The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 1, pp.53-60, Feb. 28, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.1.53
JIIBC 2015-1-7

IPsec VPN 기반 위성 통신 시스템 성능 분석

Performance Analysis of a Satellite Communication System based on IPsec VPN

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

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

요 약 위성신호는 광대역이 뛰어나 동일한 정보를 넓은 범위로 제공할 수 있으나 그만큼 데이터 보안성의 수준이 낮다는 단점이 있다. 따라서 위성 통신에서는 보안성을 보완하는 것은 무엇보다 중요한 문제라고 할 수 있다. 이 논문에서는 암호화 기술인 ARIA적용하고, IPsec VPN가 미치는 영향을 알아보기 위해서 보안 헤더인 AH와 ESP를 전송모드와 터널모드를 모두 고려하여 시뮬레이션을 하였다. 또한, 암호화 알고리즘이 미치는 영향을 분석하기 위해 암호화를 적용하지 않은 일반서비스와 비교하였다. 채널은 Markov채널을 적용하고, AWGN을 더하여 위성 통신환경을 구성하였다. 재전송 기반 에러 제어 방식의 경우에는 최근 대두되고 것 중 성능이 좋은 방식인 Type-Ⅱ HARQ 방식, Type-Ⅲ HARQ 방식을 적용하였고, 터보코드와 BPSK 변조 방식으로 구성하였다. 시뮬레이션을 보다 효과적으로 비교하기 위해서 BER과 Throughput으로 성능을 분석하였다.

Abstract Satellite signal is excellent broadband, can provide the same information in a wide range, but there is a disadvantage that much less of the security level of the data. Therefore, supplementation of safety is a serious problem than anything in the satellite communication. In this paper, it was simulated by applying ARIA in encryption technique and by applying transport mode, tunnel mode in security header AH and ESP in order to examine the effect of IPsec VPN. In addition, we had compare with general services that do not apply encryption in order to analyze the impact of the encryption algorithm. Channel, by applying the Markov channel and adding AWGN, is constituted a satellite communication environment. In case of retransmission based error control scheme, we applied Type-Ⅱ HARQ scheme and Type-Ⅲ HARQ scheme which are performance is a good way in recently, and it is constituted by a turbo code and BPSK modulation scheme. we were analyzed performance in BER and Throughput in order to compare the simulation more effectively.

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

Ⅰ. 서 론

위성 통신은 우주 공간에 떠 있는 극초단파 기지국인 위성을 이용한 통신을 말한다. 이는 극초단파 신호를 반사시키는 기능이나 신호를 수신한 후 다른 주파수를 이용하여 재전송하는 역할을 하며, 위성 통신은 64Kbps ~

*준회원, 충북대학교 전파통신공학과
**준회원, 국가보안기술연구소
***정회원, 충북대학교 정보통신공학과 부교수(교신저자)
접수일자 : 2014년 11월 28일, 수정완료 : 2015년 1월 8일
게재확정일자 : 2015년 2월 13일

Received: 28 November, 2014 / Revised: 8 January, 2015
Accepted: 13 February, 2015
***Corresponding Author: kseokkim@cbnu.ac.kr
Department of Electrical and Electronic Engineering, Chungbuk National University, Korea

6Mbps까지 고속 데이터 전송, 통신 구간의 지형 및 지물의 영향을 받지 않는 서비스 제공, 거리에 무관하여 장거리 통신 제공, 자연 재해에 강하고 사고에 의한 절단이 없어 주요 회선의 예비통로로서의 이용가치가 높아 수요와 필요성이 증대되고 있는 현실이다. 또한, 위성 통신은 광대역이 뛰어나 동일한 정보를 넓은 범위로 제공할 수 있으며 통신 거리에 관계없이 요금이 일정하게 되어 원거리 통신에도 경제적이다. 하지만 Point - to-Point Network에서만 가능하여 약 6,000Km의 먼 거리의 통신 위성 사이에서 폭 1.6m의 위성이 지구의 자기장으로 흔들리는 상태에서 전파를 주고 받아야하기 때문에 고도의 기술이 필요하다. 또 사용한 주파수가 높을수록 기후 현상에 대한 신호의 감쇄가 심하고, 위성이 고장을 일으킬 경우 수리가 거의 불가능하다. 이밖에도 전송 지연 문제나 통신의 비밀 보장 문제도 위성 통신이 가지고 있는 문제점이라 할 수 있다. 보안하기 위하여 인터넷 상에서 암호화 기술과 가상 사설 통신망(VPN ; Virtual Private Network) 기술 등이 개발 되고 있다[1]. 본 논문은 이러한 위성 통신의 데이터의 보안성의 단점을 보안하기 위하여 ARIA 암호화를 적용하고, AH나 ESP 헤더를 적용한 시뮬레이션을 분석하고 결과를 도출한다.

