차세대 무선 네트워크를 위한 물리계층 보안 기술


임상훈
한국과학기술원 전기 및 전자공학부


윤상석
한국과학기술원 전기 및 전자공학부


박정욱
한국과학기술원 전기 및 전자공학부

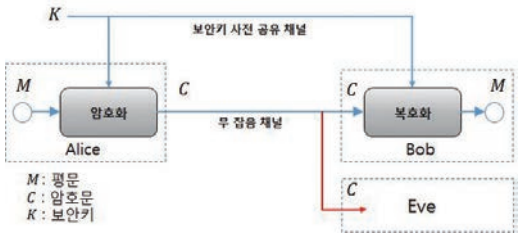

하정석
한국과학기술원 전기 및 전자공학부

Ⅰ. 서 론

최근 스마트폰을 비롯한 모바일기기들의 폭발적인 보급에 따라 금융, 전자상거래와 같은 다양한 형태의 모바일 서비스들이 개발되어 폭넓게 활용되고 있다. 모바일 기반 서비스가 다양해짐에 따라 무선 통신을 통한 민감한 개인 정보와 금융정보의 전송 또한 빈번히 이루어지고 있다. 하지만 무선 채널을 통한 정보 전송은 무선 채널의 개방적인 특성 때문에 도청에 취약할 수밖에 없으며, 이를 악용한 보안 사고사례가 사회 문제로 대두되고 있다. 이에 따라 무선통신 환경에서 보안 강화를 위한 연구가 학계 및 산업계에서 활발히 이뤄지고 있다.

양자 역학의 원리를 이용하여 초고속 연산이 가능한 양자컴퓨터가 상용화 된다면, 연산 복잡도기반의 보안시스템은 도청에 취약해질 수 있다.

현재 무선 네트워크에서 널리 활용되고 있는 보안 기술로는 전통적인 암호학 기반의 보안 기술이 표준적으로 이용되고 있다. 〈그림 1〉은 대칭키 기반 암호시스템의 동작과정을 나타낸다. 기밀메시지 M을 암호화하여 암호문 C를 송신하기 위해서는 적법한 송·수신자 Alice와 Bob이 사전에 보안키 K를 공유하고 있어야하며, 암호화/복호화를 위한 보안알고리즘이 필요하다.



〈그림 1〉 대칭키 기반 암호 시스템

전통적인 암호학기반의 정보보호 기술은 많은 장점을 가지고 있음에도 불구하고 다음과 같은 한계점을 가진다. 첫째, 도청자가 암호문 C를 해독할 수 있는 효율적인 알고리즘이 알려져 있지 않거나, 현존하는 연산 능력으로 암호화된 정보를 유의미한 시간 이내에 해독 불가능하다는 전제로 보안을 제공한다. 따라서 연산 능력을 비약적으로 향상 시킬 수 있는 양자 컴퓨터[1]가 개발된다면 기존 연산복잡도 기반의 보안 기술은 무용지물이 될 수 있기 때문에, 도청자의 연산능력과 무관하게 완벽 보안[2]을 제공할 수 있는 대안 기술이 필요하다. 둘째, 보안 통신을 위해서는 보안키 분배를 위한 신뢰된 제 3의 기관 또는 기반 시설이 요구된다. 잘 알려진 비대칭키 기반의 보안 기술인 RSA를 이용하면 사전키 분배과정 없이도 공개키를 이용한 보안키 전송이 가능하다. 그러나 Shor는 양자 컴퓨터에서 양자 알고리즘을 이용하여 공개키로부터 보안키를 알아내는데 걸리는 시간이 보안키 길이에 선형적으로 증가하는 결과를 보였다[1]. 이는 기존 연산 기술로 암호문을 해독할시 보안키의 길이에 대해 지수적으로 해독 시간이 증가하던 결과와 크게 대비되는 결과이다.

도청 채널 부호를 이용하면 채널의 물리적인 특성을 활용하여 사전 보안키 공유 없이도 도청자의 연산 능력과 무관하게 완벽보안을 유지하는 보안 전송이 가능하다.

1949년 Shannon은 도청자의 연산 능력과 무관하게 도청자가 기밀메시지에 대해서 전혀 알 수 없도록 하는 완벽 보안 시스템을 제안하였다[2]. 완벽 보안은 기밀 메시지 M과 암호문 C간에 다음의 관계가 만족하는 것을 의미한다.

$$I(M;C)=0 \text{ 또는 } H(M|C)=H(M)$$

하지만 Shannon의 연구 결과에 따르면, 완벽 보안을 보장하기 위해서는 사전에 공유해야하는 보안키의 길이 $H(K)$와 기밀메시지의 길이 $H(M)$의 관계가 다음의 필요조건을 만족해야한다는 결론을 얻었다.

$$H(K) \geq H(M)$$

즉, 보내야하는 기밀메시지 길이보다 더 길거나 같은 길이의 보안키가 존재해야만 완벽보안을 보장할 수 있다는 것을 의미한다. 따라서 기밀 메시지를 송신할 때마다 기밀 메시지와 같은 길이의 일회성 보안키를 사전에 공유하는 보안 전송 기법만이 연산복잡도와 무관하게 안전한 보안 전송기법으로 알려져 있었다.

