2019 년 1 월 18ZF1200-01-2500P

전체부수

Overhead 없이 도감청을 원천차단하는 Simultaneously-Transmitted Jamming 기술

ST-Jamming for Overhead-Free PHY Layer-Secured Communications

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

제 출 문

본 연구보고서는 주요사업인 "Overhead 없이 도감청을 원천차단하는 Simultaneously-Transmitted Jamming 기술"의 결과로서, 본 과제에 참여한 아래의 연구팀이 작성한 것입니다.

2019 년 1 월

연구책임자 : 선임연구원 주형식 (초연결통신연구소)
연구참여자 : 선임연구원 손정보 (초연결통신연구소)
연 구 원 곽동혁 (초연결통신연구소)

요 약 문

I. 제 목

Overhead 없이 도감청을 원천차단하는 Simultaneously-Transmitted Jamming 기술

II. 연구목적 및 중요성

연구 목적	- 오버헤드 없이 물리계층에서 양방향 정보 전송을 동시에 보호하는 보안 통신 기술 개발 - 보안-데이터 전송간 trade-off 극복하고 데이터 전송률(secrecy capacity)을 향상시키는 기술 개발
연구의 중요성	- 기지국과 단말이 동일대역에서 동시에 신호를 송수신할 경우, 도청자의 수신 신호에는 기지국과 단말의 송신 신호가 섞여 있으므로 기지국과 단말의 송신신호가 서로를 보호함. - 양 방향의 정보 전송이 동시에 보호될 수 있을 뿐 아니라 각각의 링크에서의 보안 오버헤드가 크게 감소하므로 보안-데이터전송 trade-off를 극복함. - 기지국과 단말 모두 주어진 자원을 전부 활용하여 정보를 전송할 수 있으므로 양방향에서 링크 효율화 지수가 증가 하게 되고, 이것이 보안 오버헤드의 감소 효과와 합쳐져 secrecy capacity를 증대시킴. - 동일대역 동시 송수신 기술과 물리계층 보안 기술 사이의 시너지를 통해 물리계층 보안과 동일대역 동시 송수신 기술의 태생적인 문제를 해결

III. 연구내용 및 범위

내 용	범 위
동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발	- 양방향 PLS 통신을 위한 동일대역 동시 송수신 장치 설계 - 양방향 PLS 전송 기술 개발 및 전송 시스템 설계 - 보안키 삽입 기술 개발
양방향 PLS 통신을 위한 보안키 설계	- X-independence를 위한 최적의 jamming sequence 및 pattern 설계 연구 - Jamming sequence와 pattern을 통한 2중 보안키 설계 연구
양방향 보안 통신 시스템 성능 분석	- 단일사용자 환경에서 제안된 동일대역 동시 송수신 기반 양방향 PLS 전송기술의 성능 분석
양방향 보안통신 성능 검증 플랫폼 개발	- 성능검증 플랫폼을 위한 HW/SW 인터페이스 개발

IV. 연구결과

성과 지표	상, 하향링크의 무선 전송 링크 효율화 지수 (w_d, w_u)	상, 하향링크에서 보안 overhead (L_u, L_d)	유효 전송 신호에 대한 도청자의 bit-error rate
목표	w_d, = 1 w_u = 1	$L_D = L_U = 0$	0.5
목표 산출 근거	이론적 한계치	이론적 한계치	이론적 한계치

성과 지표 달성 내용	$w_D = w_U = 1$ 의 동시 달성 확인 (동일 대역에서 RF 신호의 동시 송수신에 대한 feasibility 검증)	$L_D = L_U = 0$ 의 동시 달성 확인 (Legitimate Tx 신호 및 도청자의 Rx 신호간 통계적 independence 증명)	하향링크의 유효 전송 신호 decoding bit-error rate 0.5 를 동시에 달성함을 보임
평가 (검증) 방법	시뮬레이션 검증 (자기간섭 제거 성능 검증, 자기간섭 제거 이후의 유효 수신신호 decoding 성능 검증)	시뮬레이션 검증 (jamming sample 길이에 관계없이 Legitimate Tx 신호 및 도청자의 Rx 신호의 independence 가 성립함을 보임)	시뮬레이션 검증 (기지국-도청자-단말의 상대적 거리에 따른 bit-error rate 도출)

V. 연구개발결과의 활용계획

활용 계획	상세 내용
다양한 상용 통신 및 IDX convergence 분야에 적합한 보안 기술로의 확장	- 상용 통신 및 무선 백홀 시스템에서 사용자 정보 보호를 위한 PLS 기술 - 5G IoT 네트워크에 적합한 PLS 기술 - 대태러 혹은 전자전 기술로의 확장 - 차량간 통신 및 의료, 행정 IDX 등에 적합한 PLS 기술로의 확장

대형 과제 기획을 위한 pilot 기술로 활용	- 6G 이동통신 시스템 개발을 위한 요소 기술 - 차세대 국방 통신 시스템 개발을 위한 핵심 기술 - 그 외 다양한 IDX convergence 플랫폼 구축을 위한 보안 통신 요소 기술

VI. 기대성과 및 건의

1. 보안과 데이터 전송간의 trade-off 로 대표되는 물리계층 보안의 기술적 허들과 동일대역 동시 송수신 시스템의 데이터 전송률 향상 한계 극복
2. 차세대 통신 네트워크를 위한 보안 기술의 패러다임 전환 및 선점
   A. 통신과 PLS 가 완전히 통합된 새로운 PLS 통신 패러다임의 선점
   B. '보안'과 '동일대역 동시 송수신'이라는 키워드를 함께 고려함으로써
      - 보안-정보전송간 trade-off 및 PLS overhead 라는 PLS 의 한계 극복
      - 동일대역 동시송수신의 traffic 비대칭 및 2 배의 capacity 증가 한계 극복
   C. 보안과 통신을 융합하는 새로운 연구 트렌드 창출

ABSTRACT

I. TITLE

ST-Jamming for Overhead-Free PHY Layer-Secured Communications

II. THE OBJECTIVES

Objective of Research	- Development of secure communication technology that simultaneously protects bi-directional information transmission in physical layer without overhead - Development of technology to overcome trade-off between security-data transmission and improve data rate (secrecy capacity)
Importance of Research	- When the base station and the terminal transmit / receive signals simultaneously in the same band, the signals transmitted from the base station and the terminal protect each other since the signals transmitted from the base station and the terminal are mixed in the signal received by the eavesdropper. - Both directions of information transmission can be protected at the same time, and the security overhead on

	each link is greatly reduced, overcoming the security-data transmission trade-off - Since both the base station and the terminal can transmit information using all the resources, the link efficiency index increases in both directions, and this increases the secrecy capacity by combining with the effect of reducing the security overhead - Solves the inherent problem of physical layer security and simultaneous transmission and reception of the same band through synergy between simultaneous transmission and reception technology of the same band and physical layer security technology.

III. THE CONTENTS AND SCOPE OF THE STUDY

Contents	Scope
Bi-Directional PLS Transmission Technology Based on In-band	- Design of in-band full duplex transceiver for bi-directional PLS communication - Development and design of bi-directional PLS transmission technologies

Full Duplex	- Development of technologies to insert secrecy key sequences
Design of Secrecy Key for Bi-directional Communication	- Study of optimal jamming sequence and pattern design for X-independence - Design of dual-stage secrecy key based on jamming sequence and pattern
Performance Analysis of Bi-Directional Security Communication System	- Performance analysis of bi-directional PLS transmission technologies based on in-band full duplex in single user environment
Development of Performance Verification Platform of Bi-directional Secure Communication	- Development of HW/SW interface for performance verification platform

IV. RESULTS

Measurement	Link Efficiency Index in DL (w_d) & UL (w_u)	Secrecy Overhead in DL (L_d) & UL (L_u)	Bit-Error Rate for Legitimate Information
Performance Indicator	w_d, = w_u = 1	$L_D = L_U = 0$	0.5
Basis of Determining Performance Indicator	Theoretic Limit	Theoretic Limit	Theoretic Limit
Details of Achievements	Simultaneous Achievement of $w_D = w_U = 1$ (verification for simultaneous Tx and Rx of RF signal within the same frequency band)	Simultaneous Achievement of $L_D = L_U = 0$ (proof of statistical independence between legitimate Tx signal and Rx signal of eavesdropper)	Simultaneous Achievement of Decoding Bit-Error Rate 0.5 in Both DL & UL
Method	Simulation	Simulation	Simulation

V. EXPECTED RESULT & PROPOSITION

1. Overcoming Technical hurdles of physical layer security represented by trade-off between security and data transmission and limit of improvement of data transmission rate of simultaneous transmission and reception system
2. Paradigm shift and preemption of security technology for next generation communication network
   A. Preemption of a new PLS communication paradigm with fully integrated communication and PLS
   B. By considering the keywords 'security' and 'same-band simultaneous transmission and reception',
      - Overcoming the limit of PLS represented by PLS overhead and trade-off between security and information transmission
      - Overcoming inefficiency yielded by Traffic asymmetry and limit of capacity increase in in-band full duplex systems
   C. Creating new research trends that combine security and communication

CONTENTS

Tables

Figures

목 차

표 목 차

그 림 목 차

제 1장. 서 론

1절. 연구개발과제의 필요성

1. 4 차 산업 혁명 및 IDX 추진 전략에 따른 정보 보안의 중요성 증대

가. 4차 산업 혁명은 초연결과 지능을 기반으로 한 지능화 혁명으로, 제품, 서비스가 연결된 통합 서비스(플랫폼, 생태계)가 시장을 주도할 것이며, 제조, 서비스 등 민간부분 뿐 아니라 행정, 국 방 등 공공 부분에 이르는 국가 인프라 시스템이 통합될 것(IDX 플랫폼)으로 전망됨

나. IDX 플랫폼에서는 데이터의 분석 및 가공을 통한 지능화와 함께 막대한 데이터의 효율적인 수 집 및 축적이 핵심이 될 것이나, 이는 필연적으로 해킹, 도청 등을 통한 다양한 개인, 사회 정보 유출 위험을 증가시키게 될 것이며, 특히 공유·수집되는 개인, 사회적 정보의 범위가 이전과는 비교할 수 없을 만큼 넓은 만큼 이러한 정보의 유출은 상상하기 힘들 정도로 큰 파급효과를 가 져올 수 있음.

다. 따라서 미래 사회에서는 강력한 정보 보안의 필요성이 더욱 커질 것이며, 정부와 당해 기간 또 한 정보 보안을 위한 정책을 펼치고 있음

1) 미래창조과학부 'K-ICT 네트워크 발전전략(2015.12.7.)' 및 K-ICT 시큐리티 발전전략(2015. 4)

2) '글로벌 시장을 선점하는 원천 보안기술 개발' 국가 정책

3) 기술격차(선진국, 보안위협)를 해소하고 이용자 중심의 기술 확보를 위한 「글로벌 ST(Security Technology) 이니셔티브」추진

4) ‘IT 분야 정보보호 및 표준화 연구’ 등의 ETRI 기관 임무

2. 물리계층 보안을 통한 정보 보안성 증대의 필요성

가. 종래의 암호화(Crptography) 기반 보안 기법

1) 송신자가 암호키를 이용해 메시지를 암호화하여 전송하면 수신자가 암호키를 이용해 메시지를 해독하는 방법으로, LTE, WiMAX, Wi-Fi 등 대부분의 통신 시스템에 적용 가능하며, 비교적 낮은 복잡도로 암호화와 해독이 가능함.

2) 암호화 기반 보안 시스템은 계산 복잡도에 의존하기 때문에 프로세싱 속도의 발전에 따라 한 계를 드러낼 것으로 예상됨. 가령, 64 비트 DES(Data Encryption Standard)의 경우 수 시간 내에 해독이 가능함이 알려져 있으며, 처리 속도가 훨씬 빠른 양자 컴퓨터가 상용화된다면 대부분의 암호화 알고리즘이 해독될 것으로 예상됨

3) 또한, 무선 ICT 환경의 경우, 정보를 전달하는 전파 신호가 어디든 도달하므로 도청자가 기본적 으로 신호를 수신할 수 있음. 따라서 암호화 기반의 보안 기법은 무선 ICT 환경에서 근본적인 취약점을 가짐.

4) 따라서, 무선 환경에서 정보 신호를 이미 수신한 도청자가 충분한 연산 능력을 갖추고 있다면 기 존의 암호화 기반의 보만 기법만으로는 정보의 보안을 보장할 수 없음.

나. 물리계층 보안(Physical Layer Security, PLS)

1) 잡음 및 무선통신 채널의 고유한 무작위성과 무선전송기술을 활용하여 무선 채널을 통해 비밀 메시지를 안전하게 교환하기 위한 보안 기술

2) 도청자의 물리계층 채널을 의도적으로 악화시킴으로써 비밀 메시지에 대한 도청자의 decoding error 를 높이고 도청자가 얻을 수 있는 비밀 메시지에 대한 정보량을 감소시키는 기술.

① Perfect security : 도청자가 무제한의 계산 능력과 시간을 가지고 있다 할지라도 비밀 메시 지를 전혀 복호할 수 없는 상태

② Asymptotically perfect security : 비밀 메시지의 codeword 길이가 무한히 길어질 때, 도청 자가 무제한의 계산 능력과 시간을 가지고 있다 할지라도 비밀 메시지를 전혀 복호할 수 없 는 (perfect security 를 달성하는) 상태

3) 이론적으로는 메시지 전송을 위한 codeword(비밀 메시지와 보안키를 포함하는)가 무한히 길 때 PLS 를 통해 점근법적인(asymptotically) perfect security 를 달성할 수 있음.

4) 실제 통신 시스템에서는, codeword 의 길이가 유한하므로 PLS 만으로는 asymptotically perfect security 를 달성할 수 없으나, 대신 비밀 메시지에 대한 도청자의 decoding error 를 크게 높일 수 있음.

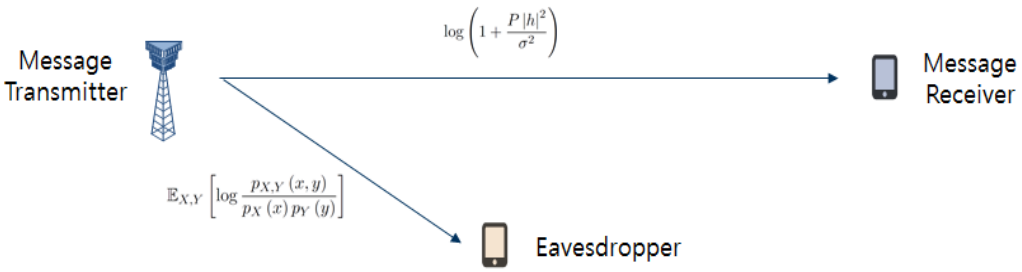
2절. 연구개발과제의 중요성

1. Secrecy Capacity

가. 점근법적인 perfect security 를 달성하면서 메시지를 원하는 수신자에게 전송할 때 얻을 수 있는 이론적인 최대 데이터 전송률로 아래 <그림 1>의 수식 (1)과 같이 정의됨.

나. 수식 (1)에서 PLS overhead L 은 송신자와 도청자 사이의 채널을 왜곡시켜

물리계층에서 보안성을 확보하기 위해 필요한 overhead 임.



$$C_S = \log\left(1+\frac{P|h|^2}{\sigma^2}\right) - \underbrace{\mathbb{E}_{X,Y}\left[\log\frac{p_{X,Y}(x,y)}{p_X(x)p_Y(y)}\right]}_{\text{PLS overhead } (L)} \qquad (1)$$

X : message transmitter의 송신 신호
Y : eavesdropper의 수신 신호
P : message transmitter의 송신 power
σ^2 : message receiver의 noise power
h : message transmitter와 message receiver 사이의 무선 채널

$p_X(x)$: message transmitter의 송신 신호가 $X=x$일 확률
$p_Y(y)$: eavesdropper의 수신 신호가 $Y=y$일 확률
$p_{XY}(x,y)$: message transmitter의 송신 신호와 eavesdropper의 수신신호가 각각 $X=x$이고 $Y=y$ 일 확률

<그림 1> Secrecy capacity 의 개념도

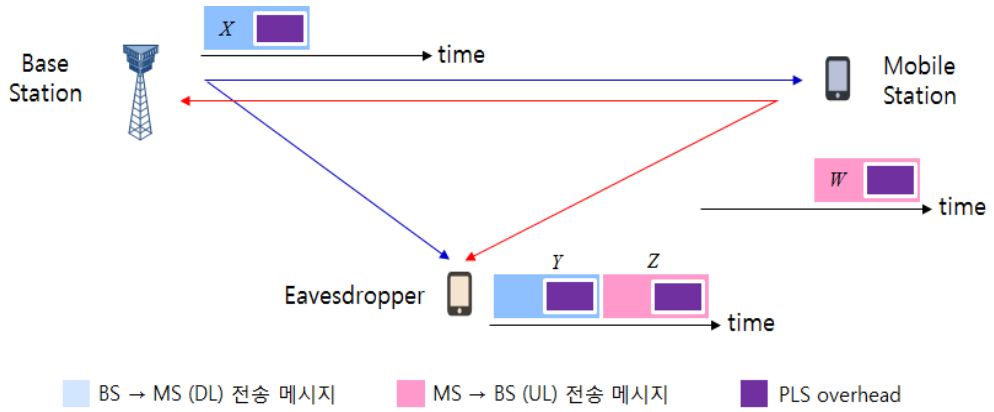
2. 양방향 무선 통신 환경에서 기존 PLS 기술의 한계

가. PLS overhead L 을 늘릴 경우 보안성은 증가시킬 수 있으나, 수식 (1)에서 볼 수 있듯이 secrecy capacity 는 감소하게 되고, secrecy capacity 를 증가시키기 위해 PLS overhead L 을 줄 일 경우 보안성에 취약점이 발생하므로 보안과 데이터 전송간에 태생적인 trade-off 가 존재함.

나. 기존의 PLS 기술이 단방향(massage transmitter → message receiver)의 통신을 보호하도록 설 계된 반면, 무선 통신 환경은 기본적으로 <그림 2>와 같이 양방향 통신(예를 들면 base station ↔ mobile station)임.

다. 일반적인 half duplex 통신 시스템(base station 과 mobile station 이 서로 다른

자원을 이용해 신호를 송신)에서 기존의 PLS 기법이 사용된 경우 secrecy capacity 는 다음 그림의 수식 (2)와 같이 표현됨.



<그림 2> 양방향 물리계층 보안 통신에서의 secrecy capacity

$$C_S = \omega_D \left(\log\left(1+\frac{P_B|h|^2}{\sigma_M^2}\right) - \underbrace{\mathbb{E}_{X,Y}\left[\log\frac{p_{X,Y}(x,y)}{p_X(x)\,p_Y(y)}\right]}_{\text{DL PLS overhead } (L_D)} \right) + \omega_U \left(\log\left(1+\frac{P_M|g|^2}{\sigma_B^2}\right) - \underbrace{\mathbb{E}_{W,Z}\left[\log\frac{p_{W,Z}(w,z)}{p_W(w)\,p_Z(z)}\right]}_{\text{UL PLS overhead } (L_U)} \right) \quad (2)$$

X : BS의 송신 신호
Y : eavesdropper의 DL 수신 신호
P_B : BS의 송신 power
σ_M^2 : MS의 noise power
h : BS → MS 무선 채널
w_D : DL에서 무선전송링크 효율화 지수
$p_X(x)$: BS의 송신 신호가 $X=x$일 확률
$p_Y(y)$: eavesdropper의 DL 수신 신호가 $Y=y$일 확률
$p_{XY}(x,y)$: BS의 송신 신호와 eavesdropper의 수신신호가 각각 $X=x$이고 $Y=y$ 일 확률

W : MS의 송신 신호
Z : eavesdropper의 UL 수신 신호
P_M : MS의 송신 power
σ_B^2 : BS의 noise power
g : MS → BS 무선 채널
w_U : UL에서 무선전송링크 효율화 지수
$p_W(w)$: MS의 송신 신호가 $W=w$일 확률
$p_Z(z)$: eavesdropper의 UL 수신 신호가 $Z=z$일 확률
$p_{WZ}(w,z)$: MS의 송신 신호와 eavesdropper의 수신신호가 각각 $W=w$이고 $Z=z$ 일 확률

1) 편의상 시분할 방식의 전송 기법을 예로 들면, 먼저 BS 가 정보를 송신한 후 MS 가 정보를 송 신하므로 도청자는 서로 다른 시간에 걸쳐 BS 와 MS 가 전송하는 정보를 모두 수신할 수 있음 (주파수 분할 방식에서도 동일한 현상 발생).

2) 기존의 PLS 기법의 경우, 단방향의 통신만을 보호할 수 있도록 설계되어 있으므로 양방향의 데이 터 전송을 동시에 보호할 수 없고, 이로 인해 각각의 방향에 대해 별도의 PLS overhead(DL 에서 의 LD 와 UL 에서의 LU)가 필요함.

3) 또한 $w_D < 1$ 및 $w_U < 1$ 이므로, 이것이 각 방향에서의 PLS overhead LD 및 LU 의 효과와 합쳐져 수식 (2)에서 볼 수 있듯이 secrecy capacity 의 심각한 저하를 발생시킴.

3절. 연구개발과제 수행의 제약요인

1. 본 연구개발과제의 수행을 통해 해결하고자 하는 PLS 의 제약요인

가. 보안-데이터 전송간 trade-off 극복

1) 보안과 데이터 전송간의 trade-off 는 전송 신호의 encoding 에 있어서 일부 자원이 PLS overhead 로 사용되기 때문에 발생함.

2) 만약 overhead 없이 PLS 를 통해 물리계층에서 정보 전송을 보호할 수 있다면 이러한 trade-off 를 극복할 수 있음.

나. 양방향 링크 통신의 동시 보호

1) 기존의 PLS 는 단방향의 통신 링크만을 보호하도록 설계되었음. 이로 인해 양방향 통신 환경에서 는 양방향의 정보 전송을 모두 보호하기 위해 각각의 링크에서 별도의 PLS overhead 를 필요로 하므로 시스템 전체의 PLS overhead 증가

2) 양방향 통신을 동시에 보호하는 PLS 가 있다면 링크별로 별도의 PLS overhead 가 필요하지 않게 되므로 통신 시스템의 전체적인 PLS

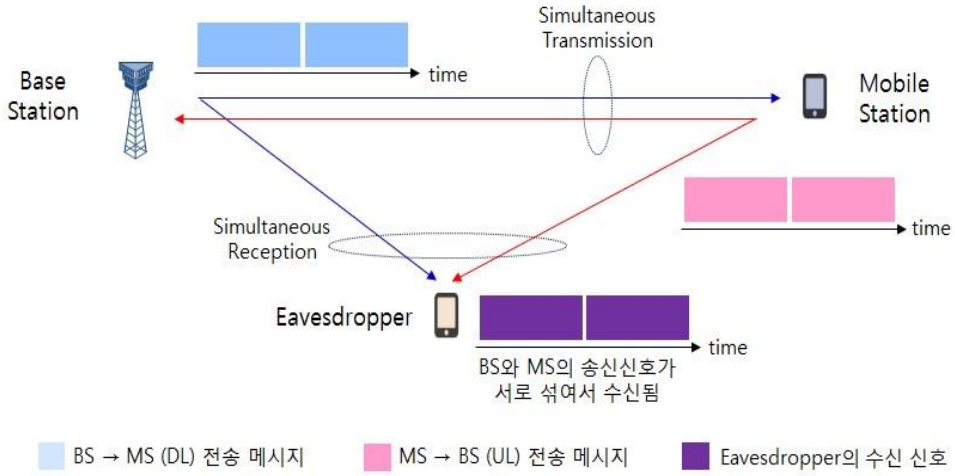
overhead 를 줄일 수 있음

다. 데이터 전송률(secrecy capacity)의 향상

1) 기존의 PLS 시스템에서는 보안과 정보전송 사이의 trade-off 와 양방향 통신 환경에서의 overhead 증가로 인한 secrecy capacity 감소와 더불어, 양 방향의 정보 전송이 서로 다른 자원을 점유, 즉 $w_D < 1$ 이고 $w_U < 1$ 이기 때문에 생기는 secrecy capacity 감소가 발생함.

2) Secrecy capacity 를 향상시키기 위해서는 overhead 를 줄이는 동시에 w_D 와 w_U 를 증가시켜 함

2. 동일 대역에서 신호의 동시 송수신을 통한 PLS 의 제약요인 해결



<그림 3> 본 연구과제 제안 기술의 개념도

가. BS 와 MS 가 동일 대역에서 동시에 신호를 송수신할 경우, 도청자의 수신 신호에는 BS 와 MS 의 송신 신호가 섞여 있음.

나. 즉, BS 와 MS 의 송신신호가 서로에 대한 보안키로 작용하여 서로를 보호

함.

다. 따라서, 양 방향의 정보 전송이 동시에 보호될 수 있을 뿐 아니라 각각의 링크에서의 PLS overhead가 필요 없거나 크게 감소하므로 PLS의 태생적인 trade-off를 극복할 수 있음.

라. 또한, BS 와 MS 모두 주어진 자원을 전부 활용하여 정보를 전송할 수 있으므로 w_D 와 w_U 증가 하게 되고, 이것이 PLS overhead 의 감소 효과와 합쳐져 secrecy capacity 의 획기적인 증가로 이 어질 수 있음.

3. 신호의 동일대역 동시 송수신을 기반으로 하는 PLS 시스템의 제약 요인

가. 동일대역 동시 송수신 기술의 feasibility

1) BS 와 MS 가 신호를 동일대역에서 동시에 송수신할 경우 송신 신호가 자신의 수신신호에 간섭 을 미치는 자기간섭(self-interference, SI)가 발생함.

2) 이러한 SI 는 일반적으로 수신해야 하는 desired signal 에 비해 수십 dB 이상 크므로 SI 의 제거 가 신호의 동일대역 동시 송수신의 핵심 요소 중 하나임.

3) 최근 SI 의 제거에 대한 이론적인 feasibility 가 증명되었을 뿐 아니라, 실제 구현상의 feasibility 가 proof-of-concept(PoC)를 통해 검증되었음

4) 미국의 KUMU Networks 및 Intel 은 MWC 2015 에서 신호의 동일대역 동시 송수신을 통한 정 보 전송 플랫폼을 전시하였음. 특히 KUMU Networks 는 스페인의 Telephonica 등의 서비스 업 체와 함께 무선 백홀 등 특정 application 에 대한 동일대역 동시 송수신 기술의 field test 를 진

행. 연세대학교 또한 GLOBECOM 2014 와 2015 에서 동일대역 동시 송수신 기술의 PoC 시연을 진행.

나. 동일대역 동시 송수신 시스템 구현 capability

1) 신호의 동일대역 동시 송수신 기반 PLS 시스템의 개발을 위해서는 신호의 동일대 역 동시 송수신 시스템 구현 capability 가 필수적으로 요구됨.

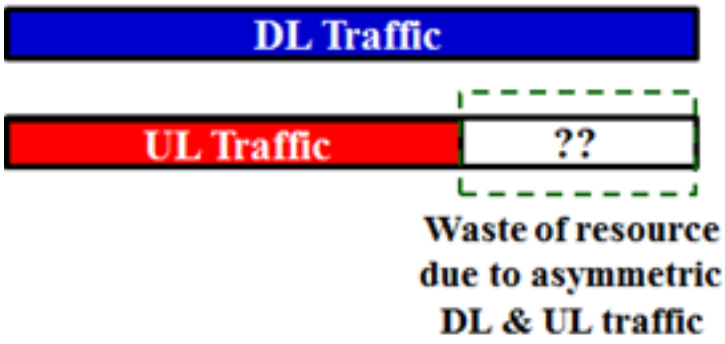
2) 본 연구 그룹은 2015 년에 SISO 환경에서 동일대역 동시 송수신을 위한 송수신기를 구현했으며, 현재 2 x 2 MIMO 동일대역 동시 송수신기 구현을 진행 중임.

다. 동일대역 동시 송수신 기술과 PLS 기술 사이의 synergy

1) PLS 기술과 마찬가지로 동일대역 동시 송수신 기술과 또한 태생적인 문제 및 한계가 있으며, 대표적으로 traffic asymmetry 에 의한 데이터 전송률 저하가 있음.

2) 동일대역 동시 송수신 시스템은 반드시 상, 하향링크가 동일한 자원을 점유하므로 상, 하향링 크의 traffic 이 다른 경우 traffic 이 적은 링크는 주어진 자원을 모두 활용하지 못하고 이로 인한 자원 낭비 및 데이터 전송률의 저하가 발생.

3) 이러한 동일대역 동시 송수신 시스템의 태생적인 한계가 PLS 와 접목되어 보안성을 향상시키 는데 활용될 수 있다면 보안성 향상과 데이터 전송 효율의 향상이라는 본 연구개발 과제의 목 표를 보다 효과적으로 달성할 수 있음.



<그림 4> 동일대역 동시 송수신에서 traffic asymmetry

제 2장. 본 론

1절. 연구 개발 현황

1. 국내외 기술 동향 및 수준

가. 물리계층 보안

1) 주로 대학을 중심으로 다음과 같은 주제로 연구가 수행되고 있음.

① 정보 이론 관점에서의 PLS 코딩 기법 : secrecy capacity 를 향상시키기 위한 전송 신호 설계 및 생성 기법으로 부호화, secret key generation, artificial noise scheme 등이 포함됨.

② 단방향 통신 환경에서의 PLS : 특정 duplex mode 를 가정한 후 그 중 한 방향에 대해서 PLS 를 다루는 연구로, 앞서 언급된 PLS 코딩기법 외에 다중안테나 signal processing, 자원 할당, cross-layer optimization 등의 연구가 수행됨.

③ 양방향 통신 환경에서의 PLS : 한 방향으로 정보를 전달하는 환경이 아닌 두 노드가 서로 정보 를 주고 받는 환경에서의 PLS 에 대한 연구로 기존의 단방향 통신을 위한 PLS 기법을 양방향 환경에 단순 적용하는 수준임.

④ 무선 응용 시스템에서의 PLS : IoT 시스템, 국방용 통신 시스템, 무선 전력 전송 시스템 등 특 정 application 에서의 PLS 기술을 다루는 연구.

2) 최근 단방향 PLS 기술 중 일부가 기술적으로 matured 되면서, IEEE 802.11ax, 3GPP LTE, IoT, 5G 등 다양한 기구에서 표준화 시도가 일어나고 있음.

나. 동일대역 동시 송수신 기술

1) 2000 년대 후반 ~ 2010 년대 초반에는 대학을 중심으로 IFD 송수신기 및 SI 제거 기술에 대한 PoC 검증에 대한 연구가 주류를 이룸

① PoC 검증을 통해 SI 를 background noise level 까지 제거할 수 있음을 보임.

② SISO/MIMO 환경에서 realtime implementation 에 대한 feasibility 가 검증됨

③ 최근에는 mmWave 대역에서의 SI 제거 PoC 검증에 대한 연구가 진행되고 있음.

2) 2010 년대 중후반 이후에는 학교를 중심으로 한 다중 사용자 IFD 에 대한 학술 연구와 기업을 중 심으로 한 표준화 시도 및 특정 application 에 대한 field test 에 대한 움직임이 본격적으로 일어 나고 있음.

① 간섭 제어, 자원 할당, 다중 사용자 beam 설계 등의 주제에 대한 학술 연구 결과(논문 등)가 활발하게 발표되고 있음.

