Study On Key Technology For Encryption And Security System In Wireless Communication Network

Hsien-Wei Tseng[1] Rong-Hou Wu[2] Chih-Yuan Lo[3] Yang-Han Lee[3] Liang-Yu Yen[3]

[1]Dept. of Computer & Communication, Engineering DE LIN Institute of Technology
Tucheng,Taipei County, Taiwan 251, R.O.C
hsienwei.tseng@gmail.com

[2]Dept. of Computer & Communication, Engineering St. John's University
Tamsui,Taipei County, Taiwan 251, R.O.C
rhwu@mail.sju.edu.tw

[3]Dept. of Electrical Engineering, Tamkang University
Tamsui,Taipei County, Taiwan 251, R.O.C.
grimmg@ee.tku.edu.tw
yhlee@ee.tku.edu.tw
skyslj@hotmail.com

Abstract—***A novel secure encryption using the recieved signal strength indicator (RSSI) has been proposed in this paper. RSSI signals are time variant and irregular, especially in more complicated environment. Changes of RSSI can generate a nonperiodical random number, and an attacker will hardly predict this number. Furthermore, we use this option, open cryptography algorithm, and rapid stream ciphers to construct an efficient encryption system for wireless communication network.***

Keywords-Encryption, Security system,

I. INTRODUCTION

Due to diversity transmission services, the new age communication system is facing more security issues than previous years [1-6]. The operation capability of computing equipement at the client end will for sure be much stronger in the next generation. Digital signature or Non-repudiation of information is the premise of commercial trade on the network; therefore, the demand for security system becomes more and more important. This is not what tradition Secret-key Cryptosystem can do. Presently, ITU-R (International Telecommunications Union – Radio communications Sector) is planning a security serverses which at least includes : Authentication, Privacy and Anonymity, Confidentiality, Integrity, Authorization and Access Control, Event Limitation, and Event Reporting.

A study of Security Mechanisms, ITU-R also presents three possible types: Secret Key Check Functionfor bi-direction I.D. authentication module, Digital Signature single direction I.D. authentication module, and Public-key Cryptosystem single direction I.D. authentication module.

In accordance with high-speed wireless LAN，IEEE 802.11 standard formulates the Wired Equivalent Privacy Algorithm (WEP), which has a equal function of data privacy algorithm as wire network. Stream Cipher technique [7-8] is the simplest and the fastest enciphering/deciphering method. Because of its limitation by hardware, it has a fixed period length, so it needs 2L output serier for feedback equations, where L is linear complicity. To overcome this imperfection, we fetch RSSI signals from IF (intermediate frequency) circuit of wireless communication, for generate random number. RSSI signals exchanged by environment are irregular, non-periodical, and have time variant. Therefore it is very suitable to use on password systems. The proposed encryption system in this paper uses the complicated environment RSSI characteristics, its unpredictable number, and the fact that wireless LAN's application is always in complicated indoors transmission environment. So this encryption system is very suitable for wireless communication network.

II. GENERATION OF ENVIRONMENT RANDOM NUMBER

The multi-path effect and environment variable are the factors that change RSSI signals. A random number generate from this RSSI is called environment random number (ERN) in this paper. The flow chart of generating ERM is shown in Fig.1 and is described in details below.

RSSI signal, which is fetched from IF circuit of wireless communication, is sampled and quantized after passing through a linear amplifier：

$R(nT) = R(t)|t=nT \quad , 0 \leqq n \leqq \infty$

Where R(t) is RSSI signals, T is sample period, and R(nT) is discrete RSSI signal.

Annual International Conference on Infocomm Technologies in Competitive Strategies (ICT 2010).

ISBN: 978-981-08-7240-3.
doi:10.5176/978-981-08-7240-3_I-27

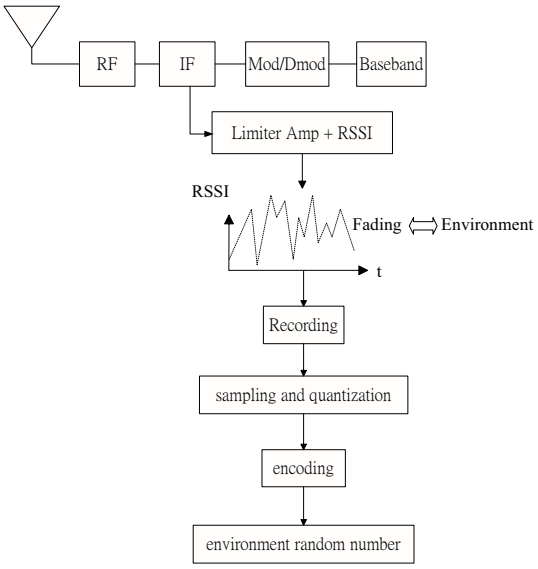

Fig. 1 The flow chart of generating environment random variable

Transfer R(nT) signal to binary number, according to the following simple algorithm is:

