한국시뮬레이션학회 논문지
Vol. 19, No. 2, pp. 73-80 (2010. 6)

# 선택적 전달 공격 탐지기법에서의 인증 메시지 전달 홉 수 제어기법

이상진[1] · 김종현 · 조대호[1†]

# Control Method for the Number of Travel Hops for the ACK Packets in Selective Forwarding Detection Scheme

Sang Jin Lee · Jong Hyun Kim · Tae Ho Cho

**ABSTRACT**

A wireless sensor network which is deployed in hostile environment can be easily compromised by attackers. The selective forwarding attack can jam the packet or drop a sensitive packet such as the movement of the enemy on data flow path through the compromised node. Xiao, Yu and Gao proposed the checkpoint-based multi-hop acknowledgement scheme(CHEMAS). In CHEMAS, each path node enable to be the checkpoint node according to the pre-defined probability and then can detect the area where the selective forwarding attacks is generated through the checkpoint nodes. In this scheme, the number of hops is very important because this parameter may trade off between energy conservation and detection capacity. In this paper, we used the fuzzy rule system to determine adaptive threshold value which is the number of hops for the ACK packets. In every period, the base station determines threshold value while using fuzzy logic. The energy level, the number of compromised node, and the distance to each node from base station are used to determine threshold value in fuzzy logic.

**Key words :** Wireless sensor network, Selective forwarding forwarding attacks, CHEMAS, ACK_TTL

**요 약**

무선 센서 네트워크는 다양한 응용분야에서, 개방된 환경에 배치되어지므로, 공격자에게 손쉽게 노출된다는 취약점을 가지고 있다. 선택적 전달 공격(Selective Forwarding Attack)은 센서 네트워크에서 발생할 수 있는 공격중의 하나로 공격자는 훼손된 노드를 통하여 전장지역에서의 적의 움직임등과 같이 중요한 정보의 기지노드까지 정상적인 전달을 차단하여 감시자의 원활한 탐지를 어렵게 한다. Xiao, Yu 그리고 Gao는 이와 같은 위협에 대한 대안으로 선택적 전달 공격 탐지기법(checkpoint-based multi-hop acknowledgement scheme; 이하 CHEMAS)를 제안하였다. CHEMAS에서 전달경로 상에 노드들은 미리 정해진 확률에 따라 감시 노드(checkpoint)로 선택되어지며 이 감시 노드들을 통해 공격 발생 지역을 탐지할 수 있다. 해당 기법에서 인증 패킷 전달 홉 수는 시스템 상에서 탐지율과 에너지 효율 사이에서 트레이드 오프 관계에 있으므로 매우 중요한 요소이다. 본 논문에서는 보안 강도를 충분히 유지하면서, 에너지 효율성 또한 제공할 수 있는 경계 값 선택을 위해 퍼지 규칙 시스템을 적용하였다. 기지노드는 퍼지 규칙 시스템을 이용하여 매 주기마다 에너지 레벨과 훼손된 노드 수 그리고 기지노드로부터의 거리를 고려하여 상황에 맞는 적절한 경계 값을 결정한다.

**주요어 :** 무선 센서 네트워크, 선택적 전달 공격, CHEMAS, ACK_TTL

## 1. 서 론

기술의 진보로 인해 무선 센서 네트워크는 다양한 분야에서 사용될 것으로 예상되어진다. 기본적으로 개방된 환경에 배치된 무선 센서네트워크는 자원적 측면과 환경적 측면에서 제약사항을 가지므로, 다양한 공격에 노출될

*이 논문 또는 저서는 2008년 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(KRF-2008-313-D00827).
2010년 1월 19일 접수, 2010년 4월 30일 채택
[1] 성균관대학교 전지전기컴퓨터공학과
주 저 자 : 이상진
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

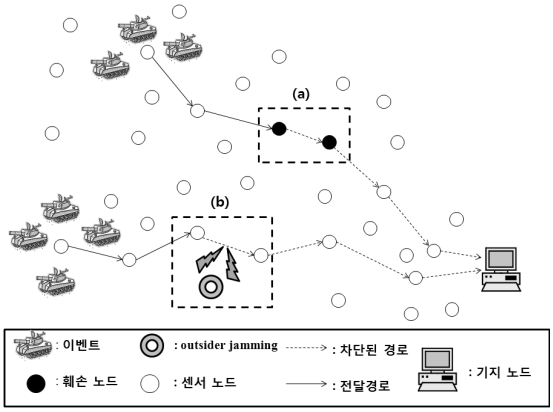


**그림 1.** 선택적 전달 공격

수 있다는 취약점을 가지고 있다[1]. 그림 1에서 볼 수 있듯이 공격자는 훼손된 노드나 외부의 전자 기기를 이용하여 선택적 전달 공격을 발생할 수 있다. 선택적 전달 공격을 통해 공격자는 이벤트 메시지의 배포를 방해하게 되며, 이는 감시자와 이벤트 발생 지역의 사이의 정보 고립 문제를 발생시키게 된다[2-3].

