(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
2020 年 4 月 2 日 (02.04.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/062073 A1

(51) 国际专利分类号:
H04W 12/00 (2009.01)

(21) 国际申请号: PCT/CN2018/108439

(22) 国际申请日: 2018 年 9 月 28 日 (28.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人:深圳大学(**SHENZHEN UNIVERSITY**) [CN/CN]; 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

(72) 发明人: 谢宁(**XIE, Ning**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。
胡吉(**HU, Ji**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518060 (CN)。

(74) 代理人: 深圳舍穆专利代理事务所 (特殊普通合伙) 等(**SHENZHEN SERMON PATENT FIRM** et al.); 中国广东省深圳市宝安区新安街道留芳路6号庭威产业园3栋5楼B2区, Guangdong 518152 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

WO 2020/062073 A1

(54) **Title:** METHOD AND SYSTEM FOR PREVENTING JAMMING ATTACK IN WIRELESS POWERED COMMUNICATION NETWORK

(54) 发明名称: 无线能量传输通信网络的加塞攻击防御方法及系统

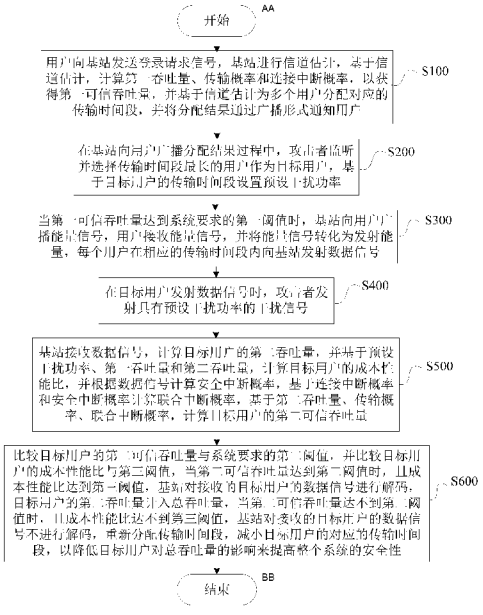

图 3

S100 A user transmits a loading request signal to a base station; the base station performs channel estimation, calculates a first throughput, a transmission probability, and a connection interruption probability on the basis of the channel estimation to obtain a first trusted throughput, allocates corresponding transmission periods for a plurality of users on the basis of the channel estimation, and notifies users of the allocation result by broadcasting

S200 During broadcasting the allocation result to the users by the base station, an attacker listens to and selects the user having the longest transmission time period as a target user, and sets a preset interference power on the basis of the transmission time period of the target user

S300 When the first trusted throughput reaches a first threshold required by a system, the base station transmits power signals to the users; the users receive the power signals and convert the power signals into transmission power; and each user transmits a data signal to the base station in a corresponding transmission time period

S400 During transmitting the data signal by the target user, the attacker transmits an interference signal having the preset interference power

S500 The base station receives the data signal, calculates a second throughput of the target user, calculates cost-performance ratio of the target user on the basis of the preset interference power, the first throughput, and the second throughput, calculates a security interrupt probability according to the data signal, calculates a combined interruption probability on the basis of the connection interruption probability and the security interrupt probability, and calculates a second trusted throughput on the basis of the second throughput, the transmission probability, and the combined interruption probability

S600 Compare the second trusted throughput of the target user with a second threshold required by the system, and compare the cost-performance ratio of the target user with a third threshold; when the second trusted throughput reaches the second threshold and the cost-performance ratio reaches the third threshold, the base station decodes the received data signal from the target user; a total throughput includes the second throughput of the target user, when the second trusted throughput does not reach the second threshold and the cost-performance ratio does not reach the third threshold, the base station does decode the received data signal from the target user, re-allocates the transmission time periods to reduce the transmission time period corresponding to the target user, so as to reduce the influence of the target user on the total throughput, thereby improving the security of the whole system

AA Start

BB End

(57) **Abstract:** The present disclosure describes a method for preventing a jamming attack in a wireless powered communication network, comprising: a base station performs channel estimation, calculates a first trusted throughput, allocates a transmission time period for each user, and notifies users of the allocation result by broadcasting; an attacker listens to the allocation result, takes the user having the longest transmission time period as a target user, and sets a preset interference power on the basis of the transmission time period of the target user; when the first trusted throughput reaches a first threshold, the base station transmits power to the user; the

[见续页]

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, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明：
- 关于发明人身份(细则4.17(i))
- 关于申请人有权申请并被授予专利(细则4.17(ii))
- 发明人资格(细则4.17(iv))

本国际公布：
- 包括国际检索报告(条约第21条(3))。

user receives power and transmits a data signal to the base station; when the target user transmits the data signal, the attacker transmits an interference signal; the base station calculates a security interrupt probability, a second trusted throughput, and a cost-performance ratio, on the basis of the received data signal, compares the second trusted throughput of the target user with a second threshold required by a system, compares the cost-performance ratio of the target user with a third threshold so as to perform attack prediction, and only if both thresholds are reached, decodes the received signal.

(57) 摘要：本公开描述了一种无线能量传输通信网络的加塞攻击防御方法，包括基站进行信道估计，计算第一可信吞吐量并给每个用户分配传输时间段，分配结果通过广播形式通知用户，攻击者监听分配结果，将传输时间段最长的用户作为目标用户，基于目标用户的传输时间段设置预设干扰功率，当第一可信吞吐量达到第一阈值时，基站向用户发射能量，用户接收能量并向基站发射数据信号，在目标用户发射数据信号时，攻击者发射干扰信号，基站基于接收的数据信号计算安全中断概率、第二可信吞吐量和成本性能比，比较目标用户的第二可信吞吐量与系统要求的第二阈值，并比较目标用户的成本性能比与第三阈值，以进行攻击预测，如果两个阈值都能满足，才对接收的信号进行解码。

无线能量传输通信网络的加塞攻击防御方法及系统

技术领域

本公开涉及无线通信技术领域，具体涉及一种无线能量传输通信网络的加塞攻击防御方法及系统。

背景技术

无线能量传输通信网络（wireless powered communication network，WPCN）是一种通过采集环境中的信号以获得能量，并将获得的能量应作为用户端的能量供给的通信网络。在现有文献中，还没有明确地应用一种机制来满足无线能量传输通信网络的某些安全要求。例如，在注册期之后，AP（混合接入点，也即基站）不包括验证发射机标识的附加机制。因此无线能量传输通信网络（WPCN）存在安全漏洞。

在无线能量传输通信网络（WPCN）中，基站与用户每完成有一次数据信号传输，主要包括四个阶段即信道估计、时间分配、能量传输和信息传输。其中，安全漏洞可能出现在信息传输阶段。攻击者向用户发射干扰信号，以破坏无线能量传输通信网络的安全性和可靠性。

发明内容

为了解决上述问题，在无线能量传输通信网络（WPCN）中引入物理层认证（PHY）来满足其安全需求。基于物理层认证，可以有目的和有效地控制安全级别。如果 WPCN 的安全性是主要优先级，则提高认证准确度要求；否则，可以放宽认证的准确度要求。为了解决上述现有问题，本公开提供一种能够有目的和有效地控制安全级别并提高网络安全性的无线能量传输通信网络的加塞攻击防御方法及系统。

为此，本公开的第一方面提供了一种无线能量传输通信网络的加塞攻击防御方法，是包含基站、用户和攻击者的无线能量传输通信网络的加塞攻击防御方法，其特征在于，包括：所述用户向所述基站发送登录请求信号，所述基站进行信道估计，基于所述信道估计为多个

所述用户分配对应的传输时间段，并将分配结果通过广播形式通知所述用户，基于所述信道估计，计算第一吞吐量、传输概率和连接中断概率，基于所述吞吐量、所述传输概率和所述连接中断概率，计算第一可信吞吐量；在所述基站向所述用户广播分配结果过程中，所述攻击者监听并选择传输时间段最长的用户作为目标用户，基于所述目标用户的传输时间段设置预设干扰功率；当所述第一可信吞吐量达到系统要求的第一阈值时，所述基站向所述用户广播能量信号，所述用户接收所述能量信号，并将所述能量信号转化为发射能量，每个所述用户在相应的传输时间段内向所述基站发射数据信号；在所述目标用户发射数据信号时，所述攻击者发射具有所述预设干扰功率的干扰信号；所述基站接收所述数据信号，计算所述目标用户的第二吞吐量，并基于所述预设干扰功率、所述第一吞吐量和所述第二吞吐量，计算所述目标用户的成本性能比，并根据所述数据信号计算安全中断概率，基于所述连接中断概率和所述安全中断概率计算联合中断概率，基于所述第二吞吐量、所述传输概率、所述联合中断概率，计算所述目标用户的第二可信吞吐量；并且比较所述目标用户的第二可信吞吐量与系统要求的第二阈值，并比较所述目标用户的成本性能比与第三阈值，当所述第二可信吞吐量达到所述第二阈值时，且成本性能比达到所述第三阈值，所述基站对接收的所述目标用户的数据信号进行解码，所述目标用户的第二吞吐量计入总吞吐量，当所述第二可信吞吐量达不到所述第二阈值时，且成本性能比达不到所述第三阈值，所述基站对接收的所述目标用户的数据信号不进行解码，重新分配传输时间段，减小所述目标用户的对应的传输时间段，以降低所述目标用户对总吞吐量的影响来提高整个系统的安全性。

在本公开中，基站进行信道估计，计算第一可信吞吐量并给每个用户分配传输时间段，分配结果通过广播形式通知用户，攻击者监听分配结果，将传输时间段最长的用户作为目标用户，基于目标用户的传输时间段设置预设干扰功率，当第一可信吞吐量达到第一阈值时，基站向用户发射能量，用户接收能量并向基站发射数据信号，在目标用户发射数据信号时，攻击者发射干扰信号，基站基于接收的数据信号计算安全中断概率、第二可信吞吐量和成本性能比，比较目标用户

的成本性能比与第三阈值，并比较目标用户的第二可信吞吐量与系统要求的第二阈值，以提高整个系统的安全性。这种情况下，能够防御攻击者的攻击行为，实现有目的和有效地控制安全级别并且提高网络安全性。

在本公开第一方面所涉及的加塞攻击防御方法中，每个所述用户的第一吞吐量由下式（Ⅰ）计算得到：$R_i=(1-\rho_i)\tau_i\log_2(1+\gamma_i)$ （Ⅰ），每个所述用户的第二吞吐量由下式（Ⅱ）计算得到：$R_{J,i}=(1-\rho_i)\tau_i\log_2(1+\gamma_{J,i})$ （Ⅱ），其中，R_i表示第 i 个用户的第一吞吐量，$R_{J,i}$表示第 i 个用户的第二吞吐量，ρ_i表示安全分配因子，τ_i表示第 i 个用户对应的传输时间段的时间分配因子，γ_i表示在所述基站接收到的瞬时信噪比，$\gamma_{J,i}$表示在接收所述干扰信号后所述基站接收到的瞬时信噪比。在这种情况下，以便得到成本性能比。

