물리계층 보안을 위한 보안 전처리 기법의 설계 방법

권경훈, 허 준
고려대학교

요 약

본 논문에서는 물리 계층에서 보안을 고려한 시스템을 제공하기 위해 Gaussian Wiretap Channel 상황에서 보안 전송을 가능하게 하는 보안 전처리 기법의 설계 방법에 대해서 살펴본다. 무선 통신 채널의 경우, 통신 채널이 누구에게나 개방되어 있기 때문에 무엇보다도 보안에 취약하다. 하지만 숨기고자 하는 보안 메시지를 채널 부호화 및 변조 과정 이전에 보안을 위한 전처리 기법을 적용함으로써 물리계층에서 데이터를 보다 안전하게 전송하는 것이 가능해진다. 이를 위해 기존의 Random하게 생성된 Scrambling matrix를 이용하여 물리계층 보안을 유지하는 전처리 기법을 바탕으로 Scrambling matrix의 hamming distance를 이용하여 높은 보안성 및 신뢰도를 가지는 Scrambling matrix 설계 방법을 제안한다. 또한 부호율 1을 가지는 soft decision decoding 기반의 새로운 보안 전처리 기법을 제안함으로써 물리계층에서의 보안성 확보 가능성을 확인하였다.

Ⅰ. 서 론

현재의 무선 통신 기술은 지난 수십 년간 눈부신 발전을 해오고 있다. 주로 송신자와 수신자간의 정보를 교환하는데 있어서 보다 빠르고 신뢰도가 높은 전송기법들 위주로 연구가 진행되었다. 그로 인해 언제 어디서나 사용자가 네트워크에 접속할 수 있도록 편의성과 휴대성을 가지고 있어서 우리 삶과 밀접한 영향을 끼치며, 우리의 생활이 모두 통신과 연관을 가지고 있다. 이처럼 무선 통신 기술은 그 편의성 때문에 생활 많은 부분에서 활용되고 있지만 통신 채널은 누구에게나 개방되어 있기 때문에 무엇보다도 보안에 취약할 수밖에 없다. 이러한 무선 통신의 특성에 의해 데이터 전송 중 도청자가 통신 시스템 내에 침입하여 원하는 정보를 도청하게 되는 경우가 발생할 수 있다. 도청자의 침입으로 인한 정보의 도청 및 해킹에 관한 문제는 무선 통신뿐만 아니라 모든 통신 시스템에 적용이 가능한 문제이다. 누구나 무선 채널로 전송되는 데이터를 획득할 수 있기 때문에 보안을 위협하는 존재를 검출하고 이를 방지하는데 큰 어려움이 있다. 이는 향후의 무선통신 시스템에 있어서 해결해야 할 중요한 문제이며, 대응방법 또한 시급히 마련되어야 한다. 최근 들어 이처럼 보안의 중요성이 부각되면서 송신자와 수신자간 정보 전송에 있어서 전송 속도, 전송 reliability 외에도 전송 security의 중요성이 대두되고 있고, security가 확보되는 시스템에 대한 연구가 진행되면서 보안의 중요성이 점차 증가하는 추세이다.

1945년 Shannon이 통신 이론을 정립하면서, secure communication에 대해 정보 이론적 관점에서의 기본적인 개념들을 정의 하였다[1]. Shannon의 정의에 따르면, 송신자 Alice는 적법한 수신자 Bob에게 k 비트의 메시지 M을 securely 하게 public channel을 통해 전송하게 된다. 이때, 전송된 메시지를 X라고 정의하면, Bob이 수신한 메시지 X와 Alice가 전송한 메시지 M 사이의 mutual information $I(M;X)=0$을 만족하게 되면 완벽 보안 (perfectly secure)가 보장된다. 따라서 이 결론으로부터 Shannon은 완벽보안을 얻기 위해서 Alice와 Bob이 서로 k 개의 비트의 키를 반드시 공유하고 있어야 한다는 것을 증명하였다. 즉, Shannon의 이론으로부터 key distribution의 대한 문제가 제기되었고, 현재의 upper layer에서 사용되는 cryptography기반 방어시스템의 근간이 되었다. 현재에 사용되는 암호학 기반의 방어시스템은 데이터가 도청자에게 노출이 되더라도 암호키가 없으면 데이터를 해독할 수 없게 하는 방식으로 대표적인 방식으로 RSA 공개키 알고리즘이 있다. 이러한 공개키 알고리즘은 보안의 완벽성을 도청자의 연산능력의 한계에 의존하고 있다. 즉, 암호키를 모른다면 현재의 정보처리 기술로는 현실적인 시간 내에 계산이 불가능하도록 암호화하여 보안의 완벽성을 보장한다. 하지만 기술이 발전함에 따라, 계산 복잡도에 의존하는 암호학 기반의 보안기술이 한계를 보일 것으로 예상된다. 그로인해 Shannon의 이론에 따른 키 분배 보안기술은 양자이론을 바탕으로 하는 양자 키 분배 기술을 통해 보안성을 확보하는 방향으

로 연구가 진행되고 있다. 하지만 양자 이론을 바탕으로 하는 기술은 양자의 성질을 다루는 것이 아직은 실제적인 문제가 아니기 때문에 앞으로 실용화 되는데 까지 많은 시간을 필요로 하는 것이 사실이다.

현재와 같은 계산 복잡도에 의존하는 보안 시스템을 대체할 기술로 물리 계층을 활용하는 방안이 있다. 기존 key distribution 문제와는 별개로 도청자가 무선 채널을 통해 획득한 데이터에서 발생된 오류의 정정을 불가능하게 하고 적법한 수신자는 오류를 정정할 수 있도록 물리 계층의 특성을 이용하는 기술이다. 물리 계층 기술을 활용한 보안기술은 도청자의 계산능력의 한계에 의존하는 것이 아니라 정보이론의 수학적 증명에 의해 보장되기 때문에 기존 암호학 기술과 달리 고속 연산 기술의 발전에 따른 위협으로부터 자유롭다는 장점이 있다.

이처럼 물리 계층 기술을 기반으로 하는 보안시스템은 1975년 Wyner가 소개한 wiretap 채널 정보이론 모델에 이론적 기초를 두고 있다[2]. Wyner가 정의한 wiretap channel 모델에 따르면, Alice와 Bob 사이의 전송 채널을 main 채널로 정의하고, 도청자 Eve가 Alice와 Bob사이의 전송되는 데이터를 도청하는 채널을 wiretap 채널로 정의한다. 또한 Bob과 Eve가 가지고 있는 채널은 모두 discrete memoryless channel로 가정한다. Alice와 Bob은 서로 보안을 유지하면서 main 채널을 통해 s 비트의 메시지 M을 전송한다고 하면, Alice는 메시지 M을 n bits의 부호어 X로 부호화 하여 전송하게 된다. 적법한 수신자 Bob과 도청자 Eve는 X를 서로 다른 각각의 main, wiretap 채널을 통해서 수신하게 된다. Bob과 Eve의 observation을 각각 Y와 Z라고 하면, Alice는 다음 두 가지 조건을 만족시키도록 메시지를 부호화하게 된다. 첫째, 메시지 M과 Bob이 수신한 메시지 Y를 복호한 M과 B사이의 오류확률이 0에 근접(무시할 수 있을 정도로 작은 값)하는 값을 가져야 한다(Reliability). 둘째, Alice의 메시지 M과 도청자 Eve가 수신한 메시지 Z를 복호한 메시지 M_E사이의 mutual information $I(M;M_E)=0$을 만족하도록 Alice와 Eve는 서로 메시지를 공유하는 부분이 없어야 한다(Security). Wyner는 wiretap 채널이 main 채널의 감쇄된 채널이라는 조건을 만족하고 있을 때, 키 전송이 없이 오류정정부호만으로 reliability와 security 조건을 만족시킬 수 있음을 증명하였다. 이때의 rate $\frac{s}{n}$을 secrecy rate로 정의 하였다. 두 가지 조건은 다음과 같은 수식으로 표현될 수 있다.

