무선 센서 네트워크에서 훼손 감내하는 터널된 패킷 여과 기법

김 형 종*

요 약

무선 센서 네트워크에서 공격자는 한 위치에서 패킷을 획득하여 획득한 패킷을 재전송하는 공모 모드에게 터널하는 웜홀 공격을 가할 수 있다. 공격자는 이웃 발견 단계 동안에 웜홀 공격을 가할 수도 있으므로, 웜홀 공격은 라우팅 프로토콜에게 매우 위험하다. 웜홀의 전략적인 배치는 네트워크를 통한 통신에서의 심각한 붕괴를 가져올 수 있다. 본 논문은 센서 네트워크를 위한 훼손 감내하는 터널된 패킷 여과 기법을 소개한다. 제안 기법은 메시지의 홉 수와 메시지에 덧붙여진 암호화된 홉 수와의 비교를 통하여 홉 수가 조작된 메시지를 탐지할 수 있다. 제안 기법은 각 노드에 할당된 보안 정보의 양을 제안함으로써 훼손된 노드를 사용하는 웜홀 공격의 영향을 줄일 수 있다.

A Compromise-Resilient Tunneled Packet Filtering Method in Wireless Sensor Networks

Hyung-Jong Kim*

ABSTRACT

In wireless sensor networks, an adversary can launch the wormhole attacks, where a malicious node captures packets at one location and tunnels them to a colluding node, which retransmits them locally. The wormhole attacks are very dangerous against routing protocols since she might launch these attacks during neighbor discovery phase. A strategic placement of a wormhole can result in a significant breakdown in communication across the network. This paper presents a compromise-resilient tunneled packet filtering method for sensor networks. The proposed method can detect a tunneled message with hop count alteration by a comparison between the hop count of the message and one of the encrypted hop counts attached in the message. Since the proposed method limits the amount of security information assigned to each node, the impact of wormhole attacks using compromised nodes can be reduced.

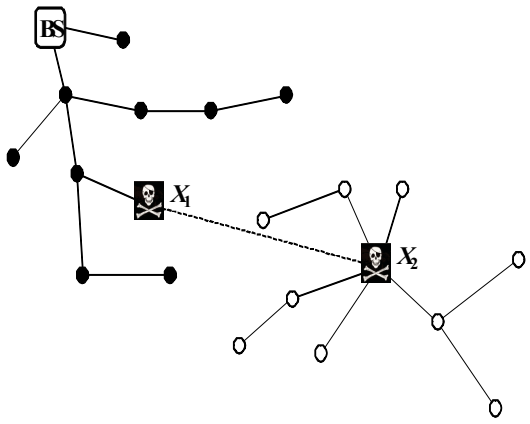
Key words : Wireless Sensor Networks, Wormhole Attacks, Node Compromising, Security

* 서울여자대학교 컴퓨터학부 전임강사

1. 서 론

무선 센서 네트워크(wireless sensor networks)는 주위 상황을 감시하는 수많은 작은 센서 노드와 감시 값을 수집하는 소수의 기지 노드(base stations)로 구성된다[1]. 센서 노드는 도청(eavesdropping)이 쉬운 무선 통신을 사용하므로 공격자는 손쉽게 웜홀(wormhole) 공격[2]을 네트워크에 가할 수 있다. 웜홀 공격에서는, 한 지점의 공격자 노드가 패킷을 획득하여 이를 다른 지점의 공모(collude) 노드에게 터널하며(tunnel), 공모 노드는 전달받은 패킷을 재전송한다. 공격자는 이웃 발견 단계(neighbor discovery phase)에서 웜홀 공격을 가할 수 있으므로, 웜홀 공격은 라우팅 프로토콜에게 매우 치명적이다[3]. 많은 라우팅 프로토콜에서, 노드는 방송 메시지의 첫 인스턴스를 보낸 이웃 노드와 라우팅 경로를 설정하고 해당 메시지의 이후 인스턴스는 무시한다. 그러므로 웜홀의 전략적 배치는 네트워크 전역에 걸친 통신 불능 사태를 야기할 수 있다[4]. (그림 1)은 웜홀 공격의 예를 보여준다. 공격자 노드 X_1은 패킷을 획득하여 점선의 빠른 링크(low-latency link)를 통하여 공모 노드인 X_2에게 터널하며, X_2는 이를 재전송한다. 채워진 원은 기지 노드와 연결된 온라인(online)노드를, 빈 원은 웜홀과 연결된 오프라인(offline) 노드를 나타낸다.

