The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 5, pp.55-62, Oct. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.5.55
JIIBC 2018-5-7

# MTD-SDR 시스템의 취약요소 변경에 따른 악의적 공격 성공 확률

# Malicious Attack Success Probability on the Change of Vulnerable Surfaces in MTD-SDR System

기장근*, 이규대**

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

**요 약** MTD(Moving Target Defense)는 자가 복원력이 있는 무선 통신 시스템을 구축할 수 있도록 대상 시스템의 다양한 구조 및 운영 관련 파라미터들을 동적으로 변경시키도록 설계함으로써 공격자의 악의적 공격으로부터 시스템의 취약점을 보호하는 기술이다. 본 논문에서는 MTD-SDR 기술을 기반으로 하는 통신 시스템에서 랜덤/순서적 스캐닝/재밍 공격 성공 확률에 대한 식을 유도하고 시뮬레이션을 통해 그 결과를 검증하였다. 결과적으로 랜덤 스캐닝 공격의 경우에는 전송채널 변화주기 값이 증가할수록 공격성공률이 증가하는 반면, 랜덤 재밍 공격의 경우에는 변화가 없다. 순서적 공격의 경우에는 랜덤 공격과 유사한 경향의 성공률 패턴을 보이지만 전송채널 변화주기가 커져서 전체 전송채널 수에 접근할수록 재밍 공격의 경우에는 최대 2배, 스캐닝 공격의 경우에는 최대 36% 정도 랜덤 공격에 비해 공격 성공률이 높은 것으로 나타났다.

**Abstract** The MTD-based approach changes various operating parameters dynamically so that the vulnerability of the system can be protected from the malicious attack. In this paper, random/serial scanning/jamming attack success probabilities have been mathematically analyzed and verified through simulation to improve the security of the wireless communication systems in which the MTD-SDR technologies are applied. As a result, for random scanning attacks, attack success probability increases as the change period of transmission channel increases, while for random jamming attacks there is no change. The attack success probability patterns for serial attacks are similar to those of random attacks, but when the change period of transmission channel approaches to the total number of transmission channels, the success probability of serial attack is getting greater than that of random attack, up to twice in jamming attacks and up to 36% in scanning attacks.

**Key Words :** Attack Success Probability, Moving Target Defense, Software Defined Radio

## Ⅰ. 서 론

최근 설치가 용이하고 비용이 저렴하며 유선에 못지 않은 고속의 전송 대역폭을 지원하는 무선 통신망이 지속적으로 확장되고 있다. 그러나 이러한 무선 기술의 사용이 확대될수록 사이버 공격 가능성 또한 증가되고 있는 실정이다. 기존의 무선 통신 프로토콜들이 보안관련 문제의 해결책을 일부 제시하고 있긴 하지만 서비스 거

*종신회원, 공주대학교 전기전자제어공학부 교수
**종신회원, 공주대학교 정보통신공학부 교수
접수일자 : 2018년 8월 9일, 수정완료 : 2018년 9월 9일
게재확정일자 : 2018년 10월 5일

Received: 9 August, 2018 / Revised: 9 September, 2018 / Accepted: 5 October, 2018
*Corresponding Author: kjg@kongju.ac.kr
Div. of Electrical, Electronic, and Control Engineering, Kongju National University, Korea

부 공격, 세션 하이재킹, 재밍 공격 등과 같은 사이버 공격들에 대한 보다 효율적인 대책이 필요하다[1-4].

MTD(Moving Target Defense) 시스템[5-7]은 통신 시스템과 통신망의 구성요소들을 동적으로 계속 변경하고 관리함으로써 악의적 공격자가 시스템을 공격할 수 있는 기회를 줄이고자 하는 목적을 가진 시스템을 말하며, 미국 백악관의 "연방정부 사이버 보안 연구 및 개발 프로그램을 위한 전략 계획"[8]에서 언급하고 있을 정도로 중요한 이슈중의 하나이다.

