무선 센서 네트워크 환경에서 링크 품질 지표에 기반한 라우팅에 대한 싱크홀 공격 탐지 기법

최병구 조응준[0] 홍충선
경희대학교 컴퓨터공학과
bgchoi@khu.ac.kr ejcho@networking.khu.ac.kr cshong@khu.ac.kr

Sinkhole Attack Detection for LQI based Routing in WSN

Byung Goo Choi Eung Jun Cho[0] Choong Seon Hong
Department of Computer Engineering, Kyung Hee University

1. 서 론

무선 센서 네트워크는 미래의 유비쿼터스 환경에 기반이 될 중요한 기술 중의 하나이다. 센서 네트워크는 저비용으로 데이터의 수집 및 측정에 폭넓게 이용될 수 있다. 그러나 센서 네트워크는 무선 통신의 특성과 제한된 성능 및 자원으로 여러 가지 공격에 노출되어 있다. 특히 라우팅 프로토콜의 경우 공격에 노출되면 네트워크의 혼란이 발생하여 서비스 불능 상태가 될 수 있다.

무선 센서 네트워크에서 라우팅 공격의 대표적인 형태중의 하나가 싱크홀 공격이다[1]. 이 공격에서 악의적인 노드는 자신이 BaseStation이나 목적지 노드에 더 가까이 있다고 거짓 광고하여 다른 노드들이 그들의 트래픽을 자신을 경유해서 보내게 한다. 따라서 싱크홀 공격의 탐지 기법은 안전한 무선 센서 네트워크를 위한 중요한 연구 분야이다. 이 논문에서는 링크품질지표에 기반한 라우팅을 수행하는 무선 센서 네트워크에서 안전한 데이터 전송을 위해 싱크홀 공격을 탐지할 수 있는 방법을 제안하였다.

2. 관련연구

2.1 링크 품질 지표(Link Quality Indicator)

링크 품질 지표는 전달 받은 패킷의 신호 세기나 품질을 나타낸다. 이것은 수신자의 신호 세기 측정 모듈을 사용하여 측정된 신호 세기 또는 신호 세기 대 잡음의 비율로 결정된다. 링크 품질 지표는 각 수신 패킷마다 측정되며 이 값은 0x00~0xFF 까지의 범위를 가지고 가장 낮은 수치가 가장 좋은 신호 품질을 의미한다[2].

2.2 홉카운트를 이용한 라우팅에서의 싱크홀 공격 탐지 기법

이전에 제시된 싱크홀 공격 탐지 기법은 홉카운트에 기반한 라우팅을 기준으로 한다[3]. 이 방법은 모든 센서 노드들이 주기적으로 BaseStation으로 데이터를 전송하는 환경을 가정한다.

싱크홀 공격이 이루어질 경우 싱크홀 노드가 취할 수 있는 대표적인 공격 방법이 Selective Forwarding이다. 이런 공격이 발생할 경우 BaseStation은 데이터를 전달 받지 못한 노드들의 목록을 작성한다. 이 노드들이 위치한 지역의 모든 노드들로부터 Next-hop 정보를 모으면 최상위에서 데이터가 집중되는 싱크홀 노드를 찾아낼 수 있다.

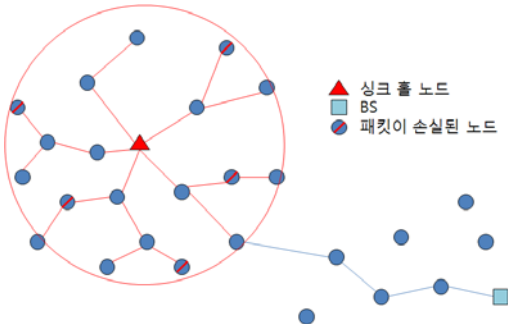

그림 1 홉카운트를 이용한 싱크홀 공격 탐지 기법

3. 제안사항

3.1 가정 사항

본 논문에서는 다음과 같은 환경을 가정한다. 노드는 다수의 일반 노드와 소수의 탐지 노드로 구분된다. 탐지 노드들은 충분히 많은 전원을 가지며 서로 간의 전용의 링크 또는 채널을 이용하여 신뢰성 있는 데이터 전송을 한다. 또한 탐지 노드들은 promiscuous 모드로 동작 가능하며 주변의 모든 Routing Request 메시지를 감시한다. 모든 노드는 고정되어 있어 이동하지 않는다. 네트워크의 라우팅 프로토콜은 경로비용으로 LQI를 사용하는 요구기반(On-demand) 거리벡터 라우팅 프로토콜을 사용한다.

"본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0016))

3.2 네트워크 초기 설정 단계

네트워크 초기 설정 단계에서 각 노드들은 이웃 노드들과의 LQI 값을 계산한다. 각 노드는 발신 가능한 범위 내에서 최대한 강한 신호를 이웃노드에게 보낸다. 이 과정을 충분히 반복하여 각 노드는 주변 노드들로부터의 최소 LQI값을 도출할 수 있다. 이 값에 따라 구성된 최소 Neighbor LQI table은 상대노드가 인위적으로 매우 강한 신호를 보냄으로써 LQI 값을 낮추어 라우팅 경로를 변경하려는 공격을 탐지하는데 사용된다. 탐지 노드의 경우에는 위의 과정과 함께 주변의 탐지 노드들을 탐색하고 각 탐지 노드사이의 최적 경로와 그때의 경로비용(누적 LQI)도 기록한다.

3.3 공격 탐지 과정

일반적으로 LQI를 기반한 라우팅에서는 각 라우팅 경로에서의 LQI를 누적하여 최소의 비용을 가지는 경로를 최적의 경로로 선택한다. 다음은 싱크홀 노드가 라우팅 경로를 자신을 거치게 하도록 수정하기 위해 취할 수 있는 방법과 그에 대한 탐지방법을 나타낸다.

