비신뢰 양방향 중계 IoT 네트워크 성능 분석

이기훈°, 정방철
충남대학교 전자공학과
kihun.h.lee@cnu.ac.kr, bcjung@cnu.ac.kr

1. 서론

사물인터넷(Internet of Thing: IoT) 네트워크는 주로 소형, 저비용, 저전력 특성을 갖는 단말을 기반으로 구성된다 [1]-[3]. 이 같은 특성을 바탕으로 [3]에서는 중계기만이 다중 안테나를 갖는 비신뢰 양방향 중계 IoT 네트워크를 고려한 물리 계층 보안 기술을 제안했다. 본 논문에서는 이와 동일한 통신 환경에서 각 IoT 단말의 통신 성능 향상을 위해, 두 번째 홉에서 잡음 제거-후-전달(Denoise-and-Forward: DF) 프로토콜 적용을 제안한다.

2. 제안하는 물리 계층 보안 기술

본 논문에서 고려하는 양방향 중계 IoT 네트워크의 시스템 모델과 첫 번째 홉에서 각 IoT 단말이 신뢰할 수 없는 중계기로 신호를 전송하는 과정은 [3]의 II와 같다. 하지만, 두 번째 홉에서는 증폭-후-전달(Amplify-and-Forward: AF) 대신 DF 프로토콜을 적용한다. 이때, 중계기는 각 IoT 단말과 동일하게 QPSK 변조기를 사용한다고 가정한다.

중계기는 첫 번째 홉에서 선형 결합한 신호 $\bar{y}_{\mathrm{R},t}$ ([3]-(4), $t \in \{1,2\}$)로부터 다음과 같은 Joint ML 검출기를 통해 잡음을 제거(denoise)한다:

$$[\hat{x}_{A,t}, \hat{x}_{B,t}] = \underset{x_{k,t}\in\mathcal{X}}{\arg\min} \left| \bar{y}_{\mathrm{R},t} - \sqrt{\frac{\gamma_{\mathrm{th}}+1}{\alpha}}\left(x_{A,t}+x_{B,t}\right)\right|^2,$$

여기서 $x_{k,t}(k \in \{A,B\})$는 IoT 단말 k가 t 번째 시간 슬롯에 전송한 QPSK 변조 신호를 나타내며, $\mathcal{X}$는 정규화된 QPSK 신호의 집합을 의미한다. 또한, γ_{th}와 α는 각각 임계 무선 채널 이득 및 이에 따른 두 IoT 단말의 전송 확률을 나타낸다 [3].

이후 중계기는 두 신호$(\hat{x}_{A,t}, \hat{x}_{B,t})$에 배타적 논리합(XOR) 연산을 수행$(x_{\mathrm{R},t} = \hat{x}_{A,t} \oplus \hat{x}_{B,t})$하고 이 결과 신호를 시공간 블록 부호(space-time block code: STBC)에 기반하여 두 IoT 단말로 전달(forward)한다. 구체적으로 중계기는 다음과 같이 각 안테나$(m \in \{1,2\})$로 두 시간 슬롯(t)에 걸쳐 신호를 광역전파한다.

	$m=1$	$m=2$
$t=1$	$x_{\mathrm{R},1}/\sqrt{2}$	$x_{\mathrm{R},2}/\sqrt{2}$
$t=2$	$-x_{\mathrm{R},2}^*/\sqrt{2}$	$x_{\mathrm{R},1}^*/\sqrt{2}$

이에 따라 IoT 단말 k로 t 번째 시간 슬롯에 수신되는 신호 $y_{k,t}$는 다음과 같이 쓸 수 있다:

$$y_{k,1} = \left(h_{k,1}x_{\mathrm{R},1} + h_{k,2}x_{\mathrm{R},2}\right)/\sqrt{2} + w_{k,1},$$
$$y_{k,2} = \left(-h_{k,1}x_{\mathrm{R},2}^* + h_{k,2}x_{\mathrm{R},1}^*\right)/\sqrt{2} + w_{k,2},$$

여기서 $h_{k,m}$은 IoT 단말 k와 중계기의 m 번째 안테나 사이 무선 채널을 나타내며, 본 논문에서 모든 채널은 서로 독립이고 $\mathcal{CN}(0,1)$의 동일한 레일리(Rayleigh) 분포를 따른다고 가정한다. 또한, $w_{k,t}$는 신호 송수신 과정에서 발생하는 열 잡음을 의미하며, 본 논문에서 모든 잡음은 $\mathcal{CN}(0,N_0)$의 분포를 따른다고 가정한다.

