The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 5, pp.147-154, Oct. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.5.147
JIIBC 2015-5-18

IPsec VPN 위성통신에서 인증알고리즘이 미치는 영향 분석

Effect Analysis of a Authentication Algorithm in IPsec VPN Satellite Communication

정원호*, 황란미*, 여봉구*, 김기홍**, 박상현**, 양상운**, 임정석**, 김경석***

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

요 약 위성통신망은 방송과 마찬가지로 지구국만 갖추고 있다면 누구나 수신이 가능한 특성을 가져 반드시 보안이 요구되는 내용이 있다면 암호화를 행해 주어야 한다. 본 논문에서는 위성통신망 IPsec VPN에서 전송모드 AH 보안헤더를 추가하여 인증데이터 부분에 인증알고리즘 MD-5와 SHA-256을 적용하여 BER과 Error rate 및 Throughput을 분석하였다. 먼저 일반 IP 패킷을 생성하여 IPsec 전송모드 AH 보안헤더를 추가하여 내부 인증 데이터를 SHA-256 및 MD-5알고리즘을 적용하여 구성하였다. 채널코더는 Rate Compatible Punctured Turbo Codes를 적용하였고, 패킷 재전송 기법은 Hybrid-ARQ Type-Ⅱ와 Type-Ⅲ을 사용하였다. 변조방식은 BPSK를 적용하였고, 무선채널은 마르코프 채널 (Rician 80%, Rayleigh 20%와 Rician 90%, Rayleigh 10%)로 위성채널 상태에 따라 인증알고리즘이 에러율과 Throughput에 어떤 영향을 미치는지 분석하였다.

Abstract Satellite broadcasting networks, like if you have if you have just received information that everyone must bring the required security attributes this earth should be done as encryption. In this paper, a satellite communication network AH additional security header in transport mode IPsec VPN by applying the SHA-256 and MD-5 authentication algorithm to authenticate the data portion Error rate and analyze the BER and Throughput. First, to generate a normal IP packet added to IPsec transport mode security header AH were constructed internal authentication data by applying the SHA-256 and MD-5 algorithm. Channel coder was applied to the Rate Compatible Punctured Turbo Codes, packet retransmission scheme Hybrid-ARQ Type-Ⅱ and Type-Ⅲ were used. Modulation method was applied to the BPSK, the wireless channel Markov channel (Rician 80%, Rayleigh 20% and Rician 90%, Rayleigh 10%) as an authentication algorithm according to the satellite channel state analyzed how they affect the error rate and Throughput.

Key Words : Satellite communication, security, encryption, IPsec VPN, HARQ, BER, Throughput

*준회원, 충북대학교 전파통신공학과
**준회원, 국가보안기술연구소
***정회원, 충북대학교 정보통신공학과 부교수(교신저자)
접수일자 : 2015년 5월 29일, 수정완료 2015년 8월 29일
게재확정일자 : 2015년 10월 9일

Received: 29 May, 2015 / Revised: 29 August, 2015 / Accepted: 9 October, 2015
***Corresponding Author: kseokkim@cbnu.ac.kr
Department of Electrical and Electronic Engineering, Chungbuk National University