$$\Pr\{M \neq M_B\} < \epsilon \ , \ \epsilon \approx 0 \ : \text{reliability} \qquad (1)$$

$$I(M;M_E) = H(M) - H(M|M_E) = 0 \ : \text{security} \qquad (2)$$

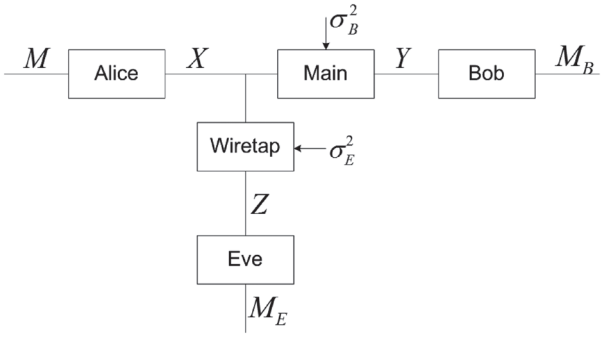

그림 1. 가우시안 Wiretap 채널 모델의 블록도

Wyner가 wiretap 채널 모델의 기본 가정을 세웠다면, Cheong은 Gaussian noisy 채널의 대한 Gaussian wiretap 채널 모델을 일반화하였다[3]. 〈그림 1〉은 Cheong이 Wyner의 Wiretap 채널 모델을 바탕으로 하여 모델링한 Gaussian Wiretap 채널 모델이다. Wyner의 wiretap 채널 기본 모델은 wiretap 채널이 main 채널의 감쇄된 채널이라고 가정하면 완벽 보안을 만족할 수 있다는 것을 보인다는 것이다. 즉, main 채널은 wiretap 채널보다 less noisy 채널로 정의 될 수 있다. 이 경우 Gaussian wiretap 채널에서는 Bob의 수신 SNR이 Eve의 수신 SNR보다 더 크다고 정의 될 수 있고, 이에 따라 Bob과 Eve 채널 사이의 보안 채널 용량 secrecy capacity C_s^{WT}는 다음과 같이 표현할 수 있다.

$$C_s^{WT} = \left\{ \frac{1}{2} log\left(1 + \frac{P}{\sigma_B^2}\right) - \frac{1}{2} log\left(1 + \frac{P}{\sigma_E^2}\right) \right\}^+ \qquad (3)$$

Reliability와 security에 관한 두 가지 조건이 만족 된다면, (3)식을 통해서 완벽 보안이 보장된다. (3)식의 완벽 보안을 만족하기 위해서 식 (1)과 (2)의 조건을 만족해야 한다. (2)식의 security를 확보하기 위해서 wiretap 채널의 confusion 정도를 결정하는 기준인 Equivocation rate $\Delta = \frac{1}{n} H(M|M_E)$의 정보가 필요하다. Equivocation rate는 Alice가 전송한 메시지 M과 Eve가 수신한 메시지 M_E사이의 conditional entropy로 표현 될 수 있으며, secrecy 정도를 측정하는 중요한 요소이다. 따라서 equivocation rate와 secrecy capacity를 측정하기 위한 방법 중에 하나가 실제 시스템에서 사용하는 coding과 modulation을 고려하였을 때, Bit Error Rate (BER)을 통해서 측정하는 방식이 중요한 metric이 될 수 있다. Eve가 수신한 메시지 M_E의 bit error probability가 0.5에 이르게 되고, 랜덤하게 발생한 오류라고 가정한다면, 도청자 Eve는 수신한 메시지를 절대 복원해낼 수 없게 된다. 0.5의 error probability는 maximum entropy를 가지게 되기 때

문이다. 이처럼 BER을 통해 security를 measure하는 방식은 "security gap"이라는 measurement로써 Klinc에 의해 제일 처음 제안되었다[5][6]. Security gap은 Physical layer에서 충분한 security level을 얻기 위해 필요한 Bob과 Eve의 수신 SNR의 차이로 정의 된다. Wiretap 채널은 main 채널의 감쇄된 모델이기 때문에, Bob의 수신 SNR이 Eve의 수신 SNR보다 크게 된다. 동일한 메시지 M에 대해서 Bob과 Eve의 수신 SNR이 security를 확보하기 위해서 Eve는 error probability가 0.5에 이르는 오류율을 가지고 있어야 하며, Bob은 reliability를 확보하기 위해서 error probability가 0에 이르는 오류율을 가져야 한다. 오류율 0은 실제 시스템에서 무시할 수 있을 정도의 아주 작은 오류율이므로 10^{-5}영역에서의 오류율을 가지는 수신 SNR로 정의한다. Bob의 10^{-5}오류율을 가지는 최소 SNR 값 $SNR_{B,Min}$과 Eve가 0.5 오류율을 가지는 최대 SNR 값 $SNR_{E,Max}$의 차이로 security gap을 정의한다.

$$S_G(\text{sec}urity\ gap) = SNR_{B,Min} - SNR_{E,Max}\ \ (dB) \quad (4)$$

(4)식의 정의에 따르면, Security gap을 줄이는 것은 Bob과 Eve의 채널 상태의 차이가 크지 않은 상황에서 security를 확보할 수 있게 만드는 기술로 정의될 수 있다. 적은 security gap은 Eve의 채널의 감쇄 정도가 크지 않아도 충분한 security 확보가 가능하게 된다는 의미이다. 따라서 security gap을 줄이기 위해서는 BER 성능 곡선을 좀 더 sharp하게 만드는 것이 중요하다.

이러한 security gap을 줄이기 위한 오류정정부호 관련 연구는 주로 LDPC 부호 위주로 이루어져 있다. LDPC 부호 위주의 연구가 진행된 이유로는 LDPC 부호가 뛰어난 오류정정 능력을 가지고 있고, density evolution이라는 LDPC BP decoder에 대해 강력한 분석 tool이 존재하기 때문이다. Klinc는 LDPC 부호를 이용해 puncturing 기법을 통해서 security를 확보하는 알고리즘을 제안하였다. Puncturing을 이용한 LDPC 부호의 security 연구는 systematic transmission을 피하기 위해 제안되었다. information 비트들을 secret 메시지로 구성하여 이를 LDPC 부호화 과정을 거쳐서 생성된 parity 비트만을 전송에 사용하고 나머지 secret information bits는 모두 puncturing 시켜서 systematic transmission에서 secret 메시지의 노출(expose)을 제거하는 방식이다. 더 이상 채널을 통해서 전송되지 않고 LDPC 복호기에서 부호어의 non-punctured part만 이용하여 최종 메시지를 복원한다. 하지만 LDPC 부호만을 사용하였을 때, information puncturing 기법 적용이 가능하고, fixed rate에 대해서만 증명을 하였기 때문에 다른 오류정정부호의 사용이나 여러 부호율을 가지는 경우에 대해서는 사용이 제한적인 단점이 있다. 또한 punctured code는 non punctured code에 비해 더 많은 power consumption이 필요한 단점도 있다. Baldi는 이러한 심한 power consumption을 줄이기 위해 non-punctured 부호 기반으로 security를 확보하는 scrambling 기법을 제시 하였다[9][10]. McEliece Cryptosystem[4]을 바탕으로 scrambling 행렬를 이용하는 기법으로써 숨기고자 하는 information 비트들을 scrambled non-systematic 부호로 구성하여 frame error가 발생하였을 때, bit error propagation시켜서 security를 확보하는 구조이다. 이 기법은 security gap을 획기적으로 줄일 수 있는 장점이 있으며, frame error rate(FER)의 손실 없이 security를 확보하게 되므로 전체 시스템 power consumption 측면에서 큰 장점이 있다. 하지만 오류정정부호의 복호과정을 끝낸 상태에서 매우 적은 오류임에도 불구하고 scrambling 기법이 오류정정 기능이 없고 hard decision 값을 이용하여 수신된 전체 frame에 대해 error propagation을 시키게 되므로 high SNR 에서도 소수의 error에 매우 민감하게 작용함으로써 전체 BER을 악화시키게 된다. Security gap을 줄이기 위해서는 보안 오류정정부호의 성능이 매우 sharp한 성능 곡선을 보여야 하기 때문에 high SNR 영역에서 생기는 소수의 error propagation 현상을 막아야 한다.

