The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 2, pp.51-56, Apr. 30, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.2.51
JIIBC 2017-2-8

MTD 기법이 적용된 SDR 통신 시스템의 성능 분석

Performance Analysis of SDR Communication System Based on MTD Technology

기장근*, 이규대**

Jang-Geun Ki*, Kyu-Tae Lee**

요 약 최근 이동 단말의 급격한 증가와 함께 통신망 구축의 용이성, 단말의 자유로운 이동성 및 세션의 연속성, 유선에 비견되는 데이터 전송 대역폭 등을 제공하는 무선 통신 기술에 대한 수요가 급증하고 있다. 그러나 이러한 무선 통신은 신호전달 특성상 도청이나 DOS 공격, 세션 하이재킹, 재밍 등과 같은 악의적 무선 사이버 공격에 취약하다는 단점을 갖는다. 이와 같은 무선 사이버 공격을 막는 다양한 방법 중 최근 많은 연구가 이루어지고 있는 MTD(Moving Target Defense) 기술은 시스템이 공격 받을 수 있는 요소들을 지속적으로 변경시킴으로써 방어 시스템의 보안 능력을 향상시키는 기법이다.
본 논문에서는 자가 방어 및 복원력이 있는 무선 통신 시스템 구축을 위해 변복조 방법, 동작 주파수, 전송 패킷 길이 등을 동적으로 변화시키는 MTD 기법이 적용된 SDR(Software Defined Radio) 무선통신 테스트베드를 개발하고, 악의적 사용자의 공격 성공률에 대한 성능분석 수식을 제안하고, 시뮬레이션을 통해 성능분석 결과의 타당성을 검증하였다.

Abstract With the rapid increase in the number of mobile terminals, demand for wireless technologies has sharply increased these days. While wireless communication provides advantages such as ease of deployment, mobility of terminals, continuity of session, and almost comparable transmission bandwidth to the wired communication, it has vulnerability to malicious radio attacks such as eavesdropping, denial of service, session hijacking, and jamming. Among a variety of methods of preventing wireless attacks, the MTD(Moving Target Defense) is the technique for improving the security capability of the defense system by constantly changing the ability of the system to be attacked.
In this paper, in order to develop a resilient software defined radio communication testbed system, we present a novel MTD approach to change dynamically and randomly the radio parameters such as modulation scheme, operating frequency, packet size.
The probability of successful attack on the developed MTD-based SDR communication system has been analysed in a mathematical way and verified through simulation.

Key Words : Moving Target Defense, Software Defined Radio, Performance Analysis

Ⅰ. 서 론

최근 개인 휴대용 단말의 폭발적인 증가와 함께 유선에 비해 상대적으로 구축이 용이하고 비용이 저렴하며 대역폭이 크게 증가된 무선 통신망의 구축이 활발히 이루어지고 있다. 그러나 신호전달 특성상 무선 통신방식

*종신회원, 공주대학교 전기전자제어공학부
**종신회원, 공주대학교 정보통신공학부
접수일자 2017년 2월 9일, 수정완료 2017년 3월 9일
게재확정일자 2017년 4월 7일

Received: 9 February, 2017 / Revised: 9 March, 2017 /
Accepted: 7 April, 2017
*Corresponding Author: kjg@kongju.ac.kr
Div. of Electrical, Electronic, and Control Engineering, Kongju National University, Korea

은 기본적으로 유선에 비해 데이터 도청이나 인가되지 않은 사용자의 악의적 접근이 비교적 용이하기 때문에 근본적으로 보안에 상당히 취약하다는 단점을 갖는다.

이와 같은 무선 보안 취약점을 개선하기 위한 많은 연구결과[1-3]로 무선 통신 보안기술이 과거에 비해 많이 발전하고 있지만, 무선 트래픽의 폭발적 증가와 함께 무선 기술에 대한 스니핑(sniffing), DOS(Denial Of Service) 공격, 세션 하이재킹(hijacking), 재밍(jamming) 공격과 같은 사이버 공격 또한 급격히 증가하고 있어 보다 효율적인 보안 대책이 필요한 실정이다.

