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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2001 (05.04.2001)

PCT

(10) International Publication Number
WO 01/24436 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US00/26880

(22) International Filing Date:
29 September 2000 (29.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/156,905 30 September 1999 (30.09.1999) US
Not furnished 28 September 2000 (28.09.2000) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: REZAIIFAR, Ramin; 10896 Caminito Arcada, San Diego, CA 92121 (US). QUICK, Roy, F., Jr.; 1150 Barcelona Drive, San Diego, CA 92106 (US). WILLIAMSON, Paul; 5775 Morehouse Drive, San Diego, CA 92121 (US). WANG, Jun; 5775 Morehouse Drive, San Diego, CA 92121 (US). TIEDEMANN, Edward, G., Jr.; 4350 Bromfield Avenue, San Diego, CA 92122 (US).

(74) Agents: WADSWORTH, Philip, R. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

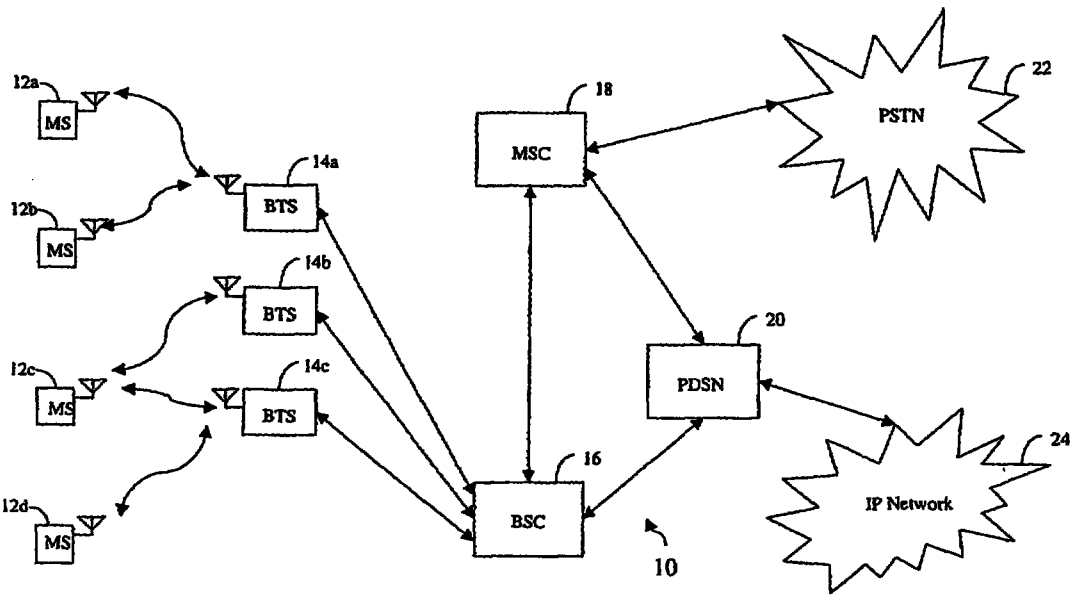
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE,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

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

Published:
— *Without international search report and to be republished upon receipt of that report.*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR ENCRYPTING TRANSMISSIONS IN A COMMUNICATION SYSTEM



(57) Abstract: Method and apparatus for encrypting transmission traffic at separate protocol layers L1 (220), L2 (210), and L3 (200) so that separate encryption elements (204) can be assigned to separate types of transmission traffic (201, 203, 205), which allows the implementation of different levels of encryption according to service requirements. Encryption elements (204) use variable value inputs, called crypto-syncs, along with semi-permanent encryption keys to protect from replay attacks from rogue mobile stations. Since crypto-sync values vary, a method for synchronizing crypto-syncs at the mobile station and base station is also presented.

WO 01/24436 A2

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.