② 현재까지 반영이 확정된 국제 표준은 없으나, study item 으로 선정하려는 시도는 꾸준히 있음.

2. 국내외 표준화 형황 또는 기술 발전 추세

가. 물리계층 보안

1) Secret key generation 기반 PLS 는 IEEE 802.11ac 표준에 기고되었으며, 3GPP 표준화에서 는 study item 으로 지정됨.

2) Artificial noise 및 beamforming 을 사용하는 secrecy coding 기반 PLS 는 IEEE 802.11ac 표 준에 기고되었으며, LTE releases, IoT & cellular IoT, 5G 등의 표준에 반영이 시도됨.

3) Key-free secure pairing 기반 PLS는 현재 3GPP, IEEE 802.11, IoT 및 5G 등의 표준에서 study item 으로 지정되어 있으며, 2020 년까지 표준 반영을 목표로 하고 있음.

나. 동일대역 동시 송수신 기술

1) KUMU Networks는 2012~2013 년에 걸쳐 IEEE 802.11ax 표준화 회의에서 study item 제정을 시도했으나 불발되었고, LG 전자는 2017 년 3GPP TSG RAN의 work item 선정 시도했으나 불발됨.

2) 이는, 현재 표준에 동일대역 동시 송수신 기술을 포함시키기에는 간섭 제어나 자원 할당 등에 있어서 기술적으로 해결해야 할 문제가 남아있기 때문임.

3) 5G 표준에도 계속해서 언급은 되었으나 현 버전에서는 일단 제외됨.

4) 간섭 제어와 효율적인 자원 할당 기술 개발과 함께 추후 5G 표준에 부분적으로 포함되거나 6G 표준부터 본격적으로 반영될 것으로 전망됨.

3. 동일, 유사 내용에 대한 국내외 관련자들의 연구 수행 내용

가. 물리계층 보안 기술

1) 정보이론 관점에서의 PLS 코딩 기법

① 특정 오류정정 부호를 PLS 에 적합한 형태로 변형해 원하는 보안 수준을 얻기 위한 전송 신 호를 설계하는 연구임.

② 단방향의 통신에서 정의되는 오류 정정부호의 특성상 단 방향 통신에서의 PLS로 그 범위가 한정되며, 동일대역에서 신호의 동시 송수

신을 통한 secrecy capacity 의 향상이 다루어지지 않음.

③ 반면 본 과제는 양방향의 통신에서 정의되는 PLS 기술이므로 더욱 진화된 형태의 기술이며, 특히 오류정정부호의 redundancy 를 요하지 않는 기술임.

2) 단방향 통신 환경에서의 PLS

① 단방향 통신 환경에서 PLS 를 향상시키기 위한 다중 안테나 신호처리, cross-layer optimization, 보안키 분배 기술 등에 대한 연구임.

② 특정 duplex 모드를 가정하므로 동일대역 동시 송수신을 지원하지 않으며, 이로 인해 단방 향의 통신만 을 보호하는 PLS 기술이라는 한계를 가짐.

③ 본 과제는 신호의 동일대역 동시 송수신 형태의 양방향 정보 전송 환경에서 두 방향의 전송을 동시에 보호하는 기술이므로 더욱 확장된 통신 환경에서 더 우수한 보안 성능을 보임.

3) 양방향 통신 환경에서의 PLS

① Two-way relay 시스템 등 특정 환경에서 PLS 를 위한 pilot 신호 및 채 널 추정기, precoder 설계 등에 대한 연구임.

② 동일 대역에서 양방향의 정보 전송이 동시에 존재할 수 있다는 본 과제와 유사점은 있으나, 각 방향의 링크별로 PLS 기법을 적용해야 하므로 overhead 및 보안과 정보 전송간 trade-off 문제가 해결될 수 없다는 한계를 지니며, 기존의 단방향 통신을 위한 PLS 기법을 양방향 환경에 단순 적용하는 수준임.

4) 무선 응용 시스템에서의 PLS

① 무선 전력 전송 통신 시스템 등의 특정 목적을 가지는 응용 시스템에서 목적 달성과 PLS 를 함께 최적화하는 기술에 대한 연구임.

② 이러한 무선 응용 시스템의 특성상 단방향의 통신 및 PLS 만을 고려하게 되므로 본 과제에서 고려하는 양방향 정보의 동시 전송을 통한 data rate 및 overhead 상의 이득을 얻을 수 없음.

나. 동일대역 동시 송수신 기술: SI 제거 기술에 대한 연구가 주류를 이루고 있으며, 최근 다중 사용자 통신 환경에서 동일대역 동시 송수신 시스템의 성능 향상에 대한 연구가 활 성화 되어가고 있음.

1) SI 제거 기술에 대한 연구

① 국외에서는 Stanford, Rice, Princeton 대학 등을 중심으로 SI 제거 기술 및 PoC 검증에 대한 연구가 주류를 이루어 옴.

② 국내에서는 연세대학교가 이 대열에 합류하여 SI 제거의 PoC 검증에 성공

③ SISO 및 MIMO 환경에서의 PoC 검증 성공 사례가 여러 차례 발표되었으며, 최근에는 Huawei 등의 기업을 중심으로 mmWave 대역에서의 SI 제거 PoC 검증에 대한 연구가 진행되고 있음.

2) 다중 사용자 통신 환경에서의 성능 향상에 대한 연구

① 최근 국내외 대학을 중심으로 다중 사용자 환경에서 동일대역 동시 송수신의 성능 향상을 위한 학술 연구가 진행되고 있음.

② 대표적으로 간섭 제어, 자원 할당, 다중 사용자 beam 설계 등의 주제에

대한 연구가 진행되고 있으며, 관련 연구 과제로는 대표적으로 유럽의 다수의 국가에서 공동으로 진행된 DUPLO project 가 있음.

4. 국내외 경쟁 기관 현황

가. 물리계층 보안 기술

1) 국내 대학

① KAIST, 광주 과기원, 고려 대학교, 인하 대학교, 한국 교통 대학교, 부산 대학교 등이 PLS 기술에 대한 연구를 수행중임.

② 오류정정부호 기반의 물리계층 보안 기술 및 다중안테나 시스템에서의 PLS 에 대한 학술적인 연구와 더불어 IoT 시스템에서의 PLS 기술의 경량화와 무선전력전송 시스템, 군용 통신 시스 템 등 다양한 응용 시스템에서의 PLS 에 대한 연구를 수행 중임.

2) 국내 기업

① 삼성전자에서는 NFC 환경에서의 물리계층 보안 기술에 대한 지식재산권을 소유하고 있음.

② 그 외에는 뚜렷한 연구 활동을 보이는 국내 기업은 관측되지 않음.

3) 국외 대학

① MIT, Princeton 대학교, Stanford 대학교, Georgia Tech., 애리조나 주립대, 펜실베니아 주 립대 등에서 PLS 기술에 대한 연구를 수행중임.

② 주로 정보이론 관점에서의 이론적인 한계와 이를 달성하기 위한 전송 신호 코딩 기법에 초 점을 맞추고 있으나, 기본적으로 단방향 통신에 대한 PLS 기법이라는 한계를 지님.

③ MIT 에서는 jamming 을 이용해 실용적이면서도 보안 성능이 우수한 물리계층 보안 기술을 개 발했으나, 보안 유지를 위한 overhead 가 크다는 점과 양방향 통신 환경에서는 이러한 overhead 가 배로 증가한다는 한계를 가짐.

④ Arizona 대학에서는 동일대역에서 데이터와 jamming 신호를 동시에 전송하는 물리계층 보안 기법을 제안했으나, 보안의 범위가 단방향 통신으로 제한되어 데이터 전송률에 손실이 생긴다는 한계를 가짐.

4) 국외 기업

① Cisco Technology, Qualcomm, Broadcom 등 대기업을 중심으로 PLS 관련 지식재산권 확보를 위한 연구 활동이 관측되고 있음.

② Advanced Micro Devices, Digital Equipment Corporation, Ls Cable 등 중소, 벤처기업에서는 repeater, 802.11 LAN, wireless PAN 등 특정 application 을 중심으로 한 PLS 기술 개발을 수행 중.

나. 동일대역 동시 송수신 기술

1) 국내외 여러 대학들이 주축이 되어 SI 제거와 다중 사용자 통신 환경에서의 성능 향상에 대한 연구를 수행하고 있음.

2) 국내외 기업들은 무선 백홀 등의 application 에 대한 field test (KUNU Networks), mmWave 환경에서 SI 제거의 feasibility 에 대한 연구 (Huawei, Intel), 표준 반영 시도 (LG 전자) 등의 활 동을 하고 있음.

3) 다만, 동일대역 동시 송수신 기술과 PLS 를 융합하려는 본격적인 움직임은 관측되지 않음.

2절. 핵심 요소 및 접근 방법

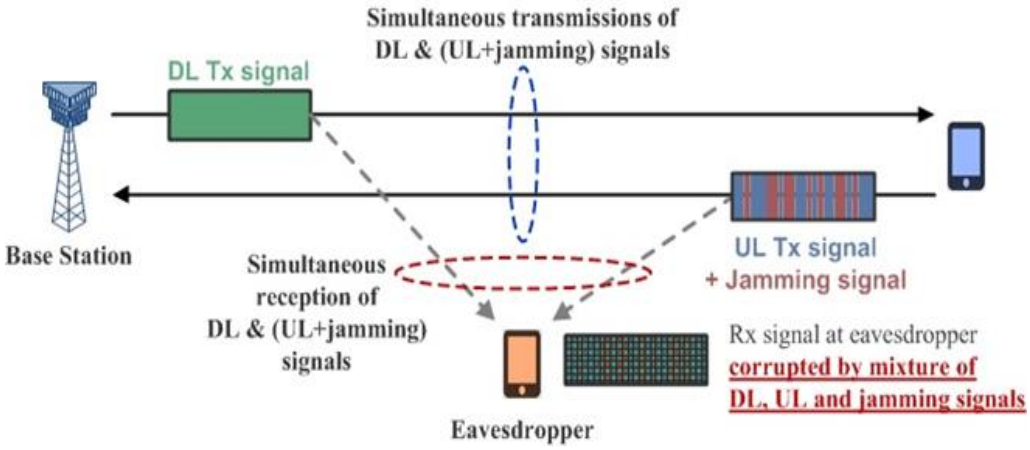
1. 동일대역 동시 송수신을 기반으로 하는 PLS 시스템 개발

가. 전송 신호 자체를 보안키로 활용하는 보안 기술

1) BS 와 MS 가 동일 대역에서 동시에 신호를 송수신할 경우, 도청자의 수신 신호에는 BS 와 MS 의 송신 신호가 섞여 있으므로 BS 와 MS 의 송신 신호가 서로에 대한 보안키로 작용하여 서로를 보호함.

2) 양방향 통신의 동시 보호 달성.

나. 수식 (2)에서 $w_D = 1$ 과 $w_U = 1$ 의 동시 달성을 통해 양 방향의 정보 전송이 서로 다른 자원을 점 유함으로 인해 발생하는 secrecy capacity 의 저하 문제 해결.



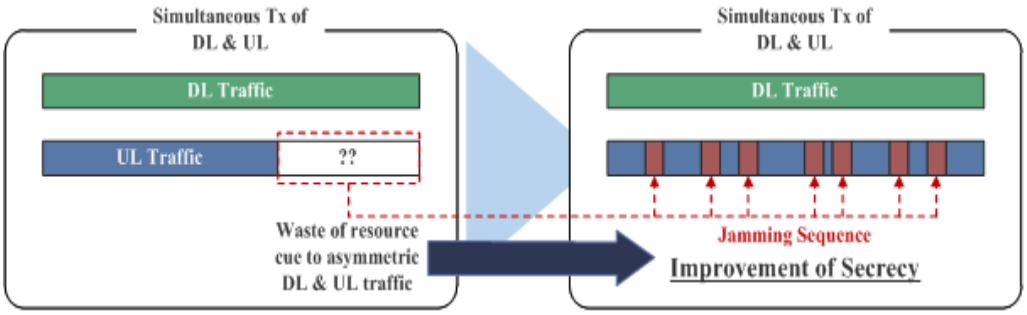
<그림 5> ST-jamming 에 의한 도청 방지 효과

2. Traffic asymmetry 를 이용한 jamming 신호 삽입 기술 개발

가. 동일대역 동시 송수신 시스템의 태생적인 문제점을 이용한 PLS 로, traffic asymmetry 로 인한 data rate 저하 문제 해결.

나. 상, 하향링크간 traffic 차이에 의해 사용되지 않는 자원을 이용하여 jamming 신호를 삽입하므로 PLS 를 위한 추가적인 자원을 사용하지 않음.

다. PLS 를 위한 추가적인 자원을 사용하지 않으면서 기지국과 단말의 전송 신호 간 independence 확 보(수식 (2)에서 $L_D = 0$ 과 $L_U = 0$ 의 동시 달성)를 통한 zero PLS overhead 달성 및 보안-정보 전 송 간 trade-off 극복.



<그림 6> Traffic asymmetry 를 활용한 물리계층 보안 성능 증대

3. 2 중 보안키를 통한 PLS 보안 성능 향상: Jamming 신호의 sequence 와 pattern 을 모두 이용함에 따른 보안성 향상.

4. 핵심 요소 및 접근 방법의 혁신성과 독창성

가. 양방향 링크 통신의 동시 보호

1) 기존의 PLS 는 양방향의 데이터 전송 링크가 서로 다른 자원을 점유하는 시스템을 기반으로 하므로 기본적으로 양방향의 데이터 전송을 동시에 보호할 수 없음.

2) 따라서, 양방향의 정보 전송을 모두 보호하기 위해서는 각각의 링크에서 별도의 PLS overhead 를 사용할 수밖에 없음.

3) 반면, 제안된 PLS 기법은 동일대역에서 BS 및 MS 전송 신호와 jamming sequence 가 동시에 전송되므로 양 방향의 정보 전송 링크가 동시에 보호됨.

① BS 의 전송 신호 : (MS 의 전송 신호 + jamming sequence)에 의해 보호됨.

② MS 의 전송 신호 : (BS 의 전송 신호 + jamming sequence)에 의해 보호됨.

나. Traffic asymmetry 에 의한 data 전송률 저하 → Secrecy 향상

1) 상, 하향 링크 간 traffic asymmetry 는 순시적인 사용자 traffic 요구량에 의해 결정되는 것이므 로 이로 인한 자원 낭비 및 data 전송률 저하 문제를 기존의 동일대역 동시 송수신 시스템에서는 해결할 수 없음.

2) 본 제안 기술은 traffic asymmetry 에 의해 낭비되는 자원을 이용해 jamming 신호를 전송하는 기술로, PLS 를 위한 추가적인 자원소모 없이 양 방향 모두에 대한 보안성을 향상시키는 기술임.

3) 특히, 삽입된 jamming 신호에 대한 sequence 및 pattern 를 통한 2 중 보안 키 기술을 통해 (DL 전송 신호 + jamming 신호)와 (UL 전송 신호 + jamming 신호) 사이의 independence 를 확보함 으로써 양방향 전송 모두에 대한 보안성을 향상 시킬 수 있음.

다. 보안 – 데이터 전송간의 trade-off 극복

1) 기존의 PLS 기법은 각 방향의 정보 전송 링크에서 각각 주어진 자원의 일부를 PLS 를 위한 encoding 을 위해 사용하므로, 수식 (2)에서 $L_D > 0$ 이고 $L_U > 0$ 이 되어 보안-정보 전송 간 trade-off 에서 자유로울 수 없음.

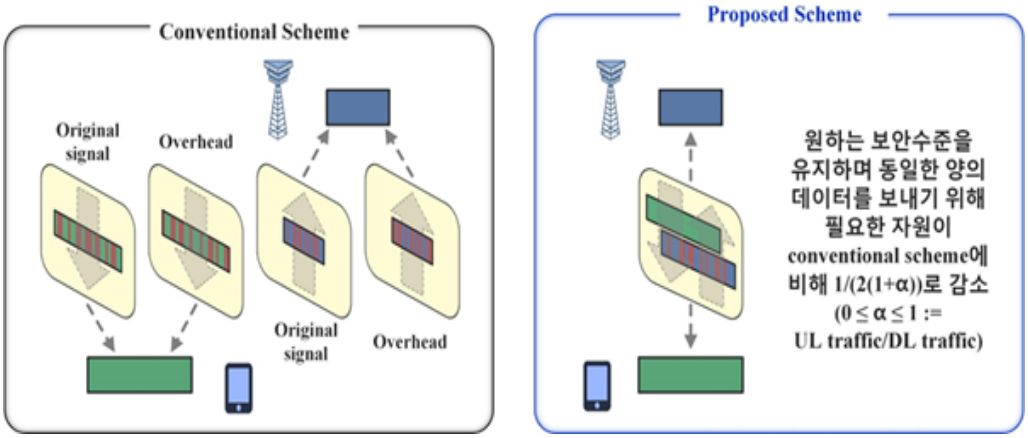
2) 특히, 양방향의 정보 전송을 모두 보호하기 위해서는 각각의 링크에서 별도

의 PLS overhead 를 사 용해야 하므로 시스템 전체의 PLS overhead 증가하며, 이로 인해 보안-정보 전송 간 trade-off 가 더욱 악화됨.

3) 반면, 제안된 PLS 기법은 주어진 자원 이외에 추가적인 자원을 PLS 를 위해 사용하지 않을 뿐 아니라 (DL 전송 신호 + jamming 신호)와 (UL 전송 신호 + jamming 신호) 사이의 independence 를 기반으로 하므로 수식 (2)에서 $L_D = 0$ 이고 $L_U = 0$ 이 되어 trade-off 를 극복할 수 있음.

라. 데이터 전송률 (secrecy capacity)의 향상

1) 제안된 PLS 시스템에서는 BS 와 MS 모두 주어진 자원을 전부 활용하여 정보를 전송하므로 $w_D = 1$ 과 $w_U = 1$ 이 동시에 달성되므로, 기존 PLS 시스템에서 발생했던 secrecy capacity 의 저하 문제 해결.



<그림 7> 제안된 ST-jamming 에 의한 데이터 전송률 증가 개념도

2) 또한, $L_D = 0$ 이고 $L_U = 0$ 으로 인한 보안-정보 전송 간 trade-off 극복 효과와 합쳐져 secrecy capacity 의 획기적인 증가로 이어짐.

3) 양방향 통신 환경에서 상, 하향링크간 traffic 의 비율을 α 라 할 때, <그림

7>에서 볼 수 있듯이 기존의 PLS 기법 대비 $2\times(1+\alpha)$ 데이터 전송률을 얻을 수 있음 (예를 들어, $\alpha = 0.5$ 인 경우 기존의 PLS 기법 대비 3 배의 데이터 전송률을 얻을 수 있음).

4) 즉, 물리계층에서의 보안 확보라는 제약 조건을 만족시키기 위해 동일 대역에서 신호의 동시 송 수신 기술의 태생적인 성질을 활용함으로써 일반적인 신호의 동일 대역 동시 송수신 기술의 capacity 증가 한계인 2 배까지도 넘어서는 성능 향상을 얻을 수 있음.

5) 반면, 기존의 PLS 시스템에서는 보안과 정보전송 사이의 trade-off 와 양방향 통신 환경에서의 overhead 증가와 더불어, 양 방향의 정보 전송이 서로 다른 자원을 점유, 즉, 수식 (2)에서 $w_D < 1$ 이고 $w_U < 1$ 이므로 의한 secrecy capacity 감소가 발생함.

3절. 연구 목표, 내용 및 범위

1. 최종 연구 목표

가. 동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발: 본 세부목표는 수식 (2)에서 $w_D = 1$ 과 $w_U = 1$ 을 동시에 달성함으로써 전송 신호 자체를 보안키로 활용하기 위한 전송 기술을 개발하는 것을 목표로 함.

1) 양방향 PLS 통신을 위한 동일대역 동시 송수신 장치 설계

① 양방향 PLS 통신을 위한 동일대역 동시 송수신 HW transceiver 설계

② 양방향 PLS 통신 SW 모뎀 설계

2) 양방향 PLS 전송 기술 개발 및 전송 시스템 설계

① 양방향 PLS 통신 시스템 구조 설계

② 양방향 PLS 통신 프레임 구조, 프로토콜, control signal 설계

3) 보안키 삽입 기술 개발: 주어진 상, 하향링크 traffic 과 jamming sequence/pattern 에 의해 생성된 2 중 보안키에 대해 secrecy capacity 를 최대화 하는 jamming 신호 삽입 기술 연구

나. 양방향 PLS 통신을 위한 보안키 설계 연구: 본 세부목표는 동일대역 동시 송수신 시스템의 traffic asymmetry 에 의해 사용되지 않는 자원에 삽입할 jamming 신호를 설계하는 것으로, 수식 (2)에서 $L_D = 0$ 과 $L_U = 0$ 을 동시에 만족하는 jamming 신호의 설계를 목표로 함.

1) X-independence 를 위한 최적의 jamming sequence 및 pattern 설계 연구

① (DL 데이터 + jamming 신호)와 UL 데이터간 independence 달성(즉, $L_D = 0$)을 위한 jamming sequence 및 pattern 설계

② (UL 데이터 + jamming 신호)와 DL 데이터간 independence 달성(즉, $L_U = 0$)을 위한 jamming sequence 및 pattern 설계

③ $L_D = 0$ 과 $L_U = 0$ 을 동시에 달성하기 위한 jamming sequence 및 pattern 설계 및 최적화

2) Jamming sequence 와 pattern 을 통한 2 중 보안키 설계 연구

① Jamming sequence 에 대한 codebook 설계 연구

② Jamming pattern 에 대한 codebook 설계 연구

다. 양방향 PLS 시스템 최적화 연구: 본 세부목표는, 동일대역 동시 송수신 기반 양방향 PLS 전송 기술 연구와 양방향 PLS 통신을 위 한 보안키 설계 연구의 결과를 기반으로 동일대역 동시 송수신 기반 양방향 PLS 시스템의 성

능을 최적화하기 위한 알고리즘을 개발하는 것을 목표로 함.

1) Jamming 신호 삽입 기술의 최적화: 상, 하향링크의 traffic, jamming sequence/pattern, 양방향 PLS 프로토콜 및 프레임 구조의 joint optimization
2) 자원 할당 최적화 기술 연구: 상, 하향링크 data 전송 신호, jamming 신호, traffic feedback 및 2 중 보안키 교환을 위한 control signal 사이의 최적화된 자원 할당 기술 연구

라. 양방향 PLS 통신 시스템 성능 분석 연구: 본 세부목표는, 단일/다중사용자 환경 제안된 동일대역 동시 송수신 기반 양방향 PLS 전송기술의 성능을 이론적으로 분석하는 것을 목표로 함.

1) 단일사용자 환경 제안된 동일대역 동시 송수신 기반 양방향 PLS 전송기술의 성능 분석
2) 다중사용자 환경 제안된 동일대역 동시 송수신 기반 양방향 PLS 전송기술의 성능 분석

마. 양방향 PLS 통신 시스템 성능 검증 플랫폼 개발: 본 세부목표는, 제안된 양방향 PLS 전송 기술, 전송신호 설계 기술, 그리고 양방향 PLS 시스템의 최적화 기술의 유효성을 검증하기 위한 성능 검증 플랫폼을 개발하는 것을 목표로 함.

1) 성능검증 플랫폼을 위한 HW/SW 인터페이스 개발
2) 동일대역 동시 송수신을 위한 HW transceiver 및 SW 모뎀 개발
3) 양방향 PLS 통신 기능 구현
4) 양방향 PLS 통신 시스템의 최적화 알고리즘 구현 및 테스트

구 분	내 용
최종목표	Overhead 없이 양방향 통신 모두에 대해 perfect secrecy를 동시에 달성하는 물리계층 보안통신 기술
세부목표	·동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발 ·양방향 PLS 통신을 위한 보안키 설계 연구 ·양방향 PLS 통신 시스템 최적화 연구 ·양방향 PLS 통신 시스템 성능분석 연구 ·양방향 PLS 통신 시스템 성능검증 플랫폼 개발

최종 결과물	
동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발	- 동일대역 동시 송수신 기반 양방향 PLS 통신 시스템 설계서 - 양방향 PLS 통신시스템 성능 검증 시뮬레이터 - 양방향 PLS 통신 시스템 시뮬레이션 성능 분석서 - 국제 특허 1 건 - 국내 특허 1 건
양방향 PLS 통신을 위한 보안키 설계 연구	- Jamming sequence/pattern 생성 알고리즘 - Jamming sequence/pattern 을 이용한 2 중 보안키 생성 기술 - 보안키 생성 및 삽입 알고리즘 제안서 - 국내 특허 1 건
양방향 보안 통신 시스템 최적화 연구	- 양방향 PLS 통신 시스템의 자원할당/최적화 알고리즘 - 양방향 PLS 통신 시스템의 자원할당/최적화 알고리즘 제안서 - 국제 특허 1 건 - 국내 특허 2 건
양방향 보안통신 시스템성능 분석 연구	- SCI 논문 2 편
양방향 보안통신 성능 검증 플랫폼 개발	- 동일대역 동시 송수신 기반 양방향 PLS 성능 검증 플랫폼 - 양방향 PLS 통신 성능 시험서

2. 연차별 연구 목표 및 내용

구 분	목 표	내 용
1 차년도 (2018)	동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발	- 양방향 PLS 통신을 위한 동일대역 동시 송수신 장치 설계 - 양방향 PLS 전송 기술 개발 및 전송 시스템 설계 - 보안키 삽입 기술 개발
	양방향 PLS 통신을 위한 보안키 설계	- X-independence 를 위한 최적의 jamming sequence 및 pattern 설계 연구 - Jamming sequence 와 pattern 을 통한 2 중 보안키 설계 연구
	양방향 보안통신 시스템 성능 분석	- 단일사용자 환경에서 제안된 동일대역 동시 송수신 기반 양방향 PLS 전송기술의 성능 분석
	양방향 보안통신 성능 검증 플랫폼 개발	- 성능검증 플랫폼을 위한 HW/SW 인터페이스 개발
2 차년도 (2019)	양방향 보안 통신 시스템 최적화	- Jamming 신호 삽입 기술의 최적화 - 자원 할당 최적화 기술 연구
	양방향 보안통신 시스템 성능 분석	- 다중사용자 환경에서 제안된 동일대역 동시 송수신 기반 양방향 PLS 전송기술의 성능 분석
	양방향 보안통신 성능 검증 플랫폼 개발	- 동일대역 동시 송수신을 위한 HW transceiver 및 SW 모뎀 개발/구현 - 양방향 PLS 통신 기능 구현 - 양방향 PLS 통신 시스템의 최적화 알고리즘 구현 및 테스트

3. 당해연도(2018 년도) 연구 목표 및 내용

가. 연구 개발 목표

연구 목표	상세 목표
동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발	- $w_D = 1$ 과 $w_U = 1$ 을 동시에 달성하는 동일대역 동시 송수신 장치 설계 - 양방향 PLS 전송 기술 개발 및 전송 시스템 설계와 $w_D = w_U = 1$ 의 유효성 검증 - 보안키 삽입 기술 개발 및 보안키 삽입 후 $w_D = w_U = 1$ 과 $L_D = L_U = 0$ 의 동시 달성 검증
양방향 PLS 통신을 위한 보안키 설계 연구	- $L_D = 0$ 과 $L_U = 0$ 을 동시에 달성하는 jamming sequence/pattern 설계 - $L_D = 0$ 과 $L_U = 0$ 의 동시 달성에 대한 이론적 검증. - Jamming sequence 와 pattern 을 통한 2 중 보안키 설계 도출
양방향 PLS 시스템 성능 분석 연구	- 단일사용자 환경에서 양방향 PLS 전송기술의 성능 분석
양방향 PLS 통신 시스템 성능검증 플랫폼 개발	- HW/SW 인터페이스 개발

나. 연구 개발 내용

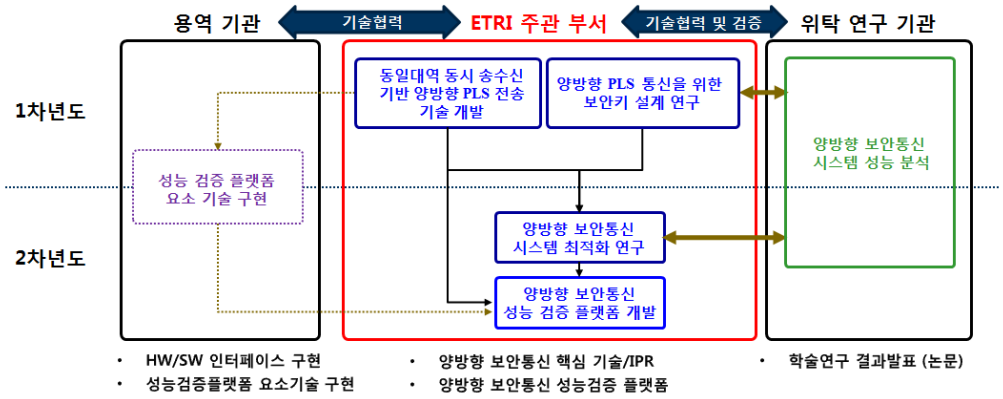
연구 목표	항목	내용	수행 기관
동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발	양방향 PLS 통신을 위한 동일대역 동시 송수신장치 설계	- 양방향 PLS 통신을 위한 동일대역 동시 송수기 HW 설계 - 양방향 PLS 통신 SW 모뎀 설계	ETRI

	양방향 PLS 전송기술 개발 및 전송 시스템 설계	- 양방향 PLS 통신 시스템 구조 설계 . 동일대역 동시 송수신기의 구조 설계 . RF 혹은 아날로그 signal processing 과 연계된 SI 제거 기능 모듈 구조 설계 . 효율적인 SI 제거를 통한 $w_D = 1$ 과 $w_U = 1$ 의 동시달성의 시뮬레이션 검증 - 양방향 PLS 통신 프레임 구조 설계 . SI training 및 데이터 신호와 jamming 신호를 포함하는 자체 규격 프레임 구조의 설계 . 설계 프레임 구조에 대해 $w_D = w_U = 1$ 의 유효성 검증 - 양방향 PLS 통신 프로토콜 및 control signal 설계 . 상, 하향링크의 traffic feedback (혹은 교환)을 위한 프로토콜 및 control signal 설계 . Jamming sequence 및 pattern 의 공유 프로토콜 및 control signal 설계	
	보안키 삽입 기술 개발	- Multi-carrier 전송 시스템의 시간 및 주파수 영역에서 최적의 jamming 신호 삽입 기술 개발 - Jamming 신호 삽입 후 $w_D = w_U = 1$ 과 $L_D = L_U = 0$ 의 동시 달성에 대한 이론적 검증 및 simulation 검증.	
양방향 PLS 통신을 위한 보안키 설계 연구	jamming sequence 및 pattern 설계 연구	- 정보이론 관점에서 $L_D = 0$ 과 $L_U = 0$ 을 동시에 달성하기 위해 최적화된 jamming sequence 및 pattern 도출 - 도출된 jamming sequence/pattern 의 $L_D = 0$ 과 $L_U = 0$ 의 동시 달성에 대한 이론적 검증. - 다양한 제약 요인에 대해 도출된 jamming sequence/pattern 유효성 시뮬레이션 성능 검증	ETRI
	2 중 보안키 설계 연구	도출된 jamming sequence/pattern 기반 2 중 보안키 설계 - 구 - 2 중 보안키 사용에 따른 도청자의 도청 성능 시뮬레이션	
양방향 PLS 시스템 성능 분석 연구	양방향 PLS 전송기술의 성능 분석	- 단일사용자 환경 제안된 동일대역 동시 송수신 기반 양방향 PLS 전송기술의 성능 분석 - ETRI 자체 연구와 위탁 연구를 통해 수행 - 학술 연구 형태로 진행될 계획이며 연구 결과를 SCI 논문 형태로 발표하는 것을 목표로 함	ETRI, 위탁 연구
양방향 PLS 통신시스템 성능검증 플랫폼 개발	HW/SW 인터페이스 개발	- 2 차년도 동일대역 동시 송수신기 및 양방향 PLS 성능검증 플랫폼 구현을 위한 HW/SW 인터페이스의 개발 - 용역 연구를 통해 수행 예정 (용역기관 미정)	용역 기관

4절. 연구개발 체계 및 방법

1. 총년도 연구개발 체계 및 방법

가. 연구개발 추진 체계



<그림 8> 총년도 연구개발 추진 체계

1) ETRI

① 본 연구과제 수행에 있어서 양방향 PLS 통신 시스템의 핵심 기술 개발 및 연구를 담당함

i. 동일대역 동시 송수신 기반 양방향 PLS 통신을 위한 핵심 기술 개발

ii. 동일대역 동시 송수신 기반 양방향 PLS 통신 시스템 설계 및 최적화

iii. 동일대역 동시 송수신 기반 양방향 PLS 통신 성능 검증 플랫폼 개발/구현

iv. 제안된 동일대역 동시 송수신 기반 양방향 PLS 통신의 유효성 증명 및 성능 검증 연구

② 위탁 연구기관과의 협력 체계

i. 단일 사용자 환경에서 동일대역 동시 송수신 기반 양방향 PLS 통신의 성능 분석을 위해 위 탁 연구기관과 연계하여 과제 수행 (1 차년도)

ii. 다중 사용자 환경에서 동일대역 동시 송수신 기반 양방향 PLS 통신의 성능 분석을 위해 위 탁 연구기관과 연계하여 과제 수행 (2 차년도)

③ 외부 용역기관과의 협력 체계

i. 동일대역 동시 송수신 기반 양방향 PLS 통신 성능 검증 플랫폼 개발/구현을 위한 SW/HW 인터페이스 개발에 있어 외부 용역기관과 연계하여 과제 수행 (1 차년도)

ii. 동일대역 동시 송수신 HW transceiver 혹은 SW modem 구현에 있어 일부 요소 기술 개발 을 외부 용역기관과 연계하여 과제 수행 (2 차년도)

2) 위탁 연구 기관

① 본 연구 과제 수행에 있어서 양방향 PLS 통신 시스템의 성능 분석에 대한 학술적 연구를 담당함

② 제안된 양방향 PLS 통신의 이론적인 성능을 point-to-point(단일 사용자) 통신 환경과 다중 사용자 네트워크 환경에서 분석.

