(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
2025 年 5 月 22 日 (22.05.2025)

WIPO | PCT

(10) 国际公布号
WO 2025/102707 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01) *H04W 12/03* (2021.01)

(21) 国际申请号: PCT/CN2024/098824

(22) 国际申请日: 2024 年 6 月 13 日 (13.06.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202311535924.7 2023年11月16日 (16.11.2023) CN

(71) 申请人: 中兴通讯股份有限公司 (**ZTE CORPORATION**) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦 518057 (CN)。

(72) 发明人: 袁立权 (**YUAN, Liquan**); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦 518057 (CN)。

(74) 代理人: 北京康信知识产权代理有限责任公司 (**KANGXIN PARTNERS , P.C.**); 中国北京市海淀区知春路甲48号盈都大厦A座16层 100098 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,

WO 2025/102707 A1

(54) **Title:** INFORMATION PROCESSING METHOD, NETWORK DEVICE, AND COMPUTER-READABLE STORAGE MEDIUM

(54) 发明名称: 信息处理方法、网络设备及计算机可读存储介质

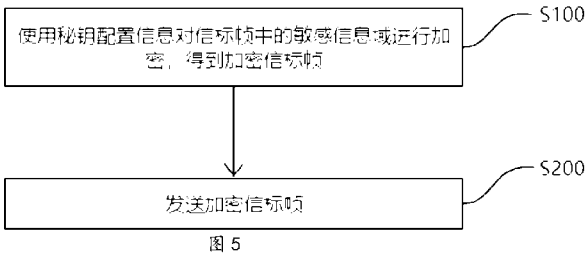


图 5

S100 Encrypt a sensitive information domain in a beacon frame by using key configuration information, so as to obtain an encrypted beacon frame

S200 Send the encrypted beacon frame

(57) **Abstract:** Provided in the present disclosure are an information processing method, a network device, and a computer-readable storage medium. The information processing method is applied to a sending-side network device, and comprises: encrypting a sensitive information domain in a beacon frame by using key configuration information, so as to obtain an encrypted beacon frame; and sending the encrypted beacon frame. In the embodiments of the present disclosure, a sending-side network device can directly use corresponding key configuration information to provide protection for a sensitive information domain in a beacon frame. In this way, a sensitive information domain in a beacon frame is encrypted by using only corresponding key configuration information, such that other network devices or third-party devices can be prevented from acquiring sensitive information in the beacon frame, thereby effectively avoiding the risk of there being a leak of user sensitive information.

(57) 摘要: 本公开提供了一种信息处理方法、网络设备及计算机可读存储介质。其中，信息处理方法应用于发送侧网络设备，包括：使用秘钥配置信息对信标帧中的敏感信息域进行加密，得到加密信标帧；发送所述加密信标帧。本公开实施例中，发送侧网络设备可以直接使用相应的秘钥配置信息对信标帧中的敏感信息域添加保护。因此，仅需使用相应的秘钥配置信息加密信标帧中的敏感信息域，从而能够防止其他网络设备或者第三方设备对该信标帧中的敏感信息的获取，进而有效规避用户敏感信息外泄的风险。

[见续页]

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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。

信息处理方法、网络设备及计算机可读存储介质

相关申请的交叉引用

本公开基于2023年11月16日提交的发明名称为“信息处理方法、网络设备及计算机可读存储介质”的中国专利申请CN202311535924.7，并且要求该专利申请的优先权，通过引用将其所公开的内容全部并入本公开。

技术领域

本公开实施例涉及但不限于通信技术领域，尤其涉及一种信息处理方法、网络设备及计算机可读存储介质。

背景技术

目前，支持严格目标唤醒时间（Restricted Target Wake Up Time，r-TWT）以及群组唤醒时间（broadcast Target Wakeup Time，b-TWT）（以下统一简称：TWT 目标唤醒时间）功能的信标帧中会默认携带 TWT 分组以及服务时间窗口信息，如果第三方设备检测到信标帧中的 TWT 信息后，可以在每次 r-TWT 服务时间窗口内占用信道，从而造成包含低时延业务的设备因为无法在对应的 TWT 窗口及时介入信道而一直等待信道介入，造成应用层的时延问题和功耗问题，进而可能会造成用户隐私外泄的风险。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本公开实施例提供了一种信息处理方法、网络设备及计算机可读存储介质，不仅能够在一定程度上防止其他网络设备或者第三方设备对该信标帧中的敏感信息的获取，还能有效规避用户敏感信息外泄的风险。

第一方面，本公开实施例提供了一种信息处理方法，应用于发送侧网络设备，包括：使用秘钥配置信息对信标帧中的敏感信息域进行加密，得到加密信标帧；发送所述加密信标帧。

第二方面，本公开实施例还提供了一种信息处理方法，应用于接收侧网络设备，包括：接收发送侧网络设备发送的第一信标帧，其中，所述第一信标帧包括使用秘钥配置信息进行加密后的敏感信息域；使用所述秘钥配置信息对所述第一信标帧中的所述敏感信息域进行解密，得到解密敏感信息；根据所述解密敏感信息执行相应的信息处理。

第三方面，本公开实施例还提供了一种网络设备，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如上所述第一方面的信息处理方法或者实现如上所述第二方面的信息处理方法。

第四方面，本公开实施例还提供一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令用于执行如上所述的信息处理方法。

附图说明

图 1 是本公开实施例提供的 NR 的结构图；

图 2 是本公开实施例提供的 MBSSID 元素的结构图；

图 3 是本公开实施例提供的 RSNE 字段结构图；

图 4 是本公开实施例提供的添加了 BIP 保护的管理帧格式；

图 5 是本公开实施例提供的一种信息处理方法的流程图；

图 6 是本公开实施例提供的发送侧网络设备利用同一秘钥生成信息完整性代码和加密敏感信息的示意图；

图 7 是本公开实施例提供的发送侧网络设备利用第一秘钥加密位于不同 IE 的敏感信息元素的结构图；

图 8 是本公开实施例提供的 RSNE 字段扩展的结构图；

图 9 是本公开另一个实施例提供的信息处理方法流程图；

图 10 是本公开实施例提供的秘钥配置信息的结构图；

图 11 是本公开实施例提供的另一种信息处理方法的流程图；

图 12 是本公开一个实施例提供的接收侧网络设备为 AP 或者 AP MLD 时的信息处理流程图；

图 13 是本公开一个实施例提供的接收侧网络设备利用第二秘钥加密位于不同 IE 的敏感信息元素的结构图；

图 14 是本公开一个实施例提供的发送侧网络设备与接收侧网络设备利用信标帧交互加密敏感信息的过程示意图；

图 15 是本公开一个实施例提供的发送侧网络设备与接收侧网络设备利用信标帧交互加密敏感信息的另一过程示意图。

具体实施方式

为了使本公开的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本公开进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本公开，并不用于限定本公开。

需要说明的是，虽然在装置示意图中进行了功能模块划分，在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于装置中的模块划分，或流程图中的顺序执行所示出或描述的步骤。说明书和权利要求书及上述附图中的术语“第一”、“第二”等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。

值得注意的是，在目前的无线通信技术中，光纤到房间(fiber-to-the-room，FTTR)技术是通过光纤连接家庭或中小企业等场景下不同房间或位置的无线路由器 AP，从而提供多 AP 之间组网的高带宽、高可靠性的连接，在此基础上，可以利用点到多点的光分配网络实现主控制 AP 和从 AP 的连接。

目前，邻居报告（NR，Neighbour report）字段包含周围其他接入点（AP）或者多链路接入点（AP MLD，以下简称 AP）的信息，一般用于终端（STA）或者多链路终端（non-AP MLD，以下简称 STA）向目标 AP 发送查询帧，查询周围其他 AP 的信息，目标 AP 向 STA 发送响应帧，反馈 STA 所查询的周围其他 AP 的信息。比如 STA 向 AP 发送接入网络查询协议（ANQP，Access Network Query Protocol）查询帧，AP 向 STA 反馈 ANQP 响应帧。或者，

AP 发送的信标帧，探测响应帧中携带 NR 字段主动广播周围其他 AP 的信息；或者，在发生漫游或者多 AP 负载均衡场景下，AP 向 STA 主动推荐周围其他 AP 的信息，而 STA 对该信息进行确认，然后向所推荐的一个 AP 发送（重）关联请求。比如，AP 向 STA 发送的 BSS 转移管理请求（BSS transition management,BTM）request 帧，并在 NR 字段中携带所推荐的 AP 的信息，STA 发送 BTM response 帧，其包含的 NR 字段中携带所期望连接的 AP 的信息，以及随后发送认证帧和（重）关联帧与目标 AP 建立连接。如图 1 所示，图 1 是本公开实施例提供的 NR 字段结构图，在该 NR 结构中，各主要字段的解释如下：

Element ID：用于表示元素标识符；

Length：用于表示元素长度；

BSSID：用于表示基本服务集合识别符（MAC 地址）；

BSSID Information：用于表示基本服务集合识别符信息字段；

Operating Class：用于表示工作信道类别；

Channel Number：用于表示信道编号；

PHY Type：用于表示物理层类型；

Optional Subelements：用于表示可选子元素；

AP Reachability：用于表示指示邻居 AP 是否可以被探测到；

Security：用于表示与当前链路安全参数是否相同；

Key Scope：用于指示与当前链路对应的认证者信息是否相同；

Capabilities：用于表示邻居 AP 的能力集信息；

Mobility Domain：用于指示邻居 AP 发送的信标帧是否携带移动域元素(MDE,Mobility Domain Element)字段；

High Throughput：用于指示邻居 AP 是否为 HT AP，即是否支持 HT 能力集；

Very High Throughput：用于指示邻居 AP 是否为 VHT AP，即是否支持 VHT 能力集；

FTM：用于指示邻居 AP 是否支持 FTM(Fine Timing measurement,精细时间测量)功能；

High Efficiency：用于指示邻居 AP 是否为 HE AP，即是否支持 HE 能力集；

ER BSS：用于指示邻居 AP 是否为支持扩展覆盖范围（ER，Extended range）功能的 AP；

Colocated AP：用于指示邻居 AP 与当前链路对应的 AP 共存在一个物理设备上；

Unsolicited Probe Responses Active：用于指示邻居 AP 可以在 6GHz 频段上每隔 20ms 发送一个非请求的探测响应帧；

Members of ESS with 2.4/5GHz Colocated AP：用于指示邻居 AP 为工作在 2.4GHz 或者 5GHz 频段，并与当前 AP 共存在一个物理设备上；

