

논문 2015-52-12-7

모바일 단말을 이용한 RCIED에 대한 repeater 방식의 반응 재밍 기법 성능 분석

(Performance Analysis on The Reactive Repeater Jamming Techniques
Against an RCIED Using Mobile Devices)

김요한*, 김동규*, 김형남**

(Yo-Han Kim, Dong-Gyu Kim, and Hyoung-Nam Kim[©])

요약

최근 무선통신 장비를 이용하여 원격으로 폭발시킬 수 있는 무선 급조폭발물 (RCIED)에 의한 테러의 위협이 전 세계적으로 증가하고 있다. 이에 대응하기 위해 급조폭발물을 기폭 시키는 무선 트리거 신호를 정상적으로 수신하지 못하게 하는 재밍 기법이 사용되고 있다. 기존의 재밍 기법으로는 전 대역에 항상 재밍 신호를 방출하는 상시 광대역 재밍(active barrage jamming) 기법이 주로 사용되고 있으나, 전력 소모가 매우 커서 주요 운송 수단인 차량 탑재용으로 사용하기에는 운용시간이 너무 짧다는 단점이 있다. 이러한 기존 기법의 단점을 극복하기 위하여 최근에 반응 재밍(reactive jamming) 기법이 관심을 받고 있다. 반응 재밍은 폭발 트리거 신호를 감지하여 신호가 존재하는 대역을 선별적으로 대응하는 재밍 기법으로서, 기존 재밍 기법에 비해 전력 효율이 높기 때문에 차량 탑재용으로도 운용 시간을 대폭 늘릴 수 있다. 하지만, 반응 재밍은 폭발 트리거 신호를 포착한 뒤 재밍 신호를 방사하기 때문에, 폭발 트리거 신호 환경에 대한 정보를 바탕으로 반응 재밍이 이루어져야 하는 반응시간에 대한 기준이 필요하다. 이를 위해서 본 논문에서는 반응 재밍을 활용할 수 있는 이동통신 환경에 대해서 필요한 반응시간을 이동통신 시스템에서의 호 처리시간(call processing time) 정보를 바탕으로 도출하고, 반응 재밍에서 사용될 수 있는 repeater 재밍에 대해 시뮬레이션을 통해 성능 분석을 수행한다.

Abstract

Recently, terroristic threats using a radio controlled improvised explosive device (RCIED) that is remotely controlled and exploded have been increased around the world. In order to prevent the explosion of an RCIED, jamming techniques that interrupt an RCIED receiver can be used, so that the receiver can not demodulate the trigger code. Conventional jamming technique is a type of active barrage jamming that always emits the noise jamming signal for all the frequency band. However, it needs large power consumption and thus is limited in operation time for a vehicle. In order to overcome the shortage of the active barrage jamming, reactive jamming technique has drawn attention. In reactive jamming, all the frequency band is firstly scanned, and then if any trigger signal exists, one emits the jamming signal to the corresponding frequency band. Therefore, the reactive jamming is superior to the active barrage jamming in terms of power efficiency. However, a reactive jammer emits a jamming signal only after the trigger signal is intercepted, which means that the jamming signal may be late for interrupting an RCIED receiver. In this sense, it is needed to evaluate a delay in an RCIED receiver. To achieve this, we analyze the reaction time and present the simulation result for jamming performance of reactive jamming against an RCIED using mobile devices.

Keywords : RCIED, jamming, reactive jamming, repeater jamming

* 학생회원, ** 평생회원, 부산대학교 전자공학과

(Department of Electronics Engineering, Pusan National University)

© Corresponding Author(E-mail: hnkim@pusan.ac.kr)

※ 이 논문은 부산대학교 기본연구지원사업(2년)에 의하여 연구되었음.

※ 본 논문은 BK21플러스, IT기반 융합산업 창의인력양성사업단에 의하여 지원되었음.

Received ; September 11, 2015 Revised ; November 11, 2015 Accepted ; November 23, 2015

I. 서 론

최근 전 세계적으로 급조폭발물(IED, improvised explosive device)을 활용한 국제 이익단체들의 테러 위협이 증가하고 있다. 특히, 통신기술의 급격한 발달과 원격 무선기기의 보급으로 인해 원격(remote) 조종으로 IED를 기폭하여 치명적인 인명 피해를 야기할 수 있는 무선 급조폭발물(RCIED, radio controlled improvised explosive device)의 위협이 크게 증가되고 있다. 또한 테러 위협은 전시뿐 아니라 급변하는 국제정세 속에서 전 세계적으로 확산되고 있으며 그 공격대상 역시 군사 전력뿐만 아니라 국가 중요인사 및 불특정 민간으로 확대되고 있는 실정이다. 특히, 다양한 무선장치들이 손쉽게 확보될 수 있다는 점에서 RCIED는 더욱 치명적인 위협이 되고 있다^{[1][2]}. 따라서, 최근 이러한 RCIED에 의한 테러 위협에 대응하기 위한 RCIED 대응장치에 대한 중요성이 미국과 유럽을 중심으로 널리 확산되고 있으며, 최근에는 다양한 차량용 RCIED 대응장치가 개발되고 있다^[3]. 이러한 RCIED 대응 장치는 IED를 기폭시키는 무선 트리거 신호가 정상적으로 수신되지 않도록 방해전파를 방사하는 재밍 기법을 이용하여 폭발물의 동작을 무력화시킨다. 이러한 RCIED 재밍의 기존 기술로는 그림 1의 예와 같이 임의의 시간에 불특정 주파수 대역으로 수신되는 위협 트리거 신호에 대비하여 광대역 재밍 신호를 상시 송출하는 상시 광대역 재밍(active barrage jamming)이 사용되고 있다. 하지만 상시 광대역 재밍 기법은 폭발 트리거가 없을 때도 항상 재밍 신호를 전 대역에 송출하기 때문에, 전력의 소비가 너무 크고 효율성이 낮아 차량 탑재용으로 사용할

