협력중계 시스템에서의 물리계층 보안 기술

Hu Jin, 김준수
경상대학교, 한국산업기술대학교

요 약

최근 물리계층 보안에 대한 관심이 높아지면서 이를 이동통신 시스템에 적용하기 위한 다양한 연구가 이루어지고 있다. 또한 차세대 이동통신의 중요한 기술적 요소로 각광받고 있는 협력 중계 기술을 기반으로 물리계층 보안을 극대화하기 위한 다양한 방식이 개발된 바 있다. 본고에서는 협력중계 시스템에서의 다양한 물리계층 보안 확보 기법을 소개하고 각각의 성능을 비교한다.

Ⅰ. 서 론

무선 채널은 기본적으로 누구든 신호를 수신할 수 있는 개방성을 가지고 있어 여타의 통신 매체에 비해 보안에 취약하다. 특히 최근 스마트폰의 급격한 보급과 이를 기반으로 하는 다양한 데이터 어플리케이션들의 확대로 인해 무선통신 시스템에서의 보안에 대한 요구 및 중요성이 날로 높아지고 있다.

최근 이러한 상황에서 정보이론 관점에서의 물리계층 보안 기술이 안전한 무선 통신 시스템 구축을 위한 유망 기술로 관심을 받고 있다. Shannon은 정보이론 관점에서 보안 전송률 (secrecy capacity)이라는 개념을 착안하였으며[1] 이를 바탕으로 Wyner는 송신단과 도청단말 사이의 무선채널이 송신단과 수신단 사이의 무선 채널보다 나쁠 경우 별도의 데이터 암호화를 사용하지 않더라도 안전한 통신이 가능함을 증명하였다[2].

협력중계 통신은 다수 중계국간의 협력을 통한 무선전송 경로의 다양화를 통해 다양성 이득 (diversity gain)을 획득하여 무선채널의 전송 성능을 향상시키는 기술로서 4세대 및 5세대 시스템의 핵심 기술로 주목 받아왔다.

따라서 높은 전송 성능을 가지면서 보안성을 확보하기 위해서는 협력중계 시스템을 기반으로 보안 전송률을 극대화할 수 있는 물리계층 보안 기법이 필요하며[3], 이러한 기술적 요구를 충족하기 위한 다양한 기법이 제안되어왔다.

협력중계 시스템을 기반으로 물리계층 보안을 확보하기 위한 다양한 기술들은 주로 협력형 빔형성 (cooperative beamforming) 또는 중계국 선택 (relay selection) 방식으로 구분할 수 있다.

협력형 빔형성 기술은 각 중계국의 전송 안테나에서 동시에 전송하는 무선 신호를 특정 목적에 맞게 변형하여 전송함으로써 서로 다른 중계국의 안테나에서 전송된 신호가 무선 채널 중에서 중첩되어 수신단에 원하는 형태로 수신될 수 있도록 하는 기술이다. 이를 위해서는 물리적으로 다른 위치에 설치된 중계국이 마치 하나의 시스템과 같이 동작해야만 한다. 이와 관련된 주요 연구는 다음과 같다.

Dong et al.은 물리계층 보안을 요구하는 다중 중계노드 환경에서 디코딩 후 전달 (decode-and-forward, DF), 증폭 후 전달 (amplify-and-forward, AF), 및 협력재밍 (cooperative jamming, CJ) 기술들을 사용하기 위한 최적의 빔형성 방식을 제안하였다[4]. DF 및 AF 방식의 중계 시스템에서 모든 중계국들은 최적의 빔형성 계수를 전송하려는 데이터 신호에 곱하여 수신단과 도청단이 수신하는 신호대잡음비 (signal-to-noise ratio, SNR)의 비율을 최대화하도록 한다. CJ 중계 방식은 송신단, 즉 기지국만 데이터 신호를 전송하고 나머지 모든 중계국들은 도청단이 이 신호를 도청하지 못하도록 인위적인 잡음을 생성하여 도청단의 수신을 방해한다. 이를 위해 중계국들은 최적의 빔형성을 통해 생성된 잡음으로 도청단말의 수신을 방해(재밍)하고 목표했던 수신단에는 간섭을 일으키지 않도록 한다. Zheng et al.은 중계국들이 각각의 전송 전력의 제약이 있을 때 협력재밍을 위한 최적 빔형성 기법을 제안하였다[5]. Zhang과 Gursoy 또한 다중 AF 및 DF 중계국들이 존재할 때 전체 및 각각의 전력 제약이 있는 경우에 대해 최적 빔형성 기법을 설계한 바 있다[6]. Zhang et al.은 양방향 (two-way) 중계 통신 시스템에서 0이상의 보안 전송률이 존재함을 증명하였고 중계국들에 대한 최적 전력할당 방식을 제안하였다[7]. 최적 빔형성 방식에 대한 연구는 다중 안테나 (Multiple-Input Multiple Output, MIMO) 시스템에서도 진행되었다[8][9].

