

HF통신에서 MELP 부호화방식을 이용한 보안통신의 전송영향 분석

이현수¹, 홍진근^{1*}, 한군희¹

Transmission Effect Analysis of security communication using MELP encoding scheme in the HF communication

Hyun-Su Lee¹, Jin-Keun Hong^{1*} and Kun-Hee Han¹

요약 본 미 정부는 열악한 채널환경에 강인한 통신 성능을 제공하기 위해 MELP 알고리즘을 새로운 군사 표준 보코더 알고리즘을 제시하였다. 논문에서는 HF channel 환경에서 MELP부호화 방식을 이용한 보안 통신의 전송영향을 분석하였다. MELP부호화 방식은 HF채널에 적합하게 적용되도록 개발되었으며 무선 버스터 환경에서 MELP 부호화 영향과 채널부호화 방식을 적용함으로써 평문통신과 보안통신의 성능을 MOS와 스펙트럼 분석을 통해 성능을 고찰하였다.

Abstract The US government has designed new military standard vocoder algorithm, which is called MELP algorithm, to provide robust communication performance on poor channel environment. In this paper, we analyze transmission effect of security communication in MELP vocoder environment of HF channel. MELP vocoder develop properly application in environment of HF channel and influence of MELP vocoder and channel encoding apply to in environment of wireless burst and performance of plaintext communication and security communication study a matter from analysis of MOS and spectrum analysis.

Key Words : MELP, HF channel

1. 서론

디지털 통신의 발전과 함께 급속도로 진행되고 있는 많은 응용사업에 있어서 음성 처리 기술의 사용과 중요도 또한 증가 하고 있다. 음성처리 기술은 얼마나 빠르게 전송 가능하며, 전달된 정보에 의해 원래의 음성을 얼마나 정확하게 왜곡이나 손실 없이 복원 가능한지가 필수 조건이 되고 있다[1]. 특히 채널환경이 열악한 HF채널 저속 환경에서는 보다 효율적인 전송 품질을 얻는 것은 주요 이슈로 대두되어 오고 있다. 미정부는 HF 채널의 저속 환경에서 보다 효율적인 보코더 표준 알고리즘 MELPe를 제시하였다. 디지털 음성은 멀티 레이트 STANAG 4591 (MELPe) 보코더나 16Kbps CVSD의 구현을 통해 가능하게 되었으며, 주파수 호핑이나 AES 암호화 기능이 디지털 음성과 데이터 통신을 위해 높은 수준의 안티재밍 기능이나 전송 보안을 제공하게 되었다.

즉 DSP 기반의 필터링과 600bps 보코더를 갖는 직렬 본 ECCM 파형은 재밍환경에서 신뢰성과 안전한 HF 통신을 제공하며 보안측면에서 안전한 디지털 음성이 75bps 부터 2400bps 전송에서 데이터와 함께 ECCM 모드에서 ARQ를 지원한다. HF 무선통신 시스템에서 보다 개선된 다중 적응적인 COMSEC/ECCM 기능은 신뢰성을 제공하는 HF 운용에 주요한 이슈가 되며 이러한 측면에서 HF 통신에서 적합하게 개발된 MELP 알고리즘 환경에서 보안 통신에 관한 연구가 필요하다. 일반적으로 통신보안은 음성, 데이터 및 버스트 통신에서 보안을 강화하기 위한 방안으로 적용되고 있으며 음성통신은 주파수나 시간, 위상 도메인에서 스크램블 처리나 고속 모델을 포함하는 무선 상에서 명확한 오차 성능을 제거하고, 디지털 암호 처리를 수행한다. 보코더, 데이터 및 버스트 통신은 디지털로 모델 내에서 고수준의 보안을 제공하기 위해 암호화 처리된다. 특히 3세대 HF 링크 자동화 STANAG 4538

¹백석대학교 정보통신학부

²ETRI 부설연구소

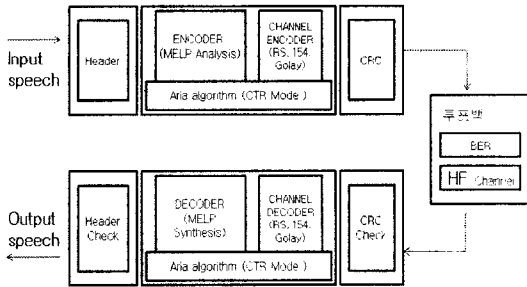
*교신저자: 홍진근(jkhong@bu.ac.kr)