$i = 0$ ， $0 \leqq n \leqq k$

if R((n+1)T) – R((nT)) > 0

p(n) = 1

if R((n+1)T) – R((nT)) < 0 (1)

p(n) = 0

if R((n+1)T) – R((nT)) == 0

p(n) = n mod 2

i = i + 1

Where P(n) is a binary ERM, K denotes the length of n, and I is a repeated number of RSSI signal after digitalized. If I is greater than K/2, it means the environment is too stable and not suitable for generating the ERM. When this case happens, we need to re-receive new RSSI signals or enlarge the value of K.

III. DIFFIE-HELLMAN EXPONENTIAL KEY EXCHANGE PROTOCOL

W.Diffie and M.E.Hellman [9] are the early two researchers who proposed using discrete logarithms applied on cryptosystem. Since then, several attempts have been made to find practical public key system depending on the difficulty of solving some problems [10-11].

General C language provises 64bits for basic operation, while commonly in basis g and a modular p have 256 or 512 bits. Therefore, it will counter the problem of how to do the high bits operation. In this proposed paper, we finished a Diffie-Hellman public key exchang protocol of g and p in 128 bits. The algorithm for modular exponentiation operation is attached, using the Chinese remainder theory(CRT) [12-16]：

- finds prime number g of 128 bits (3)
- computes $p = m_1*m_2*m_3*m_4$ where m_1, m_2, m_3, and m_4 are primes of 32 bits
- computes $\Phi(m_1)$, $\Phi(m_2)$, $\Phi(m_2)$, and $\Phi(m_3)$ where Φ is Euler quotient
- computes $g_1 = g \bmod m_1$, $g_2 = g \bmod m_2$, $g_3 = g \bmod m_3$, and $g_4 = g \bmod m_4$
- sets $m_2*m_3*m_4*y_1 = 1 \bmod m_1$, $m_1*m_3*m_4*y_2 = 1 \bmod m_2$, $m_1*m_2*m_4*y_3 = 1 \bmod m_3$, and $m_1*m_2*m_3*y_4 = 1 \bmod m_4$, and finds out y_1、y_2、y_3、y_4
- fetches RSSI signal and computeres environments random number R
- computes $R_1 = R \bmod \Phi(m_1)$, $R_2 = R \bmod \Phi(m_2)$, $R_3 = R \bmod \Phi(m_3)$, and $R_4 = R \bmod \Phi(m_4)$
- computes $c_1 = g_1^{R_1} \bmod m_1$, $c_2 = g_2^{R_2} \bmod m_2$, $c_3 = g_3^{R_3} \bmod m_3$, and $c_4 = g_4^{R_4} \bmod m_4$ ($m_2*m_3*m_4*y_1*c_1 + m_1*m_3*m_4*y_2*c_2 + m_1*m_2*m_4*y_3*c_3 + m_1*m_2*m_3*y_4*c_4$) mod p = (($y_1*c_1 \bmod m_1$)* $m_2*m_3*m_4$ + ($y_2*c_2 \bmod m_2$)* $m_1*m_3*m_4$ + ($y_3*c_3 \bmod m_3$)* $m_1*m_2*m_4$ + ($y_4*c_4 \bmod m_4$) * $m_1*m_2*m_3$) mod p = $g^R \bmod p$

The nine procedures listed above will finish the modular expontiation operation, and also lower the bits of operation.

IV. ENCRYPTION SYSTEM OF RSSI SIGNAL

A. System architecture

Fig. 2 illustrates the main architecture diagram of the encryptosystem.

