한국시뮬레이션학회 논문지
Vol. 18, No. 4, pp. 149-155 (2009. 12)

무선 센서 네트워크에서 웜홀 공격 방어기법의 에너지 효율향상을 위한 TTL 결정 기법

이선호[1] · 조대호[1†]

Determination Method of TTL for Improving Energy Efficiency of Wormhole Attack Defense Mechanism in WSN

Sun-Ho Lee · Tae-Ho Cho

ABSTRACT

Attacks in wireless sensor networks (WSN), are similar to the attacks in ad-hoc networks because there are deployed on a wireless environment. However existing security mechanism cannot apply to WSN, because it has limited resource and hostile environment. One of the typical attack in WSN is setting up wrong route that using wormhole. To overcome this threat, Ji-Hoon Yun et al. proposed WODEM (WOrmhole attack DEfense Mechanism) which can detect and counter with wormhole. In this scheme, it can detect and counter with wormhole attacks by comparing hop count and initial TTL (Time To Live) which is pre-defined. The selection of a initial TTL is important since it can provide a tradeoff between detection ability ratio and energy consumption. In this paper, we proposed a fuzzy rule-based system for TTL determination that can conserve energy, while it provides sufficient detection ratio in wormhole attack.

Key words : Wormhole, Wireless Sensor Network, Fuzzy Logic, Security

요 약

센서 네트워크에 대한 연구가 활발히 이루어지면서 센서 네트워크 보안에 대한 문제점이 많이 야기되고 있다. 무선 센서 네트워크에 대한 공격은 무선이라는 환경 때문에 애드 혹 네트워크와 유사하게 이루어진다. 그러나 애드 혹 네트워크의 보안 메커니즘은 센서 네트워크에서의 노드들이 훨씬 제한된 자원을 가지므로 그대로 적용할 수 없기 때문에 새로운 연구들을 필요로 한다. 무선 센서 네트워크에 대한 대표적인 공격방법중의 하나가 웜홀을 이용한 잘못된 경로의 설정이다. 웜홀 공격을 통해 전달되는 패킷은 도청당하거나 파괴될 수 있다. 이에 대한 대응 기법으로 Ji-Hoon Yun 등이 무선 센서 네트워크 환경에서 웜홀 공격을 탐지하고 대응하려 WODEM(WOrmhole attack DEfense Mechanism)이란 메커니즘을 제시했다. 이 기법에서는 웜홀에 대한 탐지 및 대응을 위해 홉 카운트와 처음에 미리 정해둔 TTL(Time To Live)을 비교하고 있다. TTL에 따라 탐지율과 에너지 소비에 큰 영향이 있게 되므로 TTL의 결정이 매우 중요하다. 본 논문에서는 충분한 웜홀 탐지율을 제공하면서 에너지를 보존할 수 있는 TTL을 퍼지로직을 통해 결정한다.

주요어 : 웜홀, 무선 센서 네트워크, 퍼지로직, 보안

* 이 논문 또는 저서는 2008년 정부(교육과학기술부)의 재원으로 한국 학술 진흥재단의 지원을 받아 수행된 연구임 (KRF-2008-313-D00827)

2009년 9월 24일 접수, 2009년 12월 18일 채택

[1] 성균관대학교 정보통신공학부
주 저 자 : 이선호
교신저자 : 조대호
E-mail; sunholee@ece.skku.ac.kr

1. 서 론

저 비용, 저 전력, 탐지, 계산 그리고 무선통신 능력을 가진 소형노드들의 발전은 전자공학의 진보와 더불어 센서 네트워크의 개발을 가능하게 한다.[1] 무선 센서 네트워크는 주변 환경 정보를 수집할 수 있는 감지 기능과, 정보처리 기능, 무선 통신 기능을 가지고 있는 소형 센서 노드(sensor node)들과 감지한 정보들의 집중국 역할과 사용자와 노드간의 게이트웨이 역할을 하는 베이스 스테이션(BS: base station)으로 구성된다. 기본적으로 센서 노드들은 감지한 주변 환경 정보를 베이스 스테이션으로 전달하고, 베이스 스테이션은 인터넷과 같은 기존 통신 인프라를 통하여 사용자에게 해당 정보를 제공한다.[2] 이런 센서 네트워크는 전례가 없는 수준의 다양한 응용을 가능하게 할 것으로 기대되고 있다.

