비신뢰 양방향 중계 네트워크를 위한 시공간 부호기반 무선 암호화 기술

배유경, 이기훈, 정방철
충남대학교 전자공학과
ykb1103@o.cnu.ac.kr, kihun.h.lee@cnu.ac.kr, bcjung@cnu.ac.kr

Space-Time Coded Over-The-Air Encryption for Two-Way Untrusted Relay Networks

Yoo-Kyung Bae, Ki-Hun Lee, Bang Chul Jung
Dept. of Electronics Engineering, Chungnam National University

요 약

본 논문은 각각 단일 안테나를 갖는 두 IoT 단말이 두 개의 안테나를 갖는 비신뢰적 중계기(*untrusted* relay)를 통해 서로 패킷을 주고받는 양방향 중계 IoT 네트워크에서 무선 채널의 시공간 특성을 활용한 시공간 부호기반 무선 암호화 기술(Space-Time Coded Over-The-Air Encryption: STC-OTAE)을 제안하였다. 또한, 실질적인 구현 가능성을 고려하여 두 단말의 무선 채널 이득이 임계치 이상이 될 때만 통신을 수행하는 시스템을 적용하였으며, 신호 대 잡음 비(Signal-to-Noise Ratio: SNR) 대비 비트 당 오류율(Bit-Error-Rate: BER) 성능을 모의실험하고 수학적으로 분석하였다. 결과적으로 시공간 부호화 기법과 임계 무선 채널 이득을 통해 각 IoT 단말에서의 BER 성능은 향상되면서, 이와 무관하게 신뢰할 수 없는 중계기에서의 BER 성능은 항상 25% 이상으로 열화되는 것을 확인하였다.

Ⅰ. 서론

사물인터넷(Internet-of-Things: IoT)은 4차 산업혁명의 핵심 기술 중 하나로 2021년에는 150억 개 이상의 IoT 단말이 활용될 것으로 전망됨에 따라 최근 IoT 네트워크에 관한 다양한 연구가 이루어지고 있다. 특히 IoT를 스마트 홈, 인프라 모니터링, 스마트 헬스(e-Health)와 같이 사적인 정보를 다루는 서비스에 활용이 증가하면서 보안 위협이 대두되고 있으며, 이를 위해 IoT 네트워크를 위한 보안 기술이 활발히 연구되고 있다 [1]-[4].

한편, 저전력으로 동작해야 하는 IoT 단말의 특성에 따라 중계기를 활용한 통신 시스템에 관한 연구가 이루어지고 있으며, 이와 더불어 소형으로 제작되는 IoT 단말의 특성에 따라 비교적 낮은 복잡도를 갖는 보안 기술의 적용이 요구된다. 대표적으로 무선 채널의 물리적 특성을 활용하여 보안성을 향상시키는 물리계층 보안(Physical Layer Security: PLS) 기술이 있으며, 이에 따라 양방향 중계 IoT 네트워크를 위한 PLS 기술이 활발히 연구되고 있다 [3], [4].

이 중 터미널 노드의 신호를 잠재적으로 도청할 수 있는 비신뢰적 중계기(*untrusted* relay)를 고려한 양방향 중계 네트워크의 PLS 기술이 있다. 한 예로 각 단말의 변조 신호를 무선 채널 정보를 기반으로 반전시켜 전송함으로써 중계기에서 중첩되도록 하는 기술이 있다 [3]. 이는 중계기에서 중첩되는 각 단말의 신호 성상 간 거리를 줄여 검출 성능을 열화시킴으로써 보안성을 증대시키는 기술이다. 하지만, 이를 비롯한 기존 연구는 모든 노드가 단일 안테나를 가지며, 네트워크 내 모든 채널 상태 정보를 각 노드가 알고 있는 통신 환경을 가정한다. 또한, 다중 안테나를 갖는 경우 빔포밍에 기반한 PLS 기술을 제안하지만, 이는 높은 복잡도를 가져 IoT 네트워크에 적용하기 어렵다 [4].