한편, Wyner는 1975년 채널의 물리적인 특성을 이용하여 사전에 보안키를 공유하지 않으면서도 도청자의 연산 능력과 무관하게 보안 전송이 가능한 도청 채널 부호에 대한 연구를 제안하였다[3]. 적법한 송수신자가 이루는 주 채널과 적법한 송신자와 도청자가 이루는 도청 채널의 채널 용량 (channel capacity)을 각각 C_M과 C_W라 할 때 두 채널이 대칭적 채널이라면, 완벽 보안을 유지하면서 보낼 수 있는 최대 보안 전송 효율인 보안 용량 (secrecy capacity) C_S는 다음과 같이 표현된다[4].

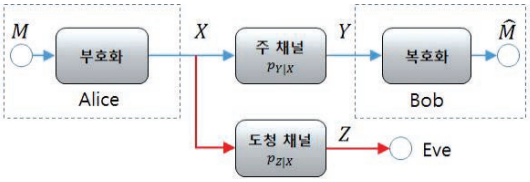
$$C_s=\max(C_M-C_W,0) = [C_M-C_W]^+,$$

여기서 양의 보안 용량을 획득하기 위해서는 주 채널의 채널 용량이 도청 채널의 채널 용량보다 더 큰 값을 가져야 한다. 따라서 일반적인 무선 채널 환경에서 보안 용량 확보를 위한 다양한 후속 연구가 활발하게 이루어져왔다.

보안 용량을 증대시키기 위한 연구로 다중안테나의 빔성형을 이용하여 정보전송 효율을 극대화 시키는 최적 빔성형 벡터설계 기술 및 이때 달성 가능한 보안 용량에 대한 연구가 수행되었다[5]. 또한 다중안테나 환경에서 주 채널에 직교하는 방향으로 의사 잡음을 송신하여 도청 채널의 수신 신호 대 잡음 비 (signal-to-noise ratio, SNR)를 낮추어 보안 용량을 증대시키는 연구가 수행되었다[6-9]. 한편 신뢰할 수 있는 중계국이 있는 환경에서 협력 중계 방식을 통해서 보안 용량을 증대시키는 연구가 활발히 수행되었다[10]. 이때 중계국은 적법한 송신자의 기밀메시지 전송을 중계함으로써 적법한 수신자의 SNR을

1) 양자 역학의 원리를 이용하여 연산을 수행하는 컴퓨터로 초고속 연산 수행이 가능한 컴퓨터이다.

2) 도청자의 연산 능력과 무관하게 도청자가 도청한 암호문 C로부터 기밀메시지 M에 대해서 전혀 알 수 없는 상태의 보안 수준을 의미. ($I(M;C)=0$) 여기서 $I(M;C)$는 랜덤변수 M과 C사이의 상호 정보량 (mutual information)을 의미한다.



〈그림 2〉 도청 채널 모델

증대시키거나, 의사 잡음을 발생시키는 보안 전송 기법이 연구되었다. 최근 인지 무선 환경에서 부 사용자가 주 사용자의 보안 전송을 도움으로써 보안 전송 용량을 증가시키는 연구가 수행되었다[11,12]. 인지 무선 환경에서는 부 사용자가 주 사용자의 메시지 중계 역할과 부 사용자 메시지의 송신 역할을 동시에 수행한다는 점에서 협력 중계 방식과는 큰 차이점이 있다.

본고의 구성은 다음과 같다. 2장에서는 물리계층 보안 전송기술에 대한 배경지식을 소개한다. 다음으로 의사 잡음 (artificial noise, AN)을 이용하여 보안 용량을 증대시키는 연구에 대해서 3장에서 살펴본다. 4장에서는 인지 무선 (cognitive radio) 통신 환경에서 부 사용자가 주 사용자의 주파수 대역을 사용하는 대가로 주사용자의 기밀 메시지를 중계하여 보안 통신을 돕는 전송 방식에 대해서 소개하겠다.

Ⅱ. 물리계층 보안 전송 기술

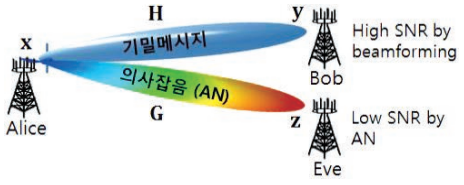
채널이라는 물리계층 자원을 이용하여 보안키 없이 완벽 보안을 제공하는 도청 채널 부호 설계에 관한 연구는 1975년 Wyner가 제안한 도청 채널 모델에 그 이론적 기반을 두고 있다[3]. 도청 채널 모델은 〈그림 2〉와 같이 기밀메시지 M을 전송하는 송신자 Alice, 이를 주 채널을 통해 수신하는 적법한 수신자 Bob, 그리고 도청 채널을 통해서 감청을 시도하는 도청자 Eve로 이루어진 채널 모델을 말한다. 이와 같은 채널 모델에서 Alice는 도청 채널부호를 이용하여 길이 k의 메시지 M을 길이 n의 부호어 X로 부호화하고, 이를 주 채널을 통해 Bob에게 전송한다. 적법한 수신자 Bob은 채널의 출력 Y로부터 기밀메시지 $\hat{M}$을 복호한다. 반면 Eve는 Alice의 송신신호 X를 도청 채널을 통해 감청하여 Z를 수신한다.

