디지털산업정보학회 논문지 제13권 제1호-2017년 3월
http://dx.doi.org/10.17662/ksdim.2017.13.1.049

사물인터넷 환경에서 안전성과 신뢰성 향상을 위한 Dual-IDS 기법에 관한 연구

양 환 석*

A Study on Dual-IDS Technique for Improving Safety and Reliability in Internet of Things

Yang Hwanseok

〈Abstract〉

IoT can be connected through a single network not only objects which can be connected to existing internet but also objects which has communication capability. This IoT environment will be a huge change to the existing communication paradigm. However, the big security problem must be solved in order to develop further IoT. Security mechanisms reflecting these characteristics should be applied because devices participating in the IoT have low processing ability and low power. In addition, devices which perform abnormal behaviors between objects should be also detected. Therefore, in this paper, we proposed D-IDS technique for efficient detection of malicious attack nodes between devices participating in the IoT. The proposed technique performs the central detection and distribution detection to improve the performance of attack detection. The central detection monitors the entire network traffic at the boundary router using SVM technique and detects abnormal behavior. And the distribution detection combines RSSI value and reliability of node and detects Sybil attack node. The performance of attack detection against malicious nodes is improved through the attack detection process. The superiority of the proposed technique can be verified by experiments.

Key Words : Internet of Things, Intrusion Detection, Support Vector Machine, Sybil Attack

Ⅰ. 서론

사물인터넷(IoT, Internet of Things)은 통신이 가능한 모듈을 탑재한 사물이 네트워크로 연결되어 사람과 사물, 사물과 사물간의 정보 교환 및 상호 통신이 되는 것을 의미하며, 현재 우리 생활을 빠르게 변화시키고 있는 주요 이슈중의 하나이다[1-3]. 사물인터넷에 참여하는 디바이스들은 유무선 네트워크를 통해서 다양한 정보를 제공할 수 있으며, 원격의 디바이스에서 생성되는 데이터들에 대한 저장 및 관리를 할 수도 있다. 이러한 통신 기술은 다양한 서비스를 제공할 수 있는 기반이 되었지만 이를 통한 다양한 보안의 취약성 역시 증가하였다[4]. 특히 사물인

* 중부대학교 정보보호학과 조교수

터넷에 참여하는 디바이스들은 저용량과 처리 능력이 떨어지기 때문에 기존의 보안 기법들이 그대로 적용될 수 없는 실정이다. 따라서 인가되지 않은 디바이스들에 의한 잘못된 정보 또는 도청에 의한 공격에 쉽게 노출되어 있다. 또한 Sybil, Wormhole 같은 공격으로 인하여 데이터 기밀성과 무결성에 대한 침해 발생이 빈번히 발생하고 있는 실정이다[5,6]. 따라서 IoT 환경에서 디바이스간의 안전한 데이터 전송을 위해서는 악의적인 노드들에 의한 공격에 대한 효율적인 탐지 기법에 대한 연구가 반드시 필요하다.

본 논문에서는 사물인터넷 환경에서 악의적인 노드들에 의한 공격 탐지의 성능을 향상시키기 위하여 D-IDS 기법을 제안하였다. 제안한 D-IDS 기법은 저전력과 제한된 대역폭을 고려하여 중앙 탐지와 분산 탐지로 나누어 수행한다. 중앙 탐지는 외부 네트워크와 내부 네트워크를 연결하는 경계 라우터에서 네트워크 전체 트래픽에 대해 SVM(Support Vector Machine)을 적용하여 비정상 행위 공격을 탐지하게 된다. 분산 탐지 기법은 사물인터넷을 구성하는 모든 노드에서 RSSI값과 신뢰도 조합으로 Sybil 공격을 탐지하게 된다. 그리고 분산 탐지를 위해 IoT에 참여하는 노드들에게 중앙 탐지 노드는 아이디 키를 발급해주는 역할을 수행한다. 본 논문에서 제안한 D-IDS의 성능은 실험을 통하여 성능을 확인할 수 있었다.