현재의 통신 시스템들은 구성과 운영에 있어 한번 정해지면 그 형태를 계속 유지하는 정적 구조를 가지고 있어 공격자에게 시스템 취약점을 찾기 위한 충분한 시간을 제공하고, 또한 공격자의 공격이 발생하는 경우에만 이를 방어하기 위한 수동적이고 일시적인 대책을 강구하는 보안전략을 주로 사용하고 있다. MTD 시스템에서는 시스템의 능동적 운영을 통해 시스템 구성요소들을 주기적으로 변화시켜 공격자들이 시스템의 취약점을 분석할 여유를 주지 않고 또한 발견된 취약점도 시간이 지나면 무효화되는 전략을 취한다. 결국 MTD 시스템은 현재 정적 시스템의 보안 벽을 쌓는 개념과는 달리 시스템 구성 및 운영 파라미터들을 끊임없이 동적으로 변화시킴으로써 취약점 노출시간을 줄여 공격자들의 공격을 매우 어렵게 만들고 공격 비용을 증가시키는 새로운 보안 패러다임을 제공한다.

MTD 기술의 실질적 적용 카테고리에 따라 네트워크 수준의 MTD, 호스트 수준의 MTD, 응용 수준의 MTD 기술로 분류할 수 있으며, 최근 시스템 랜덤화, 실행 소프트웨어의 동적 컴파일, 동적 네트워크 구성, 네트워크 및 네트워크 기능 가상화, 소프트웨어 정의 네트워킹 및 소프트웨어 정의 무선통신 등 여러 다양한 분야에 MTD 기술을 적용하는 연구가 활발히 진행되고 있고, 이러한 MTD 기술의 효율성을 모델링하고 정량화할 수 있는 방안 등에 관한 논의가 진행되고 있다. 따라서 본 연구에서는 다양한 사이버 무선 공격에 대해 자가 복구 능력을 갖는 무선 통신 시스템을 구축하기 위한 연구의 일환으로 통신에 사용되는 변복조 기법, 전송 주파수, 전송 패킷 길이 등 다양한 시스템 운영 파라미터들로 특징 지워지는 통신 채널을 동적으로 변경시킬 때 공격자의 공격 패턴에 따른 공격 성공 확률 계산식을 유도하고, 시뮬레이션을 통해 그 결과를 검증하였다.

## II. MTD-SDR 시스템과 공격 모델링

Firas, Jang-Geun 등은 본 연구의 선행 연구[9-11]에서 MTD(Moving Target Defense)와 SDR(Software Defined Radio) 기술 기반의 자가 복원력있는 무선 통신 구조를 제안하고, 기본적인 랜덤 공격에 대한 기초성능 분석을 수행한 바 있다. 이 구조에서 무선 통신 링크는 무선 채널을 동적으로 프로그램 하기 위한 SDR 기법[12,13]을 적용하고 있으며, 각 링크의 구성은 규정된 시간이 지나면 동적으로 랜덤하게 바뀐다. 제안된 구조에 대한 동작 검증을 위해 SDR 테스트 베드를 구성하고 실험적으로 다양한 공격 시나리오에 대한 기본적인 동작을 검증하였다. 구현된 SDR 테스트 베드에는 현재 일반적으로 가장 널리 사용되고 있는 GNU-Radio 툴킷을 사용하였으며. 이 툴킷에서 제공하는 다양한 모듈레이션 기법을 위한 신호처리 모듈들을 동적으로 이용하기 위한 MTD 모듈을 Python 언어를 이용하여 개발하였다.

본 연구에서는 이와 같은 MTD-SDR 통신 시스템에 대해 체계적인 성능분석의 일환으로 스캐닝 공격과 재밍 공격에 대한 공격 성능 확률 식을 유도하고 시뮬레이션을 통해 그 결과를 검증하였다.

먼저 MTD-SDR 기반 통신 시스템에 대한 공격 성공 확률을 계산하기 위한 모델링 및 가정은 다음과 같다.

