(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102098670 B
(45)授权公告日 2014.08.06

(21)申请号 201110041416.4
(22)申请日 2005.11.21
(30)优先权数据
60/630,730 2004.11.23 US
60/661,856 2005.03.15 US
60/684,257 2005.05.25 US
11/283,017 2005.11.18 US
(62)分案原申请数据
200580039662.9 2005.11.21
(73)专利权人 美商内数位科技公司
地址 美国特拉华州
(72)发明人 亚历山大·瑞茨尼克
亚伦·G·卡尔顿
亚兰·C·L·布莱恩肯
尤根德拉·C·夏
伯拉哈卡·R·季塔布
(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 南毅宁 刘国平
(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/12(2009.01)
(56)对比文件
CN 1076816 A,1993.09.29,
WO 03094520 A1,2003.11.13,
审查员 张巍

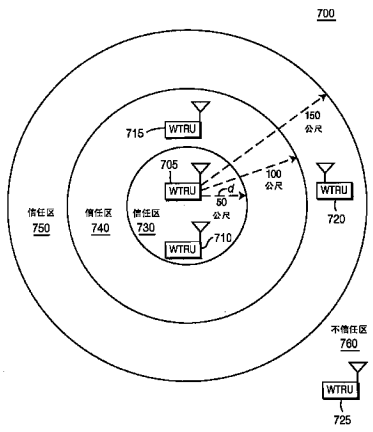
权利要求书1页 说明书8页 附图9页

(54)发明名称

确保无线通信的方法及系统

(57)摘要

本发明揭示一种用来确保无线通信的方法及系统。在一实施例中,以一接收器与一发射器间的距离为基础采取不同保密措施,借此使无线通信中的数据只有在特定信任区内被接收到方可被解调制。在另一实施例中,多个位串流片段通过多个发射器传输到一位于这些发射器发出的传输型样相交的一区域内的接收器。另一选择,接收器在发射器发出的封包数据单元(PDUs)上执行一函数。在另一实施例中,将一调制星座的主要调制点划分成邻近次要调制点的丛集,其仅可由一在发射器的范围内的接收器解调制。在另一实施例中,传输一主波形,其用具有已编码解扰密信息的分级调制(HM)叠加于一QPSK讯号。



CN 102098670 B

1. 一种用于确保无线通信的方法，该方法包括：

对数据进行扰密；

使用一分级调制来对已扰密数据和解扰密信息进行调制，其中分级调制星座包括主要调制点和至少一层次要调制点，且所述主要调制点被划分成邻近次要调制点的丛集，以及所述已扰密数据通过所述主要调制点而被调制，而所述解扰密信息通过所述次要调制点而被调制；

通过发射器传输已扰密数据和所述解扰密信息到一无线传输 / 接收单元，以致所述已扰密数据的解扰取决于与该无线传输 / 接收单元相关的一信任区，其中所述信任区通过与所述发射器间的距离而被限定。

2. 根据权利要求 1 所述的方法，其特征在于该信任区是多个地理信任区的其中之一。

3. 根据权利要求 1 所述的方法，其特征在于在包括所述无线传输 / 接收单元的信任区是一第一地理信任区的条件下允许所述已扰密数据的解调。

4. 根据权利要求 3 所述的方法，该方法还包括认证该无线传输 / 接收单元的位置。

5. 根据权利要求 4 所述的方法，其特征在于该第一地理信任区包括一第二地理信任区和一第三地理信任区，且所述认证该无线传输 / 接收单元的位置包括：

在该无线传输 / 接收单元与该第二地理信任区相关的条件下使用一第一认证方法而认证该无线传输 / 接收单元的位置；以及

在该无线传输 / 接收单元与该第三地理信任区相关的条件下使用一第二认证方法而认证该无线传输 / 接收单元的位置。

6. 根据权利要求 1 所述的方法，该方法还包括：通过调整一编码率架构、一击穿架构和 / 或一功率架构来调整所述信任区的大小。

确保无线通信的方法及系统

[0001] 本发明专利申请是国际申请号为PCT/US2005/041976，国际申请日为2005年11月21日，进入中国国家阶段的申请号为200580039662.9，发明名称为“确保无线通信的方法及系统”的发明专利申请的分案申请。

[0002] 技术领域

[0003] 本发明整体而言关于无线通信。更明确地说，本发明关于一种通过策略性定位这些通信的来源及/或受者以确保此等无线通信的方法及装置。

[0004] 背景技术

[0005] 随着无线连线活动日益普及并可靠，意料中当今受到广泛使用的所有数位运算、数据存储及媒体存储装置会变成Ad-hoc无线通信网络的一部分。但此等网络易于在许多方面有数据安全性漏洞。举例来说，个别用户直接相互通讯而不使用中间网络节点的Ad-hoc网络对于用户及网络创造出新的易受攻击特性。

[0006] 为降低无线网络的易受攻击性，顷已开发出诸如连线等效私密(WEP)、Wi-Fi保护存取(WPA)、可扩展认证协议(EAP)及GSM型加密等技术。虽然这些技术提供一些保护作用，其对于多种信任、权利、身份、私密及安全性问题依然脆弱。举例来说，虽然一特定无线通信节点可能具有与一无线用户通讯的正确WEP金钥，但该用户可能不知道该特定节点是否可信。

[0007] 此外，使用此等金钥的用户的认证通常发生在通信堆叠的较高层。据此，即使是在这些控制就定位的时，一恶质无线用户或骇客可能对该通信堆叠有一些(有限的)存取。此存取创造出弱点，譬如阻断服务攻击及其他。

[0008] 无线讯号随距离退化的事实引发一种自然的保密措施，因为要拦截一讯号需要够接近来源方能侦测到该讯号。这对小型网络来说特别显著，其传输功率通常为低而且通信通常以最高速率且以一Ad-hoc方式进行。在许多情况中，物理邻近距离对于一恶意攻击者来说可能是最难达成的属性。事实上，仅可在发射器的一极短邻近距离内被侦测到的通信不怎么需要非常完善的保护。

[0009] 因此，会期望施行一种能够利用无线讯号退化所提供的自然保密效果的优点的无线网络保密系统。此外，会期望确保要传输给一用户的任何信息仅可在该用户所在位置存取，致使一位于该用户附近但不是在该用户当前所在位置处的″窃听者″无法接收到传输给该用户的完整讯息。

发明内容

[0010] 本发明关于一种用来确保无线通信的方法及装置。在一实施例中，以一接收器与一发射器间的距离为基础采取不同保密措施，借此使无线通信中的数据只有在特定信任区内被收到方可被解调制。在另一实施例中，多个位串流片段通过多个发射器传输到一位于这些发射器发出的传输型样相交的一区域内的接收器。另一选择，接收器在发射器发出的封包数据单元(PDUs)上执行一函数。在另一实施例中，将一调制星座的主要调制点划分成邻近次要调制点的丛集，其仅可由一在发射器的范围内的接收器解调制。在另一实施例中，

传输一主波形，其用具有已编码解扰密信息的分级调制 (HM) 叠加于一 QPSK 讯号。

附图说明

[0011] 以下以举例方式并参照附图更详细地说明本发明，其中：

[0012] 图 1 是一示出一接收器解码器的有效输入 SNR 与该解码器的输出 BER 间的一关系的曲线图表现；

[0013] 图 2 是一无线通信系统的方块图，其包含依据本发明用来确保无线通信的一发射器及一接收器；

[0014] 图 3 是一示出规格化安全近接半径 (NSPR) 与已知符号在 R = 1、γ = 2 条件下的关系的曲线图表现；

[0015] 图 4 是一示出 NSPR 与已知符号在 R = 1、γ = 4 条件下的关系的曲线图表现；

[0016] 图 5 是一示出 NSPR 与已知符号在 R = 1/2、γ = 2 条件下的关系的曲线图表现；

[0017] 图 6 是一示出 NSPR 与已知符号在 R = 1/2、γ = 4 条件下的关系的曲线图表现；

[0018] 图 7 是一依据本发明一实施例具备多个用来确保无线通信的信任区的保密网络的简图；

[0019] 图 8 是一传统网络，其中一窃听者可截收一从一 AP 传输到一 WTRU 的位串 流；

[0020] 图 9 是一依据本发明另一实施例的网络，其中多个 APs 的每一者传输 PDUs 给一位于这些 APs 每一者的传输型样相交的一信任区内的 WTRU 以确保无线通信；且