OCT Supported With Reporting AP：用于指示当前链路上的 AP 与邻居 AP 支持利用频道隧道(on-channel Tunneling, OCT）技术交互 MMPDU；

Colocated With 6GHz AP：用于表示邻居 AP 为工作在 6GHz 频段，并与当前 AP 共存在一个物理设备上；

Extremely High Throughput：用于指示邻居 AP 是否为 EHT AP，即是否支持 EHT 能力集；

Reserved：用于表示预留字段。

进一步地，为了降低字段长度造成的信道资源开销，在 NR 字段的基础上，RNR(reduced neighbour report)字段进行了相应的裁剪和修改，只包括周围 AP 的关键信息，比如工作信道、

SSID，BSSID 信息等。当 STA 接收到一个 AP 发送的携带 RNR 字段的信标帧、探测响应帧等管理帧时，STA 能够快速发现周围其他 AP，进而在目标 AP 所在的信道上进一步进行探测，从而获取该 AP 的完整信息，这样降低了 STA 盲目扫描信道并探测周围 AP 的时间开销。

由于在 Wi-Fi 的一个射频链路上可以创建多个 AP，每个 AP 对应不同的 BSSID，为了降低每个 AP 发送信标帧、探测响应帧的信道资源开销，802.11 协议引入了多基本服务集合识别符（multiple BSSID，MBSSID）技术，即同一个射频上多个 AP 发送的信标帧、探测响应帧合并到一个 AP 的信标帧和探测响应帧中发送，即一个 AP 的信标帧、探测响应帧中携带同射频其他 AP 的信息，这些信息放在多 BSSID 元素字段中，其结构如图 2 所示，在该结构中，各主要字段的解释如下：

Element ID：用于表示元素标识符；

Length：用于表示元素长度；

MaxBSSID Indicator：用于表示最大基本服务集合识别符（BSSID）数量指示；

Optional Subelements：用于表示可选子元素。

其中，其他 AP 的详细信息存放在 Optional Subelements 之中。

为了增强 WLAN 的数据加密和认证性能，IEEE 通过新一代安全标准，定义了强健安全网络（Robust Security Network,RSN）的概念，并且针对 WEP 加密机制的各种缺陷做了多方面的改进，比如：加密技术和安全认证功能。强健安全网络元素(RSN element, RSNE),用于指示 RSN 中携带的和秘钥套件以及 RSN 能力相关的元素。如图 3 所示，图 3 是本公开实施例提供的 RSNE 字段结构图，在该 RSNE 结构中，各主要字段的解释如下：

Element ID：用于表示唯一标识该元素；

Length：用于表示字段长度信息；

Version：用于表示 RSN 版本信息；

Group Data Cipher Suite：用于表示组播数据帧秘钥套件信息；

Pairwise Cipher Suite Count：用于表示单播秘钥套件数量；

Pairwise Cipher Suite List：用于表示单播秘钥套件列表；

AKM(authentication and key management) Suite Count：用于表示认证和秘钥套件数量；

AKM Suite List：用于表示认证和秘钥套件列表；

RSN Capabilities：用于表示 RSN 能力集；

PMKID Count：用于表示 PMKID 数量；

PMKID List：用于表示 PMKID 列表；

Group Management Cipher Suite：用于表示组播管理帧秘钥套件信息。

进一步地，为了给组播管理帧和信标帧（Beacon）提供数据完整性和重放保护，定义了广播/多播完整性协议(BIP,Broadcast/Multicast Integrity Protocol)。其基本原理是 AP 在向 STA 发送 GTK（组临时秘钥）的同时，发送完整性组临时秘钥（integrity group temporal key，IGTK）以及一个用于 BIP 协议保护的组播帧 完整性保护 帧序号（IGTK Packet Number，IPN）给 STA，然后 AP 在发送的组播帧最后添加利用 IGTK 计算出的管理帧的信息完整性代码（message integrity code，MIC）值后发送给 STA。STA 利用相同的 IGTK 验证 MIC，如果验证成功后，证明该组播帧未被篡改。同样的，对于保护信标帧来说，AP 在向 STA 发送 GTK 的同时，发送信标帧完整性组临时秘钥（Beacon integrity group temporal key，BIGTK）以及

一个用于信标帧完整性保护的帧序号（BIPN，BIGTK PN）给 STA，然后 AP 在发送的组播帧最后添加利用 BIGTK 计算出的管理帧的 MIC 值后发送给 STA。STA 利用相同的 BIGTK 验证 MIC，如果验证成功后，证明该信标帧未被篡改。如图 4 所示，图 4 是添加了 BIP 保护的管理帧的帧格式，即在原来的管理帧的基础上，添加了包含 MIC 信息、秘钥套件索引信息（Key ID)和完整性保护帧序号帧编号信息（IPN）的管理帧信息完整性代码元素(Management MIC Element,MME）字段。

在上述的基础上，Wi-Fi 6 引入的群组唤醒时间（broadcast Target Wakeup Time,b-TWT）技术中，AP 将一段服务时间，比如一个信标周期进行切片，分成更小的服务时间片，对应不同的 b-TWT 组，并用不同的 b-TWT 组 ID 来指示服务时间片信息，然后将该信息通过信标帧广播出去，STA 可以通过协商和非协商方式加入一个 b-TWT 组。当 STA 需要与 AP 进行数据交互时，STA 在对应的 b-TWT 组服务时间内醒来，与 AP 交互上下行缓存数据，在非对应的 b-TWT 组服务时间，STA 不需要周期性醒来检测信标信息，也不需要通过 CSMA/CA 方式竞争信道资源并接收缓存数据，因此降低了 STA 周期性醒来检测信标帧的和抢占信道产生的功耗，实现超低功耗的目标。进一步地，Wi-Fi 7 在 b-TWT 技术基础上，定义了严格目标唤醒时间（Restricted Target Wake Up Time, r-TWT）技术来满足低时延、低功耗业务需求，基本原理是利用 b-TWT 技术，将信道资源按照服务时间进行切片，然后将这些时间切片周期性地分配给具有低时延业务的 STA，调度业务数据在信道中传输，满足业务的时延要求，并且 r-TWT 技术在时间切片开始边界添加保护措施，防止其他设备占用 r-TWT 服务时间段。

在目前的无线通信技术中，IEEE 成立的超高可靠性（UHR，Ultra high reliability）研究组（SG，study group）的研究方向主要集中在提高传输稳定性，包括降低时延、提高吞吐量和降低丢包率。其中一种方式是非 Wi-Fi 信号（比如蓝牙信号）干扰避免技术。具体来说，由于非 Wi-Fi 信号与 Wi-Fi 信号工作在相同的工业、科学和医学（Industrial Scientific Medical Band，ISM）频段上，当两种信号重叠时，势必相互干扰，造成接收端接收到上述重叠信号非常困难，进而导致了丢包率上升。为了解决上述问题，UHR 研究小组正在研究一种非 Wi-Fi 信号干扰避免的方式，具体来说，连接到 AP 的 STA 将自身的非 Wi-Fi 业务的特征（包括起止时间、周期等）告知 AP，AP 将该特征通过信标帧的方式广播出去，其他 STA 接收到该信息后，自动避免在非 Wi-Fi 业务的周期内传输 Wi-Fi 信号，进而降低了因相互干扰产生的丢包率的问题，提升了系统的稳定性。

但由于不同非 Wi-Fi 信号具有其典型的业务特征，比如蓝牙通话（基于蓝牙面向连接技术，即 BT SCO profile），其典型特征为周期 3.75ms 或者 7.5ms，如果第三方设备获取到该信息后，根据蓝牙业务的特征即可推断出该 BSS 周围有 STA 使用了蓝牙电话，显然，使用蓝牙电话属于用户隐私信息，直接将该信息广播出去即造成了用户隐私外泄的风险。

此外，由于支持 r-TWT 以及 b-TWT（以下统一简称：TWT 目标唤醒时间）功能的信标帧中默认携带 TWT 分组以及服务时间窗口信息，如果第三方设备检测到信标帧中的 TWT 信息后，可以在每次 r-TWT 服务时间窗口内占用信道，从而造成包含低时延业务的设备因为无法在对应的 TWT 窗口及时介入信道而一直等待信道介入，造成应用层的时延问题和功耗问题，进而可能会造成用户隐私外泄的风险。

为了能够在一定程度上防止其他网络设备或者第三方设备对信标帧中的敏感信息的获取，并且有效规避用户敏感信息外泄的风险，本公开实施例提供了一种信息处理方法、网络

设备及计算机可读存储介质，其中，发送侧网络设备可以通过使用相应的秘钥配置信息加密信标帧中的敏感信息域，得到对应的加密信标帧，然后，发送侧网络设备在网络中发送该加密信标帧，以使接收侧网络设备在解密该加密信标帧的敏感信息的过程中利用对应的秘钥配置信息对该加密信标帧的敏感信息域解密，即，在网络中保护信标帧的敏感信息传输时，可以仅需使用相应的秘钥配置信息对该信标帧的敏感信息进行加密，从而能够在一定程度上防止其他网络设备或者第三方设备对该信标帧中的敏感信息的获取，有效规避用户敏感信息外泄的风险。

基于上述分析，下面结合附图，对本公开实施例作进一步阐述。

如图 5 所示，图 5 是本公开实施例提供的一种信息处理方法的流程图，该信息处理方法可以应用于发送侧网络设备，该信息处理方法可以包括但不限于步骤 S100 和步骤 S200。

步骤 S100：使用秘钥配置信息对信标帧中的敏感信息域进行加密，得到加密信标帧。

本步骤中，可以理解的是，信标帧可以是无线局域网中定期发送的一个管理帧，信标帧包含有关该网络的信息，通常由接入点设备发送，可用于宣布该网络的存在。

在一实施例中，发送侧网络设备可以为接入点（Access Point, AP）或者多链路接入点（AP multi-link device,AP MLD），例如无线路由器等，本实施例对此并不作具体限定。

在一实施例中，敏感信息域中的信息可以包括：和用户非 Wi-Fi 业务紧密相关的信息，比如非 Wi-Fi 业务使用信道的时间和周期；和用户 Wi-Fi 业务相关的信息，比如网络设备的目标唤醒时间 TWT 的时间信息。

本实施例中，可以理解的是，信道是连接发送侧网络设备和接收侧网络设备之间的传输媒介，即信号传输的通道。此外，在 TWT 中，STA 和 AP 之间建立了一张时间表，该时间表是 STA 和 AP 协定，并由 TWT 时间周期所组成。通常 STA 和 AP 所协商的 TWT 时间周期包含一个或者多个 beacon 周期。当 STA 和 AP 所协商的时间周期到达后，STA 会醒来，并等待 AP 发送的触发帧，并进行一次数据交换。当本次传输完成后，返回睡眠状态。每一个 STA 和 AP 都会进行独立的协商，每一个 STA 都具有单独的 TWT 时间周期。AP 也可以根据多个 STA 设定的 TWT 时间周期进行分组，一次和多个 STA 进行数据传输，从而提高节能效率。