- 통신 시스템에는 총 N개의 전송 채널이 존재함
- 각 채널은 전송 주파수, 변복조 방법, 패킷 길이, IP 주소 등 다양한 가변요소들로 특징 지워짐
- 송신자는 기본적으로 매 T 시간마다 전송 채널을 변경하되 공격을 인지할 경우 바로 다음 타임 슬롯에서 전송 채널을 변경함
- 송신자는 스캐닝(scanning) 공격은 감지할 수 없고 재밍(jamming) 공격은 인식 가능함
- 악의적 공격은 매 단위시간 슬롯마다 발생하며, 공격자는 공격채널을 랜덤(random) 또는 순서대로 하나씩 선정(serial)하고, 일단 공격이 성공하면 공격 실패가 발생할 때까지 다음 타임 슬롯에서도 현재의 공격 채널을 계속 유지함
- 스캐닝 공격은 일단 한번 성공하면 송신자가 현재의 전송 채널 유지시간인 T 시간이 지날 때까지 공격이 지속적으로 성공됨
- 재밍 공격의 경우에는 송신자가 미리 규정된 T 시간

마다 전송 채널을 변경할 뿐만 아니라 재밍 공격이 성공하면 곧바로 이를 인식하고 전송 채널을 변경함

통신 시스템의 전송 채널과 공격자의 공격 채널 사이의 동작 관계를 그림 1에 나타내었다. 그림에는 스캐닝 공격과 재밍 공격의 경우 각각에 대해 공격자가 공격 채널을 랜덤하게 선택하거나 일정 순서에 의해 선택하는 경우를 구분하여 채널 번호를 예시하였다. 먼저 송신자는 사용 가능한 전체 채널 N개에서 랜덤한 순서대로 각 채널을 사용하여 사용자 데이터를 전송하되, 매 T 시간마다 전송 채널을 변경한다. 공격자는 매 타임 슬롯마다 공격 채널을 랜덤하게 선정하거나 체계적인 공격을 위해 순서적으로 선정하는데, 이 두 방법의 가장 큰 차이점은 순서적 선정의 경우 N 시간동안 모든 채널을 반드시 한 번씩 공격하게 되는 반면 랜덤 선정의 경우 확률적으로는 N 시간동안 N개의 채널이 한 번씩 선정될 수 있으나 이는 어디까지나 확률적인 이야기이고 실제로는 일부 채널이 중복 선정되고 따라서 일부 채널은 공격대상에서 빠질 수 있다는 점이다.

## Ⅲ. MTD-SDR 시스템 공격 성공 확률

MTD-SDR 기술이 적용된 통신 시스템의 성능 분석은 공격의 종류에 따라 스캐닝 공격과 재밍 공격으로 분류하고 각 공격에 대해 공격자의 공격 채널 선택 방법에 따라 아래와 같이 4가지로 세분하여 공격 성공 확률식을 유도하였다.

본 논문에서의 기본적인 공격 성공 확률은 매 타임 슬롯마다 데이터를 송수신할 때 사용되는 전송 채널과 공격자가 선택한 공격 채널의 일치 비율로 정의한다.

### 1. 랜덤 스캐닝 공격 성공 확률

스캐닝 공격시 데이터 송수신자는 공격자의 공격을 인지할 수 없으므로 스캐닝 공격 성공 확률은 데이터 송신측이 정해진 일정한 시간마다 전송 채널을 변경해 가면서 데이터를 송신할 때 공격자가 매 단위시간 타임 슬롯마다 임의로(또는 순서적으로) 선택한 공격 채널이 전송 채널과 일치하는 비율로 계산될 수 있다.

랜덤 스캐닝 공격은 공격자가 랜덤하게 공격 채널을 선택하여 송수신 데이터를 모니터링하는 공격을 말하며, 이에 대한 공격 성공률 식 (1)을 유도하기 위해 표 1에 각 단위 타임 슬롯마다 공격자가 성공적으로 전송채널을 예측하여 공격이 성공할 확률과 해당 타임 슬롯에서 공격이 성공할 경우 공격 성공이 지속되는 시간을 나타내었다. 식에서 N은 전체 전송 채널의 수를 나타내고, T는 송신자의 전송 채널 변경 주기를 나타낸다.

