비신뢰 무선 릴레이 통신 네트워크의 안전한 물리계층 키 생성 기법

박소현[1], 이일구[2]
[1]성신여자대학교 미래융합기술공학과 박사과정
[2]성신여자대학교 미래융합기술공학과 교수
220227022@sungshin.ac.kr, iglee@sungshin.ac.kr

Secure Physical Layer Key Generation in Untrusted Wireless Relay Communications and Networks

So-Hyun Park, Il-Gu Lee
Dept. of Future Convergence Technology Engineering, Sungshin Women's University

요 약

물리계층 키 생성 기법은 두 단말 간의 채널 상태 정보를 이용해 일시적인 대칭키를 생성하는 경량 키 생성 기술이다. 하지만, 두 단말 사이에 다이렉트 링크가 없는 릴레이 기반 통신 네트워크 환경에서는 물리계층 키 생성이 어렵고, 비신뢰 릴레이에 의한 키 유출 가능성이 존재한다. 본 연구는 비신뢰 릴레이 통신 네트워크 환경에서 비밀키 정보를 노출하지 않고 안전하게 키를 생성하고 공유하는 방법을 제안하고 보안성을 평가한다. 실험 결과에 따르면 종래 방식보다 제안하는 방식의 키 유출률(key leakage rate, KLR)이 87.5% 감소하였고, 릴레이 수가 증가할수록 KLR이 감소하여 제안하는 방식이 비신뢰 릴레이 환경에서 높은 보안성을 보장함을 확인하였다.

1. 서론

최근 무선랜(wireless local area network, WLAN)은 신뢰성을 추구하는 방향으로 발전하고 있으며, 특히 신호 도달 거리 밖에 있는 단말 간 릴레이를 이용해 통신하는 기술에 관한 연구가 활발히 진행되고 있다 [1]. 릴레이 노드는 AP(access point)와 STA(station)의 전송 커버리지를 확장하여 숨겨진 노드 문제(hidden node problem)를 해결할 수 있다. 하지만, 신뢰할 수 없는 릴레이 통신 네트워크 환경에서 릴레이 노드가 전송 데이터를 도청하거나 스푸핑(spoofing)할 수 있다.

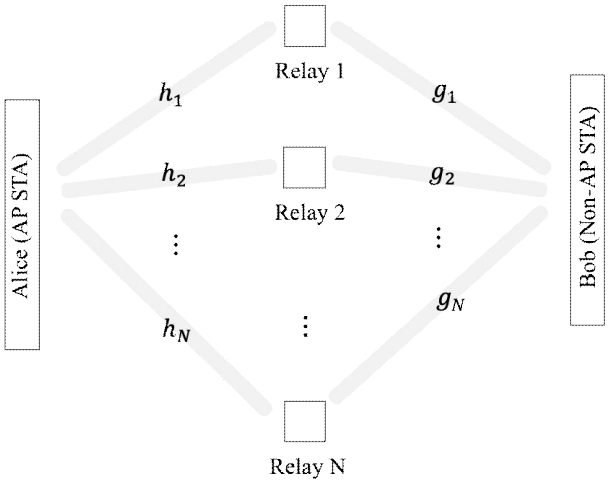
복잡한 해시 연산 기반의 종래 키 생성 기법을 대체하는 물리계층 키 생성(physical layer key generation, PLKG) 기술은 두 단말 간의 채널 상태 정보(channel state information, CSI)를 이용하여 일시적인 대칭키를 생성하는 경량 키 생성 기법이다 [2]. 무선랜과 같은 TDD(time-division duplex) 시스템에서는 일정한 기간 동안 업링크와 다운링크의 채널 응답이 유사한 특성을 이용하여 임시의 대칭키를 생성할 수 있다. PLKG는 복잡한 연산을 할 수 없는 경량 사물인터넷 네트워크에 적합하고, 채널 상관성에 따라 동일한 CSI 획득이 어렵기 때문에 키 유출을 방지할 수 있다 [3].