Ⅰ. 서 론

인증은 보안에 있어서 중요한 이슈이다. 이는 어떤 메시지를 키와 함께 암호화 하여 수신측에서 이를 검사하여 인증하는 식으로 진행되는데, 디지털 서명의 개념도 이와 비슷하다고 할 수 있다. 이러한 디지털 서명, 메시지 인증에서 메시지는 주로 키와 함께 해쉬되어 그 결과 값이 전송된다. 본 연구에서는 인증 데이터가 보안서비스 제공시 통신 성능에 어떤 영향을 미치는지 분석하기 위해 두 가지의 알고리즘 MD-5, SHA-256을 적용하여 시뮬레이션을 수행하였다. IPSec은 Internet Protocol Security의 약어로서 network 통신 중 network layer에서의 보안을 위한 표준으로 인터넷 상에서 VPN(Virtual Private Network)을 구현하는데 사용될 수 있도록 IETF (Internet Engineering Task Force)에서 개발된 프로토콜이다. 이는 안전에 취약한 인터넷에서 안전한 통신을 실현하는 통신 규약으로서 인터넷상에 전용 회선과 같이 이용 가능한 가상적인 전용 회선을 구축하여 데이터를 도청당하는 등의 행위를 방지하기 위한 통신 규약이다. IPSec은 네트워크나 네트워크 통신의 패킷 처리 계층에서의 보안을 위해, 지금도 발전되고 있는 표준으로 이전의 보안 기법들에서는 보안이 통신 모델의 응용 계층에 삽입되었었다. IPSec은 가상 사설망과 사설망에 다이얼업 접속을 통한 원격 사용자 접속의 구현에 특히 유용할 것이다. IPSec은 본질적으로 데이터 송신자의 인증을 허용하는 인증 헤더와 송신자의 인증 및 데이터 암호화를 함께 지원하는 ESP(Encapsulating Security Payload) 두 종류의 보안 서비스를 제공한다[1]. 이 논문은 2장에서 본 연구를 위한 위성통신 시스템과 분석 과정에 대해 기술하였고, 3장에서는 IPsec 기반 인증 알고리즘인 MD-5, SHA-256에 대해 설명하였고, 4장에서는 시뮬레이션 결과를 바탕으로 인증 알고리즘에 대해 분석하였으며, 5장의 결론으로 본 논문을 마무리한다.

Ⅱ. IPsec VPN 기반 위성 통신 시스템

이 논문에서의 주파수는 우리나라 위성인 무궁화 5호 (KOREASAT 5) 다운링크에서 가장 높은 송신 주파수인 20.7 GHz를 사용하였고, IP Packet의 길이는 2^{12}(4096) 비트를 사용하였다. 채널 코딩은 RCPT(Rate Compatible Punctured Turbo codes)로 적용하였고, 디코더는 MAP(Maximum A Posteriori) 알고리즘을 사용하였다. 전송방식은 무선링크의 신뢰성을 보장하기 위해 Type-Ⅱ HARQ 방식과 Type-Ⅲ HARQ 방식을 사용하였고, 최대 재전송 횟수는 6으로 제한하였다[2][3]. SNR 범위는 -10 dB에서 10 dB로 1 dB씩 간격으로 두어 변화한다. 또한 암호화 알고리즘으로 사용한 ARIA는 CTR 모드를 사용하였다. 전송 채널은 위성 통신 환경을 구성하기위해 Markov 채널을 Rician 80%, Rayleigh 20%로 구성하여 통과시키고, AWGN을 더하는 방식으로 구성하였다. IPsec 보안 시스템은 전송모드에서 AH를 적용하였다.

