ISSN 1598-9798

데이타베이스연구

28권 제1호 2012년 4월

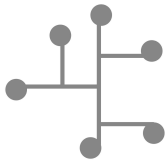
무선 센서 네트워크에서의 지연 탐지 기반의 에너지 효율적인 선택적 전송 공격 탐지 기법

An Energy-Efficient Selective Forwarding Attack Detection Scheme using Lazy Detection in Wireless Sensor Networks

박준호, 성동욱, 여명호, 이병엽, 유재수
Junho Park, Dong-ook Seong, Myungho Yeo, Byoung-yup Lee, Jaesoo Yoo

데이터베이스 소사이어티
Database Society

사단법인 한국정보과학회
The Korean Institute of Information Scientists and Engineers



무선 센서 네트워크에서의 지연 탐지 기반의 에너지 효율적인 선택적 전송 공격 탐지 기법

An Energy-Efficient Selective Forwarding Attack Detection Scheme using Lazy Detection in Wireless Sensor Networks

박준호(Junho Park)[1], 성동욱(Dong-ook Seong)[2], 여명호(Myungho Yeo)[3], 이병엽(Byoung-yup Lee)[4], 유재수(Jaesoo Yoo)[5]

요 약

무선 센서 네트워크는 다양한 분야에서 개방된 환경에 배치되므로 공격자에게 손쉽게 노출된다는 취약점을 가지고 있다. 선택적 전송 공격은 센서 네트워크에서 발생할 수 있는 공격중의 하나로 공격자는 훼손된 노드를 통하여 전장지역에서의 적의 움직임 등과 같이 중요한 정보가 기지국까지 정상적인 전달을 차단하여 감시자가 이상 현상 및 이벤트 정보의 획득을 어렵게 한다. 기존에 제안된 탐지 기법은 메시지 전달 경로 상에 감시 노드를 선정하고, 메시지가 전송 될 때마다 인증 메시지를 소스 노드에게 전송하여 공격 발생 여부 및 공격 의심 노드를 탐지한다. 하지만, 메시지를 전송할 때마다 공격 탐지를 수행하기 때문에 한정된 에너지를 바탕으로 동작하는 센서 네트워크에 적합하지 못하다. 본 논문에서는 무선 센서 네트워크 환경에서의 에너지 효율적인 선택적 전송 공격 탐지 기법을 제안한다. 제안하는 기법에서는 기존 기법에서와 같이 즉시 탐지를 수행하는 대신에 메시지 전송 시간을 고려한 네트워크 모니터링을 수행하고, 공격 노드가 존재할 가능성이 있는 경로에 대해서만 지연 탐지를 수행한다. 이를 통해, 제안하는 기법은 공격 노드의 탐지 비용을 최소화하는 것이 가능하다. 본 논문의 우수성을 보이기 위해서 시뮬레이션을 통해 성능 평가를 수행하였으며, 그 결과 기존 기법과 유사한 탐지율을 보였음에도 불구하고, 네트워크의 에너지 소모량이 평균 약 35.7% 감소하였다.

주제어: 무선 센서 네트워크, 선택적 전송 공격, 네트워크 보안, 라우팅

1 충북대학교 전자정보대학 정보통신공학부, 박사과정
2 보아스전자㈜, 연구소장
3 국방과학연구소, 선임연구원
4 배재대학교 전자상거래학과, 교수
5 충북대학교 전자정보대학 정보통신공학부, 교수, 교신저자
† 본 연구는 농림수산식품부 (생명, 첨단, 수출, 식품, 수산)기술개발사업의 지원과 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업의 결과임.(No. 2009-0089128)
+ 논문접수: 2011년 9월 13일, 심사완료: 2011년 11월 15일

Abstract

In the wireless sensor networks, sensor nodes which are deployed in hostile environments can be easily compromised by attackers. The selective forwarding attacks drop a sensitive packet on the path to transmit the data through the compromised node. The existing selective forwarding attack detection scheme randomly selects some intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgements for each received packet. The checkpoint nodes generate and transmit the acknowledgements to detect abnormal packet loss and identify suspect nodes for all packets. Therefore, the existing scheme is not suitable for the wireless sensor networks since the checkpoint nodes cause the excessive cost to detect the suspect nodes for all packets. In this paper, we propose an energy-efficient detection scheme for selective forwarding attacks in the wireless sensor networks. The proposed scheme monitors the entire networks based on the transmission time of a path for transmitting each packet. It performs a lazy detection for only the paths that have the potential to have attack nodes. By doing so, the proposed scheme can minimize the cost for detecting selective forwarding attacks. To show the superiority of our scheme, we compare it with the existing selective forwarding attack detection scheme. In the result, our scheme has the similar detection rate as the existing scheme and reduces unnecessary data transmissions by about 35.7% over the existing scheme.

