MIMO 통신 시스템에서 항재밍을 위한 반복적인 채널 추정 알고리즘

정준희*, 황유민*, 차경현*, 이재생**, 신요안***, 김진영*

Iterative Channel Estimation Algorithm for Anti-jamming in MIMO Communication Systems

Jun Hee Jung*, Yu Min Hwang*, Kyung Hyun Cha*, Jae Seang Lee**, Yoan Shin***, and Jin Young Kim*

요 약

무선 통신 시스템에서 재밍 공격은 통신 성능을 심각하게 저하시킬 수 있는 치명적 위협이다. 특히 반응 재밍은 송신기와 수신기가 통신할 때만 재밍할 수 있기 때문에 반응 재밍을 통해 공격 효율을 극대화할 수 있다. 본 논문에서 반응 재밍의 공격 효과를 저감시키기 위해 multi-input multi-output (MIMO) 기반의 orthogonal frequency-division multiplexing (OFDM) 통신 기술의 특징을 활용하고, 이에 기반한 반복적 채널 추정 알고리즘을 제안하였다. 실험 결과를 통해 본 논문에서 제안한 알고리즘과 기존 항재밍 알고리즘을 비교하였으며, 반응 재밍 공격이 있는 MIMO-OFDM 통신 시스템에서 제안한 알고리즘의 우수성을 입증한다.

Key Words : Anti-jamming, MIMO interference cancellation, iterative channel estimation algorithm, reactive jamming

ABSTRACT

In wireless communication systems, jamming attack is a critical threat. Especially, reactive jamming can jam when the sender and receiver are communicating, which can maximize the attack efficiency of jamming. In this paper, we use the property of multi-input multi-output (MIMO) technology to achieve jamming resilient orthogonal frequency-division multiplexing (OFDM) communications. In particular, we use MIMO interference cancellation to remove the jamming signals strategically. We first investigate the reactive jamming attack model and their impacts on the MIMO-OFDM systems. We then present an iterative channel estimation algorithm that exploits MIMO interference cancellation. Our simulations show various anti-jamming methods and demonstrate the efficiency of our proposed algorithm under the reactive jamming attack.

I. 서 론

Orthogonal frequency-division multiplexing (OFDM)은 이동 통신에서 주로 사용되는 통신방식으로 다중 경로 페이딩이나 잡음이 심한 환경에 강한 특성을 가지고 있다. 하지만 재밍 공격이 들어오는 경우에는 심각한 통신 성능 저하가 발생할 수 있다. 이러한 재밍 공격은 신호 간섭과 같은 다른 통신 방해요소보다 매우 치명이며, 용도 및 성능에 따라 다양한 방식으로 존재 한다 [1].

재밍 공격에 상대적으로 취약한 OFDM 통신 시스템을 위해 다양한 항재밍 기술들이 연구되고 있다. [2]은 OFDM 시스템을 위해 재밍된 파일럿 신호 탐지 및 제거 알고리즘을 제안했고 [3]은 파일럿 신호의 위치와 값을 랜덤으로 바꿔서 재밍을 제거하는 간섭 완화 기법을 제안했다. 하지만 두 방식은 동기화 및 구현 문제가 있고 특히 반응 재밍에 취약하다는 단점이 있다.

반응 재밍은 지속적으로 채널을 탐지해서 통신의 활동 유무에 따라 재밍 신호를 방출하거나 정지 상태를 유지할 수 있기 때문에 효율이 높고 효과적으로 무선 통신을 무력화할 수 있다. 또한 다른 재밍 방식과 달리 통신이 감지될 때만 재밍 신호를 방출하기 때문에 감지하기가 어렵다. 또한 소프트웨어 무선 기술 (Software defined radio)의 발전으로 반응

※ 이 논문은 2014년도 국방과학연구소 핵심기술연구개발 과제의 지원을 받아 수행되었음 (UD140076ED).
*광운대학교 전파공학과 유비쿼터스 통신 연구실(junheez@kw.ac.kr, yumin@kw.ac.kr, chagyeonghyeon@kw.ac.kr, jinyoung@kw.ac.kr)
**국방과학연구소 제2기술연구본부 1부 3팀 (jslee15@add.re.kr)
***숭실대학교 통신및정보처리 연구실 (yashin@ssu.ac.kr)
접수일자 : 2016년 8월 2일, 수정완료일자 : 2016년 9월 12일, 최종게재확정일자 : 2016년 9월 23일

재밍이 점점 더 강력해지고 있기 때문에 반응 재밍에 대비할 항재밍 기술 연구의 필요성이 점차 커지고 있다.

