The Efficient Transmission Scheme in Wireless Crypto Communication

Jinkeun Hong[1] and Kihong Kim[2]

[1] Division of Information and Communication, Cheonan University,
115 Anse-dong, Cheonan-si, Chungnam, 330-740, South Korea
jkhong@cheonan.ac.kr
[2] Graduate School of Information Security, Korea University,
1, 5-Ka, Anam-dong, Sungbuk-ku, Seoul, 136-701, South Korea
hong0612@hanmir.com

Abstract. An efficient interleaving algorithm is applied to reduce the loss of ciphered information when a cipher system transmits over a wireless fading channel environment. As such, a new scheme for deciding the interleaving depth over a wireless environment is described. Simulations confirm that the proposed effective algorithm with a variable interleaving depth produces a better performance over a fading channel than a static depth algorithm with a fixed interleaving depth. Experimental results showed that the BER performance of the proposed efficient interleaving scheme was higher than that of the fixed interleaving depth scheme. Of particular note is that the dynamic allocation algorithm (DAA) reduces degraded error bits by up to 51.5%, compared with static allocation algorithm (SAA) of depth 48 in 224MHz.

1 Introduction

Aviation industries are undergoing a major paradigm shift in the introduction of new network technologies [1–3]. Tactical information LINK22 is a NATO term for a message standard that includes an anti-jam, secure data system with standard waveforms and messages used for exchanging tactical information between different military platforms, thereby providing a common communications network to a large community of airborne, surface, and even subsurface or space elements [4–8]. In previous studies about tactical networks, performance of high rate LINK22 operation obtained by using quadrature amplitude modulation presented by R. Le Fever, et al. [4], and B. White [5] presented layered communication architecture for the global grid, while B. F. Donal [6] introduced digital messaging on the Comanche helicopter, the area of tactical data links, air traffic management, and software programmable radios has been researched by B. E. White [7]. As the coordination concept of ADS-B civil network and tactical networks becomes more widespread, the necessity of security for these networks is of increasing importance [8–10].

However, in order to solve security issues in secure tactical networks, the efficiency and transmission performance of security services must be taken into

account. From the point of view of aeronautical environmental characteristics, research on optimizing the security considerations of tactical network services, such as low bandwidth, limited consumed power energy and memory processing capacity, and cryptography restrictions is important issue. A cipher system using a link-by-link encryption technique is generally used for security. Except for error propagation, the security level is reflected by the period, common immunity, and linear complexity and since these properties are easy to implement in terms of hardware and do not create any communication channel delays, a cipher system is usually applied to wireless communications. However, when enciphered data is transmitted on a wireless channel, poor communication channel environments, multi-path fading, and interference result in a burst of errors at the decipher output. The fading received at the mobile unit is caused by multi-path reflections of the transmitted encrypted information by local scatters, such as forests, buildings, and other human-built structures, or natural obstacles such as forests surrounding a mobile unit [11–13]. Interleaving is one practical solution for combating burst errors, where a poor encryption communication channel resulting from a burst of errors can be enhanced using an interleaving scheme, and the transmission performance over a wireless channel and radio communication channel has already been evaluated when using an interleaving method in [14–17]. About the area of interleaving research, X. Gui, et al. [14] proposed a novel chip interleaving in DS SS system, and the subject of multiple access over fading multi-path channels employing chip interleaving code division direct sequence spread spectrum has researched by Y. N. Link, et al. [15], the research of required interleaving depth in Rayleigh fading channels has been proposed by I. C. King, et al. [16]. And also, in terms of transmission performance, the performance considerations for secure tactical networks, such as mobility, bandwidth, and BER, are very important. This paper presents a cipher system for security in LINK22, plus an effective interleaving scheme is applied to the ciphered information to enhance the transmission performance over a fading channel.

Section 2 reviews the nature of a fading channel and provides statistical expressions for burst error sequences, then section 3 outlines the cipher system with synchronization information. Thereafter, interleaving scheme based on a variable depth of interleaving using a non fixed interleaving depth allocation algorithm is explained and simulation results presented in section 4. Finally, section 5 summarizes the results of this study.

