이 일 구 교수 지도

석사학위 청구논문

사물인터넷을 위한 저전력 보안 아키텍처

2022

성신여자대학교 대학원

미래융합기술공학과

윤 선 우

사물인터넷을 위한 저전력 보안 아키텍처

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2021년 11월

성신여자대학교 대학원
미래융합기술공학과
윤 선 우

인 준 서

윤선우의 석사학위 논문으로 인준함

2021년 11월

심사위원장 김 성 민 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

심 사 위 원 임 연 섭 (서명 또는 인)

성신여자대학교 대학원

논문 개요

사물인터넷은 통신 네트워크 기술과 센서를 활용하여 시공간의 제약 없이 사람과 사물을 유기적으로 연결하고, 실시간으로 데이터를 송수신하여 수집, 저장, 분석할 수 있는 기술이다. 전 산업 분야에서 활용되고 있는 사물인터넷은 개체 수가 증가하고 이용 범위가 증가하면서 네트워크 연결 범위가 확장되었으며, 그에 따라 보안 솔루션에 대한 고려는 필수 요소가 되었다. 그러나 디바이스의 크기, 메모리 용량, 데이터 전송 성능 제약 때문에 고성능 보안 모듈을 적용하기 어렵다. 종래 연구에서는 주로 암호화 알고리즘을 경량화하여 전력 소모량을 감소시켰으나 보안 성능도 함께 열화되는 문제 때문에 대규모 정보 시스템 및 네트워크를 대상으로 고도화, 지능화된 공격을 방어하기 어렵다.

본 연구에서는 사물인터넷 환경에서 고성능의 보안 알고리즘을 활용할 수 있는 저전력 보안 아키텍처인 Wake-Up Security (WUS)를 제안하였다. WUS는 사물인터넷 플랫폼 내 이상 탐지를 수행하는 작은 로직을 추가하여 이상 탐지 결과에 따라 필요한 경우에만 보안 모듈을 실행시켜 이상 탐지가 발생하지 않는 경우에는 적은 전력만 소모할 수 있다. 따라서 주기적으로 고성능 보안 모듈이 실행되는 종래 방식 대비 저전력 환경에서 상대적으로 복잡도가 높은 보안 모듈을 활용하면서도 보안성과 전력 효율성을 제공할 수 있다.

제안하는 WUS의 평가를 위해 UNSW-NB15 (University of New South Wales Network Based 2015) 데이터셋 기반의 Python 시뮬레이터를 구현하여 성능을 비교하였다. 고성능 보안 모듈을 사용하는 종래 방식 및 경량 보안 모듈을 사용하는 종래 방식을 전력 소모량, 지연시간, 보안

성능 측면에서 비교 및 평가했다. 평가 결과에 따르면 제안 모델의 전력 소모량은 종래의 고성능 보안 모듈 대비 약 51.8%, 경량 보안 모듈 (2) 대비 약 27.2% 낮은 누적 전력량을 소모하였으며, 약 74.8%, 65.9% 낮은 누적 지연시간을 보였다. 반면, 공격 빈도가 높은 경우, 일부 구간에서 제안 모델이 더 높은 전력소모량과 지연시간을 보였다. 마지막으로, 보안 성능 측면에서 제안 모델은 평균적으로 약 96.5% 이상의 높은 탐지 정확도를 보였으며, 종래 모델 대비 약 33.5% 더 개선된 탐지 효율 성능을 입증하였다.

목 차

표 차 례

그림 차례

제 1 장 서론

1. 연구배경 및 목적

사물인터넷(Internet of Things, IoT) 기술은 각종 사물에 센서와 유·무선 통신 기술을 사용하여 데이터를 수집, 저장, 분석하는 기술로 상호 연결된 장치 시스템을 말한다[1]. 사물인터넷의 모든 개체는 자체적으로 식별을 위한 ID를 가지고 있으며, 통신, 감지, 계산 기능을 수행한다. 이러한 기술들은 Industry 4.0 환경에서 생산성을 향상시키고 업무를 자동화하는 기능을 제공한다. 사물인터넷 시장은 2025년까지 1,310억 달러 규모로 성장하고, 사물인터넷 네트워크는 750억 개 이상의 디바이스를 연결하는 규모로 성장할 것으로 예상된다. 이처럼 사물인터넷은 제조, 에너지, 홈, 교통, 재난, 의료 등 다양한 분야에서 필수적이자 효율적인 기술로써 활용될 것으로 기대된다[2].

사물인터넷 개체의 수가 증가할수록 수십억 개의 사물인터넷 기기들은 더 큰 무선 네트워크에 연결될 것이며, 이때 송・수신되는 모든 데이터는 수집 후 다른 개체 혹은 서버로 전송되어 활용되기 때문에 사물인터넷을 위한 보안 솔루션에 대한 고려는 필수적이다. 특히, 사물인터넷에서 송수신되는 데이터는 기밀성과 무결성이 유지되어야 하므로 사물인터넷 보안 및 개인정보 보호는 해결해야 할 중요한 문제이다[3]. 하지만 사물인터넷 장치로 구성된 노드들은 대부분 배터리로 작동하기 때문에 데이터 처리 능력이 낮고, 저장소와 대역폭이 제한되므로 완전한 보안 제품군을 적용하기 어렵다[4]. 즉, 지속적인 데이터 수집 및 공유, 다른 장치의 제어와 같은 핵심 기능 수행을 위한 컴퓨팅 성능을 유지하면서 객체 및 프로토콜 인증, 데이터 보호, 이상 탐지 등을 수행하기 위한 리소스가 부족한 환경을 가지고 있기 때문에 복잡도가 높은 보안 솔루션을 활용하기 어렵다. 종래에는 데이터 저장 공간과

처리 능력의 한계를 가진 사물인터넷의 보안을 실현하기 위해 데이터 처리, 전력 소비, 배터리 수명 요구사항에 맞춘 새로운 보안 아키텍처를 제안하거나 종래의 보안 솔루션을 조합하여 활용하는 방안에 관한 연구가 진행되었다. 그 중 사물인터넷을 구성하는 요소의 에너지 소비를 감소시키기 위해 상대적으로 적은 전력을 필요로 하거나 소모하는 센서 및 통신 기술을 채택하거나 전력 공급 시스템을 개선하는 방안들이 제안되었다[5].

디지털 통신 환경에서 송수신되는 데이터의 오남용을 방지하기 위해 암호화 기법을 주로 사용하므로 암호화 알고리즘에 관한 연구도 다수 진행되었다. 예를 들어, 서비스 품질을 유지하면서 고효율의 보안 기능을 제공하는 방법으로 대칭 및 비대칭 암호화 솔루션을 새롭게 조합하거나 새로운 경량 보안 아키텍처를 제안하는 연구가 진행되었다[6]. 사물인터넷을 활용하는 산업 분야가 점차 확산되고 다양한 크기와 형태의 장치들이 등장하면서 RSA((Rivest - Shamir - Adleman), DSA(Digital Signature Algorithm), PRESENT 등과 같은 경량 암호화 알고리즘들의 낮은 전력 소비를 이점으로 데이터를 인증하고 보호할 수 있다[7]. 이처럼 장치의 전력 및 컴퓨팅 능력의 제한이 존재하는 환경에서는 사물인터넷 장치의 적은 자원을 사용하는 것을 목표로 하며, 보안 기능 역시 기술적 한계를 고려한 보안 아키텍처를 기반으로 설계되어야 한다[8].

한편, 기술이 발전함에 따라 무선 네트워크에 연결된 개체의 수가 많아지고 복잡해질수록 더 높은 보안 수준이 요구되지만, 사물인터넷 환경에 맞추어 경량 보안 아키텍처가 제공할 수 있는 보안 성능과 확장성에는 한계가 있다. 즉, 고성능의 보안 모듈을 활용할수록 모듈의 복잡도가 커지면서 더 많은 에너지를 소비하게 되는 전력 소모와 보안 성능 간의 trade-off 문제를 야기한다.

이와 같은 문제를 해결하기 위해서는 특정 기능을 수행하는 모듈을 경량

화하는 방식이 아닌 새로운 접근 방식의 연구가 필요하다. 제한된 리소스를 가지는 환경에서 시스템 및 보안 성능을 일정 수준 이상으로 유지하면서 전력을 효율적으로 관리하는 방법이 필요하다. 즉, 사물인터넷 플랫폼에 고성능의 보안 솔루션을 적용할 수 있는 저전력 보안 아키텍처에 관한 연구가 요구된다.

본 논문에서는 사물인터넷 플랫폼에 이상 탐지를 수행하는 로직을 추가하여 위협을 감지할 경우에만 고성능 보안 모듈을 동작시키는 저전력 보안 아키텍처인 Wake-up Security (WUS)를 제안한다. WUS는 이상 행위 여부와 상관없이 주기적으로 보안 모듈 전체를 실행하여 에너지가 소비되는 종래 방식 대비 평소에는 이상 탐지를 위한 로직만 깨어나 적은 에너지를 소모하다가 필요한 경우에만 많은 에너지를 소모하기 때문에 저전력 환경에서 전력 효율성을 개선할 수 있다. 이는 보안 성능과 확장성의 한계를 가지는 경량 솔루션의 문제를 해결하고, 사물인터넷 플랫폼과 서비스 수준에 적합한 높은 수준의 보안 성능과 전력 효율성을 제공할 수 있다. 제안하는 WUS 메커니즘을 평가하기 위해 UNSW-NB15 데이터셋 기반의 파이썬 시뮬레이터를 통해 고성능 보안 모듈 및 경량 보안 모듈을 활용하는 종래 모델과 제안 모델의 전력 소모량, 지연시간, 보안 성능을 측정하여 비교・분석하였다.

2. 논문 구성

본 논문은 다음과 같이 구성된다. 2장에서는 사물인터넷의 개요와 사물인터넷 보안 취약점에 관한 종래의 연구 결과를 소개하고, 리소스 제한적인 사물인터넷 보안을 위한 종래의 경량 보안 기법에 관한 연구들을 정리한다. 3장에서는 WUS 메커니즘을 제안하며, 4장에서는 종래 모델과 제안하는 WUS 모델의 성능을 전력 소모량, 지연시간, 보안 성능 측면에서 시뮬레이션을 통해 비교・검증한다. 마지막으로 5장에서는 결론을 내리고 향후 연구 방향에 대해 논의한다.

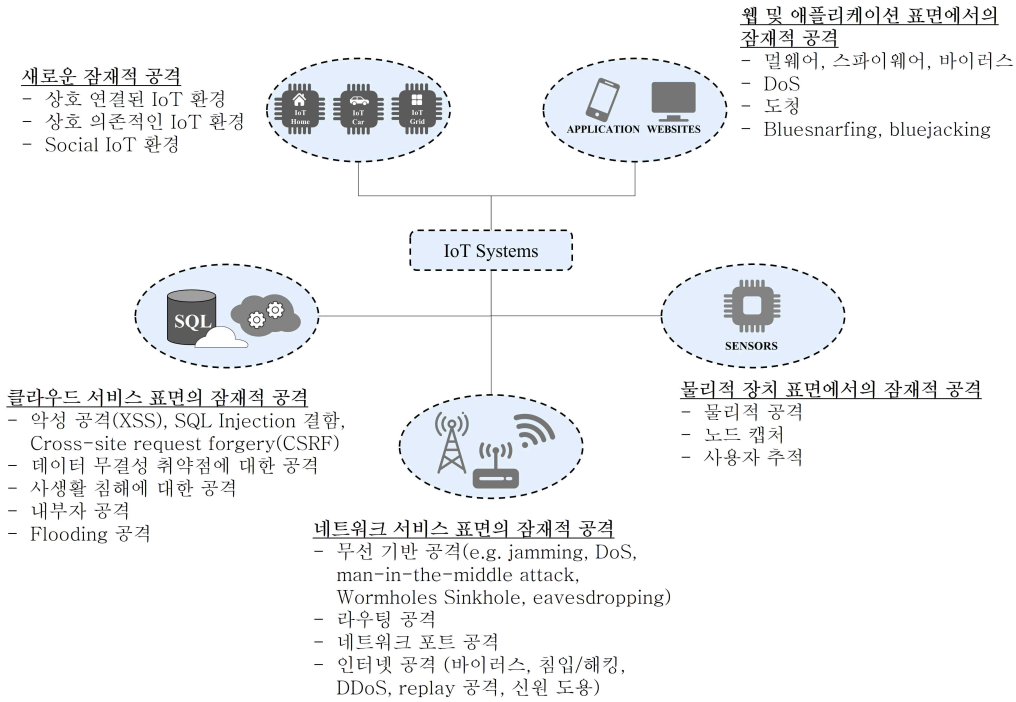
제 2 장 사물인터넷을 위한 보안 솔루션

1. 사물인터넷 개요

사물인터넷은 1998년 P&G사의 케빈 애쉬튼에 의해 도입되었다. 사물인터넷은 인터넷과 유비쿼터스 컴퓨팅 (Ubiquitous Computing)의 미래를 뜻하는 용어로서, 가전제품, 차량, 기계장치 등을 포함한 사물과 인간이 인터넷 상으로 연결된 상태를 의미한다[9]. 사물인터넷은 사람이 직접적으로 개입할 필요 없이 스마트 센서 및 사물 간 협력을 통해 새로운 애플리케이션을 제공하는 것을 전제로 한다[10]. 인터넷, 모바일 환경과 스마트 기기 간의 연결 절차인 M2M (Machine-to-Machine) 기술은 사물인터넷의 기초 단계로 분류되며, RFID (Radio-Frequency Identification) 및 기타 센서들을 일상 속 사물과 결합하여 사물인터넷을 구축할 수 있다.

