

(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
2014年6月19日 (19.06.2014)



(10) 国际公布号
WO 2014/090130 A1

- (51) 国际专利分类号:
H04W 12/02 (2009.01)
- (21) 国际申请号: PCT/CN2013/088947
- (22) 国际申请日: 2013年12月10日 (10.12.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210528207.7 2012年12月10日 (10.12.2012) CN
- (71) 申请人: 华为终端有限公司 (HUAWEI DEVICE CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地B区2号楼, Guangdong 518129 (CN)。
- (72) 发明人: 丁志明 (DING, Zhiming); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 树贵明 (SHU, Guiming); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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))。

(54) Title: METHOD, DEVICE AND SYSTEM FOR MESSAGE PROCESSING

(54) 发明名称: 报文处理方法及装置、系统

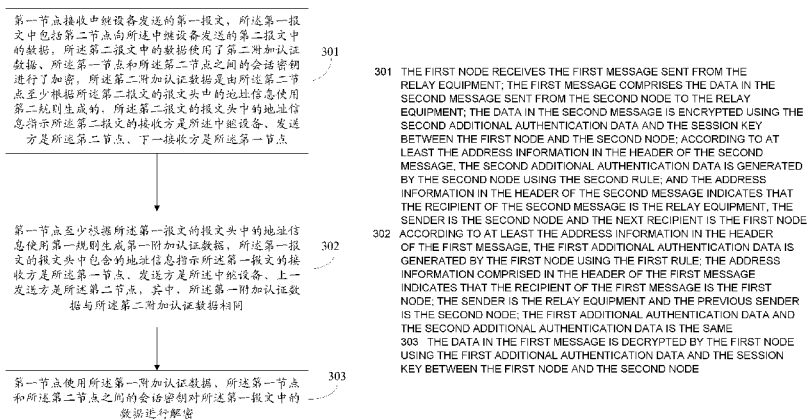


图3 / FIG. 3

(57) Abstract: A method, device and system for message processing are disclosed. A first node receives a first message sent from relay equipment; the first message comprises data in a second message sent from a second node to the relay equipment; the data in the second message is encrypted using second additional authentication data and a session key between the first node and the second node; according to at least address information in a header of the second message, the second additional authentication data is generated by the second node using a second rule; according to address information in a header of the first message, first additional authentication data is generated by the first node using a first rule; and the data in the first message is decrypted using the first additional authentication data and the session key between the first node and the second node. Resolved is the problem of channel utilization reduction, which is caused by the decryption and re-encryption processing needed in existing relay equipment when forwarding a message between a station and an access point.

(57) 摘要:

[见续页]



WO 2014/090130 A1



本发明实施例公开了一种报文处理方法及装置、系统，第一节点接收中继设备发送的第一报文，第一报文中包括第二节点向中继设备发送的第二报文中的数据，第二报文中的数据使用第二附加认证数据、第一节点和第二节点之间的会话密钥进行加密，第二附加认证数据由第二节点使用第二规则至少根据第二报文的报文头中的地址信息生成的；第一节点根据第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据；使用第一附加认证数据、第一节点和第二节点之间的会话密钥对第一报文中的数据进行解密。解决了现有的中继设备在站点和接入点之间转发报文时需要解密再加密的处理过程而导致的信道利用率降低的问题。

报文处理方法及装置、系统

本申请要求于2012年12月10日提交中国专利局、申请号为201210528207.7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。

5 技术领域

本发明实施例涉及通信技术领域，尤其涉及一种报文处理方法及装置、系统。

背景技术

10 在IEEE (Institute of Electrical and Electronics Engineers, 电子电气工程师协会) 802.11ah标准中, 为了扩展AP (英文: Access Point, 接入点, 简称AP) 的覆盖范围, 通常会在STA (英文: Station, 站点, 简称STA) 和AP之间增加中继设备 (英文: Relay), 通过Relay在STA和AP之间转发加密报文, 按照标准实现, Relay和STA之间协商有会话密钥PTKrd, 其中, PTK
15 (Pairwise Transient Key, 一对节点间的临时密钥) 为节点间的临时密钥, r表示Relay, d表示Relay的下行链路, Relay和AP之间也协商有会话密钥PTKru, 其中, r表示Relay, u表示Relay的上行链路。通常, 当Relay在转发STA发送给AP的上行加密报文时, Relay先用PTKrd解密该上行加密报文, 之后再用PTKru加密该上行加密报文; 当Relay在转发AP发送给STA的下行
20 加密报文时, Relay先用PTKru解密该下行加密报文, 之后再用PTKrd加密该下行加密报文。

上述Relay在STA和AP之间转发加密报文时需要解密再加密的处理过程, 需要占用一定的处理时间, 会降低信道利用率, 增加Relay的额外耗能。

25

发明内容

本发明提供一种报文处理方法及装置、系统, 用以解决现有的中继设备在站点和接入点之间转发报文时需要解密再加密的处理过程而导致的信

道利用率降低的问题。

第一方面，本发明提供一种报文处理方法，应用于中继设备在第一节点和第二节点之间转发报文的场景，包括：

第一节点接收中继设备发送的第一报文，所述第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥进行了加密，所述第二附加认证数据是由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成的，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点；

所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，其中，所述第一附加认证数据与所述第二附加认证数据相同；

所述第一节点使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密。

基于第一方面，在第一种实施方式中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

基于第一方面或第一方面的第一种实施方式，在第二种实施方式中，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

基于第一方面、第一方面的第一或第二种实施方式，在第三种实施方

式中，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一
5 报文。

基于第一方面、第一方面的第一、第二或第三种实施方式，在第四种实施方式中，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

第二方面，本发明提供一种报文处理方法，应用于中继设备在第一节点
10 点和第二节点之间转发报文的场景，包括：

第二节点生成第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点；

所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二
15 规则生成第二附加认证数据，使用所述第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第二报文中的数据进行加密；

所述第二节点将所述加密后的第二报文发送给所述中继设备，以使所述中继设备接收到所述第二报文后向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址
20 信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，使得所述第一节点接收到所述第一报文后至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加
25 认证数据与所述第二附加认证数据相同。

基于第二方面，在第一种实施方式中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的
30 报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报

文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

5 基于第二方面或第二方面的第一种实施方式，在第二种实施方式中，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

基于第二方面、第二方面的第一或第二种实施方式，在第三种实施方式中，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息
10 由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一报文。

基于第二方面、第二方面的第一、第二或第三种实施方式，在第四种
15 实施方式中，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

第三方面，本发明提供一种报文处理方法，应用于中继设备在第一节点和第二节点之间转发报文的场景，包括：

中继设备接收第二节点发送的第二报文，所述第二报文的报文头中的
20 地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是第一节点，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和第二节点之间的会话密钥进行了加密，所述第二附加认证数据由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成；

25 所述中继设备向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，以使所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，并使用所述第一附加认证
30 数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相

同。

基于第三方面，在第一种实施方式中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的
5 报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和
所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述
10 第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相
同。

基于第三方面或第三方面的第一种实施方式，在第二种实施方式中，
所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址
地址顺序相同。

15 基于第三方面、第三方面的第一或第二种实施方式，在第三种实施方式
中，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息
由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生
成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥
验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一
20 报文。

基于第三方面、第三方面的第一、第二或第三种实施方式，在第四种
实施方式中，所述第一节点为站点，第二节点为接入点；或，所述第一节
点为接入点，所述第二节点为站点。

25 第四方面，本发明提供一种报文处理装置，位于第一节点侧，应用于
中继设备在所述第一节点和第二节点之间转发报文的场景，包括：

接收模块，用于接收中继设备发送的第一报文，所述第一报文中包括
第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数
据使用了第二附加认证数据、所述第一节点和所述第二节点之间的会话密
钥进行了加密，所述第二附加认证数据是由所述第二节点至少根据所述第
30 二报文的报文头中的地址信息使用第二规则生成的，所述第二报文的报
文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所

述第二节点、下一接收方是所述第一节点；

解密模块，用于至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述另一第二节点，其中，所述使用所述第一规则生成的附加认证数据与所述使用所述第二规则生成的附加认证数据相同；使用所述第一附加认证数据、所述第一节点和所述另一第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

10 基于第四方面，在第一种实施方式中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

15 所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

20 基于第四方面或第四方面的第一种实施方式，在第二种实施方式中，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

基于第四方面、第四方面的第一或第二种实施方式，在第三种实施方式中，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述另一节点使用所述中继设备和所述另一节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述节点发送所述第一报文。

25 基于第四方面、第四方面的第一、第二或第三种实施方式，在第四种实施方式中，所述第一节点为站点，所述第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

第五方面，本发明提供一种报文处理装置，位于第二节点侧，应用于

中继设备在所述第二节点和第一节点之间转发报文的场景，包括：

报文生成模块，用于生成第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述节点、下一接收方是所述另一节点；

5 加密模块，用于至少根据所述第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，使用所述第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第二报文中的数据进行加密；

发送模块，用于将所述加密后的第二报文发送给所述中继设备，以使所述中继设备接收到所述第二报文后向所述第一节点发送第一报文，所述
10 第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，使得所述第一节点接收到所述第一报文后至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，使用所述第一附加认证数据、所述第一节点和所述第二节
15 点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

基于第五方面，在第一种实现方式中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的
20 报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述
25 第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

基于第五方面或第五方面的第一种实现方式，在第二种实现方式中，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

30 基于第五方面、第五方面的第一或第二种实现方式，在第三种实现方式中，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息

由所述节点使用所述中继设备和所述节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述另一节点发送所述第一报文。

5 基于第五方面、第五方面的第一、第二或第三种实现方式，在第四种实现方式中，所述第二节点为站点，所述第一节点为接入点；或，所述第二节点为接入点，所述第一节点为站点。