在本公开第一方面所涉及的加塞攻击防御方法中，所述成本性能比λ_i由下式（Ⅲ）计算得到：$\lambda_i=\frac{R_i-R_{J,i}}{P_{J,i}}$ （Ⅲ），其中，R_i表示第 i 个用户的第一吞吐量，$R_{J,i}$表示第 i 个用户的第二吞吐量，$P_{J,i}$表示所述干扰信号的发射功率。由此，可以基于成本性能比调整安全阈值。

在本公开第一方面所涉及的加塞攻击防御方法中，所述安全中断概率由下式（Ⅳ）计算得到：$P_{\mathrm{SOi}}=\mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)<\varepsilon_{\mathrm{PD}}\middle|\text{transmission of }U_i\text{ occurs}\right)$ （Ⅳ），所述连接中断概率由下式（Ⅴ）计算得到：$P_{\mathrm{COi}}=\mathbb{P}\left(R_i<\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of }U_i\text{ occurs}\right)$ （Ⅴ），其中，PD 表示检测概率，PFA 表示虚警概率，$\varepsilon_{\mathrm{PD}}$表示用户的安全阈值，$\varepsilon_{\mathrm{PCO}}$表示通信速率的下限，$R_i$表示第 i 个用户的第一吞吐量，$U_i$表示第 i 个用户。由此，能够获得第一可信吞吐量和第二可信吞吐量。

在本公开第一方面所涉及的加塞攻击防御方法中，所述第一可信吞吐量满足下式（Ⅵ）：$\eta_i=P_{\mathrm{Ti}}(1-P_{\mathrm{COi}})R_i$ （Ⅵ），所述第二可信吞吐量满足下式（Ⅶ）：$\eta_i=P_{\mathrm{Ti}}(1-P_{\mathrm{SCOi}})R_{J,i}$ （Ⅶ），其中，$P_{\mathrm{Ti}}=\mathbb{P}(\text{transmission of }U_i\text{ occurs})$，PT 表示所述传输概率，PCO 表示所述连接中断概率，R_i表示第 i 个用户的第一吞吐量，$R_{J,i}$表示第 i 个用户的第二吞吐量，PSCO 表示联合

中断概率，且满足 $P_{\mathrm{SCOi}}=1-\mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)\geq\varepsilon_{\mathrm{PD}},R_i\geq\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of }U_i\text{ occurs}\right)$ 。在这种情况下，能够通过改变可信吞吐量有目的和有效地控制无线能量传输通信网络的安全级别。

本公开的第二方面提供一种无线能量传输通信网络的加塞攻击防御系统，是包含发射装置、接收装置和攻击装置的无线能量传输通信网络的加塞攻击防御系统，其特征在于，包括：所述发射装置，其用于在所述用户装置向所述发射装置发送登录请求信号后，进行信道估计，基于所述信道估计为多个所述用户装置分配对应的传输时间段，并将分配结果通过广播形式通知所述用户装置，并基于所述信道估计，计算第一吞吐量、传输概率和连接中断概率，以获得第一可信吞吐量，当所述第一可信吞吐量达到系统要求的第一阈值时，所述发射装置向所述用户装置广播能量信号；所述用户装置，其用于接收所述能量信号，并将所述能量信号转化为发射能量，每个所述用户装置在相应的传输时间段内向所述发射装置发射数据信号；所述攻击装置，其用于在所述发射装置向所述用户装置广播分配结果过程中，监听并选择传输时间段最长的用户装置作为目标用户装置，基于所述目标用户装置的传输时间段设置预设干扰功率，在所述目标用户装置发射数据信号时，发射具有所述预设干扰功率的干扰信号；其中，所述发射装置接收所述数据信号，计算所述目标用户装置的第二吞吐量，并基于所述预设干扰功率、所述第一吞吐量和所述第二吞吐量，计算所述目标用户装置的成本性能比，并根据所述数据信号计算安全中断概率，基于所述连接中断概率和所述安全中断概率计算联合中断概率，基于所述第二吞吐量、所述传输概率、所述联合中断概率，计算所述目标用户装置的第二可信吞吐量，比较所述目标用户装置的第二可信吞吐量与系统要求的第二阈值，并比较所述目标用户装置的第二可信吞吐量与系统要求的第二阈值，并比较所述目标用户装置的成本性能比与第三阈值，当所述第二可信吞吐量达到所述第二阈值时，且成本性能比达到所述第三阈值，所述发射装置对接收的所述目标用户装置的数据信号进行解码，所述目标用户装置的第二吞吐量计入总吞吐量，当所述第二可信吞吐量达不到所述第二阈值时，且成本性能比达不到所述第

三阈值，所述发射装置对接收的所述目标用户装置的数据信号不进行解码，重新分配传输时间段，减小所述目标用户装置的对应的传输时间段，以降低所述目标用户装置对总吞吐量的影响来提高整个系统的安全性。

在本公开中，发射装置进行信道估计，计算第一可信吞吐量并给每个用户装置分配传输时间段，分配结果通过广播形式通知用户装置，攻击装置监听分配结果，将传输时间段最长的用户装置作为目标用户装置，基于目标用户装置的传输时间段设置预设干扰功率，当第一可信吞吐量达到第一阈值时，发射装置向用户装置发射能量，用户装置接收能量并向发射装置发射数据信号，在目标用户装置发射数据信号时，攻击装置发射干扰信号，发射装置基于接收的数据信号计算安全中断概率、第二可信吞吐量和成本性能比，比较目标用户装置的成本性能比与第三阈值，并比较目标用户装置的第二可信吞吐量与系统要求的第二阈值，以提高整个系统的安全性。这种情况下，能够防御攻击装置的攻击行为，实现有目的和有效地控制安全级别并且提高网络安全性。

在本公开第二方面所涉及的加塞攻击防御系统中，每个所述用户装置的第一吞吐量由下式（Ⅰ）计算得到：$R_i=(1-\rho_i)\tau_i\log_2(1+\gamma_i)$ （Ⅰ），每个所述用户装置的第二吞吐量由下式（Ⅱ）计算得到：$R_{J,i}=(1-\rho_i)\tau_i\log_2(1+\gamma_{J,i})$ （Ⅱ），其中，R_i表示第 i 个用户装置的第一吞吐量，$R_{J,i}$表示第 i 个用户装置的第二吞吐量，ρ_i表示安全分配因子，τ_i表示第 i 个用户装置对应的传输时间段的时间分配因子，γ_i表示在所述发射装置接收到的瞬时信噪比，$\gamma_{J,i}$表示在接收所述干扰信号后所述发射装置接收到的瞬时信噪比。在这种情况下，以便得到成本性能比。

在本公开第二方面所涉及的加塞攻击防御系统中，所述成本性能比λ_i由下式（Ⅲ）计算得到：$\lambda_i=\frac{R_i-R_{J,i}}{P_{J,i}}$ （Ⅲ），其中，R_i表示第 i 个接收装置的第一吞吐量，$R_{J,i}$表示第 i 个接收装置的第二吞吐量，$P_{J,i}$表示所述干扰信号的发射功率。由此，可以基于成本性能比调整安全阈值。

在本公开第二方面所涉及的加塞攻击防御系统中，所述安全中断概率由下式（Ⅳ）计算得到：$P_{\mathrm{SOi}}=\mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)<\varepsilon_{\mathrm{PD}}\middle|\text{transmission of }U_i\text{ occurs}\right)$ (Ⅳ)，所述连接中断概率由下式（Ⅴ）计算得到：$P_{\mathrm{COi}}=\mathbb{P}\left(R_i<\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of }U_i\text{ occurs}\right)$ (Ⅴ)，其中，PD 表示检测概率，PFA 表示虚警概率，$\varepsilon_{\mathrm{PD}}$表示用户装置的安全阈值，$\varepsilon_{\mathrm{PCO}}$表示通信速率的下限，$R_i$表示第 i 个用户装置的第一吞吐量，$U_i$表示第 i 个用户装置。由此，能够获得第一可信吞吐量和第二可信吞吐量。

在本公开第二方面所涉及的加塞攻击防御系统中，所述第一可信吞吐量满足下式（Ⅵ）：$\eta_i=P_{\mathrm{T}i}\left(1-P_{\mathrm{COi}}\right)R_i$ (Ⅵ)，所述第二可信吞吐量满足下式（Ⅶ）：$\eta_i=P_{\mathrm{T}i}\left(1-P_{\mathrm{SCOi}}\right)R_{J,i}$ (Ⅶ)，其中，$P_{\mathrm{T}i}=\mathbb{P}\left(\text{transmission of }U_i\text{ occurs}\right)$，PT 表示所述传输概率，PCO 表示所述连接中断概率，R_i表示第 i 个用户装置的第一吞吐量，$R_{J,i}$表示第 i 个用户装置的第二吞吐量，PSCO 表示联合中断概率，且满足 $P_{\mathrm{SCOi}}=1-\mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)\geq\varepsilon_{\mathrm{PD}},R_i\geq\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of }U_i\text{ occurs}\right)$。由此，能够通过改变可信吞吐量有目的和有效地控制无线能量传输通信网络的安全级别。

与现有技术相比，本公开中无线能量传输通信网络的加塞攻击防御方法是从物理层的角度来分析，与基于上层密码工具的传统认证机制相比，物理层认证具有两大优势。首先，特定的物理层属性直接关系到通信设备和相应的环境，这些通常非常难以模拟。其次，物理层的认证使得合法接收机能够快速区分基站和攻击者，而无需完成上层处理，且上层处理需要大量额外的网络资源。基于物理层认证，WPCN 设计人员可以有目的和有效地控制安全级别。

附图说明

图 1 是示出了本公开的示例所涉及的无线能量传输通信网络的通信网络模型示意图。

图 2 是示出本公开的示例涉及的无线能量传输通信网络的时序图。

图 3 是示出了本公开的示例所涉及的无线能量传输通信网络的加塞攻击防御方法的流程示意图。

图 4 是示出了本公开的示例所涉及的在不同能量传输时段的时间分配因子下的第一吞吐量和第二吞吐量的对比示意图。

图 5 是示出了本公开的示例所涉及的在不同能量传输时段的时间分配因子下的成本性能比波形示意图。

图 6 是示出了本公开的示例所涉及的无线能量传输通信网络的加塞攻击防御系统的结构示意图。

具体实施方式

以下，参考附图，详细地说明本公开的优选实施方式。在下面的说明中，对于相同的部件赋予相同的符号，省略重复的说明。另外，附图只是示意性的图，部件相互之间的尺寸的比例或者部件的形状等可以与实际的不同。需要说明的是，本公开的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象，而不是用于描述特定顺序。