하지만 많은 센서 네트워크 응용분야에서 센서 노드들이 개방된 환경에 배치되기 때문에, 공격자에 의한 물리적인 공격에 취약하다.[3] 이중 무선 센서 네트워크 라우팅에 대한 공격으로는 하나의 노드가 여러 식별자를 갖고 다중 노드임을 가장하는 Sybil 공격[4]과 악의적인 두 노드가 공모하여 라우팅 경로를 조작하는 경우, 데이터들이 악의적인 노드를 지나가도록하는 웜홀 공격 등이 있다.

웜홀 공격은 메시지가 공격자가 포획한 노드를 지나가게 되면 공격자는 이 메시지를 도청, 위조 또는 삭제함으로써 중요한 메시지의 내용을 가져가거나 메시지를 제대로 전달하지 못하게 하여 네트워크에 심각한 피해를 줄 수 있다. [4]에서는 이러한 다양한 공격 유형과 이를 극복하기 위한 대처방안에 대하여 기술하여 놓았다.

이러한 공격 중 웜홀의 탐지 및 대응을 위해 센서네트워크에서의 다양한 탐지기법들[4-7]이 제안되었다. Yoon 등 [7]이 제안한 WODEM(WOrmhole attack DEfense Mechanism)은 AODV 프로토콜 기반[8]의 기법으로써 메시지가 발생하면 최소한의 검증 패킷을 전송해 웜홀이 존재하는지를 원천노드와 목적노드간의 거리를 이용해 최소 홉 카운트와 비교해 탐색한다. 탐색결과 웜홀이 탐지되면 대응을 위해 TTL(Time To Live; 이하 TTL)를 이용해 하나씩 TTL을 늘려가면서 다음 노드로의 전송 홉 카운트와 실제 전송 카운트(TTL)를 비교하여 웜홀이 탐지된 경우 이웃 노드들의 리스트에서 공격노드를 제거하는 방식으로 대응한다. TTL을 1부터 증가시켜서 웜홀 노드를 찾다보면 TTL을 하나씩 증가시켜서 공격노드를 탐지하기 때문에 공격노드를 찾기 위해 패킷을 계속 주고받게 되기 때문에 많은 전력이 소모된다.

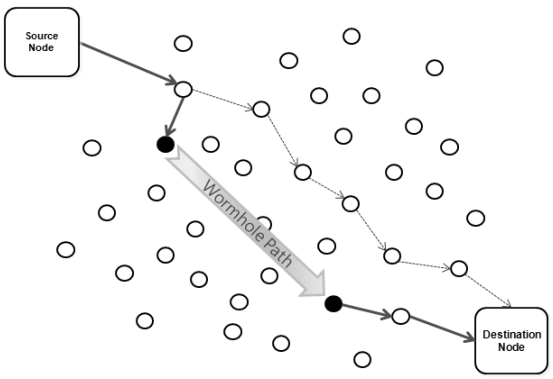


그림 1. 센서 네트워크에서의 웜홀 공격

본 논문에서는 WODEM에 퍼지로직을 적용하여 에너지 효율 향상을 위한 TTL 값을 결정하는 기법을 제안한다. 퍼지로직을 통해 노드의 밀도, 노드들의 잔여 에너지, 이벤트 발생 노드까지의 거리를 고려하여 홉 카운트 상으로 멀리 떨어져 있는 웜홀을 탐지하기 위하여 쓸데없는 에너지를 낭비하지 않는 TTL 값을 결정한다.