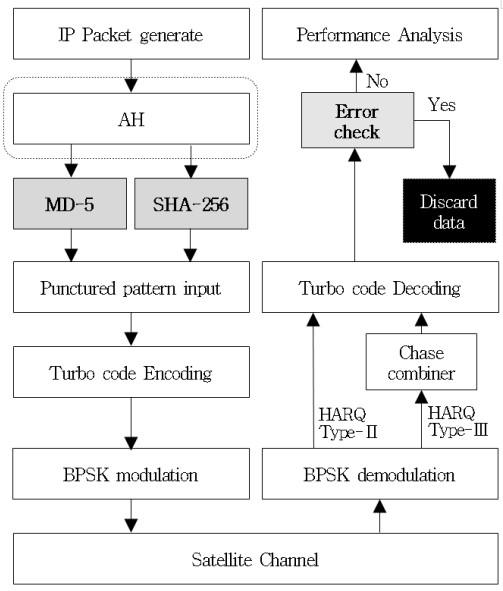


그림 1. IPsec VPN의 시뮬레이션 흐름도
Fig. 1. Simulation flow chart of IPsec VPN

IP SEC 프로토콜 구조는 AH (24bytes)를 구성하였고 전송 모드를 사용하였으며 인증 알고리즘은 SHA-256과 MD-5를 사용하여 인증 데이터 부분을 구성하였다. 암호화된 IP 패킷 데이터가 위성 채널을 통과하여 채널 디코딩과 암호화와 복호화 과정을 거친 후 인증 알고리즘에 따라 Error 체크를 하여 인증 데이터 부분의 값이 깨지게 되면 암호화 장비에서 데이터를 모두 버리게 된다고 가정하고 Error rate를 계산하였다. 인증 데이터 부분의 값이 깨진 경우 BER 체크는 하지 않고 Error가 발생하지 않은 경우에만 BER을 체크하여 시뮬레이션을 진행하였다. 전체적인 시뮬레이션 구성도는 그림 1에 나타나 있다. 그림 1에서 점선으로 표시된 AH(Authentication Header)는 그림 2와 같이 나타 낼 수 있다.

Next Header (8)	Payload Length (8)	Reserved (16)
SPI(Security Parameters Index) (32)		
Sequence Number (32)		
Authentication Data (32*n)		

그림 2. AH Header 구조
Fig. 2. Structure of AH Header

AH는 비연결형 무결성 및 데이터 발신자 인증 보안 서비스를 제공하는 헤더로, 수신자의 처리에 따라서 재전송 공격에 대한 방어를 제공할 수 있다. AH는 24바이트가 추가되게 된다. 이 논문에서는 전송모드에서의 AH를 고려하였고 그 구조는 그림 3과 같다[4].

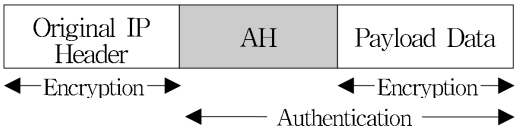


그림 3. 전송 모드에서 AH 구조
Fig. 3. Structure of AH in Transport mode

Ⅲ. 인증 알고리즘 (MD-5, SHA-256)

MD-5 알고리즘과 SHA-256은 같은 MD-4 알고리즘을 기반으로 개발되어 무결성 검사 등에 사용되며 구조상의 큰 차이점은 없고 각 라운드 연산 수식, 해쉬 출력 크기 및 충돌 유무, 입력 길이 한계에 의해 차이가 난다.

표 1. MD-5와 SHA-256 비교
Table 1. Comparison between MD-5 and SHA-256

알고리즘	MD-5	SHA-256
해쉬 값 크기	128 비트	256 비트
내부 상태 크기	128 비트	256 비트
블록 크기	512 비트	512 비트
과정 수	64 단계	64 단계
최대 입력 비트 수	무한대	2^{64}
장점	X	아직 해쉬 충돌, 공격법이 발견되지 않음
단점	해쉬 충돌 공격법 존재	X

MD(Message Digest)-5 알고리즘은 Ron Rivest가 1990년에 개발한 MD-4 알고리즘을 개선한 것으로써, 빠른 소프트웨어 구현을 위해 디자인된 해쉬 함수를 기반으로 하고 있으며 공개키 암호화 시스템에서 암호 키와 함께 압축되는 암호화 전자서명 및 무결성 검사에 주요 이용될 목적으로 고안되었다. MD-5 알고리즘의 규격은 IETF RFC 1321에 명시되어 있다. 임의의 값을 입력 받아 128비트의 해쉬 값으로 출력하는 알고리즘으로 현재는 알고리즘 공격 및 충돌이 발견되어 사용을 권장하지 않고 있다. 반면 SHA(Secure Hash Algorithm)는 MD-5 알고리즘보다 뛰어난 알고리즘으로 1993년 미국 표준 기술 연구소(NIST)에 의해 설계되었다. 설계된 순서에 따라 SHA-0, SHA-1, SHA-2라 불리고 해쉬값 크기에 따라 SHA-1, SHA-224, SHA-256, SHA-384, SHA-512로 구분이 된다. SHA-256은 구조상으로는 MD-5와 유사하지만 MD-5 알고리즘이 128비트의 암호값으로 출력하는 반면 SHA-256은 임의의 메시지를 256비트 길이의 암호값으로 출력된다. 또한 MD-5 알고리즘은 공격법, 충돌이 발견되어 사용을 권장하지는 않지만 SHA-256은 공격법, 충돌이 발견되지 않아 현재 많이 사용되고 있다[5]. 따라서 본 연구에서는 SHA-256 인증 알고리즘을 사용하여 인증데이터를 구성하여 시뮬레이션을 진행하였다.

