(12) International Application Status Report

Received at International Bureau: 28 November 2008 (28.11.2008)
Information valid as of: 21 May 2009 (21.05.2009)
Report generated on: 04 March 2021 (04.03.2021)

(10) Publication number:
WO2009/067933

(43) Publication date:
04 June 2009 (04.06.2009)

(26) Publication language:
Chinese (ZH)

(21) Application Number:
PCT/CN2008/073051

(22) Filing Date:
14 November 2008 (14.11.2008)

(25) Filing language:
Chinese (ZH)

(31) Priority number(s):
200710019090.9 (CN)

(31) Priority date(s):
16 November 2007 (16.11.2007)

(31) Priority status:
Priority document received (in compliance with PCT Rule 17.1)

(51) International Patent Classification:
H04L 9/00 (2006.01); **H04L 29/06** (2006.01); **H04L 12/28** (2006.01)

(71) Applicant(s):
CHINA IWNCOMM CO., LTD [CN/CN]; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN) *(for all designated states except US)*
TIE, Manxia [CN/CN]; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN) *(for US only)*
CAO, Jun [CN/CN]; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN) *(for US only)*
PANG, Liaojun [CN/CN]; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN) *(for US only)*
LAI, Xiaolong [CN/CN]; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN) *(for US only)*
HUANG, Zhenhai [CN/CN]; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN) *(for US only)*

(72) Inventor(s):
TIE, Manxia; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN)
CAO, Jun; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN)
PANG, Liaojun; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN)
LAI, Xiaolong; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN)
HUANG, Zhenhai; A201, Qin Feng Ge, Xi'an Software Park No. 68 Ke Ji 2nd Road, Xi'an Hi-Tech Industrial Development Zone Xi'an, Shaanxi 710075 (CN)

(74) Agent(s):
UNITALEN ATTORNEYS AT LAW; 7th Floor, Scitech Place No.22, Jian Guo Men Wai Ave., Chao Yang District Beijing 100004 (CN)

(54) Title (EN): KEY MANAGEMENT METHOD

(54) Title (FR): PROCÉDÉ DE GESTION DE CLÉ

(54) Title (ZH): 一种密钥管理方法

(57) Abstract:
(EN): A key management method, is an enhanced RSNA four-way Handshake protocol. Its preceding two way Handshake processes comprises: 1), an authenticator sending a new message (1) which is added a Key Negotiation IDentifier (KNID) and a

Message Integrity Code (MIC) based on the intrinsic definition content of the message (1) to a applicant; 2), after the applicant receives the new message (1), checking whether the MIC therein is correct; if no, the applicant discarding the received new message (1); if yes, checking the new message (1), if the checking is successful, sending a message (2) to the authenticator; the process of checking the new message (1) being the same as the checking process for the message (1) defined in the IEEE 802.11i-2004 standard document. The method solves the DoS attack problem of the key management protocol in the existing RSNA security mechanism.

(FR): L'invention concerne un procédé de gestion de clé comprenant un protocole d'établissement de liaison quadridirectionnelle RSNA. Les procédés d'établissement de liaison bidirectionnelle antérieurs comprennent les étapes suivantes: 1) un authentifiant envoie à un utilisateur un nouveau message (1) auquel est ajouté un identifiant de négociation de clé (KNID) et un code d'intégrité de message (MIC) basé sur le contenu de définition intrinsèque du message (1); 2) lorsque l'utilisateur reçoit le nouveau message (1), il vérifie si le MIC contenu dans le message est correct; si ce n'est pas le cas, l'utilisateur rejette le nouveau message reçu (1); si c'est le cas, il vérifie le nouveau message (1) et, si la vérification est réussie, il envoie un message (2) à l'authentifiant; le processus de vérification du nouveau message (1) étant identique au processus de vérification du message (1) défini dans le document de la norme IEEE 802.11i-2004. Le procédé de l'invention permet de résoudre le problème de l'attaque DoS du protocole de gestion de clé dans le mécanisme de sécurité RSNA existant.

International search report:
Received at International Bureau: 26 February 2009 (26.02.2009) [CN]

International Report on Patentability (IPRP) Chapter II of the PCT:
Not available

(81) Designated States:
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
European Patent Office (EPO) : 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
African Intellectual Property Organization (OAPI) : BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG
African Regional Intellectual Property Organization (ARIPO) : BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW
Eurasian Patent Organization (EAPO) : AM, AZ, BY, KG, KZ, MD, RU, TJ, TM