[0021] 图 10 示出一 QPSK 调制星座，其例示如何依据本发明另一实施例确保无线通信。

具体实施方式

[0022] 在本说明书中，术语 " 无线传输 / 接收单元 " (WTRU) 非局限性包含一用户设备 (UE)、一移动站、一固接或移动用户单元、一呼叫器、一站台 (STA) 或任何其他能够在一无线环境中运作的装置类型。在本说明书中，术语 " 存取点 " (AP) 非局限性包含一基地台、一 B 节点、一网点控制器或无线环境中的任何其他介接装置类型。

[0023] 本发明奠基于大多数传统信道码（例如 Turbo 码、低密度同位码 (LDPC)、或类似物）在大多数实务架构中是接近于香农极限 (Shannon limit) 运作的事实。在应用于无线通信系统时，（忽略衰落效应），接收器解调制数据的能力几乎是接收器解码器处的输入的有效 SNR 的一二进制函数。

[0024] 本发明的特征可被并入一集成电路 (IC) 内或被建构在一含有众多互连组件的电路中。

[0025] 图 1 是一示出有效解码器输入 SNR 与一解码器输出 BER 间的一关系的曲线图表现。存在一临界 SNR，致使在实际有效 SNR 掉到该临界 SNR 以下时，该解码器完全失效（亦即解码器输出 BER 是 1），且一无线通信内的数据无法被读取。相反地，如果解码器输入处的实际有效 SNR 高于该临界 SNR，则解码器输出处的误差可能性极低且无线通信内的数据有极高可能性被读取。

[0026] 由于其假设信道码逼近香农极限，故可假设编码作业系以香农容量速率进行。此外，最好实际上是考量频谱效率工作，因为这使数字结果与带宽无关。就一复数值相加高斯白杂讯 (AWGN) 信道来说，香农容量速率为：

[0027] $R = \log_2(1+SNR)$ 方程式 (1)

[0028] 其中 SNR 系以 E_b/N_0 取向使用。一般认定对于高于此速率的编码率来说，可 靠信息解码是不可能的，且对于低于此速率的编码率来说，本质上来说保证有可靠的信息解码。事实上，在有大区块长度码譬如 LDPC 和 Turbo 码的情况下，这是现实可行的假设。

[0029] SNR 基本上取决于发射器与接收器间的距离。SNR 对于离发射器的距离的相依性由下述一功率定律给出：

[0030] $SNR(d) = \frac{E}{d^{\gamma}}$ 方程式 (2)

[0031] 其中是一在 1 单位距离的标称 SNR。在开阔空间中，指数 γ 是 2，但在实务无线网络中，指数 γ 是介于 3 和 4 之间，视信道拓扑而定。

[0032] 今以 SNRc 为选定编码架构的临界 SNR。然后，用此临界 SNR 涵盖的距离由下式决定：

[0033] $d = \sqrt[\gamma]{\frac{E}{SNR_c}}$ 方程式 (3)

[0034] 且其可以 dBs 为单位被改写如下：

[0035] $\log d = \frac{1}{\gamma}(\log E - \log SNR_c) = \frac{1}{\gamma}(E_{dB} - SNR_{cdB})$ 方程式 (4)

[0036] 本发明使 d 为保密措施的一函数。通过动态地选择 d，一距离比 d 近的接收器可用一较松散的保密措施运作，而一距离比 d 远的接收器会需要一较严格保密措施。

[0037] 在一传统通信架构中，信道编码架构是固定的，因为要拥有用于完全不同编码架构的″可编程″编码器是相当昂贵的。因此，SNRc 是固定的。然后，从方程式 (3) 和 (4)，d 可通过控制一通信系统中的 E 和 γ 而受控。为了达到此目标，这些控制的至少一者必须依一接收器可能有或没有的外在保密相关信息而变动。

[0038] E 被定义为在一单位距离的标称 SNR。在现实中，E 是希望给一特定接收器的每信息位的传输功率。标称 SNR 定义是必要的，因为方程式 (2) 的功率定律模型对于小 d 值会崩溃且导出无限 SNRs。因此，控制 E 意味着控制每信息位的输出功率。举例来说，每信息位的输出功率的控制可由下列程序的任一者或组合完成：

[0039] 1. 通过直接控制施用于特定接收器数据的输出功率；

[0040] 2. 通过以对传送讯号添加一附加类噪讯讯号的方式减低输出 SNR 且因而减低接收器的接收 SNR。其好处在于维持恒定输出功率同时调节对于个别接收器的 SNR。

[0041] 3. 通过控制一调制架构（例如选择 QPSK/M 正交调幅 (QAM)/M 移相键控 (PSK)/ 频移键控 (FSK)，或类似架构）；

[0042] 4. 通过调整一位长度（例如用于 UWB 系统）；

[0043] 5. 通过控制传输作业的颤动和定时；

[0044] 6. 通过控制一用于送交接收器的数据的有效编码率，此为本发明中一较佳架构。此方法提供在一 WLAN 系统中以一维持一系统中各 APs 间的一致规律格点间距而不因波动传输功率位准影响 CSMA 系统效能的方式维持 APs 与 WTRU 间的恒定功率位准的能力；

[0045] 7. 通过改变速率匹配规则以便引发符号暨有效位能量的击穿或重复；

[0046] 8. 通过控制一调制指标；及

[0047] 9. 通过控制接收器将经历到的干扰量。

[0048] 干扰控制非局限性可由下述方式之一或组合完成：

[0049] 1. 通过应用可变干扰管理技术，譬如对期望接收器讯号及/或干扰接收器讯号作预等化处理并改变交叉干扰被去除或导入的程度；

[0050] 2. 通过选择功率控制（该功率控制可为一与保密措施共同最佳化的程序）；

[0051] 3. 通过时间/频率/码调度来控制潜在干扰者的数量；

[0052] 4. 通过动态干扰控制（例如接通和断开）；及

[0053] 5. 通过一第三方信标发信，而该信标随后发出讯号造成附加干扰型样。

[0054] 此外，在有多个接收天线存在的情况中，E 的值可为依据接收器相对于发射器的角位置（Θ）作出（亦即 E = E(Θ)），且因而 d 同样可被作成 Θ 的一函数。此引发另一组控制可能性，其非局限性包含下述方式：

[0055] 1. 以方位角、俯仰角或二者将波束成形为朝向或远离接收器；

[0056] 2. 利用智能天线技术进行干扰管理；及

[0057] 3. 传输型样的导入。

[0058] 有关 γ，γ 的值取决于接收讯号的多普勒效应范围 (Doppler spread)，其通常取决于接收器相对于发射器的相对速度及其环境的地理形势。但发射器可通过内部讯号处理来人为加大多普勒效应范围。由于 γ 的值取决于环境的地理形势，如果发射器配备多个天线，其可通过以一适当方式瞄准传送讯号的方式某种程度地控制 γ。

[0059] 接收器可用依据本发明的无线信道侦测一敌方主动干扰。如果接收器通过辅助构件被告知该接收器应当能够成功地解调制数据串流，但事实上在够多次尝试之后还是没办法这样做，且因为该接收器的保密措施和通信控制被以一促能数据串流解调制的方式设定，则该接收器可认定无线信道正在被侵犯。

[0060] 本发明较佳用一编码率作为一相依于接收器保密措施的参数。一般而言，接收器解调制一讯号的能力取决于地理形势（有效距离），其比一直线距离更复杂。若有需要，发射器及接收器可通过慢慢增加（或是慢慢减少）控制参数中之一或多个并侦测出可靠数据解码变得可能（或是不再可能）的点来找出二者间的有效距离。