사물인터넷은 시공간의 제약 없이 모든 사물과 인간의 연결을 인증하는 것을 목적으로 하므로 보안, 통신, 최적화, 법적 권리 등 다양한 측면에서 발생 가능한 문제점을 개선해야 할 필요가 있다. 종래에는 사물인터넷을 위한 보안 솔루션을 도출하기 위해 사물인터넷이 가진 보안 취약점을 분류하고 분석하는 연구들이 다수 진행되었다. 특히, 권한이 없는 사용자가 시스템에 접속하여 데이터를 추출할 수 있는 잠재적 위협에 대해 공격 표면(Attack Surface)을 정의하였다. 일반적으로 공격 표면은 물리적 장치, 네트워크, 클라우드, 웹 및 애플리케이션 인터페이스로 분류할 수 있다[11]. 사물인터넷은 RFID와 센싱 기술과 같은 하드웨어 장치를 포함할 수 있으며, 이 장치들은 실시간으로 사물 간 처리를 감독하고 상호작용하는 역할을 수행한다. 물리적 장치는 회로의 크기에 따라 사용 가능한 리소스의 제약이 있으며, 자연 재해, 단순 사고, 물리적 공격으로 인한 손실의 위협을 수반한다.

사물인터넷 장치들은 유·무선 네트워크로 연결되며, 네트워크 기술은 사물인터넷 시스템에서 필수적인 구성 요소이다. 사용자에게 높은 수준의 서비스를 제공하기 위해서 사용자 및 기기 간 네트워크 규모 및 이동성은 확장될 수 있으나, 이에 따라 네트워크 서비스 표면을 넓혀지면서 해킹, 스푸핑, DoS (Denial of Service), Man-in-the-Middle 공격과 같은 잠재적 보안 위협에 노출될 수 있다[12]. 클라우드 컴퓨팅 기술은 시공간의 제약 없이 공유 서비스의 리소스에 대해 원격 엑세스가 가능하도록 하며 정보 수집 및 공유를 용이하게 만든다. 사물인터넷 플랫폼의 주요 제약 조건인 리소스 한계를 극복하기 위한 수단으로 활용할 수 있으며[13], 사물인터넷의 비전을 실현하기 위한 기반 기술로서 플랫폼 역할을 수행할 수 있다[14]. 그러나 CSRF (Cross-Site Request Forgery), SQL injection (Structured Query Language injection), XSS (cross-site scripting)와 같은 무단 엑세스 기반 악의적인 공격에 취약하며 무결성 제어가 어려우므로 데이터베이스 유출 및 개인 정보 보호 문제를 야기할 수 있다. 웹 및 애플리케이션 라이선스 인터페이스의 경우, 대부분의 원격 액세스 서비스와 모바일을 통해 서비스가 제공되기 때문에 개인 정보 및 민감 정보가 약용될 우려가 있다. 이에 따라 멀웨어, 스파이웨어 및 DoS, 도청 등의 공격이 발생할 수 있으나, 모바일 운영체제의 개방적인 특징으로 인해 제3자의 철저한 보안 검사가 어렵다는 한계가 있다[15, 16]. 이 외에도 사물인터넷 환경의 상호 연결적인 특징과 상호 의존적 특징 등으로 인해 기존에 논의되지 않은 새로운 공격에 대한 취약성을 내포할 수 있다. [그림 1]은 사물인터넷의 공격 표면에 대해 정리한 것이다.



[그림 1] 사물인터넷 공격 표면[11]

(*본 그림은 [11]의 'Figure 5 IoT attack surfaces'를 재가공했음)

[그림 1]과 같은 위협으로부터 사물인터넷 플랫폼을 보호하기 위해서는 지속적인 모니터링을 통한 잠재적 위협 식별과 차단이 필요하다. 다양한 측면에서의 보안 위협에 대응하고, 보안 서비스를 제공하기 위해 종래에는 보안 서비스 종류에 따른 보안 메커니즘을 제공하고 있다. [표 1]은 사물인터넷의 보안 서비스 별 보안 메커니즘의 종류와 예시를 정리한 것이다.

[표 1] 보안 서비스 기반의 보안 메커니즘 예시[6]

보안 서비스[17]	보안 메커니즘	예시
기밀성	메시지 암호화/서명 암호화	대칭 암호화 메커니즘(AES (Advanced Encryption Standard-256), CBC (Cipher Block Chaining) 등), 비대칭 암호화 메커니즘 (RSA, DSA, IBE (Identity-based encryption), ABE (Key-Policy Attribute-Based Encryption) 등)
무결성	해시 기능, 전자 서명	해시 기능(SHA-256 (Secure Hash Algorithm), MD5 (Message-Digest algorithm 5) 등), 메시지 인증 코드(HMAC, keyed-hash message authentication code, hash-based message authentication code)
가용성	주파수 도약 확산 스펙트럼, 접근 제어, 침입 방지 시스템, 방화벽	서명 기반 침입 탐지, 통계적 이상 기반 침입 탐지
부인방지	전자 서명	ECDSA (Elliptic Curve Digital Signature Algorithm), HMAC
인증	해시 체인, 메시지 인증 코드	HMAC, CBC-MAC (Cipher Block Chaining Message Authentication Code), ECDSA
프라이버시	가명성, 연계불가성, k-익명성, 영지식 증명(ZKP, Zero-Knowledge Proof)	EPID (Enhanced privacy Industrial Design), DAA (Direct Access Archive), 페더슨 커밋먼트

종래 디지털 통신 환경에서는 송수신되는 데이터의 오남용을 방지하기 위해 데이터 암호화 기법을 주로 활용하고 있다. 종래에는 사물인터넷이 가지는 리소스 제약을 극복하기 위해 암호 알고리즘 및 구조를 경량화하는 연구가 다수 진행되었으며, 다음 섹션에서는 사물인터넷을 위한 경량 보안 기법에 관하여 정리하였다.

2. 사물인터넷을 위한 경량 보안 기법

1) 경량 암호 알고리즘

종래 디지털 통신 환경에서는 송수신되는 데이터의 암호화 및 인증을 수행하고, 데이터의 오남용을 방지하기 위해 주로 암호화 기법을 사용하고 있다. 그 중 사물인터넷과 같이 물리적 장치를 포함하여 리소스 제약적인 환경에서는 전통적 암호 알고리즘을 적용하는 것이 적합하지 않으므로 저전력 환경에서 활용할 수 있는 경량 암호 알고리즘에 관한 연구가 활발히 진행되고 있다[18]. [표 2]는 대표적인 경량 암호 알고리즘을 정리한 것이다.

[표 2] 경량 암호 알고리즘[19]

암호화 알고리즘	설명	블록 크기	키 길이	참고	특징
AES	NIST (National Institute of Standards and Technology)에 의해 표준화 된 블록 암호 알고리즘으로 가장 널리 사용됨, SPN (Substitution Permutation Network Structure) 구조	128bits	128, 192, 256bits	[20]	8비트 단위 연산, 사물인터넷의 마이크로프로세서에 적합
ARIA (Academy, Research Institute, Agency)	국내에서 개발한 블록 암호 체계, SPN 구조	128bits	128, 192, 256bits	[21]	대부분 XOR (exclusive or)과 같은 단순한 바이트 연산

KLEIN	Gong 등이 제안한 블록암호로, SPN 구조	64bits	64, 80, 96bits	[22]	성능 제약적인 무선 센서와 RFID에 적합하도록 설계된 소프트웨어, 하드웨어에서 컴팩트한 구현이 가능
PRESENT	Bodganov 등이 제안한 AES 기반 블록 암호	64bits	80bits	[23]	AES 대비 암호화 강도가 떨어지나 면적과 소비 전력을 개선하여 RFID, smart card, USN (Ubiquitous Sensor Network)과 같은 시스템에 최적화함, AES 대비 2.5배 작은 하드웨어 설계 가능
LEA (Lightweight Encryption Algorithm)	Hong 등이 제안하였으며, Feistel 구조	128bits	128, 192, 256bits	[24]	현재까지 알려진 모든 블록 암호에 대한 공격에 대해 안전하며, 키 스케줄 특성에 기인한 이론적 취약성이 존재하지 않음

CLEFIA	SONY에서 발표한 AES와 유사한 블록 암호, Feistel 구조	128bits	128, 192, 256bits	[25]	내부 함수에는 2종류의 sbox 데이터 처리부와 스케줄링을 통해 암/복호화
KATAN	ARX (Addition, rotation, eXclusive-or) 기반의 암호화 알고리즘	32, 48, 64bits	80bits	[26]	non-linear, boolean, shift, xor 연산으로 구성됨
QTL	일반화된 Feistel 네트워크 구조를 변형한 초경량 블록 암호, 암호화 및 암호 해독 프로세스 동일	64bits	64, 128bits	[27]	제한된 응용 프로그램에서 더 적은 영역을 차지, 하드웨어 구현 중 전력 소비 비용 감소
ANU	Bansod 등이 제안하였으며, 25개의 라운드로 구성된 초경량 암호, Feistel 구조	64bits	80, 128bits	[28]	MITM (Man in the Middle), Zeroday 및 Biclique와 같은 기본 및 고급 공격에 저항 가능

[표 2]의 암호 알고리즘 외에도 수많은 경량 암호 알고리즘 존재하며, 현재까지도 암호 알고리즘을 경량화하기 위한 연구들이 다수 진행되고 있다. 종래의 경량 암호 알고리즘은 주로 전통적인 경량 암호를 개선하거나 특정 환경에 적합한 새로운 방식의 암호 알고리즘을 제안하였으며, 알고리즘의 구조 및 블록 크기 경량화와 수식 간편화를 수행함으로써 경량 암호 알고리즘을 실현하였다[29]. 이처럼 종래에는 리소스 제약적인 사물인터넷의 한계를 극복하기 위해 암호 알고리즘을 경량화하는 방안에 관한 연구가 다수 진행되었다. 반면, 암호를 경량화하지 않고 특정 기능을 수행하는 모듈을 더 적은 전력을 소모하는 다른 모듈로 대체하거나 분산형 블록체인, 클라우드, 기계 학습과 같은 별도의 기술을 융합한 저전력 보안 솔루션들도 제안되었다.

2) 저전력 환경을 위한 보안 솔루션

전통적 암호 알고리즘을 경량화하고 성능을 개선하는 것이 아닌 타 기술과의 융합 보안 솔루션을 제시하거나 저전력 보안 아키텍처들에 관한 연구들이 다수 진행되었다. [표 3]은 저전력 환경을 위한 보안 솔루션에 관한 연구들의 핵심내용과 한계점 및 고려사항을 정리한 것이다.

[표 3] 저전력 환경을 위한 보안 솔루션에 관한 연구

참고 문헌	분류	설명	고려사항
[30]	프레임워크	• 다단계 신뢰 관리와 결합된 보안 및 개인정보보호 프레임워크 • 혼합 암호 알고리즘과 일반 텍스트 및 암호 쌍을 기반으로 하는 경량 암호 도입 및 사용자 중심의 개인 정보 보호 서비스 제공 • 의료 서비스 긴급 상황에서 보호 누설을 제한하면서 대	• 기회주의적 컴퓨팅과 지원 노드 선정 과정 중 신뢰 수준에 따른 처리 방식에 대해 순간 판단 오류가 발생할 수 있음 • 집단 내 신뢰 수준에 관한 규칙에 따라 보안 수준 및 전력 효율성 차이 존재 • 신뢰 수준이 높은 노드

		량의 PHI (Personal Health Information)를 등록하기 위해 처리 능력과 기능을 빠르게 축적 가능	가 짧은 길이의 키를 사용하여 보안 성능이 열화됨
[31]	아키텍처	• 스마트 농업을 위한 저전력, 저비용 IoT 네트워크 • 토양 수분 함량 모니터링을 위해 자체 개발 센서인 IITH mote를 싱크 및 센서 노드로 사용 • 적은 전력, 낮은 비용으로 평균 83% 연장된 수명	• 특정 기능을 수행하는 센서 및 모듈에 종속적임 • 전력소모량 및 비용, 수명은 개선되었으나 보안 성능에 대한 고려가 없음
[32]	아키텍처	• 장거리 센서 네트워크를 위한 네트워크 및 데이터 전송 아키텍처 • oneM2M IoT 표준 기반 • IN (Infrastructure Node), MN (Middle Node) 및 ASN (Application Service Node)을 네트워크 요소로 가짐 • 네트워크 서버가 제어하는 게이트웨이의 클론을 사용하여 병목 현상을 피하고, 대기로 인한 트래픽 부하 및 종단 간 전송 지연 감소로 처리량 향상	• oneM2M의 인터페이스 및 기능에 종속됨 • 게이트웨이에서 계산한 지연 시간과 시스템 상태 정보를 네트워크 서버에 보고하므로 중앙 집중 시스템으로 인한 보안 침해 가능성 존재 • IoT 네트워크 서버가 트래픽 부하 균형을 조정하므로, 트래픽 부하에 대해 사후 대책이 될 수 있음
[33]	아키텍처	• 클라우드 서버와 결합된 IoT 기반 아키텍처에 대한 인증 체계 • 단방향 해시 함수 및 배타적 논리합 연산과 같은 경량 암호화 모듈이 인증 체계에 채택됨 • Proverif가 제공하는 공식 검증을 통해 제안된 인증 체계의 보안 견고성 보장	• 알려진 공격에 대한 보안 대책으로 한정됨 • 내부자, 리플레이 어택, 사용자 사칭 공격에 툭히 취약함 • 상호 인증이 제공되지 않으며, 비밀 키가 보호되지 않음

