논문 14-39A-12-03 The Journal of Korean Institute of Communications and Information Sciences '14-12 Vol.39A No.12
http://dx.doi.org/10.7840/kics.2014.39A.12.708

# 무선 네트워크를 위한 분산형 비밀 키 추출 방식

임 상 훈◆, 전 형 석*, 하 정 석°

# A Novel Distributed Secret Key Extraction Technique for Wireless Network

Sanghun Im◆, Hyungsuk Jeon*, Jeongseok Ha°

요 약

본 연구에서는 무선 네트워크를 위하여 키 분배 관리 기반구조에 의존하지 않으며 완전 자율적이고 분산 구조의 초경량 보안 키 분배 방식을 제안하였다. 제안된 방식은 밥과 엘리스라 불리는 두 명의 적법한 사용자(legitimate users)들이 시분할 이중통신 (TDD, Time Division Duplex)방식으로 통신을 수행한다고 가정하며 채널의 쌍대성(reciprocity)에 의하여 상관성 (correlation)이 큰 무선 채널 이득을 가지는 것으로 가정하였다. 이러한 무선채널 이득을 두 적법한 사용자가 각자 독립적으로 양자화하여 얻은 무작위 비트 배열의 쌍을 생성하고 이를 보안 키로 사용하는 방식을 제안한다. 특히, 본 논문에서는 이러한 키 분배 프로토콜을 위한 적응형 양자화 기법을 제안하였다. 제안된 기법은 채널의 변화에 따라 양자화 임계값을 조정함으로써 앨리스와 밥에 의해 생성된 비트 배열 사이의 불일치 확률을 줄일 수 있는 장점을 가지고 있다. 또한 BCH 부호와 같은 실용적인 저 복잡도 부호를 사용하여 비트 배열의 쌍 간의 불일치를 정정하고 앨리스와 밥이 공유하게 될 보안키를 생성한다. 비밀 키 추출효율을 최대화하기 위해 양자화 단계와 BCH 부호의 부호율을 최적화시켰으며, 제안된 보안키 추출 시스템을 802.11a 기반의 무선 네트워크 카드를 이용하여 구현하였다. 하드웨어 기반의 실험을 통해 실내 환경에서 초 당 1 비트 이상의 보안 키를 획득하는 것이 가능함을 실험적으로 보였다.

**Key Words :** Adaptive Quantization, Key Extraction, Key Distribution, Wireless Network

ABSTRACT

In this paper, we present a secret key distribution protocol without resorting to a key management infrastructure targeting at providing a low-complexity distributed solution to wireless network. The proposed scheme extracts a secret key from the random fluctuation of wireless channels. By exploiting time division duplexing transmission, two legitimate users, Alice and Bob can have highly correlated channel gains due to channel reciprocity, and a pair of random bit sequences can be generated by quantizing the channel gains. We propose a novel adaptive quantization scheme that adjusts quantization thresholds according to channel variations and reduces the mismatch probability between generated bit sequences by Alice and Bob. BCH codes, as a low-complexity and pratical approach, are also employed to correct the mismatches between the pair of bit sequences and produce a secret key shared by Alice and Bob. To maximize the secret key extraction rate, the parameters, quantization levels and code rates of BCH codes are jointly optimized.

※ 이 논문은 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2012R1A1B3002684)
◆ First Author : Korea Institute of Science And Technology, sh.im@kaist.ac.kr, 정회원
° Corresponding Author : Korea Institute of Science And Technology, jsha@kaist.edu, 종신회원
* Korea Institute of Science And Technology, h.jeon@kaist.ac.kr, 정회원
논문번호 : KICS2014-07-266, Received July 15, 2014; Revised September 23, 2014; Accepted December 3, 2014

## Ⅰ. 서 론

최근 IoT (Internet of Things)환경에 대한 연구가 큰 주목을 받고 있다. IoT 환경에서는 다양한 종류의 사물들이 유기적으로 네트워크를 형성하고 서로 통신하며 인터넷으로의 연결성을 제공하기 때문에 부가가치를 창출할 수 있는 다양한 서비스가 발생할 것으로 예상하고 있다[1]. 하지만 네트워크를 이루는 다수의 이종 단말들이 서로 자유롭게 통신이 가능해야하므로 IoT환경은 보안 위협에 취약할 것으로 예상된다[2]. 특히, 사물 간 통신 환경에서는 다수의 분산되어있는 통신 노드가 안전하게 통신하기 위해서 사전에 보안키를 공유하는 것이 필수이다. 그러나 사물 인터넷 환경에서 통신 노드들은 연산능력 및 배터리가 제한되어 있기 때문에 기존의 키 관리 기반구조를 이용한 보안키 분배에 어려움이 있다. 이를 해결하는 방법으로 IoT 환경에서 경량화된 상호 인증 및 세션 키 합의 기술이 제안되었으나 사전에 상호 인증 및 세션 키 합의를 위한 대칭키가 미리 사물에 저장되어있는 것을 가정하고 있다[3]. 이러한 기술적 난관을 해결하고자 본 논문에서는 물리계층 보안 기술을 이용하여 매우 간단한 연산만으로도 분산되어 있는 사물들이 사전 보안키 공유 없이 자율적으로 무선 채널의 물리적인 특성을 활용하여 보안키를 생성하고 공유하는 보안키 분배 프로토콜을 제안한다.

본 연구에서 제안하는 보안키 생성 방식의 이론적 기반은 이점 증류 (advantage distillation), 정보 조정 (information reconciliation), 비밀성 증폭 (privacy amplification)의 세 단계를 통해 공격자가 전혀 예측할 수 없는 비밀 키를 생성하는 것에 있다[4,5]. 구체적으로, 이점 증류 과정에서는 높은 상관도를 가지는 측정값을 이용해 적법한 두 단말 사이의 공통된 비트열을 생성한다[5]. 하지만 실제 통신 환경에서는 잡음 및 간섭 등에 의해 두 비트열 간에 불일치가 발생하므로, 동일한 비트열을 생성하는 과정이 필요하다. 이를 위해 일반적으로 오류정정부호를 사용하며, 오류를 수정하는 과정을 정보 조정이라 한다[6]. 마지막으로 적법한 두 단말이 공통된 비트열을 획득하는 과정에서 제3자에게 누설된 정보를 제거하는 비밀성 증폭 과정을 통해 보안키를 생성할 수 있다[7].