图 1 是示出了本公开示例所涉及的无线能量传输通信网络的通信网络模型示意图。在一些示例中，如图 1 所示，基站可以有一个。用户可以包括至少一个。基站与每个用户都配有一个天线。且基站与所有的用户都在相同的频段上工作。攻击者可以包括至少一个。

在一些示例中，图 1 所示的信号模型中，基站（例如接入点）可以是指接入网中在空中接口上通过一个或多个扇区与无线终端通信的设备。基站可用于将收到的空中帧与 IP 分组进行相互转换，作为无线终端与接入网的其余部分之间的路由器，其中，接入网的其余部分可包括网际协议（IP）网络。基站还可以协调对空中接口的属性管理。例如，基站可以是 GSM 或 CDMA 中的基站（BTS，Base Transceiver Station），也可以是 WCDMA 中的基站（NodeB），还可以是 LTE 中的演进型基站（NodeB 或 eNB 或 e-NodeB，evolutional Node B）。

在一些示例中，用户可以是节点。用户还可以包括用户设备。用户设备可以包括但不限于智能手机、笔记本电脑、个人计算机（Personal Computer，PC）、个人数字助理（Personal Digital Assistant，PDA）、移动互联网设备（Mobile Internet Device，MID）、穿戴设备（如智能手表、智能手环、智能眼镜）等各类电子设备。该用户设备或测试设备的操

作系统可包括但不限于 Android 操作系统、IOS 操作系统、Symbian（塞班）操作系统、Black Berry（黑莓）操作系统、Windows Phone8 操作系统等。在一些示例中，攻击者可以包括上述的基站或用户设备。

在一些示例中，如图 1 所示，虚线 A 可以表示下行链路（downlink，DL）。下行链路（DL）中可以具有无线能量传输（wireless energy transfer，WET）。实线 B 可以表示上行链路（uplink，UL）。上行链路（UL）中的无线信息传输（wireless information transmissions，WIT）。虚线 C 可以表示攻击者向用户发送干扰信号。

在一些示例中，如图 1 所示的通信网络模型中，所有用户需要从 DL 中通过基站发射的能量信号采集能量。并且用户将收集到的能量信号存储在可充电的电池中，用于为用户的电路供电并且在 UL 中向基站传输数据信号。另外，所有的用户都被假定没有其他嵌入式能源。另外，基站和用户之间通过无线信道完成上述的能量信号的数据信号的传输。其中，DL 信道可以由复数随机变量 h_{AU_i} 表示。UL 信道可以由复数随机变量 h_{U_iA} 表示。且 DL 和 UL 信道都被假定为准静态和平坦衰落。

在一些示例中，假设 DL 和 UL 保持信道互惠性，因此 $h_{U_iA}=h_{AU_i}=h_i$。h_i 表示信道响应且满足 $h_i \sim \mathcal{CN}\left(0,\sigma_{hi}^2\right)$。其中 $\sigma_{hi}^2 \propto d_i^{-\alpha_d}$，$\alpha_d \geq 2$ 是信道路径损耗指数，d_i 是基站和用户之间的距离。

在一些示例中，如图 1 所示的通信网络模型可以包括信道估计（channel estimation，CE）、时间分配（time allocation，TA）、能量传输（WET）和信息传输（WIT）四个阶段。另外，当无线能量传输通信网络的综合性能较低时，可以实现上述的四个阶段中部分阶段。

图 2 是示出了本公开的示例所涉及的无线能量传输通信网络的时序图。在一些示例中，如图 2 所示，无线能量传输通信网络完成一次能量信号和数据信号的传输需要的时间可以是 T。也即无线能量传输通信网络完成一次信道估计、时间分配、能量传输和信息传输需要的时间可以是 T。其中，信息传输阶段中各个用户是通过时分多址（TDMA）的方式将数据信号传输至基站。

在一些示例中，如图 2 所示，T 可以根据上述的四个阶段划分为四个时段。具体而言，信道估计的时段可以为 $\tau_a T$，时间分配的时段可以

为$\tau_b T$，能量传输的时段可以为$\tau_0 T$，信息传输的时段可以为$\sum_{i=0}^{K}\tau_i T$，其中，i 可以取 1、2、3...K-1、K。K 代表用户的个数。其中，τ_a、τ_b、τ_0和τ_i可以分别代表各个阶段的时间分配因子。且满足$\tau_a+\tau_b+\sum_{i=0}^{K}\tau_i \le 1$。另外，不同的$\tau_i T$表示不同的用户的时段。

基于图 1 所示的模型和图 2 的时序图，由于无线能量传输通信网络中存在攻击者，攻击者可能会在 WIT 阶段攻击无线能量传输通信网络，以影响无线能量传输通信网络的能量传输和数据传输，因此本公开提供了无线能量传输通信网络的加塞攻击防御方法和系统（有时可以简称为加塞攻击防御方法和系统）。另外，无线能量传输通信网络的加塞攻击防御方法和系统可以是包含基站、用户和攻击者的无线能量传输通信网络的加塞攻击防御方法和系统。在本公开中，能够更准确防御攻击者的攻击行为,且有目的和有效地控制 WPCN 的安全级别。

图 3 是示出了本公开的示例所涉及的无线能量传输通信网络的加塞攻击防御方法的流程示意图。基于图 1 所示的模型和图 2 的时序图，如图 3 所示，无线能量传输通信网络的加塞攻击防御方法可以包括用户向基站发送登录请求信号，基站进行信道估计，基于信道估计为多个用户分配对应的传输时间段，并将分配结果通过广播形式通知用户，基于信道估计，计算第一吞吐量、传输概率和连接中断概率，基于吞吐量、传输概率和连接中断概率，计算第一可信吞吐量（步骤 S100）。

在步骤 S100 中，用户可以向基站发送登录请求信号，基站进行信道估计。基于上述可知，基站在时段$\tau_a T$内完成信道估计。具体而言，在时段$\tau_a T$内，所有用户可以先向基站发送登录请求。如果用户（也称为用户端）的标识属于基站的合法用户数据库，则基站向用户返回确认信号。同时，基站根据 CE 阶段基站与用户之间的信息交换完善h_{AU_i}和$h_{U_i A}$。如果用户的标识不属于基站的合法用户数据库，则用户直接丢弃该用户。

另外，在步骤 S100 中，基站还可以基于信道估计为多个用户分配多个传输时间段,并将分配结果通过广播形式通知用户。基于上述可知，基站在时段$\tau_b T$内完成时间分配。具体而言，在$\tau_b T$内，基站基于信道

估计的结果，分配 WET 和 WIT 的时间。另外，在 WIT 中不同的用户占据不同的时间，基站可以进一步完成对不同用户的时间的分配。分配的结果可以是 WET 的时间为 $\tau_0 T$ 和 WIT 的时间为 $\sum_{i=0}^{K}\tau_i T$。其中，不同的 $\tau_i T$ 表示不同的用户的时间。

另外，在步骤 S100 中，基站还可以基于信道估计，至少可以获得用户的安全分配因子、基站接收到的瞬时信噪比（SNR）和各个传输时间段的时间分配因子，进而计算用户的第一吞吐量。

在一些示例中，在 UL 中，每个用户的第一吞吐量 R_i（也即第 i 个用户的第一吞吐量）可以由下式（1）计算得到：

$$R_i = (1-\rho_i)\tau_i \log_2(1+\gamma_i) = (1-\rho_i)\tau_i \log_2\left(1+\beta_i \frac{\tau_0}{\tau_i}\right) \quad (1)$$

其中，τ_i 表示第 i 个用户对应的传输时间段的时间分配因子。γ_i 表示在基站接收到的瞬时信噪比（SNR）。且 γ_i 满足 $\gamma_i = \frac{|h_{C_i}|^2 \zeta P_A \tau_0}{\sigma_n^2 \tau_i}$。$\beta_i$ 可以表示为 $\beta_i = \frac{|h_{C_i}|^2 \zeta P_A}{\sigma_n^2}$。在 γ_i 的表达式中，$h_{C_i} = |h_i|^2$ 且 $|h_{C_i}|^2$ 的概率密度函数满足式（2）：$f_{|h_{Ci}|^2}(x) = f_{|h_i|^4}(x) = \frac{1}{2\sigma_{hi}^2\sqrt{x}} \exp\left(-\frac{\sqrt{x}}{\sigma_{hi}^2}\right)$ (2)。由此，基站可以计算得到所有用户的第一吞吐量之和，即 WPCN 的第一总吞吐量 R_{sum} 满足式（3）：$R_{\text{sum}} = \sum_{i=1}^{K} R_i$ (3)。

在步骤 S100 中，基站可以计算传输概率 PT。PT 可以度量传输延迟性能。在 WPCN 中假设存在重传机制，根据特定的协议，用户 U_i 的重传现象可能不会总是发生。因此，用户 U_i 的传输概率 PT 满足式（4）：$P_{\text{Ti}} = \mathbb{P}(\text{transmission of } U_i \text{ occurs})$ (4)，在一些示例中，式（4）可以具体表示为式（5）：$P_{\text{Ti}} = \exp\left(-\sqrt{\frac{2\varepsilon_{\text{PT}}\tau_i}{\bar{\beta}_i \tau_0}}\right) = \exp\left(-\sqrt{\frac{2\varepsilon_{\text{PT}}}{\bar{\gamma}_i}}\right)$ (5)，其中，$\bar{\beta}_i = \mathbb{E}\{\beta_i\} = \frac{2\sigma_{hi}^4 \zeta P_A}{\sigma_n^2}$，$\bar{\gamma}_i = \mathbb{E}\{\gamma_i\} = \frac{2\sigma_{hi}^4 \zeta P_A \tau_0}{\sigma_n^2 \tau_i}$。

另外，通过式（4）和式（5）分别得到传输概率的理论值和仿真

值，均随着基站的瞬时信噪比的增大，呈递增趋势。当信噪比 γ_i 超过设定门限值 $\varepsilon_{\mathrm{PT}}$ 时，用户的数据信号就会成功传输。由此，式（4）可以转化为式（6）：$P_{\mathrm{Ti}}=\mathbb{P}\left(\gamma_i>\varepsilon_{\mathrm{PT}}\right)$ (6)。其中，设定门限值 $\varepsilon_{\mathrm{PT}}$ 可以根据经验设置。设定门限值 $\varepsilon_{\mathrm{PT}}$ 衡量用户发射的数据信号的传输延迟和可靠性。