송신자가 기밀 메시지 M을 X로 부호화할 때는 다음의 두 가지 조건이 만족되어야한다.

1. 신뢰성: $\Pr(\hat{M}\neq M) \rightarrow 0$
2. 보안성: $I(M;Z)/k \rightarrow 0$또는 $H(M|Z)/k \rightarrow 1$

여기서 신뢰성 조건은 일반적인 채널 부호 설계 조건과 동일하게 주 채널을 통해서 전송된 기밀 메시지를 적법한 수신자가 임의의 낮은 오류 확률로 수신할 수 있어야함을 의미한다. 또한 보안성 조건은 Eve가 도청 채널을 통해 수신한 수신 신호 Z를 통해서 기밀 메시지 M에 대해 어떠한 정보도 알 수 없도록 보장해야함을 의미한다. 위 두 가지 조건을 만족하면서 송신자가 적법한 수신자에게 전송할 수 있는 정보 전송률을 보안 전송률 (secrecy rate) R_s로 정의하고, 달성 가능한 보안 전송률 중 최댓값을 보안 용량 (secrecy capacity)으로 정의하며 C_s로 표기한다. 특히 주 채널과 도청 채널이 각각 대칭적일 경우 보안 용량은 주 채널의 채널 용량 (channel capacity) C_M과 도청 채널의 채널 용량 C_W의 차이 ($C_s=[C_M-C_W]^+$)로 표현된다[4]. 따라서 주 채널의 채널 용량이 도청 채널의 채널 용량보다 더 높을 때에만 양의 보안 용량을 달성 가능하다는 한계점을 갖는다.

이러한 도청 채널 모델은 페이딩 채널 모델로 연구가 확장되었으며, 준정적 페이딩 (quasi-static fading) 환경에서 도청 채널의 통계적인 특성을 적법한 송신자가 알 때, 순시 채널의 보안 용량이 통신 시스템이 목표로 하는 보안 전송률 R_t보다 낮아 보안성 요구조건을 만족 못할 확률인 정전 확률 ($\Pr(C_s<R_t)$)에 대한 분석이 수행되었다[13,14]. 이후 엘가딕 페이딩 (ergodic fading) 채널에서 도청 채널의 통계적인 특성이 알려져 있을 때 달성 가능한 보안 용량에 대한 분석이 이루어졌다[15-17]. 또한 도청 채



〈그림 3〉 의사 잡음을 이용한 기밀메시지 송수신 시스템 모델

널부호에 대한 연구는 적법한 송·수신자와 도청자가 다중 안테나를 갖는 환경으로 확장되었으며 달성 가능한 보안 용량을 페이딩 채널에 대해 평균한 달성 가능한 평균 보안 용량 (achievable average secrecy capacity)가 보안 성능을 나타내는 지표로 널리 사용되기 시작했다[6].

Ⅲ. 의사 잡음을 이용한 물리계층 보안 전송 기술

무선 채널의 통계적인 특성에 의존하지 않고 의사 잡음 (artificial noise, AN)을 이용하여 보안 용량을 증가시키는 보안 전송 기법에 관한 연구는 2008년 Goel과 Negi에 의해 처음으로 제안되었다[6]. 〈그림 3〉은 다중 안테나 환경에서 의사 잡음을 이용한 보안 전송 기술에 대한 시스템 모델이다. 적법한 송신자 Alice, 적법한 수신자 Bob, 도청자 Eve는 각각 N_a, N_b, N_e개의 안테나를 갖는다고 가정한다. 주 채널 H는 $N_b \times N_a$행렬로 표현되며, 도청 채널 G는 $N_e \times N_a$행렬로 표현된다. 이때, 적법한 송·수신자는 순시 채널 행렬 H를 알고 있다고 가정하고, H를 특이값분해 (singular value decomposition, SVD)하여 $U\Lambda A^H$로 표현할 수 있다. 조건 $N_b < N_a$에 대해서 H의 행렬 계수 (rank)의 최댓값은 N_b이며, 유니타리 (unitary) 행렬 V는 행렬 H의 양의 고유 값 (eigenvalue)에 대응하는 정규 직교 벡터들로 구성된 V_1과 영 공간 (null space)를 생성 (span)하는 행렬 Z로 표현된다($V=[V_1, Z]$). 따라서 $HZ=0$을 만족한다.

다중 안테나 환경에서 의사 잡음 (artificial noise)을 이용하면 도청자의 수신 신호 대 잡음비를 낮춤으로써 보안 전송 효율을 높일 수 있다.

송신자 Alice가 전송하는 신호 x는 기밀메시지 u와 의사 잡음 v로 구성되며, 다음과 같이 표현된다.

$$\mathbf{x} = \mathbf{V}_1\mathbf{u} + \mathbf{Z}\mathbf{v} = \mathbf{V}\begin{bmatrix}\mathbf{u}\\ \mathbf{v}\end{bmatrix},$$

여기서 u와 v의 통계적인 분포는 각각 $CN(0_{N_B}, I_{N_B})$와 $CN(0_{(N_A-N_B)}, I_{(N_A-N_B)})$이다.

