



(51) International Patent Classification:
H04B 5/02 (2006.01)

(21) International Application Number:
PCT/US2013/056853

(22) International Filing Date:
27 August 2013 (27.08.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/693,622 27 August 2012 (27.08.2012) US
14/010,650 27 August 2013 (27.08.2013) US

(71) Applicants: UNIVERSITY OF HOUSTON SYSTEM [US/US]; 316 E. Cullen Building, Houston, TX 77204-2015 (US). TRUSTEES OF PRINCETON UNIVERSITY [US/US]; P.O. Box 36, Princeton University, Princeton, NJ 08544 (US). UNIVERSITY OF MIAMI [US/US]; 1400 N.W. 10th Ave. Suite 1200, Miami, FL 33136 (US).

(72) Inventors; and

(71) Applicants : HAN, Zhu [US/US]; 1207 Amhearst Dr., Sugar Land, TX 77479 (US). SAAD, Walid [US/US]; 1527 Corniche Ave, Coral Gables, FL 33146 (US). POOR,

Harold [US/US]; 59 Hardy Drive, Princeton, NJ 08540 (US).

(74) Agents: WILSON, David, M. et al.; Conley Rose, P.C., PO BOX 3267, Houston, TX 77253-3267 (US).

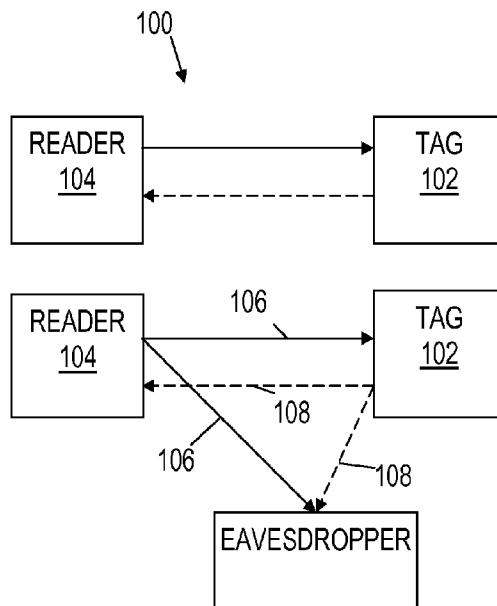
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING BACKSCATTER WIRELESS COMMUNICATION

FIG. 1



(57) Abstract: A system and method for securing backscatter communication. In one embodiment, a backscatter communication system includes a reader. The reader is configured to receive backscatter transmissions. The reader includes a transmitter configured to emit a radio frequency signal to induce backscatter communication. The transmitter includes a continuous wave (CW) carrier signal generator and a noise signal generator. The CW carrier signal generator produces a CW carrier signal. The noise signal generator generates a noise signal. The transmitter is configured to combine the CW carrier signal and the noise signal, and to transmit the combined signal to induce backscatter communication.

WO 2014/036001 A1

Published:

— *with international search report (Art. 21(3))*

SYSTEM AND METHOD FOR SECURING BACKSCATTER WIRELESS COMMUNICATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims priority to U.S. Provisional Patent Application No. 61/693,622, filed on August 27, 2012, entitled "A Method for Securing Backscatter Wireless Communication," which is hereby incorporated herein by reference in its entirety.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] This invention was made with government support under Grant No. N00014-12-1-0767 awarded by the Office of Naval Research. The government has certain rights in this invention.

BACKGROUND

[0003] Backscatter communication is a wireless transmission technique that is used in some short-range, wireless communication systems. In particular, backscatter-based radio frequency identification (RFID) is a wireless technology that allows interconnection of physical objects through the use of small, inexpensive integrated circuits, i.e., RFID tags, that are remotely powered by a wireless RFID reader. Recent advances in backscatter systems, such as the emergence of sensor equipped, semi-passive RFID tags have positioned backscatter technology to provide the physical world with cyber-capabilities such as computation and communication.

SUMMARY

[0004] A system and method for securing backscatter communication are disclosed herein. In one embodiment, a backscatter communication system includes a reader. The reader is configured to receive backscatter transmissions. The reader includes a transmitter configured to emit a radio frequency signal to induce backscatter

communication. The transmitter includes a continuous wave (CW) carrier signal generator and a noise signal generator. The CW carrier signal generator produces a CW carrier signal. The noise signal generator generates a noise signal. The transmitter is configured to combine the CW carrier signal and the noise signal, and to transmit the combined signal to induce backscatter communication.

[0005] In another embodiment, a method for backscatter communication includes generating a CW carrier signal, and generating a noise signal. The CW carrier signal and the noise signal are combined, and the combined signal is transmitted. A backscatter transmission induced by the combined signal is received. Information encoded in the backscatter transmission is extracted by filtering the noise signal from the backscatter transmission.

[0006] In a further embodiment, a radio frequency identification (RFID) reader includes a power allocation subsystem and a transmitter. The power allocation subsystem is configured to determine an amount of power to be allocated to transmission of each of a CW carrier signal and a noise signal. The transmitter is configured to combine the CW carrier signal and noise signal and to emit the combined signal to induce backscatter communication by an RFID tag.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] For a detailed description of various examples, reference will now be made to the accompanying drawings in which:

[0008] Figure 1 shows a block diagram of a radio frequency identification (RFID) communication system in accordance with principles disclosed herein;

[0009] Figure 2 shows a block diagram of an RFID reader in accordance with principles disclosed herein;

[0010] Figure 3 shows a flow diagram for a method for backscatter communication with optimized secrecy rate in accordance with principles disclosed herein;

[0011] Figure 4 shows a graph comparing secrecy rate of a conventional system and a system in accordance with principles disclosed herein; and

[0012] Figure 5 shows a graph showing the number of iterations applied to reach a Nash equilibrium in accordance with principles disclosed herein.

NOTATION AND NOMENCLATURE

[0013] Certain terms are used throughout the following description and claims to refer to particular system components. As one skilled in the art will appreciate, companies may refer to a component by different names. This document does not intend to distinguish between components that differ in name but not function. In the following discussion and in the claims, the terms “including” and “comprising” are used in an open-ended fashion, and thus should be interpreted to mean “including, but not limited to” Also, the term “couple” or “couples” is intended to mean either an indirect or direct electrical connection. Thus, if a first device couples to a second device, that connection may be through a direct electrical connection, or through an indirect electrical connection via other devices and connections. The recitation “based on” is intended to mean “based at least in part on.” Therefore, if X is based on Y, X may be based on Y and any number of other factors.