간섭 제거 기술 중 하나인 Multi-input multi-output (MIMO) 잡음 제거 기술은 MIMO의 다이버시티와 공간적 다중화 특성을 활용한다. MIMO 잡음 제거 기술은 높은 파워와 넓은 대역폭을 갖는 간섭 신호가 존재하는 환경에서도 통신을 가능하게하고, 특히 빠른 주기로 간섭을 제거하기 때문에 다른 항재밍 기술보다 반응 재밍에 효과적이다[4], [5].

따라서 본 논문에서는 반응 재밍 공격에 대처하기 위해 MIMO 간섭 제거 기술 기반의 반복적인 채널 추정 알고리즘을 제안한다. 먼저 송신기와 수신기가 통신하는 환경에서 재머가 반응 재밍을 위해 재밍 신호를 방출하는 상황을 가정한다. 이러한 상황에서, 다중 파일럿 신호를 이용하여 재밍 채널을 추정, 재밍 신호의 방향을 계산한다. 계산된 값을 이용해서 재밍 신호와 직교의 송신신호를 만들 수 있게 되고, 이를 통해 반응 재밍에 대한 OFDM 통신 시스템의 성능을 향상시킨다.

논문의 구성은 2장 시스템 모델에서 시스템 모델과 반응 재밍의 공격 모델을 도출하고 3장에서 반응 재밍에 대처하기 위한 반복적인 채널 추정 알고리즘을 제안한다. 4장에서 제안한 알고리즘의 성능분석을 위해 컴퓨터 시뮬레이션하고 결과를 분석하며, 마지막 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 시스템 모델

1. 채널 모델

채널 모델은 단일 송신기와 단일 수신기가 통신을 하고 있고 하나의 재머가 통신 성능 저하를 위해 반응 재밍 공격을 하고 있는 MIMO-OFDM 통신 시스템이라고 가정 한다 (그림 1). 이때 송신기와 재머는 하나의 안테나를 가지고 있고 수신기는 두 개의 안테나를 가지고 있다. 송신 신호 x_s와 재머 신호 x_j에 대한 수신 신호 y_1, y_2의 모델은 다음과 같다.

$$y_1 = g_s * x_s + g_j * x_j, \quad (1)$$

$$y_2 = g_s' * x_s + g_j' * x_j, \quad (2)$$

여기서 g_s와 g_j는 Rayleigh fading channel이다. OFDM 통신 시스템의 신호는 그림 2와 같이 프레임에 채널 추정을 위한 파일럿 신호를 가지고 있다. 반응 재밍은 송수신기가 통신할 때를 탐지할 때만 동작하며, 이때 재밍 신호를 발산한다. MIMO 통신 시스템에서 공간 다중화 이득은 수신 신호의 공간에 대한 차원인 자유도(Degree-of-Freedom, DOF)로 표현될 수 있다. DoF는 MIMO 통신 시스템에서 동시에 송신되는 신호 중 구별되는 신호들의 숫자를 의미한다. 수신기에서 송신기나 재머의 수신 신호 파워를 각각 P_S와 P_J라고 가정한다. 이때 송신 신호 대 재밍 신호의 비율(Signal-to-jamming ratio, SJR)을 P_S/P_J라 한다. 간섭 신호 파워는 재밍 신호의 파워에 비해 매우 작기 때문에 무시한다.

2. 재밍 공격 모델

재밍은 지속 재밍이나 랜덤 재밍, 반응 재밍 등 다양한 종류가 있지만, 본 논문은 다른 재밍에 비해 효과적이며 에너지 효율적인 반응 재밍을 공격 모델로 정한다. 반응 재밍의 주된 특징은 통신 유무 탐지 후 재밍 방식으로 통신 여부를 파악하기 위한 시간이 필요하다. 따라서 채널을 탐지하고 재밍 신호를 보내기 위한 준비 시간을 '재밍 반응 시간'이라고 정의한다. 재밍 반응 시간은 수신기에 원 신호가 도착 시간과 재밍 신호 도착 시간의 차이로 정의된다. 아무리 정교한 재머라고 해도 통신 여부를 파악하고 재밍을 결정하는데 최소한의 시간이 필요하기 때문에, 본 논문에서는 첫 파일럿 신호는 재밍 반응시간으로 인해 재밍 공격을 받지 않는다고 가정한다.

