的报文头包括SRH，换言之，报文1可以是SRv6报文。在一种实现方式中，当报文1是SRv6报文时，前述签名1可以携带在报文1的SRH中。在一个示例中，报文1的SRH可以包括扩展的TLV字段，所述签名1可以携带在所述扩展的TLV字段中。

在一个示例中，前述签名1、放重放攻击校验信息、指示信息1和指示信息2，可以携带在同一个扩展的TLV字段中。可结合图3进行理解，图3为本申请实施例提供的一种扩展的TLV字段的示意图。其中：

节点类型字段用于携带指示关键节点1的类型的指示信息2。

S（sequence）指示位可以相当于上文提及的第一指示位，用于指示第一内容包括的防重放攻击校验信息是否包括报文序列号；T（timestamp）指示位可以相当于上文提及的第二指示位，用于指示第一内容包括的防重放攻击校验信息是否包括时间戳；N（nounce）指示位可以相当于上文提及的第三指示位，用于指示第一内容包括的防重放攻击校验信息是否包括随机数。

sequence字段用于携带序列号。sequence字段在所述S指示位指示第一内容包括的防重放攻击校验信息包括报文序列号时有效。在一个示例中，若S指示位指示第一内容包括的防重放攻击校验信息不包括报文序列号，则所述TLV字段可以不包括所述sequence字段。

timestamp字段用于携带时间戳。timestamp字段在S指示位指示第一内容包括的防重放攻击校验信息包括时间戳时有效。在一个示例中，若S指示位指示第一内容包括的防重放攻击校验信息不包括时间戳，则所述TLV字段可以不包括所述timestamp字段。

nounce字段用于携带随机数。nounce字段在N指示位指示第一内容包括的防重放攻击校验信息包括随机数时有效。在一个示例中，若N指示位指示第一内容包括的防重放攻击校验信息不包括随机数，则所述TLV字段可以不包括所述nounce字段。

signature字段用于携带签名1。

在一个示例中，图3所示的扩展的TLV字段，可以位于SRH中，例如所述扩展的TLV字段可以位于SID list之后。

S102：通信装置1转发报文1。

S103：通信装置2接收报文1。

通信装置1可以获取报文1之后，可以转发所述报文1，通信装置2作为报文1的转发路径上、所述通信装置1的下游装置，可以接收所述通信装置1发送的所述报文1。此处提及的通信装置2，可以是图1所示通信装置R3、通信装置R4或者服务器S1。在一个示例中，当所述报文1为SRv6报文时，所述通信装置2可以是报文1的SRH中的SID list所指示的尾节点，例如通信装置2是图1所示的服务器S1。

S104：通信装置2验证报文1中的签名1，对签名1的验证结果用于确定报文1在转发过程

中是否经过了关键节点1。

通信装置2接收到报文1之后，可以对报文1中的签名1进行验证，以确定报文1在转发过程中是否经过了关键节点1。

如前S101中所述，在一个示例中，签名1可以是所述关键节点1利用关键节点1的第一私钥和第一哈希算法生成的。因此，通信装置2可以利用关键节点1的第一公钥和第一哈希算法，对所述签名1进行验证。其中，所述第一公钥和第一私钥构成一组公私钥对。在一个示例中，通信装置2可以利用第一公钥对签名1进行解密，得到摘要2，并利用第一哈希算法对第一内容进行哈希计算，得到摘要3，然后对摘要2和摘要3进行匹配验证。在一个示例中，若摘要2和摘要3相同，则确定签名1通过验证，若摘要2和摘要3不同，则确定签名1未通过验证。

若签名1通过验证，则通信装置2可以确定报文1在转发过程中经过了关键节点1。对于这种情况，通信装置1例如可以继续转发报文1。若签名1未通过验证，说明报文1在转发过程中被篡改了，对于这种情况，通信装置2可以丢弃报文1。

在本申请实施例的一种实现方式中，通信装置2可以基于控制管理实体的指示，对签名1进行验证。换言之，通信装置2在对签名1进行验证之前，还可以接收控制管理实体发送的指示信息3，并根据所述指示信息3对签名1进行验证，其中，指示信息3用于指示通信装置1对签名1进行验证。

在本申请实施例的一种实现方式中，通信装置2对签名1进行验证的第一公钥和/或第一哈希算法，也可以是控制管理实体发送给通信装置2的。换言之，在通信装置2对签名1进行验证之前，还可以接收控制管理实体发送的所述第一公钥和/或第一哈希算法。

本申请实施例中提及的控制管理实体例如可以为运行了网络管理软件（network manage system，NMS）的设备，又如可以为控制器。控制管理实体，可以是实现控制和/或管理功能的功能模块，也可以是运行了相关功能模块的物理实体，上述物理实体例如可以是安装了相关软件的服务器，相关软件用于实现控制管理实体的功能。本申请实施例不做具体限定。

如前文，所述第一内容可以包括防重放攻击校验信息。当所述第一内容可以包括防重放攻击校验信息时，报文1的报文头中可以包括所述防重放攻击校验信息。对于这种情况，通信装置2在对签名1进行验证之前，还可以根据该防重放攻击校验信息验证报文1是否为重放报文。若报文1为重放报文，则通信装置1可以不执行对签名1进行校验的步骤，直接丢弃报文1；若报文1不是重放报文，通信装置2可以执行对签名1进行验证的步骤。

在一个示例中，若报文1的报文头中包括指示信息1，则通信装置2可以根据该指示信息1确定所述第一内容所包括的至少一种防重放攻击校验信息。进一步地，根据所述至少一种防重放攻击校验信息，验证报文1是否为重放报文。

在一个示例中，若指示信息1指示所述第一内容包括报文序列号，则通信装置2可以从报文1的报文头中获取序列号1，并确定在一定时间段内通信装置2是否接收到报文序列号为序列号1的其它IPv6报文。若通信装置2在一定时间段内未接收到报文序列号为序列号1的其它IPv6报文，则说明报文1不是重放报文。若通信装置2在一定时间段内曾接收到报文序列号为序列号1的其它IPv6报文，则说明报文1为重放报文。

在一种实现方式中，通信装置2本地可以存储有一定时间段内接收到的IPv6报文的报文序列号，并将所述序列号1与预先存储的报文序列号进行比对。若预先存储的报文序列号中包括所述序列号1，则说明在一定时间段内通信装置2曾经接收到报文序列号为序列号1的其它IPv6报文；若预先存储的报文序列号中不包括所述序列号1，则说明在一定时间段内通信装置2未接收到报文序列号为序列号1的其它IPv6报文。

