Various threat models to circumvent air-gapped systems for preventing network attack

Eunchong Lee, Hyunsoo Kim, Ji Won Yoon

(Email: {gr4ce,aitch25,jiwon_yoon}@korea.ac.kr)

Signal Processing and Advanced Intelligence (SPAI)

Web: https://sites.google.com/site/securesiplab/

20, Aug, 2015

Index

Introduction

Air gap (networking)

From Wikipedia, the free encyclopedia

An **air gap** or **air wall**[1] is a network security measure, also known as **air gapping**,[2] employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.[3] The name arises from the technique of creating a network that does not have, and often has never had, an active unsecured connection, by having the two physically separated, with air in between. The air gap may not be completely literal, as networks employing the use of dedicated cryptographic devices that can tunnel packets over untrusted networks while avoiding packet rate or size variation can be considered "air gapped", as there is no ability for computers on opposite sides of the "gap" to communicate.

Introduction

Related Work

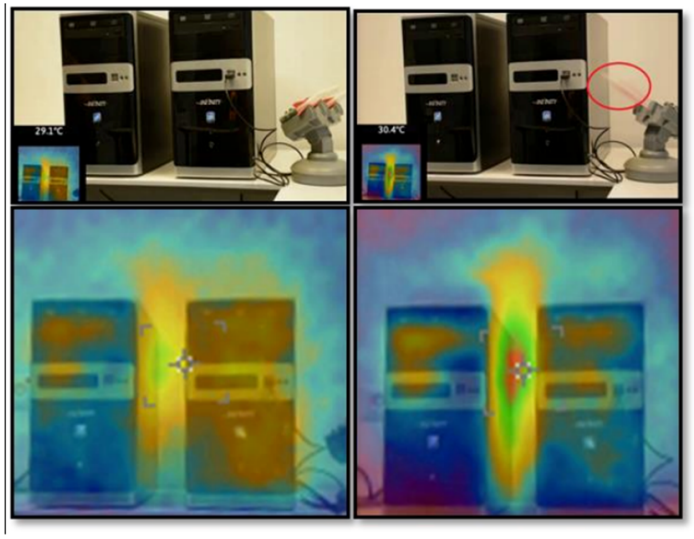
- CPU Heat

BitWhisper: The Heat is on the Air-Gap

Submitted by Cyber Security ... on Mon, 23/03/2015 - 14:31

UPDATE 30 Mar 2015: A draft of the research paper is availa

Researcher Mordechai Guri assisted by Matan Monitz and gui uncovered a new method to breach air-gapped systems. Our l published in August of 2014, using a method called *Air-Hopp* exfiltration. The new research initiative, termed *BitWhisper*, is topic of air-gap security at the Cyber Security Research Cente BitWhisper is a demonstration for a covert bi-directional com by air-gapped computers communicating via heat. The metho the two physically adjacent and compromised computers usin thermal sensors to communicate.



Related Work

- Scan rate of Moniter, Radio in Mobile

Related Work

- Speaker & Microphone

How malware could steal sensitive data from an air-gapped computer - via high frequency sound

Graham Cluley | December 2, 2013 11:12 pm | Filed under: Malware, Privacy, Vulnerability

0 0 3

It sounds like a pu

How *would* cybe
malware-infected
access to, and tha
or the internet?

At first, you might
German computer
Communication,

Michael Hanspach
(such as confident
transmitting it via t
through the infected computer's built-in speaker.