1) Routing Request 패킷을 전달할 때 정상적인 출력보다 더 강한 신호로 보내어 더 멀리 보내거나 또는 수신 노드들이 더 좋은 품질의 신호로 인지하도록 하는 방법

탐지 방법 : 싱크홀 노드가 Routing Request 메시지를 보낼 때 수신 노드에서는 최소 Neighbor LQI Table을 참조하여 신호의 세기를 검사한다. [*(현재 메시지의 LQI) < (최소 Neighbor LQI) × C*] 여기서 C는 허용 오차 범위를 의미한다. 위의 식이 참이 되면 해당 메시지가 최적의 링크 품질보다 좋게 전송된 것이므로 공격으로 판단한다.

2) 경로 탐색시 전달되는 Routing Request 패킷 내의 누적 LQI값을 더 작게 수정하는 방법

탐지 방법 : 싱크홀 노드가 Routing Request 메시지의 누적 LQI값을 위조하는 경우 위의 방법으로는 탐지가 불가능하다. 이러한 경우 탐지 노드를 이용한 공격 탐지를 수행한다. 탐지 노드들은 자신의 전파범위내의 모든 Routing Request 메시지를 감시한다. 싱크홀 공격이 이루어지는 경우에도 해당 Routing Request 메시지는 주변의 탐지 노드들에게 수집된다. [*(두 탐지 노드 사이에서 Routing Request 메시지의 경로비용 증가량) < (탐지 노드간의 최적 경로 비용) - (탐지 노드와 Routing Request를 검사한 노드사이의 경로 비용)*] 만약 이 부등식이 참이 된다면 최적의 경로보다 더 좋은 경로로 전송된 것을 의미하고 이는 공격이 발생한 것으로 판단한다.

그림 3의 예를 보면 두 탐지 노드 사이의 최적 경로 비용은 102가 된다. 그러나 Routing Request 메시지가 수집된 노드와 탐지 노드간의 비용을 제외해야 하므로 결과적으로 67이라는 값을 얻게 된다. 이 값과 Routing Request 메시지의 누적 LQI 값의 증가량인 50을 비교하면 Routing Request 메시지가 최적의 경로 보다 더 좋은 경로를 통해 전달되었다는 모순이 나타난다. 이런 경우 두 탐지 노드 사이에서 싱크홀 공격이 일어나고 있음을 판단할 수 있다.

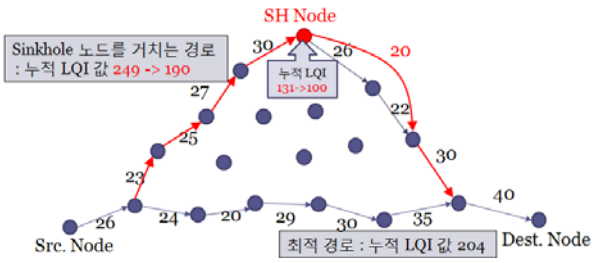

그림 2 싱크홀 공격 발생시의 경로 비용

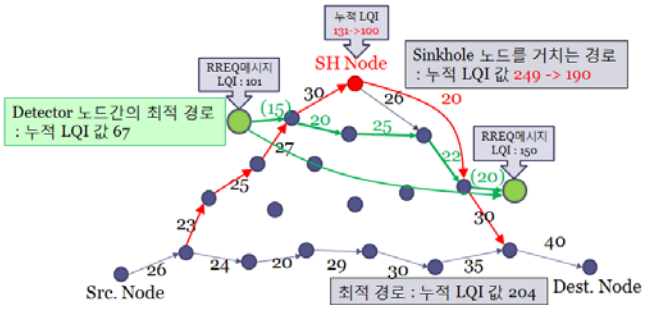

그림 3 싱크홀 공격의 탐지 예

4. 결 론

본 논문에서는 LQI에 기반한 라우팅을 수행하는 무선 센서 네트워크에서 싱크홀 공격을 탐지하기 위한 방법을 제시하였다. 초기 설정 단계에서는 싱크홀 공격의 탐지를 위한 기본 정보들을 구성하였다. 일반 노드들은 각 이웃 노드간의 최적 경로 비용을 파악하였고 탐지 노드들은 이웃 노드와의 경로 비용뿐만 아니라 근접한 탐지 노드와의 최적 경로 및 경로 비용을 파악하였다. 탐지 단계에서는 싱크홀 공격 노드가 취할 수 있는 방법에 따라 두 가지 공격 탐지 방법을 제시하였다. 경로 비용의 위조를 감지하기 위하여 탐지 노드를 사용하였고, 최소 Neighbor LQI table을 참조하여 비정상적으로 강한 신호로 데이터를 전송하는 것을 탐지 할 수 있었다. 제안한 공격 탐지 기법은 싱크홀이 발생한 후 탐지를 하는 기존의 탐지 기법과는 다르게 싱크홀 공격을 시도하는 과정에서 탐지하는 방법을 적용함으로써 기존의 방법이 가진 한계를 극복하고 더욱 다양한 환경에서 적용이 가능하도록 하였다.

5. 참고문헌

[1] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Proc. First IEEE Int’l Workshop on Sensor Network Protocols and Applications, May 2003.

[2] IEEE Computer Society, “Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, IEEE 802.15.4 Standard, 2006.

[3] Edith C. H. Ngai, Jiangchuan Liu, Michael R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", ICC 2006, Proceedings of the IEEE International Conference on Communications, Istanbul, Turkey, 2006.