第六方面，本发明提供一种报文处理装置，位于中继设备侧，应用于中继设备在第一节点和第二节点之间转发报文的场景，包括：

10 接收模块，用于接收第二节点发送的第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是第一节点，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和第二节点之间的会话密钥进行了加密，所述第二附加认证数据由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成；

15 发送模块，用于向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，以使所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，并使用所述第一附加认
20 证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

基于第六方面，在第一种实现方式中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，
25 所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据
30 中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相

同。

基于第六方面或第六方面的第一种实现方式，在第二种实现方式中，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

5 基于第六方面、第六方面的第一或第二种实现方式，在第三种实现方式中，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一
10 报文。

基于第六方面、第六方面的第一、第二或第三种实现方式，在第四种实现方式中，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

15 第七方面，本发明提供一种报文处理系统，应用于中继设备在第一节点和第二节点之间转发报文的场景，包括：第一节点、第二节点、中继设备；

所述第一节点包括上述第四方面所述的报文处理装置；

所述第二节点包括上述第五方面所述的报文处理装置；

所述中继设备包括上述第六方面所述的报文处理装置。

20 本发明通过第一节点接收中继设备发送的第一报文，其中，第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用第二附加认证数据、第一节点和第二节点之间的会话密钥进行加密，所述第二附加认证数据由所述第二节点使用第二规则至少根据所述第二报文的报文头中的地址信息生成的；第一节点至少根据第一报文中
25 的地址信息使用第一规则生成第一附加认证数据，其中，第一节点根据第一规则生成的第一附加认证数据中各地址顺序与第二节点根据第二规则生成的第二附加认证数据中各地址顺序是相同的，进一步地，第一节点利用第一附加认证数据以及第一节点和第二节点之间的会话密钥解密第一报文中的数据。从而当中继设备接收到第二节点发送的第二报文时，不需要对

第二报文先进行解密然后再加密后发送第一报文给第一节点，节省了中继设备处理报文的时间，提高了信道利用率，减小了中继设备的额外耗能。

附图说明

5 为了更清楚地说明本发明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一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例应用的一种 CCMP 加密报文的帧格式示意图；

10 图 2 为本发明实施例应用的一种 MAC 帧头的格式示意图；

图 3 为本发明一实施例提供的报文处理方法的流程示意图；

图 4 为本发明实施例应用的报文处理系统的一种架构示意图；

图 5 为本发明另一实施例提供的报文处理方法的流程示意图；

图 6 为本发明另一实施例提供的报文处理方法的流程示意图；

15 图 7 为本发明一实施例提供的报文处理装置的结构示意图；

图 8 为本发明另一实施例提供的报文处理装置的结构示意图；

图 9 为本发明另一实施例提供的报文处理装置的结构示意图；

图 10 为本发明另一实施例提供的报文处理装置的结构示意图；

图 11 为本发明另一实施例提供的报文处理装置的结构示意图；

20 图 12 为本发明另一实施例提供的报文处理装置的结构示意图；

图 13 为本发明一实施例提供的报文处理系统的一种结构示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本
25 发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

在 802.11 标准中，STA（英文：Station，站点）是指支持 802.11 协议

的设备，包括 AP 在内，AP 在标准中被称为 AP STA，不是 AP 的 STA 在标准中被称为 non-AP STA。本发明中所述的站点 STA 指应用终端，也即 non-AP STA，本发明中所述的接入点 AP，可以是标准中的 AP STA，本发明中所述的中继设备 Relay，可以是标准中的 Relay STA。

5 在 IEEE802.11ah 标准中，通常，采用计数器模式密码块链消息认证码协议(英文: Counter Mode with Cipher-block Chaining Message Authentication Code Protocol, 简称 CCMP)对报文中的数据进行加密。图 1 为本发明实施例应用的一种 CCMP 加密报文的帧格式示意图，报文头一般称为媒介访问控制帧头(英文: Media Access Control header, 简称 MAC header), 如图 1
10 所示, MAC header 和 CCMP Header 参与加密计算但本身不被加密; 待发送报文中的数据 Data 和消息完整性码(英文: Message Integrity Code, 简称 MIC)被加密(英文: Encrypted), 帧检验序列(英文: Frame Check Sequence, 简称 FCS)用于检查帧在传输过程中是否出错。本发明实施例可以应用的 CCMP 加密报文的帧格式不限于图 1 所示的帧格式。

15 在实际应用中，AP 或者 STA 采用 CCMP 算法对待发送报文中的数据 Data 和消息完整性码 MIC 加密之前，需要使用待发送报文的 MAC 帧头中的地址信息生成附加认证数据(英文: Additional Authentication Data, 简称 AAD)，图 2 为本发明实施例应用的一种 MAC 帧头的格式示意图，如图 2 所示，MAC 帧头中包括多个地址信息，其中，地址信息中包括的
20 各地址顺序为地址 A1、地址 A2、地址 A3 和地址 A4，其中，A1 是接收地址，即当前接收报文的节点地址，A2 是发送地址，即当前发送报文的节点地址。当目的地址为接收地址时，MAC 帧头中不需要写目的地址，当目的地址不是接收地址时，A3 是目的地址，通常，目的地址为下一个接收报文的节点地址；当源地址是发送地址，MAC 帧头中不需要写源地址，
25 当源地址不是发送地址时，则 A3 或 A4 中需要写入源地址，通常，源地址为上一个发送报文的节点地址。本发明实施例可以应用的 MAC 帧头的格式不限于图 2 所示的格式。

由图 2 所示的 MAC 帧头结构可知，当报文每一次被 Relay 转发时，MAC 帧头中的各地址的顺序必然改变，由于 MAC 帧头中的各地址顺序在
30 报文转发过程中是改变的，根据 MAC 帧头中的各地址顺序生成的附加认证数据 AAD 也会改变，因此，Relay 在接收到的报文之后，必须对接收到

的报文中的加密数据进行解密，在MAC帧头中重新写入转发的地址信息，然后根据重新写入的地址信息生成附加认证数据，并利用该重新生成的附加认证数据对解密后的数据进行加密。从而增加了Relay的报文处理时间，降低信道利用率，增加Relay的额外耗能。

5 鉴于上述存在的问题，本发明实施例提供一种报文处理方法，应用于中继设备在第一节点和第二节点之间转发报文的场景，可以解决现有的中继设备在站点和接入点之间转发报文时需要解密再加密的处理过程而导致的信道利用率降低的问题。

需要说明的是，以下各实施例中，若第一节点是接入点 AP 时，则第二节点为站点 STA，或者若第一节点是站点 STA 时，则第二节点是接入点 AP。

图 3 为本发明一实施例提供的报文处理方法的流程示意图；应用于中继设备在第一节点和第二节点之间转发报文的场景，如图 3 所示，报文处理方法具体包括：

301、第一节点接收中继设备发送的第一报文，所述第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥进行了加密，所述第二附加认证数据是由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成的，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点。

具体实现时：图 4 为本发明实施例应用的报文处理系统的一种架构示意图，如图 4 所示，假设接入点 AP 为第一节点，站点 STA 为第二节点，STA 生成第二报文，其中，第二报文的报文头（如图 2 所示的 MAC 帧头）中的地址信息中的各地址顺序为：A1 为 Relay 的地址，发送地址 A2 兼源地址为 STA 的地址，下一个接收方的地址 A3 为 AP 的地址。STA 至少根据第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据 AAD，之后，STA 利用第二 AAD 以及 STA 和 AP 之间的会话密钥对第二报文中的数据进行加密，并将加密后的第二报文发送给 Relay。

Relay 接收到 STA 发送的第二报文之后，可以重新组装以得到第一报文，具体可以为：填充第一报文的报文头（MAC 帧头）中的地址信息，即接收地址 A1 兼目的地址为 AP 的地址，发送地址 A2 为 Relay 的地址，源

地址 A3 为 STA 的地址; 将第二报文中的加密数据填充在第一报文中的 Data 部分中。所述第一报文也可以是在所述第二报文上进行简单的地址信息更新后得到的。本实施例中, Relay 不需要对 STA 发送的第二报文进行解密处理, 可以直接将第二报文中的加密数据填充在第一报文中的 Data 部分中, 5 之后, Relay 将第一报文发送给 AP。

可选地, 上述 STA 发送给 Relay 的第二报文中还可以包括中继消息认证信息, 所述中继消息认证信息可以由 STA 使用 STA 和 Relay 之间的消息认证密钥生成的, 用以 Relay 接收到所述第二报文之后, 使用所述消息认证密钥验证所述中继消息认证信息, 若验证通过则向 AP 发送第二报文。

10 302、第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据, 所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点, 其中, 所述第一附加认证数据与所述第二附加认证数据相同。

15 需要说明的是, 本发明实施例的应用场景是中继设备在第一节点和第二节点之间转发报文, 因此, 当 AP 接收到第一报文之后, 需要根据第一报文的报文头中的地址信息, 假设发送地址 A2 为 Relay 的地址, 则可以确定该第一报文是 Relay 转发的; 或者, 当 AP 接收第一报文之后, 假设第一报文的报文头中携带有 Relay 发送的标志位, 例如标志位为 1 时, 表示该第一
20 报文是 Relay 发送的, 0 表示该第一报文不是 Relay 发送的, 具体实现时, Relay 发送的标志位可以利用 MAC 帧头的帧控制 (英文: Frame Control, 简称 FC) 中保留的比特 (bit) 位来标识。