DETAILED DESCRIPTION

[0014] The following discussion is directed to various embodiments of the invention. Although one or more of these embodiments may be preferred, the embodiments disclosed should not be interpreted, or otherwise used, as limiting the scope of the disclosure, including the claims. In addition, one skilled in the art will understand that the following description has broad application, and the discussion of any embodiment is meant only to be exemplary of that embodiment, and not intended to intimate that the scope of the disclosure, including the claims, is limited to that embodiment.

[0015] Deployment of large-scale backscatter communication systems, such as radio frequency identification (RFID) based systems, faces a variety of challenges. In particular, securing such systems is a key issue because attacks on the system, e.g., eavesdropping the transmitted data, can lead not only to data interception but also to serious privacy breaches such as owner tracking or identity modification. Cost, size, and computational limitations make securing RFID systems difficult. Due to these limitations,

the implementation of classical cryptographic techniques in small scale backscatter systems, such as RFID systems, is infeasible in practice.

[0016] Conventional RFID security solutions are generally based on lightweight cryptography, a scaled-down version of standard cryptography. Lightweight cryptography provides security against some attacks, but exhibits serious vulnerabilities. Beyond lightweight cryptographic techniques, attempts to implement basic cryptographic schemes, such as the RC5 algorithm, on RFID tags have proven feasible only at very short ranges (e.g., 0.75 meters) and by using prototype tags which possess higher storage and computational power than state-of-the-art electronic product code UHF tags.

[0017] Embodiments of the present disclosure include a novel low-complexity security solution that is tailored to the resource-constrained nature of backscatter communication systems. Embodiments advantageously employ physical layer (PHY) security mechanisms that apply wireless channel characteristics such as fading and noise, traditionally seen as impediments, for defending wireless transmission against eavesdropping. Accordingly, the backscatter communication techniques disclosed herein provide security without the need for secret key generation or other computationally complex aspects of standard cryptography.

[0018] Embodiments optimize the secrecy rate of RFID systems by exploiting two key features of the RFID backscatter channel: (i) the nature of the backscatter channel in which the signal transmitted by the RFID reader is modulated and relayed by the RFID tag to the reader; and (ii) the presence of a signal continuously transmitted by the RFID reader for powering the RFID tag during communication. In the communication system disclosed herein, RFID readers append artificial noise signals to the continuous wave signals that propagate via the backscatter channel thereby inducing interference at eavesdroppers. Each reader optimizes the allocation of power between the continuous wave signal and the artificial noise signal. The readers determine an optimal power allocation so as to maximize the overall secrecy rates. The secrecy rate represents the maximum rate with which the reader and tag can communicate without being tapped by an eavesdropper.

[0019] Some embodiments determine the power allocation as a noncooperative continuous-kernel game. The game may use a best-response based algorithm via which the readers find Nash equilibrium of the game. By using artificial noise combined with the aforementioned game, embodiments yield significant performance gains in terms of the average secrecy rate per reader.

[0020] Figure 1 shows a block diagram of an RFID communication system 100 in accordance with principles disclosed herein. The system includes a plurality of RFID tags 102 and a plurality of RFID tag readers 104. In practice the system 100 may include one or more RFID tags 102 and/or one or more RFID tag readers 104. One or more eavesdroppers (eavesdropping devices) may be present to intercept communication between the RFID tags 102 and the RFID tag readers 104.

[0021] In the system 100, communication between reader 104 and the tag 102 occurs over a backscatter channel. The RFID reader 104 transmits a modulated signal by amplitude modulation of a continuous wave (CW) carrier signal. The carrier signal induces an RF voltage across an antenna of the tag 102. The induced voltage is used to power the tag 102. The tag 102 transmits information to the reader 104 by controlling the amount of backscatter of the impinging downlink signal. In other words, the tag 102 does not generate its own signal, but rather appends its information by modulating the downlink signal which is subsequently "backscattered" to the reader 104. Mutual interference between tags communicating with a common reader may be mitigated by an anti-collision medium access control (MAC) protocol. The RFID tag 102 may be any wireless device that transmits information via backscattering, the RFID reader 104 may be any wireless device that is configured to power the tag 102 via CW carrier signal and receive the data transmitted by the tag 102 via backscatter transmission.

[0022] In the system 100, the signal 106 transmitted by the reader 104 includes a noise signal that is unknown to an eavesdropper. The noise signal induces interference in the eavesdropper, thereby obfuscating the backscatter transmission 108 from the tag 102, and advantageously increasing the secrecy rate of the system 100.

[0023] In an RFID communication channel, the signal backscattered by a tag $k \in K_i$ toward the receive antenna of a reader i is given by:

$$y_{k,j}(t) = h_{k,i}s_k(t)h_{i,k}x_i(t) + \sum_{j \in N, j \neq i} h_{j,i}x_j(t) + n_i(t) \quad (1)$$

where:

$x_i(t)$ is the CW signal transmitted by reader i ;

$s_k(t)$ is the reflection coefficient of the tag,

$h_{k,i}$ and $h_{i,k}$ are, respectively, the tag-reader and reader-tag channel gains,

$h_{j,i}$ is the channel gain between reader i and reader j , and

$n_i(t)$ is the noise.

[0024] In conventional backscatter system operation, reader i knows the CW signal $x_j(t)$ transmitted by neighboring readers (the signal is a standardized UHF carrier signal) and, hence, reader i is able to cancel the third term in equation (1) using known signal processing techniques.

[0025] Using the Friis equation to link the transmit and received powers, for any reader $i \in N$ having a transmit power P_i , the received power following the backscatter by a tag k is given by:

$$P_{i,k}^{\alpha} = P_i \Gamma_k G_{i,k}^2 G_k^2 \left(\frac{\lambda}{4\pi d_{i,k}} \right)^4 \quad (2)$$

where:

$\Gamma_k = |s_k(t)|^2$ is the backscatter transmission loss;

$G_{i,k}$ is the antenna gain of reader i for the signal perceived at tag k ;

G_k is the antenna gain of tag k ;

λ is the wavelength; and

$d_{i,k}$ is the distance between reader i and tag k .

[0026] During backscatter communication, each reader i continuously transmits its CW signal $x_i(t)$ to power the tag circuits. Therefore, at any eavesdropper $m \in M$, the

received signal pertaining to the backscatter communication between a reader $i \in N$ and a tag $k \in K_i$ is given by:

$$y_{k,i,m}(t) = h_{k,m} s_k(t) h_{i,k} x_i(t) + \sum_{j \in N} h_{j,m} x_j(t) + n_m(t) \quad (3)$$

where $h_{k,m}$ and $h_{j,m}$ represent, respectively, the tag-eavesdropper and reader-eavesdropper channels.

