The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 1, pp.45-52, Feb. 28, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.1.45
JIIBC 2015-1-6

H-ARQ 기반 위성통신망에서 암호화 알고리즘에 따른 성능 분석

Performance Analysis of the Encryption Algorithms in a Satellite Communication Network based on H-ARQ

정원호[*], 여봉구[**], 김기홍[***], 박상현[***], 양상운[***], 임정석[***], 김경석[****]

Won Ho Jeong[*], Bong-Gu Yeo[**], Ki-Hong Kim[***], Sang-Hyun Park[***], Sang-Woon Yang[***], Jeong-Seok Lim[***], Kyung-Seok Kim[****]

요 약 위성신호는 방송신호와 같이 동보성을 지니므로 타 통신기술에 비해 데이터의 보안성이 극히 떨어진다. 따라서 통신위성에서 암호화는 매우 중요한 문제로 대두되고 있고 일반서비스와의 통신성능 분석은 반드시 필요하다. 암호화 적용 시 성능 분석을 위하여 본 논문에서는 IP 기반 위성통신에서 터보코드에 부호율 호환 펑처링을 적용시키고 무선채널은 실제 위성통신을 고려하여 레일리 페이딩과 라이시안 페이딩 두 가지 채널에 가중치를 두어 구성하였다. 재전송 기반 에러 제어 방식은 최근 고려되고 있는 여러 가지 방식 중 가장 성능이 좋은 H-ARQ Type-Ⅱ, Ⅲ 방식으로 구성하였다. 보안서비스를 암호화 알고리즘 AES, ARIA (CTR, CBC모드)로 구성하여 일반서비스 대비 위성통신망에 미치는 영향을 분석하였다.

Abstract Since the broadcast message in satellite signals the security of the data is extremely poor compared to other communication technologies such as the broadcast signal. Thus, encryption of the communication satellite has become a very important issue, an analysis of the communication performance of a general service is always required. In this paper, In order to analyze the encrypted communication the turbo code in an IP-based satellite communication applies the code rate compatible punctured and The wireless channel in consideration of the actual satellite communication was constructed by placing a weight on the Rayleigh fading and the Rician fading two channels. Retransmission-based error control scheme were constructed in the best performance of H-ARQ Type-Ⅱ, Ⅲ scheme of a number of ways that are recently considered. we analyzed the effects of normal service against a satellite communication network The security services were configured with encryption algorithms AES, ARIA (CTR, CBC mode).

Key Words : Satellite communication, encryption, ARIA, AES, BER, throughput

[*]준회원, 충북대학교 전파통신공학과
[**]준회원, 충북대학교 정보통신공학과
[***]준회원, 국가보안기술연구소
[****]정회원, 충북대학교 정보통신공학과 부교수(교신저자)
접수일자 : 2014년 11월 28일, 수정완료 : 2014년 12월 28일
게재확정일자 : 2015년 2월 13일

Received: 28 November, 2014 / Revised: 28 December, 2014
Accepted: 13 February, 2015
[****]Corresponding Author: kseokkim@cbnu.ac.kr
Department of Electrical and Electronic Engineering, Chungbuk National University, Korea

Ⅰ. 서 론

암호화는 과거에는 군사적인 용도 등의 비밀통신을 위하여 주로 사용되었으나 현재는 인터넷 기반의 사회, 경제 활동의 안정성, 신뢰성, 프라이버시 보호 등을 위한 핵심기술로서 위성통신망에도 적용하여 널리 사용되고 있다. 점차 암호화 기술은 특정분야에서 사용하는 특수 기술에서 차세대 정보 환경의 기반기술로 변화하고 있으며 중요성이 증대되고 있다. 초고속 네트워크 기반의 전자정부 시스템을 비롯해 앞으로 다가올 다양한 정보보호 환경을 대비하여 AES, ARIA 알고리즘이 널리 사용되고 있다. ARIA는 AES의 SPN 구조과 DES, Camellia의 Feistal 구조를 참고로 하는 Involution SPN (Substitution-Permutation Network) 구조이고, 128 비트 블록을 128 비트, 192 비트 그리고 256 비트의 3 종류의 키를 사용해 암·복호화를 한다. ARIA의 입, 출력 크기와 사용 가능한 키 크기는 미국 표준 블록 암호인 AES (Advanced Encryption Standard)의 입, 출력 크기 및 사용 가능한 키 크기와 동일하다[1]. 따라서 AES, ARIA 블록 암호화 알고리즘의 성능을 실제 위성통신 환경에서 평가할 필요가 있다. 본 논문에서는 AES, ARIA 알고리즘의 CTR모드와 CBC모드를 일반 위성통신망에 적용하여 일반서비스 대비 보안서비스 제공시 미치는 영향을 분석하고자 하였다.

