Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.1, Feb. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.1.83

무선 센서 네트워크에서 클러스터링 기반 Sleep Deprivation Attack 탐지 모델

김 숙 영,[1†] 문 종 섭[2‡]
[1,2]고려대학교 (대학원생, 교수)

Sleep Deprivation Attack Detection Based on Clustering in Wireless Sensor Network

Suk-young Kim,[1†] Jong-sub Moon[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

무선 센서 네트워크를 구성하는 무선 센서는 일반적으로 전력 및 자원이 극히 제한적이다. 무선 센서는 전력을 보존하기 위해 일정 주기마다 sleep 상태로 진입한다. Sleep deprivation attack은 무선 센서의 sleep 상태 진입을 막음으로써 전력을 소진 시키는 치명적인 공격이지만 이에 대한 뚜렷한 대응책이 없다. 이에 본 논문에서는 클러스터링 기반 이진 탐색 트리 구조의 Sleep deprivation attack 탐지 모델을 제안한다. 본 논문에서 제안하는 sleep deprivation attack 탐지 모델은 기계학습을 통해 분류한 공격 센서 노드와 정상 센서 노드의 특징을 사용한다. 이때 탐지 모델에 사용한 특징은 Long Short-Term Memory(LSTM), Decision Tree(DT), Support Vector Machine(SVM), K-Nearest Neighbor(K-NN)을 이용하여 결정하였다. 결정된 특징은 본 논문에서 제안한 알고리즘에 사용하여 공격 탐지를 위한 값들을 계산하였으며, 계산한 값을 판정하기 위한 임계값은 SVM을 적용하여 도출하였다. 본 논문에서 제안하는 탐지 모델은 기계학습으로 도출된 특징과 임계값을 본 논문에서 제안한 탐지 알고리즘에 적용하여 구성하였으며, 실험을 통해 전체 센서 노드 20개 중 공격 센서 노드의 비율이 0.35일 때 94%의 탐지율을 갖고 평균 에너지 잔량은 기존 연구보다 최대 26% 향상된 결과를 보였다.

ABSTRACT

Wireless sensors that make up the Wireless Sensor Network generally have extremely limited power and resources. The wireless sensor enters the sleep state at a certain interval to conserve power. The Sleep deflation attack is a deadly attack that consumes power by preventing wireless sensors from entering the sleep state, but there is no clear countermeasure. Thus, in this paper, using clustering-based binary search tree structure, the Sleep deprivation attack detection model is proposed. The model proposed in this paper utilizes one of the characteristics of both attack sensor nodes and normal sensor nodes which were classified using machine learning. The characteristics used for detection were determined using Long Short-Term Memory, Decision Tree, Support Vector Machine, and K-Nearest Neighbor. Thresholds for judging attack sensor nodes were then learned by applying the SVM. The determined features were used in the proposed algorithm to calculate the values for attack detection, and the threshold for determining the calculated values was derived by applying SVM.Through experiments, the detection model proposed showed a detection rate of 94% when 35% of the total sensor nodes were attack sensor nodes and improvement of up to 26% in power retention.

Keywords: Wireless sensor network, Sleep deprivation attack, S-MAC, Energy efficiency.

Received(10. 21. 2020), Modified(11. 30. 2020), Accepted(12. 28. 2020)

† 주저자, sykim1223@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr(Corresponding author)

I. 서 론

무선 센서 네트워크(Wireless Sensor Network, WSN)는 연산 능력과 무선 통신 능력을 갖춘 무선 센서를 응용 환경에 배치하여 자율적으로 형성한 네트워크이다. 무선 센서 네트워크는 홈 네트워크, 공장 관리, 재난 감시 등 다양한 분야에 적용 가능하며 사물인터넷(Internet of Things, IoT) 기술의 근간이 되었다. 무선 센서 네트워크에서 인접한 센서 노드들은 유사한 정보를 감지하는 특성을 가지기 때문에 임의의 센서 노드의 기능이 소멸하거나 동작이 실패하더라도 네트워크의 전체적인 동작에는 영향을 미치지 않는 장점이 있다.

일반적으로 센서 노드는 건전지를 사용하는 저전력 기기이며 접근이 어려운 지역에 임의로 배치되기 때문에 전력 소비는 무선 센서 네트워크의 가장 큰 이슈 중 하나이다. 이에 센서 노드의 수명을 연장하기 위한 에너지 효율적인 MAC 프로토콜들이 제안되어 있다. MAC 프로토콜은 센서 노드의 전력 낭비를 유발하는 오버히어링(overhearing) 문제를 해결하기 위해 통신 상태를 Sleep/Active 사이에서 주기적으로 전환하여 전력을 보존한다. 그러나 MAC 프로토콜은 Sleep deprivation attack에 취약하다[1, 2]. Sleep deprivation attack의 공격 대상은 무선 센서와 같이 건전지로 전원을 공급받고 전력을 보존하기 위해 sleep 기능을 탑재한 저전력 연산 기기이다. 공격자는 희생자 센서 노드의 전력을 소진할 목적으로 희생자 센서 노드와 통신함으로써 희생자 센서 노드가 Sleep 상태로 전환하는 것을 막는다. Sleep deprivation attack을 받는 희생자 센서 노드는 Sleep 상태로 진입하지 못하고 전력을 급격히 소진한다.

무선 센서 네트워크는 IoT 시스템의 근간으로서 센서 노드의 수명은 IoT 서비스 품질에 큰 영향을 미친다. 그러나 IoT 기술을 우리 생활에 적용하는 연구가 많이 진행된 반면 센서 노드를 위협하는 sleep deprivation attack에 대한 뚜렷한 대응 방안은 제시되지 않고 있다. 이에 본 논문에서는 무선 센서 네트워크를 대상으로 한 sleep deprivation attack을 탐지하는 모델을 제안한다.

본 논문에서 제안하는 Sleep deprivation attack 탐지 모델의 기여는 다음과 같다. 첫째, 무선 센서 네트워크에 기계학습을 적용하는 방법을 제안함으로써 공격 탐지에 사용되는 요소를 도출하고 탐지 모델의 신뢰성 및 탐지율을 높였다. 둘째, 공격 센서 노드의 특징을 학습하여 적은 양의 탐지 연산으로도 공격을 탐지할 수 있음을 보였다. 일반적으로 무선 센서 네트워크는 한정된 자원으로 인해 기계학습을 적용하기 부적합하다. 그러나 본 논문에서는 시뮬레이션 데이터 학습 단계와 센서 노드의 탐지 연산 단계를 분리함으로써 센서 노드의 연산 부담을 주지 않으면서도 기계학습의 이점을 취하였다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 살펴보고 3장에서 제안 모델을 설명한다. 4장에서 ns-2를 이용한 시뮬레이션 결과를 보이고 마지막 5장에서는 결론을 제시한다.

II. 관련 연구

본 절에서는 무선 센서 네트워크를 클러스터링하여 구성하는 이유와 본 논문에서 사용하는 기존의 클러스터 헤드 선출법을 설명하고, 본 논문에서 탐지하고자 하는 sleep deprivation attack과 sleep deprivation attack를 탐지하는 다양한 연구에 대해 설명하였다.