[0027] The second term of equation (3) corresponds to the CW signal transmitted on the forward reader-tag links, and constitutes a potential interference at the eavesdropper. However, in conventional RFID systems, the eavesdropper knows the CW $x_j(t)$ transmitted by any reader $j \in N$ and is able to cancel the effect of the term

$$\sum_{j \in N} h_{j,m} x_j(t).$$

[0028] In accordance with the Friis equation, the received power at eavesdropper m , following the backscatter communication between reader i and tag k is given by:

$$P_{i,k,m}^{\alpha} = P_i \Gamma_k G_{i,m} G_m G_k^2 \left(\frac{\lambda}{4\pi d_{i,k}} \right)^2 \left(\frac{\lambda}{4\pi d_{k,m}} \right)^2 \quad (4)$$

where:

$G_{i,m}$ is the reader's antenna gain for the signal received at the eavesdropper m ;

G_m is the antenna gain of eavesdropper m ; and

$d_{k,m}$ is the distance between tag k and eavesdropper m .

[0029] The physical layer security of the RFID system characterized by the secrecy rate $C_{i,k}$ achieved during the backscatter communication between reader i and tag k , in the presence of the eavesdroppers in M is given by:

$$C_{i,k} = \left(C_{i,k}^d - \max_{m \in M} C_{i,k,m} \right)^+ \quad (5)$$

where $a^+ \triangleq \max(a, 0)$.

[0030] In equation (5), $C_{i,k}^d = \log(1 + \gamma_{i,k})$ is the capacity of the backscatter transmission between reader i and tag k , with $\gamma_{i,k} = \frac{P_{i,k}^{\text{rx}}}{\sigma^2}$ being the signal-to-noise ratio (SNR) and σ^2 is the variance of the noise. $C_{i,k,m} = \log(1 + \gamma_{i,k,m})$ is the capacity of the backscatter transmission between reader i and tag k as received at eavesdropper m with $\gamma_{i,k,m} = \frac{P_{i,k,m}^{\text{rx}}}{\sigma^2}$ being the SNR as received at m .

[0031] Embodiments of the system 100 improve the secrecy rate versus conventional backscatter communication systems, by exploiting two key features of backscatter communication: (i) the nature of the backscatter channel in which the CW signal is modulated by the tag and transmitted back to the reader; and (ii) the fact that the CW signal is continuously transmitted by the RFID reader for powering the passive RFID tag during the entire communication process. Equation (3) shows that, by using a signal from the readers as disclosed herein, it is possible to induce interference on any eavesdropper m , thereby reducing the capacity received at the eavesdropper. During the CW transmission, the eavesdropper receives the CW signal as seen in the second term of equation (3). In conventional RFID systems, the eavesdropper has an almost complete knowledge of the CW $x_i(t)$ transmitted by any reader i , and, hence, the eavesdropper is able to cancel this term.

[0032] The system 100 exploits this feature of the RFID backscatter channel so as to introduce additional interference at the eavesdroppers. More specifically, the reader 104 appends to the CW signal $x_i(t)$ a random noise signal $z_i(t)$ generated and known by reader 104 but unknown to the eavesdroppers. Instead of transmitting $x_i(t)$, each reader $i \in N$ of the system 100 transmits $x_i(t) + z_i(t)$. Accordingly, the backscatter signal between reader i and tag k in the presence of the added noise signal (after canceling the known CW signals $x_j(t), \forall j \in N \setminus \{i\}$) is given by:

$$\hat{y}_{k,i}(t) = h_{k,i} s_k(t) h_{i,k} x_i(t) + \sum_{j \in N, j \neq i} h_{j,i} z_j(t) + n_i(t) \quad (6)$$

where $\sum_{j \in N, j \neq i} h_{j,i} z_j(t)$ is inter-reader interference. The impact of the artificial noise signal $z_i(t)$ backscattered by the tags belonging to the readers in $N \setminus \{i\}$ is assumed to be negligible because the backscattered signal's power is much smaller than the power of the forward reader-tag link.

[0033] Similarly, at any eavesdropper $m \in M$, the received signal pertaining to the backscatter communication between a reader $i \in N$ and a tag $k \in K_i$ in the presence of an artificial noise signal transmitted by all readers is given by:

$$\hat{y}_{k,i,m}(t) = h_{k,m} s_k(t) h_{i,k} x_i(t) + h_{i,m} z_i(t) + \sum_{j \in N, j \neq i} h_{j,m} z_j(t) + n_m(t) \quad (7)$$

where:

$h_{i,m} z_i(t)$ is interference from reader i ; and

$\sum_{j \in N, j \neq i} h_{j,m} z_j(t)$ is interference induced from readers in $N \setminus \{i\}$.

[0034] Equations (6) and (7) show that for a single reader embodiment of the system 100, the inclusion of an artificial noise signal by the reader 104 reduces the received power at the eavesdropper and, consequently, can lead an improved secrecy rate in equation (5) due to the reduced capacity as received at the eavesdroppers. Furthermore, for a multi-reader system 100, the use of a random artificial noise signal at any reader induces interference, not only on the eavesdroppers but also at other readers in the system 100 and accordingly the system 100 is configured to optimize the readers' secrecy.

[0035] Because each reader adds an artificial noise signal $z_i(t)$ to its CW $x_i(t)$, each reader determines how to allocate power between the CW signal and the artificial noise. For each reader $i \in N$, $\alpha_i \tilde{P}$, $\alpha_i \in [0, \alpha_{i,\max}]$ is the amount of power that the reader allocates to the artificial noise signal, with $\alpha_{i,\max} < 1$ being the maximum amount of power that can be used for noise. Consequently, $(1 - \alpha_i) \tilde{P}$ corresponds to the power

allocated to the CW signal. Accordingly, the signal-to-interference-plus-noise ratio (SINR) received at reader i during backscatter communication with a tag $k \in K_i$ is given by:

$$\hat{\gamma}_{i,k} = \frac{\hat{P}_{i,k}^{\text{rx}}}{\sigma^2 + \sum_{j \in N, j \neq i} P_{j,i}^{\text{rx}}} \quad (8)$$

where $\hat{P}_{i,k}^{\text{rx}}$ is as shown in equation (2) with $P_i = (1 - \alpha_i) \tilde{P}$, and $P_{j,i}^{\text{rx}}$ is given by:

$$P_{j,i}^{\text{rx}} = \alpha_j \tilde{P} G_{j,i} G_i \left(\frac{\lambda}{4\pi d_{j,i}} \right)^2 \quad (9)$$

where $\alpha_j \tilde{P}$ is the power of the noise generated by reader j , which interferes at reader i .