在一个示例中，若指示信息1指示所述第一内容包括时间戳，则通信装置2可以从报文1的报文头中获取时间戳1，并确定通信装置2接收报文1的时间戳2，而后计算时间戳2和时间戳1之间的差值。考虑到若报文1不是重放报文，则时间戳2和时间戳1之间的差值应当小于第一阈值，即报文1在关键节点1和通信装置2之间的传输时延小于第一阈值。而若报文1是重放报文，则时间戳2和时间戳1之间的差值则可能大于或者等于第一阈值。因此，若所述时间戳2和时间戳1的差值小于第一阈值，通信装置2可以确定报文1不是重放报文，若所述时间戳2和时间戳1的差值大于或者等于第一阈值，通信装置2可以确定报文1为重放报文。其中，时间戳2为通信装置2接收到报文1时，通信装置2的本地时间戳。

在一个示例中，若指示信息1指示所述第一内容包括随机数，则通信装置2可以从报文1的报文头中获取随机数1，并确定在一定时间段内通信装置2是否接收到携带随机数为随机数1的其它IPv6报文。若通信装置2在一定时间段内未接收到携带随机数为随机数1的其它IPv6报文，则说明报文1不是重放报文。若通信装置2在一定时间段内曾接收到携带随机数为随机数1的其它IPv6报文，则说明报文1为重放报文。

在一种实现方式中，通信装置2本地可以存储有一定时间段内接收到的IPv6报文所携带的随机数，并将所述随机数1与预先存储的随机数进行比对。若预先存储的随机数中包括所述随机数1，则说明在一定时间段内通信装置2曾经接收到携带随机数为随机数1的其它IPv6报文；若预先存储的随机数中不包括所述随机数1，则说明在一定时间段内通信装置2未接收到携带随机数为所述随机数1的其它IPv6报文。

如前所述，通信装置1和所述关键节点1可以是同一个装置，也可以是不同的装置。当通信装置1和所述关键节点是不同的装置时，通信装置1可以是报文1的转发路径中、所述关键结点1的下游装置。对于这种情况，通信装置1在转发报文1之前，还可以对签名1进行验证，并在签名1通过验证的情况下，转发报文1。关于通信装置1对签名1进行验证的具体实现，可以参考上文S104通信装置2对签名1进行验证的描述部分，此处不再重复描述。

通过以上描述可知，利用方法100，报文1的转发路径中所述关键节点1的下游装置，可以通过对签名1进行验证，从而确定报文1在转发过程中是否经过了所述关键节点1。当报文1是SRv6报文时，方法100可以克服上文对于图1的描述部分提及的由于被配置进行HMAC校验的节点被网络黑客从SRH的SID list中删除，从而导致无法通过SID list确定报文1在转发过程中是否经过了关键节点1的问题。

图4为本申请实施例提供的一种报文处理方法的流程示意图。图4所示的报文处理方法200，可以由第一通信装置执行。第一通信装置可以为以上实施例中的通信装置1。用于执行以上方法100中通信装置1执行的步骤。所述方法200例如可以包括如下S201-S202。

S201：获取第一IPv6报文，所述第一IPv6报文的报文头中包括第一签名，所述第一签名用于验证所述第一IPv6报文在转发过程中是否经过了第二通信装置。

S202：转发所述第一IPv6报文。

此处提及的第一IPv6报文，可以对应方法100中的报文1，此处提及的第一签名，可以对应方法100中的签名1，此处提及的第二通信装置，可以对应方法100中的关键节点1。

在一种实现方式中，所述第一IPv6报文是因特网协议第6版分段路由SRv6报文。

在一种实现方式中，所述第一签名包含在分段路由头SRH中。

在一种实现方式中，所述SRH包括扩展的类型长度值TLV字段，所述扩展的TLV字段包括所述第一签名。

在一种实现方式中，所述第一签名是根据所述第一IPv6报文中的第一内容进行哈希计算所得。

在一种实现方式中，所述第一内容包括以下一项或多项：

净荷中固定长度的数据和防重放攻击校验信息。

在一种实现方式中，所述报文头中还包括防重放攻击校验信息。

在一种实现方式中，所述报文头中还包括第一指示信息，所述第一指示信息用于指示所述第一内容包括的至少一种防重放攻击校验信息。

此处提及的第一指示信息，可以对应方法100中的指示信息1。

在一种实现方式中，所述防重放攻击校验信息包括以下一种或多种：

报文序列号，时间戳以及随机数。

在一种实现方式中，所述报文头还包括第二指示信息，所述第二指示信息用于指示所述第二通信装置的类型。

此处提及的第二指示信息，可以对应方法100中的指示信息2。

在一种实现方式中，所述第一通信装置和所述第二通信装置是同一个装置，所述获取所述第一IPv6报文包括：

根据所述第二通信装置的第一私钥，生成所述第一签名。

在一种实现方式中，所述第一通信装置为所述第二通信装置在所述第一IPv6报文的转发路径上的下游装置，所述转发所述第一IPv6报文之前，所述方法还包括：

根据所述第二通信装置的第一公钥，对所述第一签名进行验证。

在一种实现方式中：接收控制管理实体发送的所述第一公钥和/或计算签名所需的第一哈希算法。

图5为本申请实施例提供的一种报文处理方法的流程示意图。图5所示的报文处理方法300，可以由第一通信装置执行。第一通信装置可以为以上实施例中的通信装置2。用于执行以上方法100中通信装置2执行的步骤。所述方法300例如可以包括如下S301-S302。

S301：接收第一IPv6报文，所述第一IPv6报文包括第一签名，所述第一签名用于验证所述第一IPv6报文的转发路径是否经过了第二通信装置。

S302：验证所述第一签名，验证结果用于确定所述第一IPv6报文在转发过程中是否经过了所述第二通信装置。

此处提及的第一IPv6报文，可以对应方法100中的报文1，此处提及的第一签名，可以对应方法100中的签名1，此处提及的第二通信装置，可以对应方法100中的关键节点1。