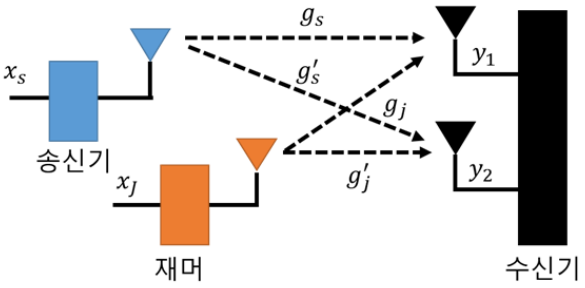

그림 1. 2x2 MIMO OFDM 시스템 모델

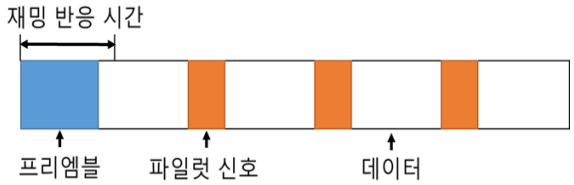

그림 2. 송신 신호의 프레임 구조

3. MIMO 간섭 제거 기법

MIMO 간섭 제거 기법은 수신 신호 $y_{1,}y_2$로부터 재밍 신호 x_j를 제거하기 위해 적용된다. 재밍 신호 x_j 제거를 위해 수신 신호를 x_j에 직교한 부분 공간에 사영합니다. 따라서 사영된 수신신호는 다음과 같습니다.

$$y_{pj} = g_j' y_1 - g_j y_2 = (g_j' g_s - g_j g_s')x_s, \quad (3)$$

여기서 사영된 신호 y_{pj}는 기준 복호기를 통해 복호되며 이러한 MIMO 간섭 제거 기법을 Zero-Forcing 라고 한다. 식 3에 따르면, 송신가와 재머의 각 채널 정보를 알면 MIMO 간섭 제거 기법을 적용할 수 있다. 송신기의 파일럿 신호를 이용하여 송신기에 대한 채널 정보를 알 수 있지만, 재머의 신호는 알 수 없기 때문에 재밍 신호의 채널 정보를 파악할 수 없다. 따라서 본 논문에서 제안한 MIMO 간섭 제거 기반 채널 추정 알고리즘을 이용해서 재머의 신호 정보 없이 재밍 채널의 정보를 구할 수 있다.

Ⅲ. 반복적인 채널 추정 알고리즘

3장에서는 반복적인 반응 재밍 공격에 대응하기 위한 MIMO 간섭 제거 기법 기반 채널 추정 알고리즘을 제안한다. 제안된 알고리즘은 재밍 채널의 정보를 반복적으로 추정하여 송신신호를 재밍 신호에 직교하게 만들어 통신 시스템의 항재밍 성능을 증가시킨다.

먼저 송신기의 채널 정보 g_s와 $g_s^{'}$의 초기값은 초기 파일럿 신호를 이용해서 구할 수 있다. 하지만 송신기의 채널정보와 달리 재밍 채널 정보 g_j와 $g_j^{'}$는 재머의 신호를 알수 없기 때문에 정확히 구할 수 없다. 하지만 신호가 갖는 방향의 불변성 때문에, 재밍 채널 정보 g_j와 $g_j^{'}$을 재밍 채널의 비인 $\frac{g_j}{g_j^{'}}$으로 대신 구할 수 있다. 여기서 기억할 점은, 송신 신호는 송신기의 신호와 재밍 신호의 합인 $J_r + S_r$로 되어있기 때문에 재밍 신호 $J_r = \begin{pmatrix} g_j \\ g_j^{'} \end{pmatrix} x_j$를 수신 신호로부터 구할 수 있다면 재밍 채널의 비를 다음과 같이 구할 수 있다.

$$\frac{g_j}{g_j^{'}} = \frac{x_j^* g_j}{x_j^* g_j^{'}}, \tag{4}$$

수신신호로부터 재밍 신호 J_r를 얻기 위해서는 재밍 신호 시작과 끝 시점을 알아야한다. 재밍 탐지 문제는 [6]에서 이미 연구되었고, 본 논문에서도 같은 방식을 사용한다. 따라서 소프트 에러 벡터는 심볼 간의 거리를 위한 탐지 거리를 정의하기 위해 사용된다. 미리 정의된 임계값을 통해 재밍 여부를 판단한다[].