본 연구에서는 AP와 STA 간의 다이렉트 링크가 없고 신뢰할 수 없는 릴레이를 이용한 무선 통신 환경에서 릴레이 노드에 비밀키를 노출하지 않으면서 AP와 STA이 CSI를 이용하여 비밀키를 생성하고 공유하는 방법을 제안한다. 또한, 릴레이 노드에 의한 키 유출률(key leakage rate, KLR)을 최소화하기 위한 보안이 강화된 키 생성 기법을 제안하고 보안성을 평가한다.

2. 시스템 모델

그림 1은 릴레이 기반 통신 시스템의 구조도를 나타낸다. Alice와 Bob, 릴레이 노드는 모두 싱글 안테나로 구성되어 있고, N개의 릴레이 노드가 Alice의 각 링크의 신호를 Amplify-and-Forward 방식으로 Bob에게 전달하는 구조이다. Alice와 Bob은 각각 AP과 STA 일 수 있고, Alice와 Bob은 Alice와 모든 릴레이 노드 사이의 채널 임펄스 응답(channel impulse response, CIR)을 조합해서 동일한 비밀키

를 생성한다. 이때, 릴레이 노드는 수동적인 도청자이거나 릴레이 노드 간 협력을 통해 모든 채널의 CIR을 알아내고 비밀키를 생성할 수 있지만, 본 연구에서는 릴레이 노드 간의 거리가 1/2 파장 이상 떨어져 있어서 각 채널이 독립적이며 릴레이 간 협력은 고려하지 않는 환경을 가정한다.



(그림 1) 릴레이 기반 통신 시스템 구조도.

Alice와 Bob은 Alice와 i번째 릴레이 노드 R_i $(i=1,2,\cdots,N-1)$ 사이의 CIR을 모두 조합하여 비밀키를 생성한다. Alice는 채널 추정을 위해 t_1의 시간에 R_i로 M개의 부반송파를 포함하는 주파수 영역의 OFDM(orthogonal frequency division multiplexing) 파일럿 심볼 $a=[a_1,a_2,\cdots,a_M]^T\in C^{M\times 1}$ 를 전송한다. 마찬가지로, R_i는 t_2의 시간에 Alice에게 파일럿 심볼 $b=[b_1,b_2,\cdots,b_M]^T\in C^{M\times 1}$ 를 전송한다. 이때, t_1과 t_2 사이의 시간은 상관 시간(coherence time) τ보다 짧아서($|t_2-t_1|<\tau$), Alice와 R_i 사이의 채널 $h_{AR_i}(t_1)$과 R_i와 Alice 사이의 채널 $h_{R_iA}(t_2)$은 무선 채널의 호혜성(reciprocity) 특성에 따라 $h_{AR_i}(t_1)\approx h_{R_iA}(t_2)$의 관계가 성립한다.

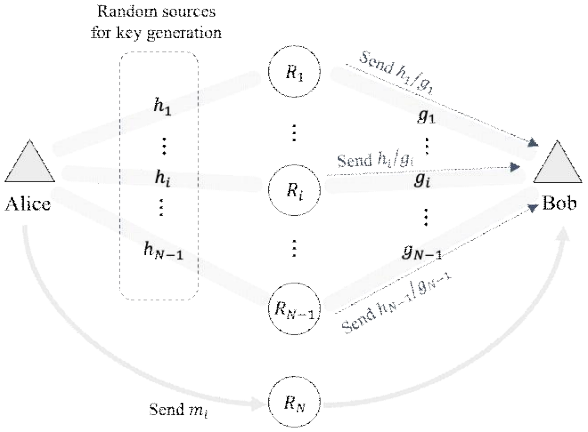
R_i가 Alice로부터 받은 신호는 식 (1)과 같이 모델링할 수 있다.

$$y_i=H_i a+Z_i \tag{1}$$

이때, Z_i는 평균이 0, 분산이 σ^2인 AWGN(additive white Gaussian noise)의 푸리에 변환이고, $H_i\in C^{M\times M}$은 R_i가 추정한 Alice로부터의 채널 주파수 응답 h_i의 대각 행렬을 나타낸다 [4].