$$P_{rand_scan} = \frac{\sum_{i=1}^{T}\left\{\left(\frac{N-1}{N}\right)^{i-1}\left(\frac{1}{N}\right)(T-i+1)\right\}}{T} \qquad (1)$$

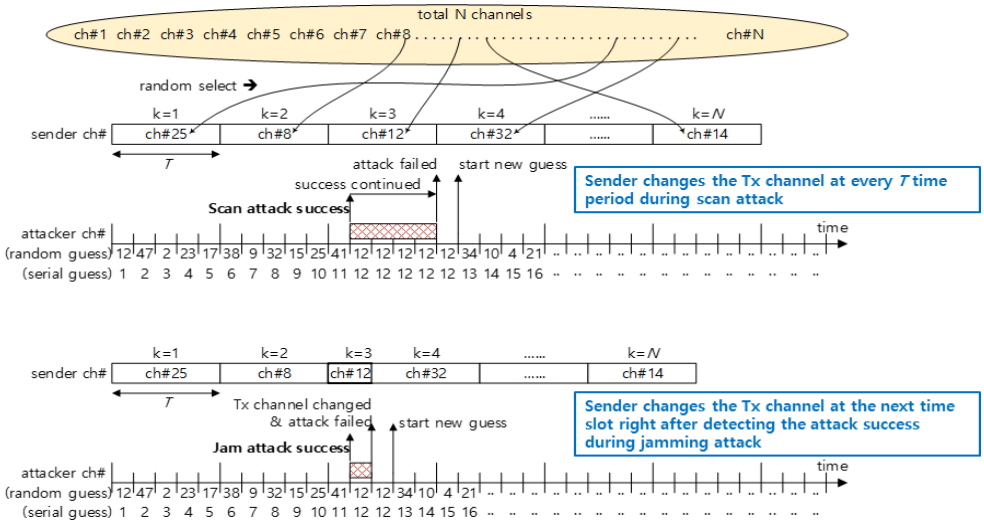


그림 1. 공격 종류에 따른 송신자 전송채널 및 공격자 공격채널 변화
Fig. 1. Sender's Tx channels and attacker's attack channels according to the attack types

**표 1. 타임 슬롯별 랜덤 스캐닝 공격 성공 확률**
Table 1. Random scanning attack success probability at each time slot

| 타임슬롯 | 각 타임 슬롯에서의 랜덤 공격 성공 확률 | 공격성공 지속시간 |
|---|---|---|
| 1 | $\frac{1}{N_{total\,CH}}$ | $T$ |
| 2 | $\left(\frac{N-1}{N}\right)^1\left(\frac{1}{N}\right)$ | $T-1$ |
| 3 | $\left(\frac{N-1}{N}\right)^2\left(\frac{1}{N}\right)$ | $T-2$ |
| … | . . . . . | . . . . . |
| i | $\left(\frac{N-1}{N}\right)^{i-1}\left(\frac{1}{N}\right)$ | $T-i+1$ |

## 2. 순서적 스캐닝 공격 성공 확률

순서적 스캐닝(scanning) 공격 성공 확률 식은 (2)와 같으며, 표 2에 각 타임 슬롯에서의 순서적 공격 성공 확률과 공격 성공 지속 시간을 나타내었다.

$$P_{serial_scan} = \frac{\sum_{i=1}^{T}\left\{\left(\frac{1}{N}\right)(T-i+1)\right\}}{T} = \left(\frac{1}{N}\right)\left(\frac{T+1}{2}\right) \quad (2)$$

**표 2. 타임 슬롯별 순서적 스캐닝 공격 성공 확률**
Table 2. Serial scanning attack success probability at each time slot

| 타임 슬롯 | 각 타임 슬롯에서의 순서적 공격 성공 확률 | 공격성공 지속시간 |
|---|---|---|
| 1 | $\frac{1}{N_{total\,CH}}$ | $T$ |
| 2 | $\left(\frac{N-1}{N}\right)\left(\frac{1}{N-1}\right)=\frac{1}{N}$ | $T-1$ |
| 3 | $\left(\frac{N-1}{N}\right)\left(\frac{N-2}{N-1}\right)\left(\frac{1}{N-2}\right)=\frac{1}{N}$ | $T-2$ |
| … | . . . . . | . . . |
| i | $\left(\frac{N-1}{N}\right)\left(\frac{N-2}{N-1}\right)\left(\frac{N-3}{N-2}\right)\cdot\cdot\left(\frac{1}{N-i+1}\right)=\frac{1}{N}$ | $T-i+1$ |