이와 같은 무선 사이버 공격을 막는 다양한 방법 중 시스템이 공격 받을 수 있는 요소들을 지속적으로 변경시키는 MTD(Moving Target Defense)[4-6] 기술에 대해 최근 많은 관심이 집중되고 있다. MTD 메커니즘이 적용된 통신시스템은 공격받는 기능요소들의 지속적인 변화로 인해 시스템 취약성 노출은 줄어들고 공격자의 공격은 더욱 복잡하게 되어 공격 비용이 증가하고 상대적으로 공격 성공률은 줄어들게 되어 궁극적으로 시스템의 자가 방어 및 복원력을 증가시키게 된다. 이러한 MTD 기법은 통신 시스템의 물리 계층부터 응용 계층에 이르는 모든 계층에 적용할 수 있으며, 다양한 계층에 복합적으로 MTD 기술이 적용될수록 보안은 강화될 수 있다.

본 논문에서는 다양한 무선 사이버 공격을 극복할 수 있는 자가 방어 및 복원력을 갖는 탄력성 있는 무선 통신 시스템을 구축하기 위해 변복조 방법, 동작 주파수, 전송 패킷 길이 등을 동적으로 변화시키는 MTD 기법을 SDR(Software Defined Radio)[7-10]의 프로그램으로 구현하고, 이에 따른 이론적인 성능분석을 수행하였다.

II. MTD-SDR 테스트 베드 구성

SDR(Software Defined Radio) 기술은 재구성이 가능한 무선 기술로 수신한 무선 신호를 컴퓨터로 보내 소프트웨어로 처리한다. SDR 시스템은 송신 또는 수신 모드에 따라 IF(Intermediate Frequency) 신호를 RF(Radio Frequency) 신호로 변환하거나 그와 반대로 변환하는 믹서, 아날로그-디지털/디지털-아날로그 변환기 그리고 소프트웨어에 기술된 신호처리 명령어들을 처리하기 위한 DSP 또는 FPGA로 구성된다[9]. 연구목적으로 SDR을 구현하기 위해 가장 많이 사용되는 소프트웨어로는 GNU-Radio[11,12]가 있다. GNU-Radio는 무료 오픈 소스 소프트웨어로 신호처리를 위한 프로그램 블록을 제공하고, Python과 C++ 언어를 지원한다. 그러나 GNU-Radio에서 제공하는 모듈만으로는 MTD 기법을 적용할 수 없기 때문에 본 논문에서는 GNU-Radio 모듈의 파라미터들을 변경할 수 있는 자체 Python 프로그램을 개발하여 사용하였다.

그림 1에 구성된 테스트 베드의 송수신기 블록도를 나타내었다. 본 논문에서 개발된 GNU-Radio 모듈을 동작시키는 Python 프로그램은 표 1에 나타낸 예와 같이 전송 주파수, 변복조 방식, 패킷 길이 등의 다양한 조합으로 구성된 채널을 일정 시간마다 임의 순서로 선택하여 전송 링크를 구성하도록 프로그램 되었다.

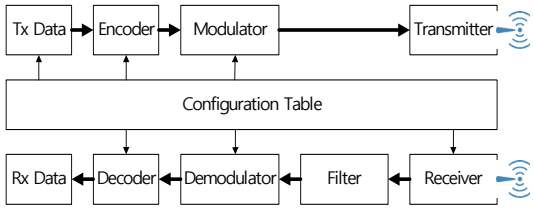

그림 1. 송수신기 블록도
Fig. 1. Transmitter/Receiver block diagram

표 1. MTD 기법 적용을 위한 전송 채널 구성 예
Table 1. Transmission channel configuration for MTD

채널 ID	주파수	모듈레이션	패킷길이
1	100 MHz	GFSK	1024Byte
2	120 MHz	GFSK	512Byte
3	80 MHz	GMSK	256Byte
.....	.....	.....	.....

GFSK : Gaussian Frequency Shift Keying
GMSK : Gaussian Minimum Shift Keying

III. MTD 시스템 성능 분석

MTD 기법이 적용된 통신 시스템의 성능을 분석하기 위한 시스템 모델링 및 가정은 다음과 같다.

통신시스템은 총 $N_{totalCH}$ 개의 전송 채널을 가지고 있으며, 매 $T_{changeCH}$ 시간 마다 전송 채널을 바꾸어 가며 데이터를 전송한다. 데이터 전송이 시작될 때 송신측은 사용할 전송 채널들의 리스트를 미리 생성하여 수신

측과 공유한다고 가정하며, 전송 채널 리스트의 크기는 N_{usedCH} 이다. 참고로 각각의 전송 채널은 표 1의 예시와 같이 MTD 기법의 적용을 위해 전송 주파수, 모듈레이션 기법, 전송 패킷 길이 등의 속성 값이 다양하게 조합되어 구성된다.

