The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 6, pp.63-67, Dec. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.6.63
JIIBC 2014-6-10

물리 계층에서 보안 재밍 신호 공유의 한계점과 이진 재밍 메시지 도청의 해결책

A Solution of Binary Jamming Message to Source-Wiretapping and Disadvantage of Sharing the Jamming Signal in Physical-Layer Security

공형윤*

Hyung-Yun Kong*

요 약 협력 재밍 기술에 기반한 분산 제로 빔포밍은 도청자가 시드 공유를 감지 할 수 없으며, 도청자가 도청하기 위해 송신단 주변에 위치한 경우 기존의 기법은 제한적으로 적용된다. 따라서 본 논문에서는 이러한 특수한 시나리오에 대한 해결책을 제시한다. 첫 번째 시간 슬롯에서 중계기는 이진 재밍 메시지를 무작위로 생성하고 송신단과 수신단으로 전송한다. 두 수신기가 안전하고 정확하게 메시지를 복호할 때, 송신단은 정보 메시지와 복호된 메시지에 대한 배타적 논리합 기법을 기반으로 다른 메시지를 만들고 전송하게 되며 도청 노드에 의한 도청을 방지할 수 있다. 마지막으로 본 프로토콜을 기존의 기법과 비교하여 성능을 분석하였으며 도청 노드의 위치에 따른 결과가 우수함을 확인하였다.

Abstract A distributed zero-beamforming based cooperative jamming technique is useless when an eavesdropper detects the sharing seed. In addition, the currently alternatives are very limited when the eavesdropper is located nearby a source for wiretapping. This letter presents a solution to this extreme case. Relay randomly generates and transmits a binary jamming message to both source and destination in the first phase. When these two receivers securely and correctly decode the message, the source creates and transmits another message based on the use of exclusive-or for its information message and the decoded message. Consequently, the next transmission can avoid the eavesdropping.

Key Words : Binary Jamming, Physical Layer Security, Half Duplex Network, Distributed Zero Beamforming

Ⅰ. 서 론

최근, 사용되는 네트워크의 높은 밀도 때문에 무선 통신의 보안이 중요한 문제가 되어 물리 계층 보안에 관한 연구가 최근 활발히 진행되고 있다[1-6]. 물리 계층 보안은 암호화 기법과 비교할 경우, 도청자가 사용하는 복호 기법에 관계없이 안전하게 전송 할 수 있다는 이점을 갖는다. 협력 재밍 기법은 물리 계층 보안에 일반적으로 사용

*정회원, 울산대학교 전기전자정보시스템공학부(교신저자)
접수일자: 2014년 8월 19일, 수정일자: 2014년 10월 10일
게재확정일자: 2014년 12월 12일

Received: 19 August, 2014 / Revised: 10 October, 2014
Accepted: 12 December, 2014
*Corresponding Author: hkong@ulsan.ac.kr
School of Electrical Engineering, University of Ulsan, Korea

되는 기법 중 하나이다. 단일 안테나를 가진 반이중 네트워크에 적용된 협력 재밍 기법은 도청자의 방해 전파로 인한 간섭을 회피하기위해 분산형 제로 빔포밍 기법을 사용한다[3]. 그러나 방해 전파는 특정 제어 채널을 사용할 수 있으며, 이 경우 유사한 방해 전파 신호를 만들기 위해 방해 시드와 공통 시드를 공유할 수 있다. 그러나 공유된 시드는 제어 메시지 전송을 들을 수 있는 강력한 도청자를 감지하기 어렵다. 이와 같은 특수한 경우, 분산 제로 빔포밍 기반의 협력 재밍은 보안이 취약하게 되므로 사용할 수 없다[3]. 협력 재밍에 대한 현재 대부분의 연구는 많은 중계기들이 원본 메시지를 검출하기 위해 중계기 전송으로부터 도청되지 않는다는 가정을 기반으로 하기 때문에 수신단에 대한 다이버시티의 사용을 허용했다[1-2]. 그러나 위와 같은 경우, 도청자가 송신단의 전송을 도청하기 위해 가까운 곳에 위치할 경우 복호 성능이 제한되며, 이와 같은 단점을 보안하기 위해 본 논문에서는 새로운 재밍 기법을 제안한다.