본 논문에서는 무선 채널응답이 적법한 두 단말 사이에서 높은 상관도를 가지면서 시변하는 특성을 이점 증류에 이용하여 채널 응답 특성으로부터 보안키를 추출하는 연구를 수행하였다. 두 적법한 사용자 앨리스와 밥은 잠재적인 도청자 이브가 존재하는 상황에서 동일 주파수를 이용해 시분할 이중통신 (TDD, Time Division Duplex) 한다. 앨리스와 밥은 상관 시간 이내에 파일럿 심볼을 교환하기 때문에 서로 상관도가 높은 채널 이득을 추정한다. 반면 엘리스와 밥으로부터 주파수의 반파장 이상의 거리에 존재하는 이브는 독립적인 채널을 통해서 파일럿을 수신한다. 많은 연구에서 이점 증류를 위한 정보로써 수신 신호 강도 지수 (RSSI, Received Signal Strength Indication)[8,9], 무선 채널의 복소 이득[10], 그리고 채널 포락선의 레벨 크로싱 빈도[11] 등 다양한 무선 채널의 성질을 활용하였다. 이처럼 적법한 사용자들은 채널 측정값 양자화를 통해 완전히 일치하지는 않지만 서로 높은 상관도를 가지는 무작위 비트열을 획득할 수 있다.

이점 증류과정에서 상관성 있는 비트열을 생성을 위해서는 양자화 과정이 필수이다. 양자화 과정에서는 양자화 단계 수와 비트 간 불일치 확률 사이에 근본적인 트레이드오프가 존재한다. 즉, 양자화 단계를 증가시킬수록 불일치 비트는 많아진다. 따라서 정보 조정을 위해 필요한 부가정보가 더욱 많이 필요하게 되며, 부가정보는 공개 채널을 통해서 전송되므로 이브에게 노출되는 정보가 늘어나 최종적으로 얻을 수 있는 보안키 생성률의 저하를 일으킨다. 이러한 문제를 해결하기 위해 본 논문에서는 공용 채널을 통해 피드백을 주고받는 적응형 양자화 방식을 제안하였고, 또 오류정정부호의 부호율과 양자화 단계 수를 최적화하여 보안키 추출률을 최대화 하였다.

먼저, 측정 순간의 채널 이득이 양자화 임계값 근방에 있을 때 양자화 비트 간 불일치 확률이 높기 때문에, 채널 상태에 따라 임계값을 조정하는 적응형 양자화 방식을 제안한다. 이 과정은 두 적법한 사용자 중 한 쪽인 엘리스에서만 수행되며, 앨리스는 공용 채널을 통해 변경된 임계값을 밥에게 전달한다. 이브 또한 이 정보를 들을 수 있기 때문에 이브가 획득한 정보를 양자화 결과를 추정하는데 이용할 수 없도록 하는 체계적인 임계값 전달 방법을 제안하였다.

본 논문에서는 정보 조정을 위해 높은 오류정정능력뿐만 아니라 다양한 부호율의 부호를 생성할 수 있는 nested BCH 부호를 사용한다. 그리고 주어진 허용 가능한 비밀 키 불일치 확률 하에서 보안키 생성률을 최대화하기 위해 부호율과 양자화 단계수를 최적화한다. 제안한 프로토콜의 실현 가능성을 확인하기 위해 IEEE 802.11a 무선 LAN 표준 기반의 무선 네트워크 인터페이스 카드를 사용하여 제안 시스템을 구현하였다. 추출 된 비밀 키의 무작위성을 측정하기 위한 다

양한 통계적 검증 실험이 실제 실내 무선 환경에서 이루어졌으며, 실험 결과 동적 (mobile) 시나리오와 정적 (static) 시나리오에서 각각 1.64 비트/초, 0.64 비트/초의 비밀 키 추출률을 달성할 수 있었다. 본 연구에서는 두 개의 적법한 단말장치만을 가정하였으나, 본 연구에서 제시된 보안 키 추출 연구는 네트워크의 노드 수와 무관한 방식으로 다수의 분산 노드들이 존재하는 확장된 네트워크로 손쉽게 적용할 수 있는 장점을 가지고 있다.

본 논문은 다음과 같이 구성된다. 먼저 2장에서는 무선 채널에서 비밀 키를 생성하기 위한 과정을 설명한다. 3장에서는 적응형 양자화 알고리즘의 세부적인 내용을 설명하고 BCH 부호를 통한 비밀 키 추출을 최적화 하였다. 4장에서는 분석적으로 제안한 방식의 성능을 평가하였고 5장에서는 실제 사무실 환경에서 실시한 실험 결과를 통해 제안한 보안 키 추출 알고리즘의 실현 가능성을 확인한다. 그리고 마지막으로 6장에서 결론을 맺는다.

본 논문에서는 다음의 표기법을 따른다. 대문자 굵은체 $\mathbf{X}$와 소문자 굵은체 $\mathbf{x}$는 각각 행렬과 벡터를 의미한다. 랜덤 변수 $X$의 확률밀도함수는 $f_X(\cdot)$으로 표기한다. $\lceil x \rceil$ 은 $x$보다 크거나 같은 정수 중 가장 작은 수를 의미한다. $1_{(x=y)}$는 $x=y$인 경우에는 1, 그 외의 경우에는 0의 값을 가지는 표시함수 (indicator function)이다.

## Ⅱ. 비밀 키 추출 방법

본 논문에서 도청자 이브는 적법한 송수신자 앨리스와 밥 사이에서 일어나는 모든 통신을 도청하며 비밀 키를 추출하기 위해 제안된 모든 절차를 알고 있다고 가정한다. 본 연구에서 제안하는 보인키 생성 시스템은 이점 증류, 정보 조정, 비밀성 증폭의 세 단계로 구성되어있으며, 이를 그림 1에 나타내었다. 본 절에서는 제안된 보안키 생성 시스템의 동작 절차를 요약하여 단계별로 설명한다.

### 2.1 이점 증류 단계

앨리스와 밥 사이의 채널은 무선 채널 응답의 무작위성 확보를 위해 충분히 산란된 무선 채널 환경을 가정하며 앨리스와 밥은 채널 이득을 추정하기 위해 TDD를 이용하여 파일럿을 교환한다. 따라서 파일럿 신호는 WSS (Wide Sense Stationary) 랜덤 프로세스를 따르는 시변 페이딩을 겪는다. 복소 채널 이득의 동상 성분은 직교 위상 성분과 독립적으로 결정되기

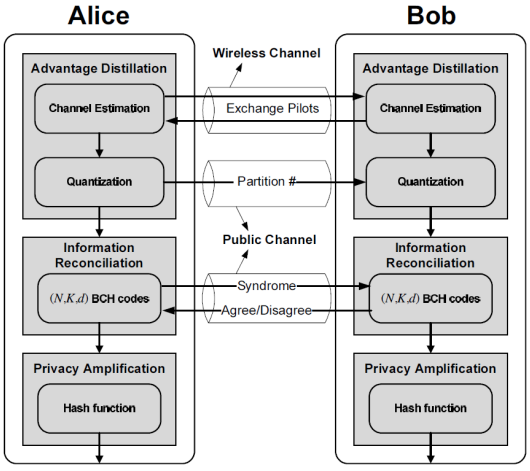



그림 1. 제안된 비밀 키 생성 시스템의 블록 다이어그램
Fig. 1. Block diagram of the proposed secret key generation system

때문에 비밀 키를 추출하는데 둘 중 하나 또는 전부를 사용할 수 있다. 본 논문에서는, 비밀 키를 추출하는데 동상 성분만을 사용하기로 한다. 시간 $t$에서의 복소 채널 이득의 동상 성분과 잡음 성분을 각각 $h(t)$와 $w(t)$이라 하자. 만일 밥이 시간 $t_1$ 에서 첫 번째 파일럿 심볼을 전송했다면 앨리스는 오류를 포함한 채널 응답 $h_A(t_1)=h(t_1)+w(t_1)$ 을 추정한다. 같은 방법으로 밥은 시간 $t_2$에서 앨리스가 보낸 파일럿 심벌을 통해 추정된 채널 $h_B(t_2)=h(t_2)+w(t_2)$ 을 얻는다.