이때, 전송 평균 전력 P는 $E[\|x\|^2]$이며, 기밀 메시지 송신 전력 P_u와 의사 잡음 송신 전력 P_v에 대해서 전송 평균 전력은 다음과 같이 표현된다.

$$P = E[\|x\|^2] = E[\|u\|^2] + E[\|v\|^2] = P_u + P_v.$$

적법한 수신자 Bob과 도청자 Eve가 수신하는 신호는 다음과 같이 표현된다.

$$y = HV_1u + HZv + n_B = HV_1u + n_B$$
$$z = GV_1u + GZv + n_E,$$

여기서 잡음 n_B와 n_E의 각 원소는 독립이고 각각 $CN(0, \sigma_{n_B}^2)$와 $CN(0, \sigma_{n_E}^2)$를 따른다.

도청자가 H, G, V_1, Z를 안다고 가정할 때, 순시 채널이득에 대한 보안 용량은 다음과 같이 표현된다.

$$C_s = \max_{p(u)}\{I(u;y) - I(u;z)\},$$

여기서

$$I(\mathbf{u};\mathbf{y}) = C\left(\frac{P_u}{N_B\sigma_{n_b}^2}\mathbf{H}\mathbf{H}^H\right),$$
$$I(\mathbf{u};\mathbf{z}) = C\left(\frac{P_u}{N_B\sigma_{n_e}^2}\mathbf{W}_1 + \frac{P_v}{(N_A-N_B)\sigma_{n_e}^2}\mathbf{W}_2\right) - C\left(\frac{P_v}{(N_A-N_B)\sigma_{n_e}^2}\mathbf{W}_2\right),$$
$$\mathbf{W}_1 = (\mathbf{G}\mathbf{V}_1)(\mathbf{G}\mathbf{V}_1)^H, \mathbf{W}_2 = (\mathbf{G}\mathbf{Z})(\mathbf{G}\mathbf{Z})^H,$$
$$C(\mathbf{X}) = \log[\det(\mathbf{I}+\mathbf{X})].$$

전체 전력 P를 기밀메시지 전송에 사용되는 전력 P_u와 의사 잡음을 전송하는데 사용하는 전력 P_v로 나누어 사용하기 때문에 적절한 전력분배가 보안 용량을 증대시키는데 있어 중요하다. P_v를 증가시키면 도청 채널의 SNR을 낮추게 되어 도청 채널 용량 $I(u;z)$를 낮출 수 있지만 기밀 메시지 송신을 위해 사용되는 전력이 감소하므로 주 채널 용량 $I(u;y)$또한 감소한다.

Qin[7]은 MISOME (multiple-input single-output multiple eavesdropper antenna) 환경에서 도청 채널의 순시 행렬 값을 적법한 송신자가 알 수 있을 때, P_u와 P_v에 대한 최적 전력 배분 (optimal power allocation)문제와 최적 빔 성형 벡터 설계 문제를 풀었다. 네트워크 내의 적법한 다른 수신자는 Alice가 Bob에게 정보 전송 시 잠

재적인 도청자로 볼 수 있으며, 이러한 경우 송신자가 잠재적인 도청자의 도청 채널에 대한 정보를 획득할 수 있으므로 적법한 사용자가 도청 채널의 순시 값을 알 수 있다는 가정이 성립할 수 있다.

순시 채널 용량을 바탕으로 페이딩 환경에서 달성 가능한 평균 보안 전송 용량은 다음의 수식을 통해서 구할 수 있다[6].

$$\bar{C}s=\max_{p(u)}\{I(u;y|H)-I(u;z|H,G)\},$$

여기서 $I(x;y|A)=E_A[I(x;y|A)]$이다.

Zhou[8]는 MISOME 페이딩 환경에서 달성 가능한 보안 전송 용량을 닫힌 해 형태로 구하였고, 수신 신호대 잡음비와 송신 안테나의 개수가 무한할 때 P_u와 P_v에 대한 최적 전력 배분 문제를 풀었다.

Ⅳ. 인지 무선(Cognitive radio)환경에서 물리계층 보안 전송 기술

1. 인지 무선(Cognitive Radio) 소개

인지 무선 기술은 한정적인 주파수 자원의 활용 극대화를 위해 사용되고 있지 않은 주파수 대역을 능동적으로 탐지하고, 사용함으로써 주파수 사용 효율을 극대화 하는 기술이다[18]. 특정 주파수 대역의 사용을 허가 (licensed) 받은 주 사용자 (primary user)가 항상 통신을 하는 것은 아니다. 따라서 비면허 (unlicensed) 부 사용자 (secondary user)는 주파수 감지 (spectrum sensing)을 통해서 비어있는 주파수 대역을 감지하고 통신을 수행할 수 있다. 이와 같이 주파수 자원의 활용 빈도를 높임으로써 주파수 효율을 증가시킬 수 있다[19]. 한편, 주 사용자가 인가된 주파수 대역을 사용 중이더라도 부 사용자는 주 사용자에게 미치는 간섭의 양적인 기준 (interference temperature)을 일정 이하로 만족하면서 해당 대역을 이용한 통신이 가능하다. 또한 부 사용자는 주 사용자가 송신하는 정보의 중계역할을 대가로 주파수 대역에 대한 사용허가를 받을 수 있다[19]. 인지 무선 네트워크에서 부 사용자의 전송 방식은 크게 두 가지로 구분할 수 있으며 〈표 1〉에 정리하였다.