③ 양방향 PLS 통신에 대한 핵심 기술 개발에는 주도적으로 참여하지 않음.

3) 외부 용역 기관

① 1 차년도 과제 수행에 있어서 동일대역 동시 송수신 기반 양방향 PLS 통신 성능 검증 플랫폼 개발/구현을 위한 SW/HW 인터페이스 개발을 담당함

② 2 차년도 과제 수행에 있어서 동일대역 동시 송수신 HW transceiver 혹은 SW modem 의 일부 요소 기술 구현을 담당할 수 있음.

나. 연구 개발 방법

연구 목표	항목	연구 방법
동일대역 동시 송수신 기반 양방향 PLS 전송 기술 개발 (1 차년도)	양방향 PLS 통신을 위한 동일대역 동시 송수신장치 설계	- FPGA 레벨에서 실시간 SI 제거를 위한 동일대역 동시 송수신 HW transceiver 설계 - 실시간 데이터 전송기능을 갖춘 양방향 PLS 통신 동일대역 동시 송수신 SW 모뎀 설계 - 시뮬레이션을 통한 $w_D = 1$ 과 $w_U = 1$ 의 동시달성 및 유효 신호의 decodability 검증 - 2 차년도 동일대역 동시 송수신 장치 구현 및 양방향 PLS 통신 시스템 성능 검증 플랫폼 개발에 연계됨
	양방향 PLS 전송기술 개발 및 전송 시스템 설계	- 양방향 PLS 통신 시스템 구조 설계 · RF, 아날로그, 디지털 영역의 인터페이스 정의 · RF, 아날로그, 디지털 영역의 연동 동작 정의 · 동일대역 동시 송수신을 위한 HW transceiver 와 양방향 PLS 통신 SW 모뎀의 인터페이스 정의 · 양방향 PLS 시스템 구조 설계는 양방향 PLS 통신 프레임 구조, protocol 및 control signal 구조 설계와 연계됨 - 양방향 PLS 통신 프레임 구조, 프로토콜 및 control signal 설계 · Jamming sequence 및 pattern 설계 연구 결과 도출된 jamming sequence 및 pattern 을 반영하여 프레임 구조, 프로토콜 및 control signal 설계 · 양방향 PLS 통신을 위한 SW 모뎀 설계와 연동됨

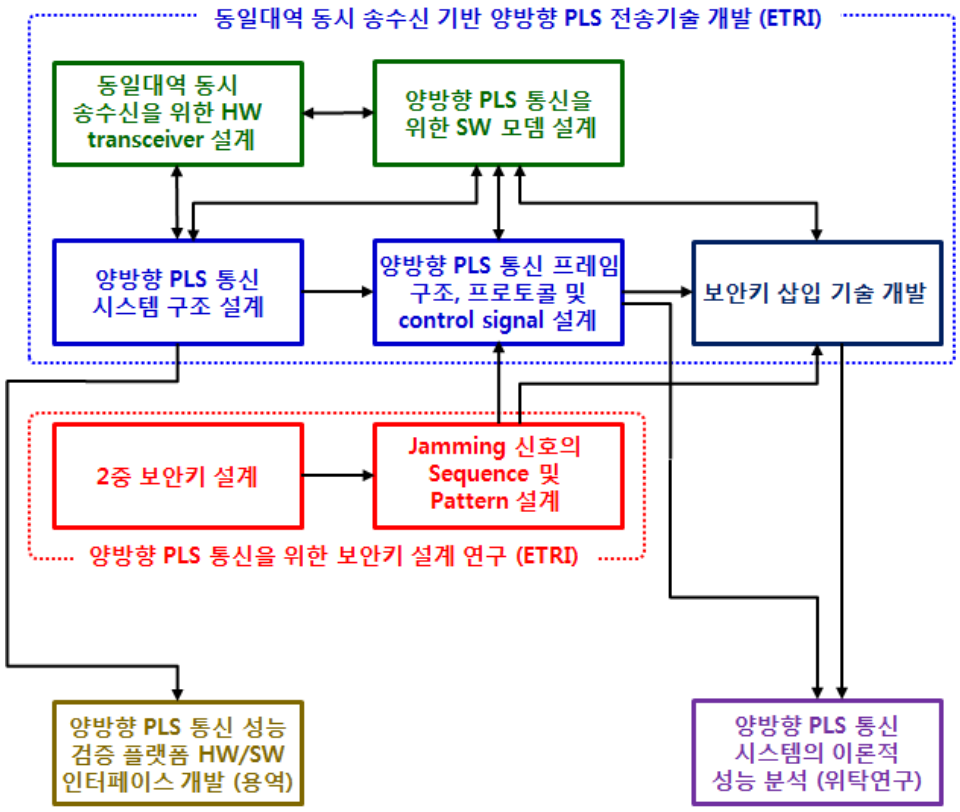
		· 시뮬레이션을 통해 설계된 프레임 구조, 프로토콜, control signal 에 대한 $w_D = w_U = 1$ 의 유효성 검증 · 양방향 PLS 통신 프레임 구조, 프로토콜 및 control signal 설계 → 보안키 삽입 기술 개발로 연계됨
	보안키 삽입 기술 개발 및 유효성 검증	- Multi-carrier 전송 시스템에서 2 중 보안키에 대해 보안키 삽입 기술 개발 - 양방향 PLS 통신 프레임 구조, 프로토콜 및 control signal 설계와 2 중 보안키 설계 연구 결과를 기반으로 함 - 시뮬레이션을 통해 Jamming 신호 삽입 후 $w_D = w_U = 1$ 과 $L_D = L_U = 0$ 동시 달성의 검증 - 양방향 PLS 통신 SW 모뎀 설계와 연동됨
양방향 PLS 통신을 위한 보안키 설계 연구 (1 차년도)	Jamming sequence 및 pattern 설계 연구	- $L_D = L_U = 0$ 동시 달성을 위해 상, 하향링크의 데이터 전송 신호의 통계적 특성을 기반으로 상, 하향링크의 데이터 전송 신호와 통계적 특성이 동일한 jamming 신호 sequence 도출 - Jamming 신호의 sequence/pattern 설계 → 2 중 보안키 설계의 연계를 가짐.
	2 중 보안키 설계 연구	- 기 도출된 jamming sequence 및 pattern 을 기반으로 정보이론 관점에서 최적의 2 중 보안키 codebook 설계 - 2 중 보안키 codebook 설계 → 보안키 삽입 기술 개발/ 양방향 PLS 통신을 위한 프로토콜 및 control signal 설계 → 양방향 PLS 통신 시스템 SW 모뎀 설계의 연계를 가짐.

연구 목표	항목	연구 방법
양방향 PLS 통신 시스템 최적화 연구 (2 차년도)	자원할당 최적화 알고리즘 개발	- Data traffic, jamming 신호, control signal 사이의 자원 할당에 대한 최적화 문제 formulation - 상기 최적화 문제에 대한 수학적인 optimal solution 을 도출하고 이를 기반으로 자원 할당 최적화 알고리즘 도출 (단, optimal solution 도출이 불가능하거나 이를 위한 complexity 가 매우 높을 경우에는 sub-optimal solution 도출 - 양방향 PLS 통신 프레임 구조, 프로토콜 및 control signal 설계를 기반으로 함

	자원할당 최적화 기술 유효성 검증	- 도출된 자원할당 최적화 알고리즘에 대해 양방향 PLS 통신 시스템에 대한 system level 시뮬레이션을 통해 유효성 검증 - 수행 및 성능 검증을 수행하되, 본 과제의 핵심 요소는 아니나 시뮬레이터 구현에 자원 투자를 많이 해야 하는 요소(예를 들면 channel coding/decoding)의 경우에는 MATLAT Simululink tool 을 사용할 수 있음.
양방향 PLS 시스템 성능 분석 연구 (1-2 차년도)	단일/다중사용자 환경에서 양방향 PLS 전송기술의 성능 분석	- 단일/다중 사용자 환경에서 동일대역 동시 송수신 기반 양방향 PLS 통신 시스템의 성능을 수학적 모델과 시뮬레이션을 통해 분석 - ETRI 와 위탁 연구기관에서 공동으로 수행 - 단일 사용자 환경에서 동일대역 동시 송수신 기반 양방향 PLS 통신 시스템의 성능 분석 연구의 경우 정보이론 관점에서의 성능 분석과 함께 link level simulation 을 활용 (1 차년도) - 다중 사용자 환경에서 동일대역 동시 송수신 기반 양방향 PLS 통신 시스템의 성능 분석 연구의 경우 Stochastic geometry 모델을 활용 (2 차년도)
양방향 PLS 통신시스템 성능검증 플랫폼 개발 (1-2 차년도)	HW/SW 인터페이스, 동일대역 동시 송수신기, 양방향 PLS 구현 및 최적화	- National Instrument 사의 FPGA module 및 LabView Communication System Design Suite tool 과 현재 개발 중인 RF/analog 및 디지털 FPGA 모듈을 이용하여 양방향 PLS 통신 시스템의 성능 검증 플랫폼 개발 - 양방향 PLS 통신 시스템의 성능 검증 플랫폼 개발에 있어서 HW/SW 인터페이스 개발은 외부 용역을 통해 수행 (1 차년도) - 동일대역 동시 송수신기 구현 (HW transceiver 와 SW 모뎀) → 양방향 PLS 통신을 위한 프로토콜, 제어신호, 보안키 삽입 기술 구현 → 자원할당 최적화 기술 구현 → 테스트의 순서로 개발 진행 - 양방향 PLS 를 위한 SW 모뎀 개발에 있어서, 본 과제의 핵심 요소는 아니나 HW PLS 송수신 장치와 SW 모뎀의 구현에 있어서 이 연구개발과제의 핵심 사항은 아니나 구현에 필요한 주변 요소 기술의 경우 용역 기관이 분담하여 수행할 수 있음 (2 차년도) - 그 외 SW 모뎀 구현에 있어서 일부 요소 기술의 구현에 MATLAB Simululink 를 활용할 수 있음 (2 차년도)

2. 당해연도 (2018 년도) 연구개발 체계 및 방법

가. 연구개발 추진 체계



<그림 9> 당해연도 연구개발 추진 체계

1) ETRI

① 본 연구과제 수행에 있어서 양방향 PLS 통신 시스템의 핵심 기술 개발 및 연구를 담당함.

i. 동일대역 동시 송수신 기반 양방향 PLS 통신을 위한 핵심 기술 개발

ii. 제안된 동일대역 동시 송수신 기반 양방향 PLS 통신의 유효성 증명 및 성능 검증 연구

iii. 동일대역 동시 송수신 기반 양방향 PLS 통신 성능 검증 플랫폼 개발/구현

② 위탁 연구기관과의 협력 체계: 단일 사용자 환경에서 동일대역 동시 송수신 기반 양방향 PLS 통신의 성능 분석을 위해 위 탁 연구기관과 연계하여 과제 수행

③ 외부 용역기관과의 협력 체계: 동일대역 동시 송수신 기반 양방향 PLS 통신 성능 검증 플랫폼 개발/구현을 위한 SW/HW 인터페이스 개발에 있어 외부 용역기관과 연계하여 과제 수행 (1 차년도)

2) 위탁 연구 기관

① 본 연구 과제 수행에 있어서 양방향 PLS 통신 시스템의 성능 분석에 대한 학술적 연구를 담당함

② 제안된 양방향 PLS 통신의 이론적인 성능을 단일 사용자 네트워크 환경(point-to-point 통신 환경)과 다중사용자 네트워크 환경에서 분석

3) 외부 용역 기관: 동일대역 동시 송수신 기반 양방향 PLS 통신 성능 검증 플랫폼 개발/구현을 위한 SW/HW 인 터페이스 개발을 담당함

나. 연구개발 방법

연구 목표	항목	연구 방법
동일대역 동시 송수신 기반	양방향 PLS 통신을 위한 동일대역 동시 송수신장치	- 동일대역 동시 송수신을 위한 SI 제거에 필요한 신호 구조(training 신호 등)가 HW transceiver 송수신기 설계 과정에서 먼저 정의된 후, 이를 반영하여 SW 모뎀을 설계함

양방향 PLS 전송 기술 개발	설계	- 양방향 PLS 통신을 위한 SW 모뎀의 설계에 있어서, 양방향 PLS 통신을 위한 프레임 구조, 프로토콜 및 control 신호의 설계와 보안키 삽입 알고리즘이 순차적으로 반영됨 - Link level 시뮬레이션을 통한 $w_D=1$ 과 $w_U=1$ 의 동시달성 및 유효 신호의 decodability 검증 - 2 차년도 동일대역 동시 송수신 장치 구현 및 양방향 PLS 통신 시스템 성능 검증 플랫폼 개발에 연계됨
	양방향 PLS 전송기술 개발 및 전송 시스템 설계	- 양방향 PLS 통신 시스템 구조 설계 · 양방향 PLS 시스템 구조 설계는 동일대역 동시 송수신기의 구조 설계 및 양방향 PLS 통신 SW 모뎀 설계와 연동되어 진행됨. · 양방향 PLS 통신 시스템 구조 설계에 있어서 RF, 아날로그, 디지털 영역의 인터페이스 정의는 동일대역 동시 송수신을 위한 HW transceiver 송수신기 설계와 연동되어 진행됨 · 동일대역 동시 송수신을 위한 HW transceiver 와 양방향 PLS 통신 SW 모뎀의 인터페이스 정의는 양방향 PLS 통신 SW 모뎀 설계의 PHY 및 MAC layer 설계를 기반으로 하며, 양방향 PLS 통신시스템 성능검증 플랫폼 개발을 위한 HW/SW 인터페이스 개발(외부용역)로 연계됨 · 양방향 PLS 시스템 구조 설계는 양방향 PLS 통신 프레임 구조, protocol 및 control signal 구조 설계와 연계됨 - 양방향 PLS 통신 프레임 구조, 프로토콜 및 control signal 설계 · SI training 및 데이터 신호와 jamming 신호를 포함하는 자체 규격 프레임 구조의 설계 · 상, 하향링크의 traffic feedback (혹은 교환) 및 Jamming sequence / pattern 의 공유를 위한 절차와 control signal 정의 · 자체 규격 프레임 구조와 정의된 control signal 및 절차를 SW 모뎀상에 정의된 프로토콜과 병합하여 양방향 PLS 통신 프로토콜 설계

		· Link level simulation 을 통해 설계된 프레임 구조, 프로토콜, control signal 에 대한 $w_D = w_U = 1$ 의 유효성 검증
	보안키 삽입 기술 개발 및 유효성 검증	- 양방향 PLS 통신 프레임 구조, 프로토콜 및 control signal 설계와 2 중 보안키 설계 연구 결과를 기반으로, multi-carrier 전송 시스템에서 주어진 상, 하향링크 traffic 과 2 중 보안키에 대해 보안키 삽입 방법에 의한 secrecy capacity 최적화 문제 formulation 및 solution 도출 - 도출된 solution 을 기반으로 시간 영역, 주파수 영역, 혹은 시간과 주파수 영역에서 최적의 jamming 신호 삽입 알고리즘 개발 - Link level simulation 을 통한 Jamming 신호 삽입 후 $w_D = w_U = 1$ 과 $L_D = L_U = 0$ 동시 달성의 검증. - System level simulation 을 통한 도청자의 유효신호 decoding 불가 검증 - 양방향 PLS 통신 SW 모뎀 설계와 연동되며, 보안키 삽입 기술 개발의 결과가 양방향 PLS 통신 SW 모뎀의 최종 설계에 반영됨

연구 목표	항목	연구 방법
양방향 PLS 통신을 위한 보안키 설계 연구	Jamming sequence 및 pattern 설계 연구	- 상, 하향링크의 데이터 전송 신호의 통계적 특성에 대한 수학적 분석 - 상, 하향링크의 데이터 전송 신호와 통계적 특성이 동일한 jamming 신호 sequence 도출 - Jamming pattern 별 상, 하향링크의 데이터 전송 신호 및 jamming 신호의 통계적 특성에 대 한 수학적 분석 및 통계적으로 최적의 pattern 도출 - (상향링크 데이터 전송신호 + jamming 신호)와 하향링크 데이터 전송 신호간 통계적 independence 에 대한 수학적 증명 - 다양한 환경 변수의 변화에 따른 (상향링크 데이터 전송신호 + jamming 신호)와 하향링크 데이터 전송 신호간 통계적 independence 의 시뮬레이션 성능 검증 - Jamming 신호의 sequence/pattern 설계 → 2 중 보안키 설계의 연계를 가짐.

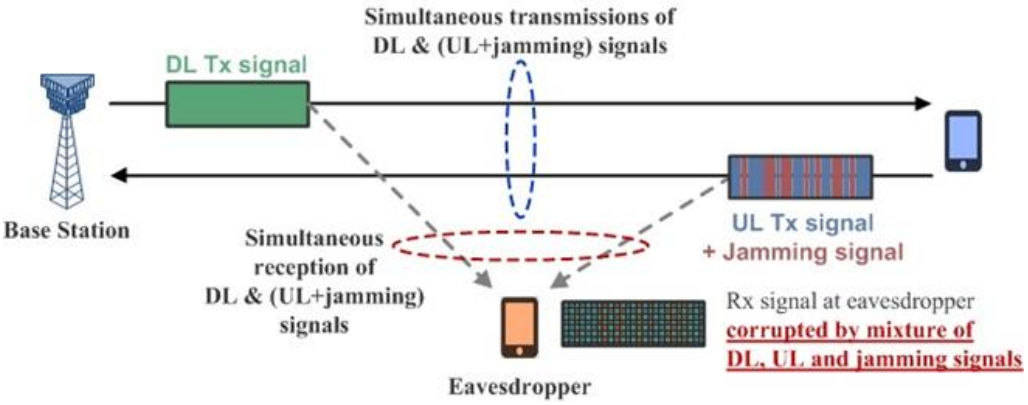
	2 중 보안키 설계 연구	- 정보이론 관점에서 jamming sequence 및 pattern 에 대한 codebook 설계를 위한 최적화 문제 formulation 및 수학적 solution 도출 (단, 2 중 보안키 codebook 설계에 대한 optimal solution 의 복잡도가 과하게 클 경우 sub-optimal solution 도출) - System level simulation 을 통한 도출된 2 중 보안키 codebook 의 유효성 검증 - Jamming 신호의 sequence/pattern 설계 → 2 중 보안키 설계의 연계를 가짐.
양방향 PLS 시스템 성능 분석 연구	단일/다중 사용자 환경에서 양방향 PLS 전송기술의 성능 분석	- ETRI 와 위탁 연구 기관에서 공동으로 수행하며, 학술 연구 형태로 진행함으로써 연구 결과를 SCI 논문 형태로 발표하는 것을 목표로 함. - ETRI 에서 개발한 양방향 PLS 통신의 jamming sequence/pattern, jamming 신호삽입 기술을 기반으로 point-to-point 및 다중사용자 통신 환경에서 양방향 PLS 통신 시스템의 성능을 이론적으로 분석
양방향 PLS 통신시스템 성능검증 플랫폼 개발	HW/SW 인터페이스 개발	- National Instrument 사의 FPGA module 및 LabView Communication System Design Suite tool 혹은 현재 개발 중인 RF/analog 및 디지털 FPGA 모듈을 기반으로 하는 HW/SW 인터페이스 개발

5절. 연구 결과의 세부 내용

1. Simultaneously-Transmitted Jamming 기술의 개발

가. Simultaneously-Transmitted Jamming 기술 개요

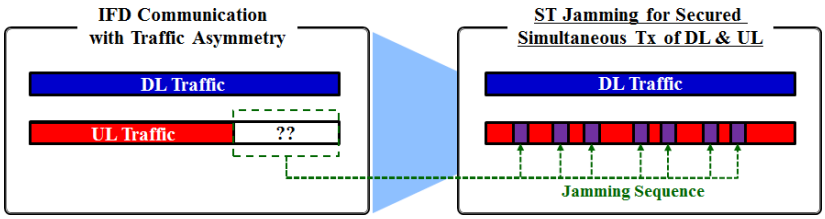
<그림 10>은 본 연구 과제에서 다루는 양방향 보안통신 시스템을 보여준다. 이 시스템은 IFD 방식으로 동작하는 BS 와 역시 IFD 방식으로 동작하는 MS 로 구성되며, 또한 BS 와 MS 가 통신을 할 때 이를 도청하고자 하는 Eve 가 존재한다. 이 때 BS 와 MS 는 모두 OFDM 등의 다중 반송파 신호를 이용해 서로에게 데이터 정보를 전송하며, 이 때 BS 와 MS 가 전송하고자 하는 traffic 의 양은 서로 다를 수 있음을 가정한다.



<그림 10> IFD 기반 물리계층 보안 통신 시스템 모델

이 시스템에서는 기지국과 단말이 동시에 신호를 동일한 대역에서 동시에 송수신하기 때문에, 상, 하향링크의 데이터 전송률이 향상될 수 있다. 또한, 도청자의 수신 신호에는 기지국과 단말의 송신신호가 섞여 있으므로 기지국과 단말의 송신신호가 서로에 대한 jammer 로 작용하여 서로를 보호하게 된다. 특히, traffic 이 적은 링크(<그림 10>의 경우 UL)에서 남는 자원을 이용해 추가적인 jamming 신호(혹은 artificial noise)를 전송함으로써 보안성을 향상시키게 된다.

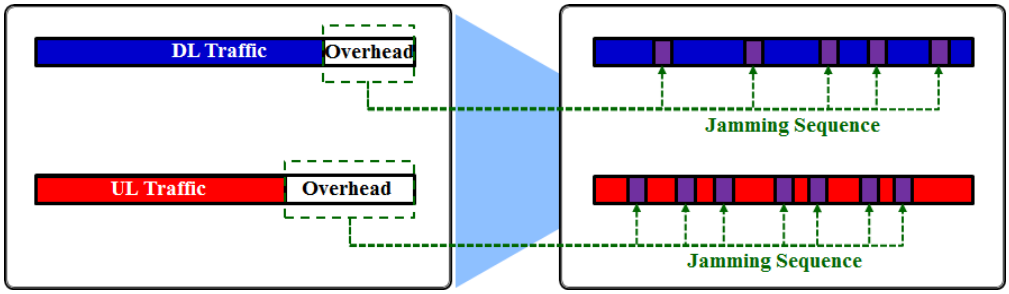
<그림 11>은 상, 하향 링크의 traffic 이 다른 경우, traffic 이 작은 링크(<그림 10>의 경우에는 UL)의 자원을 이용해 jamming sequence 를 삽입하는 일례를 보여준다. 이 방식은 하향링크의 traffic 이 상향링크의 traffic 보다 더 큰 일반적인 경우에 적용 가능하다. 이 그림에서 볼 수 있듯이, traffic 비대칭성에 의해 UL 에서 남는 resource 에 맞춰 pseudo random jamming sequence 를 생성한 후, 역시 pseudo random 하게 정해져 있는 pattern 에 따라 UL 데이터와 섞어줌으로써 MS 의 UL 전송 신호를 생성한다. 본 방식은 하향링크의 traffic 이 상향링크의 traffic 보다 작은 경우에도 동일하게 적용할 수 있다.



<그림 11> Traffic 비대칭과 재밍을 이용한 물리계층 보안 (1)

<그림 11>은 상, 하향 링크의 traffic 이 다른 경우, traffic 이 작은 링크(<그림 11>의 경우에는 UL)의 자원을 이용해 jamming sequence 를 삽입하는 일례를 보여준다. 이 방식은 하향링크의 traffic 이 상향링크의 traffic 보다 더 큰 일반적인 경우에 적용 가능하다. 이 그림에서 볼 수 있듯이, traffic 비대칭성에 의해 UL 에서 남는 resource 에 맞춰 pseudo random jamming sequence 를 생성한 후, 역시 pseudo random 하게 정해져 있는 pattern 에 따라 UL 데이터와 섞어줌으로써 MS 의 UL 전송 신호를 생성한다. 본 방식은 하향링크의 traffic 이 상향링크의 traffic 보다 작은 경우에도 동일하게 적용할 수 있다.

<그림 12>는 상, 하향링크의 전송신호 모두에 jamming 신호를 삽입하는 방법을 보여준다. 이러한 방법은 상, 하향링크의 traffic 이 동일하거나 차이가 크지 않은 경우에 적용할 수 있으며, 또한 하향링크에 더욱 강력한 보안이 요구되는 경우에 적용할 수 있다. 또한 이 방식에서는, 상, 하향 링크 모두에 대해 일정 부분의 자원을 jamming 신호 전송을 위해 사용한다. Jamming 에 할당된 자원에 맞춰 상, 하향 링크 모두 pseudo random jamming sequence 를 생성한 후, 역시 pseudo random 하게 정해져 있는 pattern 에 따라 UL 데이터와 섞어줌으로써 MS 의 UL 전송 신호를 생성하는데, 이 때 상, 하향링크에서 사용되는 jamming sequence 및 jamming pattern 은 서로 같거나 다르게 사용될 수 있다.



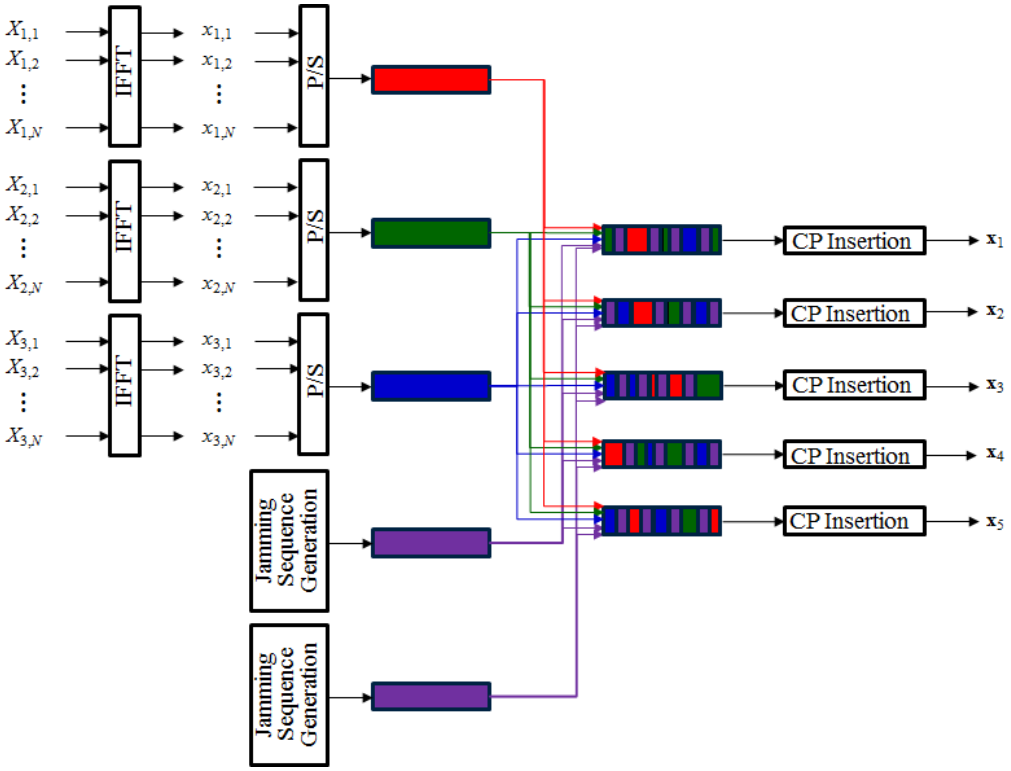
<그림 12> Traffic 비대칭과 재밍을 이용한 물리계층 보안 (2)

나. Simultaneously-Transmitted Jamming 을 위한 전송 신호 Encoding

<그림 11> 혹은 <그림 12>와 같이 상, 하향링크의 traffic asymmetry 를 활용하여 전송신호에 jamminj 신호를 삽입하는 방법으로는 1) 시간 영역에서의 jamming 신호 삽입, 2) 주파수 영역에서의 jamming 신호 삽입, 3) 시간과 주파수 영역 모두에서 jamming 신호를 삽입하는 방법의 3 가지 jamming 신호 삽입 기술이 있다. 본 절에서는 상기 2 가지 jamming 신호 삽입 기술의 각각에 대해 자세히 기술하도록 한다.