선택적 전달 공격의 탐지를 위해 Xiao 등은 선택적 전달 공격 탐지기법(checkpoint-based multi-hop acknowledgement scheme; 이하 CHEMAS)을 제안하였다[2]. CHEMAS는 선택적 전달 공격 탐지를 위해 이벤트(event), 인증(ack), 경보(alert) 등의 세 가지 패킷을 이용한다. 각 경로상의 노드들은 미리 정해진 확률에 따라 감시 노드로서 선택되어진다. 해당 노드들이 이웃노드로부터 이벤트 패킷을 전달받게 되면 이벤트 패킷을 받아 응답으로 인증 패킷을 생성하여 이벤트 발생노드로 해당 패킷을 전송하게 된다. 이때 인증 패킷은 미리 정해진 배포 홉 수(Time To Live; 이하 TTL) 만큼 전달 되어진다. CHEMAS에서 TTL은 에너지 효율과 보안 강도 사이에서 트레이드 오프하게 된다. 일반적으로 무선 센서네트워크는 일반 네트워크에 비해 자원적 측면이 매우 취약하며 잦은 위상변화[11]를 가지므로 고정적인 TTL은 해당 환경에서 부적합하다. 예를 들어 높은 강도의 탐지를 위해 높은 TTL 값을 설정할 경 우 충분한 탐지율을 제공할 수 있는 대신 탐지과정에서 과도한 에너지 소모를 발생하게 되어 결과적으로 네트워크 수명을 단축시키게 된다. 반대로 에너지 효율을 위해 TTL을 낮게 설정할 경우 자칫 보안 프로토콜 동작이 제대로 작동하지 않게 되어 탐지기능을 상실하게 된다는 문제점을 가지게 된다. 본 논문에서는 충분한 보안강도를 제공하면서 에너지 효율성 또한 제공할 수 있는 동적인 TTL의 선택기법을 제안하였다. 2장에서는 탐지 대상이 되는 공격 모델에 대한 설명과 제안기법의 기반이 되는 CHEMAS에 대한 간략한 설명을 할 것이며, 3장에서는 제안기법에 대한 동작과정, 4장에서는 제안 기법의 효율성을 검증하기 위한 시뮬레이션 결과 및 분석, 끝으로 5장에서는 결론 및 향후 과제에 대해서 언급할 것이다.

## 2. 관련 기술

### 2.1 공격모델

무선 센서 네트워크에서 각 센서노드들은 작은 메모리 공간, 한정적인 에너지, 연산력 제약등의 한정된 자원을 가지므로, 공격자는 허위보고서 주입 공격, 웜홀 공격, 헬로우 플러딩 공격, 위치배치 공격등과 같은 다양한 공격들이 가능하게 된다[1]. 본 논문에서는 다양한 공격들 중 하나인 선택적 전달 공격을 고려하고자 한다. 해당 공격은 평상시에는 정상 노드와 같이 행동하지만 사용자가 반드시 받아야하는 중요 정보의 경우 전달 경로 상의 중간 부분에서 차단함으로써 사용자의 혼란을 유발시킨다. 예를 들어, 전장지역 내에서의 탱크의 움직임, 미사일 감지 등과 같은 중요정보를 전달 경로 상에서 차단함으로써 기지노드까지의 전달을 방해하게 된다. 무선 센서네트워크 상에서의 공격자는 훼손된 노드를 통한 내부자 공격(inside attack) (그림 1(a)) 또는 정상 노드사이의 통신 채널에 대한 전파교란 공격을 가하는 외부자 공격(outside attack) (그림 1(b))등의 두 가지 형태로 공격을 시도 할 수 있다.