2. 웜홀 공격 방어 기법

WODEM(WOrmhole attack DEfense Mechanism; 이하 WODEM)은 이벤트 발생 시 노드와 노드 간에 통신을 위한 경로를 설정할 때 미리 인증 패킷을 보내 웜홀이 있는지를 탐지하고 탐지가 됐을 때에는 거리 당 최소 홉 수와 실제 홉 카운트를 비교해 웜홀 노드를 찾고 그 웜홀 노드를 이웃노드 리스트에서 삭제할 수 있다. WODEM은 아래와 같은 방법으로 웜홀을 탐지, 대응한다.

2.1 Detector scanning

탐지 노드 검색 단계에서는 탐지 시작 노드가 다른 한 탐지 노드를 검색하고 채널의 특성을 측정한다. 비밀리에 이루어지는 통신인 관계로 이 부분의 통신은 무선 센서 네트워크를 이루는 다른 노드들과는 다른 방식으로 통신을 한다. 그러므로 탐지 노드 검색 단계에서의 탐지 노드들 간의 통신은 웜홀이 있더라도 웜홀을 통과하지 않는다. 탐지 시작 노드(본 논문에서는 원천 노드로 표기; S)는 TTL 값 1을 가진 탐지 패킷을 방송한다. 탐지 패킷에는 원천 노드의 위치 L_s 와 전송 파워 레벨 P_t 정보를 가지고 있다. 원천노드는 두 개 이상의 응답 탐지 노드(본 논문에서는 목적 노드로 표기; R)로부터 응답이 올 때까지 전송파워 Δ_p를 증가시키며 계속 전송을 반복한다. 응답

패킷은 탐지 패킷의 P_t와 목적 노드의 위치 L_r를 포함하고 있다. 응답 패킷을 통해 원천 노드는 패킷 손실 모델에서 가져온 아래의 식에 따라 두 채널에서의 패킷 손실 지수 n과 상수 k를 계산할 수 있다.

$$P_t = k \times |L_s - L_r|^n \quad (1)$$

식 (1)의 계산 결과로 두 개의 탐지된 목적 노드 중에 에너지소비와 처리 시간이 낮은 노드를 목적노드로 결정하게 된다.

2.2 Wormhole detection

웜홀 탐지 단계에서는 원천 노드와 목적 노드 사이에 웜홀이 존재하는지를 체크한다. 원천 노드의 위치를 L_S, 목적 노드의 위치를 L_R, 원천 노드부터 목적노드까지의 홉 카운트를 H_{SR}이라고 하면, 웜홀이 없는 한 식 (2)의 부등식이 성립해야 한다.

$$H_{SR} \geq \min\{H_{SR}\} = \left[\frac{|L_S - L_R|}{r}\right] \quad (2)$$

오른쪽 항은 S와 R사이에서 이룰 수 있는 최소한의 홉 수이다. 원천 노드는 보통의 전송범위 r과 함께 L_S와 H_{SR}를 가진 탐지 패킷을 전송한다. 여기서 TTL 값은 목적노드가 패킷을 받기에 충분한 크기로 정한다. 목적 노드가 탐지 패킷을 받았을 때 식 (2)의 부등식을 통해 웜홀이 있는지 없는지를 확인한다. 웜홀이 탐지되면 보수 단계로 넘어가게 된다.

반면에 탐지 패킷이 웜홀로 들어간 뒤 소멸되는 경우가 생길 수 있는데 그래서 목적노드는 탐지 패킷을 수신했다는 것을 웜홀 존재 여부에 상관없이 원천노드에 알려야 한다. 패킷이 제한시간 안에 도착하지 않으면 탐지 패킷을 재전송하게 된다. 재전송이 계속되게 되면 손실률이 계속 증가하게 되고 결국 프로토콜 상에서 패킷 송신을 못하게 한다.