채널 정보는 채널의 가간섭성 시간 동안만 유지되고 시간에 따라 변화하기 때문에 반복적으로 구해야 지속적인 항재밍 효과를 볼 수 있다. 하지만 무선 통신 채널은 다중경로 페이딩 효과 때문에 시변성을 가져서 채널 정보가 바뀌며 송신기의 채널이 재밍 공격을 받는다면, 채널 정보를 파악하기는 더욱 어려워진다. 따라서 단순히 재밍 채널 정보를 파악하는 것뿐만 아니라 주기적으로 채널 정보를 파악하는 것 또한 중요하다. 초기 송신기의 채널 정보는 다음과 같다.

$$G_s(0) = \begin{pmatrix} g_s(0) \\ g_s^{'}(0) \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} / x_s^p, \tag{5}$$

여기서 x_s^p는 파일럿 신호다. 파일럿 신호를 이용해서 송신기의 채널 정보와 재머의 채널정보를 반복적으로 측정한다. 첫 번째 파일럿 신호 수신 후 업데이트된 재밍 채널의 비는 다음과 같다.

$$\frac{g_j(i)}{g_j^{'}(i)} = \frac{y_1 - x_s^{p*} g_s(i-1)}{y_2 - x_s^{p*} g_s^{'}(i-1)}, i = 1, 3, \ldots, \tag{6}$$

두 번째 파일럿 신호 수신 후 업데이트 된 송신기의 채널 정보 $G_s(i) = \begin{pmatrix} g_s(i) \\ g_s^{'}(i) \end{pmatrix}$는 다음을 통해 얻어진다.

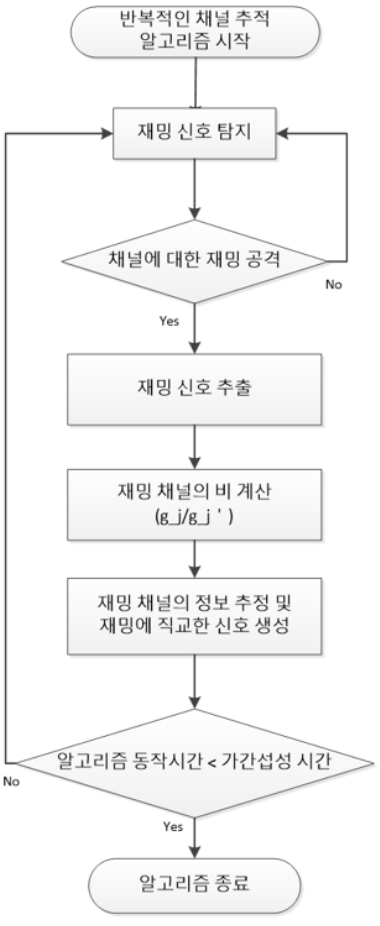

그림 3. 최적 채널 도약 알고리즘

$$g_s(i) - \frac{g_j(i-1)}{g_j^{'}(i-1)} g_s^{'}(i) = (y_1 - \frac{g_j(i-1)}{g_j^{'}(i-1)} y_2) / x_s^p,$$
$$i = 2, 4, \ldots, \tag{7}$$

식 7의 $g_s(i)$와 $g_s^{'}(i)$는 파일럿 신호가 짝수일 때마다 업

데이트되는데, 특히 $g_s(i)$는 $i=4,8,\ldots$일 때, 그리고 $g_s^{'}(i)$는 $i=2,6,\ldots$일 때 업데이트된다. 채널 추정을 위해 송신기의 신호는 짧은 가간섭성 시간 내에 두 개 이상이 존재하기 때문에 채널 정보를 빠르게 반복적으로 추정할 수 있다.

식 3 기반으로 복조한 송신기의 신호 x_s^*는 다음과 같다.

$$x_s^* = \frac{y_1 - \frac{g_j}{g_j^{'}} y_2}{g_s - \frac{g_j}{g_j^{'}} g_s^{'}}, \quad (5)$$

여기서 $\frac{g_j}{g_j^{'}}$는 식 6에서 짝수 번째의 파일럿 신호마다 업데이트되고 $g_s - \frac{g_j}{g_j^{'}} g_s^{'}$는 식 7에서 홀수 번째의 파일럿 신호마다 업데이트된다.