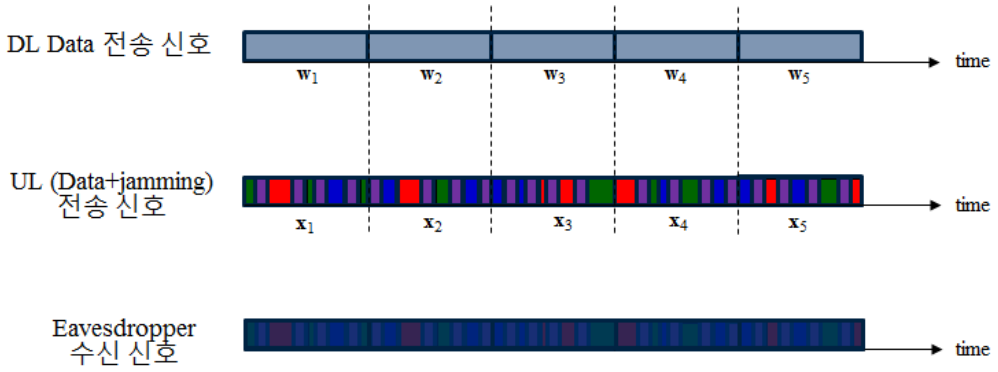
1) 시간 영역에서의 jamming 삽입 기술

<그림 13>은 OFDM modulation 을 가정했을 때 traffic 이 적은 링크에 대한 jamming 신호 삽입 기술을 도시한다. 본 방식에서는 먼저 $\{X_{i,1} \sim X_{i,N}\}$을 각각 IFFT 와 parallel-to-serial conversion 한다. 또한, 각각의 IFFT output 과 동일한 길이의 jamming sequence 개를 DL traffic 과 UL traffice 의 차이만큼 함께 생성해 준다. 이 때 N 은 OFDM symbol 의 subcarrier 수를 의미한다. 다음, 각각의 IFFT output 과 jamming sequence 를 정해진 pattern 에 따라 섞어줌으로써 DL 에서와 동일한 수의 시간영역 전송 신호를 생성한 후, 각각의 시간 영역 전송 신호에 cyclic preficx (CP)를 삽입한다.



<그림 13> 시간 영역에서의 jamming 삽입 기술

그 후, <그림 14>와 같이 DL 전송 신호($w1 \sim w5$)와 동일한 대역에서 동시에 전송한다. 이 경우, 하향링크에서는 주어진 모든 자원을 이용해 데이터를 전송하므로 데이터 전송률을 극대화 할 수 있다. 또한, 도청자의 수신신호에는 하향링크의 데이터 전송 신호와 상향 링크에서의 데이터 전송 신호, 그리고 상향링크 신호에 포함된 jamming 신호가 모두 섞여 있을 뿐 아니라, 상향 링크 전송 신호에 jamming 신호 및 데이터 신호가 섞여있는 pattern 을 알 수 없으므로 상, 하향링크 정보를 도청할 수 없게 된다.



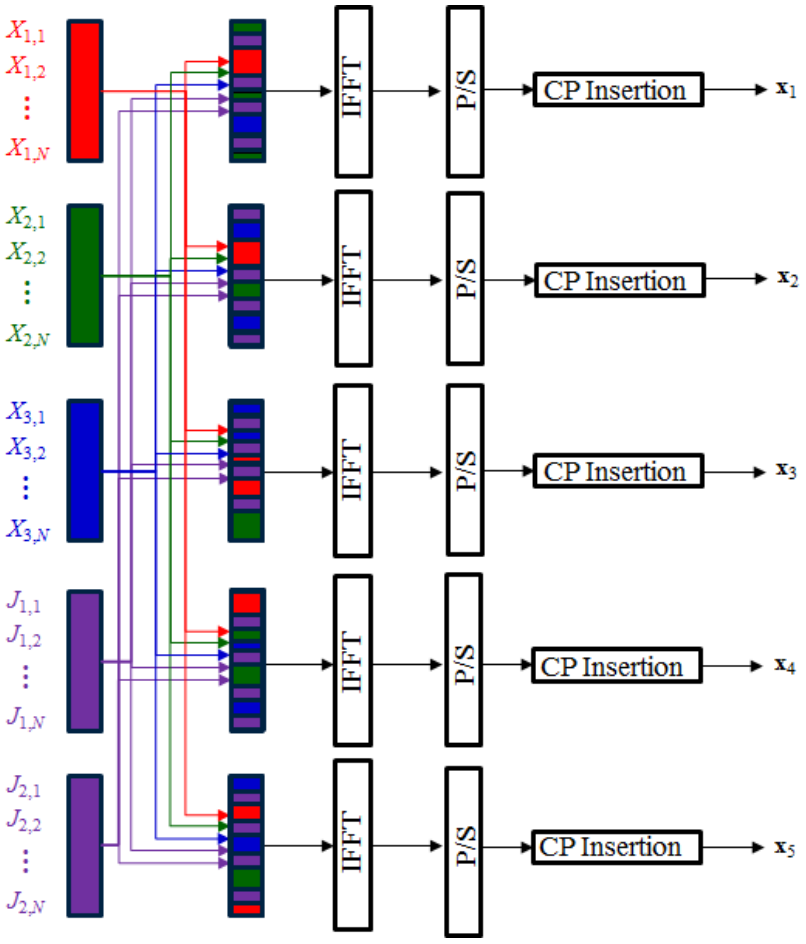
<그림 14> 시간영역에서의 jamming 신호 삽입 후 eavesdropper 에서의 수신 신호

이 방식은, 임의의 DL:UL traffic 비에 대해, 시간 영역에서의 jamming sequence 의 비율을 변화시킴으로써 DL:UL traffic 비에 관계 없이 traffic 이 적은 링크의 남는 자원을 이용해 시간 영역에서 jamming 신호를 삽입할 수 있다. 또한, 상기 예에서는 편의상 DL 의 traffic 이 UL 의 traffic 보다 큰 경우를 가정했으나, 반대의 경우, 즉 UL 의 traffic 이 DL 의 traffic 보다 큰 경우 또한 본 제안하는 방식을 동일하게 적용할 수 있다. 이와 더불어, 상기 예에서는 한 링크(위의 예에서는 UL)에서만 jamming 신호를 삽입하는 경우를 예로 들었으나, 두 링크 모두(즉, DL 과 UL 모두)에서 jamming 신호를 삽입하는 경우에도 시간 영역에서의 jamming sequence 의 비율을 변화시킴으로써 이 방식을 적용할 수 있다.

2) 주파수 영역에서의 jamming 삽입 기술

<그림 15>는 OFDM modulation 을 가정했을 때 traffic 이 적은 링크(<그림 10>의 UL)에 대한 jamming 신호를 주파수 영역에서 삽입하는 기술을 도시한다. 이 방식에서는 먼저 주파수 영역의 데이터 전송 신호 $\{X_{i,1} \sim X_{i,N}\}$을 생성하고, 이와 함께 주파수 영역에서의 jamming 신호 $\{J_{i,1} \sim J_{i,N}\}$를 생성한다. 이 때 N 은 OFDM symbol

의 subcarrier 수를 의미한다. 이후, $\{X_{i,1} \sim X_{i,N}\}$과 $\{J_{i,1} \sim J_{i,N}\}$를 정해진 pattern 에 따라 주파수 영역에서 섞어줌으로써 주파수 영역 IFFT input 을 생성한다. 다음, 각각의 IFFT input 에 대해 IFFT, parallel-to-serial conversion, CP 삽입의 과정을 거쳐 OFDM 전송 symbol($\mathbf{x}_1 \sim \mathbf{x}_5$)을 생성하고, 이를 <그림 14>에서와 같이 DL 전송 신호($\mathbf{w}_1 \sim \mathbf{w}_5$)와 동일한 대역에서 동시에 전송한다.



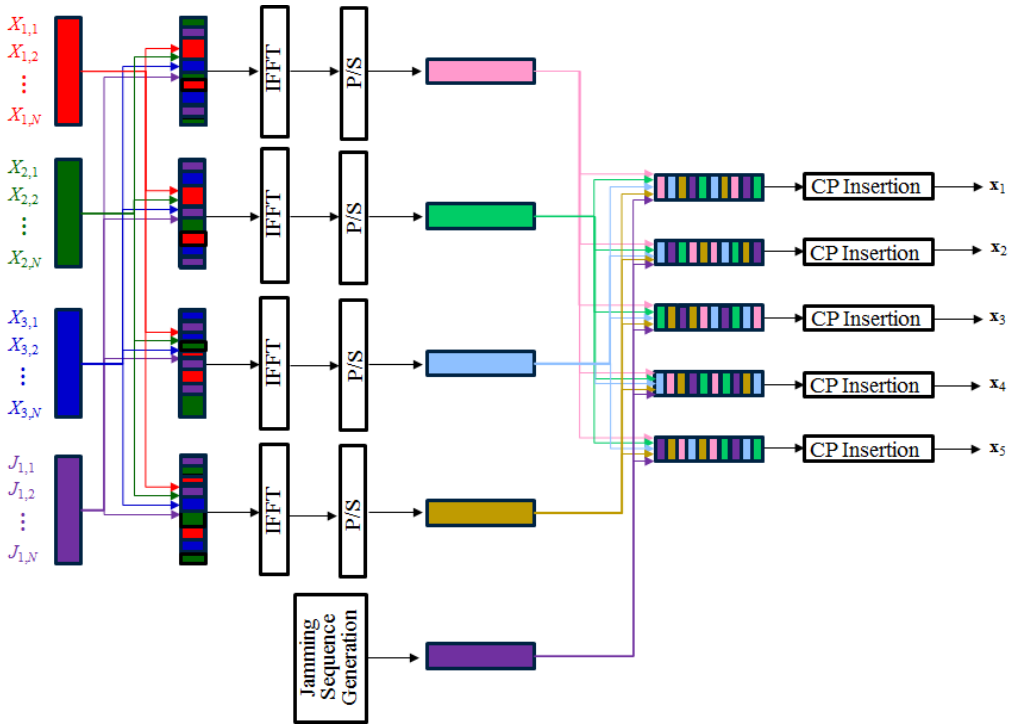
<그림 15> 주파수 영역에서의 jamming 삽입 기술

이 경우 또한 <그림 14>와 같이 하향링크에서는 주어진 모든 자원을 이용해 데이터를 전송하므로 데이터 전송률을 극대화 할 수 있다. 또한, 도청자의 수신신호에는 하향링크의 데이터 전송 신호와 상향 링크에서의 데이터 전송 신호, 그리고 상향링크 신호에 포함된 jamming 신호가 모두 섞여 있을 뿐 아니라, 상향 링크 전송 신호에 jamming 신호 및 데이터 신호가 섞여있는 pattern 을 알 수 없으므로 상, 하향링크 정보를 도청할 수 없게 된다.

상기 예에서는 편의상 DL:UL traffic 의 비가 5:3 인 경우를 가정했으나, 상기 기술의 범위가 특정 DL:UL traffic 비에 국한되지 않음을 명시한다. 임의의 DL:UL traffic 비에 대해, 주파수 영역에서의 jamming sequence 의 비율을 변화시킴으로써 <그림 15>에서 제안하는 방식을 적용할 수 있으므로, DL:UL traffic 비에 관계 없이 traffic 이 적은 링크의 남는 자원을 이용해 주파수 영역에서 jamming 신호를 삽입할 수 있다. 또한, 본 예에서는 편의상 DL 의 traffic 이 UL 의 traffic 보다 큰 경우를 가정했으나, 반대의 경우, 즉 UL 의 traffic 이 DL 의 traffic 보다 큰 경우 또한 본 제안하는 방식을 동일하게 적용할 수 있다. 이와 더불어, 본 일례에서는 한 링크(위의 예에서는 UL)에서만 jamming 신호를 삽입하는 경우를 예로 들었으나, 두 링크 모두(즉, DL 과 UL 모두)에서 jamming 신호를 삽입하는 경우에도 주파수 영역에서의 jamming sequence 의 비율을 변화시킴으로써 상기 jamming 신호 삽입 기술을 적용할 수 있음을 명시한다. 마지막으로 주파수 영역의 jamming sequence 생성 방법과 주파수 영역에서 $\{X_{i,1} \sim X_{i,N}\}$ ($i = 1, 2, 3$) 및 $\{J_{i,1} \sim J_{i,N}\}$ ($i = 1, 2$)를 섞어주는 pattern 에 관계없이 <그림 15>의 제안 방식으로 전송 신호를 생성하는 모든 방법이 본 연구의 범위에 포함됨을 명시한다.

3) 시간과 주파수 영역 모두에서 jamming 삽입 기술

<그림 16> 은 OFDM modulation 을 가정했을 때 traffic 이 적은 링크에 대한 jamming 신호 삽입 기술의 일례로 시간 및 주파수 영역을 모두에서 jamming 신호를 삽입하는 기술을 도시한다. 상기 예들과 마찬가지로 <그림 16> 또한 편의상 DL:UL traffic 의 비가 5:3 인 경우를 우선 가정한다.



<그림 16> 시간과 주파수 영역에서 jamming 삽입 기술

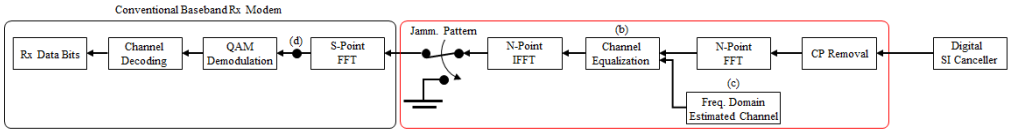
<그림 16> 의 방식에서는 먼저 주파수 영역의 데이터 전송 신호 $\{X_{i,1} \sim X_{i,N}\}$ (i = 1, 2, 3)을 생성하고, 이와 함께 주파수 영역에서의 jamming 신호 $\{J_{I,1} \sim J_{I,N}\}$을 생성한다. 이 때 N은 OFDM symbol 의 subcarrier 수를 의미한다. 이후, $\{X_{i,1} \sim X_{i,N}\}$ ($i = 1, 2,$

3)과 $\{J_{I,1} \sim J_{I,N}\}$을 정해진 pattern 에 따라 주파수 영역에서 섞어줌으로써 4 개의 주파수 영역 IFFT input 을 생성한다. 다음, 각각의 IFFT input 에 대해 IFFT 와 parallel-to-serial conversion 과정을 거쳐 5 개의 시간영역 전송 신호를 생성하며, 이 때 각각의 IFFT output 과 동일한 길이의 jamming sequence 1 개를 함께 생성한다. 다음, 각각의 IFFT output 과 시간영역 jamming sequence 를 정해진 pattern 에 따라 섞어줌으로써 5 개의 시간영역 전송 신호를 생성한 후, 각각의 시간 영역 전송 신호에 CP 를 삽입해 5 개의 OFDM 전송 신호($\mathbf{x}_1 \sim \mathbf{x}_5$)를 생성한다. 이후 <그림 14> 와 같이 5 개의 OFDM 심볼로 구성된 DL 전송 신호($\mathbf{w}_1 \sim \mathbf{w}_5$)와 동일한 대역에서 동시에 전송한다. 이 경우 또한 <그림 14>와 같이 하향링크에서는 주어진 모든 자원을 이용해 데이터를 전송하므로 데이터 전송률을 극대화 할 수 있다. 또한, 도청자의 수신신호에는 하향링크의 데이터 전송 신호와 상향 링크에서의 데이터 전송 신호, 그리고 상향링크 신호에 포함된 jamming 신호가 모두 섞여 있을 뿐 아니라, 상향 링크 전송 신호에 jamming 신호 및 데이터 신호가 섞여있는 pattern 을 알 수 없으므로 상, 하향링크 정보를 도청할 수 없게 된다.

다. Simultaneously-Transmitted Jamming 을 위한 수신 신호 Decoding

<그림 17>은 본 과제에서 제안된 양방향 보안통신 중 <그림 13>과 <그림 16>의 jamming 삽입 기술이 사용되었을 때 유효신호의 decoding 과정의 블록도를 보여준다 (<그림 15>의 jamming 삽입 기술이 사용되는 경우에는 기존의 OFDM 수신기와 동일한 유효신호의 decoding 과정을 가진다). 본 수신 신호 decoding 과정에서는, 먼저 수신된 심볼에서 CP 를 제거한 후 N-point FFT 를 수행한 후, (c)의 주파수영역 채널 정보를 이용해 (b)에서 channel equalization 을 수행한다 (일반적인 OFDM 수신

기의 경우, 주파수영역 channel equalization 은 <그림 17>의 (d) 부분에서 수행된다). 이후 이를 다시 *N*-point IFFT 하여 시간영역 심볼로 변환한 후, 주어진 jamming pattern 에 따라 jamming sample 들을 제거해 *S*-sample 시간영역 sample 을 획득한다. 이러한 *S* 개의 시간영역 sample 들을 S-point FFT 한 후, *S* 개의 subcarrier 각각에 대한 주파수 영역 수신 심볼을 획득한다. 이후의 과정은, (d) 영역에서 channel equalization 이 수행되지 않는다는 점을 제외하고는 일반적인 OFDM 수신기와 동일하게 진행된다.



<그림 17> . ST-Jamming 시스템에서 유효신호 decoding 의 블록도

라. Simultaneously-Transmitted Jamming 을 위한 Jamming 신호의 설계

1) Jamming 신호의 통계적 특성

OFDM 신호의 시간영역 샘플은 subcarrier 의 수가 커질수록 대수의 법칙에 의해 zero-mean circularly symmetric complex Gaussian (CSCG) distribution 을 가지게 된다. 따라서, jamming sequence 의 각 샘플이 OFDM 신호의 시간영역 샘플과 동일한 power 를 가지는 CSCG random variable 로 설계될 경우, 이를 수신하는 도청자는 수신 sample 의 distribution 상에서 legitimate OFDM symbol 의 sample 과 jamming sequence 의 sample 을 구분할 수 없게 된다.

2) Jamming sample 의 수와 pattern 으로 생성되는 2 중 codebook

다음은 <그림 13> - <그림 16>의 jamming 삽입 기술에서 사용되는 jamming sequence 및 jamming pattern 을 생성하는 방법이다. Jamming sequence 와 jamming pattern 은 각각 서로 다른 2 개의 codebook 형태로 생성될 수 있다. 먼저 jamming sequence 에 대한 codebook 은 다음과 같이 표현될 수 있다.

$$\mathbf{J} = \begin{bmatrix} J_{1,1} & J_{1,2} & \cdots & J_{1,N} \\ J_{2,1} & J_{2,2} & \cdots & J_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ J_{M,1} & J_{M,2} & \cdots & J_{M,N} \end{bmatrix} \tag{3}$$

수식 (3)에서 N 은 각각의 jamming sequence 의 최대 길이이며, OFDM 방식으로 전송 신호가 생성된다고 가정할 경우, OFDM 신호의 subcarrier 개수(혹은 FFT size)를 의미한다. 또한, M 은 전체 jamming sequence 의 개수를 의미한다. **J** 의 각 element (즉, $J_{n,m}$, n = 1, … N, m = 1, … M)은 zero-mean, unit variance 를 가지는 complex Gaussian distribution 을 가지는 값으로 정해진다. 수식 (3)의 codebook **J** 는 기지국과 단말에 의해 공유될 수도 있고 공유되지 않을 수도 있다. 만약 기지국과 단말이 jamming sequence 를 공유해야 할 경우에는 **J** 의 row address (즉, $J_{n,m}$ 의 m)을 공유함으로써 서로의 전송신호 생성에 사용되는 jamming sequence 를 공유한다.

$$\mathbf{Q} = \begin{bmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,N} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,\mathrm{N}} \\ \vdots & \vdots & \ddots & \vdots \\ q_{P,1} & q_{P,2} & \cdots & q_{P,N} \end{bmatrix} \tag{4}$$

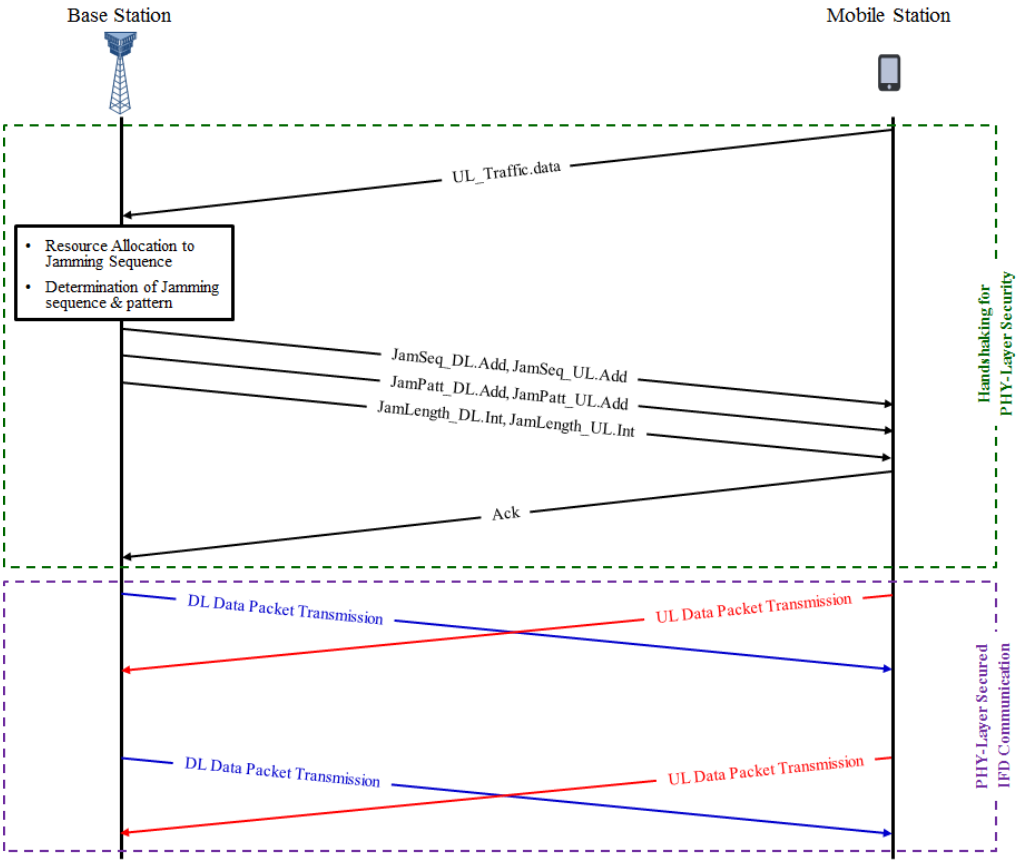
수식 (4)에서 **Q** 의 각각의 row 는 1 ~ N 사이의 random permutation 을 값으로 가지며, P 는 서로 다른 permutation 의 수를 의미한다. 기지국과 단말은 **Q** 를 공유하며, **Q** 의 row address 및 주어진 row 에서의 실제로 사용되는 permutation 의 길이를 공유함으

로써 jamming 신호의 삽입 pattern 을 서로 공유한다. 가령 DL:UL traffic 비가 5:3 이고 $N = 64$ 일 때 수식 (3)와 수식 (4)의 codebook 을 이용해 jamming sequence 를 포함하는 전송 신호를 생성할 경우, 수식 (3)의 codebook matrix **J** 중 $J_{1,1} \sim J_{1,64}$ 의 sequence 와 $J_{2,1} \sim J_{2,N}$ 의 sequence 를 이용하여 전송신호 $\mathbf{x}_1 \sim \mathbf{x}_5$ 에 jamming sequence 를 삽입한다. 이 때 $\mathbf{x}_1$ 에는 $q_{1,1} \sim q_{1,26}$ 이 가리키는 subcarrier 에 $J_{1,1} \sim J_{1,26}$ 의 sequence 를, $\mathbf{x}_2$ 에는 $q_{2,1} \sim q_{2,26}$ 이 가리키는 subcarrier 에 $J_{1,27} \sim J_{1,52}$ 의 sequence 를, $\mathbf{x}_3$ 에는 $q_{3,1} \sim q_{3,26}$ 이 가리키는 subcarrier 에 $J_{1,53} \sim J_{1,64}, J_{2,1} \sim J_{2,24}$ 의 sequence 를, $\mathbf{x}_4$ 에는 $q_{4,1} \sim q_{4,25}$ 이 가리키는 subcarrier 에 $J_{2,25} \sim J_{2,39}$ 의 sequence 를, 그리고 $\mathbf{x}_5$ 에는 $q_{5,1} \sim q_{5,25}$ 이 가리키는 subcarrier 에 $J_{2,40} \sim J_{2,64}$ 의 sequence 를 삽입한다. 상기 방법을 통해 단말이 전송신호에 jamming sequence 를 삽입하여야 하므로, 기지국은 단말에게 각각의 $\mathbf{x}_i$ 의 생성에 필요한 **Q** 의 row address 및 길이, 즉, $\mathbf{x}_1$:(1, 26), $\mathbf{x}_2$:(2,26), $\mathbf{x}_3$:(3,26), $\mathbf{x}_4$:(4,25), $\mathbf{x}_5$:(5,25)를 전달해야 한다.

마. Simultaneously-Transmitted Jamming 을 위한 통신 절차 및 제어신호의 설계

<그림 18>은 기지국과 단말이 모두 신호의 동일대역 동시 송수신이 가능한 경우 본 과제에서 제안하는 ST-jamming 기술이 동작하기 위한 절차를 보여준다. 먼저 단말은 'UL_Traffic.data' 메시지를 통해 자신의 상향링크를 통해 전송해야 하는 UL required data traffic 을 전송한다. 기지국은 수신 받은 단말의 required data traffic 과 자신이 하향링크를 통해 전송해야 하는 DL required data traffic 을 비교해 상, 하향링크에서 동시에 전송할 심볼 수를 결정한 후, <그림 11>, 혹은 <그림 12>의 상, 하향링크 전송 신호 구조 중 하나와 양 링크의 전송 신호 생성을 위해 <그림 13>, <그림 14>, 혹은 <그림 16>의 방식 중 하나를 선택한다. 다음 단말이 jamming sequence 가

포함된 전송 신호를 생성할 수 있도록, 기지국은 단말에게 jamming 길이 및 pattern 과 sequence 에 대한 정보를 다음의 메시지를 통해 전송한다.



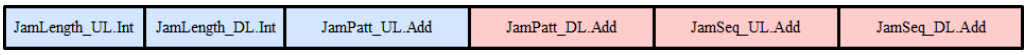
<그림 18> . ST-Jamming 을 위한 통신 절차

- JamLength_UL.Int : 각각의 UL 전송 symbol 에 포함되는 jamming sequence 의 길이를 나타내는 메시지
- JamLength_DL.Int : 각각의 DL 전송 symbol 에 포함되는 jamming sequence 의 길이를 나타내는 메시지
- JamPatt_UL.Add : 각각의 UL 전송 symbol 에 jamming sequence 를 위치 시키는 pattern 을 지시하기 위한 메시지 (예를 들어 수식 (2)에서 **Q** 의 row address)
- JamPatt_DL.Add : 각각의 DL 전송 symbol 에 jamming sequence 를 위치 시키는 pattern 을 지시하기 위한 메시지 (예를 들어 수식 (2)에서 **Q** 의 row address)

- JamSeq_UL.Add : UL 에서 사용될 jamming sequence 를 지시하기 위한 메시지 (예를 들어 수식 (1)에서의 **J** 의 row address)
- JamSeq_DL.Add : DL 에서 사용될 jamming sequence 를 지시하기 위한 메시지 (예를 들어 수식 (1)에서의 **J** 의 row address)

<그림 11>과 <그림 12>의 전송 신호 구조의 선택은 JamLength_UL.Int 와 JamLength_DL.Int 에 의해 결정된다. 가령, DL 의 traffic 이 더 크고 <그림 11>의 신호 구조를 선택한 경우에는 JamLength_DL.Int 의 모든 값은 0 이 된다 (반대의 경우도 동일하게 성립한다). 만약 <그림 12>의 신호 구조를 선택한 경우에는 JamLength_UL.Int 와 JamLength_DL.Int 모두 non-zero 의 값을 가진다. <그림 11>의 신호 구조가 선택된 경우, traffic 이 더 큰 링크에서는 전송 신호에 jamming sequence 를 삽입하지 않으므로 이 링크에 대한 jamming pattern 을 단말에게 전달할 필요가 없다. 따라서, JamPatt_DL.Add 메시지와 JamPatt_UL.Add 메시지 중 하나를 optional 메시지로 둘 수 있다. 만약 JamPatt_DL.Add 메시지와 JamPatt_UL.Add 메시지 중 하나만 사용된 경우, 이 메시지가 전달하는 pattern 은 JamLength_UL.Int 와 JamLength_DL.Int 중 non-zero 값을 가지는 링크에 대한 jamming 삽입 pattern 을 의미하며, 따라서 JamLength_UL.Int 와 JamLength_DL.Int 중 하나는 반드시 0 의 값을 가져야 한다. 만약 JamLength_UL.Int 와 JamLength_DL.Int 모두 non-zero 값을 가진다면 JamPatt_DL.Add 메시지와 JamPatt_UL.Add 가 반드시 둘 다 사용되어야 한다. 상, 하향링크에서 사용되는 jamming sequence 의 정확한 값은 데이터의 decoding 을 위해 반드시 알아야 하는 값이 아니다. 따라서 JamSeq_UL.Add 와 JamSeq_DL.Add 메시지는 optional 메시지로 둘 수 있다.

<그림 19>는 기지국이 jamming 길이 및 pattern 과 sequence 에 대한 정보를 단말에게 전달하기 위한 전송 프레임 구조의 일례이다. 앞에서 상술한 대로 JamLength_UL.Int 와 JamLength_DL.Int, 그리고 JamPatt_UL.Add 는 mandatory 이며, JamPatt_DL.Add 와 JamSeq_UL.Add, 그리고 JamSeq_DL.Add 는 optional 이다. 단말이 기지국으로부터 jamming 길이 및 pattern 과 sequence 에 대한 정보를 수신한 후 ACK 신호를 보내고 나면 기지국과 단말은 동시에 전송 신호를 송신한다. 이 때 전송신호는 위의 메시지들의 내용에 따라 jamming sequence 를 포함한다.



<그림 19> ST-jamming 을 위한 handshaking 단계에서의 전송 프레임 구조

하나의 실시 예로, LTE 시스템을 고려할 경우, 상기 <그림 18>의 절차는 RRC connection establishment 과정에 포함될 수 있다 (이 때, LTE 표준은 IFD 통신이 가능하도록 적절한 변형이 이루어져 있다고 가정한다). 먼저 'UL_Traffic.data'는 RRC Connection Request 메시지에 information 형태로 포함될 수 있다. 이 때 시스템의 상, 하향링크간 traffic 요구사항에 따라 UL_Traffic.data 는 임의의 bit 수로 구성될 수 있으며, UL_Traffic.data 메시지의 사용 여부를 결정하는 1bit 의 control message 가 사용될 수 있다. 또한 <그림 19>의 구조는 Security Mode Command 메시지에 information 형태로 포함될 수 있다. 이 때 <그림 19>의 mandatory message 는 반드시 포함되어야 하며, 나머지 메시지는 선택적으로 포함될 수 있다. 이와 더불어 Security Mode Command 에서 <그림 19>의 메시지 구조를 포함하는지 여부를 결정하는 1bit 의 control message 가 사용될 수 있다.