[0061] 图 2 是一依据本发明含有一发射器 110 和一接收器 120 的通信系统 100 的方块图。发射器 110 包括一协议堆叠单元 112、一信道编码器 114、一速率匹配单元 115、一多层安全位 (MLSB) 扰密器 116 及一物理信道处理单元 118。接收器 120 包括一物理信道处理单元 128、一 MLSB 解扰密器 126、一速率解匹配单元 125、一信道解码器 124 及一协议堆叠单元 122。协议堆叠单元 112 和 122、信道编码器 114、速率匹配单元 115、速率解匹配单元 125、信道解码器 124 及物理信道处理单元 118 和 128 本质上与传统发射器及接收器所用为相同组件。协议堆叠单元 112 产生一信息串流且此信息串流被信道编码器 114 编码以防错误，然后被物理信道处理单元 118 更进一步处理以供经由一无线信道 130（亦即一特定空中界面）传输。此程序在接收器 120 颠倒。

[0062] 信道编码器 114 将一输入数据序列映射成一输出信道符号序列。MLSB 扰密器 116 扰密这些信道符号。这些信道符号可为位或较高阶调制符号。并非所有符号都必须被扰密。MLSB 扰密器 116 可取符号的一子集并予扰密。接收器应当知道有哪些符号部分被扰密。

[0063] 数个保密层依据本发明被定义。一 MLSB 解扰密器 126 能够解扰密的已扰密符号

比例取决于保密层。对于MLSB解扰密器126能够解扰密的任何符号，MLSB解扰密器126都会予以处理。对于MLSB解扰密器126无法解扰密的任何符号，MLSB解扰密器126对该符号插入一消除讯号(erasure)(亦即0的信道观测)。任何习知解码器均有能力与消除讯号运作。因此，这不会对一当今系统造成问题。

[0064] 依据本发明的保密系统在那些无法解扰密所有符号的接收器上的效用是编码效率的提高及每信息位的有效SNR的同步减低。编码率提高及有效SNR减低的特 定量取决于保密水准，此将在下文说明。

[0065] 发射器110内的速率匹配单元115依据速率匹配规则运作，该速率匹配规则可被改变以便引发符号暨有效位能量的击穿或重复。使用一具有一编码率R的信道。R得大于每信道符号1位且保密层n的有效率由下式给出：

[0066] $$R_n = \frac{R}{1-\theta(1-e_n)}$$ 方程式(5)

[0067] 其中θ代表已扰密符号的比例且en是一具备一保密层n的解扰密器(亦即接收器120内的速率解匹配单元125)能够解扰密的符号比例。在所有情况中，$e_n \in [0,1]$、$e_1 = 0$、$e_N = 1$。初始每信息位SNR(更精确地说为E_b/N_0)由E0代表。保密层n的有效SNR由下式给出：

[0068] $E_n = E_0[1-\theta(1-e_n)]$ 方程式(6)

[0069] 比率及SNR二者单纯地依未扰密已知位的比例换算，此由下式给出：

[0070] $\eta_n = 1-\theta(1-e_n)$ 方程式(7)

[0071] 因此，足以唯独就此量编定分析公式。SNR对于离发射器的距离的相依性由方程式(2)给出。

[0072] 依据本发明，经判定已知未抹除符号(亦即接收器能够解扰密的符号)的一特定比例，即可决定能够解调制数据的发射器至接收器距离。方程式(2)被代入方程式(7)中且解d以获得下式：

[0073] $$d = \sqrt[\gamma]{\frac{E}{2^R-1}}$$ 方程式(8)

[0074] 接下来，假设符号的一百分比η未被抹除，方程式(5)和(6)被代入方程式(8)中以获得下式：

[0075] $$d(\eta) = \sqrt[\gamma]{\frac{\eta E}{2^{R/\eta}-1}}$$ 方程式(9)

[0076] 一特定保密水准η可达到的距离的百分比可被表示为全保密(η = 1)可达到的距离的百分比。此为NSPR，其被定义如下：

[0077] $$\bar{d}(\eta) = \frac{d(\eta)}{d(1)} = \sqrt[\gamma]{\frac{\eta(2^R-1)}{2^{R/\eta}-1}}$$ 方程式(10)

[0078] 该NSPR不相依于E，但其相依于标称传输速率。作为一实例，图3-6呈现4种不同架构的NSPR对上已知符号百分比的标绘图，这四种架构分别是：R = 1、γ = 2；R = 1、γ = 4；R = 1/2、γ = 2；R = 1/2、γ = 4。从模拟结果观测到通过仅显露信道符 号的50％，位于比″完全安全″传输半径的约60％更远处的接收器可能无法解调制信息。因此，如果

一接收器超出其保密参数的有效距离，其理论上来说被禁止解码具备一远高于 50％的 BER 的数据。

[0079] 图 7 示出一包含多个 WTRUs 705、710、715、720 和 725 的保密网络 700，这些 WTRUs 在多个不重叠的信任区 730、740、750 或一在这些信任区外的″不信任″区 760 内运作。信任区 730、740、750 及″不信任″区 760 依下述方式建立：

[0080] 选择传输参数譬如一编码率架构、击穿架构、功率架构或类似物致使一在信任区 750 与″不信任区″ 760 间的边界外侧的接收器（亦即一 WTRU）无法解码传输讯号，就算该接收器彻底知道所有传输参数亦如此。此外，选择一（待由 MLSB 子系统实施的）位扰密架构致使在信任区 730 内侧的接收器能够解调制数据，即使这些接收器不知道已扰密位的任一者亦如此。接收功率会高到足以让成功解调制作业得以发生，即使已扰密位是单纯地用来被击穿亦如此。

[0081] 信任区 740 内的接收器除非知道 MLSB 所施用的扰密型样的一些部分否则不再有能力解调制发送的数据。据此，位于信任区 740 内的接收器会被迫要与发射器经过某种类型的认证程序使得扰密序列的一些必要部分向其揭露。

[0082] 信任区 750 内的接收器就算知道向信任区 740 内的接收器揭露的扰密序列部分（例如通过偷听侧通信借此使这些接收器被允许存取此序列）也没有能力解调制数据发射器。事实上，这些接收器被要求要请求有关扰密序列的额外信息（例如其可能必须知道完整序列），且因此其必须经过一独立于信任区 740 内的接收器（很可能是需求更高）的认证程序。如前所述，区域 760 内的接收器在任何情况下都无法解调制发送的数据。

[0083] 依据以上所述本发明的实施例，从一发射 WTRU 705 到一接收 WTRU 的距离是保密措施的一函数。通过动态选择距离 d（例如 50 公尺），一距离比 d 近的接收 WTRU 710 可用一较松散的保密措施运作，而距离超过 d 的接收 WTRU 715、720 和 725 会需要一较严保密措施。

[0084] 图 8 示出一包含一 AP 805 和一 WTRU 810 的传统网络 800。当 AP 805 传输一位串流 815 给 WTRU 810，一在 AP 805 的范围内的窃听者 820 能够接收完整位串流譬如 111000101。

[0085] 图 9 示出一依据本发明一实施例的网络 900，其包含多个存取点 (APs) 905、910、915 及一 WTRU 920 及图 8 的窃听者 820。通过使用多个 APs 905、910、915 而不像图 8 的传统网络 800 只用单个 AP 805，位串流 815 被确保不被窃听者 820 解密。WTRU 920 被定位于 APs 905、910 及 915 的传输型样的交会区 935，借此 WTRU 920 会从 AP 905 收到位串流 815 的一第一片段 930A″ 111″，从 AP 910 收到位串流 815 的一第二片段 930B″ 000″，且从 AP 915 收到位串流 815 的一第三片段 930C″ 101″。每一片段 930A、930B、930C 被称为一 PDU，且原始位串流″ 111000101″被称为一服务数据单元 (SDU)。然后 WTRU 920 从这三个 PDUs930A、930B、930C 重组整个已加密 SDU。由于窃听者 820 并未实质位于 APs 905、910 及 915 的传输型样的交会区 935，致使所有片段 930A、930B、930C 相较于 WTRU 920 是在一错误率下被接收，窃听者 820 无法解译整个位串流 815（即使知道一密钥亦如此）。

[0086] 在图 9 的网络 900 内，被 WTRU 920 解译出来的 SDU 是 111000101，其中 PDUA ＝ 111、PDUB ＝ 000 且 PDUC ＝ 101。如果窃听者 820 勉强解译出这三个 PDUs 当中两个（例如 000 和 101），窃听者 820 会勉强得到不完整但正确的部分信息。

