무선 센서 네트워크에서 동적 여과 프로토콜의 인증키 재배포 주기 결정 기법

Determination Method of Authentication Key Re-Distribution Period in Dynamic En-route Filtering Scheme on WSN

이 선 호*, 조 대 호**
Sun-Ho Lee, Tae-Ho Cho

Abstract

센서 네트워크에 대한 연구가 활발히 이루어지면서 센서 네트워크 보안에 대한 문제점이 많이 야기되고 있다. 무선 센서 네트워크에서는 개방된 환경에서 제한적인 자원을 가지는 노드들로 구성되어 있다. 개방된 환경에 배치된 노드들은 공격자에게 쉽게 노출되어질 수 있다. 공격자는 노드를 물리적으로 포획하여 데이터 인증에 사용하는 인증키와 같은 보안 정보들을 획득할 수 있다. 공격자는 포획된 노드를 통하여 허위 보고서를 무선 센서 네트워크에 쉽게 삽입시킬 수 있다. 이는 허위 보고서로 인한 혼란 및 위조 정보의 전달과정에서 발생하는 에너지 고갈 등의 문제점을 유발시키게 된다. 이러한 허위 보고서를 조기에 탐지 및 폐기하기 위하여 동적 여과 프로토콜(DEF: Dynamic En-route Filtering scheme)이 제안되었다. DEF에서 인증키를 재배포 하는 주기는 보안 강도와 비용을 트레이드-오프 하는 관계에 놓여있으므로 매우 중요하다. 본 논문에서는 센서네트워크에서 동적 여과 프로토콜의 인증키 재배포 주기를 결정하는 기법을 제안한다. 배포된 노드들의 위상변화, BS까지 도달한 허위보고서 비율, 공격자에게 포획된 노드의 수 등을 고려하여 재배포 여부를 결정하고 재배포가 결정되면 각 클러스터 헤드들에게 재배포를 명령하게 된다.

Keywords : Sensor networks, false report injection attack, security, fuzzy logic

I. 서 론

무선 센서 네트워크는 주변 환경 정보를 수집할 수 있는 감지 기능과, 정보 처리 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[1]. 센서 노드들은 조밀하게 배치가 되어, 무선 통신을 기반으로 서로 간에 통신을 하거나, BS와 직접적으로 통신을 하게 되며[2], 적은 메모리, 제한된 배터리 용량, 컴퓨팅 성능의 제약 등 제한적인 하드웨어 자원을 가지고 있다.

일반적으로 센서 노드들은 개방된 환경에서 흩뿌려져 독립적으로 방치되어 동작하므로, 공격자들에 의해 쉽게 포획 및 훼손당하기 쉽다[3]. 공격자는 포획된 노드들을 사용하여 다양한 보안 공격들을 네트워크에 가할 수 있다. 허위보고서 주입 공격은 포획된 노드들을 이용하는 대표적인 보안 공격기법이다[4]. 이러한 허위보고서 주입 공격은 허위 경보를 유발할 뿐만 아니라, 허위 보고서를 전달하면서 다른 전달 노드들의 에너지도 같이 소비하여 전체 센서 네트워크의 수명을 단축시킨다.

접수일자 : 2009년 7월 28일
최종완료 : 2009년 8월 14일
*성균관대학교 정보통신공학부 대학원
**성균관대학교 정보통신공학부
교신저자, E-mail : {sunholee,taecho}@ece.skku.ac.kr

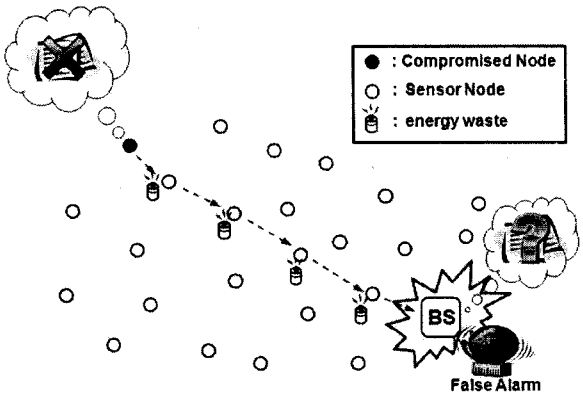


그림 1. 허위보고서 주입 공격

이러한 허위보고서를 조기에 탐지하고 차단하기 위해서 다양한 보안기법들 [4-8]이 제안되었으며, Yu와 Guan이 제안한 동적 여과 프로토콜(Dynamic En-route Filtering scheme; 이하 DEF)[8]은 그중 하나로써, 노드에서 탐지된 이벤트 보고서를 전달하는 과정 중에 허위보고서를 탐지 및 차단할 수 있는 기법이다.