이러한 과정을 통해 획득한 서로 높은 상관도를 가지는 두 랜덤 프로세스 $h_A(t_1)$과 $h_B(t_2)$는 $\triangle t=t_2-t_1$ 일 때 상관 계수 $\rho(\triangle t)$를 가지며 결합 확률 밀도 함수 (Joint PDF, Joint Probability of Density Function) $f_H(h_A,h_B)$를 따르는 상관된 랜덤 변수로 볼 수 있다. 앨리스와 밥은 각각 독립적으로 추정한 채널 응답 값을 양자화 (quantization) 함으로써 높은 상관도를 가지는 $N$비트 배열의 쌍을 생성할 수 있다. 마찬가지로 이브 또한 앨리스와 밥 사이에 전송되는 파일럿 심벌을 통해 채널 이득을 추정할 수 있지만 이브의 거리가 앨리스와 밥으로부터 사용 주파수의 반 파장이상 떨어져 있다면 $h_A(t_1)$, $h_B(t_2)$와 이브의 추정값은 무시할 만큼 작은 크기의 상관도만을 가지게 된다[11]. 따라서 양자화 된 비트열에서 비밀 키를 생성할 때, 앨리스와 밥은 이브에 비해 우위를 가지며 이점을 보안키 생성에 활용한다. 본 논문에서 제안한 양자화 기법은 다음 장에서 자세히 설명한다.

### 2.2 정보 조정 단계

TDD 환경에서 이점 증류를 통해 생성된 비트열들은 적법한 단말간의 채널 대칭성에 의해 서로 높은 상관도를 갖지만, 수신기에서의 잡음과 채널 이득의 시변성 그리고 두 사용자의 파일럿 심볼 전송 시간의 차등이 앨리스와 밥에 의해 생성된 두 비트열간의 비트간 불일치를 야기한다. 제안하는 비밀 키 추출 알고리즘에서는 nested BCH 부호를 사용하여 오류 정정 과정을 통해 이러한 불일치를 제거한다.

먼저 $\mathbf{x}_A = [x_A^1, \cdots, x_A^N]$ , $x_A^i \in \{0,1\} \; \forall i$는 앨리스에 의해 생성된 $N$비트의 비트열을 나타내며 $\mathbf{x}_B = [x_B^1, \cdots, x_B^N]$ , $x_B^i \in \{0,1\} \; \forall i$는 밥에 의해 생성된 $N$비트의 비트열을 나타낸다. 두 비트열 $\mathbf{x}_A$와 $\mathbf{x}_B$ 사이의 비트 간 불일치를 제거하기 위해, 앨리스와 밥은 $d$ 비트까지의 오류를 정정할 수 있는 $(N, K, d)$ BCH 부호를 이용해 추가 정보를 교환한다. 먼저 두 사용자는 $(N-K)\times N$ 패리티 검사 행렬 $\mathbf{H}$를 이용하여 $\mathbf{x}_A$와 $\mathbf{x}_B$에 상응하는 신드롬을 각각 생성한다. 앨리스와 밥에 의해서 계산된 신드롬을 각각 $\mathbf{s}_A = \mathbf{x}_A \mathbf{H}^T$, $\mathbf{s}_B = \mathbf{x}_B \mathbf{H}^T$라 하자. 먼저 앨리스는 신드롬 $\mathbf{s}_A$를 밥에게 공용 채널을 통해 보내게 된다. 밥은 신드롬 차 벡터 $\mathbf{s}_E = \mathbf{s}_A - \mathbf{s}_B = \mathbf{H}^T$를 계산함으로서 에러 벡터 $\boldsymbol{e} = \mathbf{x}_A - \mathbf{x}_B$를 구한다. 밥은 신드롬 차 벡터 $\mathbf{s}_E$를 통해 오류 정정이 가능하면 동의 (agree) 신호를 엘리스에게 피드백 하고, 오류 정정이 불가능하면 비동의 (disagree)신호를 보내고 해당 비트열을 버린 후 이점 증류 단계로 되돌아간다.

### 2.3 비밀성 증폭 단계

본 앞서 정보 조정 단계는 공용 채널을 통해 진행되므로 이브 또한 앨리스로부터 신드롬 벡터 $\mathbf{s}_A$를 획득한다. 따라서 $(N, K, d)$ 블록 부호를 정보 조정에 사용하는 경우, 이브에게 $(N-K)$ 비트가 노출되는 것은 불가피하다. 따라서 이브는 이를 이용해 오류 정정된 비트열을 추정할 수 있게 된다. 이를 방지하기 위해 앨리스와 밥은 정보 조정에 의해 얻어진 $N$ 비트열을 $K$ 비트열로 압축시킴으로써 이와 같은 공격을 무력화 시킨다. 일반적으로 비밀성 증폭을 위해서 유니버셜 해시 (universal hash) 함수 가 사용되며 이러한 과정을 통하여 앨리스와 밥은 이브로부터 완벽보안이 달성된 비밀 키를 추출할 수 있게 된다[12,13]. 비밀성 증폭에 대한 자세한 내용은 이 논문의 범위를 넘어서기 때문에 생략하도록 한다.

## Ⅲ. 적응형 양자화 및 비밀키 추출률 최적화

이 장에서는 본 논문에서 제안된 양자화 방식을 설명하고 보안키 생성률을 최적화 하는 문제를 제시한다. 앞서 설명한 세 단계는 모두 보안키 생성률에 영향을 주지만, 이점 증류 단계의 양자화 과정에서 생성된 비트열의 불일치 확률에 따라 마지막 두 단계에서 얻을 수 있는 보안키 생성률이 결정된다. 따라서 본 논문에서는 측정된 채널 이득에 따라 양자화 임계값을 조정하여 불일치 확률을 줄일 수 있는 양자화 방식을 제안한다. 그리고 제안한 양자화 방식을 기초로 하여 보안키 생성률을 최적화한다.

