



(51) International Patent Classification:
H04L 9/28 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/SG2009/000185

(22) International Filing Date:
26 May 2009 (26.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/056,560 28 May 2008 (28.05.2008) US

(71) Applicant (for all designated States except US): **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10, Connexis, Singapore 138632 (SG).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **QIU, Ying** [CN/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01, Connexis, South Tower, Singapore 138632 (SG). **ZHOU, Jianying** [SG/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01, Connexis, South Tower, Singapore 138632 (SG). **BAEK, Joonsang** [KR/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01, Connexis, South Tower, Singapore 138632 (SG). **TAN, Han Chiang** [SG/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01, Connexis, South Tower, Singapore 138632 (SG).

(74) Agent: **ELLA CHEONG SPRUSON & FERGUSON (SINGAPORE) PTE LTD**; P.O. Box 1531, Robinson Road Post Office, Singapore 903031 (SG).

(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, MK, 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 (Art. 21(3))

(54) Title: AUTHENTICATION AND KEY ESTABLISHMENT IN WIRELESS SENSOR NETWORKS

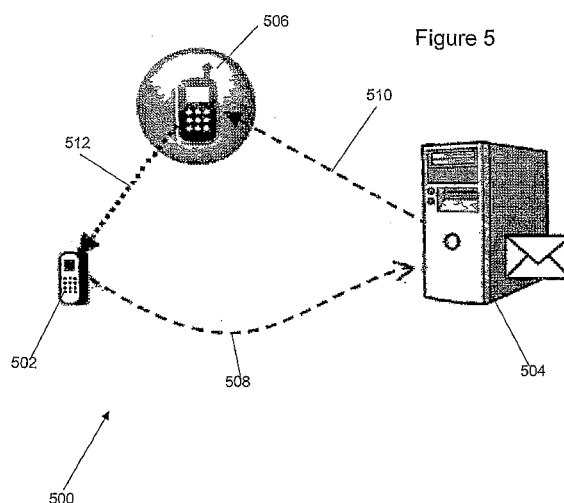


Figure 5

(57) Abstract: To establish a communication key between devices in WSN, comprising first device configured for sending a request message that identifies at least a third device with which communication key is intended, first random number and first authentication code generated using first secret key; the second device configured for authenticating the first authentication code and for generating the communication key based on first secret key, the first random number and second random number using hash function, for sending to third device an approval message in encrypted form based on second secret key shared between the second and third device, the communication key and the first and second random numbers; the third device configured for decrypting this message based on the second secret key and for sending to the first device a notice message comprising the first and second random numbers; and the first device configured for recalculating using said hash function.