접수일 08년 7월 7일

수정일 08년 8월 01일

제재확정일 08년 8월 11일

에서는 고성능의 ALE와 데이터 링크 프로토콜을 제공하며 우수한 링크 능력과 에러에 자유로운 데이터 전송을 제공한다. 현재 보다 개선된 HF 채널에서 전송성능을 개선하기 위한 MELP 보코더 및 LPC10e 보코더 등에 대한 연구가 지속적으로 이루어져 오고 있는 실정이다. HF 통신과 관련된 기존 연구에서는 600bps환경에서 MELP 보코더에 관한 연구[2]가 있었으며, HF 모뎀에 관한 미군사 표준과 성능 표준에 관한 정의[3]가 제시된 바 있다. 미군사 규격 3005 표준[4]에서는 2400bps MELP에 의해 음성 신호의 A/D 변환 규격을 정의하고 있다. 본 연구에서는 HF Channel 환경에 주로 사용되는 MELP 보코더를 시뮬레이션 할 수 있도록 하였으며, 이를 위해 HF통신채널을 고려하여 시험 환경을 구성하였다. 호스트간 소켓 보안통신 설정을 하고 이로부터 보안 통신 헤더와 프레임 CRC 코드, 채널부호화를 적용할 경우 암호화된 보안 통신의 영향을 살펴보았다. 본 논문의 구성은 2장에서 HF 채널 특성을 소개하고, MELP 알고리즘을 분석하였으며, 3장에서는 구성된 보안 통신환경에서 영향을 평가하였다. 마지막으로 4장에서 결론을 맺었다.



[그림 1] HF채널 MELP 전송시스템 구성도

2. HF채널에서 MELP 부호화 구조

2.1 HF채널 특성

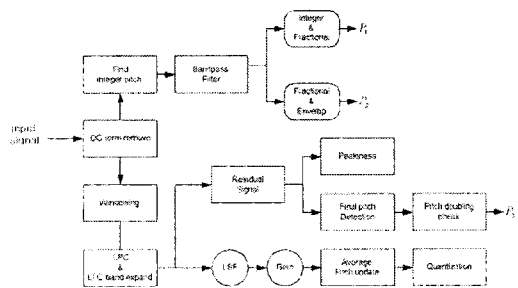
HF 채널은 HF 송수신기의 송신 안테나와 수신 안테나 사이에서 전파 매체로서 이용하는 전리층을 주로 말하는 것으로 일종의 linear time-variant operator로 볼 수 있다. 사용 주파수 대역은 3~30[MHz] 대의 HF 대역으로 지형 및 송신출력에 따라 지상파로 80~100[Km] 까지 통신이 가능하다. HF 채널은 앞에서 언급한 바와 같이 시간적, 공간적으로 변화하는 전리층을 통신채널로 사용하고 있기 때문에 그 통계적 특성도 시간에 따라 변화한다. HF 채널의 noise는 번개 등과 같은 기상조건에 따라 영향을 받으며, 타 통신장비에 의한 신호의 간섭이나 인간

에 의한 noise에 의한 영향을 받게 된다. 특히 대도시에서 멀리 떨어진 경우 3가지 가운데 앞의 2가지가 주로 통신에 영향을 미친다.

2.2 MELP 부호화 방식

음성 코딩의 방법 중 파형 부호화 방식으로 알려진 ADPCM, DPCM 등은 처리시간이 빠르고 좋은 음질을 갖지만 일정 전송률에서 음질이 심하게 왜곡되는 단점이 있다. 또 혼성부호화 방식인 CELP, MPLPC 등은 일정 대역에서 좋은 음질을 보이긴 하나 연산량이 많아 처리시간이 오래 걸린다는 단점을 가지고 있다. 그러나 본 연구에서 사용된 MELP (Mixed Excitation Linear Prediction)는 소스 부호화 방식으로 선형 예측 계수 (Linear Prediction Coefficient)를 기반으로 하고 새로운 5가지 특징을 추가하여 4.8kbps의 CELP 알고리즘 보다 2.4kbps의 전송률에서 더 좋은 음질을 가지는 보코더로 미 국방성에서 개발된 표준 코덱이다. MELP 코덱은 혼합 여기 신호, 주기적인 신호와 비 주기적인 신호, 적응 스펙트럼 강화 필터, 펄스 분산, 퓨리에 급수기법을 고려하여 구성된다.