[0036] Similarly, the SINR received at eavesdropper m during the backscatter communication between any reader $i \in N$ and tag $k \in K_i$ is:

$$\hat{\gamma}_{i,k,m} = \frac{\hat{P}_{i,k,m}^{\text{rx}}}{\sigma^2 + \sum_{j \in N} P_{j,m}^{\text{rx}}} \quad (10)$$

where $\hat{P}_{i,k,m}^{\text{rx}}$ is given in equation (4) with $P_i = (1 - \alpha_i) \tilde{P}$, and $P_{j,m}^{\text{rx}}$ is given by:

$$P_{j,m}^{\text{rx}} = \alpha_j \tilde{P} G_{j,m} G_m \left(\frac{\lambda}{4\pi d_{j,m}} \right)^2 \quad (11)$$

where $\alpha_j \tilde{P}$ is the power of the noise generated by any reader $j \in N$ that interferes at eavesdropper m .

[0037] With all readers in N using an artificial noise signal appended to their CW transmission, the secrecy rate achieved by any reader $i \in N$ when communicating with a tag $k \in K_i$ is given by:

$$\hat{C}_{i,k} = \left(\log(1 + \hat{\gamma}_{i,k}) - \max_{m \in M} \log(1 + \hat{\gamma}_{i,k,m}) \right)^+ \quad (12)$$

with $\hat{\gamma}_{i,k}$ and $\hat{\gamma}_{i,k,m}$ as in equations (8) and (10) respectively.

[0038] Comparison of equations (12) and (5) shows that by adding an artificial noise signal the readers are able to decrease the capacity at the eavesdroppers and improve their secrecy rate. The secrecy rate gains are dependent on how the readers allocate power between the CW and the artificial noise signals. The power allocation chosen by a reader i impacts not only its own secrecy rate but also that of the neighboring readers, due to the interference added to the system as seen in equations (8) and (10). Embodiments of the reader 104 apply a game-theoretic approach to determine power allocation, so as to maximize secrecy rates.

[0039] In embodiments of the reader 104, each reader $i \in N$ determines the fraction α_i of power to be allocated to the added artificial noise signal $z_i(t)$. The power allocation choices by the readers are interdependent, i.e., the choice of α_i by a reader i affects the secrecy rate of all readers in the system 100, due to mutual interference. In embodiments of the system 100, each reader 104 adjusts its power allocation so as to optimize its secrecy rate, given the power allocations chosen by the other readers 104.

[0040] Embodiments define a noncooperative game in which the readers in N are the players. Each reader $i \in N$ chooses the power allocations $\alpha_i \in A_i \triangleq [0, \alpha_{i,\max}]$ that maximize the utility function:

$$U_i(\alpha_i, \alpha_{-i}) = \sum_{k \in K_i} \hat{C}_{i,k} \quad (13)$$

where $\hat{C}_{i,k}$ is given by equation (12) and α_{-i} is the vector of power allocations chosen by the readers in $N \setminus \{i\}$. The utility function of equation (13) represents the total secrecy rate achieved by all tags that are communicating with reader i .

[0041] Given the utility function of equation (13), embodiments employ a noncooperative, nonzero-sum game in strategic form: $\Xi = \{N, \{A_i\}_{i \in N}, \{\{U_i\}_{i \in N}\}\}$. This game captures the interactions between the RFID readers that use artificial noise for optimizing the secrecy of their transmissions. In this game, each RFID reader $i \in N$ can solve the following optimization problem:

$$\max_{\alpha_i \in A_i} U_i(\alpha_i, \alpha_{-i}) \quad (14)$$

As the strategy sets are continuous and the utility functions are continuous with respect to the actions of all players, the game Ξ is said to be a continuous-kernel game. In order to solve this game, embodiments may apply the concept of a Nash equilibrium.

[0042] A strategy profile α^* constitutes a pure-strategy Nash equilibrium if, for every player i :

$$U_i(\alpha_i^*, \alpha_{-i}^*) \geq U_i(\alpha_i, \alpha_{-i}^*), \forall \alpha_i \in A_i, i \in N \quad (15)$$

[0043] Hence, for the game applied in various embodiments, the Nash equilibrium is a state in which no RFID reader i can improve its overall secrecy rate by unilaterally changing its noise power $\alpha_i^* \tilde{P}$, given that the other RFID readers choose their power allocation per the equilibrium vector α_{-i}^* .

[0044] In order to find a Nash equilibrium of the RFID security game employed by the readers, embodiments employ the concept of a best response. The best response $r(\alpha_{-i})$ of any RFID reader $i \in N$ to the profile of strategies α_{-i} is a set of power allocations for i such that:

$$r(\alpha_{-i}) = \left\{ \alpha_i \in A_i \mid U_i(\alpha_i, \alpha_{-i}) \geq U_i(\alpha'_i, \alpha_{-i}), \forall \alpha'_i \in A_i \right\} \quad (16)$$

[0045] Accordingly, embodiments of the reader 104 determine the amount of power to allocate to each of the CW carrier signal and the added noise signal by adjusting the best response until convergence to a Nash equilibrium is achieved.

[0046] Figure 2 shows a block diagram of the RFID reader 104. The reader 104 includes a transmitter 202, a receiver 210, a power allocation subsystem 208, and various other components and subsystems that have been omitted from Figure 2 in the interest of clarity. For example, the reader 104 also includes antenna(s), processor(s), memory, etc.

[0047] The transmitter 202 includes a CW carrier signal generator 204 and a noise signal generator 206. The CW carrier signal generator 204 generates the continuous wave carrier signal 214 that is transmitted in conventional systems to initiate backscatter communication with a tag, and from which the tag derives power. The noise signal generator 206 generates a noise signal 216 that is combined with the CW carrier signal 214 generated by the CW carrier signal generator 204. The noise signal 216 may be, for example, a random noise signal or a pseudo-random noise signal. The transmitter 202 transmits the combined signal 106 to initiate backscatter communication with the tag 102. Transmission of the noise signal 216 in combination with the CW carrier signal 214 interferes with detection, by an eavesdropper, of backscatter transmissions 108 and increases the secrecy rate of the system 100.

[0048] The power allocation subsystem 208 determines how much power should be allocated to transmission of each of the CW carrier signal 214 and the noise signal 216. Embodiments of the power allocation subsystem 208 may determine the power allocations by iteratively adjusting the signal powers until convergence to a Nash equilibrium is achieved as described herein with regard to equations (13)-(16) and the explanation thereof.

