Journal of the Korea Convergence Society
Vol. 8. No. 8, pp. 51-57, 2017
https://doi.org/10.15207/JKCS.2017.8.8.051

무선 센서 네트워크에서 소프트웨어 정의 네트워킹 기법을 사용한 침입 탐지 기법에 대한 연구

강용혁[1], 김문정[2*], 한문석[3]
[1]극동대학교 글로벌경영학과 [2]U1대학교 스마트IT학과 [3]강릉원주대학교 소프트웨어학과

A Study of Intrusion Detection Scheme based on Software-Defined Networking in Wireless Sensor Networks

Yong-Hyeog Kang[1], Moon Jeong Kim[2*], Moonseog Han[3]
[1]Department of Global Business Administration, Far East University
[2]Department of Smart IT, U1 University
[3]Department of Software, Gangneung-Wonju National University

요 약 무선 센서 네트워크는 자원 제약적인 센서 노드들로 구성되는 네트워크로, 분산 서비스 거부 공격, 라우팅 공격 등 다양한 악의적인 공격이 발생될 수 있다. 본 논문에서는 소프트웨어 정의 네트워킹 기술과 보안 기술을 융합하여 무선 센서 네트워크에 발생하는 다양한 공격을 탐지하고 방어하는 기법을 제안한다. 제안 기법에서는 서버에 있는 침입 탐지 및 방지 시스템이 SDN 컨트롤러를 통해 전달되는 오픈플로우 스위치의 로그 정보들을 축적하여 침입을 탐지하며, 침입을 탐지했을 때 오픈플로우 프로토콜을 이용하여 오픈플로우 스위치에 해당 침입에 대한 대응방안을 설정함으로써 침입을 방지할 수 있다. 본 논문에서는 분산 서비스 거부 공격 및 라우팅 공격 발생 시 침입 탐지 및 방지를 보임으로써 제안기법의 타당성을 보였다. 제안기법은 다른 기법과 달리 중앙 집중 서버에서 그래프 모델과 침입 탐지 모델을 융합하여 효과적이고 메시지 효율적으로 다양한 침입을 탐지하고 방지할 수 있다.

• 주제어 : 정보기술 융합, 침입 탐지, 소프트웨어 정의 네트워킹, 무선 센서 네트워크, 오픈플로우

Abstract A wireless sensor network is composed of many resource constrained sensor nodes. These networks are attacked by malicious attacks like DDoS and routing attacks. In this paper, we propose the intrusion detection and prevention system using convergence of software-defined networking and security technology in wireless sensor networks. Our proposed scheme detects various intrusions in a central server by accumulating log messages of OpenFlow switch through SDN controller and prevents the intrusions by configuring OpenFlow switch. In order to validate our proposed scheme, we show it can detect and prevent some malicious attacks in wireless sensor networks.

• Key Words : IT Convergence, Intrusion Detection, Software Defined Networking, Wireless Sensor Network, Openflow

*Corresponding Author : 김문정(tops@yd.ac.kr)
Received July 11, 2017 Revised August 9, 2017
Accepted August 20, 2017 Published August 28, 2017

1. 서론

무선 센서 네트워크(Wireless Sensor Network)는 제한된 자원과 전송 범위를 갖는 센서 노드들로 구성되는 네트워크이다[1]. 센서 노드들끼리 통신하기 위해서는 다중 홉 통신을 위한 무선 라우팅 프로토콜이 필요하다[2]. 무선 센서 네트워크가 군, 헬스케어, 농업 분야 및 산업 필드 다양한 분야로 융합되어 민감한 섹터에 사용되면서 보안의 필요성이 더욱 증가되고 있다[3]. 현재 무선 센서 네트워크의 보안을 위해서는 키를 이용한 데이터 무결성, 기밀성 등에 대한 연구가 있으며, 보안 라우팅에 대한 연구가 있으며, 인증을 이용하여 침입을 방지하는 기법들도 제안되고 있다[4, 5]. 그러나, 인증기법을 이용한 기법들은 라우팅을 위해 많은 오버헤드를 발생시킬 수 있으며, 서비스 거부 공격 등의 침입에는 적당한 대응 방안이 없다[6].