Date: 05 Apr 2015

On Acoustic Covert Channels Between Air-Gapped Systems

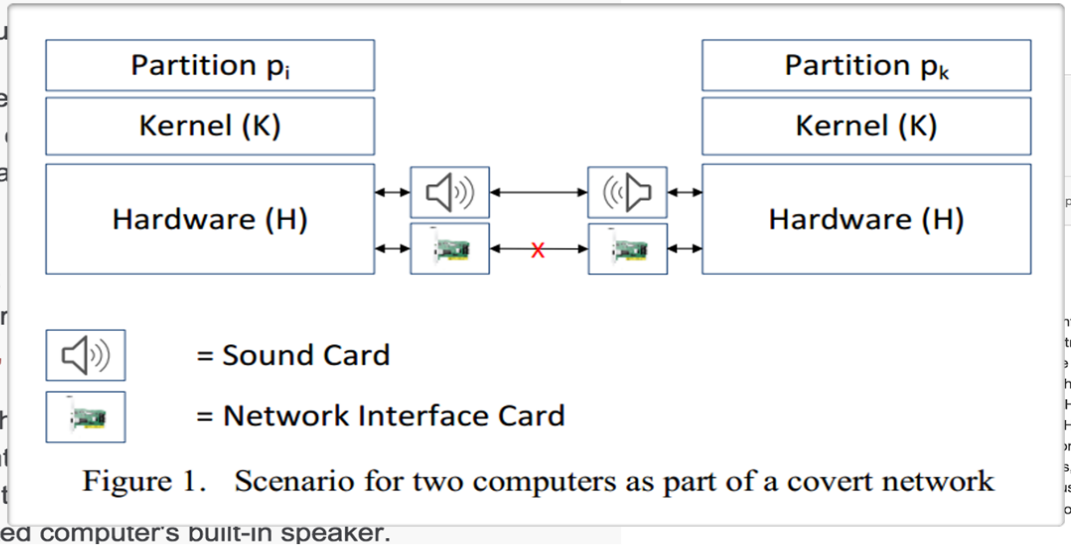


Figure 1. Scenario for two computers as part of a covert network

prices may vary according to local VAT.

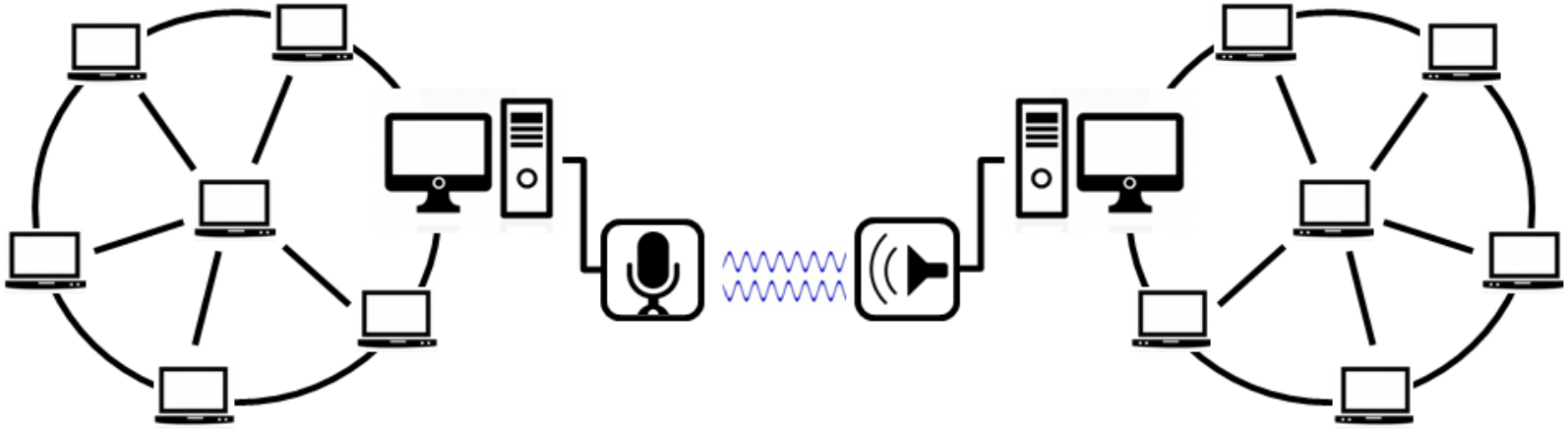
nformation from an air-gapped high-
trasonic and audible audio covert
e and a closed-door office. Our
hardware can leak data from an air-
Hz to 20.5 kHz at a rate of 140 bps
Hz to 18 kHz. Additionally, we show
n at distances up to 11 m with bit
s, our attacks are able to leak
sing audible signals when nobody is
okes and recorded audio.