Ⅱ. 암호화 적용 위성통신망 시스템

1. 시스템 구성

일반서비스 대비 보안서비스 제공시 통신 성능을 분석하기 위하여 먼저 일반서비스 위성통신시스템을 구성한 후 암호화 알고리즘 AES, ARIA (CTR, CBC 모드)를 적용하여 시뮬레이션을 진행하였다. 먼저 기본 IP packet을 matlab에서 생성한 후 텍스트파일로 저장하여 C프로그램에서 불러와 ARIA, AES 암호화 알고리즘을 실행하여 암호문을 생성하였다. 새로 생성된 암호문을 Turbo 인코더를 통과 시킨 후 BPSK 방식으로 변조 시킨다. 위성통신환경 시뮬레이션을 위해 Markov channel을 통과시키고 AWGN을 추가한다. 위성통신환경을 거친 변조 신호를 복조하고 Turbo 디코더를 실행하여 CRC 체크를 통해 오류비트를 체크하였다. 새로 얻은 암호문의 에러 비트를 확인하여 오류가 없다면 ACK 신호를 보내 다음 패킷을 받고, 오류가 있다면 NACK 신호를 보내 패킷을 재전송 받는다. 일련의 과정을 거친 패킷을 받아 BER, Throughput 값을 통해 통신 성능을 분석하였다.

2. 위성통신망에 적용되는 IP 패킷 구조

IP 기반 위성통신망 분석을 위하여 IP 패킷을 구성하여 시뮬레이션을 진행하였다. IP 패킷구조는 표 1. 과 IP 헤더와 페이로드 데이터 부분으로 구성되었으며 IP 헤더 20 바이트와 페이로드 데이터 492 바이트로 총 512바이

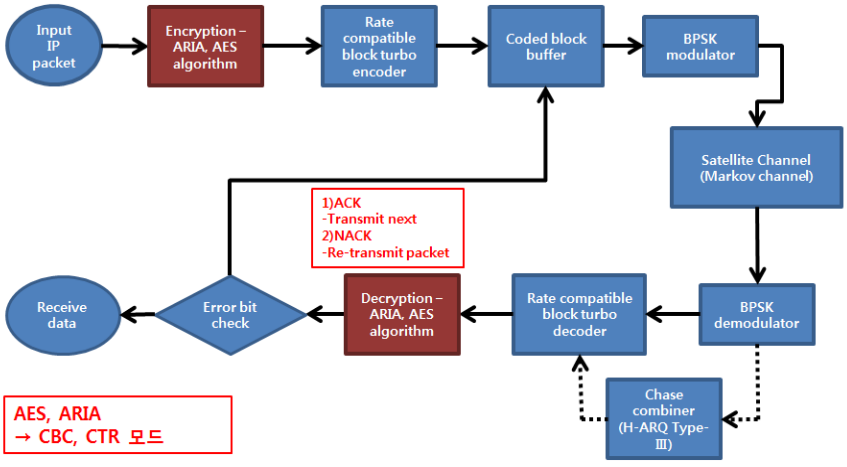


그림 1. 시뮬레이션 흐름도
Fig. 1. Simulation flow chart

트 (4096비트) 로 구성하였다. IP 헤더에는 페이로드 데이터를 설명하는 각 세션들로 구성되어 있으며 위성통신망 네트워크 상에서 IP 패킷의 구조와 길이 IP 버전 등을 나타내게 된다.

표 1. IP 패킷 구조
Table 1. IP packet structure

Version (4bits)	IHdr Len(4bits)	TOS(8bits)	Total Length in bytes(16bits)		Header (20bytes)
Identification(16bits)			Flags(3bits)	Fragment Offset(13bits)	
Time to Live(8bits)		Protocol(8bits)	Header Checksum(16bits)		
Source IP Address(32bits)					
Destination IP Address(32bits)					
Data(variable length)			Data Checksum(16bits)		Data (492bytes)

