Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.3, Jun. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.3.393

배터리 소모 공격에 대응하는 저전력 웨이크업 리시버의 적응형 파워 세이빙 메커니즘*

김 소 연,[1†] 윤 성 원,[2] 이 일 구[3‡]
[1,2,3]성신여자대학교 (대학원생, 학생, 교수)

Adaptive Power Saving Mechanism of Low Power Wake-up Receivers against Battery Draining Attack*

So-Yeon Kim,[1†] Seong-Won Yoon,[2] Il-Gu Lee[3‡]
[1,2,3]Sungshin Women's University (Undergraduate student, Graduate student, Professor)

요 약

최근 사물인터넷(Internet of Things, IoT)이 인간의 안전, 생명, 자산과 직결되는 산업과 일상생활에 널리 활용되고 있다. 그러나 저가, 경량, 저전력 요건을 충족해야 하는 IoT 장치는 배터리 소모 공격과 간섭 때문에 배터리 라이프타임이 심각하게 단축되는 문제가 있다. 이러한 문제를 해결하기 위해 웨이크업 리시버(Wake-up Receiver, WuR)를 위한 802.11ba 표준이 등장했고, 이 기능은 와이파이 기반 IoT의 에너지 소비를 최소화하는 데 중요한 역할을 하고 있다. 그러나 WuR 프로토콜은 지연시간과 오버헤드를 단축하기 위해서 보안 메커니즘을 고려하지 않았다. 따라서 본 연구에서는 배터리 소모 공격에 대응하기 위해서 저전력 웨이크업 리시버를 위한 적응형 파워 세이빙 메커니즘(Adaptive Power Saving Mechanism, APSM)을 제안한다. APSM은 공격이 잦은 환경에서 파워 세이빙 시간을 기하급수적으로 증가시킴으로써 비정상적으로 발생하는 파워 소모량을 최소화할 수 있다. 실험 결과에 따르면, APSM은 전체 트래픽 중 공격 비중이 10% 이상일 때 종래의 파워 세이빙 메커니즘(Legacy Power Saving Mechanism, LPSM)보다 13.77% 이상의 에너지 소비 효율을 개선할 수 있었다.

ABSTRACT

Recently, the Internet of Things (IoT) has been widely used in industries and daily life that directly affect human safety, life, and assets. However, IoT devices, which need to meet low-cost, lightweight, and low-power requirements, face a significant problem of shortened battery lifetime due to battery draining attacks and interference. To solve this problem, the 802.11ba standard for the Wake-up Receiver (WuR) has emerged, this feature is playing a crucial role in minimizing energy consumption. However, the WuR protocol did not consider security mechanisms in order to reduce latency and overhead. Therefore, in this study, an Adaptive Power Saving Mechanism (APSM) is proposed for low-power WuR to counter battery draining attacks. APSM can minimize abnormally occurring power consumption by exponentially increasing power-saving time in environments prone to attacks. According to experimental results, the proposed APSM improved energy consumption efficiency by a minimum of 13.77% compared to the traditional Legacy Power Saving Mechanism (LPSM) when attack traffic ratio is 10% or more of the total traffic.

Keywords: Wake-up receiver, Adaptive power-save mechanism, Battery draining attack, Low-power security mechanism

Received(03. 19. 2024), Modified(06. 03. 2024), Accepted(06. 04. 2024)

* 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).

* 본 논문은 2023년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임.

† 주저자, sykim.cselab@gmail.com

‡ 교신저자, iglee@sungshin.ac.kr(Corresponding author)

