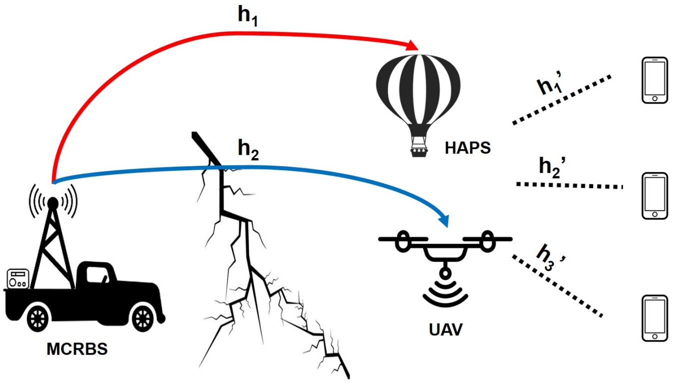
CHAPTER 1
INTRODUCTION

1.1 Background

Indonesia is located on the pacific ring of fire with a high degree of tectonic activity, it is at risk to multiple hazardous potency of natural disaster threat, such as volcanic eruptions, earthquakes, floods, landslides, and tsunami. Natural disaster destroy buildings, trees and the other infrastructures, it cause high interference of mobile station (MS) connectivity in cellular communications. High risk can occur when base transceiver station (BTS) is damaged, it causes some of MS in disaster area are losing their connection. Mobile cognitive radio base station (MCRBS) is an alternative technology to replace base station to recover cellular communication in disaster area [1]. The recovery networks can be used by victims to communicate with the closest relatives and inform their condition to rescue team when they stuck in the ruins of buildings.

Natural disaster causes too many obstacle which MCRBS unable to coverage the obstacle area. Proposed solution is MCRBS deploy high altitude platform station (HAPS) and unmanned aerial vehicle (UAV) which is illustrated on Fig. 1.1. HAPS and UAV are used to be relay node to forward the communications from MCRBS to MS in obstacle area. HAPS is better than UAV in coverage are because of it can be deployed at the height 17 - 25 km in the stratosphere. Beside that, HAPS



(a) (b)

Fig. 1.1. Deployment system of HAPS and UAV from MCRBS in area having obstacle.

has the characteristics of wide coverage, flexible deployment, low delay, high capacity, good channel condition, and economical cost [2]. In 2012, Google announced Project Loon, a network of HAPS balloon. In the following years, Facebook also launched Aquila, a HAPS-based UAV [3]. In Indonesia and India, where Project Loon planned to conduct a trial, security issue regarding Project Loon operational has raised significant concern.

Security issue in HAPS communications is needed to secure victim's data until receive to MCRBS. There are two types of security based on layer level in wireless communications, they are network layer security and physical layer security. Network layer security needs sharing secret keys to secure the data in network layers. Physical layer security is found to be more robust in security, because physical layer security can simplify the security algorithms in terms of power efficiency and computational complexity [4]. The other problems also occur on wireless sensor networks (WSN). WSN are vulnerable to many attacks such as denial of service. One approach to tackle these attacks is by using cryptography (network layer security), the problem is that cryptography are computationally expensive [5]. Physical layer security uses information theory, of which a positive signs has been demonstrated that channel impairments such as noise and fading can be used to hide messages without requiring keys between receivers and senders [6].

In information theory-based security, the target of the system is to maximize mutual information $I(X;Y)$, where X is the random variable of transmitted signal at the sender and Y is random variable of the received signal at the legitimate receiver. On the other hand, the information theory-based security minimizes $I(X,Z)$, where Z is the random variable of the received signal at the eavesdropper. Reference [7] has evaluated some physical layer security schemes using Bose-Chaudhuri-Hocquenghem (BCH), Low-Density-Parity-Check (LDPC), and Red Salomon (RS) channel coding. The results show that RS takes the least time in error correcting codes and meaning that RS has low computational complexity. However, the problem is that eavesdropper can decode the information at higher E_b/N_0. It means the security level is low. The other method in physical layer security is [8], they use channel estimation with ACK/NACK signal. It means the channel estimation method need more power consumption.

