저전력 사물인터넷 통신을 위한 동적 보안 링크 적응 기법

박채연[1], 이선진[2], 이일구[3]
[1]성신여자대학교 융합보안공학과 학부생
[2]성신여자대학교 미래융합기술공학과 박사과정
[3]성신여자대학교 융합보안공학과/미래융합기술공학과 교수
20221097@sungshin.ac.kr, 220237017@sungshin.ac.kr, iglee@sungshin.ac.kr

Dynamic Secure Link Adaptation Technique for Low-power IoT Communications

Chae-Yeon Park[1], Sun-Jin lee[2], Il-Gu Lee[3]
[1]Dept. of Convergence Security Engineering, Sungshin Women's University
[2]Dept. of Future Convergence Technology Engineering, Sungshin Women's University
[3]Dept. of Convergence Security /Future Convergence Technology Engineering, Sungshin Women's University

요 약

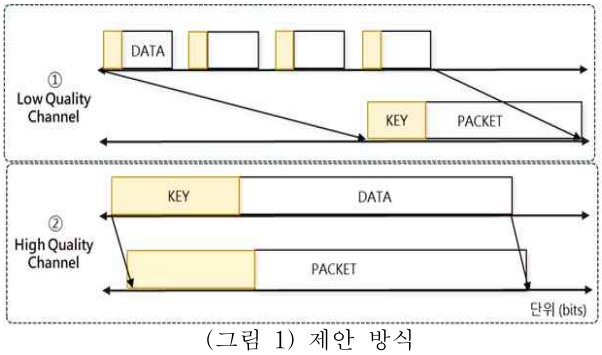
본 연구에서는 물리계층 보안을 위한 키 길이를 IoT 무선 채널 상태에 따라 조정하는 링크 적응 방법을 제안한다. 시뮬레이션 결과에 따르면 제안 방식은 종래 방식 대비 평균 78.52% 개선된 처리율과 약 2배 개선된 보안성을 보인다.

1. 서론

밀집 네트워크 환경에서 데이터 프라이버시를 보호하기 위해서는 사물인터넷 (Internet of Things, IoT) 기기의 저전력 환경에 적합한 보안 대책과 기술이 필요하다. 최근 산업에 널리 활용되고 있는 IoT 서비스는 무선 통신의 고유한 특성으로 인해 도청 및 식별 위협에 취약하다[1]. 물리 계층 인증 (Physical Layer Authentication, PLA)은 물리 계층의 프리엠블을 인증키로 활용하여 신뢰할 수 있는 물리 계층 통신을 제공한다. 종래 연구[2]에서는 좁은 대역에서 확산 코드 방식을 활용한 프레임 PLA를 개발하여 통신 성능의 저하 없이 인증 정확도를 향상했다. 그러나 IoT 네트워크 채널 상태의 동적 변동 특성을 고려하지 못하는 한계가 있다.

종래의 5G 무선 통신에서 링크 적응 기술은 통신 채널 상태에 따라 동적으로 데이터 길이를 변동하여 데이터 전송 효율성을 높인다. 이 원리를 물리 계층 보안에 응용하여 IoT 기기의 물리 계층 통신의 프리엠블을 인증키로 대신하여 종래보다 길이를 늘리면 높은 기밀성을 보장할 수 있다. 그러나 인증키 길이가 늘어나면 데이터 처리율은 낮아진다. 따라서 본 연구에서는 링크 적응 기술을 확장하여 데이터 길이뿐만 아니라 채널 상태에 따라 프리엠블 길이를 동적으로 변동하여 보안성과 데이터 처리율을 최적화하는 방법을 제안한다. 이 방법은 고품질 채널 상태에서 인증키 길이를 늘려 보안성 중심으로 최적화하고, 저품질 채널 상태에서는 기존 인증키를 분할 전송하여 데이터 처리율을 최적화한다.

2. 동적 보안 링크 적응 기법



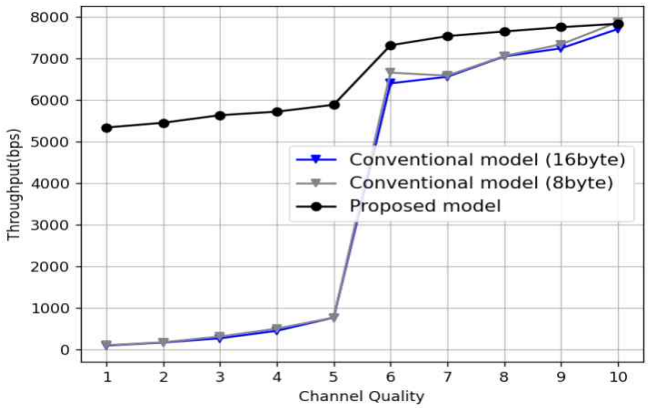
(그림 1) 제안 방식

본 연구에서 제안하는 방식의 동작 과정은 그림 1과 같다. 1번은 저품질 채널 상태이고, 2번은 고품질 채널 상태이다. 1번 채널에서는 데이터 길이를 짧게 전송하고, 프리엠블 키 길이를 1/4씩 분할 전송하여 모든 키가 모이면 데이터를 처리한다. 2번 채널에서는 데이터 길이를 길게 전송하고, 1번 채널

보다 프리엠블 키 길이를 2배 늘려 전송한다.