[0087] 在一替代实施例中，窃听者 820 确实接收到的任何 PDUs 只要不完整就变成无意义

的。举例来说，网络 900 内需要发送给 WTRU 920 的 SDU 是 111000101。但是，由三个不同 APs 905、910 和 915 发出的三个 PDUs（例如 PDU1、PDU2、PDU3）不像图 9 所示是片段的，而是经替代选择致使 SDU = PDU1XOR PDU2XORPDU3，其中 PDU1 = 100110011、PDU2 = 110000111 且 PDU3 = 101110001，致使 SDU = 100110011XOR 110000111XOR 101110001 = 111000101，其中 XOR 是一异或函数。因此，假设 WTRU 920 位于 APs 905、910 及 915 的传输型样的交会区 935，则 WTRU 920 能够接收全部三个 PDUs 并且 XOR 这些 PDUs 以解译 SDU111000101。如果窃听者 820 捕捉到这三个 PDUs 当中任两者，这对于解译该 SDU 来说完全无意义。XOR 以外的替代机制亦属可能，譬如以一除非成功接收所有传输否则就无意义的方式扰密封包并且从不同发射器发出不同位。

[0088] 在另一实施例中，一位置型认证机制可并入图 9 的网络 900 内。WTRU 920 从 APs 905、910 及 915 接收传输，且向 APs 905、910 及 915 每一者报告其位置。基于 WTRU 920 及 APs 905、910 和 915 的报告位置，APs 905、910 及 915 每一者可启动一协议以一高于或低于每一相应 AP 905、910 及 915 与 WTRU 920 间的标 称距离的建议编码率高或低的变动有效编码率发出一讯息序列，请求来自 WTRU920 的一肯定确认接收讯号 (ACK) 或一否定确认接收讯号 (NACK)。因此，该协议建立一准则，其以 WTRU 920 的位置相对于 APs 905、910 及 915 的位置为基础指定该 WTRU 是否可解码从 APs 905、910 及 915 收到的传输。如果 WTRU 920 报告的位置被判定是正确的，则该协议会通过处理 WTRU 920 回应于该讯息序列而被收到的 ACK/NACK 讯息来查验 WTRU 920 的位置的可信度。

[0089] WTRU 920 的可信度的查验亦可被进行为致使 WTRU 920（或 WTRU 920 的用户）与 APs 905、910 及 915 共享一共同秘密。举例来说，如果 APs 905、910 及 915 要求 WTRU 920 指出的位置要经认证，则 APs 905、910 及 915 经由多个 PDUs（其可如前所述经分段或加密）发送一″挑战问题″，致使该″挑战问题″只在 WTRU 920 位于其所述位置时方能由 WTRU 920 解译。因此，WTRU 920 除非位于一可解译出该″挑战问题″的位置否则就无法″回答″该″挑战问题″。

[0090] 图 10 示出一分级调制 (HM) 架构的一实例，其由主要和次要调制架构（在本例中分别是 QPSK 和 BPSK）的一组合定义。众所周知一 QPSK 调制架构系由 4 个调制点定义，这些调制点一同建构 QPSK 调制星座。这些调制点分别呈现 π/2、3π/2、-π/2 及 -3π/2 的载波相位且分别代表二个位 00、01、10 和 11。相似地，众所周知一 BPSK 调制架构系由 2 个调制点定义，这些调制点一同建构 BPSK 调制星座。这些调制点分别呈现 +δ 和 -δ 弪度的载波相位且分别代表一个位 0 或 1。然后，该 HM 架构系由 8 个调制点定义，从主要和次要调制星座建构。

[0091] HM 调制点分别呈现 (π/2-δ)、(π/2+δ)、(3π/2-δ)、(3π/2+δ)、(-π/2-δ)、(-π/2+δ)、(-3π/2-δ)、(-3π/2+δ) 的载波相位且分别代表三个位 000、001、010、011、100、101、110 和 111。这 8 个调制点构成四个丛集，每一丛集包含二个小间隔调制点。举例来说，载波相位 (π/2-δ)、(π/2+δ) 代表的调制会构成一丛集。发射器通过一无线信道发送一从该 HM 星座取得的符号序列，该无线信道随讯号走得离发射器越远会衰减并污染该讯号。整体而言，一较接近发射器的接收器会收到一具备较好讯号强度及讯号品质的讯号，使得其能准确地侦测载波相位及所属 3 个位。但一远离发射器的接收器通常会收到一具备较低讯号强度及讯号品质的讯号，使得其就算能够判断传送符号所属丛

集为何也可能无法辨别每一丛集内的小间隔调制点。因此，此一接收器能侦测主要调制但无法侦测次要调制。据 此，接收器能侦测出数据的二个位但侦测不出第三位。

[0092] 本发明此实施例可被用来实施一保密或信任区。与主要调制点相关的数据（亦即前头 2 个位）被用一密钥编码或加密或扰密，且该密钥本身经由一符号序列的第三位传输。因此，一信任区内的接收器可侦测到该密钥且用其解码或解密或解扰密主要数据。一信任区外的接收器能侦测到主要数据但侦测不到该密钥，因而无法解码或解密或解扰密主要数据。任何调制架构皆可用作本发明的主要和次要调制架构。实例包含 M-ary PSK、M-ary FSK、M-ary QAM、或类似物。此外，只有主要调制星座内的选定调制点可被次要丛集叠加。最后，可施加超过两层的分级。举例来说，QPSK 加 BPSK 加 BPSK 呈现三层的 HM。

[0093] 在另一实施例中，可实施一分层 HM 架构。图 10 示出一种简单两层式架构，其中主波形是一被叠以一双移相键控 (BPSK)HM 的 QPSK 讯号。当一接收器的 SNR 为高，其有可能辨别所有星座点。随着 SNR 减低，要区别 BPSK 层级的点与标称 QPSK 星座点变困难且因而遗失 HM 数据。

[0094] 依据本发明，已扰密数据被以主波形调制，且解扰密信息被以 HM 编码。当接收器位于一可认出该 HM 的区域内时，解扰密信息促成成功的接收。当接收器太远且因此无法提取 HM 数据时，必须通过其他信道明确请求解扰密信息。通过改变分配给 HM 波形的功率，范围可为区域受控的。

[0095] 虽然已就特定组合以较佳实施例说明本发明的特征和元素，每一特征或元素可在没有较佳实施例其他特征和元素的条件下或是在有或没有本发明其他特征和元素的多种组合的条件下使用。