2.1 키 생성 알고리즘

그림 2는 N개의 릴레이로 구성된 환경에서 비밀키를 생성하는 시스템 구조도를 나타낸다. Alice와 R_i $(i=1,2,\cdots,N-1)$ 까지의 모든 채널 h_i를 조합하여 비밀키를 생성하기 위해서, Bob은 Alice와 R_i 사이의 채널 h_i를 각 릴레이 R_i에게 전달받는다. 이때, h_i를 도청자로부터 보호하며 안전하게 전달하기 위해서 R_i와 Bob 간의 채널 g_i로 h_i를 나눈 값 h_i/g_i를 전달한다.



(그림 2) 릴레이 기반 PLKG 시스템 구조도.

종래 물리계층 키 생성은 OFDM 심볼 내 부반송파의 크기(amplitude) 또는 위치(indices)를 이용하는 방법이 있고 [5], 본 연구에서는 부반송파의 크기를 이용하여 물리계층 키를 생성하는 방식을 사용하였다.

각 채널 h_i는 독립적이며, Alice와 R_i는 채널 추정을 위해서 상관 시간 τ 동안 각각 파일럿 심볼 $a=[a_1,a_2,\cdots,a_M]^T\in C^{M\times 1}$과 $b=[b_1,b_2,\cdots,b_M]^T\in C^{M\times 1}$ 를 주고받는다. 이때 R_i가 추정한 주파수 영역의 채널은 $H_i\in C^{M\times M}$으로 나타낼 수 있다.

대각 행렬 H_i는 열벡터 $h_i=[diag(H_i)]^T\in C^{1\times M}$로 변환하고, h_i를 l개의 부반송파를 포함하는 s개의 서브그룹($l=M/s$)으로 나눈다. 즉, $p=\{1,2,\cdots,s\}$일 때 $h_i=[h_i^1,\cdots,h_i^p,\cdots,h_i^s]$와 같이 s개의 서브그룹으로 나누고, 각 서브 그룹은 $q=\{1,2,\cdots,l\}$일 때 $h_i^p=[h_i^{p,1},\cdots,h_i^{p,q},\cdots,h_i^{p,l}]$와 같이 l개의 부반송파를 포함한다.

h_i의 부반송파의 크기를 양자화하여 키를 생성하기 위해서, 먼저 식 (2)와 같이 h_i의 전체 부반송파의 평균 크기 $Av(h_i)$를 구하고, 식 (3)과 같이 $Av(h_i)$를 기준으로 각 부반송파 크기를 0 또는 1의

키 값으로 변환한다.

$$Av(h_i) = \frac{\sum_{p=1}^{s}\sum_{q=1}^{l} h_i^{p,q}}{M} \quad (2)$$

$$Key(h_i^{p,q}) = \begin{cases} 0, Av(h_i) > h_i^{p,q} \\ 1, Av(h_i) \le h_i^{p,q} \end{cases} \quad (3)$$

채널의 수신 신호 대 잡음 비 (signal-to-noise ratio, SNR)에 따라서 Alice와 R_i가 추정한 채널 간 오차가 발생하여 키 생성률 (key generation rate, KGR)이 낮아지고 키 불일치율 (key mismatch rate, KMR)이 높아질 수 있어서, 전체 부반송파 중 일부만을 키 생성에 사용하여 KMR을 낮출 수 있다. 예를 들어, 채널 h_i에서 한 서브그룹 내에서 키 생성에 사용할 부반송파의 개수를 m_i라고 할 때, 만들 수 있는 키의 길이는 $m_i \times s$ 비트이다. 최종적으로 $N-1$개의 릴레이로 구성된 환경에서 Alice와 Bob이 생성할 수 있는 총 키의 길이는 $\sum_{i=1}^{N-1} m_i \times s$ 비트이다.