在一些示例中，当 WPCN 中不存在重传机制时，$\varepsilon_{\mathrm{PT}}=0$，$P_{\mathrm{Ti}}=1$。

在步骤 S100 中，基站还可以计算连接中断概率 PCO。连接中断概率 PCO 可以评估 WPCN 的可靠性性能。当用户无法在基站无错误地解码消息时发生连接中断，连接中断概率 PCO 满足下式（7）：

$$P_{\mathrm{COi}}=\mathbb{P}\left(R_i<\varepsilon_{\mathrm{PCO}}\left|\text{transmission of } U_i \text{ occurs}\right.\right) \quad (7)$$

其中，$\varepsilon_{\mathrm{PCO}}$ 表示通信速率的下限。在这种情况下，能够判断无线能量传输通信网络的可靠性。

在一些示例中，满足 $\varepsilon_{\mathrm{PT}}\in\left[0,2^{\frac{\varepsilon_{\mathrm{PCO}}}{(1-\rho_i)\tau_i}}-1\right)$ 时，连接中断发生。因此，当 $\varepsilon_{\mathrm{PT}}\geq 0$ 时，连接中断概率 PCO 可以表示为：

$$P_{\mathrm{COi}}=\begin{cases}1-\exp\left(\sqrt{\dfrac{2}{\overline{\gamma}_i}}\left(\sqrt{\varepsilon_{\mathrm{PT}}}-\sqrt{\left(2^{\frac{\varepsilon_{\mathrm{PCO}}}{(1-\rho_i)\tau_i}}-1\right)}\right)\right), & 0\leq\varepsilon_{\mathrm{PT}}<2^{\frac{\varepsilon_{\mathrm{PCO}}}{(1-\rho_i)\tau_i}}-1\\ 0, & \varepsilon_{\mathrm{PT}}\geq 2^{\frac{\varepsilon_{\mathrm{PCO}}}{(1-\rho_i)\tau_i}}-1\end{cases} \quad (8)$$

另外，通过式（7）和式（8）分别得到连接中断概率的理论值和仿真值，均随着基站的瞬时信噪比的增大，呈递减趋势。

另外，在步骤 S100 中，基于吞吐量、传输概率和连接中断概率，计算第一可信吞吐量。第一可信吞吐量可以综合吞吐量、传输概率和连接中断概率，以准确评估无线能量传输通信网络的整体性能。每个用户的第一可信吞吐量 η_i 满足下式（9）：$\eta_i=P_{\mathrm{Ti}}\left(1-P_{\mathrm{COi}}\right)R_i$ (9)。由此，WPCN 的可信吞吐量 η_{sum} 可以表示为 $\eta_{\mathrm{sum}}=\sum_{i=1}^{K}\eta_i$。在这种情况下，能够更准确评估无线能量传输通信网络的整体性能。在一些示例中，可以基于式（1）、式（5）和式（8）获得具体的可信吞吐量 η_{sum}。

在一些示例中，如图 3 所示，加塞攻击防御方法还可以包括在基站向用户广播分配结果过程中，攻击者监听并选择传输时间段最长的

用户作为目标用户，基于目标用户的传输时间段设置预设干扰功率（步骤 S200）。在步骤 S200 中，在基站广播分配结果过程中，攻击者可以截获分配结果。也即在攻击者在 TA 阶段可以截获分配结果（即各个用户的传输时间段的分配信息）。然后攻击者选择多个用户中的传输时间段最长的用户作为目标用户。基于目标用户的传输时间段设置预设干扰功率 $P_{J,1}$。预设干扰功率 $P_{J,1}$ 可以看做攻击者攻击用户的能力。

在一些示例中，如图 3 所示，加塞攻击防御方法还可以包括当第一可信吞吐量达到系统要求的第一阈值时，基站向用户广播能量信号，用户接收能量信号，并将能量信号转化为发射能量，每个用户在相应的传输时间段内向基站发射数据信号（步骤 S300）。

在步骤 S300 中，当第一可信吞吐量达到系统要求的第一阈值 ε_1 时，基站可以向用户广播能量信号。基于上述可知，基站发射能量的时间是 $\tau_0 T$。在时段 $\tau_0 T$ 内，基站可以向所有的用户发射能量信号。基站发射的能量可以表示为 P_A。另外，P_A 足够大。相应的，当第一可信吞吐量达不到系统要求的第一阈值 ε_1 时，基站可以不用向无线信道广播能量信号，也即第一可信吞吐量达不到系统要求的第一阈值 ε_1 时，无线能量传输通信网络的综合性能较低，通信网络系统可以不用实现能量传输。另外，系统要求的第一阈值 ε_1 可以根据经验设置。

另外，在步骤 S300 中，用户接收能量信号，并将能量信号转化为发射能量，每个用户在相应的传输时间段内向基站发射数据信号。具体而言，在时段 $\tau_0 T$ 内，用户可以接收基站发射的能量信号。每个用户接收到的能量足够大，使得从接收机噪声而收获的能量可以忽略不计。每个用户接收的能量可以由式（10）计算得到：$E_i = \zeta_i \left| h_{AU_i} \right|^2 P_A \tau_0$ (10)，其中，ζ_i 是每个用户的能量收集效率系数。$0 < \zeta_i < 1$，i 可以取 1、2、3...K-1、K。K 代表用户的个数。另外，为了方便后续讨论，可以假设 $\zeta_1 = \ldots = \zeta_K = \zeta$。

另外，在步骤 S300 中，每个用户可以在相应的传输时间段内向基站发射数据信号 $\mathbf{x}_i$。基于上述可知，每个用户在 TA 阶段时从基站处获知各自对应的时段 $\tau_i T$（也即上述的相应的传输时间段）。在时段 $\sum_{i=0}^{K} \tau_i T$

内，每个用户在相应的时段$\tau_i T$内独立完成向基站的数据传输。用户收集的能量的固定部分被用于数据传输中。第 i 个用户的平均发射功率可以由式（11）计算得到：$P_i = \kappa_i E_i / \tau_i$ (11)，其中，κ_i表示第 i 个用户U_i收集的能量的固定部分。

在一些示例中，数据信号$\mathbf{x}_i$可以包括导频信号$\mathbf{p}_i$和信息信号$\mathbf{m}_i$。$\mathbf{p}_i$和$\mathbf{m}_i$的长度分别表示为$L_{i1} = \rho_i L_i$和$L_{i2} = (1-\rho_i)L_i$，其中，ρ_i表示安全分配因子，L_{i1}和L_{i2}都被假定为整数。L_i表示数据信号$\mathbf{x}_i$的信号长度。L_i满足$L_i = \tau_i f_s T$，其中的f_s是采样频率。另外，$\mathbf{p}_i$的时间长度为$\rho_i \tau_i T$。

在步骤 S300 中，在时段$\sum_{i=0}^{K} \tau_i T$内，基站接收各个用户发射的数据信号。其中，第 i 次 UL 时隙中的基站接收的数据信号可以由下式（12）的矢量形式计算得到：

$$\begin{aligned}\mathbf{y}_i &= h_{U_i A}\sqrt{P_i}\mathbf{x}_i + \mathbf{n}_i \\ &= h_{U_i A}\left|h_{A U_i}\right|\sqrt{\frac{\zeta P_A \tau_0}{\tau_i}}\mathbf{x}_i + \mathbf{n}_i \end{aligned} \quad (12)$$

，其中，$\mathbf{x}_i$表示第 i 个用户发射的数据信号，$\mathbf{x}_i = \{x_1, \ldots, x_{L_i}\}$。$\mathbf{n}_i$表示基站在时隙中的噪声。$\mathbf{n}_i = \{n_1, \ldots, n_{L_i}\}$。且$\mathbf{n}_i$服从$\mathcal{CN}(0, \sigma_n^2)$。

在一些示例中，由于数据信号$\mathbf{x}_i$可以包括导频信号$\mathbf{p}_i$和信息信号$\mathbf{m}_i$，并且假设$\mathbb{E}\{|\mathbf{x}_i|^2\} = L_i$，$\mathbb{E}\{|\mathbf{p}_i|^2\} = L_{i1}$，和$\mathbb{E}\{|\mathbf{m}_i|^2\} = L_{i2}$，因此，基站接收的数据信号可以表示为$\mathbf{y}_i = \{\mathbf{y}_{p_i}, \mathbf{y}_{m_i}\}$。

在一些示例中，如图 3 所示，加塞攻击防御方法还可以包括在目标用户发射数据信号时，攻击者发射具有预设干扰功率的干扰信号（步骤 S400）。在步骤 S400 中，攻击者可以向基站发射具有预设干扰功率的干扰信号，以影响无线能量传输通信网络的能量传输和数据传输。其中干扰信号满足$j_i \sim \mathcal{CN}(0, P_{J,i})$。

在一些示例中，如图 3 所示，加塞攻击防御方法还可以包括基站接收数据信号，计算目标用户的第二吞吐量，并基于预设干扰功率、第一吞吐量和第二吞吐量，计算目标用户的成本性能比，并根据数据信号计算安全中断概率，基于连接中断概率和安全中断概率计算联合中断概率，基于第二吞吐量、传输概率、联合中断概率，计算目标用

户的第二可信吞吐量（步骤 S500）。

另外，在步骤 S500 中，基站可以计算目标用户的第二吞吐量，并基于预设干扰功率、第一吞吐量和第二吞吐量，计算目标用户的成本性能比。第二吞吐量可以是基站接收到干扰信号后每个用户的吞吐量。在这种情况下，基站接收到的瞬时信噪比可以满足下式（13）：

$$\gamma_{J,i}=\frac{|h_i|^4\zeta P_A\tau_0}{\sigma_n^2\tau_i+P_{J,i}\sigma_J^2\tau_i} \qquad (13)$$

其中，$\gamma_{J,i}$表示在接收干扰信号后基站处接收到的瞬时信噪比。σ_J^2是基站与攻击者间信道响应的差异值。且满足$\sigma_J^2\propto d_J^{-\alpha_d}$，$d_J$是基站与攻击者间的距离。另外，为了便于分析，式（13）可以转化为下式（14）：

$$\gamma_{J,i}=\frac{|h_i|^4\zeta P_A\tau_0/\sigma_n^2\tau_i}{1+P_{J,i}\sigma_J^2\tau_i/\sigma_n^2\tau_i}=\frac{\beta_i\tau_0/\tau_i}{1+\beta_{J,i}} \qquad (14)$$