최근 [5]에서는 시공간 선 부호(Space-Time Line Code: STLC)를 상향링크 비직교 다중 접속 시스템에 그대로 적용하는 경우, 무선 채널에 의한 위상 왜곡이 보상되어 수신단에서 진폭만 변하는 STLC의 특성으로 인해 비트 당 오류율(Bit-Error-Rate: BER) 성능이 열화되는 것을 확인하였다. 본 논문에서는 이를 기반으로 중계기에서 신호 성상을 완전히 중첩되도록 함으로써 검출 성능을 열화시켜 보안성을 향상하는 PLS 기술을 제안한다.

구체적으로 본 논문에서는 하나의 안테나를 갖는 두 IoT 단말이 두 개의 안테나를 갖는 중계기를 통해 양방향 통신을 하는 양방향 중계 IoT 네트워크를 가정한다. 이때, 중계기는 잠재적으로 각 IoT 단말의 신호를 도청할 가능성을 가진 비신뢰적 중계기를 가정하며, 첫 번째 홉에서는 STLC를 통해 각 IoT 단말이 중계기로 신호를 전송하고 두 번째 홉에서는 시공간 블록 부호화(Space-Time Block Code: STBC)를 통해 중계기에서 각 단말로 신호를 증폭-후-전달(Amplify-and-Forward: AF)하는 시공간 부호기반 무선 암호화 기술(Space-Time Coded Over-The-Air Encryption: STC-OTAE)을 제안한다.

Ⅱ. 시공간 부호기반 무선 암호화 (STC-OTAE)

본 논문에서는 그림 1과 같이 각각 단일 안테나를 갖는 두 IoT 단말과 두 개의 안테나를 갖는 하나의 중계기가 있는 양방향 중계 IoT 네트워크를 고려한다. 여기서 두 IoT 단말 사이에는 거리나 방해물에 의해 직접 통신할 수 있는 링크가 없으며, 중계기는 중계 과정에서 잠재적으로 각 단말의 신호를 도청할 가능성을 가진 신뢰할 수 없는 중계기(*untrusted* relay)를 나타낸다.

또한, 각 IoT 단말만이 중계기의 파일럿 신호를 통해 자신과 중계기 각 안테나 사이의 무선 채널 정보 벡터 $\mathbf{h}_k = [h_{k,1}\ h_{k,2}]^T$를 알고 있는 상황을 가정한다.

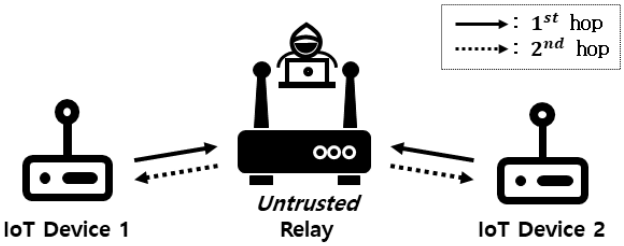

그림 1. 비신뢰 양방향 중계 IoT 네트워크 시스템 모델

여기서 $h_{k,m}$은 $k \in \{1,2\}$ 번째 IoT 단말과 중계기의 $m \in \{1,2\}$ 번째 안테나 사이 무선 채널을 나타내며, 본 논문에서 모든 무선 채널은 서로 독립이고 $\mathcal{CN}(0,1)$의 동일한 분포를 따른다고 가정한다. 모든 링크의 채널은 상호성(reciprocity)을 가지며($h_{k,m} = h_{m,k}$), 각 단말이 서로 한 프레임을 송수신하는 두 홉 동안은 변하지 않는 준-정적(quasi-static) 채널을 가정한다.