2.1 Cluster head selection

무선 센서 네트워크에서 인접한 센서 노드들은 유사한 정보를 수집하는 특징이 있으며 각 센서 노드들이 동일한 정보를 중앙 데이터 프로세서에 각각 전송하는 것은 전력 낭비이다. 이에 대한 효율적인 해결책은 클러스터링을 이용하는 것이다. 무선 센서 네트워크에서의 클러스터링은 물리적으로 인접한 센서 노드를 하나의 그룹으로 구성하는 데에 이용된다[8]. 클러스터링의 주요 이점은 데이터 취합을 가능하게 하여 중복 데이터를 네트워크에서 제거한다는 것이다. 이를 위해 클러스터의 노드 중 하나를 클러스터 헤드 노드(CH)로 선출하여, 헤드 노드가 센서 그룹의 수집 데이터의 처리하고 단일 메시지를 전송하도록 한다. 따라서 헤드 노드는 수집된 데이터를 처리하고 전송하기 때문에 다른 센서 노드들보다 에너지 소모가 크다. Low Energy Adaptive Clustering Hierarchy(LEACH)[21]는 대표적인 클러스터링 기반 라우팅 프로토콜로써, 센서 노드의 에너지 소모를 균등하게 분산하기 위해 확률 기반으로 클러스터 헤드를 선정한다. LEACH의 클러스터 헤드 선출에서 가장 중요한 요소는 센서 노드의 잔여 에너

지량이다. LEACH의 클러스터 헤드 선출 기법은 모든 센서 노드가 균등하게 에너지를 소비하지 않는 경우 클러스터 헤드를 공정하게 선정할 수 없다는 단점이 있다. 본 논문에서는 LEACH에서의 클러스터 헤드 선출 기법을 통해 클러스터 헤드를 선출한다.

2.2 Sleep Deprivation Attack

MAC 프로토콜은 Medium Access Control 계층에서 동작하며 전송 매체를 여러 센서 노드가 효율적으로 공유할 수 있게 한다. 무선 센서 네트워크에서 MAC 프로토콜의 가장 큰 설계 목적은 각 센서 노드의 에너지 소모를 최소화하여 전체 네트워크의 수명을 최대화하는 것이다. 무선 센서 네트워크에서 센서 노드의 에너지 효율적인 통신을 위해 설계된 대표적인 MAC 프로토콜은 Sensor-MAC(S-MAC)[30], Timeout-MAC(T-MAC)[29], Berkeley MAC(B-MAC)[31] 등이 있다.

무선 센서 네트워크에서 센서 노드의 상태는 크게 송신 상태, 수신 상태, Idle 상태와 Sleep 상태로 나누어지며 Sleep 상태일 때 에너지 소모가 가장 적다. MAC 프로토콜은 제어 패킷인 RTS(Request to Send) 패킷과 CTS(Clear to Send) 패킷을 이용하여 센서 노드가 예정된 통신이 있는지 확인하고 센서 노드가 통신에 참여하지 않을 때 Sleep 상태로 전환하여 에너지를 보존한다.

Sleep deprivation attack은 Stajano에 의해 처음 제시된 개념이다[1, 2]. Sleep deprivation attack은 MAC 프로토콜의 제어 패킷을 이용하여 센서 노드가 Sleep 상태로 전환하는 것을 막음으로써 센서 노드의 전력 소진을 목표한다. Fig. 1.은 sleep deprivation attack의 원리를 간단하게 묘사한 그림이다. 공격자는 희생자 센서 노드에게 통신을 요청하는 제어 패킷을 전송함으로써 희생자 센서 노드는 통신이 예정되어 있다고 착각하여 Sleep 상태로의 진입을 연기한다. 공격자는 희생자 센서 노드에게 통신을 요청하는 제어 패킷을 지속적으로 전송함으로써 희생자 센서 노드가 전력을 소진할 때까지 Sleep 상태로 전환하는 것을 막는다.

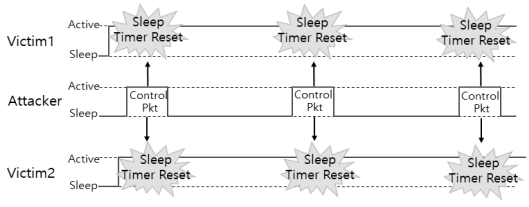

Fig. 1. Sleep deprivation attack principles

2.3 Sleep Deprivation Attack 탐지 연구

무선 센서 네트워크를 대상으로 발생하는 sleep deprivataion attack을 탐지하고 그 피해를 줄이기 위한 다양한 연구가 진행되어왔다.

Hsueh 등은 2단계 보안 전송을 기반으로 sleep deprivation attack을 탐지하는 방법을 제시하였다[12]. 센서 노드간 공유한 대칭키에 해시 체인을 적용하여 생성한 세션키를 통해 상호 인증을 수행한다. 세션키 생성에는 MD5나 SHA-1 등 연산이 빠른 해시함수를 사용한다.

Fotohi 등은 RSA 알고리즘과 Diffie-Hellman 키교환 방법과 같은 interlock 프로토콜을 이용하여 센서 노드 간에 키를 교환하고 교환한 키쌍을 통해 노드를 인증하는 방법을 적용하여 sleep deprivation attack을 탐지하는 방안을 제시하였다[23].

Gunasekaran 등은 센서 노드의 이상 행위를 분석하기 위해 효율적인 유전 알고리즘(GA)을 기반으로 sleep deprivation attack을 탐지하는 알고리즘을 제시하였다[26]. 또한 기지국(Base station)에 MRSA(Modified-RSA)을 구현하여 비대칭키쌍을 생성하고 센서 노드들에 배포하여 센서 노드의 신뢰성을 보장하였다.

Zhang 등은 각 센서 노드들이 인접한 센서 노드의 주소 및 sleep 타이머를 테이블에 기록하여 이웃 센서 노드의 sleep 주기를 예측하고 예측한 통신 가능 시간 이외에는 해당 센서 노드와의 채널을 닫음으로써 sleep deprivation attack의 영향을 감소시킨다[26].

또한, Zhang등은 PEECR(Predictive Efficient Energy Consumption Reclaim) 기반 클러스터 헤드 선출 기법을 제안하였다[27]. 센서 노드의 전력 소모를 무선 센서 네트워크 전체에 균등하게 분산시킴으로써 전력 소모를 극대화 시키는 sleep deprivation attack의 영향을 최소화하였다.

Zhang 등은 진화 게임 이론을 적용하여 부반송파(sub-carrier)할당을 최적화함으로써 무선 센서 네트워크의 에너지 효율을 높였다[28]. 센서 노드들은 대칭키쌍을 공유하여 노드 간에 인증을 수행함으로써 전력을 제어하며 이때 3-DES, DES 암호 알

고리즘을 사용한다.

Fotohi 등은 위의 sleep deprivation attack 탐지 모델에 대해 각각 GA-DoSLD[25], CrossLayer[12], ASDA-AES[27], ASDA-3DES, ASDA-DES[28] 그리고 ASDA-BlowFish[26]라고 명명하였다[23].

III. 제안 모델

본 장에서는 S-MAC 프로토콜이 적용된 무선 센서 네트워크를 대상으로 발생하는 sleep deprivation attack을 탐지하는 방법을 제안한다.

Fig. 2.와 같이 본 논문에서 제안하는 모델은 무선 센서 네트워크 클러스터링 형성, 탐지 요소 도출, 임계값 학습, 공격 센서 노드 탐지 단계로 이루어져 있다.