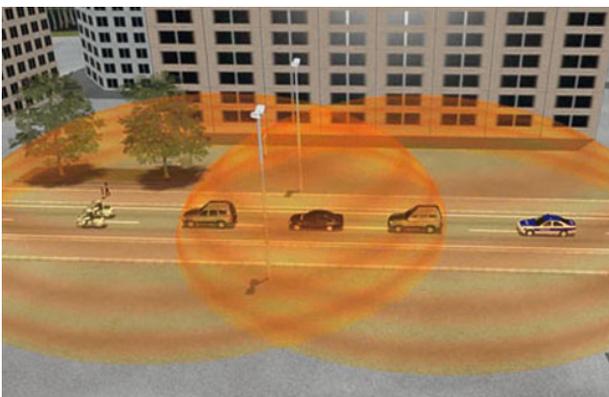


그림 1. 경호 차량용 RCIED 재머 장비 운용 예.
Fig. 1. An example of RCIED jammer on vehicle.

때 운용 시간의 제약이 크다는 문제점이 있다.

이에 반해 최근 연구되고 있는 반응 재밍(reactive jamming)은 상시 광대역 재밍과 달리, 전 대역을 스캔하면서 특정 대역에서 무선 트리거 신호가 감지되면 즉시 해당 주파수 대역에 재밍 신호를 송출하여 RCIED를 무력화시키는 방식이다^[4]. 반응 재밍은 트리거 신호를 감지한 후 재밍 신호를 송출하기 때문에 RCIED 수신기가 트리거 신호를 수신하는 과정에서 지연 시간이 존재할 때 활용 가능한 기법이다. 그 지연 시간 내에 재밍 신호를 송출하면, RCIED는 폭발하지 않는다. 따라서 반응 재밍은 무선 트리거 신호에 대한 수신 지연시간에 대한 정보가 필수적으로 요구된다. 트리거 신호의 수신 지연시간을 통해서, 신호를 감지하고 재밍 신호를 송출하는 과정의 반응 재밍이 이루어지는 데 필요한 반응시간 기준을 세울 수 있다.

반응 재밍은 재밍 신호를 생성하는 방법에 따라 두 가지로 분류할 수 있다. 재밍 신호를 생성하는 가장 기본적인 방법은 의사잡음(pseudo noise)을 사용하는 것이다. 의사잡음을 생성하여 트리거 신호가 감지된 주파수 대역에 송출하게 되면 RCIED 수신기는 트리거 신호와 잡음신호가 더해진 신호를 수신하게 되고, 이로 인해 SNR (signal-to-noise ratio)이 낮아져서 정상적으로 복조가 이루어지지 않게 된다. 재밍 신호를 구성하는 또 다른 방법은, 재머에서 스캔을 통해 감지한 폭발 트리거 신호를 활용하는 repeater 방식의 재밍 방법이 있다^[4-5]. Repeater 재밍은 수신된 트리거 신호를 주파수 왜곡을 통해서 재송출하여, RCIED 수신기에서 원 트리거 신호와 왜곡된 트리거 신호가 더해져서 간섭, 교란 효과가 나타나게 하여 트리거 신호의 복조를 방해한다. Repeater 방식의 재밍은 신호원의 변조방식, 대역 폭 등 신호원의 특성과 주파수 왜곡의 정도에 따라 재밍 성능이 영향을 받기 때문에, repeater 방식의 반응 재밍에서는 주파수 왜곡에 따른 성능에 대한 분석이 필요하다.

반응 재밍 기법에서 필요한 요구조건인 반응시간은 재밍 대상이 되는 통신 시스템마다 차이가 있고, 주파수 왜곡에 따른 재밍 성능은 통신 방식에 따라서 그 성능이 달라진다. 그래서 반응 재밍 기법 연구는 다양한 시스템 상황 하에서 연구되고 있다^[6]. 본 논문에서는 다양한 무선기기 중에서 손쉽게 구할 수 있고, 응용이 간단한 모바일 단말을 이용한 RCIED에 대응하는 반응

재밍 기법에 대해서 연구를 진행하였다. 반응 재밍이 이루어져야 하는 반응시간 기준을 모바일 단말이 사용하는 이동통신 시스템의 호 처리 과정(call processing)에서의 수신 지연시간 분석을 통해서 제시하고, 3G(WCDMA), 4G(LTE) 두 가지 이동통신 시스템에 대해서 재밍 신호에 따른 두 가지 재밍 기법인 잡음을 이용한 재밍과 repeater 방식 재밍의 성능을 비교한다. Repeater 방식의 재밍에서는 주파수 왜곡을 변화시켜 가면서 repeater 방식의 재밍에서의 성능 변화를 분석한다.

II장에서는 RCIED에 대한 소개와 각 재밍 기법에 대한 설명과, 모바일 단말을 이용한 RCIED에서 반응 재밍을 활용하기 위한 반응시간 기준에 대해서 이동통신 시스템의 호 처리 절차에 대해 살펴보고, III장에서 시뮬레이션을 통해 잡음을 이용한 재밍과 repeater 방식 재밍의 성능을 분석하고, IV장에서 본 논문의 결론을 맺는다.

II. 본 론

1. RCIED

RCIED(radio controlled improvised explosive device : 무선 급조폭발물)는 IED(improvised explosive device: 급조폭발물)에 무선 통신장치를 이용하여 원격으로 폭발시킬 수 있는 장치를 말한다. 기존의 IED만을 이용한 테러가 IED를 기폭시키는 방법에서 제한적이었던 반면에, 원격 조종을 통해서 IED를 기폭시킬 수 있는 RCIED에 의한 테러의 위협이 증대되었다^[1]. 그림 2의 모바일 단말을 이용한 RCIED 예와 같이 RCIED는 IED와 이를 동작시키는 무선 신호 수신장치(모바일 단

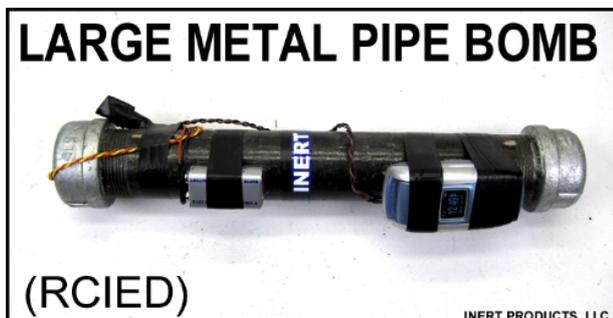


그림 2. 모바일 단말을 이용한 RCIED 사용 예.
Fig. 2. An example of RCIED using mobile device.