[0049] The receiver 210 receives backscatter transmissions 108 and processes the received backscatter signal to extract the information 220 transmitted by the tag 102. The receiver 201 includes a noise filtering module 212 that removes the noise signal 216 from the received backscatter signal. The receiver 210 is able to extract the information transmitted by the tag 102 from the backscatter signal 108 because the noise signal 216

is known to the receiver. The noise signal 216 is not known to eavesdroppers, and consequently, eavesdroppers are unable to separate the noise signal 216 from the backscatter signal.

[0050] Some portions of the reader 104, e.g., the power allocation subsystem 208, may be implemented as a processor executing software instructions retrieved from a storage device. Processors suitable for use in the reader 104 may include general-purpose microprocessors, digital signal processors, microcontrollers, or other devices capable of executing instructions retrieved from a computer-readable storage device. Processor architectures generally include execution units (e.g., fixed point, floating point, integer, etc.), storage (e.g., registers, memory, etc.), instruction decoding, peripherals (e.g., interrupt controllers, timers, direct memory access controllers, etc.), input/output systems (e.g., serial ports, parallel ports, etc.) and various other components and sub-systems.

[0051] Storage suitable for use in the reader 104 includes any non-transitory computer-readable storage medium suitable for storing instructions executable by a processor and/or data used by a processor. Such storage may include volatile storage such as random access memory, non-volatile storage (e.g., a hard drive, an optical storage device (e.g., CD or DVD), FLASH storage, read-only-memory), or combinations thereof.

[0052] Figure 3 shows a flow diagram for a method 300 for backscatter communication with optimized secrecy rate in accordance with principles disclosed herein. Though depicted sequentially as a matter of convenience, at least some of the actions shown can be performed in a different order and/or performed in parallel. Additionally, some embodiments may perform only some of the actions shown. In some embodiments, at least some of the operations of the method 300, as well as other operations described herein, can be implemented as instructions stored in computer readable storage device and executed by a processor.

[0053] In block 302, the readers of a backscatter communication system are in an initial state wherein the readers are not using any artificial noise to improve the secrecy rate.

[0054] In block 304, each of the readers executes a discovery operation to identify other readers operating in the vicinity and to determine the features of the identified readers. In some embodiments, such as pre-deployed environments, the locations and characteristics of the readers positioned in a certain area can be pre-programmed into each reader during network deployment. In more dynamic environments, e.g., systems that comprise mobile RFID readers, the discovery operation can include identification of neighboring readers via known wireless discovery techniques.

[0055] In block 306, each of the readers applies the best response algorithm disclosed herein. Each reader observes the transmissions of neighboring readers (e.g., by measuring the received CW signals), and determines the optimal power allocation (i.e., its best response), under the observed conditions. The best response dynamics phase may occur sequentially, i.e., the readers may observe their neighbors and make best response decisions in an arbitrary yet sequential order. The best response determinations continue iteratively until Nash convergence is achieved.

[0056] During the discovery and best response determination operations, the tags may not backscatter any information. Some tags may include an RFID MAC protocol that inhibits backscatter communication while the readers are performing discovery and best response determination operations. Accordingly, no tag information may be transmitted until the readers have determined how best to secure the system 100.

[0057] In block 308, the readers have achieved a Nash equilibrium, and collect information from the tags. The readers transmit a CW carrier signal that includes added noise signal to induce backscatter transmission by the tags, and data is backscattered from the tags to the readers. In essence, once equilibrium is achieved, the actual backscatter communication occurs.

[0058] In block 310, the reader 104 receives the backscatter transmission and filters the noise signal from the received backscatter signal. The information transmitted by the tag 102 is extracted from the filtered backscatter signal.

[0059] Figure 4 shows a graph comparing secrecy rate of a conventional system and secrecy rate of a system in accordance with principles disclosed herein. In Figure 4, the performance of an embodiment of the system 100 is assessed by showing the average secrecy rate achieved per reader as the number of readers varies for a network with six

eavesdroppers. Figure 4 shows that as the number of readers increases, the average secrecy rate achieved by the system 100 decreases while that of the conventional system increases. This is due to the fact that the use of artificial noise in combination with the CW carrier signal increases the reader-to-reader interference in the network and, thus, the inter-reader interference becomes significant for larger networks thereby decreasing the secrecy rate of the system 100. In contrast, for the conventional system, as more readers and tags are deployed for a fixed number of eavesdroppers, the average secrecy rate increases. Figure 4 shows that, at all illustrated network sizes, the system 100 yields significant performance gains of at least 17% relative to the conventional system (with seven readers).

[0060] Figure 5 shows a graph showing the average number of iterations and the maximum number of iterations applied to reach a Nash equilibrium in accordance with principles disclosed herein. In Figure 5, as the number of readers increases, the total number of iterations required for convergence to a Nash equilibrium increases. This is due to the fact that, as the number of readers increases, the possibility of reader-to-reader interactions increases, and, thus, additional best response actions are required prior to convergence. Figure 5 shows that the average and the maximum number of iterations vary, respectively, from 3.9 and 9 with two readers, and up to 9.2 and 24 with seven readers.

[0061] The above discussion is meant to be illustrative of the principles and various implementations of the present disclosure. Numerous variations and modifications will become apparent to those skilled in the art once the above disclosure is fully appreciated. Although embodiments of the invention have been described herein by reference to RFID systems, those skilled in the art will understand that embodiments of the invention encompass a wide variety of backscatter communication systems. It is intended that the following claims be interpreted to embrace all such variations and modifications.

CLAIMS

What is claimed is:

1. A backscatter communication system, comprising:
a reader configured to receive backscatter transmissions, the reader comprising:
a transmitter configured to emit a radio frequency signal to induce backscatter communication, the transmitter comprising:
a continuous wave (CW) carrier signal generator that produces a CW carrier signal; and
a noise signal generator that generates a noise signal;
wherein the transmitter is configured to:
combine the CW carrier signal and the noise signal; and
transmit the combined signal to induce backscatter communication.
2. The system of claim 1, wherein the reader further comprises a power allocation subsystem configured to determine an amount of power to be allocated to transmission of each of the CW carrier signal and the noise signal.
3. The system of claim 2, wherein the power allocation subsystem is configured to determine the amount of power allocated to transmission of each of the CW carrier signal and the noise signal by selecting power allocations that maximize a function representing a total secrecy rate for transmissions in the system.
4. The system of claim 2, wherein the power allocation subsystem is configured to determine the amount of power allocated to transmission of each of the CW carrier signal and the noise signal by iteratively adjusting the power allocated until a Nash equilibrium is achieved.
5. The system of claim 1, wherein the noise signal is one of a random noise signal and a pseudo-random noise signal.