### 3.1 적응형 양자화 기법

본 논문에서 제안하는 양자화 방식은 동일 발생 확률 구간을 양자화 구간으로 갖는 그레이 부호를 기반으로 한다. 앨리스와 밥이 각각 $M$비트 양자화를 사용한다고 가정하면, 양자화 구간 $\{I_m\}_{m=1}^{2^M}$에 따라 $M$비트의 시퀀스들 중 하나로 채널 추정 값을 양자화 한다. $M$비트 시퀀스들과 구간 $\{I_m\}_{m=1}^{2^M}$사이의 사상 규칙은 그레이 부호를 따른다. 하지만 제안된 양자화 기법에서는 비트 간 불일치 확률을 최소화하기 위해 서로 다른 양자화 구간 $\{I_m\}_{m=1}^{2^M}$ 와 $\{\bar{I}_m\}_{m=1}^{2^M}$을 앨리스와 밥에게 각 각 할당한다. 그레이 부호에 기반한 매핑 규칙은 $M$개의 계층 구조로 이루어져있다. 채널 이득 $h$의 확률밀도함수를 $f_H(h)$로 정의하자. 그레이 부호의 $m$번째 계층은 확률밀도함수 $f_H(h)$를 확률이 같은 $2^m$개의 세부 영역 $\{R_{mi}\}_{i=1}^{2^m}$으로 나눔으로써 생성할 수 있다. 이때, 세부 영역을 결정하는 임계값의 한계를 각각 $\nu_{m0} = -\infty$ 와 $\nu_{m2^m} = \infty$ 이라 할 때 임계값 $\{\nu_{mi}\}_{i=1}^{2^m-1}$는 다음과 같이 정의된다.

$$\int_{h \in R_{mi}} f_H(h)dh = \int_{\nu_{m(i-1)}}^{\nu_{mi}} f_H(h)dh = \frac{1}{2^m} \qquad (1)$$

여기서 $i = 1, \cdots, 2^m$ 이고 $m = 1, \cdots, M$ 이다. 따라서 $2^M$개의 양자화 영역 $\{I_m\}_{m=1}^{2^M}$은 임계값 $\{\nu_{mi}\}_{i=1}^{2^m-1}$에 의해 $I_m = [\nu_{M(m-1)}, \nu_{Mm})$, $m = 1, \cdots, M$ 으로 정의된다. 각 계층에서 0 또는 1이 세부영역 $R_{mi}$에 그레이 매핑 규칙을 따라 반복적

으로 할당되며, $R_{11}$과 $R_{12}$에 초기 값으로 0과 1을 각각 할당한다. $m$번째 계층에 할당된 벡터를 $\boldsymbol{c}_m = [c_{m1} \cdots c_{m2^m}]$ , $c_{mi} \in \{0,1\}$, $i = 1, \cdots, 2^m$ 이라 할 때 $\boldsymbol{c}_m$은 $\boldsymbol{c}_{m-1}$과 $\boldsymbol{c}_{m-1}$의 반전 시퀀스를 연접시켜 생성한다. 여기서 영역 $I_m$에 해당되는 $M$비트 시퀀스 중 $m$번째 비트에는 영역 $I_m$이 세부영역 $R_{mi}$ 위에 놓일 시 $R_{mi}$에 맵핑된 비트 $c_{mi}$를 할당한다. 예를 들어 2비트 양자화 경우를 생각해보자. 첫 번째 계층에 $c_1 = [01]$ 를 할당했기 때문에 두 번째 계층은 $c_2 = [0110]$ 이 된다. 그레이 부호에서, 양자화 영역 $I_1$, $I_2$, $I_3$, $I_4$는 결국 2비트 시퀀스 00, 01, 11, 10을 가지게 된다.

이러한 매핑 규칙을 이용해 양자화 임계값을 추정값에 따라 조정하는 적응형 양자화 기법을 제안한다. 앨리스와 밥이 생성한 $M$비트 시퀀스의 불일치 확률은 채널 이득이 양자화 임계값 근처에 놓일수록 높아지므로 채널 이득 추정 값에 따라 변하기 때문에 임계값을 적응적으로 변화시킬 필요가 있다. 예를 들어, 추정 값이 임계값 근처에 있는 경우 잡음에 의해 앨리스와 밥의 추정 값이 각각 다른 양자화 구간에 있을 확률이 증가한다. 이러한 문제를 해결하기 위해 다음과 같은 기법을 제안한다. 먼저 앨리스가 자신의 추정값이 임계값으로부터 얼마나 떨어져있는지에 대한 파티션 정보를 공용채널을 통해 전송하면 밥은 이를 바탕으로 임계값을 조정한다. 여기서 중요한 점은 이브도 앨리스가 보낸 파티션 정보를 받을 수 있기 때문에, 이브에게 보안키에 대한 어떠한 정보도 유출되지 않도록 체계적으로 정보를 교환해야 한다.

앨리스와 밥은 먼저 양자화 영역 $\{I_m\}_{m=1}^{2^M}$을 동일 확률을 가지는 $P$개의 파티션 구간으로 나눈다. 이 때 각 양자화 구역 $I_m$의 $p$번째 파티션을 $p$라 한다. 앨리스는 추정 값이 속한 파티션 번호 $p$를 밥에게 전송한다. 이에 따른 밥의 새로운 양자화 임계값들은 파티션 번호 $p$에 따라 다음과 같이 결정 된다. 먼저, 만약 $p < \frac{P+1}{2}$이라면 밥은 자신의 양자화 영역을 왼쪽으로 이동시킨다. 즉, 새로운 임계값 $\{\bar{\nu}_{Mi}\}_{i=1}^{2^M}$을 다음과 같이 결정한다.

$$\int_{\bar{\nu}_{Mi}}^{\nu_{Mi}} f_H(h)dh = \frac{1-2p+P}{P2^{M+1}}, i = 1, \cdots, 2^M \qquad (2)$$

임계값의 한계는 $\bar{\nu}_{M0} = -\infty$ , $\bar{\nu}_{M(2^M+1)} = \infty$ 로 동일하다. 새로운 양자화 구역은 $m = 2, \cdots, M$ 에 대해서 $\bar{I}_m = [\bar{\nu}_{M(m-1)}, \bar{\nu}_{Mm})$ 로 정의되고, $m = 1$에 대해서는 $\bar{I}_1 = [\bar{\nu}_{M0}, \bar{\nu}_{M1}) \cup [\bar{\nu}_{M2^M}, \bar{\nu}_{M(2^M+1)})$로 정의된다. 반면, 만약 $p > \frac{P+1}{2}$이라면 밥은 자신의 양자화 영역을 오른쪽으로 이동시킨다. 즉, 새로운 임계값 $\{\bar{\nu}_{Mi}\}_{i=0}^{2^M-1}$을 다음과 같이 결정한다.

$$\int_{\nu_{Mi}}^{\bar{\nu}_{Mi}} f_H(h)dh = \frac{1-2p+P}{P2^{M+1}}, i = 0, \cdots, 2^M-1 \qquad (3)$$

임계값의 한계는 $\bar{\nu}_{M0} = -\infty$ , $\bar{\nu}_{M(2^M+1)} = \infty$ 로 동일하다. 이 경우 새로운 양자화 구역은 $1 \le m \le M-1$ 일 때 $\bar{I}_m = [\bar{\nu}_{M(m-1)}, \bar{\nu}_{Mm})$ 이고, 그 외에 $\bar{I}_M = [\bar{\nu}_{M(-1)}, \bar{\nu}_{M0}) \cup [\bar{\nu}_{M(2^M-1)}, \bar{\nu}_{M(2^M)})$ 로 정의된다. 만약 $p = \frac{P+1}{2}$이면 현재의 임계값을 유지한다.