DEF에서 인증키 재배포 주기는 보안강도와 에너지 비용을 트레이드-오프 하므로 매우 중요하다. 인증키 재배포를 자주 하게 되면 보안강도와 네트워크 적응력이 좋아지게 되나, 키를 재배포 하는데 많은 에너지를 소모하게 된다. 센서노드는 제한된 배터리 용량을 가지고 있고 재충전

하기 어렵기 때문에 센서노드를 배포 한 후에는 잔여 에너지 량을 고려해 키 재배포가 이루어져야 한다.

본 논문에서는 DEF가 적용된 센서 네트워크에서의 센서 노드 배포 후 인증키의 재배포 주기를 정해줌으로써 보안 강도를 유지하면서 에너지 비용도 줄이기 위해 퍼지 규칙 시스템을 적용시키고자 한다. 퍼지 규칙 시스템은 배포된 노드들의 위상변화, BS까지 도달한 허위보고서 비율, 공격자에게 포획된 노드의 수 등을 입력 값으로 인증키 재배포 여부를 결정하게 된다.

본 논문은 다음과 같이 구성된다. 2장에서는 허위보고서 공격 보안기법 중 하나인 DEF에 대하여 간략하게 설명하고 3장에서는 DEF의 적절한 키 재배포 주기를 위해서 제안된 기법을 설명한다. 마지막으로 4장에서는 결론과 향후 과제에 대해서 언급할 것이다.

II. 동적 여과 프로토콜 (DEF)

동적 여과 프로토콜(DEF: Dynamic En-route Filtering scheme)[8]은 허위 보고서를 조기에 탐지 및 차단하기 위해 Yu와 Guan이 제안한 기법이다. DEF는 기존의 기법들과 비교하여 센서 네트워크의 위상 변화에 대해서 능동적으로 대처가 가능하고, 큰 규모의 센서 네트워크에서 에너지 효율적인 측면에서 다른 여러 기법들의 성능보다 우수하다. DEF는 이벤트 탐지노드에서 생성한 메시지 인증 코드(Message Authentication Code; 이하 MAC)를 이용하여 정상 보고서, 허위 보고서 여부를 판별할 수 있다. DEF 기법은 배포 전 단계(Pre-Deployment Phase), 배포 후 단계(Post-Deployment Phase), 그리고 여과 단계(Filtering Phase)로 구성된다.

배포 전 단계에서는, 각각의 센서 노드들은 하나의 인증키(Authentication Key)와 인증키 전달시 이를 암호화하기 위해 필요한 공유키 집합에서 임의로 얻어진 $l+1$개의 비밀 키(Secret Key)들을 적재한다. 배포 전 단계는 센서 네트워크가 구성되기 전에 한번만 수행이 된다.

배포 후 단계에서는, 모든 노드들이 자신의 인증키를 $l+1$개의 비밀 키를 통해 암호화 한 후 자신이 속한 클러스터 헤드(Cluster Head; 이하 CH)에게 보낸다. 클러스터내의 노드들에게 암호화된 인증키를 받은 CH는 이것을 조합하여 메시지 형태로 변환 후 자신의 근처 전달 노드들에게 미리 정해진 홉 수만큼 배포하게 된다. 인증 키 분배 메시지를 받은 각 전달 노드들은 자신이 가지고 있는 비밀키와 같은 비밀 키로 암호화된 인증키가 있는지 검사하여, 같은 비밀 키가 있다면 인증키를 저장하고, 없다면 다음 전달 노드에게 인증 키 분배 메시지를 전달하게 된다. 이 과정은 보안강도를 높이기 위해 일정한 주기를 가지고 반복될 수 있다.

그림 2는 배포 후 단계에서의 기 분배 과정을 나타낸 것이다. 각 클러스터내의 센서노드들은 자신의 인증키를 비밀 키로 암호화한 후 CH에게 보낸다(그림 2(1)). 각 센서 노드들에게 인증키를 받은 CH는 미리 정해진 배포 홉 수만큼 인증키를 배포한다.