3. 위성통신망에 적용되는 터보코드 기반 H-ARQ 방식

본 연구에서 사용된 채널 코딩 방식은 RCPT(Rate Compatible Punctured Turbo code)로서 채널 인코더를 통해 생성된 패리티 비트를 유동적으로 천공시켜 H-ARQ(Hybrid-Automatic Retransmit reQuest) 방식과 결합하여 재전송하는 방식으로 시뮬레이터를 구성하였다. 허용되는 최대 전송횟수와 각 전송 당 수신 단에서 허용되는 최대 반복 복호 횟수가 사전에 정의된다. 정보원으로부터 생성된 4096개의 메시지 비트들은 CRC(Cyclic Redundancy Check) 부호화를 통해 N비트의 CRC 부호어가 되고, 이는 다시 터보 부호화를 통해 부호율 1/3인 3N 비트의 터보 모부호어(Mother code)로 변환된다. 이 터보 모부호어는 천공(Puncturing)을 통해 서브 패킷들로 만들어진 후 송신단의 버퍼에 저장되며 전송 제어 규칙에 의해 필요시 전송된다. 채널을 통과하여 수신된 서브패킷 내의 비트들은 수신단 버퍼에 저장되어 있던 수신 부호어에 추가된다. 변조 방식으로 BPSK를 사용하였고, 이를 적용할 경우 i째 전송에서 선택한 부분 패킷에 대한 변조 심볼을 $s_i = \{s_{i,j}, 0 \le l \le L_i - 1\}$ 로 두면, 수신단이 i째 전송에서 수신한 심볼 열은 다음 [식 1]과 같다.

$$r_{i,l} = \sqrt{E_{k_i}}\,\alpha_{k_i} s_{i,l} + n_{i,l} \qquad (1)$$

여기서 k_i 는 i째 전송에서 선택된 단말, E_{k_i}와 α_{k_i}는 선택된 단말의 심볼 에너지와 페이딩 이득, $n_{i,l}$은 i째 전송의 l째 심볼 구간에서의 덧셈 잡음이다.

무선 링크의 신뢰성을 보장하기 위해 사용되는 방식인 ARQ와 FEC(Forward Error Correction), 두 가지 모두를 같이 사용하는 H-ARQ가 사용되었다. 이는 보통 네트워크 프로토콜의 2계층인 데이터 링크 계층에서 널리 사용되며 채널 환경이 일시적으로 나빠진 경우에 효과적이다. 하지만 채널의 상태가 항상 나쁘다고 볼 수 없기에 H-ARQ를 사용하여 스스로 복구할 수 있게 된다면 재전송의 개수를 줄일 수 있게 된다.

펑처링은 기존의 채널 코딩된 부호의 출력을 주기 P 마다 적절히 소거하는 것이다. 기존 채널 부호기의 부호율이 1/N 이고, 그 부호를 주기 P 마다 펑처링한다고 하면, 부호율 R은 다음과 같은 범위에서 가변 할 수 있다.

$$R = \frac{P}{P+l},\ l = 1,2,...,(N-1)P \qquad (2)$$

H-ARQ 방식의 모부호어율은 1/3로 설정 되었으며 최초 전송 시의 펑처링 부호화율은 4/5를 사용하였다. 메시지 비트를 펑처링하게 되면 MAP 복호 알고리즘의 적용상에서 성능 저하를 가져오게 되기 때문에 BER이 증가하게 되고, 처리율 저하가 발생하여 재전송 횟수가 증가하게 된다.

표 2. 펑처링 Table
Table 2. Puncturing table

Puncturing table	Rate
1111 1000 0000	4/5
1111 1010 0000	2/3
1111 1010 0101	1/2
1111 1001 1110	4/9
1111 1111 0101	2/5
1111 1111 1110	4/11
1111 1111 1111	1/3

4. 마르코프 위성 무선채널

일반 무선 통신에서 채널은 페이딩의 종류에 따라 다음 세 가지 페이딩 채널로 구분이 된다. 이 채널을 구분하는 팩터는 Rician K-factor로 LOS(Line-of-Site) 성분의 파워값과 NLOS (Non-Line-of-Site)의 성분의 파워값의 비율로 나타난다. 이 K-factor의 값이 -40dB 이하

이면 Rayleigh fading 채널이고, -40dB 이상 15dB 이하이면 Riciac fading 채널이며, 15dB 이상인 무선 채널인 경우 Log-normal fading 채널로 정의한다. 본 연구에서 위성 무선채널은 완전한 Rayleigh, Rician 일 수 없기 때문에 2개의 채널이 존재한다고 가정한 후 가중치를 주어 시뮬레이션을 진행하였다. Rayleigh channel 20%, Rician channel 80%로 가중치를 주어 마르코프 체인에 적용하여 2가지 상태의 마르코프 체인 무선채널을 구성하였다.