I. 서 론

최근 4차 산업혁명의 패러다임을 이끄는 핵심 기술인 사물인터넷(Internet of Things, IoT)과 인공지능(Artificial Intelligence, AI)이 결합한 지능형 사물인터넷(Artificial Intelligence of Things, AIoT)이 등장하여 주목받았다[1]. Global Market Insights의 보고서에 따르면, 전세계 AIoT 시장은 2022년에 90억 달러 규모로 평가되었으며, 2032년까지 연평균 대략 20%로 성장하여 250억 달러 규모에 달할 것으로 예상된다[1]. 과거의 IoT 장치는 대량의 데이터를 센싱, 수집 및 처리하는 역할만 수행했다면, AIoT 장치는 학습 기능과 추론 기능을 기본적으로 갖추고 있어서 지능화된 동작을 수행한다[2]. AIoT 기기가 실시간으로 대규모 센싱 데이터를 수집 및 분석하고, 판단하여 지능형 서비스를 제공하게 되면서 일상생활과 산업 전반에 걸쳐 널리 활용되고 있다. 그러나 대부분의 IoT 장치는 코인셀 배터리와 같이 한정된 리소스를 가지고 있어서 저가, 경량, 저전력 요건을 충족해야 한다. 배터리의 용량을 확장하는 방법도 있지만, 이는 사용자 경험과 비용 측면에서 여러 제약이 존재한다. 따라서 배터리 라이프 타임을 효율적으로 관리하는 것이 중요한 문제이다[3-5]. 특히 AIoT 장치는 다량의 데이터를 학습하고 추론하는 과정에서 배터리 소모가 크기 때문에 에너지 효율적인 동작이 중요하다. 이러한 배경에서 IoT 장치들의 전력 소모를 최소화하기 위해 무선랜 표준에서는 Power Saving Mechanism(PSM) 및 TWT(Target Wake Time)와 같은 다양한 전력 절감 방식을 도입하였다. 또한, IoT 장치의 저전력 요구사항을 만족하기 위한 Wake-up Receiver(WuR)라고 불리는 802.11ba 표준화 작업을 진행하였다. 2021년에 표준 작업이 완료되어, 무선 단말이 에너지를 절약하면서도 네트워크의 연결을 유지할 수 있도록 설계되었다. WuR은 파워세이빙하는 메인 수신기와 웨이크업 신호를 감지하여 메인 수신기를 활성화하는 저전력 서브 수신기로 구성된다. 서브 수신기가 웨이크업 신호를 감지한 경우에만 메인 수신기를 활성화하는 방식으로 동작한다[4-6]. 그러나 WuR은 처리 효율을 증대하기 위해서 별도의 보안 메커니즘을 고려하지 않고 있다. 공격자는 웨이크업 신호를 지속적으로 전송함으로써 배터리 소모 공격과 같은 리소스 고갈 공격이 가능해지고[7], 피해 IoT 장치들은 배터리 라이프 타임이 심각하게 단축되는 문제가 발생한다. IoT 단말의 리소스 소모 공격을 방어하기 위한 연구들이 진행되었지만, 대부분의 연구는 주로 공격이 발생한 이후에 조처하는 사후 대응 방식이어서 WuR에 적합하지 않다. WuR 장치를 보호하기 위해서는 단말을 깨우는 웨이크업 신호에 즉시 트리거링하지 않아야 한다[8].

따라서 본 연구에서는 배터리 소모 공격에 대응하기 위해서 WuR을 위한 적응형 파워 세이빙 메커니즘(Adaptive Power Saving Mechanism, ASPM)을 제안한다. 제안하는 APSM은 배터리 소모 공격 발생 시 파워 소모량을 최소화하고, 공격 대응 지연 시간을 줄이기 위해서 공격 발생 빈도에 따라서 파워 세이빙 시간을 변경한다.

본 논문의 기여점은 다음과 같다.

- 무선 웨이크업 리시버의 보안 취약점을 분석하였다.
- 배터리 소모 공격 발생 빈도에 따라 파워 세이빙 구간을 변경하는 적응형 파워 세이브 메커니즘을 제안하였다.

본 논문은 다음과 같이 구성된다. II장에서 WuR에 보안 메커니즘을 제안한 관련 연구를 분석한다. 그리고 III장에서 저전력 웨이크업 리시버의 적응형 파워 세이빙 메커니즘을 제안하고, IV장에서 제안 방식과 종래 방식의 성능 평가 결과를 분석한다. 그리고 V장에서 결론을 맺는다.

II. 관련 연구

WuR은 무선 통신 장치의 저전력 동작을 위해 고안된 메커니즘으로, 입력 신호가 감지되면 절전모드를 해제하고 수신모드로 전환하여 데이터를 수신할 준비를 한다. 입력신호가 감지되지 않으면 다시 절전모드로 스위칭하고 채널을 Off 하여 전력 소모를 절약한다[9]. 그러나 WuR 메커니즘은 처리 효율을 높이기 위해서 보안이 고려되지 않고 있다. 최근 WuR의 보안성을 강화하기 위한 기술이 활발하게 논의되고 있으며[8,10-13], Table 1.은 관련 연구를 정리한 표이다. 종래의 연구는 주로 토큰 기반의 인증 과정을 수행하거나[8,11-13], 별도의 통신 과정을 추가하여 공격 유무를 알려주는 방식[14]으로 WuR의 보안성을 강화하고자 했다.