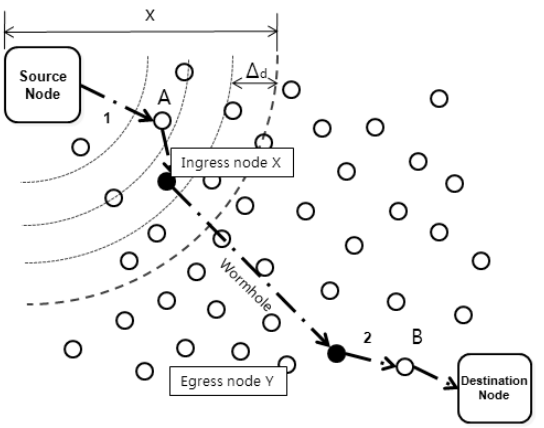


그림 2. WODEM 동작 과정

2.3 Neighbor-list repair

보수 단계에서는 원천 노드와 목적 노드가 결정되고 웜홀이 탐지 되었으면 각각의 이웃 노드들의 리스트에서 웜홀로 인해 인식되는 노드를 지워야 한다. 그림 2를 예를 들면 A와 B노드를 찾았으면 A의 이웃노드에서 B를 지우고 B의 이웃노드에서 A를 지워야 한다.

원천 노드는 처음의 전송범위 r과 TTL 1을 가지고 탐지 패킷을 전송함으로써 보수를 시작한다. 탐지 패킷은 L_S와 전송에 상응하는 전송 범위, 처음의 TTL을 포함하고 있다. 원천 노드는 Δ_d를 한 단계씩 증가시키는 방법으로 탐지 패킷이 목적노드에 직접 도달할 때까지 전송을 반복한다. 전송범위 안에 노드가 없어서 응답을 못 받게 되면 전송 범위는 재설정되고 TTL을 1 증가시킨다.

탐지 패킷이 목적노드에 도달하게 되면 목적노드는 아래의 식 (3)을 통해 패킷이 웜홀을 통과하였는지 검사한다.

$$(Initial\ TTL) \geq \min\{H_{SR}\} \quad (3)$$

식 (3)의 부등식이 성립하지 않는다면 패킷은 웜홀을 통과해 온 것이므로 마지막 노드를 이웃노드 목록에서 삭제하게 된다. $\min\{H_{SR}\}$은 아래의 식 (4)에 의해 구해질 수 있다.

$$\min\{H_{SR}\} = \left[\frac{|L_S - L_R| - R}{r}\right] + 1 \quad (4)$$

R은 탐지패킷이 전송되어서 일치했을 때의 원천 노드의 전송 범위이다.

웜홀 노드가 이웃노드에서 지워졌을 지라도 원천 노드와 목적 노드 사이의 모든 경로가 웜홀이 없다고 검색될 때까지 웜홀 탐지 단계를 반복하게 된다.

3. 제안기법

3.1 동기

WODEM은 웜홀을 발견하기위해 탐지노드를 찾는 등 여러 절차를 거쳐 웜홀을 탐지한다. 웜홀이 발견되면 이

웃노드에서 웜홀 노드를 제거하기 위해 TTL을 1부터 놓고 응답 메시지를 받고 TTL을 하나씩 증가시킨다.

무선 센서 네트워크의 센서들은 전력이 충분하지 않고 제한되어 있기 때문에 이 반복된 작업은 극도의 에너지 소모를 유발시키게 된다. 그래서 이 반복된 작업을 줄이기 위해 노드들의 밀도, 남은 전력량, 원천노드와 목적노드 간의 거리를 고려하여 퍼지로직을 적용하기로 하였다. 퍼지 기반 규칙 시스템은 오직 참과 거짓만을 선택할 수 있는 디지털 장치의 특성을 보안하기 위한 기법으로 IF-THEN 규칙을 통하여 명확하게 이분화(二分化)되지 않는 상황에서 적절한 결과 값을 도출해내기 위한 방법 중 하나이다. 본 논문에서 제안된 기법에서는 배포된 노드들의 밀도, 노드들의 잔여 에너지, 탐지노드 사이의 거리를 입력 값으로 도출된 TTL 값에 가지고 웜홀을 탐지하는 WODEM의 과정을 실행하게 된다.