2.2 키 유출률

본 연구에서는 릴레이 노드 간 협력을 통한 키 생성 확률은 고려하지 않고, 릴레이 노드 R_i가 Alice와 나머지 릴레이 노드 $R_j (j = 1, 2, \cdots, N-1, i \neq j)$ 간의 채널 h_j로부터 생성한 키 값을 무차별 대입 공격하여 알아내는 키 유출 시나리오를 가정한다. 즉, 전체 키 길이를 K라고 할 때 R_i가 나머지 키비트를 무차별 대입 공격하여 알아내는 키 유출 확률은 식 (4)와 같이 R_i가 무차별 대입 공격으로 $(K-m_i)$개의 나머지 비트를 알아낼 확률과 같다.

$$KLR_{R_i} = \frac{1}{2^{(K-m_i \times s)}} \quad (4)$$

만약 m_i가 모든 h_i에서 동일할 경우 하나의 릴레이 노드는 전체 키 길이를 $K = (N-1) \times m_i \times s$ 와 같이 구할 수 있고, 이때 R_i가 전체 키를 알아내는 KLR은 식 (4)에 의하여 $KLR_{R_i} = \frac{1}{2^{((N-2) \times m_i \times s)}}$ 와 같이 구할 수 있다.

3. 제안하는 키 생성 기법

릴레이 노드에 의한 키 유출률을 최소화하기 위해서, 그림 2와 같은 시스템 환경에서 전체 N개의 채널 중 $N-1$개의 채널 h_i마다 m_i를 다르게 할당하여 키를 생성하고, 각 채널의 m_i 정보는 신뢰할 수 있는 나머지 하나의 릴레이 노드로 전송할 수 있다. 따라서, R_i가 전체 키를 알아내는 KLR은 식 (5)와 같이 R_i가 먼저 총 키의 길이를 알아내고 자신의 키를 제외한 나머지 키를 무차별 대입 공격하여 알아내는 키 유출률과 동일하다.

$$KLR_{R_i} = (\frac{1}{l})^{(N-2)} \times \frac{1}{2^{(K-m_i \times s)}} \quad (5)$$

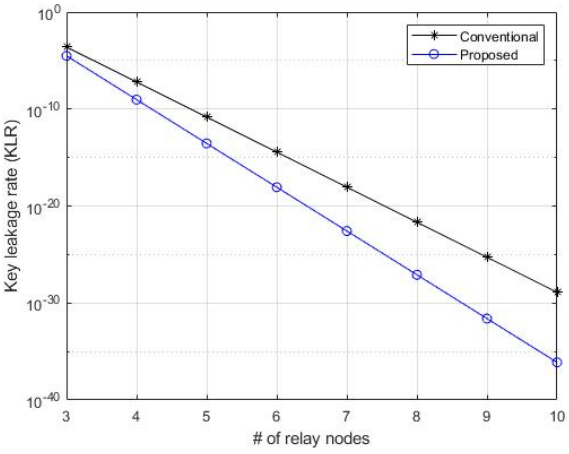
또한, 모든 채널의 m_i 정보를 전달하는 릴레이 노드에 의해 키가 유출률은 $\frac{1}{2^{((N-1) \times m_i \times s)}}$ 으로, 종래 방식보다 낮은 KLR을 가진다.

4. 성능 평가

그림 3의 그래프는 릴레이 수의 증가에 따른 종래 방식과 제안하는 방식의 KLR을 비교하고, 표 1은 성능 평가 파라미터를 나타낸다.

<표 1> 성능 평가 파라미터

Parameter	Value
M	48
s	6
$l = M/s$	8
m_i	2
N	[3:10]



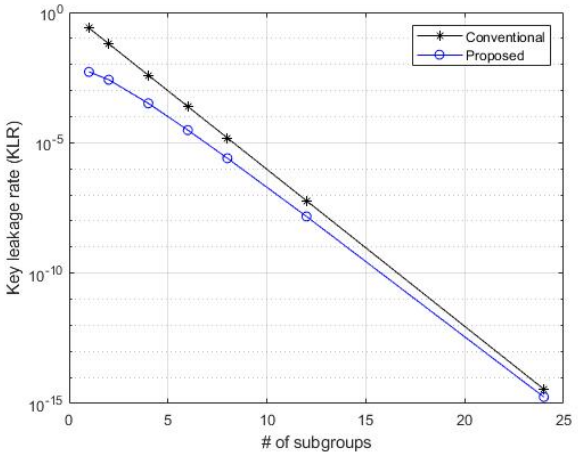
(그림 3) 릴레이 수에 따른 KLR 비교.