이상에서 언급한 다중 중계국의 빔형성을 통한 물리계층 보안

기법과 더불어 다중 중계시스템의 효율적인 활용 방안으로 고려되는 중계국 선택 기법을 기반으로 물리계층 보안을 확보하고자 하는 연구 또한 활발히 진행되고 있다.

Krikidis는 기회적인 중계국 선택을 통해 물리계층 보안을 제공하기 위한 기법을 제안한 바 있다[10]. 즉 다수의 중계국 중 하나의 중계국을 선택하되 수신단과 도청단말의 SNR비율을 극대화 하는 중계국을 매번 기회적으로 선택 (opportunistic selection)하는 방식이다. 추가로 Krikidis et al.은 중계국 선택과 재밍을 결합한 최적 선택 및 재밍 기법 (optimal selection and jamming, OSJ) 방식을 제안하였다[11]. OSJ는 한 쌍의 중계국을 선택하되 하나의 중계국이 데이터를 전송하는 동안 다른 중계국이 의도적인 재밍 신호, 즉 잡음을 발생하는 것이다. 이를 통해 선택된 두 개의 중계국은 수신단과 도청단이 수신하는 SNR의 비율을 최대화하여 보안 전송률을 최대화한다.

협력형 빔형성과 비교하면 중계국 선택 방식은 상대적으로 적은 양의 채널 정보를 필요로 하는 장점을 갖는다. 즉 중계국 선택 방식은 채널 이득의 절대값만을 요구하는 반면 협력형 빔형성은 채널 정보의 전체 값을 필요로 한다.

또한 협력형 빔형성은 다중 중계국 사이의 정보 교환 및 동기화를 요구하며 중계국이 많을 수록 그 난이도가 높아진다. 따라서 실용적인 운용을 위해 중계국의 수를 적절히 조절할 필요가 있다. 반면, 운영 복잡도를 줄이기 위해 협력에 참여하는 중계국의 수를 줄이면 협력형 빔형성으로부터 얻을 수 있는 이득이 감소한다. 따라서 Kim et al.은 중계국 선택과 협력형 빔형성을 결합하는 방법을 제안하였는데 다중 중계국중 한 쌍을 선택하여 협력형 빔형성을 수행하는 것이다[12].

본고에서는 위에서 언급한 세 분류의 협력중계 시스템에서의 물리계층 보안 기법들을 구체적으로 살펴보고 그 성능을 비교한다.

Ⅱ. 시스템 모델

일반적으로 고려하는 협력형 중계시스템에서의 물리계층 보안 모델은 하나의 송신단, M개의 중계노드, 하나의 수신단 및 하나의 도청단으로 구성된 시스템으로 〈그림 1〉과 같다. 이와 같은 모델에 대해 자주 언급되는 의문과 그에 대한 설명은 다음과 같다.

첫째, 하나의 도청단을 고려하는 이유에 대한 의문이다. 실제 상황에서는 다수의 도청단이 존재할 수 있다. 그러나 〈그림 1〉의 모델에서 고려하는 하나의 도청단은 다수의 도청단 중에서 가장 치명적인 위협을 갖는 도청단을 대표하는 것이라 할 수 있다. 즉 여러 도청단 중 수신단에 가장 가까이 있어서 도청할 가능성이 가장 높은 단말에 효율적으로 대응할 수 있으면 나머지 도청단들은 자연스럽게 해결되었다 할 수 있다.

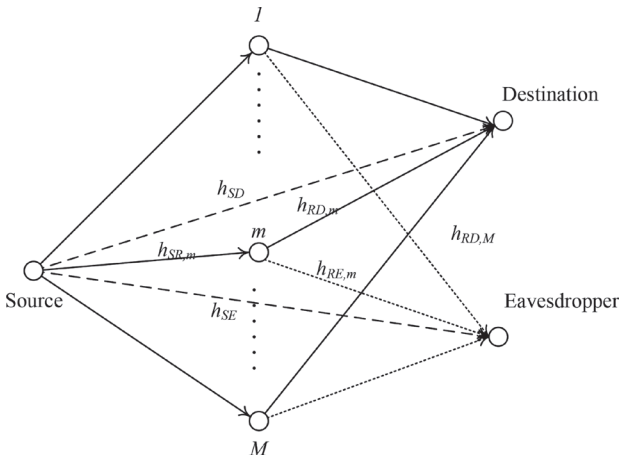

그림 1. 시스템 모델

두 번째 의문은, 송신단의 입장에서 도청단의 존재 유무를 인지하거나 심지어 도청단의 무선 채널 상황을 확보할 수 있는지 여부에 대한 것이다. 이에 대한 일반적인 설명으로, 도청단이 동일 시스템 내의 단말이라는 가정을 활용한다. 즉, 도청단말 역시 정상적인 수신단과 같은 여러 수신단 중 하나라고 가정하는 것이다. 이와 같은 가정 하에서는 의도적으로 조작된 악의적 도청단에 대한 대응이 어려우나, 일반적으로 누군가의 통신을 도청하기 위해 정상적인 수신단으로 위장하여 타인의 무선 채널을 엿듣는 것을 고려하면 현실적인 가정이라 볼 수 있다.