在一种实现方式中，所述方法还包括：

若验证不通过，则丢弃所述第一IPv6报文。

在一种实现方式中，所述第一IPv6报文是因特网协议第6版分段路由SRv6报文。

在一种实现方式中，所述第一签名包含在分段路由头SRH中。

在一种实现方式中，所述SRH包括扩展的类型长度值TLV字段，所述扩展的TLV字段包括所述第一签名。

在一种实现方式中，所述第一签名是根据所述第一IPv6报文中的第一内容进行哈希计算所得。

在一种实现方式中，所述第一内容包括以下任意一项或者多项：

净荷中固定长度的数据和防重放攻击校验信息。

在一种实现方式中，所述报文头中还包括防重放攻击校验信息。

在一种实现方式中，所述报文头中还包括第一指示信息，所述第一指示信息用于指示所述第一内容包括的至少一种防重放攻击校验信息。

此处提及的第一指示信息，可以对应方法100中的指示信息1。

在一种实现方式中，所述防重放攻击校验信息包括以下一种或多种：

报文序列号，时间戳以及随机数。

在一种实现方式中，所述报文头还包括第二指示信息，所述第二指示信息用于指示所述第二通信装置的类型。

此处提及的第二指示信息，可以对应方法100中的指示信息2。

在一种实现方式中，若所述第一指示信息指示所述第一内容包括报文序列号，在验证所述第一签名之前，所述方法还包括：

确定在一定时间段内所述第一通信装置未接收到序列号与所述第一IPv6报文中携带的所述序列号相同的其它IPv6报文。

在一种实现方式中，若所述第一指示信息指示所述第一内容包括时间戳，在验证所述第一签名之前，所述方法还包括：

获取所述第一通信装置接收所述第一IPv6报文时的第一时间戳；

确定第一时间戳与所述第一IPv6报文中携带的所述时间戳之间的差值小于第一阈值。

在一种实现方式中，若所述第一指示信息指示所述第一内容包括随机数，在验证所述第一签名之前，所述方法还包括：

确定在一定时间段内所述第一通信装置未接收到携带随机数与所述第一IPv6报文中携带的所述随机数相同的其它IPv6报文。

在一种实现方式中，所述第一签名是利用所述第二通信装置的第一私钥生成的。

在一种实现方式中，所述验证所述第一签名，包括：

根据所述第二通信装置的第一公钥，对所述第一签名进行验证。

在一种实现方式中，所述方法还包括：

接收控制管理实体发送的所述第一公钥和/或计算签名所需的第一哈希算法。

在一种实现方式中，所述方法还包括：

接收控制管理实体发送的第三指示信息，所述第三指示信息用于指示所述第一通信装置对所述第一签名进行验证。

此处提及的第三指示信息，可以对应方法100中的指示信息3。

在一种实现方式中，所述第一通信装置为所述第二通信装置在所述第一IPv6报文的转发路径上的下游装置。

在一种实现方式中，所述第一通信装置是所述第一IPv6报文的SRH中的SID list所指示的尾节点。

关于以上方法200以及方法300的具体实现，可以参考上文对于方法100的描述部分，此处不做详述。

此外，本申请实施例还提供了一种通信装置600，参见图6所示。图6为本申请实施例提供的一种通信装置的结构示意图。该通信装置600包括收发单元601和处理单元602。该通信装置600可以用于执行以上实施例中的方法100、方法200或者方法300。

在一个示例中，所述通信装置600可以执行以上实施例中的方法100，当通信装置600用于执行以上实施例中的方法100时，通信装置600相当于方法100中的通信装置1。收发单元601用于执行方法100中通信装置1执行的收发操作。处理单元602用于执行方法100中通信装置1执行的除收发操作之外的操作。例如：处理单元602用于获取报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1；收发单元601用于转发报文1。

在一个示例中，所述通信装置600可以执行以上实施例中的方法100，当通信装置600用于执行以上实施例中的方法100时，通信装置600相当于方法100中的通信装置2。收发单元601用于执行方法100中通信装置2执行的收发操作。处理单元602用于执行方法100中通信装置2执行的除收发操作之外的操作。例如：收发单元601用于接收报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1；处理单元602用于验证报文1中的签名1，对签名1的验证结果用于确定报文1在转发过程中是否经过了关键节点1。

在一个示例中，所述通信装置600可以执行以上实施例中的方法200，当通信装置600用于执行以上实施例中的方法200时，通信装置600相当于方法200中的第一通信装置。收发单元601用于执行方法200中第一通信装置执行的收发操作。处理单元602用于执行方法200中第一通信装置执行的除收发操作之外的操作。例如：处理单元602用于获取第一因特网协议第6版IPv6报文，所述第一IPv6报文的报文头中包括第一签名，所述第一签名用于验证所述第一IPv6报文在转发过程中是否经过了第二通信装置；收发单元601用于转发所述第一IPv6报文。

在一个示例中，所述通信装置600可以执行以上实施例中的方法300，当通信装置600用于执行以上实施例中的方法300时，通信装置600相当于方法300中的第一通信装置。收发单元601用于执行方法300中第一通信装置执行的收发操作。处理单元602用于执行方法300中第一通信装置执行的除收发操作之外的操作。例如：收发单元601用于接收第一IPv6报文，所述第一IPv6报文包括第一签名，所述第一签名用于验证所述第一IPv6报文的转发路径是否经过了第二通信装置；处理单元602用于验证所述第一签名，验证结果用于确定所述第一IPv6报文在转发过程中是否经过了所述第二通信装置。

此外，本申请实施例还提供了一种通信装置700，参见图7所示，图7为本申请实施例提

供的一种通信装置的结构示意图。该通信装置700包括通信接口701和与通信接口701连接的处理器702。该通信装置700可以用于执行以上实施例中的方法100、方法200或者方法300。

在一个示例中，所述通信装置700可以执行以上实施例中的方法100，当通信装置700用于执行以上实施例中的方法100时，通信装置700相当于方法100中的通信装置1。通信接口701用于执行方法100中通信装置1执行的收发操作。处理器702用于执行方法100中通信装置1执行的除收发操作之外的操作。例如：处理器702用于获取报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1；通信接口701用于转发报文1。

在一个示例中，所述通信装置700可以执行以上实施例中的方法100，当通信装置700用于执行以上实施例中的方法100时，通信装置700相当于方法100中的通信装置2。通信接口701用于执行方法100中通信装置2执行的收发操作。处理器702用于执行方法100中通信装置2执行的除收发操作之外的操作。例如：通信接口701用于接收报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1；处理器702用于验证报文1中的签名1，对签名1的验证结果用于确定报文1在转发过程中是否经过了关键节点1。