표 1. 파라메터 설명

파라미터	값
반송 주파수	2.4 GHz
변조 방식	BPSK
송신 이득	30 dB
수신 이득	30 dB
OFDM FFT 길이	64
OFDM 사용되는 톤	48
OFDM CP 길이	64
송신기와 수신기 사이의 거리	1 km
채널 모델	AWGN 채널

Ⅳ. 시뮬레이션

본 장에서는 제안한 알고리즘의 효과를 보여주기 위해 다른 항재밍 방식(801.11 Direct sequence spread spectrum (DSSS))과 기존 OFDM 시스템을 비교해서 수치적 결과를 제시하였다. 801.11 DSSS는 11 비트 barker 코드와 CSMA/CA, 그리고 순방향 오류정정법을 사용한다. 시뮬레이션 파라메터는 표 1과 같다.

그림 4는 제안한 알고리즘과 다른 통신 시스템에 대한 SJR 대비 BER을 나타낸다. 재밍 환경은 20 dB uniform noise jamming을 가하였다. 재밍 환경에서의 제안한 알고리즘의 BER을 다른 항재밍 방식과 비교하였는데, 801.11 DSSS 방식은 다른 통신 방식에 비해 가장 높은 BER을 보였다. 기존 OFDM 시스템은 낮은 BER로 재밍 공격에 취약한 모습을 보여준다. 제안된 알고리즘은 재밍 채널 정보를 추정하고 직교한 신호를 만들기 때문에 기존 OFDM 시스템보다 높은 BER을 가져 기존 OFDM 시스템보다 뛰어난 항재밍 성능을 보인다.

그림 5 역시 제안한 알고리즘과 다른 항재밍 방식을 재밍 파워 대비 네트워크 처리량을 통해 비교하였다. 재밍 파워가 증가함에 SJR 저하로 네트워크 처리량이 감소하여 일정량 이상의 재밍 파워가 되면 0에 가깝게 작아지게 된다. 기존 OFDM 시스템이 가장 높은 네트워크 처리량을 보이는데, 제안한 알고리즘 역시 이와 비슷한 네트워크 처리량을 보여준다. 따라서, 높은 항재밍 성능을 보장하면서 항재밍으로 인한 네트워크 처리량의 손실은 적은 것을 확인할 수 있다.

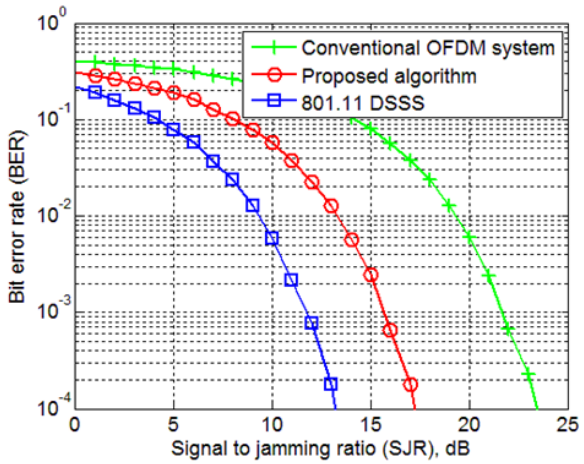

그림 4. 다양한 재밍 방식에 대한 신호대재밍비 대 BER 비교

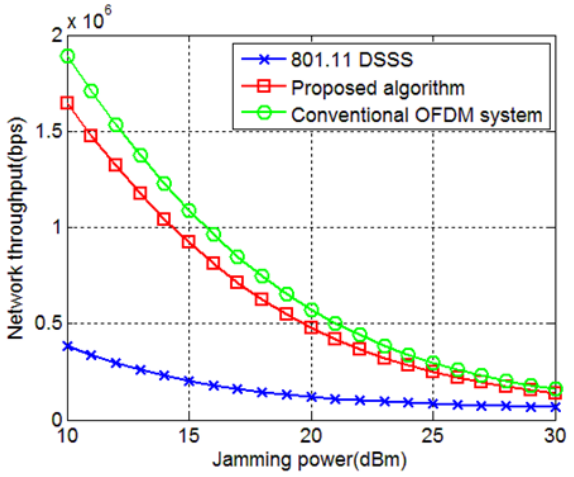

그림 5. 다양한 재밍 방식에 대한 재밍 파워 대 네트워크 처리량 비교.