소프트웨어 정의 네트워킹(SDN: Software-Defined Networking) 기술은 네트워크 제어 기능과 네트워크 전달 기능을 분리한다. 즉, 새로운 기능, 관리 및 제어를 수행하면서 동시에 프로그래밍 인터페이스를 제공하는 것과 같다. 또한, 이 기술은 네트워크를 하나의 시스템처럼 중앙 집중식으로 관리하고 응용할 수 있게 해준다. 소프트웨어 정의 네트워킹에는 스위치와 컨트롤러와의 통신을 위한 사우스바운드(southbound) 인터페이스와 응용과 컨트롤러와의 통신을 위한 노스바운드(northbound) 인터페이스가 있다[7]. 사우스바운드 인터페이스의 대표적인 구현 사례가 오픈플로우(OpenFlow) 프로토콜이다[8]. 본 논문에서는 소프트웨어 정의 네트워킹 기술을 이용하여 무선 센서 네트워크 환경에서 발생하는 침입을 탐지하고 방지하는 기법을 제안하고자 한다.

2장에서 무선 센서 네트워크에서 발생할 수 있는 침입과 침입탐지 및 방지 기술에 대해 소개한다. 3장에서 소프트웨어 정의 네트워킹의 오픈플로우를 이용하여 침입을 탐지하고 방지하는 기법을 제안하고, 제4장에서는 제안기법의 타당성을 위해 여러 가지 침입 사례에 침입 탐지와 대응 방안을 설명하고, 5장에서 결론 및 기대효과를 설명한다.

2. 관련연구

무선 센서 네트워크에서 발생할 수 있는 침입 유형과 침입탐지 기술에 대해 소개하고자 한다.

2.1 침입 유형

무선 센서 네트워크 환경에서의 공격은 내부 공격과 외부 공격으로 구분할 수 있고, 단순히 데이터를 훔치는 공격과 가짜 데이터를 통해 시스템을 변경하는 공격과 서비스 접근 거부 공격, 에너지 효율성에 영향을 주는 공격으로 구분할 수도 있다.

무선 센서 네트워크에서 다중 홉 라우팅(Multi-hop routing) 프로토콜에 대한 침입 유형은 공격 시간에 따라 경로 검색 과정에 대한 공격 유형, 라우팅 경로를 선택할 때 공격하는 유형, 그리고 라우팅 경로가 설정된 후의 공격 유형으로 분류할 수 있다[9].

경로 검색 과정에 대한 공격 유형에는 가짜 라우팅 정보 공격과 라우팅 경로 찾는 메시지의 전송을 방해하는 러싱(rushing) 공격과 라우팅 경로 찾는 메시지의 플러딩(flooding) 공격 등이 있다. 라우팅 경로를 선택할 때 공격하는 유형으로는 Hello 플러딩 공격, 싱크홀(sinkhole) 공격과 웜홀(wormhole) 공격 등이 있다[10]. Hello 플러딩 공격은 이웃노드들에게 자신을 알리는 Hello 메시지를 더 큰 영역까지 범람시켜 이웃노드들에게 자신이 옆에 있는 것처럼 속이는 공격이다. 싱크홀 공격은 이웃노드들에게 경로를 선택할 때 최적의 경로라고 속이고 공격자를 통과하는 경로를 선택하게 하여 트래픽이 공격자를 경유하도록 하는 공격이다. 웜홀공격은 적은 지연시간을 갖는 두개의 악의적인 노드들이 터널을 만들어서 더 많은 경로가 악의적인 노드들에게 전송되도록 만드는 공격이다.

라우팅 경로가 설정된 후의 공격 유형으로는 모든 메시지를 드롭(drop)하는 블랙홀(blackhole) 공격과 의미 없는 스팸 메시지를 전송하는 스팸(spam) 공격 등이 있다.

2.2 침입 탐지

침입 탐지 시스템은 센서(sensor), 탐지기(detector), 지식베이스(knowledge base), 대응 컴포넌트(response component)의 4가지 구성요소로 이루어진다. 센서는 모니터링 시스템에서 데이터를 수집하고, 탐지기는 수집된 데이터를 분석하여 침입을 탐지한다. 지식베이스는 침입 시그니처를 통해 탐지기를 돕고, 대응컴포넌트는 침입에 대하여 대응하는 액션을 관리한다.