MD-5 알고리즘에서는 128비트(4단어)의 단일 연산처리를 한 라운드라고 하며 한 라운드 당 연산수는 16번, 4 단어(한 라운드) 당 연산수는 64번 수행된다. 그림 4의 MD-5 단일연산을 수식인 수식 (1)로 표현 할 수 있다.

반면 SHA-256 알고리즘은 256비트(8개의 단어)를 한 번에 처리하며 그 단위를 라운드라 한다. SHA-256에서는 MD-5 알고리즘과는 다르게 블록 비트를 여러 개의 비트로 조합하여 단일 연산에 더하는 연산을 추가한다. 한 라운드 당 연산횟수는 64회이며 한 번의 계산으로 256비트(8개의 32 비트)의 연산 결과가 나온다. 그림 5의 SHA-256 단일연산을 수식인 수식 (2)로 표현 할 수 있다[6].

$$B \leftarrow A + CLS_s(A + F(B,C,D) + X[k] + T[i]) \qquad (1)$$

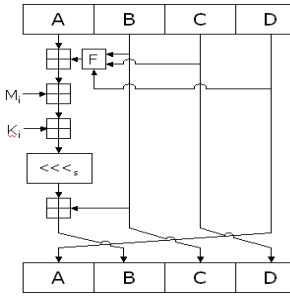


그림 4. MD-5 단일연산
Fig. 4. Single Operation of MD-5

$$A \leftarrow H + \sum_1(E) + Ch(E,F,G) + K_j + W_j + \sum_0(A) + Maj(A,B,C) \quad (2)$$
$$E \leftarrow D + H + \sum_1(E) + Ch(E,F,G) + K_j + W_j$$

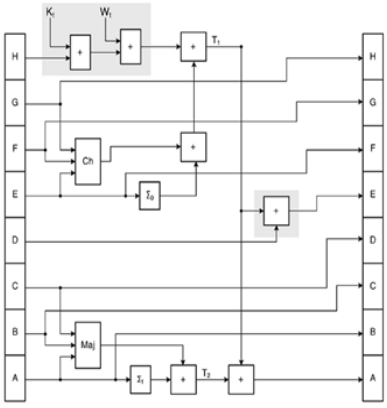


그림 5. SHA-256 단일연산
Fig. 5. Single Operation of SHA-256

Ⅳ. 시뮬레이션 결과 및 분석

표 2. 시뮬레이션 파라미터
Table 2. Simulation Parameters

Parameter	values	
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	
HARQ	Hybrid Type-Ⅱ, Hybrid Type-Ⅲ (Max. retransmissions 6)	
Modulation/ demodulation	BPSK	
Channel	Markov channel (Rician 80%, Rayleigh 20%) (Rician 90%, Rayleigh 10%)	
IPsec	Transport mode	
	AH(Authentication Header)	
	Authentication data	MD-5
		SHA-256
SNR range	-10 dB ~ 10 dB (step : 1)	

시뮬레이션 파라미터는 표 2에 표시된 것 과 같이 인증 암호화 알고리즘 SHA-256, MD-5가 추가되었고 AH 헤더와 전송 모드만 고려하였으며 무선채널 환경을 Markov channel (Rician 80%, Rayleigh 20%)와 Markov channel (Rician 90%, Rayleigh 10%)로 나누어 성능 비교를 하였다. 시뮬레이션 결과는 일반 BER과 인증 암호화 알고리즘 간의 성능 분석을 위하여 Error Rate로 측정하고 분석하였다.