2.2.1 MELP 부호화기



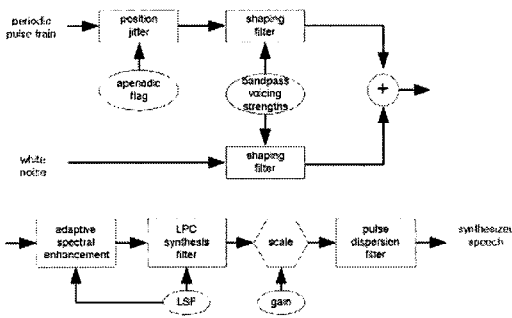
[그림 2] MELP 부호화기 흐름도

MELP 특성은 5개의 대역(0~500, 500~1000, 1000~2000, 2000~3000)별로 bandpass voicing 값을 가지며, LPC 잔차신호인 여기신호를 pulse와 random noise의 혼합구조로 모델링한다. 또한 지터링을 이용하여 비 안정 주기 펄스를 표현하고 CELP 단에서 후단여파기와 유사한 역할을 하는 적응적인 스펙트럼 개선기능을 사용한다. 마지막으로 펄스 분산필터를 적용한다. 부호화기는 그림 2에서 제시된 바와 같이 입력음성을 고주파 필터링 처리하여 DC 성분 제거하고, 정수 피치분석을 통해 fractional 피치를 구한다. 대역통과 필터를 통한 음성 신호를 해석하는데, 선형 예측(LPC) 분석을 통해 LPC 역 필터링시킨 잔여신호는 비주기적인 플래그 값과 퓨리 진폭 값을 계

산하기 위해 분석된다. 푸리 진폭 값은 잔여신호 200개의 샘플에 대해 해밍 윈도우를 적용하여 제로 패딩을 하고, 512개 포인트의 FFT를 구한 후 진폭 값으로 정한다. 이때 10개의 진폭을 양자화하기 위해 8비트가 필요하고 저주파 진폭 값을 강조하기 위해 가중치를 적용한다.

2.2.2 MELP 복호화기

복호화기는 비트 언패킹, 잡음감쇠, 파라미터 인터플레이션, 혼합여기신호, 적응 스펙트럼 강화 필터, 이득 조절, 펄스 분산 부분으로 구성된다.



[그림 3] MELP 디코더 흐름도

3. 실험 및 고찰

본 연구에서는 HF 채널 환경에서 비트오류, 프레임 오류 발생을 랜덤하게 고려하여 발생시켰으며, 전송하고자 하는 음성정보에 MELP 보코더를 적용하였다. 보안 통신을 적용하기 위해 저전력용 6비트로 사용되는 아리아 보안 알고리즘을 적용하였다. 시험을 위해 단말간 소켓 보안 통신 설정을 하고 이로부터 보안 통신 헤더와 암호화된 음성정보, CRC 코드로 프레임 구성하였으며, 채널부호화를 적용하여 암호화된 보안 통신의 영향을 살펴보았다. 실험에서는 MELP 1200bps와 MELP 2400bps 환경에 오류 비트를 일반적으로 음성 품질을 평가하는 기준으로 주로 사용되는 MOS 측정 기준은 다음과 같다. MOS 5의 경우 우수한 음성 품질을 나타내고 편안한 상태에서 청취가 용이한 경우이다. 4의 경우는 품질이 좋은 상태이며 들으려고 주의가 필요하다. 3은 품질이 보통이고 청취하기 위해 노력이 필요하다. 2의 경우 품질이 열화되어 청취하기 위해서는 상당한 노력이 필요하다. 1의 경우 음성 품질이 나쁘고 어떤 노력을 기울여도 음성의 의미를 파악할 수 없다.

3.1 BER 오류율과 BURST 오류율 비교

본 실험에서는 채널 오류 코드와 암호화 알고리즘을 적용한 MELP 보코더를 BER 오류 비트와 BURST 오류 비트를 적용하였다. 원음의 크기가 10x105비트를 사용하였으며 비트 오류율은 10⁻³ 이하의 열악한 환경에서 실험하였다. 채널 코드 ML(15,4) 코드를 적용하였을 때 주관적인 음질 및 오류율을 평가하였다. 또한 보안 알고리즘 (아리아)을 적용한 암호문과 평문의 음질 및 오류율 비교하였다.