침입 탐지 기법에는 침입을 탐지하는 접근 방식에 따

라 이상 탐지(anomaly detection) 기법과 오용 탐지(abnormal detection) 기법이 있다. 침입 탐지 시스템(IDS: Intrusion Detection System)은 구성하는 방식에 따라 중앙 집중식 침입 탐지 시스템과 분산 침입 탐지 시스템으로 구분할 수 있다[11].

2.3 소프트웨어 정의 네트워킹 기술 적용

무선 센서 네트워크 환경에서 소프트웨어 정의 네트워킹을 이용하는 기법으로, SDN 컨트롤러에서 전체 네트워크에 대한 글로벌 뷰를 유지하여 실시간으로 새로운 응용이나 서비스를 효율적으로 배치하는 기법이 제안되었다[12]. 또 다른 기법에서는 소프트웨어 정의 네트워킹을 이용하여 무선 센서 네트워크의 정책 변경 및 관리의 어려움을 해결하였다[13]. 소프트웨어 정의 네트워킹 기법은 제한된 네트워크 자원을 효과적으로 활용하기 위한 혁신적인 해결책 중의 하나로 평가되고 있다[14].

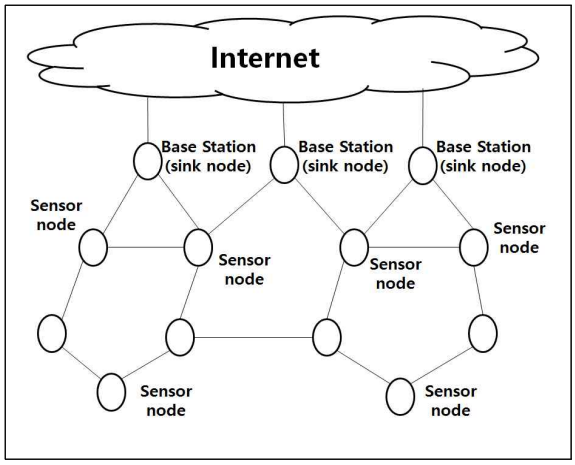
SDN 컨트롤러에 침입탐지 시스템 기능을 포함하는 기법도 제안되고 있다[15]. 침입 탐지를 위해 SDN을 이용하여 로그 파일을 서버에 저장하는 기법이 있지만 무선 네트워크의 제약사항으로 인해 로그 파일을 실시간으로 서버에 저장하는 것은 오버헤드가 많이 발생할 수 있다[16].

3. 제안기법

본 논문에서는 무선 센서 네트워크 환경에서 소프트웨어 정의 네트워킹을 활용하여 전체 네트워크 정보를 유지하여 중앙집중식으로 침입을 탐지하고 방지하는 시스템을 제안한다.

3.1 무선 센서 네트워크 구조

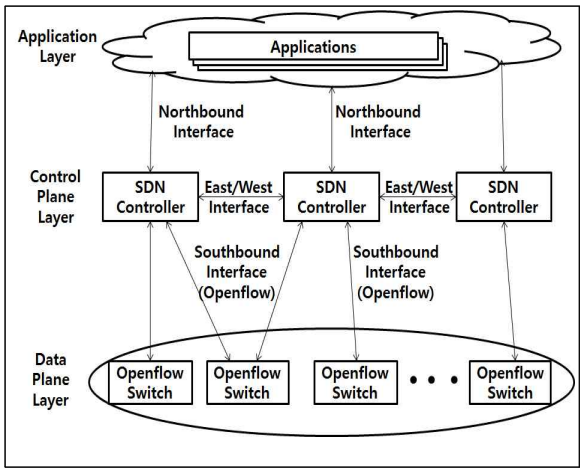
무선 센터 네트워크의 일반적인 구조는 그림 1에서 보이는 바와 같다. 무선 센서 네트워크에서 센서 노드들 간에는 다중 홉 라우팅을 하며 싱크(sink) 노드를 거쳐 인터넷에 연결된다. 본 논문에서 센서 노드들은 오픈플로우 프로토콜을 사용하며, SDN 컨트롤러는 인터넷 내에 분산되어 상호 협력한다. 소프트웨어 정의 네트워킹 구조의 응용 계층에 침임 탐지 및 방지 시스템(IDPS: Intrusion Detection and Prevention System)이 있으며 침입 탐지 및 방지 시스템 내에는 무선 센서 네트워크에 대한 정보도 저장되어 있다고 가정한다.