由于报文每一次被 Relay 转发时, 报文头中的各地址的顺序必然改变, 因此, AP 在接收到 Relay 发送的第一报文中的各地址顺序与 STA 在发送给
25 Relay 的第二报文中的各地址顺序是不同的。为了能够实现 Relay 不需要对 STA 发送的第二报文中的加密数据进行解密处理, 并且 AP 能够将 Relay 发送的第一报文中包含的来自 STA 的第二报文中的加密数据进行解密, AP 根据第一报文的报文头中的各地址信息使用第一规则生成的第一附加认证数据必须与 STA 根据第二报文的报文头中的各地址信息使用第二规则生成的
30 的第二附加认证数据是相同的。具体实现时:

若所述第一规则是第一附加认证数据中的各地址顺序与所述第一报文

的报文头中的各地址顺序相同，则所述第二规则是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得根据所述第二规则生成的第二附加认证数据中各地址顺序和根据第一规则生成的所述第一附加认证数据中各地址顺序相同；或

5 若所述第一规则是第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，则所述第二规则是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得根据所述第二规则生成的第二附加认证数据中各地址顺序和根据第一规则生成的所述第一附加认证数据中各地址顺序相同。

10 如图 4 所示，假设第二节点 STA 根据第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，该第二规则是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，则第一节点 AP 根据第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据时，该第一规则是第一附加认证数据中的各地址顺序与所述第一报文的
15 的报文头中的各地址顺序不同，使得所述第二节点 STA 根据第二报文的报文头中的地址信息使用所述第二规则生成的第二附加认证数据中各地址顺序和第一节点 AP 根据第一报文的报文头中的地址信息使用所述第一规则生成的第一附加认证数据中各地址顺序相同。

具体实现时，例如，第一节点 AP 中可以预设有地址映射表，其中，地
20 址映射表中设置有 Relay 发送的第一报文的报文头中的各地址在 AP 生成的 AAD 中的各地址字段的位置的映射关系；

其中，表 1 为本发明实施例预设的地址映射表，如表 1 所示，下行表示 AP 通过 Relay 向 STA 发送报文，上行表示 STA 通过 Relay 向 AP 发送报文；为了实现 AP 正确的解密 Relay 发送的第一报文中包含的来自 STA 的
25 第二报文中的加密数据，AP 生成的 AAD 中的各地址顺序需要与 STA 生成的 AAD 中的各地址顺序一致。表 1:

方向	AP的AAD中的第一个地址字段	AP的AAD中的第二个地址字段	AP的AAD中的第三个地址字段	AP的AAD中的第四个地址字段
下行	AP 发给 Relay 的报文中的 A3	AP 发给 Relay 的报文中的 A1	AP 发给 Relay 的报文中的 A2	
上行	Relay 发给 AP 的报文中的 A2	Relay 发给 AP 的报文中的 A3	Relay 发给 AP 的报文中的 A1	

需要说明的是，可选的，AP 的 AAD 中可以有第四个地址字段，在表 1 中未具体示出有第四个地址字段时的内容。基于上述第一节点 AP 确定第一报文是 Relay 发送的基础上，AP 获取第一报文的报文头中的地址信息，
 5 具体为：接收地址 A1 兼目的地址为 AP 的地址，发送地址 A2 为 Relay 的地址，源地址 A3 为 STA 的地址；查询表 1 所示的地址映射表，得到与上述获取的第一报文的报文头中各地址顺序对应的映射地址顺序，即第一报文的报文头中的接收地址 A1（AP 的地址）对应映射地址中的 A3，第一报文的报文头中的发送地址 A2（Relay 的地址）对应映射地址中的 A1，第一
 10 报文的报文头中的源地址 A3（STA 的地址）对应映射地址中的 A2；

之后，AP 根据第一报文的报文头中的地址信息使用的第一规则生成对应的附加认证数据时，具体可以为：AP 根据第一报文的报文头中的各地址顺序对应的映射地址顺序，分别将各映射地址填入生成附加认证数据的 MAC 帧头中对应的 A1、A2 和 A3 的位置，也就是说，将 Relay 的地址填入
 15 A1 位置，将 STA 的地址填入 A2 位置，将 AP 的地址填入 A3 位置，生成第一附加认证数据，第一附加认证数据中各地址顺序为 Relay 的地址、STA 的地址、AP 的地址。这种情况下，第一节点 AP 根据第一报文头中的地址信息使用第一规则生成对应的第一附加认证数据时，该第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文头中的各地址顺序不同，
 20 则，第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文头中的各地址顺序相同，由于第二报文头中的地址信息中的各地址顺序为：

A1 为 Relay 的地址，发送地址 A2 兼源地址为 STA 的地址，下一个接收节点的地址 A3 为 AP 的地址，则第二节点 STA 根据第二报文头中的地址信息使用第二规则生成对应的第二附加认证数据中各地址顺序为 Relay 的地址、STA 的地址、AP 的地址。从而 AP 生成的第一 AAD 中各地址顺序与 STA 5 生成的第二 AAD 中各地址顺序相同，进而可以实现 AP 正确的解密 Relay 发送的第一报文中包含的来自 STA 的第二报文中的加密数据。

需要说明的是，如图 4 所示，假设第二节点 STA 根据第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，该第二规则是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，则第一节点 AP 根据第一报文的报文头中的地址信息使用第一规则生成 10 第一附加认证数据时，该第一规则是第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，使得所述第二节点 STA 根据第二报文的报文头中的地址信息使用所述第二规则生成的第二附加认证数据中各地址顺序和第一节点 AP 根据第一报文的报文头中的地址信息使用 15 所述第一规则生成的第一附加认证数据中各地址顺序相同。具体实现时，例如，第二节点 STA 中可以预设有地址映射表，其中，地址映射表中可以设置有 Relay 发送的第一报文的报文头中的各地址在第二节点 STA 生成的 AAD 中的各地址字段的位置的映射关系，映射原理不再赘述。

303、第一节点使用根据所述第一规则生成的第一附加认证数据、所述 20 第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密。

具体实现时，可以按照 CCMP 算法，第一节点使用第一附加认证数据、第一报文中的 CCMP 头中的包序号信息、以及第一节点和第二节点之间的会话密钥等进行一系列运算产生密钥链的第一密钥值，再将这个第一密钥 25 值经过一个固定公式的计算生成第二密钥值，再将第二密钥值经过所述固定公式的计算生成第三密钥值，依此类推，这一系列的密钥值就是密钥链。密钥链中的每个密钥值可以都是 128 比特，每个密钥值依次与待解密数据中的 128 比特进行异或运算，就得到对应的明文数据，本领域技术人员可以理解的是，CCMP 算法可以是现有技术，本发明对此不作限定。

30 需补充说明的是，附加认证数据中可以只包含地址信息，也可以还使用了报文头中的除了地址信息之外的其它信息，例如帧控制 FC (Frame

Control, 帧控制) 字段、服务质量控制 QC (Quality of service Control, QoS 控制) 字段、序列控制 SC (Sequence Control) 字段, 这些字段包含很多指示信息位, 这些信息位有些在附加认证数据中保持与报文头中相同的值, 有些则在附加认证数据中被设置为固定值。为了使得所述的第一节点和所述的第二节点对于它们之间传递的同一数据产生相同的附加认证数据, 那些在 Relay 转发后会发生变化的信息位在生成的附加认证数据中可以被设为固定值, 例如 FC 字段中有两个信息位是 toDS 和 fromDS, 分别表示这个报文是否发送给网络侧或来自网络侧, 在 Relay 接收 STA 发送的报文时, 这两个信息位的值可以是“10”, 而 Relay 向 AP 发送报文时, 这两个信息位的值可以是“11”, 因此, 无论是 STA 还是 AP 在产生附加认证数据时, 都将在附加认证数据中的这两个信息位设为固定值, 例如“11”。附加认证数据中这些信息位设为固定值并不表示特定含义, 仅仅是为了 STA 和 AP 得到相同的附加认证数据。

还需补充说明的是, CCMP 算法中还可以根据报文头中的 A2 地址生成现场值(英文: Nonce), 将该现场值参与加密计算过程, 因此, 第一节点接收第一报文后需生成相同的现场值才能正确解密。如图 4 所示, Relay 发送给 AP 的第一报文中的 A2 是与 Relay 接收的来自 STA 的第二报文中的 A2 是不同的, 为了让 AP 与 STA 使用相同的现场值, 例如在上行的情形下, 需要 AP 根据表 1 所示的地址映射关系, 确定 Relay 发送给 AP 的第一报文的报文头中地址 A3 与 STA 发送给 Relay 的第二报文中的 A2 是相同的, 因此, AP 可以根据第一报文头中地址 A3 来产生现场值, 这样 AP 产生的现场值就和 STA 产生的现场值相同。

本发明实施例通过第一节点接收中继设备发送的第一报文, 其中, 第一报文中包括第二节点向所述中继设备发送的第二报文中的数据, 所述第二报文中的数据使用第二附加认证数据、第一节点和第二节点之间的会话密钥进行加密, 所述第二附加认证数据由所述第二节点使用第二规则至少根据所述第二报文的报文头中的地址信息生成的; 第一节点至少根据第一报文中的地址信息使用第一规则生成第一附加认证数据, 其中, 第一节点根据第一规则生成的第一附加认证数据中各地址顺序与第二节点根据第二规则生成的第二附加认证数据中各地址顺序是相同的, 进一步地, 第一节点利用第一附加认证数据以及第一节点和第二节点之间的会话密钥解密第

一报文中的数据。从而当中继设备接收到第二节点发送的第二报文时，不需要对第二报文先进行解密然后再加密后发送第一报文给第一节点，节省了中继设备处理报文的时间，增加了信道利用率，减小了中继设备的额外耗能。

