JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 12 : 2213~2218 Dec. 2016

네트워크 보안을 위한 중계기 선택 기법

이병수 · 성길영 · 반태원*

A Relay Selection Scheme for Network Security

Byeong Su Lee · Kil-Young Sung · Tae-Won Ban*

Department of Information and Communication, Gyeongsang National University, jinju 52828, Korea

요 약

본 논문은 복수 개의 중계기와 도청자가 존재하는 중계기 통신 네트워크에서 보안 오류 확률을 낮출 수 있는 새로운 중계기 선택 기법을 제안한다. 도청자의 복호 확률을 낮추기 위해서 데이터와 함께 재밍 신호를 전송하는 기존의 중계기 선택 방식에서는 수신자의 데이터 복호 확률도 낮아지는 문제점이 있었다. 본 논문에서 제안하는 새로운 중계기 선택 기법은 수신자의 복호 확률을 높이면서 동시에 도청자의 복호 확률을 낮출 수 있는 중계기를 쌍으로 선택하여 보안 오류 확률을 개선하였다. Monte-Carlo 기반 컴퓨터 시뮬레이션을 통한 성능 분석 결과에 따르면, 제안 중계기 선택 방식은 기존 중계기 선택 방식 대비 보안 오류 확률을 약 10~50배 개선시킬 수 있음을 확인하였다.

ABSTRACT

In this paper, we propose a new relay selection scheme which can decrease the secrecy outage probability in a relay communication network with multiple relays and an eavesdropper. In the conventional relay selection scheme, a relay transmits jamming signal toward an eavesdropper to decrease the successful decoding probability of the eavesdropper. The coventional scheme has a critical problem that the successful decoding probability of a receiver also decreases. The new relay selection scheme proposed in this paper can significantly enhance the secrecy outage probability by selecting a pair of relays which can increase the successful decoding probability of the receiver while decreasing the successful decoding probability of the eavesdropper. We performed extensive computer simulation based on Monte-Carlo. The simulation results reveal that the proposed relay selection scheme can improve the secrecy outage probability by 10 to 50 times compared to the existing relay selection scheme.

키워드 : 중계기 네트워크, 중계기 선택, 보안 전송률, 보안 오류 확률

Key word : Relay network, relay selection, secrecy rate, secrecy outage probability

Received 28 September 2016, **Revised** 29 September 2016, **Accepted** 07 October 2016

* **Corresponding Author** Tae-Won Ban(E-mail:twban35@gnu.ac.kr, Tel:+82-55-772-9177)
Department of Information and Communication, Gyeongsang National University, jinju 52828, Korea

Open Access http://doi.org/10.6109/jkiice.2016.20.12.2213 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근, 고품질의 이동통신서비스에 대한 요구가 증가하고 있다. 이러한 요구를 수용하기 위해 통신 사업자들이 전파 사각 지역에 기지국을 증설하기에는 막대한 비용이 필요하므로, 중계기 통신(Relay Communication)에 대한 관심이 높아지고 있다. 이러한 중계기 통신에서는 전송된 신호를 누구든 수신할 수 있는 무선 통신의 개방성으로 인해 통신의 보안 문제가 심각하게 대두되고 있으며[1], 이러한 보안 문제를 원천적으로 해결하기 위해 물리 계층 보안(Physical Layer Security) 기술에 대한 연구가 활발하게 진행되고 있다[2-5]. 복수의 중계기와 도청자가 존재하는 중계기 네트워크에서 도청자로부터 정보를 안전하게 보호하기 위해 중계기들과 도청자 사이의 채널 상황을 고려하여 도청이 불가능한 중계기를 선택하여 정보를 전달하는 방식이 제안되었다[2,3]. 그리고, 송신자로부터 전송받은 데이터를 성공적으로 복호한 모든 중계기를 데이터 전송에 사용하는 다중 중계기 선택 방식의 SRT(Security-Reliability Trade-off)에 대한 연구가 진행되었다[4]. 이와 달리, 도청자가 존재하는 양방향(Two-Way) 중계기 네트워크에서 데이터를 전송하기 위해서 두 송신자로부터 수신되는 각각의 SINR(Signal-to-Interference-plus-Noise Ratio)의 곱이 가장 큰 중계기를 선택하고, 그 외 나머지 중계기들은 임의의 메시지를 전송하여 도청자에게 간섭을 일으키는 방식이 제안되었다[5].