본 논문에서 제안하는 모델은 클러스터링을 통해 분할된 무선 센서 네트워크 환경을 대상으로 한다. 이에 먼저 3.1절에서 클러스터 헤드를 선출하여 네트워크를 클러스터링하는 것을 설명하며 이때 클러스터 헤드 선출은 LEACH의 클러스터 헤드 선출 기법을 사용하였다. 이후 3.2절에서 클러스터링한 무선 센서 네트워크 환경을 시뮬레이션하여 생성된 데이터로부터 sleep deprivation attack 공격 탐지에 활용할 특징을 기계학습을 이용하여 결정한다. 3.3절에서는 탐지 알고리즘에 공격 센서 네트워크를 판별하는데 사용하는 임계값을 학습하는 과정을 설명하였으며 3.4절에서는 계산된 임계값을 적용하여 sleep deprivation attack을 탐지하는 알고리즘을 제시하였다.

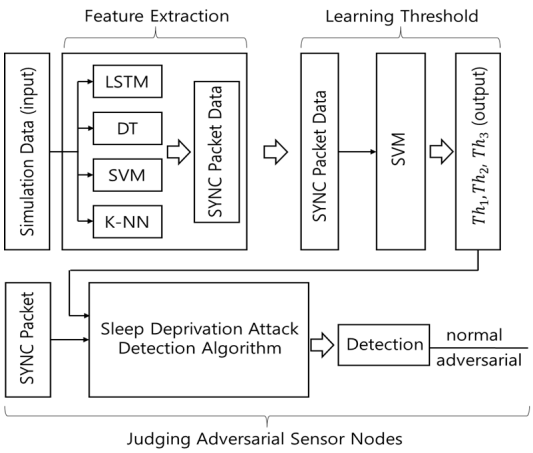

Fig. 2. Overall structure of proposed model

3.1 클러스터링 형성

본 논문에서는 이진 탐색 트리 구조의 클러스터링 기반 Sleep deprivation attack 탐지 모델을 제안한다. Fig. 3.는 본 논문에서 제안하는 클러스터링 기반 sleep deprivation attack 탐지 모델의 구조이다.

무선 센서 네트워크에서 물리적으로 인접한 센서들은 유사한 정보를 다룬다는 특징이 있다. 이에 정보수집 및 전달의 효율을 높이기 위해 물리적으로 인접한 무선 센서들을 클러스터링하여 네트워크를 분할한다. 본 논문에서 제안하는 탐지 모델에서 무선 센서 네트워크를 클러스터링할 때 각 클러스터는 이진 탐색 트리 구조로 형성된다. 무서 센서 네트워크를 트리 구조로 구성하는 것은 모든 센서 노드가 기지국(Base station)으로 데이터를 중복전송하는 것을 방지하는 장점이 있다[32]. 또한, 무선 센서 네트워크는 임의의 센서 노드가 추가되거나 삭제되는 경우가 많다. 이에 노드의 삽입 또는 삭제 연산이 용이한 이진 탐색 트리를 적용하였다.

각 클러스터에는 클러스터 헤드(CH)가 존재하며 CH는 LEACH의 클러스터 헤드 선출 기법을 이용하여 선출한다. LEACH는 무선 센서 네트워크에서 가장 널리쓰이는 클러스터링 기법으로, 클러스터 헤드 선출 시 센서 노드의 잔여 에너지량을 가장 중요한 기준으로 삼는다[21]. 이에 센서 노드의 에너지 소모를 균등하게 분산함으로써 네트워크 전체의 수명을 늘릴 수 있다는 장점이 있어 클러스터 헤드 선출에 적용하였다. 선출된 CH는 제안한 이진 탐색트리의 루트 노드로 삼는다. 선출된 CH는 인접한 센서 노드에게 클러스터로의 참여 요청 메시지를 보내고 클러스터에 참여하고자 하는 센서 노드들은 참여 요

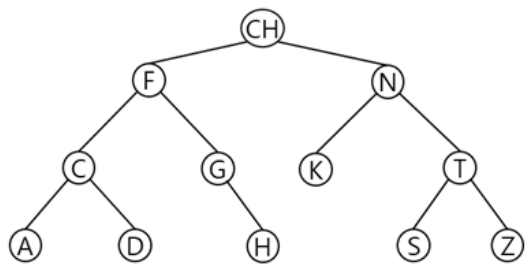

Fig. 3. Proposed detection model

청 메시지를 전송하여 클러스터를 생성한다. 모든 센서 노드들은 고유한 ID 값을 가지고 있으며 클러스터에 추가되는 순서대로 ID 값에 따라 이진 탐색 트리를 형성한다.

3.2 탐지 요소 도출

본 논문에서 제안하는 탐지 모델이 활용한 탐지 요소를 도출하기 위해 기계학습을 이용한다. 네트워크 시뮬레이션 수행 시 발생하는 트래이스(trace) 파일로 확인할 수 있는 정보를 Long Short-Term Memory(LSTM), Decision Tree(DT), Support Vector Machine(SVM), K-Nearest Neighbor(K-NN)에 각각 입력값으로 사용하여 학습함으로써 공격 센서 노드와 정상 센서 노드를 가장 잘 분류할 수 탐지 요소를 도출하였다.

Table. 1.은 트래이스 파일을 구성하고 있는 필드들과 그 의미이다. 각각의 파라미터들은 시간의 흐름에 따라 생성된다.

기계학습 알고리즘에 입력한 데이터는 전체 센서 노드 5개, 공격 센서 노드 1개로 구성한 시뮬레이션을 10번 수행하여 생성된 트래이스 파일을 취합하여 생성하였다. 이때 테스트 데이터를 생성하기 위한 시뮬레이션은 리눅스 우분투 18.4 환경에서 오픈소스 네트워크 시뮬레이터인 NS-2를 통해 수행하였으며 시뮬레이션 수행 시 사용된 파라미터는 Table. 2.와 같다.

Table. 3.은 각 공격 센서 노드를 분류하는 특징을 도출할 때 사용한 학습 데이터와 정확도를 측정하기 위한 테스트 데이터의 수를 공격 센서 노드와 정상 센서 노드별로 정리한 표이다.

생성된 데이터는 ($T_{simulation}$, $Param$)으로 파싱(parsing)한다. $T_{simulation}$은 Table. 1.의 Time을 의미하며 $Param$은 Table. 1. 중에서 Event, Pkt type, Energy 파라미터이다. 각 파라미터별로 데이터를 파싱하는 것은 어떤 파라미터가 공격 센서 노드와 정상 센서를 분류하는데 유용한지 알기 위함이다. 그리고 시간별로 파라미터를 파싱하는 것은 시간이 흐름에 따라 정상 센서 노드와 공격 센서 노드의 차이가 발생하기 때문이다. Table. 1.의 파라미

Table 1. Trace file format and descriptions

Parameters	Description
Event	The four symbols of r, +, - and d are used. Indicates receive, enqueue, dequeue and drop respectively.
Time	The time at which the event occurred.
From node	The input node connected with the link where the event occurred.
To node	The output node connected with the link where the event occurred.
Pkt type	Packet type.
Pkt size	Packet size.
Flags	The value of the flag array defined in ~ns/trace/trace.cc, each of which has the meaning of 'Congestion Experienced', 'Congestion Action', 'TCP Fast Start', etc.
Fid	Flow id of IPv6.
Scr addr	The address of the origin node.
Dst addr	The address of the destination node.
Seq num	Packet serial number.
Pkt id	Packet unique identification number.
Energy	Residual energy of node.