말기)로 구성된다. 모바일 단말을 이용한 RCIED에서는 모바일 단말로 전화를 거는 신호를 폭발 트리거 신호가 되게 RCIED를 구성한다. 모바일 단말에 정상적으로 전화가 걸리게 되면, 기폭장치를 동작하여 IED가 폭발하게 된다. RCIED의 폭발을 방지하기 위해서는 모바일 단말에 수신된 신호가 정상적으로 복조되어 전화가 연결되지 않도록 고출력 재밍 신호를 방출하여 폭발 트리거 신호를 교란하여야 한다. 재밍 신호를 송출하면 모바일 단말에서 폭발 트리거 신호와 재밍 신호가 더해져서 수신하게 된다. 그 결과 재밍 신호가 폭발 트리거 신호에 비해 충분히 크다면 신호 대 잡음비를 급격하게 낮추는 효과가 발생하여 폭발 트리거 신호를 정상적으로 복조하지 못하게 되고, 폭발은 일어나지 않게 된다.

2. 재밍(Jamming) 기법

재밍이란 적의 통신을 방해, 혼란시키는 기법을 의미한다. 일반적으로 재밍하고자 하는 대상 주파수 영역에 방해전파를 방사함으로써 특정 주파수나 전파의 사용을 방해하는 교란 형태 또는 허위 정보를 얻도록 하는 기만 형태로 행해진다. 그림 1에서 보듯이, RCIED 재머에서 재밍 신호를 송출하면 반구 형태의 전파 차단 보호막 효과를 얻을 수 있으며, 재밍 신호의 세기를 높일수록 재밍에 의한 보호 범위가 넓어지게 된다. RCIED를 기폭시키려는 폭발 트리거 신호가 존재하더라도 범위내의 모든 전파를 무력화하여 RCIED 수신기 내에서 정상적인 수신이 되지 않아 RCIED의 폭발을 방지할 수 있다.

재밍 기법은 재밍 신호를 송출하는 방식과, 재밍 신호를 구성하는 방식에 따라서 나눌 수 있다. 재밍 신호를 송출하는 방식에 따른 분류로는 항상 재밍 신호를 방출하는 상시 재밍과 평상시에는 폭발 트리거 신호를 스캔하고 있다가 폭발 트리거 신호가 감지되면 재밍 신호를 방출하는 반응 재밍 두 가지로 나눌 수 있다. 또한 재밍 신호를 구성하는 방식에 따른 분류로는 교란의 대상이 되는 신호, 폭발 트리거 신호를 활용하는 여부에 따라서 일반적인 잡음 재밍과 repeater 방식 재밍 두 가지로 나눌 수 있다.

상시 재밍이란 그림 3과 같이 폭발 트리거 신호의 유무와 상관없이 항상 재밍 신호를 송출하는 방식이다. 매 순간 고려하는 모든 주파수 대역에 고출력의 잡음 신호를 송출하므로 전 주파수 대역에 모든 수신기를 동

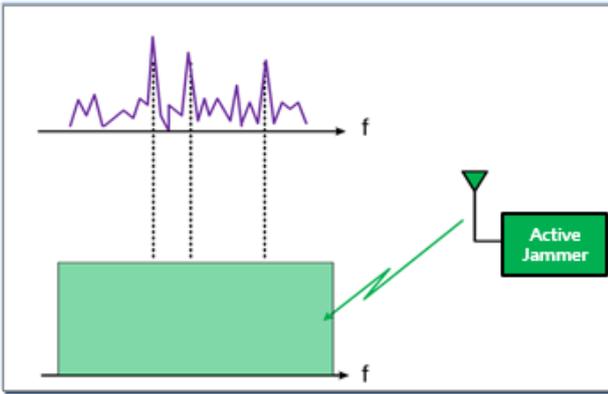


그림 3. 광대역 상시 재밍.
Fig. 3. Active barrage jamming.

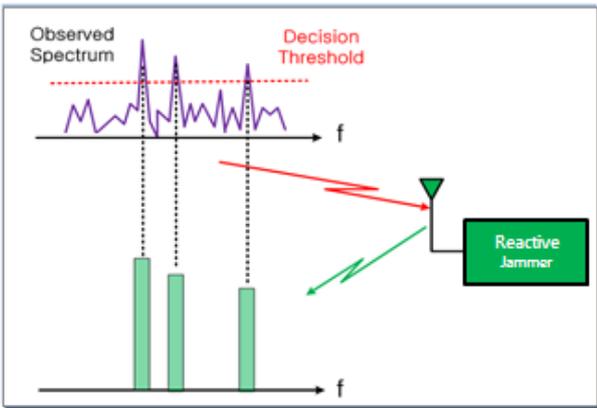


그림 4. 잡음 반응 재밍.
Fig. 4. Noise reactive jamming.

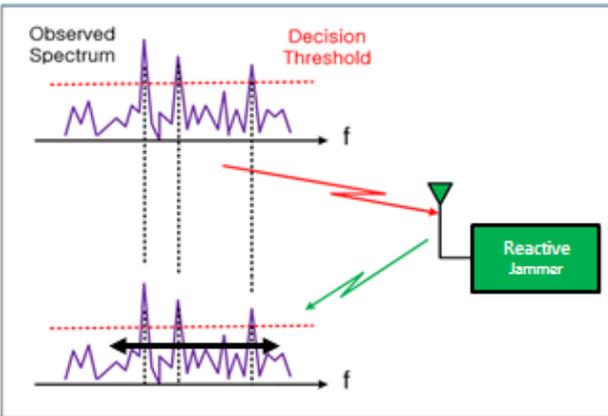


그림 5. Repeater 반응 재밍.
Fig. 5. Repeater reactive jamming.