### 2.2 선택적 전달 공격 탐지기법(CHEMAS)

선택적 전달 공격은 사용자가 반드시 받아야할 정보의 배포를 차단함으로써, 해당 지역과 유저간의 의사소통을 고립시킨다는 문제점을 가지고 있다[3]. 선택적 전달 공격에 대한 탐지 기법중 하나인 CHEMAS는 미리 정해진 확률에 따라 감시 노드들을 선택한다. 감시 노드들은 이벤트 보고서를 수신 및 방송 후 이에 대한 인증 메시지를 소스노드 방향으로 TTL 만큼 전달하게 된다(그림 2).

CHEMAS는 아래의 세 가지 패킷을 이용해서 선택적 전달 공격발생 지역을 탐지하게 된다.

**세 가지 패킷**

- 이벤트 패킷 : 이벤트 발생시 전달되는 패킷
  - DstID : 목적지 노드의 ID
  - SrcID : 이벤트 발생 노드의 ID

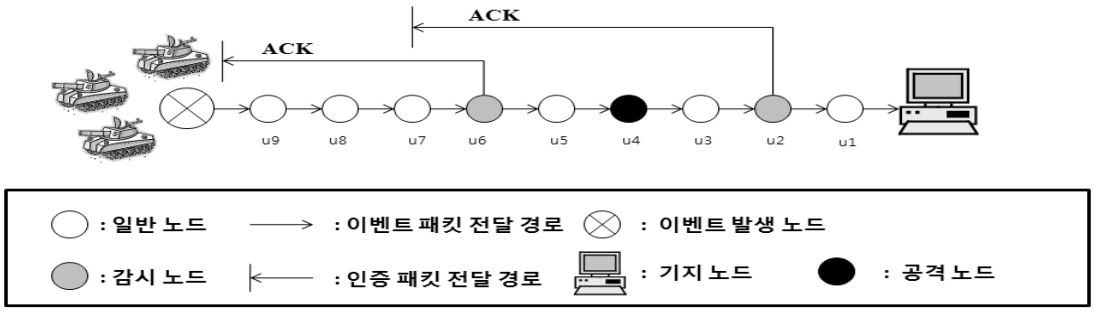


**그림 2.** 선택적 전달 공격 탐지기법

- Packet_ID : 이벤트 패킷의 ID
- Payload : 이벤트 내용
- Checkpoint_Seed : 감시 노드 생성을 위한 랜덤 값

- 인증 패킷 : 감시 노드가 이벤트 보고서 수신 시 이웃 노드에게 보내는 패킷
- PacketID : 전달된 이벤트 패킷의 ID
- NodeID : 인증 메시지 발생 노드 ID
- OHC_number, $MAC_{OHC}$ : 패킷 무결성 검증
- TTL : 인증 패킷이 전달되는 배포 범위를 제안하기 위한 값

- 경보 패킷 : 시간 내에 t개의 인증 패킷이 수신되지 않으면 발생하는 패킷
- DstID : 이벤트 발생노드의 ID
- SrcID : 경보 패킷을 발생한 노드의 ID
- Suspect_Node_ID : 공격자에게 훼손된 노드로 의심되는 노드 ID
- Lost_Packet_ID : 유실된 패킷의 ID
- MAC : 경보 패킷의 무결성 검증을 위한 코드

**감시 노드 선택**

각 경로상의 이벤트 전달 노드들은 이벤트 패킷의 checkpoint_seed을 각 노드들이가지고 있는 매핑함수(mapping function)을 통해 미리 정해진 확률로써 감시 노드로 선택되어진다.

**공격 탐지 과정**

공격 탐지 과정의 설명을 위해 아래와 같은 가정사항을 두었다.

- 노드 u4은 공격자로부터 훼손되어 중요정보를 차단한다.
- 경로 상의 감시 노드는 u2, u6이다.
- 인증 패킷의 전달 홉 수 제한은 2홉이다.

이벤트 발생 노드(이하; 소스 노드)는 중요정보를 감지하여 기지 노드로 이벤트 패킷을 방송한다. 이벤트 패킷을 수신한 각 노드들은 해당 패킷을 자신의 캐쉬 메모리에 저장 후 자신의 매핑함수에 이벤트 패킷의 checkpoint_seed값을 대입함으로써 자신이 감시 노드인지 아닌지를 판단한다. 그림 2에서 볼 수 있듯이 감시 노드로 선택된 u2, u6는 이벤트 패킷을 기지노드로 보냄과 동시에 인증 패킷을 생성하여 소스 노드 보낸다. 노드 u4은 공격자로부터 훼손되어 이벤트 패킷을 차단하고 있으므로 u5은 u2으로부터 어떤한 인증 패킷도 받을 수 없게 된다. 결국 u5은 의심되는 노드로써 u4을 보고하기 위해 경보 패킷을 발생한다.

