무선 센서 네트워크 환경에서 링크 품질에 기반한 라우팅에 대한 효과적인 싱크홀 공격 탐지 기법

(A Effective Sinkhole Attack Detection Mechanism for LQI based Routing in WSN)

최 병 구 † 조 응 준 ††
(Byung Goo Choi) (Eung Jun Cho)
홍 충 선 †††
(Choong Seon Hong)

요 약 본 논문에서는 무선 센서 네트워크 환경에서 싱크홀 공격을 탐지할 수 있는 방안을 제시한다. 싱크홀 공격은 네트워크를 흐르는 패킷들이 공격자를 통과하도록 하는 공격이다. 따라서 이는 다양한 공격으로 확장될 수 있다. 본 논문에서는 링크 품질 지표에 기반한 라우팅을 수행하는 네트워크에서 싱크홀 공격 방법들을 분석하고 각 공격 방법에 따라 공격을 탐지하기 위한 방안들을 제시한다. 제안하는 싱크홀 공격 탐지 방법은 링크 품질 지표에 기반한 동적 라우팅 프로토콜을 사용하는 모든 센서 네트워크에 적용할 수 있으며 소수의 공격 탐지 노드를 사용하여 싱크홀 공격의 탐지가 가능함을 알 수 있다.

키워드 : 싱크홀, 공격 탐지, 링크 품질 지표, 무선 센서 네트워크, 동적 라우팅 프로토콜

Abstract In this paper, we propose a detection scheme for sinkhole attacks in wireless sensor networks. Sinkhole attack makes packets that flow network pass through attacker. So, Sinkhole attack can be extended to various kind of attacks. We analyze sinkhole attack methods in the networks that use LQI based routing. For the purpose of response to each attack method, we propose methods to detect attacks. Our scheme can work for those sensor networks which use LQI based dynamic routing protocol. And we show the detection of sinkhole attack can be achieved by using a few detector nodes.

Key words : Sinkhole, Attack detection, Link quality indicator, Wireless sensor network, Dynamic routing protocol

1. 서 론

무선 센서 네트워크는 미래의 유비쿼터스 환경에 기반이 될 중요한 기술이다. 센서 네트워크는 저비용으로 데이타의 수집 및 측정을 하는 응용들에 의해 폭넓게 이용될 수 있다. 이러한 센서 네트워크의 주된 이점들 중 하나는 스스로 네트워크를 구성할 수 있고 동적 라우팅 프로토콜을 사용할 수 있기 때문에 노드의 분포 및 설정이 용이하다는 점이다.

그러나 센서 네트워크는 무선 통신의 특성과 제한된 성능 및 자원으로 인해 여러 가지 공격에 노출되어 있다. 특히 라우팅 프로토콜의 경우도 공격에 노출되기 쉬우며 공격이 발생하면 최악의 경우 서비스 불능 상태가 될 수 있다. 하지만 유선 네트워크에서 사용되는 방어 기법들은 제한된 처리성능과 컴퓨팅 자원을 갖는 무선 센서 네트워크에서는 사용하기 어렵다.

무선 센서 네트워크에서 라우팅 공격의 대표적인 형태중의 하나는 싱크홀 공격이다[1]. 이 공격은 악의적인 노드가 자신을 Base Station이나 목적지 노드에 더 가까이 있다고 거짓 광고한다. 그 결과 많은 노드들이 데이타 트래픽을 악의적인 노드를 경유해서 보내게 된다. 따라서 악의적인 노드는 자신을 거치는 네트워크의 트래픽들을 조절할 수 있으며 더욱 손쉽게 제2의 공격을 수행할 수 있다. 그러므로 싱크홀 공격의 탐지는 안전한 무선 센서 네트워크를 구성하기 위한 중요한 연구 분야이다. 따라서 이 논문에서는 안전한 데이타 전송을 위해 싱크홀 공격을 탐지할 수 있는 방법을 제안하였다.

본 논문의 구성은 2장에서 관련연구를 설명하고, 3장에서 새로운 탐지기법을 제안한다. 4장에서는 제안한 탐지기법에 대한 성능평가 결과를 보이고 5장에서 결론을 내린다.