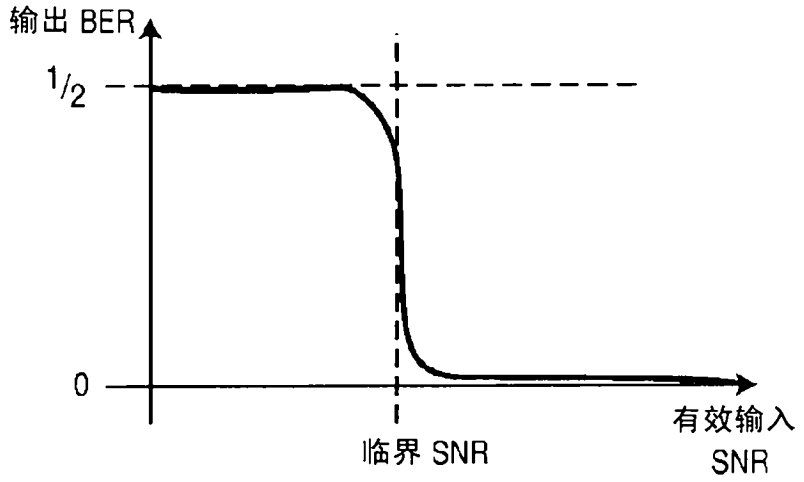

输出 BER
1/2
0
临界 SNR
有效输入
SNR

图 1

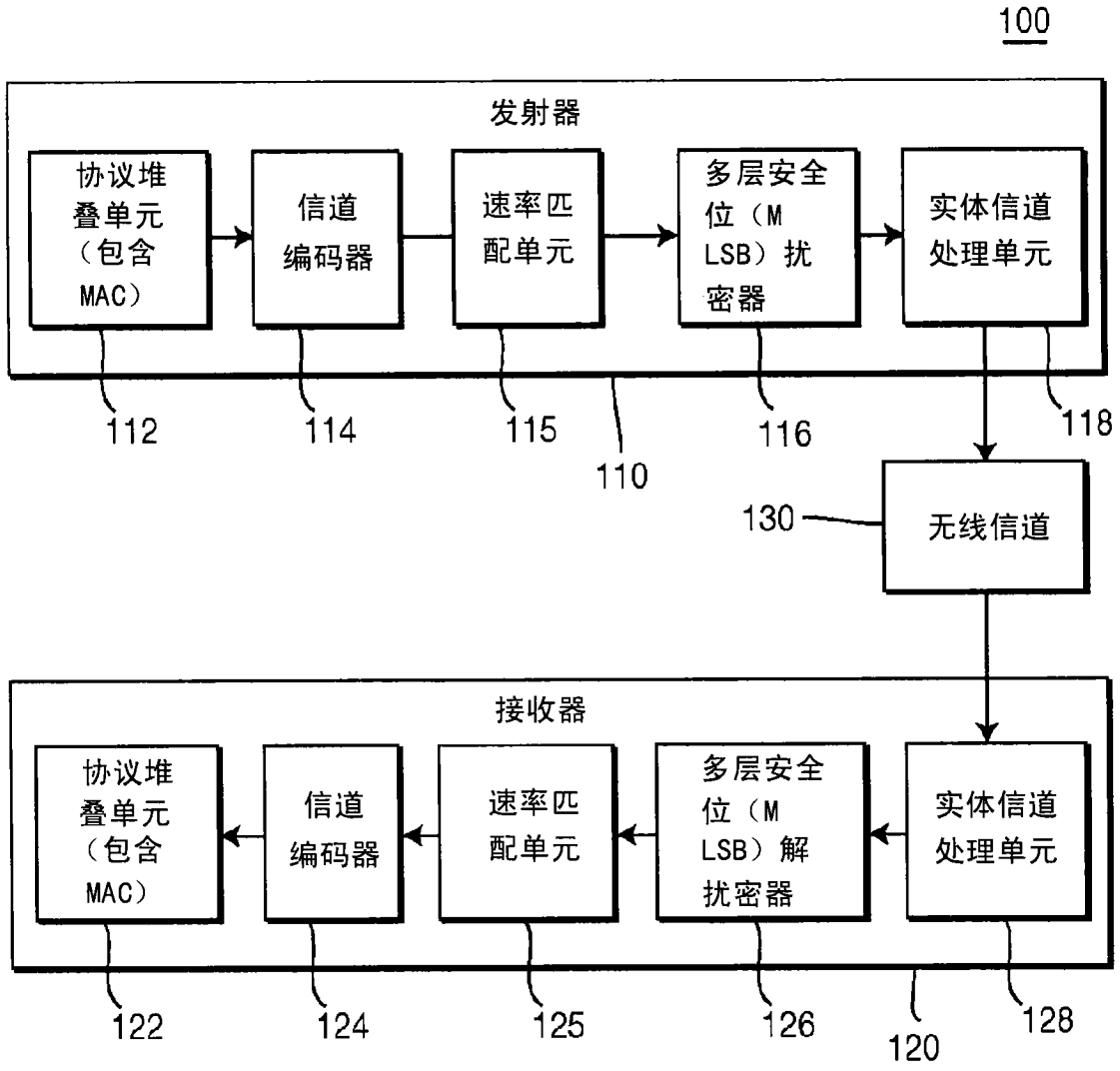

100
发射器
协议堆叠单元（包含 MAC）
信道编码器
速率匹配单元
多层安全位（M LSB）扰密器
实体信道处理单元
112
114
115
110
116
118
130
无线信道
接收器
协议堆叠单元（包含 MAC）
信道编码器
速率匹配单元
多层安全位（M LSB）解扰密器
实体信道处理单元
122
124
125
126
120
128

图 2

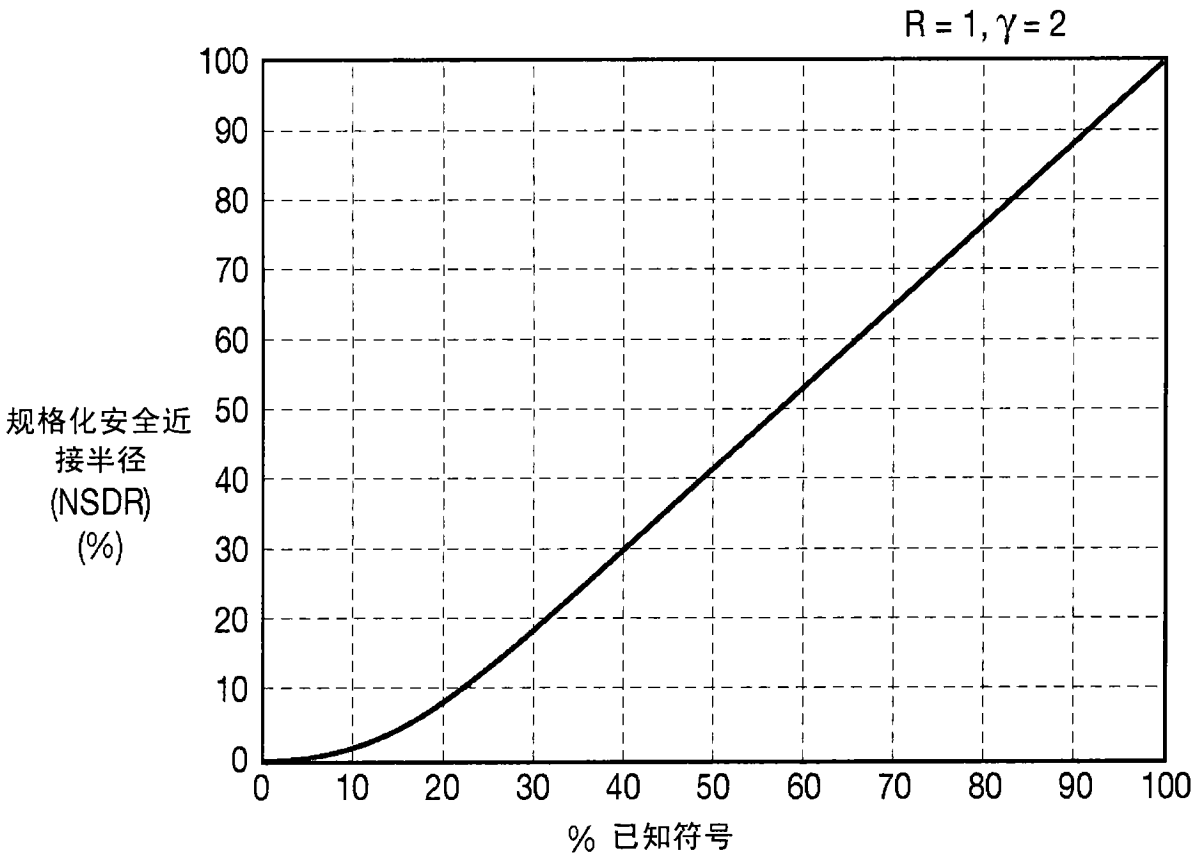

R = 1, γ = 2
规格化安全近接半径 (NSDR) (%)
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
90
100
% 已知符号