## 3. 제안기법

### 3.1 동기

CHEMAS에서는 이벤트 보고서 전달시 경로 상에 정해진 확률으로 감시 노드들을 지정하게 된다. 감시 노드들은 이벤트 보고서를 기지노드 방향의 자신의 부모 노드들에게 전달 후 인증 패킷을 이벤트 발생노드 방향으로 전달함으로써 이벤트 패킷의 차단 유무를 판단하고 경보 패킷을 통해 공격 발생 지역의 탐지가 가능하다. 이때 인증 메시지 배포제한 홉 수인 ACK_TTL은 항상 고정적인 값을 가진다. ACK_TTL이 높아질 수 록 ACK 패킷이 커버할 수 있는 범위가 높아지게 되어 탐지율은 높아지나 에너지 효율성이 떨어지게 되고 반대로 낮아질 수 록 에너지 효율성은 높아지지만 충분한 보안 강도를 제공하지 못한다는 단점을 가지고 있다. 무선 센서 네트워크는 기본적으로 한정적인 자원을 가지고 있으므로 보안과 더불어 에너지 효율 또한 고려해야만 한다.

본 논문에서는 네트워크 전체 수명에 영향을 주지 않는 적절한 ACK_TTL 선택을 위해 퍼지 규칙 시스템을 이용하였다. 퍼지 규칙 시스템은 각 주기마다 각 경로상의 평균 에너지량, 기지 노드까지의 홉 수, 그리고 훼손된 노드 수를 고려하여 적절한 ACK_TTL을 선택하게 된다 (그림 3).

### 3.2 인증 패킷 배포 홉 수(ACK_TTL)

CHEMAS는 경로 상의 감시 노드가 생성하는 인증 패킷과 각 노드들이 생성하는 경보 패킷에 의해서 선택적 전달 공격을 탐지하게 된다. 이때 인증 패킷이 전달가능한 홉 수는 미리 설정되는 ACK_TTL에 의해서 결정되어진다. ACK_TTL이 높아질 수 록 탐지율은 높아지나 에너지 소모를 많이 하게 되는 보안율과 에너지 효율사이의 트레이드 오프관계에 놓여져 있다.

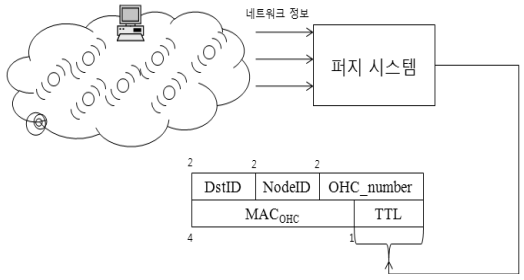


**그림 3.** 제안기법 구성도

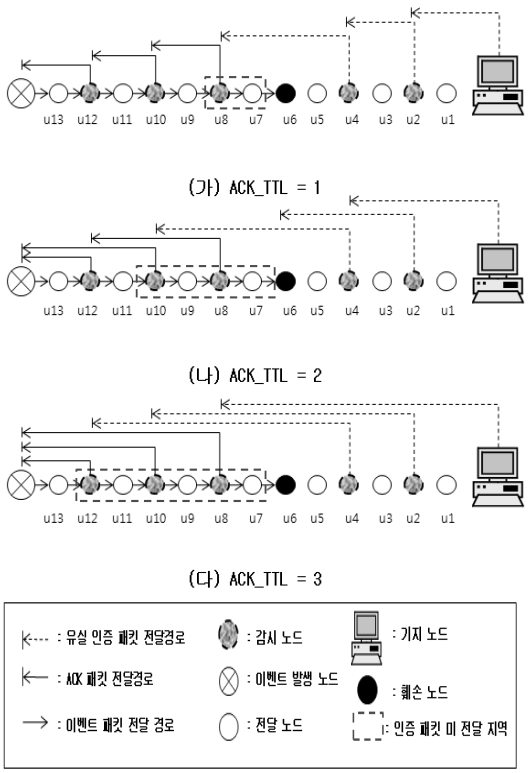


**그림 4.** 인증 배포 값에 따른 탐지 범위

그림 4는 보안경계 값 강도별 탐지 적용 범위를 나타낸다. u6는 공격자에게 훼손되어 평상시에는 정상 노드인척 행동을 하게 된다. 적군의 움직임, 화재등과 같은 중요정보 발생 시 u6는 해당 정보를 차단하여 감시자와 이벤트 발생지역 사이의 중요정보에 대한 고립을 유발하게 된다.