在一个示例中，所述通信装置700可以执行以上实施例中的方法200，当通信装置700用于执行以上实施例中的方法200时，通信装置700相当于方法200中的第一通信装置。通信接口701用于执行方法200中第一通信装置执行的收发操作。处理器702用于执行方法200中第一通信装置执行的除收发操作之外的操作。例如：处理器702用于获取第一因特网协议第6版IPv6报文，所述第一IPv6报文的报文头中包括第一签名，所述第一签名用于验证所述第一IPv6报文在转发过程中是否经过了第二通信装置；通信接口701用于转发所述第一IPv6报文。

在一个示例中，所述通信装置700可以执行以上实施例中的方法300，当通信装置700用于执行以上实施例中的方法300时，通信装置700相当于方法300中的第一通信装置。通信接口701用于执行方法300中第一通信装置执行的收发操作。处理器702用于执行方法300中第一通信装置执行的除收发操作之外的操作。例如：通信接口701用于接收第一IPv6报文，所述第一IPv6报文包括第一签名，所述第一签名用于验证所述第一IPv6报文的转发路径是否经过了第二通信装置；处理器702用于验证所述第一签名，验证结果用于确定所述第一IPv6报文在转发过程中是否经过了所述第二通信装置。

此外，本申请实施例还提供了一种通信装置800，参见图8所示，图8为本申请实施例提供的一种通信装置的结构示意图。

该通信装置800可以用于执行以上实施例中的方法100、方法200、或者方法300。

如图8所示，通信装置800可以包括处理器810，与所述处理器810耦合连接的存储器820，收发器830。收发器830例如可以是通信接口，光模块等。处理器810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810可以是指一个处理器，也可以包括多个处理器。存储器820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820还可以包括上述种类的存储器的组合。存储器820可以是指一个存储器，也可以包括多个存储器。在一个实施方式中，存储器820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821，处理模块822和接收模块823。处理器810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810根据所述软件模块的指示而执行的操作。

在一个示例中，所述通信装置800可以执行以上实施例中的方法100，当通信装置800用于执行以上实施例中的方法100时，通信装置800相当于方法100中的通信装置1。收发器830用于执行方法100中通信装置1执行的收发操作。处理器810用于执行方法100中通信装置1执行的除收发操作之外的操作。例如：处理器810用于获取报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1；收发器830用于转发报文1。

在一个示例中，所述通信装置800可以执行以上实施例中的方法100，当通信装置800用于执行以上实施例中的方法100时，通信装置800相当于方法100中的通信装置2。收发器830用于执行方法100中通信装置2执行的收发操作。处理器810用于执行方法100中通信装置2执行的除收发操作之外的操作。例如：收发器830用于接收报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1；处理器810用于验证报文1中的签名1，对签名1的验证结果用于确定报文1在转发过程中是否经过了关键节点1。

在一个示例中，所述通信装置800可以执行以上实施例中的方法200，当通信装置800用于执行以上实施例中的方法200时，通信装置800相当于方法200中的第一通信装置。收发器830用于执行方法200中第一通信装置执行的收发操作。处理器810用于执行方法200中第一通信装置执行的除收发操作之外的操作。例如：处理器810用于获取第一因特网协议第6版IPv6报文，所述第一IPv6报文的报文头中包括第一签名，所述第一签名用于验证所述第一IPv6报文在转发过程中是否经过了第二通信装置；收发器830用于转发所述第一IPv6报文。

在一个示例中，所述通信装置800可以执行以上实施例中的方法300，当通信装置800用于执行以上实施例中的方法300时，通信装置800相当于方法300中的第一通信装置。收发器830用于执行方法300中第一通信装置执行的收发操作。处理器810用于执行方法300中第一通信装置执行的除收发操作之外的操作。例如：收发器830用于接收第一IPv6报文，所述第一IPv6报文包括第一签名，所述第一签名用于验证所述第一IPv6报文的转发路径是否经过了第二通信装置；处理器810用于验证所述第一签名，验证结果用于确定所述第一IPv6报

文在转发过程中是否经过了所述第二通信装置。

本申请还提供了一种计算机可读存储介质，所述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前述实施例中任一实施例所述的方法（例如，方法100，方法200和方法300）中任意一个或多个操作。

本申请还提供了一种计算机程序产品，包括计算机程序，当其在计算机上运行时，使得所述计算机执行前述实施例中任一实施例所述的方法（例如，方法100，方法200和方法300）中任意一个或多个操作。

本申请还提供了一种通信系统，包括以上实施例提及的任一种执行方法200的第一通信装置和任一种执行方法300的第一通信装置。通信系统还可以包括前文所述的控制管理实体，用于实现上述实施例有控制管理实体所执行的操作。

本申请还提供了一种通信系统，包括至少一个存储器和至少一个处理器，该至少一个存储器存储有指令，该至少一个处理器执行所述指令，使得所述通信系统执行本申请前述实施例中任一实施例所述的方法（例如，方法100，方法200和方法300）中任意一个或多个操作。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

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

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

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

另外，在本申请各个实施例中的各业务单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件业务单元的形式实现。

集成的单元如果以软件业务单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，

该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的业务可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些业务存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