Table. 2. Setting of simulation parameters

Parameters	Value
Sensor network size (m x m)	80 x 80 m^2
Simulation time	70 s
Duty cycle	20
Transmission range	150 - 250 m
Traffic type	CBR
Packet size	512 $Bytes$
RTS, CTS, ACK size	30 $Bytes$
The Initial energy	35 J
The Idle power	41 mW
The Receiving power	45 mW
The Transmission power	41 mW
The Sleep power	25 μW

Table 3. Dataset used in feature selection

Dataset	# adversary	# normal	# total
Train	72,200	436,704	508,904
Test	24,274	391,559	415,833

터 중 Event, Pkt type, Energy를 기계학습에 적용하는 이유는 해당 파라미터들이 공격 센서 노드의 특징을 나타낼 수 있기 때문이다. 예를 들어, From node, To node, Scr addr, Dst addr, Fid 등은 센서 노드의 주소와 관련된 정보로, 공격 센서 노드의 행동적 특징을 나타내지 못한다. 지도학습을 통해 공격 센서 노드의 주소정보를 학습하더라도 다른 데이터로 테스트 시 공격 센서 노드의 주소정보가 변경되기 때문에 학습을 통한 탐지가 불가능하다. 마찬가지로 Seq num, Pkt id, Flags는 각 패킷의 독립적인 정보를 나타낼 뿐 노드의 행동적 특징을 분류할 수 있는 유의미한 정보를 표현하지 못한다. Pkt size의 경우 Pkt type과 마찬가지로 패킷의 종류를 구분하는데 이용될 수 있지만, ACK, CTS, RTS 패킷의 크기가 동일하여 구분할 수 있는 패킷의 종류가 Pkt type보다 적어 학습에 사용하지 않았다. 따라서 공격 센서 노드의 특징을 나타낼 수 있을 것으로 보이는 이 외의 파라미터인 Event, Pkt type, Energy에 대해서 기계학습을 적용한다.

Fig. 4.는 탐지 요소를 도출하기 위해 기계학습을 적용하는 구조이다. 공격 센서 노드와 정상 센서 노드를 분류하는 특징을 찾기 위해 파싱된 데이터를 4개의 기계학습 알고리즘에 적용하여 정상 센서 노드와 공격 센서 노드를 분류하였다. 이때 LSTM, DT, SVM, K-NN은 서로 조합하지 않고 각각 적용하였다.

Table. 4.는 파라미터별로 LSTM, DT, SVM, K-NN을 적용하여 공격 센서 노드와 정상 센서 노드를 분류하였을 때의 정확도와 정확도의 평균을 나타낸 것이다. Table. 4.를 통해 Energy, Pkt type, Event 파라미터가 공격 센서 노드와 정상 센서 노드를 분류할 수 있는 특징임을 알 수 있으며, Eneryge, Pkt type, Event 순으로 공격 센서 노드의 특징을 잘 나타냄을 알 수 있다. 그러나 시뮬레이션

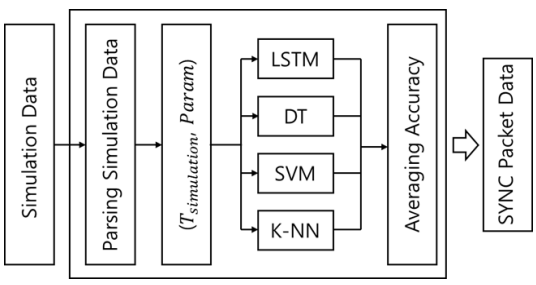

Fig. 4. Structure of feature selection

Table 4. Accuracy by parameters and algorithms

	Energy	Pkt type	Event
LSTM	96.6	95.2	95.2
DT	98.9	94.2	94.2
SVM	78.1	94.2	94.1
K-NN	97.0	77.3	74.7
Avg	92.6	90.2	89.5

환경이 아닌 실제 환경의 경우, 패킷을 수신하는 센서 노드는 Pkt type 이외의 정보를 알기 어렵다. 따라서 본 논문에서 제안하는 공격 탐지 모델은 Pkt type 만을 탐지 요소로 사용하였다. 시뮬레이션 시 생성되는 패킷의 타입은 Data, Request To Send(RTS), Clear To Send(CTS) 그리고 SYNC 패킷 4가지이다. 본 논문에서 제안하는 모델은 S-MAC 프로토콜이 적용된 센서 네트워크를 대상으로 발생하는 sleep deprivation attack 탐지를 목표한다. SYNC 패킷은 S-MAC 프로토콜에서 sleep 주기를 조절하는 제어 패킷으로 sleep deprivation attack에 사용되어 공격의 특징이 가장 잘 드러나는 패킷이다[3, 6]. 따라서 Data, RTS, CTS, SYNC 패킷 중 SYNC 패킷을 임계값 학습 및 탐지 알고리즘에 사용한다.

3.3 *Th* 값 학습

본 논문에서 제안하는 탐지 모델은 공격 센서 노드를 판별하기 위해 3단계에 거쳐 탐지 연산을 수행한다. 탐지 알고리즘에는 기계학습은 활용되지 않고, 탐지 연산의 각 단계마다 SYNC 패킷 정보를 이용하여 계산한 값과 사전에 기계학습을 통해 도출한 임계값을 비교하여 공격 센서 노드 여부를 검사한다. 탐지 알고리즘을 구성할 때 기계학습 모델을 적용하지 않는 이유는 기계학습 시 연산능력 및 전력량 등 요구되는 자원이 큰 반면, 무선 센서 노드의 하드웨어 자원은 극히 제한적이기 때문이다. 따라서 탐지 연산의 각 단계에 사용하는 임계값은 기계학습을 통해 사전에 계산하고, 센서 노드의 탐지 과정에는 기본 연산만을 수행함으로써 센서 노드의 자원 소모량을 최소화한다.

Fig. 5.는 전체 탐지 알고리즘 중 3단계의 탐지 연산만을 보여주는 그림이다. 탐지 연산을 3단계로 구분한 것은 SYNC 패킷을 이용한 sleep depriva

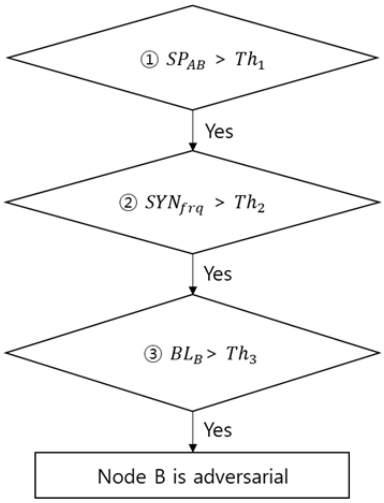

Fig. 5. Three steps of the detection operation

tion attack의 공격 특징을 바탕으로 공격을 탐지하기 위함이다. S-MAC 프로토콜이 적용된 센서 네트워크 대상의 sleep deprivation attack은 공격 센서 노드가 일정 주기마다 SYNC 패킷만을 지속적으로 전송함으로써 수행된다. 이에 1단계에서 특정 센서 노드가 전송한 SYNC 패킷의 개수를, 2단계에서는 누적된 SYNC 패킷의 개수를 이용하여 SYNC 패킷이 전송되는 주기를 확인한다. 3단계는 앞선 단계의 결과를 종합하여 센서 노드가 공격 센서 노드인지 아닌지 판결을 내리는 단계이다. 탐지 연산의 각 단계에서 위와 같은 목표를 가지고 임계값과 비교하는 SP_{AB}, SYN_{frq}, BL_B은 SYNC 패킷 정보를 이용하여 계산한 값이다. 각 센서 노드들은 수신한 SYNC 패킷의 정보를 저장하는 SYNC Packet (SP) 테이블을 갖고 있다. 첫 번째 탐지 연산의 SP_{AB}는 센서 노드 A가 센서 노드 B로부터 수신한 SYNC 패킷의 개수이다. 두 번째 탐지 연산의 SYN_{frq}는 SP_{AB}값을 이용해 계산하며 센서 노드 B가 SYNC 패킷을 전송한 주기를 의미한다. 세 번째 탐지 연산의 BL_B은 클러스터 헤드가 유지하는 블랙리스트 테이블에서 센서 노드 B가 두 번째 탐지 연산에 저촉된 횟수를 의미한다. 탐지 연산의 각 단계에서 사용하는 임계값 Th_1, Th_2, Th_3은 기계학습을 통해 사전에 도출한 값이며 정상 센서 노드와 공격 센서를 분류하는 기준값이다.