따라서 본 논문에서는 linear block code에서 사용하는 information puncturing 기법의 제한적인 단점을 극복하고 기존의 scrambling 기법에서 random하게 생성된 scrambling 행렬을 minimum hamming distance를 고려하여 high SNR 영역에서 error propagation을 억제시킬 수 있는 Scrambling 행렬 설계 방식을 제안한다. 또한 복원 과정에서 기존의 hard decision decoding 방식이 아닌 soft decision decoding 방식이 가능하고 부호율 1을 유지시키는 보안 전처리 부호를 제안한다. Feed-forward 구조를 가진 Rate-1 부호의 보안 전처리 기법은 수신단에서 BCJR decoding 알고리즘을 사용하기 때문에 단일 오류에 대해서 오류정정이 가능하다. 이로 인해, high SNR에서 단일 오류로 인한 error propagation을 피하게 되므로 전체시스템의 security gap을 줄일 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 이전의 연구에서 진행된 LDPC 부호의 information puncturing 기법과 conventional Scrambling 기법에 대해서 간략히 살펴본다. 3장에서는 minimum hamming distance를 고려하여 설계된 Scrambling 기법과 새롭게 제안하는 Rate-1 feed-forward 전처리 기법의 부호화 및 복호화 과정에 대해서 설명하고 이들의 성능을 살펴본다. 4장에서는 제안된 기법들이 적용된 전

송 시스템에서의 reliability 성능과 security 성능을 살펴본다. reliability 성능은 일반적인 BER 성능 곡선을 통해서 살펴보고, security 성능은 security gap을 보안 성능지표로 삼아 security gap 측면에서 성능을 살펴본다. 5장에서는 모의 실험을 토대로 보안을 확보할 수 있는 파라메터에 대하여 살펴보고, 앞으로 추가 연구되어야 할 부분에 대하여 기술하며 본 논문의 끝을 맺는다.

Ⅱ. Preliminaries and Related Works

1. System Model

우리는 AWGN 환경에서 도청자 Eve가 존재하고 있을 때, Gaussian Wiretap 채널에 대해서 앞서 설명하였다. 송신자 Alice는 secret 메시지 $M \in [1,2,\cdots,2^k]$을 적법한 수신자 Bob에게 전송하기 위해서 n-bit의 전송된 시퀀스 $X \in [x_1,x_2,\cdots,x_n]$로 부호화를 하여 전송한다. Bob과 Eve의 수신 시퀀스를 각각 Y^n, Z^n이라고 하고, 전송 시퀀스 X는 BPSK 변조를 통해 전송하게 되면 Gaussian Wiretap 채널을 다음과 같이 모델링 할 수 있다[7][8].

$$\begin{aligned} Y_i &= X_i + N_i^{bob} \\ Z_i &= X_i + N_i^{eve} \end{aligned} \tag{5}$$

N_i^{bob}과 N_i^{eve}는 independent and identically distributed (i.i.d) zero-mean을 따르고 variance σ^2을 가지는 Gaussian random variable로 정의 할 수 있다. Wyner의 Wiretap 채널 모델에서는 Wiretap 채널 상태가 Main 채널에 대해서 감쇄된 모델을 따르고 있다.

Alice가 보내고자 하는 secret message M의 길이가 s비트이고, 오류정정부호의 information part의 dimension을 k, channel을 통해 전송된 비트의 수를 n_{ch}, 오류정정부호의 codeword dimension을 n_{code}라고 할 때, 오류정정부호의 design rate $R_d = k/n_{ch}$, secret rate $R_s = s/n_{ch}$, code rate $R_c = k/n_{code}$로 정의 할 수 있다. 이 때, secret 메시지의 길이 s와 오류정정부호의 information 길이 k가 $s = k$로 같다면 $R_s = R_d$가 된다. Alice가 전송하고자 하는 secret 메시지가 uniform 분포를 따른다고 하면, Alice와 도청자 Eve 사이의 전송되는 정보의 양 mutual information은 $I(M;Z) = H(M) - H(M|Z) = 1 - H(M|Z)$가 된다. $H(M|Z)$의 값은 Alice와 Eve 채널 사이의 equivocation rate R_e로 정의 될 수 있으며, 도청자가 얻게 되는 secret 메시지의 정도를 수량화 할 수 있다. Security 확보를 위해 equivocation rate R_e의 값을 최대로 하여 $I(M;Z) = 0$을 만족해야 한다. 따라서 $R_e = R_s$를 만족하게 되면 perfectly secrecy를 얻을 수 있다.

2. Information puncturing & Scrambling scheme

D.Klinc et.al. 는 [5]에서 LDPC 부호의 puncturing 기법을 이용하여 Gaussian wiretap 채널에서 security를 확보하는 punctured LDPC 부호를 제안하였다. Systematic LDPC 부호의 secret 메시지인 information part를 부호화한 후, information puncturing을 통해 나머지 parity part만을 채널을 통해 전송하여 secret 메시지가 채널로부터의 노출을 직접적으로 막는 방법이었다. 이때의 puncturing fraction p값이 실제적으로 secret information 비트의 fraction을 의미하고 있고, secret information 비트를 puncturing 시키기 때문에 $R_d = R_s$를 만족시키는 부호를 사용하게 된다. 이러한 이유로 mother code는 $R_c = p$인 부호를 사용해야 $R_d = R_s$를 만족시키는 부호를 생성할 수 있고, 전체 부호율 $R_c < 0.5$인 mother code를 사용해야 한다. 이러한 punctured 부호를 사용하게 되면 non-punctured 부호(systematic code)에 비해 security gap을 현저하게 줄일 수 있다는 것을 증명하였다. 하지만 결과적으로 punctured 부호는 non-punctured 부호에 비해 낮은 reliability 성능을 가지게 되므로 충분한 reliability를 얻기 위해 더 높은 power consumption을 요구하게 된다. 이러한 단점을 극복하기 위해 Scrambling 행렬을 이용하여 security를 확보하는 새로운 방법이 제시 되었다[9][10]. Scrambling 기법은 Alice의 secret 메시지를 먼저 scrambling 행렬과 곱해서 생성된 encrypted 메시지를 오류정정부호의 부호기를 통해 부호화 하여 전송하는 기법을 의미한다. 이 과정에서 systematic 부호는 non-systematic 부호의 구조 형태를 가지게 된다. 기존의 puncturing 기법과는 달리 code rate의 손실 없이 전송되기 때문에 $R_c = R_s$를 만족하게 된다. Scrambling 기법의 부호화 과정을 수식적으로 표현하면 다음과 같다.

$$x = m \cdot \ S \cdot \ G \tag{6}$$

$1 \times n$의 암호화된 부호어 X는 $1 \times s (= 1 \times k)$의 secret 메시지 벡터 m과 $k \times k$의 scrambling 행렬 S와의 곱을 통해 생성된 암호화 메시지에 $k \times n$ systematic 형태의 생성행렬 G를 곱한 형태로 생성된다. Puncturing 기법과 Scrambling 기법의 예시는 〈그림 2〉에 나타나 있다. Scrambling 행렬 S는 역행렬이 존재하는 non-singular 행렬이다. 수신한 메시지는 오

류정정부호의 decoding 과정을 통해 1차적으로 오류정정과정을 거친 후, inverse scrambling 행렬 S^{-1}와 곱을 통해서 최종 decrypted 메시지 $\hat{m}$을 구해낸다.

$$\hat{m} = (x+e)\cdot S^{-1} = x\cdot S^{-1} + e\cdot S^{-1} = m + e\cdot S^{-1} \quad (7)$$

오류정정부호의 복호 과정이 성공적으로 수행되었다면 secret 메시지를 복원하는 것이 가능하지만 복호 실패의 경우, 식 (7)의 $e\cdot S^{-1}$부분에 의해 오류벡터 e에서 1의 위치에 해당하는 S^{-1}의 column vector들의 합의 형태로 error propagation이 일어나게 된다. Perfect scrambler는 S^{-1}의 각각의 column degree(1의 분포도)가 0.5이기 때문에 한 개의 오류가 발생하여도 복원된 메시지는 0.5의 오류율로 오류가 발생하게 된다. 오류율 0.5는 수신 벡터의 entropy가 최대가 되는 값이기 때문에 Eve의 채널에서 오류가 발생하게 되면 Eve는 원래의 메시지를 복원해 낼 수 없게 된다. 따라서 perfect scrambler의 성능은 frame error와 밀접한 관련이 있다. 1개의 frame error가 발생하였을 때, perfect scrambler는 0.5의 bit error rate을 가지게 된다. perfect scrambler가 보안 전처리 기법으로 사용되면 오류정정부호와 변조기법이 적용된 채널부호군에서의 frame error 성능에 따라 bit error, 즉 security 성능이 결정된다. 이로 인해 scrambling 기법은 security를 확보할 수 있지만 high SNR 영역에서의 reliability는 conventional 오류정정부호에는 크게 못 미치게 된다. Low SNR 영역에서 수식 (2)의 security를 만족시키고, 수식 (1)에서의 충분한 reliability를 확보하기 위해서 더 낮은 SNR로 수식 (1)을 만족시키는 보안 전처리 기법이 필요하다.