시에 전파방해 할 수 있지만, 전력 소모가 매우 크다. 일반적으로 상시 재밍은 위협이 되는 신호를 스캔하지 않기 때문에, 잡음을 이용한 재밍이 많이 사용되고 있다. 이에 반해, 반응 재밍은 그림 4와 같이 평상시에는

신호를 스캔하고, 일정 수준 이상의 신호가 감지되면, 재밍 신호를 송출하는 방식이다. 반응 재밍은 신호가 존재하는 주파수 대역에만 재밍 신호를 방사하는 것이 가능하기 때문에, 시간 및 주파수 측면 모두에서 상시 재밍에 비해 전력 효율을 크게 높일 수 있다.

반응 재밍은 재밍 신호를 생성할 때, 수신 신호의 활용여부에 따라 크게 두 가지로 나눌 수 있는데, 신호가 감지되었을 때 해당 주파수 대역에 잡음 신호를 방사하는 일반적인 반응 재밍과, 수신 신호 자체를 왜곡하여 방사하는 repeater 방식의 재밍이 있다^[2]. 그림 5와 같이 repeater 방식의 재밍은 수신신호를 활용하여 수신신호에 주파수에 왜곡을 주고 재전송하여 RCIED 수신단에서는 원래 수신신호와 주파수 왜곡이 들어간 재밍 신호가 더해져서 신호를 오인하게 된다.

Repeater 방식 재밍은 수신신호를 활용한다는 측면에서 잡음을 이용한 재밍에 비해 효과적일 수 있다. 여러 개의 폭발 트리거 신호가 동시에 들어올 때, 혹은 한 개의 폭발 트리거 신호가 대역변조 등을 통해서 여러 주파수 대역으로 동시에 수신되는 경우에 한 번에 대응이 가능하다는 장점이 있다.

Repeater 방식의 재밍 기법에서 재밍 신호로 수신신호의 주파수를 왜곡해서 재전송할 때, 재밍 파라미터인 주파수를 얼마만큼 왜곡할 것인가에 관한 주파수 왜곡 구간과, 그리고 RCIED 수신기에서에서 왜곡된 주파수를 채널 추정, 채널 보상 과정 등을 통해서 복구하지 못하도록 주파수 왜곡 값을 업데이트 하는 빈도인 왜곡 주기, 두 가지를 고려할 필요가 있다. 본 논문에서는 repeater 재밍에서 필요한 왜곡 주파수 구간과, 왜곡 주기, 두 가지 재밍 파라미터의 변화에 따른 재밍 성능을 분석하고, 이를 가우시안 잡음을 이용한 잡음 반응 재밍과 비교 분석한다.

3. 호 처리 과정 (Call Procedure)

반응 재밍이 전력효율 측면에서는 상시 재밍에 비해 우수하지만, 상시 재밍이 항상 전 대역에 잡음 신호를 송출함으로써 재밍 성능이 보장 되는 반면에, 반응 재밍은 재밍의 반응시간과, repeater 방식의 성능에 대한 분석이 필요하다. 반응 재밍은 RCIED 수신단과 재밍에 폭발 트리거 신호가 동시에 들어왔다고 가정했을 때, RCIED 수신단에서 폭발 명령코드가 정상적으로 복조되기 전까지 재밍은 폭발 트리거 신호 감지와 재밍 신

호를 송출해야 한다. 이 때 RCIED 수신단에서 수신신호가 처리되는 수신 지연시간 내에 재머가 반응을 해야 하므로 폭발 트리거 신호에 대한 분석이 필요하다. 모바일 단말을 이용한 RCIED의 경우에는, 호 처리 과정을 통해서 수신 지연시간을 산출한다. 모바일 단말기로 트리거 되는 RCIED는 센서를 부착하고, 해당 단말기에 전화를 걸어서 전화가 울리면 센서가 작동하고 이 신호를 통해 폭발물이 폭발한다. 이러한 RCIED를 반응 재밍 기법으로 재밍하기 위해서는 원거리에서 RCIED 착신 단말에 전화를 걸었을 때, RCIED 착신 단말에 전화가 울리기까지의 시간 내에 재밍 신호를 방사해서 착신 단말에 전화가 정상적으로 수신되는 것을 막아야 한다. 그러기 위해서는 이동통신 시스템 상에서 발신 단말에서 전화를 걸어서 착신 단말에 전화가 연결되기까지의 시간보다 빠르게 재머가 반응해야 한다. 그림 6과 같이 통신망에서 양 끝 단의 단말기 간의 통화가 이루어지기까지의 일련의 과정을 호 처리 절차(call procedure) 라고 하고, 호 처리 절차에 소요되는 시간을 호 처리 시간(call setup time) 이라고 한다^[7~8]. 재머는 RCIED 착신 단말에 신호가 도착하는 16번 과정 이후에서야 트리거

신호를 감지하고 반응 재밍을 시작할 수 있다. 그러므로 전체 호 처리 시간보다 짧은 시간 내에 반응 재밍 과정이 이루어져야 한다. 착신 단말에 신호가 처음 도달해서, 전화벨이 울리기까지의 수신 지연시간 이내에 반응 재밍이 이루어져야 한다. 그런데 이 수신 지연시간은 각각의 국가별, 지역별, 여러 변수에 따라서 많은 차이를 보이기 때문에, 통계적인 관점에서 수신 지연시간을 구할 수밖에 없다. 그림 7은 3G/4G 환경에서 호 처리 시간을 통계 조사한 데이터의 분석 결과이다^[9]. MO(Mobile Originated - 발신측 호 처리 시간), MT (Mobile Terminated - 착신측 호 처리 시간) delay가 각각 3G (UMTS) 에서 3.4초, 1.8초, 4G(LTE)에서 4.7초, 2.84초인 것을 알 수 있다. 그림 6의 16번 과정 이후의 지연시간은 MT delay와 관련이 있으므로, 3G에서 1.8초, 4G에서 2.84초의 평균 지연이 있음을 알 수 있다.