각 단말은 중계기에서 자기 신호의 기밀성을 유지하기 위해 신호 송신 과정에서 자신이 가진 채널 정보를 기반으로 변조 심벌을 반전시켜 중계기에서 신호 성상이 완전히 중첩되도록 한다. 이때, 채널 반전 과정에서 야기될 수 있는 전력 문제를 고려하여 두 IoT 단말의 무선 채널 이득 $\gamma_k = \|\mathbf{h}_k\|^2$이 모두 임계값 $\gamma_{\text{th}}\ (\geq 0)$ 이상인 경우에만 전송한다 [6]. 이는 각 단말에서 자신의 무선 채널 이득이 $\gamma_k \geq \gamma_{\text{th}}$인 경우에만 중계기로 송신 요구(Request to Send: RTS) 신호를 송신하고 중계기는 두 단말의 RTS 신호를 모두 수신했을 때에만 송신 가능(Clear to Send: CTS) 신호를 광역전파(broadcasting)함으로써 구현할 수 있다. 이때, 두 IoT 단말의 송신 확률 α은 다음과 같이 정의할 수 있다:

$$\alpha = \Pr(\gamma_1 \geq \gamma_{\text{th}}, \gamma_2 \geq \gamma_{\text{th}}) = \left(e^{-\gamma_{\text{th}}}(\gamma_{\text{th}}+1)\right)^2. \quad (1)$$

첫 번째 홉에서는 각 IoT 단말이 자신의 무선 채널 정보를 이용하여 두 quadrature phase shift keying (QPSK) 변조 심벌을 STLC 신호로 부호화한 후 전송한다. 앞서 서술한 대로 두 IoT 단말의 무선 채널 이득이 모두 $\gamma_k \geq \gamma_{\text{th}}$인 경우에만 신호를 송신하며, 중계기에서 검출할 후보 성상이 중첩되도록 다음과 같이 부호화된 신호를 전송한다:

$$s_{k,1} = \sqrt{\frac{\gamma_{\text{th}}+1}{\alpha\gamma_k}}\ \frac{h_{k,1}^* x_{k,1} + h_{k,2}^* x_{k,2}^*}{\sqrt{\gamma_k}},\ s_{k,2} = \sqrt{\frac{\gamma_{\text{th}}+1}{\alpha\gamma_k}}\ \frac{h_{k,2}^* x_{k,1}^* - h_{k,1}^* x_{k,2}}{\sqrt{\gamma_k}}, \quad (2)$$

여기서 $s_{k,t}$와 $x_{k,t}$는 k 번째 IoT 단말이 $t \in \{1,2\}$ 번째 시간 슬롯에 전송하는 신호와 k 번째 단말의 t 번째 QPSK 변조 심벌을 각각 나타낸다.

두 IoT 단말은 부호화한 신호 (2)를 두 시간 슬롯에 걸쳐 동시에 같은 반송파를 통해 전송한다. 무선 채널을 통과하여 중계기(R)의 각 안테나로 수신된 신호는 다음 행렬로 나타낼 수 있다:

$$\begin{bmatrix} y_{\text{R},1,1} & y_{\text{R},1,2} \\ y_{\text{R},2,1} & y_{\text{R},2,2} \end{bmatrix} = [\mathbf{h}_1\ \mathbf{h}_2] \begin{bmatrix} s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2} \end{bmatrix} + \begin{bmatrix} w_{\text{R},1,1} & w_{\text{R},1,2} \\ w_{\text{R},2,1} & w_{\text{R},2,2} \end{bmatrix}, \quad (3)$$

여기서 $y_{\text{R},m,t}$와 $w_{\text{R},m,t}$는 중계기의 m 번째 안테나로 t 번째 시간 슬롯에 수신한 신호와 여기에 발생하는 잡음을 각각 의미하며, 본 논문에서 모든 잡음은 $\mathcal{CN}(0,N_0)$의 분포를 따른다고 가정한다. 중계기는 네 수신 신호를 다음과 같이 선형결합한다.

$$\bar{y}_{\mathrm{R},1} = y_{\mathrm{R},1,1} + y^{*}_{\mathrm{R},2,2} = (x_{1,1}+x_{2,1})\sqrt{(\gamma_{\mathrm{th}}+1)/\alpha} + w_{\mathrm{R},1,1} + w^{*}_{\mathrm{R},2,2},$$
$$\bar{y}_{\mathrm{R},2} = y^{*}_{\mathrm{R},2,1} - y_{\mathrm{R},1,2} = (x_{1,2}+x_{2,2})\sqrt{(\gamma_{\mathrm{th}}+1)/\alpha} + w^{*}_{\mathrm{R},2,1} - w_{\mathrm{R},1,2}. \quad (4)$$

이후, 두 번째 홉에서는 중계기가 선형결합한 신호를 STBC를 이용하여 증폭-후-전달(AF) 프로토콜을 통해 광역전파한다. 구체적으로 아래와 같이 각 안테나로 두 시간 슬롯에 걸쳐 증폭된 신호를 각 단말로 전송한다.