이러한 공격 유형을 선택적 전달 공격이라고 명시하고 있으며 CHEMAS에서는 3가지 패킷(이벤트, ACK, 경보) 정보를 이용하여 선택적 전달 공격 발생 노드(즉, 그림4에서의 u6)을 탐지할 수 있게 된다.

그림 4에서 볼 수 있듯이 ACK_TTL이 1인 경우 하나의 감시노드에서 발생하는 인증 패킷이 거치는 노드 홉수가 적기 때문에 패킷의 전달로 인해 발생되는 오버헤드는 상대적으로 적지만 해당 경로에서 발생되는 공격에 대한 탐지율은 ACK_TTL이 2,3인 경우보다 낮아지게 된다.

CHEMAS에서 인증 패킷을 받지 못한 감시 노드들(점선안의 감시 노드들)은 경보 패킷을 발생하게 되며 기지노드는 수집된 경보 패킷내부의 정보를 이용하여 공격 발생 노드에 대한 탐지가 가능하다.

u6가 훼손되었다고 가정했을때 u6가 공격 발생 노드라고 탐지할 수 있는 노드는 감시노드 u4의 인증패킷 전달 범위 안에 있는 노드들이다.

그림 4(가)에서 볼 수 있듯이 ACK_TTL이 1인 경우 u8,u7 두개의 노드만이 훼손 노드 u6에 대한 이상 징후를 감지할 수 있으며, ACK_TTL이 높을수록 u6에 대한 이상 징후를 감지할 수 있는 노드의 수 즉, 점선 내의 감시노드 수가 증가하는 것을 볼 수 있다(그림4(나),(다)). 이것은 u6가 훼손된 노드라는 증거가 많아진다는 것을 의미하며, 이러한 증거가 많아질수록 탐지율은 높아지게 된다. 하지만 인증 패킷 전달시 발생하는 에너지 소모의 증가로 인해 자칫 해당 경로의 마비를 가져올 수 있다는 단점을 가지고 있다.

### 3.3 가정

배치 전 단계에서 각 노드들은 기지노드의 공유 키 집합에서 무작위로 배포된 키 쌍(pairwise key)을 서로 공유한다. 노드 배치 및 초기 경로 설정 단계에서 각 노드들은 기지노드와 위치 정보를 공유 및 시간 동기화 그리고 동

일한 에너지 측정값($E_{IV}$)을 가지고 있다고 가정한다. 또한 배치 단계에서 공격자는 노드를 훼손할 수 없다. 공격자는 중요 패킷만을 선별하여 차단하고 무조건적인 패킷 차단은 하지 않는다고 가정한다[6].

### 3.4 퍼지 규칙 시스템

무선 센서 네트워크의 자원 제한적인 특성과 동적으로 변화하는 환경의 특성 상 고정적인 ACK_TTL은 보안적 측면과 에너지 효율적인 측면 모두를 충족하지 못한다.

퍼지 규칙 기반 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.

제안기법에서는 이러한 퍼지 규칙 기반 시스템의 특징을 이용하여 명확하게 나누어지지 않는 네트워크 환경에서의 적절한 ACK_TTL을 선택하고자 한다.

제안 기법에서 기지노드는 수집된 경 경로상의 측정 에너지량(ER : Energy Rate), 기지 노드까지의 홉 수(Hops), 그리고 훼손된 노드(MN : Malicious Node)를 고려하여 적합한 경계값을 결정하게 된다.

- ER : 측정 에너지량이 낮은 상태에서의 높은 ACK_TTL은 과도한 검증 과정으로 인해 해당 경로의 에너지 고갈로 인한 마비를 가져올 수 있으므로 이 경우 최소한의 보안 강도를 유지함으로써 네트워크의 수명을 연장하는 것이 더 효과적이다. 반대로 에너지량이 높을 경우 충분한 보안강도를 위한 높은 ACK_TTL 설정이 필요하다.