본 논문의 구성은 다음과 같다. 2장에서는 사물인터넷에 존재하는 보안 위협과 침입탐지 기법 대하여 살펴보고 3장에서는 본 논문에서 제안한 D-IDS 기법에 대하여 설명하였다. 4장에서는 실험을 통해 제안한 기법의 성능을 확인하고 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 사물인터넷에서의 보안위협

사물인터넷은 다양한 기기들이 유·무선 네트워크를 이용하여 많은 서비스들을 이용하는 복잡한 특성을 갖는다. 이러한 특성 때문에 사물인터넷을 구성하는 각 요소들에 보안 취약성이 존재하기 때문에 다양한 보안 위협들이 존재한다. 사물인터넷 환경에서 발생할 수 있는 보안 위협들은 기존의 네트워크 환경에서 나타날 수 있는 위협들이 그대로 상속되고 대표적인 기밀성, 무결성, 가용성을 침해하는 위협들이 나타난다[7]. 사물인터넷 각 구성요소에서 발생할 수 있는 보안 위협들의 종류를 살펴보면 <표 1>과 같다[8].

<표 1> 사물인터넷 구성요소별 보안 위협

구성요소	보안 위협
단말	단말 분실 및 도난, 파괴
네트워크	데이터 위변조, 정보유출, 신호교란, 서비스 거부
애플리케이션	데이터 위변조, 정보유출, 서비스거부

사물인터넷 디바이스는 유·무선 네트워크를 통해 다른 사용자들과 정보를 주고받기 때문에 비인가된 접근, 복제공격, 보호되지 않은 펌웨어 등의 공격 위협이 존재하고 있다. 또한 디바이스에 대한 보안체계가 마련되어 있지 않고 패스워드 길이 역시 제한되어 있는 경우가 대부분이기 때문에 무작위 공격도 가능하다. 디바이스간 통신 주파수에 노이즈를 발생시키거나 주파수를 위변조하여 정상 신호를 방해하는 공격부터 공유된 네트워크 키를 취득하여 허가되지 않은 위조 디바이스를 네트워크 접속시켜 악의적인 행위를 하도록 조종하는 스푸핑까지 수많은 공격들이 존재한다[9].

2.2 사물인터넷 기반 침입탐지

사물인터넷 환경에서 악의적인 공격 탐지를 위한 침입탐지 기법에 대해 다양한 연구가 진행되어왔다. SAM (Statistical Analysis based appoach) 기법은 웜홀 링크의 탐지를 위하여 다양한 경로의 프로토콜에서 특정 목적지에 대해 되돌아오는 연결 발생을 모니터링하는 방법을 이용하였다[10]. DCL(Distance Calculate based Location) 기법은 하나의 노드에서 수신된 패킷들의 RSS(Received Signal Strength)를 기초로 송신 노드까지의 거리를 측정한다. 그리고 이를 이용하여 패킷에 있는 위치 정보로부터 계산된 거리와 비교를 하여 공격 노드를 탐지하였다[11-13]. E2SIW는 웜홀 공격을 방지하기 위하여 GPS로부터 수신한 위치 정보를 이용하였다. 이 기법은 웜홀 노드의 탐지나 대응 방법은 제공하지 않았다[14,15]. 사물인터넷을 위해 설계된 기존의 침입탐지시스템을 <표 2>에서 보여주고 있다.