각 노드가 자신과 기지 노드와의 홉 수(hop count)를 어림할 수 있고 암호화를 사용한다면, 이러한 웜홀 공격으로 인한 피해를 줄일 수 있다. 공모 노드로 터널되어 재전송된 패킷의 홉 수와 실제 혹은 어림한 값과 크게 차이가 나기 때문이다[5]. 그러나 센서 네트워크의 많은 응용 분야에서, 센서 노드는 개방된 환경에 배포되므로 공격자는 노드를 물리적으로 포획하여 손쉽게 암호 키를 훼손(compromising)할 수 있다[6]. 앞서 설명한 거리 추측과 암호화는 이러한 훼손된 노드를 사용한 웜홀 공격으로부터 네트워크를 보호할 수 없다. 공격자는 훼손된 키를 사용하여 패킷의 홉 수를 조작할 수 있기 때문이다. 대부분의 기존 웜홀 탐지 기법[2, 4, 7]은 어떤 하나의 노드가 훼손된 경우에는 무력한 모습을 보인다.



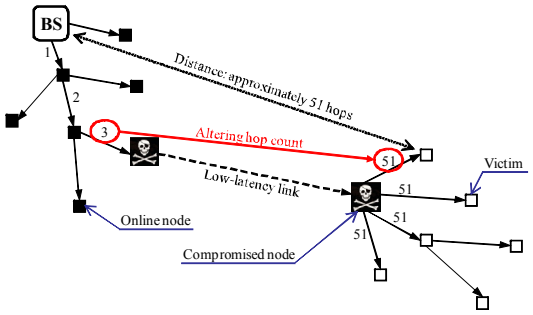
(그림 1) 웜홀 공격

본 논문에서는 센서 네트워크를 위한 훼손에 감내하는 터널된 패킷 여과 기법을 제안한다. 각 방송 메시지는 메시지의 홉 수 검증에 사용되는 몇 개의 암호화된 홉 수를 포함한다. 암호화된 홉 수는 메시지의 전파와 함께 전달 노드에 의해 갱신되므로, 암호화된 홉 수와 메시지의 홉 수간의 차이는 사전 정의된 범위 안에 들어야한다, 그러므로 홉 수가 조작되고 터널된 메시지를 탐지할 수 있다. 공격자는 몇 개의 노드를 훼손하여 암호화된 홉 수를 조작할 수도 있다. 그러나 제안 기법은 각 노드에 할당된 정보의 양을 제한하므로, 웜홀 공격은 훼손되지 않은 키를 가진 노드에게는 영향을 주지 못한다. 그러므로 제안 기법은 훼손 노드를 사용한 웜홀 공격의 피해를 줄일 수 있다.

논문의 구성은 다음과 같다. 제 2장에서는 훼손 노드들 사용한 웜홀 공격에 대하여 간단히 소개하며, 제 3장에서는 제안 기법을 상세히 설명한다. 제 4장에서는 시뮬레이션 결과를 검토하며, 제 5장에서 결론을 맺는다.