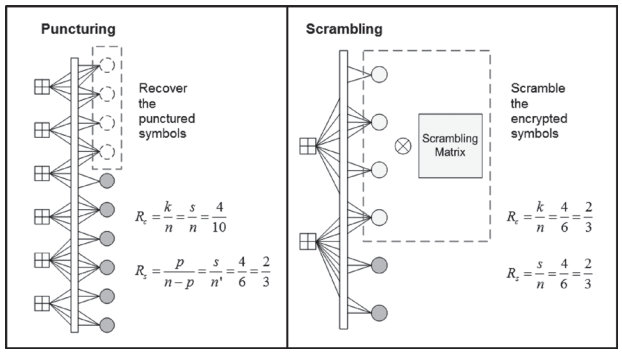

그림 2. information puncturing scheme과 Scrambling scheme에 대한 예시

Ⅲ. The Proposed Security Preprocessing Scheme for Physical Layer Security

1. Scrambling matrix considering minimum hamming distance

기존의 Scrambling 행렬의 생성은 $k\times k$의 non-singular 행렬을 각 column에 1의 분포를 최대화 시키는 방식으로 생성된다. 일반적으로 $k\times k$ 행렬을 full rank를 만족하면서 1의 분포를 최대로 늘려서 행렬을 생성하는 것은 쉬운 일이 아니다. 또한 오류가 생긴 수신 벡터와 연산할 때, 최대한 많은 오류를 발산시키려 한다면 inverse scambling 행렬의 row나 column에서의 1의 분포가 균등하면서 충분히 많아야 한다. 이러한 scrambling 행렬은 full rank를 가지는 random한 행렬로 생성되기 때문에 minimum distance를 고려하고 있지 않다. 1 비트의 단일 오류에 대해서 최대의 minimum distance를 가지는 scrambling 행렬을 설계한다면 high SNR 영역에서 최대의 security를 확보할 수 있게 된다. 발생되는 오류의 패턴이 random 오류임을 감안한다면 크기가 작은 여러 개의 scrambling 행렬을 이용하여 Low SNR 영역에서의 security 또한 확보가 가능하다.

제안된 기법의 원리는 〈그림 3〉과 같이 기존의 scrambling 행렬을 $k\times k$ 행렬로 구현하는 대신에 $k'\times k'$ 행렬 $(k'<k)$로 구성하여 이를 indentity matrix와 kronecker product를 통해서 생성한다. 즉, secret 메시지를 작은 sub-block으로 구성하여 각각의 sub-block을 제안한 scrambling 행렬을 통해 하나의 큰 block으로 구성하는 방식이다. 이때, 생성되는 scrambling 행렬은 크기가 작은 sub-block에 대한 행렬로 구성하게 된다. 이렇게 할 경우, low SNR 영역에서 생기는 다수의 오류들은 각 sub-block에 대해서 single 혹은 double 오류로만 표현을 할 수가 있게 된다. 각 sub-block에 single 오류가 발생하는 경우라 가정하면, 제안하는 scrambling 행렬을 단일 오류에 대해 가장 큰 minimum distance를 가지는 matrix로 mapping이 가능하다. 제안된 scrambling 행렬을 4×4 행렬로 가정하면 단일 오류에 대한 오류 벡터 e는 0001, 0010, 0100, 1000의 네 가지 경우로 발생할 수 있고, 이 네 가지 경우에 대해서 가장 큰 distance를 가지는 벡터를 mapping 시켜줌으로써 sub-block에 대해 error propagation을 최대로 해주는 scrambling 행렬을 생성 할 수 있다. sub-block을 4 bits로 구성하게 될 경우 가장 큰 distance를 가지는 mapping 방법은 〈표 1〉과 같다.

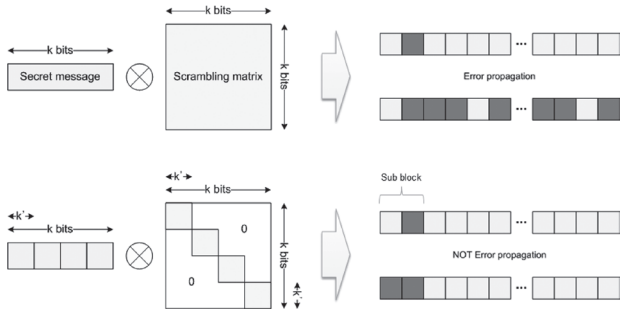

그림 3. Conventional Scrambling 기법과 Proposed Scrambling 기법

표 1. sub-block의 길이를 4 bits로 하였을 때, 최대의 distance를 가지는 mapping 기법

secret message				mapping 된 message			
0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	1
0	0	1	0	0	0	1	1
1	1	0	1	0	0	1	0
0	1	1	0	0	1	1	0
1	0	0	1	0	1	1	1
0	1	0	0	0	1	0	1
1	0	1	1	0	1	0	0
1	1	0	0	1	1	0	0
0	0	1	1	1	1	0	1
1	1	1	0	1	1	1	1
0	0	0	1	1	1	1	0
1	0	1	0	1	0	1	0
0	1	0	1	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	0	0	0

〈표 1〉의 mapping 기법을 바탕으로 sub-block에 대한 4×4 scrambling 행렬은 다음 수식 (8)로 표현이 가능하다.

$$S=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\\1&1&1&0\end{bmatrix},\qquad S^{-1}=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&1\end{bmatrix}\tag{8}$$

수식 (8)에서의 scrambling 행렬과 역행렬은 sub-block의 길이에 따라서 동일한 형태로 구성이 가능하게 된다. 각각의 sub-block은 모두 single 오류에 대해서 가장 큰 hamming distance를 가지게 되고 다수의 sub-block을 구성하게 될 경우, 수신 벡터에 존재하는 오류는 random 오류임을 가정하게 되면 각각의 sub-block 당 1개 혹은 2개의 오류를 포함하고 있게 되기 때문에 error propagation 현상이 두드러지게 나타나게 된다. 하지만 high SNR 영역에서 오류가 거의 존재하지 않게 되는 경우에도 수신된 프레임이 모두 오류가 발생하는 것을 막기 때문에 기존의 scrambling 기법에 비해서 error floor 현상을 줄일 수 있게 된다.

2. Rate-1 Feed-forward Code as the Security Preprocessing

Physical Layer Security를 달성하기 위해서는 오류정정부호의 rate loss 없이 security processing 과정이 필요하다. Secret 메시지와 encrypted 메시지는 동일한 dimension 상에서 존재하여야 하고, 그를 위해 encrypted 메시지가 부호율 1을 가지는 security processing을 통해 생성되어야 한다. 또한 security processing 과정은 오류정정부호 부호화 과정 이전에 추가되는 과정이므로 그 복잡도가 오류정정부호 부호화 보다 낮은 복잡도를 가져야지 security를 적용하는데 있어서 효율적인 방법이 된다. 기존의 scrambling 기법이 scrambling 행렬을 secret 메시지와 곱한 형태의 방식이었다면, 제안하는 부호는 1개의 register만을 사용하여 1개의 tail bit만을 가지는 convolutional encoding 방식을 사용한다. Convolutional 부호나 turbo 부호에서 사용하는 부호기의 경우 systematic 형태의 RSC(Recursive and Systematic Convolutional) 구조를 가지고 있다. RSC 구조를 이용하여 부호화를 하게 되면 n번째의 encoding symbol이 이전의 symbol들과 서로 correlation을 가지면서 encoding symbol을 생성하고 code의 minimum hamming distance를 증가 시킬 수 있게 되어 결과적으로 오류정정의 기능을 가지게 된다. 하지만 security processing을 하기 위해서는 오류정정의 기능이 아니라 error propagation 기능을 가지고 있어야지만 Eve의 채널 오류에 대해서 강력한 security 확보가 가능해진다. 따라서 본 논문에서는 security processing 부호로 Rate-1 Feed-forward 부호를 제안한다. 제안하는 Rate-1 Feed-forward 부호는 매우 낮은 복잡도를 지니고 있으면서 RSC 구조가 아닌 Feed-forward 구조를 채택하고 있다. 제안하는 부호의 생성 다항식은 $g(D)=1+D$로 부호기를 구성한다. Register는 1개를 사용하기 때문에 이 부호의 memory order $m=1$을 가진다. 다음 〈그림 4〉는 제안하는 Rate-1 Feed-forward 부호기의 블록도 이다.