其中，$\beta_{J,i}=\frac{P_{J,i}\sigma_J^2}{\sigma_n^2}$，由此，基于式（1）的第一吞吐量$R_i$，每个用户的第二吞吐量$R_{J,i}$（也即第 i 个用户的第二吞吐量$R_{J,i}$）满足下式（15）：

$$R_{J,i}=(1-\rho_i)\tau_i\log_2(1+\gamma_{J,i}) \qquad (15)$$

比较式（1）和式（15），可以得到$R_{J,i}\le R_i$。根据式（15）可以得到目标用户的第二吞吐量$R_{J,i}$。

在步骤 S500 中，基于干扰信号的发射功率$P_{J,i}$，第一吞吐量R_i和第二吞吐量$R_{J,i}$，可以得到目标用户的成本性能比（CPR），且目标用户的成本性能比（CPR）满足下式（16）：

$$\lambda_i=\frac{R_i-R_{J,i}}{P_{J,i}} \qquad (16)$$

其中，λ_i的单位是 bps/Hz/W，且λ_i可以表示每单位功率攻击者的攻击增益。

在步骤 S500 中，根据数据信号可以计算安全中断概率。由于数据信号可能来自于用户，也可能来自于攻击者，因此，数据信号的传输存在预设条件、虚警概率和漏检概率。安全中断概率 PSO 可以基于预设条件、虚警概率和漏检概率获得。

具体而言，预设条件包括第一条件和第二条件。第一条件为基站接收的数据信号不是来自于用户。第二条件为基站接收的数据信号来自于用户。例如，第一条件 H_0 和第二条件 H_1 可以设定为：

$$\begin{aligned} H_0:&\quad \mathbf{y}_{p_i}=\mathbf{n}_{p_i} \\ H_1:&\quad \mathbf{y}_{p_i}=h_i\sqrt{P_i}\mathbf{p}_i+\mathbf{n}_{p_i}=h_i|h_i|\sqrt{\frac{\zeta P_A\tau_0}{\tau_i}}\mathbf{p}_i+\mathbf{n}_{p_i} \end{aligned} \tag{17}$$

其中，$\mathbf{n}_{p_i}$ 是导频信号簇中的采样噪声信号，其长度与 $\mathbf{y}_{p_i}$ 一样。基站构建一个测试统计信息 δ_i，测试统计信息 δ_i 满足：$\delta_i=\mathbb{R}\{\varphi_i\}=\mathbb{R}\left\{\frac{h_i^*\mathbf{p}_i^H\mathbf{y}_{p_i}}{|h_i|}\right\}$，其中，$\mathbb{R}\{\cdot\}$ 表示实际值。

另外，基于（17），第一条件和第二条件的检验统计量可以分别表示为：$\begin{cases}\varphi_i|H_0=\frac{h_i^*\mathbf{p}_i^H\mathbf{n}_{p_i}}{|h_i|}\\ \varphi_i|H_1=|h_i|^2\rho_iL_i\sqrt{\frac{\zeta P_A\tau_0}{\tau_i}}+\frac{h_i^*\mathbf{p}_i^H\mathbf{n}_{p_i}}{|h_i|}\end{cases}$，设定 $\mathbb{E}\{\mathbf{p}_i^H\mathbf{n}_{p_i}\}=0$，则 $\mathbb{E}\{\varphi_i|H_0\}=0$。

因此，$\mathrm{var}\{\varphi_i|H_0\}=\rho_iL_i\sigma_n^2$。也即 $\varphi_i|H_0\sim\mathcal{CN}(0,\rho_iL_i\sigma_n^2)$。并且满足 $\mathbb{E}\{\varphi_i|H_1\}=|h_i|^2\rho_iL_i\sqrt{\zeta P_A\tau_0/\tau_1}$，$\mathrm{var}\{\varphi_i|H_1\}=\rho_iL_i\sigma_n^2$，$\varphi_i|H_1\sim\mathcal{CN}\left(|h_i|^2\rho_iL_i\sqrt{\zeta P_A\tau_0/\tau_1},\rho_iL_i\sigma_n^2\right)$。

由此，基于 $\delta_i=\mathbb{R}\{\varphi_i\}$，预设条件的假设的阈值检验可以转化为：

$$\begin{aligned} H_0:&\quad \delta_i\sim\mathcal{N}\left(0,\frac{\rho_iL_i\sigma_n^2}{2}\right) \\ H_1:&\quad \delta_i\sim\mathcal{N}\left(|h_i|^2\rho_iL_i\sqrt{\frac{\zeta P_A\tau_0}{\tau_i}},\frac{\rho_iL_i\sigma_n^2}{2}\right) \end{aligned} \tag{18}$$

根据式（18）可知，阈值检验可以被看作是二元假设问题，具有不同的均值但方差相同。其中基于 δ_i 的用户 U_i 的 φ_i 的真实性可以是根据 $\varphi_i=\begin{cases}0, & \delta_i<\theta_i\\ 1, & \delta_i\geq\theta_i\end{cases}$，其中，$\theta_i$ 是检测阈值。

当第一条件为真时接受第二条件称为虚警。当第二条件为真时接受第一条件称为漏检。预设条件的最优决策由 Neyman-Pearson 定理给出，即最优决策满足式（19）：$\begin{aligned}\max\quad & P_{\mathrm{D}i}(P_{\mathrm{FA}i})\\ \text{subject to}\quad & P_{\mathrm{FA}i}\leq\varepsilon_{\mathrm{PFA}}\end{aligned}$ (19)，其中，PD 为

检测概率，PFA 为虚警概率，$\varepsilon_{\mathrm{PFA}}$ 是基站允许的 PFA 的上限。由于 $P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)$ 可以量化用户的认证准确度，并且可以表示基站区分数据信号是否来自用户的能力。

在一些示例中，用户的虚警概率可以表示为式（20）：

$$\begin{aligned} P_{\mathrm{FA}i} &= \mathbb{P}\left\{\delta_i > \theta_i \middle| H_0\right\} \\ &= Q\left(\frac{\theta_i}{\sqrt{\mathrm{var}\left\{\delta_i \middle| H_0\right\}}}\right) = Q\left(\theta_i \sqrt{\frac{2}{\rho_i L_i \sigma_n^2}}\right) \end{aligned} \quad (20)$$

其中，$Q(\cdot)$ 标准正态分布的尾部概率函数。另外，检测的最佳阈值 θ_i^0 由 $P_{\mathrm{FA}i} = \varepsilon_{\mathrm{PFA}}$ 决定，可以得到 $\theta_i^0 = Q^{-1}\left(\varepsilon_{\mathrm{PFA}}\right)\sqrt{\frac{\rho_i L_i \sigma_n^2}{2}}$。由此，检测概率 PD 满足式（21）：

$$\begin{aligned} P_{\mathrm{D}i} &= \mathbb{P}\left\{\delta_i > \theta_i^0 \middle| H_1\right\} = Q\left(\frac{\theta_i^0 - \left|h_i\right|^2 \rho_i L_i \sqrt{\frac{\zeta P_A \tau_0}{\tau_i}}}{\sqrt{\mathrm{var}\left\{\delta_i \middle| H_1\right\}}}\right) \\ &= Q\left(Q^{-1}\left(\varepsilon_{\mathrm{PFA}}\right) - \left|h_i\right|^2 \sqrt{\frac{2\rho_i L_i \zeta P_A \tau_0}{\sigma_n^2 \tau_i}}\right) \end{aligned} \quad (21)$$

，当无法保证认证准确度时发生安全中断，安全中断概率 PSO 满足式（22）：

$$P_{\mathrm{SO}i} = \mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right) < \varepsilon_{\mathrm{PD}} \middle| \text{transmission of } U_i \text{ occurs}\right) \quad (22)$$

其中，ε_{PD} 是允许来自用户的传输下限，也即用户的认证准确度的下限。U_i 表示第 i 个用户。在这种情况下，能够判断无线能量传输通信网络的安全性。

在一些示例中，基于式（21）和式（22），安全中断概率 PSO 可以表示为：

$$P_{\mathrm{SO}i} = \begin{cases} 1 - \exp\left(\sqrt{\frac{2}{\bar{\gamma}_i}}\left(\sqrt{\varepsilon_{\mathrm{PT}}} - \frac{Q^{-1}\left(\varepsilon_{\mathrm{PFA}}\right) - Q^{-1}\left(\varepsilon_{\mathrm{PD}}\right)}{\sqrt{2\rho_i L_i}}\right)\right), & \sqrt{\varepsilon_{\mathrm{PT}}} < \frac{Q^{-1}\left(\varepsilon_{\mathrm{PFA}}\right) - Q^{-1}\left(\varepsilon_{\mathrm{PD}}\right)}{\sqrt{2\rho_i L_i}} \\ 0, & \text{otherwise} \end{cases} \quad (23)$$

另外，通过式（22）和式（23）分别得到安全中断概率的理论值和仿真值，均随着基站的瞬时信噪比的增大，呈递减趋势。

在步骤 S500 中，由于 WPCN 中的安全性和可靠性是相关的，因此定义一个新的概率即联合中断概率 PSCO，以综合评估无线能量传输通信网络的安全性和可靠性。基于连接中断概率和安全中断概率可以

计算联合中断概率。联合中断概率 PSCO 满足下式（24）：

$$P_{\mathrm{SCOi}}=1-\mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)\geq\varepsilon_{\mathrm{PD}},R_i\geq\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of }U_i\text{ occurs}\right)\quad(24)$$

由此，能够综合判断无线能量传输通信网络的安全性和可靠性。基于式（8）和式（23），联合中断概率 PSCO 可以表示为：

$$P_{\mathrm{SCOi}}=\begin{cases}P_{\mathrm{COi}}, & \left(Q^{-1}\left(\varepsilon_{\mathrm{PFA}}\right)-Q^{-1}\left(\varepsilon_{\mathrm{PD}}\right)\right)^2<\left(2^{\frac{\varepsilon_{\mathrm{PCO}}}{(1-\rho_i)\tau_i}}-1\right)2\rho_iL_i\\ & 0\leq\varepsilon_{\mathrm{PT}}<2^{\frac{\varepsilon_{\mathrm{PCO}}}{(1-\rho_i)\tau_i}}-1\\ P_{\mathrm{SOi}}, & \text{otherwise}\end{cases}\quad(25)$$

另外，通过式（24）和式（25）分别得到联合中断概率的理论值和仿真值，均随着基站的瞬时信噪比的增大，呈递减趋势。因此，基于第二吞吐量、传输概率和联合中断概率获得第二可信吞吐量。其中，第二吞吐量、传输概率和连接中断概率可以由步骤 S200 获得。每个用户的第二可信吞吐量η_i满足式（26）：$\eta_i=P_{\mathrm{T}i}\left(1-P_{\mathrm{SCOi}}\right)R_{J,i}$ (26)，由此，WPCN 的第二可信吞吐量η_{sum}可以表示为$\eta_{\mathrm{sum}}=\sum_{i=1}^{K}\eta_i$。在这种情况下，能够更准确评估无线能量传输通信网络的整体性能。另外，可以基于式（5）、式（15）和式（25）获得具体的第二可信吞吐量η_{sum}。例如，可以获得目标用户的第二可信吞吐量。