일회성 웨이크업 토큰을 활용한 초저전력 WuR을 제안한 연구[11]는 일회성 웨이크업 토큰이 수신된 경우에만 저전력 상태에서 노드를 활성화하는 방법을

Table 1. Comparison of the Limitations of Related Work

Existing studies		Methods	Limitations
Token-based Authentication	A. T. et al. [11]	An ultra-low power wake-up radio is designed to rouse a sensor node from its dormant state solely upon receiving a valid wake-up token.	The continual generation of disposable tokens results in a considerable expenditure of energy.
	R. Falk et al. [8]	Proposed a robust and lightweight key management protocol based on public key encryption in response to sleep denial attacks; also complemented by leveraging the Fully-Hashed MQV protocol for resource-limited devices.	The use of key encryption increases complexity, which also limits scalability. It faces difficulties in terms of security features when adding new features.
	Pradeep Sudhakaran et al. [12]	Enhancing security of WuR by generating tokens based on device reliability to ensure quick authentication and approval	Reliance on threshold values to assess measuring device reliability heightens the likelihood of encountering false positives and false negatives.
	A. Oun et al. [13]	PUF-based security wake-up that cannot be replicated or imitated	For PUF synchronization, each step requires additional computation, communication, and control, which can increase the complexity of the system.
Additional Communication	H. Park [14]	A general operating procedure of WuR for ensuring low-power consumption and an algorithm for detecting malicious attacks.	Too many additional processes to slow data reception

제안했다. WuR에는 토큰 참조 값 목록을 저장하고 있는데, 송신기가 웨이크업 신호와 토큰을 전송하면, 수신 WuR은 미리 저장하고 있던 토큰 참조 값 목록을 확인하여 인증한다. 토큰 참조 값 목록과 일치하는 토큰의 경우에만 WuR의 메인 수신기를 절전 상태에서 활성화 상태로 천이한다. 또한, 수신 노드가 절전 상태로 전환되면 토큰값이 변경되는 일회성 토큰이므로 이미 재생된 토큰은 인정되지 않는다. 따라서 토큰값을 미리 알지 못하는 공격자에 대해 방어가 가능하다. 그러나 일회성 토큰을 계속해서 생성하는 과정과 송수신기 사이의 토큰을 주고받는 과정에서 오버헤드가 발생하는 한계점이 존재한다.

WuR의 DoS(Denial of Service) 공격에 대한 취약성을 언급하며 수면 거부 공격에 대응한 AntiDoS 프레임워크를 제안한 연구[8]에서는 인증된 피어만 알고 있는 주요 정보를 바탕으로 한 WuR 키값을 의사 무작위 방식으로 생성하고 업데이트하는 방식을 제안하였다. 해당 방식은 공격자가 유효한 WuR 키값를 생성하더라도 공유 비밀 키를 모르면 노드를 깨울 수 없게 되는데, 암시적 인증서와 Fully-Hashed MQV 기반 방식의 키 교환 프로토콜을 함께 사용하여 WuR의 보안 체계를 강화하고자 했다. 실험 결과에 따르면, 논문에서 제안하는 AntiDoS 프로토콜은 종래의 WuR 보안 메커니즘보다 오버헤드를 줄이면서, 무선 기반 네트워크에서 수면 거부 공격에 대응하는 방법임을 입증하였다. 또한 에너지 사용량을 평가하여 리소스가 제한된 장치에서 적용할 수 있었다. 하지만, 여전히 키를 암복호화하는 과정에서 복잡성이 증가하는 한계가 존재한다. 또한, 키 인증을 수행하는 과정에서 통신 과정이 추가되므로, 통신 복잡도가 증가하는 문제가 있다.

IoT를 위한 EEDLAE(Energy Efficient Distributed Lightweight Authentication and Encryption) 기법을 제안한 논문[12]에서는 장치의 신뢰도를 기반으로 빠른 인증 및 승인을 보장하는 토큰 생성 방식을 제안하였다. 제안 방식에서 수신자는 각 발신자에 대해 토큰을 생성하고, 발신자의 신뢰도를 고려하여 토큰 만료 시간을 결정하는데, 디바이스의 신뢰도는 공격 감지 확률을 통해 측정된다. 암호화 방식으로는 CCM(Cipher Block

Chaining-Message Authentication Code) 기술을 이용한 신뢰 기반 인증 및 카운터를 사용하였다. 공격 빈도에 따른 잔여 에너지와 처리량을 평가하는 실험을 진행한 결과에 따르면 제안 방식은 종래의 방식 대비 처리량이 9% 증가하고, 잔여 에너지가 2% 증가하여 에너지 효율성을 입증하였다. 하지만, 임계 값 기반으로 각 디바이스의 신뢰도를 결정하고, 공격을 탐지 때문에 임계 값에 따라서 정상 신호를 오탐하거나, 비정상 신호를 미탐하는 경우가 발생하는 한계가 존재한다.