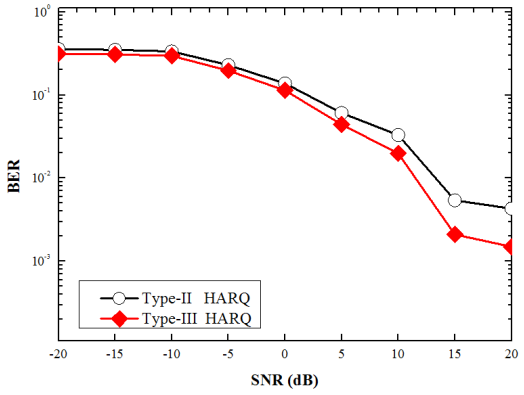


그림 6. Rician 80%, Rayleigh 20% 환경에서 HARQ에 따른 BER 성능 비교 (SHA-256)
Fig. 6. BER performance comparison associated with the HARQ in Rician 80%, Rayleigh 20% environment (SHA-256)

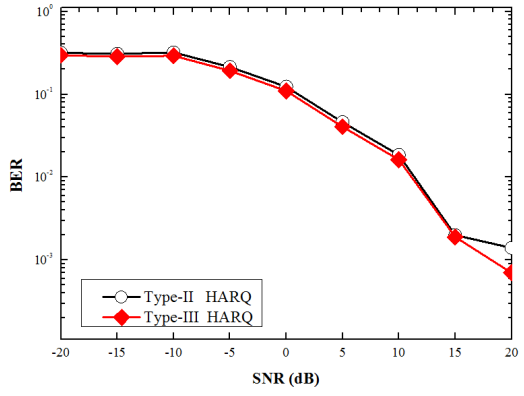


그림 7. Rician 90%, Rayleigh 10% 환경에서 HARQ에 따른 BER 성능 비교 (SHA-256)
Fig. 7. BER performance comparison associated with the HARQ in Rician 90%, Rayleigh 10% environment (SHA-256)

그림 6은 HARQ 방식에 따른 BER을 나타낸 그래프이다. 그림 7의 결과가 채널 상태가 그림 6의 환경보다 나아졌기 때문에 전체적인 성능이 향상 된 것을 볼 수 있다.

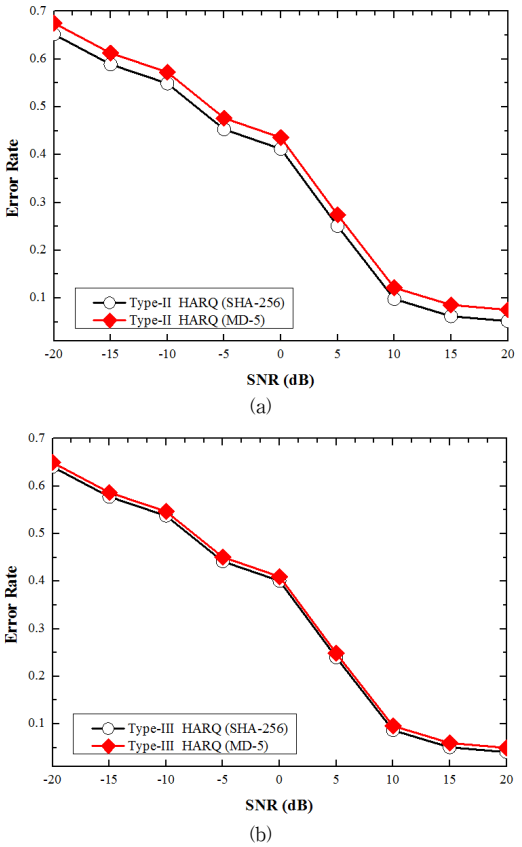


그림 8. Error rate (Rician 80%, Rayleigh 20%)
(a) Type II HARQ (b) Type III HARQ
Fig. 8. Error rate (Rician 80%, Rayleigh 20%)
(a) Type II HARQ (b) Type III HARQ

