선택적 전달 공격 탐지 기법에서의 감시 노드 수 제어기법

Control Method for the number of check-point nodes in detection scheme for selective forwarding attacks

이 상 진*, 조 대 호**

Sang-Jin Lee, Tae-Ho Cho

Abstract

Wireless Sensor Network (WSN) can easily compromised from attackers because it has the limited resource and deployed in exposed environments. When the sensitive packets are occurred such as enemy's movement or fire alarm, attackers can selectively drop them using a compromised node. It brings the isolation between the basestation and the sensor fields. To detect selective forwarding attack, Xiao, Yu and Gao proposed checkpoint-based multi-hop acknowledgement scheme (CHEMAS). The check-point nodes are used to detect the area which generating selective forwarding attacks. However, CHEMAS has static probability of selecting check-point nodes. It cannot achieve the flexibility to coordinate between the detection ability and the energy consumption. In this paper, we propose the control method for the number fo check-point nodes. Through the control method, we can achieve the flexibility which can provide the sufficient detection ability while conserving the energy consumption.

Keywords : wireless sensor network (WSN), selective forwarding attacks, fuzzy rule-based system, checkpoint nodes

I. 서 론

기술의 진보로 인한 소형 프로세서의 등장으로 인하여 무선 센서 네트워크는 다양한 응용분야에서 활용이 가능하다 [1]. 무선 센서네트워크는 제한적 자원을 가지고 노출된 환경에 배치되므로 공격자로부터 손쉽게 노출된다는 취약점을 가지고 있다. 공격자는 경로상의 훼손된 노드를 이용하여 중요정보의 기지노드까지의 전달을 차단함으로써 기지노드의 센싱필드 사이의 정보고립을 유발한다. 이러한 공격을 선택적 전달 공격(selective forwarding attack)이라고 부른다[secure routing]. 선택적 전달 공격의 탐지를 위해 Xiao, Yu, 그리고 Gao는 checkpoint-based multi-hop acknowledgement scheme (CHEMAS)라는 기법[4]을 제안하였다. CHEMAS는 확률적을 경로상의 노드들중 감시 노드(checkpoint)를 선출한다. 감시노드로 선출된 노드들은 이벤트 메시지를 수신 후 확인 메시지를 전달경로 역방향으로 보냄으로써 이벤트 메시지의 안전한 전송을 보장하게 된다. CHEMAS에서 감시노드 선출 확률 p는 항상 고정적이다. 앞서 언급했듯이 무선 센서 네트워크는 자원적으로 제약성을 가지므로 무조건적인 보안강도의 증가는 자칫 네트워크 전체의 마비를 가져올 수 있으므로 상황에 맞는 적절한 보안 강도의 조절이 필수적이다. p가 높을수록 탐지율은 높아지지만 탐지를 위한 감시노드의 동작의 증가로 인한 오버헤드가 높아진다는 단점을 가지게 된다.

본 논문에서는 적절한 보안강도를 유지하면서도 에너지 효율을 제공할 수 있는 p의 선택을 위해 퍼지 규칙 기반 시스템을 이용한 감시 노드 수 제어기법을 제안하고자 한다. 퍼지 규칙 기반 시스템은 잔여 에너지, 경보 패킷의 수를 고려하여 정해진 규칙으로 인한 적절한 감시 노드 수 제공이 가능하다.

논문의 구성은 다음과 같다. 2장에서는 제안기법의 타겟이 되는 선택적 전달 공격에 대한 간략한 기술과 선택적 전달 공격에 대한 탐지기법 중 하나인 CHEMAS에 대한 설명을 하고, 3장에서 본 제안기법인 감시 노드 수 제어기법의 구성 및 동작과정에 대해서 설명하고자 한다. 끝으로 4장에서는 결론 및 향후과제에 대해서 언급할 것이다.