2. 훼손 노드들 사용한 웜홀 공격

일반적으로 센서 노드는 개방된 환경에 배포된 이후에 방치되므로 공격자가 노드를 물리적으로 포획할 수 있는 물리적 공격에 취약하다[6]. 웜홀 공격에 훼손된 노드가 사용되면, 홉 수 기반 거리 측정과 암호화만으로는 웜홀 공격의 피해를 줄일 수 없다. 공격자는 훼손된 노드의 암호 키를 사용하여 자유롭게 획득한 패킷의 내용을 조작할 수 있기 때문이다. (그림 2)는 훼손된 노드를 사용한 웜홀 공격의 예를 보여준다. 기지 노드와, 터널된 패킷을 재전송하는 공모 노드 주변의 노드간의 거리는 약 51홉이다. 공격자는 기지 노드 근처에서 획득한 방송 메시지의 홉 수를 훼손한 키로 조작하여 공모 노드에게 터널, 재전송하게 한다. 공모 노드 주변의 노드는 터널된 패킷의 홉 수가 추측한 값과 크게 다르지 않으므로 공모 노드와 라우팅 경로를 설정하게 된다. 공격자는 웜홀을 통해 선택적 전달(selective forwarding)이나 도청 등의 공격을 수행할 수 있다.



(그림 2) 훼손된 노드를 사용한 웜홀 공격

3. 터널된 패킷 탐지 기법

3.1 가정

본 논문에서는 수많은 노드들로 구성된 센서 네트워크를 고려한다. 센서 노드는 MICAz[8]와 같은 현 세대의 센서 노드들과 계산 능력, 통신 능력, 전원 공급 측면에서 유사하다. 노드는 키를 저장할 수백 바이트의 저장 공간을 가지고 있다. 각 노드는 자신과 기지 노드간의 홉 수를 알거나 추측할 수 있다. 그러므로 네트워크는 터널 후 재전송하는 간단한 웜홀 공격으로부터 보호된다. 비용 문제로 노드는 훼손에 저항하는(tamper-resistant) 하드웨어를 장착하지 않고 않다. 노드가 훼손되면 노드가 가지고 있는 모든 정보가 훼손된다고 가정한다. 그러나 기지 노드는 훼손되지 않는다. 감지 지역의 효율적 감시를 위하여 추가적인 노드가 배포될 수 있다. 공격자는 훼손된 노드를 사용하여 웜홀 공격을 수행할 수 있다. 이웃 발견 단계에서 기지 노드는 이웃 발견 메시지를 방송하며 메시지는 네트워크를 통해 퍼져나간다. 이웃 발견 메시지는 디렉티드 디퓨전(directed diffusion)[9]에서처럼 사용자가 요구하거나, 노드의 추가 배포 등으로 네트워크의 위상(topology) 변화가 발생할 때 시작된다.

3.2 개요

제안 기법에서 기지 노드는 전역 키 풀(global key pool)을 관리한다. 모든 노드는 배포되기 전에 전역 키 풀에서 임의로 선택된 몇 개의 키를 저장한다. 각 방송 메시지는 하나의 홉 수와 전역 키 풀의 키를 사용하여 암호화된 몇 개의 홉 수를 포함한다. 암호화된 홉 수는 메시지가 네트워크를 통해 전파될 때 방문 노드들에 의해 갱신된다. 메시지의 홉 수는 평문으로 저장되므로, 공격자는 획득한 메시지의 홉 수를 조작할 수 있다. 그러나 조작된 홉 수와 전달 노드가 갱신한 암호화된 홉 수간의 차이가 크기 때문에 조작된 메시지는 탐지 가능하다. 공격자는 훼손한 노드들 사용하여 암호화된 홉 수를 조적할 수도 있다. 그러나 조작된 메시지는 오직 훼손된 키와 동일한 키를 가진 노드만

이 수락(accept)하므로, 웜홀 공격의 피해를 줄일 수 있다.

3.3 전역 키 풀 및 메시지 형식

통계적 전달 중 여과 기법(statistical en-route filtering scheme)[10]과 유사하게, 기지 노드는 p개의 중복되지 않는 구획 $\{P_i,\ 0 \le i < p\}$로 나뉘고, k개의 키 $\{K_i,\ 0 \le i < k\}$로 구성된 전역 키 풀을 관리한다. 각 키는 고유의 키 색인(index)을 가진다. 배포 전에, 모든 센서 노드는 전역 키 풀 중 임의로 선택된 한 구획에서 n개($n < k/p$)의 키를 해당 키 색인과 함께 적재한다.