본 절에서는 각 단계마다 SYNC 패킷으로부터 계산한 값을 SVM으로 학습하여 Th_1, Th_2, Th_3 값을 구하였다. SVM은 분류와 예측 문제에 적합하므로 본 논문에서 제안하는 탐지 모델의 임계값을 도출하는데 사용하였다.

SVM 학습 시 이용한 학습 데이터는 리눅스 우분투 18.4 환경에서 오픈소스 네트워크 시뮬레이터인 NS-2를 통해 생성하였으며 Table. 5.는 시뮬레이션 수행 시 사용된 파라미터를 정리한 것이다.

시뮬레이션 데이터 생성하기 위해 전체 센서 노드의 개수를 정함에 앞서, 임계치 학습은 각 공격 센서 노드가 생성하는 SYNC 패킷의 개수로 수행되므로 시뮬레이션 시 전체 센서 노드는 중요하지 않을 것으로 보인다. 이를 확인하기 위해 지역 모니터링을 위해 38개의 무선 센서 노드를 배치하여 구성한 하이브리드 WSN[33]과 같이 38개의 센서 노드를 배치한 경우와 그 절반 비율의 19개의 센서 노드를 배치한 경우의 시뮬레이션을 수행하였다. 각 공격 센서 노드가 생성하는 SYNC 패킷의 평균 개수 약 108개로 유사하였으며, 이를 통해 임계치 학습에 활용되는 각 공격 센서 노드가 생성하는 SYNC 패킷의 개수는 전체 센서 노드 개수에 영향을 받지 않음을 알 수 있다. 이에 임계값 학습을 위한 시뮬레이션은 전체 센서 노드 19개 중 정상 센서 노드의 수는 16개, 공격 센서 노드의 수는 3개로 구성하였다.

Table. 6.는 각 임계값을 학습할 때 사용한 학습 데이터의 수이다.

Fig. 6.는 임계값을 학습하는 과정을 나타낸 그림

Table 5. Setting of simulation parameters

Parameters	Value
Sensor network size (m x m)	80 x 80 m^2
Simulation time	70 s
Duty cycle	20
Transmission range	150 - 250 m
Traffic type	CBR
Packet size	512 $Bytes$
RTS, CTS, ACK size	30 $Bytes$
The Initial energy	35 J
The Idle power	41 mW
The Receiving power	45 mW
The Transmission power	41 mW
The Sleep power	25 μW

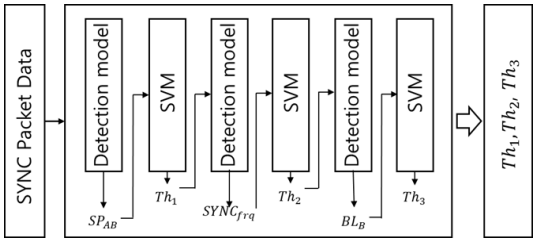

Fig. 6. Structure of learning threshold

Table 6. Dataset used in learning threshold

Dataset	# Th_1	# Th_2	# Th_3
Train	8,466	8,723	2,138

이다. Fig. 5. 와 Fig. 6.에서 볼 수 있듯이 각 탐지 단계에서 사용하는 임계값들은 앞선 탐지 단계의 결과에 종속적이므로 Th_1, Th_2, Th_3을 순차적으로 학습하여야 한다.

가장 먼저 첫 번째 단계의 임계값 Th_1은 시간에 따른 SP_{AB}의 변화를 확인하여 공격 센서 노드를 분류하기 위한 값이다. 따라서 시간에 따른 SP_{AB} 값을 SVM으로 학습하였을 때 공격 센서 노드와 정상 센서 노드를 분류하는 직선이 Th_1가 된다. 이때 SYNC 패킷은 시간이 흐름에 따라 누적되므로 Th_1는 상수가 아닌 시간에 따라 변하는 1차 함수로 표현되며 식 (1)과 같이 도출된다. 식 (1)에서 t는 네트워크가 시작된 이후 탐지를 위한 첫 번째 단계를 검사하는 시점의 시간을 의미한다. t의 계수는 Th_1 함수의 기울기로서 시간에 따른 SYNC 패킷의 증가 추이를 나타내며 시간이 흐를수록 누적 SYNC 패킷의 값은 증가하므로 양의 기울기를 가진다. 상수 값은 이에 따른 보정값으로 SVM을 통해 도출하였다.

$$Th_1 = 0.11248172827*t - 0.050379196465 \quad (1)$$

Th_2를 학습하기 위해 SVM의 입력값으로 들어가는 SYN_{frq}은 식 (2)로 계산한다. 식 (2)에서 t는 네트워크가 시작된 이후 탐지를 위한 첫 번째 단계를 검사하는 시점의 시간이다.

$$SYN_{frq} = \frac{SP_{AB}}{t} \quad (2)$$

Th_2는 식 (2)에서 계산한 SYN_{frq}값을 SVM으로 학습하여 공격 센서 노드와 정상 센서 노드를 분류하는 직선에 대한 식이다. SYN_{frq}은 SP_{AB}에 따라 생성되는 값이기 때문에 Th_2도 식 (1)과 마찬가지로 시간에 따른 1차 함수로 표현되며 식 (3)과 같이 도출되었다. t의 계수는 Th_2 함수의 기울기로서 시간에 따른 SYNC 패킷의 전송 주기 변화를 나타내며 식 (1)과 식 (2)에 따라 SYNC 패킷의 증가폭이 시간의 증가폭보다 작으므로 음의 기울기를 가진다. 상수 값은 이에 따른 보정값으로 SVM을 통해 도출하였다.

$$Th_2 = -(6.04474*10^{-4})*t + 0.404375747 \quad (3)$$

마지막으로 Th_3은 BL_B값을 SVM의 입력값으로 하여 공격 센서 노드와 정상 센서 노드를 분류하는 식이다. BL_B은 앞선 식 (1)과 식 (3)을 각각 Th_1, Th_2에 대입하여 탐지 알고리즘을 수행하였을 때, 센서 노드 B가 앞선 단계에 공격 센서 노드로 분류된 횟수를 저장한 값이다. 즉, BL_B값에 따라 정상 센서 노드와 공격 센서 노드가 분포되어있을 때 정상 센서 노드와 공격 센서 노드를 분류하는 직선이 Th_3이다. 이때 BL_B는 SP_{AB}과 SYN_{frq}의 값에 영향을 받으므로 Th_3는 식 (4)과 같이 시간에 따른 1차 함수로 표현된다. t의 계수는 Th_3의 기울기로서 시간이 흐름에 따라 두 번째 탐지 연산에 저촉된 횟수의 증가 추이를 나타내며 앞선 탐지 연산에 모두 저촉된 이 후 증가되는 값이기 때문에 증가율이 매우 작다. 상수 값은 이에 따른 보정값으로 SVM을 통해 도출하였다.

$$Th_3 = (2.9219815221*10^{-5})*t + 0.99921452 \quad (4)$$

SVM 학습을 통해 도출된 임계값으로 정상 센서 노드와 공격 센서 노드를 분류한 정확도를 측정하였다. 이때 테스트 데이터를 생성하기 위한 시뮬레이션은 리눅스 우분투 18.4 환경에서 오픈소스 네트워크 시뮬레이터인 NS-2를 통해 수행하였으며 시뮬레이션 수행 시 사용된 파라미터는 Table. 7.과 같다.