최근에는 복수 개의 중계기가 존재하는 협력 통신(Cooperative Communication) 네트워크에서 중계기가 의도적인 재밍(Jamming) 신호를 전송하여 도청자의 데이터 복호를 방해하는 중계기 선택 방식들이 제안되었다[6-8]. [6]에서는 수신자에게 데이터를 전송하는 중계기와 도청자에게 재밍 신호를 전송하는 중계기를 동시에 선택하여 신호를 전송하는 중계기 쌍 선택 방식이 제안되었다. 이와 달리, [7]에서는 첫 번째 단계(1^{st} Phase)와 두 번째 단계(2^{nd} Phase)에서 데이터를 송·수신하는 중계기는 동일하지만, 각 단계 별로 재밍 신호를 전송하는 중계기를 다르게 선택하는 기법이 제안되었다. [8]에서는 [7]에서 제안된 중계기 선택 방식을 도청자가 존재하는 양방향 중계기 네트워크로 확장하였다.

이렇게 데이터를 전송하는 중계기 외에 재밍 신호를 전송하는 중계기를 동시에 선택하여 신호를 전송하는 기존의 중계기 선택 방식들은 도청자의 데이터 복호 확률을 감소시키지만, 재밍 신호로 인해 수신자의 데이터 복호 확률 또한 감소시킨다. 따라서, 본 논문에서는 재밍 신호를 전송하는 중계기 대신 동일한 데이터 신호를 전송하는 중계기 쌍을 선택하여 수신자의 데이터 복호 확률을 증가시킴과 동시에 도청자의 데이터 복호 확률은 감소시킬 수 있는 새로운 중계기 선택 기법을 제안한다.

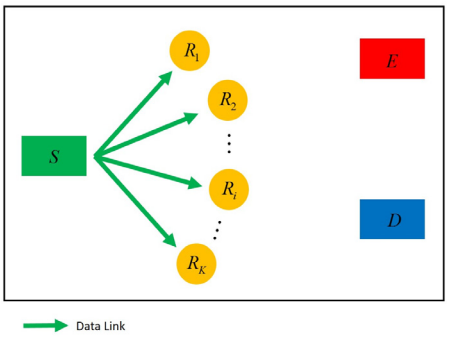
본 논문은 다음과 같이 구성된다. 2장에서는 시스템 모델을 설명하고, 3장에서는 제안하는 중계기 선택 방식을 구체적으로 기술한다. 4장에서는 컴퓨터 시뮬레이션 결과를 설명하고, 5장에서 결론을 제시한다.

Ⅱ. 시스템 모델

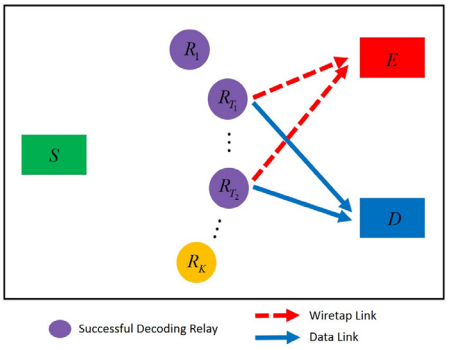
본 논문에서는 그림 1과 같이 하나의 송신자 (Source: S)와 수신자 (Destination: D), 도청자 (Eavesdropper: E), 그리고 K개의 Decode-and-Forward (DF) 기반 중계기가 존재하는 네트워크를 고려한다. 네트워크에 존재하는 K개의 중계기를 포함하는 집합은 $\boldsymbol{R}_{\mathcal{E}} = \{R_1, R_2, ..., R_K\}$로 표현된다. 송신자와 수신자, 도청자 및 중계기들은 각각 한 개의 안테나를 가지고 있으며, 송신자와 수신자 그리고 송신자와 도청자 사이에는 직접적인 통신경로는 없다고 가정한다.

데이터 전송은 송신자에서 중계기로, 중계기에서 수신자로, 총 두 단계에 걸쳐 이루어진다. 첫 번째 단계에서는 송신자가 네트워크 내 존재하는 모든 중계기들을 향해 데이터를 전송하고, 중계기들은 전송받은 데이터의 복호 여부를 판단한다. 데이터 복호에 성공한 중계기들은 복호 집합에 포함되고, 이들은 다음 단계에서 수신자에게 데이터를 전송할 수 있는 후보가 된다. 두 번째 단계에서는 중계기 선택 방식에 의해 선택된 중계기가 수신자에게 데이터 또는 재밍 신호를 전송한다. 이 단계에서 도청자가 중계기에서 수신자로 전달되는 신호를 도청할 수 있다.