각 방송 메시지는 메시지의 홉 수 h_0과 다음과 같은 p개의 서로 다른 구획의 키 색인 및 해당 키로 암호화한 홉 수를 포함한다.

$$\left\{i_1, E_{i_1}(h_1), i_2, E_{i_2}(h_2), \cdots, i_p, E_{i_p}(h_p)\right\} \qquad (1)$$

여기서 $i_1, \cdots, i_p$는 키 색인을 나타내며, $h_1, \cdots, h_p$는 홉 수, $E_i(d)$는 키 K_i를 사용한 데이터 d의 암호화이다.

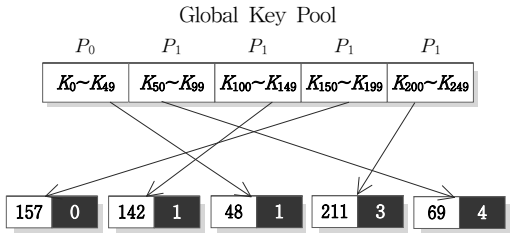
p개의 암호화된 홉 수는 암호화되지 않은 홉 수인 h_0이 조작되었는지를 검사하기 위하여 사용된다. h_0의 값과 메시지의 암호화된 홉 수는 메시지의 전파와 함께 전달 노드들에의해 갱신된다. 그러므로 이들 간의 차이는 사전 정의된 범위(predefined range) 내에 들어야만 한다. 공격자는 손쉽게 h_0을 조작할 수 있지만, 훼손된 노드 없이는 암호화된 홉 수를 조작할 수 없다. 그러므로 h_0이 조작된 메시지는 탐지될 수 있다. 공격자는 훼손된 노드를 사용하여 웜홀 공격을 가할 수 있다. 그러나 홉 수는 서로 다른 구획의 키로 암호화되어있고, 하나의 노드는 전역 키 풀의 한 구획에서 일부의 키만을 적재한다. 그러므로 하나의 노드는 암호화된 홉 수 중 하나 또는 미만(즉, 0개의 암호화된 홉 수)의 값만을 복호화할 수 있다. 따라서 메시지의 모든 암호화된 홉 수를 조작하기 위해서는 p개 이상의 노드들 훼손해야만 한다. 실세계에서 이러한 많은 수의 노드를 발각되지 않고 훼손하는 것은 대단히 어려운 일이다. 웜홀 공격에 소수의 노드를 사용하는 경우에는, 공격의 피해를 줄일 수 있다. 공격자는 훼손되지 않은 키를 가진 노드들에게 영향을 미칠 수 없기 때문이다.

3.4 메시지 준비

기지 노드는 메시지를 방송하기 전에 서로 다른 구획에 속한 p개의 키를 임의로 선택하여 다음과 같이 키 색인 및 암호화된 홉 수 목록을 생성한다.

$$\left\{i_1, E_{i_1}(0), i_2, E_{i_2}(1), \cdots, i_p, E_{i_p}(p-1)\right\} \qquad (2)$$

그리고 기지 노드는 생성한 목록을 메시지에 덧붙이고 h_0를 p-1로 초기화하여 메시지를 방송한다.