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

(5)

여기서 $s_{\mathrm{R},t}(=\sqrt{\beta}\,\bar{y}_{\mathrm{R},t})$는 중계기의 t 번째 선형결합 신호 (4)를 $\sqrt{\beta}$ 만큼 증폭한 신호를 나타내며, 본 논문에서는 중계기의 송신 전력을 정규화하는 β를 다음과 같이 정의한다:

$$\beta = \left(\frac{2(\gamma_{\mathrm{th}}+1)}{\alpha} + 2N_0\right)^{-1}. \quad (6)$$

이에 따라 각 단말로 두 시간 슬롯 동안 수신되는 신호는 다음이 쓸 수 있다:

$$y_{k,1} = \frac{1}{\sqrt{2}}h_{k,1}s_{\mathrm{R},1} + \frac{1}{\sqrt{2}}h_{k,2}s_{\mathrm{R},2} + w_{k,1},$$
$$y_{k,2} = -\frac{1}{\sqrt{2}}h_{k,1}s^{*}_{\mathrm{R},2} + \frac{1}{\sqrt{2}}h_{k,2}s^{*}_{\mathrm{R},1} + w_{k,2}, \quad (7)$$

여기서 $y_{k,t}$와 $w_{k,t}$는 k 번째 IoT 단말이 t 번째 시간 슬롯에 수신하는 신호와 여기서 발생한 잡음을 각각 나타낸다.

각 단말은 수신된 신호 (7)에 자신의 채널 정보를 이용하여 STBC 복호화를 수행한다. 일반성을 잃지 않고, 첫 번째 IoT 단말($k=1$)에서의 이 과정은 다음 행렬로 나타낼 수 있다:

$$\bar{\mathbf{y}}_1 = \begin{bmatrix}\bar{y}_{1,1}\\ \bar{y}_{1,2}\end{bmatrix} = \sqrt{\frac{1}{\gamma_1}}\begin{bmatrix}h^{*}_{1,1} & h_{1,2}\\ h^{*}_{1,2} & -h_{1,1}\end{bmatrix}\begin{bmatrix}y_{1,1}\\ y^{*}_{1,2}\end{bmatrix} \quad (8)$$
$$= \sqrt{\frac{\gamma_1}{2}}\left(\sqrt{\frac{\beta(\gamma_{\mathrm{th}}+1)}{\alpha}}\begin{bmatrix}x_{1,1}+x_{2,1}\\ x_{1,2}+x_{2,2}\end{bmatrix} + \sqrt{\beta}\begin{bmatrix}w_{\mathrm{R},1,1}+w^{*}_{\mathrm{R},2,2}\\ w^{*}_{\mathrm{R},2,1}-w_{\mathrm{R},1,2}\end{bmatrix}\right) + \begin{bmatrix}\tilde{w}_{1,1}\\ \tilde{w}_{1,2}\end{bmatrix}.$$

마지막으로 위 신호로부터 α, β, γ_{th}, 및 γ_1을 고려하여 자기 신호를 제거(cancellation)한 후 Maximum Likelihood (ML) 검출기를 통해 상대 IoT 단말($k=2$)이 전송한 신호를 복호한다:

$$\hat{x}_{2,t} = \arg\min_{x_{2,t}\in\mathcal{X}} |r_{1,t} - x_{2,t}|^2, \quad (9)$$

여기서 $r_{1,t}(=\bar{y}_{1,t} - \sqrt{\gamma_1\beta(\gamma_{\mathrm{th}}+1)/2\alpha}\,x_{1,t})$는 첫 번째 IoT 단말의 t 번째 STBC 복호 신호에서 자신이 전송한 QPSK 심벌을 제거한 신호를 나타내며, $\mathcal{X}$는 정규화된 QPSK 변조 심벌의 집합을 의미한다. 두 번째 IoT 단말 또한 위와 같은 과정을 통해 첫 번째 IoT 단말이 전송한 신호를 복호할 수 있다.