III. 시뮬레이션

1. 시뮬레이션 환경

시뮬레이션은 Matlab Simulink 환경에서 진행하였다. 공통적으로 채널은 AWGN을 고려하였고, 채널 잡음에 의한 bit 에러의 영향을 최소화하여 재밍 신호에 의한 bit 에러를 비교하였다. 각 시스템에서 재밍 신호가 없을 때, BER은 10^{-4} 이하로 설정하였다. 변조방식은 QPSK를 사용하였고, 각각의 시스템 환경에 맞게 3G의 경우 채널 대역폭은 5 MHz로, 4G의 경우 20 MHz를 사용하였다. 시뮬레이션은 JSR (jamming to signal ratio)를 기준으로 가우시안 잡음 신호를 이용한 재밍과 repeater 방식 재밍의 성능을 비교 분석하였다.

Repeater 재밍에서 수신신호에 대한 왜곡 파라미터는 왜곡 주파수 구간과, 주기 두 가지로 구성되어 있다. 왜곡 주파수 파라미터에 따라 주파수 왜곡치를 최소 주파수에서 최대 주파수 사이의 값을 랜덤하게 발생시켜서 결정된 값으로 주파수 왜곡을 주었고, 왜곡 주기 파라미터에 따라 그 주기마다 랜덤 값을 생성하여서 왜곡 주파수를 업데이트하면서, 시뮬레이션을 진행하였다.

2. 시뮬레이션 결과

그림 8, 9는 3G(WCDMA) 시스템에서의 재밍 성능을 왜곡 주파수 구간과, 왜곡 주기에 따라서 나타낸 것이다. 왜곡 주파수 구간에 따른 시뮬레이션 결과인 그림 8

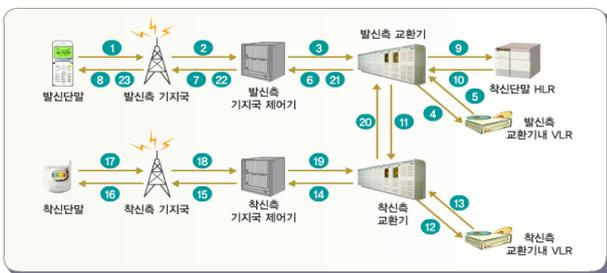


그림 6. 이동통신의 호 처리 절차도
Fig. 6. Call procedure of mobile communications.

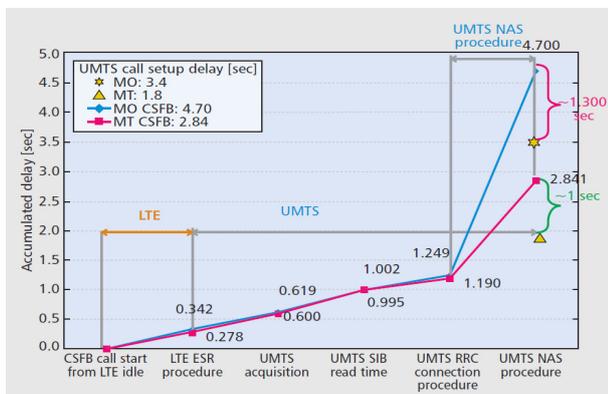


그림 7. 평균 호 처리 시간
Fig. 7. Average of call setup time.