마지막으로 여과 단계에서는, 각 노드들은 배포 후 단계에서 분배된 인증키를 키를 키를이벤트 메시지 내의 분배

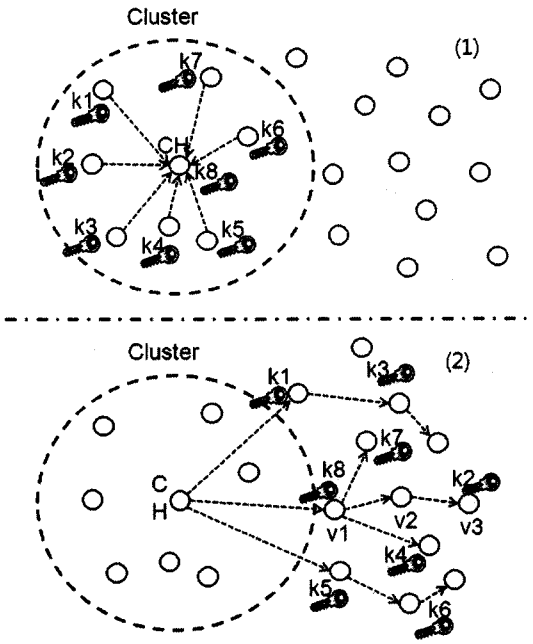


그림 2. 배포 후 단계

된을 검증함으로써메시지내의 를 탐지함으로써메시지내의 이 단계는 메시지가 발생할 때마다 실행된다.

그림 3은 여과 단계에서의 여과 과정을 보여준다. 그림 3에서 CH를 획득한 공격자는 허위보고서 상에 해당 MAC을 첨부하고 나머지 MAC은 임의의 값으로 재워 넣게 된다. v1은 CH의 MAC을 검증할 수 있는 인증키를 가지고 있지만 공격자가 이미 해당 MAC을 획득하여 여과과정 없이 지나갈 수 있지만, 결국 v3에서 허위보고서는 해당 MAC 값을 허위로 생성하였으므로 탐지 및 차단된다.

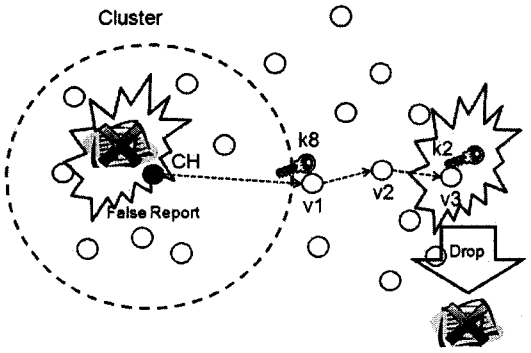


그림 3. 여과 단계

III. 인증키 재배포 주기 결정 기법

1. 동기

DEF에서 각 CH들은 일정한 주기를 가지고 클러스터 노드들에게 인증키를 재배포한다. 이때 정해지는 주기는 DEF에서 보안강도와 네트워크 수명 사이에서 트레이드-오프 하므로 매우 중요한 요소 중 하나이다. 주기가 짧을수록 보안강도는 높아지지만 인증키 재배포 과정에서 더 많은 에너지를 소모하게 된다. 그러므로 DEF에서는 적절한 인증키 재배포 주기의 결정이 반드시 필요하다.

2. 가정

각 노드들은 배치 후 자동으로 여러 개의 클러스터로 구성되어진다고 가정한다. CH는 노드간의 에너지 균형을 위해서 순차적으로 교대되어진다. BS는 모든 노드들의 위치정보를 파악할 수 있고, 클러스터 안의 노드 수, 키 배포 제한 홉 수, 각 노드들의 에너지 량을 알 수 있다고 가정한다. 또한 BS는 방송 메시지를 인증할 수 있는 메커니즘을 가지고 있고, 모든 노드들은 방송 메시지를 검증할 수 있다고 가정한다.

3. 개요

본 논문에서 제안된 기법은 DEF의 동작 과정 중 배포 후 단계에서 인증키를 재배포하는 주기를 위해 퍼지 규칙 기반 시스템을 적용하였다. 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 도출해 내기 위한 방법 중 하나이다. 그림 4에서 볼 수 있듯이 배포된 노드들의 위상변화, BS까지 도달한 S까지 도달비율, 공격자에게 포획된 노드의 수를 입력 값들로 도출된 인증키 재배포 여부는 BS에 의해서 각각의 CH들에게 전달되어지며, 재배포하라는 결과가 나오게 될 경우에 인증키를 재배포하게 된다.