PUF(Physical Unclonable Function)를 이용한 일회성 웨이크업 토큰을 제안한 논문[13]에서는 악의적인 공격으로 인해 웨이크업 토큰(Wake-up Token, WuT)이 비동기화 되는 문제에 대해 논의하였으며, 이를 해결하고자 복제 및 모방이 어려운 PUF 특성을 활용하였다. PUF는 물리적으로 무작위하고 고유한 디바이스의 특성을 활용하여 제조 과정에서 발생하는 미세한 물리적 차이를 활용하여 디바이스 간의 고유한 식별자를 생성하는 방식을 의미한다[15]. 이 고유성은 외부에서 복제나 모방을 어렵게 하며, 이를 통해 디바이스의 무결성을 보장한다. 이는 시스템의 신뢰성을 강화하는 데 핵심적인 역할을 한다. 제안하는 방식의 주요 절차는 다음과 같다. 먼저, 초기 WuT 설정 및 업데이트하는 과정을 수행한 뒤, WuT를 재동기화한다. 다음으로 그룹의 WuT를 설정하고 업데이트하는 과정을 반복한다. 제안하는 방식은 물리적 특성을 기반으로 작동하는 PUF을 토큰에 삽입함으로써 저전력 무선 통신 시스템에서 효율적인 에너지 관리가 가능함을 입증하였다. 하지만 PUF를 동기화하는 과정이 지속해서 발생하기 때문에 통신 복잡성이 증가하는 한계가 있다. 또한, WuT 토큰값을 업데이트하는 과정에서 동기화가 중단되는 문제가 발생할 수 있으므로, 이는 시스템의 정확한 동작을 방해하고 효율성 또한 감소시킬 수 있다.

WuR의 보안을 위한 프로토콜을 제안한 연구[14]에서는 WuR 장치의 취약성에 대해 논의하였으며, 이를 해결하고자 AMA-WuR(Anti-Malicious Attack WuR) 프로토콜을 제안하였다. 이는 DoSL(denial-of sleep) 공격, 스푸핑(spoofing) 공격에 센서 노드를 즉시 깨우지 않고, WuR AP(Access point)를 확인한 후 PCR(Primary Connectivity Radio)을 깨우는 방법이다. AP에 WuR ACK(acknowledgment)를 보내 공격을 알리고 이를 수신한 AP는 해당 WuR 장치에 새로운 WUID를 부여한다. WuR 장치가 이 WUID를 수신하면 새 WUID를 사용하여 ACK를 보내야 한다. 이 연구는 추가적인 과정들을 통해 센서 노드를 바로 깨우지 않는 방식으로, 에너지 소비 효율이 개선되었다. 하지만 이는 데이터 수신 속도가 느려지는 문제가 있다.

WuR의 보안성을 고려한 연구[8,11-14]에서 제안한 대응 메커니즘은 오버헤드가 증가하는 한계가 있어서 WuR 단말에 적합하지 않다. 반면, 제안하는 APSM 방식은 인증 과정이나 추가 통신 과정이 필요하지 않기 때문에 복잡도 측면에서 효율적으로 동작할 수 있다.

III. 저전력 웨이크업 리시버의 적응형 파워 세이빙 메커니즘

본 장에서는 배터리 소모 공격에 대응할 수 있는 WuR을 위한 적응형 파워 세이빙 메커니즘을 제안한다. 종래의 WuR 프로토콜은 웨이크업 신호가 발생하면, 서브 수신기(sub receiver)에서 웨이크업 신호(wake-up signal)를 감지하고 메인 수신기(main receiver)를 활성화하여 메인 수신기에서 데이터 패킷을 수신하도록 동작한다. 무선 단말은 별도의 인증 과정 없이 웨이크업 신호를 수신한 즉시 메인 수신기를 활성화하기 때문에 이러한 동작 방식은 심각한 보안 위협을 초래한다. 공격자는 안전하지 않은 웨이크업 신호 트리거링 취약점을 활용하여 서비스 거부 공격의 한 유형인 배터리 소모 공격을 수행할 수 있다[7]. 피해 단말은 절전 모드에 들어가지 못한 상태로 전력을 계속해서 소모하게 되고, 배터리가 고갈되거나 가용성을 보장받지 못하게 된다. 따라서 제안 모델에서는 배터리 소모 공격을 탐지한 후, 적응형으로 절전 모드의 시간을 조절하는 메커니즘을 제안하여 지속적인 배터리 소모 공격에 대응하고자 한다.

제안하는 APSM이 적용된 WuR의 구조는 Fig. 1.과 같다. 적응형 파워 세이빙을 수행하기 위해서, 종래 WuR 구조에 배터리 소모 공격을 탐지하는 모듈과 적응형 전력 관리 모듈을 추가하였다. APSM의 동작 과정은 다음과 같다. 먼저, 웨이크업 신호가 발생하면 서브 수신기는 웨이크업 신호를 감지한다. 다음으로, 배터리 소모 공격 탐지기(battery draining attack detector)는 웨이크업 신호가