在一些示例中，如图 3 所示，加塞攻击防御方法还可以包括比较目标用户的第二可信吞吐量与系统要求的第二阈值，并比较目标用户的成本性能比与第三阈值，当第二可信吞吐量达到第二阈值时，且成本性能比达到第三阈值，基站对接收的目标用户的数据信号进行解码，目标用户的第二吞吐量计入总吞吐量，当第二可信吞吐量达不到第二阈值时，且成本性能比达不到第三阈值，基站对接收的目标用户的数据信号不进行解码，重新分配传输时间段，减小目标用户的对应的传输时间段，以降低目标用户对总吞吐量的影响来提高整个系统的安全性（步骤 S600）。

在步骤 S600 中，可以通过比较目标用户的第二可信吞吐量与系统要求的第二阈值ε_2，以及比较目标用户的成本性能比与第三阈值ε_3，预测攻击者的攻击行为。当第二可信吞吐量达不到第二阈值ε_2且成本性

能比达不到第三阈值ε_3时，用户受到攻击，即目标用户接收到干扰信号，基站对目标用户的数据信号不进行解码，重新分配传输时间段，减小目标用户的对应的传输时间段，当第二可信吞吐量达到第二阈值ε_2且成本性能比达到第三阈值ε_3时，用户没有受到攻击，用户没有接收到干扰信号，基站对接收的目标用户的数据信号进行解码，目标用户的第二吞吐量计入总吞吐量。在这种情况下，根据成本性能比和第二可信吞吐量，对不同情况下的用户采取相应的措施，以便更好的维护无线能量传输通信网络的整体性能。

下面结合图 4 至图 5 进行分析。图 4 至图 5 均分析单个用户的情况，基于单个用户的情况可以类比至所有用户的普遍情况。

图 4 是示出了本公开的示例所涉及的在不同能量传输时段的时间分配因子下的第一吞吐量、第二吞吐量和第二可信吞吐量的对比示意图。波形 A 代表第一吞吐量，波形 B 代表第二吞吐量，波形 C 代表第二可信吞吐量。如题 4 所示，在$\rho_1 = 0.1$、$\overline{\beta}_1 = 20\,\mathrm{dB}$、$P_{J,1} = 0.1\,\mathrm{W}$和$\sigma_J^2 = 0.1$的条件下，第二吞吐量和第二可信吞吐量相对于第一吞吐量显然下降。点 M 代表第一吞吐量最大化的情况。当$\tau_0 < \tau_0^*$时，第一吞吐量随着能量传输时段的时间分配因子τ_0的增加而增加。当$\tau_0 \geq \tau_0^*$时，第一吞吐量随着τ_0的增加而下降。其中τ_0^*代表点 M 对应的横坐标。

图 5 是示出了本公开的示例所涉及的在不同能量传输时段的时间分配因子下的成本性能比波形示意图。点 M 代表成本性能比最大化的情况。与图 4 类似，图 5 的成本性能比也是关于不同能量传输时段的时间分配因子的凸函数。图 4 中第一吞吐量最大化的点 M 与图 5 中成本性能比最大化的点 N 相比，无线能量传输通信网络的成本性能比（点 N）更能准确防御到攻击者的攻击行为。也即点 N 对应的用户更容易收到攻击者的攻击。由此，可以调节点 N 对应的目标用户的安全阈值$\varepsilon_{\mathrm{PD}}$，以增强目标用户的安全性要求，从而降低目标用户对总吞吐量的贡献。

图 6 是示出了本公开的示例所涉及的无线能量传输通信网络的加塞攻击防御系统的结构示意图。无线能量传输通信网络的加塞攻击防御系统可以是包括发射装置、接收装置和攻击装置的无线能量传输通信网络的加塞攻击防御系统。本公开中的发射装置和基站可以是相同

的概念，接收装置和用户可以是相同的概念。攻击装置和攻击者可以是相同的概念。

在一些示例中，如图 6 所示，无线能量传输通信网络的加塞攻击防御系统 1（有时简称加塞攻击防御系统 1）可以包括发射装置 10（例如 CDMA 中的基站）、用户装置 20（例如移动电话）和攻击装置 30（例如个人计算机）。发射装置 10 可以用于进行信道估计。基于上述步骤 S100 可知，发射装置 10 在时段 $\tau_a T$ 内完成信道估计。发射装置 10 还可以基于信道估计，计算第一吞吐量、传输概率和连接中断概率，以获得第一可信吞吐量。第一吞吐量、传输概率、连接中断概率和第一可信吞吐量的计算方法可以类比步骤 S100 中相应的计算方法。

在另一些示例中，发射装置 10 还可以基于信道估计为多个用户装置 20 分配对应的传输时间段，并将分配结果通过广播形式通知用户装置 20。具体而言，在 $\tau_b T$ 内，发射装置 10 基于信道估计的结果，分配 WET 和 WIT 的时间。

在一些示例中，用户装置 20 可以用于接收能量信号，并将能量信号转化为发射能量，每个用户装置 20 在相应的传输时间段内向发射装置 10 发射数据信号。每个用户装置 20 接收的能量信号和数据信号可以参见步骤 S300 中的计算方法。

在一些示例中，攻击装置 30 可以用于在发射装置 10 向用户装置 20 广播分配结果过程中，监听并选择传输时间段最长的用户装置 20 作为目标用户装置 20，基于目标用户装置 20 的传输时间段设置预设干扰功率。攻击装置 30 可以在目标用户装置 20 发射数据信号时，发射具有预设干扰功率的干扰信号。$P_{J,i}$ 为预设干扰功率。$P_{J,1}$ 可以看做攻击装置 30 攻击用户装置 20 的能力。干扰信号满足 $j_i \sim \mathcal{CN}\left(0, P_{J,i}\right)$，攻击装置 30 可以用于向发射装置 10 发射具有预设干扰功率的干扰信号。

在一些示例中，发射装置 10 接收数据信号，计算目标用户装置 20 的第二吞吐量，并基于预设干扰功率、第一吞吐量和第二吞吐量，计算目标用户装置 20 的成本性能比。第二吞吐量和成本性能比的计算方法可以类比步骤 S500 中相应的计算方法。发射装置 10 根据数据信号计算安全中断概率，基于连接中断概率和安全中断概率计算联合中断

概率，基于第二吞吐量、传输概率、联合中断概率，计算目标用户装置 20 的第二可信吞吐量。安全中断概率和第二可信吞吐量可以参见步骤 S500 中相应的计算方法。

在一些示例中，发射装置 10 比较目标用户装置 20 的第二可信吞吐量与系统要求的第二阈值，并比较目标用户装置 20 的成本性能比与第三阈值，以进行攻击预测，当第二可信吞吐量达不到第二阈值时，且成本性能比达不到第三阈值，发射装置 10 对接收的目标用户装置 20 的数据信号不进行解码，重新分配传输时间段，减小目标用户装置 20 的对应的传输时间段，以降低目标用户装置 20 对总吞吐量的影响来提高整个系统的安全性。当第二可信吞吐量达到第二阈值时，且成本性能比达到第三阈值，发射装置 10 对接收的目标用户装置 20 的数据信号进行解码，目标用户装置 20 的第二吞吐量计入总吞吐量。

虽然以上结合附图和实施例对本公开进行了具体说明，但是可以理解，上述说明不以任何形式限制本公开。本领域技术人员在不偏离本公开的实质精神和范围的情况下可以根据需要对本公开进行变形和变化，这些变形和变化均落入本公开的范围内。

权 利 要 求 书

1.一种无线能量传输通信网络的加塞攻击防御方法，是包含基站、用户和会发射干扰信号的攻击者的无线能量传输通信网络系统的加塞攻击防御方法，其特征在于，

包括：

所述用户向所述基站发送登录请求信号，所述基站进行信道估计，基于所述信道估计为多个所述用户分配对应的传输时间段，并将分配结果通过广播形式通知所述用户，基于所述信道估计，计算第一吞吐量、传输概率和连接中断概率，基于所述吞吐量、所述传输概率和所述连接中断概率，计算第一可信吞吐量；

在所述基站向所述用户广播分配结果过程中，所述攻击者监听并选择传输时间段最长的用户作为目标用户，基于所述目标用户的传输时间段设置预设干扰功率；

当所述第一可信吞吐量达到系统要求的第一阈值时，所述基站向所述用户广播能量信号，所述用户接收所述能量信号，并将所述能量信号转化为发射能量，每个所述用户在相应的传输时间段内向所述基站发射数据信号；

在所述目标用户发射数据信号时，所述攻击者发射具有所述预设干扰功率的干扰信号；所述基站接收所述数据信号，计算所述目标用户的第二吞吐量，并基于所述预设干扰功率、所述第一吞吐量和所述第二吞吐量，计算所述目标用户的成本性能比，并根据所述数据信号计算安全中断概率，基于所述连接中断概率和所述安全中断概率计算联合中断概率，基于所述第二吞吐量、所述传输概率、所述联合中断概率，计算所述目标用户的第二可信吞吐量；并且

比较所述目标用户的第二可信吞吐量与系统要求的第二阈值，并比较所述目标用户的成本性能比与第三阈值，当所述第二可信吞吐量达到所述第二阈值时，且成本性能比达到所述第三阈值，所述基站对接收的所述目标用户的数据信号进行解码，所述目标用户的第二吞吐量计入总吞吐量，当所述第二可信吞吐量达不到所述第二阈值时，且成本性能比达不到所述第三阈值，所述基站对接收的所述目标用户的数据信号不进行解码，重新分配传输时间段，减小所述目标用户的对应的传输时间段，以降低所述目标用户对总吞吐量的影响来提高整个系统的安全性。

2.根据权利要求 1 所述的加塞攻击防御方法，其特征在于，

每个所述用户的第一吞吐量由下式（Ⅰ）计算得到：

$R_i=(1-\rho_i)\tau_i\log_2(1+\gamma_i)$ （Ⅰ），

每个所述用户的第二吞吐量由下式（Ⅱ）计算得到：

$R_{J,i}=(1-\rho_i)\tau_i\log_2(1+\gamma_{J,i})$ （Ⅱ），

其中，R_i表示第 i 个用户的第一吞吐量，$R_{J,i}$表示第 i 个用户的第二吞吐量，ρ_i表示安全分配因子，τ_i表示第 i 个用户对应的传输时间段的时间分配因子，γ_i表示在所述基站接收到的瞬时信噪比，$\gamma_{J,i}$表示在接收所述干扰信号后所述基站接收到的瞬时信噪比。