[Fig. 1] Structure of a Wireless Sensor Network

3.2 소프트웨어 정의 네트워킹 구성도

본 논문에서 사용되는 소프트웨어 정의 네트워킹 구성도는 그림 2에서 보이는 바와 같다.



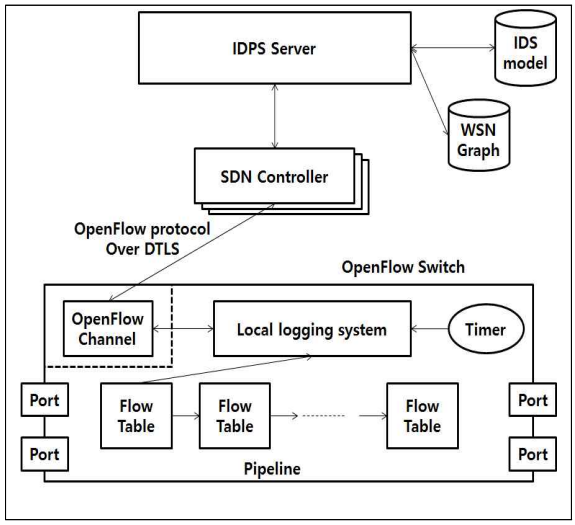
[Fig. 2] Structure of SDN of Our Proposed Scheme

그림 2에서, 칩임 탐지 및 방지 시스템은 응용 계층에 구현된다. 칩임 탐지 및 방지 시스템은 오픈플로우 스위치로부터 전달되어 SDN 컨트롤러를 통과한 로그 메시지를 기반으로 침입을 탐지하고, SDN 컨트롤러를 통해 오픈플로우 스위치를 제어할 수 있다. 분산된 SDN 컨트롤러들은 메시지 교환을 통해 상호 협력하여 동작한다.

3.3 침입 탐지 및 방지 시스템 설계

본 논문에서 제안하는 침입 탐지 및 방지 시스템 설계

는 그림 3에서 보이는 바와 같다.



[Fig. 3] Design of IDPS of Our Proposed Scheme

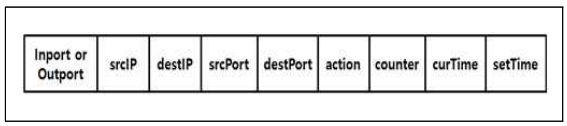
그림 3에서 보이는 바와 같이, 제안기법의 침입 탐지 및 방지 시스템(IDPS) 서버에서는 무선 센서 네트워크에 대한 침입탐지와 관련된 모든 정보를 모아서 관리한다. SDN 컨트롤러는 IDPS 서버에서 오는 요청을 받아서 오픈플로어 스위치를 보안 설정하거나 오픈플로어 스위치의 상태 정보를 받아서 IDPS 서버에게 알려준다. 오픈플로우 스위치는 패킷에 대한 정보를 로그 형태로 저장하고 적당한 시기에 로그 정보들을 SDN 컨트롤러를 통해 IDPS 서버에 전달한다. 오픈플로우 채널은 SDN 컨트롤러와 오픈플로우 스위치와의 통신을 담당하고, 포트는 패킷의 입출력을 담당한다. 플로우 테이블은 매칭필드, 액션, 카운터 등으로 구성된다. 입력포트로 들어온 패킷은 플로우 테이블들의 설정에 따라 처리된다.