· 이 연구는 "2005년도 경희대학교 교원연구년 연구결과"와 "정보통신부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과(IITA-2008-(C1090-0801-0016))"로 수행되었음
· 이 논문은 2008 한국컴퓨터종합학술대회에서 '무선 센서 네트워크 환경에서 링크 품질 지표에 기반한 라우팅에 대한 싱크홀 공격 탐지 기법'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 경희대학교 컴퓨터공학과
bgchoi@khu.ac.kr
†† 정 회 원 : 경희대학교 컴퓨터공학과
ejcho@networking.khu.ac.kr
††† 종신회원 : 경희대학교 컴퓨터공학과 교수
cshong@khu.ac.kr

논문접수 : 2008년 8월 27일
심사완료 : 2008년 11월 16일

2. 관련연구

2.1 거리 백터 라우팅 프로토콜

거리 백터 라우팅 프로토콜은 홉카운트나 경로 지연, 대역폭 같은 요소들에 근거하여 최적의 경로를 선택하기 위해 자주 사용된다[2]. 이 논문에서는 최적의 경로를 선택하기 위한 요소로 링크 품질 지표(Link Quality Indicator, LQI)를 사용하는 라우팅 프로토콜을 다루도록 한다. 이러한 라우팅 프로토콜의 예는 6LowPAN의 거리 백터 라우팅 프로토콜로 제안되었던 LOAD 라우팅 프로토콜을 들 수 있다[3]. LOAD 라우팅 프로토콜은 AODV 라우팅 프로토콜을 간소화한 버전이지만 AODV와는 다르게 홉카운트가 아닌 LQI에 기반을 둔 라우팅을 수행한다.

2.2 링크 품질 지표(Link Quality Indicator)

링크 품질 지표는 전달 받은 패킷의 신호 세기나 품질을 나타낸다. 수신자의 신호 세기 측정 모듈을 사용하여 신호의 세기를 측정하고 측정된 값과 잡음의 비율로 링크 품질 지표를 결정한다. 링크 품질 지표는 각 수신 패킷마다 측정되며 이 값은 0×00~0×FF까지의 범위를 가지고 가장 높은 수치(0×FF)가 가장 좋은 신호 품질을 의미한다. 링크 품질 지표를 기반으로 링크비용을 계산하면 좋은 신호 품질은 낮은 경로비용으로 나타난다[4].

2.3 싱크홀 공격 분석

싱크홀 공격은 자신이 Base Station과 같은 중요한 노드 또는 목적지 노드로 향하는 가장 효율적인 경로인 것으로 가장하는 공격이다. 단지 하나의 싱크홀 노드가 존재하는 것만으로도 네트워크에 큰 악영향을 미칠 수 있다[1].

동적 라우팅 프로토콜의 경우 센서 노드들 사이의 경로 탐색과 유지를 네트워크의 상황에 따라 사용자의 개입 없이 자동적으로 수행하도록 설계되었다. 따라서 이러한 프로토콜의 경우 주기적이거나 또는 필요에 의해 네트워크 정보를 수집하고 그에 따라 라우팅 경로를 판단한다. 그러나 이러한 라우팅 프로토콜은 싱크홀 공격에 노출되어 공격당하기 쉽다. 아래에 나타난 그림 1은 싱크홀 공격이 발생할 경우의 네트워크 상태를 보여준다. 주변 노드의 데이타 트래픽이 싱크홀 노드를 거치기 때문에 싱크홀 노드가 다른 공격들을 수행할 경우 더욱 넓은 범위의 노드들이 공격에 노출되게 된다.

그림 1 싱크홀 공격의 예

2.4 홉카운트기반 라우팅에서의 싱크홀 공격 탐지 기법

홉카운트에 기반한 라우팅을 하는 네트워크에서 싱크홀 공격을 탐지하는 기법은 트리 라우팅을 수행하며 모든 센서 노드들이 주기적으로 BaseStation으로 데이타를 전송하는 환경을 가정한다[5].

싱크홀 공격이 이루어질 경우 싱크홀 노드가 취할 수 있는 대표적인 공격 방법이 Selective Forwarding이다[6]. Selective Forwarding은 악의적인 노드가 자신을 경유하는 패킷들의 일부를 고의적으로 전달하지 않음으로써 패킷을 손실시키는 공격이다. 이 공격이 발생할 경우 Base Station은 각 주기마다 데이타를 보고받지 못한 노드들의 목록을 작성한다. 이러한 노드가 특정 지역에서 나타날 경우 이 노드들이 위치한 지역의 모든 노드들로부터 Next-hop 정보를 모으고 이를 기반으로 네트워크 트리 구조를 구성하여 공격을 탐지한다. 그림 2를 예로 설명하면, 트리 라우팅을 수행하는 네트워크에서 특정 지역의 노드들이 데이타 손실이 일어난다면 그 지역 노드들의 최상위 트리에 위치한 노드가 싱크홀 공격 노드임을 추측할 수 있다.