在一实施例中，终端想要建立一个 TWT 连接，该终端可以将自己的节能调度信息告知给 AP，然后 AP 将会分配 TWT 周期，并将该周期反馈给终端，接着终端会在指定的 TWT 周期时苏醒，并和 AP 进行数据帧交换。在本轮交换中，TWT 周期信息在传输的过程中可能被第三方设备获取，当第三方设备获取到 TWT 周期信息后，可以在每次 r-TWT 服务时间窗口内占用信道，从而造成包含低时延业务的设备因为无法在对应的 TWT 窗口及时介入信道而一直等待信道介入，进而造成应用层的时延问题和功耗问题。因此，将 TWT 周期信息作为信标帧的敏感信息进行加密后再传输，其他网络设备或者第三方设备因未能获得该敏感信息域的秘钥信息，无法对加密的敏感信息域进行解密，从而使得包含低时延业务的网络设备能够在对应的 TWT 窗口及时介入信道，提高了传输稳定性和吞吐量，同时降低时延和丢包率。

在一实施例中，敏感信息域可以仅包含本设备的敏感信息域，也可以包括发送侧网络设备的第一敏感信息域和邻居网络设备的第二敏感信息域，而对于第二种情况，发送侧网络设备在利用秘钥配置信息对信标帧中的敏感信息域进行加密时，可以使用秘钥配置信息对信标帧中的第一敏感信息、第二敏感信息域进行加密，得到加密信标帧。

在一实施例中，在保护信标帧的敏感信息传输时，发送侧网络设备可以使用相应的秘钥配置信息对该信标帧的敏感信息域进行加密，然后发送该加密信标帧和该秘钥配置信息，接收侧网络设备接收到该加密信标帧和该秘钥配置信息后，能够直接利用对应的秘钥配置信息对该信标帧的敏感信息域进行解密，从而能够在一定程度上防止其他网络设备或者第三方设备对该信标帧的敏感信息的获取，进而有效规避了用户敏感信息外泄的风险。

在一实施例中，秘钥配置信息可以采用与 BIP 技术相同的帧编号信息、秘钥套件信息和/或秘钥信息，即发送侧网络设备利用该秘钥信息，例如信标帧完整性组临时秘钥（Beacon integrity group temporal key，BIGTK），同时生成信息完整性代码（message integrity code，MIC）和加密敏感信息。

参见图 6，图 6 是发送侧网络设备利用同一秘钥生成信息完整性代码和加密敏感信息的示意图，其基本原理是：AP 在向 STA 发送组临时密钥（Group Temporal Key，GTK）的同时，发送信标帧完整性组临时秘钥以及一个用于信标帧完整性保护的帧序号（BIPN，BIGTK PN）给 STA，然后 AP 在发送的组播帧最后添加利用 BIGTK 计算出的管理帧的 MIC 值后发送给 STA，STA 利用相同的 BIGTK 验证 MIC 值，如果验证成功后，证明该信标帧未被篡改，如果验证失败，则证明该信标帧被篡改。

在一实施例中，当发送侧网络设备发送的信标帧中在邻居报告（neighbour report，NR）、缩减邻居报告（Reduced neighbour report，RNR）或者多基本服务集合识别符（MBSSID）中携带邻居 AP 的敏感信息时，可以使用第一秘钥信息对本 AP 的第一敏感信息域以及邻居 AP 的第二敏感信息域进行加密。

其中，MBSSID 技术能够降低每个 AP 发送信标帧、探测响应帧的信道资源开销。

本实施例中，参见图 7，图 7 示例性地给出发送侧网络设备利用同一秘钥加密位于不同 IE 的敏感信息元素的结构图。其中，发送侧网络设备发送的信标帧中的 MBSSID 字段携带邻居 AP 的敏感信息，在使用秘钥配置信息中的第一秘钥信息对信标帧中的敏感信息域和邻居 AP 的敏感信息域加密时，发送侧网络设备可以使用第一秘钥信息分别对信标帧中的敏感信息域和邻居 AP 的敏感信息域加密。

在一实施例中，发送侧网络设备发送的信标帧中携带秘钥套件指示信息，秘钥套件指示信息可以用于指示对敏感信息域进行加密时所选择的秘钥套件信息，以便接收侧网络设备接收到发送侧网络设备发送的信标帧后，能够利用信标帧中携带的秘钥套件指示信息指示对敏感信息域进行解密。

步骤 S200：发送加密信标帧。

在一实施例中，通过采用上述步骤 S100 的信息处理方法，使得加密信标帧中至少包括加密后的敏感信息域、用于指示对敏感信息域进行加密时所选择的秘钥套件信息的秘钥套件指示信息，从而在网络传输的过程中，能够防止其他网络设备或者第三方设备对该加密信标帧的敏感信息的获取，规避了用户敏感信息外泄的风险。

在一实施例中，加密信标帧可以在包括但不限于互联网、企业内部网、局域网、移动通信网及其组合中发送。

在一实施例中，连接到 AP 的 STA 可以将自身的非 Wi-Fi 业务的特征（包括起止时间、周期等）告知 AP，AP 将该特征通过信标帧加密后广播出去，其他 STA 接收到该信息后，自动避免在非 Wi-Fi 业务的周期内传输 Wi-Fi 信号，进而降低了因相互干扰产生的丢包率的问

题，提升了系统的稳定性。

在一实施例中，在执行步骤S100之前，该信息处理方法可以包括但不限于以下步骤S110。

S110：通过管理帧与接收侧网络设备交互双方对于敏感信息保护的支持能力。

本步骤中，可以理解的是，管理帧至少包括以下一种：信标帧(Beacon frame)、探测请求帧（probe request）、探测响应帧（probe response）、多链路探测请求帧（ML probe request）、多链路探测响应帧（ML probe response）、关联请求（association request）帧、重关联请求（reassociation request）帧、关联响应（association response）帧、重关联响应（reassociation response）帧、认证(authentication)帧和行动帧（action frame）。

在一实施例中，敏感信息保护的支持能力集可以携带于RSNE字段中，其中，RSNE可以用于指示强健安全网络（robust security network，RSN）中携带的和秘钥套件以及RSN能力相关的元素，有利于增强WLAN的数据加密和认证性能。

在一实施例中，管理帧可以包括强健安全网络元素字段，如图8所示，图8示例性地给出了RSNE字段扩展的结构，在RSNE的RSN Capabilities能力集字段中，可以存在多个Reserved比特指示位，如图8所示的B10标志位，B11标志位，B12标志位，B15标志位，这些标志位都可以用来作为敏感信息保护能力指示标志位，用于指示是否支持信标帧中的敏感信息保护。在指示支持信标帧中的敏感信息保护时，可以在预留的标志位中任意选择一个，然后将该标志位的比特置1即可。此外，如果指示不支持信标帧中的敏感信息保护，可以将该标志位的比特置0。例如图8中的B10标志位，把原来的Reserved比特指示位设置为敏感信息保护能力指示标志位（Sensitive Info Protection），当该敏感信息保护能力指示标志位置1，说明能够支持信标帧中的敏感信息保护；当该敏感信息保护能力指示标志位置0，说明不支持信标帧中的敏感信息保护。

如图9所示，图9是本公开另一个实施例提供的信息处理方法流程图，在步骤S100中的加密信标帧之前，该信息处理方法可以包括但不限于步骤S300至步骤S400。

S300：生成秘钥配置信息。

在一实施例中，发送侧网络设备可以在本地生成用于加密、解密信标帧中敏感信息的秘钥配置信息。其中，秘钥配置信息包括秘钥信息、信标帧编号信息和秘钥套件信息。如图10所示，图10示例性地给出了秘钥配置信息的结构，在该结构中，各主要字段的解释如下：

Key ID：用于表示秘钥套件指示信息；

PN：用于表示帧编号；

Key：用于表示秘钥信息。

其中，秘钥信息可以用于生成信息完整性代码以及用于对信标帧中的敏感信息域进行加密。

在一实施例中，秘钥套件信息可以至少包括以下一种：AES-128-CMAC、AES-128-GMAC、AES-256-CMAC、AES-256-GMAC和SM4。

S400：通过信息帧将秘钥配置信息发送给接收侧网络设备。

本步骤中，信息帧的类型可以包括以下任意一种：认证帧；EAPOL帧；动作帧。另外，接收侧网络设备可以为接入点（Access Point, AP）、多链路接入点（AP multi-link device,AP MLD）、终端（Station，STA）和多链路终端(non-AP MLD)。

在一实施例中，发送侧网络设备可以通过信息帧与接收侧网络设备进行秘钥配置信息的

交互，以使接收侧网络设备获取到对应的秘钥配置信息，并使用该秘钥配置信息中的秘钥信息对接收到的信标帧的敏感信息域进行解密，得到解密信息。

在一实施例中，发送侧网络设备的信息处理方法还可以包括：不在敏感信息域承载的敏感信息所对应的业务接入信道的时间窗口内发起竞争以及使用信道资源。

此外，如图 11 所示，图 11 是本公开实施例提供的另一种信息处理方法的流程图，该信息处理方法应用于接收侧网络设备，该信息处理方法可以包括但不限于步骤 A100 至步骤 A300。

步骤 A100：接收发送侧网络设备发送的第一信标帧，其中，第一信标帧包括使用秘钥配置信息进行加密后的敏感信息域。

在一实施例中，接收侧网络设备接收到发送侧网络设备发送的第一信标帧可以携带秘钥套件指示信息，其中，秘钥套件指示信息用于指示对第一信标帧的敏感信息域进行解密时所选择的秘钥套件信息。

值得注意的是，本实施例中对第一信标帧、敏感信息域的相关介绍及解释，与前述步骤 S100 中所示的实施例中对于信标帧、敏感信息的相关介绍及解释相一致，针对本实施例中对第一信标帧、敏感信息域的相关介绍及解释，可参照前述步骤 S100 中所示的实施例中对于信标帧、敏感信息的相关介绍及解释，此处不再做赘述。

步骤 A200：使用秘钥配置信息对第一信标帧中的敏感信息域进行解密，得到解密敏感信息。

本步骤中，需要说明的是，秘钥配置信息可以包括秘钥信息、信标帧的编号信息和秘钥套件信息，其中，秘钥信息可以用于验证信息完整性代码以及用于对第一信标帧中的敏感信息域进行解密。