전체 센서 노드 20개 중 정상 센서 노드의 수 18개, 공격 센서 노드의 수는 2개로하여 임의로 구성

Table 7. Setting of simulation parameters

Parameters	Value
Sensor network size (m x m)	80 x 80 m^2
Simulation time	70 s
Duty cycle	20
Transmission range	150 - 250 m
Traffic type	CBR
Packet size	512 $Bytes$
RTS, CTS, ACK size	30 $Bytes$
The Initial energy	35 J
The Idle power	41 mW
The Receiving power	45 mW
The Transmission power	41 mW
The Sleep power	25 μW

하였다. 각 단계에서 공격 센서 노드를 분류한 정확도를 측정하기 위해 사용된 테스트 데이터의 수는 Table. 8.과 같다.

정확도는 식 (5)와 같이 계산하였다.

$$Accuracy = \frac{(TP+TN)}{(TP+FP+FN+TN)} \quad (5)$$

식 (5)에서 TP는 True Positive로 공격 센서 노드를 공격 센서 노드로 올바르게 예측한 경우, TN은 True Negative로 정상 센서 노드를 공격 센서 노드로 예측한 경우, FP는 False Positive로 공격 센서 노드를 정상 센서 노드로 예측한 경우, FN은 False Negative로 정상 센서 노드를 정상 센서 노드로 예측한 경우를 의미한다. Table. 9은 Th_1, Th_2, Th_3값을 대입하였을 때 각 단계에서 공격 센서 노드와 정상 센서 노드를 분류한 정확도를 나타낸다.

Table 8. Dataset used in testing threshold

Dataset	# Th_1	# Th_2	# Th_3
Test	57,340	48,620	5,880

Table 9. Accuracy

Parameter	Accuracy(%)
Th_1	91.0
Th_2	86.3
Th_3	98.5

3.4 공격 센서 노드 판정

본 논문에서 제안하는 탐지 모델의 탐지 과정은 Fig. 7.과 같다. Fig. 7.에서의 Th_1, Th_2, Th_3는 3.3.절에서 SVM을 통해 도출한 임계값이다.

공격 탐지를 위한 탐지 연산은 크게 3단계로 수행된다. 공격 탐지에는 앞서 탐지 요소 도출 단계에서 결정한대로 시간에 따라 누적된 SYNC 패킷을 사용한다. 각 센서 노드들은 수신한 SYNC 패킷의 정보를 저장하는 SYNC Packet(SP) 테이블을 갖고 있다. SP_{AB}는 클러스터링을 형성함과 동시에 SP_{AB}=0으로 초기화한다. 첫 번째 탐지 연산에서는 SP_{AB}와 Th_1이 이용된다. Th_1는 공격 센서로 의심되는 센서를 가리기 위한 임계값이다. 센서 노드는 SP_{AB}을 Th_1과 비교하여 SP_{AB}가 Th_1보다 작으면 통신을 지속하여 SYNC 패킷의 정보를 수집하고 SP_{AB}가 Th_1보다 커지면 다음 검사로 넘어간다.

두 번째 탐지 연산에서 SYN_{frq}과 Th_2를 비교하여 SYN_{frq}값이 Th_2보다 작으면 통신을 계속하고 SYN_{frq}값이 Th_2보다 커지면 마지막 탐지 연산을 수행한다.

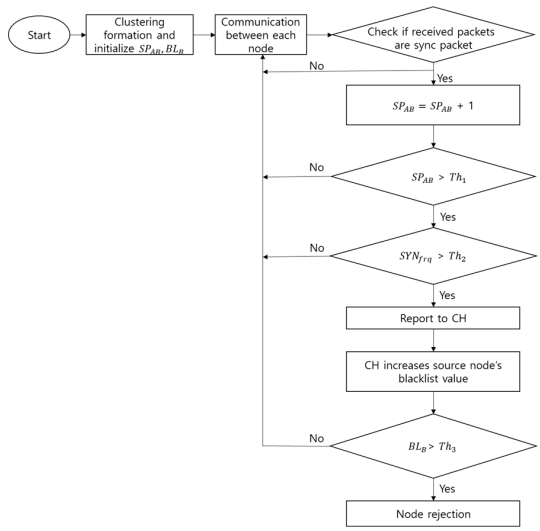

Fig. 7. Flowchart of the proposed model

세 번째 탐지 연산에서 BL_B은 처음 네트워크가 시작할 때 BL_B=0으로 초기화되며 임의의 센서 노드 B가 두 번째 탐지 연산에서 Yes가 나올 때 마다 1씩 증가한다. 마지막 탐지 연산에서 BL_B값과 Th_3을 비교하여 BL_B값이 Th_3보다 작으면 공격 노드가 아니라고 판단하여 통신을 계속하며 BL_B값은 다음 탐지 판정을 위해 유지한다. BL_B값이 Th_3보다 커지면 센서 노드 B를 공격 센서 노드로 판단하여 클러스터 전체에 공격 센서 노드의 정보를 브로드캐스팅하고 센서 노드 B가 전송하는 패킷을 모두 차단 및 센서 노드 B와 통신을 해지하여 센서 노드 B를 네트워크에서 고립시킨다.

IV. 실험 결과

본 절에서는 앞서 제안한 sleep deprivation attack 탐지 모델의 성능을 측정하기 위한 실험 구성과 평가 요소에 따른 실험 결과를 제시한다.

4.1 평가 요소

본 절에서는 제안한 탐지 모델에 대해 센서 노드의 평균 에너지 잔량 감소율과 탐지율을 평가하고 기존의 탐지 모델 CrossLayer[12], ASDA-RSA[23], GA-DoSLD[25], ASDA-BlowFish[26], ASDA-AES[27] 그리고 ASDA-3DES, ASDA-DES[28]과 비교하였다.

4.1.1 평균 에너지 잔량

평균 에너지 잔량 감소율 RE_{avg}은 공격을 받지 않는 정상적인 네트워크 환경에서 센서 노드들의 평균 에너지 잔량($RE_{Nonattacked}$)에 대해 공격을 받는 환경에서 센서 노드들의 평균 에너지 잔량($RE_{Attacked}$) 비율을 계산한 값을 의미하며, 식 (6)과 같이 계산한다.

$$RE_{avg} = \frac{RE_{Attaked}}{RE_{Nonattacked}} \tag{6}$$

4.1.2 탐지율

탐지율은 실제 공격 센서 노드에 대해 탐지된 공격 센서 노드의 비율이다. 탐지율은 식 (7)와 같이 계산한다[23].

$$DR = (\frac{TPR}{TPR + FNR})*100 \tag{7}$$

Table. 10.는 탐지율 계산에 사용된 파라미터를 정리한 것이다.

