논문 2016-2-5

공격 가능 요소들의 변경에 대한 랜덤 공격 성공율

기장근*

Random Attack Success Probability on the Moving Target Defense

Jang-Geun Ki*

요 약

최근 유선과 견줄 수 있는 전송속도를 지원하면서 손쉬운 망 구축 및 이에 따른 구축 비용 절감 등의 장점을 갖는 무선 통신망에 대한 연구가 활발히 진행되고 있으나, 이러한 무선 통신 기술은 근본적으로 악의적 사이버 공격에 취약하다는 단점을 갖는다.

본 논문에서는 자가 복원력이 있는 무선 통신망 구축을 위해 MTD 기술을 적용한 SDR 망 구성시 공격자의 공격 성공율을 분석하였다. 공격성공률은 수학적 방법과 시뮬레이션 방법을 이용하여 비교 분석하였으며 두 결과가 일치함을 보였다.

Abstract

These days, wireless communications provide several advantages such as easy deployment, less network construction cost, and comparable bandwidth to the wired network. But the wireless network is more vulnerable to the malicious cyber attacks.

In this paper, attack success probability in the SDR network to which the MTD technology is applied is analyzed in a mathematical way and compared with the simulation results.

한글키워드 : 공격 가능 요소 변경, 공격 성공률

keywords : attack element, success rate of attack

1. 서 론

최근 유선에 비해 망 구축이 간단하고, 비용이 적게 들며, 전송 대역폭이 유선에 비견될 만큼 증가하고 있는 무선 통신 기술에 대한 연구가 활발히 진행되고 있다. SDR(Software Defined Radio)[1]은 무선 통신 시스템에서 기존에 하드웨어로 구현되던 구성요소들을 개인용 컴퓨터나 임베디드 시스템의 소프트웨어로 구현하는 무선 통신 시스템을 말하며, 대부분의 신호처리가 특정 하드웨어가 아닌 범용 프로세서에 의해 처리됨으로써 아주 다양한 무선 프로토콜들을 쉽게 지원할 수 있는 장점을 갖는다.

그러나 이러한 무선 통신 기술은 무선의 특성상 기본적으로 스캐닝(scanning)이나 재밍

* 공주대학교 전기전자제어공학부
(email: kjg@kongju.ac.kr)
접수일자: 2016.11.27. 심사완료: 2016.12.15.
게재확정: 2016.12.22.

(jamming) 등과 같은 악의적 사이버 공격에 취약하다는 단점을 갖는다.

이러한 무선망의 단점을 극복하고, 사이버 공격의 위험으로 부터 통신 시스템을 방어하기 위해 시스템이 공격받을 수 있는 요소들을 지속적으로 변경하는 MTD(Moving Target Defense)[2-5] 기술에 대한 연구가 최근 활발히 진행되고 있다. MTD 기술을 이용하면 다양하고 끊임없이 변경되는 통신 요소들로 인해 사이버 공격자의 공격은 어렵고 복잡해지며 비용 또한 증가하게 된다. 따라서 시스템의 방어 취약성을 개선하고, 스스로의 복구능력을 키울 수 있게 된다.

본 논문에서는 자가 복구력을 갖는 무선망 구축을 위해 SDR 기술을 사용한 무선망에서 MTD 기술의 적용에 따른 사이버 공격 방어능력 개선 정도를 평가하였다.

2. MTD 기술 적용 무선 노드 구성

MTD(Moving Target Defense)[2-5] 기술은 시스템이 공격 받을 수 있는 요소들을 끊임없이 변경함으로써 사이버 공격을 최대한 막고자 하는 기술을 말한다.

SDR(Software Defined Radio)은 재구성이 가능한 무선 기술로, 무선신호를 수신하여 컴퓨터로 전달해 소프트웨어를 이용해 신호를 처리한다. 관련연구를 위해 가장 많이 사용되는 오픈소스 소프트웨어로는 GNU-Radio[6,7]가 있다.