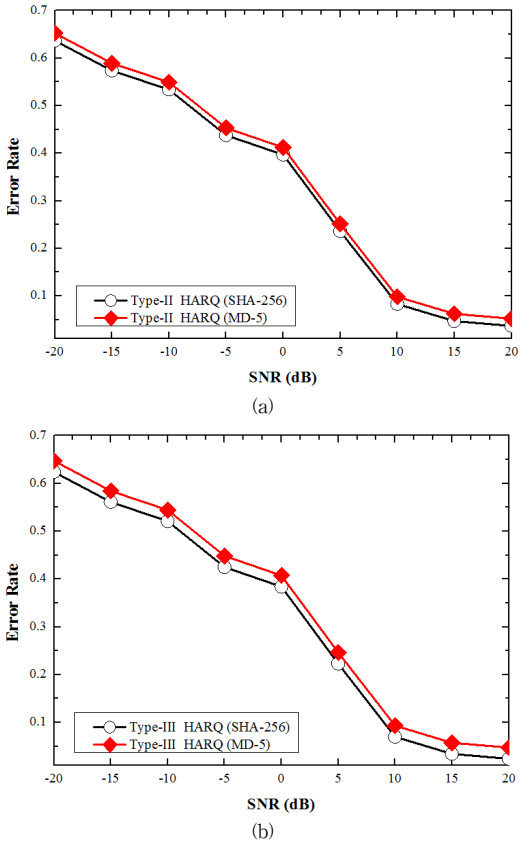
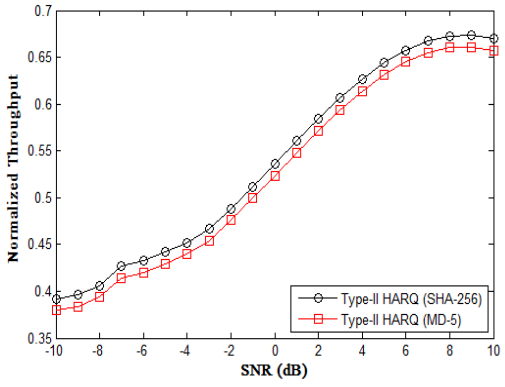


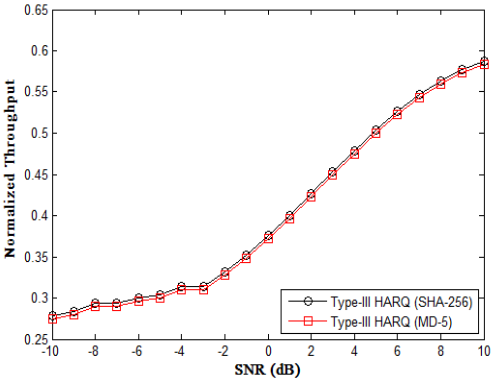
그림 9. Error rate (Rician 90%, Rayleigh 10%)
(a) Type II HARQ (b) Type III HARQ
Fig. 9. Error rate (Rician 90%, Rayleigh 10%)
(a) Type II HARQ (b) Type III HARQ

그림 8은 무선채널이 Rician 80%, Rayleigh 20%인 환경으로 SHA-256와 MD-5의 인증 암호화 알고리즘을 적용하여 Error rate를 시뮬레이션을 한 결과이다. 그림 8-(a)는 Type Ⅱ HARQ 방식이고 그림 8-(b)는 Type Ⅲ HARQ 방식을 적용한 그래프이다. Type Ⅲ HARQ 결과가 Type-Ⅱ 방식보다는 성능이 향상 된 것을 볼 수 있는데 이는 Type-Ⅲ 방식에서는 NACK 신호가 들어와 재전송 과정에서 생성된 패리티 비트와 정보 비트를 모두 재전송하기 때문에 오류 정정 기능이 향상되기 때문이다. 인증 암호화를 적용한 SHA-256와 MD-5의 그래프에서는 SHA-256을 적용한 것이 Error rate가 MD-5 적용 대비 약 10% 좋음을 볼 수 있다. 이는 SHA-256와 MD-5의 해쉬값 차이로 인해 생성 암호비트의 길이가 달라져 성능 차이가 나는 것을 볼 수 있다.