{157, $E_{157}(0)$, 142, $E_{142}(1)$, 48, $E_{48}(2)$, 211, $E_{211}(3)$, 69, $E_{69}(4)$}

(그림 3) 메시지 준비

(그림 3)과 같이 5개의 구획으로 나뉜 250개의 키를 가진 전역 키 풀이 있다고 가정해보자(즉, k = 250, p = 5). 메시지를 방송하기 위하여 기지 노드는 서로 다른 구획에 속하는 임의의 5개의 키 $\{K_{157}, K_{142}, K_{48}, K_{211}, K_{69}\}$를 선택하여 키 색인과 암호화된 홉 수 목록 {157, $E_{157}(0)$, 142, $E_{142}(1)$, 48, $E_{48}(2)$, 211, $E_{211}(3)$, 69, $E_{69}(4)$}를 준비한다. 기지 노드는 준비한 목록을 메시지에 덧붙이고 h_0을 4로 초기화한 후, 메시지를 방송한다.

3.5 전달 중 검증(En-Route Verification)

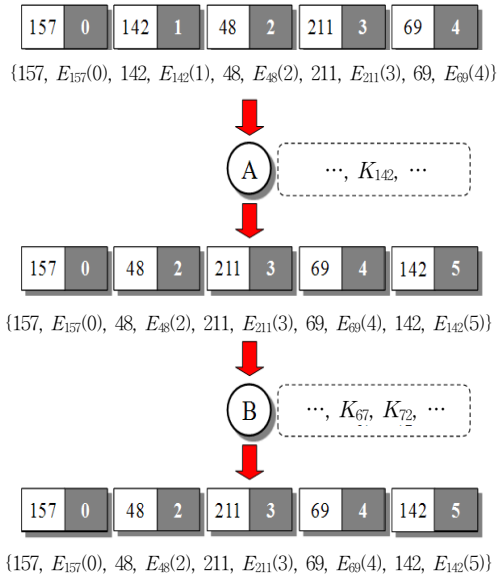
전달 노드가 방송 메시지를 받으면, 노드는 먼저 메시지에 서로 다른 구획에 속한 p개의 키 색인과 암호화된 홉 수가 있는지를 확인한다. p개보다 적은 수의 색인이나, 이보다 적은 암호화된 홉 수, 또는 동일 구획에서 두 개 이상의 색인이 있는 메시지는 폐기한다. 만약 노드가 p개의 색인이 가리키는 키 중 어떠한 것도 가지지 않은 경우에는 메시지를 수락한다. 그리고 h_0을 1 증가(즉, $h_0 \leftarrow h_0 + 1$) 시킨 후에 메시지를 방송한다.

만약 노드가 p개의 키 중 i번째($1 \le i \le p$) 키를 가졌다면, i번째의 암호화된 홉 수를 해당 키로 복호화하고, 복호화한 홉 수 h_i와 h_0과 비교한다. 메시지는 아래 조건을 만족하는 경우에만 수락된다.

$$h_0 - h_i + i - p \le r \tag{3}$$

여기서 r은 사전 정의된 오차 범위이다. 메시지 수락 후에 노드는 h_0을 증가시키고 i번째 키 색인과 암호화된 홉 수를 제거한다. 그리고 h_0을 해당 키로 암호화한 후에 키 색인과 암호화된 홉 수를 목록의 맨 끝에 덧붙인다. 마지막으로 노드는 메시지를 방송한다.

예를 들어, (그림 4)의 노드 A가 (그림 3)에서 방송한 메시지를 받았을 때, 노드는 먼저 메시지에 서로 다른 구획의 5개의 키 색인과 암호화된 홉 수가 있는지 확인한다. 노드는 목록 중 2번째 색인이 가리키는 K_{142}를 가지고 있으므로 노드는 두 번째 암호화된 홉 수 $E_{142}(1)$를 복호화할 수 있다. (4 - 1 + 2 - 5) = 0 ≤ r이라면 메시지는 수락될 것이다. 메시지 수락 후에, 노드는 h_0을 1 증가시킨다(그러므로, $h_0 = 5$). 그리고 {142, $E_{142}(1)$}를 목록에서 제거하고 목록의 끝에 {142, $E_{142}(5)$}를 추가한다. 그리고 노드는 목록 {157, $E_{157}(0)$, 48, $E_{48}(2)$, 211, $E_{211}(3)$, 69, $E_{69}(4)$, 142, $E_{142}(5)$}를 포함하는 메시지를 방송한다. 노드 B가 노드 A가 방송한 메시지를 받으면, 역시 5개의 키 색인과 암호화된 홉 수가 있는지 확인한다. 노드는 메시지에 포함된 키 색인이 가리키는 키 중 어떠한 키도 소유하고 있지 않으므로, 메시지는 수락된다. 노드는 h_0을 증가시키고 메시지를 방송한다.