<표 2> 사물인터넷 기반 침입탐지시스템 특징

종류	특징
SVELTE	호스트 기반의 침입탐지시스템으로 6BR 시스템에 네트워크 토폴로지를 구성
RIDES	서명 기반 침입탐지시스템으로 서명 매칭을 위해 bloom filter를 사용
Kasinathan[13]	네트워크 기반 침입탐지시스템으로 DoS 탐지를 위해 개발
Le[14]	유한 상태 기반 침입탐지 시스템
Jun[15]	복잡한 사건 처리 침입탐지시스템으로 EPL과 SQL을 사용하여 공격 패턴을 정의

Ⅲ. Dual-IDS 기법

본 장에서는 사물인터넷 환경에서 악의적인 노드들에 대한 공격 탐지 성능을 향상시키기 위하여 본 논문에서 제안한 Dual-IDS (Dual-Intrusion Detection System) 기법에 대하여 설명하였다.

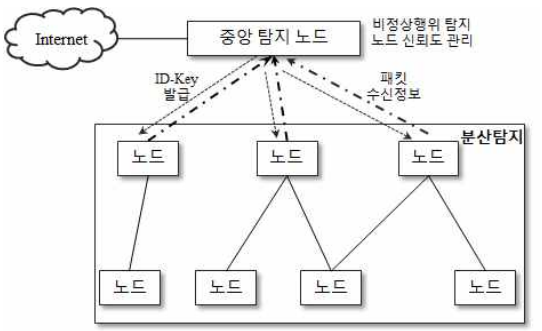
3.1 시스템 구조

모든 것이 인터넷으로 연결되어 정보가 생성, 수집, 활용되는 초연결 네트워크인 사물인터넷은 Open API 기반의 사물인터넷 서비스를 제공하는 서비스/플랫폼, 저전력 통신망과 멀티홉 라우팅을 이용한 네트워크, 대부분 오픈 소스에 IP가 내장되어 있는 서비스 지향적인 디바이스로 구분된다. 이러한 사물인터넷 환경에서 보안 위협을 차단하기 위한 기술로 사물인터넷 침해 사고를 탐지하고 대응하는 것이 매우 중요한 부분을 차지하고 있다. 특히 사물인터넷에 참여하는 노드들은 저전력과 제한된 대역폭을 사용하기 때문에 기존의 침입탐지 기법을 그대로 적용할 수 없는 한계를 가지고 있다.

Dual-IDS 기법은 사물인터넷 환경의 특징인 저전력과 제한된 대역폭의 특징을 고려하면서 공격 탐지의 성능을 높이기 위해서 네트워크 전체 트래픽을 검사하는 중앙 탐지와 사물인터넷에 참여하는 모든 센서 노드에서 공격을 탐지하는 분산 탐지, 즉 이중 침입탐지를 수행하게 된다. 먼저 중앙 탐지 기법은 외부 네트워크와 내부 네트워크를 연결하는 경계 라우터, 즉 중앙 탐지 노드에서 이루어지며 네트워크 전체 트래픽을 검사한 후 SVM(Support Vector Machine) 기법을 이용하여 비정상 행위 공격을 탐지하게 된다. 그리고 중앙 탐지 노드에서는 분산 탐지를 위해 사물인터넷에 참여하는 노드들에게 아이디 키를 발급해주는 역할을 수행한다. 분산 탐지 기법은 네트워크를 구성하는 모든 센서 노드에서 RSSI 값과 아이디 키를 이용한 신뢰도의 조합으로 공격을 탐지하게 된다. 고정된 범위 내에 모든 센서 노드들

로부터 수신되는 신호 강도만으로 공격 탐지시 오탐률이 높아진다. 따라서 본 논문에서는 공격 탐지율을 높이기 위해 모든 노드에서 자신의 이웃 노드들에 대해 측정한 신뢰도를 공격 탐지에 이용하였다. 또한 제한된 대역폭의 사용과 저전력을 고려하여 각 노드들에 대한 신뢰도 계산 및 정보 저장은 중앙 탐지 노드에서 관리하도록 하였다. 이렇게 본 논문에서 제안한 시스템은 REST(Representational State Transfer) 전송 방식과 인터넷에서 센서 노드와 같이 제한된 컴퓨팅 성능을 갖는 디바이스들의 통신을 실현하기 위해 개발된 CoAP(Constrained Environments Application Protocol)가 적용되는 네트워크 환경에서 보안성을 높일 수 있다.