$\bar{R}_{Mm} = \bar{I}_m$ , $1 \le m \le 2^M$ 인 $\{\bar{R}_{Mi}\}_{i=1}^{2^M}$을 임계값의 이동에 의해 새로 정의된 $M$번째 계층의 부분영역이라 하면, 밥의 $m$번째 계층의 부분영역은 $\bar{R}_{(m-1)i} = \bar{R}_{m(2i-1)} \cup \bar{R}_{m(2i)}$ , $m = 1, \cdots, M-1$ , $1 \le i \le 2^m$ 으로 재 정의된다.

그림 2에 $M = 2$ , $P = 3$ 일 때 적응형 양자화의 결과를 나타내었다. $h_A$가 영역 $I_2$의 첫 번째 부분에 있기 때문에, 기존 양자화 구간을 $\frac{1-2p+P}{P2^{M+1}}$만큼 왼쪽으로 순환 시프트 시켜서 새로운 양자화 구간 $\{\bar{I}_m\}_{m=1}^{2^M}$을 정의한다. 이렇게 함으로써, 밥은 $p$번째 파티션이 각 구간의 중앙에 위치한 새로운 구간

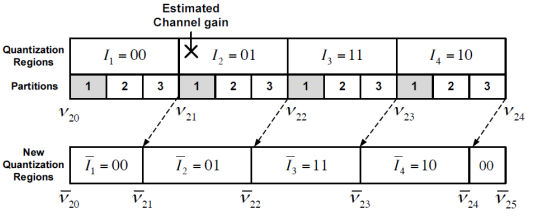



그림 2. 제안된 적응형 양자화 기법 (M=2, P=3)
Fig. 2. Proposed adaptive quantization scheme for M=2 and P=3

$\{\bar{I}_m\}_{m=1}^{2^M}$을 얻게 된다. 앨리스와 밥의 추정값 사이의 상관도가 상당히 높기 때문에 추정 값이 새로운 영역 $\bar{I}_2$의 중심부근에 위치할 확률이 매우 높아져, 두 사용자가 생성한 시퀀스의 불일치 확률이 감소하게 된다. 이브는 앨리스가 보내는 파티션 번호를 얻을 수 있지만, 이브의 추정 값은 앨리스의 추정 값과 매우 낮은 상관도를 가지기 때문에 파티션 번호가 속한 양자화 영역을 예측하는 것이 불가능하다.

### 3.2 비밀 키 최적화

본 제안하는 양자화 방식에서 앨리스와 밥에 의해 생성된 비트열 간 불일치 확률은 비트의 위치에 따라 달라진다. 그레이 부호로 이루어진 $M$개의 계층 구조를 생각해보면, 임계값의 한계 $\nu_{m0}$, $\nu_{m2^m}$을 제외한 $m$번째 계층에 대한 임계값의 개수는 $2^m-1$과 같다. 즉, $M$비트 시퀀스의 $m$번째 비트에 대한 비트 불일치 확률은 $m$이 클수록 증가한다.

따라서 다음과 같이 정보 조정 과정에서 비트의 위치 $m$에 따라 서로 다른 부호율을 가지는 BCH 부호를 적용시킨다. 먼저 $n$번째 채널 측정값에 대한 $M$비트 양자화 결과를 $n$번째 열에 할당함으로써 $M\times N$ 행렬을 생성한다. 같은 행에 위치한 값들은 동일한 비트 오류율을 가지고 있으며, 각 행은 정보 조정 프로세스에 필요한 신드롬을 생성하는 부호어로 사용된다. $(N, K_m, d_m)$ BCH 부호를 $M\times N$ 행렬의 $m$번째 행에 적용한다고 가정하면 $M\times N$ 행렬로부터 생성된 비밀 키의 총 비트수는 $\sum_{m=1}^{M} K_m$이다. 따라서 $l_{key}$ 비트의 비밀 키를 얻기 위해서는 $N\lceil l_{key}/\sum_{m=1}^{M} K_m \rceil$ 번의 채널 이득을 측정해야한다. 여기서 $\lceil x \rceil$은 $x$보다 크거나 같은 정수 중 가장 작은 수를 의미한다.

이러한 과정을 통해 앨리스와 밥이 각각 생성한 비밀 키 간의 불일치 확률을 제약조건으로 두고 $R=\sum_{m=1}^{M}(K_m/N)$ 로 정의된 비밀 키 추출률을 최적화하고자 한다. 주어진 블록 크기 $N$에 대한 $R$을 최대화하기 위해 양자화 단계 $M$과 BCH 부호들의 부호율 $K_1/N,\cdots,K_M/N$을 조절한다. 양자화 된 $M$비트 시퀀스의 $m$번째 비트의 불일치 확률$p_b(m)$은 다음과 같이 나타낼 수 있다.

$$p_b(m)=1-\sum_{i=1}^{2^m}\sum_{l=1}^{2^m}\int_{h_A\in R_{mi}}\int_{h_B\in \tilde{R}_{ml}} f_H(h_A,h_B) \times 1_{(c_{mi}+c_{ml} \bmod 2=0)} dh_B dh_A \quad (4)$$

단, 여기서 $1_{(x=y)}$는 $x=y$인 경우에는 1, 그 외의 경우에는 0의 값을 가지는 표시함수이다. 이전 과정에서 $N$ 채널 측정치들로부터 생성한 $M\times N$ 행렬의 $m$번째 행에 적용할 BCH 부호를 $(N, K_m, d_m)$라 하면 해당 BCH 부호의 워드 오류율 $p_w(m)=1-\sum_{j=0}^{d_m}\binom{N}{j}(p_b(m))^j(1-p_b(m))^{N-j}$ 이다. 이에 따라 전술한 비밀 키 추출률의 최대화 문제를 다음과 같이 정의할 수 있다.

$$R=\max_{M,K_1,\cdots,K_M}\sum_{m=1}^{M}\frac{K_m}{N} \quad (5)$$

$$1-(1-p_w(m))^{\lceil l_{key}/K_m \rceil} \le \alpha \quad \forall m \quad (6)$$

여기서 $\alpha$는 앨리스와 밥이 생성한 비밀 키가 서로 불일치 확률의 허용 가능 최댓값이다. $M$을 고정했을 때 최적 해는 (6)을 만족하는 $(N, K_m, d_m)$ BCH 부호 중 가장 큰 $K_m$이다. 따라서 $M$을 증가시키면서 모든 경우에 대해 $R$을 계산한다면 주어진 최적화 문제를 해결하는 해 $\{M, K_1,\cdots,K_M\}$ 을 찾아낼 수 있다.