以上的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上仅为本发明的具体实施方式而已。

以上，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

# 权 利 要 求

1.一种报文处理方法，其特征在于，由第一通信装置执行，所述方法包括：

获取第一因特网协议第6版IPv6报文，所述第一IPv6报文的报文头中包括第一签名，所述第一签名用于验证所述第一IPv6报文在转发过程中是否经过了第二通信装置；

转发所述第一IPv6报文。

2.根据权利要求1所述的方法，其特征在于，所述第一IPv6报文是因特网协议第6版分段路由SRv6报文。

3.根据权利要求2所述的方法，其特征在于，所述第一签名包含在分段路由头SRH中。

4.根据权利要求3所述的方法，其特征在于，所述SRH包括扩展的类型长度值TLV字段，所述扩展的TLV字段包括所述第一签名。

5.根据权利要求1-4任意一项所述的方法，其特征在于，所述第一签名是根据所述第一IPv6报文中的第一内容进行哈希计算所得。

6.根据权利要求5所述的方法，其特征在于，所述第一内容包括以下一项或多项：

净荷中固定长度的数据和防重放攻击校验信息。

7.根据权利要求1-6任一项所述的方法，其特征在于，所述报文头中还包括防重放攻击校验信息。

8.根据权利要求5或6所述的方法，其特征在于，所述报文头中还包括第一指示信息，所述第一指示信息用于指示所述第一内容包括的至少一种防重放攻击校验信息。

9.根据权利要求7或8所述的方法，其特征在于，所述防重放攻击校验信息包括以下一种或多种：

报文序列号，时间戳以及随机数。

10.根据权利要求1-9任意一项所述的方法，其特征在于，所述报文头还包括第二指示信息，所述第二指示信息用于指示所述第二通信装置的类型。

11.根据权利要求1-10任意一项所述的方法，其特征在于，所述第一通信装置和所述第二通信装置是同一个装置，所述获取所述第一IPv6报文包括：

根据所述第二通信装置的第一私钥，生成所述第一签名。

12.根据权利要求1-10任一项所述的方法，其特征在于，所述第一通信装置为所述第二通信装置在所述第一IPv6报文的转发路径上的下游装置，所述转发所述第一IPv6报文之前，所述方法还包括：

根据所述第二通信装置的第一公钥，对所述第一签名进行验证。

13.根据权利要求12所述的方法，其特征在于，所述方法还包括：接收控制管理实体发送的所述第一公钥。

14.一种报文处理方法，其特征在于，由第一通信装置执行，所述方法包括：

接收第一因特网协议第6版IPv6报文，所述第一IPv6报文包括第一签名，所述第一签名用于验证所述第一IPv6报文的转发路径是否经过了第二通信装置；

验证所述第一签名，根据验证结果处理所述第一IPv6报文。

15.根据权利要求14所述的方法，其特征在于，所述方法还包括：

若验证不通过，则丢弃所述第一IPv6报文。

16.根据权利要求14或15所述的方法，其特征在于，所述第一IPv6报文是因特网协议第6版分段路由SRv6报文。

17.根据权利要求16所述的方法，其特征在于，所述第一签名包含在分段路由头SRH中。

18.根据权利要求17所述的方法，其特征在于，所述SRH包括扩展的类型长度值TLV字段，所述扩展的TLV字段包括所述第一签名。

19.根据权利要求14-17任意一项所述的方法，其特征在于，所述验证所述第一签名，包括：

根据所述第一IPv6报文中的第一内容进行哈希计算，将计算结果与所述第一签名进行比较。

20.根据权利要求14-18任意一项所述的方法，其特征在于，所述第一内容包括以下任意一项或者多项：

报文净荷中固定长度的数据和防重放攻击校验信息。

21.根据权利要求14-20任一项所述的方法，其特征在于，所述报文头中还包括防重放攻击校验信息。

22.根据权利要求19或20所述的方法，其特征在于，所述报文头中还包括第一指示信息，所述第一指示信息用于指示所述第一内容包括的至少一种防重放攻击校验信息。

23.根据权利要求21或22所述的方法，其特征在于，所述防重放攻击校验信息包括以下一种或多种：

报文序列号，时间戳以及随机数。

24.根据权利要求14-23任意一项所述的方法，其特征在于，所述报文头还包括第二指示信息，所述第二指示信息用于指示所述第二通信装置的类型。

25.根据权利要求22或23所述的方法，其特征在于，若所述第一指示信息指示所述第一内容包括报文序列号，在验证所述第一签名之前，所述方法还包括：

验证所述报文序列号的合法性。

26. 根据权利要求22或23所述的方法，其特征在于，若所述第一指示信息指示所述第一内容包括时间戳，在验证所述第一签名之前，所述方法还包括：确定所述第一通信装置当前时间与所述第一IPv6报文中携带的所述时间戳之间的差值小于等于第一阈值。

27. 根据权利要求22或23所述的方法，其特征在于，若所述第一指示信息指示所述第一内容包括随机数，在验证所述第一签名之前，所述方法还包括：

验证所述随机数的合法性。

28.根据权利要求14-27任意一项所述的方法，其特征在于，所述第一签名是利用所述第二通信装置的第一私钥生成的。

29.根据权利要求14-28任一项所述的方法，其特征在于，所述验证所述第一签名，包括：

根据所述第二通信装置的第一公钥，对所述第一签名进行验证。

30.根据权利要求29所述的方法，其特征在于，所述方法还包括：

接收控制管理实体发送的所述第一公钥。

31.根据权利要求14-30任意一项所述的方法，其特征在于，所述方法还包括：

接收控制管理实体发送的第三指示信息，所述第三指示信息用于指示所述第一通信装

置对所述第一签名进行验证。

32.根据权利要求14-31任意一项所述的方法，其特征在于，所述第一通信装置为所述第二通信装置在所述第一IPv6报文的转发路径上的下游装置。

33.根据权利要求32所述的方法，其特征在于，所述第一通信装置是所述第一IPv6报文的SRH中的SID list所指示的尾节点。

34.一种通信装置，其特征在于，所述通信装置包括存储器和处理器；

所述存储器，用于存储程序代码；

所述处理器，用于运行所述程序代码中的指令，使得所述通信装置执行以上权利要求1-13任意一项所述的方法。

35.一种通信装置，其特征在于，所述通信装置包括存储器和处理器；

所述存储器，用于存储程序代码；

所述处理器，用于运行所述程序代码中的指令，使得所述通信装置执行以上权利要求14-33任意一项所述的方法。

36.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有指令，当其在计算机上运行时，使得所述计算机执行以上权利要求1-33任意一项所述的方法。