6. The system of claim 1, wherein the noise signal increases the secrecy rate of the backscatter transmissions.
7. The system of claim 1, wherein the noise signal induces interference in an eavesdropper monitoring the backscatter transmissions.
8. The system of claim 1, further comprising at least one tag configured to receive the combined signal and wirelessly transfer information from the tag via backscatter transmission.
9. The system of claim 1, wherein the reader comprises a receiver configured to detect information in the backscatter transmissions by cancelling the noise signal from the received backscatter transmissions.
10. A method for backscatter communication, comprising:
 - generating a continuous wave (CW) carrier signal;
 - generating a noise signal;
 - combining the CW carrier signal and the noise signal;
 - transmitting the combined signal;
 - receiving a backscatter transmission induced by the combined signal; and
 - extracting information encoded in the backscatter transmission by filtering the noise signal received with the backscatter transmission.
11. The method of claim 10, further comprising determining an amount of power to be allocated to transmission of each of the CW carrier signal and the noise signal.
12. The method of claim 11, wherein the determining comprises selecting power allocations that maximize a function representing a total secrecy rate for transmissions in the system.

13. The method of claim 11, wherein the determining comprises iteratively adjusting the power allocated until a Nash equilibrium is achieved.
14. The method of claim 10, further comprising inducing, via the noise signal, interference in an eavesdropper monitoring the backscatter transmission.
15. The method of claim 10, further comprising increasing, via the noise signal, a secrecy rate of the backscatter transmission.
16. A radio frequency identification (RFID) reader, comprising:
 - a power allocation subsystem configured to determine an amount of power to be allocated for transmission of each of a continuous wave (CW) carrier signal and a noise signal;
 - a transmitter configured to:
 - combine the CW carrier signal and the noise signal; and
 - emit the combined signal to induce backscatter communication by an RFID tag.
17. The RFID reader of claim 16, wherein the power allocation subsystem is configured to determine the amount of power allocated to transmission of each of the CW carrier signal and the noise signal by selecting power allocations according to a function representing a total secrecy rate for the backscatter communication.
18. The RFID reader of claim 16, wherein the power allocation subsystem is configured to determine the amount of power allocated to transmission of each of the CW carrier signal and the noise signal by iteratively adjusting the power allocated until a Nash equilibrium is achieved.
19. The RFID reader of claim 16, further comprising a receiver configured to detect information in the backscatter transmission by cancelling the noise signal from a received backscatter transmission.

20. The RFID reader of claim 16, wherein the noise signal increases a secrecy rate of the backscatter transmission by inducing interference that inhibits reception of the backscatter transmission by an eavesdropper.

FIG. 1

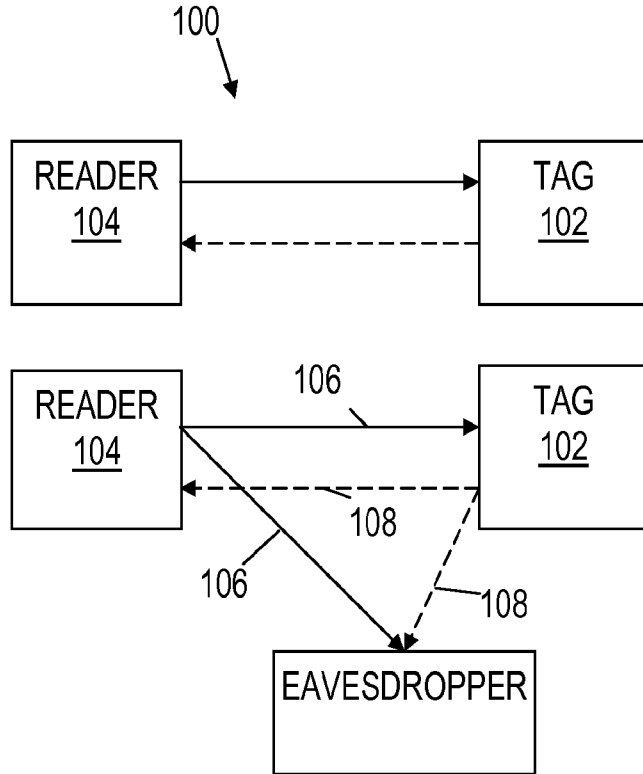
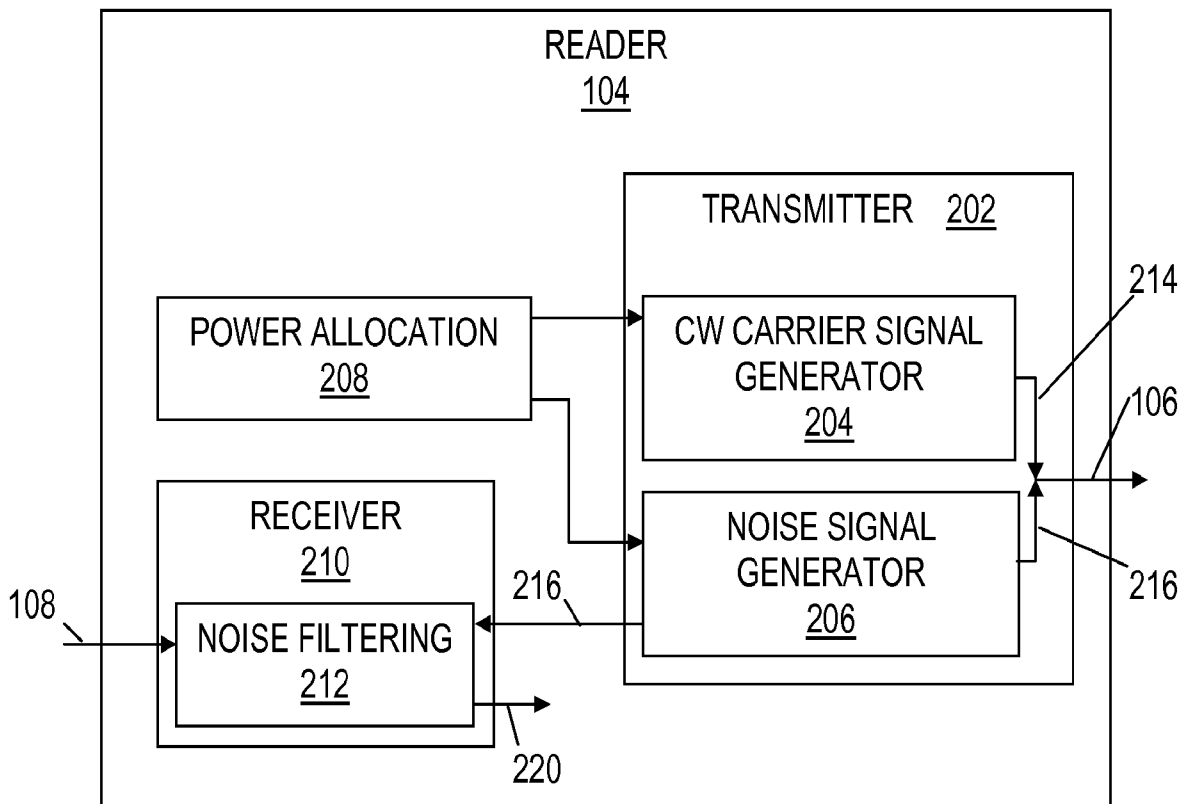