5 图 5 为本发明另一实施例提供的报文处理方法的流程示意图；应用于中继设备在第一节点和第二节点之间转发报文的场景，如图 5 所示，报文处理方法具体包括：

501、第二节点生成第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点。

具体实现时，如图 4 所示，假设第二节点为 AP，第一节点为 STA，当 AP 需要发送一个加密数据到 STA 时，AP 可以生成第二报文，在第二报文的报文头中填入各地址信息，接收地址 A1 为 Relay 的地址，发送地址 A2 兼源地址为 AP 的地址，目的地址 A3 为 STA 的地址；将待发送的数据填入到第二报文的 Data 部分。

502、第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，使用所述第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第二报文中的数据进行加密；

具体实现时，AP 在发送第二报文之前，AP 需要生成第二附加认证数据，本实施例中，AP 至少根据第二报文中的地址信息使用第二规则生成第二附加认证数据，其中，第二规则可以是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同；或第二规则也可以是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同。

25 之后，AP 使用第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第二报文中的数据进行加密，具体实现时，可以按照 CCMP 算法，AP 使用第二附加认证数据、第二报文中的 CCMP 头中的包序号信息、以及 AP 和 STA 之间的会话密钥等进行一系列运算产生密钥链的第一密钥值，再将这个第一密钥值经过一个固定公式的计算生成第二密钥值，再将第二密钥值经过所述固定公式的计算生成第三密钥值，依此类推，30 这一系列的密钥值就是密钥链。密钥链中的每个密钥值可以都是 128 比特，

每个密钥值依次与待加密数据中的 128 比特进行异或运算，就可以得到对应的密文数据。

503、第二节点将所述加密后的第二报文发送给所述中继设备，以使所述中继设备接收到所述第二报文后向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，使得所述第一节点接收到所述第一报文后至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

本实施例中，如图 4 所示，当 Relay 接收到 AP 发送的第二报文之后，不需要对第二报文中的加密数据进行解密，Relay 可以重新组装以得到第一报文，具体地可以为，将第二报文中的加密数据填充到第一报文的 Data 部分，将第一报文的报文头的地址信息填充为：接收地址 A1 兼目的地址为 STA 的地址，发送地址 A2 为 Relay 的地址，源地址 A3 为 AP 的地址。所述第一报文也可以是在所述第二报文上进行简单的地址信息更新后得到的。之后，Relay 将第一报文发送给 STA。

为了使得 STA 能够正确解密出第一报文中包含的来自 AP 的第二报文中的加密数据，STA 根据第一报文中的地址信息使用第一规则生成的第一附加认证数据必须与 AP 根据第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据是相同的，可以包括，STA 使用第一规则生成的第一附加认证数据中的各地址顺序必须与 AP 使用第二规则生成的第二附加认证数据中的各地址顺序相同。具体实现时可以为：

若 AP 使用的第二规则是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，则 STA 使用的第一规则是第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，使得 STA 根据使用所述第一规则生成的第一附加认证数据中各地址顺序和 AP 根据使用所述第二规则生成的第二附加认证数据中各地址顺序相同；或

若 AP 使用的第二规则是第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，则 STA 使用的第一规则是第一附加

认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，使得 STA 使用所述第一规则生成的第一附加认证数据中各地址顺序和 AP 使用所述第二规则生成的第二附加认证数据中各地址顺序相同。

进一步地，在本发明的一个可选实施方式中，AP 生成的第二报文中还可以包括中继消息认证信息，所述中继消息认证信息由 AP 使用 Relay 和 AP 之间的消息认证密钥生成，以便 Relay 接收到 AP 发送的第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向 STA 发送第一报文。其中，上述中继消息认证信息可以是 AP 对所述第二报文的 FCS 字段使用所述消息认证密钥进行加密或哈希运算得到的。在具体实现时可以为：

例如图 4 所示，AP 发送第二报文给 Relay 之前，可以与 Relay 协商一个中继消息认证密钥，该中继消息认证密钥用于对 AP 发送给 Relay 的第二报文进行简单的消息认证，通常，AP 可以使用该 AP 与 Relay 之间协商好的中继消息认证密钥对待发送的第二报文中的 FCS 字段进行加密或哈希（hash）运算，将加密或哈希后的 FCS 作为中继消息认证信息代替原有的 FCS 字段，本实施例中，为了说明的方便，可以将哈希后的 FCS 称为中继认证字段 R-Auth。Relay 接收到 AP 发送的第二报文之后，使用所述中继消息认证密钥验证所述中继消息认证信息，验证第二报文中携带的中继认证字段 R-Auth，具体验证方法可以是采用 AP 产生 R-Auth 相同的过程产生 R-Auth'，然后比较 R-Auth' 和报文中的 R-Auth，若两者相等，则验证成功，否则验证失败。Relay 在验证 R-Auth 成功的基础上，将该第二报文中的加密数据组装到第一报文中并发送给 STA；可选地，若 Relay 验证 R-Auth 不成功，Relay 可以直接丢弃第二报文。

本发明实施例通过第二节点根据第二报文中的地址信息使用第二规则生成第二附加认证数据，利用第二附加认证数据、第一节点与第二节点之间的会话密钥对第二报文中的数据进行加密后，将第二报文发送给中继设备，使得中继设备不需要对第二报文中的加密数据进行解密，而是将第二报文中的加密数据直接携带在第一报文中发送给第一节点，以使第一节点根据第一报文中的地址信息使用第一规则生成第一附加认证数据，其中，使用第一规则生成第一附加认证数据与使用第二规则生成第二附加认证数据是相同的，第一节点利用第一附加认证数据、第一节点和第二节点之间

的会话密钥对第一报文中的加密数据进行解密。从而能够实现中继设备在转发加密报文的过程中不需要先解密后再加密的过程，节省了报文处理的时间，增加了信道利用率，减小了中继设备的额外耗能。

图 6 为本发明另一实施例提供的报文处理方法的流程示意图；应用于
5 中继设备在第一节点和第二节点之间转发报文的场景，如图 6 所示，报文处理方法具体包括：

601、中继设备接收第二节点发送的第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是第一节点，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和第二节点之间的会话密钥进行了加密，所述
10 第二附加认证数据由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成。

602、中继设备向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述
15 第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，以使所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，并使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据
20 进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

本实施例中，中继设备在接收到第二节点发送的第二报文之后，不需要将第二报文中的加密数据进行解密，可以直接将所述加密数据填充到第一报文的 Data 部分，将第一报文的报文头的地址信息填充为：接收地址 A1 兼目的地址为第一节点的地址，发送地址 A2 为中继设备的地址，源地址
25 A3 为第二节点的地址；之后，中继设备将第一报文发送给第一节点。

其中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址
30 顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报

文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

5 进一步地，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

其中，所述第一节点为站点，所述第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

进一步地，在本发明的一个实施方式中，所述中继设备接收第二节点发送的第二报文中还可以包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，以便所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一报文。其中，上述中继消息认证信息由第二节点使用所述中继设备和所述
10 第一节点之间的消息认证密钥生成，在具体实现时，可以是第二节点对所述第二报文的 FCS 字段使用所述消息认证密钥进行加密或哈希运算得到上述中继消息认证信息。具体可参考前述相关部分的描述，此处不再赘述。

本发明实施例的中继设备在接收到第二节点发送的第二报文时，不需要中继设备对第二报文中的加密数据先解密后加密的过程，可以直接将该
20 加密数据重新组装到第一报文中，节省了中继设备处理报文的时间，增加了信道利用率，减小了中继设备的额外耗能。

图 7 为本发明一实施例提供的报文处理装置的结构示意图；位于第一节点侧，应用于中继设备在第一节点和第二节点之间转发报文的场景，如图 7 所示，包括：

25 接收模块 71，用于接收中继设备发送的第一报文，所述第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥进行了加密，所述第二附加认证数据是由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成的，所述第二报文的报
30 文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点；

解密模块 72，用于至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述另一第二节点，其中，所述使用所述第一规则生成的附加认证数据与所述使用所述第二规则生成的附加认证数据相同；使用所述第一附加认证数据、所述第一节点和所述另一第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

其中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

进一步地，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

进一步可选的，所述第二报文中还可以包括中继消息认证信息，所述中继消息认证信息由所述另一节点使用所述中继设备和所述另一节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述节点发送所述第一报文。

其中，所述第一节点为站点，所述第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

本发明实施例通过第一节点接收中继设备发送的第一报文，其中，第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用第二附加认证数据、第一节点和第二节点之间的会话密钥进行加密，所述第二附加认证数据由所述第二节点使用第二规则至少

根据所述第二报文的报文头中的地址信息生成的；第一节点至少根据第一报文中的地址信息使用第一规则生成第一附加认证数据，其中，第一节点根据第一规则生成的第一附加认证数据中各地址顺序与第二节点根据第二规则生成的第二附加认证数据中各地址顺序是相同的，进一步地，第一节点利用第一附加认证数据以及第一节点和第二节点之间的会话密钥解密第一报文中的数据。从而当中继设备接收到第二节点发送的第二报文时，不需要对第二报文先进行解密然后再加密后发送第一报文给第一节点，节省了中继设备处理报文的时间，增加了信道利用率，减小了中继设备的额外耗能。

10 图 8 为本发明另一实施例提供的报文处理装置的结构示意图；位于第二节点侧，应用于中继设备在所述第二节点和第一节点之间转发报文的场景，包括：

15 报文生成模块 81，用于生成第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述节点、下一接收方是所述另一节点；

加密模块 82，用于至少根据所述第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，使用所述第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第二报文中的数据进行加密；

20 发送模块 83，用于将所述加密后的第二报文发送给所述中继设备，以使所述中继设备接收到所述第二报文后向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，使得所述第一节点接收到所述第一报文后至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

30 其中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址

顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述
5 第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

进一步地，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

进一步可选的，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述节点使用所述中继设备和所述节点之间的消息认证密
10 钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述另一节点发送所述第一报文。