37.一种通信系统，其特征在于，包括权利要求34所述的通信装置以及权利要求35所述的通信装置。

38.根据权利要求37所述的通信系统，其特征在于，还包括控制管理实体，用于向通信装置发送用于计算签名和/或验证签名所需的公钥。

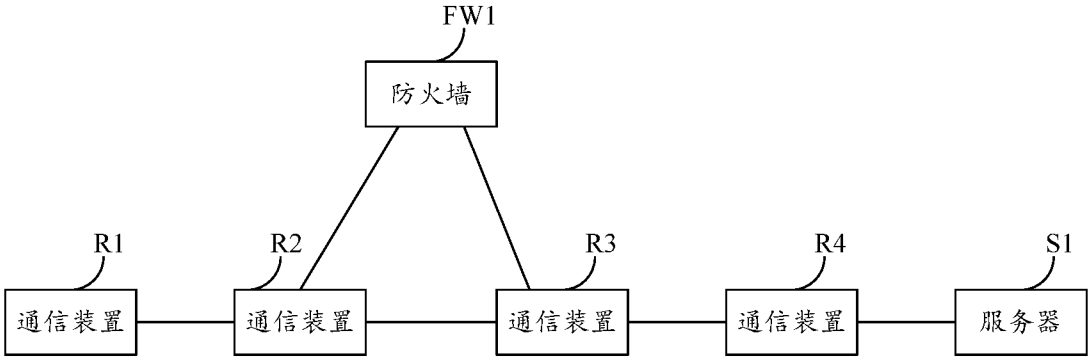



图 1

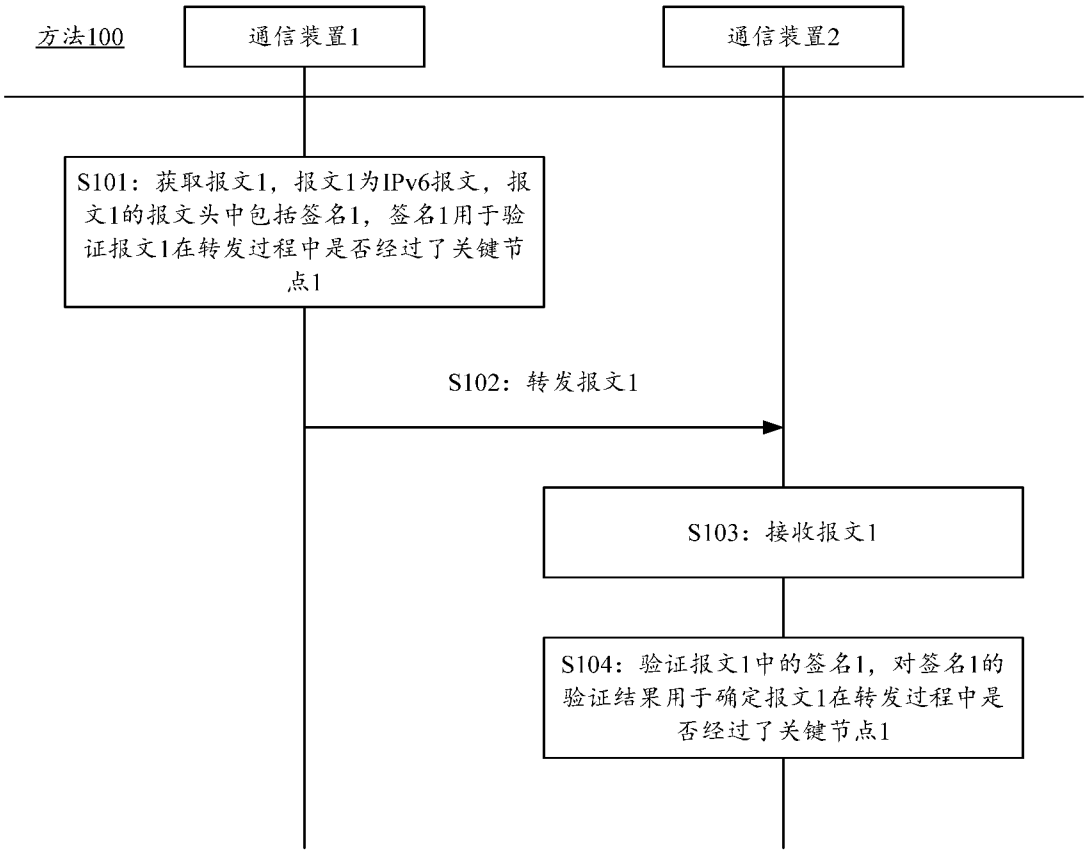

方法100
通信装置1
通信装置2
S101：获取报文1，报文1为IPv6报文，报文1的报文头中包括签名1，签名1用于验证报文1在转发过程中是否经过了关键节点1
S102：转发报文1
S103：接收报文1
S104：验证报文1中的签名1，对签名1的验证结果用于确定报文1在转发过程中是否经过了关键节点1

图 2

| 类型<br>type | 长度<br>length | 预留<br>reserved | 节点类型 | S指示位 | T指示位 | N指示位 |
|---|---|---|---|---|---|---|
| 序列号<br>sequence | | | | | | |
| 时间戳<br>timestamp | | | | | | |
| 随机数<br>nounce | | | | | | |
| 签名<br>signature | | | | | | |