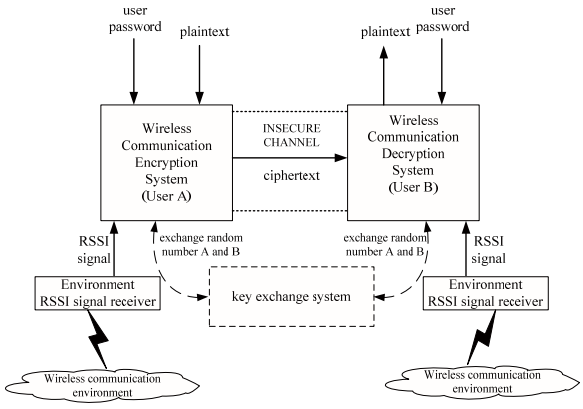

Fig.2 The main architecture diagram of the encryptosystem

The processing steps are described as follow:

- Insert user password on both the transmitting end and receiving end. At the mean time, both ends transceiver receive its RSSI signals under wireless communication environment and then transfer it to binary ERM.
- Switch both ends of transceiver of ERM using key exchange system.
- Combine each used password and exchanged ERM to become a real user password in this transformation time.
- Both transceiver ends successly using exchanged ERM, through stream chipper skill to encipher, transmit, and decipher, at the mean time continuously exchange ERN.
- Both transceiver ends re-receive RSSI signal, when ERM is almost depleted, and re-do step 4.
- Repeat processing step 4 and step 5 until the whole transformation is finished.

B. Method of enciphering and deciphering

Fig. 3 shows the encipher architecture and we will decribed in detail as follow.

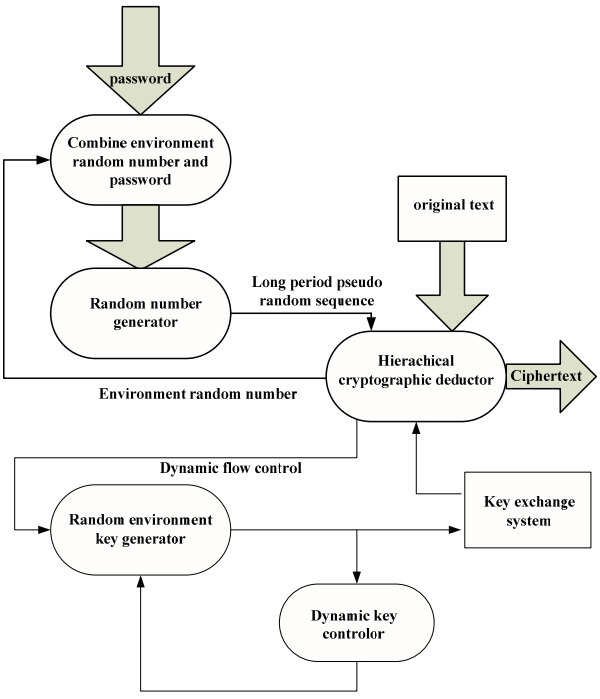

Fig.3 The encipher architecture

ERN on both transceiver end, which generated from Random environment number key generator , is sent to Key exchange system, which becomes a common REN and stores it to Hierachical cryptographic deductor, supply for system sequence to encrypt and decrypt.

Dynamic key controlor monitors the complicity of RSSI in the real time, and adjusts the complicity by Random environment number key generator when the complicity is too low, in order to keep the reasonable complicity of ERN. To achieve the idea of dymanic user password, combine common ERN and input uesr password, let each time the exactly user password is different when sent it to random number generator. This let attacker couldn't attack the ciphtext message even if his has stolen the user password.

Random number generator according to present transmit user password to generate a low-correlation and long period fixed pseudo random series. Meanwhile sent it to Hierachical cryptographic deductor, which is a dynamic adjustment pseudo random serier to generate nonfixed period for using in cryptosystem.

Hierachical cryptographic deductor has a large memory capacity to storage ERN, which is from the key exchange system. ERN is combined to the pseudo random sequence, which is from random number generaror, and is used to extend the fixed period pseudo random sequence in dynamic time variable, as shown in Fig. 4. The function of Hierachical cryptographic deductor is not only in charge of the output of message encryption but also monitors the storage mass of inner ERN. It will send flow control signal to create new ERN when reserve mass is too low.

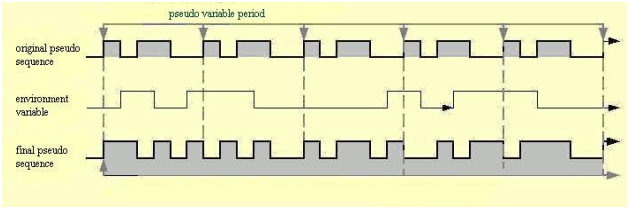

Fig. 4 Dynamic extension of pseudo random sequence

As to decipher architecture, the difference to encipher architecture is only at Hierachical cryptographic deductor part. That is, the receiverd ciphertext is set to the input end of plaintex on encryption system, and plaintext will output from ciphertext output end.