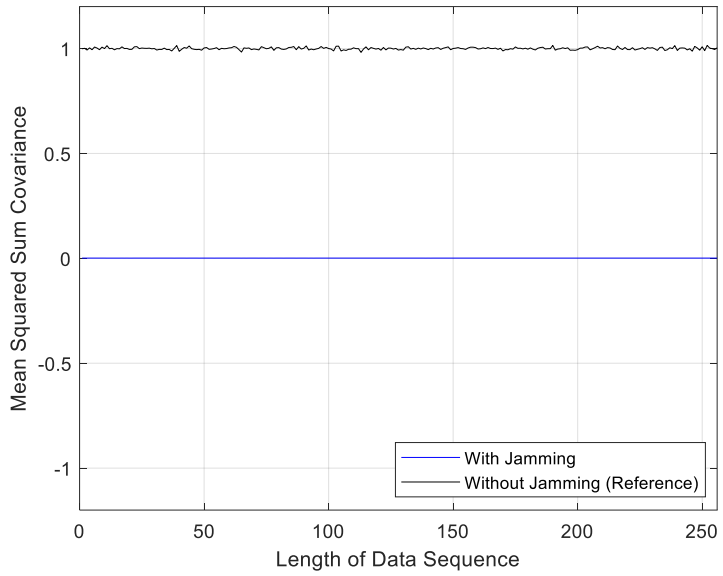
2. Simultaneously-Transmitted Jamming 기술의 성능 분석

가. Jamming 신호 삽입으로 인한 송, 수신 신호간 Independence

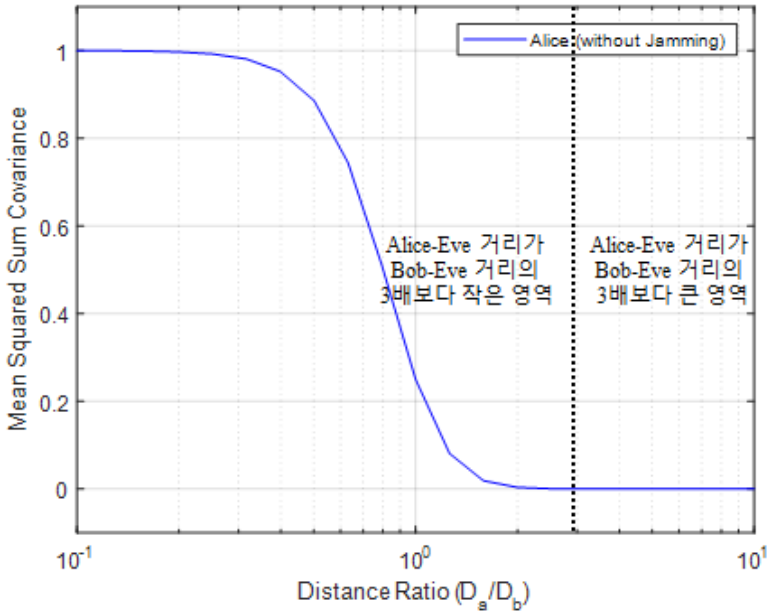
앞서 제안한 ST-jamming 기술이 사용될 경우, 도청자(이하 'Eve'라 표기)가 기지국 (이하 'Alice'라 표기) 혹은 단말 (이하 'Bob'이라 표기)의 legitimate information 을 도청하기 위해서는 Alice 와 Bob 각각이 사용하는 jamming sequence 의 sample 수와 삽입 pattern 및 순서를 정확히 알아야 한다. 만약 Eve 이중 하나라도 정확하지 않은 정보를 가지게 될 경우, 아래와 같은 문제로 인해 legitimate information 의 도감청이 불가능해진다.

- 수신 OFDM 심볼 내 각 subcarrier 간 orthogonality 상실
- 시간영역 data 샘플의 손실
- 주파수 영역 data symbol 의 손실

또한 이로 인해 Eve 의 수신 신호는 Alice 혹은 Bob 의 송신 신호와 통계적으로 다른 신호가 될 수 있다. 수식 (2)의 상향링크(Bob-to-Alice link) 및 하향링크 (Alice-to-Bob link) overhead (각각 L_U 와 L_D)의 정의에 의해 Alice 혹은 Bob 의 송신 신호와 Eve 의 수신 신호가 통계적으로 independent 할 경우, 제안된 ST-jamming 기술은 본 과제의 성능 목표인 $L_D = L_U = 0$ 을 달성한다. <그림 20>과 <그림 21>은 각각 Bob 의 송신 신호와 Eve 의 수신 신호, 그리고 Alice 의 송신 신호와 Eve 의 수신 신호간 통계적 independence 여부를 보여준다.



<그림 20> OFDM 심볼 내 data 샘플 수에 따른 Eve 에서 Bob 전송 신호의 MSSC



<그림 21> Alice-Eve-Bob 거리의 비에 따른 Eve 에서 Alice 전송 신호의 MSSC

상기 결과를 도출함에 있어서, Alice 의 required traffic 이 Bob 의 required traffic 보다 크다는 가정 하에, Alice 는 jamming 신호를 사용하지 않되 Bob 만 jamming 신호를 전송 신호에 삽입함을 가정했다. 또한 Bob 의 jamming 신호 삽입은 <그림 13> 의 방식을 따랐다. 이로 인해 Bob 의 전송 신호는 Alice 의 전송에 의한 간섭과 jamming 신호 둘 다에 의해 보호되는 반면, Alice 의 전송 신호는 Bob 의 전송 신호에 의한 간섭으로만 보호받는다. 이러한 setup 을 통해 Alice 와 Bob 모두 데이터 전송률의 손실이 발생하지 않는다.

Alice 혹은 Bob 의 전송 신호와 Eve 의 수신신호 사이의 independence measure 로는 covariance matrix 의 mean squared sum (mean squared sum covariance, MSSC)을 이용하였다. 두 각각 길이 N 과 M 을 가지는 complex vector $\mathbf{x} = [x(0), \ldots, x(N\text{-}1)]^T$ 과 $\mathbf{y} = [y(0), \ldots y(M\text{-}1)]^T$ 에 대하여 MSSC 는 다음과 같이 정의된다.

$$MSSC = \frac{1}{NM}\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} C(n,m) \tag{5}$$

이 때, $C(n, m)$은 두 벡터 x 와 y 의 cross-covariance matrix $\mathbf{C}$ 의 n 번째 row 와 m 번째 column 에 위치한 element 를 의미하며, cross-covariance matrix C 는 다음과 같이 정의된다.

$$\mathbf{C} = \left[C(n,m) \right] = \mathrm{E}[\mathbf{x}\mathbf{y}^H]. \tag{6}$$

수식 (5)의 MSMC 는 서로 길이가 다를 수 있는 두 random vector 사이의 independence 여부를 하나의 숫자로 표기하기 위해 정의한 값으로써 두 random vector 가 통계적으로 independence 한 경우에만 MSMC = 0 의 값을 가지며, 두 random vector 가 동일한 경우에는 MSMC = 1 의 값을 가진다.

먼저 ST-jamming 이 적용된 Bob 의 전송 신호의 경우, <그림 20>에서 볼 수 있듯이 data sample 의 수 (동등하게 jamming sample)의 수와 관계 없이 Bob 의 전송 신호와 Eve 의 수신신호가 independent 하며, 이로 인해 Bob 의 전송에 있어서의 overhead 는 $L_U = 0$ 임을 알 수 있다.

반면 Alice 의 전송 신호의 경우, <그림 21>에서 볼 수 있듯이 distance ratio 가 2 보다 커져야 Alice 의 전송 신호와 Eve 의 수신신호가 independent 해 짐을 알 수 있다. 이 때 distance ratio 는

Alice-to-Eve distance / Bob-to-Eve distance (7)

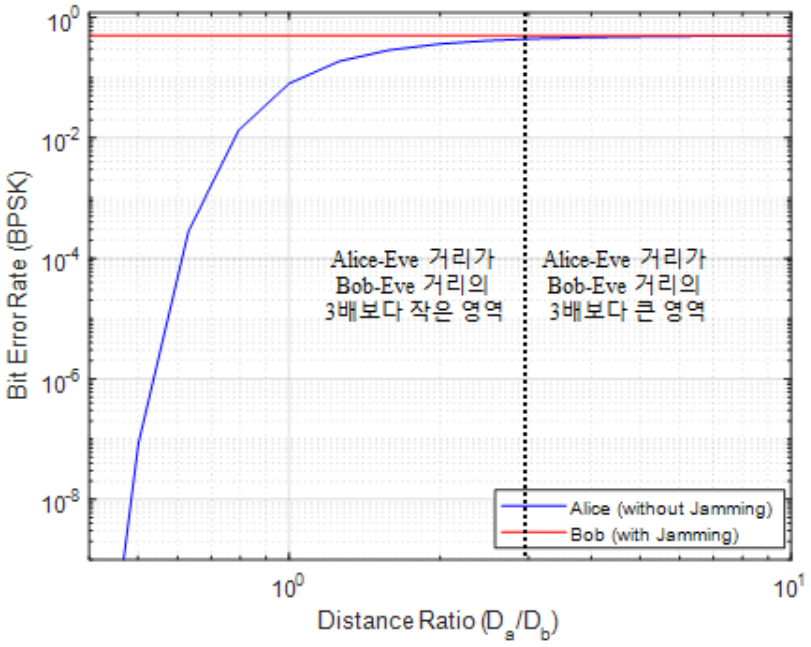
로 정의된다. 즉, <그림 21>의 결과로부터 본 과제의 성과 목표인 기지국-도청자의 거리(=Alice-to-Eve distance)가 단말-도청자의 거리(Bob-to-Eve distance)의 3 배 이상일 때 Alice 의 전송에 있어서의 overhead $L_D = 0$ 을 달성함을 알 수 있다.

나. Jamming 신호 삽입으로 인한 Legitimate Data 신호의 Bit-Error Rate

<그림 22>는 (7)에서 정의된 distance ratio 값에 따른 Alice 와 Bob 의 전송신호에 대한 Eve 의 decoding bit-error rate 을 보여준다. 본 결과를 도출하는 과정에서 Alice 와 Bob 의 traffic 비 2:1 과 사용 가능한 총 subcarrier 의 수 $N = 512$ 임을 가정했다. 또한 Alice 는 N 개의 subcarrier 을 모두 이용해 데이터 심볼 전송 (즉 jamming 삽입하지 않음)하는 반면, Bob 은 <그림 11>의 방법을 통해 N/2 개의 subcarrier 를 이용해 데이터 심볼 전송하고 N/2 개의 시간영역 샘플을 이용해 jamming 신호를 삽입하였다.

<그림 22>에서 볼 수 있듯이, Bob 의 전송신호의 경우에는 jamming 신호를 전송 신호에 삽입함으로써 Bob 의 전송 신호와 Eve 의 수신신호가 통계적으로 완전히 다른 신호가 되어 버리므로 distance ratio 값에 관계 없이 Eve 의 decoding bit-error rate 은 0.5 가 된다. 반면 Alice 의 전송신호의 경우에는 jamming 신호를 전송신호에

삽입하지 않으므로 오직 Bob 의 전송 신호에 의한 Eve 에서의 interference 에 의해서만 보호된다. 따라서 Alice 의 전송신호와 Bob 의 전송신호에 따른 interference 의 상대적 세기, 즉 distance ratio 값에 의해 Eve 의 bit-error rate 이 결정되게 된다.



<그림 22> Alice, Eve, Bob 거리 비에 따른 Eve 에서의 유효신호 decoding error rate

또한, distance ratio 값이 작은 경우, 즉 Alice 가 Bob 보다 Eve 에게 가까이 있는 경우에는 Eve 가 Alice 의 신호를 쉽게 decoding 할 수 있다. 반면 distance ratio 값이 커질수록, 즉 Alice 보다 Bob 이 Eve 에 가까이 위치할수록 Eve 는 Alice 의 신호를 decoding 할 수 없게 된다. 이 그림에서 볼 수 있듯이, 기지국-도청자의 거리(=Alice-to-Eve distance)가 단말-도청자의 거리(Bob-to-Eve distance)의 3 배 이상일 때 Alice 와 Bob 모두의 전송에 대한 bit-error rate 0.5 달성이라는 본 과제의 성과 목표를 달성함을 알 수 있다.

다. 도청자에서의 Legitimate Information 분석

본 절에서는 ST-jamming system 에서의 information leakage 성능을 분석한다. 이를 위하여 Alice, Bob, Eve 는 모두 하나씩의 안테나를 가지고 있으며, Alice 와 Bob 은 IFD 방식으로 동작하는 반면 Eve 는 도청을 위한 수신 모드로만 동작함을 가정한다. 이와 함께 Alice 와 Bob 에서는 perfect SIC 를 가정한다. 이후 성능 분석에 있어 I_N 와 0_N 는 각각 $N \times N$ identity matrix 와 $N \times 1$ zero vector 를 의미한다. 또한 $N \times M$ matrix C 의 i-th row 와 k-th column 의 element 를 $C(i,k)$ 로 표기하며, 이러한 matrix 를 동일하게 $C = [C(i,k)]$, $i = 0, \cdots, N-1$, $k = 0, \cdots, M-1$ 로 표현한다. 이와 함께 diagonal entri 가 vector x 로 주어지는 diagonal matrix 를 $\mathrm{diag}(x)$ 로 표기한다. $\mathrm{FFT}_N(\cdot)$ 와 $\mathrm{IFFT}_N(\cdot)$ 는 각각 N-point FFT 와 IFFT 를 의미한다. 또한, $\mathcal{CN}(\nu, \Sigma)$ 은 mean vector 와 covariance matrix 가 각각 ν 와 Σ 로 주어지는 circularly symmetric complex Gaussian (CSCG) random vector 를 뜻한다. 마지막으로, $\mathrm{E}[\cdot]$ 와 ϕ 는 각각 statistical expectation 과 공집합을 의미한다.

Alice 로부터 Bob 으로의 wireless channel 과 Bob 에서 Alice 로의 wireless channel 은 각각 impulse response h_{ab} and h_{ba} 로 표현된다. 또한 Alice 와 Bob 으로부터 Eve 까지의 무선 채널은 각각 g_a 와 g_b 의 impulse responses 로 표현된다. g_a 와 g_b 의 impulse responses 반면 Eve 는 g_a 와 g_b 에 대한 perfect knowledge 를 가지는 반면 h_{ba} 혹은 h_{ab} 에 대한 정보는 전혀 가지고 있지 않다.

Alice 와 Bob 의 시간영역 전송 신호는 모두 N 개의 samples 을 가지며 $x_a = [x_a(0), \cdots, x_a(N-1)]^T$ 와 $x_b = [x_b(0), \cdots, x_b(N-1)]^T$ 로 표기된다. 이 때

Alice 와 Bob 의 수신 신호는 아래와 같이 표기된다.

$$\begin{aligned} y_a &= h_{ba} * x_b + z_a, \\ y_b &= h_{ab} * x_a + z_b, \end{aligned} \tag{8}$$

이 때 z_a 와 z_b 는 각각 Alice 와 Bob 에서의 received noise vectors 를 의미하며, z_a 와 z_b 의 각 element 는 independent and identically distributed (i.i.d) zero-mean CSCG random variable 로 주어진다. 또한 z_a 와 z_b 의 각 element 들은 각각 σ_a 와 σ_b 의 variance 를 가진다고 가정한다. 한편 Eve 의 수신 신호는 아래와 같다.

$$y_e = g_a * x_a + g_b * x_b + z_e, \tag{9}$$

이 때 z_e 는 Eve 에서의 received noise vector 을 의미하며, z_e 의 각 element 는 zero mean 과 σ_e 의 variance 를 가지는 i.i.d CSCG random variable 이라 가정한다. 위의 (9) 에서 볼 수 있듯이, Alice 와 Bob 의 signal transmission 은 동일한 대역에서 동시에 수행되기 때문에 Eve 에서 수신될 때 서로에게 간섭을 미친다.

1) Legitimate Node 의 전송 신호 생성

Alice 는 자신의 required traffic 에 따라 M_a ($M_a \le N$)개의 data symbols 을 time domain transmit signal x_a 를 통해 Bob 에게 전송한다. 이를 위해 $W_a = [W_a(0), \cdots, W_a(M_a - 1)]^T$ 로 표기되는 주파수 영역 데이터 심볼을 생성하며, 이때 각각의 i 에 대해 $\mathrm{E}[|W_a(i)|^2] = P_a$ 의 관계가 성립한다. 이러한 W_a 로부터 시간 영역 데이터 signal $w_a = [w_a(0), \cdots, w_a(M_a - 1)]^T$ 을 다음과 같이 생성한다.

$$\begin{aligned} w_a &= \mathrm{IFFT}_{M_a}(W_a) \\ &= A_{M_a} W_a, \end{aligned} \tag{10}$$

이 때 $A_M = [A_M(i,k)]$, $i = 0,\cdots,M-1$, $k = 0,\cdots,M-1$,은 M -point IFFT matrix 를 의미하며, A_M 의 각 element 는 아래와 같이 주어진다.

$$A_M(i,k) = \frac{1}{\sqrt{M}} exp\left(j\frac{2\pi}{M} ik \right). \tag{11}$$

Alice 의 시간영역 Tx signal x_a 는 (10)의 w_a 와 jamming sequence $q_a = [q_a(0),\cdots,q_a(N-M_a-1)]^T$ 를 섞어줌으로써 생성된다. 이를 위해 아래와 같은 2 개의 set 을 정의한다.

$$\begin{aligned} \mathrm{D}_a &= \{d_a(0),\cdots,d_a(M_a-1)\}, \\ \mathrm{J}_a &= \{j_a(0),\cdots,j_a(N-M_a-1)\}, \end{aligned} \tag{12}$$

이 때 $\mathrm{D}_a \cap \mathrm{J}_a = \phi$ 와 $\mathrm{D}_a \cup \mathrm{J}_a = \{0,\cdots,N-1\}$ 의 관계가 성립한다. 위의 w_a 및 q_a 와 (12)로부터 , $x_a = [x_a(0),\cdots,x_a(N-1)]^T$ 는 아래와 같이 생성된다.

$$x_a(k) = \begin{cases} w_a(i), & \text{if } k \in \mathrm{D}_a \text{ and } k = d_a(i), \\ q_a(i), & \text{if } k \in \mathrm{J}_a \text{ and } k = j_a(i). \end{cases} \tag{13}$$

위의 (13)에서 볼 수 있듯이, D_a 와 J_a 는 각각 w_a 와 q_a 를 x_a 에 삽입하기 위한 index set 을 의미한다. 앞서 다룬바와 같이 q_a : $\mathcal{CN}(0_{N-M_a}, P_a I_{N-M_a})$ 가 되도록 생성한다. 이러한 방식으로 x_a 를 생성해 줌으로써 Eve 는 data part (i.e., w_a)와 jamming part (i.e., q_a)를 통계적인 특성을 이용해 구분할 수 없게 되며, 따라서 Eve 가 자신의 received signal 로부터 data samples 을 정확히 고르는 것을 방지한다. 이렇

게 x_a가 생성된 후 일반적인 OFDM system 에서와 같이 CP 를 붙여 Bob 에게 전송한다. Bob 에서도 (10)-(13)의 동일한 과정을 통해 x_b를 생성하되, M_a, W_a, D_a, 및 J_a 대신 M_b, W_b, D_b, 및 J_b의 값을 이용한다. 여기서 M_a와 M_b는 Alice 와 Bob 의 required traffics 에 대한 asymmetry 를 반영한다. 또한 Alice 와 Bob 은 D_a 및 D_b (동등하게 J_a와 J_b)을 공유한다고 가정한다.

2) Legitimate Node 에서의 수신 신호 복원

Alice 가 (8)의 y_a로부터 CP 를 제거하고 여기에 N-point FFT 를 적용함으로써 아래와 같은 Rx signal 의 frequency domain description 을 얻을 수 있다.

$$Y_a = H_{ba} X_b + Z_a, \tag{14}$$

이 때 $H_{ba} = \mathrm{diag}([H_{ab}(0), \cdots, H_{ab}(N-1)]^T)$ 는 각 diagonal entry 가 h_{ba}의 N-point FFT 인 $[H_{ab}(0), \cdots, H_{ab}(N-1)]^T = \mathrm{FFT}_N(h_{ba})$로 구성되는 diagonal matrix 이다. 또한, X_b는 아래와 같이 주어지는 x_b의 frequency domain expression 이다.

$$X_b = B_N x_b, \tag{15}$$

이 때 $B_N = [B_N(i,k)]$, $i = 0, \cdots, N-1$, $k = 0, \cdots, N-1$은 N-point FFT matrix 이며 각각의 $B_N(i,k)$는 다음과 같이 주어진다.

$$B_N(i,k) = \frac{1}{\sqrt{N}} exp\left(-j\frac{2\pi}{N}ik\right). \tag{16}$$

마지막으로 Z_a는 z_a의 frequency domain expression 이다. 이 때, CSCG random sequence 의 FFT 결과는 여전히 동일한 통계적 특성을 가지는 CSCG random

sequence 이므로 Z_a : $\mathbb{CN}(0_N, \sigma_a I_N)$ 이다.

Alice 는 자신이 가지고 있는 H_{ba} 의 정보를 이용하여 아래와 같이 주파수 영역에서 channel equalization 을 수행한다.

$$\begin{aligned} Y_a &= H_{ba}^{-1} Y_a \\ &= X_b + Z_a, \end{aligned} \tag{17}$$

이 때 $Z_a = H_{ba}^{-1} Z_a$ 이다. Y_a 에 N -point IFFT 를 적용함으로써 아래와 같이 channel-equalized Rx signal 의 time domain expression 을 얻을 수 있다.

$$\begin{aligned} y_a &= A_N Y_a \\ &= x_b + z_a, \end{aligned} \tag{18}$$

여기서 $z_a = A_N Z_a$ 이다. $\mathbb{D}_b$ 의 정보를 이용해 (18)의 y_a 로부터 jamming sample 들을 제거함으로써 $y_a = [\bar{y}_a(0), \cdots, \bar{y}_a(M_b - 1)]^T$ 를 얻을 수 있으며, 이 때 $\bar{y}_a(k)$, $k = 0, \cdots, M_b - 1$는 다음과 같이 주어진다.

$$\begin{aligned} \bar{y}_a(k) &= \tilde{y}_a(i), \qquad \text{if } i = d_b(k) \in \mathbb{D}_b, \\ &= x_b(i) + \tilde{z}_a(i), \text{ if } i = d_b(k) \in \mathbb{D}_b, \\ &= w_b(k) + \bar{z}_a(k). \end{aligned} \tag{19}$$

이 때 $z_a = [\bar{z}_a(0), \cdots, \bar{z}_a(M_b - 1)]^T$ 이며, $\bar{z}_a(k) = \tilde{z}_a(i)$, $i \in \mathbb{D}_b$, $k = d(i)$ 로 주어진다. (19)의 y_a 에 M_b -point FFT 를 적용함으로써 Bob 이 전송한 frequency domain data symbol 인 $W_b = [W_b(0), \cdots, W_b(M_b - 1)]^T$ 을 다음과 같이 구할 수 있다.

$$\begin{aligned} Y_a &= B_{M_b} y_a \\ &= W_b + Z_a, \end{aligned} \tag{20}$$

여기서 $Z_a = B_{M_b} z_a$ 이다. Bob 에서는, Alice 가 전송한 frequency domain data symbol W_a 를 (14)-(20)의 과정을 통해 동일하게 구하되, y_b, M_b 및 D_b 가 각각 y_a, M_a 및 D_a 로 대체된다.

W_a 와 W_b 는 각각 Bob 와 Alice 이 각각 (M_a, D_a) 와 (M_b, D_b)에 대한 perfect knowledge 를 가지고 있을 때에만 각각의 수신신호로부터 복원될 수 있다. 만약 Alice 와 Bob 의 Tx signal 이 Eve 에 의해 수신된다 해도, Alice 와 Bob 의 Tx signal 에 jamming sequence 를 삽입함으로써 Eve 가 (M_a, D_a) 와 (M_b, D_b) 모두에 대한 perfect knowledge 를 가지지 않는 이상 Alice 와 Bob 의 transmitted data 를 복원할 수 없다.

3) Eve 의 동작

ST-jamming 에 의한 Eve 에서 legitimate information 의 누설 성능 분석에 앞서 Eve 의 동작을 아래와 같이 설명한다. 이 때 편의상 Eve 가 Alice 의 legitimate information 을 도청하기 위한 동작 과정만을 기술하나, Eve 가 Bob 의 legitimate information 을 위한 동작 과정도 동일하다.

Alice 의 legitimate 신호를 도청하기 위한 Eve 의 수신신호 처리 과정 중 channel-equalized time domain Rx signal 을 얻기까지의 과정은, Eve 가 수신한 Bob 의 전송 신호가 background noise 로 간주된다는 점 외에는 (14)-(18)과 동일하다. 따라서, (2)에서 주어진 Eve 의 수신 신호는 아래와 같이 수정되어 표현될 수 있다.

$$y_e = g_a * x_a + z_e', \tag{21}$$

이 때 z_e'는 effective noise 이며 아래와 같이 표현된다.

$$z_e' = g_b * x_b + z_e. \tag{22}$$

위의 (21)로부터, CP 제거 및 N -point FFT 이후 수신신호의 frequency domain description 을 다음과 같이 얻을 수 있다.

$$Y_e = G_a * X_a + Z_e', \tag{23}$$

이 때, $[G_a(0),\cdots,G_a(N-1)]^T = \mathrm{FFT}_N(g_a)$ 라 하면, $G_a = \mathrm{diag}([G_a(0),\cdots,G_a(N-1)]^T)$ 이고, $X_a = B_N x_a$ 이다. (17)과 (18)에서 Y_a 를 (23)의 Y_e 로 치환함으로써 Eve 의 channel-equalized Rx signal 에 대한 the time domain expression 을 아래와 같이 구할 수 있다.

$$y_e = x_a + z_e, \tag{24}$$

이 때 $z_e = [\tilde{z}_e(0),\cdots,\tilde{z}_e(N-1)]^T$ 이며, 아래와 같이 구해진다.

$$z_e = A_N G_a^{-1} Z_e', \tag{25}$$

여기서 Z_e'는 (15)의 z_e'에 대한 frequency domain expression 이다.

Eve 는 M_a 혹은 D_a (따라서 J_a)에 대한 정확한 정보를 가지고 있을 수도, 가지고 있지 않을 수 도 있다. 따라서 우리는 M_a 에 대응되는 새로운 값 $0 \le L_a \le N-1$ 을 새로 정의한다. 또한 D_a 와 J_a 의 각각에 대응되는 2 개의 새로운 set $\mathrm{D}_{e,a}$ 와 $\mathrm{J}_{e,a}$ 을 다음과 같이 새로이 정의한다.

$$\begin{aligned} \mathrm{D}_{e,a} &= \left\{ d_{e,a}(0), \cdots, d_{e,a}(L_a - 1) \right\}, \\ \mathrm{J}_{e,a} &= \left\{ j_{e,a}(0), \cdots, j_{e,a}(N - L_a - 1) \right\}, \end{aligned} \tag{26}$$

이 때 $\mathrm{D}_{e,a} \cap \mathrm{J}_{e,a} = \phi$ 와 $\mathrm{D}_{e,a} \cup \mathrm{J}_{e,a} = \{0, \cdots, N-1\}$ 의 관계가 성립한다. (24)와 (26)으로부터, 우리는 $y_e = [\overline{y}_e(0), \cdots, \overline{y}_e(L_a - 1)]^T$ 을 다음과 같이 구할 수 있다.

$$\overline{y}_e(k) = \tilde{y}_e(i), \text{ if } i = d_b(k) \in \mathrm{D}_{e,a}, \tag{27}$$

이를 통해 Alice 의 legitimate Tx data 에 대한 Eve 의 frequency domain recovery 를 다음과 같이 얻을 수 있다.

$$Y_e = B_{L_a} y_e. \tag{28}$$

Eve 가 Bob 의 legitimate data 를 도청하기 위한 processe 는, (14)의 y_e 와 (18)의 z_e' 가 각각 다음의 값으로 대체된다는 점을 제외하고는, (21)-(28)과 같다.

$$\begin{aligned} y_e &= g_b * x_b + z_e', \\ z_e' &= g_a * x_a + z_e. \end{aligned} \tag{29}$$

이 때, (16)의 $X_a = B_N x_a$ 와 G_a 또한 각각 $X_b = B_N x_b$ 와 $G_b = \mathrm{diag}([G_b(0), \cdots, G_b(N-1)]^T)$ ($[G_b(0), \cdots, G_b(N-1)]^T = \mathrm{FFT}_N(g_b)$)로 대체된다. 마지막으로 새로운 set $\mathrm{D}_{e,b}$ 와 $\mathrm{J}_{e,b}$ 는 새로이 적용된 값 L_b 에 대해 (26)이 성립하도록 정해질 수 있다.

4) Leakage of Information at Eve

Eve 가 Alice 혹은 Bob 의 legitimate information 을 도청하는 성능을 분석하기 위해 legitimate Tx Signal 과 Eve 의 Rx Signal 사이의 mutual information (MI)를 분석한다. 이 때 편의상 Eve 의 수신 신호와 Alice 의 송신 신호 사이의 MI 만을 분석하나 Eve

의 수신 신호와 Bob 의 송신 신호간 MI 도 동일한 방법으로 분석될 수 있다. legitimate information 을 위한 동작 과정도 동일하다.