其中，所述第二节点为站点，所述第一节点为接入点；或，所述第二
15 节点为接入点，所述第一节点为站点。

本发明实施例通过第二节点根据第二报文中的地址信息使用第二规则生成第二附加认证数据，利用第二附加认证数据、第一节点与第二节点之间的会话密钥对第二报文中的数据进行加密后，将第二报文发送给中继设备，使得中继设备不需要对第二报文中的加密数据进行解密，而是将第二
20 报文中的加密数据直接携带在第一报文中发送给第一节点，以使第一节点根据第一报文中的地址信息使用第一规则生成第一附加认证数据，其中，使用第一规则生成第一附加认证数据与使用第二规则生成第二附加认证数据是相同的，第一节点利用第一附加认证数据、第一节点和第二节点之间的会话密钥对第一报文中的加密数据进行解密。从而能够实现中继设备在
25 转发加密报文的過程中不需要先解密后再加密的过程，节省了报文处理的时间，增加了信道利用率，减小了中继设备的额外耗能。

图 9 为本发明另一实施例提供的报文处理装置的结构示意图；位于中继设备侧，应用于中继设备在所述第二节点和第一节点之间转发报文的场景，包括：

30 接收模块 91，用于接收第二节点发送的第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是

所述第二节点、下一接收方是第一节点，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和第二节点之间的会话密钥进行了加密，所述第二附加认证数据由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成；

- 5 发送模块 92，用于向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，以使所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，并使用所述第一附加
- 10 认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

- 其中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址
- 15 顺序相同；或

- 所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述
- 20 第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

进一步地，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

- 25 进一步可选的，所述第二报文中还可以包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一报文。

- 30 其中，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

本发明实施例的中继设备在接收到第二节点发送的第二报文时，不需要中继设备对第二报文中的加密数据先解密后加密的过程，可以直接将该加密数据重新组装到第一报文中，节省了中继设备处理报文的时间，增加了信道利用率，减小了中继设备的额外耗能。

5 图 10 为本发明另一实施例提供的报文处理装置的结构示意图；位于第一节点侧，应用于中继设备在第一节点和第二节点之间转发报文的场景，本实施例的报文处理装置具体可以为接入点或者站点，如图 10 所示，第一节点包括：处理器、存储器和通信总线，其中，处理器和存储器通过通信总线连接，存储器中保存有用于中继设备在第一节点和第二节点之间转发
10 报文的场景时的报文处理方法的实现指令；进一步地，第一节点还包括通信接口，通过通信接口与其他网元设备（例如中继设备）通信。

当处理器调取存储器中的指令时，可以执行如下步骤：

接收中继设备发送的第一报文，所述第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥进行了加密，
15 所述第二附加认证数据是由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成的，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点；

20 至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述另一第二节点，其中，所述使用所述第一规则生成的附加认证数据与所述使用所述第二规则生成的附加认证数据相同；使用所述第一附加认证数据、
25 所述第一节点和所述另一第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

其中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得
30 所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

进一步地，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

进一步可选的，所述第二报文中还可以包括中继消息认证信息，所述中继消息认证信息由所述另一节点使用所述中继设备和所述另一节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述节点发送所述第一报文。

其中，所述第一节点为站点，所述第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

本发明实施例通过第一节点接收中继设备发送的第一报文，其中，第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用第二附加认证数据、第一节点和第二节点之间的会话密钥进行加密，所述第二附加认证数据由所述第二节点使用第二规则至少根据所述第二报文的报文头中的地址信息生成的；第一节点至少根据第一报文中的地址信息使用第一规则生成第一附加认证数据，其中，第一节点根据第一规则生成的第一附加认证数据中各地址顺序与第二节点根据第二规则生成的第二附加认证数据中各地址顺序是相同的，进一步地，第一节点利用第一附加认证数据以及第一节点和第二节点之间的会话密钥解密第一报文中的数据。从而当中继设备接收到第二节点发送的第二报文时，不需要对第二报文先进行解密然后再加密后发送第一报文给第一节点，节省了中继设备处理报文的时间，增加了信道利用率，减小了中继设备的额外耗能。

图 11 为本发明另一实施例提供的报文处理装置的结构示意图；位于第二节点侧，应用于中继设备在第一节点和第二节点之间转发报文的场景，具体可以为接入点 AP 或站点 STA，如图 11 所示，第二节点包括：处理器、存储器和通信总线，其中，处理器和存储器通过通信总线连接，存储器中

保存有用于中继设备在第一节点和第二节点之间转发报文的场景时的报文处理方法的实现指令；进一步地，第二节点还包括通信接口，通过通信接口与其他网元设备（例如中继设备）通信。

当处理器调取存储器中的指令时，可以执行如下步骤：

5 生成第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述节点、下一接收方是所述另一节点；

至少根据所述第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，使用所述第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第二报文中的数据进行加密；

10 将所述加密后的第二报文发送给所述中继设备，以使所述中继设备接收到所述第二报文后向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，使得所述第一节点接收到所述第一报文后至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

20 其中，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

25 所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

30 进一步地，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

进一步可选的，所述第二报文中还可以包括中继消息认证信息，所述中继消息认证信息由所述节点使用所述中继设备和所述节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述另一节点发送
5 所述第一报文。

其中，所述第二节点为站点，所述第一节点为接入点；或，所述第二节点为接入点，所述第一节点为站点。

本发明实施例通过第二节点根据第二报文中的地址信息使用第二规则生成第二附加认证数据，利用第二附加认证数据、第一节点与第二节点之间的会话密钥对第二报文中的数据进行加密后，将第二报文发送给中继设备，使得中继设备不需要对第二报文中的加密数据进行解密，而是将第二
10 报文中的加密数据直接携带在第一报文中发送给第一节点，以使第一节点根据第一报文中的地址信息使用第一规则生成第一附加认证数据，其中，使用第一规则生成第一附加认证数据与使用第二规则生成第二附加认证数据是相同的，第一节点利用第一附加认证数据、第一节点和第二节点之间的会话密钥对第一报文中的加密数据进行解密。从而能够实现中继设备在转发加密报文的
15 过程中不需要先解密后再加密的过程，节省了报文处理的时间，增加了信道利用率，减小了中继设备的额外耗能。

图 12 为本发明另一实施例提供的报文处理装置的结构示意图；位于中
20 继设备侧，应用于中继设备在第一节点和第二节点之间转发报文的场景，具体可以为 Relay，如图 12 所示，中继设备包括：处理器、存储器和通信总线，其中，处理器和存储器通过通信总线连接，存储器中保存有用于中继设备在第一节点和第二节点之间转发报文的场景时的报文处理方法的实现指令；进一步地，中继设备还包括通信接口，通过通信接口与其他网元
25 设备（例如接入点或站点）通信。

当处理器调取存储器中的指令时，可以执行如下步骤：

接收第二节点发送的第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是第一节点，所述第二报文中的数据使用了第二附加认证数据、
30 所述第一节点和第二节点之间的会话密钥进行了加密，所述第二附加认证数据由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第

二规则生成;

向所述第一节点发送第一报文, 所述第一报文中包含所述第二报文中的数据, 所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点, 以使所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据, 并使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密, 其中, 所述第一附加认证数据与所述第二附加认证数据相同。

其中, 所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同, 所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同, 使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同; 或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同, 所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同, 使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

进一步地, 所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

进一步可选的, 所述第二报文中还可以包括中继消息认证信息, 所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成, 用以所述中继设备接收到所述第二报文之后, 使用所述消息认证密钥验证所述中继消息认证信息, 若验证通过则向所述第一节点发送所述第一报文。

其中, 所述第一节点为站点, 第二节点为接入点; 或, 所述第一节点为接入点, 所述第二节点为站点

本发明实施例的中继设备在接收到第二节点发送的第二报文时, 不需要中继设备对第二报文中的加密数据先解密后加密的过程, 可以直接将该加密数据重新组装到第一报文中, 节省了中继设备处理报文的时间, 增加了信道利用率, 减小了中继设备的额外耗能。

图 13 为本发明另一实施例提供的报文处理系统的一种结构示意图，应用于中继设备在第一节点和第二节点之间转发报文的场景，如图 13 所示，所述系统具体包括：中继设备 11、第一节点 12 和第二节点 13；

其中，第一节点 12 包括上述图 7 或图 10 所示实施例提供的报文处理装置，详细内容参考图 7 或图 10 所示实施例提供的报文处理装置中的相关描述；

第二节点 13 包括上述图 8 或图 11 所示实施例提供的报文处理装置，详细内容参考图 8 或图 11 所示实施例提供的报文处理装置中的相关描述；

中继设备 11 为上述图 9 或图 12 所示实施例提供的报文处理装置，详细内容参考图 9 或图 12 所示实施例提供的报文处理装置中的相关描述；

在实际应用，若第一节点是接入点 AP 时，则第二节点为站点 STA，或者若第一节点是站点 STA 时，则第二节点是接入点 AP。

本发明实施例通过第一节点接收中继设备发送的第一报文，其中，第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用第二附加认证数据、第一节点和第二节点之间的会话密钥进行加密，所述第二附加认证数据由所述第二节点使用第二规则至少根据所述第二报文的报文头中的地址信息生成的；第一节点至少根据第一报文中的地址信息使用第一规则生成第一附加认证数据，其中，第一节点根据第一规则生成的第一附加认证数据中各地址顺序与第二节点根据第二规则生成的第二附加认证数据中各地址顺序是相同的，进一步地，第一节点利用第一附加认证数据以及第一节点和第二节点之间的会话密钥解密第一报文中的数据。从而当中继设备接收到第二节点发送的第二报文时，不需要对第二报文先进行解密然后再加密后发送第一报文给第一节点，节省了中继设备处理报文的时间，增加了信道利用率，减小了中继设备的额外耗能。