Keywords: Wireless Sensor Networks, Selective Forwarding Attack, Network Security, Routing

1. 서 론

최근 컴퓨팅 기술의 비약적인 발전과 신호 처리 기술, 소형 전자 장치 개발 기술, 무선 통신 기술이 발전함에 따라 센서 네트워크에서 사용되는 센서 노드는 소형화, 저비용, 저 전력이 가능하게 되었다. 많은 수의 센서 노드들과 통신으로 이루어지는 센서 네트워크는 사람이 직접 수집하기 어려운 데이터들을 수집하고자 다양한 환경에 설치되어 현상에 대한 감시, 정보의 전달, 그리고 이웃 노드와의 협동 작업 등을 수행한다[1][2]. 이러한 센서 네트워크는 야생 환경 모니터링, 안전 모니터링, 군사 목적의 모니터링 등 특수 응용 분야에서부터 스마트 도시, 화재 감지, 환경오염 모니터링, 생체 의료 모니터링 등 생활 응용 분야에 이르기까지 그 활용 범위가 방대하며, 대상 정보에 대한 정확한 측정과 안전한 수집 및 전달을 요구한다[3][4]. 하지만 센서 네트워크는 이러한 활용성에도 불구하고 센서 정보의 도청, 비정상적 메시지의 유통, 메시지의 재사용 등의 데이터 위조 및 변조 문제와 네트워크 전체를 마비시킬 수 있는 서비스 거부 공격에 쉽게 노출된다. 따라서 센서 네트워크에서 보안 기능은 반드시 필요한 필수 요구사항이다[5][6].

선택적 전송 공격은 센서 네트워크에서 발생 가능한 가장 대표적인 라우팅 공격 중 하나이다[5][6][7]. 선택적 전송 공격은 메시지가 전송되는 경로 상에 위치한 공격 노드가 수신한 메시지를 다음 노드에 전달 및 전송하지 않고 삭제하는 공격 형태를 말한다. 선택적 전송 공격을 통해 기지국에서 현재 상태에 대한 정보를 파악하는 것을 방해하여, 센서 네트워크의 주요 목적인 모니터링 기능을 무력화시킴으로써, 특정 현상에 대한 대처를 불가능하게 하거나 지연시키는 문제점을 야기한다. 그러므로 선택적 전송 공격과 같은 라우팅 공격의 탐지는 안전한 센서 네트워크를 구성하고 이벤트를 정확하게 감지하기 위한 주요 보안 연구 중 하나이다.

선택적 전송 공격의 탐지를 위해, [8]은 감시 노드 기반의 선택적 전달 공격 탐지 기법(CHEckpoint based Multi-hop Acknowledgement Scheme; 이하 CHEMAS)을 제안하였다. 메시지 전달 경로 상의 노드들은 미리 정해진 확률에 따라 감시 노드로서 선택된다. 해당 노드들이 이웃 노드로부터 데이터 메시지를 전달받게 되면 그 응답으로 인증 메시지를 생성하여 소스 노드방향으로 미리 정해진 배포 홉-수만큼 전달하고, 인증 메시지의 수신 여부에 따라 공격 노드의 존재 유무를 판단하여 공격을 탐지한다. 하지만, 이벤트 감지 메시지를 전송 할 때마다 모든 감시 노드들이 인증 메시지를 생성하여 역방향으로 전송 및 확인하는 즉시 탐지(Eager Detecting)을 수행하기 때문에, 많은 에너지를 소모하게 되고, 한정된 에너지를 바탕으로 동작하는 센서 네트워크에는 적합하지 못하다.

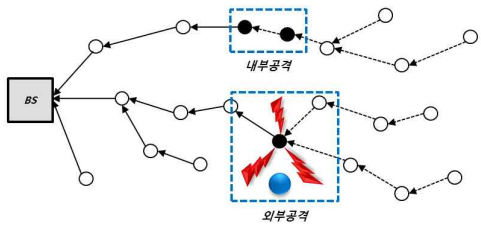
이러한 문제를 해결하기 위해, 본 논문에서는 센서 네트워크의 특성을 활용하여 탐지율을 충분히 유지하면서도 에너지 효율적인 선택적 전달 공격 탐지 기법을 제안한다. 제안하는 기법은 이벤트의 발생 여부와 관계없이 주기적으로 확인 메시지의 전송을 수행하는 센서 네트워크의 특성을 이용하여, 경로 상의 메시지 전송 시간에 기반을 둔 네트워크 상태 모니터링을 수행한다. 네트워크 모니터링 중 평균 메시지 전송 시간 내에 확인 메시지 혹은 이벤트 감지 메시지가 수집되지 않는 노드가 발생할 경우, 즉시 네트워크 초기화 단계에서 생성한 감시 노드를 활용하여 공격 노드 탐지를 위한 지연

탐지(Lazy Detecting)절차를 수행한다. 이를 통해, 선택적 전송 공격을 수행하는 공격 노드 탐지율을 충분히 유지하면서도 효율적인 에너지 활용이 가능하다.

본 논문의 구성은 다음과 같다. 먼저, 제2장에서는 기존에 제안된 선택적 전송 공격 탐지 기법에 대해서 분석하고 연구 방향을 제시한다. 제3장에서는 제안하는 선택적 전송 공격 탐지 기법을 정의하고, 공격 노드 탐지 절차를 설명한다. 제4장에서는 성능 평가와 분석을 통해 제안하는 기법의 우수성을 보이고, 제5장에서 본 연구의 결론과 향후 연구 방향을 제시한다.