V. RESULTS AND DISCUSSIONS

Fig. 4.5(a), Fig.4.5(b), and Fig.4.5(c) shows the results of encyption system in wireless communication network, according to the previously described of the proposed encyption system.

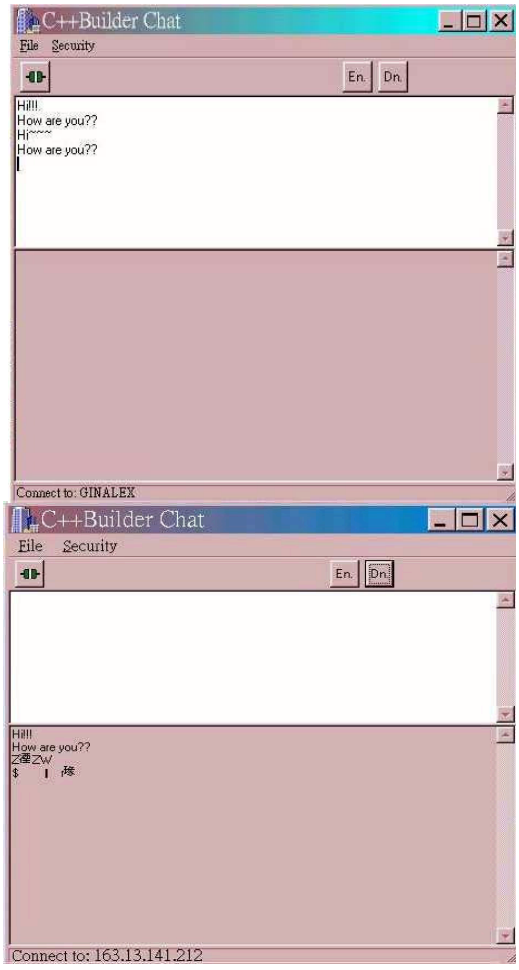

Fig. 5 (a) Encrypt message

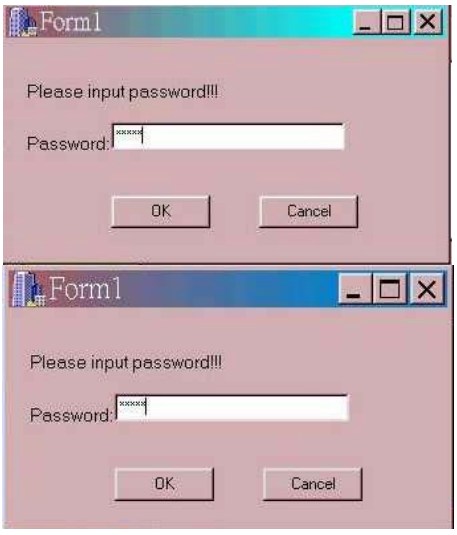

Fig.5(b) Insert password on both side

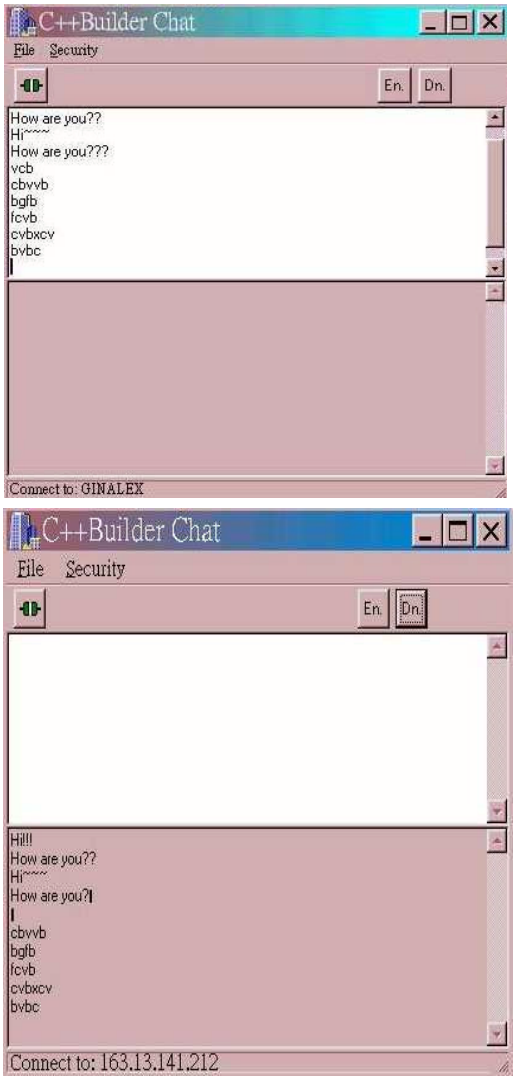

Fig.5(c) Plaintext message after decryption

VI. CONCLUSION

A novel secure encryptosystem using the RSSI signal has been proposed in this paper. This proposed encyptosystem offers several advantages (properties): (a) Ciphertext message is time variable, so can against the plaintext attack. (b) User authentication is dymatic time variable can prevent ciphtertext message for attack. (c) Dymatic extent original fixed pseudo sequence period, slove the traditional stream chipher has fixed period problem. (d)It's suitable for real time message transmit: do not need to add redundance information in chipertext message, simple procedure time, and increse message security level. It overcomes the self-contrdictiory issue between transmission effiency and message security.

VII. REFERENCES

[1] Pandya, R., Grillo, D., Lycksell, E., Mieybegue, P. Okinaka, H. and Yabusaki, M. 1997. IMT-2000 Standards: Network Aspects. IEEE Personal Communications Magazine. Vol. 4. No. 4. (Aug. 1997)

[2] GSM 03.20: Security Related Network Functions. European Telecommunications Standards Institute. (Jun. 1993)

[3] Shieh, S. P., Lin, C. T. and Hsueh, J. T. 1995. Secure Communication in Global Systems for Mobile Telecommunications. Proceeding of International Mobile Computing Conference.(1995)

[4] Yin Zhiyu, Zhang Linwei, Li Wenna, "Study on Security Strategy of Wireless Mobile Office System," Education Technology and Computer Science, 2009. ETCS '09, vol.2, pp.495-498 (2009)

[5] N. Baghaei, R. Hunt, "IEEE 802.11 wireless LAN security performance using multiple clients," International Conference on Networks, ICON 2004, vol.1, pp.299 -303 (2004)