각 IoT 단말은 수신한 신호 $y_{k,t}$로부터 자기 채널

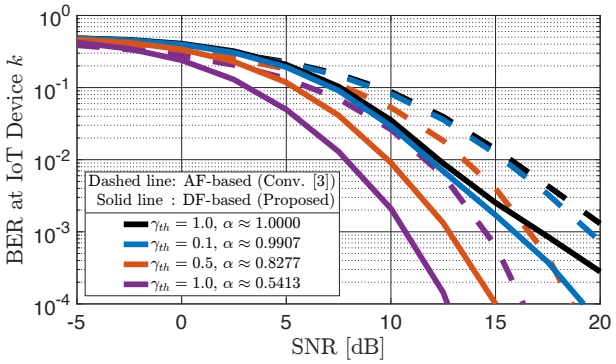

그림 1. 각 IoT 단말에서의 SNR 대비 BER 성능

정보를 통해 다음과 같이 STBC 복호화를 수행한다:

$$\begin{bmatrix}\bar{y}_{k,1}\\ \bar{y}_{k,2}^*\end{bmatrix} = \sqrt{\frac{1}{\gamma_k}}\begin{bmatrix}h_{k,1}^* & h_{k,2}\\ h_{k,2}^* & -h_{k,1}\end{bmatrix}\begin{bmatrix}y_{k,1}\\ y_{k,2}^*\end{bmatrix} = \sqrt{\frac{\gamma_k}{2}}\begin{bmatrix}x_{\mathrm{R},1}\\ x_{\mathrm{R},2}\end{bmatrix} + \begin{bmatrix}\tilde{w}_{k,1}\\ \tilde{w}_{k,2}\end{bmatrix}.$$

이후 아래와 같은 ML 검출기를 통해 중계기가 전송한 QPSK 신호를 검출한다:

$$\hat{x}_{\mathrm{R},t} = \underset{x_{\mathrm{R},t}\in\mathcal{X}}{\arg\min} \left|\bar{y}_{k,t} - x_{\mathrm{R},t}\right|^2.$$

마지막으로 각 IoT 단말은 검출한 중계기의 전송 신호와 첫 번째 홉에서 자신이 중계기로 전송한 신호를 XOR 연산$(\hat{x}_{k',t} = \hat{x}_{\mathrm{R},t} \oplus x_{k,t})$함으로써 상대 IoT 단말의 전송 신호 $\hat{x}_{k',t}$를 복호한다.

3. 모의실험 결과 및 결론

그림 1 은 본 논문에서 제안한 비신뢰 양방향 중계 네트워크를 위한 무선 암호화 기술의 신호 대 잡음비(SNR) 대비 비트 당 오류율(BER) 성능 모의실험 결과이다. 첫 번째 홉에서 [3]과 같은 과정을 통해 동작하므로 두 IoT 단말은 여전히 기밀성을 유지한 채 통신할 수 있다. 한편, 각 IoT 단말에서는 본 논문에서 제안한 잡음 제거-후-전달(DF, 실선)이 기존 증폭-후-전달(AF, 점선) 프로토콜을 적용할 때 보다 향상된 BER 성능을 보이는 것을 확인했다.

4. ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크기술 특화연구센터 사업의 일환으로 수행되었습니다. (UD190033ED)

5. 참고 문헌

[1] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas and B. Ottersten, "Energy- and cost-efficient physical layer security in the era of IoT: The role of interference," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 81-87, Apr. 2020.

[2] H. S. Jang, H. Jin, B. C. Jung and T. Q. S. Quek, "Versatile access control for massive IoT: throughput, latency, and energy efficiency," *IEEE Trans. Mobile Comput.*, vol. 19, no. 8, pp. 1,984-1,997, Aug. 2020.

[3] 배유경, 이기훈, 정방철, "비신뢰 양방향 중계 네트워크를 위한 시공간 부호기반 무선 암호화 기술," *한국통신학회 하계종합학술발표회*, pp. 1,378-1,379, Aug. 2020.