## Ⅳ. 레일레이 페이딩 채널에서의 비밀 키 추출률

이 장에서는 채널 분포가 $\mathcal{CN}(0,1)$를 따르는 레일레이 페이딩 채널 환경 하에서 제안된 방식을 사용할 때 획득할 수 있는 보안키 생성률을 채널의 확률 밀도 함수를 통해 계산하고 몬테 카를로 (Monte Carlo) 시뮬레이션 결과로 검증한다. 정규화 된 송신 전력을 1이라 할 때 수신 잡음 성분의 분포는 표준정규분포 $\mathcal{N}(0, N_0/2)$을 따른다. 본 논문에서는 채널 이득의 동상 성분만을 고려하기 때문에, 결합 확률밀도함수 $f_H(h_A,h_B)$는 다음과 같이 나타낼 수 있다[14].

$$f_H(h_A,h_B)=\frac{1}{2\pi\sigma_{h_A}\sigma_{h_B}\sqrt{1-\rho^2(\triangle t)}}\times \exp\left[-\frac{\left(\frac{h_A}{\sigma_{h_A}}\right)^2-\frac{2\rho(\triangle t)h_Ah_B}{\sigma_{h_A}\sigma_{h_B}}+\left(\frac{h_B}{\sigma_{h_B}}\right)^2}{2(1-\rho^2(\triangle t))}\right] \quad (7)$$

여기서 $\sigma_{h_A}=\sigma_{h_B}=(1+N_0)/2$이다. 이 때 $J_0(\cdot)$와 $f_D$를 각각 0차 제 1종 베셀 함수와 도플러 주파수라 할 때 Clarke의 이차원 등방성 채널 모델에

따르면 상관계수 $\rho(\triangle t)=E\{h_A(t)h_B(t+\triangle t)\}/(\sqrt{Var\{h_A(t)\}}\sqrt{Var\{h_B(t)\}})=\frac{J_0(2\pi f_D\triangle t)}{1+N_0}$ 이다[15].

그림 3에 $M$이 2일 때 정적 채널, 즉 $\rho(\triangle t)=1$인 채널에 대해 제안하는 적응형 양자화를 적용한 경우와 기존의 임계값 재설정 과정이 없는 그레이 매핑 기반의 양자화를 적용한 경우의 비트 불일치 확률을 신호 대 잡음비에따라 나타내었다. 한계 성능과의 비교를 위해 $P=\infty$인 경우를 고려하였다. 그림 3을 보면 파티션 개수에 상관없이 제안된 방식이 기존의 방식(conventional)에 비해 훨씬 우수한 성능을 보여준다는 것을 확인할 수 있다. 뿐만 아니라, 채널의 변화가 비트 간 불일치 확률에 주는 영향을 확인하기 위해 파일럿 전송 시간차 $\triangle t$의 변화에 따른 비트 불일치 확률을 그림 4에 나타내었다. 그림 3과 동일한 환경에서 $P=3$으로 고정했을 때의 결과를 나타내었으며 비트의 위치에 따라 비트 불일치 확률이 서로 다르므로, 수식 (4)의 첫 번째 비트 $(m=1)$의 불일치 확률 $p_b(1)$을 이용해 성능을 비교하였다. 앨리스가 3.6 km/h와 60 km/h로 이동할 때, 5.2 GHz 반송파 주파수에 대한 상관 시간은 각각 10 ms, 0.6 ms이다. 두 경우 모두 파일럿 전송 시간차가 상관 시간보다 커짐에 따라 비트 불일치 확률이 급격히 0.5에 접근하는 것을 확인할 수 있다. 이는 파일럿 전송 시간차가 커질수록 앨리스와 밥이 측정한 채널이득 사이의 상관도가 급격히 감소하기 때문이다. 파일럿 전송 시간차 $\triangle t=1$ ms이고 사용자의 이동속도가 3.6 km/h일 때 신호 대 잡음비에 따른 비밀 키 추출률을 그림 5에 나타내었다. 여기서 비트 불일치 확률 $\alpha=10^{-3}$으로 제한하였다. 비밀 키 추출률의 상한으로는 $h_A(t_1)$과 $h_B(t_2)$의 상호 정보량을 계산하여 사용하였다[10].

다양한 블록 크기 $N$에서 컴퓨터 시뮬레이션을 통해 최적의 비밀 키 추출률을 계산하였다. 신호 대 잡음비가 향상되면 양자화 단계를 증가시킬 수 있기 때문에 많은 수의 비밀 키를 추출할 수 있게 된다. 따라서 신호 대 잡음비의 향상에 따라 양자화 단계가 증가되는 곳에서 비밀 키 추출률이 급격히 증가하여 비밀 키 추출률의 증가 양상이 전체적으로 계단 형태를 띠는 것을 확인할 수 있다.

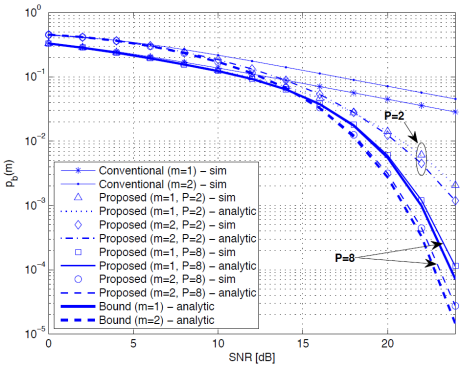



그림 3. M=2일 때의 SNR에 대한 불일치 확률. Conventional은 임계값의 이동이 없는 그레이 매핑의 기존 양자화 기법을 나타냄

Fig. 3. Mismatch probability as a function of SNR for M = 2. Conventional schemes represent Gray mapping based quantization without shifting thresholds

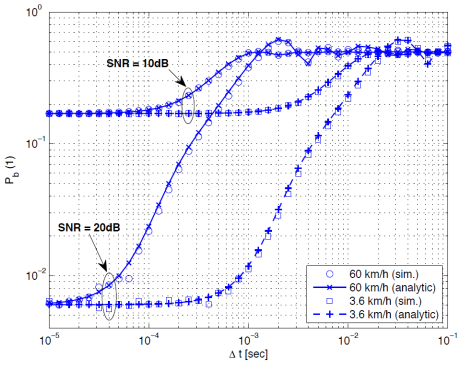



그림 4. M=2, P=3일 때, 시간차에 대한 불일치 확률

Fig. 4. Mismatch probability as a function of time difference for M=2, P=3

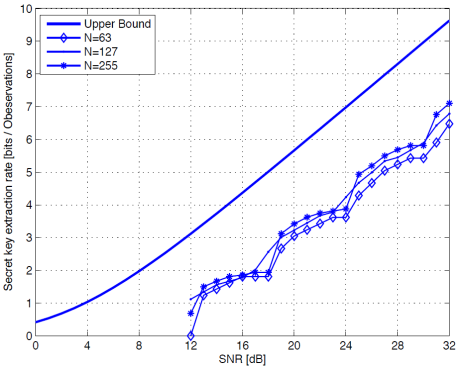



그림 5. $\triangle t$ = 1 ms, 이동속력 3.6 km/h일 때 SNR에 따른 비밀 키 추출률

Fig. 5. Secret key extraction rate as a function of SNR for $\triangle t$ = 1 ms and moving speed at 3.6 km/h