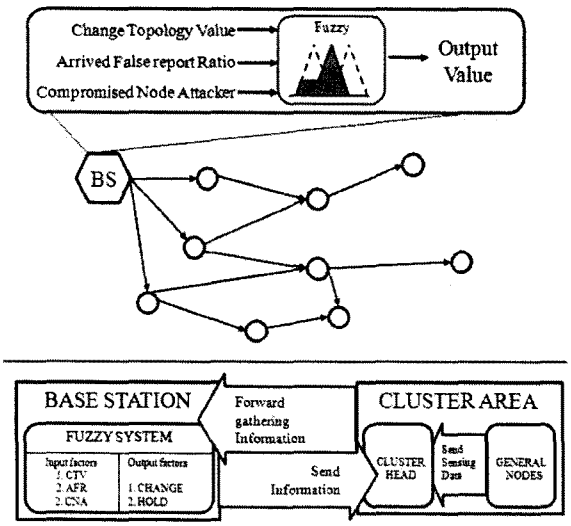


그림 4. 제안 기법 개요도

4. 재배포 주기 결정을 위한 입력 값

퍼지 규칙 기반 시스템을 이용하여 검증 확률을 조절하는 입력 값으로는 배포된 노드들의 위상변화(Changed Topology Value; 이하 CTV), BS까지 도달한 허위보고서 비율(Arrived False report Ratio; 이하 AFR), 공격자에게 포획된 노드의 수(Compromised Node by Attacker; 이하 CNA) 등이 있다.

CTV는 배포된 후 노드가 포획을 당했거나, 물리적으로 손상을 입었거나, 천재지변등 기타 어떤 이유로 노드들의 위상이 크게 변동이 있을 때 값이 높게 나타난다. 이때 클러스터의 재구성과 인증키의 재배포가 필요하므로 고려 대상이 된다.

AFR은 센서 네트워크 내의 여과 프로토콜이 제대로 작동하고 있는지의 여부를 판단 할 수 있다. 높은 AFR은 대부분의 허위 보고서가 전달과정 중 여과되지 않았다는 것을 의미한다. 여과되지 않았다는 것은 이미 많은 수의 노드가 공격자에게 포획되었다는 것을 말한다. 그러므로 인증키의 재배포가 필요하기 때문에 고려대상이 된다.

CNA는 공격자에게 포획된 노드가 많을수록 공격자가 획득할 수 있는 인증키가 많아지므로 허위 보고서가 BS까지 도달할 확률이 증가하게 된다. 그러므로 이때도 역시 인증키의 재배포가 이루어져야하므로 고려대상이 된다.

5. 퍼지 규칙 설계

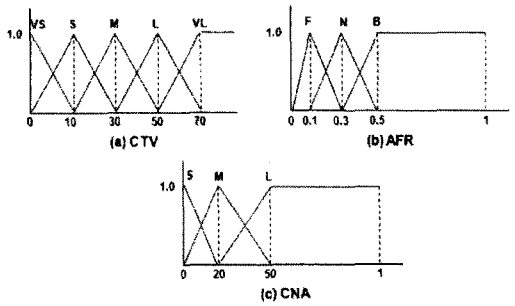


그림 5. 퍼지 입력 값 멤버십 함수

그림 5는 제안된 퍼지 규칙 시스템의 입력 값 세 가지(CTV, AFR, CNA)에 대한 멤버십 함수이다.

다음은 퍼지 입력 변수들의 명칭들을 나타낸다.

- CTV = {VS(Very Small), S(Small), M(Medium), L (Large), VL(Very Large)}
- AFR = {F(Fine), N(Normal), B(Bad)}
- CNA = {S(Small), M(Middle), L(Large)}

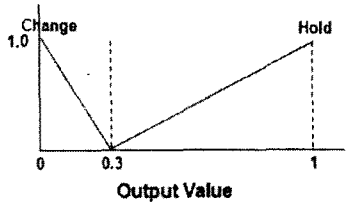


그림 6. 퍼지 출력 값 멤버십 함수

그림 6은 제안된 퍼지 규칙 시스템의 출력 값을 나타내며, 각 명칭들은 다음과 같다.