따라서 본 논문에서는 새로운 재밍 기법을 제안하였다. 제안된 기법은 도청 노드와 전송 노드는 시드로 공유되지 않는다. 또한 이진 전송 메시지와 임의적으로 생성되는 이진 재밍 메시지 사이에 배타적 논리 연산을 적용한다. 따라서 메시지는 도청에 관계없이 송신단에서 수신단까지 전송할 수 있다.

II. 시스템 모델

본 논문에서 제안된 시스템 모델은 그림 1에 표현하였다. 그림 1은 송신단 S와 수신단 D, 중계기 R 그리고 도청자 E로 구성되었다. 또한, h_{RS}, h_{RD}, h_{RE}, h_{SD}, h_{SE}는 각각 R-S, R-D, R-E, S-D, S-E간의 채널 상태 정보를 나타낸다. 본 논문에서 $i,j \in S,R,D,E$ 일 때, 노드 i와 j에 의해 h_{ij}를 완벽히 알 수 있다고 가정하면, 송신 요구와 송신 가능과 같은 제어 메시지의 추정 결과로 나타 낼 수 있다. 또한, 높은 우선순위를 가지는 사용자를 위한 인가되지 않은 메시지에 도청자가 접근할 경우 도청될 수 있는 네트워크의 전형적인 노드를 확인해야한다. 이 네트워크에 의해 도청자의 신원, 위치, 채널 상태 정보 등을 알 수 있다. 채널 상태 정보는 레일리 페이딩으로서 h_{RS}, h_{RD}, h_{RE}, h_{SD}, h_{SE}으로 가정된다. 또한, 평균 전력은 Ω_0, Ω_1, Ω_2, Ω_3, Ω_4로 나타낸다. 채널 상태 정보는 독립적으로 분산되었다. 본 논문에서는 i = 0, 1, 2, 3, 4에 해당하는 S-D, R-S, R-D, R-E, S-E의 거리를 d_i로 나타내었으며 그에 따른 평균 전력을 $\Omega_i = d^{-\theta_i}$으로 표현하였다. 표기된 θ는 경로 손실 지수를 나타내며 모든 노드는 단일 안테나를 가지는 반 이중 방식이다. 기존의 기법은 수신단 D에서 간섭이 발생하지 않는 동안 도청 노드 E에서 무작위로 적절한 제로 빔포밍 가중치 z를 생성하며 송신단과 중계기는 동일한 재밍 신호를 전송하는 분산형 제로 빔포밍 기법을 적용하였다[3]. 따라서 보안율이 향상된다. 동일한 임의 재밍 신호 z를 생성하기위한 시드에 대한 정보는 송신단 S와 중계기 R이 가지고 있어야한다. 따라서 송신단 S와 중계기 R은 시드의 공유를 요구한다. 실제로 도청 노드는 시드가 전송되는 공통 채널을 수신하거나 해독함으로서 시드를 쉽게 복구한다. 이 때, 시드는 노드 E가 가지게 되므로 기존의 기법은 불필요해진다[3]. 이러한 경우, [1-2]에서 제안된 기법을 대안으로 사용할 수 있다. 이 기법에서는 송신단 S에서 중계기 R 사이의 전송이 도청되지 않는다는 가정한다. 그 결과 그림 1과 같이 도청자가 송신단으로부터 도청하기 위해 의도적으로 송신단 근처에 위치한 경우, 복호 과정이 제한된다. 이러한 극단적인 경우는 반 이중 및 단일 안테나를 가지는 네트워크의 연구과제이다.