3.根据权利要求 1 所述的加塞攻击防御方法，其特征在于，

所述成本性能比λ_i由下式（Ⅲ）计算得到：

$$\lambda_i=\frac{R_i-R_{J,i}}{P_{J,i}}$$ （Ⅲ），

其中，R_i表示第 i 个用户的第一吞吐量，$R_{J,i}$表示第 i 个用户的第二吞吐量，$P_{J,i}$表示所述干扰信号的发射功率。

4.根据权利要求 1 所述的加塞攻击防御方法，其特征在于，

所述安全中断概率由下式（Ⅳ）计算得到：

$P_{\mathrm{SOi}}=\mathbb{P}\left(P_{\mathrm{Di}}\left(P_{\mathrm{FA}i}\right)<\varepsilon_{\mathrm{PD}}\middle|\text{transmission of }U_i\text{ occurs}\right)$ （Ⅳ），

所述连接中断概率由下式（Ⅴ）计算得到：

$P_{\mathrm{COi}}=\mathbb{P}\left(R_i<\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of }U_i\text{ occurs}\right)$ （Ⅴ），

其中，PD 表示检测概率，PFA 表示虚警概率，$\varepsilon_{\mathrm{PD}}$表示用户的安全阈值，$\varepsilon_{\mathrm{PCO}}$表示通信速率的下限，$R_i$表示第 i 个用户的第一吞吐量，$U_i$表示第 i 个用户。

5.根据权利要求 1 所述的加塞攻击防御方法，其特征在于，

所述第一可信吞吐量满足下式（Ⅵ）：

$\eta_i=P_{\mathrm{Ti}}(1-P_{\mathrm{COi}})R_i$ （Ⅵ），

所述第二可信吞吐量满足下式（Ⅶ）：

$\eta_i = P_{\mathrm{Ti}}\left(1-P_{\mathrm{SCOi}}\right)R_{J,i}$ (Ⅶ)，

其中，$P_{\mathrm{Ti}} = \mathbb{P}\left(\text{transmission of } U_i \text{ occurs}\right)$，PT 表示所述传输概率，PCO 表示所述连接中断概率，R_i表示第 i 个用户的第一吞吐量，$R_{J,i}$表示第 i 个用户的第二吞吐量，PSCO 表示联合中断概率，且满足 $P_{\mathrm{SCOi}} = 1-\mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)\geq\varepsilon_{\mathrm{PD}}, R_i\geq\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of } U_i \text{ occurs}\right)$ 。

6.一种无线能量传输通信网络的加塞攻击防御系统，是包含发射装置、接收装置和攻击装置的无线能量传输通信网络的加塞攻击防御系统，其特征在于，

包括：

所述发射装置，其用于在所述用户装置向所述发射装置发送登录请求信号后，进行信道估计，基于所述信道估计为多个所述用户装置分配对应的传输时间段，并将分配结果通过广播形式通知所述用户装置，并基于所述信道估计，计算第一吞吐量、传输概率和连接中断概率，以获得第一可信吞吐量，当所述第一可信吞吐量达到系统要求的第一阈值时，所述发射装置向所述用户装置广播能量信号；

所述用户装置，其用于接收所述能量信号，并将所述能量信号转化为发射能量，每个所述用户装置在相应的传输时间段内向所述发射装置发射数据信号；

所述攻击装置，其用于在所述发射装置向所述用户装置广播分配结果过程中，监听并选择传输时间段最长的用户装置作为目标用户装置，基于所述目标用户装置的传输时间段设置预设干扰功率，在所述目标用户装置发射数据信号时，发射具有所述预设干扰功率的干扰信号；

其中，所述发射装置接收所述数据信号，计算所述目标用户装置的第二吞吐量，并基于所述预设干扰功率、所述第一吞吐量和所述第二吞吐量，计算所述目标用户装置的成本性能比，并根据所述数据信号计算安全中断概率，基于所述连接中断概率和所述安全中断概率计算联合中断概率，基于所述第二吞吐量、所述传输概率、所述联合中断概率，计算所述目标用户装置的第二可信吞吐量，比较所述目标用户装置的第二可信吞吐量与系统要求的第二阈值，并比较所述目标用户装置的第二可信吞吐量与系统要求的第二阈值，并比较所述目标用户装置的成本性能比与第三阈值，当所述第二可信吞吐量达到所述第二阈值时，且成本性能比达到所述第三阈值，所述发射装置对接收的所述目标用户

装置的数据信号进行解码，所述目标用户装置的第二吞吐量计入总吞吐量，当所述第二可信吞吐量达不到所述第二阈值时，且成本性能比达不到所述第三阈值，所述发射装置对接收的所述目标用户装置的数据信号不进行解码，重新分配传输时间段，减小所述目标用户装置的对应的传输时间段，以降低所述目标用户装置对总吞吐量的影响来提高整个系统的安全性。

7.根据权利要求 6 所述的加塞攻击防御系统，其特征在于，

每个所述用户装置的第一吞吐量由下式（Ⅰ）计算得到：

$$R_i=(1-\rho_i)\tau_i\log_2(1+\gamma_i) \quad (Ⅰ),$$

每个所述用户装置的第二吞吐量由下式（Ⅱ）计算得到：

$$R_{J,i}=(1-\rho_i)\tau_i\log_2(1+\gamma_{J,i}) \quad (Ⅱ),$$

其中，R_i表示第 i 个用户装置的第一吞吐量，$R_{J,i}$表示第 i 个用户装置的第二吞吐量，ρ_i表示安全分配因子，τ_i表示第 i 个用户装置对应的传输时间段的时间分配因子，γ_i表示在所述发射装置接收到的瞬时信噪比，$\gamma_{J,i}$表示在接收所述干扰信号后所述发射装置接收到的瞬时信噪比。

8.根据权利要求 6 所述的加塞攻击防御系统，其特征在于，

所述成本性能比λ_i由下式（Ⅲ）计算得到：

$$\lambda_i=\frac{R_i-R_{J,i}}{P_{J,i}} \quad (Ⅲ),$$

其中，R_i表示第 i 个接收装置的第一吞吐量，$R_{J,i}$表示第 i 个接收装置的第二吞吐量，$P_{J,i}$表示所述干扰信号的发射功率。

9.根据权利要求 6 所述的加塞攻击防御系统，其特征在于，

所述安全中断概率由下式（Ⅳ）计算得到：

$$P_{\mathrm{SOi}}=\mathbb{P}\left(P_{\mathrm{Di}}\left(P_{\mathrm{FA}i}\right)<\varepsilon_{\mathrm{PD}}\middle|\text{transmission of } U_i \text{ occurs}\right) \quad (Ⅳ),$$

所述连接中断概率由下式（Ⅴ）计算得到：

$$P_{\mathrm{COi}}=\mathbb{P}\left(R_i<\varepsilon_{\mathrm{PCO}}\middle|\text{transmission of } U_i \text{ occurs}\right) \quad (Ⅴ),$$

其中，PD 表示检测概率，PFA 表示虚警概率，$\varepsilon_{\mathrm{PD}}$表示用户装置的安全阈值，$\varepsilon_{\mathrm{PCO}}$表示通信速率的下限，$R_i$表示第 i 个用户装置的第一吞吐量，$U_i$表示

第 i 个用户装置。

10.根据权利要求 6 所述的加塞攻击防御系统，其特征在于，

所述第一可信吞吐量满足下式（Ⅵ）：

$\eta_i = P_{\mathrm{Ti}}\left(1-P_{\mathrm{COi}}\right)R_i$ （Ⅵ），

所述第二可信吞吐量满足下式（Ⅶ）：

$\eta_i = P_{\mathrm{Ti}}\left(1-P_{\mathrm{SCOi}}\right)R_{J,i}$ （Ⅶ），

其中，$P_{\mathrm{Ti}} = \mathbb{P}\left(\text{transmission of } U_i \text{ occurs}\right)$，PT 表示所述传输概率，PCO 表示所述连接中断概率，R_i表示第 i 个用户装置的第一吞吐量，$R_{J,i}$表示第 i 个用户装置的第二吞吐量，PSCO 表示联合中断概率，且满足 $P_{\mathrm{SCOi}} = 1-\mathbb{P}\left(P_{\mathrm{D}i}\left(P_{\mathrm{FA}i}\right)\geq \varepsilon_{\mathrm{PD}}, R_i \geq \varepsilon_{\mathrm{PCO}} \middle| \text{transmission of } U_i \text{ occurs}\right)$ 。

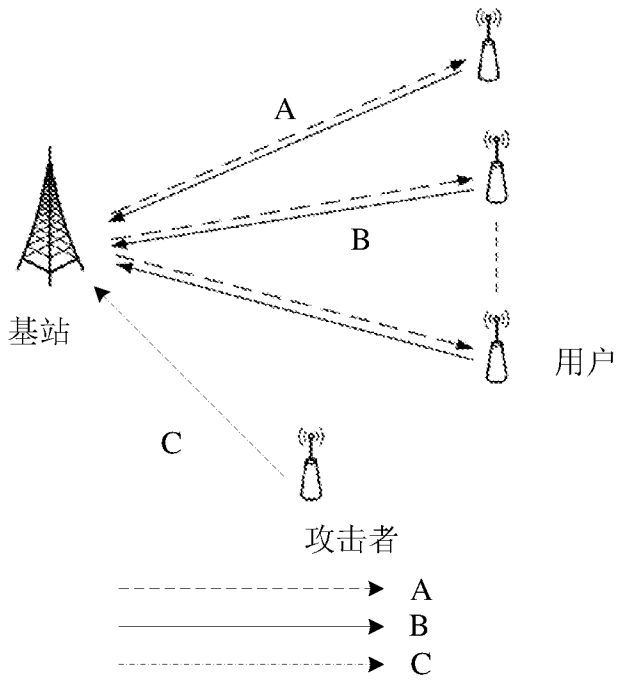
A
B
C
基站
用户
攻击者
A
B
C

图 1

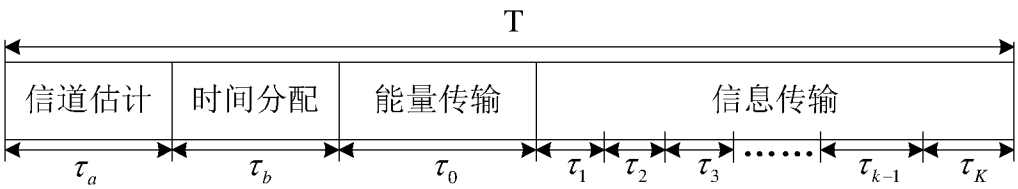
T
信道估计
时间分配
能量传输
信息传输
τ_a
τ_b
τ_0
τ_1
τ_2
τ_3
τ_{k-1}
τ_K