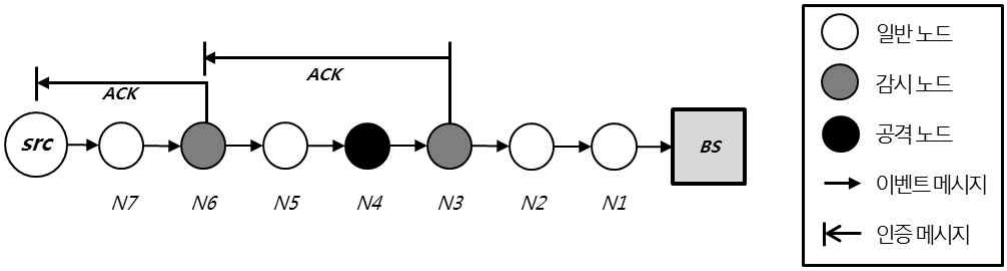
2. 관련 연구

무선 센서 네트워크에서 센서 노드들은 적은 메모리 공간, 부족한 에너지, 제한된 연산 능력, 개방된 배포 환경 등의 다양한 제약 사항을 가지고 있다. 이로 인하여 공격자는 쉽게 노드를 훼손 및 변형하여 다양한 공격을 시도 할 수 있다. 대표적인 라우팅 공격 중 하나인 선택적 전달 공격은 사용자에게 반드시 도달해야 할 중요 정보들을 경로 중간에서 차단하여 사용자의 혼란을 발생 시킨다[6]. 예를 들면, 전장 지역에서 병력의 움직임이나, 매복 감지등과 같은 중요한 정보를 훼손된 노드가 경로 중간에서 차단하여 기지국까지의 전달을 방해한다. 이러한 선택적 전송 공격의 대표적인 수행 형태는 [그림 1]과 같이 내부 공격과 외부 공격으로 구분된다. 내부 공격은 특정 노드의 훼손 및 변형을 활용한 공격으로서, 메시지를 모니터링 한 후 특정 메시지의 전송 거부를 수행하고, 외부 공격은 정상 노드 사이의 통신 채널에 대한 전파 교란 공격으로 인해 전체 메시지의 전송을 방해한다. 이러한 선택적 전송 공격은 단순한 공격 형태이지만 공격의 감지가 어렵고, 공격이 수행될 경우 기지국에서 파악해야 할 정보의 전송을 차단함으로써, 특정 모니터링 지역을 고립시킨다. 또한, 그러므로 센서 네트워크를 목표로 하는 다양한 공격 형태 중 많은 연구를 필요로 하는 분야이다.



[그림 1] 선택적 전송 공격의 수행 형태

이를 고려하여 기존에 제안된 선택적 전송 공격 탐지 기법은 통신하고 있는 상대 센서 노드의 신원을 확인하는 인증 기법을 이용하거나 탐지 노드를 네트워크에 배치하여 다중 연산을 통해 공격 노드를 탐지하는 기법이 일반적이었다. 하지만, 기존 기법은 이웃 노드와의 많은 통신과 키를 생성하거나 공격 노드를 탐지하기 위한 큰 연산 비용을 감수해야 하므로 센서 네트워크의 특성에 적합하지 못하다. 또한 공격 주체가 정상 노드를 획득하여 인증 알고리즘 획득 및 내부 코드를 변형하여 공격을 진행할 경우, 선택적 전송 공격을 탐지하는 것은 불가능하다. 이러한 문제를 해결하기 위한 기법인 CHEMAS[8]는 라우팅 경로에서 미리 정해진 확률에 따라 일부 노드들을 감시 노드(Checkpoint)로 선택한다. 감시 노드들은 이벤트 메시지(Event_packet)을 수신 및 상위 노드로 전송한 후, 이에 대한 인증 메시지(Ack_packet)을 발생시켜 이를 소스 노드 방향으로 정해진 배포 범위만큼 전달



[그림 2] 기존 선택적 전송 공격 탐지 기법(CHEMAS) [8]

한다. 이벤트 메시지를 전송한 노드는 인증 메시지가 전송되어 오지 않으면 이벤트 메시지가 삭제되었음을 인지하고 경고 메시지를 발생시켜 이를 알린다.

[그림 2]는 [8]의 탐지 과정을 나타낸다. [그림 2]에서 감시 노드로 선택 된 노드 *N3*와 노드 *N6*는 이벤트 메시지를 기지국으로 전송함과 동시에 인증 메시지를 생성하여 소스 노드 방향으로 보낸다. 노드 *N3*는 선택적 전달 공격을 수행하는 공격 노드 *N4*로부터 이벤트 메시지를 차단당하고 있으므로 노드 *N6*는 감시 노드 *N3*로부터 어떠한 인증 메시지도 받을 수 없다. 결국 노드 *N6*는 공격 수행이 의심되는 노드로써 노드 *N4*와 노드 *N5*를 보고하기 위해 경보 메시지를 생성하여 전송한다.