접수일자 : 2009년 08월 07일
최종완료 : 2009년 08월 14일
*성균관대학교 정보통신공학부
**성균관대학교 정보통신공학부
교신저자, E-mail : {sjlee,taecho}@ece.skku.ac.kr

II. 관련 연구

1. 선택적 전달 공격 (Selective forwarding attacks)

무선 센서 네트워크에서 각 센서 노드들은 작은 메모리 공간, 부족한 에너지, 연산력 제약등의 한정된 자원을 가지므로, 공격자는 손쉽게 노드들을 포획하여 다양한 공격들의 시도가 가능하다. 이러한 다양한 공격들 중 하나인 셀렉티브 포워딩 공격은 사용자가 반드시 받아야하는 중요정보와 같은 것들을 전달 경로 상의 중간 부분에서 차단함으로써 사용자의 혼란을 유발시킨다. 예를 들어, 전장지역 내에서의 탱크의 움직임, 미사일 감지등과 같은 중요정보를 전달 경로 상에서 차단함으로써 기지노드까지의 전달을 방해하게 된다. 무선 센서네트워크 상에서 공격자는 그림 1(가)와 같은 훼손된 노드를 통하여 중요 정보를 차단하는 내부자 공격(inside attack) 또는 그림 1(나)와 같은 정상

노드 사이의 통신 채널에 대한 전파 방해 공격(jamming attack)을 가하는 외부자 공격(outside attack)등의 두 가지 형태로 공격을 시도 할 수 있다. 본 논문에서는 그림 1(가)에서 나타나는 내부자 공격(즉, 훼손된 노드를 통한 공격)만을 고려하고자 한다.

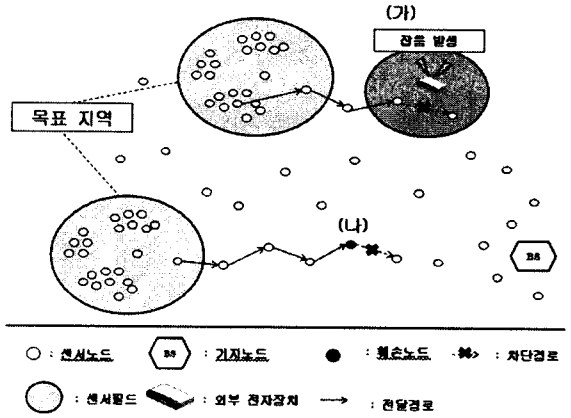


그림 1. 선택적 전달 공격

2. 감시노드 기반 탐지기법 (CHEMAS)

Xiao, Yu 그리고 Gao는 선택적 전달 공격의 탐지를 위해서 감시노드 기반 탐지기법(이하; CHEMAS)을 제안하였다 [4]. 대부분의 여과기법과 마찬가지로 CHEMAS 역시 배치 단계(*deployment phase*), 침입 탐지 단계(*intrusion detection phase*), 대응 단계(*decision and response phase*)의 3가지 단계로 동작한다.

배치 단계에서 각 노드들은 기존의 라우팅 기법에 의해 주변 노드를 탐색하여 네트워크 위상을 구성한다 [6]. 그 후 자신의 키 체인에서 첫 번째 키를 자신의 이웃노드와 공유하게 된다. 침입 탐지 단계에서는 감시노드들 통한 선택적 전달 공격의 발생여부를 탐지하게 된다. 마지막으로 대응 단계에서는 침입 탐지를 통하여 수합된 증거자료를 통하여 공격의 원인이 되는 노드를 파악하여 이에 따른 대응 정책을 제시한다.

● 3가지 패킷 유형

CHEMAS는 이벤트 패킷(*event packet*), ACK 패킷(*ack packet*), 경보 패킷(*alert packet*)의 3가지 패킷들을 통하여 공격의 발생 유무를 탐지하게 된다.

그림 2은 각 패킷의 구성을 나타내며, 각 요소들은 아래와 같다.

▶ 이벤트 패킷(그림 2(가))
- DstID, SrcID, Packet_ID, Payload : 라우팅 프로토콜에서 패킷 구성 시 기본적으로 사용하는 부분으로써 각각 목적지 노드 ID, 이벤트 발생 노드 ID, 패킷 ID, 그리고 이벤트 감지 메시지를 나타냄.
- Checkpoint_seed : 감시 노드 선택을 위해서 이벤트 감지노드가 생성하는 랜덤 변수 값

▶ ACK 패킷 (그림 2(나))
- Packet_ID : 전달된 이벤트 패킷의 ID
- OHC_Number, MAC_{OHC} : ACK 메시지의 무결성 검증을 위한 메시지 인증 코드
- TTL : ACK 패킷이 전달되는 범위 제한을 위한 값

▶ 경보 패킷 (그림 2(다))
- DstID : 이벤트 발생 노드의 ID
- SrcID : 경보 패킷을 발생한 노드의 ID
- Suspect_Node_ID : 공격자로 의심되는 노드의 ID
- Lost_Packet_ID : 유실된 패킷의 ID
- MAC : 경보 패킷의 무결성 검증을 위한 메시지 검증 코드