〈표 1〉 인지 무선 네트워크 전송 방식

비협력적 전송 (Non-cooperative transmission)	부 사용자는 주 사용자가 주파수 대역을 사용하고 있지 않을 때에만 주 사용자의 주파수 대역을 사용한다.
협력적 전송 (Cooperative transmission)	부 사용자는 주 사용자의 통신을 방해하지 않는 범위에서 주 사용자의 주파수 대역을 사용하고, 주 사용자의 통신을 도와준다.

두 가지 방식 모두 부 사용자는 주 사용자의 기밀메시지에 대한 감청을 시도할 수 있다. 따라서 주 사용자는 부 사용자를 잠재적인 도청자로 간주한다. 정보이론 관점에서 비협력적 전송 방식의 경우 주 사용자는 도청을 막기 위해 Wyner가 제안한 도청 채널 모델을 이용하여 보안 전송을 할 수 있다[3]. 협력적 전송 방식의 경우 주 사용자, 신뢰 할 수 있는(trusted) 부 사용자, 도청자가 존재할 경우 도청자에게 누출되는 정보를 막기 위해 주 사용자와 부사용자가 협력 하는 협력 보안 전송 기법(cooperative secure transmission strategy)들이 제안되었다[11,20,21]. 또한 협력 보안 전송 방식에서 주 사용자 수신단과 부 사용자 수신단이 공통의 메시지(common message)를 수신해야하는 상황에서, 부 사용자 수신단이 부 사용자 송신단으로부터 기밀 메시지를 수신 받아야 하는 경우 달성 가능한 보안 전송율에 대한 연구가 수행되었다[22].

인지 무선 (cognitive radio) 통신환경에서 주 사용자는 부사용자가 자신의 기밀 메시지 전송을 돕는 대가로 부사용자의 주파수 대역 사용을 허가할 수 있다. 이러한 방식을 사용하면 주 사용자가 부사용자의 주파수 대역사용을 허가하지 않는 비협력적 전송 방식에 비해 높은 보안 전송 효율을 달성할 수 있다.

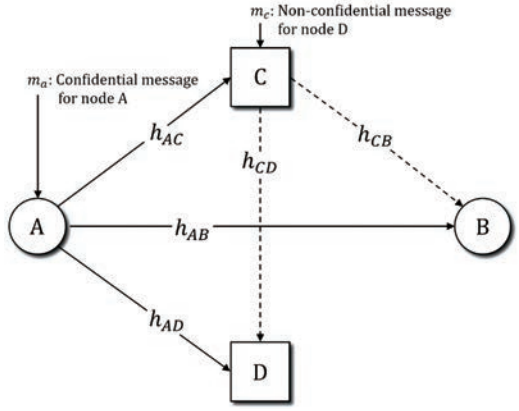
본고에서는 협력적 전송 방식으로 주 사용자의 기밀 메시지를 신뢰하지 않는 부 사용자가 중계함과 동시에 부 사용자의 비기밀 메시지 (non-confidential)를 송신하는 협력적 전송 환경에서 달성 가능한 보안 용량에 대한 분석 결과를 소개한다[12]. 또한 비협력적 전송 방식의 보안 전송률과 비교를 통해 협력적 전송 방식이 주 사용자 부

사용자 모두에게 이득이 되는 통신 환경에 대한 분석 결과를 소개하겠다.

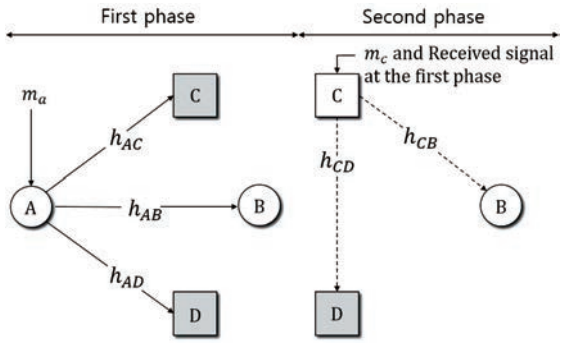
2. 인지 무선 네트워크의 시스템 모델

본고에서는 〈그림 4〉에서와 같이 주 사용자 송신단 노드 A, 주 사용자 수신단 노드 B, 부 사용자 송신단 노드 C, 부 사용자 수신단 노드 D로 구성된 인지 무선 통신 시스템을 가정한다. 주 사용자 송신단 노드 A는 기밀 메시지, $m_a \in M_a$를 송신하고, 부 사용자 송신단 노드 C는 비기밀 메시지, $m_c \in M_c$를 송신한다. 실선은 비협력적 전송방식을 의미하고 실선과 점선을 모두 고려하면 협력적 전송 방식을 의미한다. 모든 송수신단은 단일 안테나를 가지고 있으며, h_{ij}는 노드 i와 노드 j사이의 채널 이득(channel gain)을 말한다. 모든 채널은 독립적인 블록 페이딩(independent block fading)을 가정한다.

비협력적 전송 방식의 경우 부 사용자는 주사용자가 주



〈그림 4〉 인지 무선 네트워크 시스템 모델



〈그림 5〉 협력적 전송 방식

파수 대역을 사용하지 않을 때만 통신을 수행하며, 주사용자가 기밀 메시지를 보내는 상황에서는 부 사용자 노드 C와 D를 잠재적인 도청자로 간주하여 보안 전송을 수행한다.