송신자가 전송한 데이터를 성공적으로 복호하기 위해 필요한 채널 전송률을 γ_0, 데이터를 도청당하지 않고 안전하게 전송할 수 있는 보안 전송률 (Secrecy rate)을 γ_S라고 정의한다.



(a) 1st Phase



(b) 2nd Phase

Fig. 1 System model

모든 송신전력은 P이며, $h_{a,b}$는 a가 b로 전송할 때의 채널 지수 (Channel coefficient)이며, $a \in (\{S\} \cup \boldsymbol{R}_\Xi)$이고, $b \in (\boldsymbol{R}_\Xi \cup \{D, E\})$이다. 모든 채널 지수들은 평균이 0이고 분산이 1인 복소 정규분포~$CN(0,1)$를 따른다. 채널 이득은 $g_{a,b} = P|h_{a,b}|^2$으로 나타낼 수 있다. 그리고 n은 AWGN(Additive White Gaussian Noise)을 나타내며 평균은 0이고, 분산은 1이다.

Ⅲ. 중계기 선택 방식

3.1. 기존 중계기 선택 방식

3.1.1. Optimal Selection (OS) [2]

OS 방식은 첫 번째 단계에서 다음과 같이 송신자로부터 전송된 신호를 성공적으로 복호한 중계기를 복호 집합($\boldsymbol{R}_N$)에 포함시킨다.

$$\boldsymbol{R}_N \in \left\{ R_i \mid \frac{1}{2} log_2\left(1+g_{S,R_i}\right) \geq \gamma_0, 1 \leq i \leq K \right\} \quad (1)$$

두 번째 단계에서, $\boldsymbol{R}_N$에 속한 중계기 중 다음과 같이 수신자와의 채널 이득 대 도청자와의 채널 이득 비율이 최대가 되는 하나의 중계기만을 선택한다.

$$R^* = \underset{R_q \in \boldsymbol{R}_N}{\arg\max} \left\{ \frac{g_{R_q,D}}{g_{R_q,E}} \right\} \quad (2)$$

이때, 보안 용량은 다음과 같이 정의되며

$$C_{OS} = \left[\frac{1}{2}\log_2\left(1+g_{R^*,D}\right) - \frac{1}{2}\log_2\left(1+g_{R^*,E}\right) \right]^+, \quad (3)$$

주어진 보안 용량에 대한 보안 오류 확률은 다음과 같이 정의된다.

$$S_{OS} = \Pr\{C_{OS} < \gamma_S\}. \quad (4)$$

이때, (3)에서 $[x]^+ = \max\{0, x\}$을 나타낸다.

3.1.2. Optimal Selection with Jamming (OSJ) [6]

OSJ 방식은 복수 개의 중계기가 존재하는 중계 시스템에서 수신자를 향해서 데이터를 전송하는 중계기(R)와, 도청자의 도청을 방해하기 위해서 데이터와 전혀 무관한 재밍 신호를 전송하는 중계기(J)를 쌍으로 선택한다. 데이터 전송용 중계기R과 재밍 신호 전송용 중계기 J가 선택되었을 때 보안 전송 용량은 다음과 같이 정의된다.

$$C_{OSJ}(R,J) = \frac{1}{2}\log_2\left(\frac{1+\frac{g_{R,D}}{1+g_{J,D}}}{1+\frac{g_{R,E}}{1+g_{J,E}}} \right) \quad (5)$$

OSJ 방식은 다음과 같이 보안 전송 용량을 최대화시킬 수 있는 R과 J를 선택한다.

$$(R^*, J^*) = \underset{\substack{R \in \boldsymbol{R}_N \\ J \in \boldsymbol{R}_\Xi - \{R\} \\ R \neq J}}{\arg\max} \{C_{OSJ}(R,J)\} \quad (6)$$

R^*는 $\boldsymbol{R}_N$에 속한 중계기들 중에서 선택되고, J^*는 전체 중계기 집합 $\boldsymbol{R}_\Xi$중에서 R^*을 제외한 나머지 중계기들 중에서 선택된다. 그리고, 이에 따른 보안 오류 확

률은 다음과 같다.

$$S_{OSJ} = \Pr\left\{C_{OSJ}(R^*, J^*) < \gamma_S\right\} \quad (7)$$

OSJ 방식은 J^*가 전송하는 재밍 신호가 도청자의 도청을 방해하는 반면, 이 재밍 신호가 수신자에게도 전달되기 때문에 수신자 또한 데이터를 복호하는데 어려움을 겪게 된다.