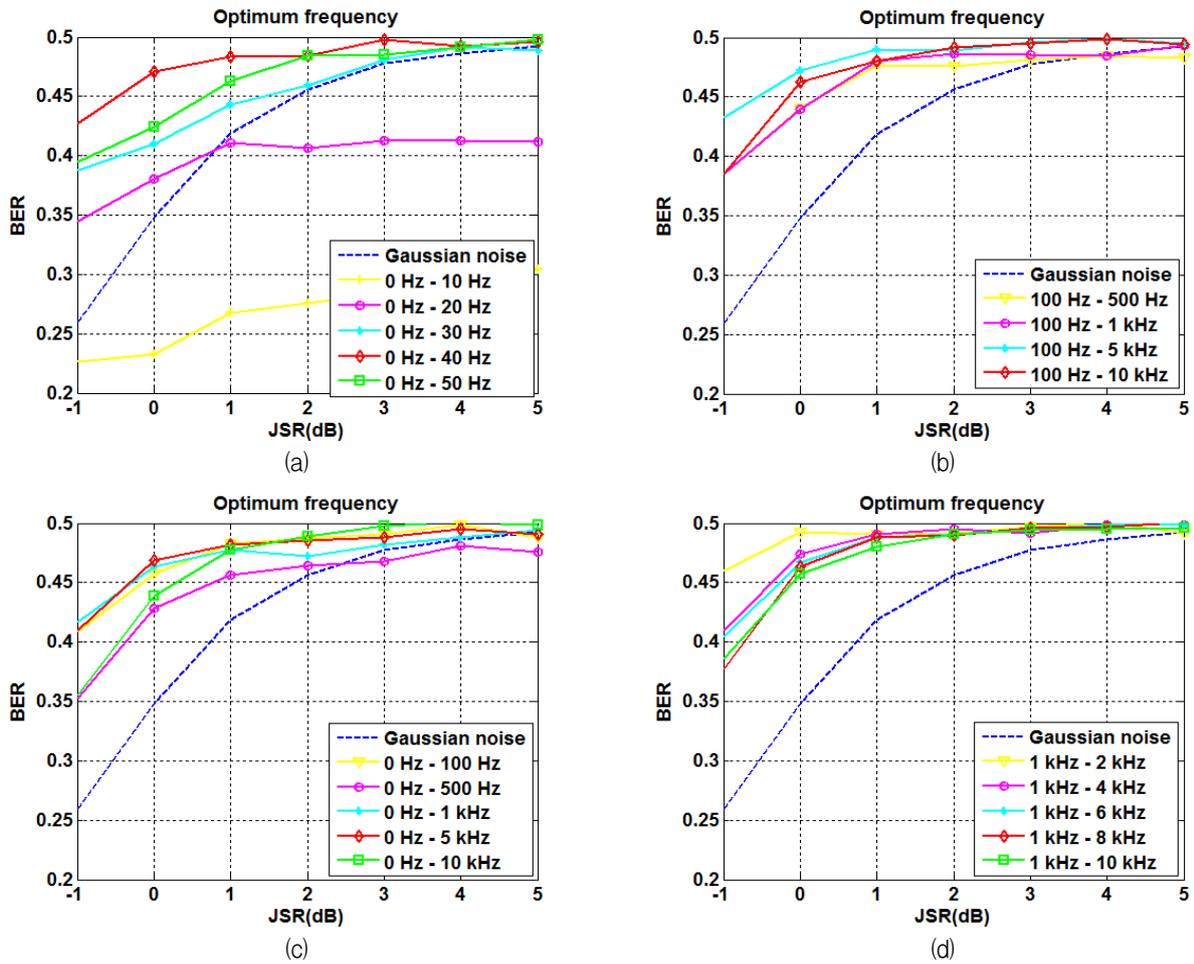


그림 8. 3G(WCDMA) 환경에서 왜곡 주파수 구간에 따른 재밍 성능.
 (a) 최소: 0Hz, 최대 10Hz-50Hz (b) 최소: 100Hz, 최대: 500Hz-10kHz
 (c) 최소: 0Hz, 최대: 100Hz-10kHz (d) 최소: 1kHz, 최대: 2kHz-10kHz

Fig. 8. Jamming performance according to disturbing frequency band in 3G(WCDMA) system.
 (a) min: 0Hz, max: 10Hz-50Hz (b) min: 100Hz, max: 500Hz-10kHz
 (c) min: 0Hz, max: 100Hz-10kHz (d) min: 1kHz, max: 2kHz-10kHz

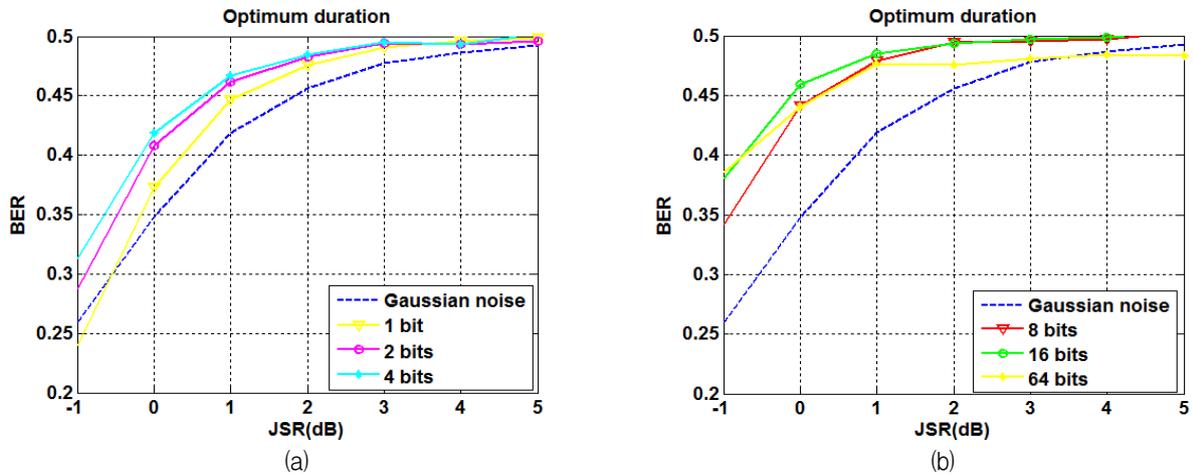


그림 9. 3G(WCDMA) 환경에서 왜곡 주기에 따른 재밍 성능. (a) 1 bit, 2 bits, 4 bits, (b) 8, 16, 64 bits

Fig. 9. Jamming performance according to disturbing duration in 3G(WCDMA) system.
 (a) 1 bit, 2 bits, 4 bits, (b) 8, 16, 64 bits