그림 9는 무선채널이 Rician 90%, Rayleigh 10%인 환경으로 SHA-256와 MD-5의 인증 암호화 알고리즘을 적용하여 Error rate를 시뮬레이션을 한 결과이다. 그림 9-(a)는 Type Ⅱ HARQ 방식이고 그림 9-(b)는 Type Ⅲ HARQ 방식을 적용한 그래프이다. 마찬가지로 Type Ⅲ HARQ 결과가 Type-Ⅱ 방식보다는 성능이 향상 된 것을 볼 수 있다. 또 그림 8 결과 보다는 전체적으로 성능이 향상 된 것을 볼 수 있다. 이는 무선채널의 환경이 좋아짐에 따라 전체적인 에러율이 작아 졌음을 의미한다. 마찬가지로 인증 암호화를 적용한 SHA-256와 MD-5의 그래프에서는 SHA-256을 적용한 것이 Error rate가 MD-5 적용한 것 보다 성능이 향상된 것을 보였다.



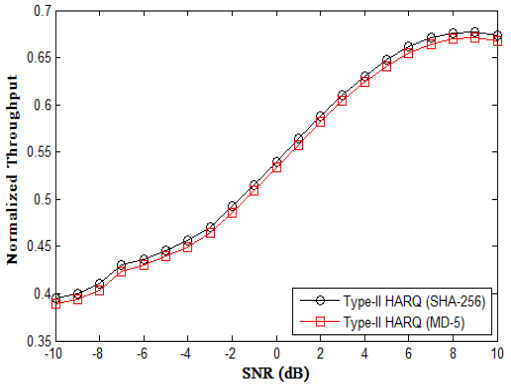
(a)



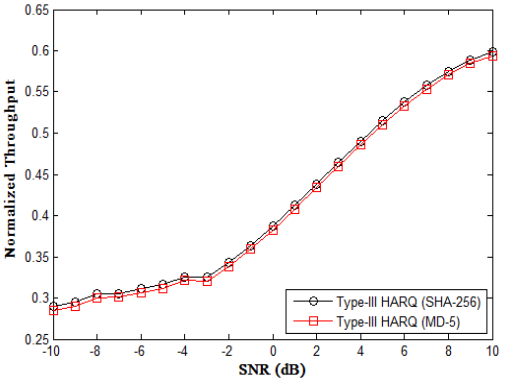
(b)

그림 10. Normalized Throughput (Rician 80%, Rayleigh 20%)
(a) Type II HARQ (b) Type III HARQ

Fig 10. Normalized Throughput (Rician 80%, Rayleigh 20%)
(a) Type II HARQ (b) Type III HARQ



(a)



(b)

그림 11. Normalized Throughput (Rician 90%, Rayleigh 10%)
(a) Type II HARQ (b) Type III HARQ

Fig 11. Normalized Throughput (Rician 90%, Rayleigh 10%)
(a) Type II HARQ (b) Type III HARQ

그림 10은 무선채널이 Rician 80%, Rayleigh 20%인 환경으로 SHA-256와 MD-5의 인증 암호화 알고리즘을 적용하여 Throughput을 시뮬레이션을 한 결과이다. 그림 10-(a)는 Type Ⅱ HARQ 방식이고 그림 10-(b)는 Type Ⅲ HARQ 방식을 적용한 그래프이다. Type Ⅲ HARQ 결과가 Type-Ⅱ 방식보다는 성능이 저하 된 것을 볼 수 있는데 이는 Type-Ⅲ 방식에서는 NACK 신호가 들어와 재전송 과정에서 생성된 패리티 비트와 정보 비트를 모두 재전송하기 때문에 전송 비트수가 많아져 Throughput 측면에서 성능 저하를 보인다. SHA-256이 MD-5 보다 약간 좋은 성능을 보이는 것을 볼 수 있다. 그림11은 무선채널이 Rician 80%, Rayleigh 20%인 환경으로 SHA-256와 MD-5의 인증 암호화 알고리즘을 적용하여 Throughput을 시뮬레이션을 한 결과이다. 무선 채널이 Rician 80%, Rayleigh 20% 환경과 동일한 패턴의 결과를 보였으며 그림10의 결과보다는 전체적인 성능 향상을 보였다.