FIG. 2



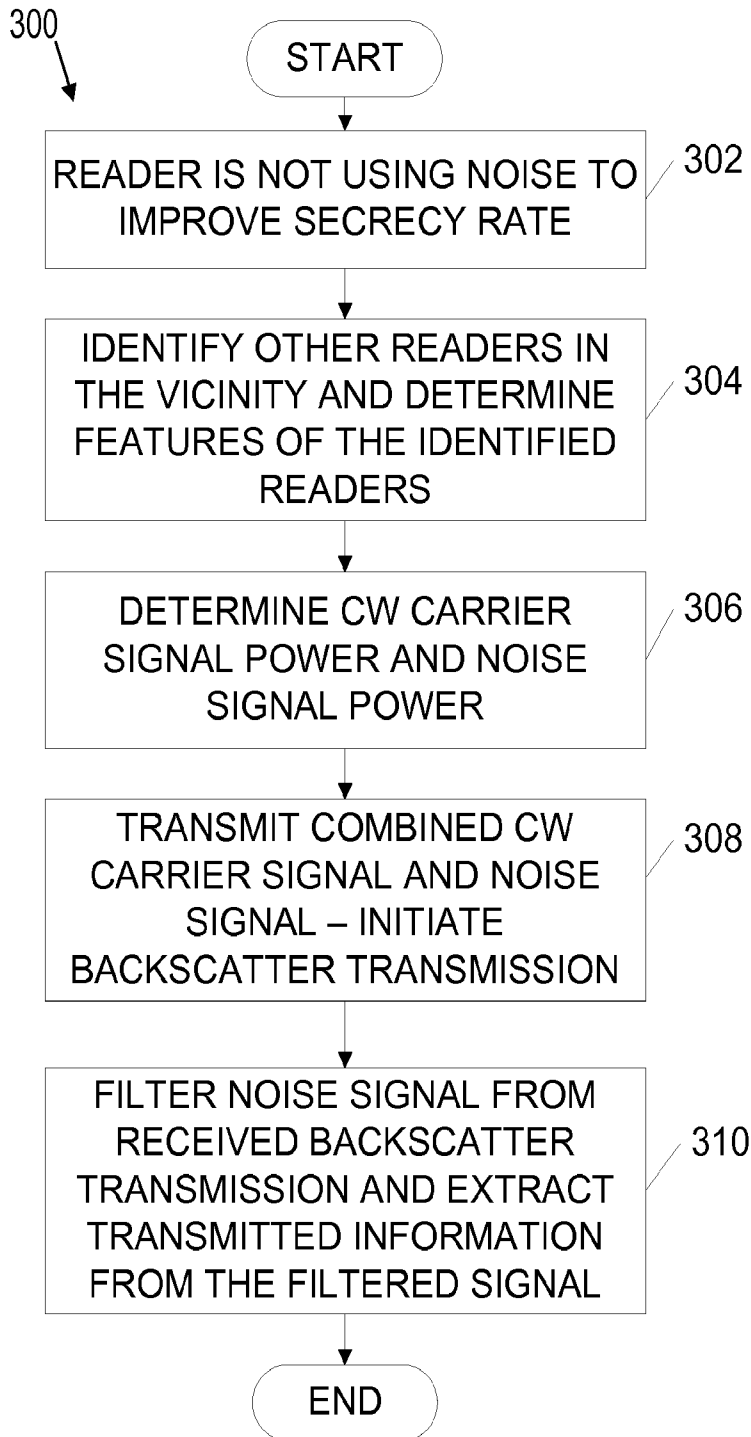


FIG. 3

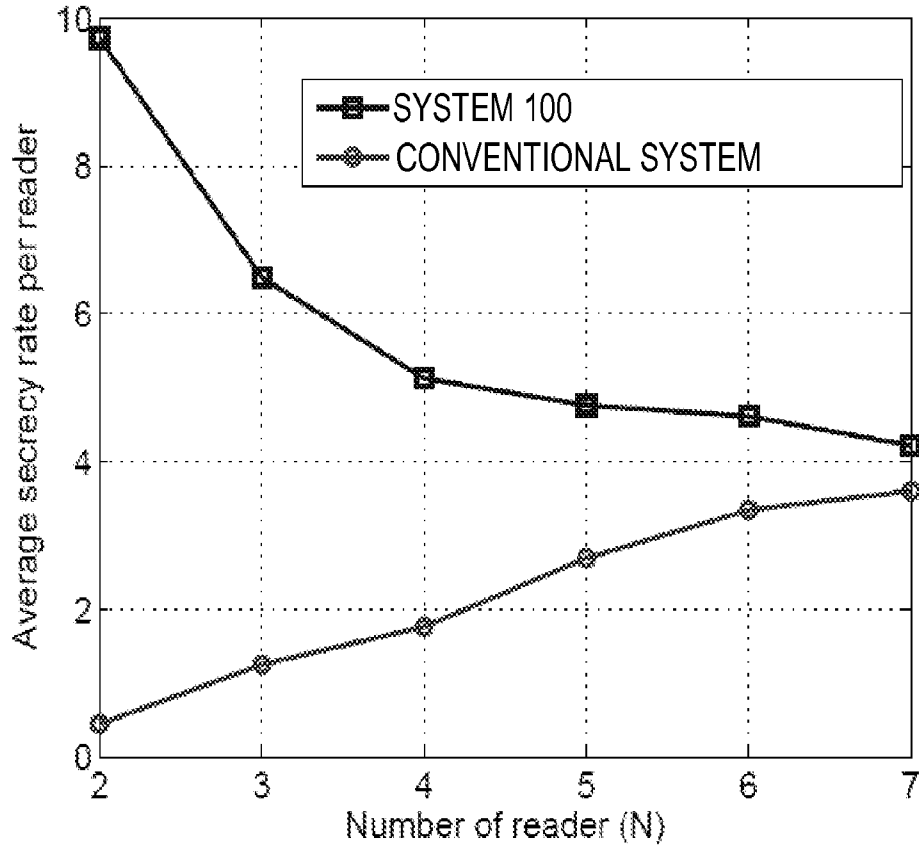


FIG. 4

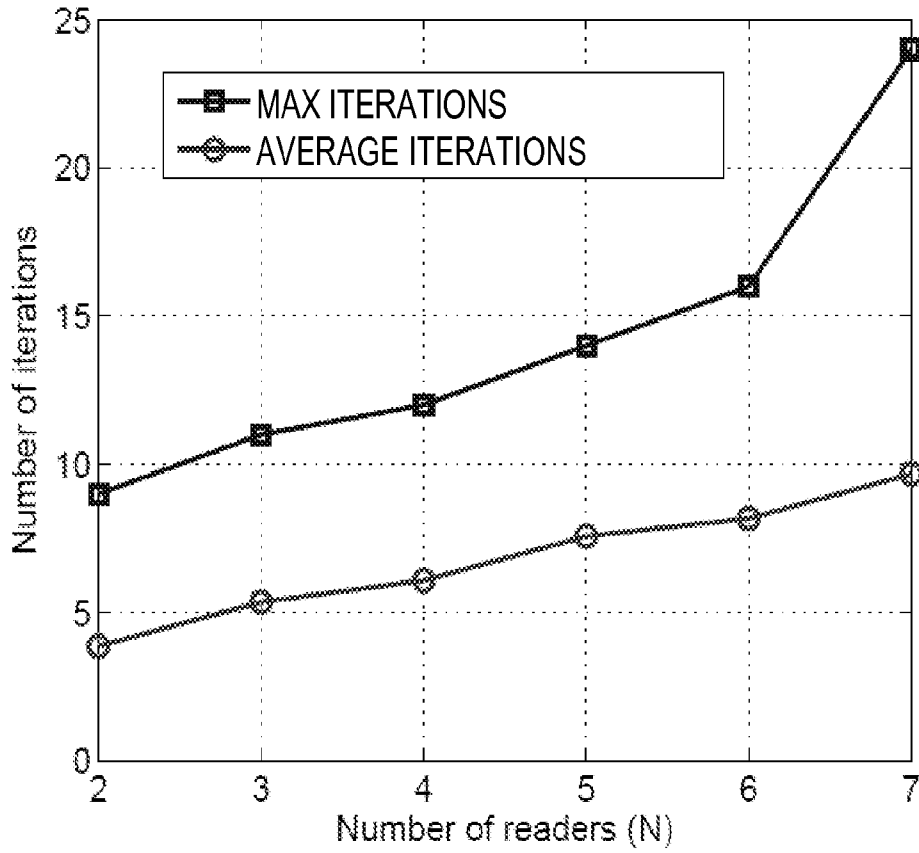


FIG. 5

A. CLASSIFICATION OF SUBJECT MATTER**H04B 5/02(2006.01)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)

H04B 5/02; H04K 1/00; H04B 15/00; G08B 13/14; H04Q 5/22

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: backscatter communication, reader, continuous wave carrier signal, noise signal, power allocation subsystem

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007-0177738 A1 (DIORIO et al.) 02 August 2007	1, 5-10, 14-15
A	See paragraphs [0013], [0040]-[0046]; claims 11-24; and figure 4.	2-4, 11-13, 16-20
A	US 2011-0140858 A1 (OVARO et al.) 16 June 2011	1-20
A	See paragraphs [0062]-[0086]; and figures 6-8.	
A	US 2011-0133890 A1 (DURON et al.) 09 June 2011	1-20
A	See paragraphs [0052]-[0053]; and figure 6.	
A	US 2011-0181397 A1 (KANG et al.) 28 July 2011	1-20
A	See paragraphs [0024]-[0041]; and figures 5-7.	
A	US 2008-0174410 A1 (SARANGAPANI et al.) 24 July 2008	1-20
A	See paragraphs [0031]-[0069]; and figures 3a-3b.	

 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

10 December 2013 (10.12.2013)

Date of mailing of the international search report

10 December 2013 (10.12.2013)

Name and mailing address of the ISA/KR


 Korean Intellectual Property Office
 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,