II. IPsec VPN 기반 위성 통신 시스템

IPsec VPN란 IP 패킷 단위로 인증 및 암호화를 하는 기술로서 통신 구간에 터널링을 형성하여 VPN에서 많이 사용되는 터널링 프로토콜이다. IPsec 프로토콜은 패킷을 전송하기 전, 부가적인 IP 헤더인 AH(Authentication Header)와 ESP(Encapsulation Security Payload)를 사용하여 IP 패킷을 암호화 한다[2]. 인터넷과 같이 불특정 다수의 기업과 개인이 공동으로 네트워크를 이용하면서도 인증, 암호, 터널링과 같은 기술을 이용하여 가상적인 사설 보안 네트워크를 구축하는 것이다. 즉 공중망을 사이에 둔 네트워크 간의 전용선으로 연결한 것과 같이 안전하게 통신할 수 있도록 해주는 기술로서 각광 받고 있다. 이유는 비용대비 효율성이 높은 저렴한 공중망을 사설망처럼 이용할 수 있다는 경제성 측면 즉 저렴한 공중망을 사설망처럼 안전하게 사용할 수 있다는 큰 장점이 있다[3].

본 논문에서는 시뮬레이션 흐름도는 위에 제시된 그림 1.과 같다. ARIA에서 CTR로 암호화가 된 IP Packet의 값이 AH나 ESP 헤더로 적용되고 그 값은 펑처드 터보코드를 거쳐 BPSK 변조를 하게 된다. 송신단에서 보내진 데이터는 위성 통신 환경을 구성한 채널에 더해진다. 수신단은 송신단과 역순으로 BPSK 복조를 한 후, 터보코드 디코딩을 한다. 이 값은 바로 ARIA에서 해석이 되고 최종 출력 값은 처음 입력된 값과 비교하여 성능을 분석한다.

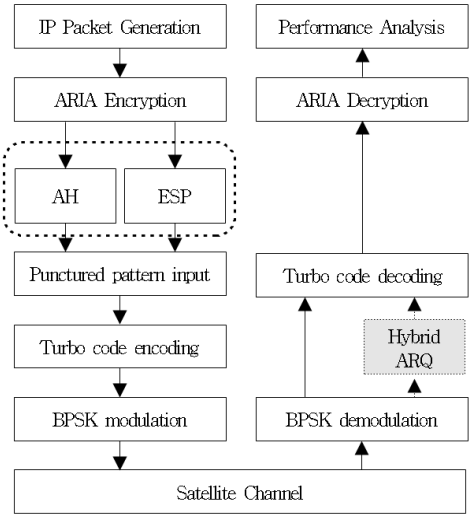


그림 1. IPsec VPN의 시뮬레이션 흐름도
Fig. 1. Simulation flow chart of IPsec VPN

1. Hybrid ARQ 프로토콜 적용

Hybrid ARQ(HARQ)는 재전송 요청 프로토콜(ARQ ; Automatic Retransmit reQuest)과 정방향 오류 정정 부호(FEC ; Forward Error Correction) 두 가지를 같이 사용하는 기술이다. 링크 계층에서 프레임의 손실을 감지하고 재전송 기능을 수행하게 된다. 손실된 프레임을 수신 측으로 전달하여 재빠르게 복구할 수 있어서 상위 계층 프로토콜에 대해서 무선 링크의 신뢰성을 보다 효율적으로 보장한다[4-5]. 이 논문에서는 최근 대두되는 것 중 성능이 우수한 방식인 Type-Ⅱ HARQ 방식과 Type-Ⅲ HARQ 방식을 사용하였다.