[표 1] 보안통신 환경에서 비트오류율 비교

(환경: 전송속도 2400bps, 전송 비트량 10x105bits)

		비트 오류율(%)			
		10-2	10-3	10-4	10-5
ML(15,4) 적용	암호문	45.68	26.52	0.29	0
	평 문	45.28	15.81	0	0
ML(15,4) 미적용	암호문	50.19	29.67	0.33	0
	평 문	49.81	24.56	0.28	0

[표 2] 보안통신 환경에서 비트오류율 비교

(환경: 전송속도 2400bps, 전송 비트량 10x105bits)

		BURST 오류율(%)			
		10-2	10-3	10-4	10-5
ML(15,4) 적용	암호문	41.88	19.71	0	0
	평 문	41.49	15.37	0	0
ML(15,4) 미적용	암호문	41.91	20.22	0	0
	평 문	41.62	15.97	0	0

[표 3] 보안통신 환경에서 MOS 비교

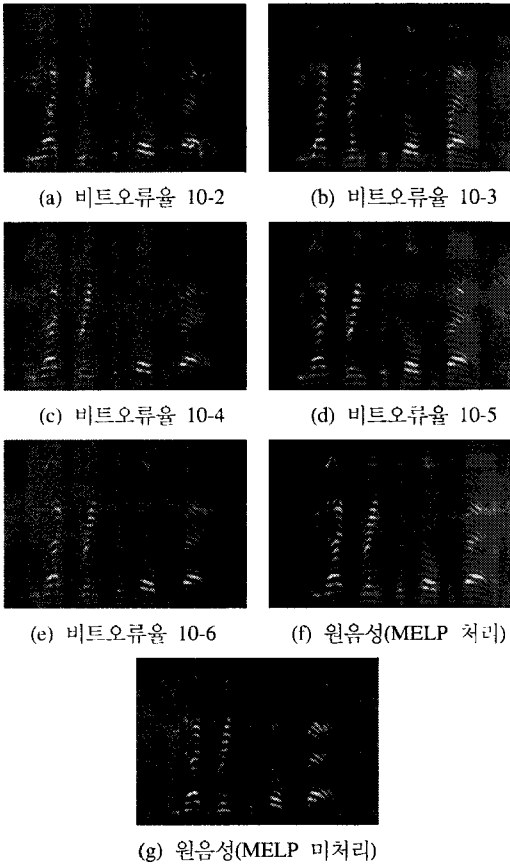
(환경: 전송속도 2400bps, 전송 비트량 10x105bits)

		비트 오류율			
		10-2	10-3	10-4	10-5
ML(15,4) 적용	암호문	1.5	2.5	3.5	4
	평 문	2	3	4	4
ML(15,4) 미적용	암호문	1	2.5	3.5	4
	평 문	1.5	2.5	3.5	4

[표 4] 보안통신 환경에서 MOS 비교

(환경: 전송속도 2400bps, 전송 비트량 10x105bits)

		BURST 오류율			
		10-2	10-3	10-4	10-5
ML(15,4) 적용	암호문	1.5	3	4	4
	평 문	1.5	3	4	4
ML(15,4) 미적용	암호문	1	3	4	4
	평 문	1.5	3	4	4



[그림 4] 보안통신 환경에서 전송된 음성스펙트럼 비교

3.2 MELP 2400bps 환경에 Intereaving 적용

[표 5] 보안통신 환경에서 비트오류율 비교

(환경: 전송속도 2400bps, 전송 비트량 10x105bits, Intereaving 적용)

채널부호/전송문상태		비트 오류율(%)			
		10-2	10-3	10-4	10-5
ML(15,4) 미적용	암호문	42.57	15.87	0	0
	평 문	41.90	13.13	0	0
ML(15,4) 적용	암호문	41.83	14.20	0	0
	평 문	35.65	12.32	0	0

[표 6] 보안통신 환경에서 MOS 비교

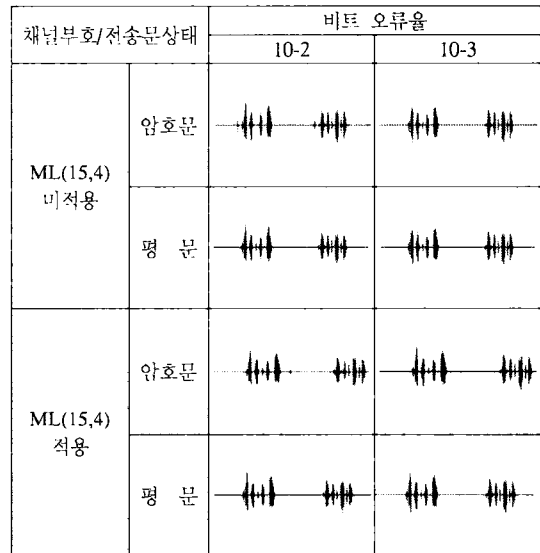
채널부호/전송문상태		비트 오류율			
		10-2	10-3	10-4	10-5
ML(15,4) 미적용	암호문	1.5	3	4	4
	평 문	1.5	3	4	4
ML(15,4) 적용	암호문	1.5	3	4	4
	평 문	2	3	4	4