## 3. 랜덤 재밍 공격 성공 확률

재밍(jamming) 공격은 데이터 송수신에 영향을 주어 데이터 송수신자가 공격자의 공격을 인식할 수 있으므로, 데이터 송신측이 기본적으로 정해진 일정한 시간마다 전송 채널을 변경해 가면서 데이터를 송신하다가 공격을 인식할 경우 바로 전송 채널을 변경하게 된다. 따라서 공격이 한번 성공했다고 해도 다음 타임 슬롯에서 공격이 실패하게 되고 랜덤 재밍 공격의 경우 새로운 공격 채널을 랜덤하게 선택하게 됨으로 공격 성공 확률은 식 (3)과 같게 된다.

$$P_{rand_jam} = \frac{1}{N} \quad (3)$$

## 4. 순서적 재밍 공격 성공 확률

순서적 재밍 공격 성공 확률을 구하기 위해 앞에서 구한 식 (2)의 순서적 스캐닝 공격 성공 확률로부터 먼저 그림 2에 나타낸 것과 같이 N 시간동안 공격이 성공할 수 있는 평균 시간을 $L_s = N \times P_{serial_scan}$ 와 같이 계산할 수 있고 따라서 전체 N 시간 중 공격 실패할 시간구간은 아래 식 (4)와 같이 구할 수 있다.

$$\begin{aligned} L_f = N - L_s &= N - N \times P_{serial_scan} \\ &= N(1 - P_{serial_scan}) \end{aligned} \quad (4)$$

평균적으로 볼 때 공격 실패할 시간 구간 $L_f$가 지나면 공격이 한번 성공하게 되고 다시 송신자가 송신 채널을 변경하게 됨으로 공격은 다시 실패하게 된다. 따라서 매 $L_f+2$ 타임 슬롯마다 한번의 공격 성공이 이루어지게 되어 순서적 재밍 공격 성공 확률은 식 (5)와 같이 구할 수 있게 된다.

$$P_{serial_jam} = \frac{1}{L_f+2} = \frac{1}{N(1-P_{serial_scan})+2} \quad (5)$$

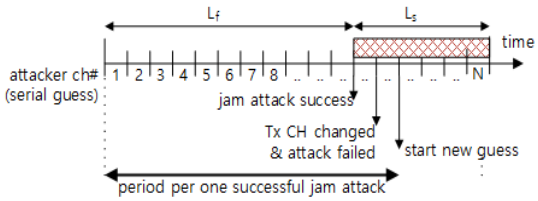


**그림 2. 순서적 재밍 공격 성공 확률 계산**
Fig. 2. Calculation of attack success probability in serial jamming attack

## Ⅳ. MTD-SDR 시스템 성능분석

앞장에 기술한 MTD-SDR 시스템의 공격 종류별 공격 성공률 식들의 타당성 검증을 위해 C 언어로 시뮬레이션 프로그램을 개발하고, 이론적인 계산식의 결과와 시뮬레이션 프로그램의 실행 결과를 비교 분석하였다.

악의적 공격의 종류로는 공격채널을 임의로 선택하는 랜덤 공격과 모든 채널을 차례로 한번씩 공격채널로 선택하는 순서적 공격으로 나누어 시뮬레이션을 수행하였다. 참고로 순서적 공격에서는 N 시간동안 모든 채널이 중복없이 한번씩 차례로 공격 대상이 되나, 랜덤 공격에서는 공격 채널이 중복되어 선택될 가능성이 있으므로 전체 시뮬레이션 시간은 1000N 시간으로 설정하였다.