2 Characteristics of Wireless Mobile Environment

Wireless fading channel modeling is used to perform a statistical analysis based on defining the relational functions, such as the probability density function (PDF), cumulative probability distribution (CPD), level crossing rate (LCR), average duration of fades (ADF), and bit error rate (BER). The mean burst length is derived from the defined relational functions and experiments are used to consider the interleaving depth based on the mean burst length.

In the above equation ρ is the C/N ratio and K is the power ratio of the direct wave and reflected waves. The equation of $CPD(F(L))$ for Rician fading is used as follows :

$$BER(\rho, K) = \frac{1+K}{2(\rho+1+K)} exp(\frac{-K\rho}{\rho+1+K}) \quad (1)$$

In a Rician fading channel, the symbol error rate (SER) is applied in Eq. (1).

$$SER(\rho, K) = 1 - (1 - BER)^8 \quad (2)$$

It can be derived mean burst length as in Fig. 1 [11–13]. Where frequency range is from 224MHz to 400MHz, the variation of power deviations is down to -25dB, and the velocity of mobile device is 24Km/h.

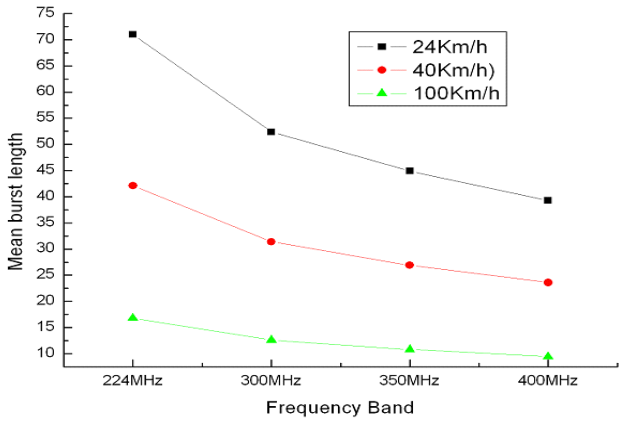

Fig. 1. Mean burst length for variation of power in tactical data link environment

3 Secure Wireless Cipher System

This paper presents a secure cipher system. Plus, interleaving scheme is also applied to the ciphered information to enhance the transmission performance over a fading channel. To provide robust encrypted communication, the transmitter and receiver are both synchronized using a synchronization pattern. If the received synchronization pattern is detected normally, the error-corrected coded session key bit-stream is received and the ciphered data is deciphered. The LINK22 system consists of the data link processor (DLP) for presentation layer, the system network controller (SNC) for transport and network layer, link level COMSEC (LLC) and signal processing controller for data link. The service of SPC in data link supports point to point link oriented. The data rate

of SPC are 16Kbps in fixed frequency mode of UHF. The Reed-Solomon code scheme(such as RS(90,66), RS(90,75), according to the number of message per slot) is applied signal processing controller (SPC) of data link layer.

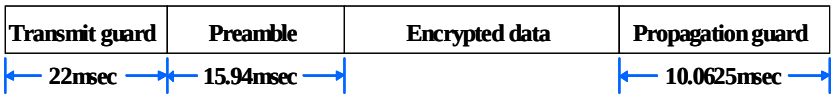

Fig. 2. TDMA time slot architecture of LINK22 tactical data link

The key-stream generator was designed considering the security level [18,19], i.e. the linear complexity, randomness, common immunity, period, and composition of a nonlinear function. In Fig. 2, the transmit guard part is assigned during 22msec, the preamble is 15.94msec, and propagation guard is 10.0625msec The propagation/guard interval is the time period that allows for the propagation of the signal to the maximum range and time required for the NUs to prepare for the transmissions in the next time slot. In encrypted region, the allowed latency time of maximum encryption and decrytion is between 12.1msec and 15.8msec. The encrypted date rate in link layer COMSEC of LINK22 is between 4.8Kbps and 115.2Kbps.