在一实施例中，秘钥配置信息可以包括用于加密第一信标帧中的敏感信息域和生成第一信标帧中的信息完整性代码的秘钥信息、第一信标帧的编号信息以及秘钥套件信息。

在一实施例中，当接收侧网络设备接收到发送侧网络设备发送的加密信标帧后，接收侧网络设备可以利用先前接收到的发送侧网络设备发送的秘钥配置信息的秘钥信息，对该加密信标帧中的敏感信息域进行解密，并对其 MIC 信息进行验证。如果验证成功，证明该信标帧未被篡改；如果验证失败，则证明该信标帧被篡改。

在一实施例中，当第一信标帧中的敏感信息域包括发送侧网络设备的第一敏感信息域，以及发送侧网络设备的邻居网络设备的第二敏感信息域时，接收侧网络设备可以利用所接收到的秘钥配置信息的秘钥信息对第一敏感信息域和第二敏感信息域进行解密，得到对应的解密敏感信息，以便后续可以根据解密敏感信息执行相应的操作。

步骤 A300：根据解密敏感信息执行相应的信息处理。

在一实施例中，当接收侧网络设备为终端或者多链路终端时，接收侧网络设备执行相应的信息处理可以包括：不在解密敏感信息对应的业务接入信道的时间窗口内发起竞争以及使用信道资源。

本实施例中，可以理解的是，网络设备通信可以是随机信道接入，即网络设备不占据固定的资源，为了安排不同网络设备之间对资源的使用，通常需要通过“竞争”的过程来完成。解密敏感信息对应的业务接入信道的时间窗口指的是，在一段时间内，信道资源是被解密敏感信息对应的业务占用的，接收侧网络设备能够根据该解密敏感信息的指示，在该解密敏感

信息对应的业务接入信道的时间窗口内，不去发起竞争以及使用信道资源，以便对应的业务能够使用信道资源。

参见图 12，图 12 示例性地给出了接收侧网络设备为 AP 或者 AP MLD 时的信息处理流程图。在一实施例中，当接收侧网络设备为接入点或者多链路接入点时，相应的信息处理可以包括但不限于步骤 A310 至步骤 A320。

A310：使用接收侧网络设备本地生成的秘钥配置信息对解密敏感信息进行加密，得到加密信息。

在一实施例中，由接收侧网络设备本地生成的秘钥配置信息可以包括用于加密第二信标帧中的敏感信息域和生成第二信标帧中的信息完整性代码的第二秘钥信息、第二信标帧的编号信息以及秘钥套件信息。

在一实施例中，当接收侧网络设备利用接收到的秘钥配置信息中的第一秘钥信息对第一信标帧中的敏感信息域进行解密，得到解密信息后，可以再次使用该接收侧网络设备本地生成的第二秘钥信息对所得到的解密信息进行加密，接着将再次加密后的解密信息复制到第二信标帧中的存放发送侧网络设备敏感信息字段中，然后，接收侧网络设备可以将该第二信标帧在网络中发送。

A320：根据加密信息生成第二信标帧，第二信标帧包括用于存放加密信息的敏感信息字段。

在一实施例中，第二信标帧中存放发送侧网络设备敏感信息的字段，其中，用于存放的字段可以包括：NR 字段、RNR 字段或者 MBSSID 字段，NR 字段、RNR 字段或者 MBSSID 字段可以用于表示邻居 AP 包含了敏感信息，此处的邻居 AP 为发送侧网络设备。

在一实施例中，参见图 13，图 13 示例性地给出接收侧网络设备利用第二秘钥加密位于不同 IE 的敏感信息元素的结构图。其中，第二信标帧中的 NR 字段用于存放发送侧网络设备敏感信息，接收侧网络设备在使用秘钥配置信息中的秘钥信息对第二信标帧中的敏感信息域和发送侧网络设备敏感信息域加密时，可以使用第二秘钥信息分别对第二信标帧中的敏感信息域和发送侧网络设备敏感信息域加密。

在一实施例中，当接收侧网络设备为接入点或者多链路接入点时，相应的信息处理还可以包括：不在解密敏感信息对应的业务接入信道的时间窗口内发起竞争以及使用信道资源。

本实施例中，接收侧网络设备接收到的信标帧可以支持 r-TWT 以及 b-TWT 功能，此时，信标帧中默认携带 TWT 分组以及服务时间窗口信息，接收侧网络设备能够根据该解密敏感信息的指示，在该解密敏感信息对应的业务接入信道的时间窗口内，如果不是对应的 r-TWT 以及 b-TWT 组成员，则不去发起竞争以及使用信道资源，以便对应的业务能够在对应的 TWT 窗口及时介入信道，从而可以降低传输时延、提高吞吐量和降低丢包率。

在一实施例中，当接收侧网络设备为接入点或者多链路接入点时，相应的信息处理可以包括但不限于以下两种：接收侧网络设备不在解密敏感信息对应的业务接入信道的时间窗口内发起竞争以及使用信道资源；接收侧网络设备使用本地生成的秘钥配置信息对解密敏感信息进行加密，得到加密信息，紧接着根据加密信息生成第二信标帧，其中，第二信标帧包括用于存放加密信息的敏感信息字段，然后发送第二信标帧。

值得注意的是，本实施例中，相应的信息处理的具体实施方式和技术效果的相关介绍及解释，与上述步骤 A300、A310 和 A320 中任意一项实施例所描述的信息处理方法的具体实

施方式和技术效果的相关介绍及解释相一致，针对本实施例中相应的信息处理的具体实施方式和技术效果的相关介绍及解释，可参照上述步骤 A300、A310 和 A320 中任意一项实施例所描述的信息处理方法的具体实施方式和技术效果的相关介绍及解释，此处不再赘述。

A330：发送第二信标帧。

在一实施例中，通过采用包括有上述步骤 A310 和步骤 A320 的信息处理方法，可以使得第二信标帧中至少包括加密后的第二信标帧中的敏感信息域和加密后的发送侧网络设备的敏感信息域、用于指示对敏感信息域进行加密时所选择的秘钥套件信息的秘钥套件指示信息。

在一实施例中，接收侧网络设备可以和第三接收侧网络设备交互双方对于敏感信息保护的支持能力，并且第三接收侧网络设备也可以接收并保存接收侧网络设备通过第二信息帧发送的第二秘钥配置信息，从而使得当第三接收侧网络设备接受到加密的第二信标帧时，能够根据第二秘钥配置信息中的秘钥信息对第二信标帧的加密敏感信息域进行解密和验证，得到解密的敏感信息后再根据解密信息作出后续的信息处理。如此，不仅能够防止其他网络设备或者第三方设备获取该加密的第二信标帧的敏感信息，还有效规避了用户敏感信息外泄的风险。

在一实施例中，在执行步骤 A100 之前还可以包括步骤：通过管理帧与发送侧网络设备交互双方对于敏感信息保护的支持能力。

在一实施例中，接收侧网络设备通过将管理帧的强健安全网络元素字段中的标志位的比特置 1，与发送侧网络设备交互敏感信息保护的支持能力。

值得注意的是，本实施例中涉及的信息处理的具体实施方式和技术效果的相关介绍及解释，与上述步骤 S110 中任意一项实施例所描述的信息处理方法的具体实施方式和技术效果的相关介绍及解释相一致，针对本实施例中涉及的具体实施方式和技术效果的相关介绍及解释，可参照上述步骤 S110 中任意一项实施例所描述的信息处理方法的具体实施方式和技术效果的相关介绍及解释，此处不再赘述。

在一实施例中，在执行步骤 A100 之前还可以包括步骤：接收发送侧网络设备通过信息帧发送的秘钥配置信息。

其中，秘钥配置信息可以包括：用于加密该信标帧中的敏感信息域和生成该信标帧中的信息完整性代码的秘钥信息、该信标帧的编号信息以及秘钥套件信息。

在一实施例中，秘钥套件信息可以至少包括以下一种：AES-128-CMAC、AES-128-GMAC、AES-256-CMAC、AES-256-GMAC 和 SM4。此外，信息帧的类型可以包括以下任意一种：认证帧，EAPOL 帧，动作帧。

在一实施例中，发送侧网络设备可以随时在网络中通过信息帧发送更新后的秘钥配置信息，当接收侧网络设备接收到该信息帧后，可以获得更新的秘钥配置信息，然后将更新的秘钥配置信息替换原来保存的秘钥配置信息。

本公开实施例中，对于连接到该 AP 的 STA 设备来说，STA 设备直接使用对应的秘钥信息解密保护的敏感信息域，即可获得该敏感信息，并且能够防止在其工作时间周期内使用相同的信道，而对于其他 STA 或者第三方设备来说，因为没有获得相应的秘钥，也就无法获取和用户业务有关的敏感信息，从而有效规避了用户敏感信息外泄的风险。

针对上述实施例所提供的信息处理方法，下面以具体的示例进行详细的描述：

示例一：

参见图 14，图 14 是发送侧网络设备与接收侧网络设备利用信标帧交互加密敏感信息的过程示意图。其中，图 14 所示的发送侧网络设备可以是接入点或者多链路接入点，接收侧网络设备可以是终端或者多链路终端，该交互过程具体示例如下：

步骤 1：发送侧网络设备通过管理帧与接收侧网络设备交互敏感信息保护支持能力。

步骤 2：发送侧网络设备本地生成用于加密、解密信标帧中敏感信息的秘钥配置信息 1。

步骤 3：发送侧网络设备与接收侧网络设备在进行帧的交互过程中，发送侧网络设备向接收侧网络设备发送一个信息帧，将上述秘钥配置信息 1 发送给接收侧网络设备。

步骤 4：接收侧网络设备将上述秘钥配置信息 1 本地保存。

步骤 5：发送侧网络设备发送已使用上述秘钥配置信息 1 加密其敏感信息域的信标帧。

步骤 6：接收侧网络设备接收到上述信标帧后，使用上述秘钥配置信息 1 解密其敏感信息。

步骤 7：接收侧网络设备根据解密的敏感信息指示，做出相应的信息处理。

需要说明的是，上述交互过程中的发送侧网络设备可以为 AP 或者 AP MLD，接收侧网络设备可以是 AP、AP MLD、STA、non-AP MLD 中的任意一个。