결과적으로 모든 이론적 계산결과와 시뮬레이션 결과들은 최대 약 1.5% 이내의 오차만을 보였으며, 따라서 본 논문에 제시하는 결과 데이터들은 모두 시뮬레이션 결과만을 그래프로 나타내었다.

### 1. 랜덤 공격 성공 확률 분석

그림 3에 전송채널 변화주기 T의 변화에 따른 랜덤 스캐닝 공격과 랜덤 재밍 공격의 성공 확률에 대한 시뮬레이션 결과를 나타내었다.

그림 3으로부터 랜덤 스캐닝 공격의 경우에는 전송채널 변화주기 T 값이 증가할수록 공격성공률이 증가하는 반면, 랜덤 재밍 공격의 경우에는 변화가 없음을 알 수 있다. 이는 랜덤 재밍 공격의 경우 공격이 성공하면 데이터의 송수신이 정상적으로 이루어지지 않아 데이터 송수신자가 데이터 전송채널을 다른 채널로 즉시 변경하기 때문에 그 공격성공이 지속되지 않고 따라서 공격자는 다시 데이터 채널을 랜덤하게 예측하는 과정을 새롭게 시작해야 하기 때문이다. 반면에 랜덤 스캐닝 공격의 경우에는 데이터 송수신자가 공격 성공 유무를 알지 못함으로 정해진 시간(전송채널 변화주기)동안 지속적으로 현재의 데이터 채널을 유지하기 때문에 전송채널 변화주기가 길어질수록 공격 성공 확률은 커지게 된다. 또한 그림 3에서 데이터 송수신에 사용되는 전체 전송채널의 수 N의 변화에 따른 공격 성공 확률을 살펴보면 스캐닝 공격이든 재밍 공격이든 간에 전체 전송채널 수 N이 커질수록 공격 성공 확률이 작아짐을 알 수 있다.

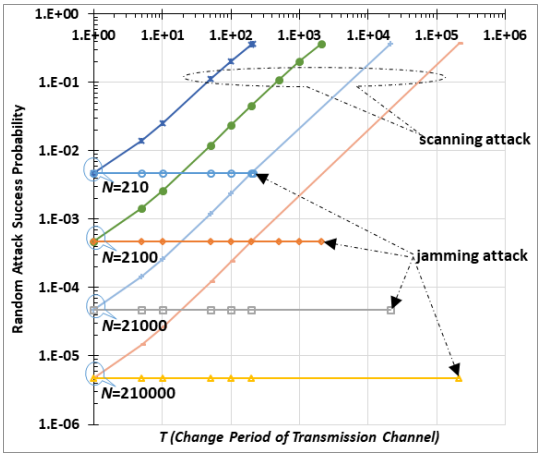


그림 3. 랜덤 공격 성공 확률
Fig. 3. Random attack success probability

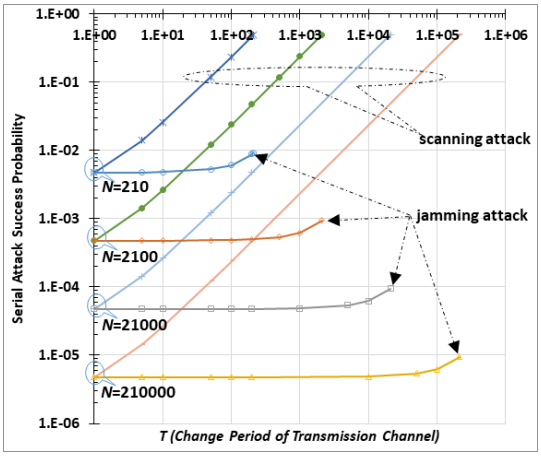


그림 4. 순서적 공격 성공 확률
Fig. 4. Serial attack success probability

### 2. 순서적 공격 성공 확률 분석

그림 4에는 전송채널 변화주기 T의 변화에 따른 순서적 스캐닝 공격과 순서적 재밍 공격의 성공 확률을 나타내었다.