제안기법에서, IDPS 서버는 SSL(Secure Socket Layer)로 연결된 모든 SDN 컨트롤러로부터 침입 탐지와 관련된 로그 정보들을 수신하며, 수신된 로그 정보를 이용하여 침입을 탐지한다. 특히, 센서 노드들에 대한 위치 정보와 트래픽 정보 및 네트워크 연결 정보를 저장하고 있는 센서 네트워크에 대한 그래프를 구성하여 침입 탐지에 활용한다[17]. 이 기법은 서버에 패킷 정보에 대한 빅데이터를 구성하고 침입을 분석하는 기법과 유사하다[18]. 침입을 탐지 한 경우, IDPS서버는 공격당한 센서 노드와 연결된 SDN 컨트롤러에게 침입 대응을 위한 정보를 전송한다. 침입 대응 정보를 받은 SDN 컨트롤러는 해당 오픈플로우 스위치의 플로우 테이블을 설정함으로써 침입에 대한 대응을 한다.

3.4 지역 로깅 시스템

기존 유선 네트워크 환경에서는 들어오는 패킷을 복제하여 침입탐지시스템에게 전송하여 침입을 탐지할 수 있지만, 무선 네트워크는 무선 통신의 제약성으로 인해 바로 복제하여 전송하는 것은 어렵다. 들어오는 패킷에 대한 로그 정보를 침입탐지시스템에 곧바로 전송하는 것보다는 지역 로깅 시스템(local logging system)을 이용하여 효율적으로 처리해야 한다. 저장될 로그 정보들은 저장 공간과 전송의 효율성을 위해 축약과정을 거쳐 통합하여 저장된다. 유사한 패킷들이 들어왔을 경우 모든 패킷에 대한 정보를 개별로 저장하는 것보다는 축약하여 저장하는 것이 효율적이다.

본 논문에서 제안하는 기법은 오픈플로우 스위치에서 오는 로그 정보를 이용하여 침입 탐지를 수행하는 것이다. 로그 정보에는 오픈플로우 스위치가 수신하는 패킷에 대한 정보와 오픈플로우 스위치가 수행한 액션정보가 포함된다. 그림 4는 오픈플로우 스위치가 SDN 컨트롤러를 통해 IDPS 서버에 전달하는 로그 메시지에 대한 형식을 보인다.



[Fig. 4] Format of a Log

그림 4에서 보이는 바와 같이, 지역 로깅 시스템에는 침입탐지에 필요한 모든 정보를 유지할 수 있으나 지역 로깅 시스템의 메모리 제약성으로 인해 응용계층 데이터는 옵션으로 하고 각 입력 포트(Inport) 또는 출력포트(Outport)마다 전송계층에서 사용되는 소스 포트번호(srcPort) 및 목적지 포트번호(destPort)들과 네트워크 계층에서 사용되는 소스 IP 주소(srcIP)및 목적지 IP 주소(destIP)들을 저장한다. 항목 중에서 srcIP, destIP, srcPort, destPort 부분은 설정에 따라서 모두 구분하여 저장할 수 있거나 모두 합쳐서 저장할 수 있다. 모두 구분할수록 더 많은 로그정보들을 테이블 형태로 유지하게 된다.

패킷이 도착하였을 때 해당 패킷의 정보를 로그로 구성하여 로깅 시스템에 전달된다. 전달되어 오는 로그 정

보를 이용하여 새롭게 테이블 항목을 구성할 수도 있고, 기존 로깅 시스템에 기록된 로그와 중복된 메시지인 경우 가장 정확하게 매칭되는 테이블 항목을 갱신한다. 카운터(counter)를 두어서 중복된 메시지를 계수하며, 해당 패킷 유형이 로깅시스템에 처음 로깅된 시간 또는 새롭게 설정된 시간(setTime)과 마지막으로 로깅되는 시간(curTime)을 기록한다. 이러한 카운터와 시간 정보는 패킷 전송 속도를 측정할 때 사용될 수 있다.