在一实施例中，当步骤（5）中的信标帧的敏感信息域包括本发送侧网络设备的第一敏感信息和邻居 AP 的第二敏感信息时，发送侧网络设备需要使用同一秘钥信息对第一敏感信息、第二敏感信息进行加密，而当接收侧网络设备为 AP 或者 AP MLD 时，接收侧网络设备在根据秘钥配置信息对敏感信息域进行解密之后，需要再次利用其本地生成的第二秘钥信息对该解密信息域进行加密。

值得注意的是，由于本示例一中所涉及的具体实施方式和技术效果的相关介绍及解释，包括有上述任意一项实施例所描述的信息处理方法，因此，有关本示例一中所涉及的具体实施方式和技术效果的相关介绍及解释，可参照上述任意一项实施例所描述的信息处理方法，在此不做赘述。

示例二：

参见图 15，图 15 是发送侧网络设备与接收侧网络设备利用信标帧交互加密敏感信息的另一过程示意图。其中，图 15 所示的发送侧网络设备可以是接入点或者多链路接入点，接收侧网络设备可以是接入点或者多链路接入点。此时，图 15 所示的接收侧网络设备可以重复图 14 中所示的发送侧网络设备的操作，对应的，图 15 所示的发送侧网络设备重复图 14 中所示的接收侧网络设备的操作。因此，在图 14 所示的交互过程的基础上，图 15 所示的交互过程具体还包括如下步骤：

步骤 A：接收侧网络设备通过管理帧与发送侧网络设备交互敏感信息保护支持能力。

步骤 B：接收侧网络设备本地生成用于加密、解密信标帧中敏感信息的秘钥配置信息 2。

步骤 C：接收侧网络设备与发送侧网络设备在进行帧的交互过程中，接收侧网络设备向发送侧网络设备发送一个信息帧，将上述秘钥配置信息 2 发送给发送侧网络设备。

步骤 D：发送侧网络设备将上述秘钥配置信息 2 本地保存。

步骤 E：接收侧网络设备发送已使用上述秘钥配置信息 2 加密其敏感信息域的信标帧。

步骤 F：发送侧网络设备接收到上述信标帧后，使用上述秘钥配置信息 2 解密其敏感信息。

步骤 G：发送侧网络设备根据解密的敏感信息指示，做出相应的信息处理。

值得注意的是，由于本示例二中所涉及的具体实施方式和技术效果的相关介绍及解释，包括有上述任意一项实施例所描述的信息处理方法，因此，有关本示例二中所涉及的具体实施方式和技术效果的相关介绍及解释，可参照上述任意一项实施例所描述的信息处理方法，在此不做赘述。

本公开中的发送侧网络设备和接收侧网络设备分别包括有存储器和处理器，其中，存储器和处理器可以通过总线或者其他方式连接。

存储器作为一种非暂态计算机可读存储介质，可用于存储非暂态软件程序以及非暂态性计算机可执行程序。此外，存储器可以包括高速随机存取存储器，还可以包括非暂态存储器，例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施方式中，存储器可选包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至该处理器。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

本公开实施例描述的发送侧网络设备和接收侧网络设备利用信标帧交互加密的敏感信息的应用场景是为了更加清楚的说明本公开实施例的技术方案，并不构成对于本公开实施例提供的技术方案的限定，本领域技术人员可知，随着新应用场景的出现，本公开实施例提供的技术方案对于类似的技术问题，同样适用。

基于上述信息处理方法，本公开的一个实施例提供了一种网络设备，该网络设备包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序。

处理器和存储器可以通过总线或者其他方式连接。

需要说明的是，本实施例中的网络设备，可以应用于本公开实施例中的发送侧网络设备、接收侧网络设备以及第三接收侧网络设备，这些实施例均属于相同的发明构思，因此这些实施例具有相同的实现原理以及技术效果，此处不再详述。

实现上述实施例的信息处理方法所需的非暂态软件程序以及指令存储在存储器中，当被处理器执行时，执行上述实施例的信息处理方法，例如，执行以上描述的图 5 中的方法步骤 S100 至 S200、图 9 中的方法步骤 S300 至 S400、图 11 中的方法步骤 A100 至 A300、图 12 中的方法步骤 A310 至 A330。

以上所描述的装置实施例仅仅是示意性的，其中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，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。

此外，基于上述信息处理方法，本公开的一个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存储有计算机可执行指令，该计算机可执行指令被一个处理器或控制器执行，例如，被上述网络设备实施例中的一个处理器执行，可使得上述处理器执行上述实施例中的信息处理方法，例如，执行以上描述的图 5 中的方法步骤 S100 至 S200、图 9 中的方法步骤 S300 至 S400、图 11 中的方法步骤 A100 至 A300、图 12 中的方法步骤 A310 至 A330。

本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统可以被实施为软件、固件、硬件及其适当的组合。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质（或非暂时性介质）和通信介质（或暂时性介质）。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息（诸如计算机可读指令、数据

结构、程序模块或其他数据）的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

以上是对本公开的较佳实施进行了具体说明，但本公开并不局限于上述实施方式，熟悉本领域的技术人员在不违背本公开精神的前提下还可作出种种的等同变形或替换，这些等同的变形或替换均包含在本公开权利要求所限定的范围内。

权 利 要 求 书

1. 一种信息处理方法，应用于发送侧网络设备，所述方法包括：

使用秘钥配置信息对信标帧中的敏感信息域进行加密，得到加密信标帧；

发送所述加密信标帧。

2. 根据权利要求 1 所述的方法，其中，所述使用秘钥配置信息对信标帧中的敏感信息域进行加密之前，所述方法还包括：

通过管理帧与接收侧网络设备交互双方对于敏感信息保护的支持能力。

3. 根据权利要求 2 所述的方法，其中，所述管理帧包括强健安全网络元素字段，所述强健安全网络元素字段包括敏感信息保护能力指示标志位，所述敏感信息保护能力指示标志位用于指示是否支持对所述信标帧的所述敏感信息域进行保护。

4. 根据权利要求 3 所述的方法，其中，所述管理帧包括如下之一：

信标帧；

探测请求帧；

探测响应帧；

多链路探测请求帧；

多链路探测响应帧；

关联请求帧；

重关联请求帧；

关联响应帧；

重关联响应帧；

认证帧；

行动帧。

5. 根据权利要求 1 所述的方法，其中，所述使用秘钥配置信息对信标帧中的敏感信息域进行加密之前，所述方法还包括：

生成所述秘钥配置信息；

通过信息帧将所述秘钥配置信息发送给接收侧网络设备。

6. 根据权利要求 5 所述的方法，其中，所述秘钥配置信息包括秘钥信息、信标帧编号信息和秘钥套件信息。

7. 根据权利要求 6 所述的方法，其中，

所述秘钥信息用于生成信息完整性代码以及用于对所述信标帧中的所述敏感信息域进行加密。

8. 根据权利要求 6 所述的方法，其中，所述信标帧包括秘钥套件指示信息，所述秘钥套件指示信息用于指示对所述敏感信息域进行加密时所选择的所述秘钥套件信息。

9. 根据权利要求 5 所述的方法，其中，所述信息帧包括如下之一：

认证帧；

EAPOL 帧；

动作帧。

10. 根据权利要求 1 所述的方法，其中，所述敏感信息域包括所述发送侧网络设备的第一敏感信息域和邻居网络设备的第二敏感信息域；

使用秘钥配置信息对信标帧中的敏感信息域进行加密，得到加密信标帧，包括：

使用所述秘钥配置信息对所述信标帧中的所述第一敏感信息域进行加密，并且使用所述秘钥配置信息对所述信标帧中的所述第二敏感信息域进行加密，得到加密信标帧。

11. 根据权利要求 1 所述的方法，所述方法还包括：

不在所述敏感信息域承载的敏感信息所对应的业务接入信道的时间窗口内发起竞争以及使用信道资源。

12. 一种信息处理方法，应用于接收侧网络设备，所述方法包括：

接收发送侧网络设备发送的第一信标帧，其中，所述第一信标帧包括使用秘钥配置信息进行加密后的敏感信息域；

使用所述秘钥配置信息对所述第一信标帧中的所述敏感信息域进行解密，得到解密敏感信息；

根据所述解密敏感信息执行相应的信息处理。

13. 根据权利要求 12 所述的方法，其中，所述接收发送侧网络设备发送的第一信标帧之前，所述方法还包括：

通过管理帧与所述发送侧网络设备交互双方对于敏感信息保护的支持能力。

14. 根据权利要求 13 所述的方法，其中，所述管理帧包括强健安全网络元素字段，所述强健安全网络元素字段包括敏感信息保护能力指示标志位，所述敏感信息保护能力指示标志位用于指示是否支持对所述第一信标帧的所述敏感信息域进行保护。

15. 根据权利要求 14 所述的方法，其中，所述管理帧包括如下之一：

信标帧；

探测请求帧；

探测响应帧；

多链路探测请求帧；

多链路探测响应帧；

关联请求帧；

重关联请求帧；

关联响应帧；

重关联响应帧；

认证帧；

行动帧。

16. 根据权利要求 12 所述的方法，其中，所述接收发送侧网络设备发送的第一信标帧之前，所述方法还包括：

接收所述发送侧网络设备通过信息帧发送的所述秘钥配置信息。

17. 根据权利要求 16 所述的方法，其中，所述秘钥配置信息包括秘钥信息、信标帧编号信息和秘钥套件信息。

18. 根据权利要求 17 所述的方法，其中，所述秘钥信息用于验证信息完整性代码以及用于对所述第一信标帧中的所述敏感信息域进行解密。

19. 根据权利要求 17 所述的方法，其中，所述第一信标帧包括秘钥套件指示信息，所述秘钥套件指示信息用于指示对所述敏感信息域进行解密时所选择的所述秘钥套件信息。