잔여 에너지량의 경우 아래의 식 (1)로부터 예측이 가능하다.

$$E_{remain} = E_{remain} - E_{comm} \quad (1)$$

각 노드들의 초기 $E_{remain}$ 값은 초기 측정에너지 값 $E_{IV}$과 같다. $E_{IV}$는 경로설정 시 기지노드가 각 경로별로 측정한 값이며, 각 소스 노드들의 캐쉬 메모리에 저장되어진다. 이벤트가 발생하게 되면 소스 노드는 이벤트 패킷 안에 $E_{remain}$값을 삽입 후 보내게 된다. 각 노드는 자신이 소모한 에너지 $E_{comm}$ 만큼 $E_{remain}$값을 감소시킨다.

- Hops : 홉 수가 적은 지역에서의 높은 ACK_TTL은 무의미하며, 반대로 높은 지역에서 낮은 ACK_TTL은 충분한 보안강도를 제공하지 못할 수도 있기 때문에 ACK_TTL은 반드시 각 전달 경로 상의 홉 수를 고려해야 한다.
- MN : 훼손된 노드가 많을 수 록 좀 더 높은 ACK_TTL 값을 주어 탐지율을 높여주고, 반대로 훼손된 노드가 적을 수 록 낮은 ACK_TTL 값을 주어 ACK 패킷이 전달됨으로써 발생하는 에너지 소모, 전송 트랙픽 증가 등의 오버헤드을 낮추어 네트워크 수명을 높이는 것이 효율적이다.

$$\frac{n}{m} \times 100 \quad (2)$$

훼손된 노드의 경우 경로 상의 노드 수 전체를(즉, 기지 노드와 소스 노드를 제외한 전달 노드의 수) m으로 두고 의심 노드의 수를 n으로 정의했을 때 식 (2)을 통해 비율로써 변환되어 입력 값으로 사용된다.

**입력 파라미터**

- ER = {R (Rare), N (Normal), E (Enough)}
- Hops = {A (Around), N (Normal), D (Distant)}
- MN = {VS (VerySmall), S (Small), N (Normal), L (Large), VL (VeryLarge)}

그림 5는 퍼지 규칙 시스템에서의 입력 값 멤버십 함수를 나타낸다.

**출력 파라미터**

출력 값은 인증 패킷의 전달 홉수를 나타낸다.

- TTL = {VS (VerySmall), S (Small), N (Normal), L (Large), VL (VeryLarge)}

**퍼지 규칙의 일부**

규칙 05 : IF ( ER IS Enough) AND (Hops IS Distant) AND (MN IS Large) THEN (TTL IS VeryLarge)

규칙 35 : IF (ER IS Rare) AND (Hops IS Distant) AND (MN IS VeryLarge) THEN (TTL IS VerySmall)

규칙 48 : IF (ER IS Enough) AND (Hops IS Around) AND (MN IS VeryLarge) THEN (TTL IS Medium)

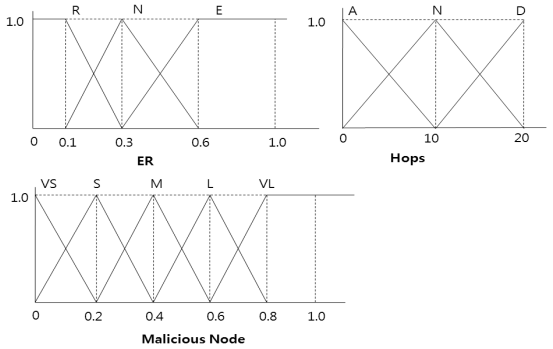


**그림 5.** 퍼지 멤버십 함수 : 입력 값

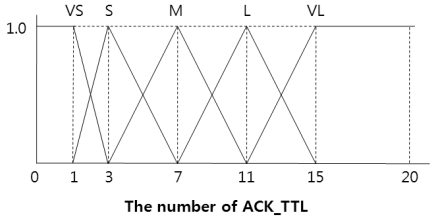


**그림 6.** 퍼지 멤버십 함수 : 출력 값

기본적으로 퍼지 규칙 시스템은 에너지(이하 ER)가 충분하고 이벤트 발생 거리(이하 Hops)가 멀고 훼손된 노드가 많을 경우에는 높은 ACK_TTL을 설정하게 된다(규칙 05). 공격 탐지를 위한 보안 동작 과정 역시 에너지 소모를 발생한다. 네트워크 에너지가 거의 고갈 된 상태에서의 탐지 과정은 자칫 해당 경로의 전송 마비를 초래할 수 있으므로 퍼지 규칙 시스템은 ACK_TTL을 최소한으로 설정하게 된다(규칙 35).