n번째 secret 메시지 m_n이 입력으로 들어오게 되면 이전 비트인 m_{n-1}과 m_n은 modulo-2 연산을 통해서 출력 비트인 u_n을 생성한다. 1번째 secret 메시지 m_1에 대해서 register는 초기화 된 값인 0을 가지고 있으므로 비트의 입력 시퀀스의 수식

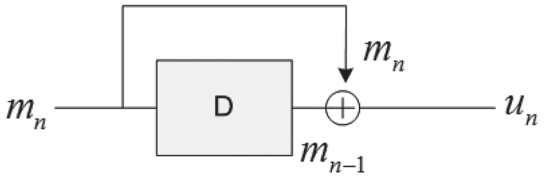

그림 4. Rate-1 Feed-forward code의 부호화기

은 다음과 같다.

$$\begin{aligned} u_1 &= m_1 \\ u_2 &= m_1 \oplus m_2 \\ u_3 &= m_2 \oplus m_3 \\ &\vdots \\ u_n &= m_{n-1} \oplus m_n \end{aligned} \tag{9}$$

앞서 언급한 Rate-1 Feed-forward 부호의 encrypted 메시지 $U=(u_1,u_2,\cdots,u_n)$는 생성 다항식 $g(D)=1+D$로 구성하고 있기 때문에 역함수는 $g^{-1}(D)=\frac{1}{1+D}$가 되고, 따라서 decrypted 메시지 $\hat{M}=(\hat{m_1},\hat{m_2},\cdots\hat{m_n})$의 복호기 구조는 〈그림 5〉와 같이 구성하게 된다.

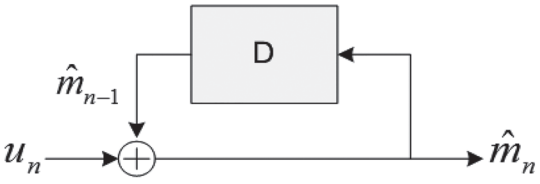

그림 5. Rate-1 Feed-forward code의 경판정 복호기

〈그림 5〉와 같이 복호기의 구조는 부호기의 feed-forward 구조와는 반대로 recursive 구조를 가지고 있다. 이러한 구조 때문에 decrypted 메시지 $\hat{M}=(\hat{m_1},\hat{m_2},\cdots,\hat{m_n})$은 다음과 같은 규칙성을 가진다.

$$\hat{m_n}=u_n\oplus\hat{m_{n-1}} \tag{10}$$

복호기의 recursive 구조는 이전의 비트에 오류가 발생하게 되면 발생된 오류가 복호기의 register에 계속적으로 누적 된다. 누적된 에러는 다음 비트에 대해서도 오류로 발생하게 되고, 그 후의 비트에 오류로써 영향을 계속적으로 끼치게 된다. 이러한 구조적인 특징으로 인하여 error propagation을 진행시키게 된다. 수식 (10)은 hard decision value를 이용하여 이전의 decrypted 메시지와 modulo 연산을 진행하는데 결과적으로 sequence detection 결과를 가지게 된다. Feed-forward 부호의 구조는 기본적으로 convolutional encoder를 사용하고 있기 때문에 이를 trellis diagram으로 표현이 가능한데, 〈그림 5〉에서는 hard decision value만을 이용해 forward recursion만을 사용하여 최종 decrypted 메시지를 구해내고 있다. 표현되는 trellis diagram은 SISO(Soft-in Soft-output) decoder 또는 symbol by symbol Maximum A Posteriori (MAP) algorithm 사용이 가능하다. Classical turbo decoding에 사용되는 대표적인 MAP algorithm으로 BCJR(Bahl, Cocke, Jelinek, Raviv) algorithm이 있다. BCJR algorithm[13]은 sequence detection에서의 forward recursion 뿐만 아니라, backward recursion과 각각의 state에서의 branch metric을 이용하여 decision 하기 때문에 각각의 symbol 에서 MAP decoding이 가능하다. 따라서 BCJR algorithm의 soft decision decoding을 사용하여 symbol detection 함으로써 hard decision decoding의 sequence detection에서 생기는 성능의 차이를 크게 줄일 수 있다.

결과적으로 Rate-1 feed-forward 부호는 한 개의 memory register만을 사용하고, 1개의 tail bit가 존재하기 때문에 2-state diagram으로 표현이 가능하다. 〈그림 6〉에서 Rate-1 feed-forward 복호기의 2-state diagram을 보여준다.

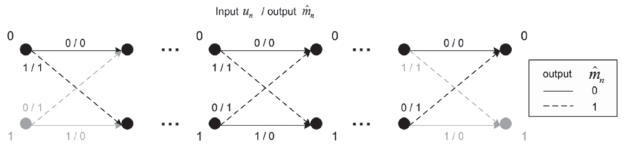

그림 6. 제안된 Rate-1 Feed-forward code의 2-state trellis diagram

〈그림 6〉에서 n번째 decrypted 메시지 $\hat{m_n}$이 0인 경우 solid line으로, 1인 경우 dotted line으로 표현이 가능하다. 수신된 encrypted 메시지 u_n은 이전 state (0 또는 1)에 따라서 decrypted 메시지 $\hat{m_n}$을 복호한다. 제안된 feed-forward 부호는 한 개의 비트를 복호 할 때, 이전과 이후의 모든 비트와 correlation을 가지고 soft decision decoding을 수행하기 때문에 hard decision decoding에 비해서 coding gain이 발생할 수 있다. 아래 그림에서 보안 전처리 과정을 통하여 메시지를 암호화 하였을 경우에 생기는 coding gain에 대해서 살펴보고자 한다. 아래 〈그림 7〉은 E_b/N_0에 대한 Uncoded 상황에서의 BPSK 변조 성능과 보안 전처리 과정을 수행한 시스템의 비트 오류율을 나타내고 있다. information 비트의 길이는 1024 비트이다.

그림에서 볼 수 있듯이 Uncoded BPSK의 BER 10^{-5}영역에서의 성능에 해당하는 E_b/N_0 값은 약 9.5dB이다. Perfect Scrambling을 적용한 시스템의 경우 BER 10^{-5}영역에서의 성능이 약 11.6dB로써 Uncoded BPSK에 비해 약 2.1dB 가량의 성능 열화가 생긴다. 하지만 제안하는 Sub block Scrambler의 경우, Perfect Scrambling 에 비해서 더 낮은 E_b/N_0 값을 통해서 BER 10^{-5}을 달성할 수 있다. 또한 제안하는 Rate-1 Feed-forward 부호의 경우는 low SNR 영역에서 BER이 0.5에 이르는 값을 가지지만 high SNR 영역으로 갈수록 Uncoded BPSK의 성능에 근접하게 된다. BER 10^{-5}에서의 E_b/N_0 값은 Uncoded BPSK 보다 약 0.5dB 가량 열화된 약 10dB의 값을 가진다. Rate-1 Feed-forward 부호의 경우 BCJR 복호기를