Eve 가 복원한 frequency domain legitimate Tx symbols 을 앞서 (29)에 기술한 형태로 표현해서는 Eve 의 수신 신호와 Alice 의 송신 신호 사이의 MI 를 분석하기 어렵다 이는 Y_e가 x_a의 일부와 q_a의 또 다른 일부가 섞여있는 형태에 대한 FFT 를 통해 구해지기 때문이다. 따라서 우리는 x_a를 아래와 같이 다른 형태로 표현한다.

$$x_a = x_{a,w} + x_{a,q}, \tag{30}$$

이 때, $x_{a,w} = [\tilde{x}_{a,w}(0), \cdots, \tilde{x}_{a,w}(N-1)]^T$ 이며, 또한

$$\tilde{x}_{a,w}(k) = \begin{cases} w_a(i), & \text{if } k \in \mathrm{D}_a, \text{and } k = d_a(i), \\ 0, & \text{if } k \in \mathrm{J}_a, \text{and } k = j_a(i), \end{cases} \tag{31}$$

이다. 그리고 $x_{a,q} = [\tilde{x}_{a,q}(0), \cdots, \tilde{x}_{a,q}(N-1)]^T$ 이며, 이 때 다음과 같은 관계가 성립한다.

$$\tilde{x}_{a,q}(k) = \begin{cases} 0, & \text{if } k \in \mathrm{D}_a, \text{and } k = d_a(i), \\ q_a(i), & \text{if } k \in \mathrm{J}_a, \text{and } k = j_a(i). \end{cases} \tag{32}$$

이로 인해 (24)의 y_e 은 다음과 같이 수정된다.

$$y_e = x_{a,w} + x_{a,q} + z_e, \tag{33}$$

이를 이용하여 (27) 이후의 y_e를 다음과 같이 구할 수 있다.

$$y_e = x_{a,w}^{L_a} + x_{a,q}^{L_a} + z^{L_a}, \tag{34}$$

이 때 $x_{a,w}^{L_a} = [\bar{x}_{a,w}^{L_a}(0), \cdots, \bar{x}_{a,w}^{L_a}(L_a - 1)]^T$ 와 $x_{a,q}^{L_a} = [\bar{x}_{a,q}^{L_a}(0), \cdots, \bar{x}_{a,q}^{L_a}(L_a - 1)]^T$ 는 각

각 아래와 같이 주어진다.

$$\begin{aligned}\overline{x}_{a,w}^{L_a}(k) &= \tilde{x}_{a,w}(i), \text{if } i = d_b(k) \in \mathrm{D}_{e,a}, \\ \overline{x}_{a,q}^{L_a}(k) &= \tilde{x}_{a,q}(i), \text{if } i = d_b(k) \in \mathrm{D}_{e,a}.\end{aligned} \tag{35}$$

또한 $z^{L_a} = [\overline{z}^{L_a}(0), \cdots, \overline{z}^{L_a}(L_a - 1)]^T$ 는 다음과 같이 구해진다.

$$\overline{z}^{L_a}(k) = \tilde{z}_e(i), \text{if } i = d_b(k) \in \mathrm{D}_{e,a}. \tag{36}$$

따라서, (33)-(36)으로부터 (28)의 Y_e 를 다음과 같이 구할 수 있다.

$$Y_e = B_{L_a} x_{a,w}^{L_a} + B_{L_a} x_{a,q}^{L_a} + B_{L_a} z^{L_a}. \tag{37}$$

먼저 Alice 가 전송한 legitimate information 의 성능을 분석하기 위해 하나의 set $\mathrm{L}_{a,w} = \{l_{a,w}(0), \cdots, l_{a,w}(L_w - 1)\} = \mathrm{D}_a \cap \mathrm{D}_{e,a}$ 을 정의한다. 이 때 L_w 는 set $\mathrm{L}_{a,w}$ 의 element 수를 의미한다. 즉, $\mathrm{L}_{a,w}$ 는 w_a 내의 element 들 중 $x_{a,w}^{L_a}$ 에 포함된 element 들의 index set 을 의미하게 된다. 따라서 (37)의 $B_{L_a} x_{a,w}^{L_a}$ 는 다음과 같이 표현된다.

$$B_{L_a} x_{a,w}^{L_a} = B_{L_a}^{L_w} x_{a,w}^{L_w}, \tag{38}$$

이 때 $x_{a,w}^{L_w}$ 는 다음과 같이 주어진다.

$$x_{a,w}^{L_w} = \left[w_a\left(l_{a,w}(0)\right), \cdots, w_a\left(l_{a,w}(L_w - 1)\right) \right]^T. \tag{39}$$

또한 $B_{L_a}^{L_w}$ 은 아래와 같이 주어진다.

$$B_{L_a}^{L_w} = \left[b_{L_a}\left(l_{a,w}(0)\right), \cdots, b_{L_a}\left(l_{a,w}(L_w - 1)\right) \right], \tag{40}$$

이 때 $b_{L_a}(i)$ 는 B_{L_a} 의 i -th column vector 를 의미한다. 여기서 $x_{a,w}^{L_w}$ 가 index set

$\mathrm{L}_{a,w}$ 에 의해 선택된 w_a 의 일부임을 상기하면, $x_{a,w}^{L_w}$ 는 다시 아래와 같이 표현될 수 있다.

$$x_{a,w}^{L_w} = A_{M_a}^{L_w} W, \tag{41}$$

이 때 $A_{M_a}^{L_w}$ 는 아래와 같다.

$$A_{M_a}^{L_w} = \left[\left(a_{M_a}(l_{a,w}(0)) \right)^T, \cdots, \left(a_{M_a}(l_{a,w}(L_w - 1)) \right)^T \right]^T, \tag{42}$$

위의 (42)에서 $a_{M_a}(i)$ 는 A_{M_a} 의 i-th row vector 를 의미한다. 상기 (38)과 (41)로부터, (37)의 $B_{L_a} x_{a,w}^{L_a}$ 는 동등하게 아래와 같이 표현된다.

$$B_{L_a} x_{a,w}^{L_a} = C_{M_a}^{L_a} W. \tag{43}$$

이 때 $C_{M_a}^{L_a} = B_{L_a}^{L_w} A_{M_a}^{L_w}$ 이다.

Alice 의 Tx signal 에 포함된 jamming sequence 의 영향을 분석하기 위해 우리는 또 하나의 set $\mathrm{L}_{a,q} = \left\{ l_{a,q}(0), \cdots, l_{a,q}(L_q - 1) \right\} = \mathrm{D}_a \cap \mathrm{J}_{e,a}$ 을 정의한다. 이 때 L_q 는 set $\mathrm{L}_{a,q}$ 의 element 수를 의미한다. 그러면, $\mathrm{L}_{a,q}$ 는 $x_{a,q}^{L_a}$ 에 포함된 q_a 의 element 들의 index set 을 의미한다. 따라서, (37)의 $B_{L_a} x_{a,q}^{L_a}$ 는 아래와 같이 표현될 수 있다.

$$Q_a^{L_a} = B_{L_a} x_{a,q}^{L_a} = B_{L_a}^{L_q} x_{a,q}^{L_q}, \tag{44}$$

이 때 $x_{a,q}^{L_q}$ 와 $B_{L_a}^{L_q}$ 는 각각 아래와 같이 주어진다.

$$x_{a,q}^{L_q} = \left[q_a \left(l_{a,q}(0) \right), \cdots, q_a \left(l_{a,q}(L_q - 1) \right) \right]^T, \tag{45}$$

$$B_{L_a}^{L_q} = \left[b_{L_a}\left(l_{a,q}(0)\right), \cdots, b_{L_a}\left(l_{a,q}(L_q - 1)\right) \right]. \tag{46}$$

이 때, $x_{a,q}^{L_q}$ 는 $q_a : (0_N, P_a I_N)$ 중 L_q sample 을 선택함으로써 얻어지므로 $x_{a,q}^{L_q} : (0_{L_q}, P_a I_{L_q})$ 임을 상기하면, $x_{a,q}^{L_q}$ 의 linear transform 인 $Q_a^{L_a}$ 또한 complex Gaussian random vector 이며, 이 때 mean 과 covariance matrix 는 각각 다음과 같이 주어진다.

$$\mathrm{E}\left[Q_a^{L_a} \right] = B_{L_a}^{L_q} \left(\mathrm{E}\left[x_{a,q}^{L_q} \right] \right) = 0_{L_a}, \tag{47}$$

$$\mathrm{cov}\left(Q_a^{L_a} \right) = \mathrm{E}\left[B_{L_a}^{L_q} x_{a,q}^{L_q} \left(B_{L_a}^{L_q} x_{a,q}^{L_q} \right)^H \right] \tag{48}$$

$$= P_a B_{L_a}^{L_q} \left(B_{L_a}^{L_q} \right)^H. \tag{49}$$

여기서 x_b 가 CSCG random variable 의 vector, 즉 $x_b : \mathcal{CN}(0, P_b I)_N$ 로 간주될 수 있음을 상기하면, 다음과 같은 관계를 도출할 수 있다.

$$z_{e'} : \mathcal{CN}\left(0_N, \left(P_b \left| g_a \right|_2^2 + \sigma_e^2 \right) I_N \right), \tag{50}$$

이 때 $z_{e'}$ 는 N sample 로 이루어진 $z_{e'} = g_b * x_b + z_e$ 의 일부이며, (21)의 y_e 에서 CP 를 제거함으로써 얻을 수 있다. $Z_{e'} = B_N z_{e'}$ 로 얻어지는 (23)의 $Z_{e'}$ 는, (50)에서 추론할 수 있듯이 Eve 에서 AWGN 으로 작용한다. 또한, (32)의 z_e 는 다음과 같이 표현될 수 있다.

$$z_e = A_N G_a^{-1} B_N z_{e'}. \tag{51}$$

새로운 set L_z 를 다음과 같이 정의한다.

$$\mathrm{L}_{a,z} = \mathrm{L}_{a,w} \cup \mathrm{L}_{a,q} = \left\{ l_{a,z}(0), \cdots, l_{a,z}(L_a - 1) \right\}. \tag{52}$$

Eve 의 Rx signal y_e 로부터 (20)에 따라 L_a sample 을 선택한 후, (34)과 (36)에 주어진 z^{L_a} 는 동일하게 다음과 같이 표현될 수 있다.

$$z^{L_a} = A_N^{L_a} G_a^{-1} B_N z_{e'}, \tag{53}$$

이 때 $A_N^{L_a}$ 는 다음과 같이 주어진다.

$$A_N^{L_a} = \left[\left(a_N \left(l_{a,w}(0) \right) \right)^T, \cdots a_N \left(\left(l_{a,w}(L_a - 1) \right) \right)^T \right]^T, \tag{54}$$

여기서 $a_N(i)$ 은 A_N 의 i-th row vector 를 의미한다. 따라서 the effective receiver noise 와 Bob 의 전송에 의해 생성되는 interference 의 합에 대한 frequency domain representation 은 다음과 같다.

$$Z_e = C_e z_{e'}, \tag{55}$$

이 때 $C_e = B_{L_a} A_N^{L_a} G_a^{-1} B_N$ 이다. (55)의 random vector Z_e 는 $Z_e : \mathbb{CN}(0_{L_a}, D_{e,a} S_{e,a} D_{e,a}^H)$ 의 분포를 가지며, 이 때 covariance matrix 는 다음의 값을 이용해 표현된다.

$$D_{e,a} = B_{L_a} A_N^{L_a}, \tag{56}$$

$$S = \mathrm{diag}\left(\beta_a \left[|G_a(0)|^{-2}, \cdots, |G_a(N-1)|^{-2} \right]^T \right), \tag{57}$$

$$\beta_a = P_b |g_a|_2^2 + \sigma_e^2. \tag{58}$$

(43), (44), 그리고 (55)로부터, (37)의 Y_e 는 아래와 같이 표현될 수 있다.

$$Y_e = C_{M_a}^{L_a} W_a + Q_a^{L_a} + Z_e. \tag{59}$$

이 때 (59)를 통해 표현되는 시스템은 Gaussian multiple-input multiple-output channel 과 등가이며, 이 때 W_a, Y_e, $C_{M_a}^{L_a} W_a$, 그리고 $(Q_a^{L_a} + Z_e)$는 각각 input, output, channel, and noise 에 대응된다. 따라서, 주어진 D_a, $\mathrm{L}_{a,w}$, $\mathrm{L}_{a,q}$, 그리고 G_a에 대해, Alice 의 legitimate Tx Signal 와 Eve 의 Rx Signal 사이의 MI 는 아래와 같이 주어진다.

$$C_a\left(\mathrm{D}_a, \mathrm{L}_{a,w}, \mathrm{L}_{a,q}, G_a\right) = \log_2\left(\left| I_{L_a} + P_a C_{M_a}^{L_a}\left(U_a^{L_a}\right)^{-1}\right|\right), \tag{60}$$

이 때 $C_{M_a}^{L_a}$ 과 $U_a^{L_a}$ 는 각각 아래와 같이 주어진다.

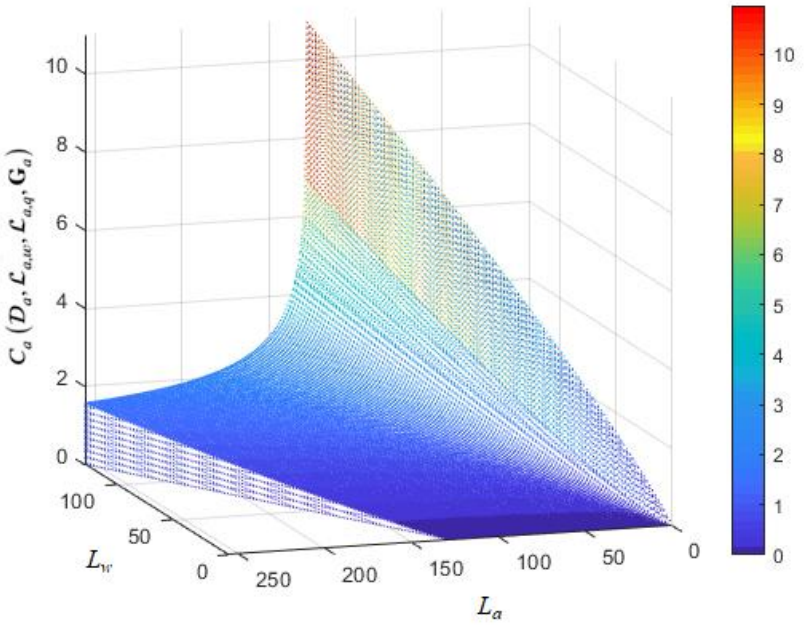
$$C_{M_a}^{L_a} = C_{M_a}^{L_a}\left(C_{M_a}^{L_a}\right)^H, \tag{61}$$

$$U_a^{L_a} = P_a B_{L_a}^{L_q}\left(B_{L_a}^{L_q}\right)^H + D_{e,a} S_{e,a} D_{e,a}^H. \tag{62}$$

<그림 23>은 x_a 에 w_a 와 함께 전송되는 jamming sequence q_a 가 $C_a\left(\mathrm{D}_a, \mathrm{L}_{a,w}, \mathrm{L}_{a,q}, G_a\right)$에 미치는 영향을 L_a와 L_w의 값에 따라 보여준다. 이 결과를 얻기 위해 N , M_a 그리고 G_a 의 값은 $N = 256$, $M_a = 128$, 그리고 $G_a = I_N$로 설정하였다. 또한 Alice 에서 jamming sequence q_a 의 삽입에 대한 효과에 집중하기 위해 $g_b = 0$, 즉 Bob 의 전송에 의한 interference 가 존재하지 않는 상황을 가정하였다. 또한 P_a와 σ_e^2는 $P_a / \sigma_e^2 = 30$ dB 가 되도록 설정하였다.

이 그림에서 볼 수 있듯이, $C_a\left(\mathrm{D}_a, \mathrm{L}_{a,w}, \mathrm{L}_{a,q}, G_a\right)$의 최대값은 $L_a = L_w = 128$

일 때 얻을 수 있으며, 이는 Eve 가 x_a 내에서 w_a 의 위치를 완벽하게 아는 경우에 해당된다. 이 경우, Alice 의 모든 정보는 Eve 에 의해 도청된다. 반면, $C_a\left(\mathrm{D}_a,\mathrm{L}_{a,w},\mathrm{L}_{a,q},G_a\right)$ 는 L_w 이 감소할수록 감소하는 동시에 L_a 가 증가할수록 감소한다. 특히 L_a 의 증가가 $C_a\left(\mathrm{D}_a,\mathrm{L}_{a,w},\mathrm{L}_{a,q},G_a\right)$ 의 감소에 보다 중요한 영향을 미침을 알 수 있다. 또한, Bob 의 전송에 의한 interference 가 없더라도 L_a 및 L_w 의 값이 충분히 작을 때 $C_a\left(\mathrm{D}_a,\mathrm{L}_{a,w},\mathrm{L}_{a,q},G_a\right)$ 의 값은 0 에 충분히 작아짐을 알 수 있다.



<그림 23> Jamming sequence 가 information leakage 에 미치는 영향

위의 <그림 23>에서의 MI 는 OFDM 의 orthogonality 를 고려하지 않았을 때 Eve

가 얻을 수 있는 legitimate information 의 단순 양을 의미한다. 따라서 OFDM system 에서 ST-jamming 에 의해 legitimate Tx signal 과 Eve 의 Rx signal 이 통계적으로 independent 한 경우라도 위의 MI 값은 0 보다 큰 값을 가질 수 있다.

5) 시뮬레이션 결과

앞서 성능 분석에 이어, 이번에는 Alice 와 Bob 의 transmission 으로부터 Eve 로의 information leakage 를 다양한 Eve 의 위치에 대해 시뮬레이션을 통해 분석한다. 이러한 Alice 와 Bob 의 Tx signal 과 Eve 의 Rx signal of Eve 사이의 mutual information 을 통해 계측된다.

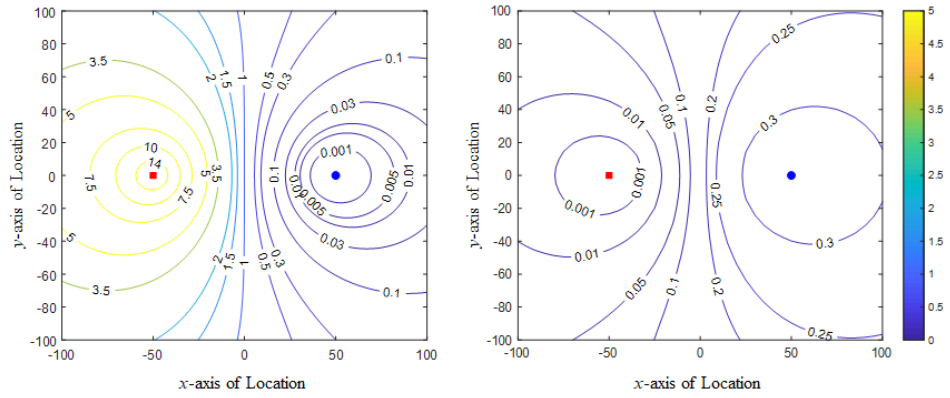
<그림 24> - <그림 26>은 Alice 의 Tx signal 과 Eve 의 Rx signal 사이의 mutual information(좌)과 Bob 의 Tx signal 과 Eve 의 Rx signal 사이의 mutual information (우)을 bps/Hz 의 단위로 보여준다. Alice 와 Bob 의 거리는 100m 로 고정되어 있으며, <그림 24> - <그림 26>에서 (-50,0)에 위치한 red square 는 Alice 를, (50,0)에 위치한 blue circle 은 Bob 을 의미한다.

Alice 와 Bob 에서 $P_a = P_b = 20$ dBm 과 $N = 512$ 를 가정하였다. 또한 M_a 는 $M_a = N$ 로 고정한 반면, Alice 와 Bob 사이의 traffic asymmetry 를 반영하기 위해 $M_b =$ 128 (<그림 24>), 256 (<그림 25>), and 384 (<그림 26>) 로 다양하게 설정하였다. Eve 에서는 Eve 가 Alice 및 Bob 이 전송한 data sample 들을 하나도 잃지 않도록 $L_a = L_b = N$ 로 두었다. 또한 channel bandwidth 와 Eve 에서의 noise spectral density 는 각각 20MHz 와 -174dBm/Hz 임을 가정했다. 이와 더불어 legitimate data sequence 와 동시에 전송되는 jamming sequence 의 영향에 집중하기 위해 Alice 와 Bob, 그리고 Eve 사이의 모든 wireless channel 들은 frequency-flat channel 들이되, channel 의 평균 power

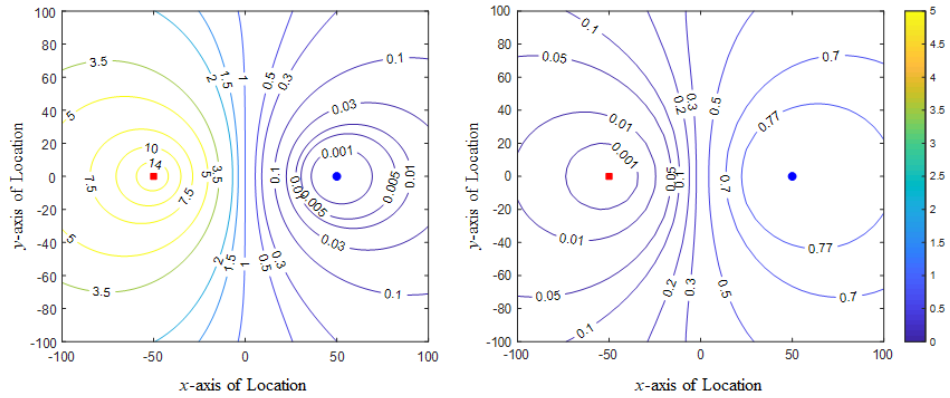
gain 만이 distance-dependent signal power attenuation 의 영향을 받음을 가정하였다. 따라서, G_a 와 G_b 는 각각 $G_a = \gamma_a I_N$ 와 $G_b = \gamma_b I_N$ 로 가정했으며, 이 때 $\gamma_a = |g_a|_2^2$ 와 $\gamma_b = |g_b|_2^2$ 는 각각 Alice 와 Bob 으로부터 Eve 로의 signal power attenuation 을 의미한다. Rreference distance 인 1m 거리에서의 power attenuation 이 30dB 라는 가정 하에, γ_a 와 γ_b 는 각각 $\gamma_a = 10^{-3} d_{ae}^{-\alpha}$ 와 $\gamma_b = 10^{-3} d_{be}^{-\alpha}$ 로 주어지며, 이 때 d_{ae} 와 d_{be} 는 각각 Alice 와 Bob 으로부터 Eve 까지의 거리를 의미한다. 마지막으로 path-loss exponent α 는 $\alpha = 4$ 라 가정하였다.

<그림 24> - <그림 26>에서 볼 수 있듯이, Alice 의 transmission 으로부터 발생하는 leakage of information 는 M_b 값의 영향을 받지 않는다. 이는 Alice 의 transmission 에 대한 secrecy 가 온전히 Bob 의 transmission 으로 인해 Eve 에서 발생하는 co-channel interference (CCI)에 의해 획득되기 때문이다. 따라서 Alice 의 transmission 에 대한 보안성은 Eve 가 Bob 과 가까이 위치하여 Eve 에서의 CCI 세기가 충분히 강할 때에는 높게 유지되지만, Eve 가 Alice 와 가까이 위치할 때에는 Alice 의 transmission 으로부터 많은 정보가 Eve 에게 누설되게 된다.

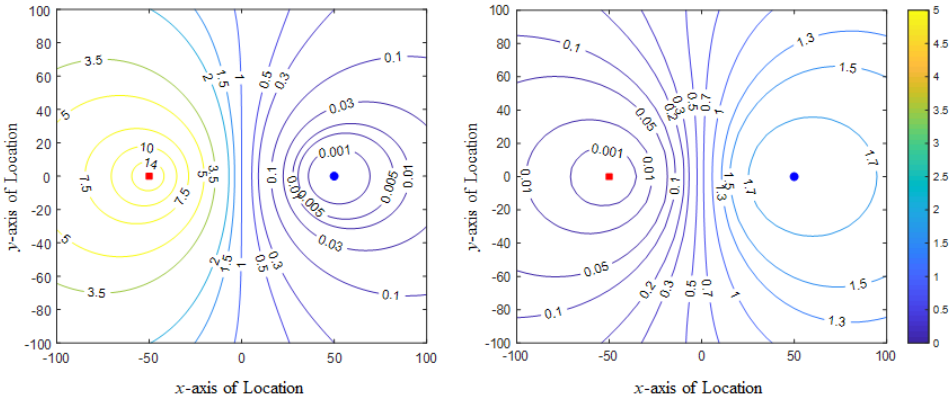
반면, Bob 의 Tx signal 과 Eve 의 Rx signal 사이의 mutual information 으로부터 볼 수 있듯이, ST-jamming 기술을 활용하여 jamming sequence 를 Tx signal 에 삽입하는 것은 Eve 에서의 정보 누설을 매우 효과적으로 감소시킨다. 특히 Eve 가 Bob 과 가까이 위치할 때의 secrecy 향상이 Eve 가 Alice 근처에 위치하는 경우에 비해 훨씬 두드러진다. 또한, Eve 에서의 정보 누설은 jamming sequence 의 길이가 커질수록 감소함을 알 수 있다.



<그림 24> Eve 의 위치에 따른 Alice (좌), Bob(우)으로부터의 정보 누설 ($M_b = 128$)



<그림 25> Eve 의 위치에 따른 Alice (좌), Bob(우)으로부터의 정보 누설 ($M_b = 256$)

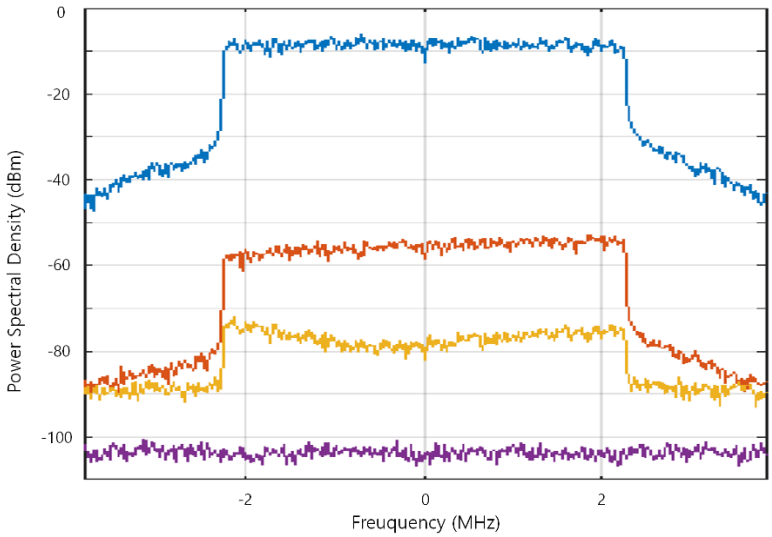


<그림 26> Eve 의 위치에 따른 Alice (좌), Bob(우)으로부터의 정보 누설 ($M_b = 384$)

3. Simultaneously-Transmitted Jamming 을 위한 송수신기의 설계 및 구현

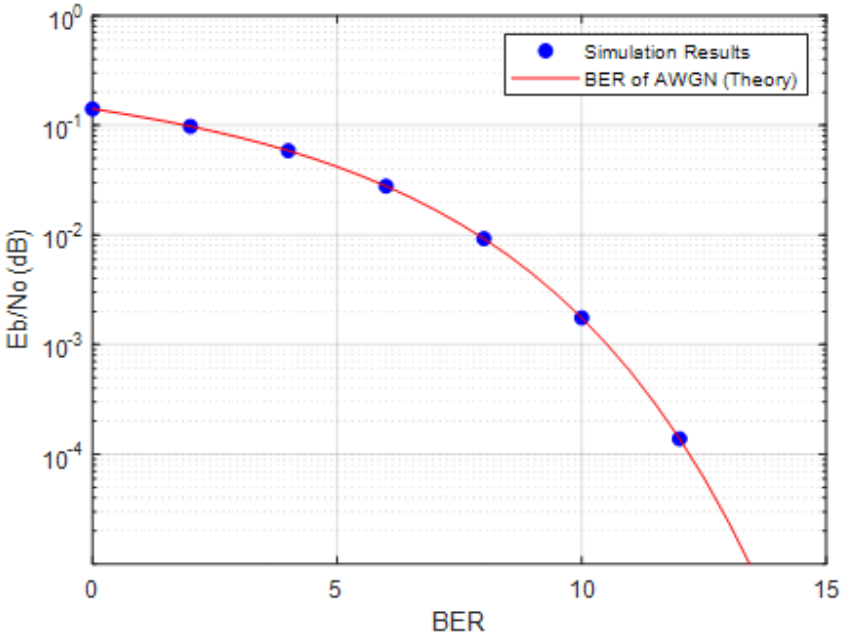
가. 동일대역 동시 송수신에 대한 Simulation 성능 검증

<그림 27>은 ASIC, HSIC, 그리고 DSIC 이전(파란색 그래프)과 이후(주황색 그래프)의 power spectral density 에 대한 simulation 결과를 보여준다. 이 그림에서 볼 수 있듯이, 전체 SIC 과정이 끝난 후 잔존 SI 는 background noise 와 동일한 level 까지 감소하며, 이로 인해 동일 대역에서 신호의 동시 송수신에 따른 interference 는 사실상 존재하지 않음을 알 수 있다.



<그림 27> SIC 에 따른 power spectral density 의 변화

<그림 28>은 모든 SIC 과정이 종료된 후 유효 수신 신호에 대한 bit-error rate 의 simulation 결과를 보여준다. <그림 28>에서 볼 수 있듯이 SIC 를 통해 모든 자기간섭이 제거되었으므로, 유효신호의 BER 은 자기간섭이 전혀 없는 환경에서의 BER 과 동일함을 알 수 있다.



<그림 28> SIC 이후 BER 성능 (16QAM)

<그림 27>과 <그림 28>에서 알 수 있듯이, 동일 대역에서 신호를 동시에 송수신 하더라도 제안된 SIC 기술을 적용함으로써 유효신호를 성공적으로 수신할 수 있다. 즉, 상향링크와 하향링크에서 시간이나 주파수 자원의 분할 없이 신호를 동일대역에서 동시에 송수신 할 수 있으므로, 이를 통해 본 과제의 성과 목표인 $w_D = w_U = 1$ 을 달성함을 알 수 있다.

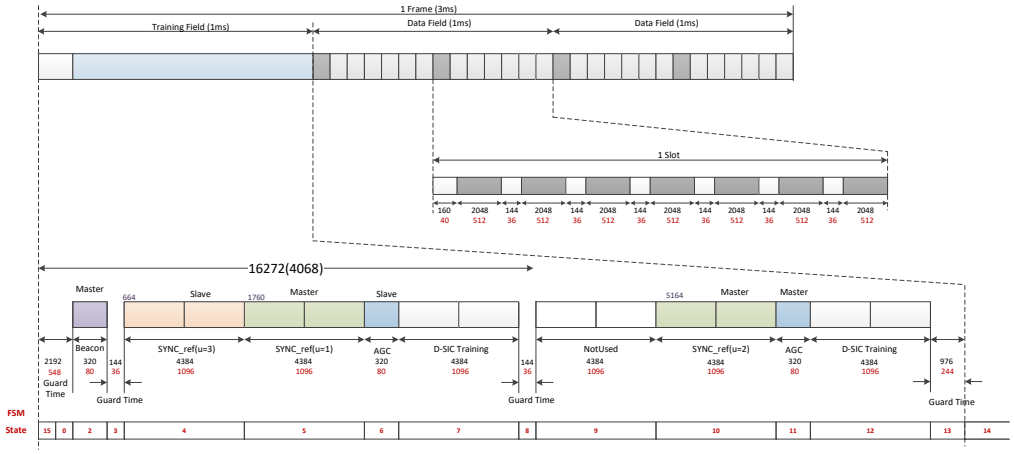
나. 프레임 구조 설계

ST-jamming 기술의 성능 검증 플랫폼 구현을 위한 전송 신호의 frame 구조는 LTE 의 frame 구조를 차용하되 beacon 및 SIC 를 위한 training 구간은 자체적으로 설계한다. 아래 <표 1>은 본 frame 구조의 주요 parameter 이다.

<표 1> Parameter Values

Parameter	Value
Channel bandwidth (MHz)	5
# of resource blocks	25
# of occupied subcarriers	300
Occupied bandwidth (MHz)	4.5
Subcarrier spacing (kHz)	15
Sampling frequency (MHz)	7.68
FFT size	512
Oversampling frequency (MHz)	7.68 x 4 = 30.72
Samples per slot (at over sampling rate)	15360

<그림 29>는 검증 플랫폼 구현을 위한 전송 신호의 frame 구조를 보여준다. 1 개의 frame 은 총 3ms 의 주기를 가지며, training field 와 data field, 그리고 guard time 으로 구성된다. 이 중 training field 와 data field 의 주기는 각각 928.6458us 와 2ms 이며, data field 에서의 전송이 끝난 후에는 1 개의 OFDM 심볼 주기에 해당하는 71.3542us 의 guard time 을 가진다.



<그림 29> Frame structure

Training field 구간동안에는, 먼저 master 가 beacon signal 을 전송하고 그 다음 slave 가 training sequence 를 전송한 후 다시 master 가 training sequence 를 전송한다. 이 때 beacon signal 의 주기는 10.417us 이며, slave 와 master 의 training sequence 의 주기는 각각 438.542us 이다. 또한, master 의 beacon 전송과 slave training sequence 전송 사이, 그리고 slave 의 training sequence 전송과 master 의 training sequence 전송 사이에는 각각 4.8675us 의 guard time 이 존재하며, master 의 training sequence 전송 후 data field 가 시작되기 전까지 31.7708us 의 guard time 이 존재한다. Data field 구간은 각각 0.5ms 의 주기를 가지는 4 개의 slot 으로 구성되며, 각각의 slot 은 7 개의 OFDM symbol 로 구성된다. 이 때, 각 slot 의 1 번째 OFDM symbol 은 71.875us 의 주기를 가지는 반면, 나머지 6 개의 OFDM symbol 은 71.3542us 의 주기를 가진다.