20. 根据权利要求 16 所述的方法，其中，所述信息帧包括如下之一：

认证帧；

EAPOL 帧；

动作帧。

21. 根据权利要求 12 所述的方法，其中，所述敏感信息域包括所述发送侧网络设备的第一敏感信息域和邻居网络设备的第二敏感信息域；

所述使用所述秘钥配置信息对所述第一信标帧中的所述敏感信息域进行解密，得到解密敏感信息，包括：

使用所述秘钥配置信息对所述第一信标帧中的所述第一敏感信息域进行解密，并且使用所述秘钥配置信息对所述第一信标帧中的所述第二敏感信息域进行解密，得到解密敏感信息。

22. 根据权利要求 12 所述的方法，其中，所述接收侧网络设备为终端设备，所述根据所述解密敏感信息执行相应的信息处理，包括：

不在所述解密敏感信息对应的业务接入信道的时间窗口内发起竞争以及使用信道资源。

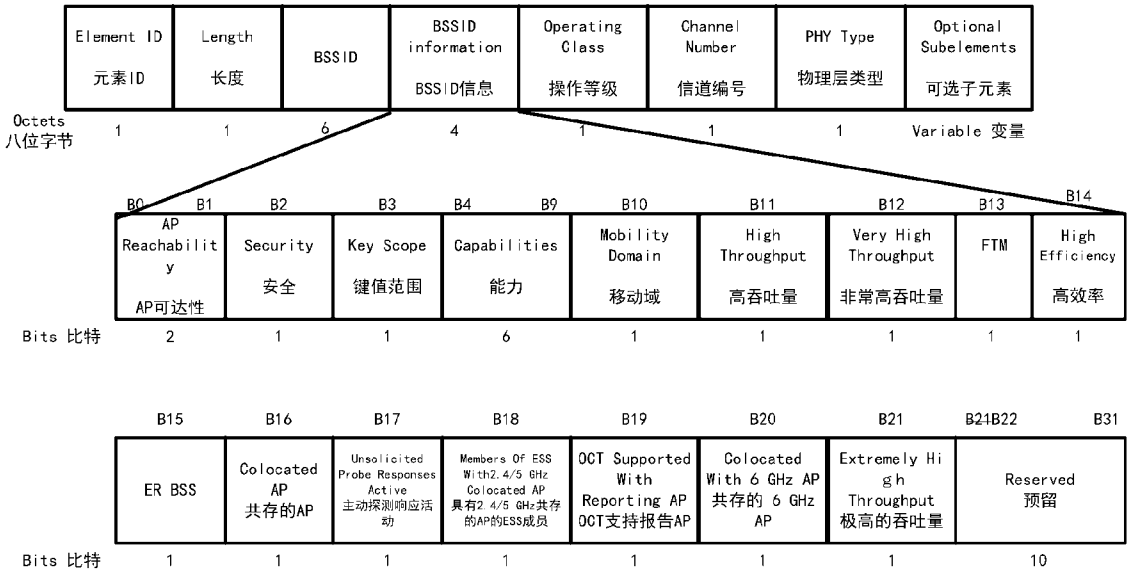
23. 根据权利要求 12 所述的方法，其中，所述接收侧网络设备为接入点设备，所述根据所述解密敏感信息执行相应的信息处理，包括以下至少之一：

不在所述解密敏感信息对应的业务接入信道的时间窗口内发起竞争以及使用信道资源；

使用本地生成的秘钥配置信息对所述解密敏感信息进行加密，得到加密信息；根据所述加密信息生成第二信标帧，所述第二信标帧包括用于存放所述加密信息的敏感信息字段；发送所述第二信标帧。

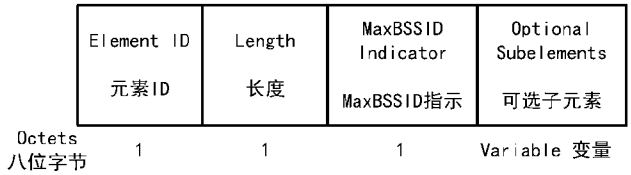
24. 一种网络设备，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如权利要求 1 至 23 任意一项所述的信息处理方法。

25. 一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令用于执行如权利要求 1 至 23 任意一项所述的信息处理方法。



BSSID Information field format
BSSID信息字段格式

图 1



Multiple BSSID element format
多个BSSID元素格式

图 2

	Element ID 元素ID	Length 长度	Version 版本	Group Data Cipher Suite 组播数据帧秘钥套件	Pairwise Cipher Suite Count 单播秘钥套件	Pairwise Cipher Suite List 单播秘钥套件列表
Octets 八位字节	1	1	2	0或4	0或2	0或（4×m）

	AKM Suite Count AKM套计数量	AKM Suite List AKM套件列表	RSN Capabilities RSN能力集	PMKID Count PMKID数量	PMKID List PMKID列表	Group Management Cipher Suite 组播管理帧秘钥套件
Octets 八位字节	0或2	0或（4×n）	0或2	0或2	0或（16×s）	0或4

RSNE format
RSNE格式

图 3

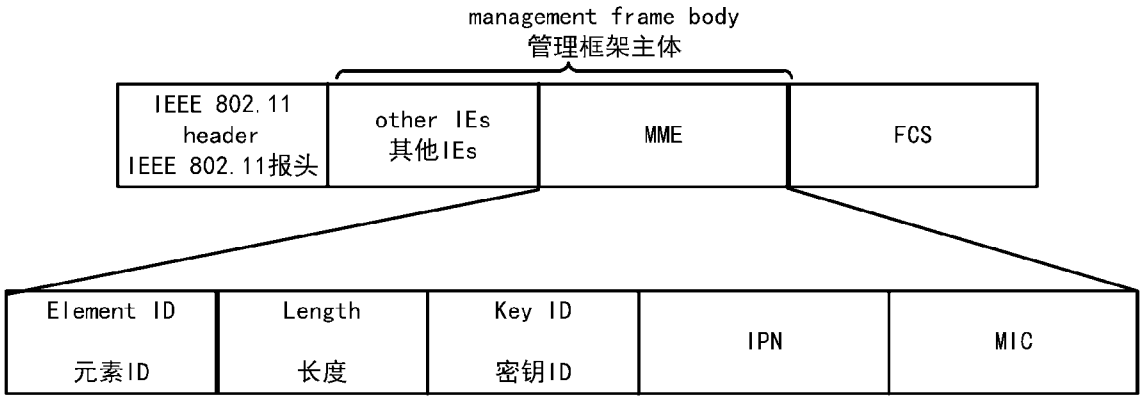


图 4

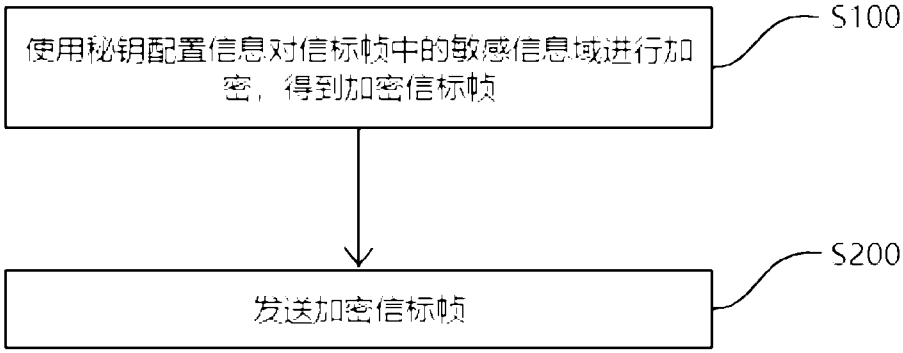

使用秘钥配置信息对信标帧中的敏感信息域进行加密，得到加密信标帧
S100
发送加密信标帧
S200

图 5

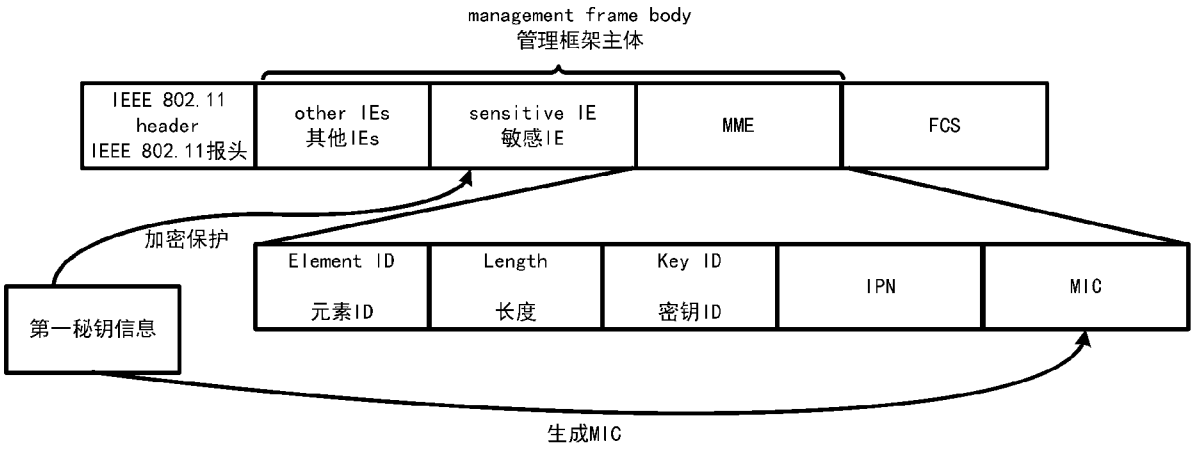

management frame body
管理框架主体
IEEE 802.11 header
IEEE 802.11报头
other IEs
其他IEs
sensitive IE
敏感IE
MME
FCS
加密保护
第一秘钥信息
Element ID
元素ID
Length
长度
Key ID
密钥ID
IPN
MIC
生成MIC

图 6

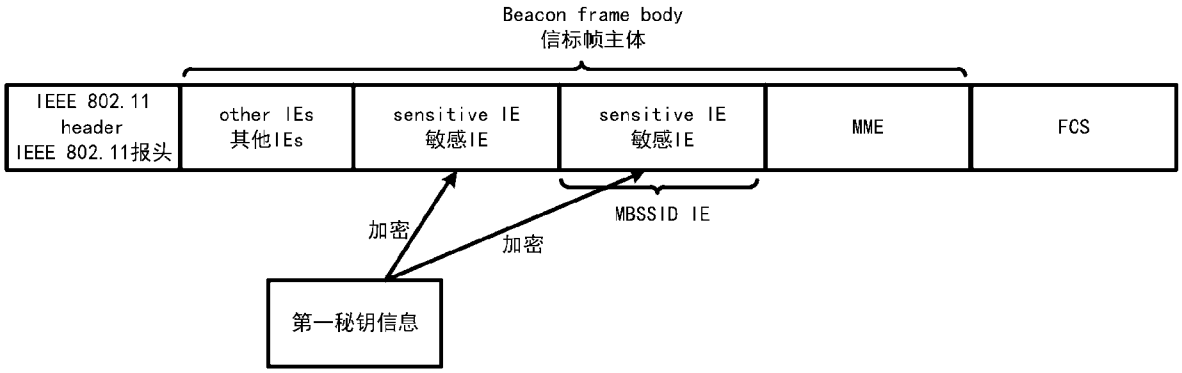

Beacon frame body
信标帧主体
IEEE 802.11 header
IEEE 802.11报头
other IEs
其他IEs
sensitive IE
敏感IE
sensitive IE
敏感IE
MME
FCS
MBSSID IE
加密
加密
第一秘钥信息