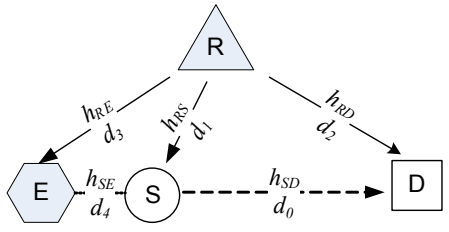

그림 1. 시스템 모델
Fig. 1. System Model

따라서 본 논문에서는 위와 같은 극단적인 모델에 대한 해결책을 제안하였다. 첫 번째 시간 슬롯에서 중계기는 u에 의해 표현되는 M_J인 임의 이진 재밍 메시지를 전송한다. u와 신호 z의 차이점은 u는 상당한 양의 이진 정보를 운반하지만 z는 그렇지 않다. 임의 메시지 M_J를 생성하기 위한 시드는 다른 노드들과 공유되지 않으며 도청 노드에 의해 검출됨으로서 보호된다. 중계기는 주변 노드에게 메시지 u를 전송하며 주변 노드는 $y_{j,1} = \sqrt{P_1} h_{Rj} u + n_{j,1}$, $j \in S,D,E$을 수신하게 된다. 여

기서 송신 전력은 P1으로 평균이 0이며 백색 가우시안 잡음은 $n_{j,1}$로 표현한다. 또한, 송신단 S가 수신단 D로 전송하고자하는 메시지를 M_S로 표기한다. 메시지 M_S와 M_J는 동일한 크기를 가지며 이 길이는 공통 메시지를 통해 중계기 R에게 전송된다. 송신단 S와 수신단 D에서 메시지 M_J를 정확하게 복호할 경우, 송신단 S는 배타적 논리합 연산 $\oplus$를 사용하여 $M_{\oplus} = M_S \oplus M_J$ 메시지를 생성한다. 여기서 메시지 $M_{\oplus}$를 나타내는 신호는 v로 표기한다. 송신단 S는 직접 전송을 통해 수신단 D에게 신호 v를 전송한다. 따라서 수신단 D는 $y_{D,2} = \sqrt{P_2} h_{SD} v + n_{D,2}$를 수신한다. 여기서, 송신 전력은 P_2이며 백색 가우시안 잡음은 $n_{D,2}$로 표현한다. 만약 수신단 D가 메시지 $M_{\oplus}$를 성공적으로 복호할 경우, $M_S = M_{\oplus} \oplus M_J$의 결과로 메시지 M_S을 추출한다. 첫 번째 시간 슬롯에서 메시지 M_J가 안정하게 전송되었기 때문에 도청 노드는 두 번째 시간 슬롯에서 메시지 $M_{\oplus}$를 성공적으로 복호하더라도 도청자는 메시지 M_S를 추출 할 수 없다. 만약 첫 번째 시간 슬롯에서 M_J가 안전하고 정확하게 복호되지 않을 경우 송신단 S는 작동하지 않는다.

다음으로 본 논문에서 제안된 기법의 아웃티지 성능을 확인한다. 이 과정에서 신호 u, v는 복소 신호로서 $E\{u\} = E\{v\} = 0$, $E|u|^2 = E|v|^2 = 1$으로 일반화한다. $C_{j,k}$는 k 번째 시간 슬롯에서 노드 j에서 수신된 신호의 달성률을 나타내며 노드간 신호대 잡음비를 $\gamma_{ij} = |h_{ij}|^2$으로 정의하여 달성률을 다음과 같이 표현할 수 있다.

$$C_{j,1} = \frac{1}{2} log(1 + P_1 \gamma_{ij}), j \in S, D, E \tag{1}$$

따라서 식 (1)을 사용하여 메시지 M_J 복호에 대한 S와 D의 보안 달성률은 각각 다음과 같다.

