무선 센서 네트워크에서 동적 여과를 위한 퍼지 기반 확률 조절 기법

Probability Adjustment Scheme for the Dynamic Filtering in Wireless Sensor Networks Using Fuzzy Logic

한만호 *, 이해영, 조대호
(Man-Ho Han, Hae Young Lee, Tae Ho Cho)

Abstract : Generally, sensor nodes can be easily compromised and seized by an adversary because sensor nodes are hostile environments after dissemination. An adversary may be various security attacks into the networks using compromised node. False data injection attack using compromised node, it may not only cause false alarms, but also the depletion of the severe amount of energy waste. Dynamic en-route scheme for Filtering False Data Injection (DEF) can detect and drop such forged report during the forwarding process. In this scheme, each forwarding nodes verify reports using a regular probability. In this paper, we propose verification probability adjustment scheme of forwarding nodes though a fuzzy rule-base system for the Dynamic en-route filtering scheme for Filtering False Data Injection in sensor networks. Verification probability determination of forwarding nodes use false traffic rate and distance form source to base station.

Keywords: False data injection attack, false traffic rate, fuzzy logic, verification probability adjustment scheme, Sensor node

I. 서론

일반적으로 센서 네트워크는 환경을 감시하는 많은 수의 센서 노드들과 감지 값을 수집하는 몇 개의 기지 노드(Base Station; 이하 BS)들로 구성된다. 센서 노드들은 조밀하게 배치가 되며, 노드들은 기지 노드 뿐만 아니라 서로간에도 통신을 할 수 있다. 센서 네트워크는 감지, 처리, 전송 기능을 가지고 있으며, 작고 저렴한 비용의 센서 노드들로 이루어져 있다. 일반적으로 센서 노드들은 개방된 환경에서 배포된 후 독립적으로 방치되어 동작하므로, 공격자들에 의해 쉽게 포획 및 훼손 당하기 쉽다. 공격자는 훼손된 노드들을 사용하여 다양한 보안 공격들은 네트워크에 가할 수 있다. 위조 보고서 주입 공격은 훼손된 노드들을 사용하는 대표적인 보안 공격이다. 이러한 허위 보고서 주입공격은 허위 경보를 유발할 뿐만 아니라, 네트워크의 제한된 에너지 고갈을 야기할 수 있다. 그림 1을 보면 허위 보고서 공격은 허위 보고서만 기지 노드에게 전달하는 뿐만 아니라, 허위 보고서를 전달하면서 다른 전달 노드들의 에너지도 같이 소비하여 전체 센서 네트워크의 수명을 단축시킨다.

이러한 허위보고서를 조기에 검출, 제거하기 하여 에너지 소비를 줄이기 위해 여러 가지 보안 기법들이 제안 되었으며, 그 중 하나가 Yu 와 Guan이 제안한 동적 전달 중 여과 프로토콜(Dynamic En-route scheme for Filtering False Date Injection; 이하 DEF) 이다.

동적 전달 중 여과 프로토콜은 노드에서 탐지된 이벤트 보고서를 전달하는 과정 중에 허위 보고서를 탐지 및 폐기할 수 있는 기법이다. 이 기법에서 각 노드는 일정한 확률을 가지고 보고서를 검증한다.

동적 전달 중 여과 프로토콜은 이벤트가 발생하면 검증을 하고 허위 보고서인 경우 폐기한다. 하지만 허위 보고서임이 판별되기 까지 모든 노드들을 거쳐야 한다.

본 논문에서는 동적 전달 중 여과 프로토콜이 적용된 센서 네트워크에서 퍼지 규칙 기반 시스템을 통하여 전달 노드들의 검증 확률을 조절하는 기법을 제한 한다. 전달 노드들의 검증 확률의 결정에는 허위 트래픽 비율(false traffic rate; 이하 FTR) 과 소스와 기지 노드까지의 거리가 사용된다.

본 논문의 나머지 섹션의 구성은 다음과 같다. 섹션 2에서는 동적 전달 중 여과 프로토콜(DEF)에 대해 간략하게 설명을 하고, 섹션 3에서는 제안 기법에 대한 자세한 설명을 한다. 마지막으로 섹션 4에서는 결론과 향후 과제에 대해서 언급 할 것이다.