본 실험에서는 앞 절에서 실시한 실험에 Intereaving

코드를 적용하여 MELP 보코더를 비교하였다. HF channel 환경에서 Intereaving 적용이 비트 오류율(%)과 주관적인 음질 평가에 어느 정도 효과를 보였지만 음질 평가에서는 미치는 효과가 적었다. Intereaving의 크기를 고려하면 더욱 효과를 볼 것으로 사료된다.

3.3 버스트오류 환경에서 MELP 1200bps와 MELP 2400bps 비교

제한된 환경에서 실험한 결과 버스트 오류를 20비트로 고정했을 때 채널코드 및 압호화 알고리즘을 적용한 MELP 보코더 환경에서 1200bps 와 2400bps 전송속도로 전송할 때 전송영향을 비교하였다. 실험 결과 MELP 2400bps 환경에서 주관적인 음질과 비트 오류율이 좋았으며 2400bps 환경에서 MOS의 차이가 평균 0.5정도 높게 나타났다. 버스트 오류환경에서 채널부호기의 적용과 인터리빙 적용은 채널이 열악할 수록 성능 열화가 뚜렷하게 나타나고 채널상태가 호전 될수록 유사한 성능에 근접하게 나타났다. 이와같은 효과는 MELP 보코더의 특성을 잘 반영하고 있음을 알 수 있다.



[그림 5] 보안통신 환경에서 전송된 음성 파형 비교

[표 7] 보안통신 환경에서 비트오류율 비교

(환경: 전송속도 1200bps, 전송 비트량 10x105bits, Intereaving 적용)

채널부호/전송문상태		버스트 오류비트 20bit (%)			
		10-2	10-3	10-4	10-5
ML(15,4) 미적용	암호문	48.57	15.87	0	0
	평 문	41.90	3.13	0	0
ML(15,4) 적용	암호문	45.83	14.20	0	0
	평 문	41.65	2.32	0	0

【표 8】 보안통신 환경에서 MOS 비교

채널부호/전송문상태		비트 오류율			
		10-2	10-3	10-4	10-5
ML(15,4) 미적용	암호문	1	3	4	4
	평 문	1.5	3.5	4	4
ML(15,4) 적용	암호문	1.5	3	4	4
	평 문	1.5	3.5	4	4

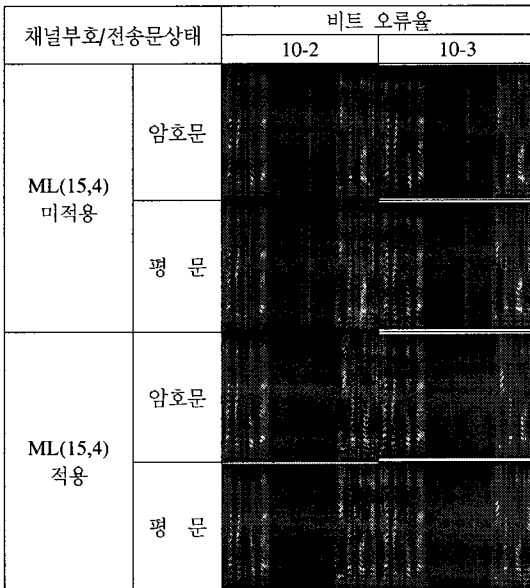
【표 9】 보안통신 환경에서 비트오류율 비교

(환경: 전송속도 2400bps, 전송 비트량 10x105bits, Intereaving 적용)

채널부호/전송문상태		버스트 오류비트 20bit (%)			
		10-2	10-3	10-4	10-5
ML(15,4) 미적용	암호문	44.22	21.87	0	0
	평 문	43.21	21.11	0	0
ML(15,4) 적용	암호문	42.39	19.00	0	0
	평 문	37.71	18.21	0	0