<그림 1>는 본 논문에서 제안한 Dual-IDS의 시스템 구조를 보여주고 있다.



<그림 1> Dual-IDS 구조

3.2 SVM을 이용한 중앙 탐지 기법

사물인터넷 환경은 무선 네트워크의 제한된 대역폭과 저전력의 특성을 가지고 있기 때문에 기존의 침입 탐지 기법들을 그대로 적용할 수 없고 경량화된 알고리즘 적용이 필수적이다. 이러한 환경을 고려하여 본 논문에서는 사물인터넷에 참여하는 노드들에 대한 비정상 행위를 탐지하기 위하여 네트워크 경계 라우터에서 SVM을 이용한 중앙 탐지가 이루어지는 기법을 제안하였다. 중앙 탐지를 수행하는 중앙 탐지 노드는 크게 두 가지의 역할을 수행한다. 첫 번째는 네트워크 전체 트래픽 검사를 통해 SVM 기법을 적용하여 비정상행위 노드를 탐지하는 역할을 한다. 두 번째는 분산 탐지를 위해 네트워크에 참여하는 노드들에게 아이디 키를 발급 및 관리를 수행하고 모든 노드들에 대한 신뢰값을 관리 및 배포하는 역할을 담당한다.

네트워크 트래픽을 검사하여 비정상행위를 탐지하기 위해 적용한 SVM의 원리는 다음과 같다. 먼저 네트워크 전체 트래픽을 모니터링을 통해 특징을 추출한 후 학습 단계를 거친다. 수집한 트래픽의 이진 분류를 위한 초평면은 식 (1)과 같이 표현할 수 있다.

$$d(x) = w^T x + b = 0 \quad (1)$$

여기서 x는 학습 데이터를 나타내는 특징 벡터이고, $x = (x_1, \cdots, x_d)^T$로 나타낼 수 있다. $d(x)$는 전체 특징 공간을 두 영역으로 분할하며, w는 초평면의 법선 벡터이고 b는 위치를 나타내는 매개변수이다. 그리고 학습 데이터는 초평면을 기준으로 이 분법으로 분리한 후 가장 거리가 먼 초평면을 찾는 과정을 거치게 된다. 임의의 점 x와 초평면까지의 거리는 식 (2)에 의해 계산된다.

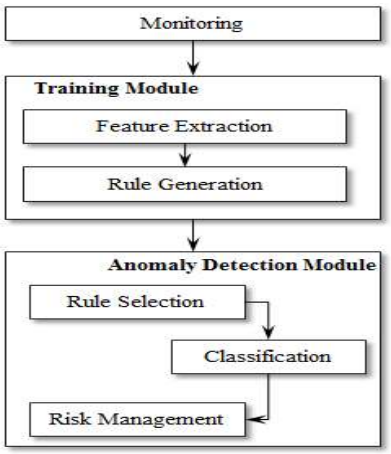
$$h = \frac{|d(x)|}{\| w \|} \quad (2)$$

식 (2)에 의해 얻어진 거리들 중에서 직선과 가장 가까운 특징들을 서포트 벡터라고 하며, 이는 여백의 크기를 좌우하는 중요한 요소이다. 이렇게 분류된 값에 의해 비정상행위를 탐지할 수 있지만 그 성능은 다소 떨어질 수 있다. 따라서 이러한 특징 값들이 있는 공간을 더 높은 공간으로 새롭게 매핑을 하면 선형 분류가 어려운 특징들도 분류가 가능하여 공격 탐지 성능을 향상시킬 수 있다. 이를 위하여 두

개의 매개변수 벡터 x와 y를 갖는 커널함수 $K(x, y)$를 적용하였으며, 식 (3)의 커널 함수를 적용하였다.