## 4. 시뮬레이션 결과

본 논문에서는 제안기법의 효율성을 검증하기 위해 다음과 같은 시뮬레이션 환경을 가정하였다. 500×500$m^2$의 크기의 필드에 400개의 센서 노드들을 무작위로 배치하였다. 각 노드든 전송 에너지로 16.25 μJ, 수신에너지로 12.5 μJ를 소모하며, 초기 방송 메시지의 크기는 25byte로 가정하였다[10]. 테스트 지역의 거리는 15～20홉 사이이며, 비교 대상이되는 CHEMAS의 경우 ACK_TTL은 3에서 6으로 설정하였다. 또한 기지 노드에서 경로 설정을 위한 초기 메시지 단계에서는 공격자로부터 안전하다고 가정하였으며, 경로별 노드 훼손도는 25%로 고정하였다.

제안기법의 결정 주기는 이벤트 발생횟수에 따라 발생

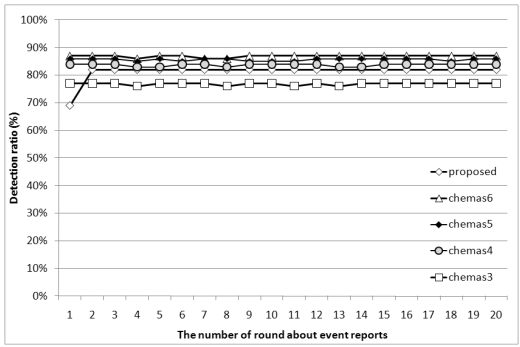


**그림 7.** 탐지율 비교

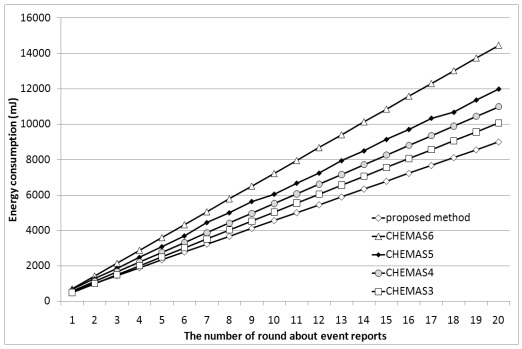


**그림 8.** 에너지 소모율 비교

하며 주기의 간격은 200회로 설정하였으며, 퍼지 규칙 시스템 적용을 위해 오픈 소스인 FFLL(Free Fuzzy Logic Library)를 사용하였다[15].

그림 7은 이벤트 발생횟수에 따른 탐지율을 기존의 기법과 비교한 그래프이다. 그림에서도 볼 수 있듯이 제안된 기법은 퍼지 규칙 시스템에 따라 매 주기마다 각 상황에 맞는 적절한 ACK_TTL을 선택하므로 일정한 탐지율을 보여준다.

제안기법의 초기 탐지율이 낮은 것은 초기 ACK_TTL을 ACK_TTL=1로써 낮게 설정해줬기 때문이다.

그림 7에서 보여주었던 탐지율의 경우 CHEMAS(6)가 가장 높은 탐지율을 보여줬으나, 그림 8에서 볼 수 있듯이 제안된 기법은 상황에 맞는 적절한 ACK_TTL을 선택함으로써, 에너지 효율성 측면에서 기존의 기법보다 좀 더 나은 결과를 보여 주었다.

CHEMAS(5,6)의 경우 높은 탐지율에 의해 좀 더 많은 정보들을 기지노드에게 전달할 수 있지만 이벤트 발생 횟수가 증가할 수록 누적되는 에너지 소모량이 급격하게 증가함에 따라 네트워크 수명이 급감하게 된다는 단점을 가

지고 있다.

보안적인 측면에서는 ACK_TTL이 6으로 높게 설정되어진 CHEMAS가 가장 높은 성능을 보여주었으나 에너지 효율성 측면의 경우 가장 좋지 않은 성능을 보여주었다. 높은 보안 설정 값은 충분한 탐지율을 제공하지만, 반대로 많은 에너지를 소모하여 전체 네트워크 수명에 영향을 미치는 단점을 가지고 있다.