V. 결 론

IPsec은 네트워크 통신의 패킷 처리 계층에서의 보안을 위해 가상 사설망을 구성하는 것이다. 본 논문에서는 이러한 IPsec VPN을 위성통신망에 적용하여 IPsec 내부 인증알고리즘(SHA-256, MD-5)이 미치는 영향을 분석하였다. 먼저 일반 IP 패킷을 생성하여 IPsec 전송모드 AH 보안헤더를 추가하여 내부 인증 데이터를 SHA-256 및 MD-5알고리즘을 적용하여 구성하였다. 이 인증 데이

터 부분이 깨지게 되면 위성통신 장비에서 정보 데이터까지 모두 버리기 때문에 시뮬레이션 상에서 에러로 체크하여 에러율을 도출하였다. 채널코더는 Rate Compatible Punctured Turbo Codes를 사용하여 재전송마다 펑처링 패턴을 가변시켜 적용하였고 패킷 재전송 기법은 Hybrid-ARQ Type-Ⅱ와 Type-Ⅲ을 사용하였다. 변조방식은 BPSK를 적용하였고 무선채널은 마르코프 채널 Rician 80%, Rayleigh 20% 와 Rician 90%, Rayleigh 10% 로 무선채널 상태에 따라 인증알고리즘이 에러율에 어떤 영향을 미치는지 분석하였다. 분석결과 무선채널이 나아지게 되면 그에 에러율 성능이 좋아지는 것을 볼 수 있었고, SHA-256 가 MD-5 보다 에러율이 적은 것을 볼 수 있었다. 이는 알고리즘 내부 Fadding Length가 영향을 미침을 알 수 있었다. 마지막으로 인증알고리즘에 따른 Throughput을 비교하여 SHA-256 이 MD-5보다 성능이 좋은 것을 확인하였다.

References

[1] 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.

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

[3] Peng Wu, Nihar Jindal, “Performance of Hybrid-ARQ in Block-Fading Channels: A Fixed Outage Probability Analysis” IEEE Trnas. Commun., vol. 58, no. 4, Apr., 2002.

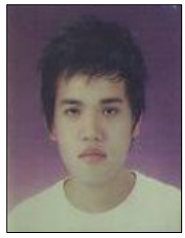
[4] Francesco Chiti and Romano Fantacci, “A Soft Combining Hybrid-ARQ Technique Applied to Throughput Maximization within 3G Satellite IP Network”, IEEE Trans. Vehicular Technology., vol. 56, no.2, Mar., 2001.

[5] D. N. Rowitch and L. B. Milstein, “On the Performance of Hybrid FEC/ARQ Systems Using Rate Compatible Punctured Turbo (RCPT) Codes”, IEEE Trans. Commun., vol.48, no.6, June., 2000.

[6] 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.

저자 소개

정 원 호(준회원)



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

<주관심분야 : 전파전파, MIMO 무선 채널, 채널모델, 위성통신, 무선 통신 암호화 알고리즘>

황 란 미(준회원)

- 2014년 2월 : 충북대학교 정보통신공학과 졸업
- 2014년 3월 ~ 현재 : 충북대학교 전파공학과 대학원(석사 과정)

<주관심분야 : MIMO-OFDM, 위성 통신, 무선 통신 암호화 알고리즘>

여 봉 구(준회원)

- 2015년 2월 : 충북대학교 정보통신공학과 졸업
- 2015년 3월 ~ 현재 : 충북대학교 전파공학과 대학원(석사 과정)

<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 2월 : 충북대학교 졸업(학사)
- 1998년 2월 : 충북대학교 졸업(석사)
- 2010년 2월 : 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>