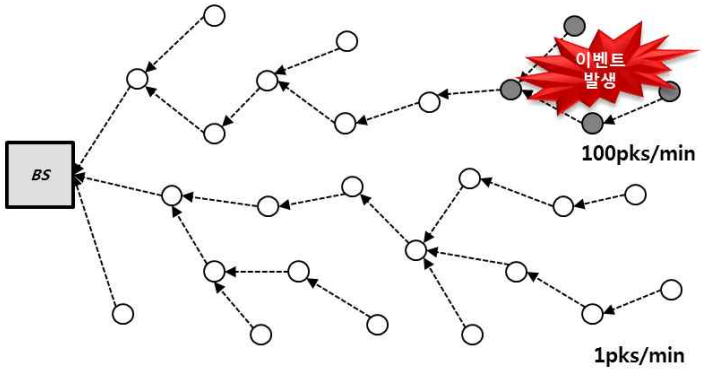
[8]은 별도의 키나 암호화 기법 없이 다수의 감시 노드를 생성하고 지속적으로 인증 메시지를 전송함으로써 높은 확률로 선택적 포워딩 공격을 탐지한다는 장점이 있다. 하지만 [8]은 센서 노드에서 이벤트 메시지를 전송 할 때마다 공격 탐지를 수행하기 위해 많은 수의 인증 메시지를 전송하기 때문에 한정된 에너지를 바탕으로 동작하는 센서 네트워크에서 활용하는 것은 한계를 가진다. 그러므로 높은 공격 노드 탐지율은 유지하면서도 에너지 효율적인 탐지 기법에 대한 연구가 필요하다.

3. 제안하는 선택적 전송 공격 탐지 기법

본 장에서는 공격 노드를 탐지하기 위한 센서 네트워크의 모니터링 특성에 기인한 에너지 효율적인 선택적 포워딩 공격 탐지 기법을 제안한다. 제안하는 기법은 크게 인증 노드 선정과 기반 정보 수집을 위한 네트워크 초기화 단계와 이를 바탕으로 하는 공격 노드 탐지 단계로 구성된다.

3.1 네트워크 초기화

제안하는 기법에서는 에너지 효율적인 선택적 전송 공격의 탐지를 위해, 일반적인 센서 네트워크의 특성을 활용하여 성능을 극대화한다. 센서 네트워크의 모니터링 응용에서는 잦은 데이터 전송으로 인한 에너지 소모를 최소화하기 위해 일반적인 모니터링 상황에서는 긴 주기로 상황 정보를 수집 및 전송하여 네트워크 및 일반적인 상황에 대한 모니터링을 수행하고, 특정한 이벤트를 감지한 상황에서는 즉각적인 파악 및 대처를 가능하게 하는 충분한 데이터를 제공하기 위해, 짧은 주기로 상황 정보를 수집 및 전송하는 기법을 사용한다[9]. 예를 들면, [그림 3]과 같이 화재 감지 위한 센서 네트워크 응용에서 정상 상태의 경우 분당 1개의 메시지를 전송하게 하고, 고온 등의 이상 상태 및 이벤트를 감지하였을 경우에는 분당

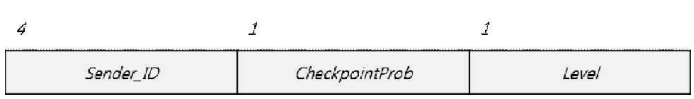


[그림 3] 센서 네트워크에서의 이벤트 감지에 따른 가변 전송 기법

100개의 메시지를 전송하여 정밀한 분석을 가능하게 할 수 있다. 제안하는 기법은 이러한 센서 네트워크의 모니터링 특성에 기반을 두어 에너지 효율적인
선택적 전송 공격 탐지 감지 기법을 제안한다.

제안하는 기법은 공격 노드 탐지를 수행하기 위한 기반 정보를 수집하기 위해 최초 네트워크 초기화 과정을 수행한다. 네트워크 초기화 과정에서 기지국은 [그림 4]와 같은 형태의 네트워크 초기화 메시지를 생성하고, 이를 전체 네트워크에 브로드캐스팅한다. 네트워크 초기화 과정을 통해, 기지국과 모니터링 영역 내의 센서 노드는 트리 형태의 데이터 전송 경로를 형성하고, 모든 센서 노드는 기지국과 노드 간의 경로 설정 및 초기화 완료를 의미하는 초기화 응답 메시지를 전송한다. 또한, 네트워크 초기화 응답 단계를 통해 기지국에서 센서 노드 아이디 기반의 인증함으로써 네트워크 이전 단계에서 공격자에 의해 배포되는 악의적인 비정상 노드를 구분하고 활동이 불가능하도록 격리 등의 추가적인 조치를 수행하는 것이 가능하다. 네트워크 초기화 메시지는 전송 노드의 *식별자(Sender_ID)*와 데이터 전송 경로 상에 인증 노드 선정을 위한 *선정 확률(CheckpointProb)* 및 수신 노드의 *라우팅 계층 정보(Level)*를 포함하여 전송한다. 이웃 노드로부터 네트워크 초기화 메시지를 받으면 메시지를 전송한 노드의 식별자를 후보 부모 노드로 저장하고, 메시지의 라우팅 계층 정보를 라우팅 경로 상에서의 자신의 레벨로 설정한다. 후보 부모 노드 리스트 큐에서 해당 노드의 레벨이 가장 작은 노드를 부모 노드로 설정하고, 다수의 동일 레벨 후보 부모 노드가 존재할 경우, 가장 먼저 메시지를 전송한 노드가 부모 노드로 설정된다. 그리고 네트워크 초기화 메시지의 전송 노드의 식별자에는 자신의 아이디를, 라우팅 계층 정보에는 자신의 레벨에 1을 더한 값으로 설정한 후, 이웃 노드에게 전달한다. 본 과정은 모든 센서 노드가 자신의 레벨과 부모 노드를 설정하고, 인증 노드 선정 확률을 저장할 때까지 반복한다.