공격자는 매 단위 시간마다 $N_{totalCH}$ 개의 전송 채널들 중 임의의 하나를 선택해 공격을 시도하며, 일단 공격이 성공하게 되면 공격 실패가 일어나기 전까지 계속 공격 채널을 유지한다.

공격자의 공격 방법에 따라 데이터 송수신측은 공격 성공 여부를 감지 할 수 있는 경우도 있고, 그렇지 않은 경우도 있을 수 있다. 예를 들어 공격자가 단순히 전송 데이터의 스캐닝(scanning)이나 모니터링(monitoring) 공격을 한다면 감지가 어렵게 되고, 반면에 재밍(jamming)과 같은 공격을 한다면 공격을 용이하게 감지할 수 있을 것이다. 따라서 본 논문에서는 데이터 송수신측이 공격 성공여부를 감지할 수 있는 경우와 감지할 수 없는 2가지 경우로 나누어 성능을 분석한다. 공격을 감지할 수 없는 경우에는 공격 성공 여부에 관계없이 데이터 전송채널이 일정한 $T_{changeCH}$ 시간 마다 변경되며, 공격 성공을 감지할 수 있는 경우에는 공격 성공이 감지된 바로 다음 단위시간부터 전송 채널을 바꾸게 된다.

1. 스캐닝 공격 성공률

스캐닝(scanning) 공격 성공률은 그림 2에 나타낸 것과 같이 데이터 송수신측이 공격 성공 여부에 상관없이 정해진 $T_{changeCH}$ 시간마다 전송 채널을 변경해 가면서 데이터를 송수신할 때 공격자가 매 단위시간마다 임의로 선택한 공격 채널이 전송 채널과 일치하는 비율로 정의한다.

스캐닝 공격 성공률 식을 유도하기 위해 표 2에 $T_{changeCH}$ 구간내의 매 단위시간 슬롯마다 공격자가 성공적으로 전송채널을 예측하여 공격이 성공할 확률과 해당 타임 슬롯에서 공격이 성공할 경우 공격 성공이 지속되는 시간을 나타내었다.

표 2. 단위시간별 공격 성공률 및 공격성공 지속시간
Table 2. Attack success probability and success duration at each unit time slot

단위시간 슬롯	각 단위시간 슬롯에서의 공격 성공률	공격성공 지속시간
1	$\frac{1}{N_{totalCH}}$	$T_{changeCH}$
2	$\left(\frac{N-1}{N}\right)^1\left(\frac{1}{N}\right)$	$T_{changeCH}-1$
3	$\left(\frac{N-1}{N}\right)^2\left(\frac{1}{N}\right)$	$T_{changeCH}-2$
...	.....	.....
i	$\left(\frac{N-1}{N}\right)^{i-1}\left(\frac{1}{N}\right)$	$T_{changeCH}-i+1$

따라서 스캐닝 공격 성공률은 아래 식 (1)과 같이 계산될 수 있다. 참고로 스캐닝 공격 성공률은 $T_{changeCH}$ 시간동안의 확률을 구하면 되는데, 이는 스캐닝 공격이 $T_{changeCH}$ 시간마다 같은 조건으로 반복적으로 수행되어 $T_{changeCH}$ 시간을 공격의 한 주기로 생각할 수 있기 때문이다.

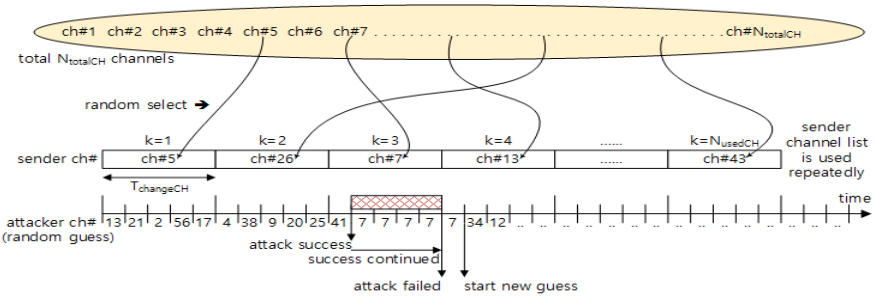

그림 2. 데이터 전송 채널 및 공격 채널 동작
Fig. 2. Operation of data transmission channel and attack channel

$$P_{success\_random\_scan\_attack} = \frac{\sum_{i=1}^{T_{changeCH}} \left(\frac{N_{totalCH}-1}{N_{totalCH}}\right)^{i-1} \left(\frac{1}{N_{totalCH}}\right) (T_{changeCH}-i+1)}{T_{changeCH}} \quad (1)$$