위에서 언급한대로, data field 는 LTE frame 을 차용하여 설계된 반면 training field 는 SIC 의 수행을 위해 자체적으로 설계되었으므로 training field 에서의 beacon sequence 와 training sequence 의 설계에 대해서 자세히 기술하도록 한다.

1) Beacon sequence

<표 2>는 beacon sequence 의 생성 과정을 보여준다. Beacon sequence 는 10.417us 의 주기를 가지며, 시간축 상에서 5 번 (CP 구간 포함) 반복되는 sequence 로 생성된다. Beacon sequence 는 7.68MHz 혹은 30.72MHz sampling 주파수를 통해 전송될 수 있다. 먼저 7.68MHz sampling 주파수를 통해 전송될 경우, 시간 영역에서 총 80 sample 로 구성되며, <표 2>의 sequence 가 5 번 반복되는 구조를 가진다. 다음 30.72MHz sampling 주파수를 통해 전송될 경우, 시간 영역에서 총 320 sample 로 구성되며, <표 3>의 sequence 가 5 번 반복되는 구조를 가진다. 이와 같이 생성된 beacon signal 은 주파수 영역에서는 3.84 MHz 대역폭 내에 분포하게 된다.

<표 2> 7.68MHz sampling 주파수를 사용할 때 beacon sequence 의 반복 신호

Index	Sample Value	Index	Sample Value
0	0.0000 + 0.0000*i*	8	0.0000 + 0.0000*i*
1	-0.0780 - 0.0104*i*	9	-0.0104 - 0.780*i*
2	-0.0625 - 0.0625*i*	10	-0.0625 - 0.0625*i*
3	0.1259 - 0.0375*i*	11	-0.0375 + 0.1259*i*
4	0.2500 + 0.0000*i*	12	0.0000 + 0.2500*i*
5	0.1259 - 0.0375*i*	13	-0.0375 + 0.1259*i*
6	-0.0625 - 0.0625*i*	14	-0.0625 - 0.0625*i*
7	-0.0780 - 0.0104*i*	15	-0.0104 - 0.0780*i*

<표 3> 30.72MHz sampling 주파수를 사용할 때 beacon sequence 의 반복 신호

Index	Sample Value	Index	Sample Value	Index	Sample Value	Index	Sample Value
0	0.0000 + 0.0000*i*	16	0.1250 + 0.0000*i*	32	0.0000 + 0.0000*i*	48	0.0000 + 0.1250*i*
1	-0.0078 + 0.0042*i*	17	0.1205 - 0.0015*i*	33	0.0042 - 0.0078*i*	49	-0.0015 + 0.1205*i*
2	-0.0180 + 0.0045*i*	18	0.1076 - 0.0057*i*	34	0.0045 - 0.0180*i*	50	-0.0057 + 0.1076*i*
3	0.0000 + 0.0000*i*	19	0.0877 - 0.0118*i*	35	0.0011 - 0.0291*i*	51	-0.0118 + 0.0876*i*
4	-0.0291 + 0.0010*i*	20	0.0629 - 0.0187*i*	36	-0.0052 - 0.0390*i*	52	-0.0187 + 0.0629*i*
5	-0.0390 - 0.0052*i*	21	0.0360 - 0.0252*i*	37	-0.0130 - 0.0457*i*	53	-0.0252 + 0.0360*i*
6	-0.0456 - 0.0130*i*	22	0.0098 - 0.0300*i*	38	-0.0208 - 0.0473*i*	54	-0.0300 + 0.0097*i*
7	-0.0473 - 0.0208*i*	23	-0.0133 - 0.0322*i*	39	-0.0272 - 0.0427*i*	55	-0.0322 - 0.0133*i*
8	-0.0427 - 0.0272*i*	24	-0.0313 - 0.0313*i*	40	-0.0313 - 0.0313*i*	56	-0.0313 - 0.0313*i*
9	-0.0313 - 0.0313*i*	25	-0.0427 - 0.0272*i*	41	-0.0322 - 0.0133*i*	57	-0.0272 - 0.0427*i*
10	0.0097 - 0.0300*i*	26	-0.0473 - 0.0208*i*	42	-0.0300 + 0.0097*i*	58	-0.0207 - 0.0473*i*
11	0.0360 - 0.0252*i*	27	-0.0457 - 0.0130*i*	43	-0.0252 + 0.0360*i*	59	-0.0130 - 0.0457*i*
12	0.0629 - 0.0187*i*	28	-0.0390 - 0.0052*i*	44	-0.0187 + 0.0629*i*	60	-0.0051 - 0.0390*i*
13	0.0877 - 0.0118*i*	29	-0.0291 + 0.0011*i*	45	-0.0118 + 0.0877*i*	61	0.0010 - 0.0291*i*
14	0.1076 - 0.0057*i*	30	-0.0180 + 0.0045*i*	46	-0.0057 + 0.1076*i*	62	0.0045 - 0.0180*i*
15	0.1205 - 0.0015*i*	31	-0.0079 + 0.0042*i*	47	-0.0015 + 0.1205*i*	63	0.0042 - 0.0078*i*

2) Training sequence

Training field 동안 master와 slave가 전송하는 training sequence는 서로 동일하며, 각각 HSIC training sequence, DSIC training sequence, 그리고 AGC training sequence로 구성된다. 이 때, HSIC training sequence, DSIC training sequence, 그리고 AGC training sequence는 각각 285.416us, 142.708us, 그리고 10.417us의 주기를 가진다. AGC training sequence로는 beacon과 동일한 sequence가 사용된다.

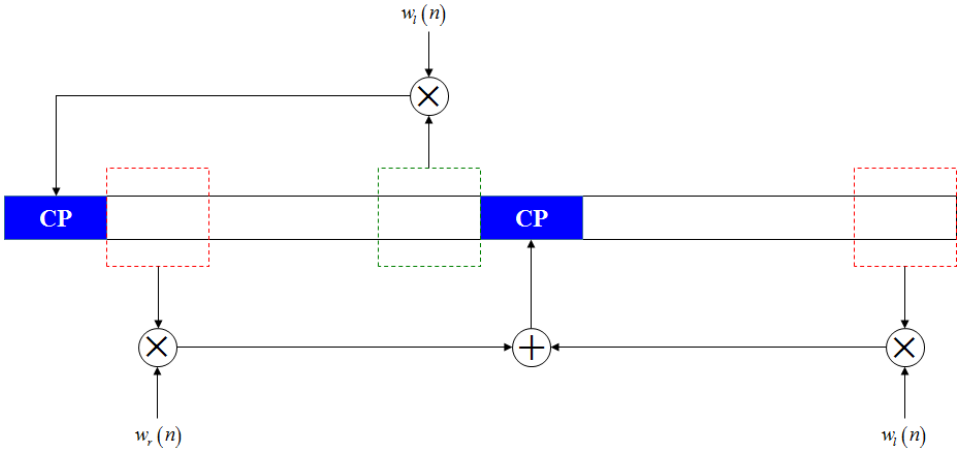
DSIC training sequence는 2개의 OFDM symbol로 구성되며, 각각의 OFDM symbol은 71.3542us의 주기를 가진다. DSIC training sequence를 구성하는 각각의 OFDM symbol은 다음의 과정을 통해 생성된다. DSIC training sequence는 512-point IFFT를 이용해 생성된다. LTE의 규격을 차용하는 data filed의 구조에 맞춰 D-SIC training sequence 또한 4.5MHz 대역폭 내의 300개의 subcarrier만을 사용한다. 또한 DSIC training의 목적이 비선형 성분의 다양한 SI에 대한 채널 coefficient의 추정이므로, DSIC training sequence의 amplitude는 큰 폭으로 변화하는 특성을 지니는 것이 좋다. 따라서, DSIC training sequence를 생성하기 위한 i 번째 안테나의 j 번째 OFDM symbol에 대한 주파수 영역의 신호(즉, IFFT 입력)는 다음과 같이 주어진다.

$$D_{i,j}(k) = \sqrt{\frac{512}{\beta}} \times \begin{cases} d_i(k), & -150 \le k \le -1,\ 1 \le k \le 150 \\ 0, & \text{otherwise} \end{cases}. \quad (63)$$

수식 (63)에서 $k \in \{-256, 255\}$는 subcarrier index이며, 또한 i=1과 $j \in \{1,2\}$는 각각 Tx antenna와 symbol index이다. 또한 $d_i(k) \sim \mathcal{CN}(0,1)$ 255로 주어진다. Normalization factor β는 IFFT output의 power를 1로 normalize하기 위해 사용되며, 다음과 같이 주어진다.

$$\beta = \sum_{k=-256}^{255} \left| d_i(k) \right|^2. \tag{64}$$

위와 같이 생성된 IFFT output 은 parallel-to-serial conversion 후 CP insertion 과 ADC 을 거쳐 analog & RF 영역으로 전달된다. 이 때, 각 안테나의 1 번째 OFDM symbol 과 2 번째 OFDM symbol 의 연속적인 전송으로 인해 발생하는 high frequency term 의 효과를 상쇄하기 위해 <그림 30>과 같이 windowed CP 를 삽입한다.



<그림 30> Windowed CP insertion

먼저 1 번째 transmit antenna 의 j 번째 symbol 에 대한 IFFT output 의 n 번째 sample 을 $d_{i,j}(n)$, $0 \le n \le 511$ 이라 하고, 이 symbol 의 CP 신호를 $c_{i,j}(m)$, $0 \le m \le 144$, 이라 한다. 각 안테나에 대해 $c_{i,1}(m)$과 $c_{i,2}(m)$는 각각 다음과 같이 주어진다.

$$c_{i,1}(m) = d_{i,1}(368+m)\, w_l(m), \quad 0 \le m \le 143, \tag{65}$$

$$c_{i,2}(m) = d_{i,2}(368+m)\, w_l(m) + d_{i,1}(m)\, w_r(m), \quad 0 \le m \le 143. \tag{66}$$

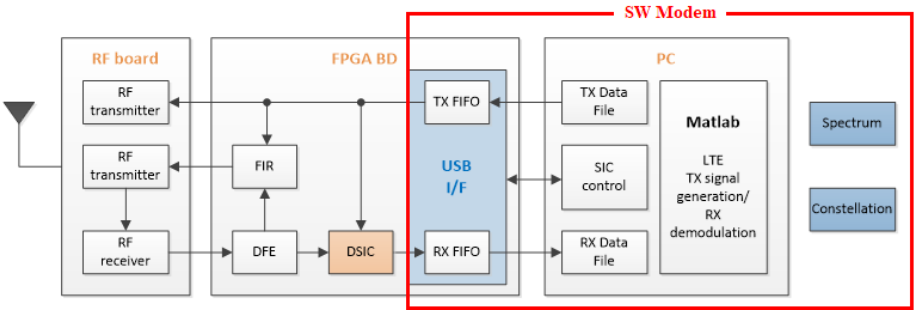
이 때, windowing 함수 $w_l(m)$과 $w_r(m)$은 각각 다음과 같이 주어진다.

$$w_l(m)=\left(\cos\left(\frac{\pi(144-m)}{288}\right)\right)^2,\ 0\le m\le 143, \tag{67}$$

$$w_r(m)=\left(\cos\left(\frac{\pi(m+1)}{288}\right)\right)^2,\ 0\le m\le 143. \tag{68}$$

다. 양방향 물리계층 보안 통신을 위한 SW 모뎀 설계

<그림 31>은 본 과제에서 개발하는 ST-jamming 을 위한 SW 모뎀의 구조를 보여준다. 본 SW modem 은 host PC 에서 MATLAB 을 통해 송신 신호의 생성해 Tx FIFO 를 통해 HW 송수신기로 생성된 송신 신호를 전송하고, 이와 동시에 Rx 를 통해 HW 송수신기로부터 전달받은 수신 샘플을 host PC 에서 MATLAB 을 통해 처리한다 (Tx/Rx FIFO 를 통한 HW 송수신기와 SW modem 간 인터페이스의 설계 및 구현은 다음 절에서 다룬다). 또한 AGC 와 synchronization 기능을 함께 수행한다.

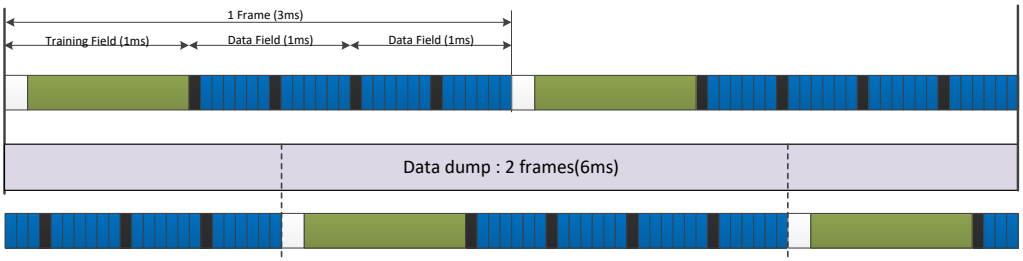


<그림 31> SW modem 의 구조

1) HW 송수신기와의 송수신 sample stream 교환

<그림 32>는 Tx FIFO 와 Rx FIFO 를 통한 HW 송수신기와 SW modem 간 sample stream 의 교환을 보여준다. 먼저 Tx FIFO 를 통한 송신 sample stream 전송시에는 <

그림 29>의 3ms frame 을 단위로 sample stream 을 전송한다. 이 때 host PC 에서 추가적인 sample stream 이 만들어지 않을 경우에는 계속해서 같은 sample stream 을 반복하여 전달한다. Rx FIFO 를 통해 HW 송수신기에서 수신 sample stream 을 받아올 때에는 하나의 frame 주기의 2 배인 6ms 의 sample stream 을 받아온다. 이는 SW modem 에서 동기를 맞추는 과정에서 frame 수신 샘플의 손실을 방지하기 위해서이다.



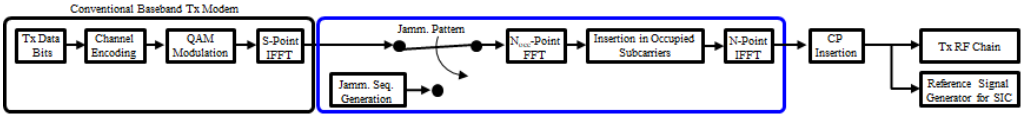
<그림 32> HW 송수신기로와의 송수신 sample stream 교환

2) AGC 및 Synchronization

본 기능은 HW 송수신기와 SW modem 사이의 인터페이스 연동되어 기능한다. 동작 알고리즘은 일반적인 LTE 의 AGC 및 synchronization 알고리즘을 따르며, <표 2>와 <표 3>에서 주어지는 beacon sequence 를 이용하여 수행된다. AGC 및 synchronization 의 구체적인 제어는 HW 송수신기와 SW modem 사이의 인터페이스에서 수행되며, synchronization 의 경우에는 Rx FIFO 로 받은 수신 sample stream 의 beacon sequence 부분을 활용하여 time synchronization → coarse frequency synchronization → fine frequency synchronization 의 순서를 따른다.

3) SW modem 송신부

<그림 33>은 본 과제에서 개발하는 SW modem 의 송신부를 보여준다. 본 SW modem 은 5MHz channel bandwidth 에서 512 개의 subcarrier 중 300 개의 occupied subcarrier 를 사용하는 LTE frame format 으로 생성된 OFDM 심볼을 <그림 29>의 frame 구조에 맞춰 생성한다. 즉, 212 개의 subcarrier 는 null subcarrier 로 사용되며, <그림 33>의 SW 모뎀은 이러한 null subcarrier 가 있을 때 <그림 11>과 <그림 16>의 jamming 삽입 기술이 사용할 수 있게 한다 (이후, N 은 전체 subcarrier 의 수 512 를, N_{occ} 는 occupied subcarrier 의 수 300 을, S 는 기저대역 모뎀 송신부에서 생성하는 주파수 영역 data symbol 의 개수를 의미하며, $N > N_{occ} \geq S$ 의 관계가 성립한다.)



<그림 33> ST-Jamming 시스템 SW 모뎀부의 블록도

<그림 33>에서 'conventional banseband Tx modem'으로 표기된 블록들은 OFDM 전송을 기반으로 하는 일반적인 (IFD) 기저대역 모뎀 송신부와 유사하며, S 개의 QAM 심볼에 대한 S-point IFFT 를 수행하여 S-sample IFFT output 을 생성한다. 이렇게 생성된 S-sample IFFT output 에 주어진 jamming sample pattern 에 따라 N_{occ} - S 개의 jamming sample 을 삽입하여 총 N_{occ} 개의 sample 을 생성한다. 이렇게 생성된 N_{occ} 개의 sample 에 대해 N_{occ}-point FFT 수행한 후, 이를 N_{occ} 개의 occupied subcarrier 에 삽입하고, 여기에 $N - N_{occ}$ 개의 null subcarrier 를 추가하여 N 의 길이를 가지는 주파수 영역 전송 신호를 생성한다. 길이 N 의 주파수 영역 전송 신호에 대해 N-point IFFT 를

수행하여 시간 영역 전송 신호를 생성한 후 여기에 cyclic prefix (CP)를 붙여 기저대역 OFDM 전송 심볼을 생성한다.

<그림 29>의 frame 구조의 data field 에서 각 subframe 은 다음과 같이 활용된다.

- 1 번 subframe 의 1 번째 OFDM symbol : channel estimation 을 위한 pilot 으로 활용되며 zero-mean unit variance 를 가지는 circularly symmetric complex Gaussian sequence 로 미리 생성됨
- 1 번 subframe 의 2 번째 OFDM symbol : jamming sequence 삽입 및 data encoding/decoding 을 위한 header 로 사용되며 QPSK modulation 과 repetition coding 을 이용해 생성됨. . Header symbol 에는 아래와 같은 정보가 포함됨.
  - TxHeaderModQAM : data symbol 의 modulation 정보. QPSK, 16QAM, 64QAM, 256QAM 의 modulation order 를 전송할 수 있으며 2 개의 bit 를 점유함.
  - TxHeaderDataQAM : ST-jamming 기술이 적용될 때 주파수영역 데이터 심볼 수 (S)
  - TxJammPatternIndex : ST-jamming 의 codebook 에서 jamming sequence 의 index
- 1 번 subframe 의 3 번째 OFDM symbol – 4 번 subframe 의 7 번째 OFDM symbol : ST-jamming 기술이 적용된 data symbol 의 전송을 위해 사용됨.

다음은 <그림 33>의 SW modem 송신부의 동작을 위해 사용되는 함수들과 그 기능을 정의한다.

함수명	HeaderEncoding.m
입력	NumDataSamples, NumRepHeader, Mod
출력	TxHeaderSymbols, JammIndex
기능	내부 함수를 동작시켜 ST-jamming 을 위한 header sequence 를 생성함

함수명	HeaderEncodingTxJamming.m
입력	NumRepHeader, NumOccSubcarrier
출력	TxHeaderJammIndexQAM, TxJammPatternIndex
기능	Jamming sequence 의 index 에 대한 header sequence 생성

함수명	HeaderEncodingModulation.m
입력	Mod
출력	TxHeaderModQAM
기능	Data symbol 의 modulation 에 해당되는 header sequence 생성

함수명	HeaderEncodingDataLength.m
입력	NumSubcarrierData
출력	TxHeaderDataQAM
기능	Data symbol 의 data sample length 에 해당되는 header sequence 생성

함수명	IndexCreator.m
입력	JammPatternIndex, NumJamSamples
출력	DataIndex, JammIndex
기능	Jamming sequence 의 index 에 대한 header sequence 로부터 Tx 내에서 jamming sequence 와 data sequence 가 각각 차지하는 sample index 생성

함수명	TxEncoder.m
입력	DataIndex, JammIndex, NumDataSamples, NumJamSamples, TxHeaderSymbols, Mod
출력	TxBits, TxQAMSym, TxDataSymbols
기능	Jamming sequence 삽입 전 주파수 영역 OFDM symbol stream 생성 Jamming sequence 가 삽입된 시간영역 전송신호 생성 Tx header 와 시간영역 전송신호가 포함된 data field 의 Tx sequence 생성

함수명	JammInsertedModulation.m
입력	InputBits, DataIndex, JammIndex, Mod NumDataSamples, NumJamSamples, NumSymDaata,
출력	TxData, TxQAMSymbols
기능	TxEncoder 의 내부 함수 Jamming sequence 삽입 전 주파수 영역 OFDM symbol stream 생성 Jamming sequence 가 삽입된 시간영역 전송신호 생성

함수명	TxSignalGeneration.m
입력	TxPilotOFDM, TxDataSymbols, ScalingFactor,
출력	TxSequence_DataField
기능	1 개의 frame 전송을 위한 data field 생성

4) SW modem 수신부

본 과제에서 개발하는 SW modem 의 수신부 구조는 <그림 15>의 수신부 구조와 동일하다. SW modem 의 수신부는 Rx FIFO 를 통해 HW 송수신기로부터 전달받은 1 개 frame 수신 샘플들로부터 channel estimation, header decoding, jamming sequence 제거, OFDM demodulation 등의 과정을 수행한다.

다음은 <그림 15>의 SW modem 수신부의 동작을 위해 사용되는 함수들과 그 기능을 정의한다.

함수명	RxSignalRecovery.m
입력	RxSequence, ScalingFactor
출력	RxPilotSymbols, RxDataSymbols
기능	수신 sample 들 중 pilot 부분과 데이터 부분(header 포함)을 분리

함수명	ChannelEstimation.m
입력	RxPilotSymbols, RxPilotFreq
출력	EstChannel
기능	수신된 pilot symbol 을 이용하여 주파수 영역 무선 채널을 추정

함수명	RxDecoder.m
입력	RxDataSymbols, EstChannel, NumRepHeader
출력	RxBits, RxQAMSym, EstMod, RxJammPatterIndex
기능	내부 함수를 동작시켜 수신 신호에 대한 채널 equalization, jamming sequence 제거, data sample 복조 등의 기능을 수행
비고	SW modem 수신부의 수신 신호 처리 top function

함수명	HeaderDecoding.m
입력	RxHeader, NumRepHeader, LengJammIndex, EstChannel
출력	EstMod, EstNumDataSamples, RxJammPatternIndex
기능	Header 에 포함된 정보 decoding 에 대한 top function 으로, 최종적으로 modulation order, data sample length, codebook 내 jamming sequence index 의 추정값을 출력함.

함수명	HeaderDecodingModulation.m
입력	RxHeader, NumRepHeader, LengJammIndex, EstChannel
출력	EstMod, EstNumDataSamples, RxJammPatternIndex
기능	HeaderDecoding.m 의 내부함수로, data field 의 OFDM symbol 들에 대한 modulation order 의 추정값을 출력함.

함수명	HeaderDecodingRxJamming.m
입력	RxHeader, NumRepHeader, LengJammIndex, EstChannel
출력	EstMod, EstNumDataSamples, RxJammPatternIndex
기능	HeaderDecoding.m 의 내부함수로, codebook 내 jamming sequence index 의 추정값을 출력함.

함수명	HeaderDecodingDataLength.m
입력	RxHeader, NumRepHeader, LengJammIndex, EstChannel
출력	EstMod, EstNumDataSamples, RxJammPatternIndex
기능	HeaderDecoding.m 의 내부함수로, data sample length 의 추정값을 출력함.

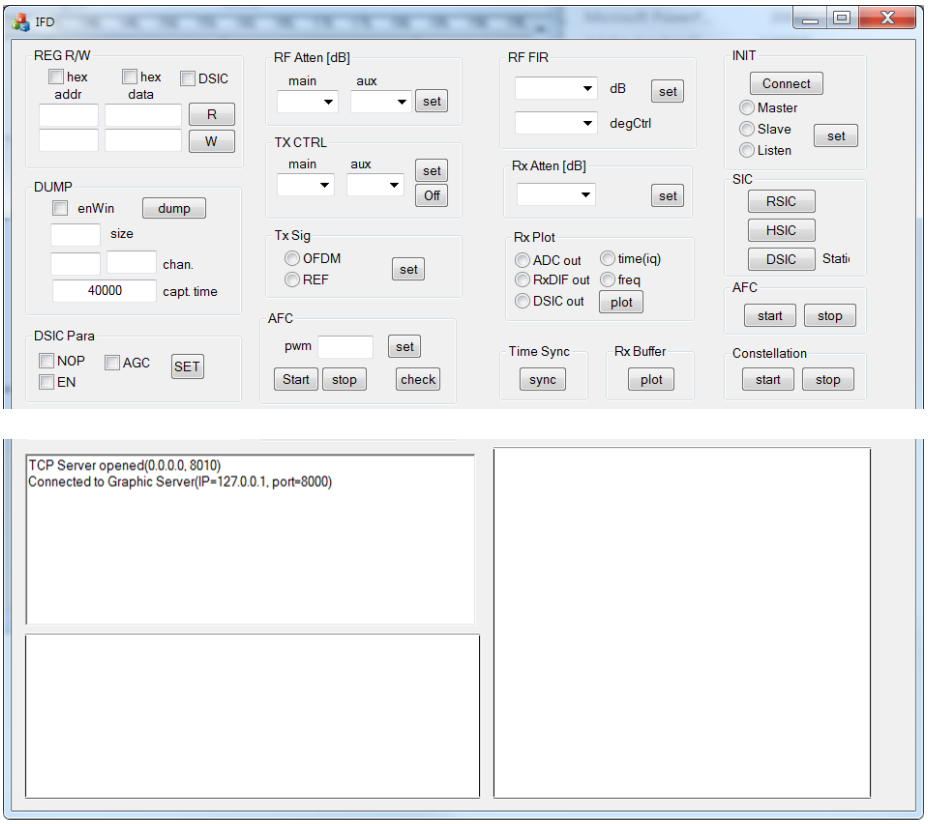
함수명	RxJammRemover.m
입력	RxData, EstJammIndex, EstNumDataSamples, EstChannel
출력	RxJammOut
기능	시간영역 수신 신호로부터 jamming sequence 제거
비고	

함수명	DataDecoding.m
입력	RxJammOut, EstMod, EstNumDataSamples, NumSymData
출력	RxBitsSF, RxQAMSymSF
기능	Subframe 단위의 Rx 복조 신호 출력
비고	

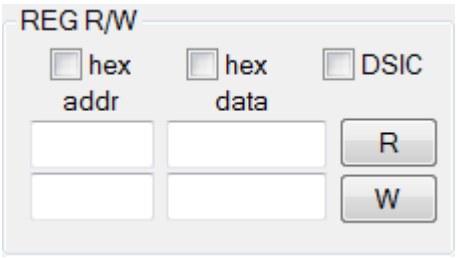
라. HW 송수신기와 SW 모뎀간 인터페이스 설계 및 구현

1) 제어부

아래 그림은 메인 창 화면 구성을 나타낸 것으로, 주로 HW 송수신기의 RF 및 FPGA 에서 수행되는 기능의 제어를 수행한다. 각 제어 그룹별 기능은 아래에 순차적으로 기술한다.

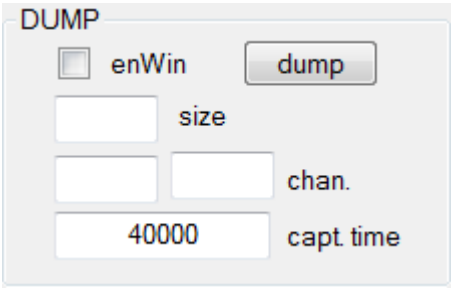


REG R/W 그룹: FPGA 내부 레지스터들을 읽고 쓰는데 사용함



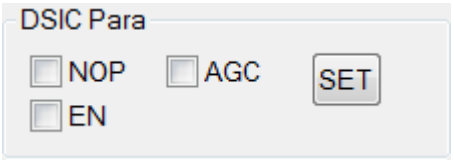
캡션	기능
hex	텍스트 박스에 입력한 주소와 데이터가 십진수인지 16 진수인지를 설정함
DSIC	DSIC 블록 레지스터를 읽을 것인지 그 외부 블록 레지스터인지를 설정함
R	레지스터 값을 읽음
W	레지스터 값을 씀

DUMP 그룹: FPGA 내부 각 블록들의 출력값을 도시하는 데 사용함

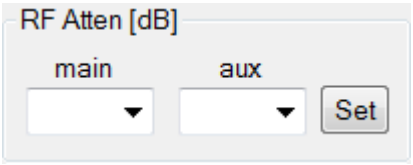


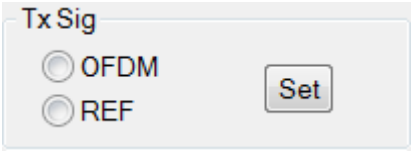
캡션	기능
enWin	측정 데이터의 스펙트럼을 그릴 때 윈도우 적용 여부를 설정함
size	측정 데이터의 시간 샘플 개수를 설정함
chan	Dump 받을 채널을 설정함
capt. time	DSIC 출력값을 받을 때 Rx Timer 의 timing 값을 설정함
dump	데이터를 캡쳐하고 PC 로 가져오는 기능 수행

DSIC Para 그룹: DSIC 블록의 기능을 제어함.

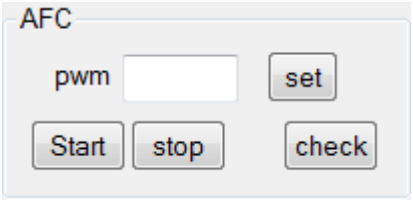


캡션	기능
NOP	DSIC 블록의 기능을 OFF 함
AGC	AGC 동작 여부를 설정함
EN	DSIC 동작의 OFF 함
SET	UI 설정값을 적용함

Tx RF Atten 그룹: RF 송신부의 감쇄값을 제어함		
	캡션	기능
	Main	Main 송신 채널값의 이득을 설정함
	Aux	Aux 송신 채널값의 이득을 설정함
	SET	설정된 값을 적용함

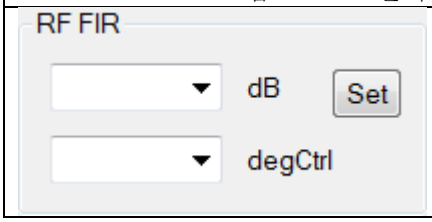
DSIC Para 그룹: DSIC 블록의 기능을 제어함.		
	캡션	기능
	Main	Main 송신채널의 FIR 필터값을 설정함 0: 모든 필터 계수를 0 으로 함 1: 가운데 탭값을 1 로하고 나머지는 0 으로 설정함 2: HSIC 에서 계산한 값을 적용함
	Aux	Aux 송신채널의 FIR 필터값을 설정함 0: 모든 필터 계수를 0 으로 함 1: 가운데 탭값을 1 로하고 나머지는 0 으로 설정함 2: HSIC 에서 계산한 값을 적용함
	Set	텍스트 박스에 입력된 값에 따라 FIR 필터 계수를 설정함
	off	Main/Aux 채널의 FIR 필터 계수를 모두 0 으로 함
Tx Sig 그룹: 송신할 데이터를 선택하는 데 사용함.		
	캡션	기능
	OFDM	3msec 프레임 데이터를 전송하도록 설정
	REF	시스템 시험용으로 15MHz 대역의 기준 신호를 전송하도록 설정
	Set	UI 설정값을 적용함

AFC 그룹: Slave 혹은 Listen 모드에서 시간/주파수 동기화를 수행할 때 사용함.