그림 3은 제안된 기법의 실행과정을 보여준다. 웜홀이 존재했을 시 1, 2, 3 의 순서로 메시지가 전달되다가 웜홀을 통해서 4로 넘어가게 된다. 이때 청색 점선이 이론상의 전파거리 증가도를 나타내므로 메시지가 웜톨을 통해 전파될 경우 실제 메시지 위치와 이론상 메시지의 위치를 비교해서 웜홀을 탐지할 수 있다.

제안기법에서는 웜홀을 탐지하기위해 거리를 한단계씩 증가시켜 비교하는 WODEM의 방식에 초기 거리를 밀도와 잔여에너지 원천노드와 목전노드간의 거리를 이용하여 퍼지로직을 통하여 계산한 Aggressiveness TTL 값을 사용하여 전파거리 증가도를 미리 적당한 값으로 결정해 놓고 비교를 시작하므로써 불필요한 에너지 소모를 줄였다.

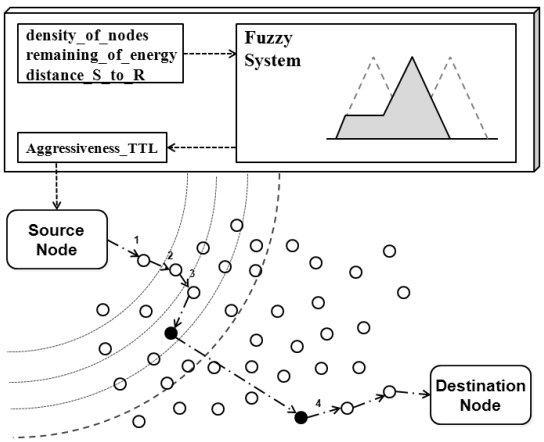


그림 3. TTL 결정 후 전파과정

3.2 가정

본 논문에서 제안한 기법에서는 다음과 같은 가정을 가지고 있다.

네트워크는 많은 수의 센서 노드들과 몇몇의 원천노드나 목적노드 같은 탐지노드, 고성능의 BS로 구성된다. BS는 전체 노드의 정보를 파악하여 기록해 두고, 탐지노드는 위치정보 시스템을 탑재해 그들의 위치를 인식하고 있다.[8] 또한 BS와 탐지노드는 보통의 센서노드보다 많은 전력량과 처리 능력을 가진다.

3.3 TTL 결정을 위한 퍼지 로직의 적용

3.3.1 TTL 결정을 위한 결정 요소들

BS는 원천 노드와 목적 노드의 주변 노드들과 미리 가지고 있는 노드들의 정보를 통하여 TTL을 결정한다. BS는 노드가 배치될 때 지역에 따른 배치 범위와 노드의 수를 고려하여 밀도 값을 계산한다. 또한 원천 노드와 목적노드 사이의 노드들에 대한 전력량 정보를 이용해 남은 에너지를 계산한다. 그리고 탐지 노드 검색 단계에서 두 탐지노드 들을 결정한 후 탐지노드들 간의 거리를 구한다. 이 세 가지 값을 가지고 퍼지 로직에 대입하여 적절한 TTL을 구한다.

노드들의 밀도는 네트워크를 구성하는 노드들의 단위 면적당 분포도로 이 값이 높아질 경우 노드들의 거리가 가깝다는 것을 의미하므로 TTL을 결정할 때 중요한 참고 값으로 쓰이게 된다.

또한 잔여 에너지량은 분포되어 있는 노드들의 에너지량을 측정해서 에너지에 여유가 있다면 좀더 세밀하게 검사를 하여 보안강도를 높이도록 TTL값을 작게 잡아줄 수도 있고 에너지의 여유가 없다면 TTL값을 가능한 한 크게 주어 적은 반복으로 웜홀을 탐지해낼 수 있다.

탐지노드들 간의 거리를 사용하는 이유는 거리가 멀수록 웜홀이 존재할 수 있는 공간이 커지게 되므로 가까운 경우보다 웜홀을 탐지하기 위한 TTL값에 변화가 있어야 하기 때문이다..