(그림 4) 전달 중 검증

식 (3)에서 r값의 선택은 네트워크의 보안 강도와 가용성을 결정한다. 작은 r값은 몇몇 노드를 기지 노드와 웜홀 모두와 연결되지 않게 만들 수 있다. 반면에 큰 r값은 웜홀 공격의 피해를 증가시킬 수 있다. 그러므로 네트워크 설계자는 주의 깊게 r의 값을 결정해야만 한다. 이론적으로 r의 값은 다음 식으로 계산할 수 있다.

$$r = \frac{k}{p.n} \tag{4}$$

실세계에서 식 (4)의 r값은 다수의 오프라인 노드를 유발하므로, r값은 이보다 훨씬 커야한다.

3.6 전달 중 여과(En-Route Filtering)

어떠한 노드도 아직 훼손되지 않은 경우에도 공격자는 웜홀 공격을 가하기 위하여 메시지의 h_0을 조작할 수 있다. 조작의 결과로 h_0은 조작되지 않은(암호화된) 홉 수와 크게 차이가 날 것이다. 그러므로 키 색인이 가리키는 키 중 하나를 소유한 노드는 메시지를 폐기할 것이다. 반면에, 키 색인이 가리키는 키 중 하나도 가지지 않은 노드는 메시지를 수락하여 웜홀 공격에 영향 받을 것이다. v를 제안 기법이 적용되지 않은 네트워크에서의 웜홀 희생 노드의 수라할 때, 제안 기법이 적용된 네트워크에서의 희생 노드의 수 v_{TPF}는 다음 식으로 계산할 수 있다.

$$v_{TPF} = v\frac{k + p \cdot n}{k} \tag{5}$$

실세계에서는 h_0이 조작된 메시지는 메시지를 검증할 수 있는 노드의 장벽을 넘어 전파될 수 없으므로, v_{TPF}F는 식 (5)의 값보다 상당히 작을 것이다.

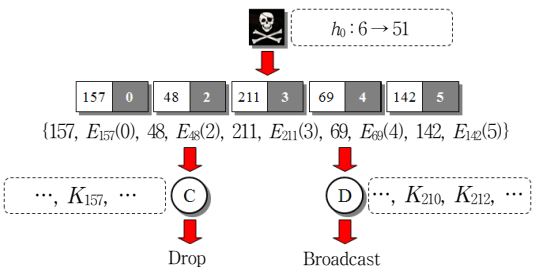
공격자가 (그림 4)의 노드 B가 방송한 메시지를 기지 노드로부터 약 50홉 정도 떨어진 공모노드에게 터널한다고 생각해보자. (그림 5)와 같이 메시지의 h_0 값은 51로 조작되어 재전송될 것이다. 노드 C는 첫 번째 키 색인이 가리키는 키 K_{157}을 가지고 있으므로, 첫 번째 암호화된 홉 수를 복호화할 수 있다. $(51-0+1-5)=47 \leq r$이라면 노드는 메시지를 폐기할 것이다. 반면에 노드 D는 5개의 키 중 어떠한 키도 가지고 있지 않으므로 메시지를 수락할 것이다. 그러므로 이 노드는 희생 노드가 될 것이다.