이상에서 언급한 것 이외에 다양한 의문이 존재하나, 물리계층 보안 기술의 단계가 초기적인 점을 고려할 때 〈그림 1〉은 현 상황에서 고려할 수 있는 가장 적합한 모델이라 할 수 있다.

협력형 중계시스템은 하나의 패킷을 전송하기 위해 두 단계로 동작한다. 첫번째 단계에서는 송신단이 전송하는 패킷을 수신하고 다음 단계에서는 그 패킷을 수신단에 재전송하는 것이다. 또한 중계국은 도청단과 수신단까지의 채널 정보를 알 수 있다고 가정한다.

본고의 성능비교에서는 물리계층 보안을 위한 협력중계 방식의 영향에 초점을 두기 위하여 송신단과 수신단 (source-destination, SD) 및 도청단 (source-eavesdropper, SE) 사이의 링크가 차단되었다고 가정한다. 즉 $h_{SD} \approx 0$ 및 $h_{SE} \approx 0$ 으로 도청단은 송신단에서 전송하는 신호를 직접 엿들을 수 없다고 가정한다. 이러한 시스템에서 중계국들은 우선 송신단의 신호를 수신하고 다음 그 신호를 다시 인코딩하고 빔형성 계수를 곱하여 수신단에 전송한다. 또한 간결한 설명을 위하여 송신단과 중계노드 (source-relay, SR) 사이의 채널은 충분히 좋아서

중계국들이 송신단의 신호를 성공적으로 수신할 수 있다고 가정한다. 일반적으로 시스템을 구축할 때 중계국들을 송신단과 Line-of-Sight (LOS) 채널이 형성되도록 설치하기 때문에 중계국의 성공적 수신은 합리적인 가정이라 할 수 있다.

이상에서의 가정 아래에서, 〈그림 1〉과 같은 시스템의 특징은 중계국과 수신단 (Relay-Destination, RD) 및 중계국과 도청단 (Relay-Eavesdropper, RE) 사이의 무선 채널의 특성으로 표현할 수 있다. 즉, 이 시스템이 얻을 수 있는 보안 전송률은 다음과 같다.

$$C_S \triangleq \max\{C_D - C_E, 0\}$$

$$C_D \triangleq \frac{1}{2}\log_2(1+\gamma_D), \quad C_E \triangleq \frac{1}{2}\log_2(1+\gamma_E)$$

이때 γ_D와 γ_E는 각각 수신단과 도청단의 수신 SNR이다. 협력중계 시스템에서 중계국들의 역할은 바로 γ_D를 최대화하는 동시에 γ_E를 최소화하는 것이다.

Ⅲ. 협력중계 기반 물리계층 보안 기술

본 장에서는 Ⅱ장에서 제시한 시스템 모델을 바탕으로 각각의 협력중계 기반 물리계층 보안 방식을 구체적으로 설명한다.

1. 협력재밍(CJ) 방식

협력재밍 (cooperative jamming, CJ) 방식에서 중계국들은 임의의 잡음을 생성하여 도청단의 수신을 방해하는 역할을 담당한다. 따라서 중계국은 데이터를 전송하지 않고 오직 전송단만 신호를 전송하며 각 중계국에서 발생한 잡음은 도청단에만 영향을 미치도록 생성되어야 한다[5]. 이러한 방식에서 최적 빔형성은 수신단에 도착하는 중계국 신호 (인위적 잡음)의 합이 0이 되도록 하여 수신단의 데이터 복구에 영향을 주지 않고 도청단의 수신만 방해한다. 이는 다수의 중계국을 전적으로 도청단을 차단하는 용도로만 활용하는 것으로 협력이득을 통해 데이터 전송 성능 향상을 획득하고자 하는 협력 중계시스템의 취지와는 다소 상이한 측면을 가지고 있다.