먼저, 종래 방식과 제안하는 방식에서 모든 채널의 m_i 값은 동일하게 2로 설정하고 총 생성되는 키

길이가 동일한 환경일 때를 가정하였다. 그림 3은 릴레이 수에 따른 종래 방식과 제안 방식의 KLR을 보여준다. 그림 3에서 릴레이 노드가 3개이고, 그 중 2개의 릴레이 노드의 채널로 키를 생성하고 나머지 하나의 릴레이 노드는 키 정보를 전달하는 환경일 때, 종래 방식 대비 제안하는 방식의 KLR은 87.5% 감소하였고, 릴레이 노드의 개수가 증가할수록 KLR이 감소하는 것을 확인할 수 있다.

<표 2> 성능 평가 파라미터

Parameter	Value
M	48
s	[1, 2, 4, 6, 8, 12, 24]
$l = M/s$	[48, 24, 12, 8, 6, 4, 2]
m_i	2
N	3



(그림 4) 채널 당 서브그룹 수에 따른 KLR 비교.

그림 4는 릴레이 노드의 수는 3, m_i는 2로 고정하고 서브그룹 s의 개수를 증가시키며 종래 방식과 제안하는 방식의 KLR을 비교한 그래프이다. 종래 방식과 제안하는 방식은 모두 서브그룹 수가 증가할수록 키의 길이가 증가하여 KLR이 감소하였고, 제안하는 방식은 $s = 2$일 때 종래 방식보다 KLR이 약 95.8% 감소하였다.

즉, 각 릴레이 채널마다 생성되는 키 길이를 다르게하여 총 생성되는 비밀키의 길이를 비식별화함으로써 비신뢰 릴레이에 의한 키 유출을 방지할 수 있다. 또한, 릴레이의 수와 서브그룹 수가 증가하면 키의 길이가 증가하여 릴레이에 의한 키 유출에 더욱 강인해진다.

5. 결론

본 연구는 비신뢰 무선 릴레이 기반의 통신 네트워크 시스템에서 릴레이 노드에게 비밀키 정보를 노출하지 않고 채널 상태 정보를 기반으로 물리계층 비밀키를 생성하는 방법을 제안하였다. 각 채널의 키 길이를 다르게 할당하여 비밀키를 생성하는 방식으로 비신뢰 릴레이에 의한 키 유출률을 최소화하고 안전하게 비밀키를 공유할 수 있다. 향후 연구로는 다중 비신뢰 무선 릴레이 통신 네트워크 시스템에서, 각 채널 상태에 따라 KGR 및 KMR을 최적화할 수 있는 파워 할당 기법을 연구하고자 한다.

ACKNOWLEDGMENT

본 논문은 2024년도 산업통상자원부 및 한국산업기술진흥원의 산업혁신인재성장지원사업 (RS-2024-00415520)과 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0 사업의 연구결과로 수행되었음 (No. IITP-2022-RS-2022-00156310)

참고문헌

[1] Wang, X., Shu, F., Shi, W., Liang, X., Dong, R., Li, J., & Wang, J. (2022). Beamforming design for IRS-aided decode-and-forward relay wireless network. IEEE Transactions on Green Communications and Networking, 6(1), 198-207.

[2] Aldaghri, N., & Mahdavifar, H. (2020). Physical layer secret key generation in static environments. IEEE Transactions on Information Forensics and Security, 15, 2692-2705.

[3] Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical layer security for the Internet of Things: Authentication and key generation. IEEE Wireless Communications, 26(5), 92-98.

[4]Wang, D., Chen, F., Chen, Y., Zheng, M., & Zheng, J. (2022). Scramble-Based Secret Key Generation Algorithm in Physical Layer Security. Mobile Information Systems, 2022.

[5] Furqan, H. M., Hamamreh, J. M., & Arslan, H. (2020). New physical layer key generation dimensions: Subcarrier indices/positions-based key generation. IEEE Communications Letters, 25(1), 59-63.