네트워크 초기화 메시지를 수신한 각 노드들은 [그림 5]와 같은 형태의 네트워크 초기화 응답 메시



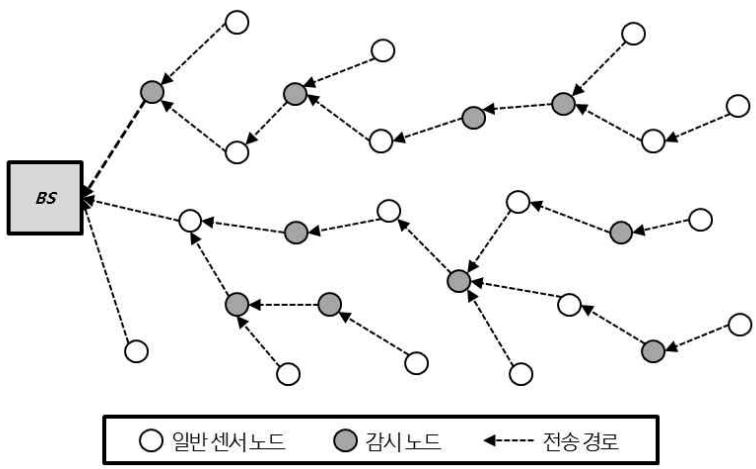
[그림 4] 네트워크 초기화 메시지 형식

[그림 5] 네트워크 초기화 응답 메시지 형식

지를 생성하여 기지국에 전송한다. 네트워크 초기화 응답 메시지는 응답하는 노드를 구분하기 위한 노드 식별자(Source_ID)와 해당 노드의 메시지 송신 시간(MessageSendTime) 및 해당 노드의 인증 노드 선정 여부를 포함한다. 기지국에서는 이를 수신하고 네트워크 초기화 응답 메시지에 담긴 메시지 송신 시간(MessageSendTime)을 바탕으로 식(1)을 이용하여 메시지 전송 시간을 연산하게 된다. 기지국에서는 전체 노드의 전송 시간을 관리하게 되며, 이를 바탕으로 모니터링 데이터 전송 단계에서 선택적 전송 공격이 이루어지는 경로 및 수행하는 공격 노드를 탐지하기 위한 기반 정보로 활용한다.

$$ssage\ Transmission \quad T_{ReceivedTime} - T_{SendTime} \qquad \text{식 (1)}$$

기지국에서 네트워크 초기화 메시지를 수신한 모든 센서 노드는 메시지에 담긴 정해진 선정 확률에 따라 감시 노드 선정 연산을 수행한다. 모든 노드에서는 랜덤 연산을 통해 자신의 확률을 구하고, 자식 노드의 수를 함께 포함하여 최종으로 노드의 선정 확률을 결정한다. 이때 선정 확률이 기지국에서 전송한 선정 확률보다 높을 경우, 해당 노드는 감시 노드로 최종 선정된다. 네트워크 초기화 메시지에 담긴 수 네트워크의 특성상, 많은 수의 자식 노드와 연결이 되어 있는 부모 노드는 감시 노드의 역할 수행에 있어서 보다 효율적이고 정확한 감지를 수행하는 것이 가능하다. 그러므로 제안하는 기법에서는 기지국에서 설정한 선정 확률과 자식 노드의 수를 이용하여 감시 노드를 선출한다. 감시 노드의 수가 많아질수록 탐지율 및 탐지 신속성은 높아지지만, 이를 위한 네트워크 상태 확인 메시지가 증가하고 이에 따른 네트워크 에너지 소모가 높아지므로 탐지율 및 탐지 신속성과 에너지 효율은 상보(Trade-off) 관계에 있다. 그러므로 이를 적절한 수준에서 제어하는 것이 필요하다. [그림 6]은 네트워크 초기화 완료 후의 센서 네트워



[그림 6] 네트워크 초기화 완료

크를 나타낸다. 센서 네트워크의 전송 경로 상에서 확률과 자식 노드의 수를 이용한 감시 노드가 부분적으로 위치하게 된다. 이와 더불어, 기지국에서는 [그림 7]과 같은 네트워크 관리 테이블을 구성하고, 각 노드에서의 메시지 수신 시간을 관리한다.