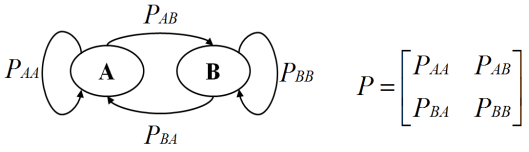


그림 2. 마르코프 체인 채널
Fig. 2. Markov chain channel

Ⅲ. 위성통신망에 적용되는 암호화 알고리즘

1. ARIA 및 AES 알고리즘 비교

ARIA는 암호의 난이도에 따라서 128, 192, 256비트 길이의 암호키를 선택할 수 있으며, 128비트 데이터 블록에 대해 암호화, 복호화를 수행한다. 암호화, 복호화는 Involution SPN 구조를 가지며, 키의 길이에 따라서 라운드 함수가 12, 14, 16번 반복 실행한다. 라운드 함수에 필요한 라운드 키는 암호키로부터 키 확장을 통해서 생성한다.

DES의 안정성에 대안으로 1997년에 새 표준에 대한 작업을 시작하여 2000년 10월에 AES라는 새 표준을 채택하였다. 1997년 새 표준에 대한 제안에 의하면 새암호 알고리즘의 블록 크기는 128비트이어야 하며, 알고리즘에 대한 변경 없이 128비트, 196비트, 256비트 길이의 키를 지원해야 한다. 1998년도에 제출된 여러 제안 중에 15개를 일차적으로 선정하였고, 1999년에 이 중에 다섯 개를 최종 후보로 선정하였다. 이 중에 벨기에 암호학자인 Daemen과 Rijmen이 제안한 Rijndael 암호알고리즘이 AES로 채택되었다[3].

가. CTR (CounTeR) 모드

DES의 안정성에 대한 여러 가지 공격 방법들이 발표되면서 미국의 NIST에서는 1998년에 차세대 블록 암호 알고리즘인 AES를 공모하였다. 그 후 2년간의 심사과정을 걸쳐 2000년에 Rijndael을 AES 알고리즘으로 선정하였으며, 2001년에 표준으로 채택되었으며 FIPS-197로 등록되었다. CTR 모드 AES 알고리즘은 암호화와 복호화 모두에서 라운드 키 추가 단계를 시작으로 4단계 과정으로 이루어진 9회의 라운드가 진행되고, 3단계 과정으로 이루어진 마지막 10번째 라운드가 실행된다. 라운드 키 추가 단계에서만 유일하게 키 값을 사용하며, 이 때문에 암호는 라운드 키 덧셈 단계로 시작되고 끝난다. 각 단계는 역이 가능하며 라운드 키 추가 단계에 대한 역함수는 같은 라운드 키를 블록에 XOR하여 얻을 수 있다. 복호화 알고리즘은 확장키의 역순을 사용하여 이루어지고 복호화 알고리즘과 암호화 알고리즘은 동일하게 진행된다[4].

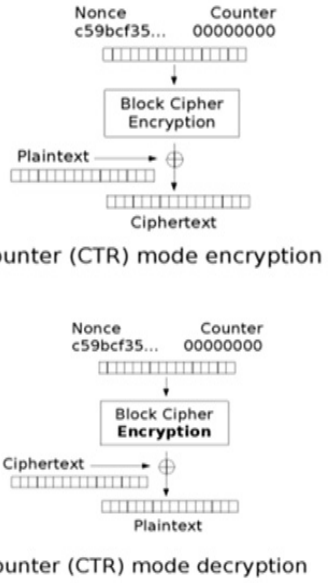


그림 3. CTR 모드 구성도
Fig. 3. CTR mode structure

나. CBC (Cipher Block Chaining) 모드

CBC 모드 알고리즘은 전단의 암호화 했던 데이터가 다음 암호화에 영향을 미치게 된다. 각 단계는 역이 가능하며 라운드 키 추가 단계에 대한 역함수는 같은 라운드 키를 블록에 XOR하여 얻을 수 있다. 복호화 알고리즘은 확장키의 역순을 사용하여 이루어지나, 복호화 알고리즘과 암호화 알고리즘은 동일하지 않아 각 암·복호화 알고리즘이 필요하다[2].