[34]	아키텍처	• 클라우드 컴퓨팅 환경을 위한 경량 IoT 기반 인증 체계 • [33]에 대해 로그인, 상호 인증, 키 동의 단계를 고려한 새 버전 제안 • 적은 통신 비용이 특징	• 인증 단계 중 사용자 식별 단계를 추가해 시스템 복잡도 및 지연 증가 • 상호 인증 및 연결을 위해 많은 데이터가 필요하므로 사전 체계 구축에 대한 비용이 소모됨 • 클라우드 기반 IoT 플랫폼의 보안요구사항 정리
[35]	아키텍처	• 클라우드 컴퓨팅 환경에서 IoT를 위한 안전하고 가벼운 3단계 인증 기법 • 종래 관련 연구[34]의 보안 취약성과 상호 인증 및 익명성 제공이 불가함을 입증 • 비밀 매개변수와 생체 인식을 활용한 상호 인증 및 익명성 제공	• 중간자 공격 및 리플레이 어택에 저항함을 입증하기 위해 AVISPA (Automated Validation of Internet Security Protocols and Applications) 시뮬레이션 도구 활용 • 대규모 네트워크를 대상으로 하는 지능화 및 고도화된 공격에 대한 고려 필요
[36]	프로토콜	• 블록체인 네트워크의 노드에 의해 구현된 저전력 블록체인 프로토콜 • 유용한 데이터 구조만 다운로드하는 경량 소프트웨어 구현 • 이더리움 프로토콜의 경우, 낮은 신호 대 잡음비에 대한 장치의 듀티 사이클 감소, 다운링크에서 전송된 정보의 양 감소 달성 • 통신 비용을 일정하게 유지하면서 프라이버시 증가	• 채널 품질 및 제공 속도, 유용한 데이터 구조에 대한 통계 기반 집계로 중앙집중형 및 분산형 구조의 모순 생성 • IoT 네트워크 내 계정 상태 업데이트 주기에 따른 성능 차이 • 블록체인의 포크 기능 및 불변성에 의한 데이터 특성이 반영된 트랜잭션에 관한 추가 연구 필요

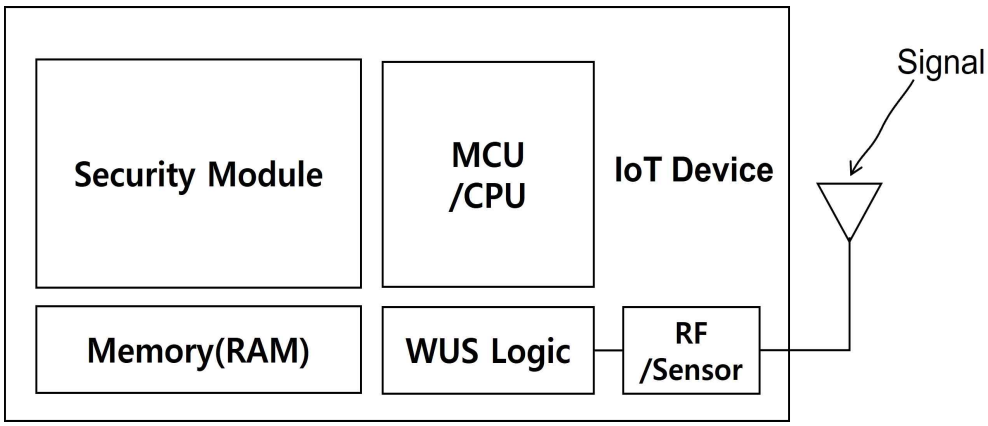
[37]	프로토콜	• WSN (Wireless Sensor Networks) 시스템을 위한 강력하고 가볍고 에너지 효율적인 보안 프로토콜 • 상호 인증 메커니즘 및 대칭 보안 채널 구성	• AES 암호 기반 보안 채널로 경량화를 실현했으나 복잡한 구조를 가짐 • 계층별 특징에 따른 보안 솔루션으로 확장가능성 제시 • 실행한 적 있는 프로토콜에 대해 약한 신뢰성 보장으로 사칭, 도청, 스푸핑 등으로 인한 문제 해결책 필요
[38]	알고리즘	• 저장 용량을 확보하기 위해 각 디바이스에서 블록체인을 압축하는 SCC (Storage Compression Consensus) 알고리즘 • 기존 알고리즘에 대비 63%의 저장 용량 감소	• 블록체인 크기 감소로 인한 전체 성능 개선 효과에 대한 평가가 미비함 • 노드 수에 따라 감소되는 블록체인의 크기와 지연 관계에 대한 고려가 필요
[39]	알고리즘	• 자원 제약이 있는 IoT 기기를 위한 가볍고 안전한 상호 인증 기법 • Dolev-Yao 공격 모델에서 안전한 체계로 입증됨	• 보안 성능이 고려되었으나, 가설적 추론을 기반으로 한 보안 검증으로 보다 객관적인 시뮬레이션 평가 결과 필요
[40]	알고리즘	• IoT를 위한 암호 설계 성능 개선 및 에너지 소비 최적화 방식 • 배터리 소모 공격에 대해 IoT의 수명을 향상시키는 에너지 관리 알고리즘 • 암호 에너지 소비 관리 알고리즘 • 블록 크기가 크고 구현된 라운드 수가 많은 구현을 통해 최적의 처리량을 얻을 수 있음	• 에너지 및 비트당 에너지 메트릭 최적화를 개선했으나, 그 외 컴퓨팅 성능은 유지 수준임 • 보안 성능에 대한 고려가 되지 않음

종래의 저전력 환경을 위한 보안 솔루션에 관한 연구들은 전체적인 전력 소모량과 메모리 사용량을 감소시킬 수 있으나, 보안 관련 로직이 고려되지 않거나 경량화 됨으로써 보안 성능이 열화되어 에너지-보안 최적 솔루션을 적용한 수준까지 도달하기 어렵다는 한계가 있다. 특히, 종래의 경량 보안 솔루션은 많은 로직 중에서도 암호 알고리즘과 같은 보안 기능을 수행하는 로직을 우선적으로 경량화했는데, 대규모 네트워크를 대상으로 발생하는 사이버 공격을 방어하기엔 부족한 성능이다. 이처럼 종래의 사물인터넷 플랫폼에서는 보안 성능보다 데이터 처리와 같은 컴퓨팅 성능이 더 중요했기 때문에 보안 모듈이 경량화되거나 고려되지 못한 연구들이 많았다. 이에 본 논문에서는 적은 에너지를 소모하는 이상 탐지 로직을 추가하여 저전력 환경에서 완전 보안 제품 수준의 고성능 보안 모듈을 활용할 수 있는 방안에 관한 연구를 진행하였다. 3장에서는 사물인터넷을 위한 저전력 보안 아키텍처인 Wake-Up Security 메커니즘을 소개한다.

제 3 장 사물인터넷을 위한 저전력 보안 아키텍처

1. WUS 메커니즘과 구조

Wake-Up Security (WUS) 메커니즘은 사물인터넷 플랫폼에 이상 탐지를 수행하는 작은 로직을 추가한 것으로, 필요한 경우에만 보안 모듈을 동작시켜 저전력 환경에서 고성능 보안 모듈을 활용할 수 있도록 한다. [그림 2]는 WUS 메커니즘의 구조도이다.



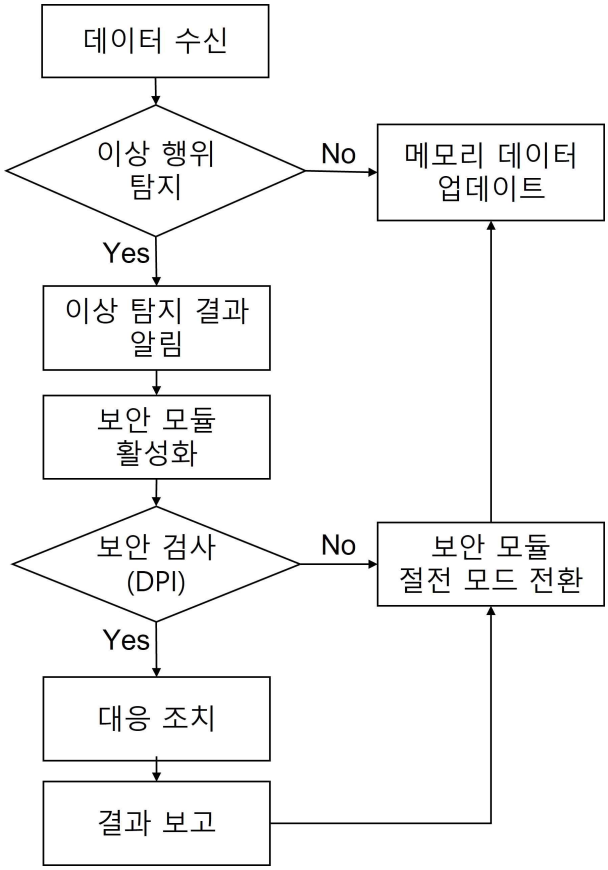
[그림 2] WUS 메커니즘 구조도

사물인터넷 플랫폼의 입력부에 WUS가 위치하며, 제어 로직에 해당하는 Micro Controller Unit (MCU)과 외부 신호를 수신하는 센서, 보안 기능을 수행하는 보안 모듈, 메모리를 포함한다. 이때, 사물인터넷 기기에 추가된 WUS 로직은 외부 신호를 수집하는 센서부에서 데이터를 전달받아 이상 행위 탐지를 수행한다. WUS 로직을 갖는 사물인터넷 구조는 이상 행위 탐지를 수행하는 로직인 WUS 로직과 보안 기능을 수행하는 보안 모듈이 분리되었다. WUS 로직에서 사용하는 이상 탐지 모델은 사물인터넷의 기능 및

사용자의 선호에 따라 종래의 이상 탐지 모델을 중 선택하여 적용할 수 있다. 본 논문에서는 시뮬레이션 평가를 위해 UNSW-NB15 데이터셋을 의사결정 트리 알고리즘으로 학습한 이상 탐지 모델을 활용했다. 해당 모델은 트래픽 정보 중 상관성이 높은 15개의 라벨 값을 바탕으로 패턴 기반 탐지를 수행한다. 로직에 적용된 모델은 리소스 제약이 없는 외부 서버에서 학습이 완료된 모델이며, 주기적으로 업데이트가 가능하다. 본 논문에서 제안하는 WUS 메커니즘은 트래픽 분석 과정 중 WUS가 이상 행위를 감지했을 때에만 다른 보안 모듈을 실행하기 위한 로직들을 활성화하는 것이 특징이다. 즉, 이상 행위가 발생하지 않는 상황에서 다른 로직들은 절전 모드로 전환되며 WUS 로직만 활성 상태를 유지한다. 이상 행위가 감지된 경우에는 다른 보안 로직들도 모두 활성 상태가 되어 이상 행위에 대한 보안 조치를 수행한다.

2. WUS 동작 원리

WUS 메커니즘의 동작 원리에 따른 흐름도는 이상 행위 탐지 단계와 보안 검사 단계로 구성된다. WUS 메커니즘의 세부 동작 구조에 따른 흐름도는 [그림 3]과 같다.



[그림 3] WUS 메커니즘 흐름도

WUS 로직을 포함한 사물인터넷의 동작 원리는 다음과 같다. 사물인터넷은 주기적 혹은 비주기적으로 외부로부터 신호를 수신한다. 사물인터넷에 탑재된 센서가 수신한 신호 데이터는 WUS 로직에 의해 이상 행위 탐지 단계에 들어간다. WUS 메커니즘에서 이상 행위 탐지를 수행하는 WUS 로직은 알려진 공격에 대한 공격 패턴 기반 탐지, 전송 신호 이상치 탐지, 송수신되는 데이터의 무결성 탐지와 같은 종래 이상 행위 탐지 기술을 활용할 수 있다. 이상 행위가 발생한 경우, WUS 로직은 고성능 보안 모듈을 호출하여 추가 탐지 및 대응에 해당하는 보안 조치를 수행한다. 반면, 이상 행위

가 발생하지 않았다면 별도의 보안 모듈 호출과 동작 없이 수신한 트래픽으로 생성된 변경사항을 업데이트하고 저장한다.