3.2. 제안하는 중계기 선택 방식

본 절에서는 제안하는 새로운 방식의 중계기 선택 기법을 기술한다. 제안 방식에서는 OSJ 방식과 동일하게 복호 중계기 집합 $\boldsymbol{R}_N$에서 수신자를 향해 데이터를 전송할 중계기 R을 선택한다. 그러나, OSJ 방식에서는 도청자의 도청을 방해하기 위해서 전체 중계기 집합 $\boldsymbol{R}_E$에서 재밍 신호를 전송하는 중계기 (J)를 선택하는 반면, 제안 방식에서는 복호 중계기 집합 $\boldsymbol{R}_N$에서 도청자의 복호 확률을 낮추면서 수신자의 복호 확률을 높일 수 있는 중계기 (H)를 선택한다. 이때, 제안 방식의 두 번째 단계에서 수신자와 도청자가 수신하는 신호는 각각 다음과 같이 주어지며,

$$y_D = \sqrt{P}\left(h_{R_{T_1},D} + h_{R_{T_2},D}\right)x + n \quad (8)$$

$$y_E = \sqrt{P}\left(h_{R_{T_1},E} + h_{R_{T_2},E}\right)x + n \quad (9)$$

보안 용량은 아래와 같이 정의할 수 있다.

$$C_{prop}(R,H) = \frac{1}{2}\log_2\left\{\frac{1+P|h_{R,D}+h_{H,D}|^2}{1+P|h_{R,E}+h_{H,E}|^2}\right\} \quad (10)$$

제안방식에서는 다음과 같이 (10)의 보안용량 값을 최대화하기 위한 (R,H) 조합을 다음과 같이 선택한다.

$$\begin{aligned}(R^*,H^*) &= \underset{\substack{R,H\in\boldsymbol{R}_N \\ R\neq H}}{\arg\max}\, C_{prop}(R,H) \quad (11)\\ &= \underset{\substack{R,H\in\boldsymbol{R}_N \\ R\neq H}}{\arg\max}\left\{\frac{1+|h_{R,D}+h_{H,D}|^2}{1+|h_{R,E}+h_{H,E}|^2}\right\}\end{aligned}$$

이에 따른 제안 방식의 보안 오류 확률은 아래와 같이 정의된다.

$$S_{prop} = \Pr\left\{C_{prop}(R^*,H^*) < \gamma_S\right\} \quad (12)$$

Ⅳ. 시뮬레이션 결과

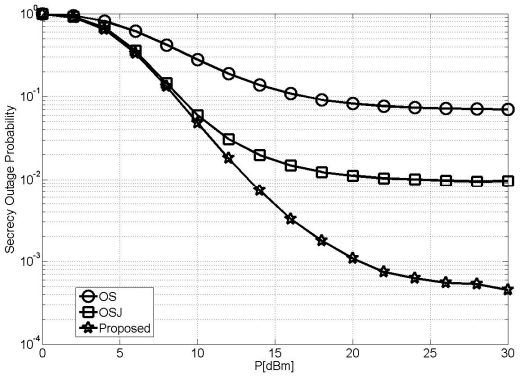


Fig. 2 Secrecy outage probability when $K=12$, $\gamma_0=1$, and $\gamma_S=1$.

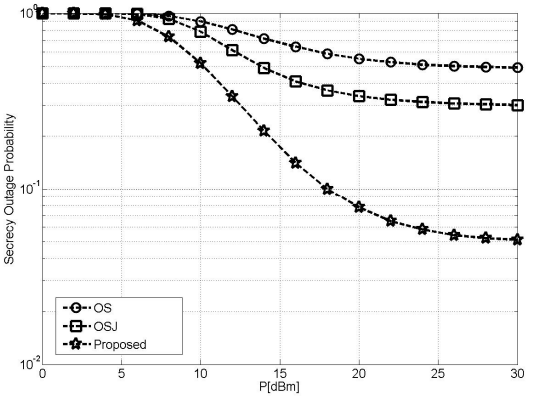


Fig. 3 Secrecy outage probability when $K=12$, $\gamma_0=1$, and $\gamma_S=2$.