〈그림 5〉는 본고에서 다루는 협력적 전송 방식의 동작을 보여준다. 부 사용자의 송신단은 주 사용자의 기밀 메시지를 중계하는 방식으로 증폭 후 전달 (amplify and forward, AF)방식을 이용하며 반이중 전송방식 (half-duplex)로 동작한다. 협력적 전송 방식은 2단계로 이루어진다. 첫 번째 단계에서는 노드 A가 기밀 메시지 m_a를 전송하고 나머지 노드들이 이를 수신한다. 이때 노드 C와 D가 기밀메시지에 대한 잠재적인 도청자이다. 두 번째 단계에서는 노드 C가 노드 A로부터 수신한 신호 y_c를 증폭하고 부사용자의 비기밀 메시지와 중첩하여 송신한다. 이때, 노드 C는 중계하고자하는 기밀 메시지 전송에 이용되는 송신 전력과 비기밀 메시지 전송에 이용되는 송신 전력의 비를 $\beta/(1-\beta)$로 설정하여 각 신호를 전송한다. 이때 노드 C는 노드 A의 기밀 메시지에 대한 보안 전송율이 비협력 통신환경에서 달성 가능한 값보다 높은 조건을 만족하면서도 비기밀 메시지에 대한 전송율을 최대화 시키도록 최적화된 β를 결정한다. 2번째 단계에서는 노드 D가 기밀메시지에 대한 잠재적인 도청자가 된다.

잠재적인 도청자 D는 두 단계에 걸쳐 기밀 메시지에 대한 정보를 수신한다. 따라서 도청 채널은 서로 공모(colluding)하는 두 도청자가 각각 독립적인 채널인 h_{AD}와 h_{cD}를 통해서 기밀메시지를 수신 하는 상황으로 볼 수 있다.

3. 보안 전송률

비협력적 전송 방식에서 송신 전력을 P_{nc}로 가정했을 때 주 사용자의 달성 가능한 보안 전송률은 다음과 같다[3,23].

$$R_{nc} = 2\left[C\left(|h_{AB}|^2 P_{nc}\right) - C\left(\max\left[|h_{AC}|^2, |h_{AD}|^2\right] P_{nc}\right)\right]^+.$$

$$C(\mathbf{A}) \equiv \frac{1}{2}\log\det(\mathbf{I}_N + \mathbf{A}),$$

여기서 달성 가능한 보안 전송율은 주 채널의 채널 용

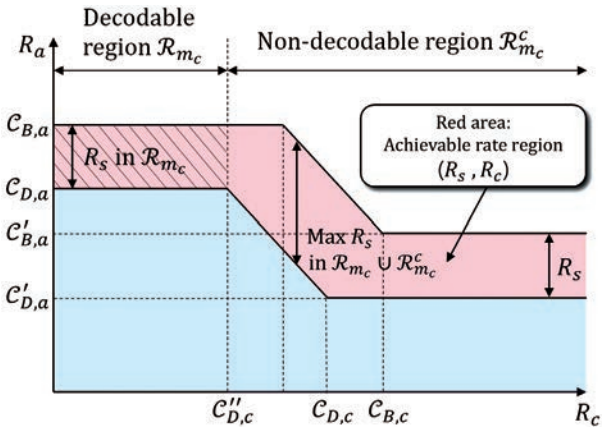
량에서 도청 채널의 채널 용량을 뺀 값으로 결정되는데, 잠재적인 도청 노드 C와 D중 노드 A로부터의 채널이득이 더 높은 쪽을 기준으로 보안 용량이 결정된다.

협력적 전송 방식의 경우 주 사용자의 기밀 메시지와 부 사용자의 비기밀 메시지를 모두 고려해야 한다. 그러므로 R_a는 m_a에 대한 전송률이고 R_c는 m_c에 대한 전송률일 때, 전송률 쌍 (R_a,R_c)를 고려한다. 먼저 노드 B, C, D에서 각각 달성 가능한 전송률 영역 R_B, R_C, R_D를 구한 후 보안 전송을 위한 제약 조건에 맞는 보안 전송률 R_s를 구한다[3,24]. 전송률 영역을 구할 때 m_a에 대해서는 노드 B가 복호화 할 수 있는 경우만 고려하고, m_c에 대해서는 노드 D가 복호화 할 수 있는 경우와 할 수 없는 경우 모두를 고려한다. [20]의 *Theorem* 1 을 이용하면 보안 전송률은 다음과 같다.

$$R_s=[R_a-R_e]^{+3)}$$
$$\text{subject to C1: C2:}(R_a,R_c)\in R_B \text{ and}$$
$$C2(R_e,R_c)\notin\{Rc\cup R_D\}$$

〈그림 6〉은 $R_C\subset R_D$인 경우, 즉 노드 D가 우세한(dominant) 도청자인 상황에서 노드 B와 노드 D의 달성 가능한 전송률 영역을 나타낸다. 여기서 우세하다는 것은 노드 D가 노드 C보다 m_a에 대한 정보를 더 많이 가지고 있다는 것을 의미한다. 전송률 영역의 형태는 송신 전력 P_a와 P_c, 전력 할당 비율 인자(power allocation ratio factor) β[4], 각 노드 간 채널 이득으로 결정된다. 〈표 2〉는 각각의 x축과 y축 값을 의미한다.