표 1. Hybrid ARQ 비교
Table 1. Comparison of Hybrid ARQ

Type-Ⅱ HARQ	Type-Ⅲ HARQ
천공 패턴이 추가되는 패리티 비트만을 재전송	전체 코드를 재전송
전송 데이터양이 적음	전송 데이터양이 많음
처리율 향상	오류 정정 기능 향상

Ⅲ. IPsec 보안 시스템 구조

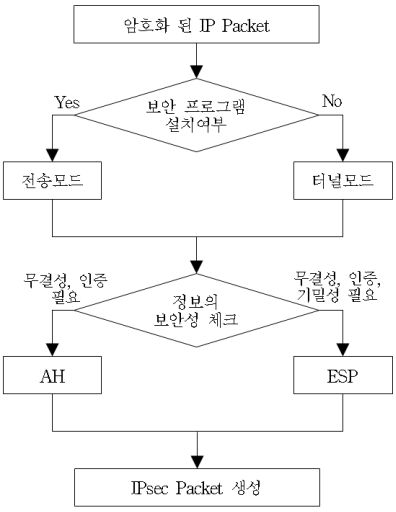


그림 2. IPsec 보안 구조
Fig. 2. Security mechanism of IPsec

그림 2.은 그림 1.의 점선부분을 세밀하게 분석한 IPsec 보안 구조다. 암호화가 된 패킷은 먼저 IPsec 보안 프로그램 설치 여부에 따라서 전송모드와 터널모드로 나눠진다. 그림 3.과 같이 입력 데이터는 보안 프로그램이 설치되어 있을 경우에는 전송모드로, 보안 프로그램이 없어 가상으로 보안 터널을 만들어서 통신을 할 경우에 터널모드로 전송된다.

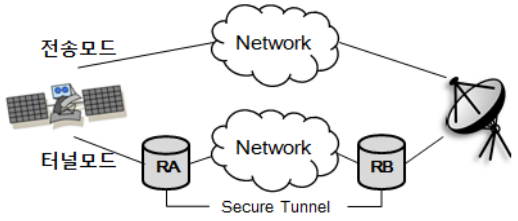


그림 3. 전송모드와 터널모드
Fig. 3. Transport mode and Tunnel mode

무결성(비인가적 대상으로부터 정보의 변조, 삭제 등을 막는 것), 인증(정보의 완전성을 검증하기 위해 사용되는 처리)만 필요한 경우에는 AH로, 무결성과 인증 그리고 기밀성(인가된 대상에게만 정보를 제공)도 필요한 경우에는 ESP로 정보의 보안성을 체크한 후 전송된다. 전송 된 값은 IPsec Packet을 생성하고 완료 된다.

1. AH(Authentication Header)

AH는 암호화와 복호화에 의한 기밀성 서비스는 제공하지 않지만, 비연결형 무결성 및 데이터 발신자 인증 보안 서비스를 제공한다. 또한 수신자의 처리에 따라 선택적으로, 재전송 공격에 대한 방어도 제공할 수 있다.

AH는 IP 헤더를 포함하여 가능한 한 많은 범위를 보호하려고 시도하지만, IP 헤더에는 전송 중에 변경될 수 있는 부분들이 있으므로, 이러한 필드를 제외하고 나머지 필드를 포함하여 상위 프로토콜들의 헤더 및 데이터 영역까지 보호한다. AH는 24바이트가 추가된다.

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

그림 4. AH 헤더 구조
Fig. 4. Structure of AH Header

2. ESP(Encapsulating Security Payload)

ESP은 암호화와 복호화에 의한 기밀성과 데이터 근원지 인증 서비스를 제공하고, 선택적으로 비연결형 무결성 서비스를 제공한다. ESP은 단독으로 사용되거나, 또는 AH과 결합되어 사용될 수 있다. ESP는 64바이트가 추가된다.