본 절에서는 컴퓨터 시뮬레이션을 통해서 제안하는 중계기 선택 방식의 성능을 보안 오류 확률 측면에서 분석하고, 이를 기존의 OS와 OSJ 방식의 성능과 비교한다. 그림 2는 중계기의 수가 $12(K=12)$이고 데이터 전송률이 $1(\gamma_0=1)$이고, 보안 전송률이 $1(\gamma_S=1)$일 때, 각 중계기 선택 기법에 대한 보안 오류 확률을 나타낸다. 그림 2에서 볼 수 있듯이 송신 전력이 낮을 때에는 기존 방식들과 제안 방식의 성능이 비슷하지만, 송신 전력이 증가할수록 기존 방식 대비 제안 방식의 성능이 우수해짐을 알 수 있다. 구체적으로, 송신 전력이

30dBm 일 경우, 제안 방식의 보안 오류 확률은 OS와 OSJ 방식 대비 각각 약 10배와 50배 우수함을 확인할 수 있다. 그림 3은 중계기의 수가 12($K=12$)이고, 데이터 전송률이 1이고, 보안 전송률이 2($\gamma_S=2$)일 때, 각 중계기 선택 기법에 대한 성능을 보여준다. 보안 조건을 강화하기 위해서 보안 전송률을 증가시키더라도 제안하는 중계기 선택 방식이 기존의 중계기 선택방식에 비해 더 우수한 보안 오류 확률을 나타낸다.

Ⅴ. 결 론

본 논문에서는 복수 개의 중계기와 도청자가 존재하는 협력 통신 네트워크에서 보안 오류 확률을 낮출 수 있는 새로운 중계기 선택 기법을 제안하였다. 제안하는 방식은 송신자가 전송된 데이터를 성공적으로 복호한 중계기 중에서 한 쌍의 중계기를 선택함으로써 수신자의 복호 확률은 높이면서 도청자의 도청 확률은 낮출 수 있다. 컴퓨터 시뮬레이션을 통하여 제안 방식의 성능을 보안 오류 확률 측면에서 분석하였으며, 이를 기존의 OS와 OSJ 기법의 성능과 비교하였다. 성능 분석 결과에 따르면, 제안하는 중계기 선택 방식이 기존의 OS와 OSJ 방식 대비 보안 오류 확률 측면에서 우수한 성능을 보임을 확인하였다.

ACKNOWLEDGMENTS

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.B0101-16-1272, Development of Device Collaborative Giga-Level Smart Cloudlet Technology)

REFERENCES

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless Information-Theoretic Security,” *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[2] I. Krikidis, “Opportunistic relay selection for cooperative networks with secrecy constraints,” *IET Communications*, vol. 4, no. 15, pp. 1789-1791, Oct. 2010.

[3] B. V. Nguyen, K. Kim, “Secrecy outage probability of optimal relay selection for secure AnF cooperative networks,” *IEEE Communications Letter*, vol. 19, no. 12, pp. 2086-2089, Oct. 2015.

[5] J. Xiong, D. Ma, C. Liu, X. Wang, “Secure communications for two-way relay networks via relay chatting,” *Communications and Network*, vol. 5, no. 3C, pp. 42-47, Sep. 2013.

[4] J. Zhu, Y. Zou, B. Champagne, W. Zhu, and L. Hanzo, “Security-reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems,” *IEEE Trans. on Vehicular Technology*, vol. 65, no. 7, pp. 5825-5831, July. 2015.

[6] I. Krikidis, J. S. Thompson, S. Mclaughlin, “Relay selection for secure cooperative networks with jamming,” *IEEE Trans. on Wireless Communications*, vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

[7] W. Liu, D. Tan, G. Xu, “Low complexity power allocation and joint relay-jammer selection in cooperative jamming DF relay wireless secure networks,” 2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID), pp. 1-5, Oct. 2013.

[8] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, “Joint relay and jammer selection for secure two-way relay networks,” *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012.

이병수(Byeong Su Lee)

2012년 2월 경상대학교 정보통신공학과 학사
2012년 3월 ~ 현재 경상대학교 정보통신공학과 석박사통합과정
※관심분야 : 이동통신, 협력 및 중계통신, 전이중 통신

성길영(Kil-Young Sung)

1980년 2월 경북대학교 전자공학과 학사
1985년 2월 건국대학교 전자공학과 석사
2000년 2월 부경대학교 전자공학과 박사
현재 경상대학교 정보통신공학과 교수
※관심분야 : VLSI array, Computer architecture, Image compression

반태원(Tae-Won Ban)

1998년 2월 경북대학교 전자공학과 학사
2000년 2월 경북대학교 전자공학과 석사
2010년 2월 KAIST 전기전자공학과 박사
2000년 2월 ~ 2012년 8월 KT 네트워크부문
2012년 9월 ~ 현재 경상대학교 정보통신공학과 조교수
※관심분야 : 이동통신, 자원관리, 간섭관리, 협력 및 중계통신, 인지통신, 주파수 공유