Polar codes have encoding and decoding computation complexity in the order of $O(N \ \log \ N)$ [9] Indicating that Polar codeshas low and similar to fast Fourier transform (FFT). In [10], they show Polar codes have lower hardware complexity than LDPC and Turbo codes. Beside the hardware complexity, Polar codes can be use for physical layer security. Polar codes suitable for HAPS communication, because can be process the channel coding and security data at the same time than the other methods. Polar codes have the unique bit arrangement, which contain of information bits and frozen bits. Frozen bits are used to protect the information bits for data transmission. The arrangement of information bits and frozen bits depend on Polar construction and the block-length. Generally, frozen bits have the value with zero ‘0’, but actually, frozen bits value can be fill with ‘0’ and ‘1’. With two kind of frozen bits value, it can increase the probability of the arrangement of encoding data. Therefore, the various frozen bits pattern make the eavesdropper is hard to decode the information. The arrangement of frozen bits value proposed as the security scheme to protect information bits in physical layer.

Polar codes have the problem in multipath fading, because its original construction is depends on channel, therefore Polar codes need send feedback to robust the channel varying. Huawei propose the new Polar construction which independent with the channels [11]. The name of proposed method is Polar Weight, where the Polar construction is built with binary operation which depend on block-length of Polar codes. This method can improve the Polar codes performance in multipath fading, because Polar construction have been independent with channels.

From the various problems, this thesis propose (i) The proposed security schemes of Polar codes, (ii) Performance of Polar codes with security scheme in AWGN Rayleigh fading channels, (iii) Performance of Polar codes lattices with security scheme in AMGN channel, (iv) Performance of Polar codes with security scheme in HAPS channel with orthogonal frequency division multiplexing (OFDM), and (v) Validate Polar codes with security scheme in real-field with universal software radio peripheral (USRP).

1.2 Problem Identification and Objective

Natural disaster causes too many obstacle which MCRBS unable to coverage the obstacle area. MCRBS should deploy HAPS or UAV as the relay. As the temporary base station, the security of victim’s data is important. However, there is no existing security scheme between MCRBS and HAPS/UAV communications. It causes the communication between MCRBS and HAPS/UAV vulnerable to attack

1.3 Scope of Work

To simplify the description, several points are assumed as follows:

1. The proposed method is examined through power-constrained channel

(AWGN, Rayleigh fading, and HAPS channel model).

2. The proposed method is examined through power-unconstrained channel (AMGN channel).

3. The proposed method is further evaluated in real-field condition experiments utilizing USRP.

4. System evaluated with computer-based simulation (MATLAB and SIMULINK).

5. The Experimental scenario sets the drone does not fly.

1.4 Research Methodology

This thesis is divided into three work packages (WP) to make efficient and high quality results.

1. WP1: Forming frozen bits for security key
   In this WP, this thesis choose and arrange frozen bit's values for security system. This WP arrange frozen bits in block-length of 128 bits.

2. WP2: Polar codes with construction D lattice
   In this WP, this thesis combine Polar codes with construction D lattice. This WP also obtain the optimal rates and Polar codes lattice construction to examine the performance in power-unconstrained channel.

3. WP3: HAPS Communication configuration
   In this WP, this thesis configure parameters of HAPS communication. This WP also obtain channel model characteristic of HAPS Communication based on these parameters.

4. WP4: Performance evaluations
   This thesis combine Polar codes as channel coding and Polar codes as physical security through AWGN, Rayleigh Fading, HAPS Communication channel, and AMGN channel.

5. WP5: Result validation
   The system is validated using BER and FER performance of physical security with Polar codes and examine in real-field condition.

1.5 Structure of Thesis

The rest of this thesis is organized as follows:

CHAPTER II: Basic Concept

This chapter describes the basic concept of the general communications, including Polar codes, BPSK modulation, AWGN channel, Rayleigh fading channels, Construction D Lattice and BER theory.

CHAPTER III: System Model and The Proposed Methods

This chapter discusses the system model of HAPS Communication, Polar codes lattices design method, and the propose security scheme using Polar codes.

CHAPTER IV: Results and Validations

This chapter discusses the simulation results of proposed security schemes in different percentage of known frozen key value.

CHAPTER V: Conclusion

This chapter concludes the effect of known frozen key values as the security of Polar codes based on the results.