4. 결론

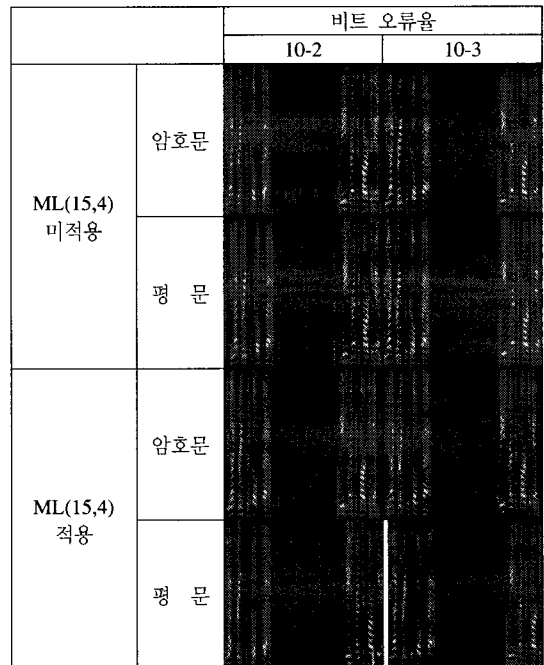
디지털 음성은 멀티 레이트 STANAG 4591 (MELPe) 보코더나 16Kbps CVSD의 구현을 통해 가능하게 되었으며, 주파수 호핑이나 AES 암호화 기능이 디지털 음성과 데이터 통신을 위해 높은 수준의 안티재밍 기능이나 전송 보안을 제공하게 되었다. HF 무선통신 시스템에서 보다 개선된 다중 적응적인 COMSEC/ ECCM 기능은 신뢰성을 제공하는 HF 운용에 주요한 이슈가 되며 이러한 측면에서 HF 통신에서 적합하게 개발된 MELP 알고리즘 환경에서 보안 통신에 관한 연구가 필요하다. 본 논문에서는 HF 채널 환경에서 MELP 부호화 방식을 이용한 보안 통신에 관한 전송 영향을 살펴보았다. MELP 부호화 방식은 HF 채널 특성을 고려하여 개발된 방식으로 타 부호화 방식에 비해 낮은 전송률과 열악한 통신채널에 적합한 것으로 고려된다. 전송속도 2400bps, 전송 비트량 10x105비트 환경에서 음성데이터를 송신한 결과 비트 오류는 10-4, 버스트 오류는 10-3환경에서 전송 영향을 고찰하였으며, 채널 상태가 호전 될수록 MELP 보코더의 특성상 주관적으로 유사한 성능을 알 수 있었다. 향후 600bps, 1200bps, 2400bps 전송환경에서 보다 적합한 채널 부호화 방식과 보안 동기 구조에 대한 연구가 필요하다고 사료된다.



【그림 6】 보안통신 환경에서 전송된 음성스펙트럼 비교

【표 10】 보안통신 환경에서 MOS 비교

채널부호/전송문상태		비트 오류율			
		10-2	10-3	10-4	10-5
ML(15,4) 미적용	암호문	1.5	2.5	4	4
	평 문	1.5	3	4	4
ML(15,4) 적용	암호문	1.5	3	4	4
	평 문	2	3	4	4



【그림 7】 보안통신 환경에서 전송된 음성스펙트럼 비교

참고문헌

- [1] A.M.Kondoz, "Digital speech coding for low bit rate communications systems."
- [2] Chamberlain, M.W., "A 600 bps MELP vocoder for use on HF channels," MILCOM2001, Communications for Network-Centric Operations: Creating the Information Force.
- [3] MIL-STD-188-110B, "Mil. Std. Interoperability and performance standards for data modems," draft version revised 7 March 2000.
- [4] MIL-STD-3005, "Analog-to-Digital conversion of voice by 2400bps mixed excitation linear prediction (MELP)," MIL-STD-3005, Dec. 1999.

한 군 희(Kum-Hee Han)

[종신회원]

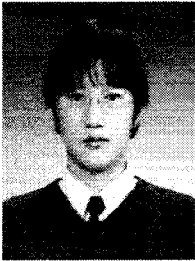


- 2008년 8월 현재 : 백석대학교 정보통신학부 교수

<관심분야>
RFID, 경영정보컨설팅

이현수(Hyun-Hu Lee)

[준회원]



- 2008년 8월 현재 : 백석대학교 정보통신학부

<관심분야>
센서네트워크, RFID, 무선랜 보안

홍진근(Jin-Keun Hong)

[정회원]



- 2008년 8월 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전송통신, 센서넷, RFID, 무선랜 보안