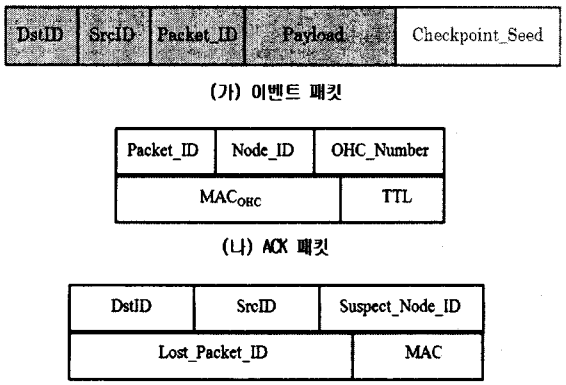


그림 2. 3가지 패킷의 구성

● 감시노드 선택

감시노드는 그림 2(가)와 같은 이벤트 패킷에 포함된 checkpoint_seed r값을 식(1)에 대입하므로써 선택된다.

$$f_p(F_{ID}(r)) \quad (1)$$

F_{ID}는 일방향 해쉬 함수를 나타낸다. ID는 현재 이벤트 패킷을 수신한 노드의 ID이며, f_p는 매핑함수(mapping function)로써 0과1을 각각 확률p 와 확률 $(1-p)$로써 선택한다. f_p를 통해 1이 선택되면, 해당 노드는 감시노드로 선택되어지고 ACK 패킷을 소스노드 방향으로 전달한다.

● 공격 탐지 과정 (그림 3)

노드 u8가 훼손되어 중요정보를 차단시키고 있다고 가정해보자. 감시노드는 u7과 u3이며, ACK 패킷의 전달 홉 수 제한(즉, 그림 2(나)에서의 TTL)은 2이라고 가정한다.

이벤트 발생노드(이하; 소스 노드)는 중요정보 감지 후 기지노드 방향으로 이벤트 패킷을 방송한다. 이벤트 패킷을 수신한 각 노드들은 이벤트 패킷을 수신 후 자신의 캐쉬 메모리에 저장한다. 동시에 앞서 언급한 수식 (1)에 이벤트 패킷의 checkpoint_seed값을 대입하여 자신이 감시노드인지 아닌지를 파악한다. 감시 노드로 선택된 u3, u7은 이벤트 패킷을 기지 노드 방향으로 보내고 이와 동시에 소스 노드 방향으로 ACK 패킷을 보내게 된다. u8이 훼손되어 이벤트 패킷을 차단하고 있으므로 마지막 감시 노드인 기지 노드는 ACK 패킷을 소스 노드 방향으로 보낼 수 가 없다. 결국 u7는 u8으로부터 ACK패킷을 보내지 못하게 되며, u7은 의심가는 노드로써 u8을 Suspect_NodeID로 저장 후 소스 노드방향으로 전달함으로써, 공격에 대한 탐지가 가능하게 된다.

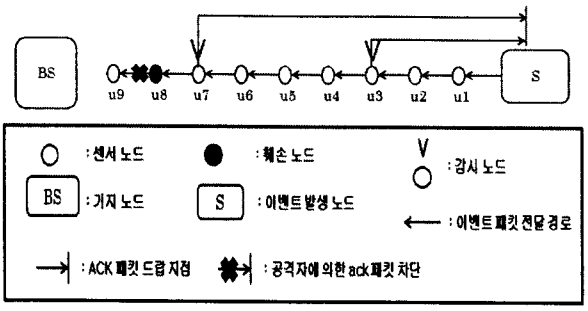


그림 3. CHEMAS 탐지과정

III. 감시노드 수 제어기법

1. 동기

CHEMAS는 경로 상의 감시 노드를 통하여 공격의 탐지가 가능하다. 이러한 감시 노드의 수는 미리 정해진 확률 p를 통해서 결정되어진다. 경로상의 감시 노드가 많을수록 탐지율은 높아지지만 각 감시 노드가 발생하는 ACK 패킷에 따른 오버헤드로 인해 해당 전달 노드들의 에너지가 많이 고갈된다는 단점을 가지고 있다.

본 논문에서는 상황에 따른 감시 노드 수 제어를 위해 퍼지 규칙 시스템을 적용하여 p를 조절함으로써 적절한 탐지율을 유지하면서도 에너지 효율 또한 제공할 수 있는 감시 노드 수를 제공하고자 한다.

