

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
19 February 2004 (19.02.2004)

PCT

(10) International Publication Number
WO 2004/015541 A3

(51) International Patent Classification⁷: **G06F 11/30**,
12/30, H04L 9/00, 9/32

(21) International Application Number:
PCT/US2003/025066

(22) International Filing Date: 11 August 2003 (11.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/217,017 12 August 2002 (12.08.2002) US

(71) Applicant: **HARRIS CORPORATION** [US/US]; 1025
W. Nasa Blvd., Melbourne, FL 32919 (US).

(72) Inventor: **BILLHARTZ, Thomas, Jay**; 2355 Polonius
Lane, Melbourne, FL 32934 (US).

(74) Agents: **YATSKO, Michael, S.** et al.; Harris Corporation,
1025 W. Nasa Blvd., Melbourne, FL 32919 (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, SD, SE, SG,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, 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).

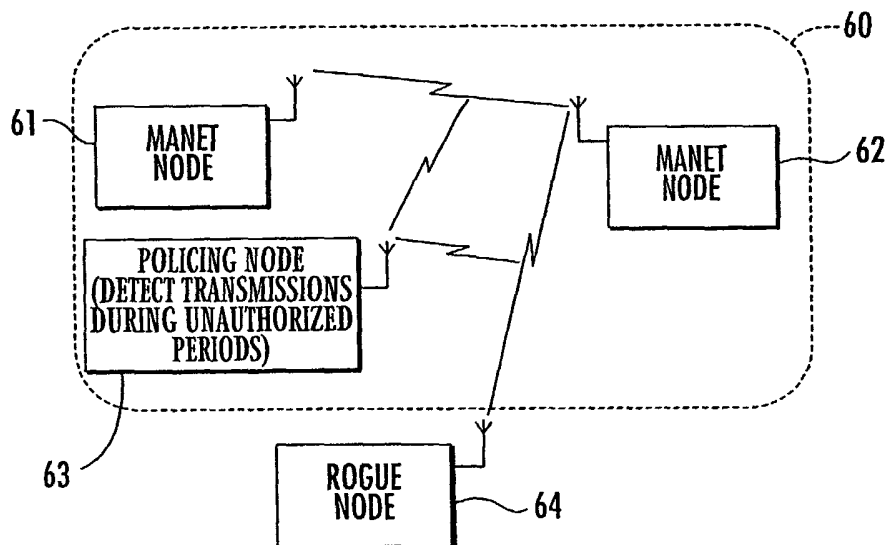
Published:

- with international search report
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments

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

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

(54) Title: MOBILE AD-HOC NETWORK WITH INTRUSION DETECTION FEATURES AND RELATED METHODS



(57) Abstract: A mobile ad-hoc network (MANET) (60) may include a plurality of nodes (61, 62) for transmitting data therebetween and a policing node (63). The policing node (63) may detect intrusions (64) into the MANET (60) by monitoring transmissions among the plurality of nodes (61, 62) to detect transmissions during an unauthorized period and generate an intrusion alert based thereon. The policing node (63) may also detect intrusions (64) based upon one or more of integrity check values which do not correspond with respective data packets, usage of non-consecutive media access control (MAC) sequence numbers by a node, and collisions of packet types and/or MAC addresses.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/25066

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30, 12/30; H04L 9/00, 9/32

US CL : 713/200, 201; 709/223, 224; 380/270; 370/338, 389, 908, 912, 913

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. : 713/200, 201; 709/223, 224; 380/270; 370/338, 389, 908, 912, 913

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.
Y	ZHANG ET AL, "Intrusion detection in wireless ad-hoc networks" ACM, 2000, see sections 4.1, 4.4, 5.2	1-9
Y	US 5,991,881 A (CONKLIN ET AL) 23 November 1999, see col. 1, lines 20-30, col. 3, lines 1-14, col. 6, lines 10-20 & 50-54, Figures 1-3,6	1-9

☐ 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

24 January 2004 (24.01.2004)

Date of mailing of the international search report

09 FEB 2004

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

INTERNATIONAL SEARCH REPORT

PCT/US03/25066

Continuation of B. FIELDS SEARCHED Item 3:

BRS (files: USPAT, DERWENT, JPO, EPO, IBM TDBs, USPGPUB)

search terms: monitor, monitoring, monitored, analyze, analysis, analyzing, analyzed, intrusion, attack, attacked, attacking, malicious, suspicious, audit, manet, wireless, mobile, ad hoc, anomaly, anomalous, deviant, suspect, threshold, behavior, misuse, packet, frame, communication, transmission, data, information