4 Performance of DAA and Experimental Results

When ciphered information is transmitted over a Rician fading channel in which the received signal level is time variant, some of the ciphered information is lost due to burst errors, resulting a loss of the synchronization pattern and error in the session key in a period of synchronization. Interleaving is an effective way of randomizing burst errors, plus, burst errors can not be corrected without the application of interleaving and deinterleaving. The function of the received power (nL) at $K = 0$ can be expressed as follows :

$$\begin{pmatrix} n_{L_0} \\ \vdots \\ n_{L_{n-1}} \end{pmatrix} = \begin{pmatrix} L_0 e^{-L_0} \\ \vdots \\ L_{n-1} e^{-L_{n-1}} \end{pmatrix} \tag{3}$$

The ADF, $t(L)$ can be expressed as follows :

$$\begin{pmatrix} t(L_0) \\ \vdots \\ t(L_{n-1}) \end{pmatrix} = \begin{pmatrix} \frac{F(L_0)}{n_0} \\ \vdots \\ \frac{F(L_{n-1})}{n_0} \end{pmatrix} \tag{4}$$

Therefore, the relationship between the mean burst length (mbl), the transmission rate (B), and the average duration of fades ($t(L)$) can be expressed as follows :

$$\begin{pmatrix} mbl_0 \\ \vdots \\ mbl_{n-1} \end{pmatrix} = \begin{pmatrix} B \times t(L_0) \\ \vdots \\ B \times t(L_{n-1}) \end{pmatrix} \tag{5}$$

Let $k_n, n = 0, 1, 2, \cdots$, be a constant process with a finite set of states $k_0, k_1, \cdots, k_{n-1}$. In deriving the equation, the required condition under which the FEC scheme can still correct all errors is as follows :

$$\begin{pmatrix} k_0 \\ \vdots \\ k_{n-1} \end{pmatrix} = \begin{pmatrix} mbl_0 \\ \vdots \\ mbl_{n-1} \end{pmatrix} \times \begin{pmatrix} d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} \tag{6}$$

These interleaving schemes were evaluated in a simulation environment where the wireless channel is a Rician fading channel, the date rate was 16Kbps, the frame size is 14.4Kbits, the communication access time was 60minutes, the SER was 7.9×10^{-4}, the data rate of LLC was between 4.8Kbps and 115.2Kbps, the moving velocity was 24Km/h, and the carrier frequency applied was from 244MHz to 400MHz. The performance of the DAA and SAA interleaving depth algorithms was then evaluated though simulations. Since the structure of interleaving basically depends on the interleaving depth (d), four types of DAA structure were used: $depth(d) \times span(S) = 4 \times 1200, 8 \times 1200, 12 \times 1200, 24 \times 1200, 48 \times 1200, 96 \times 1200$. When the depth is 12, the delay time is consumed about 1sec. As the depth increase, the delayed time increase. But as transmission rate of SPC is fixed and date rate of LLC increase, the delayed time decrease. However, it is difficult to adapt the depth of interleaving in a variational fading channel, plus, the required depth should be sufficient to handle the resulting errors in the SAA. Therefore, to adapt the depth of interleaving in the variational fading channel, the flexible DAA method was applied.

In condition of N0 RS coding and RS(120,75) coding with SER of 7.9×10^{-4} channel, the resulting performance of the SAA is shown in Fig. 3 and Fig. 4, respectively. When the transmission rate was 16Kbps, the date rate of LLC was 14.4Kbps, the SER was 7.9×10^{-4}, the iteration was 48, the depth of the SAA was 24, as shown in Fig. 3, the error bits of the deciphered data without RS coding were degraded 17% at a SAA depth of 8. In condition of transmission condition with RS(120,75) coding, the depth of the SAA was 24, the error bits of the deciphered were degraded 65% at a SAA depth of 8. Of particular note is that the RS(120, 75) coding reduces degraded error bits by up to 65.9%, compared with No RS coding at SAA depth of 24 in 224MHz environment. When the depth of the DAA was 12, 24, 48, 96, as shown in Table 1, the performance of the DAA block interleaving was better than that of the others. The corrected symbol rate in the DAA applied is higher than that of the other types ($depth = 4, 8, 12, 24, 48, 96$).