图 2

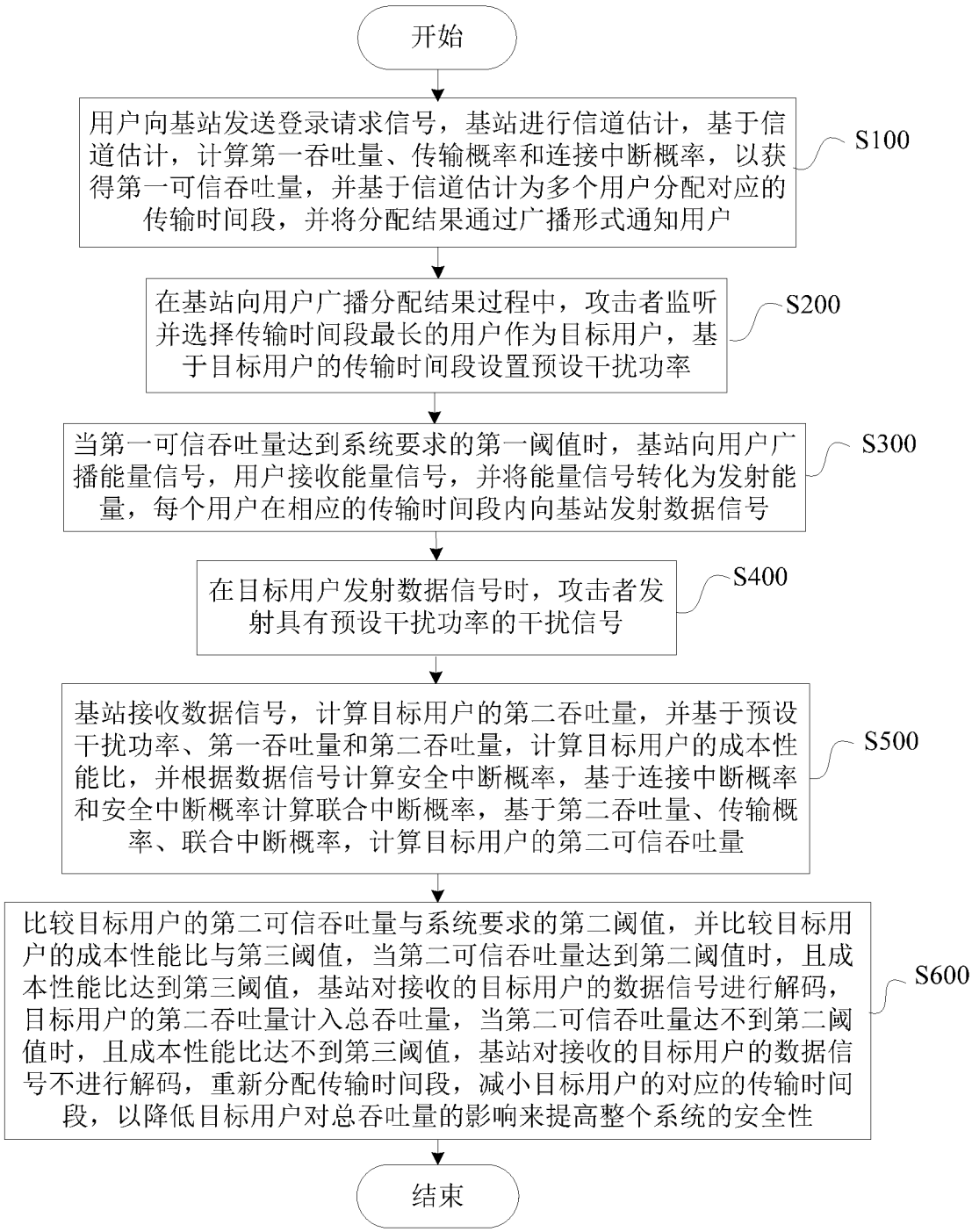
开始
用户向基站发送登录请求信号，基站进行信道估计，基于信道估计，计算第一吞吐量、传输概率和连接中断概率，以获得第一可信吞吐量，并基于信道估计为多个用户分配对应的传输时间段，并将分配结果通过广播形式通知用户
S100
在基站向用户广播分配结果过程中，攻击者监听并选择传输时间段最长的用户作为目标用户，基于目标用户的传输时间段设置预设干扰功率
S200
当第一可信吞吐量达到系统要求的第一阈值时，基站向用户广播能量信号，用户接收能量信号，并将能量信号转化为发射能量，每个用户在相应的传输时间段内向基站发射数据信号
S300
在目标用户发射数据信号时，攻击者发射具有预设干扰功率的干扰信号
S400
基站接收数据信号，计算目标用户的第二吞吐量，并基于预设干扰功率、第一吞吐量和第二吞吐量，计算目标用户的成本性能比，并根据数据信号计算安全中断概率，基于连接中断概率和安全中断概率计算联合中断概率，基于第二吞吐量、传输概率、联合中断概率，计算目标用户的第二可信吞吐量
S500
比较目标用户的第二可信吞吐量与系统要求的第二阈值，并比较目标用户的成本性能比与第三阈值，当第二可信吞吐量达到第二阈值时，且成本性能比达到第三阈值，基站对接收的目标用户的数据信号进行解码，目标用户的第二吞吐量计入总吞吐量，当第二可信吞吐量达不到第二阈值时，且成本性能比达不到第三阈值，基站对接收的目标用户的数据信号不进行解码，重新分配传输时间段，减小目标用户的对应的传输时间段，以降低目标用户对总吞吐量的影响来提高整个系统的安全性
S600
结束

图 3

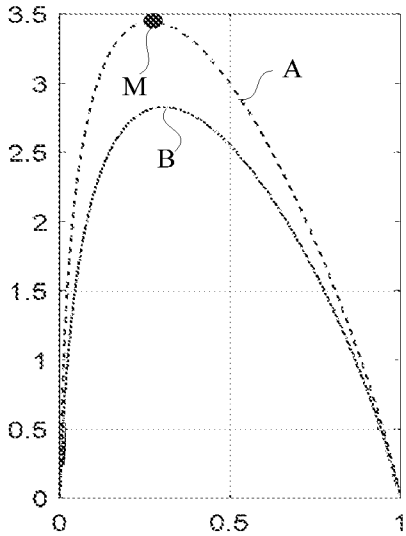
3.5
3
2.5
2
1.5
1
0.5
0
0
0.5
1
M
A
B
能量传输时段的时间分配因子

图 4

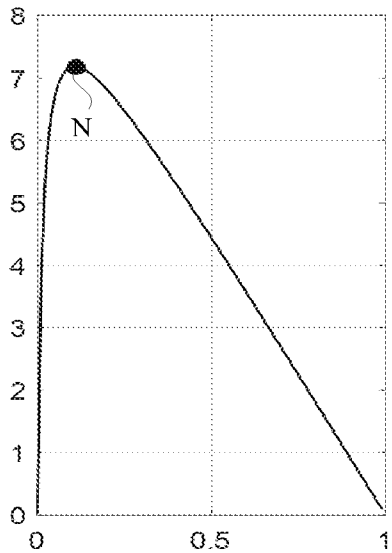
8
7
6
5
4
3
2
1
0
0
0.5
1
N
能量传输时段的时间分配因子

图 5

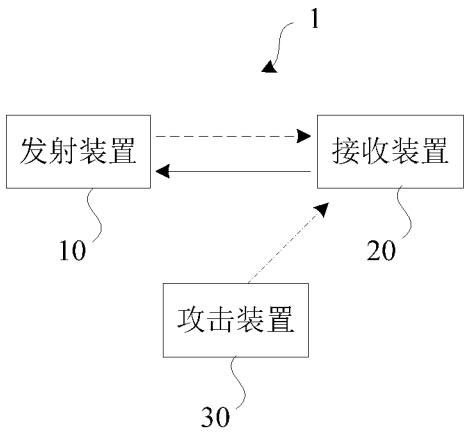
1
发射装置
接收装置
10
20
攻击装置
30

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/108439

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00(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)

H04W; H04Q; H04L

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

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

CNPAT, CNKI, WPI, EPODOC: 基站, 接入设备, 基地台, 网络侧, 概率, 可信吞吐, 可信吞吐量, 吞吐, 干扰, 攻击, 加塞攻击, 分配, 信道估计, 加塞攻击, BS, enb, enodeb, bts, nodeb, throughput, probability, interference, attack, allocat+, estimat+, channel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 106130935 A (XI'AN JIAOTONG UNIVERSITY) 16 November 2016 (2016-11-16) claim 1	1-10
A	CN 102223637 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 19 October 2011 (2011-10-19) entire document	1-10
A	US 2014241196 A1 (APPLE INC.) 28 August 2014 (2014-08-28) entire document	1-10
A	WO 2016181861 A1 (SHARP KABUSHIKIKAISHA) 17 November 2016 (2016-11-17) entire document	1-10

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 May 2019	**29 May 2019**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/108439

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106130935	A	16 November 2016	None			
CN	102223637	A	19 October 2011	None			
US	2014241196	A1	28 August 2014	EP	2803145	A1	19 November 2014
				CN	104126278	A	29 October 2014
				US	2013258877	A1	03 October 2013
				JP	2015511475	A	16 April 2015
				JP	2016213872	A	15 December 2016
				KR	20140132715	A	18 November 2014
				TW	201345219	A	01 November 2013
				WO	2013148514	A1	03 October 2013
WO	2016181861	A1	17 November 2016	JP	2018107483	A	05 July 2018

国际检索报告

国际申请号
PCT/CN2018/108439

A. 主题的分类

H04W 12/00(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)

H04W; H04Q; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC:基站，接入设备，基地台，网络侧，概率，可信吞吐，可信吞吐量,吞吐，干扰，攻击，加塞攻击，分配，信道估计，加塞攻击，BS,enb，enodeb，bts,nodeb，throughput，probability， interference, attack, allocat+, estimat+,channel

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 106130935 A (西安交通大学) 2016年 11月 16日 (2016-11-16) 权利要求1	1-10
A	CN 102223637 A (北京邮电大学) 2011年 10月 19日 (2011-10-19) 全文	1-10
A	US 2014241196 A1 (APPLE INC.) 2014年 8月 28日 (2014-08-28) 全文	1-10
A	WO 2016181861 A1 (SHARP KABUSHIKIKAISHA) 2016年 11月 17日 (2016-11-17) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 5月 15日	2019年 5月 29日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	姚雅倩
传真号 (86-10)62019451	电话号码 86-(10)-53961604

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/108439

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	106130935	A	2016年 11月 16日	无			
CN	102223637	A	2011年 10月 19日	无			
US	2014241196	A1	2014年 8月 28日	EP	2803145	A1	2014年 11月 19日
				CN	104126278	A	2014年 10月 29日
				US	2013258877	A1	2013年 10月 3日
				JP	2015511475	A	2015年 4月 16日
				JP	2016213872	A	2016年 12月 15日
				KR	20140132715	A	2014年 11月 18日
				TW	201345219	A	2013年 11月 1日
				WO	2013148514	A1	2013年 10月 3日
WO	2016181861	A1	2016年 11月 17日	JP	2018107483	A	2018年 7月 5日