따라서 FPR, FNR, TPR, TNR은 식 (8)~(11)과 같이 계산하며, 식 (8)~(11)에서 TP, TN, FP, FN은 Table. 11.과 같다[23].

$$FPR = (\frac{FP}{FP+TN})*100 \tag{8}$$

$$FNR = (\frac{TP+TN}{ALL})*100 \tag{9}$$
$$;(All = FP+FN+TP+TN)$$

$$TPR = (\frac{TP}{TP+FN})*100 \tag{10}$$

$$TNR = (\frac{TN}{TN+FP})*100 \tag{11}$$

Table 10. Parameters used for detection rate

Parameters	Description
True Positive Rate(TPR)	The ratio of normal sensor node that were correctly detected as a normal node.
False Positive Rate(FPR)	The ratio of normal sensor node to total normal sensor that were mistakenly detected as a malicious node.
True Negative Rate(TNR)	The ratio of malicious sensor node the were correctly detected as a malicious node.
False Negative Rate(FNR)	The ratio of malicious sensor node to total normal node that were mistakenly detected as a normal node.

Table 11. Parameters used for detection rate

Parameters	Description
True Positive (TP)	The number of normal sensor node that were correctly detected as a normal node.
False Positive (FP)	The number of normal sensor node to total normal sensor that were mistakenly detected as a malicious node.
True Negative (TN)	The number of malicious sensor node the were correctly detected as a malicious node.
False Negative (FN)	The number of malicious sensor node to total normal node that were mistakenly detected as a normal node.

4.2 시뮬레이션 구성

본 논문에서 제안한 모델에 대한 실험은 리눅스 우분투 18.4 환경에서 오픈소스 네트워크 시뮬레이터인 NS-2를 통해 수행하였다. Table. 12.은 시뮬레이션 수행 시 사용된 파라미터를 정리한 것이다

Table 12. Setting of simulation parameters

Parameters	Value
Sensor network size (m x m)	80 x 80 m^2
Simulation time	70 s
Number of nodes	20
Duty cycle	20
Transmission range	150 - 250 m
Traffic type	CBR
Packet size	512 $Bytes$
RTS, CTS, ACK size	30 $Bytes$
The Initial energy	35 J
The Idle power	41 mW
The Receiving power	45 mW
The Transmission power	41 mW
The Sleep power	25 μW

4.3 실험 결과

실험 결과는 공격 센서 노드의 비율을 달리하여 탐지율과 평균 에너지 잔량을 측정하였다. 실험을 진행할 때에는 각 공격 센서 노드의 비율에 대하여 10번의 시뮬레이션을 수행하여 평균을 구하였다.

Fig. 8.은 본 논문에서 제안한 탐지 모델과 기존의 모델 간의 탐지율을 비교한 것이며 Fig. 9.는 평균 에너지 잔량을 비교한 것이다. 평균 에너지 잔량은 공격 센서가 없는 환경에서의 에너지 잔량과 sleep deprivation attack을 받는 환경에서의 에너지 잔량의 비율을 계산한 값이다.

Fig. 8.과 Fig. 9.에서 확인할 수 있듯이 대부분의 다른 모델들보다 탐지율과 평균 에너지 잔량이 높은 것을 알 수 있다. 이는 기존의 탐지 방법들이 암호 알고리즘을 이용하여 연산 비용이 높은 반면, 본 논문에서 제안한 탐지 모델은 사전에 기계학습을 이용하여 탐지 요소를 도출하고 공격 센서의 특성을 학습하였기에 에너지 효율이 높으면서도 높은 탐지율을 보였다. 또한 Fig. 8.에서 본 논문에서 제안한 모델은 공격 센서 노드의 비율이 증가할수록 탐지율 감소 기울기가 ASDA-RSA보다 가파르게 감소하고 있

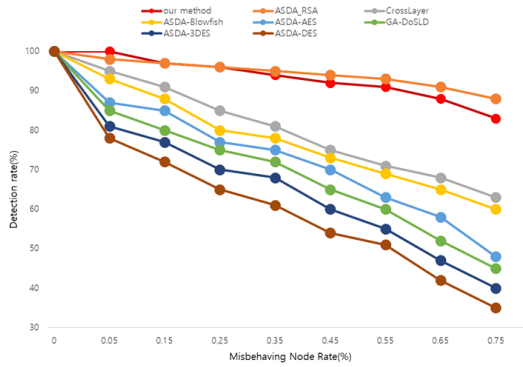

Fig. 8. Detection rate comparison of the proposed model and other models

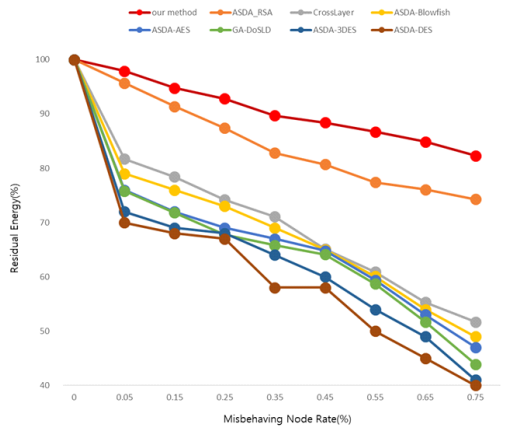

Fig. 9. Residual energy comparison of the proposed model and other models

다. 이에 공격 센서 노드의 비율이 0.35에서 탐지율이 94%로 ASDA-RSA보다 탐지율이 1% 낮아진다. 그러나 탐지검사 시 연산량이 적고 탐지율이 높아 공격 센서 노드의 공격을 차단하여 ASDA-RSA보다 평균 에너지 잔량이 6% 높게 측정되었다. 따라서 본 논문에서 제안하는 sleep deprivation attack 탐지 모델은 연산 비용이 적고 탐지 효율이 높아 자원 제한적인 센서 네트워크에 적합하다.

Fig. 10.은 센서 노드의 개수에 따라 본 논문에서 제안한 모델의 탐지율을 비교한 것이며 Fig. 11.은 센서 노드의 개수에 따라 본 논문에서 제안한 모델의 에너지 잔량을 비교한 그래프이다. 전체 센서 노드의 수가 증가함에 따라 탐지율 및 에너지 잔량이 소폭 증가하는 추세를 보인다.

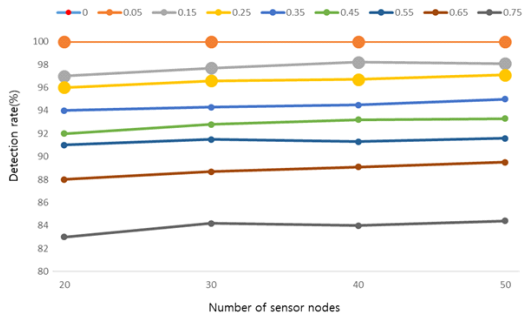

Fig. 10. Detection rate comparison of the proposed model by the number of sensor nodes

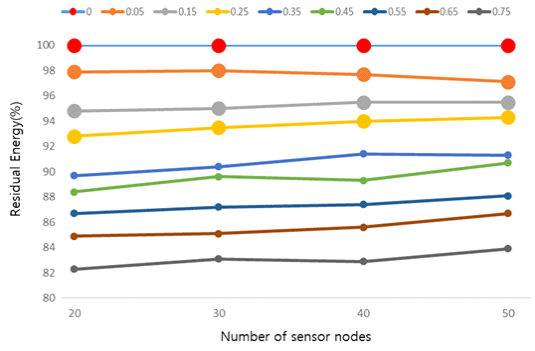

Fig. 11. Residual energy comparison of on the proposed model by the number of sensor nodes

V. 결 론

본 논문에서는 기계학습을 통해 탐지 요소를 도출하고 S-MAC 대상 sleep deprivation attack의 특성을 이용해 공격을 탐지하는 모델을 제안하였다. 기계학습을 통해 탐지 요소를 도출하고 공격의 특성을 이용함으로써 추가 정보를 얻기 위한 가정과 복잡한 연산 없이도 sleep deprivation attack 탐지 시에 높은 성능을 나타내는 것을 확인하였다. 본 논문에서 제안한 sleep deprivation attack 탐지 모델은 공격 센서 노드의 비율을 0.35 이상으로 하여 ASDA-RSA와 비교하였을 때, 정확도는 크게 떨어지지 않으면서도 탐지 연산량이 적어 에너지 효율이 높으므로 센서 네트워크에 적합하다.