At a SAA depth of 24, the corrected symbol rate was corrected 14.5%, 48.5% at a SAA depth of 48, 100% at a SAA depth of 96, in severe channel without RS coding of 224MHz environment. Meanwhile, Table 2 presents a comparison

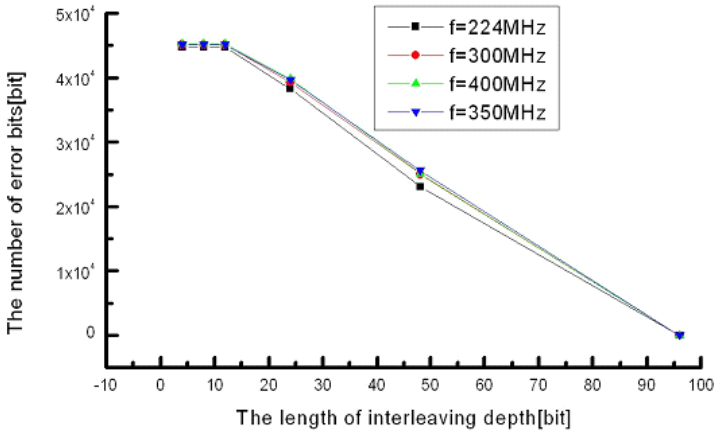

Fig. 3. Error bits relative to depth of SAA (SER : 7.9×10^{-4}, No RS coding)

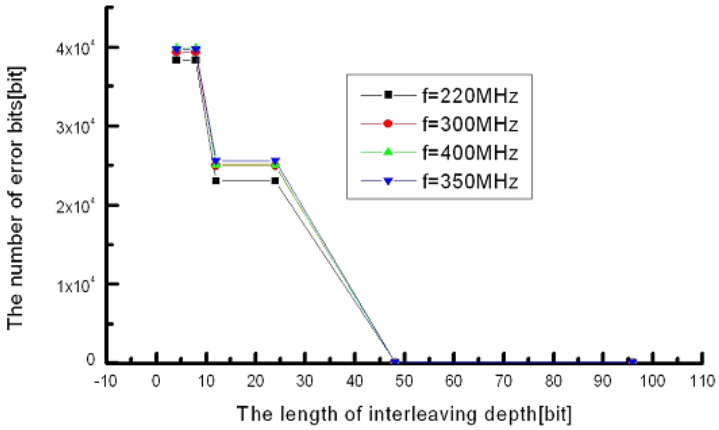

Fig. 4. Error bits relative to depth of SAA (SER : 7.9×10^{-4}, RS(120,75))

Table 1. Comparison of delayed time relative to depth of SAA

Trans. rate (Kbps)		Depth=4	Depth=8	Depth=12	Depth=24	Depth=48	Depth=96
SPC=16	LLC=14.4	0.25sec	0.5sec	1sec	2sec	4sec	8sec
	LLC=28.8	0.125sec	0.25sec	0.5sec	1sec	2sec	4sec
	LLC=57.6	0.0625sec	0.125sec	0.25sec	0.5sec	1sec	2sec
	LLC=115.2	0.03125sec	0.0625sec	0.125sec	0.25sec	0.5sec	1sec

of DAA and SAA with 55 iterations. When the delayed time when using DAA was about 3,095sec, however, the delayed time by the SAA depth of 24 was about 1,738sec, the SAA depth of 48 was 3,476sec, the SAA depth of 96 was 6,952sec. Therefore, when increasing the depth, the corrected symbol rate and delayed time were enhanced. With regard to the delayed time and corrected symbol rate, the performance of the proposed method was superior to that of SAA when applied to allow the delayed time of DAA. Consequently, the results of the transmission performance when using the DAA and SAA confirmed that the performance of the proposed DAA method was better for the case of signal recovery in an erasure channel.