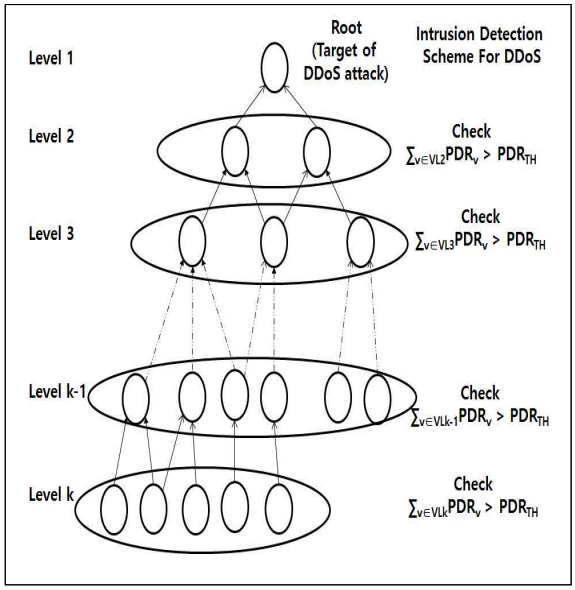
저장된 정보는 타이머에 의해 주기적이나 긴급한 메시지인 경우 실시간으로 컨트롤러에게 전송할 수 있다. 로깅 시스템에는 타이머 기능이 있어서 주기적으로 전송하거나 로깅 공간이 다 차거나 긴급 메시지 전송이 필요한 경우에는 곧바로 컨트롤러에게 전송된다. 로깅 정보를 전송하는 컨트롤러와의 통신은 한쪽 방향으로만 가는 것이므로 TCP 기반 보다는 UDP 프로토콜이 사용하며, 보안기능이 필요할 때에는 오픈플로우 프로토콜이 사용하고 있는 SSL 보다 UDP를 사용하는 전송 계층 보안 기법인 DTLS(Datagram Transport Layer Security) 기법을 사용한다[19].

4. 제안기법의 타당성

제안기법에서 IDPS 서버는 전체 무선 센서 네트워크에 대한 위치 및 트래픽 정보 등을 이용하여 네트워크의 위상 정보 그래프, 트래픽 그래프 등 다양한 그래프 정보를 유지한다. 제안기법에서는 그래프 정보들을 침입탐지 모델과 결합하여 다양한 유형의 침입 공격을 탐지할 수 있다.

4.1 분산 서비스 거부 공격 탐지 및 방지

분산 서비스 거부 공격(DDoS: Distributed Denial of Service)은 트래픽을 분산시켜 한곳으로 집중하는 공격 기법으로, 특정 포트 번호나 특정 IP 주소로 트래픽이 집중되는 것을 탐지함으로써 대응할 수 있다. 본 논문에서 제안하는 기법에서 IDPS 서버에는 분산 서비스 거부 공격을 탐지하기 위해 오픈플로우 스위치로부터 오는 로그 메시지를 이용하여 목적지 IP주소를 루트로 하는 DAG(Direct Acyclic Graph)을 그림 5와 같이 구성하고 유지한다[20, 21].



[Fig. 5] DDoS Detection by using Graph Algorithm

그림 5에서, 그래프 노드의 값은 목적지로 가는 트래픽의 속도(PDR: Packet Data Rate) 값이다. 목적지 IP주소를 루트(root)로 하는 DAG에서 동일한 레벨에 있는 노드들의 패킷 전송 속도(PDR)들을 더한 값 $\sum_{v\in VLi} PDRv$(i번째 레벨(VL_i)에 있는 노드들의 PDR의 합)이 임계값(PDR_{TH})을 넘을 경우 분산 서비스 거부 공격이라고 탐지하게 된다.

침입을 탐지한 경우 가장 트래픽의 속도가 높은 노드들부터 차례대로 오픈플로우 프로토콜을 이용하여 SDN 컨트롤러를 통해 해당 오픈플로우 스위치에 있는 트래픽을 제거함으로써 분산 서비스 거부 공격에 의해 시스템의 피해를 방지할 수 있다.

4.2 라우팅 공격 탐지 및 방지

제안기법의 IDPS 서버는 웜홀 공격의 탐지를 위해 트래픽 정보 그래프와 무선 센서 네트워크 위상 그래프를 이용한다. 임의의 패킷의 트래픽들을 분석하여 트래픽의 경로가 무선 센서 네트워크 위상 그래프 상에서 건너 띄어져 있을 때 웜홀 공격을 탐지할 수 있다. 공격이 탐지된 후에는 오픈플로우 프로토콜을 이용하여 웜홀 공격을 받는 지역에 있는 오프플로우 스위치들에게 웜홀 공격에 사용된 패킷을 수신할 경우 폐기하도록 설정함으로써 공격을 방지할 수 있다.

