

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
12 March 2009 (12.03.2009)

PCT

(10) International Publication Number
WO 2009/032324 A3

(51) International Patent Classification:
H04M 1/66 (2006.01)

(21) International Application Number:
PCT/US2008/010458

(22) International Filing Date:
8 September 2008 (08.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/970,576 7 September 2007 (07.09.2007) US

(71) Applicants (for all designated States except US): **UNIVERSITY OF MARYLAND** [US/US]; 0133 Cole Student Activities Bldg., College Park, MD 20742-1001 (US). **UNITED STATES OF AMERICA as represented by the SECRETARY OF THE ARMY INTERNAL** [US/US]; 101 Army Pentagon, Washington, DC 20310 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BARAS, John, S.** [US/US]; 10912 Burbank Drive, Potomac, MD 20854 (US). **YU, Paul, L.** [US/US]; 14 Serpentine Court, Silver Spring, MD 20904 (US). **SADLER, Brian, M.** [US/US]; 10405 Derby Drive, Laurel, MD 20723 (US).

(74) Agents: **ROSENBERG, Morton, J.** et al.; Rosenberg, Klein & Lee, 3458 Ellicott Center Drive, Suite 101, Ellicott City, MD 21043 (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, BR, BW, BY, BZ, CA, CH, 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, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

(88) Date of publication of the international search report:
22 May 2009

(54) Title: WIRELESS COMMUNICATION METHOD AND SYSTEM FOR TRANSMISSION AUTHENTICATION AT THE PHYSICAL LAYER

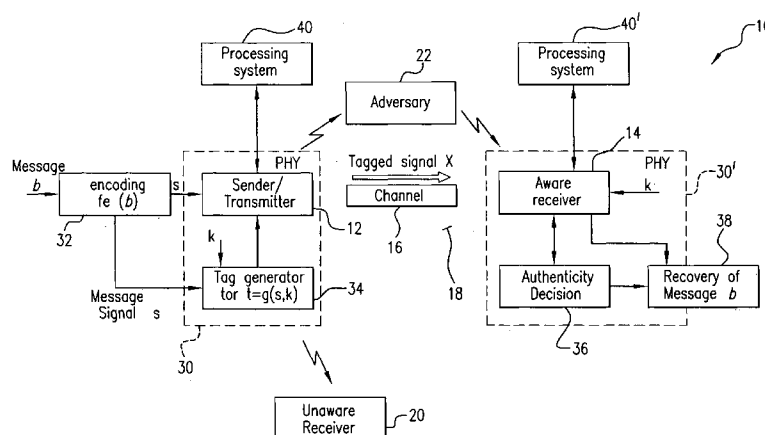


FIG. 1

(57) Abstract: The subject authentication scheme encompasses a large family of authentication systems which may be built over existing transmission systems. By superimposing a carefully designed secret modulation on the waveforms, authentication is added to the signal without requiring additional bandwidth. The authentication information (tag signal) is sent concurrently with data (message signal). The authentication is designed to be stealthy to the uninformed user, robust to interference, and secure for identity verification. The tradeoffs between these three goals are identified and analyzed. The use of the authentication for channel estimation is also considered, and improved bit errors are demonstrated for time-varying channels. With a long enough authentication code word an authentication system is achieved with very slight data degradation. Additionally, by treating the authentication tag as a sequence of pilot symbols, the data recovery may be improved by the aware receiver.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/10458

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04M 1/66 (2009.01)

USPC - 455/411

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8): H04M 1/66 (2009.01)

USPC: 455/411

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 455/411; 726/4 (keyword limited - see terms below)

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

PubWEST(PGPB, USPT, EPAB, JPAB); Google; Search Terms: authentication, authenticity, physical layer, wireless communication, wireless, communication, channel, node, receiving, transmitting, key, secret, secret key, connecting, signal, tag, encoding, authenticity, estimating, estimate, estimation, tag, tagged signal, recover

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/0022444 A1 (RHOADS) 05 February 2004 (05.02.2004), entire document, especially para. [0013], [0016], [0032], [0043]-[0044], [0071]-[0073], [0080], [0086]-[0087], [0095], [0104]-[0105], [0121], [0130], [0136], [0141], [0145], [0162], [0186], [0206], [0218]-[0219], [0236], [0240]-[0241], [0244]-[0247], [0258], [0273], [0277], [0282], [0295], [0310], [0312], [0314], [0348], [0359], [0372], [0375], [0381], [0386], [0423], [0438], [0445], [0448], [0479], [0508], [0511], [0514], [0526], [0550], [0552]-[0553], [0585], [0616], [0652], [0656], [0666], [0686], [0691], [0693], [0698], [0723], [0735]-[0736], [0739], [0800], [0802], [0824], [0849], [0903], [0912], and [0914]-[0915].	1-20
A	US 2007/0206838 A1 (FOUQUET) 06 September 2007 (06.09.2007), entire document	1-20
A	US 2006/0191000 A1 (O'HARA et al.) 24 August 2006 (24.08.2006), entire document	1-20
A	US 2005/0202804 A1 (SILVERBROOK et al.) 15 September 2005 (15.09.2005), entire document	1-20

☐ Further documents are listed in the continuation of Box C.

* 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 February 2009 (10.02.2009)

Date of mailing of the international search report

20 FEB 2009

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774