图 3

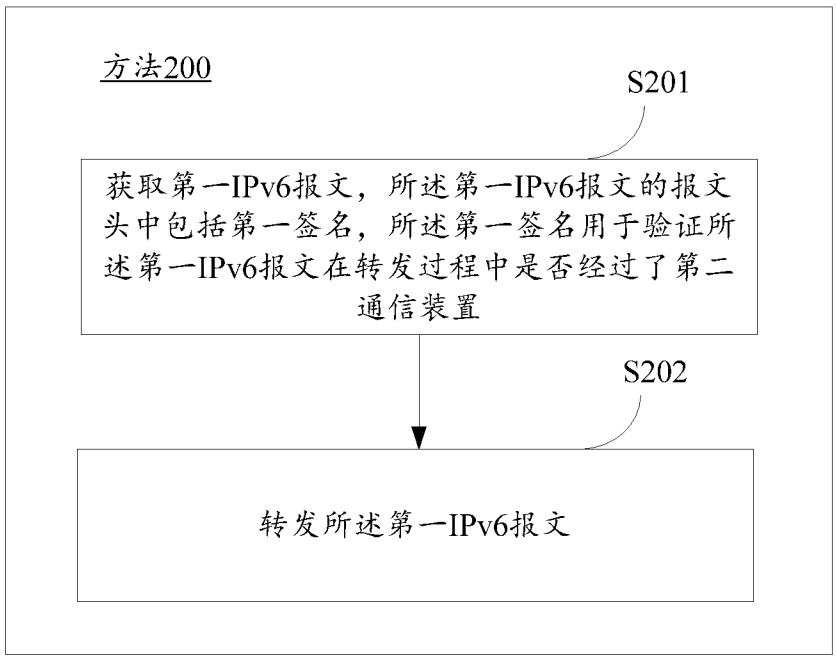



图 4

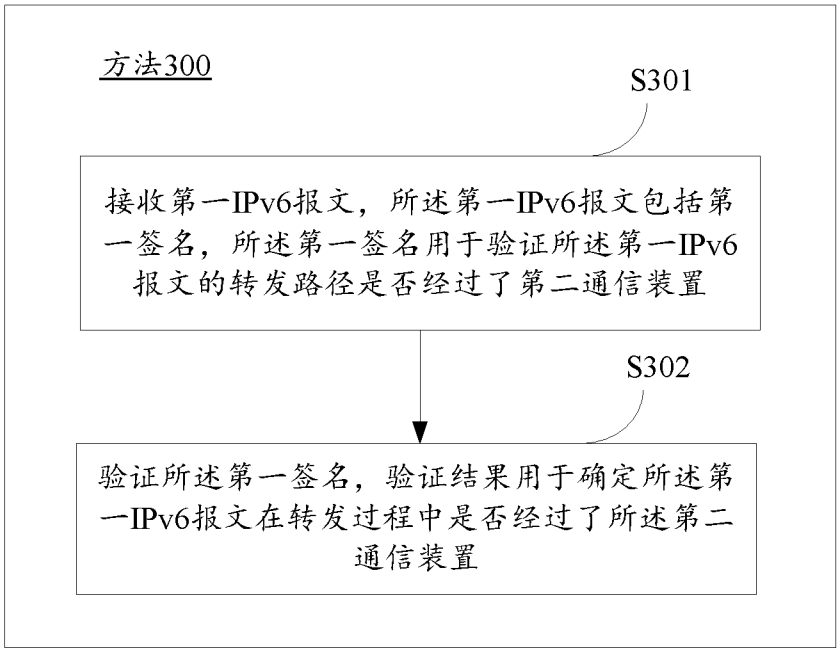

方法300
S301
接收第一IPv6报文，所述第一IPv6报文包括第一签名，所述第一签名用于验证所述第一IPv6报文的转发路径是否经过了第二通信装置
S302
验证所述第一签名，验证结果用于确定所述第一IPv6报文在转发过程中是否经过了所述第二通信装置

图 5

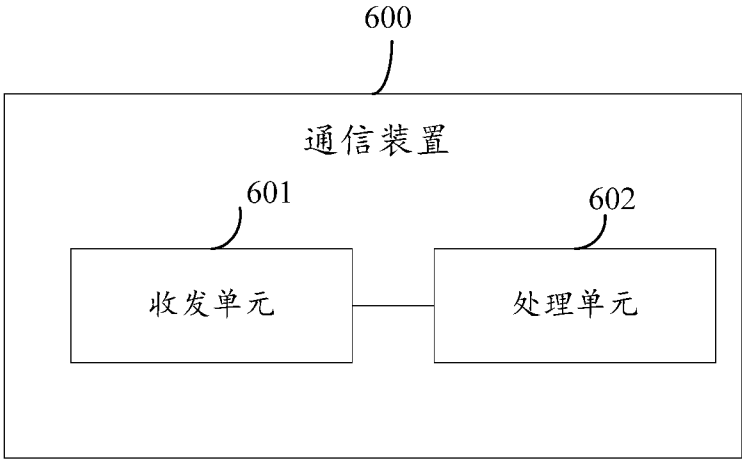

600
通信装置
601
602
收发单元
处理单元

图 6

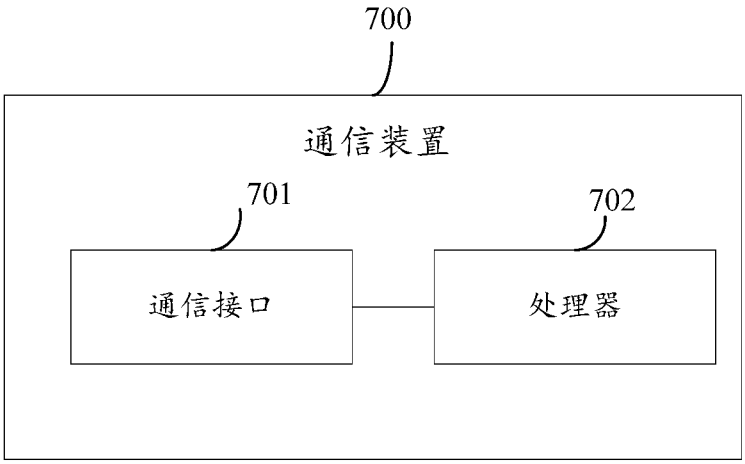

700
通信装置
701
702
通信接口
处理器

图 7

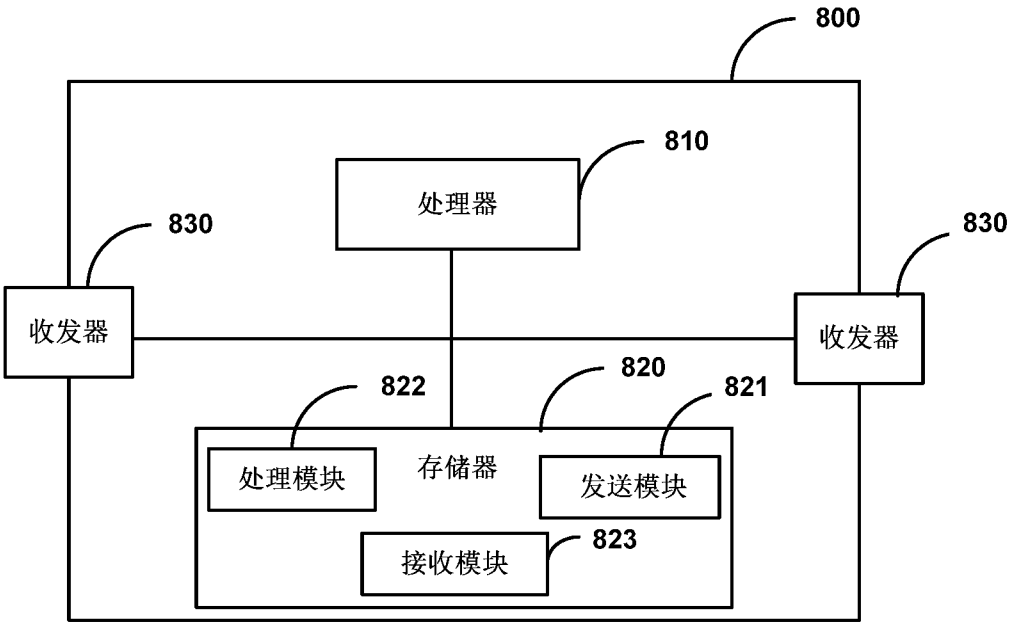

800
810
处理器
830
830
收发器
收发器
822
820
821
处理模块
存储器
发送模块
823
接收模块

图 8

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2021/109153**

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04W 12/06(2021.01)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, H04W