2. 가정 사항

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 동일한 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.

3. 네트워크 상황에 따른 감시노드 제어

기지노드는 각 경로별 잔여 에너지, 의심 노드의 수와 같은 네트워크 상황 값들을 표1과 같은 형태로 저장한다.

표 1. 경로 테이블

	품 질 (E_{remain})	의심 노드의 수
경로 1	1000	5
경로 2	500	2
경로 3	1500	4
⋮	⋮	⋮
경로 n	2000	3

그림 4에서 볼 수 있듯이 시스템의 한 주기가 끝나게 되면 기지 노드는 경로 테이블에 저장된 경로별 잔여 에너지, 의심 노드의 수를 토대로 퍼지 규칙 시스템을 기반으로 하여 감시 노드 수 제어 값을 출력 값으로 도출한다. 이 출력 값은 p와의 곱을 통해 높낮이를 조절함으로써 각 경로별 감시 노드 수를 제어할 수 있게 된다.

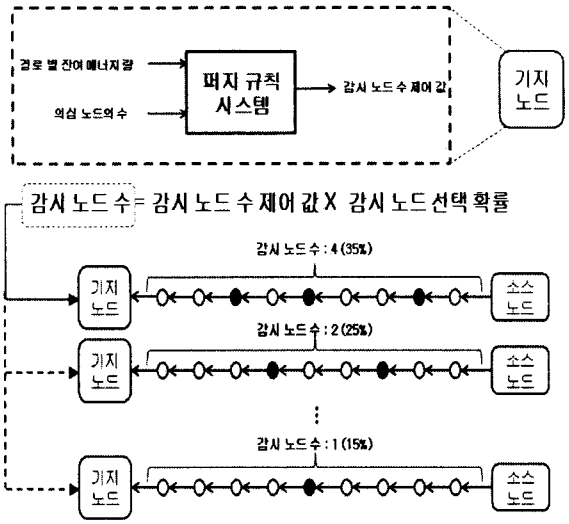


그림 4. 퍼지 규칙 기반 감시노드 수 제어

3.1 감시 노드 수 조절을 위한 퍼지 규칙 시스템

퍼지 규칙 시스템에서는 감시 노드 수 제어 값 도출을 위해 경로별 잔여 에너지량과 의심 노드의 수를 입력 값으로 사용한다.

- 경로별 잔여 에너지(E_{remain}) : 경로별 잔여 에너지의 경우 아래의 식(2)에 의하여 예측이 가능하다.

$$E_{remain} = E_{remain} - E_{comm} \quad (2)$$

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

- 의심 노드의 수(the number of the suspect nodes) : 의심 노드의 수가 많을 수록 경보 패킷의 수도 증가할 것이다. 이것은 해당 지역이 공격자로부터의 공격이 빈번하게 일어난다는 것을 의미하며, 그 만큼 노드훼손이 많다는 것을 의미하게 된다.

$$\frac{n}{m} \times 100 \quad (3)$$

의심 노드 수의 경우 경로 상의 노드 수 전체를(즉, 기지 노드와 소스 노드를 제외한 전달 노드의 수) m으로 두고 의심 노드의 수를 n으로 정의했을 때 식(3)을 통해 비율로써 변환하여 입력 값으로 사용된다.

● 규칙 설계

그림 5는 퍼지 시스템에서의 입력 값에 대한 멤버쉽 함수이다.

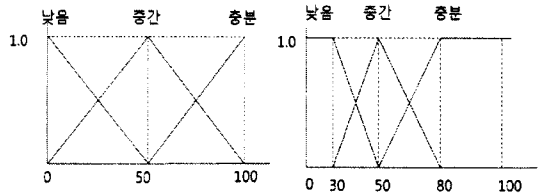


그림 5. 퍼지 입력 값 멤버쉽 함수

퍼지 출력 값은 {증가, 유지, 감소}로 나뉘어지며, 증가 시 현재 확률의 값에 1.5배를 증가하며, 감소 시에는 0.5배를 감소하게 된다. 예를 들어 현재의 감시 노드 선택 확률 p가 50%라고 가정하였을때 퍼지 출력 값이 증가일 경우 p = 75%, 감소일 경우 p = 25%가 된다. 단, p는 10%이하로 감소하지 못하며, 100%이상 증가하지 못한다.

아래는 표 2는 퍼지 규칙의 일부를 나타낸 것이다.