3.3.2 퍼지로직의 입, 출력 파라미터

- 입력 파라미터

density_of_nodes
= {Very_Low, Low, Middle, High, Very_High}
remaining_energy = {Small, Medium, Much}
distance_S_to_D
= {Very_Short, Short, Middle, Long, Very_Long}

• 출력 파라미터

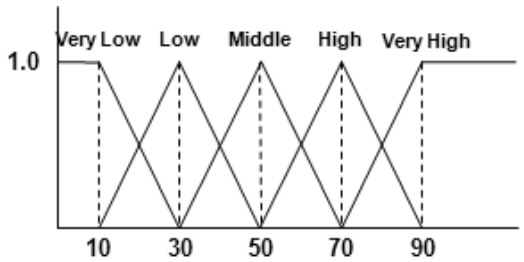
Aggressiveness_TTL

= {Very_Small, Small, Medium, Large, Very_Large}

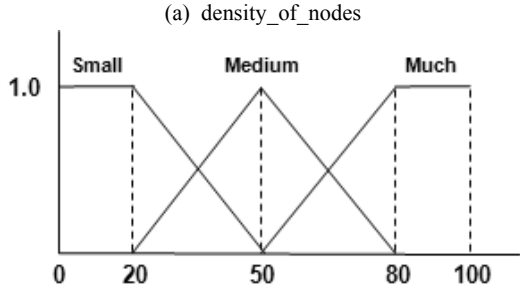
3.3.3 멤버십 함수

그림 4의 (a) ~ (c)는 퍼지규칙에 사용된 입력 멤버십 함수를 나타낸다. 각 파라미터들은 0~100사이의 값으로

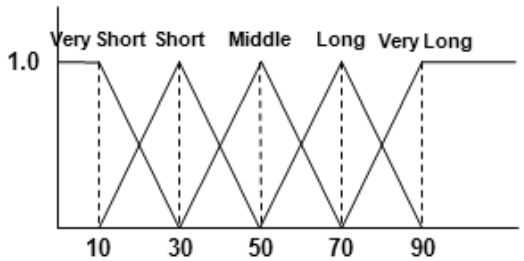
• 입력 멤버십 함수



(a) density_of_nodes

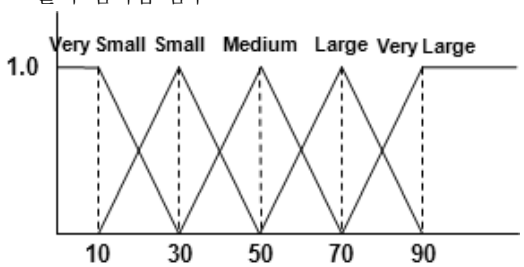


(b) remaining_energy



(c) distance_S_to_D

• 출력 멤버십 함수



(d) Aggressiveness_TTL

그림 4.

나타내어 명시된 룰에 따라 출력 값을 계산한다.

그림 4의 (d)는 퍼지규칙을 통해 도출된 TTL 값의 멤버십함수를 나타낸다. 출력된 값은 0~100사이의 값으로 결정되고 이 값은 아래의 계산식을 통해 탐지노드 사이의 홉 수에 비례해 TTL값을 정하게 된다.

$$TTL = h_{SD} \times \frac{Agg\,TTL}{100} \tag{5}$$

식 (5)에서 h_{SD}는 원천노드와 목적노드 사이의 노드의 개수이다. 원천노드와 목적노드 사이의 노드의 개수에 0~100 까지의 값으로 나오는 결과값을 100분율로 계산해 곱해주어 TTL의 값을 구하게 된다

3.3.4 퍼지 로직

퍼지로직은 세 가지 입력 값을 가지고 조합하여 적절한 결과 값이 나오도록 시뮬레이션을 통한 튜닝과정을 거쳐 결정되었다[9-11]. 아래는 몇 가지 퍼지규칙을 예로 들었다.