图 7

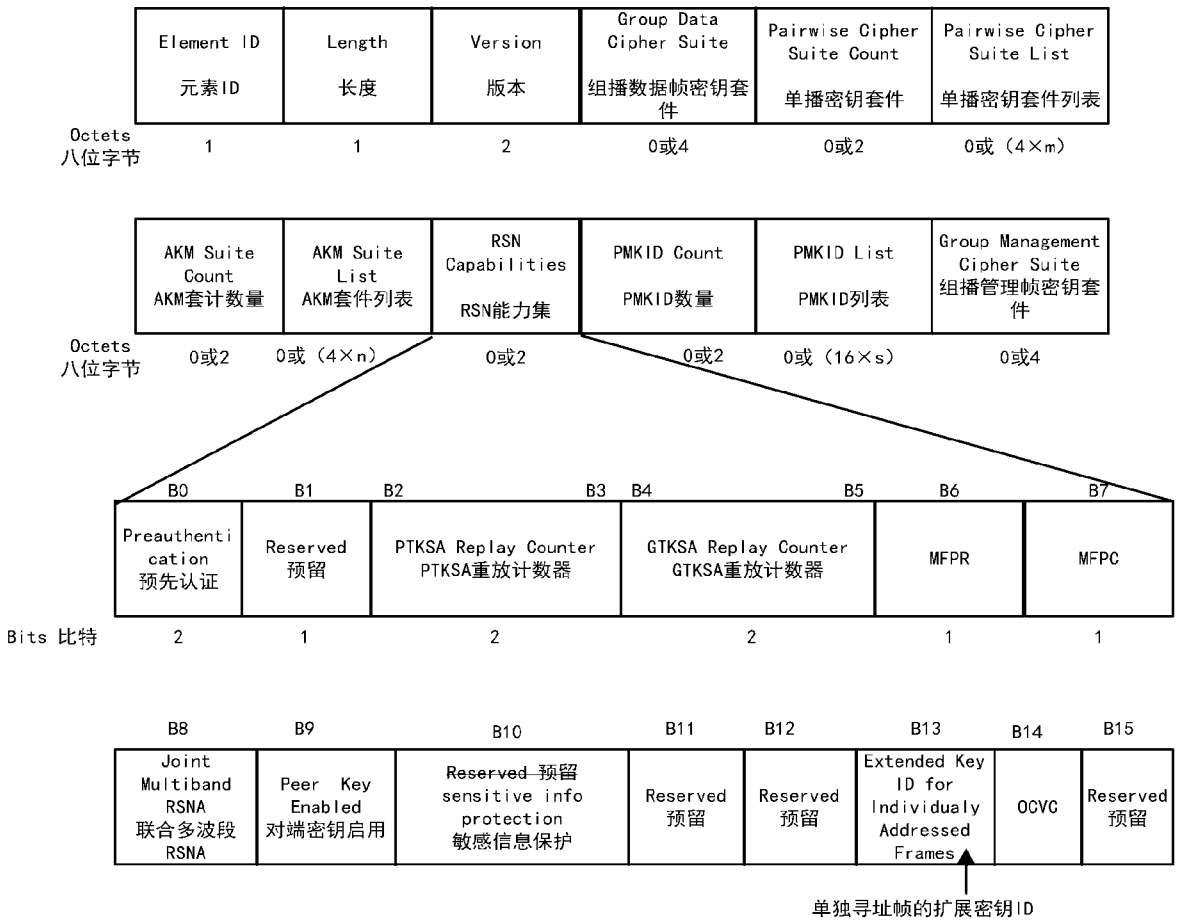

Element ID
元素ID
Length
长度
Version
版本
Group Data Cipher Suite
组播数据帧密钥套件
Pairwise Cipher Suite Count
单播密钥套件
Pairwise Cipher Suite List
单播密钥套件列表
Octets
八位字节
1
1
2
0或4
0或2
0或（4×m）
AKM Suite Count
AKM套计数量
AKM Suite List
AKM套件列表
RSN Capabilities
RSN能力集
PMKID Count
PMKID数量
PMKID List
PMKID列表
Group Management Cipher Suite
组播管理帧密钥套件
Octets
八位字节
0或2
0或（4×n）
0或2
0或2
0或（16×s）
0或4
B0
B1
B2
B3
B4
B5
B6
B7
Preauthentication
预先认证
Reserved
预留
PTKSA Replay Counter
PTKSA重放计数器
GTKSA Replay Counter
GTKSA重放计数器
MFPR
MFPC
Bits 比特
2
1
2
2
1
1
B8
B9
B10
B11
B12
B13
B14
B15
Joint Multiband RSNA
联合多波段RSNA
Peer Key Enabled
对端密钥启用
Reserved 预留
sensitive info protection
敏感信息保护
Reserved
预留
Reserved
预留
Extended Key ID for Individualy Addressed Frames
OCVC
Reserved
预留
单独寻址帧的扩展密钥ID

图 8

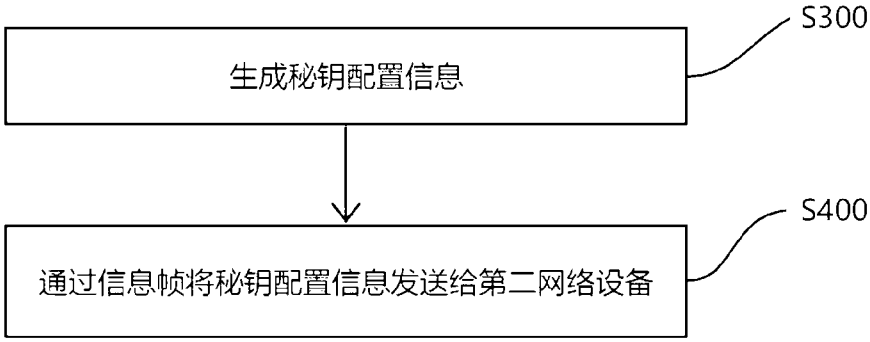

S300
生成秘钥配置信息
S400
通过信息帧将秘钥配置信息发送给第二网络设备

图 9

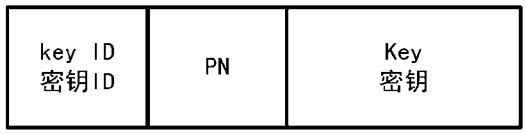

key ID
密钥ID
PN
Key
密钥

图 10

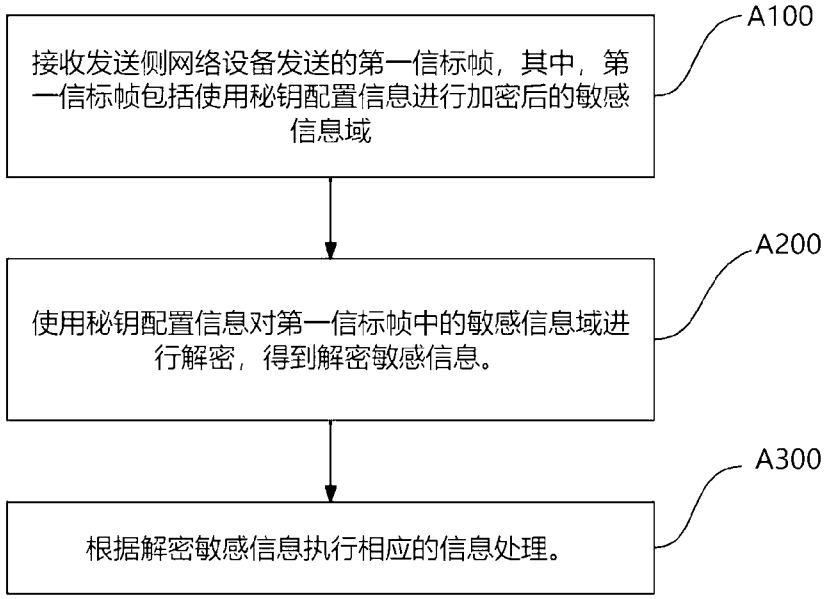

A100
接收发送侧网络设备发送的第一信标帧，其中，第一信标帧包括使用秘钥配置信息进行加密后的敏感信息域
A200
使用秘钥配置信息对第一信标帧中的敏感信息域进行解密，得到解密敏感信息。
A300
根据解密敏感信息执行相应的信息处理。

图 11

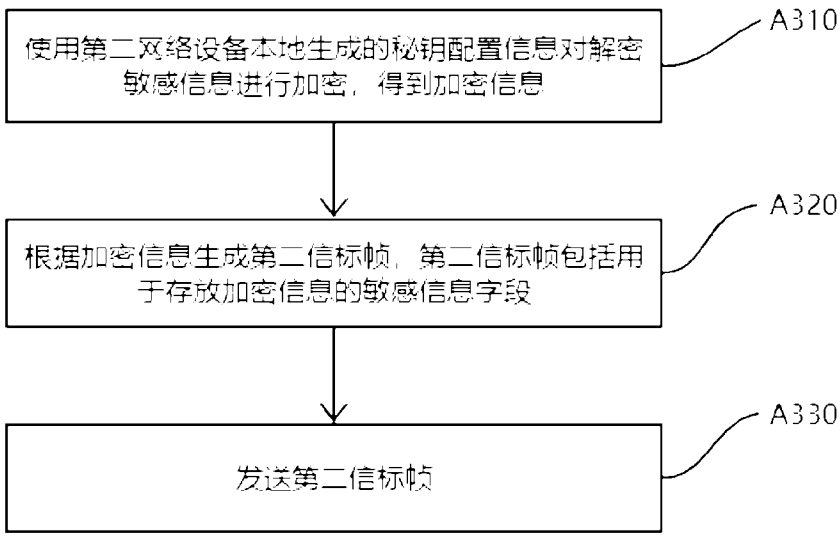

A310
使用第二网络设备本地生成的秘钥配置信息对解密敏感信息进行加密，得到加密信息
A320
根据加密信息生成第二信标帧，第二信标帧包括用于存放加密信息的敏感信息字段
A330
发送第二信标帧