2. 재밍 공격 성공률

재밍(jamming) 공격 성공률은 기본적으로 매 $T_{changeCH}$ 시간마다 전송 채널을 변경해 가면서 데이터를 전송하되, 만일 공격자의 재밍 공격이 성공할 경우 즉시 전송채널을 변경하는 환경에서의 공격 성공률을 의미한다. 재밍 공격은 특성상 데이터를 단순히 훔쳐보는 스캐닝 공격과는 달리 데이터 전송을 방해함으로 데이터 송수신 노드는 재밍 공격의 성공을 비교적 용이하게 알아낼 수 있다.

공격자의 재밍 공격 성공률은 아래 식 (2)와 같이 간단히 구할 수 있으며, 이는 공격자가 한번 공격에 성공한다고 해도 바로 다음 슬롯에서 전송 채널이 바뀌게 되어 공격자는 매 타임 슬롯마다 전송 채널을 새로 예측해야하기 때문이다.

$$P_{success\_random\_jam\_attack} = \frac{1}{N_{totalCH}} \quad (2)$$

3. 공격 성공률 검증용 시뮬레이션 프로그램

앞에서 유도한 공격 성공률 식의 타당성을 검증하기 위해 C 언어를 사용하여 통신 시스템을 모델링하고 시뮬레이션 프로그램을 개발하였다. 그림 3에 시뮬레이션 프로그램의 순서도를 가상코드(Pseudo Code)로 나타내었다.

```
create CHlist[NusedCH] filled with txCH IDs at random;
For (each unit time slot)          // for every time slot
  If (attacked && jamming)         // choose Tx channel
    change txCH;
  Else
    If (time TchangeCH is up for current txCH)
      change txCH;
    Endif
  Endif
  choose attackCH randomly         // choose attack channel
  attacked = 0;
  If (txCH == attackCH)            // decide if attack succeeds
    attacked = 1;
    update the statistics;
  Endif
Endfor
```

그림 3. 공격성공률 계산을 위한 시뮬레이션 가상코드
Fig. 3. Simulation pseudo code for successful attack probability

먼저 송신측은 데이터 전송에 사용할 채널들의 리스트(총 N_{usedCH} 개로 구성)를 생성하며, 사용할 채널들의 순서는 랜덤하게 결정된다. 시뮬레이션 프로그램에서 필요한 난수를 생성하기 위해 주기가 길고 실행속도가 빠른 WELL 알고리즘[13]을 사용하였고, 효율적인 전송 채널 리스트(CHlist[])를 구성하기 위해 그림 4와 같이 isher - Yates 셔플(shuffle) 알고리즘[14]을 변형하여 사용하였다.

```
for (j = 0; j < NtotalCH; j++)
        tempCHlist[j] = j;
for (j = 0; j < NusedCH; j++)
{       randnum = getWELLrand(NtotalCH - j) + j;
        exchange tempCHlist[j] with tempCHlist[randnum];
        CHlist[j] = tempCHlist[j];
}
```

그림 4. 전송채널 리스트 구성을 위한 시뮬레이션 가상코드
Fig. 4. Simulation pseudo code for creating the Tx channel list

4. 성능 분석 결과

그림 5에 랜덤 스캐닝 공격 성공률에 대한 시뮬레이션 결과를 나타내었으며, 이 결과는 식 (1)에 의해 계산된 값과 1% 미만의 차이를 보여 그래프에는 수식에 의해 계산된 값은 나타내지 않았다. 그림에서 확인할 수 있듯이 랜덤 스캔 공격의 경우 전송채널의 변화 주기인 $T_{changeCH}$ 값이 클수록 공격 성공률이 증가함을 볼 수 있다. 또한 사용할 수 있는 전체 채널 개수를 의미하는 $N_{totalCH}$ 값이 클수록 공격 성공률은 작은 값을 가짐을 볼 수 있다.