2. 최적 중계국 선택 (OS) 방식

최적 중계국 선택 (optimal selection, OS) 방식은 모든 중계국 중에서 수신단과 도청단의 수신 SNR의 비율이 가장 큰 중계국을 선택하여 선택된 중계국을 통해 데이터를 전송하는 방식이다[10]. 중계국이 많을수록 수신단과의 채널 성능은 좋고 도청단과의 채널 성능은 낮은 중계국이 존재할 확률이 높아지므로, 중계국이 많을수록 복잡한 빔형성 기법을 사용하지 않고 단순한 선택을 통해 물리계층 보안을 확보할 수 있다. 이를 위해 각각의 중계국들은 수신단과 도청단 까지의 채널의 이득만 알면 되고 채널의 위상을 필요로 하지 않기 때문에 협력형 빔형성 기법보다 운영 복잡도 측면에서 단순한 기법이라 할 수 있다.

3. 최적 중계국 선택 및 재밍 (OSJ) 방식

최적 중계국 선택 및 재밍 (optimal selection and jamming, OSJ) 방식은 OS방식의 확장 기술로서 다중 중계국 중 두 개의 중계국을 선택하여 하나의 중계국은 데이터 전송을, 다른 하나의 중계국은 도청 방해를 위한 인위적 잡음 생성을 담당하도록 하는 방식이다. OS에 비해 인위적 잡음 생성을 통해 보안성능을 높이려는 시도이나 생성된 인위적 잡음이 도청단을 방해할 뿐만 아니라 수신단에 간섭을 발생할 수 있다[11].

4. 최적 빔형성 (OB-CSI) 방식

만약 M개의 중계국들이 모두 빔형성에 참여하게 되면 수신단과 도청단이 수신하는 신호는 다음과 같다.

$$y_D = \sqrt{P_0}\, w^T h_{RD} s + n_D$$

$$y_E = \sqrt{P_0}\, w^T h_{RE} s + n_E$$

이중 s는 전송 심볼, P_0는 전송 전력, $w \triangleq [w_1, \cdots, w_M]^T$, $h_{RD} \triangleq [h_{RD,1}, \cdots, h_{RD,M}]^T$, $h_{RE} \triangleq [h_{RE,1}, \cdots, h_{RE,M}]^T$이며 n_D와 n_E는 수신단과 도청단의 잡음이다. 따라서 각각의 수신 SNR은 다음과 같다.

$$\gamma_D = \gamma_0 \left| w^T h_{RD} \right|^2 = \gamma_0 w^T H_{RD} w^*$$

$$\gamma_E = \gamma_0 \left| w^T h_{RE} \right|^2 = \gamma_0 w^T H_{RE} w^*$$

이때 $\gamma_0 \triangleq P_0 / \sigma_N^2$는 전송 SNR이고 $H_{RD} \triangleq h_{RD} h_{RD}^H$와 $H_{RE} \triangleq h_{RE} h_{RE}^H$은 랭크 1인 매트릭스들이며 σ_N^2는 잡음전력밀도 (power spectral density)이다. 보안전송률 C_S를 최대화 하려면 $C_D - C_E$을 최대화 하여야 한다. 따라서 빔형성 벡터 w는 아래와 같은 최적화 문제의 해답이 될 것이다.

$$\max_{w} \quad \frac{1+\gamma_D}{1+\gamma_E} = \frac{1+\gamma_0 w^T H_{RD} w^*}{1+\gamma_0 w^T H_{RE} w^*}$$

$$\text{s.t.} \quad w^H w = 1$$

이때 $w^H w = 1$은 총 전송전력 P_0를 만족하기 위한 조건이다. 위의 최적화 문제를 풀면 최적의 빔형성 벡터를 아래와 같이 얻을 수 있다[13].

$$w_{\text{opt}} = u_{\max}\left(\left(I+\gamma_0 H_{RE}\right)^{-1}\left(I+\gamma_0 H_{RD}\right)\right)$$

이 중 $u_{\max}(A)$는 행렬 A의 고유값 (eigenvalue) 중 최대 값에 대응하는 고유벡터 (eigenvector)이고 I 는 단위 행렬이다. 따라서 최적 빔형성 방식은 매번 채널정보를 이용하여 w_{opt}를 계산하여 빔형성을 수행한다. 이 과정에서 채널 정보를 모두 알고 있어야만 최적 빔형성이 가능하므로 이 기법을 채널정보를 모두 활용하는 최적 빔형성 (optimal beamforming with channel state information, OB-CSI) 기법이라 명명한다.

5. 중계국 선택 및 최적 빔형성 (OB-CSI-RS) 방식

OB-CSI방식은 모든 중계국이 빔형성에 참여하므로 매우 많은 정보가 필요하고 빔형성 벡터 생성을 위한 계산 복잡도 또한 높다. 이를 극복하기 위해 M개의 중계국 중 두 개의 중계국만을 선택하고, 선택된 중계국을 통해 빔형성을 시도하는 방식이 중계국 선택 및 최적 빔형성 (optimal beamforming with channel state information and relay selection, OB-CSI-RS) 방식이다[12]. 두 개의 중계노드만 선택하므로 중계국 사이의 동기화 문제 등을 해결하기 위한 복잡성이 줄어들게 된다. 또한 추가적인 차선(sub-optimal)의 빔형성 기법을 사용할 수 있어 그 복잡도를 더욱 줄일 수 있다.