Table 2. Comparison of DAA and SAA with 55 iterations (SER : 7.9×10^{-4}, 28.8Kbps)

Depth	Corrected Symbol Rate	Delay
DAA	100%	3,095sec
Depth = 4	1.0%	217sec
Depth = 8	2.3%	434sec
Depth = 12	5.4%	8,695sec
Depth = 24	14.5%	1,738sec
Depth = 48	48.5%	3,476sec
Depth = 96	100%	6,952sec

5 Conclusions

This paper examines a cipher system for security in tactical network, plus an interleaving scheme is applied to the ciphered information to enhance the transmission performance over a fading channel. As such, a frame of ciphered information is lost if the synchronization pattern and session key for the frame are lost. Therefore, applying an interleaving method to reduce the frame loss and thereby enhance the transmission performance would seem to be an effective option that can be evaluated using the non fixed interleaving depth scheme. A cipher system was proposed using an effective interleaving scheme for the interleaving depth to enhance the transmission performance of the ciphered information.

Experimental results showed that the SER performance of the proposed efficient interleaving scheme was higher than that of the fixed interleaving depth scheme. Of particular note is that the DAA reduces degraded error bits by up to 51.5%, compared with SAA of depth 48 in 224MHz.

References

1. T. Mulkerin. Free Flight Is in the Future : Large-Scale Controller Pilot Data Link Communications Emulation Testbed. *IEEE Aerospace and Electronic Systems Magazine*, 2003.
2. R. T. Oishi. Future Applications and the Aeronautical Telecommunication Network. *IEEE Aerospace Conference*, 2001.
3. EUROCONTROL. Feasibility Study for Civil Aviation Data Link for ADS-B Based on MIDS/LINK 16. *TRS/157/02*, 2000.
4. R. Le Fever and R. C. Harper. Performance of High Rate LINK22 Operation Obtained by Quadrature Amplitude Modulation (QAM). *IEEE Milcom'01*, 2001.
5. B. E. White. Layered Communication Architecture for the Global Grid. *IEEE Milcom'01*, 2001.
6. B. F. Donald. Digital Messaging on the Comanche Helicopter. *DASC'00*, 2000.
7. B. E. White. Tactical Data Links, Air Traffic Management, and Software Programmable Radios. *DASC'99*, 1999.
8. H. J. Beker and F. C. Piper. *Cipher Systems : The Protection of Communicstions*, Northwood Books, Londos, 1982.
9. Bruce Schneier. *Applied Cryptography*, 2nd ed., John Wiley and Sons Inc., 1996.
10. A. R. Rainer. Analysis and Design of Stream Ciphers. *Springer-Verlag*, 1986.
11. W. C. Y. Lee *Mobile Cellular Telecommunications : Analog and Digital Systems*, 2nd ed., McGraw-Hill, 1996.
12. C. Y. William. *Mobile Communications Engineering*, McGraw-Hill, 1982.
13. C. Y. William. *Mobile Communications Design Fundamentals*, John Willey & Sons, 1993.
14. X. Gui and T. S. Ng. A novel Chip Interleaving DS SS System. *IEEE Trans. Veh. Technol.*, Vol.49, No.1, pp.21-27, 2000.
15. Y. N. Link and D. W. Lin. Multiple Access Over Fading Multi-Path Channels Employing Chip Interleaving Code Division Direct Sequence Spread Spectrum. *IEICE Trans. Commun.*, 2001.
16. I. C. King and C-I C. Justin. Required Interleaving Depth in Rayleigh Fading Channels. *Globecom'96*, 1996.
17. S. J. L. et al. Effective Interleaving Method in Wireless ATM Networks. *ICT'97*, 1997.
18. M. Kimberley. Comparison of Two Statistical Tests for Key-Stream Sequences. *Electronics Letters*, Vol.23, No.8, pp.365-366, 1987.
19. M. G. Helen. Statistical Analysis of Symmetric Ciphers *Thesis submitted in accordance with the regulations for Degree of Doctor of Philosophy, Queensland University of Technology*, 1986.