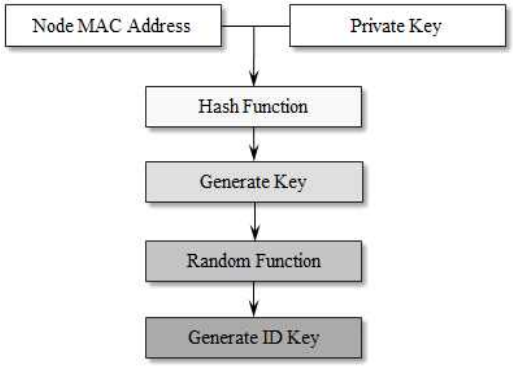
$$K(x, y) = (x \cdot y + 1)^p \quad (3)$$

<그림 2>는 중앙 탐지가 이루어지는 과정을 보여주고 있다.



<그림 2> 중앙 탐지 흐름도

중앙 탐지 노드에서는 노드들의 계산량을 줄여 전력 소모량을 줄이기 위하여 모든 노드에서 분산 탐지를 위해 사용되는 아이디 키를 발급하며, 이를 관리하게 된다. 노드들에게 발급되는 아이디 키는 보안 성능을 향상시키기 위하여 모든 노드들의 MAC 주소값과 사용자 비밀키를 입력 값으로 하여 해시함수를 통해서 키 값을 생성한 후, 랜덤 함수를 이용하여 6자리의 키를 생성하게 된다. 발급된 아이디 키는 NIKMT(Node Id Key Management Table)에 저장 및 관리 된다. <그림 3>은 아이디 키 발급 흐름도를 보여주고 있다.



<그림 3> 아이디 키 발급 과정

3.3 분산 탐지 기법

사물인터넷 환경에서는 중앙에서 감시를 할 수 있는 구조가 아니기 때문에 Sybil 공격과 같이 거짓 노드에 의한 잘 못된 정보에 의한 공격의 피해는 매우 크다. 따라서 본 논문에서는 이러한 잘못된 거짓 정보에 의한 공격을 탐지하기 위하여 아이디 키를 기반으로 한 신뢰도와 RSSI를 조합한 공격 탐지 기법을 제안하였다. 물론 이 기법은 네트워크에 참여하는 노드들의 저전력 특성을 고려하였다.

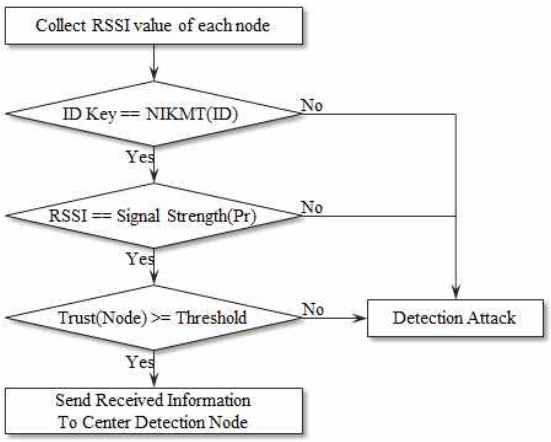
분산 탐지를 위해 사용되는 RSSI 값과 신뢰도 측정 과정은 다음과 같다. 첫째로 네트워크 초기에 two ray propagation model로 식 (4)을 이용하여 고정된 신호 값을 계산한다.

$$P_r = \frac{(P_t \times G_t \times G_r \times H_t^2 \times H_r^2)}{(d^4 \times L)} \quad (4)$$

단, 고정된 전송 범위내의 모든 노드들은 똑같은 송·수신 신호 강도를 갖는다는 것을 가정한다.