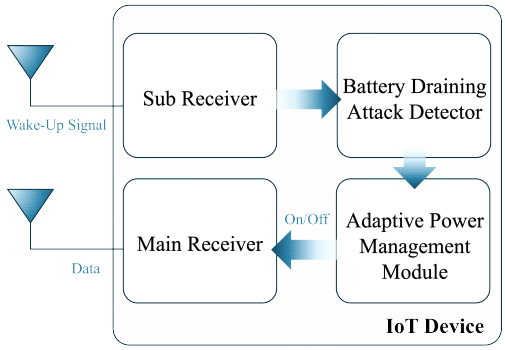

Fig. 1. APSM Structure

비정상적으로 발생한 신호인지 판단하고 메인 수신기의 활성화 여부를 결정하게 된다. 본 논문에서는 DoS 공격을 탐지할 때 주로 사용하는 모델[17] 중 하나인 랜덤 포레스트(random forest) 기반 이진 분류기로 배터리 소모 공격 탐지기를 구축하였다. 정상적인 신호로 판단하면 메인 수신기를 절전 모드(sleep mode)에서 데이터를 수신할 수 있는 활성 모드(awake mode)로 천이시킨다. 비정상적인 신호로 판단하면 적응형 전력 관리 모듈(adaptive power management module)을 동작시켜서 공격의 발생 빈도에 따라 적응형으로 절전 모드의 시간을 조절하고, 메인 수신기의 상태를 변화시키지 않는다.

Fig. 2.는 APSM에서 배터리 소모 공격을 탐지하고, 동적으로 파워 세이빙 시간을 결정하는 절차를 보여준다. 단말은 입력으로 들어오는 신호를 확인하여, 머신러닝 기반으로 배터리 소모 공격을 탐지한다. 비정상 신호로 판단하면 단말을 절전 모드로 천이하고, 절전 모드의 시간을 증가시킨다. 반면, 정상 신호로 판단하면 단말을 절전 모드에서 정상 모드로 천이하고, 다음에 진행되는 절전 모드의 시간을 감소시킨다.

종래의 방법은 저전력으로 동작하는 WuR의 공격 표면(attack surface)을 줄이기 위해서 토큰, PUF 기반의 일회용 인증 방식을 사용하거나 통신 과정을 추가하여 공격을 탐지하고 알람을 주는 방식을 적용했다. 그러나 이러한 방식들은 오버헤드가 증가하기 때문에 저전력으로 구동되어야 하는 WuR 단말에 적합하지 않다. APSM은 인증 과정이나 추가 통신 과정이 필요하지 않으므로 복잡도가 줄어서 저전력 아키텍처에서 동작할 수 있다. 그리고 배터리 소모 공격은 트리거 신호를 지속해서 발생시켜 짧은 시간 동안 리소스를 고갈시키는 특징이 있다. 종래의

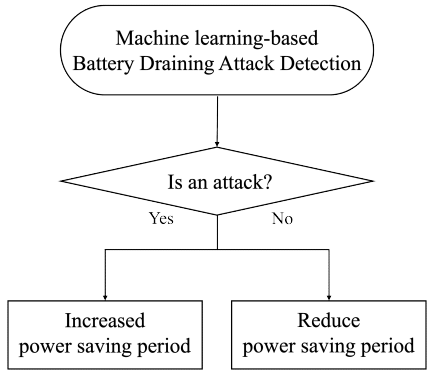

Fig. 2. APSM of Flowchart

WuR 보안 메커니즘을 적용하면, 오히려 에너지 소비가 증가하여 배터리 수명이 단축되는 결과를 초래한다. 따라서, 비정상 신호의 빈도가 잦을수록 파워 세이빙 시간을 기하급수적으로 증가시켜서 불필요한 에너지 소모를 줄이는 것이 효율적이다.

IV. 성능 평가

본 장에서는 WuR을 활용하는 무선통신 환경에서 종래 방식과 제안하는 APSM을 에너지 효율성과 지연시간 측면에서 비교 분석한다. 종래 방식은 탐지 및 대응 메커니즘이 없는 LPSM 방식과 일회용 토큰을 발급하여 인증을 수행한 후 WuR을 활성화하는 OTP(One Time Password) 방식으로 구현하였다. 머신러닝 기반의 배터리 소모 공격을 탐지하기 위해서 Fig. 1.의 APSM 시뮬레이션 모델을 구현하고, 네트워크 트래픽 데이터셋으로 UNSW-NB15[16]을 사용하였다. UNSW-NB15 데이터셋은 9가지의 공격 유형이 존재하는데, 그중 배터리 소모 공격에 해당하는 DoS 공격만 사용하여 정상 신호와 이진 분류를 진행했다. 전처리 과정을 통해 정상 신호와 공격 신호를 각 10,000개씩 총 20,000개로 데이터 전처리 과정을 진행하고, 훈련 데이터와 테스트 데이터를 7:3의 비율로 분할하여 1,000번 학습을 진행하였다. 랜덤 포레스트 모델로 이진 분류를 한 결과의 평균값은 Table 2.와 같다. 배터리 소모 공격의 탐지 정확도는 99.43%이고, 학습 결과를 예측하는 데 걸리는 시간인 latency는 평균적으로 0.151s가 소요되었다.