Related Work

- The dangerousness and vulnerability of eavesdropping using loud-speakers

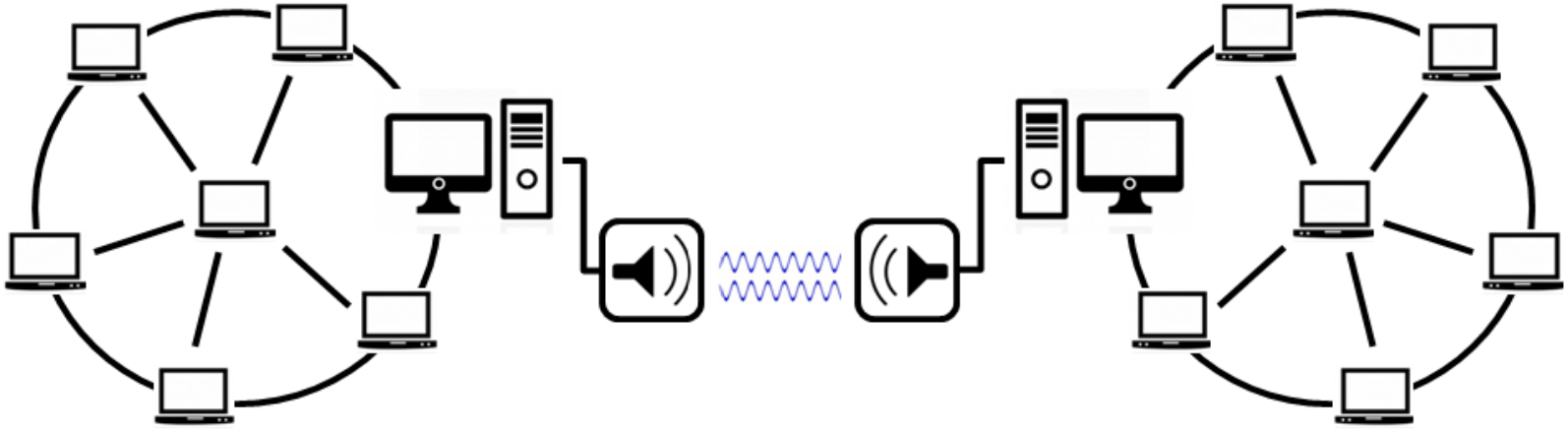
Threat Model

- Case A



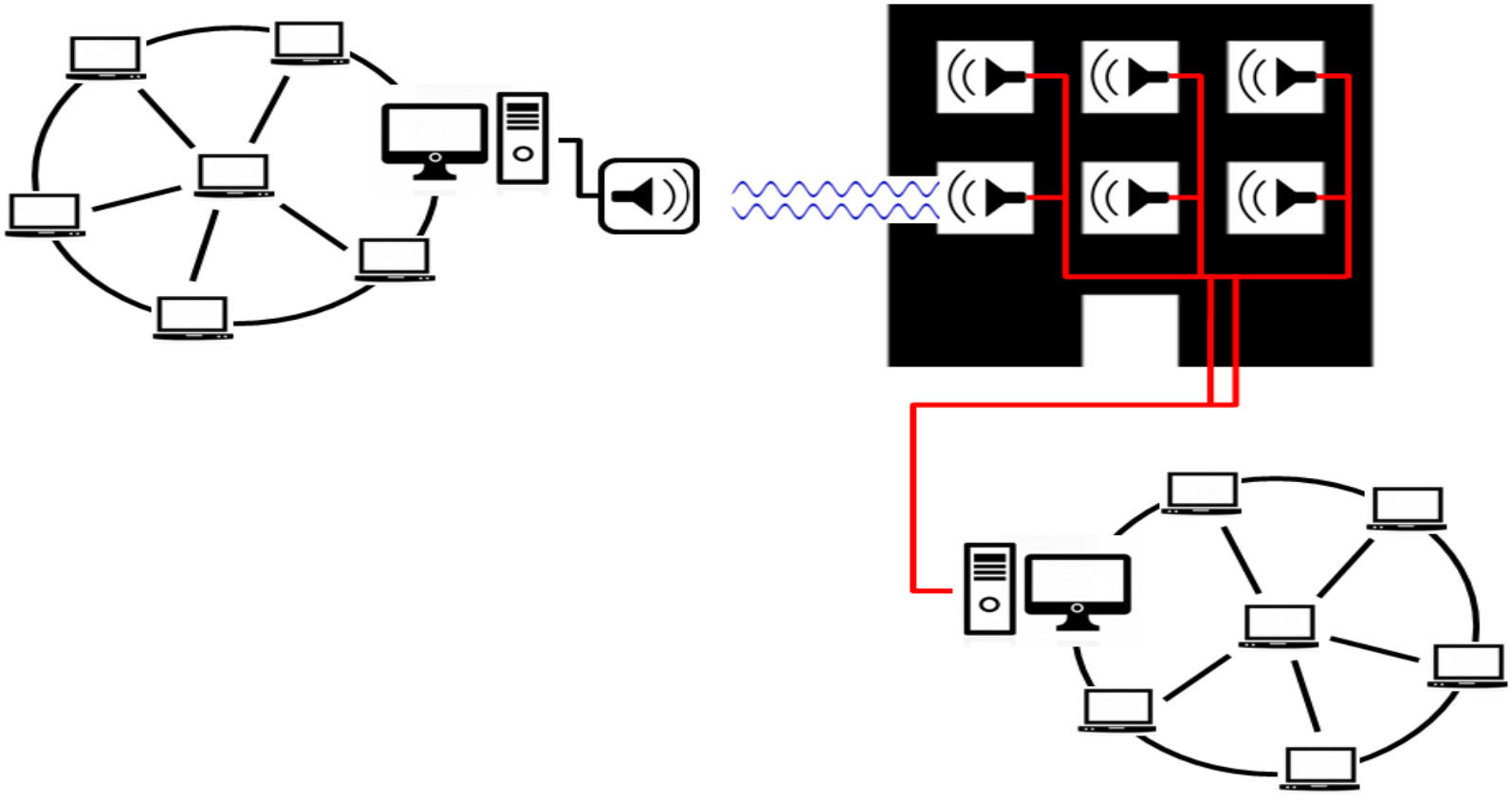
Threat Model

- Case B



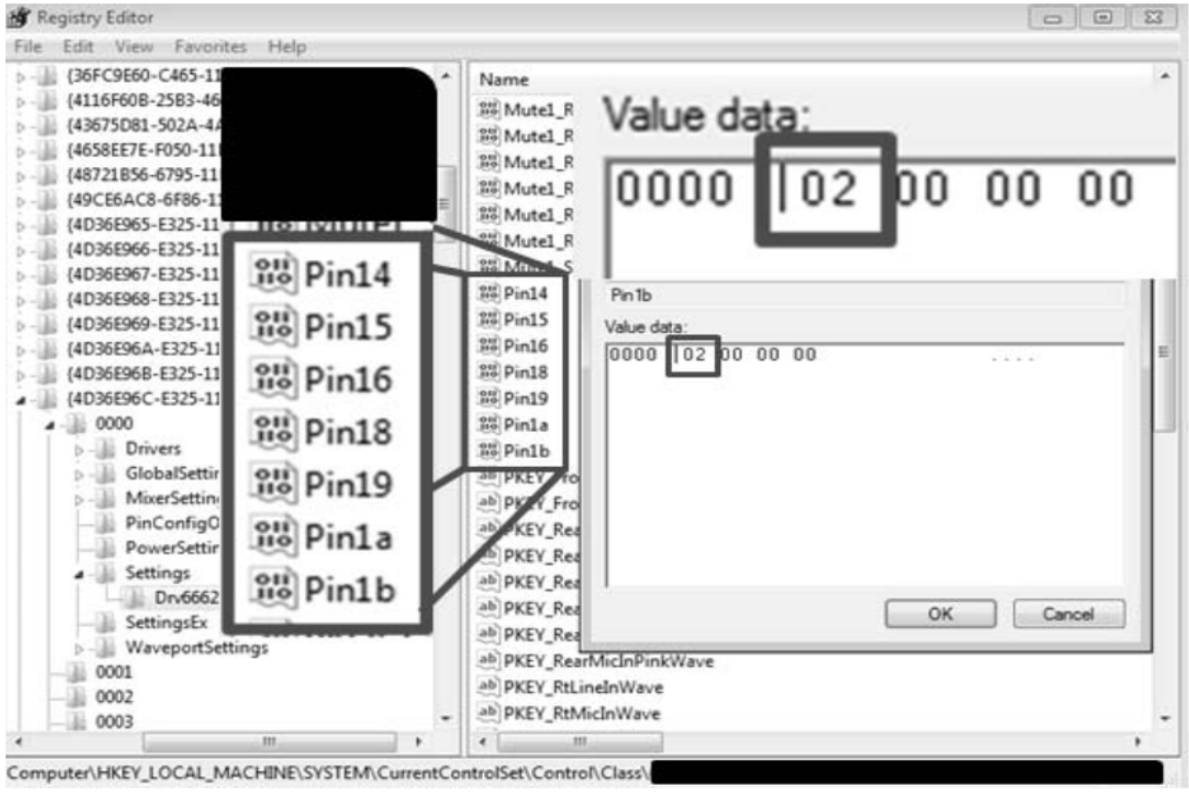
Threat Model

- Case C



Technical Background

- How to rig Windows registry
  - Through changing value of a pin number, we can use a speaker as a microphone