본 논문에서 제안하는 탐지 모델의 한계점은 탐지 방안이 S-MAC 대상의 sleep deprivation attack에 특화되어 다른 MAC 프로토콜 대상의 sleep deprivation attack은 탐지가 어렵다는 것이다.

본 논문에서 제안하는 모델의 한계점은 다양한 MAC 프로토콜 대상의 sleep deprivation attack 탐지에 공통적으로 영향을 미치는 탐지 파라미터를 추가함으로써 개선할 수 있을 것으로 예상된다.

References

[1] F. Stajano, "Security for Ubiquitous Computing," International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg, pp. 2-2, Dec. 2004.

[2] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks," International workshop on security protocols, pp. 172-194, Apr. 1999.

[3] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 2, pp. 74-81, 2008.

[4] M. Rirretti, S.Zhu, N. Vijaykrishnan, P. Mcdaniel and M. Kandemir, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," International Journal of Distributed Sensor Networks. vol. 2, no. 3, pp. 267 - 87, Jul. 2006.

[5] Seong-hwan Jeong, Woo-jin. Jang and Chang-hun Lee, "Modeling and Performance Analysis of S-MAC Protocol in Tandem Sensor Networks," Korean Institute Of Industrial Engineers, pp. 436-442, May. 2007.

[6] D.R Raymond, R.C. Marchany, M.I. Brownfield and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Transactions on vehicular technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[7] T. Bhattasali, R. Chaki and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network," arXiv preprint arXiv:1203.0231, 2012.

[8] A. Gallais, T.H. Hedli, V. Loscri and N. Mitton, "Denial-of-Sleep Attacks against IoT Networks," 2019 6th International Conference on Control, Decision and Information Technologies(CoDIT). IEEE, pp. 1025-1030, Apr. 2019.

[9] Jae-hong Park, Kyeung-seek Lew and Yong-deak Kim, "Energy Efficient MAC Protocols based on S-MAC for Wireless Sensor Networks," Journal of the Institute of Electronics Engineers of Korea CI, 44 (2), pp. 19-24, Mar. 2007.

[10] Chan-young Yun, "Energy efficient S-MAC Protocol in Wireless Sensor Network." The Journal of Korean Institute of Communications and Information Sciences, 33(2), pp. 20-26, Feb. 2008.

[11] S. Naik and N. Shekokar, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," Procedia Computer Science 45. pp. 370-379, Mar. 2015.

[12] C. T. Hsueh, C. Y. Wen and Y. C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," IEEE Sensors Journal, vol. 15, no. 6, pp. 3590-3602, 2015.

[13] W. Ye, J. Heidemann and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1567-1576, 2002.

[14] J. Granjal, E. Monteiro and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015.

[15] G. Mahalakshmi and P. Subathra, "A Survey on Prevention Approaches for Denial of Sleep Attacks in Wireless Networks," Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 1, pp. 106-110, 2014.

[16] E. Gelenbe and Y. M. Kadioglu, "Energy Life-Time of Wireless Nodes with Network Attack and Mitigation," 2018 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, pp. 1-6, 2018.

[17] M. Brownfield, Y. Gupta and N. Davis, "Wireless Sensor Network Denial of Sleep Attack," Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop. IEEE, pp. 356-364, Jun. 2005.

[18] D. R. Raymond and S. F. Midkiff, "Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks," MILCOM 2007-IEEE military communications conference. IEEE, pp. 1-7, Oct. 2007.

[19] C. Chen, L. Hui, Q. Pei, L. Ning and P. Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," 2009 Fifth International Conference on Information Assurance and Security. Vol. 2. IEEE, vol. 2, pp. 446-449, 2009.

[20] S. Bandyopadhyay and E. J. Coyle, "An Energy-Efficient Hierarchical Clusterin

g Algorithm for Wireless Sensor Networks," IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), vol. 3, pp. 1713-1723, 2003.

[21] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Micro-sensor Networks," Proceedings of the 33rd Hawaii international conference on system sciences, vol. 8, pp. 3005-3014, Jan. 2000.

[22] D. E. Boubiche and A. Bilami, "A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks," Journal Of Emerging Technologies In Web Intelligence, vol. 5, no. 1, Feb. 2013.

[23] R.Fotohi, S.F. Bari and M. Yusefi, "Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol," International Journal of Communication Systems. vol 33, no. 4, 2020.

[24] C. T. Hsueh, C. Y. Wen and Y. C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," IEEE Sensors journal, vol. 15, no. 6, pp. 3590-3602, 2015.

[25] M. Gunasekaran and S. Periakaruppan, "GA DoSLD: genetic algorithm based denial of sleep attack detection in WSN," Security and Communication Networks, 2017.

[26] D. G. Zhang, S. Zhou and T.M. Tang, "A low duty cycle efficient MAC protocol based on self adaption and predictive strategy," Mobile Networks and Applications. vol. 23, no. 4, pp. 828-839, 2018.

[27] D. G. Zhang, H. L. Niu and S. Liu, "Novel PEECR based clustering routing approach," Soft Computing, vol 21, no. 24, pp. 7313-7323, 2017.

[28] D. G. Zhang, C. Chen, Y.Y. Cui and T. Zhang, "New method of energy efficient subcarrier allocation based on evolutionary game theory," Mobile Networks and Applications, pp. 1-14, 2018.

[29] T. V. Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," Proceedings of the 1st international conference on Embedded networked sensor systems, pp. 171-180, Nov. 2003.

[30] W. Ye, J. Heidemann and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1567-1576, Jun. 2002.

[31] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 95 - 107, Nov. 2004.

[32] F. Adebayo, "Detecting Denial of Service attack in Wireless Sensor Networks," PhD Thesis, 2014.

[33] D. Popescu, C. Dragana, F. stoican, L. Ichim and G. Stamatescu, "A Collaborative UAV-WSN Network for Monitoring Large Areas," Sensors, vol. 18. no. 12, 2018.

〈저자소개〉

김 숙 영 (Sukyoung Kim) 정회원
2018년 2월: 상명대학교 컴퓨터과학과 학사
2019년 3월: 고려대학교 정보보호학과 석사 과정
〈관심분야〉 정보보호, 사물인터넷 보안

문 종 섭 (Jongsub Moon) 종신회원
1981년 2월: 서울대학교 계산통계학과 학사
1983년 2월: 서울대학교 계산통계학과 석사
1991년 2월: Illinois Institute of Technology 전산학과 박사
1993년 3월~현재: 고려대학교 전자 및 정보공학부 교수
2001년 2월~현재: 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 정보보호, 운영체제, 침입탐지