[6] Qu Zhiming, Wang Jingmei, "Application of primary components analysis of security threat in wireless network," International Colloquium on Computing, Communication, Control, and Management, CCCM 2009, vol.4, pp.234-237 (2009)

[7] Herlestam, T. 1982. On the Complexity of Function of Linear Shift Register Sequence. Int Symp Inform. Theory Les Arc. Frane. (1982)

[8] Lan Luo, ZhiGuang Qin, ShiJie Zhou, ShaoQuan Jiang, Juan Wang, "A Middleware Design for Block Cipher Seamless Connected into Stream Cipher Mode,"International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08, pp.64-47 (2008)

[9] Diffie, W., and Hellman, M. 1976. New directions in cryptography. IEEE Trans. Inform. Theory, vol. IT-22(1976), 472-496.

[10] Rivest, R. L., Shamir, A. and Adleman, L. 1978. A method for obtaining digital signatures and public-key cryptosystem. Commum. of ACM. Vol.21. No.2 (1978), 120-126.

[11] ElGamal, T. 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Inform. Theory. Vol.31. No.4(July 1985), 469-472.

[12] Knuth, D. E. 1981. The art of computer programming, volume 2, Seminumerical algorithms. second edition. Addison-Wesley. Reading. Massachusetts. (1981).

[13] Kawamura, S., Takabayashi, K. and Shimbo, A. 1991. A fast modular exponentiation algorithm. A fast modular exponentiation algorithm. Vol.E-74. No.8.(Aug. 1991), 2136-2142.

[14] Dimitrov, V. and Cooklev, T. 1995. Two algorithms for modular exponentiation using non-standard arithmetics. IEICE Trans. Fundamentals of Electronics, Comm., and Computer Sciences. Vol.E78-A. No.1(Jan. 1995), 82-87.

[15] Hung-Min Sun, Shih-Ying Chang, Yu-Hsiang Hung, Yu-Kai Tseng, Hsin-Ta Chiao, "Decomposable Forward Error Correction Codes Based on Chinese Remainder Theorem," 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 pp.260-265 (2009)

[16] Wen Tao Zhu, "Analyzing Euler-Fermat Theorem Based Multicast Key Distribution Schemes with Chinese Remainder Theorem," IFIP International Conference on Network and Parallel Computing, 2008. NPC 2008, pp.11-17 (2008)