한편, 중계기는 수신된 두 IoT 단말의 중첩 신호 (4)로부터 에너지 검출 방법을 통해 각 단말 신호의 수신 전력 $\sqrt{(\gamma_{\mathrm{th}}+1)/\alpha}$ 을 추정할 수 있으며, 이를 기반으로 아래와 같이 Joint ML 검출기를 통해 각 단말의 신호를 복호함으로써 도청자로 동작할 수 있다:

$$[\hat{x}_{1,t}\ \hat{x}_{2,t}] = \arg\min_{x_{k,t}\in\mathcal{X}} \left|\bar{y}_{\mathrm{R},t} - (x_{1,t}+x_{2,t})\sqrt{(\gamma_{\mathrm{th}}+1)/\alpha}\right|^2. \quad (10)$$

Ⅲ. BER 성능 분석

본 논문에서 제안한 양방향 중계 IoT 시스템에서 각 IoT 단말의 평균 BER 성능을 다음과 같이 수학적으로 분석하였다.

$$P_b^{(k)} \approx \left[\frac{2\sqrt{N_0}}{(16N_0+1)\sqrt{\pi}}\left[\sqrt{A}e^{-\left(A+\frac{A}{16N_0}\right)} - \sqrt{\gamma_{\mathrm{th}}}e^{-\left(\gamma_{\mathrm{th}}+\frac{\gamma_{\mathrm{th}}}{16N_0}\right)}\right]\right.$$
$$-\frac{24N_0+1}{2(16N_0+1)^{3/2}}\left[\mathrm{erf}\left(\sqrt{A+\frac{A}{16N_0}}\right) - \mathrm{erf}\left(\sqrt{\gamma_{\mathrm{th}}+\frac{\gamma_{\mathrm{th}}}{16N_0}}\right)\right]$$
$$-\left[\frac{A+1}{2}\mathrm{erfc}\left(\sqrt{\frac{A}{16N_0}}\right)e^{-A} - \frac{\gamma_{\mathrm{th}}+1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma_{\mathrm{th}}}{16N_0}}\right)e^{-\gamma_{\mathrm{th}}}\right]$$
$$\left.+\frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{A}{16N_0}}\right)(A+1)e^{-A}\right]\frac{e^{\gamma_{\mathrm{th}}}}{\gamma_{\mathrm{th}}+1}, \quad (11)$$

여기서 $k\in\{1,2\}$이고, $A=2(\gamma_{\mathrm{th}}+1)/\alpha$이다.

또한, 신뢰할 수 없는 중계기에서의 평균 BER 성능은 아래와 같다.

$$P_b^{(\mathrm{R})} \geq \frac{1}{4}\left(1+\frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma_{\mathrm{th}}+1}{4\alpha N_0}}\right)\right). \quad (12)$$