## V. IEEE 802.11a를 통한 실증

### 5.1 실험 환경

본 이 장에서는 본 논문에서 제안하는 비밀 키 추출 알고리즘을 하드웨어로 구현하여 실제 실내 환경에서 실험한 결과를 보인다. 하드웨어 기반의 구현을 위해 Linux의 Madwifi 드라이버를 이용하는 5.2 GHz 대역의 상용 IEEE 802.11a 무선 네트워크 카드 세 대를 사용하였다.두 적법 송수신기 사이에서 랜덤 시퀀스를 생성하기 위해 이점 증류 과정에서는 상대방으로부터 수신한 신호의 세기 (Received Signal Strength Indicator, RSSI)를 측정하고 이를 본 논문에서 제안하는 방법을 이용해 양자화 하였다.

그림 6에 동적 시나리오와 정적 시나리오에서의 실험 환경을 나타내었다. 정적 시나리오에서 앨리스는 밥으로부터 6미터 떨어진 위치에 정지해있다.동적 시나리오에서는 밥으로부터 6미터 떨어진 앨리스가 고정된 경로를 따라 이동하며 밥과 통신을 수행한다. 두 경우 모두에서 이브는 밥으로부터 1미터 떨어진 위치에 정지해있다. 칸막이들에 의해 앨리스와 다른 사람 간에는 직진파가 형성되지 않는다. 양자화에 활용되는 수신 신호 강도 지수 값은 ICMP ping 패킷을 매 50ms마다 주고받으며 획득한다. 네트워크 측정 애플리케이션 *TCPDUMP*를 사용하였고, 타임스탬프 또한 ICMP 패킷을 이용해 기록하였다.

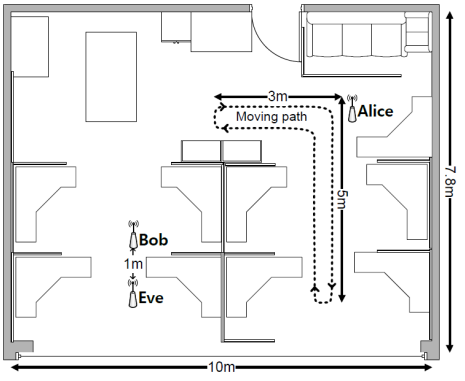



그림 6. 실험 배치도
Fig. 6. The layout of experiments

### 5.2 측정 결과, 보안 성능 검증 및 토론

본 앨리스, 밥, 이브에서 측정한 수신 신호 강도 지수 값을 그림 7에 나타내었다. RSSI 측정 신호로부터 대규모 페이딩에 의한 영향을 제거하기위해 윈도우 크기 10의 필터를 이용하여 이동 평균 기법을 수행하

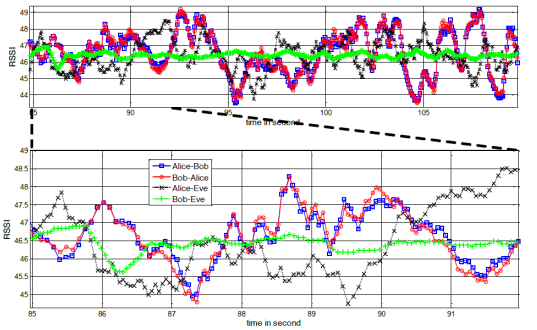



그림 7. 구간 평균을 뺀 RSSI. □과 X는 각각 밥과 이브가 앨리스로부터 수신한 신호의 RSSI이며 ○와 +는 각각 앨리스와 이브가 밥으로부터 수신한 신호의 RSSI이다
Fig. 7. RSSI values after subtracting windowed mean. Lines with squares and x-marks represent RSSI values capture by Bob and Eve corresponding to Alice's signals. Lines with circles and cross in turn represent RSSI values capture by Alice and Eve corresponding to Bob's signals

였다. 밥과 이브의 거리가 1m로 매우 가깝고 정지해 있기 때문에 둘 사이의 채널이 정적이므로 그림 7에서와 같이 RSSI값의 변화가 상대적으로 작은 것을 관찰할 수 있다. 앨리스와 밥 사이의 채널은 채널 상호성 (channel reciprocity)에 의해 높은 상관성을 가지며 시변 하는 것을 관찰할 수 있다. 반면에 이브는 완전히 다른 수신 강도로 신호를 수신한다. RSSI 측정값이 이점증류로 사용하기에 충분한지 확인하기위해 측정한 RSSI들 사이의 상관 계수를 계산하여 표 1에 나타내었다.

모든 시나리오에서 앨리스와 밥이 측정한 RSSI들은 높은 상관 계수를 가지는 반면, 앨리스와 이브 및 밥과 이브가 측정한 RSSI들은 낮은 상관 계수를 가지는 것을 확인할 수 있다. 5.2 GHz 무선 신호의 파장은 약 5.8 cm이기 때문에 실험 환경에서 설정한 밥과 이브 사이의 거리는 밥과 이브가 무시할 만큼 작은 상관도를 가지는 두 추정치를 획득할 만큼 충분히 멀다는 것을 실험을 통해서 확인할 수 있다. 본 논문에서

표 1. RSSI 값들과 각 노드들의 상관관계. $I_{XY}$는 $Y$가 송신한 신호에 대한 $X$의 RSSI 값. $A$, $B$, $C$는 각각 앨리스, 밥, 이브를 나타낸다
Table 1. Correlation of RSSI values between each node. $I_{XY}$ denotes $X$'s RSSI values corresponding to $Y$'s transmitted signals. $A$, $B$, and $C$ indicate Alice, Bob and Eve, respectively

| | Mobile Scenario | Static Scenario |
|---|---|---|
| $\rho I_{AB} I_{BA}$ | 0.9597 | 0.9835 |
| $\rho I_{AE} I_{AB}$ | -0.0527 | 0.0893 |
| $\rho I_{BE} I_{BA}$ | -0.0533 | 0.0016 |

제안한 보안키 생성 프로토콜의 보안 성능을 검증하기 위해 NIST (National Institute of Standard and Technology)에서 제시한 보안키의 보안 성능 검증기법을 적용하였고, 검증 결과를 표 2에 나타내었다. 추출한 비밀 키에서 충분한 무작위성이 보장되지 않는다면 이브가 통계적인 방법으로 비밀 키를 해독할 수 있기 때문에 NIST 테스트[16]에 따라 생성된 비밀 키의 무작위성을 보여주는 $p$값을 측정하여 표2에 함께 나타내었다.