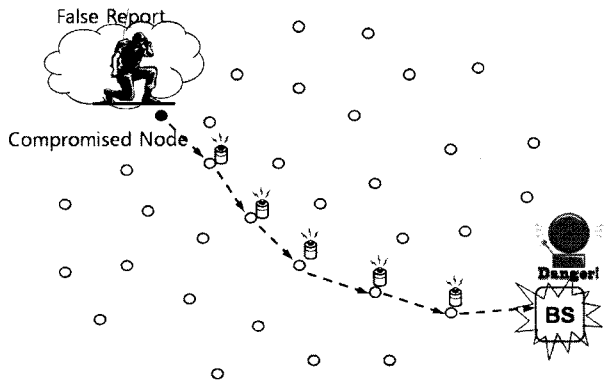


그림 1. 허위 보고서 주입 공격.

* 책임저자(Corresponding Author)
논문접수: 2008. 7. 21., 채택확정 : 2008. 7. 31.
한만호, 이해영, 조대호 : 성균관대학교 정보통신공학부
(sjlee@ece.skku.ac.kr, sofware@ece.skku.ac.kr, taecho@ece.skku.ac.kr)
※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (IITA-2008-C1090-0801-0028)

II. 동적 전달 중 여과 프로토콜 (DEF)

Yu와 Guan은 조기에 허위 보고서를 탐지 및 제거하기 위해서 DEF를 제안 하였다. DEF는 기존에 다른 여과 기법들 비교하여 동적 위상을 보다 잘 다룰 수 있는 장점이 있으며, 특히 큰 규모의 센서 네트워크에서 에너지 효율적인 측면에서 다른 여러 기법들의 성능보다 우수하다. DEF는 이벤트 탐지 노드에서 생성한 메시지 인증 코드(Message Authentication Code; 이하 MAC)를 이용하여 정상 보고서, 허위 보고서 인지를 판별한다.

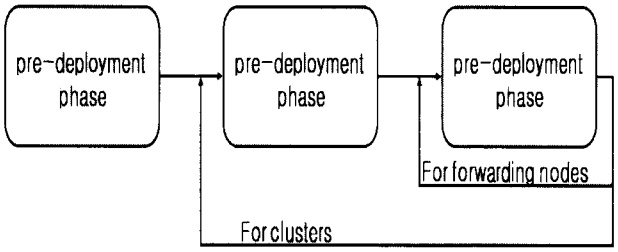


그림 2. DEF의 구성

DEF는 배포 전 단계(pre-deployment), 배포 후 단계(post-deployment phase), 그리고 여과 단계(filtering phase)의 세 단계로 구성된다. 배포 전 단계에서, 각각의 센서 노드들은 하나의 인증 키(Authentication Key)와 인증 키 전달 시 암호화 하기 위해 필요한 전역 키 풀에서 임의로 선택된 / +1 개의 비밀 키들(secret keys)을 적재한다. 배포 전 단계는 한 번만 수행을 한다. 배포 후 단계에서는 모든 클러스터 노드들은 자신의 인증 키를 자신의 /+1개의 비밀 키들로 암호화하여 클러스터 헤드(Cluster head; 이하 CH)에게 보낸다 (그림 3(a)). 각 클러스터 헤드는 클러스터 내의 모든 노드들의 인증 키들을 전달 노드들에게 보낸다 (그림 3(b)). 각 전달 노드들은 인증 키을 받으면, 인증 키를 암호화한 비밀 키를 가지고 있으면 가지고 있는 인증 키를 복호화하여 저장을 한 후 다시 인증 키들을 다음 전달 노드들에게 보낸다. 여과 단계에서는 미리 저장된 전달 노드들에 인증키를 이용하여 위조 보고서들이 탐지되어 폐기한다. 인증 키들의 배포 한 후, 클러스터 헤더는 클러스터 노드들의 메시지 인증 코드들로 사건 보고서를 생성하여 전달 할 수 있다. 공격자들이 그림 3(c)와 같이 클러스터 노드를 훼손하였다고 가정하였을 때, 공격자들은 C_1 과 공유하는 인증 키 F_6를 훼손하였고, C_2는 클러스터 노드와 공유하는 인증키가 없음으로, 노드 C_1과 C_2는 위조 보고서가 주입 되도 계속해서 다음 노드로 전달할 것이다. 하지만 공격자가 F_3를 훼손하지 않는 한, C_3에서 위조 보고서 임이 탐지되어 폐기되고 말 것이다. 이처럼 여과 단계에서 DEF는 위조 보고서가 기지 노드까지 전달 되지 않고, 전달 노드들에 의해 위조 보고서인지 정상 보고서인지를 중간에 검증 되어 폐기된다.