LPSM과 APSM의 에너지 소모량을 비교한 그래프는 Fig. 3.과 같다. 제안하는 APSM은 머신 러

Table 2. Machine learning-based Battery Draining Attack Detection Result

Performance Metrics	Result
Detection Accuracy(%)	99.43
Latency (s)	0.151
Precision (%)	99.43
Recall (%)	99.43
F1-Score (%)	99.43

닝 기반의 배터리 소모 공격 탐지 모델 분류 결과를 바탕으로 단말의 상태를 전환하고, 절전 모드의 시간을 결정한다. 반면, LPSM은 탐지 메커니즘이 없으므로, 신호의 유형에 상관없이 활성화 상태로 전환된다. WuR가 활성화 모드에 있는 경우와 절전 모드에 있는 경우의 에너지 소모량은 상용 WuR의 전류 소모량을 참고하여, 각 0.0072mA, 0.0008mA로 설정하였다[18]. LPSM은 정상 신호와 공격 신호 구분 없이, WuR이 웨이크업 신호를 수신하면 메인 수신기의 상태를 천이시키기 때문에 총 20,000개의 송신 신호에 대하여 144mA의 에너지를 소모한다. 반면 제안하는 APSM는 88mA의 에너지를 소모하여, LPSM 대비 대략 38.89% 에너지를 절약하였다. 이는 머신 러닝 기반 탐지 모델을 사용하여 공격 신호를 정확하게 식별하고, 공격 신호가 수신될 때마다 메인 리시버를 절전모드로 천이하고, 절전모드 시간을 2^n씩 증가시켰기 때문이다.

Fig. 4.는 전체 수신 트래픽 중 공격 트래픽 비율(α)에 따른 종래 방식과 제안 방식의 에너지 효율성을 나타낸다. α 값이 0에 가까울수록 정상 신호가

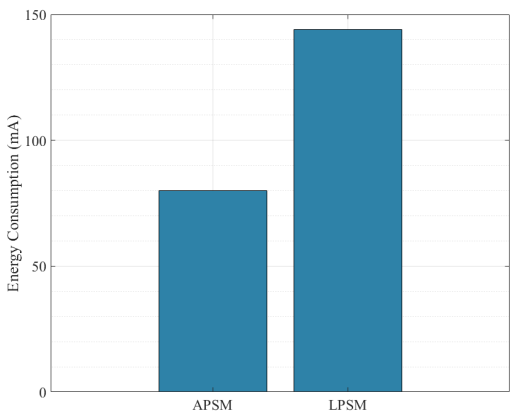

Fig. 3. Energy Consumption Based on Binary Classification Results of UNSW-NB15 Dataset

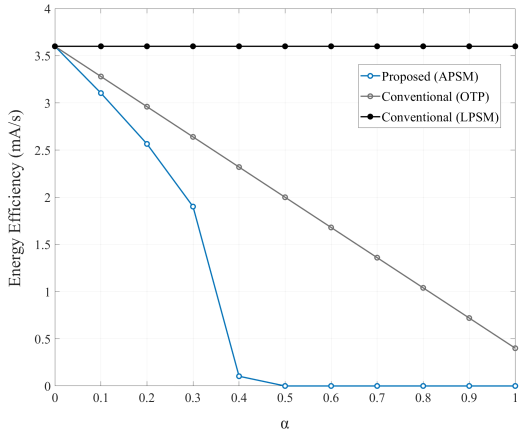

Fig. 4. Energy Efficiency based on the Ratio of Attack Traffic to Total Received Traffic

많이 발생하는 경우이고, α 값이 1에 가까울수록 공격 신호가 많은 상황을 나타낸다. 각 방식이 총 10,000바이트의 20,000개의 신호를 처리하는 데에 소모한 에너지와 시간을 측정하여, 초당 에너지 사용량으로 에너지 효율성(energy efficiency)을 계산하였다. 이때, 활성 상태의 에너지는 0.0072mA, 절전 상태의 에너지는 0.008mA를 소모한다. LPSM은 정상 신호와 공격 신호를 구분하는 메커니즘이 없으므로, α 값에 관계없이 3.6mA/s의 에너지 효율성을 유지한다. 종래의 OTP 방식은 8바이트의 일회용 토큰을 발급하여 인증을 수행한 뒤, 토큰 값이 일치하면 WuR을 활성화하기 때문에 LPSM 방식보다 에너지 효율이 개선된다. 그러나 일회용 토큰 발급 및 인증 과정에서 발생하는 오버헤드로 인해서 제안하는 APSM 방식보다는 에너지 소모가 크다. 반면, APSM은 공격 신호가 발생하면 파워 세이빙 시간을 2^n씩 증가시키기 때문에 α 값이 증가할수록 에너지 효율이 개선되는 결과를 보인다. 특히 공격이 잦은 환경에서 제안 방식의 에너지 효율이 크게 개선된 것을 확인할 수 있다. 공격 신호가 10%일 때(α=0.1), APSM의 에너지 효율성은 대략 3.104mA/s로 LPSM 대비 대략 13.77%, OTP 방식 대비 대략 5.3% 에너지 효율을 개선하였다. 공격 신호가 40%일 때(α=0.4), APSM은 LPSM보다 약 99.13%, OTP 방식 보다 95.5%의 에너지 효율을 개선하였다.