M개의 중계노드 중 임의의 두 개의 중계국을 m과 n으로 표현하면 두 개의 중계국 (m,n)이 전송 할 때의 최적 빔형성 벡터를 4절에서와 같이 $h_{RD,(m,n)} \triangleq \left[h_{RD,m}, h_{RD,n}\right]^T$ 및 $h_{RE,(m,n)} \triangleq \left[h_{RE,m}, h_{RE,n}\right]^T$을 이용하여 계산할 수 있다. $\gamma_{D,(m,n)}$과 $\gamma_{E,(m,n)}$으로 최적 빔형성을 수행했을 때 얻을 수 있는 수신단의 SNR과 도청단의 SNR의 비율을 최대화하는 두 중계국을 선택한다. 즉, 선택된 두 중계국은 다음과 같은 선택 규칙을 따른다.

$$\left(m^*, n^*\right) = \underset{\substack{m,n\in\{1,\cdots,M\}\\ m\neq n}}{\arg\max} \frac{1+\gamma_{D,(m,n)}}{1+\gamma_{E,(m,n)}}$$

6. 중계국 선택 및 도청채널 삭제 (ECN-RS) 방식

중계국 선택 및 도청채널 삭제 (eavesdropper channel nulling with relay selection, ECN-RS) 방식은 중계국 선택 및 최적 빔형성 (OB-CSI-RS)의 단순화 방식이다. 즉, ECN-RS는 OB-CSI-RS와 같이 다수의 중계국 중 두 개의 중계국을 선택하여 빔형성을 시도한다. 그러나 이때 OB-CSI-RS가 수신단의 SNR을 최대화하고 도청단의 SNR을 최소화하는 방향으로 빔형성하는 것과 달리 도청단의 SNR을 최소화하는 것 만을 목표로 빔형성한다. 이를 통해 보안 전송률의 성능 저하를 최소화하면서 시스템 동작을 위한 복잡도를 OB-CSI-RS에 비해 크게 줄이는 효과를 얻을 수 있다.

7. 중계국 선택 및 분산적 위상정렬 (DPA-RS) 방식

중계국 선택 및 분산적 위상정렬 (distributed phase alignment with relay selection, DPA-RS) 방식은 앞서 소개한 ECN-RS에서 시스템 운영 복잡도를 한 단계 더 줄이는 방식이다. ECN-RS는 다수의 중계국 중 두 개의 중계국을 선택하고, 두 중계국의 안테나에 최적의 빔형성 벡터를 적용하여 도청단이 수신하는 SNR을 0으로 만든다. 그러나, 현실적으로 도청단이 수신하는 SNR을 0으로 만들기 위해서는 각 중계국으로부터 도청단 사이의 무선 채널의 값을 모두 알고 있어야만 가능하다. 이러한 가정이 이론적으로는 가능하나, 실제 시스템에서는 여러 이유에 의해 무선 채널 정보를 정확하게 확보하는 것이 매우 어렵다.

따라서 DPA-RS는 선택된 두 개의 중계국과 도청단 사이의 채널 정보 중 위상 정보만을 이용해 도청 채널의 SNR을 최소화하는 방식이다. 이는 ECN-RS에 비해 적은 정보를 요구하므로 상대적으로 운영 복잡도가 낮은 장점이 있으나 도청 채널의 SNR을 완전히 0으로 만들 수 없기 때문에 전송 성능은 DPA-RS보다 저하된다.

8. 협력중계 방식들의 간단한 정리

〈표 1〉은 이상에서 살펴본 물리계층 보안을 위한 협력중계 방식들을 간단히 정리한 표이다. 방식의 약자는 다음과 같다.

CJ: 협력재밍 (cooperative camming)
OS: 최적 중계국 선택 (optimal selection)
OSJ: 중계국 선택 및 재밍 (optimal selection and jamming)
OB-CSI: 최적 빔형성 (optimal beamforming with channel state information)
OB-CSI-RS: 중계국 선택 및 최적 빔포밍 (optimal beamforming with channel state information and relay selection)
ECN-RS: 중계국 선택 및 도청채널 삭제 (eavesdropper channel nulling and relay selection)
DPA-RS: 중계국 선택 및 분산적 위상정렬 (distributed phase alignment and relay selection)