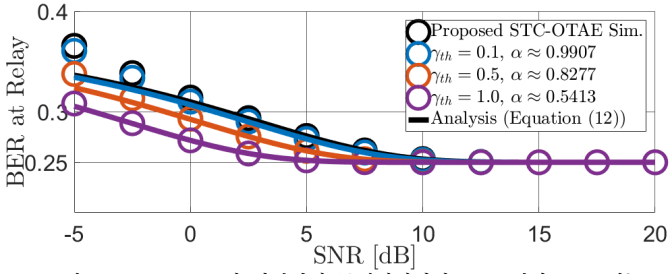

그림 2. STC-OTAE의 비신뢰적 중계기에서의 SNR 대비 BER 성능

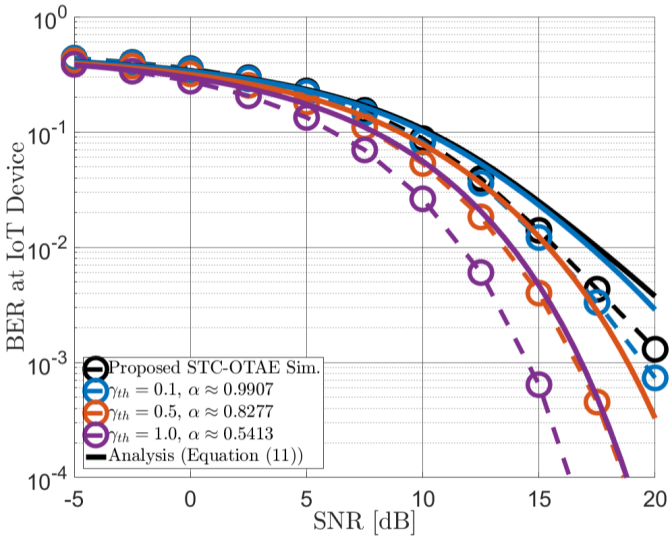

그림 3. STC-OTAE의 IoT 단말에서의 SNR 대비 BER 성능

Ⅳ. 모의실험 결과 및 결론

그림 2와 3은 본 논문에서 제안한 비신뢰 양방향 중계 네트워크를 위한 시공간 부호기반 무선 암호화 기술(STC-OTAE)의 중계기(그림 2)와 각 IoT 단말(그림 3)에서의 신호 대 잡음 비(Signal-to-Noise Ratio: SNR) 대비 평균 BER 성능 모의실험(○, Θ) 및 성능 분석(—) 결과를 각각 나타낸다. 이로부터 Ⅲ에서 수행한 수학적 성능 분석 결과((11), (12))를 검증하였으며, 임계 무선 채널 이득(γ_{th})이 높아짐에 따라 전송 확률(α)은 줄어들지만, IoT 단말 간에 높은 신뢰성(reliability)을 갖는 통신이 가능한 것을 확인하였다. 한편, 이와는 무관하게 중계기에서의 BER 성능은 항상 25% 이상으로 열화되므로 기밀성을 유지하면서 중계 시스템을 활용해 통신할 수 있음을 확인하였다. 또한, 본 논문에서는 채널 반전 과정에서 발생할 수 있는 IoT 단말의 송신 전력 문제를 γ_{th}를 적용함으로써 해결하였으며, 종래 기법들과 다르게 각 단말 노드만 무선 채널 정보를 갖고 있어도 충분하므로 더욱 실질적인 구현 가능성을 가지면서 낮은 복잡도를 갖는 PLS 기술임을 시사한다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (2020-0-00144-001, 제조 현장의 무선 연결성 한계 극복을 위한 산업용 비면허대역 무선 IoT 네트워크 핵심기술 개발)

참 고 문 헌

[1] I. Bang and B. C. Jung, "Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers," *IEEE Access*, vol. 7, pp. 127078-127089, Sept. 2019.

[2] J. Choi, J. Joung, and B. C. Jung, "Space-time line code for enhancing physical layer security of multiuser MIMO uplink transmission," *IEEE Syst. J.*, pp. 1-12, Jun. 2020 (early access).

[3] H. Xu and L. Sun, "Encryption over the air: Securing two-way untrusted relaying systems through constellation overlapping," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8268-8282, Dec. 2018.

[4] 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.

[5] K. -H. Lee, J. S. Yeom, B. C. Jung, and J. Joung, "A novel non-orthogonal multiple access with space-time line codes for massive IoT networks," *IEEE VTC2019-Fall*, Honolulu, HI, USA, pp. 1-5, Sept. 2019.

[6] B. C. Jung, J. S. Yoo, and W. Lee, "A practical physical-layer network coding with spatial modulation in two-way relay networks," *The Computer Journal*, vol. 61, no. 2, pp. 264-272, Feb. 2018.