 302-701, Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

SONG, Ho Keun

Telephone No. +82-42-481-5580



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/056853

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0177738 A1	02/08/2007	US 2005-0058292 A1 WO 2005-027022 A2 WO 2005-027022 A3	17/03/2005 24/03/2005 09/06/2005
US 2011-0140858 A1	16/06/2011	AU 1999-34938 A1 AU 1999-35608 A1 AU 3560899 A CA 2321508 A1 CA 2321643 A1 CN 1235661 A0 EP 0934484 A1 EP 0934484 B1 EP 1073858 A1 EP 1073858 B1 EP 1073859 A1 EP 1073859 B1 JP 2000-504399 A JP 3347741 B2 US 2002-0015436 A1 US 2007-0290808 A1 US 2007-0290809 A1 US 2007-0290810 A1 US 2008-0180253 A1 US 2013-0069767 A1 US 5871239 A US 6050609 A US 6073973 A US 6324211 B1 US 6459726 B1 WO 98-19095 A1 WO 99-56233 A1 WO 99-56414 A1 WO 99-57476 A1 WO 99-57477 A1	16/11/1999 16/11/1999 16/11/1999 11/11/1999 11/11/1999 17/11/1999 11/08/1999 28/08/2002 07/02/2001 09/11/2005 07/02/2001 25/02/2004 11/04/2000 20/11/2002 07/02/2002 20/12/2007 20/12/2007 20/12/2007 31/07/2008 21/03/2013 16/02/1999 18/04/2000 13/06/2000 27/11/2001 01/10/2002 07/05/1998 04/11/1999 04/11/1999 11/11/1999 11/11/1999
US 2011-0133890 A1	09/06/2011	US 8400272 B2	19/03/2013
US 2011-0181397 A1	28/07/2011	CN 102257741 A EP 2424121 A2 EP 2424121 A4 EP 2424121 B1 KR 10-0914850 B1 WO 2010-110618 A2 WO 2010-110618 A3	23/11/2011 29/02/2012 19/09/2012 03/07/2013 02/09/2009 30/09/2010 23/12/2010
US 2008-0174410 A1	24/07/2008	US 8143996 B2	27/03/2012