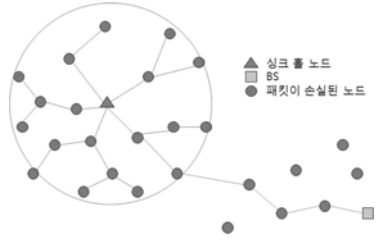


그림 2 홉카운트를 이용한 싱크홀 공격탐지기법

그러나 이 탐지 기법의 경우 공격 노드가 싱크홀 공격 이외에 Base Station이 공격 발생을 인지 가능한 공격(위의 경우에서는 Selective Forwarding)을 해야만 탐지과정을 수행한다는 단점이 있다. 다시 말해서 싱크홀 공격만 이루어지는 공격에서는 최상위의 노드를 찾아도 싱크홀 공격 여부를 판단할 기준이 모호해진다. 또한 공격이 발생하고 그것이 탐지되기 전까지 센서 노드들은 공격에 그대로 노출되게 된다.

2.5 LQI기반 라우팅에서의 싱크홀 공격 탐지 기법

LQI를 이용한 라우팅 환경에서 싱크홀 공격을 탐지하는 기존의 기법은 악의적인 노드가 route update 패킷을 위조한다고 가정한다[7]. 악의적인 노드가 싱크홀 공격을 하기 위해 자신의 LQI값을 최대로 광고하는 것과 동시에 공격 성공률을 높이기 위하여 주변의 노드와 그 부모노드간의 LQI를 거짓으로 낮추어 광고하는 것이다.

악의적인 노드가 route update 메시지의 Source 주소를 위조하여 광고했을 때 이를 수신한 노드들은 이 메

시지의 발신 노드가 자신의 이웃노드가 맞는지 여부와 자신의 주소가 도용당했는지 여부를 검사한다. 공격 발생이 탐지되었다면 각 노드들은 경고메시지에 자신의 이웃노드목록을 포함하여 브로드캐스트하며, 공격발생을 탐지한 노드들의 이웃 목록에 공통적으로 나타나는 노드가 싱크홀 노드로 판단하게 된다.

그러나 이 공격탐지 방법의 경우 악의적인 노드가 타 노드의 route update 메시지를 위조하는 것으로써 공격을 탐지한다. 이는 악의적인 노드가 공격 성공률이 떨어지더라도 자신의 링크 품질을 최대로 광고하는 방식만을 사용한다면 탐지할 수 없다.

3. 제안사항

3.1 가정 사항

본 논문에서는 다음과 같은 환경을 가정한다.

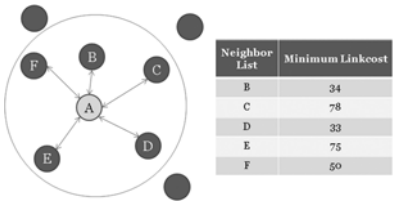
- 센서 노드는 다수의 일반 노드와 소수의 탐지 노드로 구성된다. 일반 노드 대 탐지 노드의 비율은 탐지율에 영향을 미치므로 성능 평가를 통해 적정한 비율을 찾아낼 필요가 있다.
- 탐지 노드들은 일반 노드보다 더 많은 연산을 수행하므로 그에 비례하여 더 많은 전원을 소모한다. 또한 서로 간의 전용의 링크 또는 채널을 이용하여 신뢰성 있는 데이타 전송을 할 수 있어야 한다. 이러한 조건을 충족하기 위해서 탐지노드는 일반 노드와는 다른 고성능의 H/W 자원, 대용량의 전원을 가진다고 가정한다.
- 탐지 노드들은 promiscuous 모드로 동작 가능하며 전파범위 내의 Routing Reply 메시지를 감시한다.
- 모든 노드는 고정되어 있어 이동하지 않는다.

이러한 환경은 이동성을 고려할 필요가 없고, 장기간 동안 안정적인 데이타 수집을 요구하는 환경에 적합하다고 할 수 있다. 예를 들어 안전 사고 예방을 위하여 각종 기반 시설들에 센서 네트워크를 이용할 경우를 들 수 있다.