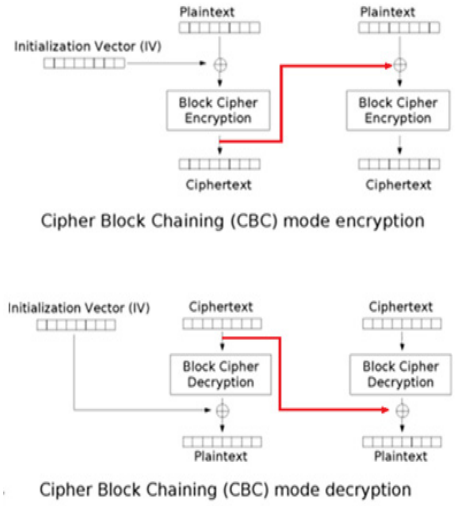


그림 4. CBC 모드 구성도
Fig. 4. CBC mode structure

Ⅳ. 시뮬레이션 결과 및 분석

1. 시뮬레이션 환경

본 연구에서 송신주파수는 무궁화 5호 다운링크에서 가장 높은 20.7GHz를 사용하였고, IP 패킷 길이는 2^{12} (4096)비트를 사용하였다. 채널코더는 RCPT (Rate Compatible Punctured Turbo codes)로 하였고 디코더는 MAP 알고리즘을 사용하였다. 전송방식은 무선링크의 신뢰성을 보장하기 위해 Hybrid ARQ을 사용하였다. 본 연구에서는 H-ARQ Type-Ⅱ, H-ARQ Type-Ⅲ 방식을 사용하였다. 최대 재전송 횟수는 6으로 제한하였다. 전송 채널은 위성통신환경을 구성하기위해 Markov channel (Rician 80%, Rayleigh 20%)을 통과하고, AWGN을 더하는 방식으로 구성하였다. SNR 범위는 -10dB ~ 10dB 이고, 1dB씩 변화한다. 마지막으로 암호화 알고리즘으로는 AES, ARIA (CTR, CBC 모드)를 사용하였다.

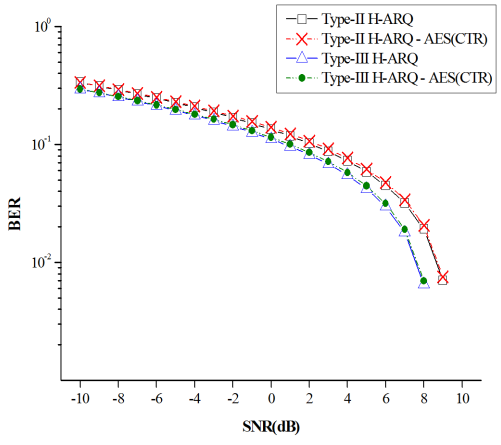
표 3. 시뮬레이션 환경
Table 3. The environment of Simulation

Parameter	Value
Satellite Type	KOREASAT 5, Geosynchronous Earth Orbit (GEO)
Frequency	20.7 GHz
Information sequence length	K=2^{12}(4096) bits
Channel coder	RCPT
Channel decoder	MAP Algorithm
H-ARQ	Hybrid Type-Ⅱ, Hybrid Type-Ⅲ
	(Max. retransmissions 6)
Modulation/ demodulation	BPSK
Channel	Markov channel (Rician 80%, Rayleigh 20%)
SNR range	-10 dB ~ 10 dB (step : 1)
Encryption Algorithm	AES, ARIA
	(CBC, CTR mode)

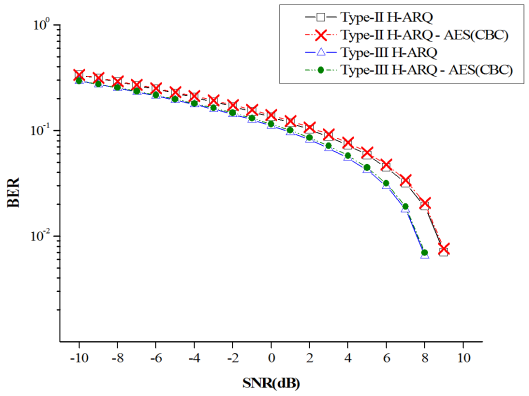
일반서비스 대비 보안서비스 제공시 나타나는 성능을 분석하기 위해 BER 및 Throughput 데이터를 얻었다.

2. BER

보안서비스 AES와 ARIA를 시뮬레이션 결과를 통해 비교하면 다음 그림 5.과 그림 6.과 같다. BER을 비교하였을 때, AES 알고리즘이 ARIA 알고리즘보다 좋은 성능을 보였다. H-ARQ Type-Ⅲ에서는 SNR 1dB 이전에는 ARIA가 좋았으나, SNR 1dB 이후에 AES 알고리즘이 ARIA 알고리즘보다 좋은 BER을 보였다. ARIA를 적용하였을 때, AES 보다 BER이 저하되는 것을 볼 수 있었다. 또한, CTR 모드가 CBC 모드보다 약간 좋은 성능을 보였다.