표 2. 네트워크 처리량 성능 비교

항재밍 방식	평균 네트워크 처리량 (Mbps)
801.11 DSSS	0.3
Conventional OFDM system	1.20
Proposed algorithm	1.07

Ⅴ. 결론

본 논문에서는 재밍 환경에서 OFDM 통신 시스템의 성능 향상을 위해 MIMO 간섭 제거 기법 기반 반복적인 채널 추정 알고리즘을 제안한다. 제안된 알고리즘은 재밍 채널을 추정하여 재밍 신호에 직교한 신호를 만들어 항재밍 성능을 향상시킨다.

최적의 채널 할당 strategy와 최적 전송 세기를 산출하였다. 시뮬레이션 결과를 통해 기존 기법에 대비해 제안한 알고리즘의 항재밍 성능이 높은 것을 확인하였다.

참 고 문 헌

[1] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: A survey,” Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197-215, Dec. 2014.

[2] M. Han et al., “OFDM channel estimation with jammed pilot detector under narrow-band jamming,” IEEE Trans. Veh. Technol., vol. 57, no. 3, pp. 1934 - 1939, May 2008.

[3] T. C. Clancy, “Efficient OFDM denial: Pilot jamming and pilot nulling,” in Proc. IEEE ICC, Jun. 2011, pp. 1 - 5.

[4] S. Gollakota, S. D. Perli, and D. Katabi, “Interference alignment and cancellation,” in Proc. SIGCOMM, Aug. 2009, pp. 159 - 170.

[5] S. Gollakota, F. Adib, D. Katabi, and S. Seshan, “Clearing the RF smog: Making 802.11n robust to cross-technology interference,” in Proc. SIGCOMM, Aug. 2011, pp. 170 - 181.

[6] Y. Liu and P. Ning, “BitTrickle: Defending against broadband and highpower reactive jamming attacks,” in Proc. IEEE INFOCOM, Mar. 2012, pp. 909 - 917.

저자

정 준 희(Jun Hee Jung)

- 2015년 2월 : 광운대학교 전자융합공학과 졸업
- 2015년 3월 ~ 현재 : 광운대학교 전파공학과 석사과정

<관심분야> : 차세대 이동통신, LBS, 헬스케어, 무선에너지하비스팅

황 유 민(Yu Min Hwang) **준회원**

- 2012년 2월 : 광운대학교 전파공학 학사졸업
- 2012년 3월 ~ 현재 : 광운대학교 전파공학과 석박통합과정

<관심분야> : 차세대 이동통신, 디지털 통신, LBS, 무선에너지하비스팅

차 경 현(Gyeong Hyeon Cha) **준회원**

- 2014년 7월 : 광운대학교 전자융합공학과 졸업
- 2014년 8월 ~ 현재 : 광운대학교 전파공학과 석박사통합과정

<관심분야> : 무선통신, 항재밍, LBS, 데이터마이닝, 무선에너지하비스팅

이 재 생(Jae-Seang Lee) **준회원**

- 2006년 2월 : 고려대학교 전기전자전파공학부 학사
- 2008년 2월 : 한국과학기술원 전기 및 전자공학과 석사
- 2008년 2월 ~ 현재 : 국방과학연구소 선임연구원

<관심분야> : 이동통신, Ad-hoc 네트워크, Trust Network 등

신 요 안(Yoan Shin) **종신회원**

- 1992년 12월: Univ. of Texas at Austin 전기 및 컴퓨터공학과 공학박사
- 1994년 9월 ~ 현재: 숭실대학교 전자정보공학부 교수
- 2008년 1월 ~ 2008년 12월: 한국통신학회 이동통신연구회 위원장

<관심분야> : 이동 및 무선통신, 통신신호처리

김 진 영 (Jin Young Kim) **종신회원**

- 1998년 2월 : 서울대학교 전자 공학과 공학박사
- 2001년 2월 : SK텔레콤 네트웍 연구소 책임연구원
- 2001년 3월 ~ 현재 : 광운대학교 전자융합공학과 교수

<관심분야> : 디지털통신, 가시광통신, UWB, 부호화, 인지무선통신, 차세대 이동통신