3.2 네트워크 초기 설정 단계

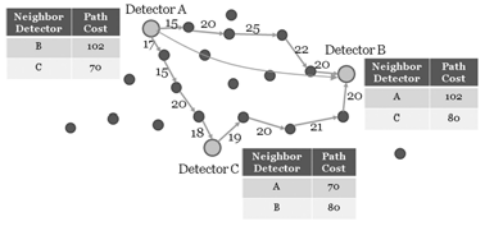
네트워크 초기 설정 단계에서 각 노드들은 이웃 노드들과의 최소링크비용을 계산한다. 각 노드들은 발신 가능한 범위 내에서 최대한 강한 신호를 이웃노드에게 보내고 신호를 수신한 노드는 측정된 링크 품질 지표에 따라 링크비용을 계산한다. 그리고 이전의 링크비용과 비교하여 더 작은 값을 유지한다. 이 과정을 충분히 반복하면 각 노드들은 그림 3과 같이 주변 노드들로부터의 최소링크비용을 도출할 수 있다. Minimum neighbor link cost table은 악의적인 노드가 인위적으로 매우 강한 신호를 보내어 링크비용을 낮추고 라우팅 경로를 변경하려는 공격을 탐지하는데 사용된다.

탐지 노드의 경우에는 위의 절차를 수행하며 주변의



Neighbor List	Minimum Linkcost
B	34
C	78
D	33
E	75
F	50

그림 3 Minimum neighbor link cost table의 예



Neighbor Detector	Path Cost
B	102
C	70

Neighbor Detector	Path Cost
A	102
C	80

Neighbor Detector	Path Cost
A	70
B	80

그림 4 탐지 노드 사이의 최소 경로 비용 예

탐지 노드들을 찾고 그때의 경로 비용(링크비용의 합)을 계산한다[8]. 이것은 악의적인 노드가 라우팅 제어 패킷의 경로 비용을 위조하여 싱크홀 공격을 수행하고자 할 때 공격 탐지를 위해 사용된다. 그림 4는 각 탐지 노드 사이의 최소 경로 비용을 기록한 예이다.

3.3 공격 탐지 과정

일반적으로 링크 품질 지표에 기반한 라우팅에서는 링크 품질 지표를 기반으로 링크 비용을 계산하고 이를 누적하여 최소의 값을 가지는 경로를 최적의 경로로 선택한다. 이러한 라우팅 환경에서 송신 노드와 수신 노드 사이의 최적 경로비용과 싱크홀 노드를 거치는 경우의 경로비용을 그림 5에 나타내었다. 일반적인 경로 탐색의 경우 최적 경로의 비용은 204이고 싱크홀 노드를 거치는 경로는 비용이 249가 되므로 경로 비용이 더 작은 최적 경로에 따라 패킷이 전송된다. 이때 악의적인 노드가 싱크홀 공격을 달성하기 위한 방법은 다음과 같다.

공격 방법 1 : Routing Request/Reply 패킷을 매우 강한 신호로 보내어 더 멀리 보내거나 수신 노드들이 더 좋은 품질의 링크로 인지하도록 하는 방법

공격 방법 2 : 송수신 노드 사이의 경로 탐색과정에서 전달되는 Routing Request/Reply 패킷 내의 누적된 링크비용을 더 작게 수정하는 방법

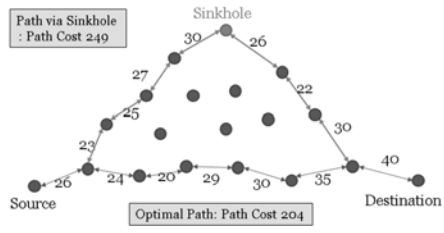


그림 5 송수신노드 사이의 최적 경로 비용

그림 6은 위와 같은 방법을 사용하여 공격을 수행하는 과정을 보여준다. 싱크홀 노드가 Routing Reply 패킷내의 누적된 링크비용을 131에서 100으로 위조하고 정상적인 출력보다 더 강한 신호로 메시지를 전달한 경우 경로 비용은 원래의 249가 아닌 201이 되어 최적 경로로 선택될 수 있다.

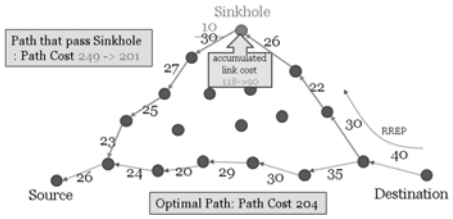


그림 6 싱크홀 공격 발생시의 경로 비용

이러한 공격을 탐지하기 위해서 다음의 두가지 방법이 사용가능하다.