RULE 5: IF Very_High AND Medium AND Very_Long THEN Very_Large;

RULE 7: IF Very_High AND Medium AND Middle THEN Large;

RULE 18: IF High AND Much AND Short THEN Medium;

RULE 33: IF Middle AND Much AND Short THEN Small;

RULE 64: IF Very_Low AND Much AND Very_Short THEN Very_Small;

4. 시뮬레이션 결과

제안된 기법의 효과를 보이기 위하여 제안된 기법을 WODEM과 시뮬레이션을 통하여 비교하였다. 이 시뮬레이션은 1000m×400m의 평지라고 가정한 환경에서 100개의 노드로 구성된 네트워크를 통해 구성되었다. 각 노드는 한 바이트 당 송/수신에 16.25μJ/12.5μJ을 소비한다.

그림 5에서는 여러 환경에서 메시지(패킷)의 전달성공 확률이다. X축은 메시지가 웜홀에 빠져 손실되는 확률이고 Y축은 메지시의 전송 성공 확률이다. 그림에서 보듯이, WODEM의 라우팅 프로토콜인 AODV로만 구성된 네트워크(채워진 다이아몬드)에서는 웜홀에 걸려 메시지

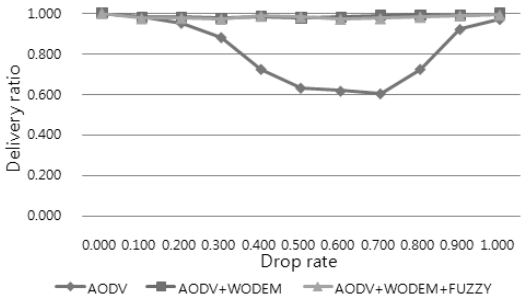


그림 5. 제안된 환경에서의 전달 성공 확률

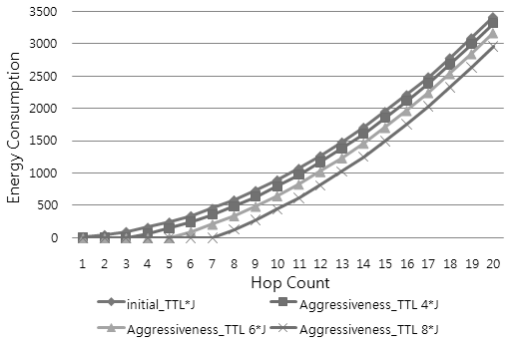


그림 6. TTL의 변화에 따른 송신에너지 소비

를 손실할 확률이 40% 가까이 나타났지만 WODEM(채워진 사각형)과 제안된 기법(채워진 삼각형)에서는 거의 완벽하게 웜홀을 탐지해 낼 수 있었다. 제안기법이 기존의 기법과 동등한 탐지율을 보임으로써 에너지 효율을 높이면서 보안강도는 유지하는 것을 볼 수 있다.

그림 6는 퍼지이론을 통해 도출한 Aggressiveness TTL의 변화에 따른 누적 송신에너지 소비를 보여준다. X축은 메시지가 전송된 홉 의 수를 나타내었고 Y축은 누적 에너지 소비량을 나타내었다. WODEM에서 사용하는 initial TTL은 항상 1부터 시작되어서 처음부터 에너지 소모가 있는 반면에 제안된 기법에서의 TTL은 퍼지를 통해 초기 값을 가지고 시작하므로 그에 따른 에너지 소모를 막을 수 있었다. 채워진 사각형은 퍼지로직에 따라 Aggressiveness TTL 값이 4로 정해졌을 경우 에너지 소모량이다. WODEM의 웜홀 탐지 로직을 수행하기위한 TTL 값이 증가되었으므로 증가된 만큼의 에너지소모가 절약되는 모습을 볼 수 있다. Aggressiveness TTL값이 6일 경우(채워진 삼각형)와 8일 경우(가위 표)를 보면 시작 TTL값이 증가되어 더 많은 에너지를 절약할 수 있는 것을 볼 수 있다. 보여준 시뮬레이션 이외에도 퍼지 결과 값에 따라 Aggressiveness TTL 값이 크게 나오는 경우 더 많은 에너지를 절약할 수 있다.