둘째로 신뢰도 측정은 다음과 같다. 사물인터넷에 참여하는 모든 노드들은 앞 절에서 설명한 과정을 통해서 중앙 탐지 노드로부터 아이디 키를 발급받는다. 모든 노드들은 데이터 전송시 아이디 키를 함께 전송한다. 이렇게 함으로써 아이디 키를 발급받지

않은 노드는 데이터 전송을 불가하게 함으로써 거짓 노드의 참여를 배제시켰다. 그리고 데이터를 수신한 노드는 중앙 탐지 노드에게 자신이 전송받은 패킷의 정보, 즉 어느 노드로부터 얼마의 데이터를 수신했는지 해당 정보를 전송하게 된다. 중앙 탐지 노드에서는 신뢰도 테이블에 노드들의 패킷 전송 정보를 계산 및 저장한 후 주기적으로 방송하게 된다. 모든 노드에서는 데이터를 수신할 때 RSSI값을 검사하고 노드의 신뢰도를 비교하여 공격을 탐지하게 된다. 분산 탐지 과정은 <그림 4>와 같은 과정을 통해 이루어진다.



<그림 4> 분산 탐지 과정

Ⅳ. 모의실험 및 결과

4.1 실험 환경

본 논문에서 제안한 Dual-IDS 기법의 성능을 Contiki's 네트워크 시뮬레이터를 이용하여 다음과 같은 모의실험 환경에서 실험하였다. 전체 모의실험 시간은 300초로 하였다. 실험 시간동안에 20번의 Sybil 공격을 발생시켰다. <표 3>에서는 모의실험을 위한 환경변수 값들을 보여주고 있다.

<표 3> 실험에 사용한 환경 변수

Parameter	Value
Number of Nodes	30, 60
Routing Protocol	RPL
MAC Protocol	802.15.4
Radio Interface	cc2420

4.2 실험 결과

본 논문에서는 제안한 기법의 성능을 측정하기 위하여 DLC기법과 비교 실험을 하였으며, 성능 평가 기준은 침입탐지에서 가장 중요한 요소인 True Positive Rate(TPR)와 False Positive Rate(FPR), 그리고 공격 탐지시 패킷 오버헤드로 하였다. 먼저 TPR과 FPR은 다음 식 (5)와 식 (6)으로 계산된다.

$$TPR = \frac{TP(True\ \ Positive)}{TP + FN(False\ \ Negative)} \quad (5)$$

$$FPR = \frac{FP(False\ \ Positive)}{FP + TN(True\ \ Negative)} \quad (6)$$

<표 4>와 <표 5>는 노드 30, 60개가 있는 상황에서 TPR과 FPR 측정 결과를 보여주고 있다. 이것은 침입탐지시스템의 가장 중요한 공격 탐지 성능을 측정하기 위한 실험이다. 실험 결과에서 확인할 수 있듯이 제안한 기법이 DLC 기법보다 우수한 성능을 보였으며, 노드의 수에 큰 영향을 받지 않았음을 확인할 수 있었다. 이는 분산 탐지와 중앙 탐지가 제대로 이루어지고 있다는 것을 의미하게 된다. 즉, 노드

들이 이동으로 인한 신호 강도가 정확하게 계산되지 않더라도 신뢰도 값을 이용하기 때문에 공격 탐지율이 높게 나타났다. 이에 비해 DLC 기법은 노드로부터 수신한 위치 정보와 수신 강도를 이용하기 때문에 노드의 이동이 높을수록 오탐율이 증가하는 결과를 보여주며, 수신 강도와 거리 정보만을 이용하기 때문에 탐지율이 낮아지는 결과를 보여주었다.