공격 방법 1 : Routing Request/Reply 패킷을 매우 강한 신호로 보내어 링크 품질을 향상시키는 방법

대처 방안 1 : 싱크홀 노드가 Routing Request/Reply 메시지를 보낼 때 수신 노드에서는 Minimum Neighbor Link Cost Table을 참조하여 링크비용을 검사한다.

(수신 메시지의 링크비용) < (최소 링크 비용) - C (1)

여기서 C는 최소 링크 비용의 허용 오차 범위를 의미한다. 위의 식 (1)이 참이 되면 해당 메시지는 고의적으로 매우 강하게 전송된 것으로 판단하고 공격으로 판단한다.

공격 방법 2 : 송수신 노드 사이의 경로 탐색과정에서 전달되는 Routing Request/Reply 패킷 내의 누적 링크비용을 더 작게 수정하는 방법

대처 방안 2 : 싱크홀 노드가 Routing Request/Reply 메시지의 누적 링크비용을 위조하는 경우 신호세기 측정 방법으로는 탐지가 불가능하다. 이러한 공격의 경우 탐지 노드가 공격을 탐지하게 된다. 탐지 노드들은 자신의 전파범위내의 모든 Routing Reply 메시지를 감시한다. 브로드캐스트되는 Routing Request 패킷과 달리 Routing Reply 메시지는 유니캐스트로 전송되므로 경로 추적 및 공격탐지에 적합하다. 싱크홀 공격이 이루어지는 경우에도 해당 Routing Reply 메시지는 주변의 탐지 노드들에 수집된다.

(Routing Reply 패킷의 누적 링크 비용의 증가량) < *(탐지 노드간 경로 비용) - (탐지 노드와 Routing Reply를 검사한 노드사이의 경로 비용)* (2)

만약 이 식 (2)가 참이 된다면 최적의 경로보다 더 좋은 경로로 전송된 것을 의미하므로 이는 모순이다. 따라서 공격이 발생했다고 판단 할 수 있다.

그림 7의 예를 보면 두 탐지 노드 사이의 최적 경로 비용은 102가 된다. 그러나 Routing Reply 메시지가 수집된 노드와 탐지 노드간의 비용을 제외해야 하므로(I과 A, B와 II) 결과적으로 67이라는 값을 얻게 된다. 이 값과 Routing Reply 메시지의 누적 링크비용의 증가량인 30을 비교하면 Routing Reply 메시지가 최적의 경로보다 더 좋은 경로를 통해 전달되었다는 것을 알 수 있으나 이는 모순이다. 이런 경우 두 탐지 노드 사이에서 싱크홀 공격이 일어나고 있음을 판단할 수 있다.

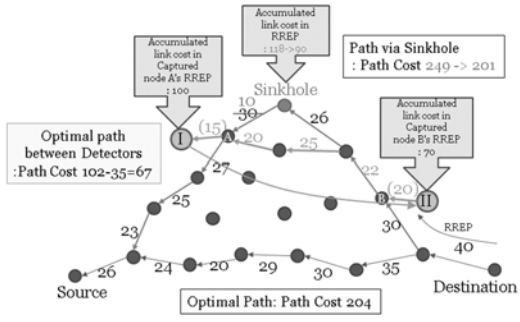


그림 7 싱크홀 공격의 탐지 예

4. 성능평가

제안한 공격 탐지 방법의 성능평가를 위해서 표 1과 같은 네트워크 환경을 가상으로 구성하였다.

그림 8은 싱크홀 노드가 Routing Request/Reply 패킷을 고의적으로 매우 강한 신호로 보내는 경우에 대한 공격 탐지 방법(식 (1))에서 사용된 허용오차범위 C값에 따른 False Positive 확률을 나타낸 것이다. 네트워크 초기 설정 단계에서 계산한 최소 링크비용을 기준으로 탐지단계에서 계산될 수 있는 링크비용의 분산도에 따라 5가지의 결과를 나타내었다. 또한 2.5절에서 제시한 싱크홀 공격 탐지 기법에서 공격 탐지율을 결정짓는 주요 인자인 평균 이웃 노드 개수에 따른 False Positive 확률과 비교하였다. (A)는 최악의 경우, (C)는 최상의

표 1 실험 환경

Parameter	Value
네트워크 넓이	100m × 100m
노드의 수	100
전송 범위	20m
전송 파워	5.85e-5
실험 반복 횟수	각 50회