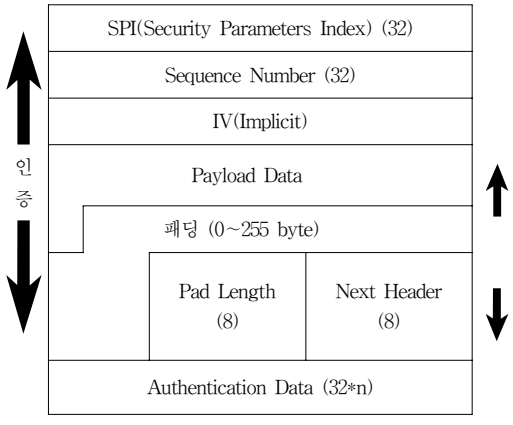


그림 5. ESP 헤더 구조
Fig. 5. Structure of ESP Header

3. 전송모드와 터널모드

IPsec 보안 프로그램이 설치되어 있어 전송모드로 전송 된 정보는 그림 6.과 같은 헤더 구조를 갖는다.

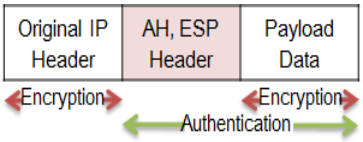


그림 6. 전송 모드에서 AH, ESP 헤더 구조
Fig. 6. Structure of AH, ESP Header in Transport mode

전송모드의 경우, 원래 IP 헤더와 상위 프로토콜 헤더인 페이로드 데이터 사이에 놓이게 된다. 암호화는 원래 IP 헤더와 페이로드 데이터에 적용되며, 인증은 AH, ESP헤더와 페이로드 데이터에 적용된다.

IPsec 보안 프로그램이 설치되어 있지 않아 터널에 의해 새로 생성된 IP 헤더가 추가되게 되는 터널모드는 그림 7.과 같다.

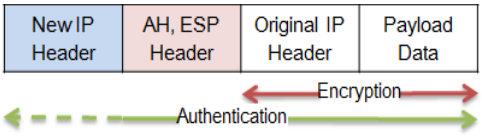


그림 7. 터널 모드에서 AH, ESP 헤더 구조
Fig. 7. Structure of AH, ESP Header in Tunnel mode

터널모드는 원래 IP 헤더 및 페이로드 데이터 앞에 새로 생성된 IP 헤더를 붙이고, 원래 IP 헤더와 새로운 IP 헤더의 중간에 AH와 ESP 헤더를 추가한다. 암호화는 전송모드와 마찬가지로 원래 IP 헤더와 페이로드 데이터에 적용되고, 인증은 전송모드와 달리 전반적으로 헤더 전체에 적용된다.

Ⅳ. 시뮬레이션 결과 및 분석

본 논문에서 주파수는 우리나라 위성인 무궁화 5호(KOREASAT 5) 다운링크에서 가장 높은 송신 주파수인 20.7 GHz를 사용하였고[6], 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. 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 라우시안 80%, 레일레이 20%로 구성하여 통과시키고, AWGN을 더하는 방식으로 구성하였다. IPsec 보안 시스템은 전송모드와 터널모드에 각각 AH와 ESP 헤더를 적용하였다.

표 2. 시뮬레이션 환경
Table 2. 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
HARQ	Hybrid Type-Ⅱ, Hybrid Type-Ⅲ (Max. retransmissions 6)
Modulation/ demodulation	BPSK
Channel	Markov channel (Rician 80%, Rayleigh 20%)
IPsec	Transport mode, Tunnel mode
	AH, ESP
SNR range	-10 dB ~ 10 dB (step : 1)
Encryption Algorithm	ARIA (CTR mode)

시뮬레이션 결과는 일반 서비스와 보안 서비스의 성능 분석을 위하여 BER과 Throuthput을 측정하고 분석하였다.