표 2. 퍼지 규칙

규칙 #	IF		THEN
	경로별 잔여 에너지	의심 노드의 수	감시 노드 제어 값
규칙 1	충분	높음	증가
규칙 4	중간	높음	유지
규칙 7	낮음	높음	감소

퍼지 규칙 시스템에서의 출력 값인 감시 노드 수 제어 값과 감시 노드 선택 확률은 비례 관계이다. 기본적으로 퍼지 규칙 시스템은 의심 노드의 수가 많아지면 감시 노드 수 제어 값을 증가시키게 된다. 의심 노드의 수가 많다는 것은 감시 노드의 훼손 확률 또한 높아진다는 것을 의미하므로 퍼지 규칙 시스템은 현재 시스템에 적용된 감시 노드의 수보다 더 높은 감시 노드 수 적용을 통해 탐지율을 유지해야 할 필요가 있다고 판단하기 때문이다. 하지만 잔여 에너지가 얼마남지 않은 상태의 경우에는 감시 노드 수를 유지 또는 감소시키게 된다. 에너지 잔여량이 얼마남지 않은 상태에서 탐지율 유지를 위한 예방책으로 감시 노드 수를 높이는 것은 자칫 과도한 검증 과정으로 인한 네트워크 마비를 초래할 수 있기 때문이다.

VI. 결론 및 향후과제

무선 센서 네트워크는 기본적으로 제약적인 자원이라는 취약점을 가지고 있다. 보안 프로토콜에서의 높은 강도의 보안 프로세스는 검증과정으로 인한 급격한 에너지 소모로 인해 자칫 무선 센서 네트워크 동작의 마비를 초래할 수 있다. *CHEMAS*는 고정적인 감시 노드 선택 확률 값(즉, 탐지율)을 가지므로 네트워크 상황에 맞는 감시 노드 선택이 불가능하다. 본 논문에서는 경로별 잔여 에너지와 의심 노드의 수를 입력 값으로 하는 퍼지 규칙 시스템을 통해 상황별로 가장 적합한 p 값을 선택하도록 설계하였다. 차후 시뮬레이션을 통한 제안기법과 *CHEMAS*와의 비교 분석을 통해 효율성을 검증할 예정이다. 또한 *CHEMAS*의 경우 대응책은 간단한 정책만을 언급할 뿐 구체적인 설계가 없으므로, 이 역시 향후 연구를 통해 구체적인 대응정책과 대응법을 설계 할 예정이다.

감사의 글

이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (No. 2009-0076504)

[참 고 문 헌]

[1] P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards," *Computer Communications*, 30, 2007, pp. 1655-1695.

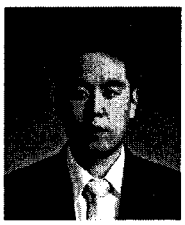
[2] N. Al-Karaki , and A.E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communication Magazine*, vol. 11, no. 6, pp. 6-28, 2004.

[3] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," in *ACM SenSys*, 2003.

[4] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify suspect nodes in selective forwarding attacks," *J. Parallel Distrib. Comput.*, vol. 67, no. 11, pp. 1218-1230, 2007.

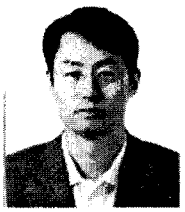
[5] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. *2003 IEEE International Workshop on*, vol., no., pp. 113-127, 11 May 2003

[6] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks." *Proc. of MOBICOM*, 56-67, ACM, 2000



이 상 진

2007년 백석대학교 소프트웨어공학 학사
2008년~현재 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 정보보호, 무선 센서 네트워크, 모델링 시뮬레이션
<email> sjlee@ece.skku.ac.kr



조 대 호

1983년 성균관대학교 전자공학과 학사
1988년 Univ. of Alabama 전자공학과 석사
1993년 Univ. of Arizona 전자 및 컴퓨터 공학과 박사
1993년~1995년 경남대학교 전자계산학과 전임강사
1995년~1999년 성균관대학교 전기전자 및 컴퓨터 공학부 조교수
1999년~2002년 성균관대학교 전기전자 및 컴퓨터 공학부 부교수
2002년~2004년 성균관대학교 정보통신공학부 부교수
2002년~현재 성균관대학교 정보통신공학부 교수
<관심분야> 유비쿼터스 센서 네트워크, 모델링 시뮬레이션, 지능 시스템, 네트워크 보안
<email> taecho@ece.skku.ac.kr