제안기법은 패킷 송수신 속도의 차이가 특정 임계치

보다 작을 경우 블랙홀 공격이라 탐지한다. 오픈플로우 프로토콜을 이용하여 블랙홀공격을 수행하는 노드를 경로 상에서 회피하도록 설정하여 공격에 대응할 수 있다.

4.3 제안 기법의 장점

본 논문에서 제안하는 기법은 기존 기법과 다르게 많은 장점을 가질 수 있다. 첫 번째 장점으로는 다양한 침입 탐지 모델들과 무선 센서 네트워크에 대한 그래프 모델을 융합하여 효과적으로 다양한 침입을 탐지할 수 있다는 점이다. 두 번째 장점으로는 센서 노드와 서버간의 통신 메시지를 축약하거나 필요한 정보만을 전송함으로써 효율적으로 동작할 수 있다는 점이다. 세 번째 장점으로는 서버에서 침입 탐지와 방지 대책을 제어함으로써 전체 네트워크에 대한 종합적이고 정책적인 보안 관리를 할 수 있다는 점이다.

5. 결론 및 향후 연구과제

무선 센서 네트워크는 자원 제약적인 센서 노드들이 협력적으로 구성하는 네트워크이며 다양한 응용에 적용되고 있다. 응용 범위가 넓어짐에 따라 보안의 중요성이 증가하였지만, 센서 노드들의 제약성으로 인해 다양한 유형의 침입을 탐지하는 문제를 해결하기가 쉽지 않다.

본 논문에서는 소프트웨어 정의 네트워킹 기술을 사용하여 무선 센서 네트워크에 부하를 낮추면서 중앙집중적으로 침입을 탐지하고 방지하는 기법을 제안하였다. 제안 기법으로 무선 센서 네트워크에서 발생하고 있는 다양한 공격을 탐지하고 방지할 수 있음을 보였다. 제안 기법에서 사용하는 그래프 모델을 활용하면 무선 센서 네트워크에서 발생하는 많은 침입들을 탐지할 수 있을 것으로 기대된다.

향후 연구과제로는 제안기법을 통해 탐지할 수 있는 여러 가지 침입들을 사례가 아닌 구체적인 알고리즘을 통해 구현하고, 다양한 침입 기법들에 적용할 수 있는지를 연구하는 것이다. 또한, 다양한 침입탐지를 위해 제안 기법으로 인해 발생할 수 있는 오버헤드를 평가하여 자원제약적인 무선 센서 네트워크에 효율적으로 사용할 수 있을 지를 평가한다.

REFERENCES

[1] Onechul Na, Hyojik Lee, Soyoung Sung, Hangbae Chang, “A Study on Construction of Optimal Wireless Sensor System for Enhancing Organization Security Level on Industry Convergence Environment”, Journal of the Korea Convergence Society, Vol. 6, No. 4, pp. 139-146, 2015.

[2] K. Akkaya, M. Younis, “A Survey on Routing Protocols for Wireless Sensor Networks”, Ad hoc networks Vol. 3. No. 3 pp.325-349, 2005.

[3] C. J. Chae, H. J. Cho, “Smart Fusion Agriculture based on Internet of Thing”, Journal of the Korea Convergence Society, Vol. 7, No. 6, pp. 49-54, 2016.

[4] H. W. Choi, H. S. Kim, “Convergent Secure Wireless Sensor Network Routing Algorithm”, Journal of Digital Convergence, Vol. 14, No. 10, pp. 287-29370, 2016.

[5] S. Khan, J. L. Mauri, Security for Multihop Wireless Networks, CRC Press, pp. 224, 2014.

[6] S. H. Hong, “Research on Wireless Sensor Networks Security Attack and Countermeasures: Survey”, Journal of IT Convergence Society for SMB, Vol. 4. No. 4 pp. 1-6, 2014.

[7] S. Azodolmolky, Software Defined Networking, Packt Publishing, pp. 3, 2013.

[8] Open Networking Foundation, OpenFlow Switch Specification Version 1.5.0, http://www.opennetworking. org.