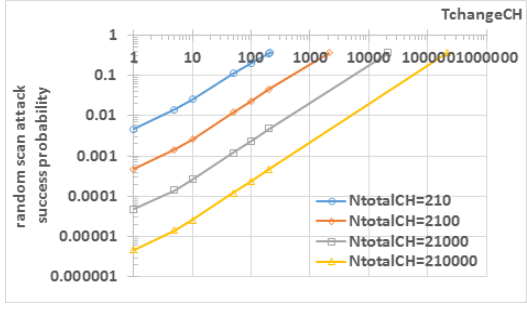

그림 5. 랜덤 스캐닝 공격 성공 확률
Fig. 5. Random scanning attack success probability

그림 6에는 랜덤 재밍 공격 성공률에 대한 시뮬레이션 결과를 나타내었으며, 이 결과 역시 식 (2)의 계산 값과

1% 미만의 아주 작은 오차를 보였다. 랜덤 재밍 공격의 경우 송수신자가 공격 성공을 감지할 수 있어 공격이 성공할 경우 즉시 채널을 변경하기 때문에 매 타임 슬롯마다 공격자는 새롭게 채널을 예측해야 하고 따라서 전송 채널의 기본 변화 주기인 $T_{changeCH}$ 값에 상관없이 일정한 공격성공률을 가지게 된다. 랜덤 재밍 공격은 랜덤 스캐닝 공격과 마찬가지로 전체 채널 개수 $N_{totalCH}$ 값이 클수록 공격 성공률은 일정 비율로 작은 값을 가짐을 볼 수 있다.

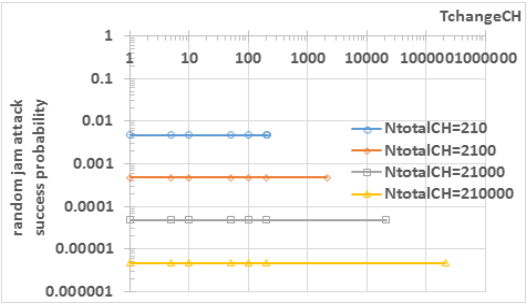

그림 6. 랜덤 재밍 공격 성공 확률
Fig. 6. Random jamming attack success probability

Ⅳ. 결론

최근 폭발적인 이동 단말의 증가와 함께 통신망 구축이 용이하고 단말의 자유로운 이동성 및 세션의 연속성 등을 보장하면서도 유선에 비견되는 데이터 전송 대역폭을 제공하는 무선 통신 기술에 대한 수요가 급증하고 있다. 그러나 무선통신은 무선의 신호전달 특성상 데이터 도청이나 DOS(Denial Of Service) 공격, 세션 하이재킹(hijacking), 재밍(jamming) 등과 같은 악의적 무선 사이버 공격에 취약하다는 보안 관련 단점을 갖는다.

이와 같은 무선 사이버 공격을 막는 다양한 방법 중 최근 많은 연구가 이루어지고 있는 MTD(Moving Target Defense) 기술은 시스템이 공격 받을 수 있는 요소들을 수시로 변경시킴으로써 시스템 취약성 노출시간을 줄이고 공격자의 공격을 더욱 복잡하게 만들어 공격 비용은 증가시키고 공격성공률은 낮추어 방어 시스템의 보안 능력을 향상시키는 기법이다

본 논문에서는 자가 방어 및 복원력이 있는 무선 통신 시스템 구축을 위해 변복조 방법, 동작 주파수, 전송 패킷 길이 등을 동적으로 변화시키는 MTD 기법이 적용된 SDR(Software Defined Radio) 무선통신 테스트베드를 개발하고, 보안 관련 성능 분석을 위해 악의적 사용자의 공격성공률 계산을 위한 수식을 제안하고, 시뮬레이션을 통해 결과가 일치함을 보임으로써 타당성을 검증하였다.

앞으로 데이터 링크 계층뿐만 아니라 망 계층에도 IP 주소 변경 등과 같은 MTD 기법이 복합적으로 적용된 확장된 테스트 베드를 구축하고, 보다 다양한 공격 방식에 대한 성능 분석을 수행할 예정이다.

References

[1] Se-Hwan Park, Jong-Kyu Park, "IoT Industry & Security Technology Trends," International Journal of Advanced Smart Convergence (IJASC), Vol. 5, No. 3, pp. 27-31, Sept., 2016. DOI: https://doi.org/10.7236/ijasc.2016.5.3.27

[2] Myongyeal Lee, Jaepyo Park, "Analysis and Study on Invasion Threat and Security Measures for Smart Home Services in IoT Environment," Journal of The Institute of Internet, Broadcasting and Communication (JIIBC), Vol.16, No.5, pp.27-32, Oct., 2016.