외부로부터 수신한 트래픽이 WUS 로직의 탐지 결과에 따라 신호 이상, 무결성 침해와 같은 이상 행위로 탐지된 경우 보안 모듈을 호출하게 되며, 이에 관한 구체적인 동작은 다음과 같다. WUS 로직에서 이상 행위를 감지하면 제어 로직에 해당하는 MCU에 이상 탐지 결과를 보고한다. WUS로부터 이상 탐지 이벤트를 전달받은 MCU는 보안 모듈을 활성화한다. 이때, 보안 모듈은 사물인터넷 플랫폼에서 제공하는 서비스 및 산업 분야에 따라 상이할 수 있으며, 본 논문에서는 DPI (Deep Packet Inspection)로 가정하였다. 일반적으로 DPI는 수신한 데이터에 대해 전체 문자열의 일치 여부를 검사하여 해당 데이터를 깊이 있게 분석하는 것을 의미한다[41]. 하지만 데이터의 형식에 따라 서명이 복잡해지는 문제로 네트워크 침입 탐지 시스템에 대해 정규식을 구성하여 데이터 검사를 수행한다. 대부분의 DPI 응용 프로그램은 정규식으로 표현되는 언어를 인식하여 서명 일치 기능을 사용할 수 있는 FSM (finite-state machine)을 활용한 패턴 기반 검사를 기반으로 한다[42]. DPI를 수행하는 보안 모듈은 공격이 없는 평상시에는 절전 모드 상태를 유지하고 있으며, 이상 행위가 감지될 경우에는 제어 로직에 의해 깨어난다. 활성 상태로 전환된 보안 모듈은 DPI를 수행하여 실제 공격 여부와 침해 수준에 대해 파악하고, 이를 외부 서버에 전달하여 대응 조치를 수행한다. 모든 보안 관련 업무가 완료된 보안 모듈은 MCU에 문제 사항 및 조치 사항을 보고한 후 다시 절전 모드로 전환되며, 제어 로직은 사물인터넷 기기와 메모리를 업데이트 및 패치한다.

임베디드 시스템에서 에너지 소모량은 시스템 복잡도 및 회로의 크기와 비례하는데, WUS 메커니즘에서 메인 로직은 이상 행위가 탐지되지 않을 때와 보안 업무 종료 후 절전 모드 상태가 되기 때문에 평상시에 소모되는

전력과 메모리가 적다. 따라서 리소스 제약적인 사물인터넷 환경에서도 상대적으로 복잡도가 큰 보안 솔루션이나 에너지-보안 최적 솔루션을 활용할 수 있다.

본 논문에서는 WUS 메커니즘을 제안함으로써, 이상 행위 발생 시에만 고성능 보안 모듈을 활용하는 방식으로 전력 효율성을 개선하고자 하였다. 이상 행위 탐지 기술은 현실적인 데이터셋과 학습 방법에 관한 연구들이 활발하게 진행되고 있으며[43], 머신러닝 알고리즘과 데이터셋에 따라 성능 차이가 있을 수 있다.

본 논문에서는 Australian Center for Cyber Security (ACCS)의 Cyber Range Lab에서 IXIA PerfectStorm 도구를 사용하여 생성한 UNSW_NB15 데이터셋과 의사결정 트리 분류기를 활용하여 이상 탐지 모델을 구축했으며, 이 외에도 사용자는 활용 분야에 따라 WUS 메커니즘에 다양한 이상 탐지 모델을 도입할 수 있다. WUS 로직에서 활용되는 이상 행위 탐지 모델의 경우에는 사물인터넷 플랫폼 자체에서 생성하는 것이 아니라 데이터 전처리, 데이터 정규화, 피처 추출, 데이터셋 학습 및 분할, 분류 등의 작업을 수행할 수 있는 충분한 리소스를 가진 외부 플랫폼에서 만든다. 생성된 모델은 상황에 따라 지속적인 업데이트가 가능하며, 이미 학습된 모델을 WUS 로직에 추가하여 탐지하므로 종래의 고성능 및 경량 보안 모듈 대비 매우 적은 에너지로 사전 탐지가 가능하다.

보안 모듈이 작동하는 동안에도 WUS 로직에서 이상 행위 탐지를 수행할 수 있으며, 이는 이상 행위 여부와 관계없이 보안 모듈을 통해 주기적으로 검사하는 종래 방식 대비 낮은 지연시간을 가지며, 추가 위협에 대한 빠른 대응 조치가 가능하다. 특히, 이벤트가 많이 발생하지 않는 환경에서는 더 많은 리소스를 절약함으로써 효율적인 이상 행위 탐지 및 대응 로그 관리가 가능하다. 절약된 메모리 공간에는 유의미한 정보를 포함한 로그만을 저장

하고 관리할 수 있으므로 보안 감사 및 제어 이력에 대한 추적과 관리도 쉬워진다. 또한, 클라우드 기술을 통해 외부 네트워크에서 데이터를 처리하는 방식과 비교하여 사물인터넷 플랫폼 자체의 보안 아키텍처를 개선하는 WUS 메커니즘은 데이터 유출 범위를 제한하여 개인 정보 및 민감 정보 유출과 같은 2차 피해도 방지할 수 있다. 본 논문에서 제안한 WUS는 종래의 특정 기능을 수행하는 모듈을 경량화하는 방식과 비교하여 불필요한 에너지 소모를 줄이고 전력 효율성을 개선하여 사물인터넷을 위한 양질의 서비스를 제공할 수 있다.

4장에서는 본 장에서 제안한 WUS 메커니즘과 종래 모델에 대해 전력 소모량, 지연시간, 보안 성능 측면으로 UNSW-NB15 데이터셋 기반 시뮬레이션을 진행한 후, 그 결과를 비교·평가하였다.

제 4장 평가 및 분석

1. 시뮬레이션 환경 설정

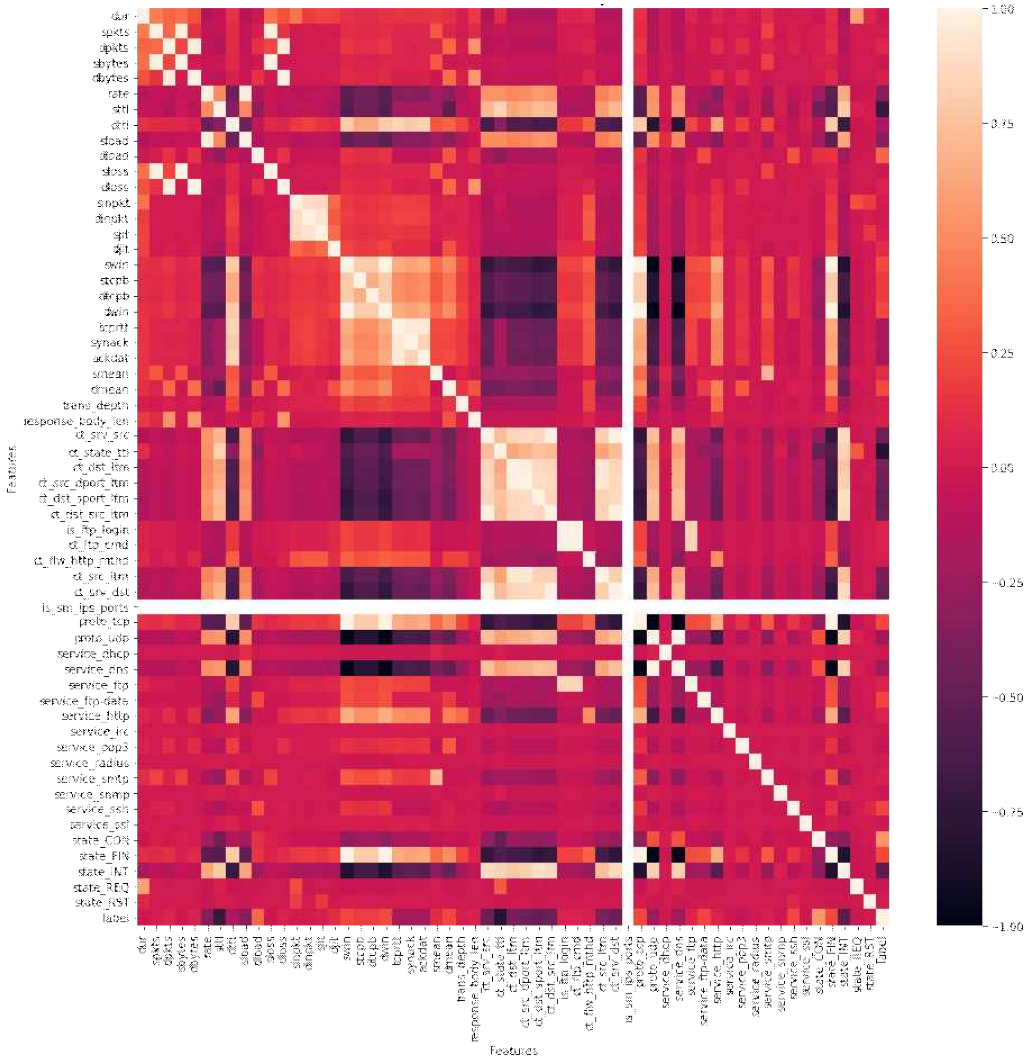
1) 데이터셋

본 논문에서는 이상 행위 탐지를 위한 데이터셋으로 UNSW-NB15 데이터셋을 활용하였다. UNSW-NB15 데이터셋은 ACCS의 Cyber Range Lab에서 IXIA PerfectStorm 도구로 작성한 일반 트래픽과 9개의 공격 트래픽으로 이루어진 공개 데이터셋이다[44]. 이 데이터셋은 Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode 및 Worms의 9가지 공격 유형을 포함하며, 총 49개의 피처로 구성되어 있다. 시뮬레이션 평가에서는 'label' 피처 값을 활용하여 트래픽의 공격 여부에 따른 이진 분류를 기반으로 실험을 진행하였다.

Network Intrusion Detection System (NIDS)에 관한 github 오픈 소스 코드를 사용하여 UNSW-NB15 데이터셋에 대하여 데이터 전처리 및 인코딩, 정규화 작업을 진행하였다[45]. 시뮬레이션 평가에서는 활용 가능한 UNSW-NB15 데이터셋 중 'UNSW_NB15_testing-set.csv'를 활용했다. 해당 데이터셋은 null 값을 제외하고 45개의 피처와 81173개의 행으로 구성되며, 정상 트래픽이 75.99%, 비정상 트래픽이 24.01%를 차지하고 있다.

One-Hot 인코딩을 통해 범주형 속성을 가진 데이터 프레임을 생성하였으며, 생성한 데이터 프레임에 대해 MinMax Scaler를 사용하여 데이터 정규화를 진행했다. 그 결과, 이진 데이터셋은 81173개의 행과 61개의 열로 구성되며, 'label' 속성은 '정상'과 '비정상'의 두 가지 범주로 분류된다. 피처 추출을 위해 피어슨 상관 계수 방법을 사용했으며, 이는 두 변수 간에 어떤 선형적 관계가 있는지를 분석하는 방법이다. 계수의 절댓값이 클수록 변수 사

이의 강한 관계를 나타내며, 본 논문에서는 대상 속성 레이블과 상관 계수가 0.3 이상인 속성이 선택되었다. [그림 4]는 이진 분류 데이터셋에 대한 상관 계수 메트릭이다.



[그림 4] 이진 레이블에 대한 상관 메트릭[45]

(*본 그림은 [45]의 'correlation_matrix_bin'을 재가공했음)

이진 데이터의 속성 중 추출된 피처는 'rate', 'sttl', 'sload', 'dload',

‘ct_srv_src’, ‘ct_state_ttl’, ‘ct_dst_ltm’, ‘ct_src_dport_ltm’, ‘ct_dst_sport_ltm’, ‘ct_dst_src_ltm’, ‘ct_src_ltm’, ‘ct_srv_dst’, ‘state_CON’, ‘state_INT’, ‘label’로 15개가 선택되었다. 각 데이터 속성에 대한 설명은 [표 4]와 같다.