图 3

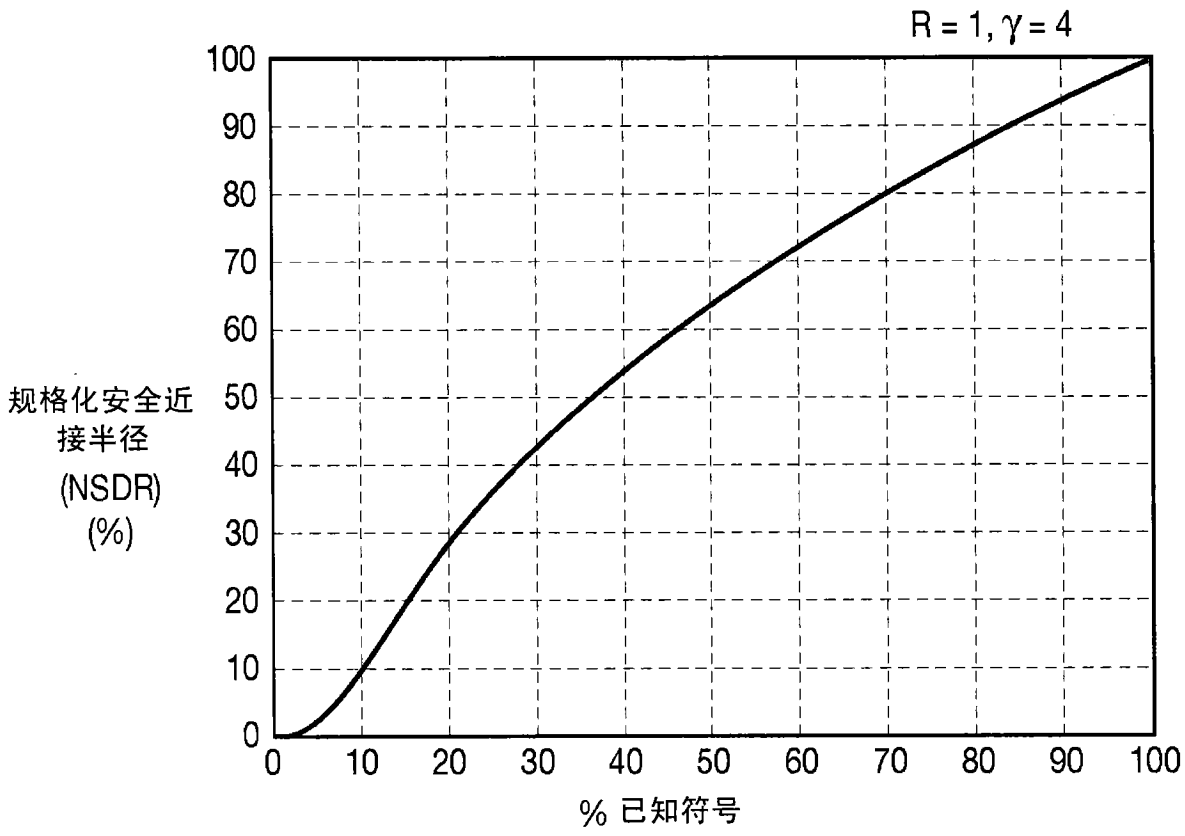

R = 1, γ = 4
规格化安全近接半径 (NSDR) (%)
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
90
100
% 已知符号

图 4

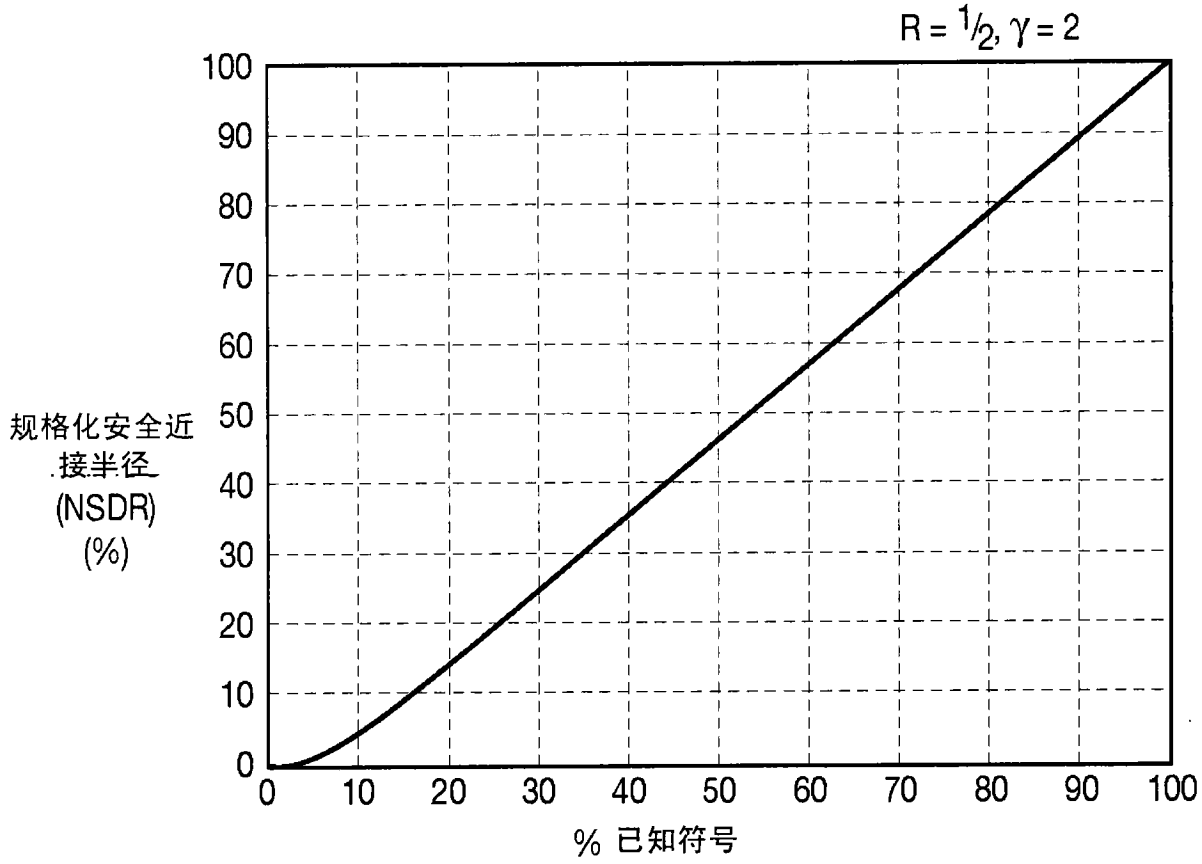

R = 1/2, γ = 2
规格化安全近接半径 (NSDR) (%)
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
90
100
% 已知符号

图 5

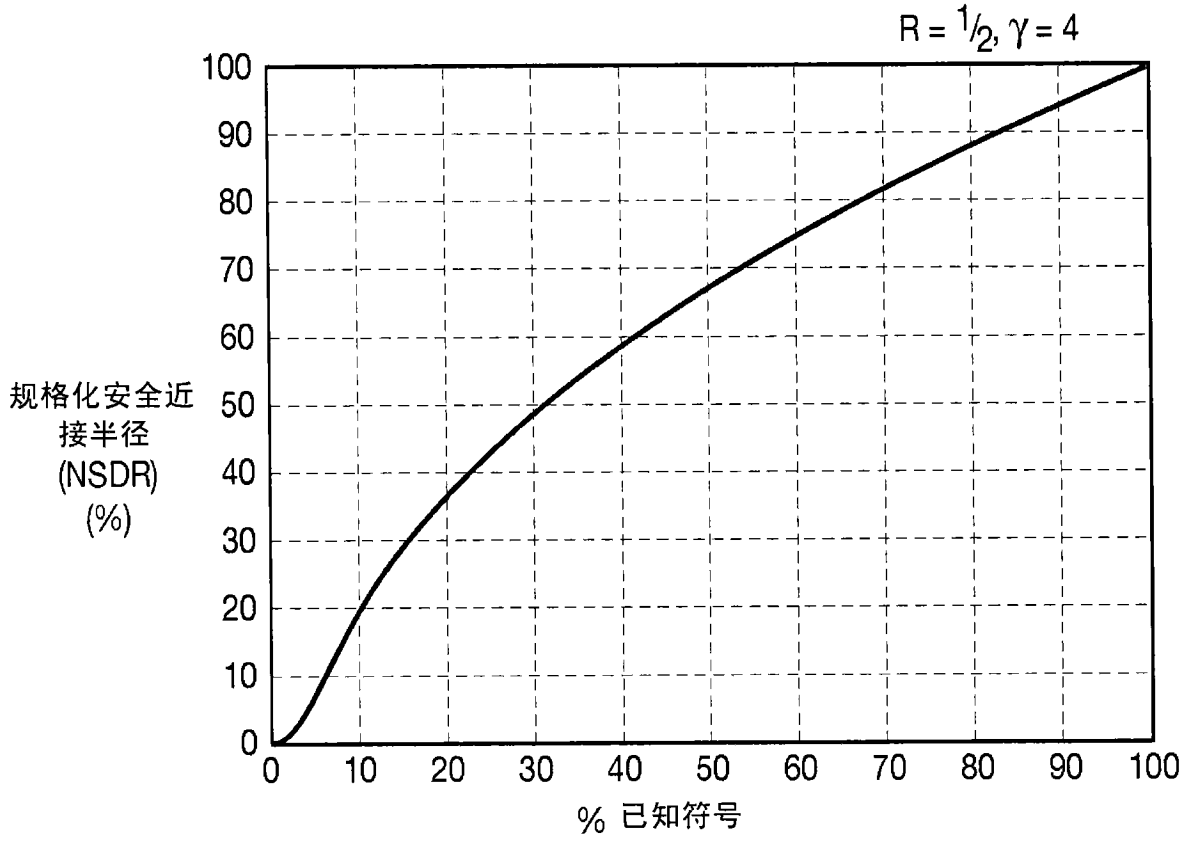

R = 1/2, γ = 4
规格化安全近接半径 (NSDR) (%)
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
90
100
% 已知符号