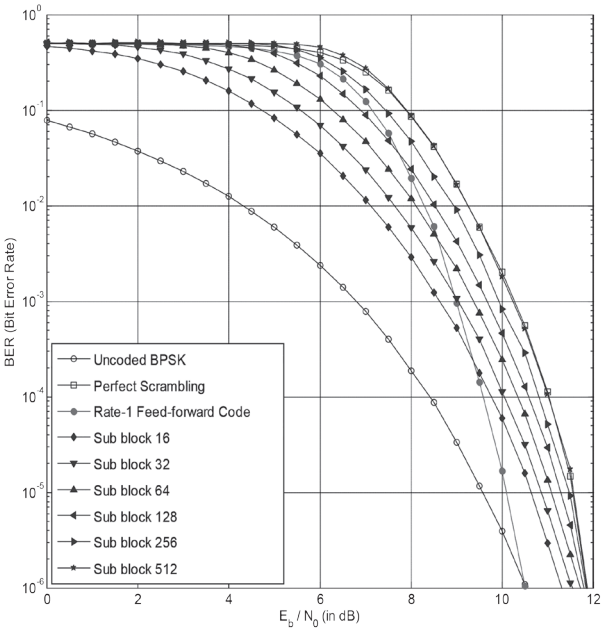

그림 7. Uncoded 시스템에서 BPSK 변조, Perfect Scrambling, 제안된 Sub block Scrambler 및 Rate-1 Feed-forward 부호의 오류 성능 곡선 (Sub block의 길이는 16, 32, 64, 128, 256, 512 bits로 각각 제한하였음)

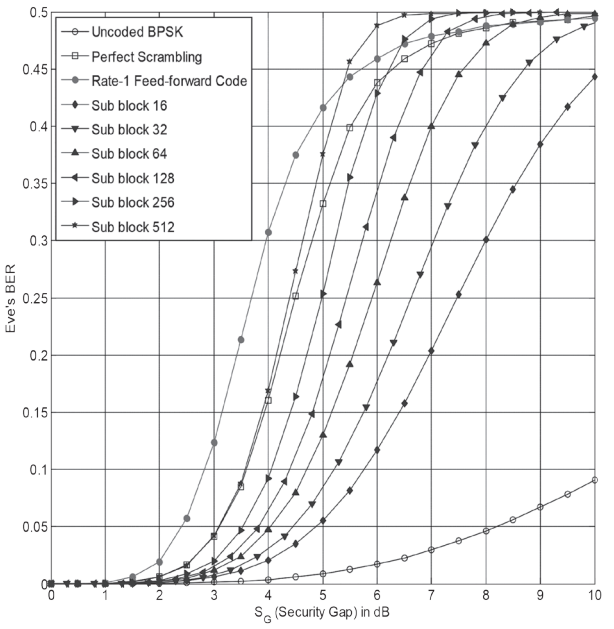

그림 8. Uncoded 시스템에서 BPSK 변조, Perfect Scrambling, 제안된 Sub block Scrambler 및 Rate-1 Feed-forward 부호의 Security Gap 성능 곡선 (Sub block의 길이는 16, 32, 64, 128, 256, 512 bits로 각각 제한하였음)

통해 soft decision decoding을 하기 때문에 high SNR에서 생기는 소수의 오류에 대해서 오류 정정이 가능하게 되고 그로 인해 성능 이득이 생긴다..

앞서 설명했듯이, 수식 (1)과 (2)의 reliability와 security를 만족하는 성능을 측정하기 위해서 Security Gap의 개념을 소개 하였다. Security Gap은 수식 (1)의 reliability를 만족하는 BER 0.5에 해당하는 SNR 값과 수식 (2)의 security를 만족하는 BER 10^{-5}의 SNR 값의 차이로 식 (4)에서 정의되었다. 따라서 〈그림 7〉에서의 BER 성능 곡선을 바탕으로 Securtiy Gap 측면에서 reliability와 security 성능을 〈그림 8〉을 통해 살펴보고자 한다.

충분한 security를 확보하기 위한 Eve의 비트 오류율 $P_e^{Eve} > 0.4$을 기준으로 삼는다면, 〈그림 8〉에서처럼 Uncoded BPSK 시스템이 충분한 security를 확보하기 위해서 20dB이상의 security gap이 필요하다. 하지만 기존의 Perfect Scrambling 기법의 경우 5.5dB의 security gap 만으로 충분한 security 확보가 가능해진다. Perfect Scrambling은 reliability 관점에서 Uncoded BPSK와의 reliability 성능 차이가 약 2.1dB 가량 났지만 error propagation 현상으로 인해 low SNR에서 충분한 security를 확보할 수 있는 $P_e^{Eve} \approx 0.5$에 근접하므로 security gap 측면에서 성능이득을 얻을 수 있다. Eve의 비트 오류율 P_e^{Eve}을 0.4 기준으로 살펴보면, Perfect Scrambling에 비해 제안하는 Sub block Scrambler는 Sub block size 512일 때 약 0.4dB의 security gap 이득이 발생하고, Rate-1 Feed-forward 부호의 경우 약 0.8dB의 security gap 이득이 발생한다. 이는 Perfect Scrambling의 경우 security를 확보하기 위해서는 Eve의 채널에서의 수신 SNR이 Bob의 채널에서의 수신 SNR보다 5.5dB 가량 감쇄된 채널이어야 보안을 확보할 수 있게 되지만 Rate-1 Feed-forward 부호를 적용한 경우 Eve의 수신 SNR이 Bob의 수신 SNR에 비해 약 4.7dB 가량만 감쇄된 채널이더라도 충분한 보안을 확보할 수 있게 된다는 것이다.

Eve의 비트 오류율 P_e^{Eve}가 0.5에 근접할 때 완벽 보안이 가능한 이유는 Eve가 도청한 시퀀스 Z로부터 최대한 많은 정보를 추출할 수 없게 되기 때문이다. 이는 앞서 설명한 Eve의 Equivocation Rate Δ가 채널의 비트 오류율에 관련된 식으로 정의되고, Eve가 최종 복호한 시퀀스에 대한 Entropy의 값으로 표현이 가능하기 때문이다. 즉, Eve가 최종 복호한 시퀀스의 Entropy 값이 1에 근접할수록 Eve는 원래의 메시지를 복원해 내기 어렵게 된다. 따라서 〈그림 8〉의 security gap 성능은 다음 그림 9와 같이 Eve의 Equivocation Rate에 대한 성능 곡선으로 표현함으로써 Eve가 수신하여 복호한 시퀀스의 Entropy에 관한 지표로 확인이 가능하다. 그림에서 볼 수 있듯이 기존의 Perfect Scrambling 기법은 Eve가 충분히 원래의 메시지를 복원해 낼 수 없는 Entropy의 값 (=Equivocation rate) $\Delta = \frac{1}{n} H(M|M_E) > 0.9$ 인 지점에서 Security gap이 5dB

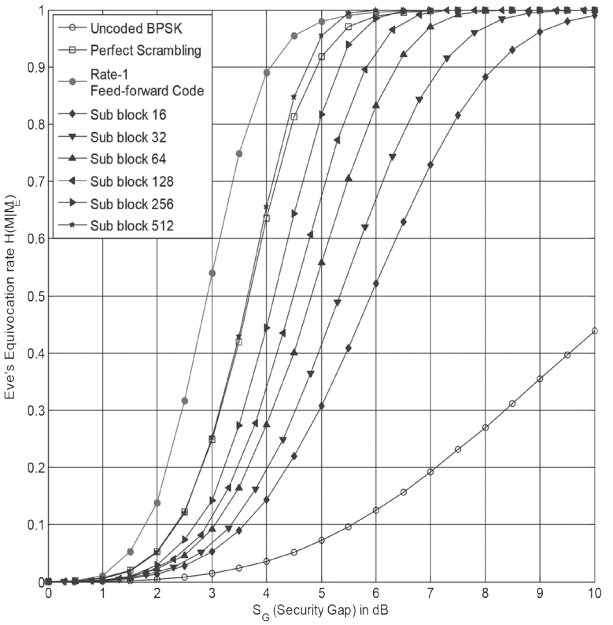

그림 9. Uncoded 시스템에서 BPSK 변조, Perfect Scrambling, 제안된 Sub block Scrambler 및 Rate-1 Feed-forward 부호의 Security Gap에 따른 Equivocation Rate (Sub block의 길이는 16, 32, 64, 128, 256, 512 bits로 각각 제한하였음)

인 반면에 제안하는 Rate-1 Feed-forward 부호가 적용된 기법은 Security gap 약 4dB의 값을 가지고 있다. 즉, Eve의 수신 시퀀스에 대한 Entropy 측면에서도 제안된 Rate-1 Feed-forward 부호가 기존의 Perfect Scrambling 기법에 비해 1dB 가량의 Security gap 성능 이득이 있다.