[표 4] UNSW-NB15에서 추출한 Feature[46]

라벨 이름	데이터 타입	설명
rate	Float	송신/수신 속도 값
sttl	Integer	송신지에서 수신지까지의 TTL (Time to Live) 값
sload	Float	초당 송신 비트 수
dload	Float	초당 수신 비트 수
ct_state_ttl	Integer	송신 및 수신의 왕복 TTL 값의 특정 범위에 따라 각 상태에 대한 수
ct_dst_ltm	Integer	res_bdy_len에 따른 100개의 연결 중 동일한 수신지 주소의 연결 수
ct_src_dport_ltm	Integer	res_bdy_len에 따른 100개의 연결 중 동일한 송신지 주소와 수신지 포트의 연결 수
ct_dst_sport_ltm	Integer	res_bdy_len에 따른 100개의 연결 중 동일한 수신지 주소와 송신지 포트의 연결 수
ct_dst_src_ltm	Integer	res_bdy_len에 따른 100개의 연결 중 동일한 송신지 및 수신지의 주소의 연결 수
ct_src_ ltm	Integer	res_bdy_len에 따른 100개의 연결 중 동일한 송신지 주소의 연결 수
ct_srv_dst	Integer	res_bdy_len에 따른 100개의 연결 중 동일한 서비스와 수진지 주소를 포함하는 연결 수
state_CON	nominal	상태 및 종속 프로토콜 표현
state_INT		
label	binary	정상은 0, 공격(비정상)은 1로 기록

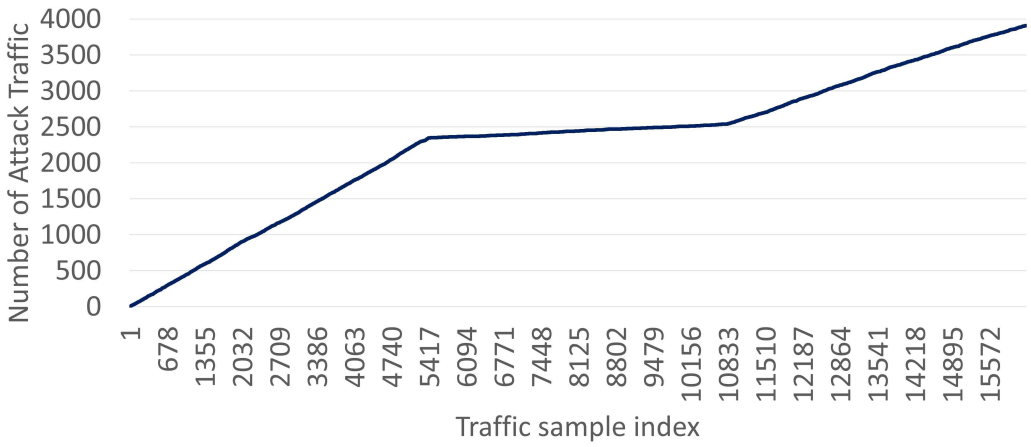
2) 의사결정 트리 분류기 기반 이상 탐지 모델 구축

시뮬레이션 평가는 정규화된 이진 분류 데이터셋으로 진행하였다. 피처 추출을 완료한 이진 데이터셋 중 80%는 훈련 데이터로, 20%는 테스트 데이터로 무작위 분할했으며, 훈련에는 의사결정 트리(Decision Tree)를 사용했다. 의사 결정 트리는 일련의 규칙을 통해 데이터를 분류 및 회귀하는 지도 학습 모델로, 결과 모델이 트리 구조를 가지기 때문에 종래 연구에서 다수 활용되고 있는 모델이다[47]. [그림 5]는 실제 공격 트래픽의 분포를 나타낸 그래프이다.

[그림 5] 실제 공격 트래픽 분포

의사결정 트리 기반의 이진 분류 결과에 따르면, 약 98.1의 정확도와 약 0.019의 평균 절대 오차 및 평균 제곱 오차, 약 0.138의 제곱 평균 제곱근 오차를 가진다. 데이터셋의 전체 구간은 정상 트래픽과 공격 트래픽이 골고루 분포되어 있으며, 본 논문에서는 시뮬레이션 평가를 위해 공격 트래픽의 분포를 임의로 조정하였다. 전체 구간을 3개의 영역으로 나눈 후, 첫 번째

구간은 전체 공격 트래픽의 60%를, 두 번째 구간은 5%를, 세 번째 구간은 35%를 분포시켰다. 재분포한 공격 트래픽의 분포 그래프는 [그림 6]과 같다.



[그림 6] 후가공한 공격 트래픽 분포

3) 비교 모델 및 가정 사항

시뮬레이션 평가에서는 제안 모델인 WUS 메커니즘과 종래 모델인 고성능 및 경량 보안 모듈 기반 메커니즘을 비교한다. 제안 모델의 경우에는 이상 행위 탐지를 수행하는 WUS 로직에서 이상 행위를 탐지한 경우에만 보안 모듈을 동작시킨다. 이때, 보안 모듈은 종래 모델의 고성능 보안 모듈과 동일하다. 반면, 종래 모델의 경우에는 고성능 혹은 경량 보안 모듈이 이상 행위 여부와 관계없이 주기적으로 동작한다. 본 논문에서는 데이터셋 전체를 하나의 시나리오로 가정하여 평가를 진행했으며, 종래 모델의 경우 매 트래픽마다 보안 모듈을 동작시키는 구조이다. 이때, 종래 및 제안 모델의 모든 보안 모듈의 행위는 DPI로 가정하였으며, 이는 콘텐츠 내용까지 세부 분석을 통해 네트워크 보안 및 관리, 개인정보 침해 방지를 수행할 수 있다.

실험 과정에서 제로데이 공격은 고려하지 않는다.

비교 모델인 종래 모델은 고성능 보안 모듈만 활용하는 모델과 경량 보안 모듈만 활용하는 모델로 구분할 수 있다. 고성능 보안 모듈과 경량 보안 모듈 모두 매 트래픽마다 DPI를 수행하는 것은 동일하나, DPI 수행 시 소모되는 전력량과 연산량의 차이가 있다. 고성능 보안 모듈, 경량 보안 모듈, WUS 로직에서 소모되는 전력 소모량의 비율은 암호 알고리즘의 공간 복잡도를 기반으로 측정하였다. 공간 복잡도는 프로그램을 실행시킨 후 완료하는 데 필요로 하는 자원 공간의 양을 말하며, 일반적으로 입력 값의 크기에 비례한다. 이때, 시스템의 입력 값이 클수록 더 많은 전력을 소모하므로 공간 복잡도가 클수록 더 많은 양의 전력이 소모됨을 알 수 있다[48]. 고성능의 보안 모듈일수록 더 많은 메모리 및 배터리 용량을 요구하며, 사물인터넷의 회로의 크기도 커진다. 회로의 크기가 클수록 공간 복잡도가 증가하며, 이에 따라 전력 소모량도 증가한다. 이에 본 논문에서는 고성능 보안 모듈일수록 더 높은 공간 복잡도를 가지는 암호 알고리즘이 적용됨을 가정하였으며, ‘A comparative analysis of encryption algorithms for better utilization’의 연구 결과인 [표 5]를 참고하였다[49].

[표 5] 암호화 알고리즘의 공간 복잡도 비교[49]

암호 알고리즘	암호화 전	암호화 후	복호화 후
XOR	130KB	130KB	130KB
DES (Data Encryption Standard)	130KB	188KB	130KB
Triple-DES (TDES)	130KB	360KB	130KB
Blowfish	130KB	544KB	130KB

[표 5]의 암호화 후 공간 복잡도 수치를 바탕으로 각 보안 모듈의 전력 소모 비율을 정하였다. WUS 로직은 의사결정 분류기를 통해 학습된 이상 탐지 모델을 바탕으로 트래픽의 라벨 값을 분석하여 패턴 기반 탐지를 수행하는 로직으로, 본 논문의 시뮬레이션 평가에서는 이진 분류 데이터를 기반으로 이상 행위 여부를 분류하였기 때문에 XOR의 공간 복잡도 값으로 가정하였다. [표 5]에서 비교된 암호 알고리즘 중 가장 복잡도가 높은 Blowfish는 고성능 보안 모듈의 공간 복잡도 값으로 가정했으며, 경량 보안 모듈은 DES와 TDES로 구분하여 2개의 경량 모델을 모두 실험에 포함했다. 각 보안 모듈에 따른 전력 소모량 설정 값은 [표 6]과 같다.

[표 6] 보안 모듈별 전력 소모량 설정 값

Method	고성능 보안 모듈	경량 보안 모듈		WUS 로직
Algorithm	Blowfish	DES	TDES	XOR
Total Power	544mW	188mW	360mW	130mW

[표 6]에 따라, 고성능 보안 모듈은 매 트래픽마다 544mW의 전력을 소모하며, 경량 보안 모듈은 매 트래픽마다 각각 188mW, 360mW의 전력을 소모한다. 반면, 제안 모델은 매 트래픽마다 130mW의 전력을 소모하며, WUS 로직에서 이상 행위가 탐지되었을 경우에만 고성능 보안 모듈을 동작시켜 544mW의 전력을 추가로 소모하게 된다.

2. 시뮬레이션 평가 및 결과

본 논문에서는 Python 기반 시뮬레이터를 통해 제안 모델과 비교 모델의 전력 소모량, 지연시간, 보안성능을 측정하여 비교・평가하였다. 시뮬레이션은 운영체제 Windows 10 Home, RAM 8GB, CPU 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz의 PC 환경에서 진행했다.

시뮬레이션 평가에서는 공개 데이터셋인 UNSW-NB15 데이터셋 중 'UNSW_NB15_testing-set.csv'을 활용하였으며, 정상 트래픽 12326개, 공격 트래픽 3909개의 총 16235개 트래픽을 포함한다. 시뮬레이션은 해당 데이터셋의 모든 트래픽을 수집 및 분석하는 작업을 수행하며, 전체 데이터셋을 분석하기까지의 전력 소모량과 지연시간, 탐지정확도 및 탐지 효율성을 측정하였다.

1) 전력 소모량

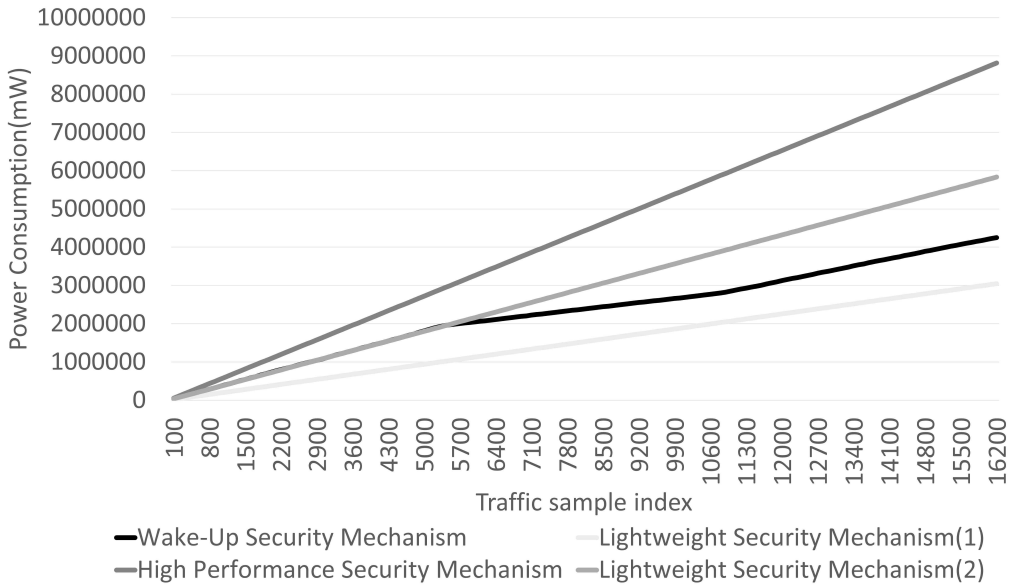
일반적으로 전력은 동적 전력과 정적 전력으로 구성되며, 다음의 수식으로 표현할 수 있다[40].

$$P = P_{static} + P_{dynamic} \tag{1}$$

정적 전력(P_{static})은 사물인터넷과 같은 마이크로프로세서가 동작하지 않는 클록이 멈춘 상태에서 정적으로 소비되는 전력을 말하며, 바이어스 전류, 누설 전류, 소비 전력 등을 포함한다. 반면, 동적 전력($P_{dynamic}$)은 회로 용량(C)과 전압(V), 주파수(F)에 따라 값이 달라지며, 다음과 같은 수식으로 표현할 수 있다[50].

$$P_{dynamic} = C \times F \times V^2 \tag{2}$$

본 논문에서는 [표 6]과 같이 보안 모듈별로 소모하는 전력량을 암호 알고리즘의 공간 복잡도 값을 기반으로 설정하였으며, 이는 복잡도가 높은 모듈일수록 회로의 크기가 커짐에 따라 전력 소모도 비례하여 증가함을 보여준다. 시뮬레이션에서는 정적 전력은 무시하고 계산하였으며, 트래픽 분석 및 보안 조치에 대해 각 모델이 소모하는 전력량을 누적하여 전체 전력 소모량을 측정하였다. 이때, 각 트래픽의 플로우나 트랜잭션의 길이는 전력소모량 계산에 반영되지 않았으나, 향후 UNSW-NB15 데이터셋의 라벨 중 송수신 트랜잭션의 길이를 나타내는 sbytes, dbytes를 활용하여 보다 현실적인 평가 시뮬레이션을 진행할 수 있을 것으로 기대한다. [그림 7]에서 전력소모량은 시간의 흐름에 따라 100개의 트래픽마다 누적된 전력소모량을 측정한 그래프이다. Wake-Up Security Mechanism은 제안 모델을, High Performance Security Mechanism은 고성능 보안 모듈을 나타낸다. Lightweight Security Mechanism의 경우, (1)은 DES, (2)는 TDES의 공간 복잡도를 반영한 모델이며, 본 논문에서 진행한 모든 실험에 동일하게 적용했다.