[9] Y. Xiao, "Security in Sensor Networks," Auerbach Publications, pp. 8-15, 2007.

[10] K. N. Kim, J. M. Lee, S. H. Hong, MyounJae Lee, “Convergent Secure Wireless Sensor Network Routing Algorithm”, Journal of the Korea Convergence Society, Vol. 6, No. 1, pp. 65-70, 2015.

[11] O. Can, O. K. Sahingoz, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks”, 6th International Conference on in Modeling, Simulation, and Applied Optimization (ICMSAO), pp.1-6, 2015.

[12] A. D. Gante, M. Aslan, A. Matrawy, “Smart

Wireless Sensor Network Management Based on Software Defined Networking", IEEE 27th Biennial Symposium on. Communications (QBSC), pp.71-75, 2014..

[13] T. Luo, H-P. Tan, T. Q. S. Quek, "Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks," IEEE Communications Letters, Vol. 16, No. 11, 2012.

[14] Y. H. Choi, Y. C. Choi, Y. G. Hong, "Study on Coupling of Software-Defined Networking and Wireless Sensor Networks", ICUFN2016, pp.900-902, 2016.

[15] B. R. Granby, B. Askwith, A. K. Marnerides, "SDN-PANDA: Software-Defined Network Platform for ANomaly Detection Applications", In Network Protocols (ICNP), 2015 IEEE 23rd International Conference on, pp.463-466, 2015.

[16] A. Le, P. Dinh, H. Le, N. C. Tran, "Flexible Network-based Intrusion Detection and Prevention System on Software-defined Networks", 2015 International Conference on Advanced Computing and Application, pp.106-111, 2015.

[17] U. Vazirani, C. Papadimitriou, S. Dasgupta, Algorithms, McGraw-Hill Education, 2006.

[18] Y. A. Hur, K. H. Lee, "A Study on Countermeasures of Convergence for Big Data and Security Threats to Attack DRDoS in U-Healthcare Device", Journal of the Korea Convergence Society, Vol. 6, No. 4, pp. 243-248, 2015.

[19] E. Rescorla, N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, 2012.

[20] N. Chaki, R. Chaki, Intrusion Detection in Wireless Ad-hoc Networks, CRC Press, pp.176-185, 2014.

[21] E. Horowitz, S. Sahni, D. P. Mehta, Fundamentals of Data Structures in C++, Silicon Press, 2007.

저자소개

강 용 혁(Yong-Hyeog Kang) [정회원]

- 1998년 2월 : 성균관대학교 일반대학원 정보공학과 (공학석사)
- 2003년 8월 : 성균관대학교 일반대학원 전기전자 및 컴퓨터공학과 (공학박사)
- 2003년 3월 ~ 현재 : 극동대학교 글로벌경영학과 교수

<관심분야> : 사물인터넷, 보안컴퓨팅, 분산컴퓨팅, 정보경영

한 문 석(Moon-Seog Han) [정회원]

- 1986년 2월 : 중앙대학교 일반대학원 전자계산학과(이학석사)
- 2003년 2월 : 성균관대학교 일반대학원 정보공학과(공학박사)
- 1994년 3월 ~ 1996년 2월: 한국영상대학교 교수
- 1996년 4월 ~ 현재 : 강릉원주대학교 소프트웨어학과 교수

<관심분야> : 모바일시스템, 분산시스템, 데이터베이스 시스템, 지능형시스템

김 문 정(Moon Jeong Kim) [정회원]

- 1998년 2월 성균관대학교 정보공학과(공학사)
- 2000년 2월 성균관대학교 전기전자및컴퓨터공학과(공학석사)
- 2005년 2월 성균관대학교 전기전자및컴퓨터공학과(공학박사)
- 2006년 7월 ~ 2007년 11월 고려대학교 정보보호대학원 연구교수
- 2007년 12월 ~ 2009년 2월 성균관대학교 정보통신공학부 연구교수
- 2009년 3월 ~ 현재 유원대학교 스마트IT학과 교수

<관심분야> : 이동컴퓨팅, 무선애드-혹네트워크, 유비쿼터스컴퓨팅