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; VEN; EPTXT; WOTXT; USTXT; CNKI: 因特网协议第6版, 报文, 报文头, 报头, 包头, 签名, 验证, 转发, 是否, 经过, 来自, 私钥, 公钥, 密钥, 哈希, 序号, 序列号, 时间戳, 随机数, 丢弃, IPv6, packet, head, signature, validate, forward, whether, if, from, private key, public key, hash, sequence number, timestamp, random number, discard

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN 102196423 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 21 September 2011 (2011-09-21)<br>description, paragraph [0045] | 1-38 |
| A | CN 109981458 A (HUAWEI TECHNOLOGIES CO., LTD.) 05 July 2019 (2019-07-05)<br>entire document | 1-38 |
| A | CN 101640631 A (CHENGDU HUAWEI SUNTENGDA SCIENCE & TECHNOLOGY CO., LTD.) 03 February 2010 (2010-02-03)<br>entire document | 1-38 |
| A | US 2019182051 A1 (INAUTH INC.) 13 June 2019 (2019-06-13)<br>entire document | 1-38 |

☐ 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 |
|---|---|
| **13 September 2021** | **22 September 2021** |
| Name and mailing address of the ISA/CN<br>**China National Intellectual Property Administration (ISA/CN)**<br>**No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China**<br>Facsimile No. **(86-10)62019451** | Authorized officer<br><br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/CN2021/109153**

| Patent document cited in search report | | | Publication date (day/month/year) | Patent family member(s) | | | Publication date (day/month/year) |
|---|---|---|---|---|---|---|---|
| CN | 102196423 | A | 21 September 2011 | CN | 102196423 | B | 06 July 2016 |
| CN | 109981458 | A | 05 July 2019 | WO | 2020181992 | A1 | 17 September 2020 |
| CN | 101640631 | A | 03 February 2010 | WO | 2010012171 | A1 | 04 February 2010 |
| | | | | EP | 2309686 | A1 | 13 April 2011 |
| | | | | US | 2011119534 | A1 | 19 May 2011 |
| | | | | CN | 101640631 | B | 16 November 2011 |
| | | | | EP | 2309686 | A4 | 14 December 2011 |
| | | | | EP | 2309686 | B1 | 18 June 2014 |
| US | 2019182051 | A1 | 13 June 2019 | WO | 2016118523 | A1 | 28 July 2016 |
| | | | | US | 10848317 | B2 | 24 November 2020 |
| | | | | EP | 3248360 | A1 | 29 November 2017 |
| | | | | US | 10237073 | B2 | 19 March 2019 |
| | | | | EP | 3248360 | A4 | 05 December 2018 |
| | | | | US | 2020177395 | A1 | 04 June 2020 |
| | | | | EP | 3248360 | B1 | 06 May 2020 |
| | | | | US | 2016248590 | A1 | 25 August 2016 |

# 国际检索报告

国际申请号
PCT/CN2021/109153

A. 主题的分类

H04L 29/06(2006.01)i; H04W 12/06(2021.01)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, H04W

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;VEN;EPTXT;WOTXT;USTXT;CNKI:因特网协议第6版，报文，报文头，报头，包头，签名，验证，转发，是否，经过，来自，私钥，公钥，密钥，哈希，序号，序列号，时间戳，随机数，丢弃，IPv6, packet, head, signature, validate, forward, whether, if, from, private key, public key, hash, sequence number, timestamp, random number, discard

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 102196423 A (腾讯科技深圳有限公司) 2011年 9月 21日 (2011-09-21)<br>说明书第[0045]段 | 1-38 |
| A | CN 109981458 A (华为技术有限公司) 2019年 7月 5日 (2019-07-05)<br>全文 | 1-38 |
| A | CN 101640631 A (成都市华为赛门铁克科技有限公司) 2010年 2月 3日 (2010-02-03)<br>全文 | 1-38 |
| A | US 2019182051 A1 (INAUTH INC) 2019年 6月 13日 (2019-06-13)<br>全文 | 1-38 |

☐ 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 9月 13日 | 2021年 9月 22日 |
| ISA/CN的名称和邮寄地址<br>中国国家知识产权局(ISA/CN)<br>中国 北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451 | 受权官员<br>邓璐<br>电话号码 86-(010)-62089138 |

# 国际检索报告
## 关于同族专利的信息

国际申请号
PCT/CN2021/109153

| 检索报告引用的专利文件 | | | 公布日<br>(年/月/日) | 同族专利 | | | 公布日<br>(年/月/日) |
|---|---|---|---|---|---|---|---|
| CN | 102196423 | A | 2011年 9月 21日 | CN | 102196423 | B | 2016年 7月 6日 |
| CN | 109981458 | A | 2019年 7月 5日 | WO | 2020181992 | A1 | 2020年 9月 17日 |
| CN | 101640631 | A | 2010年 2月 3日 | WO | 2010012171 | A1 | 2010年 2月 4日 |
| | | | | EP | 2309686 | A1 | 2011年 4月 13日 |
| | | | | US | 2011119534 | A1 | 2011年 5月 19日 |
| | | | | CN | 101640631 | B | 2011年 11月 16日 |
| | | | | EP | 2309686 | A4 | 2011年 12月 14日 |
| | | | | EP | 2309686 | B1 | 2014年 6月 18日 |
| US | 2019182051 | A1 | 2019年 6月 13日 | WO | 2016118523 | A1 | 2016年 7月 28日 |
| | | | | US | 10848317 | B2 | 2020年 11月 24日 |
| | | | | EP | 3248360 | A1 | 2017年 11月 29日 |
| | | | | US | 10237073 | B2 | 2019年 3月 19日 |
| | | | | EP | 3248360 | A4 | 2018年 12月 5日 |
| | | | | US | 2020177395 | A1 | 2020年 6月 4日 |
| | | | | EP | 3248360 | B1 | 2020年 5月 6日 |
| | | | | US | 2016248590 | A1 | 2016年 8月 25日 |