$$R_{S,1} = [C_{S,1} - C_{E,1}]^+ = \left[\frac{1}{2} log_2\left(\frac{1 + P_1 \gamma_{RS}}{1 + P_1 \gamma_{RE}}\right)\right]^+$$
$$R_{D,1} = [C_{D,1} - C_{E,1}]^+ = \left[\frac{1}{2} log_2\left(\frac{1 + P_1 \gamma_{RD}}{1 + P_1 \gamma_{RE}}\right)\right]^+$$
$$, [x]^+ = \max\{0, x\} \tag{2}$$

$$R_{S,1} \approx [\frac{1}{2} log_2(\frac{\gamma_{RS}}{\gamma_{RE}})]^+$$
$$R_{D,1} \approx [\frac{1}{2} log_2(\frac{\gamma_{RD}}{\gamma_{RE}})]^+, P_1 \gg 1 \tag{3}$$

식 (2), (3)에서 표현된 보안 달성률은 달성 송신률 R_t를 기준으로 한다. 송신단 S와 수신단 D에서 M_J의 안전하고 정확한 복호 조건은 다음과 같다.

$$(R_{S,1} > R_t) \cap (R_{D,1} > R_t) \tag{4}$$

식 (4)의 조건이 성립할 때, 메시지 M_S를 안전하고 정확하게 복호하기 위한 조건은 다음과 같다.

$$C_{D,2} > R_t$$
$$C_{D,2} = \frac{1}{2} log_2(1 + P_2 \gamma_{SD}) \tag{5}$$

두 번째 단계에서 M_S의 복호는 $M_{\oplus}$의 송신과 보안 메시지 M_J를 필요로하기 때문에 보안률이 달성률과 같다. 따라서 메시지M_S가 안전하게 전송되고 완벽하게 복호될 경우의 아웃티지 확률은 다음과 같다.

$$\begin{aligned} P_0 &= 1 - \Pr\left\{\begin{matrix}(R_{S,1} > R_t) \cap (R_{D,1} > R_t) \\ \cap (C_{D,2} > R_t)\end{matrix}\right\} \\ &\approx 1 - \Pr\left\{\begin{matrix}\gamma_{RS} > \gamma_{RE} \underbrace{2^{2R_t}}_{\rho}, \gamma_{RD} > \gamma_{RE} 2^{2R_t} \\ , \gamma_{SD} > \underbrace{2^{2R_t} - 1}_{P_2},\end{matrix}\right\} \\ &= 1 - \underbrace{\Pr\{\gamma_{RS} > \gamma_{RE}\rho, \gamma_{RD} > \gamma_{RE}\rho\}}_{J_1} \underbrace{\Pr\left\{\gamma_{SD} > \frac{\rho - 1}{P_2}\right\}}_{J_2} \end{aligned} \tag{6}$$

또한, $\Omega = \Omega_0, \Omega_1, \Omega_2, \Omega_3, \Omega_4$에 대한 신호대 잡음비는 각각 γ_{SD}, γ_{RS}, γ_{RD}, γ_{RE}, γ_{SE}으로 주어지며 γ_{ij}의 확률 밀도 함수는 다음과 같이 주어진다.

$$f_{\gamma ij}(x) = \frac{1}{\Omega} exp(-\frac{x}{\Omega}) \tag{7}$$

따라서 J_1과 J_2는 다음과 같이 계산된다.

$$J_1 = \int_0^\infty \left(\int_{z\rho}^\infty f_{\gamma RS}(x)dx \right) \left(\int_{z\rho}^\infty f_{\gamma RD}(y)dy \right) \times \int_{z\rho}^\infty f_{\gamma RE}(z)dz = \int_0^\infty \exp\left(-\left(\frac{\rho}{\Omega_1} + \frac{\rho}{\Omega_2} \right) z \right) \frac{1}{\Omega_4} \exp\left(\frac{z}{\Omega_4} \right) dz = \left(\Omega_4 \left(\frac{\rho}{\Omega_1} + \frac{\rho}{\Omega_2} + \frac{\rho}{\Omega_4} \right) \right)^{-1}, \; P_1 \gg 1 \quad (8)$$

$$J_2 = \int_{\frac{\rho-1}{P_2}}^\infty \frac{1}{\Omega_0} exp\left(-\frac{x}{\Omega_0} \right) dx = \exp(-\frac{\rho-1}{P_2\Omega_0}) \quad (9)$$