Ⅳ. Numerical Results

오류정정부호는 채널의 수신 오류율 P_e를 낮추면서 채널의 reliability를 높이기 위해 사용된다. 전송하고자 하는 information 비트 이외에 잔여의 parity 비트를 같이 전송하여 information 비트에 포함된 오류 비트를 parity 비트를 통해 원래의 메시지로 복원해 낸다. 그 효과로 인해 기존의 uncoded 시스템보다 더 높은 채널 reliability를 가지게 된다. 따라서 기존의 오류정정부호와 제안하는 Security Preprocessing과의 직렬 연접 시스템을 통해 채널 Reliability를 충분히 확보하면서 Security도 확보할 수 있는 시스템의 성능을 살펴보고자 한다. 다음 〈그림 10〉은 보안 전처리 기법이 적용된 전송 시스템의 구성 블록도 이다.

송신자 Alice는 보내고자 하는 secret 메시지 M을 먼저 보안 전처리 기법을 통해 암호화 한 후, 오류정정부호의 부호기를 이

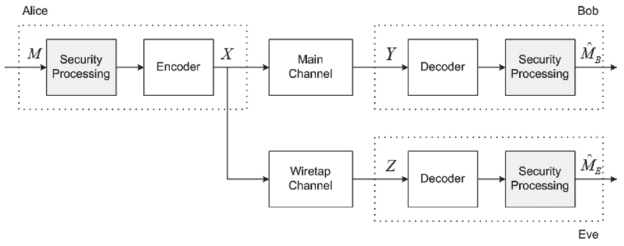

그림 10. Gaussian Wiretap 채널 상에서 보안 전처리 기법이 적용된 오류정정부호 시스템의 블록도

용하여 부호어를 생성한다. 생성된 부호어는 Bob과 Eve에게 각각의 Main 채널과 Wiretap 채널을 통해 전송되고, Bob과 Eve는 수신 시퀀스 Y와 Z를 이용하여 오류정정부호의 복호를 수행한다. 오류정정부호의 복호 과정을 거친 부호어는 각각의 보안 전처리 기법의 복호화 과정을 통해서 최종 secret 메시지를 복원해 낸다. 모의 실험에 사용된 변조 방법으로는 BPSK를 사용하였고, 오류정정부호는 부호율 0.5, information 길이 1024비트의 Convolutional 부호를 사용하였다. 오류정정부호의 복호 기법으로는 BCJR 알고리즘을 사용하였다. 아래 〈그림 11〉은 사용된 Convolutional 부호의 부호화기의 구조를 나타낸다.

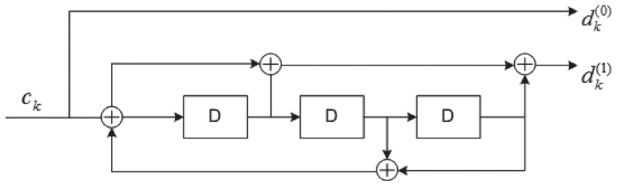

그림 11. 부호율 0.5의 Convolutional 부호의 부호화기 구조

Scrambling 기법은 오류정정부호의 복호를 마친 hard decision 값을 descrambling 행렬과 곱하여 최종 secret 메시지를 추출하고, 제안하는 Rate-1 Feed-forward 부호는 오류정정부호의 복호를 수행하여 얻은 soft decision 값을 Rate-1 Feed-forward 부호의 BCJR 복호기를 통해 최종 secret 메시지를 복원하므로 복잡도에 있어서 차이가 있을 수 있지만 부호율은 동일한 부호율을 가지고 있다. 〈그림 12〉는 제안된 연접 시스템의 채널 reliability에 관한 성능을 BER 측면에서 관측한 결과이다.

제안된 Rate-1 Feed-forward 부호와 Scrambling 기법이 적용된 coded 시스템에서도 low SNR 영역에서 error propagation 현상이 발생하는 것을 관찰할 수 있다. 하지만 Scrambling 기법의 경우, 오류정정부호의 복호 후 잔여오류가 descrambling 행렬의 column degree에 따라서 error propagation 현상이 발생하기 때문에 reliability 성능이 일정한 간격을 유지하게 된다. 하지만 Rate-1 Feed-forward 부호

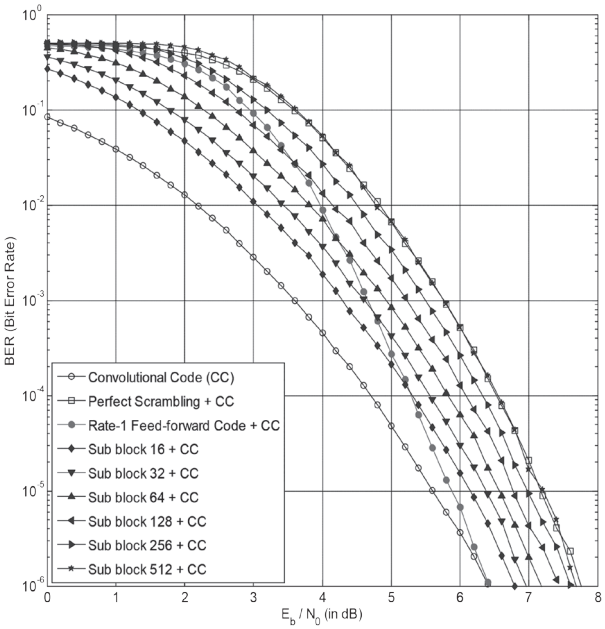

그림 12. Convolutional coded 시스템에서 BPSK 변조, Perfect Scrambling, 제안된 Sub block Scrambler 및 Rate-1 Feed-forward 부호의 오류 성능 곡선 (Sub block의 길이는 16, 32, 64, 128, 256, 512 bits로 각각 제한하였음)

의 경우 BCJR 알고리즘을 수행하기 때문에 오류정정부호로 인한 coding gain 이외에 보안 전처리 과정으로 인한 성능 이득이 발생한다. 이러한 reliability에 대한 성능 이득은 다음 〈그림 13〉과 〈그림 14〉를 통해서 security 성능에도 크게 영향을 미치

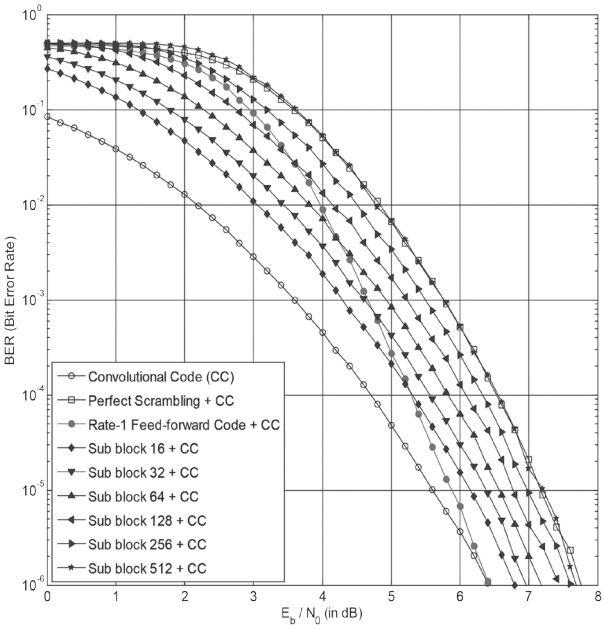

그림 13. Convolutional coded 시스템에서 BPSK 변조, Perfect Scrambling, 제안된 Sub block Scrambler 및 Rate-1 Feed-forward 부호의 Security Gap 성능 곡선 (Sub block의 길이는 16, 32, 64, 128, 256, 512 bits로 각각 제한하였음)

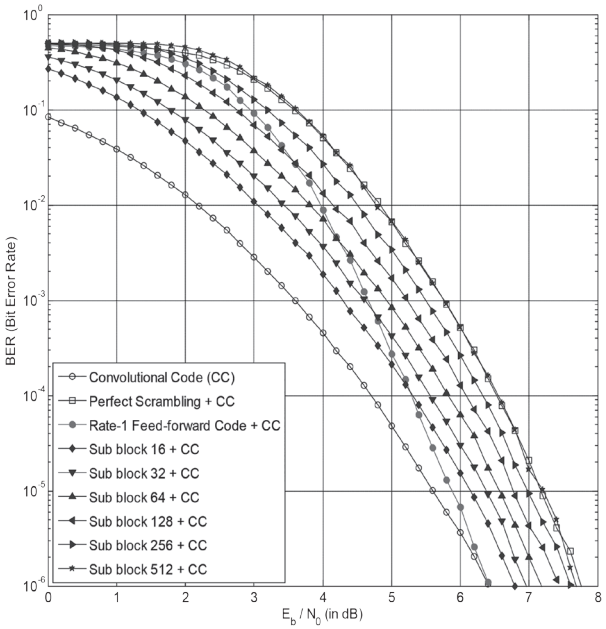

그림 14. Convolutional coded 시스템에서 BPSK 변조, Perfect Scrambling, 제안된 Sub block Scrambler 및 Rate-1 Feed-forward 부호의 Security Gap에 따른 Equivocation Rate (Sub block의 길이는 16, 32, 64, 128, 256, 512 bits로 각각 제한하였음)

는 것을 알 수 있다.