본 연구에서는 MTD 기술을 적용한 SDR 망을 구성하기 위한 테스트 베드를 설계하였다. 송수신 노드들은 표 1의 예시와 같이 구성조합을 일정한 시간마다 변경해 가면서 데이터를 송수신하도록 프로그램 되었다. 이와 같이 송신 채널을 수시로 변경하게 되면 공격자의 공격 성공률은 감소하게 되는데, 본 논문의 3장에서 공격 성공률 계산 공식을 유도하고, 4장에서는 유도된 공식에 대한 시뮬레이션 검증에 관해 기술하였다.

표 1. 송신채널 구성표 예
Table 1. Tx channel specification

channel number	Frequency [MHz]	Modulation	Packet Length
1	80	GFSK	256
2	110	GMSK	1024
3	100	GFSK	512
4	130	GMSK	256
.....	.....	.....	.....

3. 공격 성공 확률 평가

공격 성공 확률을 계산하기 위해 시스템의 동작원리를 그림 1에 나타내었다.

통신에 사용할 수 있는 전체 채널의 개수는 N 라고 하고, $T_{changeCH}$ 시간마다 채널을 바꾸어 가면서 통신을 시도한다고 가정한다. 통신에 사용할 채널의 순서는 전체 사용가능 채널들 중에서 랜덤한 순서로 선택해 사용할 채널리스트를 만들어 놓고 이 리스트 순서에 따라 $T_{changeCH}$ 시간마다 다음 채널을 사용한다.

공격자는 매 단위시간마다 공격할 채널을 랜덤하게 선택하며, 선택된 채널과 통신자가 사용하는 채널번호가 같으면 공격 성공으로 간주한다. 공격자는 매 단위시간마다 공격 채널을 랜덤하게 선택하고, 송신자는 매 $T_{changeCH}$ 시간마다 채널을 바꾸게 됨으로, 통신자의 채널이 특정채널로 정해지면 공격자는 그동안 $T_{changeCH}$ 회수만큼 공격시도를 할 수 있다. 또한 송신자가 채널을 다음채널로 바꿀 때마다 공격자의 입장에서는 새로이 공격을 시작하는 것과 마찬가지가 됨

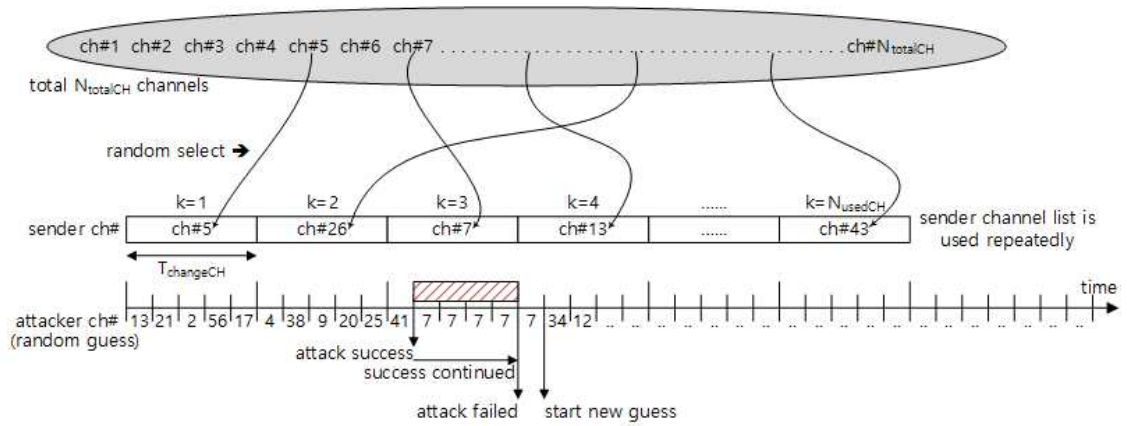

그림 1. 통신 시스템과 공격자의 동작 원리
Fig. 1. Communication system and attacker operation

으로 $T_{changeCH}$ 시간동안의 공격 성공률을 계산하면 이 시스템의 공격성공률을 알 수 있게 된다.