마지막으로 위 식 (8), (9)를 이용하여 송신 전력 P_0를 다음과 같이 구할 수 있다.

$$P_0 \approx \frac{\exp\left(\frac{\rho-1}{P_2\Omega_0} \right)}{d_4^{-v}(d_1^{-v} + d_2^{-v})\rho + 1} \quad (10)$$

Ⅲ. 모의실험 및 결과

노드 S, D, R, E의 위치는 각각 (0, 0), (d_0, 0), ($\frac{d_0}{2}$, y_1), (x_4, 0)라고 가정한다. 따라서, 각각에 대한 거리는 다음과 같이 나타낼 수 있다.

$$d_1 = \sqrt{(0.5d_0)^2 + y_1^2}$$
$$d_2 = \sqrt{(0.5d_0)^2 + y_1^2}$$
$$d_3 = \sqrt{y_1^2 + (0.5d_0 - x_4)^2}$$
$$d_4 = |x_4| \quad (11)$$

위 식 (11)과 시스템 모델에 표현된 각 값은 d_0=1, $y_1 = d_0/2$, $\theta = 5$, P_1=15(dB), P_2=20(dB), R_t =0.5(bits/s/Hz)으로 설정한다.

또한, 도청 노드가 공유될 때, 공유 시드를 알 수 있기 때문에 분산 제로 빔포밍 기반의 접근 방식을 사용할 수 없다. 따라서 본 논문에서는 제안된 기법과의 비교를 위해 두 가지 방식을 사용한다. 첫 번째, 송신단 S에서 수신단 D로의 직접 전송을 위해 중계기의 송신 전력 대비 $\frac{P_1}{2}$으로 임의 재밍 신호를 생성하는 두 단계를 거치며 이 경우 이진 메시지를 포함하지 않으며 공정한 비교를 위해 위의 송신 전력이 선택되었다. 따라서 이 방법의 아웃티지 확률은 다음과 같다.

$$P_0^I = 1 - \Pr\left\{ \left[\log_2 \frac{\left(1 + \frac{0.5P_2\gamma_{SD}}{1+0.5P_1\gamma_{RD}} \right)}{1 + \frac{0.5P_2\gamma_{SE}}{1+0.5P_1\gamma_{RE}}} \right]^+ > R_t \right\} \quad (12)$$

두 번째, 첫 번째 시간 슬롯에서 송신단 S는 송신 전력 P_1으로 중계기 R에게 신호 운반을 담당하는 메시지 M_S 를 전송한다. 중계기 R이 안전하고 정확하게 복호할 경우, 두 번째 시간 슬롯에서 송신 전력 P_2로 수신단 D에게 복호된 신호를 전송한다. 이 경우의 아웃티지 확률은 다음과 같다.

$$P_0^{II} = 1 - \left(\Pr\left\{ \left[\frac{1}{2} log_2 \frac{(1+P_1\gamma_{RS})}{1+P_1\gamma_{SE}} \right]^+ > R_t \right\} \times \Pr\left\{ \left[\frac{1}{2} log_2 \frac{(1+P_2\gamma_{RD})}{1+P_2\gamma_{RE}} \right]^+ > R_t \right\} \right) \quad (13)$$