图 6

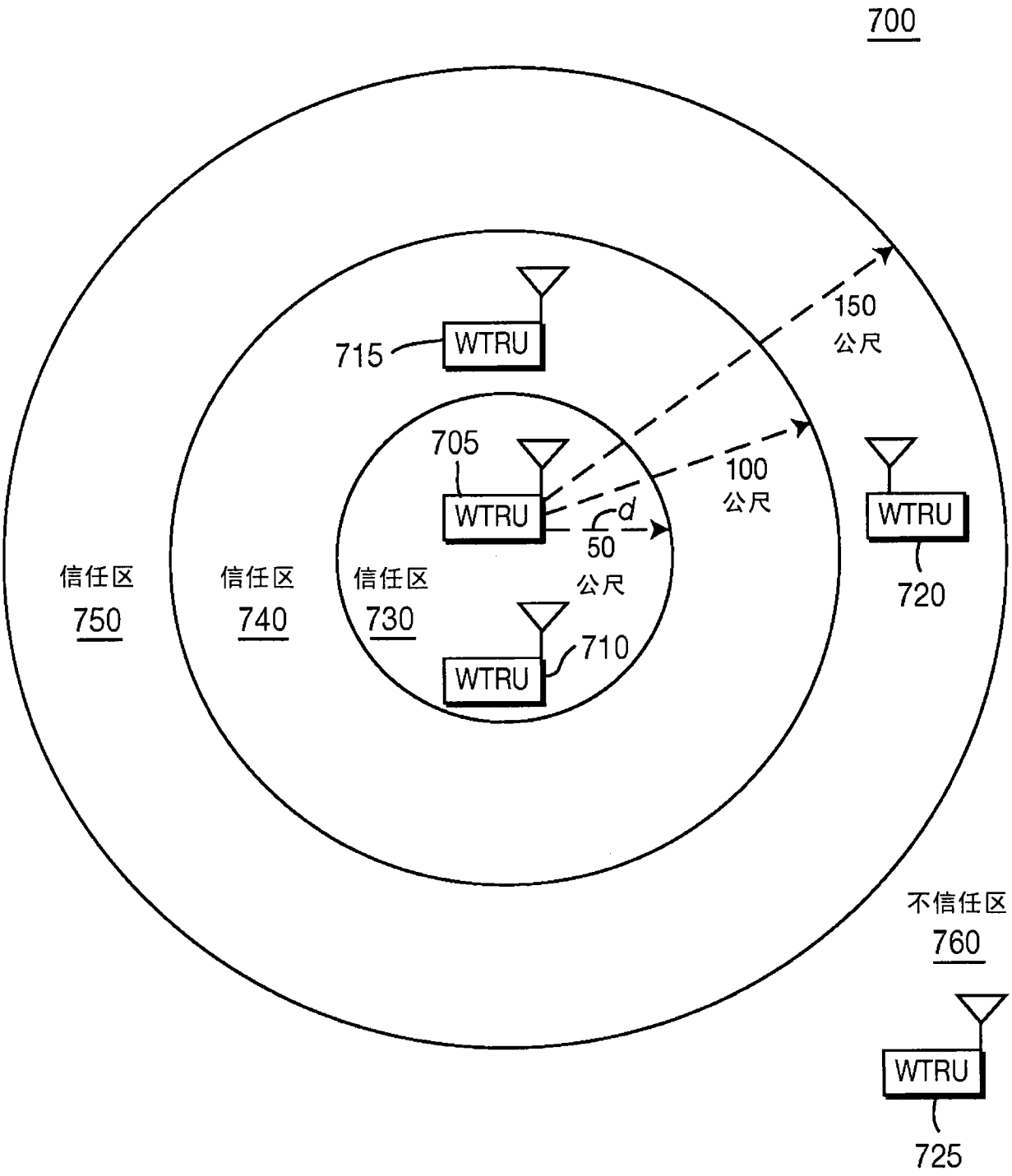

700
715
WTRU
705
WTRU
150
公尺
100
公尺
d
50
公尺
WTRU
720
信任区
750
信任区
740
信任区
730
710
WTRU
不信任区
760
WTRU
725