1. AH 시뮬레이션 결과 및 분석

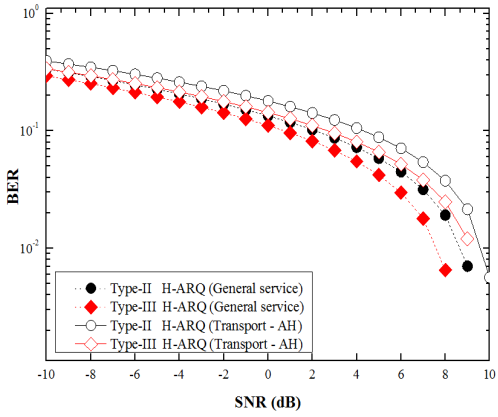


그림 8. HARQ와 보안 헤더(전송 모드-AH)에 따른 BER 성능 비교
Fig. 8. BER performance comparison associated with the HARQ and Security header (Transport mode-AH)

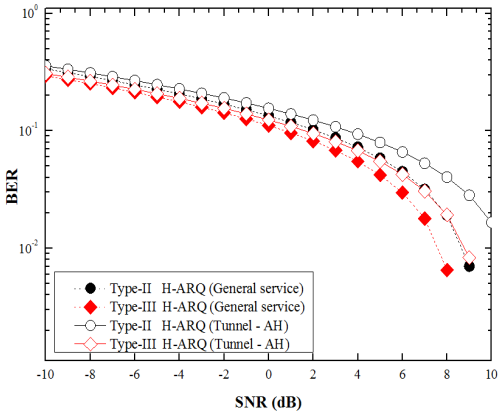


그림 10. HARQ와 보안 헤더(터널 모드-AH)에 따른 BER 성능 비교
Fig. 10. BER performance comparison associated with the HARQ and Security header (Tunnel mode-AH)

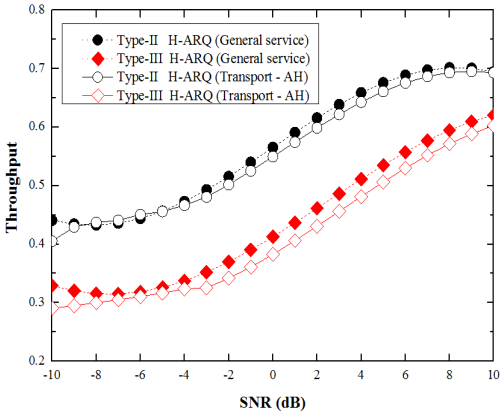


그림 9. HARQ와 보안 헤더(전송 모드-AH)에 따른 처리율 성능 비교
Fig. 9. Throughput performance comparison associated with the HARQ and Security header(Transport mode-AH)

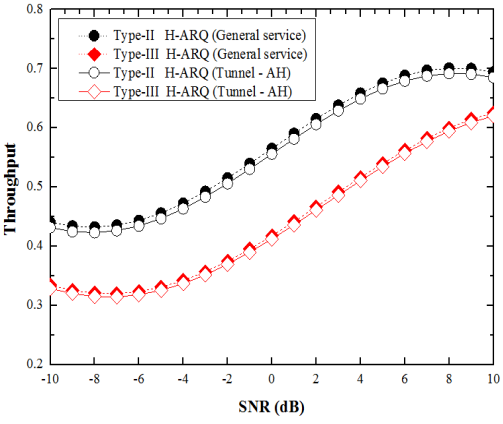


그림 11. HARQ와 보안 헤더(터널 모드-AH)에 따른 처리율 성능 비교
Fig. 11. Throughput performance comparison associated with the HARQ and Security header(Tunnel mode-AH)

그림 8.과 그림 9.은 각각 Type-Ⅱ HARQ와 Type-Ⅲ HARQ에서 AH 보안 헤더를 전송 모드에서 구성한 것의 BER과 Throughput 결과이다. BER에서 모두 일반 서비스가 AH 보안 헤더를 전송 모드에서 구성한 것보다 성능이 약 1 dB정도 상향되는 것을 알 수 있다. Throughput에서는 Type-Ⅱ HARQ와 Type-Ⅲ HARQ의 경우 모두에서 보안헤더를 적용하지 않은 일반서비스가 처리율이 더 높은 것을 확인할 수 있다.