图 12

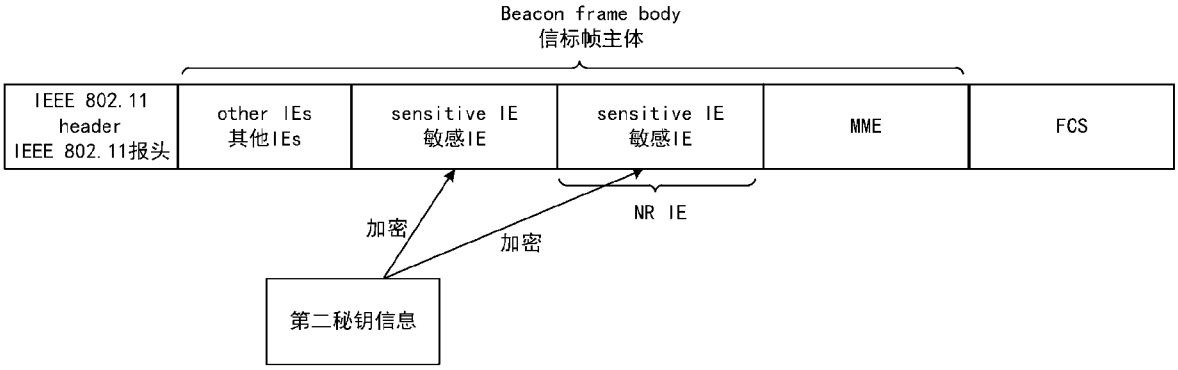

Beacon frame body
信标帧主体
IEEE 802.11 header
IEEE 802.11报头
other IEs
其他IEs
sensitive IE
敏感IE
sensitive IE
敏感IE
MME
FCS
NR IE
加密
加密
第二秘钥信息

图 13

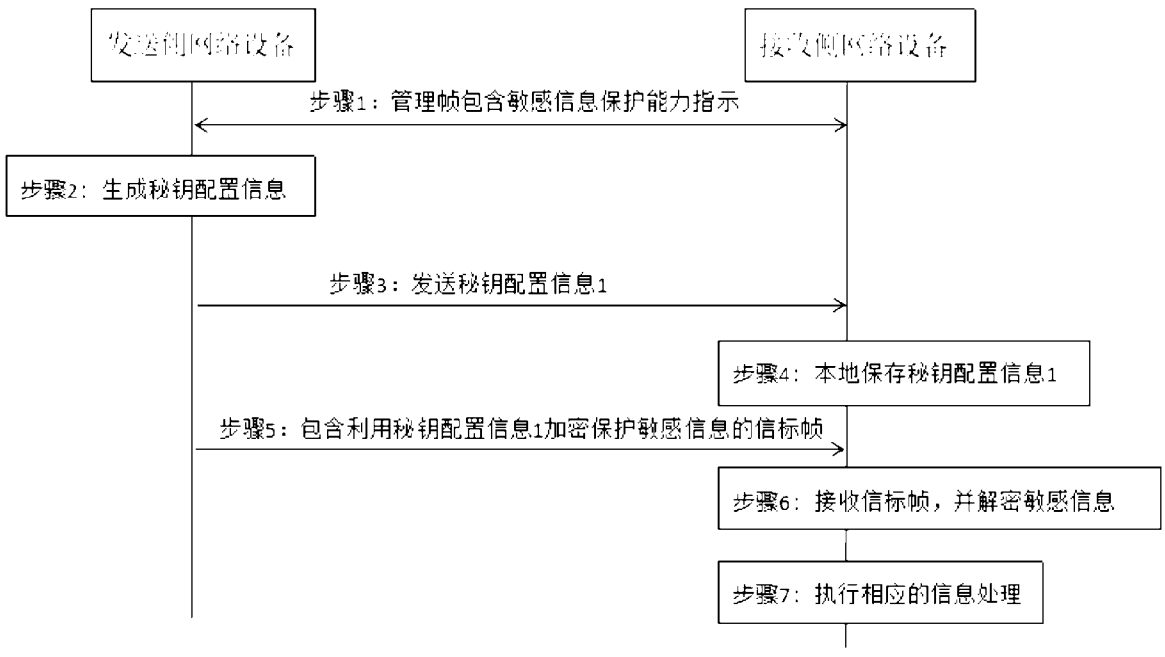

发送侧网络设备
接收侧网络设备
步骤1：管理帧包含敏感信息保护能力指示
步骤2：生成秘钥配置信息
步骤3：发送秘钥配置信息1
步骤4：本地保存秘钥配置信息1
步骤5：包含利用秘钥配置信息1加密保护敏感信息的信标帧
步骤6：接收信标帧，并解密敏感信息
步骤7：执行相应的信息处理

图 14

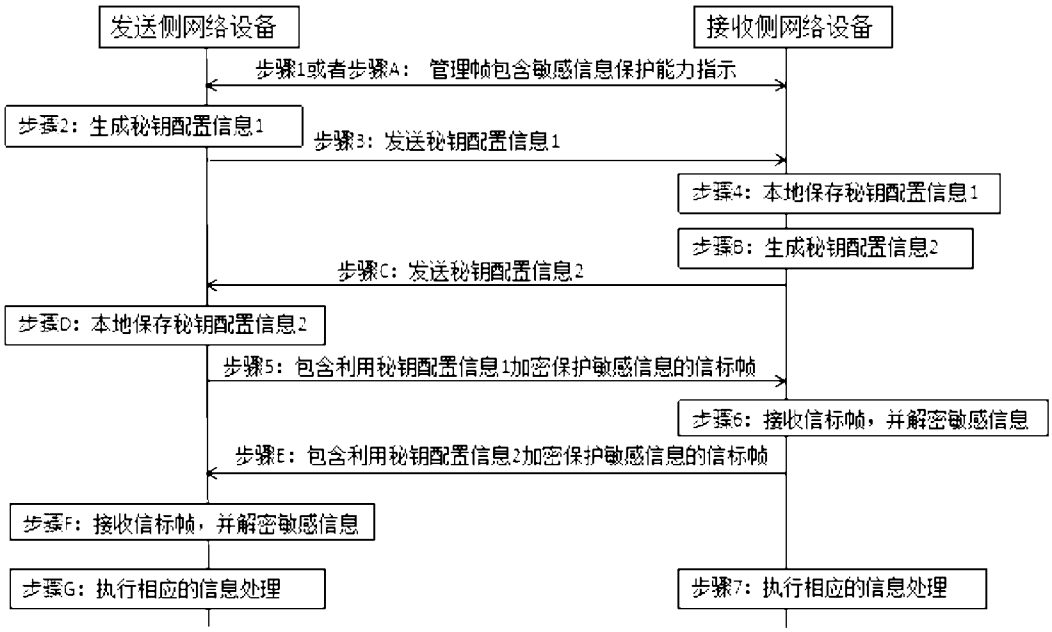

发送侧网络设备
接收侧网络设备
步骤1或者步骤A： 管理帧包含敏感信息保护能力指示
步骤2：生成秘钥配置信息1
步骤3：发送秘钥配置信息1
步骤4：本地保存秘钥配置信息1
步骤B：生成秘钥配置信息2
步骤C：发送秘钥配置信息2
步骤D：本地保存秘钥配置信息2
步骤5：包含利用秘钥配置信息1加密保护敏感信息的信标帧
步骤6：接收信标帧，并解密敏感信息
步骤E：包含利用秘钥配置信息2加密保护敏感信息的信标帧
步骤F：接收信标帧，并解密敏感信息
步骤G：执行相应的信息处理
步骤7：执行相应的信息处理

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/098824

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/40(2022.01)i; H04W12/03(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)

IPC:H04L9/-; H04W12/-

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, 万方, WANFANG, VEN, EPTXT, WOTXT, USTXT, 3GPP, IEEE: 信标帧, 管理帧, beacon帧, 敏感, TWT, 时间, 周期, 目标唤醒时间, 密钥, 秘钥, 加密, 解密, 发送侧, AP, 接入点, 多链路接入点, AP MLD, 无线路由器, 接收侧, 客户端, STA, 站, beacon frame?, management+ frame?, sensit+, Target Wake Up Time, Target Wake-Up Time, Target WakeUp Time, secret key?, cipher?, encrypt+, decrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 113613245 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 05 November 2021 (2021-11-05) description, paragraphs 34-47, 67-78, and 94-95	1-25
A	CN 101986726 A (CHINA IWNCOMM CO., LTD.) 16 March 2011 (2011-03-16) entire document	1-25
A	CN 113747430 A (CHENGDU BRANCH OF NEW H3C TECHNOLOGIES CO., LTD.) 03 December 2021 (2021-12-03) entire document	1-25
A	US 2023171594 A1 (BEIJING XIAOMI MOBILE SOFTWARE CO., LTD.) 01 June 2023 (2023-06-01) entire document	1-25

☐ 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
"D" document cited by the applicant in the international application
"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
16 August 2024	**18 August 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/098824

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 113613245 A	05 November 2021	None	
CN 101986726 A	16 March 2011	WO 2012055204 A1	03 May 2012
		CN 101986726 B	07 November 2012
CN 113747430 A	03 December 2021	CN 113747430 B	07 November 2023
US 2023171594 A1	01 June 2023	WO 2021208025 A1	21 October 2021

国际检索报告

国际申请号
PCT/CN2024/098824

A. 主题的分类

H04L9/40(2022.01)i；H04W12/03(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)

IPC:H04L9/−; H04W12/−

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,万方,VEN,EPTXT,WOTXT,USTXT,3GPP,IEEE:信标帧,管理帧,beacon帧,敏感,TWT,时间,周期,目标唤醒时间,密钥,秘钥,加密,解密,发送侧,AP,接入点,多链路接入点,AP MLD,无线路由器,接收侧,客户端,STA,站, beacon frame?,management+ frame?, sensit+,Target Wake Up Time，Target Wake−Up Time，Target WakeUp Time, secret key?,cipher?,encrypt+,decrypt+

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 113613245 A (支付宝（杭州）信息技术有限公司) 2021年11月5日 (2021 - 11 - 05) 说明书34−47、67−78、94−95段	1−25
A	CN 101986726 A (西安西电捷通无线网络通信股份有限公司) 2011年3月16日 (2011 - 03 - 16) 全文	1−25
A	CN 113747430 A (新华三技术有限公司成都分公司) 2021年12月3日 (2021 - 12 - 03) 全文	1−25
A	US 2023171594 A1 (BEIJING XIAOMI MOBILE SOFTWARE CO., LTD.) 2023年6月1日 (2023 - 06 - 01) 全文	1−25

☐ 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

“D” 申请人在国际申请中引证的文件

“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
2024年8月16日	2024年8月18日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 李桂红 电话号码 (+86) 028−62969220

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/098824

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	113613245	A	2021年11月5日	无			
CN	101986726	A	2011年3月16日	WO	2012055204	A1	2012年5月3日
				CN	101986726	B	2012年11月7日
CN	113747430	A	2021年12月3日	CN	113747430	B	2023年11月7日
US	2023171594	A1	2023年6月1日	WO	2021208025	A1	2021年10月21日