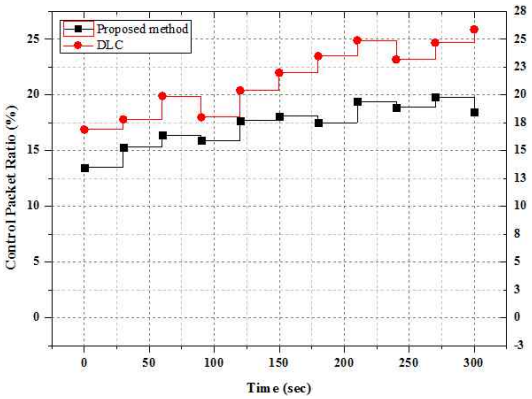
<표 4> 제안한 방법의 TPR과 FPR

공격	TPR(%)		FPR(%)	
	30 nodes	60 nodes	30 Nodes	60 nodes
Sybil	0.96	0.95	0.04	0.041
Wormhole	0.94	0.94	0.052	0.062

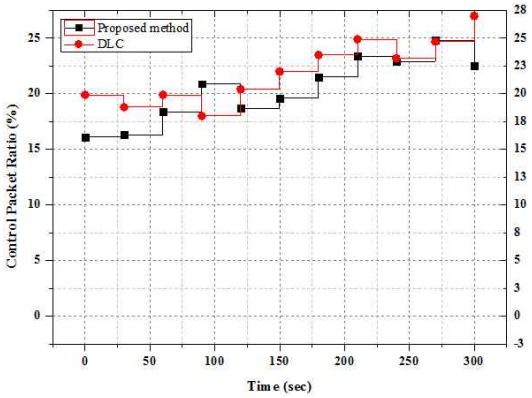
<표 5> DLC의 TPR과 FPR

공격	TPR(%)		FPR(%)	
	30 nodes	60 nodes	30 Nodes	60 nodes
Sybil	0.93	0.92	0.064	0.06
Wormhole	0.94	0.924	0.071	0.08

<그림 5>에서는 공격 탐지 동안의 패킷 오버헤드를 측정한 결과를 보여주고 있다. 사물인터넷은 제한된 대역폭을 이용하기 때문에 패킷의 오버헤드가 성능을 좌우할 수 있다. 그림에서 확인할 수 있듯이 노드 수가 증가할 수 록 패킷의 오버헤드는 높아졌으며, 제안한 기법이 DLC 기법보다 다소 좋은 결과를 보여주고 있다. 제안한 기법에서 패킷 오버헤드는 분산 탐지를 위해 노드들이 중앙 탐지 노드에 전송하는 패킷 수신 정보 때문에 증가하는 결과를 보였다. DLC 기법은 하나의 노드에서 수신한 패킷들에 대한 수신 강도와 위치 정보를 모두 계산해야 되고, 해당 정보를 전송해야하기 때문에 패킷 오버헤드가 높은 결과를 보였다.



(a) 노드 수 30개



(b) 노드 수 60개

<그림 5> 노드 수에 따른 패킷 오버헤드 비율

V. 결론

사물인터넷은 다양한 분야에서 그 활용도가 나날이 증가하고 있으며, 사물들에 종류 역시 다양해지고 있는 실정이다. 이러한 사물인터넷에서 보안은 더욱 중요한 분야 중에 하나이다. 왜냐하면 사물인터넷에 참여하는 디바이스들의 저성능, 저전력의 특성과 디바이스를 활용한 다양한 서비스에 많은 취약점이 존재하기 때문이다. 따라서 본 논문에서는 사물인터넷 환경에서 악의적인 노드들에 의한 공격의

탐지 성능을 향상시키기 위하여 D-IDS 기법을 제안하였다. 제안한 기법은 저전력과 제한된 대역폭을 고려하여 중앙 탐지와 분산 탐지 기법을 적용하였다. 중앙 탐지에서는 노드들의 전력 소모를 고려하여 경계 라우터에서 수행하며 SVM을 이용하여 비정상행위 노드를 탐지한다. 그리고 분산 탐지를 위해 각 노드에게 아이디 키 발급 및 신뢰도 관리를 수행하게 된다. 분산 탐지는 사물인터넷에 참여하는 모든 노드에서 수행되며, RSSI값과 신뢰도의 조합으로 이루어지게 된다. 분산 탐지에서는 Sybil 공격과 같이 악의적인 노드들에 의한 잘못된 정보를 송신하는 노드를 탐지하게 된다. 또한 네트워크 참여하는 모든 노드들은 중앙 탐지 노드로부터 아이디 키를 발급받아야 하기 때문에 인증을 받지 못한 노드는 데이터 전송에 참여할 수 없게 된다. 이러한 과정으로 악의적인 노드들에 대한 네트워크 참여를 배제시키고 공격 탐지가 이루어져 탐지 성능이 향상되었다. 제안한 D-IDS 기법의 성능을 측정하기 위하여 DLC 기법과 비교 실험하였으며, 실험을 통해 침입 탐지의 우수한 성능을 확인하였다.