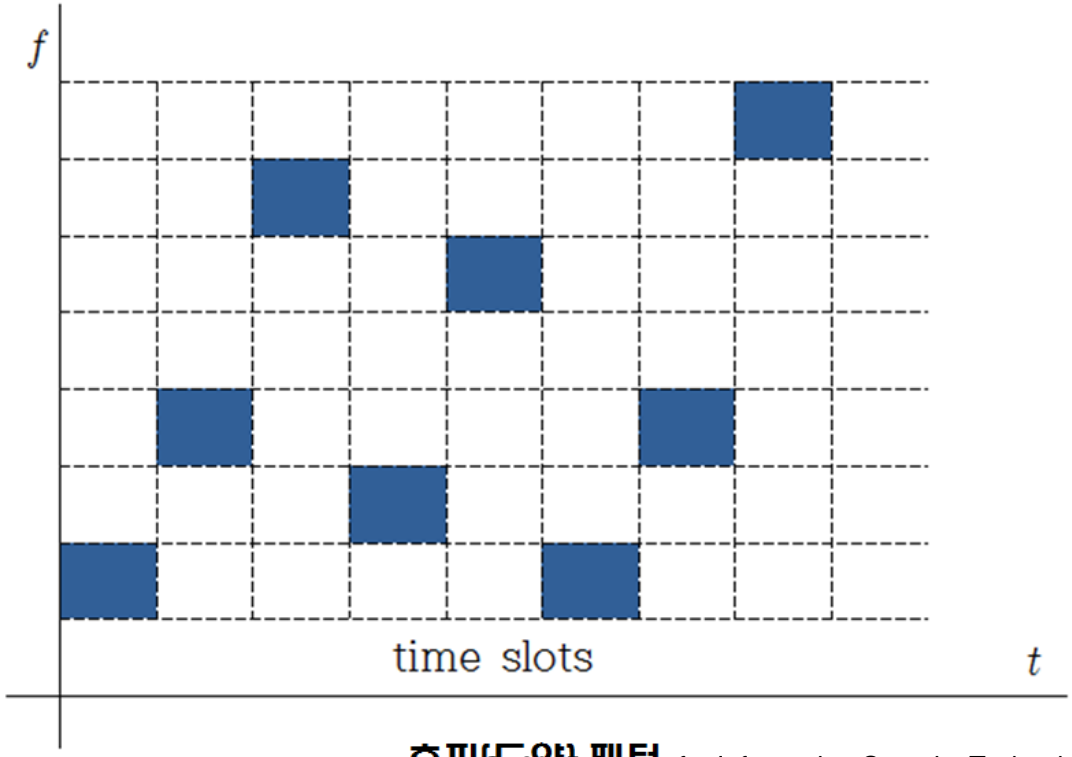


Technical Background

- Speed, OFDM
  - Orthogonal frequency-division multiplexing
    - A method of encoding digital data on multiple carrier frequencies
    - An FDM modulation technique for transmitting large amounts of digital data over a radio wave
    - A method of digital modulation in which a signal is split into several narrowband channels at different frequencies
    - A digital transmission technique that uses a large number of carriers spaced apart at slightly different frequencies
  - Definition
    - Total bandwitdth available within a communications system is divided into smaller non-overapping frequency sub-bands
    - Usually a separate data signal is associated to each frequency sub-band
    - Passband filter at receiver extracts requested sub-band / data signal