3.2 공격 노드 탐지

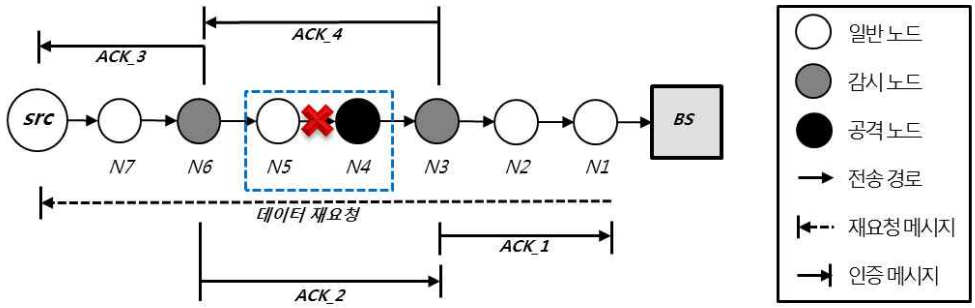
네트워크 초기화에 성공한 노드들은 모니터링 및 데이터 전송 단계가 즉시 수행된다. 앞서 언급한 것과 같이 트리 형태의 센서 네트워크는 질의에 만족하는 이벤트의 감지와는 관계없이 주기적으로 상태 메시지를 기지국으로 전송하게 되고, 기지국은 이를 수신하여 [그림 7]과 같이 각 노드들이 전송한 데이터가 정상적으로 수신하고 있는지 메시지 전송 시간 기반의 네트워크 상태 점검을 수행하게 된다. 더불어, 최근 메시지 수집 시간을 관리하고 이를 이용하여 주기적으로 네트워크 관리 테이블을 주기적으로 업데이트를 수행함으로써 상황 적응적인 네트워크 관리를 수행한다. 기지국은 모든 노드들이 이벤트 감지 메시지 혹은 상태 메시지가 정상적으로 수집 되고 있는지의 여부를 네트워크 관리 테이블을 이용하여 모니터링을 수행하다가 [그림 7]의 노드 *N2*와 같이 식 (2)의 수신 주기를 벗어나서 메시지가 전송되지 않는 노드의 발생 즉시 공격 노드 탐지를 수행한다. 이때, 각 경로의 상태에 따라 메시지의 수신 주기는 편차가 발생한다. 그러므로 수신 주기는 노드에서 기지국 사이에 생성된 경로에서 이전에 성공적으로 전송 완료된 평균 메시지 전송 시간과 기존 수집 주기 기반의 표준 편차를 유예 시간으로 설정하고, 수신 주기 이상으로 메시지가 수집되지 않을 경우, 감지 이벤트 발생으로 간주한다.

$$ceivePeriodic \quad \frac{\sum_{k=1}^{n} T_{duration(f(n))}}{n} \qquad \text{식 (2)}$$

공격 노드의 탐지를 위해 [그림 8]과 같이 *재요청 메시지(ReqAck_Message)*을 해당 노드가 위치한 경로로 전송하여 지연 탐지를 수행한다. 이 때, 일반 노드는 인증 요청 패킷의 포워딩만을 담당하고, 경로상에 위치한 감시 노드에서 인증 메시지를 역방향으로 전송한다. 제안하는 기법의 공격 노드 탐지는 크게 2가지 인증으로 이루어진다. 첫 번째는 데이터 재요청 메시지에 대한 인증이고, 두 번째는 재전송된 데이터 메시지에 대한 인증이다. 데이터 재요청 메시지에 대한 인증은 데이터 재요청 메시지를 수신한 감시 노드는 인증 패킷을 기지국 방향으로 전송하여, 누락 메시지 재전송을 요청할 노드까지 인증 요청이

NodeID	*초기 수신*	*f(1) 수신*	*f(2) 수신*	...	*f(n) 수신*	*노드당 평균 수신 주기(s)*
N1	13:14:02	14:15:49	15:16:42	...	20:21:23	1:00:48
N2	13:19:00	14:19:04	14:49:02	...	-	0:48:02
...	...	...	...	...	...	...
N_n	13:42:28	14:44:36	15:05:02	...	20:05:12	1:01:38

[그림 7] 네트워크 관리 테이블



[그림 8] 제안하는 기법의 공격 노드 탐지

정상적으로 이루어졌음을 보증하고, 재전송된 데이터 메시지에 대한 인증은 재전송된 데이터 메시지를 수신한 감시 노드가 인증 메시지를 소스 노드 방향으로 전송하여, 해당 노드까지는 데이터가 전송되었음을 보증하기 위함이다. 이는 공격 노드에 의해 데이터 메시지뿐만 아니라, 기지국에서 전송한 재요청 메시지 또한 삭제 가능함을 고려한 확인 절차이다.

예를 들어, [그림 8]에서 감시 노드 *N3*와 *N6*는 재요청 메시지 및 재전송된 메시지를 수신하였을 경우, 이에 대한 인증 메시지를 전송함으로써 응답을 수행한다. 하지만 재요청 메시지 전송 시, 인증 노드 *N3*를 경유한 메시지가 공격 노드 *N4*에 의해 누락 될 경우, 인증 노드 *N6*는 인증 메시지를 전송 할 수 없다. 인증 노드 *N3*의 인증 메시지를 수신한 기지국에서는 인증 노드 N3와 N6사이에 공격 노드가 존재함을 인지하고 해당 노드를 격리시킨다. 또한, 소스 노드 *Src*가 재요청 메시지를 정상적으로 수신하여 데이터 메시지가 재전송되고, 공격 노드 *N4*에 의해 누락되는 경우에도 인증 노드 *N3*로부터 인증 메시지가 발생되지 못하므로, 인증 노드 *N6*와 *N3*사이에 공격 노드가 있음을 인지하고 공격 노드를 파악하는 것이 가능하다. 이러한 양방향 공격 탐지 과정을 통해, 공격 노드의 위치의 파악이 가능하며, 기존 기법과 달리 메시지 전송 시마다 인증 단계를 수행하지 않으므로 에너지 효율적인 선택적 전송 공격의 탐지가 가능하다.