Fig. 5.는 전체 수신 트래픽 중 공격 트래픽 비율(α)에 따른 종래 방식과 제안 방식의 지연 시간(latency)을 나타낸다. α 값이 0에 가까울수록 정

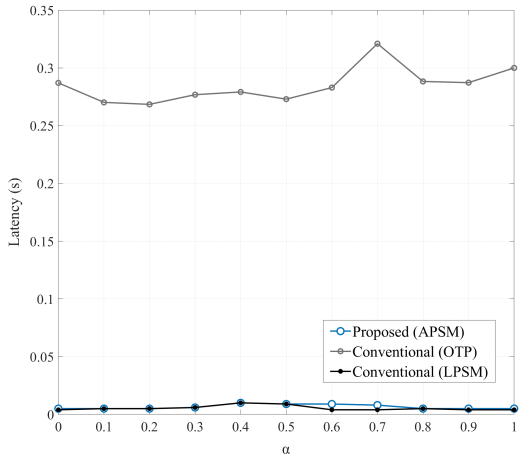

Fig. 5. Latency based on the Ratio of Attack Traffic to Total Received Traffic

상 신호가 많이 발생하고, α 값이 1에 가까울수록 공격 신호가 많이 발생한다. 지연 시간은 공격 신호에 대응하는 데 소요 되는 시간으로, 파이썬 time 모듈의 time 함수를 사용하여 계산하였다. OTP 방식은 일회용 토큰을 발급하고 인증하는 과정에서 오버헤드가 발생하여 LPSM 방식과 APSM 방식보다 지연 시간이 큰 폭으로 증가하였다. 반면, 제안하는 APSM 방식은 대응 메커니즘이 없는 LPSM 방식보다 평균적으로 15%의 지연 시간이 발생했지만, OTP 방식보다는 평균 95%의 지연 시간을 줄였다. 따라서 APSM 방식은 배터리 소모 공격으로 인한 에너지 소모를 줄이고, 공격에 대응하는 지연 시간을 개선함을 확인하였다.

V. 결 론

IoT는 산업과 일상생활의 모든 측면에서 널리 활용되고 있어서 저전력 요건을 충족해야 하는 IoT 장치 특성상 배터리 라이프 타임을 효율적으로 관리하는 것은 중요하다. 그러나, 배터리 소모 공격이나 간섭으로 인해 배터리 라이프 타임이 심각하게 단축되는 문제가 있다. 종래 IoT 장치의 에너지 소모를 최소화하기 위한 표준 기술은 지연시간과 오버헤드를 줄이기 위해서 별도의 보안 메커니즘을 마련하지 않았다. 따라서 본 논문에서는 저전력 웨이크업 리시버를 위한 적응형 파워 세이빙 메커니즘을 제안한다. 머신러닝 기반의 배터리 소모 공격 탐지 모델을 바탕으로 에너지 소모량을 비교한 실험에서는 제안하는 적응형 파워 세이빙 메커니즘이 종래의 레거시 파워 세이빙 메커니즘 대비 38.89%의 에너지를 절약하였다. 그리고 공격 신호의 비율에 따른 에너지 효율성을 비교한 실험에서는 제안 모델이 종래의 방법 대비 공격 트래픽이 전체 트래픽의 10% 이상일 때, 13.77% 이상의 에너지 효율을 개선하였다. 따라서 제안하는 방법은 지속적으로 다량의 신호를 발생시켜서 짧은 시간 안에 리소스를 고갈시키는 배터리 소모 공격에 대응할 수 있는 효율적인 메커니즘임을 확인하였다. 향후 연구에서는 파워 세이빙 시간을 증가시키면 발생하는 가용성 문제를 해결하기 위해서 한 링크가 파워 세이빙 모드에 있더라도 다른 링크를 통해 정상 트래픽을 수신할 수 있도록 멀티링크를 적용한 연구를 진행하고자 한다.

References

[1] Abdul Matin, Md Rafiqul Islam, Xianzhi Wang, Huan Huo, and Guandong Xu, "AIoT for sustainable manufacturing: Overview, challenges, and opportunities," Internet of Things, vol. 24, Aug. 2023.