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

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实

现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

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

10 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，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，也可以采用硬件加软件功能单元的形式实现。

15 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元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，或者网络设备等等）执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（Read-Only Memory，简称ROM）、随机存取存储器（Random Access Memory，简称RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

20 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，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发明各实施例技术方案的精神和范围。

25

权利要求

1、一种报文处理方法，应用于中继设备在第一节点和第二节点之间转发报文的场景，其特征在于，包括：

第一节点接收中继设备发送的第一报文，所述第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥进行了加密，所述第二附加认证数据是由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成的，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点；

所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，其中，所述第一附加认证数据与所述第二附加认证数据相同；

所述第一节点使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密。

2、根据权利要求1所述的方法，其特征在于，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

3、根据权利要求1或2所述的方法，其特征在于，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

4、根据权利要求1-3任一所述的方法，其特征在于，所述第二报文中

还包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一报文。

5 5、根据权利要求 1-4 任一项所述的方法，其特征在于，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

6、一种报文处理方法，应用于中继设备在第一节点和第二节点之间转发报文的场景，其特征在于，包括：

10 第二节点生成第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点；

所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，使用所述第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第二报文中的数据进行加密；

15 所述第二节点将所述加密后的第二报文发送给所述中继设备，以使所述中继设备接收到所述第二报文后向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，使得所述第一节点接收到所述第一报文

20 后至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

25 7、根据权利要求 6 所述的方法，其特征在于，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

30 所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据

中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

8、根据权利要求 6 或 7 所述的方法，其特征在于，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

9、根据权利要求 6-8 任一所述的方法，其特征在于，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一报文。

10、根据权利要求 6-9 任一项所述的方法，其特征在于，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

11、一种报文处理方法，应用于中继设备在第一节点和第二节点之间转发报文的场景，其特征在于，包括：

中继设备接收第二节点发送的第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是第一节点，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和第二节点之间的会话密钥进行了加密，所述第二附加认证数据由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成；

所述中继设备向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，以使所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，并使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

12、根据权利要求 11 所述的方法，其特征在于，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺

序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

5 所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

10 13、根据权利要求 11 或 12 所述的方法，其特征在于，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

14、根据权利要求 11-13 任一所述的方法，其特征在于，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述第一节点发送所述第一报文。

15 15、根据权利要求 11-14 任一项所述的方法，其特征在于，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

16、一种报文处理装置，位于第一节点侧，应用于中继设备在所述第一节点和第二节点之间转发报文的场景，其特征在于，包括：

接收模块，用于接收中继设备发送的第一报文，所述第一报文中包括第二节点向所述中继设备发送的第二报文中的数据，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和所述第二节点之间的会话密钥进行了加密，所述第二附加认证数据是由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成的，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是所述第一节点；

解密模块，用于至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述另一第二节点，其中，所述使用所述第一规则生成的附加

认证数据与所述使用所述第二规则生成的附加认证数据相同；使用所述第一附加认证数据、所述第一节点和所述另一第二节点之间的会话密钥对所述第一报文中的数据解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

5 17、根据权利要求 16 所述的装置，其特征在于，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

10 所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

15 18、根据权利要求 16 或 17 所述的装置，其特征在于，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

19、根据权利要求 16-18 任一所述的装置，其特征在于，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述另一节点使用所述中继设备和所述另一节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述节点发送所述第一报文。

20 20、根据权利要求 16-19 任一项所述的装置，其特征在于，所述第一节点为站点，所述第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

25 21、一种报文处理装置，位于第二节点侧，应用于中继设备在所述第二节点和第一节点之间转发报文的场景，其特征在于，包括：

报文生成模块，用于生成第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述节点、下一接收方是所述另一节点；

30 加密模块，用于至少根据所述第二报文的报文头中的地址信息使用第二规则生成第二附加认证数据，使用所述第二附加认证数据、所述第一节

点和所述第二节点之间的会话密钥对所述第二报文中的数据进行了加密；

发送模块，用于将所述加密后的第二报文发送给所述中继设备，以使所述中继设备接收到所述第二报文后向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，使得所述第一节点接收到所述第一报文后至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据进行解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

22、根据权利要求 21 所述的装置，其特征在于，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

23、根据权利要求 21 或 22 所述的装置，其特征在于，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

24、根据权利要求 21-23 任一所述的装置，其特征在于，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述节点使用所述中继设备和所述节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认证信息，若验证通过则向所述另一节点发送所述第一报文。

25、根据权利要求 21-24 任一项所述的装置，其特征在于，所述第二节点为站点，所述第一节点为接入点；或，所述第二节点为接入点，所述第一节点为站点。

26、一种报文处理装置，位于中继设备侧，应用于中继设备在第一节

点和第二节点之间转发报文的场景，其特征在于，包括：

接收模块，用于接收第二节点发送的第二报文，所述第二报文的报文头中的地址信息指示所述第二报文的接收方是所述中继设备、发送方是所述第二节点、下一接收方是第一节点，所述第二报文中的数据使用了第二附加认证数据、所述第一节点和第二节点之间的会话密钥进行了加密，所述第二附加认证数据由所述第二节点至少根据所述第二报文的报文头中的地址信息使用第二规则生成；

发送模块，用于向所述第一节点发送第一报文，所述第一报文中包含所述第二报文中的数据，所述第一报文的报文头中包含的地址信息指示所述第一报文的接收方是所述第一节点、发送方是所述中继设备、上一发送方是所述第二节点，以使所述第一节点至少根据所述第一报文的报文头中的地址信息使用第一规则生成第一附加认证数据，并使用所述第一附加认证数据、所述第一节点和所述第二节点之间的会话密钥对所述第一报文中的数据解密，其中，所述第一附加认证数据与所述第二附加认证数据相同。

27、根据权利要求 26 所述的装置，其特征在于，所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序相同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序不同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同；或

所述第一规则是所述第一附加认证数据中的各地址顺序与所述第一报文的报文头中的各地址顺序不同，所述第二规则是所述第二附加认证数据中的各地址顺序与所述第二报文的报文头中的各地址顺序相同，使得所述第二附加认证数据中各地址顺序和所述第一附加认证数据中各地址顺序相同。

28、根据权利要求 26 或 27 所述的装置，其特征在于，所述第二附加认证数据中的各地址顺序和所述第一附加认证数据中的各地址顺序相同。

29、根据权利要求 26-28 任一所述的装置，其特征在于，所述第二报文中还包括中继消息认证信息，所述中继消息认证信息由所述第二节点使用所述中继设备和所述第二节点之间的消息认证密钥生成，用以所述中继设备接收到所述第二报文之后，使用所述消息认证密钥验证所述中继消息认

证信息，若验证通过则向所述第一节点发送所述第一报文。

30、根据权利要求 26-29 任一项所述的装置，其特征在于，所述第一节点为站点，第二节点为接入点；或，所述第一节点为接入点，所述第二节点为站点。

- 5 31、一种报文处理系统，应用于中继设备在第一节点和第二节点之间转发报文的场景，其特征在于，包括：中继设备、第一节点和第二节点；
所述中继设备包括如权利要求 26-30 任一项所述的报文处理装置；
所述第一节点包括如权利要求 16-20 任一项所述的报文处理装置；
所述第二节点包括如权利要求 21-25 任一项所述的报文处理装置。