공격자는 메시지의 암호화된 홉 수를 조작하기 위하여 몇몇 노드를 훼손할 수 있다. 그러나 모든 홉 수를 조작하기 위해서는 다수의 노드를 훼손해야만 한다. 실세계에서 발각되지 않으면서 이러한 많은 수의 노드를 훼손하는 것은 대단히 어려운 일이다. 그러므로 웜홀 공격은 소수의 훼손된 노드를 사용하여 수행될 것이다. 이런 경우, 소수의 암호화된 홉 수가 조작될 수 있지만, 메시지는 훼손된 키를 가진 노드만이 수락할 것이다. 반면에 다른 노드들은 메시지를 여과할 것이다. 그러므로 웜홀 공격에 따른 피해를 감소시킬 수 있다. a를 공격자에 의해 조작된 암호화된 홉 수의 수라하면, 제안 기법을 적용한 네트워크에서의 희생 노드의 수 v_{TPF}는 다음 식으로 계산할 수 있다.

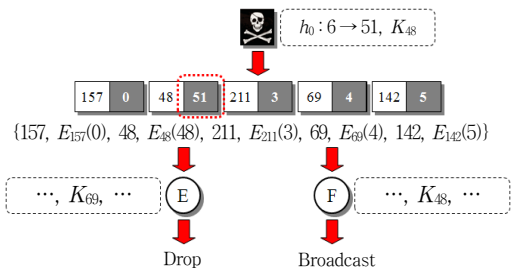
$$v_{TPF} = v\frac{k + (a-p)n}{k} \tag{6}$$

그러나 앞서 언급한 바와 같이, 실세계에서의 v_{TPF}는 이보다 훨씬 작을 것이다.

(그림 6)에서 공격자가 K_{48}을 훼손하여 (그림 4)의 노드 B가 방송한 메시지의 두 번째 암호화된 홉 수를 조작할 수 있다고 가정하자. 노드 F는 공격자에 의해 훼손된 키와 동일한 키를 가지고 있



(그림 5) 전달 중 여과(외부 공격자)



(그림 6) 전달 중 여과(내부 공격자)

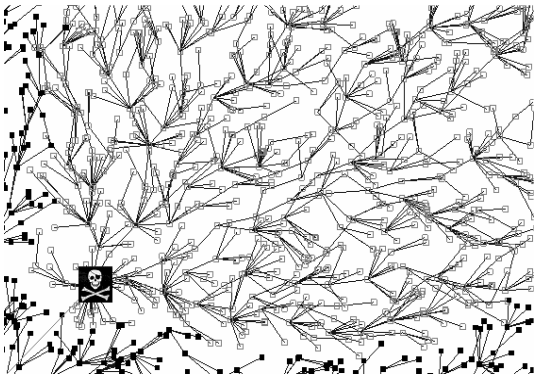
으므로 공격자가 방송한 메시지를 수락할 것이다. 반면에 노드 E는 4번째 홉 수를 복호화할 수 있으므로 메시지를 여과할 것이다.

4. 시뮬레이션 결과

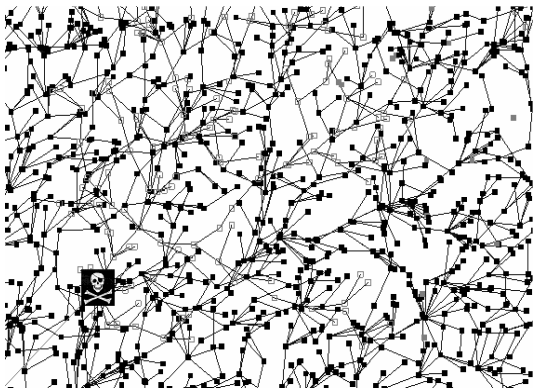
제안 기법의 효과를 보여주기 위하여 시뮬레이션을 통하여 제안 기법을 평가하였다. 센서 네트워크는 $1,000 \times 1,000m^2$의 지역 내에 균등하게 분포된 4,000개의 센서 노드로 구성된다. <표 1>은 k = 1,000, p = 10, n = 80, $2 \leq r \leq 14$일 때, 네트워크에서의 온라인 노드의 수, 희생 노드의 수, 오프라인 노드의 수, 그리고 피해 감소율(제안 기법이 미 적용된 네트워크에서의 희생 노드 수 대비)이다. 공격자는 하나의 암호화된 홉 수를 조작할 수 있다. 제안 기법에서의 웜홀 공격에 대한 피해 감소율은 r에 따라 변동하지만, 피해를 최대 80% 정도 감소시킬 수 있음을 알 수 있다 (그림 7)은 제안 기법이 미 적용된 네트워크에서의 웜홀 공격의 피해를 보여주는 화면이며, (그림 8)은 제안 기법이 적용된 네트워크에서의 피해를 보여주는 화면이다 채워진 사각형은 기지 노드와 연결된 온라인 노드이며, 빈 사각형은 웜홀과 연결된 희생 노드이다. 그림에서 알 수 있듯이 제안 기법은 모든 노드를 웜홀 공격으로부터 보호하지는 않지만, 희생되지 않은 노드를 통해 대부분의 지역을 커버하여 감시할 수 있음을 알 수 있다.