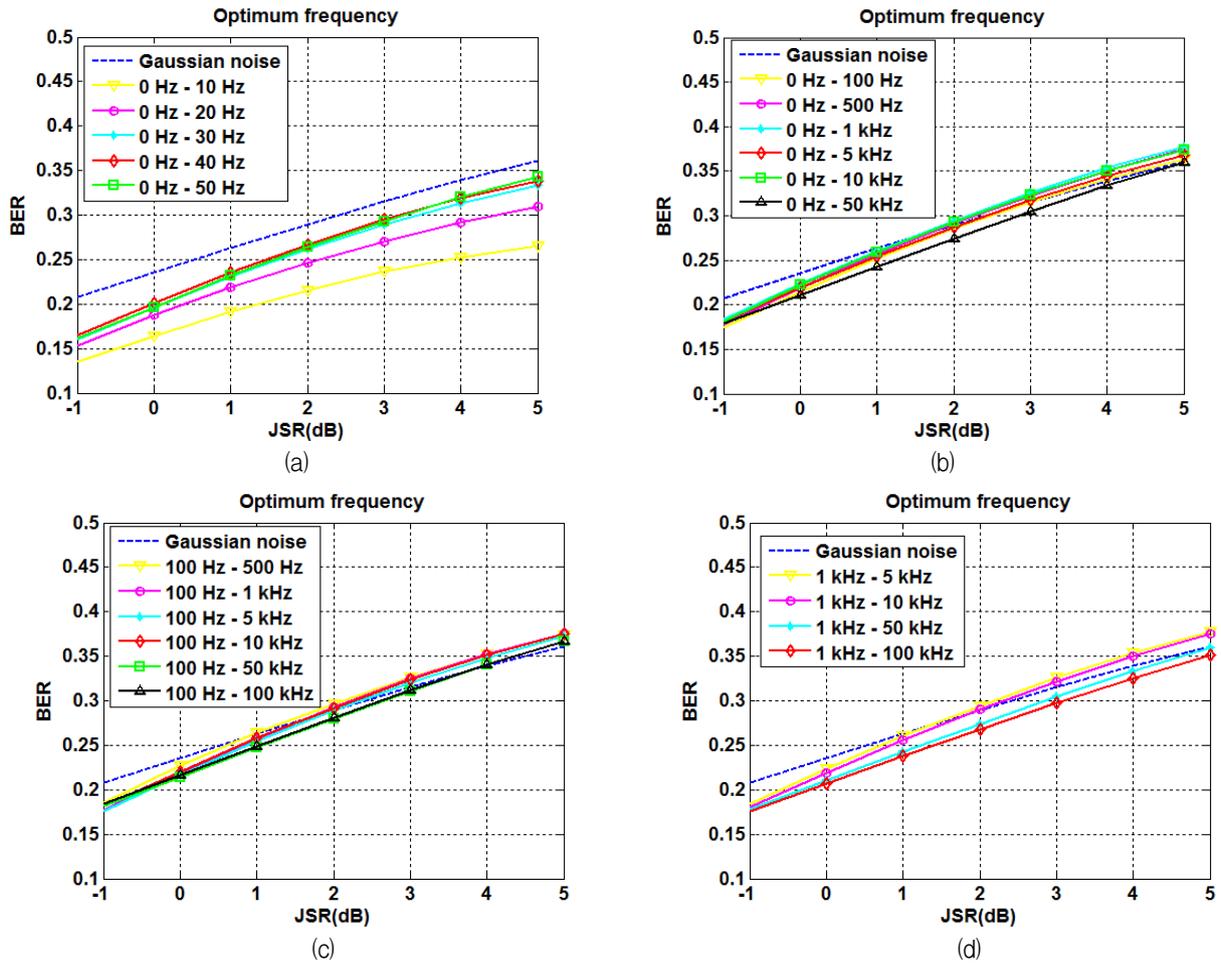


그림 10. 4G(LTE) 환경에서 왜곡 주파수 구간에 따른 재밍 성능.
(a) 최소: 0Hz, 최대: 10Hz-50Hz (b) 최소: 0Hz, 최대: 100Hz-50kHz
(c) 최소: 100Hz, 최대: 500Hz-100kHz (d) 최소: 1kHz, 최대: 5kHz-100kHz

Fig. 10. Jamming performance according to disturbing frequency band in 4G(LTE) system.
(a) min: 0Hz, max: 10Hz-50kHz (b) min: 0Hz, max: 100Hz-50kHz
(c) min: 100Hz, max: 500Hz-100kHz (d) min: 1kHz, max: 5kHz-100kHz

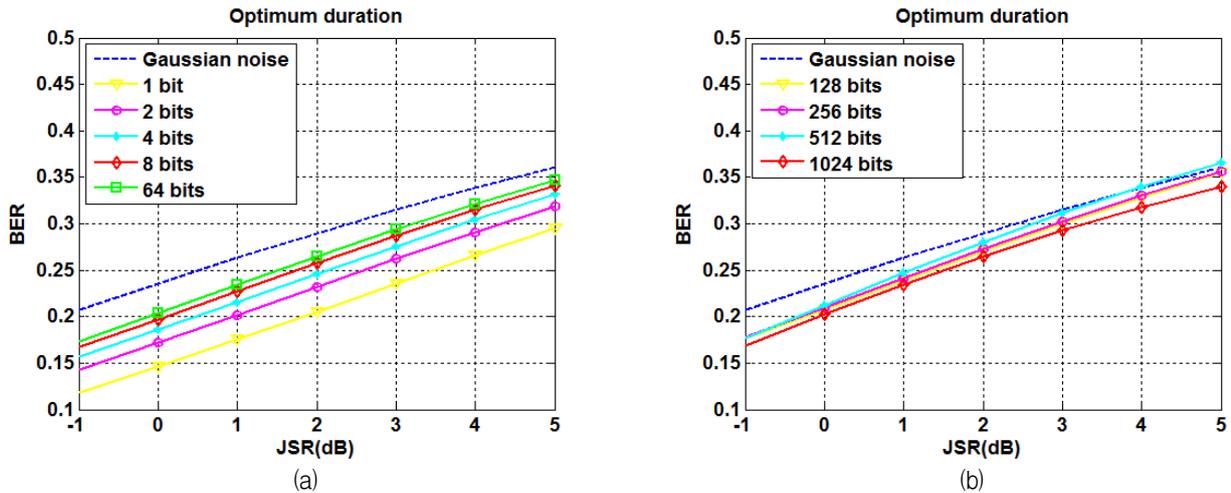


그림 11. 4G(LTE) 환경에서 왜곡 주기에 따른 재밍 성능. (a) 1 bit-64 bits (b) 128-1024 bits
Fig. 11. Jamming performance according to disturbing duration in 4G(LTE) system. (a) 1 bit-64 bits (b) 128-1024 bits.

을 보면, 그림 8의 (a)에서 왜곡 주파수 구간이 0-20 Hz 이하의 경우 왜곡 주파수 구간이 너무 좁은 경우 재밍 성능이 떨어지기 때문에 그 이상의 주파수 왜곡 구간의 폭이 필요하다는 것을 알 수 있다. 그림 8의 (b)-(d)까지 다양한 왜곡 주파수 구간에 대해서 JSR에 상관없이 repeater 재밍이 가우시안 잡음을 이용한 재밍에 비해 성능이 우수한 것으로 나타났다. 또한 그림 9에서 주파수 왜곡 주기의 변화에 따라서 시뮬레이션을 시행한 결과, 그림 9의 (a)에서 주파수 왜곡 주기가 짧은 경우보다 그림 9의 (b)에서 주파수 왜곡 주기가 8-64bits의 경우에 재밍 성능이 우수한 것을 알 수 있다.