〈그림 6〉의 붉은 영역과 푸른 영역을 모두 합한 영역은 노드 B의 달성 가능한 전송률 영역을 나타내고, 푸른 영역은 노드 D의 달성 가능한 전송률 영역을 나타낸다. 〈그림 6〉에서 주어진 R_c에 대해 붉은 영역과 푸른 영역의 y축 차이 값 R_s는 보안 전송률을 나타낸다. 노드 D에서 m_c에 대한 전송률 영역은 m_c를 복호화 할 수 있는 전송률 영역 R_{m_c}와 복호화 하지 못하는 전송률 영역 $R^c_{m_c}$으로 나눌 수 있다. 복호화 하지 못하는 전송률 영역에서 m_c는 더미 메시지(dummy message)로써 도청자가 m_a를 복호화 할 때 혼란을 주는 역할을 한다. 빗금 친 영역은 주 사용자와 부 사용자의 각각 전송하고자 하는 메시지 m_a와 m_c가 각 수신단에서 성공적인 복호화가 가능한 전송률 영역을 말한다.



〈그림 6〉 달성 가능한 전송률 영역(R_a,R_c)[12]

〈표 2〉 그림 6의 채널 용량

$C_{i,j}$	노드 i에서 m_a, m_c둘 다 복호화 할 수 있을 때 메시지 m_j에 대한 채널 용량
$C'_{i,a}$	노드 i에서 m_c를 잡음으로 간주할 때에 m_a대한 채널 용량
$C''_{D,c}$	노드 D에서 m_a를 잡음으로 간주할 때에 m_c대한 채널 용량

부 사용자는 자신의 메시지 전송뿐만 아니라 주 사용자의 기밀 메시지를 중계해야 하므로 한정된 송신 전력을 효과적으로 각 메시지에 할당해야한다. 이때 부사용자는 주사용자 보안 전송 효율에 대한 QoS기준을 만족하도록 전송 전력 비 최적화를 수행한다.

4. 부 사용자의 전송 전력 비 최적화문제

협력적 전송 방식의 경우 각 노드 사이의 채널 이득과 노드 B에서 전력 할당을 어떻게 했는지에 따라 보안 전송률 달라진다. 이때, 주 사용자는 협력 전송의 결과로 비협력 전송 방식을 이용하였을 시보다 더 높은 보안 전송 효율을 획득할 수 있어야하며, 부사용자는 기밀메시지 중계의 보상으로 자신의 메시지를 전송할 수 있어야한다. 따

3) R_e는 노드의 달성 가능한 전송률 영역에서 포함되지 않는 m_a에 대한 전송률을 의미한다.

4) β값이 증가하면 m_a에 대한 전력이 증가하고 m_c에 대한 전력이 줄어든다. 반대로 β값이 감소하면 m_a에 대한 전력이 감소하고 m_c에 대한 전력이 줄어든다.

〈표 3〉 채널 환경 분류

case 1	β의 값과 전송 방식에 상관없이, 노드 C가 우세한 도청자인 조건
case 2	β의 값에 전송 방식에 상관없이, 노드 D가 우세한 도청자인 조건
case 3	협력적 전송 방식의 경우 β의 값에 따라 우세한 도청자가 노드 C 혹은 노드 D가 되고, 비협력적 전송방식의 경우 노드 C가 우세한 도청자가 되는 조건

라서 최적화 문제는 협력 전송의 결과로 주 사용자가 비협력 전송방식에서 달성 가능한 보안 용량 또는 미리 정한 일정 수준의 보안 전송률 $\lambda(\geq 0)$를 획득할 수 있어야 하는 제약 조건을 만족해야한다. 이때 부사용자가 달성 가능한 채널용량에 대한 최적화 문제는 다음과 같다.

$$\max_{\beta \in U_\beta} [R_c]^+$$
$$\text{subject to } R_s > \max[\lambda, R_{nc}],\ R_c \in R_{m_c}$$

여기서 $U_\beta = \{\beta \mid 0 < \beta < 1\}$

m_c의 전송률 R_c의 최댓값을 구하는 것은 [12]의 *proposition* 1 에 의해서 두 제약 조건을 만족하는 β의 영역에서 가장 작은 β값을 찾는 것과 같다. 위의 제약 조건을 만족하는 β의 영역은 〈표 3〉과 같이 3가지 채널 환경(channel condition)으로 분류해서 구할 수 있다.

[12]의 결과에 따르면 신뢰하지 않는 부 사용자의 중계를 이용한 협력적 통신 방식이 부 사용자와 주 사용자 모두에게 이득이 되는 것을 알 수 있다. 특히 부 사용자의 송신 전력 P_c가 주 사용자의 송신 전력 P_a보다 큰 경우 협력적 전송 방식은 비협력적 전송 방식에 비해 큰 장점을 가진다.

Ⅴ. 결 론

본고에서는 차세대 무선네트워크의 보안 강화를 위해, 다중 안테나를 갖는 차세대 셀룰러 네트워크에 적용가능한 의사 잡음을 이용한 보안 전송기술, 분산 네트워크에서 협력 통신을 통해 보안 전송 효율을 높이는 기술, 인지무선 통신에서 부 사용자가 면허대역을 사용하는 대가로 주 사용자의 보안 통신을 돕는 기술 등을 살펴봤다.