〈표 1〉 시뮬레이션 결과

노드 수		온라인	희생	오프라인	피해감소 (%)
미적용		2891	1109	0	0.0
제안 기법 적용	r=2	1340	382	2278	65.6
	r=4	2707	228	1066	79.6
	r=6	3229	244	527	78.0
	r=8	3535	238	227	78.5
	r=10	3704	229	67	79.4
	r=12	3139	694	167	37.4
	r=14	3129	726	145	34.5



(그림 7) 웜홀 공격의 영향(제안 기법 미적용)



(그림 8) 웜홀 공격의 영향(제안 기법 적용)

5. 결 론

본 논문에서는 무선 센서 네트워크에서 훼손 감내하는 터널된 패킷 여과 기법을 제안하였다. 제안 기법은 메시지 홉 수와 암호화된 홉 수의 비교를 통하여 터널된 메시지를 탐지할 수 있다. 제안 기법은 각 노드에 할당하는 보안 정보를 제한하여, 훼손된 노드를 사용한 웜홀 공격의 피해를 줄일 수 있다.

참 고 문 헌

[1] L. Buttyan, L. Dora, I. Vajda, “Statistical Wormhole Detection in Sensor Networks”, Lecture Notes in Computer Science, Vol. 3813, 2005.

[2] Y. Hu, A. Perrig, D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, Proceedings of INFOCOM, 2003.

[3] R. Kaissi, A. Kayssi, A. Chehab, Z. Dawy, “DAWWSEN: A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks”, Proceedings of IIT, 2005.

[4] J. Kwok, “A Wireless Protocol to Prevent Wormhole Attacks”, Thesis, University of Virginia, 2004.

[5] Z. Li, Y. Zhang, W. Trappe, and B. Nath, “Securing Wireless Localization : Living with Bad Guys”, Proceedings of DIMACS Workshop on Mobile and Wireless Security, 2004.

[6] B. Przydatek, D. Song, A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks”, Proceedings of SenSys, 2003.

[7] L. Hu., D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks”, Proceedings of NDSS, 2004.

[8] http://www.xbox.com/

[9] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, “Directed Diffusion for Wireless Sensor Networking”, IEEE/ACM Transactions on Networking, Vol. 11, No. 1, 2003.

[10] F. Ye, H. Luo, and S. Lu, “Statistical En-Route Filtering of Injected False Data in Sensor Networks”, IEEE Journal of Selected Areas in Communications, Vol. 23, No. 4, 2005.

김 형 종

1996년 성균관대학교 정보공학과 (공학사)

1998년 성균관대학교 대학원 정보공학과(공학석사)

2001년 성균관대학교 대학원 전기전자및컴퓨터학과 (공학박사)

2001년~2007년 한국정보보호진흥원 수석연구원

2004년~2006년 미국 카네기멜론대학 Visiting Researcher

2007년~현재 서울여자대학교 컴퓨터학부 전임강사