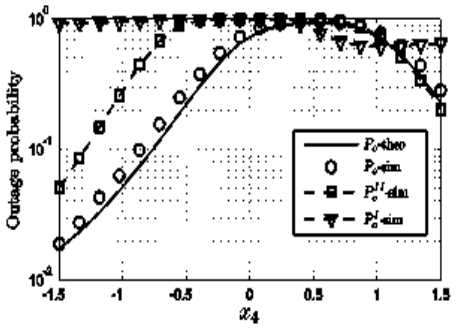

그림 2. 아웃티지 성능 비교
Fig. 2. A Comparison of Outage Performances

본 논문에서 제안한 시스템 모델의 아웃티지 성능과 비교 대상을 그림 2에 표현하였다. 그림 2에서 $|x_4| \le 0.5$ 인 경우, 도청 노드는 송신단 S에 대해 닫힌계이며 제한된 기존 기법의 성능을 확인할 수 있다. 그림 2에서 송신 채널을 도청 하는 부분은 정격 감소 계수로 인해 P_0^I와 P_0^{II}의 성능이 불능 상태에 머물러 있다. 이 경우, 송신단에게 전송되는 배타적 논리 연산이 적용된 메시지 $M_\oplus$의 도청을 방지한다. 따라서 제안된 기법이 기존의 기법

보다 우수하다는 것을 증명할 수 있다. 본 논문에서 제안된 기법은 도청 노드가 송신단 주변에 존재하는 극단적인 시나리오에서 유효함을 증명한다. 또한 제안된 기법은 도청 노드의 위치에 따른 성능이 우수하다. 특히, $x_4 < -0.5$보다 먼 지역에 위치할 때 기존의 기법에 비해 우수한 것을 확인할 수 있다.

Ⅳ. 결론

본 논문에서는 도청 노드가 송신단 주변에서 존재할 때, 전송된 메시지를 도청하고 공유 시드를 감지하게 되는 특수한 시나리오에 대한 해결책을 제안하였다. 도청 방해 신호로 이진 재밍 메시지를 사용하였으며, 배타적 논리 연산을 적용하여 전송된 메시지의 도청을 방지하였다. 또한 도청 노드는 시드를 얻을 수 없으므로 송신단 S와 중계기 R, 수신단 D 사이의 전송은 보호받게 된다. 따라서 본 논문에서 제안된 기법은 기존 기법의 아웃티지 성능에 비해 우수함을 확인할 수 있으며 특수한 시나리오에 대한 해결책으로 타당함을 증명하였다.

References

[1] Krikidis, I., Thompson, J.S., and McLaughlin, S., “Relay Selection for Secure Cooperative Networks with Jamming”, Wireless Communications, IEEE Transactions on, 2009, 8, (10), pp 5003-5011,

[2] Sun, X., Xu, W., Jiang, M., and Zhao, C., 'Opportunistic Selection for Decode-and-Forward Cooperative Networks with Secure Probabilistic Constraints', Wireless Personal Communications, 2012.

[3] Yupeng, L., Jiangyuan, L., and Petropulu, A.P., 'Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security', Information Forensics and Security, IEEE Transactions on, 2013, 8, (4), pp. 682-694.

[4] Pham Ngoc Son, Hyung Yun Kong "Performance Analysis of the Amplify-and-Forward Scheme under Interference Constraint and Physical Layer Security", JIIBC, 2014. 14, (1), pp 179-187.

[5] Pham Ngoc Son, Hyung Yun Kong, "Spectrum Sharing with Secure Transmission", EURASIP, 2014, 2014, (134), pp 1-15.

[6] Tran Thanh Truc, Hyung Yun Kong, "CSI-Secured Orthogonal Jamming Method for Wireless Physical Layer Security", IEEE Comm Lett, 2014, 18, (5), pp 841-844.

저자 소개

공 형 윤(정회원)

- 1989년 2월 : New York Institute of Technology(미국) 전자공학과 학사
- 1991년 2월 : Polytechnic University (미국) 전자 공학과 석사
- 1996년 2월 : Polytechnic University (미국) 전자 공학과 박사
- 1996년 ~ 1996년 : LG전자 PCS팀장
- 1996년 ~ 1998년 : LG 전자 회장실 전략 사업단
- 1998년 ~ 현재 : 울산대학교 전기전자정보시스템공학부 교수

<주관심분야> 모듈레이션, 채널 부호화, 검파 및 추정 기술, 협력통신, 센서네트워크