$T_{changeCH}$ 시간 구간내의 각 단위시간에서의 공격 성공률과 공격이 성공했을 때 지속되는 공격 성공 지속시간은 표 2와 같이 계산할 수 있다.

따라서 공격성공 확률은 아래 식과 같게 된다.

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

위의 공격 성공 확율 계산식은 공격자가 전체 N 개의 채널 중에서 공격 채널을 랜덤하게 선택하는 경우에 해당하며, 랜덤 선택 채널은 중복될 가능성이 있음에 유의해야 한다. 즉 N 번의 연속적인 공격 시도에서 매번 랜덤하게 공격 채널 번호를 이전 시도와 상관없이 독립적으로 선택함으로 중복 되는 채널 번호를 공격할 가능성이 존재하고 따라서 공격에서 누락되는 채널 번호도 있을 수 있다. 그러나 오랜 시간동안의 확률로 보면 N 번의 연속적인 공격 시도에서 모든 채널이 평균 1번씩은 공격을 받게 된다.

표 2. $T_{changeCH}$ 시간 구간내 각 단위시간에서의 공격 성공률과 공격성공지속시간
Table 2. Consistence time of attack hit

단 위 시간	공격성공률	공격성공 지속시간
1	$\frac{1}{N}$	$T_{changeCH}$
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	$\left(\frac{N-1}{N}\right)^{i-1}\left(\frac{1}{N}\right)$	$T_{changeCH}-i+1$
	. . . . .	. . . . .
T	$\left(\frac{N-1}{N}\right)^{T-1}\left(\frac{1}{N}\right)$	1

4. 검증 및 성능분석

앞에서 제시한 공격성공 확률식을 검증하기 위해 C언어로 시뮬레이션 프로그램을 작성하여 실험하였다. 시뮬레이션 프로그램에서 송신자는 $T_{changeCH}$ 시간마다 송신 채널을 랜덤하게 변경하며, 공격자는 매 단위시간마다 랜덤하게 채널을 선택하고 이 채널이 송신자의 채널과 같으면 공격이 성공한 것으로 간주하고 다음 단위시간에도 이 채널을 계속 유지하며, 송신자의 채널 변경으로 인해 공격채널이 더 이상 송신채널과 같지 않게 되면 다시 랜덤하게 공격 채널을 선택하는 과정을 반복한다.

표 3에 시뮬레이션 및 수학적 공식에 의한 계산 결과를 비교하여 나타내었다. 표에서 확인할 수 있듯이 앞장에서 유도된 공식을 이용해 정확하게 공격 성공확률을 계산할 수 있음을 볼 수 있다. 그림 2는 시뮬레이션 결과 값을 그래프로 나타낸 것이며, 계산값을 그래프에 나타내어도 같은 결과를 얻을 수 있고, 시뮬레이션 값과 계산 값의 오차가 거의 없어 그래프에는 시뮬레이션 결과 값만을 나타내었다.

그래프에서 확인할 수 있듯이 송신자가 하나의 채널을 사용하고 있는 동안에 공격자가 몇번 공격을 시도할 수 있는지를 나타내는 $T_{changeCH}$ 값이 클수록 공격성공률은 증가하되, 값이 커질수록 증가율은 둔화된다. 또한 전체 사용가능 채널 수(N)가 많을수록 공격성공률은 감소한다.

5. 결 론

최근 망구축의 용이성 및 단말의 자유로운 이동성을 보장하면서도 유선과 견줄 수 있는 데이터 전송 대역폭을 제공하는 무선 통신에 대한 수요가 급증하고 있다. 이와 같은 무선통신은 무선의 특성상 도청이나 재밍(jamming) 등의 악의적 사이버 공격에 취약하다는 단점을 갖는다.