표 2의 마지막 4행에 다양한 테스트를 통해 계산한 $p$값을 나타내었다. $p$값이 0.01보다 크다면, 해당 시퀀스는 충분히 무작위하다고 판단할 수 있기 때문에 제안된 기법을 이용하여 얻은 시퀀스가 보안키로 활용하기에 충분하다는 점이 검증된다. 실험을 통해서 얻은 시퀀스들은 전부 NIST 테스트를 통과하였다. 실험 결과 제안된 프로토콜을 통해서 충분히 무작위한 보안키를 동적 및 정적 시나리오에서 각각 1.64 비트/초, 0.65 비트/초의 속도로 생성할 수 있다는 결과를 얻었다.

표 2. 실험 결과 요약
Table . Summary of experimental results

| | Mobile Scenario | Static Scenario |
|---|---|---|
| Duration of Experiments | 2225 sec | 2681 sec |
| Quantization level | 3-bit | 1-bit |
| Probability of key-mismatch | 0 | 0 |
| Secret key rate | 1.64 bits/sec | 0.65 bits/sec |
| Frequency (mono bit) test | 0.443 (Random) | 0.655 (Random) |
| Frequency test within a block | 0.718 (Random) | 0.612 (Random) |
| Runs test | 0.731 (Random) | 0.154 (Random) |
| Cumulative sums test | 0.687 (Random) | 0.173 (Random) |

## Ⅵ. 결 론

본 논문에서는 두 적법한 사용자가 키 관리 기반구조에 의존하지 않고 공통된 비밀 키를 효율적으로 획득하는데 필요한 적응형 양자화 방법을 제안하였다. 제안하는 양자화 방법은 양자화 임계값들을 측정된 채널 이득에 따라 적응적으로 변화시킴으로서 비트 불일치 확률을 감소시키고 결과적으로 비밀 키 추출률을 증가시킨다. 또한 최적화 문제를 해결함으로써 비밀 키 추출률을 최대화하는 양자화 단계와 오류정정부호의 부호율을 결정하였다. 뿐만 아니라 상용 802.11a 네트워크 카드를 이용해 제안한 비밀 키 추출 방법을 실제로 구현하여 동적 상황과 정적 상황에서 비밀 키를 각각 1.64 비트/초, 0.65 비트/초의 속도로 생성할 수 있다는 것을 증명하였다. 제안된 기법을 이용하면 시변 하는 무선 채널로부터 지속적으로 보안키를 생성하고 공유할 수 있기 때문에 사전 키 분배없이 강력하고 효율적인 대칭키(AES, Advavnced Encryption Standard)와 같은 기술을 사용하여 강력한 기밀성을 제공할 수 있을 것으로 기대된다. 또한 개별 노드가 세션 키 공유를 위해 사전에 저장하고 있어야 할 정보가 없기 때문에 노드 포획 (node capture) 공격에 강인한 특성을 갖는다. 특히 보안 키 생성을 위해 수행해야하는 연산이 양자화 및 간단한 행렬 연산을 통해서 이루어지기 때문에 자원 및 연산 능력이 제한되어있는 Internet of Things와 같은 자율 분산형 시스템에 활용되기 좋은 기술이다.

## References


[1] 임용재 외 2, "미래 인터넷의 진화방향: Internet of Things," PM Issue Report 2012, vol. 2, no. 1, 2012.

[2] 김동희 외 2, "IoT 서비스를 위한 보안," *Inf. Commun. Mag.*, vol. 30, no. 8, pp. 53-59, 2013.

[3] J. Park, S. Shin, and N. Kang, "Mutual Authentication and Key Agreement Scheme between Lightweight Devices in Internet of Things," *J. KICS*, vol., 38B no. 09, pp. 707-714, 2013.

[4] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography, Part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121-1132, Jul. 1993.

[5] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733-742, May 1993.

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptology*, vol. 5, pp. 3-28, 1992.

[7] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, “Generalized privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915-1923, Nov. 1995.

[8] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robust key generation from signal envelopes in wireless networks,” in *Proc. ACM Comput. Commun. Security*, pp. 401-410, Oct. 2007.

[9] N. Patwari, J. Croft, S. Jana, and S. Kasera, “High-rate uncorrelated bit extraction for shared secret key generation from channel measurements,” *IEEE Trans. Mob. Comput.*, vol. 9, no. 1, pp. 17-30, Jan. 2010.

[10] C. Ye, A. Reznik, and Y. Shah, “Extracting secrecy from jointly gaussian random variables,” in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2593-2597, Jul. 2006.

[11] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio telepathy: Extracting a secret key from an unauthenticated wireless channel,” in *Proc. ACM Int. Conf. Mob. Comput. Netw. (MobiCom ’08)*, pp. 128-139, San Francisco, CA, Sept. 2008.

[12] J. L. Carter and M. N. Wegman, “Universal classes of hash functions,” *J. Comp. Syst. Sci.*, vol. 18, pp. 143-154, 1979.

[13] M. N. Wegman and J. L. Carter, “New hash functions and their use in authentication and set equality,” *J. Comp. Syst. Sci.*, vol. 22, pp. 265-279, 1981.

[14] W. B. Davenport, Jr. and W. L. Root, *An Introduction to the Theory of Random Signals and Noise,* NY: McGraw-Hill, 1958.

[15] W. C. Jakes, *Microwave Mobile Communications*, NY: IEEE Press, 1974.

[16] NIST, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, 800th Ed., National Institute of Standards and Technology, 2001.

**임 상 훈** (Sanghun Im)

2009년 : 숭실대학교 전기 및 전자공학부 공학사

2011년 : 한국과학기술원 전기 및 전자 공학과 공학석사

2011년~현재 : 한국과학기술원 전기 및 전자 공학과 박사과정

<관심분야> 무선통신 신호처리, 정보이론, 물리계층 보안

**전 형 석** (Hyungsuk Jeon)

2004년 2월 : 동국대학교 공학사

2005년 8월 : 한국과학기술원 공학석사

2010년 8월 : 한국과학기술원 공학박사

2010년 9월~2011년 8월 : 한국과학기술원 연수연구원

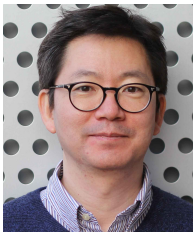
2010년 12월~2011년 8월 : Georgia Technology Institute 방문 연구원

2011년 9월~2014년 7월 : Georgia Technology Institute Postdoc

2014년 8월~현재 : Reverb Networks Inc. Senior Member of Technical Staff

<관심분야> 무선통신 신호처리, 정보이론, 물리계층 보안

**하 정 석** (Jeongseok Ha)



1992년 : 경북대학교 전자공학과 학사

1994년 : 포항공과대학교 전자전기 석사

2003년 : Georgia Tech 박사

2004년~2010년 : 한국정보통신대학교 조교수

2010년~현재 : 한국과학기술원 부교수

<관심분야> 통신, 채널부호, 물리계층 보안