그림 10.과 그림 11.는 Type-Ⅱ HARQ와 Type-Ⅲ HARQ에서 AH 보안 헤더를 터널 모드에 구성하여 BER과 Throughput으로 나타낸 시뮬레이션 결과이다. BER에서 AH 보안 헤더를 터널모드에 구성한 것은 일반 서비스보다 성능이 약 1-2 dB정도 하향되는 것을 확인 할 수 있다. Throughput에서 Type-Ⅱ HARQ에서는 보안 헤더를 적용한 경우보다 일반 서비스가 더 높은 것을 확인 할 수 있으나, Type-Ⅲ HARQ에서는 큰 차이가 없다.

2. ESP 시뮬레이션 결과 및 분석

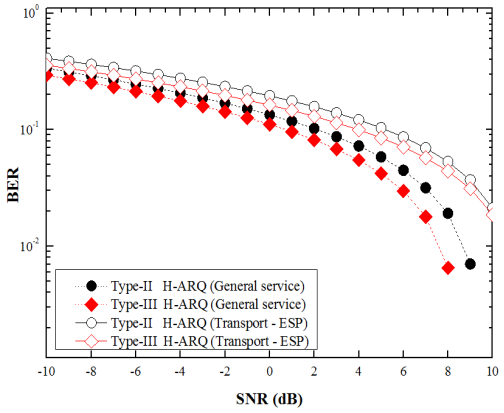


그림 12. HARQ와 보안 헤더(전송 모드-ESP)에 따른 BER 성능 비교

Fig. 12. BER performance comparison associated with the HARQ and Security header (Transport mode-ESP)

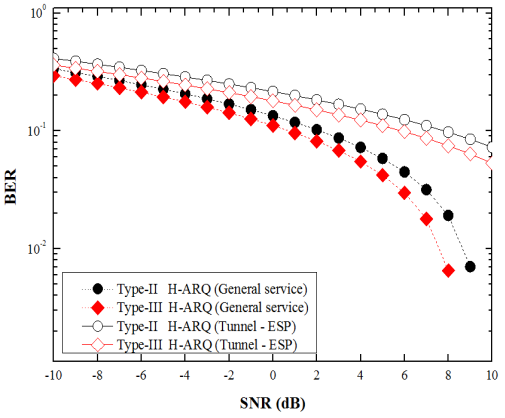


그림 14. HARQ와 보안 헤더(터널 모드-ESP)에 따른 BER 성능 비교

Fig. 14. BER performance comparison associated with the HARQ and Security header (Tunnel mode-ESP)

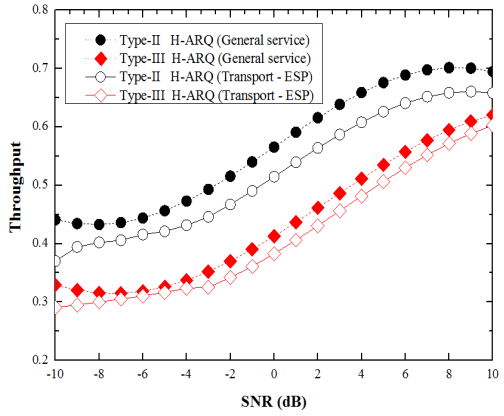


그림 13. HARQ와 보안 헤더(전송 모드-ESP)에 따른 처리율 성능 비교

Fig. 13. Throughput performance comparison associated with the HARQ and Security header(Transport mode-ESP)

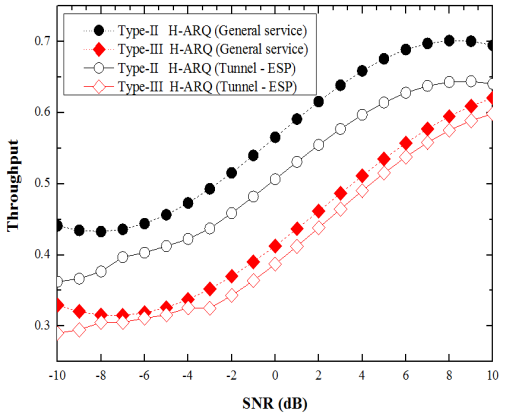


그림 15. HARQ와 보안 헤더(터널 모드-ESP)에 따른 처리율 성능 비교

Fig. 15. Throughput performance comparison associated with the HARQ and Security header(Tunnel mode-ESP)