3. 실험 평가

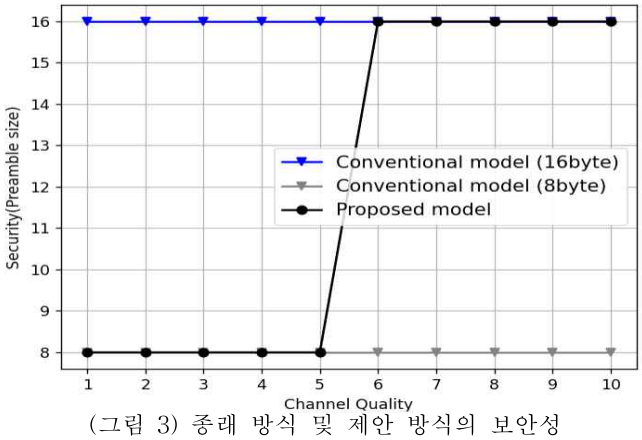
본 연구에서는 종래의 링크 적응 방식과 제안하는 동적 보안 링크 적응 방식을 데이터 처리율과 보안성 총 두 가지 측면에서 비교하였다. 이 중 보안성은 절대적인 키 사이즈로 평가하였다. 채널 품질이 향상될수록 전송 실패 확률이 감소한다. 종래 방식과 제안 방식 모두 1에서 5까지의 채널 품질에서는 108byte의 데이터 패킷으로, 6에서 10까지는 1508byte의 데이터 패킷으로 전송된다. 이때 종래 방식은 모든 채널 품질에서 키 길이를 각각 8byte 또는 16byte으로 고정했으며, 제안 방식의 키 길이는 채널 품질에 따라 동적으로 변한다. 1에서 5까지의 채널 품질에서는 키 길이를 2byte씩 분할 전송한 후 총 합 8byte가 되면 키를 합쳐 패킷으로 전송하며, 6에서 10까지는 키 길이를 16byte로 설정하였다. 이 실험에서 패킷 전송 실패 시 8회까지 재전송을 시도하며 1,000회 반복한 후 평균값으로 시각화하였다.



(그림 2) 종래방식 및 제안방식의 처리율

그림 2는 종래 방식과 제안 방식의 처리율을 측정한 결과를 나타낸 것이다. 채널 품질이 5 이하에서는 제안 방식이 종래 방식에 비해 약 5배 높은 처리율을 보인다. 채널 품질이 5 이상에서는 제안 방식이 두 종래 방식에 비해 약 200bps 높은 처리율을 보인다.

그림 3은 종래 방식과 제안 방식의 보안성을 나타낸다. 종래 방식은 각 키 길이를 8byte, 16byte로 고정하여 모든 채널 품질에서 보안성이 일정하다. 반면에 제안 방식은 채널 품질이 5보다 낮을 때 종래 방식과 일치하는 보안성을 유지하고, 채널 품질이 5보다 높을 때 종래 방식 대비 보안성이 2배 향상되었다.



(그림 3) 종래 방식 및 제안 방식의 보안성

4. 결론

물리 계층 인증은 프리엠블을 인증키로 활용하여 고신뢰 물리 계층 통신을 보장한다. 종래 링크 적응형 방식은 프리엠블에서 유동적인 IoT 채널 상태를 고려하지 못하고, 전송 효율성 및 보안성 중 한쪽으로만 최적화된다. 본 연구에서는 밀집 네트워크의 IoT 채널 상태를 고려하여 프리엠블 키 길이를 조정한다. 실험 결과에 따르면, 제안 방식은 종래 방식 대비 처리율을 평균 78.52% 개선하였고, 채널 품질이 높을 때 보안성을 2배 개선하였다.

5. Acknowledgement

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)

6. 참고문헌

[1] X. Lu, N. Cong Luong, D. T. Hoang, D. Niyato, Y. Xiao and P. Wang, "Secure Wirelessly Powered Networks at the Physical Layer: Challenges, Countermeasures, and Road Ahead," in Proceedings of the IEEE, vol. 110, no. 1, pp. 193-209, Jan. 2022

[2] Y. Leng, R. Zhang, W. Wen, P. Wu and M. Xia, "Physical-layer Authentication with Watermarked Preamble for Internet of Things," 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Montreal, QC, Canada, 2023, pp. 212-217