참고문헌

[1] Shancang Li, Li Da Xu, Shanshan Zhao, “The internet of things: a survey,” Springer Information Systems Frontiers, Volume 17, Issue 2, 2015, pp. 243-259.

[2] M. Hossain, M. Fotouhi and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” 2015 IEEE World Congress on Services, 2015.

[3] Okan CAN, Ozgur Koray SAHINGOZ, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks,” 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015.

[4] Kasinathan, Prabhakaran, et al. “Denial-of-Service detection in 6LoWPAN based internet of things.” Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on. IEEE, 2013.

[5] 최희식, 조양현, “사물인터넷 보안 문제제기와 대안,” 디지털산업정보학회지, 제11권, 제1호, 2015, pp. 69-78.

[6] Chen Jun, Chen Chi, “Design of Complex Event-Processing IDS in Internet of Things,” Sixth International Conference on Measuring Technology and Mechatronics Automation, IEEE DOI: 10.1109/ICMTMA.2014.57, 2014.

[7] A. Anand, B. Patel, “An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols,” International Journal of Advanced Re-search in Computer Science and Software Engineering, vol. 2, no. 8, 2012.

[8] M. Hossain, V. Raghunathan, Aegis, “A lightweight rewall for wireless sensor networks,” Distributed Computing in Sensor Systems, 2010, pp. 258-272.

[9] M. Livani, M. Abadi, “A pca-based distributed approach for intrusion detection in wireless sensor networks,” in: International Symposium on Computer Networks and Distributed Systems (CNDS), IEEE, 2011, pp. 55-60.

[10] Raza, Shahid, Linus Wallgren, and Thiemo

Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” Ad hoc networks Vol. 11, No. 8, 2013, pp. 2661-2674.

[11] Q. M. Ashraf and M. H. Habaebi, “Autonomic schemes for threat mitigation in Internet of Things,” Journal of Network and Computer Applications, Vol. 49, 2015, pp. 112-127.

[12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, Vol. 29, No. 7, 2013, pp. 1645-1660.

[13] Kashinahan, Prabhakaran, et al., “Denail-of-Service detection in 6LoWPAN based internet of things,” Wireless and Mobile Computing, Networking and Communications (WiMob), 2013.

[14] Le, Anhtuan, et al., “Specification-based IDS for securing RPL from topology attacks,” Wirelees Days (WD), 2011 IFIP. IEEE, 2011.

[15] Jun, Chen, and Chen Chi., “Design of Complex Event Processing IDS in Internet of Things,” Measuring Technology and Mechanronics Automation (ICMYMA), 2014 Sixth International Conference on. IEEE, 2014.

■ 저자소개 ■

양 환 석
(Yang Hwanseok)

2011년 9월~현재
중부대학교 정보보호학과 조교수
2006년 2월~2011년 2월
호원대학교 사이버수사경찰학과
연구교수
2005년 2월 조선대학교 전산통계학과(이학박사)
1998년 2월 조선대학교 전산통계학과(이학석사)

관심분야 : 정보보호, 침입탐지시스템, MANET
E-mail : yanghs@joongbu.ac.kr

논문접수일 : 2017년 01월 24일
수 정 일 : 2017년 02월 17일
게재확정일 : 2017년 02월 27일