[3] Hee-Sook Kim, "A Study on Security System of 4G Network System," Journal of The Institute of Internet, Broadcasting and Communication (JIIBC), Vol.16, No.6, pp.15-23, Dec., 2016.

[4] Valentina Casola, Alessandra De Benedictis, and Massimiliano Albanese, "A Moving Target Defense Approach for Protecting Resource-Constrained Distributed Devices," IEEE 14th International Conference on Information Reuse and Integration(IRI), Aug., 2013.
DOI: https://doi.org/10.1109/iri.2013.6642449

[5] Panos Kampanakis, Harry Perros, and Tsegereda Beyene, "SDN-based solutions for Moving Target Defense network protection," IEEE 15th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2014.

DOI: https://doi.org/10.1109/wowmom.2014.6918979

[6] S. Jajodia, A. K. Ghosh, V. S. Subrahmanian, V. Swarup, C. Wang, and X. S. Wang, editors. Moving Target Defense II: Application of Game Theory and Adversarial Modeling, Springer, ISBN 978-1-4614-5416-8, 2013.

[7] Markus Dillinger, Kambiz Madani, Nancy Alonistioti, Software Defined Radio: Architectures, Systems and Functions, John Wiley & Sons, ISBN 0-470-85164-3, 2003.

[8] Chi-Yuan Chen, Fan-Hsun Tseng, Kai-Di Chang, Han-Chieh Chao, and Jiann-Liang Chen, "Reconfigurable Software Defined Radio and Its Applications," Tamkang Journal of Science and Engineering, Vol. 13, No. 1, pp.29-38, 2010.

[9] Rehan Muzammil, M. Salim Beg, Mohsin M. Jamali, "A Dynamically Reconfigurable Transceiver for Software Defined Radio," International Journal of Computer Applications (0975 - 8887), Vol.76, No.17, Aug., 2013.
DOI: https://doi.org/10.5120/13344-0716

[10] Moshe Timothy Masonta, Mjumo Mzyece, and Ntsibane Ntlatlapa, "Spectrum Decision in Cognitive Radio Networks: A Survey," IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, pp.1088-1107, 3rd quarter 2013.
DOI: https://doi.org/10.1109/surv.2012.111412.00160

[11] GNURAdio, http://gnuradio.org/, 2017.

[12] Feng Ge, C. Jason Chiang, Yitzchak M. Gottlieb, and Ritu Chadha, "GNU Radio-Based Digital Communications: Computational Analysis of a GMSK Transceiver," Global Telecommunications Conference (GLOBECOM), Dec., 2011.
DOI: https://doi.org/10.1109/glocom.2011.6133692

[13] François Panneton, Pierre L'ecuyer, and Makoto Matsumoto, "Improved Long-Period Generators Based on Linear Recurrences Modulo 2," ACM Transactions on Mathematical Software, Vol. 32, No. 1, pp.1-16, March 2006.
DOI: https://doi.org/10.1145/1132973.1132974

[14] Donald E. Knuth, The Art of Computer Programming Vol.2, 3rd Ed., pp.145-146, Addison-Wesley, 1997.

저자 소개

기 장 근(종신회원)

- 1986년 2월 고려대학교 전자공학과졸업
- 1988년 2월 고려대학교 전자공학과 석사
- 1992년 2월 고려대학교 전자공학과 박사
- 2002년 6월 ~ 2003년 6월 Univ. of Arizona 방문교수
- 2010년 8월 ~ 2011년 8월 Univ. of Arizona 방문교수
- 2016년 8월 ~ 2017년 8월 Univ. of Arizona 방문교수
- 1992년 3월 ~ 현재 : 공주대 전기전자제어공학부 교수

<주관심분야 : 통신프로토콜, 이동통신시스템>

이 규 대(종신회원)

- 1984년 고려대 전자공학과 졸업
- 1986년 고려대 전자공학과 석사
- 1991년 고려대 전자공학과 박사
- 2001년 미 죠지아텍 교환 교수
- 2006년 미 일리노이주립대 교환 교수
- 2007년 ~ 2009년 : 한국전자통신연구원 이동통신연구소 초빙연구원
- 1992년 3월 ~ 현재 : 공주대 정보통신공학부 교수

<주관심분야 : 회로 및 시스템, 신호처리, VLC>

※ 본 논문은 공주대학교 연구년 사업에 의하여 연구되었음.