그림 12.와 그림 13.는 Type-Ⅱ HARQ과 Type-Ⅲ HARQ에서 ESP 헤더를 적용하고 패킷 구성을 전송 모드로 구성한 구조의 BER과 Throughput의 시뮬레이션 결과이다. BER 그래프에서 Type-Ⅱ HARQ와 Type-Ⅲ HARQ 모두 암호화를 적용하지 않은 일반 서비스가 성능이 약 2-3 dB 좋은 것을 확인 할 수 있다. Throughput 역시 일반 서비스가 성능이 더 우수함을 볼 수 있다.

ESP 헤더를 적용하고 패킷 구성을 터널 모드로 한 그림 14.와 그림 15.도 Type-Ⅱ HARQ과 Type-Ⅲ HARQ 모두 시뮬레이션의 결과를 BER과 Throughput으로 분석하였다. ESP 헤더를 적용한 터널 모드의 암호화 서비스의 경우, 암호화를 적용하지 않은 일반서비스와 비교할 때 약 BER이 5 dB이상 악화되었고, Throughput도 마찬가지로 성능이 많이 하향됨을 볼 수 있다.

V. 결 론

이 논문에서 AH 보안 헤더를 추가하여 일반 서비스와 통신 성능을 분석한 결과 BER과 Throughput은 일반 서비스 대비 약 90%의 통신성능을 보였다. BER과 Throughput의 시뮬레이션을 통해서 AH 보안 헤더를 적용한 전송 모드와 터널 모드는 모두 보안 서비스를 적용하지 않은 일반서비스보다 성능이 하향됨을 알 수 있다. ESP 보안 헤더를 추가하여 일반 서비스와 통신 성능을 분석한 결과 BER과 Throughput은 일반 서비스 대비 약 85%의 통신성능을 보였다. AH 보안 헤더를 추가한 위의 결과보다 ESP의 보안 헤더를 추가한 결과의 BER과 Throughput의 성능이 AH 보안 헤더를 적용한 것보다 더욱 저하된 것을 보였다. 이러한 성능 차이는 AH와 ESP의 보안 헤더의 길이의 차이에 의해 발생한 것으로 보인다. 또한, 일반 서비스보다 보안 헤더를 추가한 서비스가 성능이 더 저하 되는 이유는 정보 비트가 아닌 보안 헤더 추가 시 보내지는 비트 수가 증가함에 따라 비트가 깨질 확률이 높아지게 되고 그에 따라 성능이 저하된다고 확인 할 수 있다.

본 연구의 결과인 IPsec VPN 기반의 위성 통신 시스템의 환경에서 보안 헤더와 HARQ의 종류에 따른 통신 특성을 통하여 위성 통신 성능을 향상시키기 위해서 활용될 수 있을 것으로 기대된다.

References

[1] Jung-Su Kim, “A Study of Penetration Test for applying a Remote Monitoring System for Virtual Private Network”, KAERI, 2003.

[2] Seung-Hee Oh, “Performance Evaluation of VPN Protocols in Testbed”, Electronics and Telecommunications Research Institute, 2001.

[3] Tae-Hee Kim, “Ubiqultous Workplace, SSL VPN is troubleshooter”, Arraynetwork,

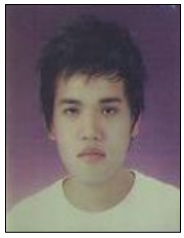
[4] G. Fairhurst and L. Wood, “Advice to Link Designers on Link Automatic Repeat reQuest (ARQ),” RFC 3366, Aug., 2002.

[5] G. Fairhurst and L. Wood, “Advice to Link Designers on Link Automatic Repeat reQuest (ARQ),” RFC 3366, Aug., 2002.

[6] Chun-Won Kim and Chi-Hyun Cheon, “The Antenna Design for Korea SAT-5 Satellite Communication in Ka-band”, J. of The Korean Society for Aeronautical and Space Science, December 10, 2013

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>

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>

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>