10

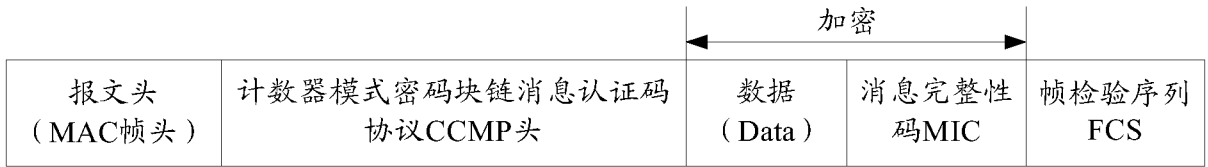


图 1



图 2

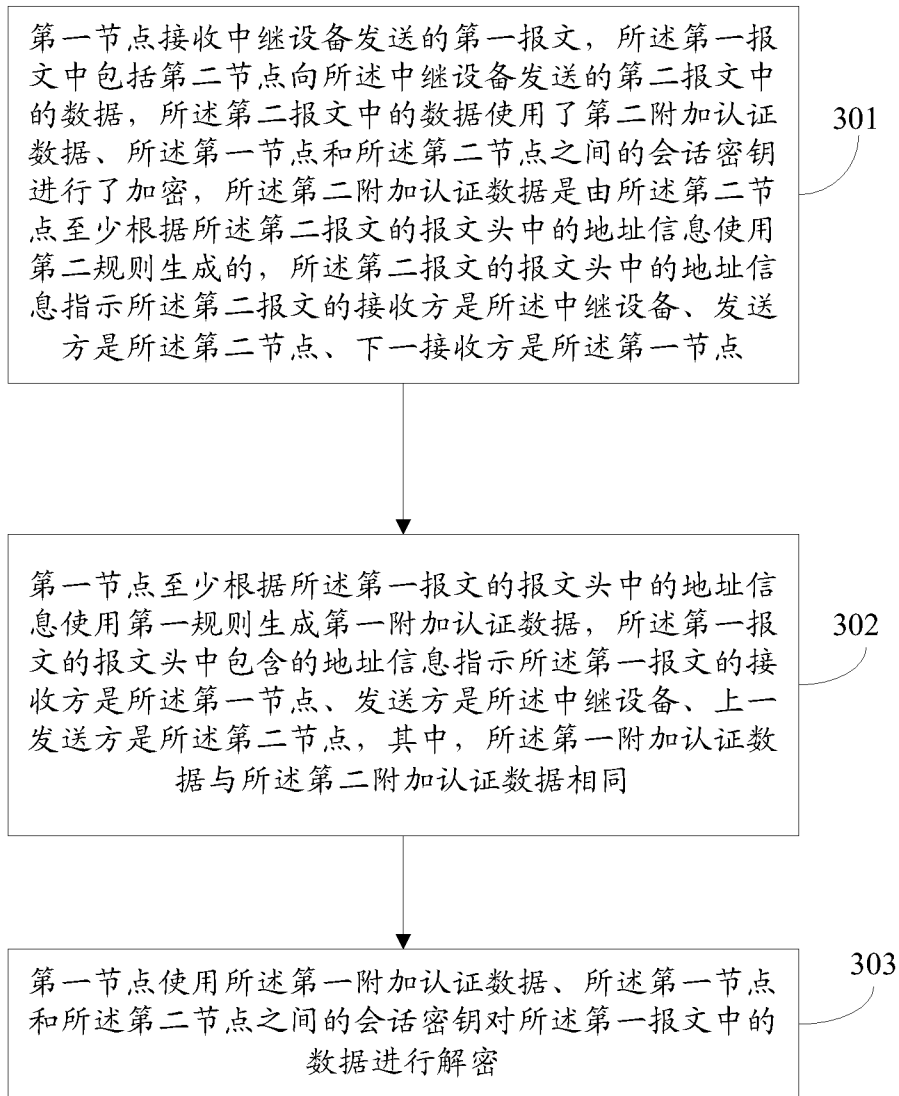


图 3

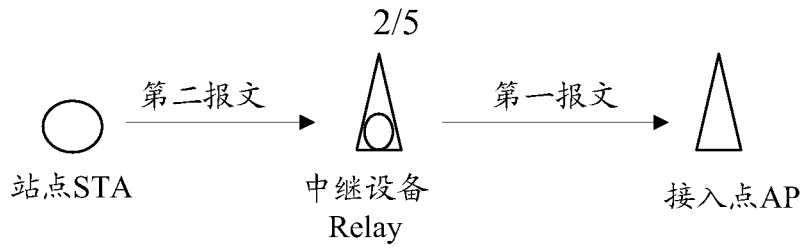


图 4

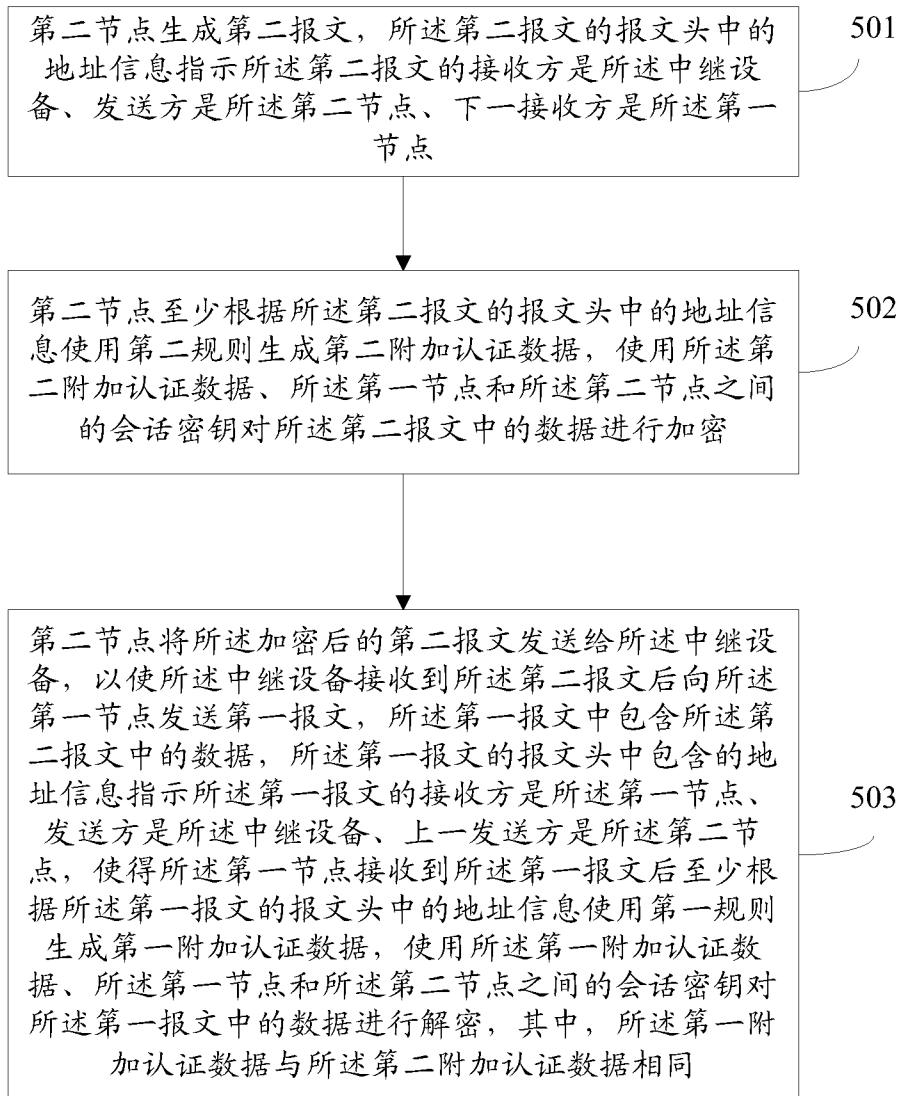


图 5

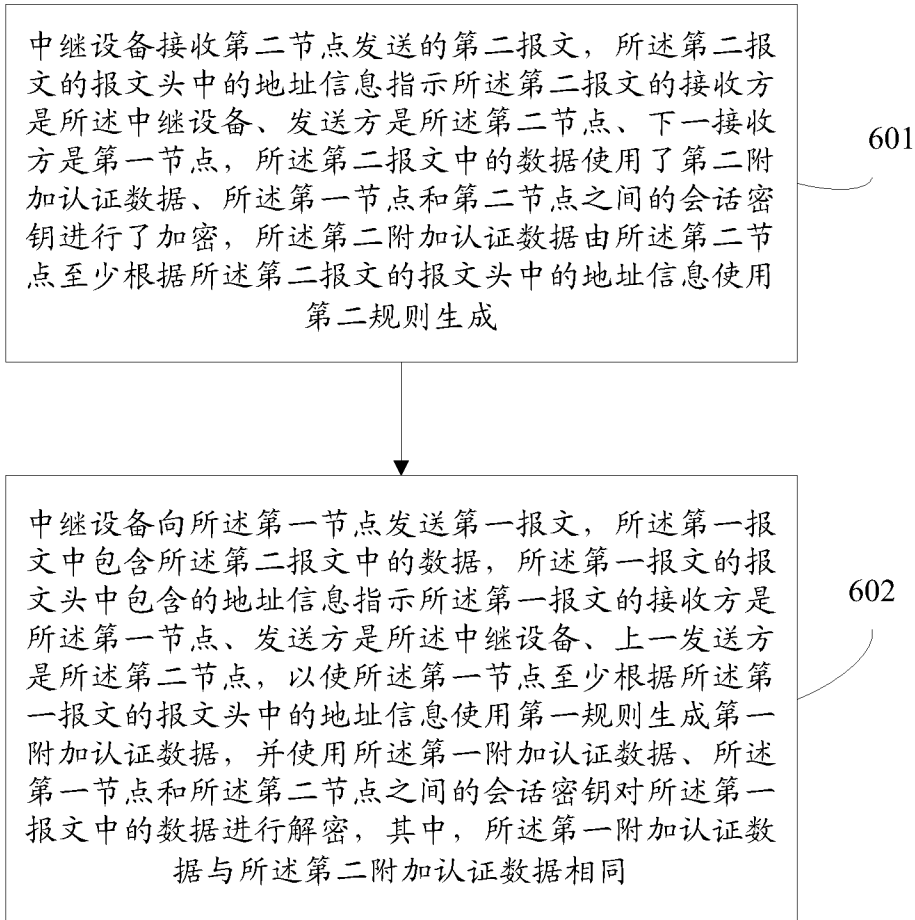


图 6

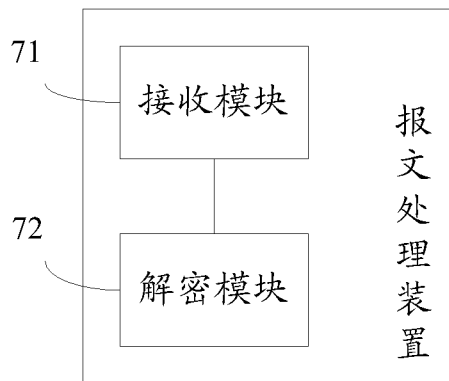


图 7

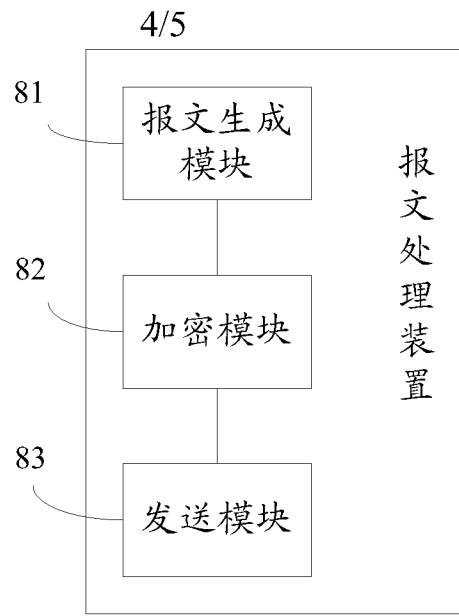


图 8

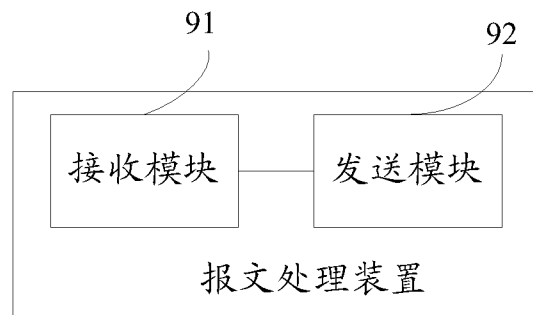


图 9

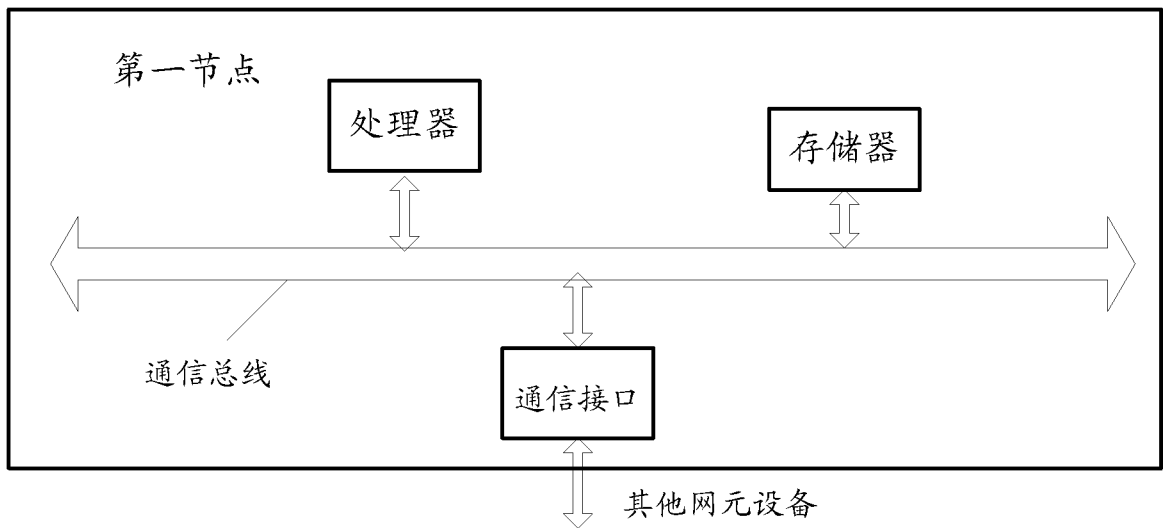


图 10

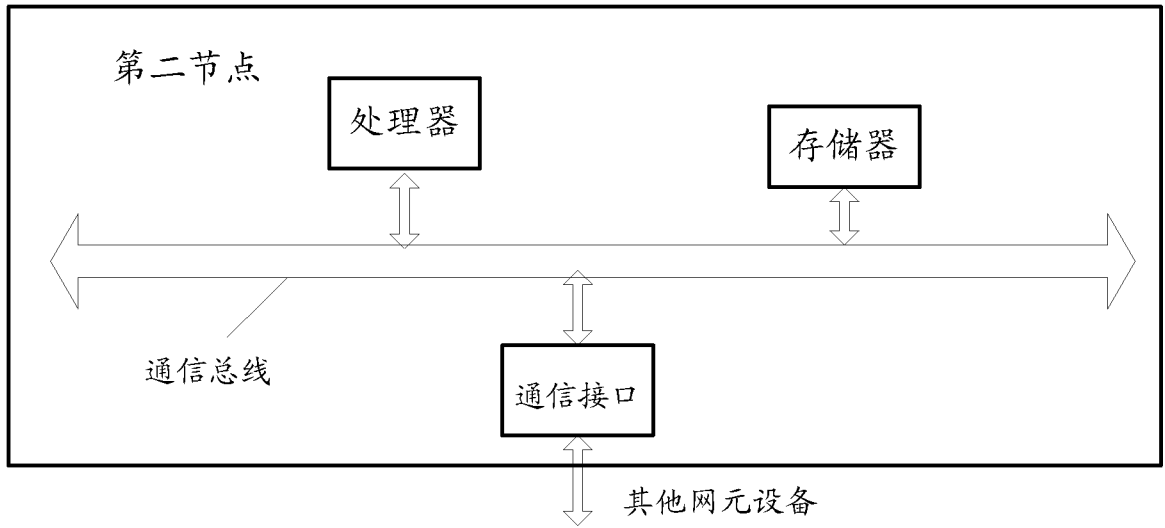


图 11

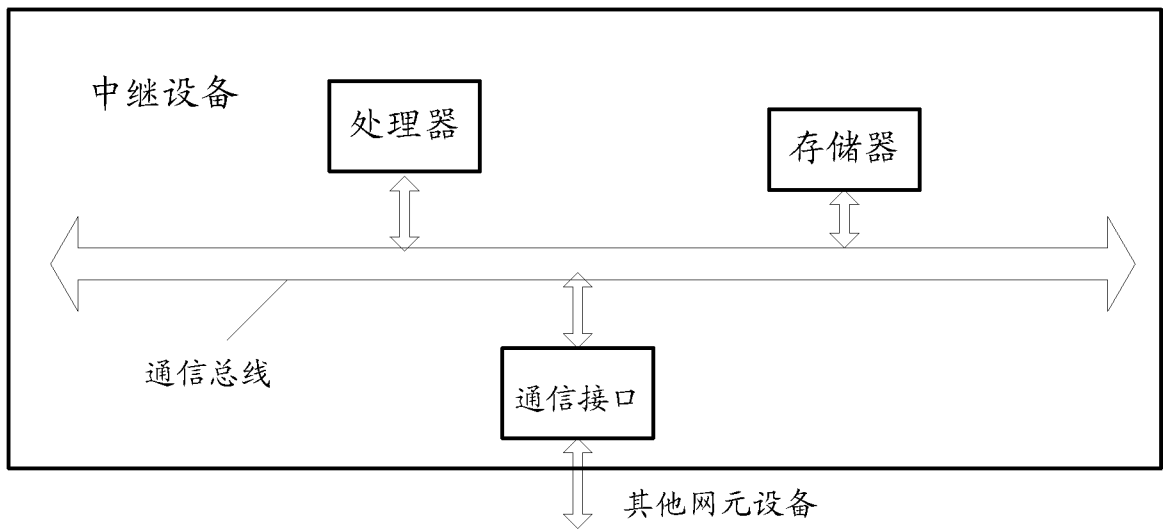


图 12

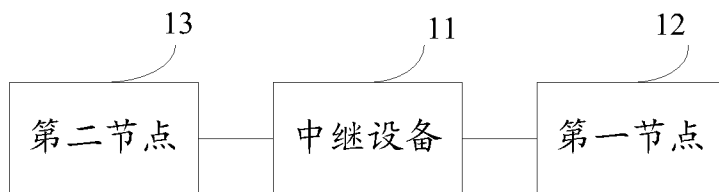


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/088947**A. CLASSIFICATION OF SUBJECT MATTER**

H04W 12/02 (2009.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: 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, CNKI: RELAY, address, field, message, message header, frame header, masthead, node, access point, AP, station, base station, STA, transmit, encryption, decryption, key, IEEE, 802.11

VEN, IEEE: relay, address, transmit, field, node, AP, STA, report, AAD, 802.11

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102647355 A (HUAWEI TECHNOLOGIES CO., LTD.), 22 August 2012 (22.08.2012), the whole document	1-31
A	CN 102143164 A (ZTE CORP.), 03 August 2011 (03.08.2011), the whole document	1-31
A	WO 2011090257 A1 (LG ELECTRONICS INC. et al.), 28 July 2011 (28.07.2011), the whole document	1-31

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

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search
03 March 2014 (03.03.2014)Date of mailing of the international search report