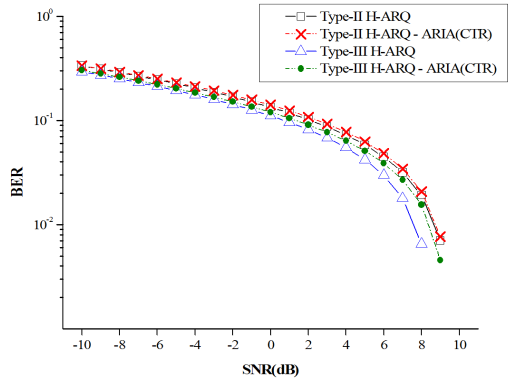
(a)



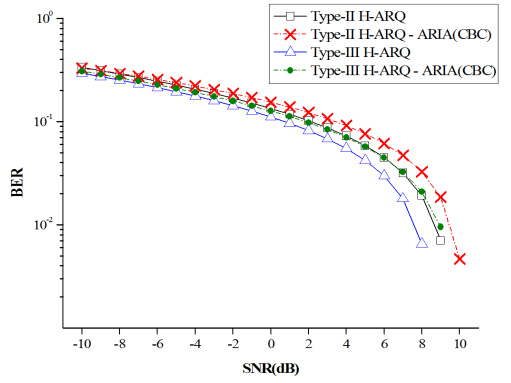
(b)

그림 5. AES 알고리즘 적용 시 H-ARQ에 따른 BER 성능 비교 (a) CTR 모드 (b) CBC 모드

Fig. 5. BER performance comparison associated with the H-ARQ in AES Algorithm environment (a) CTR mode (b) CBC mode



(a)



(b)

그림 6. ARIA알고리즘 적용 시 H-ARQ에 따른 BER 성능 비교 (a) CTR 모드 (b) CBC 모드

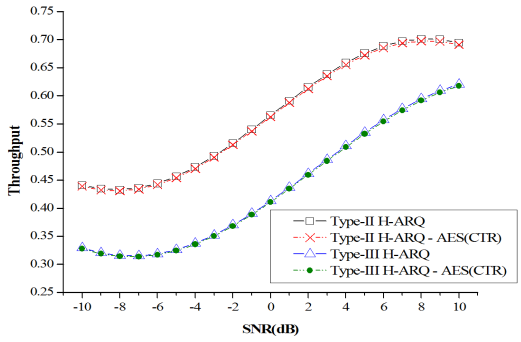
Fig. 6. BER performance comparison associated with the H-ARQ in ARIA Algorithm environment (a) CTR mode (b) CBC mode

3. 처리율 (Throughput)

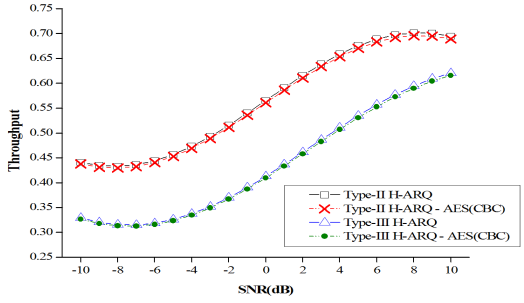
본 논문에서는 위성통신망 시스템의 성능을 판단하는 척도로 처리율을 고려하였다. 정의된 처리율은 하나의 비트를 전송함으로써 수신단이 얻을 수 있는 오류 없는 메시지 비트의 정도이며, [식 3]으로 정의 된다.

$$\eta = \left(\frac{\sum_{i=1}^{N} K_i}{\sum_{i=1}^{N} N_i} \right) (1 - BER) \qquad (3)$$

여기서 K는 패킷 당 정보비트 수이고 N은 재전송 과정에서 정보비트와 패리티 비트의 합인 전체 전송비트 수이며 i는 재전송 횟수를 의미한다. 재전송 시 패리티 비트만을 전송하는 H-ARQ Type-Ⅱ 방식이 재전송 시 정보비트와 패리티 비트를 모두 전송하는 H-ARQ Type-Ⅲ 방식보다 Throughput 면에서 높은 성능을 보이게 되고 반면 BER 성능은 떨어지게 된다.