CJ, OB-CSI, OB-CSI-RS, ECN-RS는 완벽한 채널 정보를 요구하므로 피드백 채널을 위한 대역폭을 많이 요구한다. 반면 OS, OSJ, DPA-RS는 부분적 채널정보를 이용하기에 상대

표 1. 물리계층 보안을 위한 협력중계 방식

방식	필요한 채널 정보	협력 중계 국의 갯수	빔형성
CJ	Full CSI	M	Optimal BF
OS	Channel gain	1	No BF
OSJ	Channel gain	2	No BF
OB-CSI	Full CSI	M	Optimal BF
OB-CSI-RS	Full CSI	2	Optimal BF
ECN-RS	Full CSI	2	Sub-optimal BF
DPA-RS	Partial CSI	2	Sub-optimal BF

적으로 적은 대역폭을 요구한다. 중계노드 선택 방식들인 OS, OSJ, OB-CSI-RS, ECN-RS, DPA-RS는 기본적으로 한 개 또는 두 개의 중계국 참여로 협력중계를 시도하여 중계국간의 정보교환 및 동기화를 위한 복잡도가 낮다고 할 수 있다.

Ⅳ. 성능 비교

본 장에서는 앞서 소개한 다양한 협력중계 방식의 성능을 비교한다.

〈그림 2〉는 두 개의 중계노드가 존재하고 RD 및 RE 링크의 채널이득이 0dB일때의 보안 전송율을 보여준다. 그림에서와 같이 OB-CSI가 가장 좋은 성능을 보이고 있으며 OB-CSI-RS는 OB-CSI와 거의 같은 성능을 보여줌을 알 수 있다. 또한 ECN-RS의 보안 전송율은 SNR이 무한대일 때OB-CSI-RS에 근접하는 것을 확인할 수 있다. 하지만 DPA-RS는 부분적 채널 정보를 이용하므로 높은 SNR 영역에서 특정한 값 이하로 포화되는 것을 확인 할 수 있다. 두 개의 중계노드가 있기에 CJ

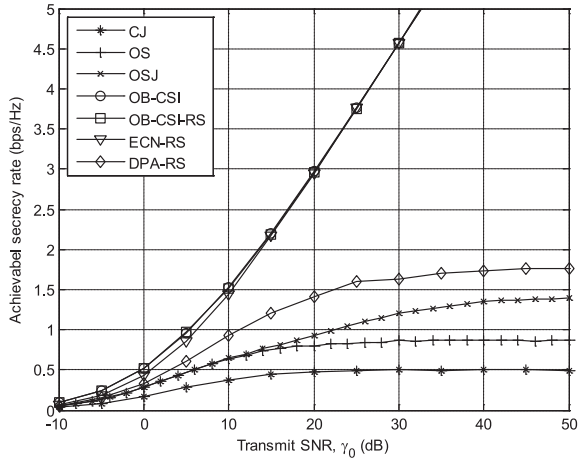

그림 2. 보안 전송율 ($M = 2,\ \rho_{rd} = \rho_{re} = 0dB$)

방식에서는 임의의 한 중계노드는 데이터를 전송하고 다른 하나는 재밍을 시도하게 되는데 단지 하나의 중계노드로는 협력 재밍을 할 수 없어 그 성능이 낮게 나타나고 있다. OS와 OSJ는 비록 그 구현방법에서는 간단하지만 단순한 중계국 선택만으로는 다른 방식에 비해 보안 성능이 제한적임을 알 수 있다.

〈그림 3〉은 6개의 중계노드가 존재 할 때의 보안 전송율 비교이다. 적은 수의 선택된 중계국이 협력 빔형성에 참여하기에 OB-CSI-RS는 OB-CSI에 비하여 다소 낮은 성능을 보여준다. 또한 ECN-RS는 OB-CSI-RS와 비슷한 성능을 보인다. 그림 2의 경우와 비교해 CJ 방식이 많은 성능 향상을 보이는데 이는 5개의 중계국들의 협력 재밍을 통한 효과라 할 수 있다. 또한 그림 2에 비해 DPA-RS가 가장 큰 성능 향상을 보이는데 이는 무선 채널의 위상정보만 이용하기에 실제 시스템의 응용 가능성은 더욱 높다고 할 수 있다.