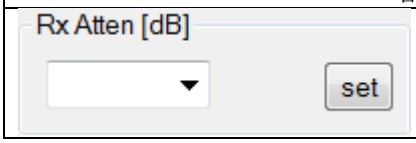
캡션	기능
Pwm	FPGA 내부 PWM 발생기의 펄스 폭을 제어함
Start/stop	시간/주파수 동기를 자동으로 찾는 블록을 동작(중지) 시키는 데 사용함.
Set	PWM 입력값을 FPGA 에 Write 함
check	Master 에서 전송하는 두 개의 SYNC 채널 간 위상값을 측정하여 주파수 동기가 정상적인지 확인함

RF FIR 그룹: RF FIR 필터의 위상변위기와 전력감쇄기를 제어함.



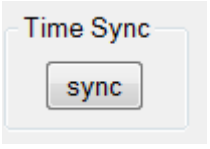
캡션	기능
dB	전력감쇄값을 설정함
dgCtrl	위상변위기의 제어값을 설정함
Set	UI 설정값을 적용함

Rx Atten 그룹: 수신기의 이득을 제어한다.

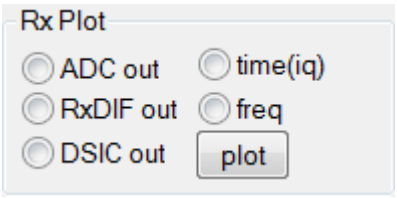


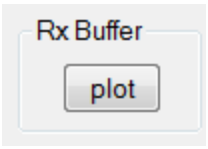
Dropbox 에 설정된 값들 중 선택

Time Sync: Master(혹은 Slave)가 송신하는 동기채널을 이용하여 timing 오차를 수정하고, 다시 데이터를 수신 후 동기채널 상관값을 도시함.

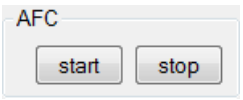


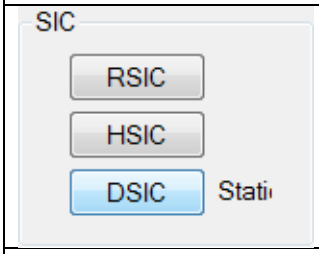
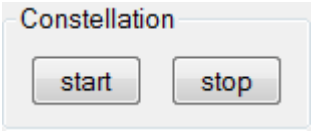
Button press

Rx Plot 그룹: 수신단 각 블록의 출력값을 시간 혹은 주파수 영역에서 도시함.		
	캡션	기능
	ADC out	ADC 출력값 선택, 샘플링주파수: 122.88 MHz
	RxDIF out	DSIC 이전의 신호값 선택 (샘플링 주파수:30.72MHz)
	DSIC out	DSIC 이후의 신호값 선택 (샘플링 주파수: 7.68MHz)
	time (iq)	수신 데이터를 시간영역에서 도시
	freq	수신 데이터를 주파수 영역에서 도시
	plot	설정한 입력값을 적용하고 데이터를 도시함

Rx Buffer 그룹: 6msec 동안 수신된 데이터를 도시함.	
	Button press

Init 그룹: DSP 서버와 연결을 하고, 동작 모드를 설정한다.		
	캡션	기능
	Connect	DSP 서버에 접속함. DSP 서버는 192.168.1.254 로 IP 고정
	Mastter	Master 모드 설정
	Slave	Slave 모드 설정
	Listen	Listen 모드 설정
	Init	모드 설정을 하고, TxBuffer 에 3msec 데이터를 전송함

AFC 그룹: 시간/주파수 Lock 이 될 때까지 PWM 값을 조정함.		
	캡션	기능
	Start	시간/주파수 동기 추적을 시작함
	Stop	시간/주파수 동기 추적을 중지함

RF FIR 그룹: RF FIR 필터의 위상변위기와 전력감쇄기를 제어함.		
	캡션	기능
	RSIC	RF SIC 기능을 수행함
	HSIC	Hybrid SIC 기능을 수행함
	DSIC	디지털 SIC 기능을 ON/OFF 설정함
Constellation 그룹: 모뎀처리를 수행하여 성상도를 그래프에 도시함.		
	캡션	기능
	Start	수신 데이터를 로딩하여 모뎀 처리하여 성상도를 연속적으로 그림
	Stop	성상도 처리하여 도시하는 것을 중단함

2) 신호처리부: 신호처리부는 제어부와 TCP/IP 를 통하여 통신을 하며 주요 함수 및 기능은 아래와 같음.

① TCP/IP 함수

TCP 패킷 제작 함수		
함수명	makePkt(msgId, cmdId, pktType, data, dataLen)	
기능	H1	Sync
	H2	msg_id
	H3	cmdId
	H4	pktType
	H5	dataLen
		data
입력	sync : 송수신 데이터 동기화 확인 패킷 msg_id : 메세지 번호 cmd_id : 명령어 번호 pktType : 데이터 패킷 번호 dataLen : 데이터 길이 data : 데이터	
출력	없음	

데이터 송신 함수		
함수명	sendData(cmdId, data)	
기능	- 제어부로 명령어 번호와 데이터를 전송함 - makePkt( ) 함수를 이용하여 data를 패킷으로 바꿈 - fwrite( ) 함수 : 지정한 tcpId의 주소에 makePkt 함수를 사용해서 만든 패킷 pktData를 전송함	
	H1	sync = 0x574B574B
	H2	msg_id = 0
	H3	cmdId
	H4	pktType = 0
	H5	dataLen = length(Data)
		Data
입력	cmdId : 명령어 번호 data : 송신 데이터	
출력	없음	

데이터 수신 함수		
함수명	recvData()	
기능	- 제어부에서 전송하는 데이터를 수신하는 기능 - numBytesPerBlk 변수에 한번에 수신하는 data의 길이를 정의함 (해당 길이는 처음 tcpID를 선언할때에 정의한 tcp.InputBufferSize 보다 작아야 함) - 반복문을 사용하여 모든 데이터를 나누어서 수신함 - fread(tcp, numBytesPerBlk) : 지정한 tcpId의 주소로부터 numBytesPerBlk 만큼의 데이터를 수신함.	
	H1	Sync
	H2	msg_id
	H3	cmdId
	H4	pktType0
	H5	dataLen
		Data
입력	없음	
출력	함수 내부에서 header 와 data 를 분리한 후 데이터 부분만 출력함.	

데이터 수신 함수		
함수명	recvData()	
기능	- 제어부에서 전송하는 데이터를 수신하는 기능 - numBytesPerBlk 변수에 한번에 수신하는 data의 길이를 정의함 (해당 길이는 처음 tcpID를 선언할때에 정의한 tcp.InputBufferSize 보다 작아야 함) - 반복문을 사용하여 모든 데이터를 나누어서 수신함 - fread(tcp, numBytesPerBlk) : 지정한 tcpId의 주소로부터 numBytesPerBlk 만큼의 데이터를 수신함.	
	H1	Sync
	H2	msg_id
	H3	cmdId
	H4	pktType0
	H5	dataLen
		Data
입력	없음	
출력	함수 내부에서 header 와 data 를 분리한 후 데이터 부분만 출력함.	

② 시스템 명령어: 상기 기본 함수들을 이용하여 IFD 시스템을 제어하는 명령어

송신 데이터 복사 기능		
기능		장비제어부가 초기에 계산한 3ms 송신 데이터를 가져옴
송신포맷	H1	sync = 574B574B
	H2	msgId = 0
	H3	cmdId = 110
	H4	pktType = 0
	H5	dataLen = 1
		data = 1
수신포맷	H1	sync = 574B574B
	H2	msgId = 0
	H3	cmdId = 110
	H4	pktType = 0
	H5	dataLen = 7680*3*2
		I(0)
		Q(0)
		I(1)
		...
		Q(dataLen – 1)

송신 데이터 업로드 기능		
기능		- TxBuffer에 데이터를 업로딩하는 기능 - MATLAB에서 계산한 3ms data를 장비제어부에 전송
송신포맷	H1	sync = 574B574B
	H2	msgId = 0
	H3	cmdId = 107
	H4	pktType = 0
	H5	dataLen = 7680*3*2
		I(0)
		Q(0)
		I(1)
		...
		Q(dataLen – 1)
수신포맷	없음	

수신 데이터 다운로드 기능		
기능		RxBuffer에서 수신한 6msec 데이터를 다운로딩하는 기능
송신포맷	H1	sync = 574B574B
	H2	msgId = 0
	H3	cmdId = 108
	H4	pktType = 0
	H5	dataLen = 2
		data(0) = 7680 : start index
		data(1) = 6*7680 : txData length
수신포맷	H1	sync = 574B574B
	H2	msgId = 0
	H3	cmdId = 108
	H4	pktType = 0
	H5	dataLen = 7680*62
		I(0)
		Q(0)
		I(1)
		...
		Q(dataLen – 1)

데이터 루프백 기능		
기능		장비 제어부에 3ms의 data를 전송 및 장비제어부로부터 6ms의 data 수신
송신포맷	H1	sync = 574B574B
	H2	msgId = 0
	H3	cmdId = 112
	H4	pktType = 0
	H5	dataLen = 7680*3
		txData(0) = 1
		txData (1) = 2
		txData (2) = 3
		...
		txData (dataLen - 1) = dataLen
수신포맷	H1	sync = 574B574B
	H2	msgId = 0
	H3	cmdId = 108
	H4	pktType = 0
	H5	dataLen = 7680*6
		rxData(0) = txData(0)
		rxData(1) = txData(1)
		rxData(2) = txData(2)
		...
		rxData(dataLen/2) = txData(0)
		...
		rxData(dataLen - 1) = txData(dataLen/2 - 1)

3) 동작 시험

① 사용 절차: HW/SW 인터페이스 시스템의 동작 시험 절차는 아래와 같다.

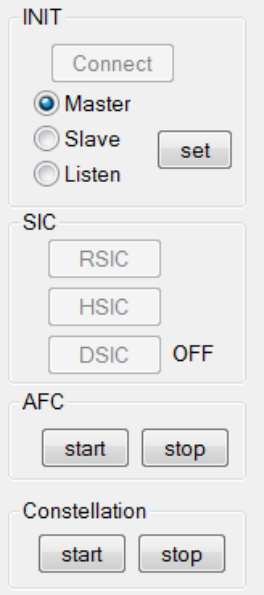
- 하드웨어 연결

· DSP Eth 포트와 PC 를 연결한다.

· USB 1 번 포트와 PC 의 USB 포트를 연결한다.

· PC 의 IP 주소를 DSP 의 IP 주소(192.168.1.254)와 연결될 수 있도록 192.168.1.xxx 로 설정한다.

- 전원 켜기
  - 시스템 전원을 켠다
  - LED 1 번이 깜빡이면 FPGA 가 로딩되었음을 표시한다.
  - LED 2 번이 깜빡이면 DSP 가 성공적으로 부팅되었음을 표시한다.
- 제어부 실행
  - 제어부 실행 파일을 더블 클릭하여 실행한다.
  - 제어부 창이 뜨면 아래 그림에 표기된 창만을 이용하여 프로그램을 구동시킨다.



- USB 및 DSP 연결: Connect 버튼을 클릭하여 USB 와 DSP 를 연결한다.

- 동작 모드 설정
  - Master/Slave/Listen 모드 중 하나를 선택한 후 Set 버튼을 클릭한다.
  - 동작 모드에 따라 미리 정의된 데이터를 계산한 후 FPGA 내부 TxBuffer 에 전송한다.
- SIC 실행
  - RSIC 버튼을 클릭하여 RSIC 기능을 실행한다. 화면에 표시된 수신 데이터를 스펙트럼을 보고 추가 cancellation 이 필요하면 RSIC 버튼을 한 번 더 클릭한다.
  - HSIC 버튼을 클릭하여 HSIC 기능을 실행한다. HSIC 기능이 끝나면 수신 이득이 변하고, Tx 블록의 FIR 필터 설정값이 결정된다.
  - DSIC 버튼을 클릭하여 DSIC 기능을 ON 한다.
- AFC 실행
  - Slave 와 Listen 모드에만 해당됨. Master 모드는 비활성화 됨.
  - Start 버튼을 클릭하면 주파수 Lock 이 될 때까지 PWM 값을 연속적으로 바꾼다.
  - 도중에 중단하고 싶으면 stop 버튼을 클릭한다.
- Constellation 실행
  - Start 버튼을 클릭하면 주파수 Lock 이 걸렸는지 확인한 후 Lock 이 걸렸으면 모뎀처리를 수행한다. Lock 이 걸리지 않았으면 기능을 종료한다.

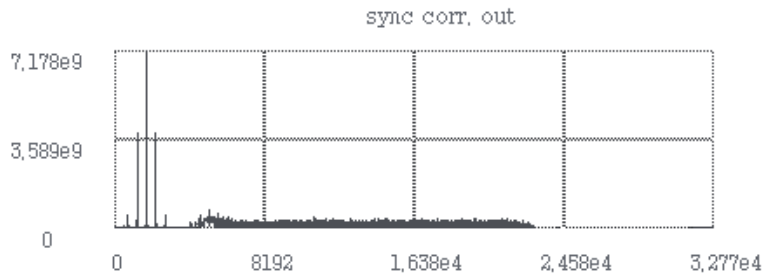
· FPGA 에서 수신데이터를 로딩한 후 모뎀 복조처리한 성상도 결과를 화면에 표기한다.

· 주기적으로 timing 체크를 하여 FPGA 내부 타이머를 조정하여 송수신간 시간 동기가 유지되도록 한다.

② HD mode 에서의 송수신 시험: 아래는 HW/SW 간 인터페이스 프로그램과 SW 모뎀을 연동시켜 HD 모드에서의 송수신을 테스트 한 결과이다.

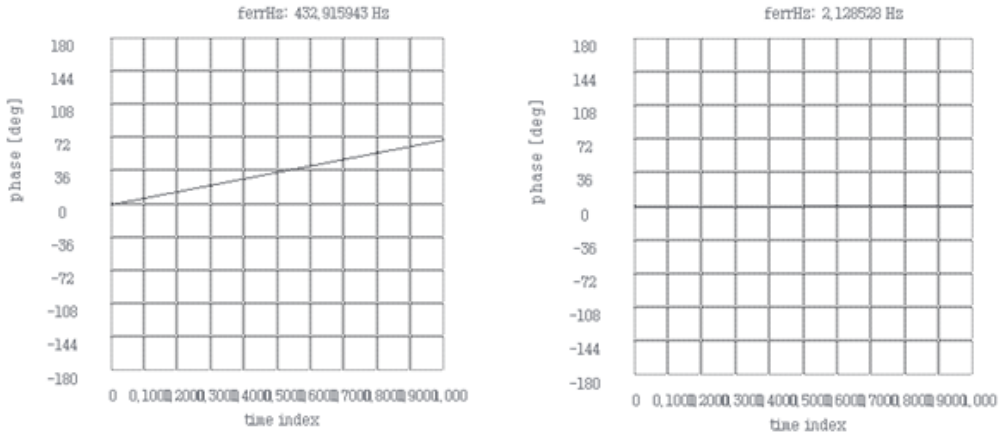
- AFC 기능: 본 테스트에서는 AFC 기능이 정상 동작하는 지 확인한다.

<그림 34>는 Slave 가 Master 에서 송신된 동기채널 중 시간적으로 앞에 위치한 동기채널에 대한 상관을 한 결과이다. 이 상관값을 이용하여 수신 타이머를 조정하고, 주파수 동기를 추적한다.



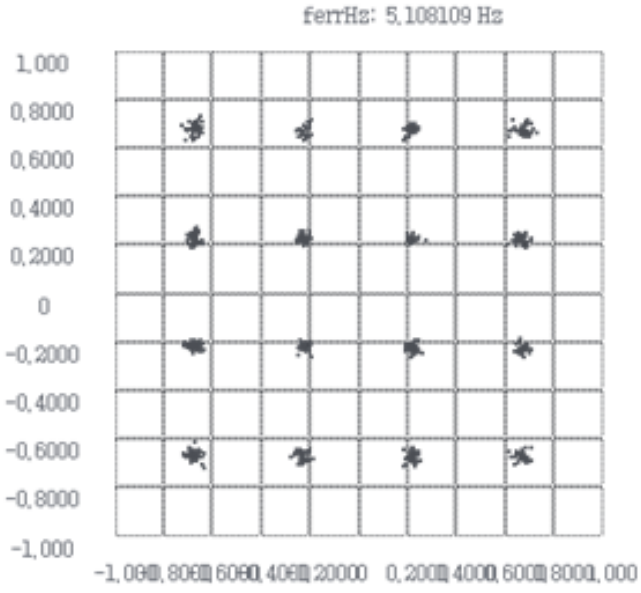
<그림 34> 동기 채널 상관 결과

<그림 35>는 주파수 Lock 이전에 동기채널간 위상변화를 그린것이다. 주파수 오차로 인하여 위상차이가 존재한다. 반면에 주파수 Lock 이후의 동기채널간 위상변화는 거의 없다



<그림 35> 주파수 lock 이전(좌)과 이후(우)의 두 동기채 널간 위상 변화

- HD 모드에서 수신신호 복조 시험: 본 테스트에서는 HD 모드에서 인터페이스 프로그램과 SW 모뎀을 연동시켜 신호를 전송한 후 이를 복조한다.

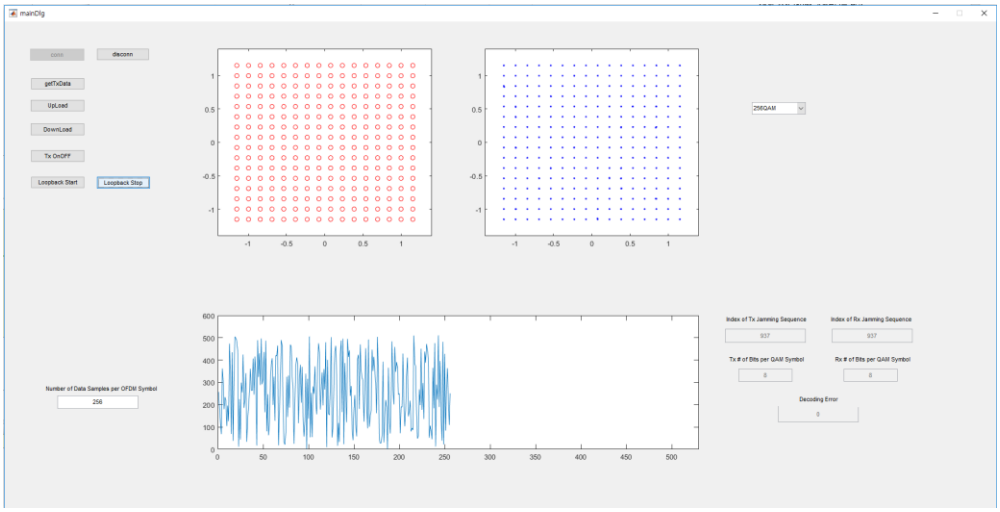


<그림 36> HD mode 에서 송수신 시험 결과

<그림 36>은 이러한 과정을 통해 얻은 성상도이다. 이때, SW 모뎀과 인터페이스 프로그램간 연동 시험에 초점을 맞추기 위해 전송 신호에 jamming sequence 는 삽입하지 않았다. 아래 그림에서 볼 수 있듯이, SW 모뎀과 인터페이스 프로그램간 연동이 잘 이루어지고 있으며, 이로 인해 HD 모드에서의 수신 신호 복조가 잘 이루어지고 있음을 알 수 있다.

③ Loopback mode 에서의 ST-jamming 동작 시험

<그림 37>은 인터페이스의 loopback 모드와 SW 모뎀을 연동시켜 ST-jamming 적용에 따른 jamming 신호 삽입 및 제거 후 수신신호의 성상도를 나타낸 것이다. 이 그림에서 볼 수 있듯이, data 신호의 modulation order 나 jamming sequence 의 길이와 관계 없이, SW 모뎀에서의 jamming 신호 삽입과 이를 인터페이스 프로그램과 교환, 다시 SW 모뎀에서의 jamming 신호 제거 및 수신신호 복조가 정상적으로 동작한다.



<그림 37> Jamming 신호 삽입 및 제거 후 수신신호 성상도 (256QAM)

제 3장. 연구 개발 결과의 활용 계획

1절. 기술적 파급효과

1. 보안과 데이터 전송간의 trade-off 로 대표되는 물리계층 보안의 기술적 허들과 동일대역 동시 송수신 시스템의 데이터 전송률 향상 한계 극복
2. 차세대 통신 네트워크를 위한 보안 기술의 패러다임 전환 및 선점

가. 통신과 PLS 가 완전히 통합된 새로운 PLS 통신 패러다임의 선점

나. '보안'과 '동일대역 동시 송수신'이라는 키워드를 함께 고려함으로써

1) 보안-정보전송간 trade-off 및 PLS overhead 라는 PLS 의 한계 극복

2) 동일대역 동시송수신의 traffic 비대칭 및 2 배의 capacity 증가 한계 극복

다. 보안과 통신을 융합하는 새로운 연구 트렌드 창출

2절. 연구 개발 결과를 기반으로 하는 미래 연구 분야 창출

1. 다양한 상용 통신 및 응용 시스템(무선 백홀, IoT 등)에서 보안 강화 및 정보 전송량 증대의 동시 달성

가. 본 과제의 기반 기술인 동일대역 동시 송수신 기술의 3GPP 표준화를 준비하기 위한 FDR IG 참석 및 기술 제안.

나. 3GPP Rel. 17 혹은 18 에서 동일대역 동시 송수신 기술의 study item 제정을 목표로 하고 있으며, 성공시 본 과제의 기반 기술을 상용 통신 시스템에 적용 가능

2. 차량간 통신 시스템에서 충분한 데이터 전송률을 확보하면서 의도치 않은 정보의 누설을 방지 하는 기술적 안전망 확보

3. 군사/대태러 보안 통신 기술의 새로운 패러다임 제시

가. 보안, 통신, 전자전이 통합된 차세대 국방 시스템의 연구 패러다임 선점.

나. 무선통신을 활용하는 전장 환경에서 아군에게 고성능 데이터 통신과 데이터 통신의 기밀성, 그리고 적 통신망에 대한 공격을 동시에 제공하는 기술로 확장

다. 아군에게는 자유로운 고성능 데이터 통신을 제공하는 한편 적에게는 정보 감청 및 적 주체간 데이터통신을 무력화시키는 지리적 보안성 'zone'을 생성하는 기술로 진화

4. 행정, 의료 등 다양한 IDX 플랫폼을 위한 보안통신 요소기술의 기술적 벤치마크

가. 고신뢰 금융 거래 시스템에서 보안과 통신이 통합된 새로운 패러다임의 연구 분야 선점

나. 바이오 의료 지능 시스템에서 환자 정보의 안전한 수집을 위한 기반 기술 연구 분야 선점

3절. 연구 개발 결과를 이용한 응용 및 산업화 추진 방향

1. 6G 이동통신 대형 통합 과제 기획에 활용

가. 6G 이동 통신을 위한 새로운 통신 패러다임 중 하나로 보안과 양방향 통신이 통합된 본 제안 기술을 제시

나. 향후 연구를 통해 본 제안과제의 양방향 PLS 기술과 동일대역 동시 송수신

의 성능 개선을 위한 간섭 제어, 자원 할당 기술 등을 통합함으로써 ETRI 6G 이동 통신 시스템의 차별화된 기술적 진보성 제시

다. 본 과제의 개발 내용(동일대역 동시 송수신 기술 기반의 물리계층 보안 통신 기술)을 포함하는 다목적 송수신 장치 개발에 대한 6G 통신인프라 핵심기술 개발 사업 예타 기술 수요 조사서 제출 : 과제 선정시 본 과제에서 개발된 기술에 다양한 응용기술이 합쳐진 새로운 패러다임의 송수신 장치 개발로 이어질 수 있음

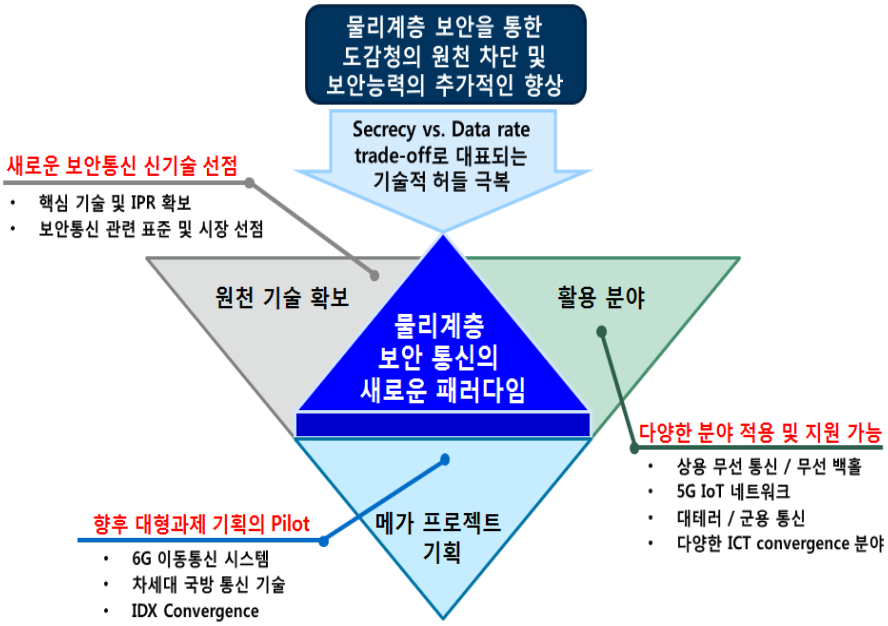
2. 차세대 국방 시스템 개발 과제 기획 활용

가. 본 제안 기술은, 도청을 방지하는 목적뿐만 아니라 주변에 위치하는 장치들의 통신을 무력 화 시키는 형태로도 응용될 수 있으므로, 이를 전자전 형태로 활용.

나. 따라서, 본 제안 기술을 기반으로 보안, 통신, 전자전이 통합된 군사 통신의 새로운 패러다 임을 제시하고 이를 요소기술로 활용하는 차세대 국방 시스템 개발 과제의 기획 및 수탁에 활용이 가능함.

다. 본 과제의 중간 결과를 활용하여 ‘미래 국방 기초 원천 R&D’ 과제 제안 및 RFP 작성 : 12월 중으로 상세 기획 보고서 작성 예정이며, 과제 선정시 본 과제의 결과 기술을 직접 활용하여 전자전과 정보 보안, 고성능 데이터 통신을 동시에 지원하는 미래 국방 통신 기술 개발에 착수함.

3. 행정, 의료 등 다양한 IDX 플랫폼을 위한 보안통신 요소기술의 기술적 벤치마크



<그림 38> 연구 개발 결과의 활용 방향

제 4장. 결 론

본 연구 과제에서는 동일대역 동시 송수신 기법을 기반으로 하는 새로운 형태의 물리계층 보안 통신 기술을 개발하고, 이에 대한 성능 분석 및 향후 성능 검증 플랫폼 개발을 위한 설계를 수행하였다.

먼저, 동일대역 동시 송수신 기술에서 태생적으로 발생하는 상, 하향링크간 트래픽 비대칭을 활용하여 시간 영역, 주파수 영역, 혹은 시간과 주파수 영역에서 재밍 신호를 삽입함으로써 도청자가 정보 도청을 불가능하게 하는 전송 기술 및 효율적인 도감청 방지를 위한 재밍 신호 설계 기법을 개발하였다. 또한, 이러한 전송 기법이 사용되었을 때 원하는 신호를 복원하기 위한 수신 신호처리 기법을 함께 개발하였으며, 이러한 기법들을 사용하기 위한 송수신 프로토콜 및 제어 신호를 설계하였다.

다음으로는 개발된 보안 통신 기술에 대한 성능 분석 연구를 진행하였다. 시뮬레이션을 통해 개발된 재밍 신호의 유효성을 검증하였으며, 또한 다양한 도청자의 위치에 따라 유효신호에 대한 도청자의 비트 에러율을 도출하여 제안된 보안 통신 기술의 유효성을 보였다. 이와 함께, 제안된 보안 통신 기술이 적용되었을 때 도청자에서의 정보 누설양을 이론적으로 분석함으로써 본 제안 기술의 우수성을 증명하였다.

마지막으로 2 차년도에 진행될 본 제안 기술의 성능 검증 플랫폼의 개발을 위한 송수신기 및 인터페이스 설계를 진행하였다. 성능 검증 플랫폼은 하드웨어 송수신기와 소프트웨어 모뎀으로 구성되는 바, 하드웨어 송수신기와 소프트웨어 모뎀 사이의 인터페이스를 개발하였으며, 소프트웨어 모뎀의 상세 설계를 완료하였다.

본 제안 기술은 보안과 데이터 전송 사이의 trade-off 로 대표되는 물리계층 보안의 기술적 허들과 동일대역 동시 송수신 시스템의 데이터 전송률 향상 한계를 극복할 수 있는 기술이다. 따라서 향후 다양한 상용 통신 및 응용 시스템은 물론 군사/대태러 보안 통신 기술에 널리 사용될 수 있을 것으로 기대된다. 특히, 차세대 국방 기술 개발 관련 과제에 적극적으로 활용함으로써 국방력 강화에 이바지할 수 있을 것으로 기대된다.

제 5장. 연구 시설, 장비 현황

기자재 및 시설명	규격	수량	용도
MATLAB Toolboxes	Parallel Computing Fixed-Point Designer	2	- 동일대역 동시 송수신기 HW 설계 - 양방향 PLS 통신 성능검증 플랫폼 HW/SW 인터페이스 개발
	MATLAB Coder MATLAB Compiler Instrument Control Symbolic Math	1	- 양방향 PLS 통신 SW 모뎀 설계 - 양방향 PLS 통신 성능검증 플랫폼 HW/SW 인터페이스 개발 - 양방향 PLS 통신 LLS/SLS 개발 - 2 중보안키 유효성 검증 시뮬레이션
	Simulink Simulink Coder	1	- 양방향 PLS 통신 성능검증 플랫폼 HW/SW 인터페이스 개발
개발 전용 PC	인텔 코어 i9 32GB 메모리 SSD 256GB 700W 파워	3	- 양방향 PLS 통신 알고리즘 검증 - 양방향 PLS 통신 링크레벨 및 인터페이스 시뮬레이션 - 양방향 PLS 통신 시스템 성능분석
시연용 노트북	인텔 코어 i7 16GB DDR4 1TB SSD	2	- HW/SW 인터페이스 테스트 - 자기간섭 제거 시뮬레이션

약 어 표

약어	원문
PLS	Physical Layer Secrecy
IFD	In-band Full Duplex
RF	Radio Frequency
SI	Self-Interference
SIC	Self-Interference Cancellation
RSIC	RF SIC
HSIC	Hybrid SIC
DSIC	Digital SIC
OFDM	Orthogonal Frequency-Division Multiplexing
FFT	Fast Fourier Transform
IFFT	Inverse Fast Fourier Transform
CP	Cyclic Prefix
QAM	Quadrature Amplitude Modulation
DL	Downlink
UL	Uplink
FGPA	Field Programmable Gate Array
HW	Hardware
SW	Software

주 의

1. 이 연구보고서는 한국전자통신연구원의 주요사업으로 수행한 최종연구결과입니다.

2. 이 보고서의 내용을 발표할 때에는 반드시 한국전자통신연구원에서 수행한 주요사업 결과임을 밝혀야 합니다.