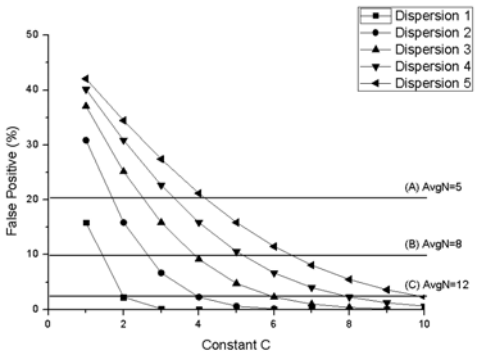


그림 8 허용 오차 범위 C에 따른 False Positive

경우이며 (B)는 본 성능평가의 환경과 가장 유사한 경우를 나타낸다.

그림 9에서는 싱크홀 노드가 Routing Reply 패킷을 위조하는 공격을 탐지하기 위한 대처방안 2에 대해서 노드 100개 당 탐지 노드의 숫자에 따른 공격 탐지율을 나타낸다. 또한 2.5절에서 제시한 공격 탐지 기법과 비교하였다. 제안하는 공격 탐지 방법은 Routing Reply 패킷이 싱크홀 노드에 의해 변조 되기 전, 후의 값을 수집할 수 있는 위치에 있어야 한다. 따라서 탐지 노드의 밀도가 높을수록 탐지율이 높아지게 된다. 아래의 결과 그래프에서 보이듯 탐지 노드의 개수가 20개일 때 약 70%, 30개가 넘으면 90%가 넘는 탐지율을 보여준다.

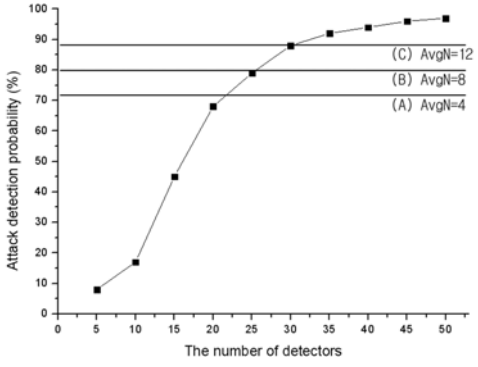


그림 9 탐지 노드의 수에 따른 공격 탐지율

5. 결 론

본 논문에서는 링크 품질 지표에 기반한 라우팅을 수행하는 무선 센서 네트워크에서 싱크홀 공격을 탐지하기 위한 방법을 제시하였다. 알고리즘은 초기 설정 단계와 탐지 단계로 나누어진다.

초기 설정 단계에서는 싱크홀 공격의 탐지를 위한 기본 정보들을 구성하였다. 일반 노드들은 각 이웃 노드간의 최적 링크 비용을 파악하였고 탐지 노드들은 이웃 노드와의 최적 링크 비용뿐만 아니라 근접한 탐지 노드와의 최적 경로 및 경로 비용을 파악하였다.

탐지 단계에서는 악의적인 노드가 취할 수 있는 두가지 싱크홀 공격 방법에 따라 각각의 탐지 방안을 제시하였다. Routing Reply 메시지 내의 경로 비용 위조를 탐지하기 위하여 탐지 노드를 사용하였고 Minimum Neighbor Link Cost table을 참조하여 비정상적으로 강한 신호로 데이타를 전송하는 공격을 탐지할 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 안전한 센서 네트워크를 구성하는데 기여할 수 있다. 특정 싱크홀 노드를 찾아내고 해당 노드를 네트워크에서 격리하는 방법은 앞으로 진행할 연구 사항이다.

참 고 문 헌

[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] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector Routing," RFC 3561, July 2003.

[3] K. Kim, S. Daniel Park, G. Montenegro, N. Kushalnagar, "6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD)," Internet-Draft (Expired), June 19, 2007.

[4] 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.

[5] Edith C. H. Ngai, Jiangchuan Liu, Michael R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," Computer Communications, Sept. 2007.

[6] B. Yu, B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," Proceedings of the Second International Workshop on Security in Systems and Networks (IPDPS 2006 Workshop), pp. 1-8, 2006.

[7] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks," ALGOSENSORS 2007, LNCS 4837, pp. 150-161, 2008.

[8] Ji-Hoon Yun, Il-Hwan Kim, Jae-Han Lim, and Seung-Woo Seo, "WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks," ICUCT 2006, LNCS 4412, pp. 200-209, 2007.