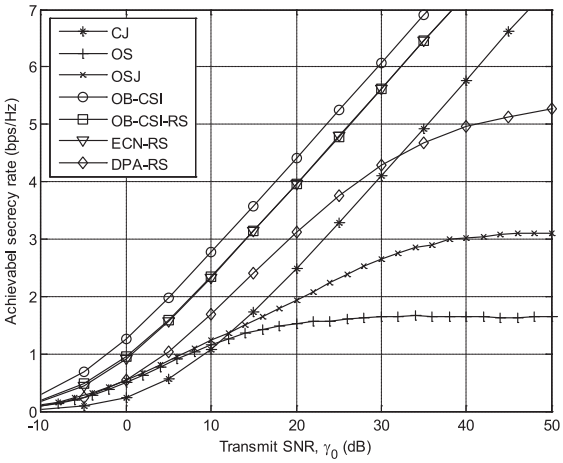

그림 3. 보안 전송율 ($M = 6,\ \rho_{rd} = \rho_{re} = 0dB$)

〈그림 4〉와 〈그림 5〉는 SR링크가 존재 할 때의 결과 그림이다. 우선 중계노드가 4개가 있고 RD 및 RE 링크의 SNR은 -3dB로 설정하였고 SR링크의 SNR은 각각 -10dB와 -30dB로 설정하였다. SR링크상의 데이터 전송률 요구를 $C_{th} = 1bps/Hz$로 설정하고 채널상황이 좋지 못하여 이 전송률을 지원하지 못할 경우 중계국들은 다음 단계에서 수신단으로 데이터 전송을 하지 못한다. SR 링크가 좋을 때 〈그림 4〉 거의 모든 중계국들이 성공적으로 데이터를 복구하여 수신단으로의 전송에 참여하므로 완벽한 SR 링크의 경우와 유사한 성능을 갖는다.

반면 SR 링크의 성능이 좋지 못할 때 〈그림 5〉에서와 같이 중계국들의 복구 실패로 인한 성능저하 현상이 현저하게 나타난다. 그러나 이러한 경우에도 협력 빔형성을 지원하는 ECN-RS, DPA-RS 및 CJ는 협력 빔형성을 하지 않는 OSJ와 OS에

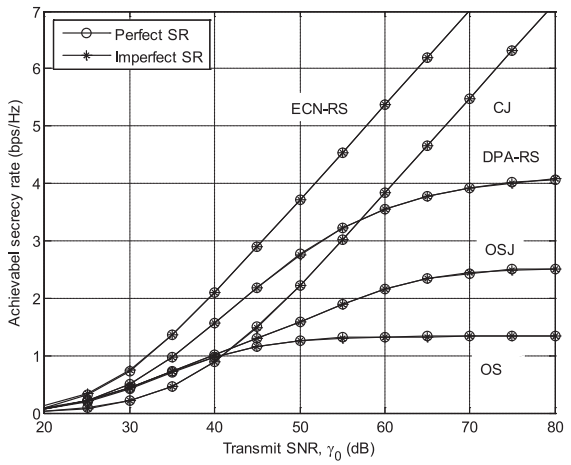

그림 4. SR링크가 존재할 때의 보안 전송율
($\rho_{rd} = \rho_{re} = -30dB,\ M = 4,\ \rho_{sr} = -10dB$)

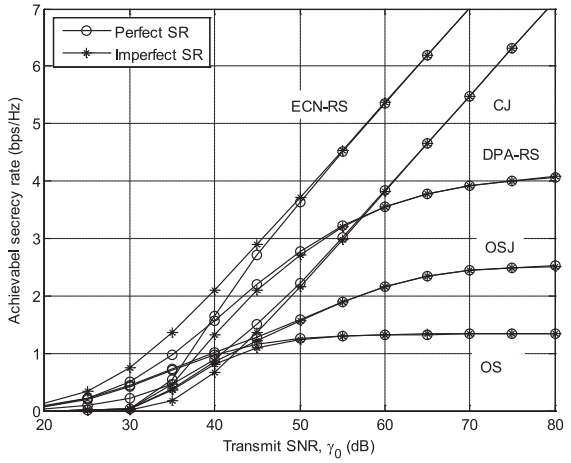

그림 5. SR링크가 존재할 때의 보안 전송율
($\rho_{rd} = \rho_{re} = -30dB,\ M = 4,\ \rho_{sr} = -30dB$)

비하여 좋은 성능을 보여준다.

물리계층 보안에 있어, 보안 전송율도 중요하지만 많은 어플리케이션에서는 최소의 보안 전송율 보장을 요구하기도 한다. 이러한 어플리케이션에 대해서는 outage가 중요한 척도로 활용된다. 즉, secrecy outage probability는 $P_{\sec-out} = \Pr\{C_S < C_{th}\}$와 같이 현재 획득한 보안 전송율이 시스템이 요구하는 보안 전송율보다 낮을 확률로 정의된다. 그림 6은 4개의 중계국이 있고 $\rho_{sr} = \rho_{rd} = \rho_{re} = -30dB$이며 최소 $C_{th} = 1bps/Hz$의 보안 전송율이 요구되는 경우의 secrecy outage probability를 보여준다. 그림에서와 같이 OB-CSI는 가장 우수한 outage 성능을 보이고 있으며 OB-CSI-RS와 ECN-RS는 유사한 outage 성능을 갖는다. 반면 OS, OSJ 및 DPA-RS는 전송 SNR이 증가하더라도 특정 outage이하로 떨어지지 않는 포화현상을 보인다.