본 논문에서는 자가 복원력이 있는 무선 통신망 구축을 위해 MTD 기술을 적용한 SDR 망 구성시 공격자의 공격 성공율을 분석하였다. MTD 기술은 시스템이 공격자로 부터 받을 수 있는 공격 요소를 수시로 변경함으로써 시스템을 보호하는 방법을 의미한다. 성능분석을 위해 본 논문에서 제안된 공격성공률 수식은 수학적 방법과 시뮬레이션 방법을 이용하여 비교 분석하였으며 두 결과가 일치함을 보였다.

표 3. 공격성공확률 비교 (시뮬레이션값 / 계산값)

Table 3. Comparison of hit probability

N \ $T_{changeCH}$	1	5	10	50
210	0.0047368095	0.0140765095	0.0255977714	0.1115325476
	0.0047619047	0.0141953346	0.0258198662	0.1125005079
2100	0.0004758295	0.0014270385	0.0026133995	0.0120317400
	0.0004761904	0.0014276647	0.0026153096	0.0120489499
21000	0.0000476130	0.0001428188	0.0002619364	0.0012132107
	0.0000476190	0.0001428480	0.0002618673	0.0012133418
210000	0.0000047634	0.0000142864	0.0000261817	0.0001214153
	0.0000047619	0.0000142856	0.0000261901	0.0001214191

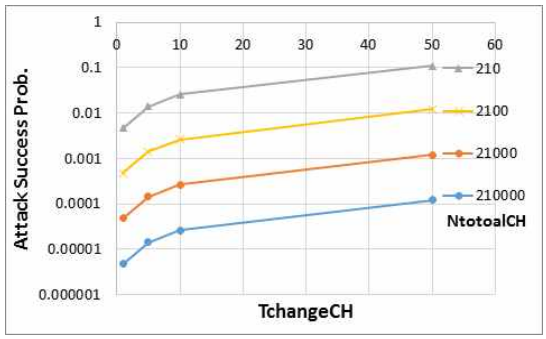

그림 2. 공격 성공 확률

Fig. 2. Attack hit rates

참 고 문 헌

[1] Friedrich K. Jondral, “Software-Defined Radio.Basics and Evolution to Cognitive Radio”, EURASIP Journal on Wireless Communications and Networking, pp.275-283, 2005.

[2] Sushil Jajodia, Anup K. Ghosh, Vipin Swarup, Cliff Wang, X. Sean Wang, “Moving Target Defense”, Springer ISSN 1568-2633, 2011.

[3] Valentina Casola, Alessandra De Benedictis, “A Moving Target Defense Approach for Protecting Resource-Constrained Distributed Devices”, IEEE IRI 2013, San Francisco, California, USA, Aug.14-16, 2013.

[4] Jafar Haadi Jafarian, Ehab Al-Shaer, Qi Duan, “Openflow random host mutation: transparent moving target defense using software defined networking”, ACM SIGCOMM 2012 Conference, pp.127-132, Aug.13-17, 2012.

[5] Rui Zhuang, Scott A. DeLoach, Xinming Ou, “Towards a Theory of Moving Target Defense“, MTD2014 Proceedings of the First ACM Workshop on Moving Target Defense, pp.31-40, Nov.7, 2014.

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

[7] Feng Ge, C. Jason Chiang, Yitzchak M. Gottlieb, Ritu Chadha, “GNU Radio-Based Digital Communications: Computational Analysis of a GMSK Transceiver”, Global Telecommunications Conference (GLOBECOM), 2011.

저 자 소 개

기장근(Jang-Geun Ki)

1986.2 고려대학교 전자공학과 졸업
1988.2 고려대학교 전자공학과 석사
1992.2 고려대학교 전자공학과 박사
2002.6-2003.6 Univ. of Arizona 방문교수
2010.6-2011.8 Univ. of Arizona 방문교수
2016.8-2017.8 Univ. of Arizona 방문교수
1992.3-현재 : 공주대학교 공과대학 전기전자제어공학부 교수
<주관심분야 : 통신프로토콜, 이동통신시스템>