그림 4의 순서적 공격의 경우에 대한 결과를 살펴보면 그림 3에 나타내었던 랜덤 공격의 경우와 전반적으로 비슷한 경향의 공격 성공 확률 결과를 보여주고 있다. 즉, 스캐닝, 재밍 두 경우 모두 전송 채널 수 N이 클수록 공격 성공 확률은 작고, 전송 채널 변화주기 T에 대해서는 스캐닝 공격의 경우 T값에 비례해 커지는 반면 재밍 공격의 경우에는 대부분의 T값 변화 구간에서 거의 변화가

없다가 T값이 N값에 가까워지는 끝 부분에서는 증가하는 경향을 나타내고 있다. 이러한 변화를 비교해 보기위한 예로써 그림 5에 전송 채널 수 N=2100인 경우 랜덤과 순서적 재밍 공격 성공 확률을 하나의 그래프로 나타내었다. 그림에서 T=N=2100에 해당하는 끝 지점의 랜덤 공격 성공 확률은 4.7619E-04 이고, 순서적 공격 성공 확률은 9.5102E-04 이며, 따라서 순서적 공격이 랜덤 공격에 비해 최대 2배 정도의 공격 성공 확률을 보임을 알 수 있다. 그림 6에는 전송 채널 수 N=2100인 경우 스캐닝 공격의 랜덤과 순서적 공격 성공 확률을 비교하여 나타내었다. 스캐닝 공격의 경우 T=N=2100 지점에서 랜덤 공격 성공 확률은 3.6809E-01 이고, 순서적 공격 성공 확률은 5.0024E-01 이며, 따라서 순서적 공격이 랜덤 공격에 비해 최대 약 36% 정도 성공확률이 높게 나타났다.

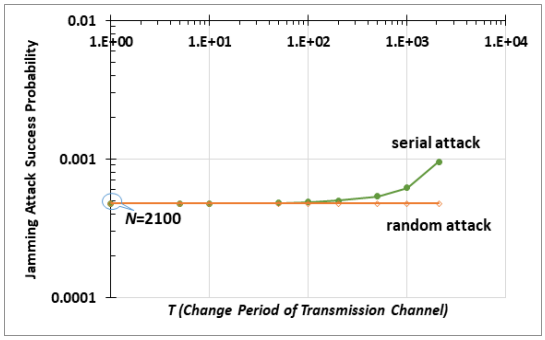


그림 5. 재밍 공격 성공 확률 비교
Fig. 5. Comparison of jamming attack success probabilities

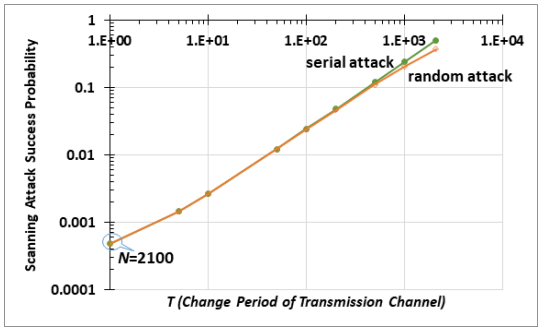


그림 6. 스캐닝 공격 성공 확률 비교
Fig. 6. Comparison of scanning attack success probabilities

## Ⅳ. 결 론

급격히 증가하고 있는 다양한 형태의 무선 단말들로 인해 무선 통신망이 지속적으로 확장되고 새로운 무선 통신 기술에 대한 연구가 활발히 이루어지고 있다. 그러나 무선 기술은 근본적으로 유선에 비해 보안에 취약하다는 단점을 갖는다. MTD-SDR(Moving Target Defense-Software Defined Radio) 시스템은 무선 통신 시스템과 통신망의 구성요소들을 동적으로 계속 변경하고 관리함으로써 악의적 공격자가 시스템을 공격할 수 있는 기회를 줄이고자 하는 목적을 가진 시스템이며, 미국의 “연방정부 사이버 보안 연구 및 개발 프로그램을 위한 전략 계획”에서도 MTD 시스템에 대해 언급하고 있을 정도로 중요한 이슈중의 하나이다.