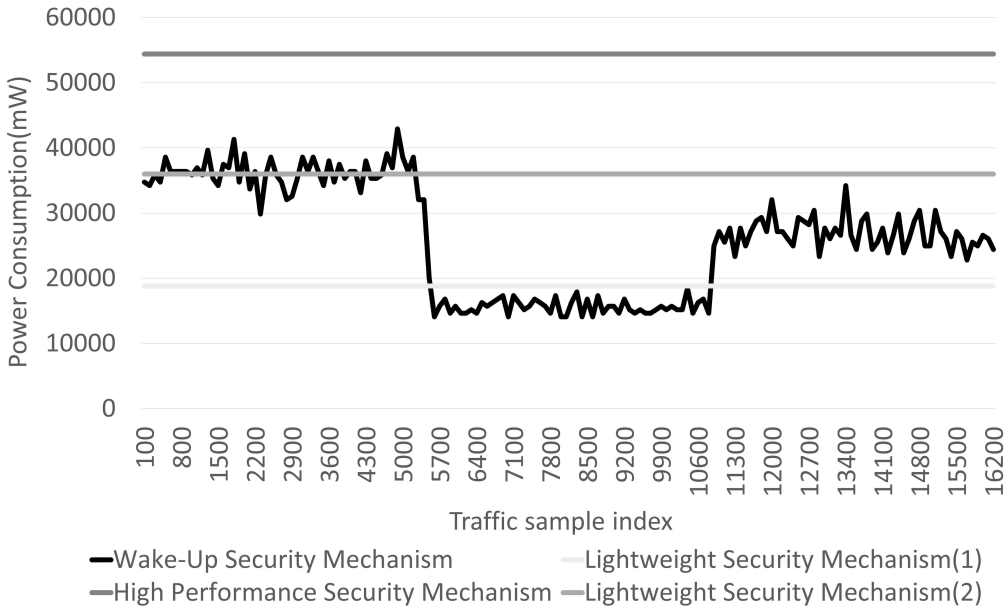


[그림 7] 전력 소모량 평가 결과

[그림 7]의 평가 결과에 따르면, 가장 적은 전체 누적 전력 소모량을 가지는 것은 경량 보안 모듈 (1)이다. 매 트래픽마다 전력을 소비하지만, 그 값이 제안 모델과 유사하므로 전체적으로 가장 낮은 전력 소모량을 가진다. 제안 모델을 제외한 고성능 및 경량 보안 모듈은 매 트래픽마다 전력을 소모하기 때문에 시간이 지남에 따라 더 빠른 속도로 전력 소모량이 증가하는 것을 확인할 수 있다. 가장 많은 전력을 소모하는 고성능 보안 모듈이 가장 가파른 기울기로 증가한다. 반면, 제안 모델의 경우, 공격의 빈도에 따라 그래프의 기울기가 다른 것을 확인할 수 있다. 이는 제안 모델의 WUS 로직이 이상 행위를 탐지할 경우, 고성능 보안 모듈을 활성화하여 추가적으로 전력을 소모하기 때문이다. 가장 공격 빈도가 높은 첫 번째 구간에서 가장 가파른 기울기로 전력 소모량이 증가하였으며, 가장 공격 빈도가 적은 두 번째 구간에서 가장 완만한 기울기로 전력 소모량이 증가하는 것을 확인할

수 있다. 전체 전력 소모량의 경우, 제안 모델이 두 번째로 적은 전력을 소모하였다. 이러한 결과에 따라 WUS 메커니즘은 이상 행위가 적은 환경일수록 더 적은 전력을 소모할 것으로 예상되며, 이는 리소스 제한적인 사물인터넷 플랫폼의 전력 효율성을 개선할 수 있다.

누적 전력 소모량에 이어 실시간 전력 소모량도 측정하였다. 실시간 전력 소모량에 대한 평가 결과는 [그림 8]과 같다.



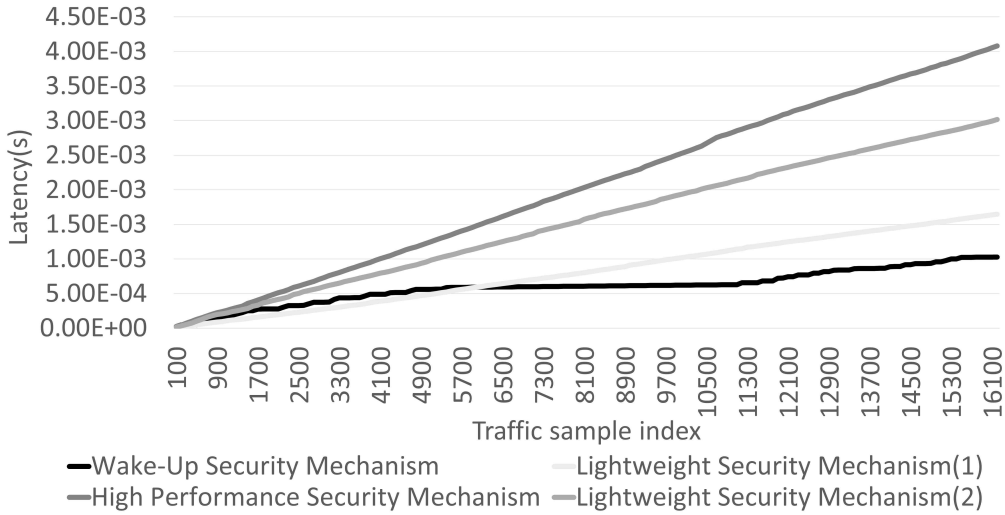
[그림 8] 실시간 전력 소모량 평가 결과

[그림 8]의 평가 결과에 따르면, 제안 모델을 제외한 나머지 모델은 매 트래픽마다 동작하며, 이상 행위 여부와 상관없이 항상 같은 전력량을 소모하기 때문에 수평선을 그린다. 반면, 제안 모델의 경우, 공격 빈도에 따라 실시간 전력 소모량의 차이가 큰 것을 확인할 수 있다. 가장 공격 빈도가 높은 첫 번째 구간에서 가장 많은 전력 소모량을 가지며, 가장 공격 빈도가

낮은 두 번째 구간에서는 가장 적은 전력을 소모하였다. 특히, 두 번째 구간의 경우 경량 보안 모듈 (2)보다 적은 전력 소모량을 가지는 것을 확인할 수 있다.

2) 지연시간

데이터셋의 트래픽 흐름에 따라 보안 모듈 및 관련 로직의 동작에 대한 실행 시간을 지연시간으로 정의하였다. 시뮬레이션에서는 보안 모듈의 동작인 DPI를 수학적 연산 장치로 모델링했으며, 100개의 트래픽마다 실행 시간을 누적한 값을 측정하여 비교했을 때 지연시간에 관한 평가 결과는 [그림 9]와 같다.

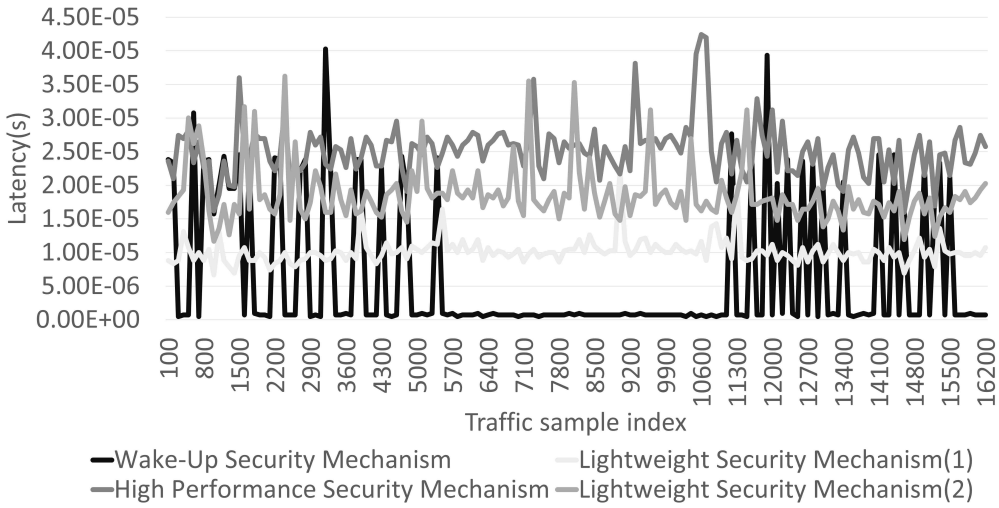


[그림 9] 지연시간 평가 결과

[그림 9]의 평가 결과에 따르면, 전체 누적 지연시간은 제안 모델인 WUS 메커니즘이 가장 작으며, 고성능 보안 모듈이 가장 크다. 제안 모델을 제외한 고성능 및 경량 보안 모듈은 이상 행위 여부와 상관없이 매 트래픽마다 동작하므로 시간에 비례하여 지연시간이 증가하는 것을 확인할 수 있다. 반면, 제안 모델은 공격 빈도에 따라 구간별 누적 지연시간이 상이하고 상승 그래프의 기울기가 달라지는 양상을 확인할 수 있다. 가장 공격 빈도가 높은 첫 번째 구간에서는 경량 보안 모듈 (2)보다 더 많은 지연시간이 발생하

였으나, 가장 공격 빈도가 낮은 두 번째 구간에서는 지연시간이 미세하게 증가하는 것을 확인할 수 있다. 그리고 세 번째 구간에 진입하면서 다시 지연시간이 점진적으로 증가하였다. 이는 제안 모델의 WUS 로직에서 이상 행위가 발견될 경우, 고성능 보안 모듈에 대한 지연시간이 발생하기 때문이며, 해당 구간에서 지연이 더 많이 발생할수록 그래프의 기울기가 커진다. 데이터셋의 후반부에 갈수록 분석한 트래픽의 양이 많아지면서 각 모듈 간의 지연시간 차이가 점차 커지는 것을 확인할 수 있다. 이러한 결과에 따라 WUS 메커니즘은 전력 소모량과 마찬가지로 이상 행위가 적은 환경일수록 더 적은 지연이 발생할 것으로 예상되며, 이는 시스템 효율성과 서비스 가용성을 개선할 수 있다.

누적 지연시간에 이어 실시간 지연시간도 측정하였다. 실시간 지연시간에 대한 평가 결과는 [그림 10]과 같다.



[그림 10] 실시간 지연시간 평가 결과

[그림 10]의 평가 결과에 따르면, 공격 빈도가 매우 높은 첫 번째 구간과

중간인 세 번째 구간에서는 제안 모델의 실시간 지연시간이 고성능 보안 모듈보다 높을 때가 존재하며, 평균적으로 경량 보안 모듈 (2)가 적은 지연시간을 유지하는 것을 확인할 수 있다. 반면, 공격 빈도가 가장 낮은 두 번째 구간에서 제안 모델은 가장 적은 실시간 지연시간을 가지나, 종래 모델은 오히려 다른 구역보다 더 높은 지연시간을 가지는 것을 확인할 수 있다. 결과적으로, WUS 메커니즘은 공격 빈도에 따라 실시간 지연시간의 차이가 큰 것을 확인할 수 있다.

3) 보안 성능

본 논문에서는 보안 성능을 평가하기 위해 탐지 정확도와 탐지 효율성 2가지를 측정하고 비교・분석하였다. 탐지 정확도는 각 비교 모델과 제안 모델이 비정상 트래픽 탐지에 성공할 확률을 측정하는 평가지표이다. 탐지 효율성은 각 모델이 정상 및 비정상 트래픽의 공격 여부를 얼마나 정확하게 예측하여 탐지하는지를 평가하는 지표이다. 보안 성능 평가는 혼동 행렬 지표를 활용하여 1000개 및 100개의 트래픽마다 성능을 측정하여 평균값을 계산하였다. 혼동 행렬 지표에 대한 정의는 [표 7]의 내용과 같다.