〈그림 13〉과 〈그림 14〉는 〈그림 12〉를 바탕으로 security gap 관점과 equivocation rate 관점에서 비교 분석한 그래프이다. 〈그림 13〉에서 보듯이 Eve의 비트 오류율 P_e^{Eve}가 0.4인 지점에서의 security gap은 Perfect Scrambling을 적용하였을 때 약 5.2dB이다. 제안한 Sub block Scrambler는 Sub block의 길이가 256일 때 Perfect Scrambling과 비슷한 Security gap을 가지고, Sub block 길이가 512일 때 약 4.9dB로 0.3dB 가량의 Security gap 성능 이득이 생긴다. 또한 Rate-1 Feed-forward 부호를 적용한 시스템의 경우, Security gap이 약 4.5dB인 지점에서 P_e^{Eve}가 0.4의 값을 가지기 때문에 기존의 Perfect Scrambling 기법에 비해 0.7dB 가량의 security gap 성능 이득이 생긴다. 그림 14에서처럼 Equivocation Rate 관점에서 살펴보아도 제안한 Rate-1 Feed-forward 부호가 적용된 시스템이 기존의 Perfect Scrambling 기법이나 Sub block Scrambler 기법에 비해서도 큰 성능 이득을 가지는 것을 확인할 수 있다.

Uncoded 시스템과 Coded 시스템의 성능 비교를 통해 알 수 있는 것은 강력한 오류정정부호를 사용한다면 security gap을 더 줄일 수 있다는 사실이다. 오류정정 능력이 강한 부호일수록 성능의 water fall 현상이 강하게 나타나고 BER 성능의 slope에 따라서 reliability 성능이 결정된다. 또한 error propagation 현상을 더욱 심화시키는 보안 전처리 기법을 사용

함에 따라 security 확보가 더 용이해진다. 또한 보안 전처리 기법은 오류정정부호의 복호 복잡도에 비해 현저히 낮은 복잡도를 가지고 있다. 비록 Scrambling 기법이 hard decision 값을 통한 행렬연산임에 비해 Rate-1 feed-forward 부호가 BCJR 복호 알고리즘을 사용하기 때문에 보안 전처리 기법만의 복잡도 측면에서는 제안된 부호가 더 복잡도 높지만 오류정정부호와 결합된 시스템에서는 그 차이가 미미하게 나타나게 된다.

V. 결 론

본 논문에서는 물리계층에서 보안성을 확보하기 위해 보안 전처리 기법으로 사용될 수 있는 부호의 설계 방법에 대해 다루어 보았다. 물리계층 보안을 위한 오류정정부호 연구는 LDPC 부호의 puncturing 기법을 이용하는 방식으로 연구가 진행되었으나 선형 블록 부호에만 적용이 가능하다는 제한적인 단점이 있었다. 그리하여 Scrambling 기법이 적용된 보안 오류정정부호 연구를 통해 여러 종류의 오류정정부호와 연접이 가능하게 되었다. 하지만 Scrambling 기법은 오류정정부호의 성능에 의존적이어서 오류정정부호에 따라 오류마루 현상이 심해지는 단점이 있다. Scrambling 기법을 바탕으로 오류마루 현상을 완화시키는 Sub block Scrambler의 설계 방법을 제안하였고, 나아가 reliability 성능과 security 성능을 향상시킨 Rate-1 Feed-forward 부호의 설계 방법을 제안하였다.

제안한 Rate-1 Feed-forward 부호는 BER 관점으로 볼 때, high SNR 영역에서 충분한 reliability 성능을 가지고 있고 보안 전처리 기법이 적용되지 않은 경우와 유사한 성능으로 수렴한다. 또한 low SNR 영역에서 충분한 error propagation 현상을 만족시키기 때문에 security 성능에서도 기존의 Scrambling 기법에 뒤지지 않는 security 성능을 가진다. Coded 시스템의 경우 reliability 성능($P_e \approx 10^{-5}$)은 Scrambling 기법이 약 7.2dB인 반면 Rate-1 feed-forward 부호 기법이 약 5.9dB로써 약 1.3dB의 reliability 성능 이득을 가진다. Security 성능($P_e^{Eve} = 0.4$) 또한 security gap을 기준으로 scrambling 기법이 약 5.2dB의 security gap을 가지지만 Rate-1 Feed-forward 부호 기법이 약 4.5dB의 security gap을 가지기 때문에 약 0.7dB 가량의 security gap 이득을 가지고 있음을 확인하였다. Wiretap 채널 기반의 물리계층 보안 연구가 Main 채널에 비해 감쇄된 도청 채널을 가정하고 있기 때문에, 채널 상태가 더 우수한 도청 채널에 대한 물리계층 보안 연구가 진행된다면 Eve의 채널 상태에 관계없이 보안 전송 용량 증대가 가능하게 될 것이다.

Acknowledgement

This research was supported by DMC R&D Center in Samsung Electronics Co., Ltd.

참 고 문 헌

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656-715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Trans. Inf. Theory, vol. IT-24, no. 4, pp. 451-456, Jul. 1978.

[4] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," Jep Propulsion Lab, 1978, pp. 114-116, DSN Progress Report 44

[5] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 532-540, Sep, 2011.

[6] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for physical layer security," in Proc. IEEE Global Telecommunications Conf. (GLOBECOM 2009), Honolulu, HI, Nov. 2009.

[7] C. W. Wong, T. F. Wong, and J. M. Shea, "LDPC code design for the BPSK-constrained Gaussian wiretap channel," in Proc. IEEE GLOBECOM Workshops 2011, Houston, TX, Dec. 2011.

[8] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 551-564, Sep. 2011.

[9] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in Proc. IEEE Information Theory Workshop (ITW 2010), Dublin, Ireland, Aug. 2010.

[10] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with Scrambling, Concatenation, and HARQ for the

AWGN Wire-Tap Channel: A Security Gap Analysis," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp.883-894, Jun, 2012.

[11] 3GPP, "3GPP TS 36.212 v8.7.0 3rd generation partnership project; technical specification group radio access network; evolved universal terrestrial radio access; multiplexing and channel coding (release 8)," 3rd Generation Partnership Project, Tech. Rep., May. 2009.

[12] Shu Lin, and Danial J. Costello, "Error Control Coding: Fundamentals and Applications," 2nd Ed. Pearson Prentice Hall., 2004

[13] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," IEEE Trans. Inf. Theory, vol. IT-20, pp. 284-287, Mar. 1974.

약 력

권 경 훈

2010년 세종대학교 전자전기컴퓨터공학과 학사
2012년 고려대학교 전기전자전파공학부 석사
2012년~현재 고려대학교 전기전자전파공학부 박사과정 재학
관심분야: Channel Coding (LDPC code, Turbo code)

허 준

1989년 서울대학교 전자공학과 학사
1991년 서울대학교 전자공학과 석사
2002년 University of Southern California 박사
1991년~1996년 LG전자 영상미디어 연구소, 주임연구원
1996년~2002년 LG전자 중앙연구소, 선임연구원
2000년~2001년 Trellisware Technologies Inc., Member of technical staff
2002년~2003년 Hynix 반도체 System IC Comp. 책임연구원
2003년~2007년 건국대학교 전자공학부 조교수
2007년~2012년 고려대학교 전기전자전파공학부 부교수
2012년~현재 고려대학교 전기전자전파공학부 정교수
관심분야: Channel Coding, Network Coding, Cooperative communication, Quantum Information Theory