본 논문에서는 다양한 사이버 무선 공격에 대해 자가 방어 및 복구 능력을 갖는 무선 통신 시스템을 구축하기 위한 연구의 일환으로 통신에 사용되는 변복조 기법, 전송 주파수, 전송 패킷 길이 등 다양한 시스템 운영 파라미터들로 특징 지워지는 통신 채널을 동적으로 변경시킬 때 공격자의 공격 패턴에 따른 공격 성공 확률식을 유도하고 시뮬레이션을 통해 결과를 검증하였다. 공격자의 악의적 공격은 랜덤 및 순서적, 스캐닝 및 재밍 공격에 의한 4가지 조합으로 분류하여 공격 성공 확률 식을 유도하였으며, C언어로 작성된 시뮬레이션 프로그램을 이용하여 결과의 타당성을 검증하였다. 결과적으로 랜덤 스캐닝 공격의 경우에는 전송채널 변화주기 T 값이 증가할수록 공격성공률이 증가하는 반면, 랜덤 재밍 공격의 경우에는 변화가 없다. 순서적 공격의 경우에는 랜덤 공격과 유사한 경향의 성공률 패턴을 보이지만 전송채널 변화주기 T가 커져서 전송채널 수 N에 접근할수록 재밍 공격의 경우에는 최대 2배, 스캐닝 공격의 경우에는 최대 36% 정도 랜덤 공격에 비해 공격 성공률이 높은 것으로 나타났다.

## References

[1] 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.

DOI: https://doi.org/10.7236/JIIBC.2016.16.6.15

[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.
DOI: http://dx.doi.org/10.7236/JIIBC.2016.16.5.27

[3] 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

[4] Yong-Hee Jeon, "A Study on the Security Modeling of Internet of Things(IoT)," Journal of Korean Institute of Information Technology, Vol.15, No.12, pp.17-27, Dec., 2017.
DOI: https://doi.org/10.14801/jkiit.2017.15.12.17

[5] Sushil Jajodia, Anup K. Ghosh, Vipin Swarup, Cliff Wang, X. Sean Wang, "Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats", Springer, ISBN:1461409764 9781461409762, 2011.

[6] Rui Zhuang, Scott A. DeLoach, Xinming Ou, "Towards a Theory of Moving Target Defense", Proceedings of the First ACM Workshop on Moving Target Defense, pp.31-40, Nov. 7, 2014.
DOI: https://doi.org/10.1145/2663474.2663479

[7] Jun Xu, Pinyao Guo, Mingyi Zhao, Robert F. Erbacher, Minghui Zhu, Peng Liu, "Comparing Different Moving Target Defense Techniques", Proceedings of the First ACM Workshop on Moving Target Defense, pp.97-107, Nov. 7, 2014.
DOI: https://doi.org/10.1145/2663474.2663486

[8] Executive Office of the President National Science and Technology Council, "TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM", https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf, pp.8-9, Dec., 2011.

[9] Firas Almoualem, Pratik Satam, Jang-Geun Ki, Salim Hariri, "SDR-Based Resilient Wireless Communications," International Conference on Cloud and Autonomic Computing (ICCAC), Sept., 2017.
DOI: https://doi.org/10.1109/ICCAC.2017.18

[10] Jang-Geun Ki, Kyu-Tae Lee, "Performance Analysis of SDR Communication System Based on MTD Technology," Journal of The Institute of Internet, Broadcasting and Communication (JIIBC), Vol.17, No.2, pp.51-56, Apr., 2017.
DOI: https://doi.org/10.7236/JIIBC.2017.17.2.51

[11] Jesus Pacheco, Cihan Tunc, and Salim Hariri, "Design and Evaluation of Resilient Infrastructures Systems for Smart Cities," IEEE International Smart Cities Conference (ISC2), Sept., 2016.

[12] Jose Raul Machado-Fernandez, "Software Defined Radio: Basic Principles and Applications," Revista Facultad de Ingenieria, Vol.24, No.38, pp.79-96, 2015.
DOI: https://doi.org/10.19053/01211129.3160

[13] 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.

## 저자 소개

**기 장 근(종신회원)**

- 1986년 2월 : 고려대학교 전자공학과 졸업
- 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>