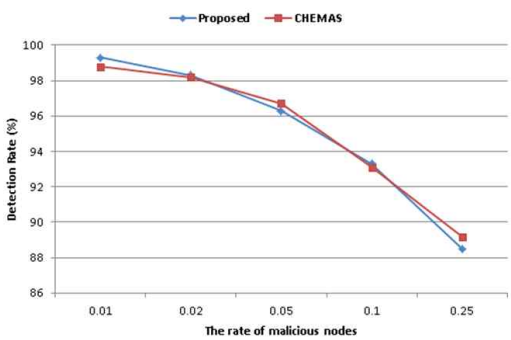
4. 성능 평가

본 장에서는 제안하는 기법의 우수성을 보이기 위해 기존에 제안된 선택적 전송 공격 탐지 기법[8]과 시뮬레이션을 통해 성능을 비교 평가 하였다. 성능 평가는 400개의 센서 노드가 임의로 배포 된 환경에서 표 1과 같은 환경 변수를 이용하여 수행하였다. 센서 노드의 메시지 전송에 소모되는 에너지 모델은 {*메시지 크기*}×({*전송 비용*}+{*증폭비용*}×{*거리*})이며, 전송 비용은 *50nJ/b*, 증폭 비용은 *100pJ/b/m*^{2}으로 설정하였다. 메시지 수신에 소모되는 에너지 모델은 {*메시지 크기*} × {*수신 비용*} 이며, 수신 비용은 50nJ/b으로 설정하였다[10][11]. 공격 노드 생성 시, 임의의 노드가 공격자에 의해 공격 참여 노드(Compromised Nodes)로 변형이 가능하지만, 싱크 노드 인근의 영역은 안전 영역으로 설정하여 최소 공격 노드 발생 범위 외의 영역에서 공격 노드가 임의로 발생하는 환경에서 성능 평가를 진행하였다.

[표 1] 성능 평가 환경

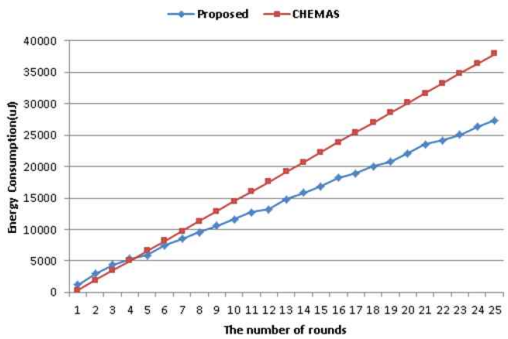
파라미터	값
센서네트워크 크기 (m × m)	500 × 500
배포 된 센서의 수 (개)	40
기지국의 위치 (x, y)	(0, 0)
데이터 패킷의 크기 (Bytes)	4
최소 공격 노드 발생 거리 (홉)	2
감시 노드 선정 비율 (%)	30

[그림 9]는 공격 노드의 수에 따른 탐지율을 기존의 기법과 비교한 그래프이다. 실험에서는 제안하는 기법의 감시 노드 선정 비율은 0.3, 기존 기법의 인증 패킷의 전송 범위를 3-홉으로 각각 설정하였다. 성능 평가에서 보는 것처럼 공격 노드의 숫자가 증가함에 따라 감시 노드가 공격 참여 노드로 변형되는 비율이 증가하게 된다. 그에 따라 제안하는 기법과 기존 기법 모두 점차 공격 노드를 탐지하는 비율이 감소하는 결과를 보였지만, 제안하는 기법은 인증 노드를 활용한 유사한 공격 노드 탐지 알고리즘을 사용하므로 기존 기법과 유사한 탐지율을 보였다.



[그림 9] 공격 노드의 수에 따른 탐지율

그림 10은 공격 노드의 지속적인 생성에 따른 에너지 소모율을 비교한 그래프이다. 이전의 실험과 마찬가지로 기존 기법의 감시 노드 선정 비율과 인증 메시지 전송 범위를 동일하게 설정하였으며, 매 5라운드마다 새로운 공격 노드가 추가되도록 시나리오를 구성하였다. 기존 기법의 경우, 공격 노드의 생성과 무관하게 메시지 전송 시마다 지속적으로 인증 메시지를 전송하기 때문에 높은 에너지 소모율을 보인다. 하지만 제안하는 기법의 경우 메시지가 수집되지 않을 경우, 해당 경로에만 인증 요청 메시지를 전송하기 때문에, 낮은 에너지 소모를 보인다. 성능 평가 결과, 네트워크 동작에 따른 에너지 소모가 기존 기법에 비해 평균 35.7% 감소하였다.



[그림 10] 네트워크 에너지 소모율

5. 결론 및 향후 연구

본 논문에서는 센서 네트워크에서 에너지 효율적인 선택적 전송 공격을 탐지 기법을 제안하였다. 기존에 제안된 선택적 전송 공격 탐지 기법은 메시지 전달 경로 상에 감시 노드를 선정하고, 메시지가 전송 될 때마다 인증 메시지를 소스 노드에게 전송하여 공격 발생 여부를 탐지하는 것이 가능하다. 하지만 센서 노드에서 감지 메시지를 전송 할 때마다 공격 탐지를 수행하기 위해 많은 수의 인증 메시지를 전송하기 때문에 한정된 에너지를 바탕으로 동작하는 센서 네트워크에 적합하지 못하다. 제안하는 기법에서는 센서 네트워크의 특성과 노드에서의 메시지 전송

시간을 고려한 네트워크 모니터링을 수행하고, 공격 받았을 가능성이 있는 경로에 대해서만 지연 탐지를 수행하여 공격 노드를 탐지한다. 시뮬레이션을 통한 실험 결과, 기존 탐지 기법과 유사한 탐지율을 보이면서도, 센서 네트워크의 에너지 소모율이 약 35.7% 감소하였다. 향후 연구로는 공격 노드로의 라우팅 경로를 인접한 라우팅 경로로 분산시켜 공격 노드를 네트워크에서 격리시키는 기법의 접목 및 추가적인 성능 평가를 통해 제안하는 기법의 우수성을 입증하는 것이다.