图 7

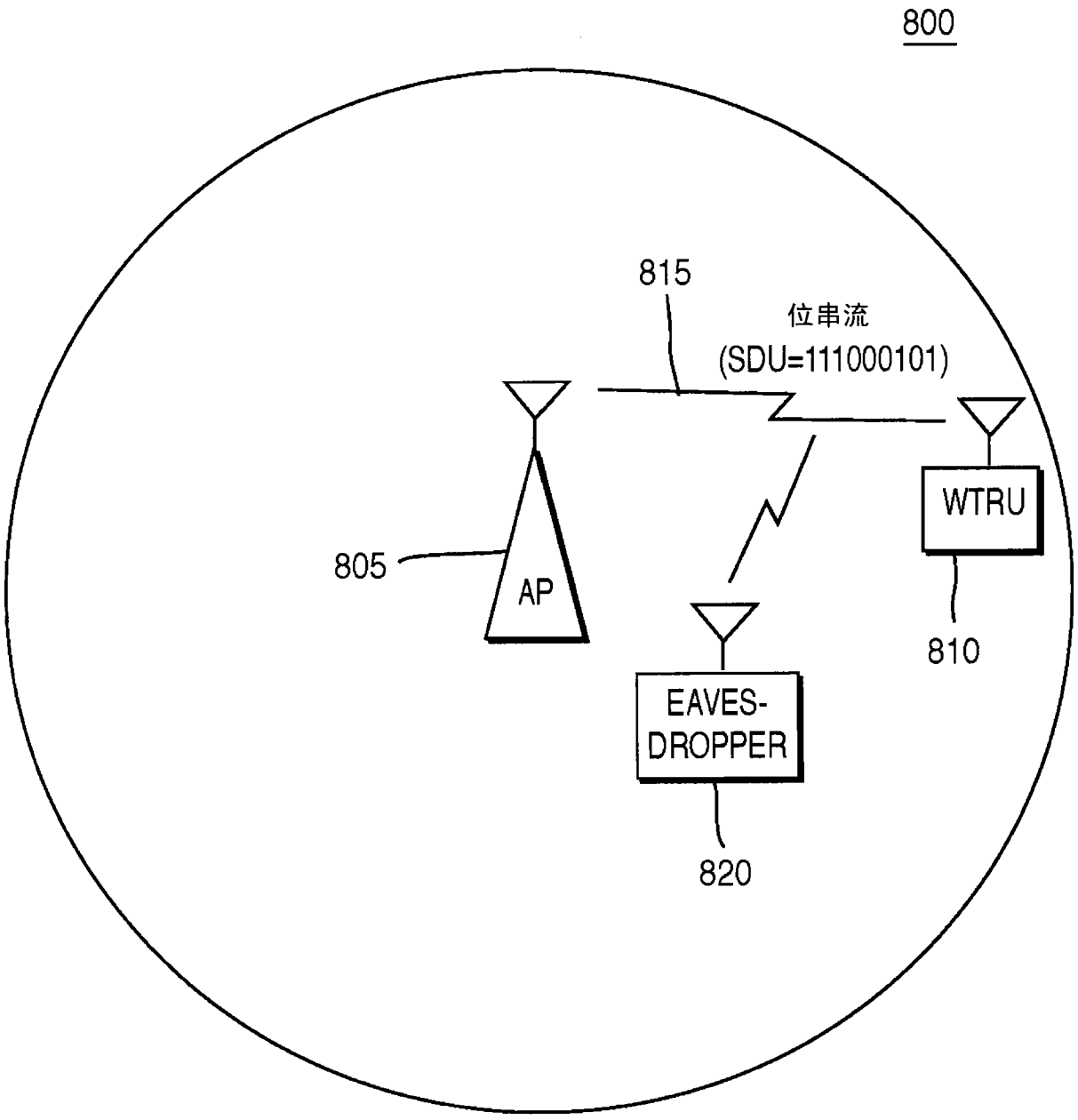


图 8
现有技术

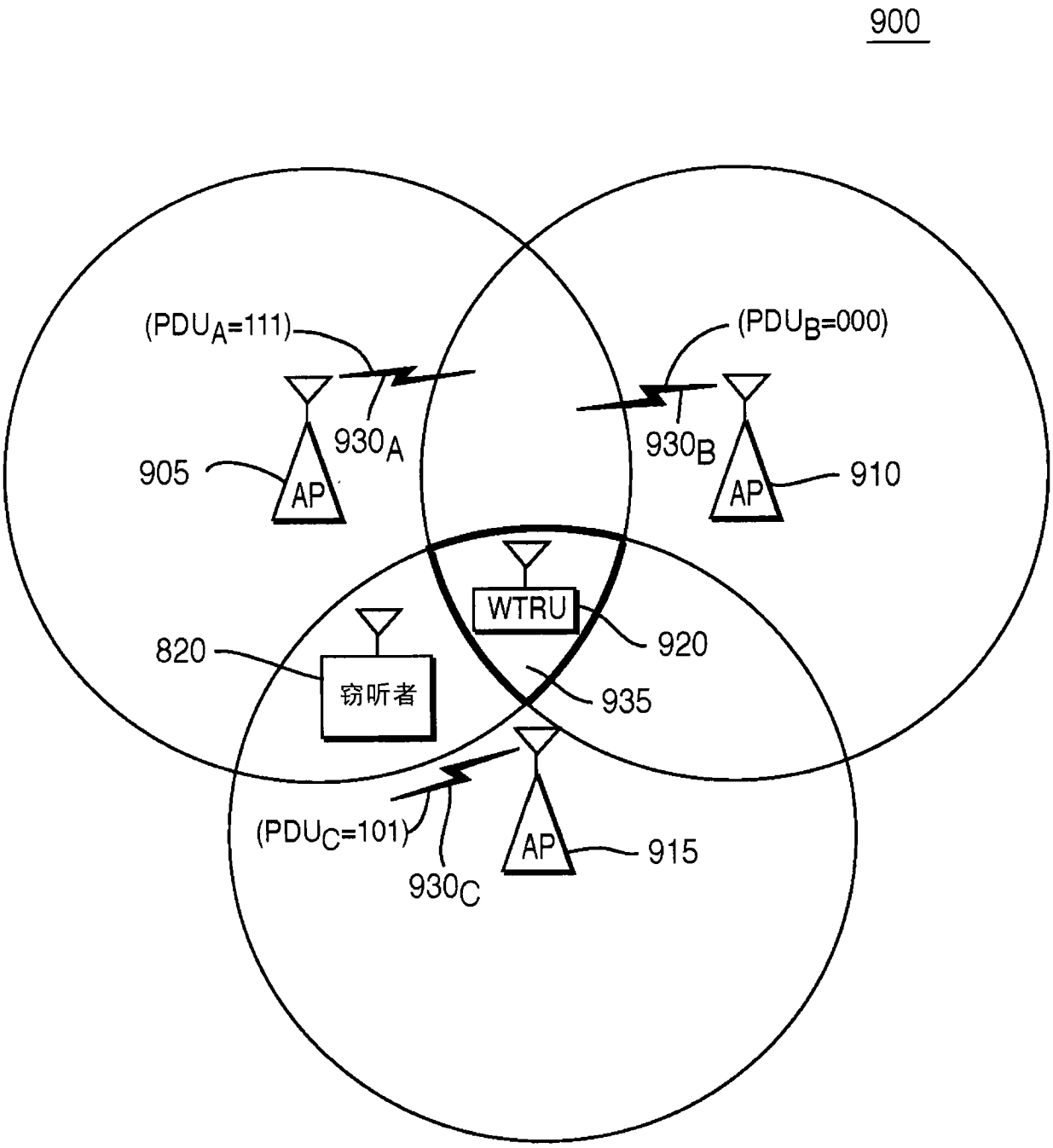

900
(PDU$_A$=111)
930$_A$
905
AP
(PDU$_B$=000)
930$_B$
AP
910
WTRU
920
820
窃听者
935
(PDU$_C$=101)
930$_C$
AP
915

图 9

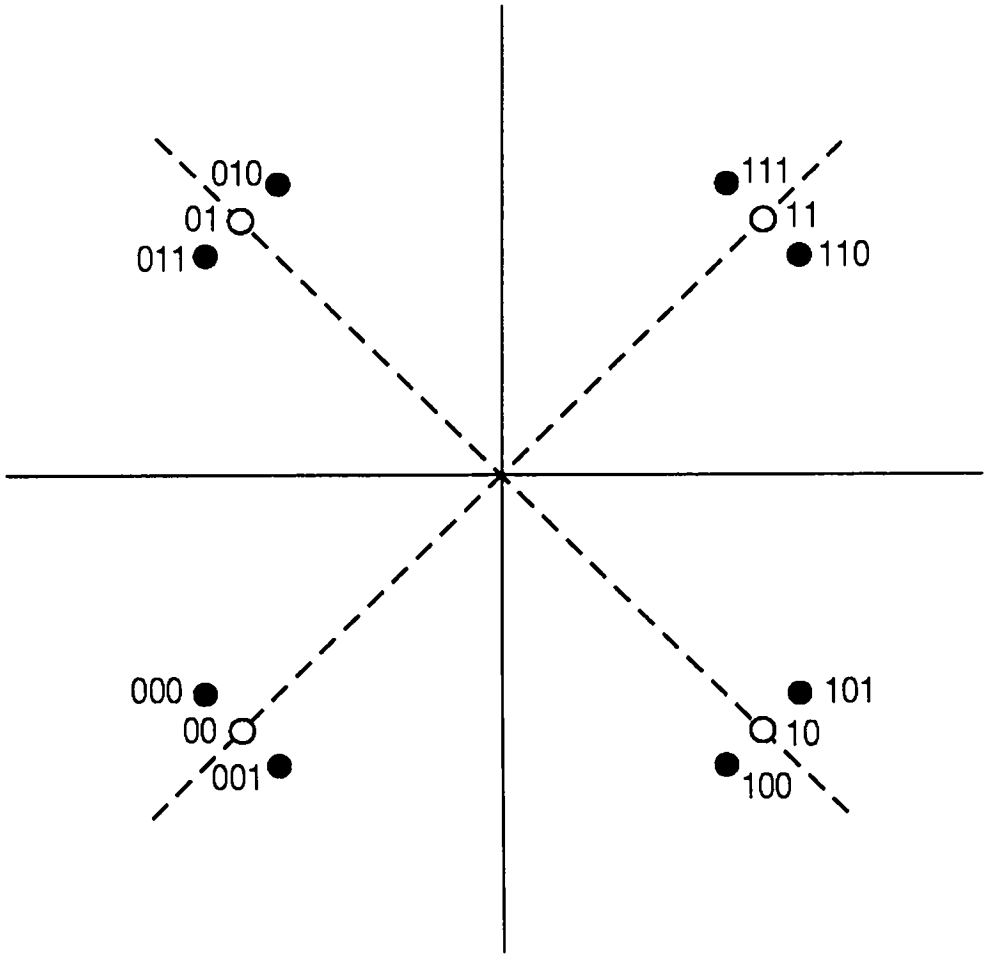


图 10