Technical Background

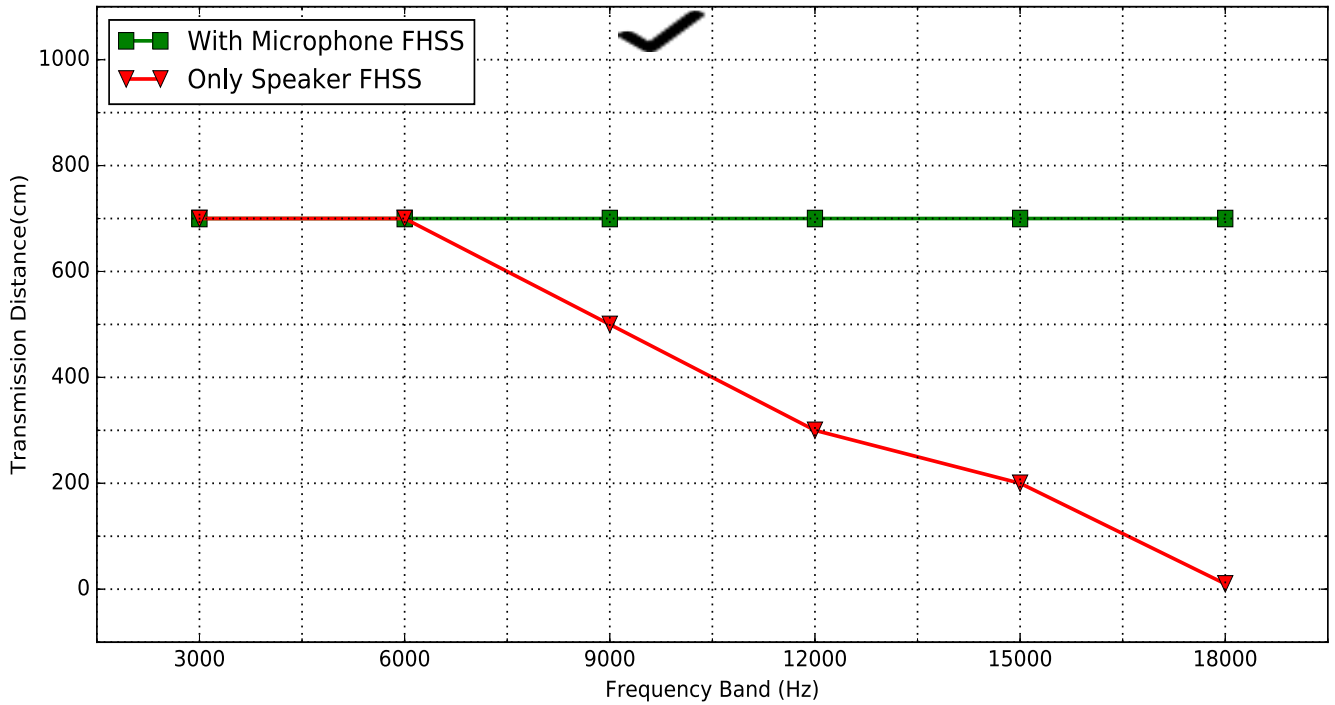
- Stability, FHSS
  - Frequency Hopping Spread Spectrum
    - Communication scheme between a transmitter and a receiver
    - Involves spread spectrum modulation and switching frequency according to a known standard
    - FHSS is a very robust technology, with little influence from noises, reflections, other radio stations or other environment factors
    - Multiple networks can operate in close proximity without interfering