물리 계층 보안 전송기술은 도청자의 연산 능력과 무관하게 완벽 보안을 제공할 수 있는 강력한 보안 기술로서 가까운 미래에 기존 보안기술을 보완하거나 대체할 수 있을 것으로 기대된다.

참 고 문 헌

[1] R. V. Meter, K. M. Itoh, and T. D. Ladd. "Architecture-dependent execution time of Shor's algorithm," in Proc. Int. Symp. on Mesoscopic Superconductivity and Spintronics. 2006.

[2] C. Shannon, "Communication theory of secrecy systems," Bell Syst. Technical J., vol. 28, no. 4, pp. 656–715, 1949.

[3] A. D. Wyner "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1255–2387, Oct. 1975.

[4] S. K. Leung-Yan-Cheong, "On a special class of wiretap channels," IEEE Trans. on Inf. Theory, vol. 23, no. 5, pp. 625–627, Sept. 1977.

[5] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas&–Part II: The MIMOME Wiretap Channel," IEEE Trans. on Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[6] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," IEEE Trans. on Wireless Commun., vol. 7, no. 6, pp. 2180–2189, June 2008.

[7] H. Qin, X. Chen, Y. Sun, M. Zhao, and J. Wang, "Optimal Power Allocation for Joint Beamforming and Artificial Noise Design in Secure Wireless Communications," IEEE Int. Conf. on Commun. Workshops (ICC) , June 2011, pp.1–5.

[8] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," IEEE Trans. on Vehicular Tech., vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[10] Hu Jin, 김준수, "협력중계 시스템에서의 물리계층 보안 기술," 한국 통신학회지, 제 31권 제2호, 91–97, 2014년 2월

[11] K. Lee, C. Chae, and J. Kang. "Spectrum leasing via cooperation for enhanced physical-layer secrecy," IEEE Trans. on Vehicular Tech., vol. 62, no. 9, pp. 4672–4678, June 2013.

[12] H. Jeon, S. W. McLaughlin, I. Kim, and J. Ha, "Secure

communications with untrusted secondary nodes in cognitive radio networks," IEEE Trans. on Wireless Commun. vol. 13, no. 4, pp. 1790–1805, Apr. 2014.

[13] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in Proc. IEEE Int. Symp. Inf. Theory, Sep. 2005, pp. 2152–2155.

[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information–theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, June 2008.

[15] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in Proc. 44th Annu. Allerton Conf. Communications, Control and Computing, Monticello, Sep. 2006, pp. 841–848.

[16] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secrecy capacity region of fading broadcast channels," in Proc. IEEE Int. Symp. Information Theory, Nice, Jun. 2007, pp. 1291–1295.

[17] P. K. Gopala, L. Lai, and H. El–Gamal, "On the secrecy capacity of fading channels," in Proc. IEEE Int. Symp. Inf. Theory, Nice, June 2007, pp. 1306–1310.

[18] Mitola III, Joseph, and Gerald Q. Maguire Jr. "Cognitive radio: making software radios more personal," IEEE Personal Commun., vol. 6. no. 4, pp. 13–18, Aug. 1999.

[19] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 40–48, Apr. 2008.

[20] Y. Wu, and K. J. Liu. "An information secrecy game in cognitive radio networks," IEEE Trans. Inform. Forensics and Security, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[21] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," IEEE Trans. Wireless Commun., vol. 12, no. 1, pp. 134–145, Jan. 2013.

[22] Y. Liang, A. Somekh–Baruch, H. V. Poor, S. Shamai (Shitz), and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," IEEE Trans. Inf. Theory, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[23] M. Bloch and J. Barros, Physical–Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.

[24] X. Tang, R. Liu, P. Spasojevi´c, and H. V. Poor, "Interference assisted secret communication," IEEE Trans. Inf. Theory, vol. 57, no. 5, pp. 3153–3167, Sept. 2011.

임 상 훈

• 2009년 2월 숭실대학교 정보 통신 전자 공학부 학사
• 2011년 2월 한국과학기술원 전기 및 전자 공학과 석사
• 2011년 3월~현재 한국과학기술원 전기 및 전자 공학부 박사과정

〈관심분야〉
무선통신 신호처리, 정보이론, 물리계층 보안

윤 상 석

• 2010년 8월 부산대학교 전자전기공학부 학사
• 2012년 2월 부산대학교 전자전기공학부 석사
• 2012년 3월~현재 한국과학기술원 전기 및 전자 공학부 박사과정

〈관심분야〉
물리계층 보안, 무선 통신

박 정 욱

• 2015년 2월 부산대학교 전자전기공학부 학사
• 2015년 3월~현재 한국과학기술원 전기 및 전자 공학부 석사과정

〈관심분야〉
물리계층 보안, 무선 통신

하 정 석

• 1992년 2월 경북대학교 전자공학과 학사
• 1994년 2월 포항공과대학교 전자전기 석사
• 2003년 2월 Georgia Institute of Technology 박사
• 2004년~2010년 한국정보통신대학교 조교수
• 2010년~현재 한국과학기술원 부교수

〈관심분야〉
통신, 채널부호, 물리계층 보안