[표 7] 보안 성능 평가를 위한 혼동 행렬 지표

	정상(예측)	**비정상(예측)**
정상(실제)	TP	FN
비정상(실제)	FP	TN

- TP (True Positive): 정상이라고 예측한 트래픽이 실제로 정상인 경우
- TN (True Negative): 비정상이라고 예측한 트래픽이 실제로 비정상인 경우
- FP (False Positive): 정상이라고 예측한 트래픽이 실제로 비정상인 경우
- FN (False Negative): 비정상이라고 예측한 트래픽이 실제로 정상인 경우

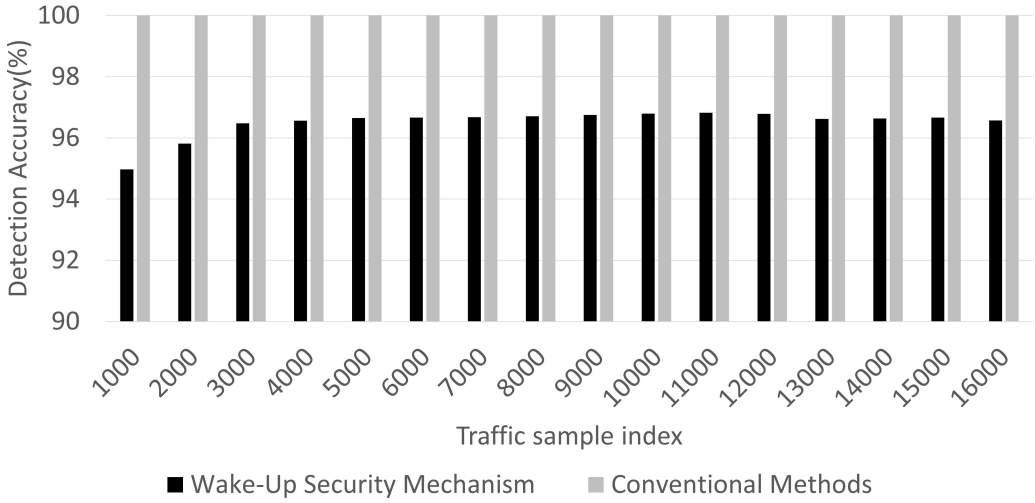
탐지 정확도는 데이터셋이 포함한 전체 비정상 트래픽 중 비정상 트래픽을 비정상 트래픽으로 올바르기 탐지한 비율로, 다음의 수식으로 계산할 수 있다.

$$Detection\ Accuracy = \frac{TN}{Number\ of\ Abnormal\ Data} \times 100 \quad (3)$$

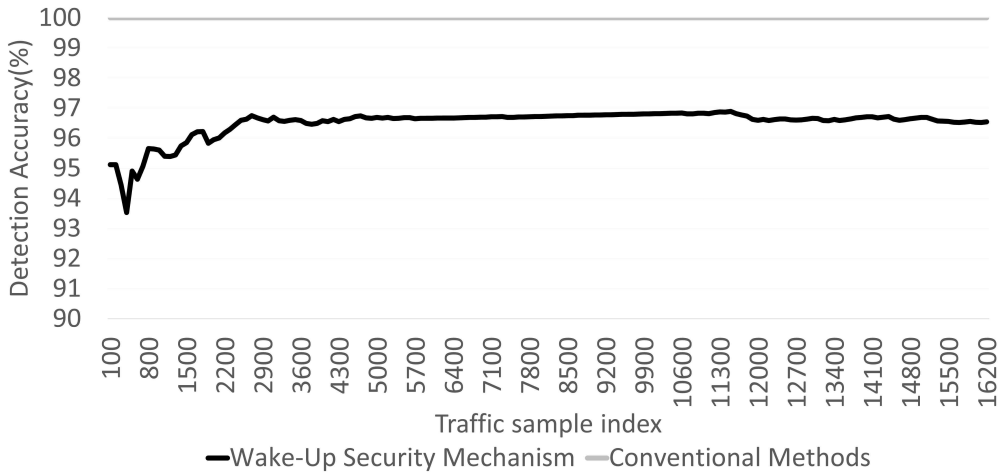
탐지 효율성은 각 모델의 동작이 사물인터넷 보안에 있어 유의미한 영향을 끼친 정도를 확인하기 위한 평가지표로, 모델이 수신한 트래픽의 공격 라벨을 얼마나 정확히 예측하는지 확인하였다. 즉, 각 모델이 잘못된 탐지로 인해 전력량을 낭비하거나 지연시간이 증가하지 않도록 정확하게 탐지를 수행하는 능력을 나타낸다. 이는 머신러닝의 예측 정확도를 측정하는 다음의 수식으로 계산할 수 있다[46].

$$Detection\ Efficiency = \frac{TP + TN}{TP + TN + FN + FP} \times 100 \quad (4)$$

수식 (3)에 의해 측정된 탐지 정확도를 1000개의 트래픽마다 평균으로 계산한 평가 결과는 [그림 11], 100개의 트래픽마다 평균으로 계산한 평가 결과는 [그림 12]와 같다. 이때, 고성능 및 경량 보안 모듈은 모든 트래픽에 대해 DPI를 수행하기 때문에 동일한 데이터셋 시나리오에서 똑같은 탐지 정확도와 탐지 효율성을 가진다. 따라서 본 논문의 보안 성능 평가에서는 고성능 및 경량 보안 모듈을 종래 도구(Conventional Methods)로 통일하여 비교하였다.



[그림 11] 탐지 정확도 평가 결과 (1)

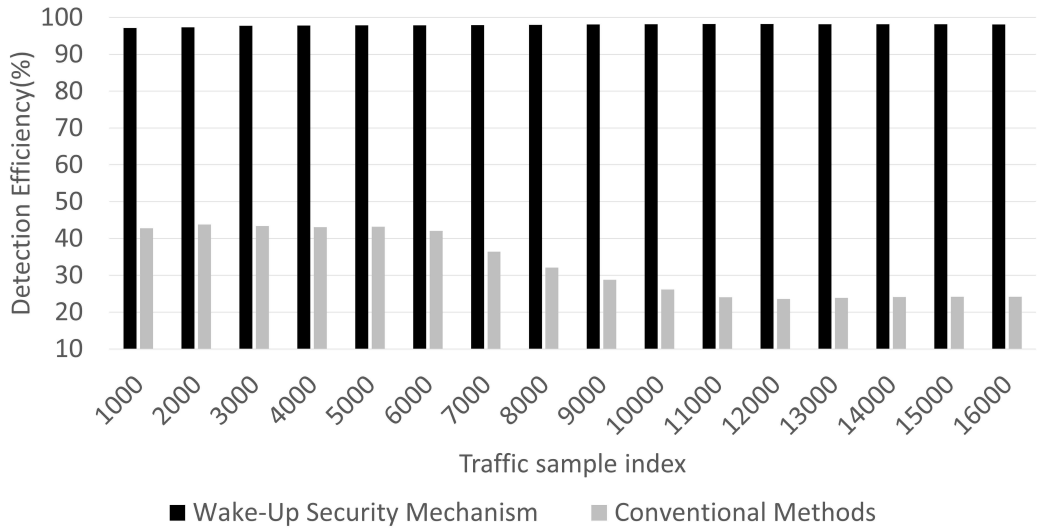


[그림 12] 탐지 정확도 평가 결과 (2)

평가 결과에 의하면, 모든 모델이 전체 구간에서 93% 이상의 높은 탐지 정확도를 보인다. 종래 모델들은 모든 트래픽에 대해 DPI를 수행하며, 제로데이 공격이 고려되지 않았으므로 100%의 탐지 정확도를 가진다. 반면, 제안 모델은 WUS 로직에 적용된 이상 탐지 모델에 따라 탐지 정확도의 차이

가 발생할 수 있다. 본 연구에서는 WUS 로직에 UNSW-NB15 공개 데이터셋을 의사결정 트리 알고리즘으로 학습한 모델을 적용하였으며, 그 결과 평균적으로 약 96.5%의 탐지 정확도를 달성하였다. 데이터 흐름에 따른 변화가 상세한 [그림 12]의 평가 결과에 따르면, 공격 빈도가 높은 데이터셋의 전반부에서 제안 모델은 상대적으로 낮고 불규칙한 탐지 정확도를 가지나, 더 많은 트래픽을 수집할수록 탐지 정확도가 상승하는 것을 확인할 수 있다. 공격 빈도가 다시 증가하는 데이터셋의 후반부에서 탐지 정확도가 떨어지는 양상을 보이나 96% 이상의 높은 탐지 정확도를 가진다.

수식 (4)에 의해 측정된 탐지 효율성을 1000개의 트래픽마다 평균으로 계산한 평가 결과는 [그림 13]과 같다.



[그림 13] 탐지 효율성 평가 결과

평가 결과에 의하면, 제안 모델은 평균적으로 약 98%의 높은 탐지 효율성을 보인다. 이때, WUS 로직에 적용된 이상 탐지 모델 성능에 따라 탐지 효율성은 달라질 수 있다. 반면, 종래 모델은 모든 트래픽에 대해 보안 모듈

이 동작하기 때문에 항상 활성 상태이며, 이는 즉 모든 트래픽을 비정상으로 예측하여 탐지한 후 DPI를 통해 트래픽의 공격 여부를 확인하는 것과 같다. 종래 모델인 고성능 보안 모듈과 경량 보안 모듈은 전력 소모량과 연산량의 차이가 있을 뿐 매 트래픽마다 DPI를 수행하는 것은 동일하기 때문에, 평균적으로 약 32.8%의 동일한 탐지 효율성을 가진다. 이는 제안 모델인 WUS 메커니즘의 탐지 효율성과 비교하여 현저하게 낮은 수치이며, 이상 행위 탐지 로직을 통해 1차 탐지를 수행하는 방식이 효율성이 높다는 것을 알 수 있다. 한편, 종래 모델은 시간이 지나감에 따라 탐지 효율성이 떨어지는 양상을 보이는데, 이는 수집하는 트래픽의 양이 많을수록 트래픽에 대해 정확한 예측을 하는 것이 어렵다는 것을 확인할 수 있다. 이에 따라, 트래픽의 양이 많을수록 WUS 로직을 추가한 제안 모델의 탐지 효율성이 훨씬 높은 성능을 가짐을 알 수 있다.

결론적으로, 본 논문에서는 UNSW-NB15 데이터셋 기반 시뮬레이션을 통해 WUS 로직을 포함한 제안 모델과 고성능 및 경량 보안 모듈만 활용하는 비교 모델을 전력소모량, 지연시간, 보안 성능 측면에서 비교·평가를 진행하였다. 평가 결과에 따르면, WUS 메커니즘은 두 번째로 낮은 누적 전력 소모량을 달성하였으며, 고성능 보안 모듈 대비 약 51.8%, 경량 보안 모듈 (2) 대비 약 27.2% 낮은 전력 소모량을 가졌다. 반면, 누적 지연시간은 제안 모델이 가장 낮은 지연시간을 가졌으며, 공격 빈도가 높은 구간에서는 제안 모델의 순시적인 지연시간이 더 높게 측정되기도 했다. 마지막으로, 보안 성능 평가 지표 중 탐지 정확도는 종래 모델은 100%, 제안 모델은 약 96.5%의 높은 수치를 달성하였으며, 탐지 효율성은 종래 모델이 약 32.8%, 제안 모델이 약 98%를 달성하여 약 33.5% 더 좋은 효율을 보였다. 이때, 제안 모델의 보안 성능은 WUS 로직에 도입된 이상 탐지 모델의 성능에 따라 차이가 발생할 수 있다.

제 5장 결론 및 향후 연구

사물인터넷은 통신 네트워크 및 센서 기술을 이용하여 사람과 사물을 유기적으로 연결함으로써 실시간 데이터 송수신 및 데이터 수집, 저장, 분석을 수행하는 기술이다. 사물인터넷이 산업 분야를 포함한 여러 분야에 활용되면서 그 개체 수가 증가했으며, 적용 범위 및 연결되는 네트워크의 범위 또한 광범위해졌다. 이에 따라 사물인터넷의 보안성 측면에서도 필수적인 요소로 대두되고 있다.

사물인터넷은 디바이스 및 메모리 크기, 데이터 전송을 위한 자원 제약 때문에 제한적인 배터리 성능을 효율적으로 사용하는 방법이 중요하다. 종래 연구에서는 이를 해결하기 위해 보안 모듈을 경량화하는 방식으로 전력 소모량을 감소시키고자 하였으나, 보안 모듈의 경량화로 인해 보안 성능이 열화되어 대규모 정보 시스템 및 네트워크 대상의 고도화, 지능화된 공격을 탐지할 수 없다는 한계점이 존재했다.

따라서 본 연구에서는 사물인터넷 환경에서 고성능 보안 모듈을 효율적으로 사용할 수 있는 저전력 보안 아키텍처인 WUS를 제안하였다. WUS는 사물인터넷 플랫폼에 이상 탐지를 수행할 수 있는 작은 모듈을 추가하여 이상 행위가 발생한 경우에만 고성능 보안 모듈을 깨움으로써 이상 행위가 발생하지 않을 때 소모되는 전력 소모량을 효율적으로 절감시킬 수 있다.

제안하는 WUS의 평가를 위해 UNSW-NB15 공개 데이터셋 기반의 시뮬레이터를 구현하여 전력 소모량, 지연시간, 보안 성능 측면에서 성능 평가를 수행하였다. 평가 결과, 종래의 고성능, 경량 보안 모듈 (2) 대비 약 51.8%, 27.2% 낮은 전력 소모량을 달성하였으며, 공격 빈도에 따라 순시적인 전력 소모량의 차이가 발생하였다. 누적 전력 소모량은 두 번째로 작은 전력을 소모하였다. 반면, 누적 지연시간은 전체 모델 중 가장 낮은 지연시간을 달

성하였으나, 공격 빈도가 높은 구간에서는 고성능 및 경량 보안 모듈보다 순시적인 지연시간이 높은 구간이 일부 존재하였다. 마지막으로 보안 성능의 경우, 모든 모델이 전체 구간에서 약 93% 이상의 높은 탐지 정확도를 보였으며, 종래 모델 대비 약 33.5% 더 좋은 탐지 효율성을 보였다. 향후 연구로는 완전한 보안 제품군에 해당하는 실제 보안 모듈을 추가하여 현실적인 모델에 대해 평가를 진행할 예정이다. 또, 인공지능을 접목하여 사물인터넷 플랫폼의 유동적인 환경 변화와 활용 분야, 데이터 특성에 맞는 자동화 된 데이터 처리 방식 및 이상 탐지 모델 선정 방안에 관한 연구도 진행할 수 있다.