(a)



(b)

그림 7. AES 알고리즘 환경에서 H-ARQ에 따른 Throughput 성능 비교 (a) CTR 모드 (b) CBC 모드

Fig. 7. Throughput performance comparison associated with the H-ARQ in AES Algorithm environment (a) CTR mode (b) CBC mode

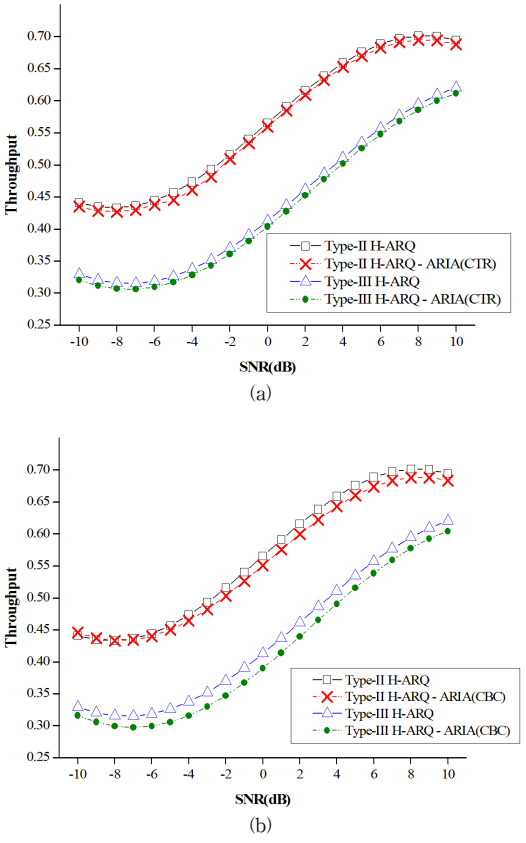


그림 8. `ARIA 알고리즘환경에서 H-ARQ에 따른 Throughput 성능 비교 (a) CTR 모드 (b) CBC 모드

Fig. 8. Throughput performance comparison associated with the H-ARQ in ARIA Algorithm environment (a) CTR mode (b) CBC mode

Throughput도 AES가 ARIA 보다 효율이 좋음을 알 수 있다. 분석 결과 암호화 알고리즘을 사용해 암호문을 구성하였을 때, 일반 시스템 대비 BER이 약 90%의 성능을 보이는 것을 볼 수 있었다. 이는 평문을 암호문으로 변경하였을 때 생성되는 랜덤한 정보비트를 채널 인코더와 무선채널, 채널 디코더를 통과할 시 비트가 깨질 확률이 증가하기 때문이다. 이는 정보비트가 아닌 보안헤더 추가 시 보내지는 비트수가 증가함에 따라 비트가 깨질 확률이 높아지게 되고 그로인해 평균 전송횟수와 Throughput의 성능이 저하되는 것을 보였다. 또한 CBC 모드가 CTR모드보다 성능이 저하되는 것을 보였다.

Ⅵ. 결 론

위성통신은 고속 데이터 전송, 지형 및 지물의 영향을 받지 않는 서비스 제공, 자연 재해에 강하고 사고에 의한 절단이 없어 주요 회선의 예비통로로서의 이용가치가 높아 수요와 필요성이 증대되고 있는 현실이다. 하지만 전송의 지연 문제나 통신의 보안문제는 위성 통신이 가지고 있는 문제점이라 할 수 있다. 본 연구에서는 일반서비스 대비 보안서비스 제공시 통신 성능을 분석하기 위하여 먼저 일반서비스 위성통신시스템을 구성한 후 암호화 알고리즘 AES, ARIA (CTR, CBC 모드)를 적용하여 시뮬레이션을 진행하였다. 위성통신망 시스템을 거친 후 일반서비스와 보안서비스 제공 시 패킷을 받아 BER, Throughput 값을 통해 통신 성능을 분석하였다. 분석 결과 AES, ARIA 암호화 알고리즘을 사용해 암호문을 구성하였을 때 일반 평문을 시뮬레이션 했을 때 대비 BER과 Throughput 성능이 약 90%의 성능을 보이는 것을 볼 수 있었다. 또 CTR모드가 CBC모드보다 성능이 좋은 것을 확인하였다. 본 연구에서 도출된 연구 결과를 바탕으로 위성 데이터 통신망 IP 중계 모뎀에서 보안서비스 추가 패킷에 따른 통신 특성을 시뮬레이션을 통해 분석하고 그 결과를 이용해 위성통신망에서 보안서비스 제공여부를 확인할 수 있으리라 기대한다.

References

[1] Jinsub Park et al., “Design and Implementation of ARIA Cryptic Algorithm”, The Institute of Electronics and Information Engineers, vol. 42, no. 4, 2005.

[2] Deepshikha Garg and Fumiyuki Adachi, “Application of Rate Compatible Punctured Turbo Coded Hybrid ARQ to MC-CDMA Mobile Radio”, ETRI Journal, vol. 26, no. 5, Oct., 2004.