에너지 효율성 측면에서는 CHEMAS(3)이 가장 좋은 성능을 보여 주었으나, 그림 7에서 볼 수 있듯이 제대로 된 보안 성능을 나태내고 있지 않다는 것을 확인할 수 있다. CHEMAS(4)의 경우 보안적 측면에서는 제안된 기법보다 좀 더 나은 성능을 보여주며, 에너지 효율성 또한 높게 보안이 설정된 기존 기법 CHEMAS(5,6)보다는 좋은 성능을 보였지만 그림 8에서 확인할 수 있듯이 에너지 효율성 측면에서 제안기법보다는 뒤쳐지는 효과를 보여주고 있다.

결론적으로 제안기법은 퍼지 규칙 시스템을 통해 전체 네트워크 수명에 많은 영향을 주지 않는 보안 설정 값을 선택한다는 것을 그림 7과 8에서 확인할 수 있다.

## 5. 결 론

CHEMAS에서 ACK_TTL(ACK_TTL 배포 제한 홉 수) 결정은 에너지 비용과 보안강도 사이에서 트레이드 오프하므로 매우 중요하다. 기존의 CHEMAS에서 고정된 ACK_TTL은 네트워크 상황에 맞는 적절한 ACK_TTL 선택이 불가능하였다. 본 논문에서는 네트워크 상황에 맞는 효율적인 ACK_TTL을 도출하고자 퍼지 규칙 기반 ACK_TTL을 결정 기법을 제안하였다. 시뮬레이션 결과를 통하여 제안된 기법이 충분한 보안 강도를 유지하면서도 효율적인 에너지 소비를 제공한다는 것을 보여주었다. 향후에는 CHEMAS에서 ACK 메시지를 발생하는 노드의 적절한 선택을 위한 방법에 대해 연구할 예정이다.

## 참 고 문 헌


1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirici, “A survey on sensor networks,” IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, Aug. 2002.
2. B. Xia, B. Yu, C. Gao, “CHEMAS: Identify suspect nodes in selective forwarding attacks,” Journal of Parallel and Distributed Computing, vol. 67 issue 11, pp. 1218-1230, Apr. 2007.
3. Karlof, C., Wagner, D. 2003. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, 1( 2-3), 293-315.
4. N. Al-Karaki, and A.E. Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication Magazine, Vol. 11, No. 6, pp. 6-28, 2004.
5. B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks,” in ACM SenSys, 2003.
6. T.H. Hai, E. Huh, “Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge”, in Proceeding of Seventh IEEE International Symposium on Network Computing and Applications, 2008.
7. D. Djenouri and L. Khelladi, “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks,” IEEE Communication Surveys and Tutorials, Vol. 7, No. 4, pp. 2-28, December 2005.
8. Zhu S, Setia S, Jajodia S, Ning P. “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks,” In Proc. S&P, pp. 259-271, 2004.
9. H.Y. Lee and T.H. Cho, “Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks,” Lect. Notes Comput. Sc., Vol. 4317, pp.116-127, Dec. 2006.
10. Ye F, Luo H, Lu S. Statistical En-Route Filtering of Injected False Data in Sensor Networks. IEEE J. Sel. Area Comm., 23(4): pp. 839-850, 2005.
11. F. Li and J. Wu, “A probabilistic voting-based filtering scheme in wireless sensor networks,” Proc. IWCMC, pp. 2732, July 2006.
12. B.H. Kim and T.H. Cho, “Condition-based Key Dissemination Period Determining Method in Sensor Networks”, In Proc. Of ICACT, 2008.
13. Perrig A, Szewczyk R, Tygar J D, Wen V, Culler D E. SPINS: Security Protocols for Sensor Networks. Wirel. Netw., 8(5): 521-534, 2002.
14. Intanagonwiwat, C., Govindan, R., Estrin, D., Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. Proc. of MOBICOM, 56-67, ACM, 2000.
15. FFLL, http://ffll.sourceforge.net

**이 상 진** (sjlee@ece.skku.ac.kr)

2007 백석대학교 소프트웨어공학과 학사
2008～현재 성균관대학교 전자전기컴퓨터공학과 석사과정

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

**김 종 현** (jonghkim@ece.skku.ac.kr)

2009 단국대학교 컴퓨터과학과 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 공학사
1987 University of Alabama 전자공학과 공학석사
1993 University of Arizona 전자 및 컴퓨터공학과 공학박사
1995～현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 시뮬레이션, 지능 시스템, 모델링 방법론, 네트워크 보안 시뮬레이션, 전사적 자원 관리