[2] C.-C. Liao and C.-C. Chen, "Research on the use of AIoT and 5G in Mobile Commerce," 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), pp. 1-2, Sep. 2021.

[3] B. Jolly, "The Last Thing IoT Device Engineers Think About: End of Battery Life Behavior for IoT Devices," 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 837-840, Aug. 2019.

[4] M.C. Caballé, A.C. Augé, E. Lopez-Aguilera, E. Garcia-Villegas, I. Demirkol and J.P. Aspas, "An Alternative to IEEE 802.11ba: Wake-Up Radio With Legacy IEEE 802.11 Transmitters," IEEE Access, vol. 7, pp. 48068-48086, Apr. 2019.

[5] D.-J. Deng et al., "IEEE 802.11ba:

Low-Power Wake-Up Radio for Green IoT," IEEE Communications Magazine, vol. 57, no. 7, pp. 106-112, July 2019.
〔6〕 D.-J. Deng, S.-Y. Lien, C.-C. Lin, M. Gan and H.-C. Chen, "IEEE 802.11ba Wake-Up Radio: Performance Evaluation and Practical Designs," IEEE Access, vol. 8, pp. 141547-1415 57, Jul. 2020.
〔7〕 Il-Gu Lee, Kyungmin Go, and Jung Hoon Lee, "Battery Draining Attacks and Defense against Power Saving Wireless LAN Devices," Sensors, Vol. 20, No. 7, Apr. 2020.
〔8〕 A.T. Capossele, V. Cervo, C. Petrioli and D. Spenza, "Counteracting Denial-of-Sleep Attacks in Wake-Up-Radio-Based Sensing Systems," 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1-9, Jun, 2016.
〔9〕 M.N. Bhuiyan, M.M. Rahman, M.M. Billah and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10474-10498, Jul. 2021.
〔10〕 Sun-Woo Yun, Na-Eun Park and Il-Gu Lee, "Wake-up Security: Effective Security Improvement Mechanism for Low Power Internet of Things," Intelligent Automation & Soft Computing, Vol. 37, No. 3, pp. 2897-2917, Sep. 2023.
〔11〕 R. Falk and H.-J. Hof, "Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks," 2009 Third International Conference on Emerging Security Information, Systems and Technologies, pp. 191-196, 2009.
〔12〕 Pradeep Sudhakaran, Malathy C, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," 2019 Special Issue: CapsNet-based computing in cognitive communications, vol. 35, Nov. 2019.
〔13〕 A. Oun and M. Niamat, "PUF-Based Authentication for the Security of IoT Devices," 2023 IEEE International Conference on Electro Information Technology(eIT), pp. 067-070, Jul. 2023.
〔14〕 H. Park, "Anti-Malicious Attack Algorithm for Low-Power Wake-Up Radio Protocol," IEEE Access, vol. 8, pp. 127581-127592, Jul. 2020.
〔15〕 U.K. Anchana, S. Singh, M. Mogireddy and E. Kadavergu, "Design And Analysis Of Physical Unclonable Function," 2023 2nd International Conference for Innovation in Technology (INOCON), pp. 1-4, Apr. 2023.
〔16〕 N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 Military Communications and Information Systems Conference (MilCIS), pp. 1 - 6, Dec. 2015.
〔17〕 A. Raza, K. Munir, M.S. Almutairi and R. Sehar, "Novel Class Probability Features for Optimizing Network Attack Detection With Machine Learning," IEEE Access, vol. 11, pp. 98685-98694, Sep. 2023.
〔18〕 I. Demirkol, C. Ersoy and E. Onur, "Wake-up receivers for wireless sensor networks: benefits and challenges," IEEE Wireless Communications, vol. 16, no. 4, pp. 88-96, Aug. 2009.

〈저자소개〉

김 소 연 (So-Yeon Kim) 학생회원
2021년 2월: 성신여자대학교 융합보안공학과 학사 졸업
2023년 2월: 성신여자대학교 미래융합기술공학과 석사 졸업
2023년 3월~현재: 성신여자대학교 미래융합기술공학과 박사과정
〈관심분야〉 통신 네트워크 보안, 융합보안, 정보보호

윤 성 원 (Seong-Won Yoon) 학생회원
2021년 3월~현재: 성신여자대학교 융합보안공학과 학사과정
〈관심분야〉 정보보호, IoT 보안

이 일 구 (Il-Gu Lee) 종신회원
2003년 2월: 서강대학교 전자공학 학사
2005년 2월: KAIST 정보통신 석사
2016년 2월: KAIST 전산학부 박사
2005년 2월~2017년 2월: 한국전자통신연구원 선임연구원
2017년 3월~현재: 성신여자대학교 융합보안공학과/미래융합기술공학과 부교수
〈관심분야〉 융합보안, 정보보호, 정보통신