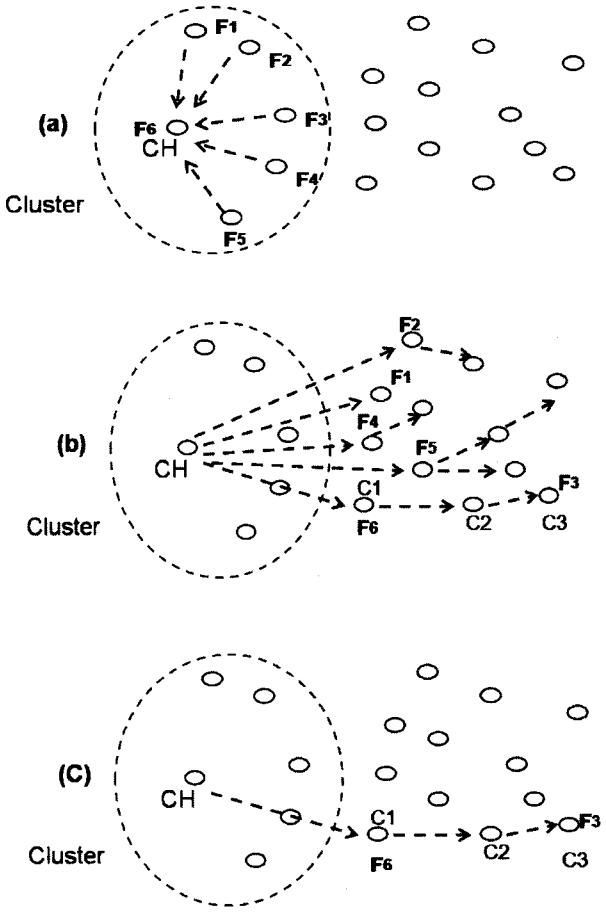


그림 3. DEF에서 키 분배 및 여과 과정

III. 제안 기법

3.1 가정

본 논문에 제안한 기법은 다음과 같은 가정 사항들을 가지고 있다. 센서 노드들은 배포 후에 여러 개의 클러스터로 구성 된다. 그리고 기지 노드는 클러스터들의 수, 훼손된 노드들의 수, 네트워크 내 허위보고서의 비율, 그리고 DEF의 탐지 능력을 예측하거나 알 수 있다고 가정한다. 기지 노드는 방송 메시지를 검증 할 수 있는 메커니즘을 가지고 있으며, 모든 노드들은 방송 메시지를 검증 할 수 있다고 가정한다.

3.2 개요

본 논문에서 제안 기법은 클러스터 노드에서 기지 노드로 보고서를 전달하는 과정 중, 각 전달 노드들이 보고서를 검증할 때 검증하는 노드들의 수에서 기존의 DEF방식과 차이점을 가진다. 그림 3(c)의 여과 단계에서 각 전달 노드들은 클러스터 노드에서 보낸 보고서를 모두 다 검증을 한다. 하지만 제안한 기법은 전달 노드들의 검증 노드 수를 줄여 센서 네트워크의 에너지 효율을 증가 시키는 방법을 제안한다. 기지 노드는 퍼지 규직 기반 시스템을 통하여 전달 노드들의 검증 확률을 주기적으로 조절 할 수 있다. 검증 확률 결정에는 허위 보고서 확률과 소스와 기지 노드까지의 거리가 사용된다.