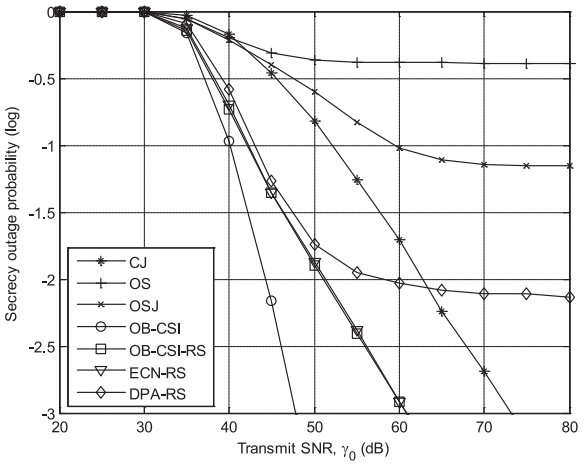

그림 6. Secrecy outage probability 비교
($\rho_{rd} = \rho_{re} = \rho_{sr} = -30dB,\ M = 4$)

Ⅲ. 결 론

본고에서는 물리계층 보안을 강화하기 위한 협력중계 기법들을 살펴보았다. 협력중계 기법은 크게 세 가지 기법, 즉 협력 재밍, 협력 빔형성 및 중계국 선택 기법으로 나눌 수 있다. 각 기술을 대표하는 7가지 물리계층 보안 기법을 살펴보았으며 동일한 환경에서 정량적인 전송 성능을 비교하였다. 비교 결과 협력에 참여하는 중계국의 수, 빔형성을 위해 사용하는 채널 정보의 양, 선택을 위한 복잡도 등에 따라 보안 전송 성능이 다양함을 확인하였다.

물리계층 보안 기술은 현재 진행의 기술로 현실화하기 위해 해결해야 할 많은 과제를 안고 있다. 그러나 무선통신에서의 보안 요구는 더 이상 미룰 수 없는 요소로 자리잡고 있어 향후 지속적인 연구를 통해 미래 이동통신 시스템을 위한 현실적이고 효율적인 물리계층 보안 기술의 개발이 절실하다.

참 고 문 헌

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

[2] A. Wyner, "Wire-tap channel," Bell Syst. Technical J., vol. 54, no. 8, pp. 1355-1387, 1975.

[3] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," IEEE Trans. Inf.

Theory, vol. 54, no. 9, pp. 4005 – 4019, Sept. 2008.
[4] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875 – 2010, Mar. 2010.
[5] G. Zheng, L.–C. Choo, and K.–K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," IEEE Trans. Signal Process., vol. 59, no. 3, pp. 1317 – 1322, Mar. 2011.
[6] J. Zhang and M. Gursoy, "Relay beamforming strategies for physical–layer security," in Proc. CISS, Mar. 2010, pp. 1 – 6.
[7] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in Proc. IEEE GLOBECOM, Dec. 2010.
[8] A. Wolf and E. A. Jorswieck, "On the zero forcing optimality for friendly jamming in MISO wiretap channels," in Proc. IEEE SPAWC, June 2010, p. 1.
[9] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," IEEE Trans. Signal Process., vol. 59, no. 1, pp. 351 – 361, Jan. 2011.
[10] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints,"IET Commun., vol. 4, no. 15, pp. 1787 – 1791, Oct. 2010.
[11] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Trans. Wireless Commun., vol. 8, no. 10, pp. 5003 – 5011, Oct. 2009.
[12] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative Beamforming for physical layer security," J. Commun. Netw., vol. 14, no. 14, Aug. 2012.
[13] G. H. Golub and C. F. V. Loan, Matrix Computations. 3rd ed., Baltimore, MD: The Johns Hopkins Univ. Press, 1996.

약 력

Hu Jin

2004년 University of Science and Technology of China 학사
2006년 한국과학기술원 공학석사
2011년 한국과학기술원 공학박사
2011년~2013년 The University of British Columbia 박사후연구원
2013년~현재 경상대학교 정보통신공학과 연구교수
관심분야: 무선통신, 물리계층보안, 랜덤엑세스네트워크, 셀룰라시스템

김 준 수

2001년 KAIST 공학사
2003년 KAIST 공학석사
2009년 KAIST 공학박사
2009년~2009년 KAIST 정보전자연구소, 연구원
2009년~2011년 University of British Columbia (UBC), 박사후연구원
2011년~현재 한국산업기술대학교, 조교수
관심분야: 무선자원관리, 협력통신, 인지무선통신, 물리계층보안