ACKNOWLEDGEMENTS

본 논문은 한국정보통신학회 학술대회에서 발표한 ‘사물인터넷을 위한 저전력 보안 아키텍쳐[51]’ 논문을 바탕으로 확장하여 후속 연구를 수행한 연구 결과입니다. 본 논문을 지도해주신 이일구 교수님과 제안 연구의 구체화를 위한 논의와 초기 시뮬레이션 평가 개발 및 관련 연구 분석에 기여해 준 박나은 학생에게 감사드립니다.

참고 문헌

[1] K. Ashton, “That Internet of Things thing”, RFID Journal, vol. 22, no. 7, pp. 97-114, Jun. 2009.

[2] M. H Vinayak and T Jarin, “An overview of security issues in Intern et of Things based smart environments”, EAI Endorsed Transactions on Energy Web, Jun. 2021.

[3] S.U. Rehman, I.U. Khan, M. Moiz and S. Hasan, “Security and privacy issues in IoT”, International Journal of Communication Networks and Infor mation Security (IJCNIS), vol. 8, no. 3, pp. 147-157, Dec. 2016.

[4] A. Kumar, M. Zhao, K.-J. Wong, Y. L. Guan and P. H. J. Chong, “A comprehensive study of the IoT and WSN MAC protocols: Research issue s challenges and opportunities”, IEEE Access, vol. 6, pp. 76228-76262, De c. 2018.

[5] Ł Apiecionek, M Großmann and U Krieger, “Harmonizing IoT-Archite ctures with Advanced Security Features-A Survey and Case Study”, JUC S-Journal of Universal Computer Science, vol. 25, no. 6, pp. 571-590, Ma y. 2019.

[6] D. E. Kouicem, A. Bouabdallah and H. Lakhlef, “Internet of Things Se curity: A top-down survey”, Computer Networks, vol. 141, pp. 199-221, A ug. 2018.

[7] M.U. Farooq Muhammad, Waseem Anjum and Khairi Sadia Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (Io T)”, International Journal of Computer Applications (0975 8887), vol. 111, no. 7, Feb. 2015.

[8] O. Yousuf and R. N. Mir, “A survey on the Internet of Things securit y: State-of-art architecture issues and countermeasures”, Information & C omputer Security, vol. 27, no. 2, pp. 292-323, Jun. 2019.
[9] A. Shah and M. Engineer, “A survey of lightweight cryptographic alg orithms for IoT-based applications”, Smart Innovations in Communication and Computational Sciences, Springer, pp. 283-293, Nov. 2019.
[10] R. P. Kumar and D. S. Smys, “A Novel Report on Architecture Proto cols and Applications in Internet of Things (IoT)”, 2018 2nd International Conference on Inventive Systems and Control (ICISC), IEEE, pp. 1156-116 1, Jan. 2018.
[11] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du and M. Guizani, “A survey of machine and deep learning methods for internet of things (IoT) security”, IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1 646-1685, Apr. 2020.
[12] Y. Liu, C. Cheng, T. Gu, T. Jiang and X. Li, “A Lightweight Authen ticated Communication Scheme for Smart Grid”, IEEE SENSORS JOURN AL, vol. 16, no. 3, Feb. 2016.
[13] M. Díaz, C. Martín and B. Rubio, “State-of-the-art, challenges, and o pen issues in the integration of Internet of things and cloud computing”, J ournal of Network and Computer Applications, vol. 67, pp. 99-117, Jan. 20 16.
[14] C. Stergiou, K. E. Psannis, B.-G. Kim and B. Gupta, “Secure integrat ion of the IoT and cloud computing”, Future Generation Computer System s, vol. 78, pp. 964-975, Jan. 2018.
[15] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti

and M. Rajarajan, “Android security: a survey of issues, malware penetrat ion, and defenses”, IEEE communications surveys & tutorials, vol. 17, no. 2, pp. 998-1022, 2nd Quart. 2015.
[16] J. Huang, X. Zhang, L. Tan, P. Wang and B. Liang, “Asdroid: Detect ing stealthy behaviors in android applications by user interface and progra m behavior contradiction”, Proceedings of the IEEE/ACM International Co nference on Software Engineering (ICSE), pp. 1036-1046, May. 2014.
[17] F. Dalipi and S. Y. Yayilgan, “Security and privacy considerations for IoT application on smart grids: Survey and research challenges”, Proc. IE EE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW), p p. 63-68, Aug. 2016.
[18] N. A. Gunathilake, A. Al-Dubai and W. J. Buchana, “Recent Advance s and Trends in Lightweight Cryptography for IoT Security”, 2020 16th I nternational Conference on Network and Service Management (CNSM), p p. 1-5, Nov. 2020.
[19] S. H. Mun, M. U. Kim, and T. G. Gwon, “Trends in lightweight encr yption technology for IoT communication environments”, Information and Communications Magazine, vol. 33 no. 3, pp. 80-86, Feb. 2016.
[20] J. Daemen, and V. Rijmen, “The design of Rijndael: AES-the advanc ed encryption standard”, Springer, 2013.
[21] D. Kwon, J. Kim, S. Park, S. Sung, Y. Sohn, J. Song, Y. Yeom, E. Yoon, S. Lee, J. lee, S. Chee, D. Han, and J. Hong, “New Block Cipher: A RIA”, Information Security and Cryptology (ICISC03), LNCS 2971, Springe r, pp. 432-445, 2004.
[22] Z. Gong, S. Nikova, and Y. Law, “KLEIN: A New Family of Lightwe

ight Block Ciphers", RFID SP, LNCS, Springer, vol. 7055, pp. 1-18, 2012.
[23] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", CHES 2007, LNCS, Springer, vol. 4727, pp. 450-466, 2007.
[24] D. Hong, J. Lee, D. Kim, D. Kwon, K. Ryu, and D. Lee, "LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors", ISA, LNCS, Springer, vol.8267, pp. 3-27, 2013.
[25] T. Shirai, K. Shibutani, T. Akishita, S. Moriai and T. Iwata, "The 128-bit blockcipher CLEFIA", Proc. Fast Softw. Encryption., pp. 181-195, 2007.
[26] T. Eisenbarth, Z. Gong, T. Güneysu, S. Heyse, S. Indesteege, S. Kerckhof, F. Koeune, T. Nad, T. Plos, F. Regazzoni, F. X. Standaert and L. O. Oldenzeel, "Compact implementation and performance evaluation of block ciphers in ATtiny devices", Progress in Cryptology - AFRICACRYPT 2012, vol. 7374, pp. 172-187, 2012.
[27] L. Li, B. Liu and H. Wang, "QTL: a new ultra-lightweight block cipher", Microprocessors Microsyst., vol. 45, pp. 45-55, Aug. 2016.
[28] G Bansod, A Patil, S Sutar and N Pisharoty, "An ultra lightweight encryption design for security in pervasive computing", Big Data Security on Cloud (Big Data Security) IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Jul. 2016.
[29] S. Singh, P. K. Sharma, S. Y. Moon and J. H. Park, "Advanced light weight encryption algorithms for IoT devices: survey, challenges and solut

ions", Journal of Ambient Intelligence and Humanized Computing, pp. 1-18, May. 2017.

[30] P. Guo, J. Wang, S. Ji, X. H. Geng and N. N. Xiong, "A lightweight encryption scheme combined with trust management for privacy-preserving in body sensor networks", Journal of medical systems, vol. 39, no. 12, pp. 1-8, Dec. 2015.

[31] S. Heble, A. Kumar, K. V. V. D. Prasad, S. Samirana, P. Rajalakshmi and U. B. Desai, "A low power IoT network for smart agriculture", 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 609-614, Feb. 2018.

[32] D. Y. Kim and M. W. Jung, "Data transmission and network architecture in long range low power sensor networks for IoT", Wireless Personal Communications, vol. 93, no. 1, pp. 119-129, Jul. 2016.

[33] L. Zhou, X. Li, K.-H. Yeh, C. Su and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance", Future generation computer systems, vol. 91, pp. 244-251, Feb. 2019.

[34] R. Martínez-Peláez, H. Toral-Cruz, J. R. Parra-Michel, V. García, L. J. Mena, V. G. Félix and A. Ochoa-Brust, "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances", Sensors, vol. 19, no. 9, pp. 2098, May. 2019.

[35] S. J. Yu, K. S. Park and Y. H. Park, "A secure lightweight three-factor authentication scheme for IoT in cloud computing environment", Sensors, vol. 19, no. 16, pp. 1-20, Aug. 2019.

[36] P. Danzi, A. E. Kalør, Č. Stefanović and P. Popovski, "Delay and communication tradeoffs for blockchain systems with lightweight IoT client

s", IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2354-2365, Apr. 2019.

[37] M. T. Hammi, E. Livolant, P. Bellot, A. Serhrouchni and P. Minet, "A lightweight IoT security protocol", Proc. IEEE 1st Cyber Security Netw. Conf. (CSNet), pp. 1-8, Jan. 2017.

[38] T. Kim, J. Noh and S. Cho, "SCC: storage compression consensus for blockchain in lightweight IoT network", Proc. IEEE Int. Conf. Consum. Electron. (ICCE), pp. 1-4, Mar. 2019.

[39] A. Adeel, M. Ali, A. N. Khan, T. Khalid, F. Rehman, Y. Jararweh and J. Shuja, "A multi attack resilient lightweight IoT authentication scheme", Transactions on Emerging Telecommunications Technologies, Jul. 2019.

[40] B. J. Mohd and T. Hayajneh, "Lightweight block ciphers for IoT: energy optimization and survivability techniques", IEEE Access, vol. 6, pp. 35966-35978, Jun. 2018.

[41] G. De La T. Parra, P. Rad and K.-K. R. Choo, "Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities", Journal of Network and Computer Applications, vol. 135, pp. 32-46, Jun. 2019.

[42] C. Xu, S. Chen, J. Su, S. M. Yiu and L. C. K. Hui, "A survey on regular expression matching for deep packet inspection: applications, algorithms, and hardware platforms", IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2991-3029, 4th Quart. 2016.

[43] A. L. P. Gómez, L. F. Maimo, A. H. Celdran, F. J. G. Clemente, C. C. Sarmiento, C. J. Del Canto Masa, and R. M. Nistal, "On the generation of anomaly detection datasets in industrial control systems", IEEE Access,

vol. 7, pp. 177460-177473, Dec. 2019.
[44] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive dataset for network intrusion detection systems (UNSW-NB15 network dataset)”, Pro c. IEEE Mil. Commun. Inf. Syst. Conf. (MilCIS), pp. 1-6, Nov. 2015.
[45] Abhinav Dubey, IoT-Network-Intrusion-Detection-System-UNSW-N B15, Sep. 2021, [online] Available: https://github.com/abhinav-bhardwaj/Io T-Network-Intrusion-Detection-System-UNSW-NB15
[46] N. Moustafa, “Designing an online and reliable statistical anomaly det ection framework for dealing with large high-speed network traffic”, Diss. University of New South Wales, Jun. 2017.
[47] J. Hassannataj Joloudari, M. Haderbadi, A. Mashmool, M. Ghasemigol, S. S. Band and A. Mosavi, “Early detection of the advanced persistent thr eat attack using performance analysis of deep learning.”, IEEE Access, vo l. 8, pp. 186125-186137, Oct. 2020.
[48] J. B. Gross, D. Jacoby, K. Coogan and A. Helman, “Motivating compl exity understanding by profiling energy usage”, Proceedings of the 2021 ACM SIGPLAN International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software, pp. 85-96, Oct. 2021.
[49] A. Kumar, S. Sinha and R. Chaudhary, “A comparative analysis of e ncryption algorithms for better utilization”, International Journal of Comput er Applications, vol. 71, no. 14, pp. 17-23, May. 2013.
[50] D. A. Neri, R. P. Medina, and A. M. Sison, “An XBOX-based key ge neration technique for vigenere algorithm”, In Proceedings of the 3rd Inter national Conference on Cryptography, Security and Privacy, pp. 66-70, Ja n. 2019.

[51] S. W. Yun, N. E. Park and I. G. Lee, “Low Power Security Architect ure for the Internet of Things”, The Korea Institute of Information and C ommunication Engineering Conference (KIICE), Oct. 2021.

ABSTRACT

Low Power Security Architecture for the Internet of Things

Sunwoo Yun
Department of Future Convergence Technology Engineering
Graduate School of
Sungshin University

In this study, we proposed Wake-Up Security (WUS), a low-power security architecture that can utilize high-performance security algorithms on the Internet of Things environment. WUS adds a small logic that performs anomaly detection in IoT platform and executes the security module only when necessary according to the anomaly detection result. Therefore, it is possible to improve security and power efficiency while using a relatively high-complexity security module in a low-power environment compared to the conventional method of periodically executing a high-performance security module. In this paper, we implemented a Python simulator based on the UNSW-NB15 dataset to evaluate the power consumption, latency, and security performance of the proposed methods. According to the evaluation results, the power consumption of the proposed WUS mechanism is about 51.8% lower than that of the conventional high-performance security module and

about 27.2% lower than that of the lightweight security module, and the latency is about 74.8% and 65.9% lower. Furthermore, the WUS mechanism showed a high detection accuracy of about 96.5% or more and proved the detection efficiency performance improved by about 33.5% compared to the conventional model.