[3] Francesco Chiti and Romano Fantacci, “A Soft Combining Hybrid-ARQ Technique Applied to Throughput Maximization within 3G Satellite IP Network”, IEEE Trans. Vehicular Technology., vol. 56, no.2, Mar., 2001.

[4] D. N. Rowitch, L. B. Milstein, “On the Performance of Hybrid FEC/ARQ Systems Using Rate Compatib

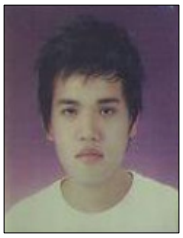
le Punctured Turbo(RCPT) Codes", IEEE Trans. Commun., vol.48, no.6, June., 2000.

[5] Sunghyun Choi and Kang G. Shin, "A Class of Adaptive Hybrid ARQ Schemes for Wireless Links", IEEE Trans. Vehicular Technology., vol. 50, no. 3, May., 2002.

[6] Jung-Fu Cheng, "Coding Performance of Hybrid ARQ Schemes" IEEE Trans. Commun., vol. 54, no.6, June., 2002.

저자 소개

정 원 호(준회원)



- 2011년 2월 : 충북대학교 정보통신공학과 졸업
- 2013년 2월 : 충북대학교 전파공학과 대학원(공학석사)
- 2013년 3월 ~ 현재 : 충북대학교 전파통신공학과 대학원(박사 과정)

<주관심분야 : 전파전파, MIMO 무선채널, 채널모델, 위성 통신, 무선 통신 암호화 알고리즘>

여 봉 구(준회원)

- 2009년 2월 ~ 현재 : 충북대학교 정보통신공학과

<주관심분야 : 위성 통신 분석, 무선 통신 암호화 알고리즘 >

김 기 홍(준회원)

- 1998년 2월 : 경북대학교 졸업(학사)
- 2000년 2월 : 경북대학교 졸업(석사)
- 2007년 8월 : 고려대학교 졸업(박사)
- 1999년 12월 ~ 2000년 9월 : LG전자(주)
- 1999년 12월 ~ 현재 : 한국전자통신연구원 부설연구소 선임연구원

<주관심분야 : 유무선 통신, 신호처리, 정보보호>

박 상 현(준회원)

- 1993년 2월 : 충남대학교 졸업(학사)
- 1996년 2월 : 충남대학교 졸업(석사)
- 2008년 2월 : 충남대학교 졸업(박사)
- 1996년 1월 ~ 2000년 11월 : 국방과학연구소
- 2000년 11월 ~ 현재 : 한국전자통신연구원 부설연구소 책임연구원

<주관심분야 : 정보보호, VPN, VoIP>

양 상 운(준회원)

- 1992년 3월 : 충북대학교 졸업(학사)
- 1998년 3월 : 충북대학교 졸업(석사)
- 2010년 3월 : 충북대학교 졸업(박사)
- 1992년 3월 ~ 2000년 4월 : 국방과학연구소
- 2000년 5월 ~ 현재 : 한국전자통신연구원 부설연구소 책임연구원

<주관심분야 : 위성관제 및 통신, IoT기기 보안, 고성능 IPSec 암호프로세서, 스마트그리드 보안>

임 정 석(준회원)

- 1987년 2월 : 한양대학교 졸업(학사)
- 1989년 2월 : 한양대학교 졸업(석사)
- 2007년 2월 : 한양대학교 졸업(박사)
- 1989년 2월 ~ 2000년 1월 : 국방과학연구소
- 2000년 2월 ~ 현재 : 한국전자통신연구원 부설연구소 책임연구원

<주관심분야 : 채널코딩, 유무선 통신, 정보보호>

김 경 석(정회원)

- 1989년 1월 ~ 1998년 12월 : 한국전자통신연구원 무선통신연구단 선임연구원
- 1999년 1월 ~ 2002년 3월 : University of Surrey(영국) 전기전자공학과 대학원 졸업(공학박사)
- 2002년 2월 ~ 2004년 8월 : 한국전자통신연구원 이동통신연구단 책임연구원
- 2004년 9월 ~ 2005년 2월 : 전북대학교 생체정보공학부 전임강사
- 2005년 3월 ~ 현재 : 충북대학교 정보통신공학과 부교수

<주관심분야 : SDR, Cognitive Radio, MIMO-OFDM, 전력선통신, 가시광통신, 디지털라디오, 전파채널분석, 전파감시/관리시스템, 위성망분석>