그림 10, 11은 4G(LTE) 환경에서의 재밍 성능을 왜곡 주파수 구간과, 왜곡 주기에 따라서 각각 나타낸 것이다. 왜곡 주파수 구간에 따른 시뮬레이션 결과인 그림 10을 보면, 그림 10의 (a)에서 왜곡 주파수 구간이 0-50 Hz 이하의 경우 왜곡 주파수 구간이 너무 좁은 경우 재밍 성능이 떨어지기 때문에 그 이상의 주파수 왜곡의 폭이 필요하다는 것을 알 수 있다. 그림 10의 (b)-(d)에서 다양한 왜곡 주파수 구간에 대해서 1-2 dB 이하의 JSR에서는 repeater 재밍이 가우시안 잡음을 이용한 재밍보다 약간 낮은 성능을 가지지만, 1-2 dB 이상의 JSR에서는 repeater 재밍이 가우시안 잡음을 이용한 재밍보다 조금 나은 성능을 보였다. 또한 그림 11에서 주파수 왜곡 주기의 변화에 따라서 시뮬레이션을 시행한 결과, 그림 11의 (a)와 같이 주파수 왜곡 주기가 짧은 경우보다 그림 11의 (b)와 같이 주파수 왜곡 주기가 64-1024 bits의 경우에 재밍 성능이 높아지는 것을 알 수 있다.

결과를 종합해보면, 3G와 4G 시스템에서 공통적으로 반응 재밍을 효과적으로 사용하기 위해서는 최소한의 왜곡 주파수 구간과 주파수 왜곡 주기가 필요함을 알 수 있다. 재밍 성능에서는 3G 환경에서 repeater 방식의 반응 재밍이 전체 주파수 왜곡 구간에 대해서 전반적으로 가우시안 잡음 재밍보다 성능이 우수하게 나타났고, 4G 환경에서는 1-2 dB 이하의 낮은 JSR에서는 전반적으로 가우시안 잡음 재밍보다 성능이 약간 떨어지지만, 1-2 dB 이상의 JSR에서는 가우시안 잡음 재밍보다 조금 나은 성능을 보였다.

IV. 결 론

본 논문은 이동통신 시스템을 통해 모바일 단말기로 트리거되는 RCIED 장비에 대응하기 위해서 효율적인 전파교란 기법을 개발하고자 했다. 이를 위해 RCIED의 트리거 신호원이 될 수 있는 대표적인 시스템인 3G(WCDMA)와 4G(LTE) 시스템에 대해 반응 재밍에서 필요한 반응시간을 호 처리 절차 분석을 통해서 제시하였다. 또한 Matlab Simulink를 통해서 3G/4G 두 가지 시스템에서 repeater 방식의 재밍에 대해 왜곡 파라미터에 따른 재밍 성능을 분석하여, 왜곡 파라미터의 값에 따른 성능의 변화를 제시하였다. 이를 통해 적절한 왜곡 파라미터를 적용하였을 때, repeater 방식의 재밍 기법은 3G 환경에서는 기존 잡음 재밍기법에 비해 우수한 성능을 보였고, 4G 환경에서는 기존 잡음 재밍과 비슷한 성능을 보임을 알 수 있었다.

REFERENCES

- [1] Glenn Zorpette, "Countering IEDs", *IEEE SPECTRUM*, pp. 26-35. Sep 2008.
- [2] K. Wilgucki. R. Urban, G.Baranowski, P. Gradzki, p. Skarzynski, "Automated protection system against RCIED", *In Proc. Military Communication Institute (MCI)*, 2012.
- [3] K. Wilgucki. R. Urban, G.Baranowski, P. Gradzki, p. Skarzynski, "Selected aspects of effective RCIED Jamming", *In Proc. Military Communication Institute (MCI) 2012*.
- [4] Jan Mietzner, Patrick Nickel, Askold Meusling Patrick Loos Gerhard Bauch, "Responsive Communications Jamming Against Radio - Controlled Improvised Explosive Devices", *IEEE Communication Magazine*, pp. 38-46. Oct 2012.
- [5] Wang Hang, "Performance of DSSS against Repeater Jamming" *IEEE Electronics, Circuits and Systems*, 2006.
- [6] Matthias Wilhelm, "Short Paper: Reactive Jamming in Wireless Networks - How Realistic is the Threat?", *WiSec'11 Proceedings of the fourth ACM conference on Wireless network security. 2011*.
- [7] T. Y. Byun, "Understanding of Mobile Communication", *Intervision*, 2008.
- [8] C. S. Gang, "Mobile Communications: Theories and Applications", *Cheong Moon Gak*, 2010.

- [9] Jose E. Vargas Bautista, "Performance of CS Fallback from LTE to UMTS", *IEEE Communications Magazine*, September 2013.

— 저 자 소 개 —



김 요 한(학생회원)
2014년 부산대학교 전자전기통신
공학부 학사 졸업.
2014년~현재 부산대학교 전자
전 기공학과 석사과정.
<주관심분야 : 통신 및 신호처리,
레이더 및 소나시스템>



김 동 규(학생회원)
2011년 부산대학교 전자전기통신
공학부 학사 졸업.
2011년~현재 부산대학교
전자전기컴퓨터공학과
석박통합과정.

<주관심분야 : 통신 및 신호처리, 레이더 및 소나
시스템>



김 형 남(평생회원)- 교신저자
1993년 2월 포항공과대학교
전자전기공학과 학사
1995년 2월 포항공과대학교
전자전기공학과 석사
2000년 2월 포항공과대학교
전자전기공학과 박사
2000년 3월~2000년 4월 포항공과대학교
전자컴퓨터공학부 박사 후 연구원
2000년 5월~2003년 2월 한국전자통신연구원
선임연구원
2003년 3월~2007년 2월 부산대학교
전자공학과 조교수
2007년 3월~2012년 2월 부산대학교
전자전기공학부 부교수
2012년 3월~현재 부산대학교 전자공학과 교수
<주관심분야 : 적응신호처리, 레이더 및 소나 신
호처리, 디지털 방송신호처리, 생체신호처리>