호핑(도약) 패턴

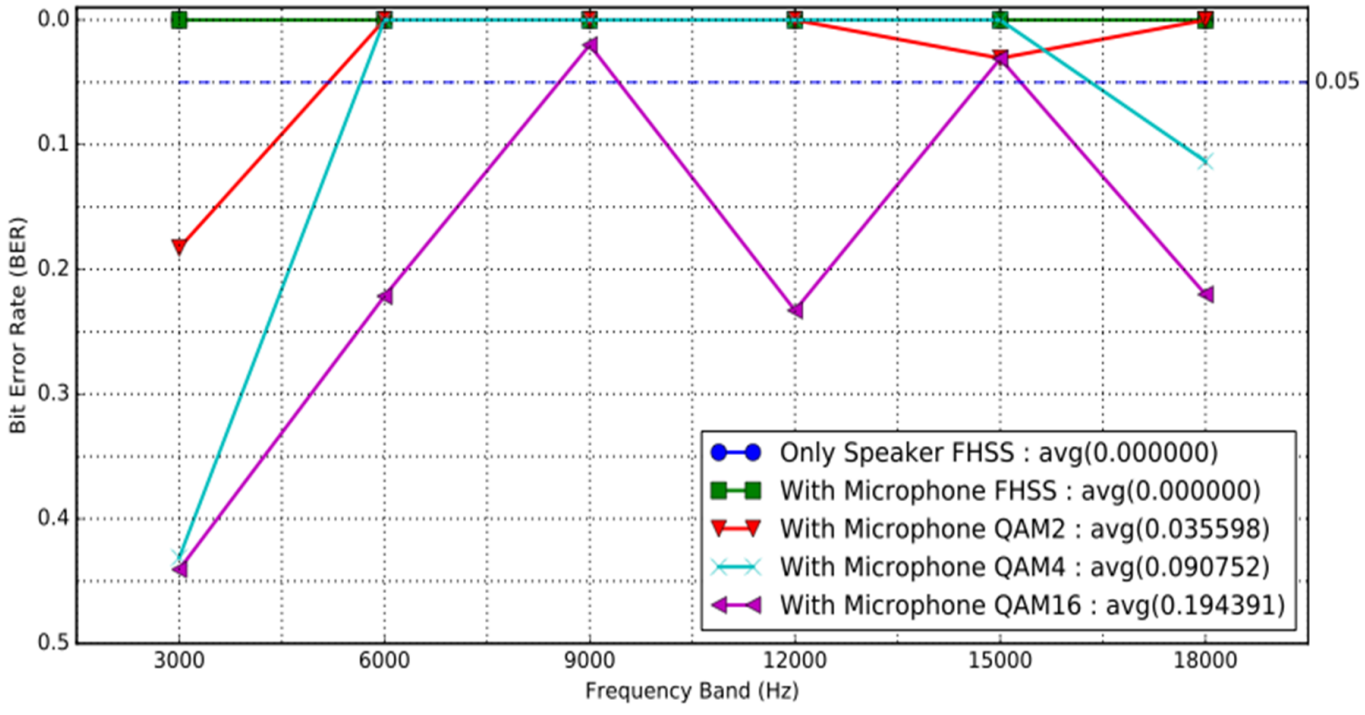
Experiment

- Implementation, Distance



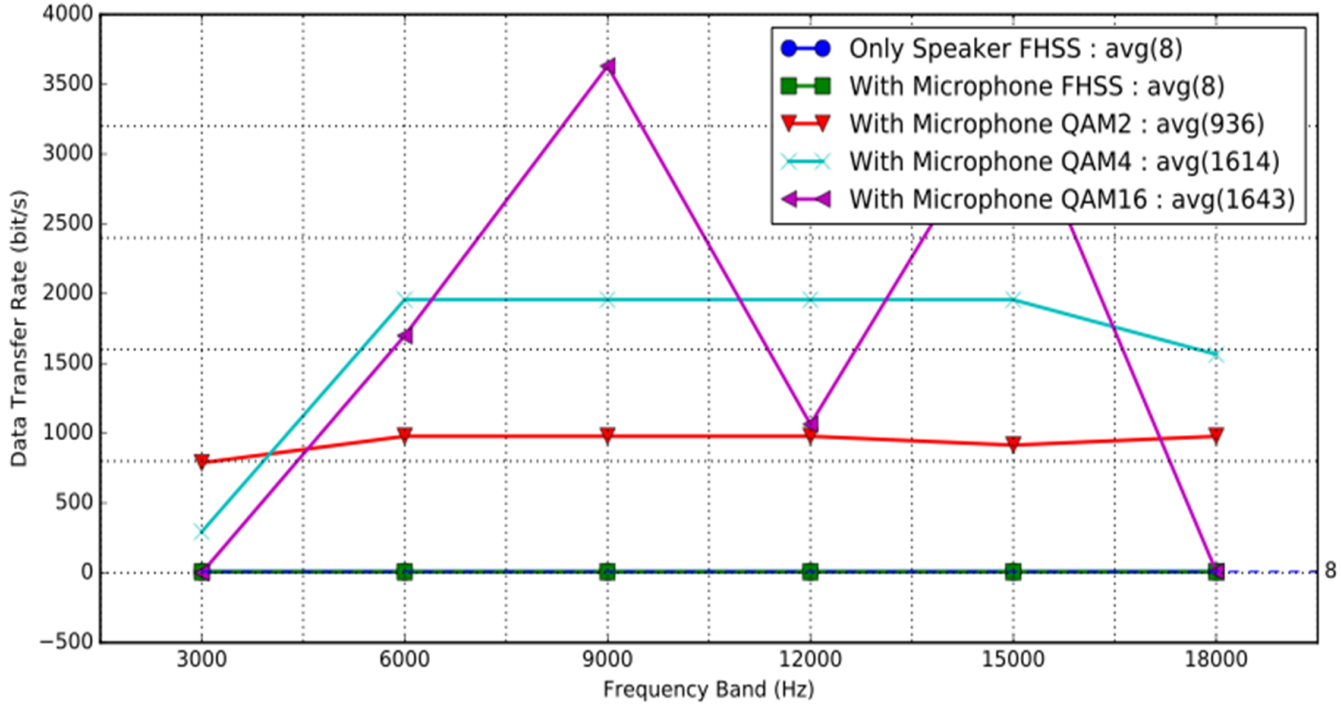
Experiment

- Implementation, Error rate



Experiment

- Implementation, Transmission rate



Discussion

- We can remove speaker

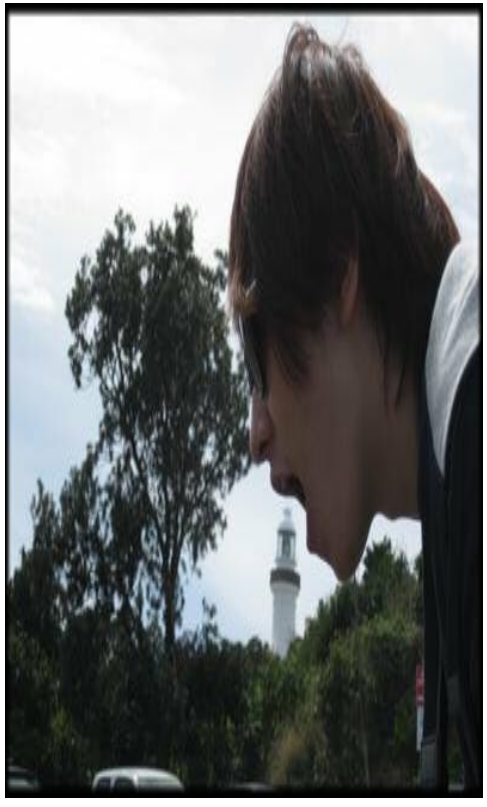
Discussion

- We can do jamming

Discussion

- We can perceive

Conclusion



(a) Eunchong Lee

(b) Hyunsoo Kim

(c) Ji Won Yoon

- Email : { gr4ce, aitch25, jiwon_yoon}@korea.ac.kr
- Signal Processing and Advance Intelligence Laboratory (SPAI)
- Graduate School of Information Security, Korea University, Korea

Eunchong Lee (Email: gr4ce@korea.ac.kr)
Signal Processing and Advanced Intelligence (SPAI)
Web: https://sites.google.com/site/securesiplab/
20, Aug, 2015