6. 참고문헌

[1] D. Culler, D. Estrin, and M. Srivastava, "Guest Editors' Introduction: Overview of Sensor Networks," Journal of IEEE Computer, vol.37, no.8, pp.41-49, 2004.

[2] D. Estrin, L. Girod, G. Pottie and M. Srivastava, "Instrumenting the World with Wireless Sensor Networks," Proc. of International Conference Acoustics, Speech, and Signal Processing, pp.2033-2036, 2001.

[3] A, Cerpa, J. Elson, D. Estrin, L, Girod, M, Hamilton and J, Zhao, "Habitat Monitoring: Application Driver for Wireless Communications Technology," Proc. of ACM Workshop on Data Communications in Latin America and the Caribbean, pp.20-41, 2001.

[4] S. Tanachaiwiwat, P. Dave, R. Bhindwale and A. Helmy,"Locationcentric Isolation of Misbehavior and Trust Routing in Energyconstrained Sensor Networks," Proc. of International Conference On Performance, Computing and Communications, pp. 463-469, 2004.

[5] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. of 1st IEEE International Workshop on Sensor Network Protocols and Applications, pp.113-127, 2003.

[6] X. Chen, K. Makki, K. Yen and N. Pissinou, "Sensor Network Security: a Survey," IEEE Communications Surveys and Tutorials, vol.11, no.2, pp.52-73, 2009.

[7] I.F. Akyildiz, W. Su, Y. Sankarasubramanism and E. Cayirci, "A Survey on Sensor Networks," Proc. of IEEE Communications Magazine, vol.40, no.8, pp.102-114, 2002.

[8] B. Xiao, B. Yu and C. Gao, "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks," Journal of Parallel and Distributed Computing, vol.67, no.11, pp.1218-1230, 2007.

[9] C. Wang, B. Li, K, Sohraby, M. Daneshmand, and Y. Hu, "Upstream Congestion Control in Wireless Sensor Networks through Cross-Layer Optimization," IEEE Journal on Selected Areas in Communications, vol.25, no.4, pp.786-795, 2007.

[10] W. Heinzelman, "Application-Specific Protocol Architecture for Wireless Networks," Ph.D dissertation, Massachusetts Institute of Technology, 2000.

[11] X. Tang and J. Xu, "Extending Network Lifetime for Precision-Constrained Data Aggregation in Wireless Sensor Networks," Proc. of 25th IEEE International Conference on Computer Communications, pp.1-12, 2006.

박 준 호

2008년 2월 충북대학교 정보통신공학과 공학사.

2010년 2월 충북대학교 정보통신공학과 공학석사.

2010년 3월 ~ 현재 충북대학교 전자정보대학 정보통신공학부 박사과정.

관심분야 : 데이터베이스 시스템, 무선 센서 네트워크, RFID, 차세대 웹, LMS/LCMS, 바이오인포메틱스 등

성 동 욱

2005년 2월 충북대학교 정보통신공학과 공학사.

2007년 2월 충북대학교 정보통신공학과 공학석사.

2011년 2월 충북대학교 정보통신공학과 공학박사.

2011년 3월 ~ 2012년 2월 한국과학기술원 전산학과 연수연구원.

2012년 3월 ~ 현재 보아스전자㈜ 연구소장.

관심분야 : 무선 센서 네트워크, 데이터베이스 시스템, FLASH 메모리 저장 시스템, LCMS/LMS, 위치기반 서비스 등

여 명 호

2004년 2월 충북대학교 정보통신공학과 공학사.
2006년 2월 충북대학교 정보통신공학과 공학석사.
2010년 2월 충북대학교 정보통신공학과 공학박사.
2010년 2월 ~ 현재 국방과학연구소 선임연구원.
관심분야 : 메인 메모리 기반 데이터베이스, 시공간 데이터베이스, 무선 센서 네트워크 등

이 병 엽

1991년 2월 한국과학기술원 전산학과 공학사.
1993년 2월 한국과학기술원 전산학과 공학석사.
1997년 2월 한국과학기술원 경영정보공학 공학박사.
1993년 1월 ~ 2003년 2월 대우정보시스템 차장
2003년 3월 ~ 현재 배재대학교 전자상거래학과 부교수
관심분야 : XML, 지능정보시스템, 데이터베이스시스템, 전자상거래학 등

유 재 수(교신저자)

1989년 2월 전북대학교 컴퓨터공학과 공학사.
2007년 2월 한국과학기술원 전산학과 공학석사.
2011년 2월 한국과학기술원 전산학과 공학박사.
1995년 3월 ~ 1996년 8월 목포대학교 전산통계학과 전임강사.
1996년 8월 ~ 현재 충북대학교 전자정보대학 정보통신공학부 및 컴퓨터정보통신연구소 교수.
관심분야 : 데이터베이스 시스템, 정보검색, 센서 네트워크 및 RFID, 멀티미디어 데이터베이스, 분산 객체 컴퓨팅, 바이오인포메틱스 등
E-mail : yjs@chungbuk.ac.kr