- Output Value = {Change, Hold}

퍼지 규칙 시스템은 앞서 설명한 세 가지 입력 값을 통해 상황에 맞는 적절한 출력 값을 도출하게 된다.

표 1은 제안된 기법의 퍼지 규칙 일부를 표시한 것이다.

표 1. 퍼지 규칙

Rule #	IF			THEN
	CTV	AFR	CNA	Output
1	VS	F	S	Hold
11	S	F	M	Hold
23	M	N	M	Hold
24	M	N	L	Change
31	L	N	S	Change
39	VL	F	L	Change

6. 추론

추론에는 퍼지 이론의 추론 모델 중 하나인 맘다니(mandani) 모델의 min-max 합성방법(composition)을 사용하고, 실수 값 출력을 위한 역 퍼지화(defuzzification) 방법에는 무게 중심법(COA: Center of Area)을 사용한다.

7. 동작 과정

BS에서는 현재 센서 네트워크 상황에 맞는 재배포 주기를 결정하기 위해 현재 네트워크의 상황을 파악한다. 네트워크의 위상변화와, BS까지의 허위 보고서 도달 비율, 포획된 노드의 수 등을 계산하여 퍼지 로직에 적용하여 재배포 주기를 결정하고 재배포하라는 결과 값이 나오면 각 CH들에게 재배포를 명령한다.

IV. 결론 및 향후 과제

DEF에서 인증키 재배포 주기는 에너지 비용과 보안 강도 사이에서 트레이드-오프 하므로 매우 중요하다. 기존의 DEF상에서 임의로 정해서 사용하는 재배포 주기는 네트워크 상황에 맞게 인증키를 재배포해 주지 못했다. 본 논문에서는 네트워크 상황에 맞는 효율적인 인증키 재배포를 위하여 퍼지 규칙 기반 인증키 재배포 주기 결정 기법을 제안하였다. 향후 과제로는 제안된 퍼지 규칙 시스템으로 도출된 인증키 재배포 주기가 임의로 정해서 재배포 하였을 때와 비교하여 얼마나 효율적인 성능은 분석하기 위한 시뮬레이션을 수행할 것이며, 본 논문에서 제안한 입력 값 이외에 다른 요소들도 입력 값으로 선택하여 좀 더 효율적인 재배포 주기를 결정할 수 있는 값들을 찾아볼 것이다.

감사의 글

이 논문은 교육과학기술부의 재원으로 시행하는 한국과학 재단의 연구 지원 프로그램으로 지원받았습니다. (No. 2009-0076504)

[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] J.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.

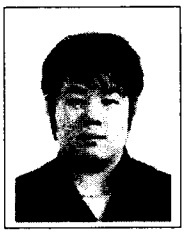
[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," in *IEEE Symposium on Security and Privacy*, 2004.

[5] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-route Detection and Filtering of Injected False Data in Sensor Networks," in *IEEE INFOCOM*, 2004.

[6] H. Yang, S. Lu, "Commutative Cipher Based En-route Filtering in Wireless Sensor Networks," in *IEEE Vehicular Technology Conference (VTC) 2004-Fall Symposium on Wireless Technologies for Global Security*, 2004.

[7] F. Li and J. Wu, "A probabilistic voting-based filtering scheme in wireless sensor networks," *Proc. IWCMC*, pp.27 - 32, July 2006.

[8] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," in Proc. *IEEE INFOCOM'06*, Apr. 2006.



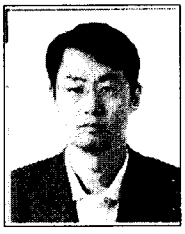
이 선 호

2009년 경원대학교 인터넷미디어학과 졸업

2009년~현재 성균관대학교 정보통신공학부 전자전기컴퓨터공학과 석사과정

<관심분야> 무선센서 네트워크, 모델링 및 시뮬레이션, 인공 지능, 정보 보안

<e-mail> sunholee@ece,skku.ac.kr



조 대 호

1983년 성균관대학교 전자공학과 학사.

1988년 Univ. of Alabama 전자공학과 석사.

1993년 Univ. of Arizona 전자 및 컴퓨터공학과 박사

<관심분야> USN 모델링 및 시뮬레이션, 지능 시스템, 네트워크 보안.

<e-mail> taecho@ece.skku.ac.kr