센서 네트워크에서의 서비스 거부(Denial of Service) 공격에 대한 보안요구사항 연구

임휘빈*, 박상진*, 김미주**, 신용태*, 최종원***
*숭실대학교 컴퓨터학과
**한국인터넷진흥원 정보보호본부
***숙명여자대학교 컴퓨터과학과
e-mail:hblim@cherry.ssu.ac.kr

A Study on Security Requirement against Denial of Service Attack in Sensor Network

Hui-Bin Lim*, Sang-Jin Park*, Mi-Joo Kim**,
Yong-Tae Shin*, Jong-Won Choe***
*Dept of Computing, Soong-Sil University
**Korea Information & Security Agency
***Dept of Computer Science, Sook-Myung Women's University

요 약

센서 네트워크에 대한 보안은 일반 네트워크와 동일하게 보안성, 무결성, 가용성 등이 요구된다. 그러나 일반적으로 센서 네트워크는 무선 통신을 하는 네트워크이고, 고정된 인프라가 없으며, 네트워크 토폴로지가 자주 변하는 특징으로 인해 보안문제는 어려운 것으로 인식되고 있다. 특히, 센서 노드의 에너지와 같은 자원 고갈을 유발하여 정상적인 동작을 못하게 하는 서비스 거부(Denial of Service, DoS)와 같은 공격에 취약하다.

본 논문에서는 센서 네트워크의 일반적인 구성을 통해 발생할 수 있는 DoS 공격의 유형을 분석하고, 보안요구사항을 제시하였다. 제시한 보안요구사항은 DoS 공격 뿐 아니라 센서 네트워크에서 발생할 수 있는 다양한 공격 유형에 대한 보안요구사항을 마련하는 데에 기초가 될 것으로 기대한다.

1. 서론

센서 네트워크(Sensor Network)는 무선 통신 방식으로, 정형화된 네트워크 토폴로지를 가지지 않음으로 인해 유선 네트워크에 비해 다양한 보안 취약성을 가진다. 특히, 센서 노드의 에너지를 고갈시켜서 정상적인 센서 네트워크의 운영을 방해하는 서비스 거부 공격(Denial of Service, DoS)이나 분산 서비스 거부 공격(Distributed Denial of Service, DDoS)에 취약하다[2,5].

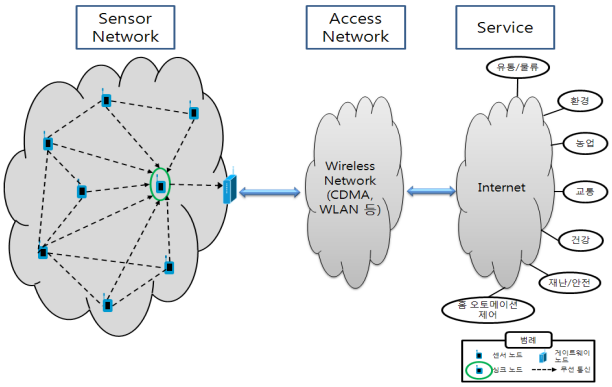
이에 본 논문에서는 센서 네트워크에서의 DoS 공격에 대한 유형을 분석하고, 이에 대한 보안요구사항을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 센서 네트워크의 구성을 검토한다. 3장에서는 센서 네트워크에서의 DoS 공격 유형을 분석하고, 이에 대한 보안요구사항을 제안한다. 마지막으로 4장에서 결론을 맺는다.

2. 센서 네트워크의 구성

센서 네트워크는 (그림 1)과 같이 크게 센서 노드(sensor node), 싱크 노드(sink node), 게이트웨이 노드(gateway node)로 구성할 수 있다[4].

센서 노드는 풍향, 조도, 습도, 온도 등의 데이터를 수집하고자 하는 영역에 배치되어 측정·수집한다. 그리고 수집한 데이터를 무선 통신을 사용하여 싱크 노드에게 전송하는 역할을 한다. 싱크 노드는 센서 노드가 전송한 데이터를 전송받아서 통합하거나 통합하지 않고 게이트웨이 노드로 전송하는 역할을 한다. 하나의 센서 네트워크에는 다수의 싱크 노드가 존재할 수 있다. 게이트웨이 노드는 싱크 노드가 전송한 메시지를 외부의 서비스와 연결된 액세스 네트워크로 전송하는 역할을 한다.



(그림 1) 센서 네트워크의 구성

본 연구는 정보통신기술협회의 정보통신표준기술력향상 사업의 일환으로 수행하였음. [2009-P1-32-08J46]

3. DoS 공격 유형 및 보안요구사항

3.1 DoS 공격 유형

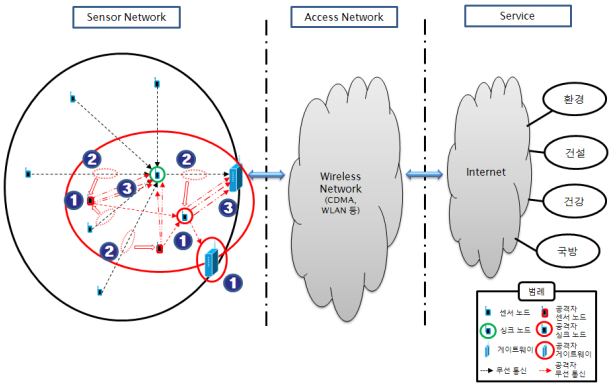
센서 네트워크에서의 DoS 공격은 노드의 에너지와 같은 자원을 고갈시켜 네트워크의 정상적인 동작을 방해하는 행위이다. 센서 네트워크에서의 DoS 공격 유형은 유선 네트워크에서의 DoS 공격에서 사용하는 플러드(flood) 공격, 랜드(land) 공격 등과 같은 방법이 활용될 수 있다[1,3].