5. 결 론

본 논문에서는 웜홀 탐지 대응 기법의 하나인 WODEM (WOrmhole attack DEfense Mechanism)의 동작 과정을 분석하였다. WODEM은 웜홀을 탐지하기위해 탐지노드들을 찾고 탐지노드들사이의 패킷 전송을 통하여 웜홀의 존재여부를 탐지하고 TTL을 이용한 단계별 검색으로 웜홀을 탐지해 이웃노드 리스트에서 제거하는 방법을 사용한다. 동작 과정에 의해 탐지를 하면 여러 차례 반복되는 방식 때문에 불필요한 에너지 소모가 많이 일어나게 된다. 무선 센서 네트워크에서의 노드들은 작고 유한한 에너지를 가지기 때문에 에너지 소모를 줄이는 방법이 항상 중요하게 다루어져 왔다. 본 논문에서는 WODEM에서 웜홀을 탐지한 후 이웃 노드 목록에서 웜홀을 제거하기위해 단계별로 이루어지는 탐지 과정에서의 TTL의 값을 노드의 밀도, 남은 에너지, 탐지노드들 간의 거리를 고려해 1이 아닌 적당한 수로 주어 불필요한 반복을 줄여 에너지 소모를 줄이는 기법을 제안하고, 제안된 기법의 효과를 시뮬레이션을 통하여 보았다. 앞으로의 과제는 본 논문에서 제안한 기법에서 탐지율을 높이면서 더 높은 에너지 효율을 위한 고려사항을 찾아보고 적용하는 연구를 수행할 것이다.

참 고 문 헌

1. I.F. Akyldiz, W. Su, Y. Sankarasubramaniam, E. Cayirci., “A Survey on Sensor Networks”, IEEE Wireless Communication Magazine, Vol. 40, No. 8, pp. 102-116, 2002.
2. J.N. Al-Karaki, A.E. Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication Magazine, Vol. 11, No. 6, pp. 6-28, 2004.
3. Przydatdek, B. Song, D. and Perrig, A. (2003), “SIA: Secure Information Aggregation in Sensor Networks”, ACM, in Proc. of SenSys, pp. 255-265.
4. C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. 1st IEEE Int”l., Wksp. Sensor Network Protocols and Applications, May 2003.
5. Y.-C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc

Networks," Proc. 22nd Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2003), IEEE Press, 2003, pp. 1976-1986.
6. J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack," in ICNP, 2006.
7. J.-H. Yun, I.-H. Kim, J.-H. Lim, and S.-W. Seo. WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks. In Ubiquitous Convergence Technology(ICUCT 2006), pp. 200-209. LNCS 4412, 2007.
8. Charles E. Perkins: Ad hoc On-Demand Distance Vector AODV) Routing, RFC 3561, IETF, July 2003.
9. S.J. Lee, H.Y. Lee and T.H. Cho, "A Threshold Determining Method for the Dynamic Filtering in Wireless Sensor Networks Based on Fuzzy Logic", International Journal of Computer Science and Network Security, Vol. 8, No. 4, pp. 155-159, Apr. 2008.
10. S.J. Lee and T.H. Cho, "An En-route Filtering Scheme Based on Priority as determined by the Fuzzy rule-based system", International Journal of Computer Science and Network Security, Vol. 9, No. 7, pp. 46-50, July. 2009.
11. H.Y. Lee and T.H. Cho, "Fuzzy-Based Path Selection Method for Improving the Detection of False Reports in Sensor Networks", IEICE Transactions on Information and Systems, Vol. E92-D, No. 8, pp. 1574-1576, Aug. 2009.

이 선 호 (sunholee@ece.skku.ac.kr)
2009 경원대학교 인터넷미디어학부 학사
2009~현재 성균관대학교 정보통신공학부 석사

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 인공 지능, 정보 보안

조 대 호 (taecho@ece.skku.ac.kr)
1983 성균관대학교 전자공학과 학사
1987 Univ. of Alabama 전자공학과 석사
1993 Univ. of Arizona 전자 및 컴퓨터공학과 박사
1995~현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 지능 시스템, 모델링 방법론