(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 December 2003 (04.12.2003)

PCT

(10) International Publication Number
WO 2003/101023 A3

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/US2003/015076

(22) International Filing Date: 15 May 2003 (15.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/147,308 17 May 2002 (17.05.2002) US

(71) Applicant: **NETWORK SECURITY TECHNOLOGIES, INC.** [—/US]; 13525 Dulles Technology Drive, Herndon, VA 20171 (US).

(72) Inventors: **AMMON, Ken**; 18571 Norborne Court, Leesburg, VA 20176 (US). **O'FERRELL, Chris**; 20812 Wallingford Square, # 302, Sterling, VA 20165 (US). **MITZEN, Wayne**; 7839 Sabre Court, Manassas, VA 20190 (US). **FRASNELLI, Dan**; 43135 Gatwick Square, Ashburn, VA 20147 (US). **WIMBLE, Lawrence**; 1600 NW 20th Avenue, Crystal River, FL 34429 (US). **YANG, Yin**; 13567 Cobra Drive, Herndon, VA 20171 (US). **MCHALE, Tom**; 2232 Cedar Cove Court, Reston, VA 20191 (US). **DOTEN, Rick**; 205 Winter Frost Court, Sterling, VA 20165 (US).

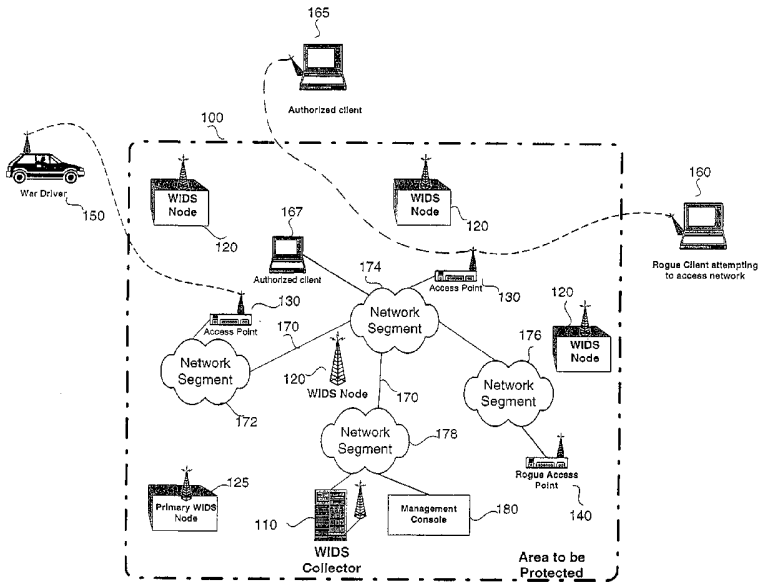
(74) Agent: **COOLEY GODWARD LLP**; Patent Group, One Freedom Square-Reston Town Center, 11951 Freedom Drive, Reston, VA 20190-5656 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR WIRELESS INTRUSION DETECTION



(57) Abstract: A wireless intrusion dection system (WIDS) is disclosed for monitoring both authorized and unauthorized access to a wireless portion of a network. The WIDS consists of a collect (110) and one or more nodes (120) that communicate via an out of band means that is separate from the network. Unauthorized access points (140) and unauthorized clients (160) in the network can be detected. The WIDS can be used to monitor, for example, a network implemented using the 802.11 protocol. In addition, the WIDS can be used by one company to provide a service that monitors the wireless network of another company.

WO 2003/101023 A3

Published:
— *with international search report*

(88) Date of publication of the international search report:
1 April 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/15076

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/32
US CL : 713/201
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)
U.S. : 713/153,200,201; 714/39

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US PUB 2003/0188190 A1 (Aaron) 02 October 2003 (02.10.2003), entire page 7.	1-3, 5-11, 13-26, 28-42 ---------- 4, 12, 27
Y	US 5,784,298 (Hershey) 21 July 1998 (21.07.1998), columns 1-4.	4, 12, 27
X	US 5,784,298 (Hershey et al.) 21 July 1998 (21.07.1998), columns 1-4.	35-37
X	Intrusion detection using mobile agents in wireless ad hoc networks Kachirski, O.; Guha, R.; Knowledge Media Networking, 2002. Proceedings. IEEE Workshop on , 10-12 July 2002 Page(s): 153 -158	1-3, 5-18, 20-30, 32-42
A	Intrusion Detection in Wireless Ad Hoc Network. Yongguang Zhang and W. Lee. Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pp. 275-283, Boston, Massachusetts, Aug 2000.	1-42
A	US 6,088,804 A (Hill) 11 July 2000 (11.07.2000), column 2, line 63 -- column 3, line 40).	1-42

☒ **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 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
14 November 2003 (14.11.2003)

Date of mailing of the international search report
03 DEC 2003

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. (703)305-3230

Authorized officer
Ayaz Sheikh
Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

PCT/US03/15076

INTERNATIONAL SEARCH REPORT

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US PUB 2003/0151513 A1 (Herrmann) 14 August 2003 (14.07.2003), [0007-0009].	1-42

INTERNATIONAL SEARCH REPORT

PCT/US03/15076

Continuation of B. FIELDS SEARCHED Item 3:
IEEE, INSPEC
search terms: wireless, intrusion, dectection