플러드 공격의 대표적인 시나리오는 (그림 2)와 같다.

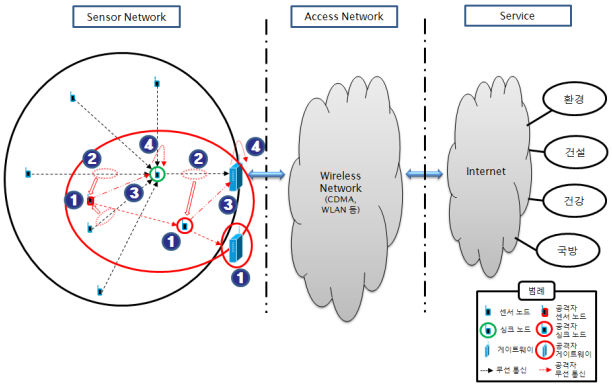
① 공격자는 자신의 노드를 정상적인 센서 네트워크에 배치한다.

② 공격자 노드는 정상적인 노드의 전송 데이터를 가로채서 분석한다.

③ 공격자 노드는 불법적으로 획득한 전송 데이터 또는 불법적인 다량의 데이터를 생성하여 정상적인 노드로 전송한다.



(그림 2) DoS 공격 유형 - 플러드(flood) 공격



(그림 3) DoS 공격 유형 - 랜드(land) 공격

랜드 공격의 대표적인 시나리오는 (그림 3)과 같다.

① 공격자는 자신의 노드를 정상적인 센서 네트워크에 배치한다.

② 공격자 노드는 정상적인 노드의 전송 데이터를 가로채서 분석한다.

③ 공격자 노드는 불법적으로 획득한 데이터를 생성하여 정상적인 노드로 전송한다.

④ 정상적인 노드는 공격자 노드가 전송한 데이터에 대한 응답 신호를 자기 자신에게 반복적으로 전송하게 된다. 정상적인 노드는 이러한 데이터를 처리하기 위해 에너지를 불필요하게 소비한다.

이와 같은 센서 네트워크에서의 다양한 DoS 공격 방법을 통해 공격자 노드는 정상적인 노드의 에너지를 고갈시키거나 노드 간의 통신 채널을 점유하게 된다. 따라서 센서 네트워크를 구성하는 정상적인 노드의 동작 및 노드 간의 연결을 방해하여 네트워크 운영을 방해한다.

3.2 보안요구사항

센서 네트워크에서의 DoS 공격에 대한 보안요구사항은 다음과 같다.

첫째, 기밀성 보장을 위한 제어 및 측정 메시지에 대한 암호화 기법이 필요하다. 둘째, 암호화 기법을 위한 센서 네트워크에 적합한 암호 알고리즘 및 키 관리 메커니즘과 이에 대한 호환성이 필요하다. 셋째, 전송 채널의 암호화 및 복수의 전송채널의 확보가 필요하다. 넷째, 정상적인 노드(센서-센서, 센서-싱크, 싱크-게이트웨이) 간의 인증 메커니즘이 필요하다. 다섯째, 공격자 노드의 접근을 차단할 수 있는 접근제어 기술이 필요하다. 여섯째, 수신한 메시지에 대한 정상적인 메시지인지를 판단할 수 있는 침입탐지 기술이 필요하다.

4. 결론

센서 네트워크에서의 DoS 공격은 정상적인 노드의 에너지 고갈을 유발시키거나 노드 간의 연결을 방해하여 정상적인 센서 네트워크 운영을 방해한다.

본 논문에서는 센서 네트워크에서의 DoS 공격에 대한 유형을 분석하고, 이에 대한 보안요구사항을 제안하였다. 향후에는 이러한 보안요구사항에 대한 검증을 통해 타당성을 검토하고 이를 확장하여 다른 공격에 대한 보안을 향상시킬 수 있는 연구가 필요하다.

참고문헌

[1] 이병주, 홍순좌, 이승형, “유비쿼터스 네트워크에서 서비스 거부(Denial of Service) 공격의 특성 및 위험성 분석,” *정보보호학회*, 2004

[2] 조현숙, 정교일, 최두호, 강유성, “RFID/USN 보안 기술 개발 동향,” *한국전파학회*, 2008

[3] Anthony D. Wood, John A. Stamkovic. “Denial of Service in Sensor Networks,“ *Computer*, 2002

[4] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci, “A Survey on Sensor Networks,” *IEEE Communications Magazine*, 2002

[5] Yong Wang, Garhan Attebury, Byrav Ramamurthy, “A survey of security issues in wireless sensor networks,” *IEEE Communications Surveys & Tutorials*, 2006