13 March 2014 (13.03.2014)Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451Authorized officer
LUO, Xinyao
Telephone No.: (86-10) **62412039**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/088947

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102647355 A	22.08.2012	WO 2013152589 A1	17.10.2013
CN 102143164 A	03.08.2011	None	
WO 2011090257 A1	28.07.2011	KR 20110085836 A	27.07.2011
		US 2012307685 A1	06.12.2012

国际检索报告

国际申请号
PCT/CN2013/088947

A. 主题的分类		
H04W 12/02 (2009.01) i		
按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
IPC: 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,CNKI: 中继, RELAY, 地址, 字段, 报文, 报文头, 帧头, 报头, 节点, 接入点, AP, 站点, 基站, STA, 转发, 加密, 解密, 密钥, IEEE, 802.11		
VEN, IEEE: relay, address, transmit, field, node, AP, STA, report, AAD, 802.11		
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
A	CN 102647355 A (华为技术有限公司) 22.8 月 2012(22.08.2012) 全文	1-31
A	CN 102143164 A (中兴通讯股份有限公司) 03.8 月 2011(03.08.2011) 全文	1-31
A	WO 2011090257 A1 (LG ELECTRONICS INC.等) 28.7 月 2011(28.07.2011) 全文	1-31
<input type="checkbox"/> 其余文件在 C 栏的续页中列出。 <input checked="" type="checkbox"/> 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 03.3 月 2014 (03.03.2014)		国际检索报告邮寄日期 13.3 月 2014 (13.03.2014)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		授权官员 罗信瑶 电话号码: (86-10) 62412039

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2013/088947

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 102647355 A	22.08.2012	WO 2013152589 A1	17.10.2013
CN 102143164 A	03.08.2011	无	
WO 2011090257 A1	28.07.2011	KR 20110085836 A	27.07.2011
		US 2012307685 A1	06.12.2012