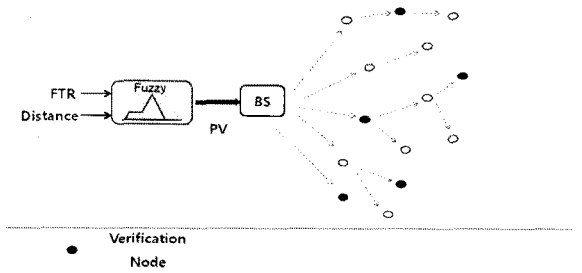


그림 4. 제안한 기법의 개요

그림 4는 퍼지 규칙 기반 시스템을 이용하여 나온 확률(PV)값을 기지 노드에게 전달을 한다. 기지 노드는 퍼지 규칙 기반 시스템에서 나온 확률 값을 기반으로 검증 노드들을 결정을 하고 결정된 검증 노드들은 보고서를 검증하고 위조된 보고서일 경우 폐기시키고, 정상 보고서인 경우 다음 검증 노드에서 전달한다.

3.3 검증 확률 조절 입력 값

퍼지 규칙 기반 시스템을 이용하여 검증 확률을 조절 하는 입력 값으로는 소스와 기지 노드사이의 거리와 네트워크 내 허위 보고서의 비율이 있다.

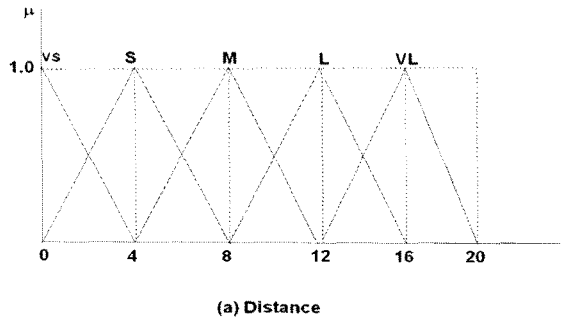
클러스터 노드들로 부터 기지 노드까지의 거리 별로 검증 확률들이 다르게 나오기 때문에 거리는 퍼지 규칙 기반 시스템의 입력 값으로 고려 대상이 된다.

네트워크의 허위 보고서의 비율이 높다는 것은 현재 네트워크의 보안 강도가 충분하지 못하다는 것을 의미하므로 센서 노드의 검증 확률을 높여야 한다. 대조적으로 허위 보고서의 비율이 낮다는 것은 보안 강도가 어느 정도 어느 정도 유지되거나 충분하다는 것을 의미하기 때문에 센서 노드의 검증 확률을 유지하거나 낮춰야 한다.

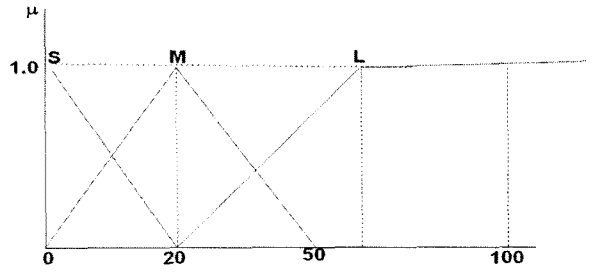
3.4 퍼지 규칙 기반 시스템의 설계

본 논문에서 제안한 기법은 허위 보고서의 비율은 추정 값이기 때문에 어느 정도의 오차를 가지고 있고, 주어진 입력 값은 기준에 따라 크고 작음이 다르게 판단 할 수 있다. 이러한 불확실 성과 애매성 때문에 복잡한 연산 없이 퍼지 규칙 기반 시스템을 이용하여 최적의 해를 구한다.

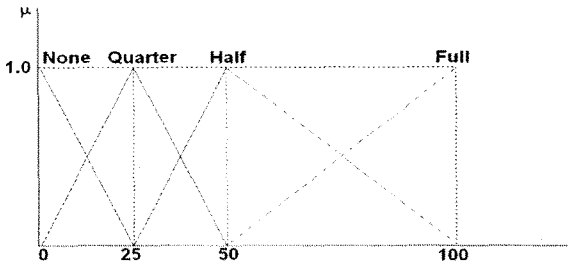
그림 5(a),(b)는 퍼지 규칙 기반 시스템에 두 가지 입력 변수 (Distance, FTR)와 멤버십 함수들을 보여 준다.



(a) Distance



(b) FTR



(C) PV

그림 5. 입력 값 및 출력 값 멤버십 함수

◦ Distance = {VS (Very Small), S (Small), M (Medium), L (Large), VL (Very Large)}
◦ FTR = {S (Small), M (Medium), L (Large)}

표 1은 해당 퍼지 함수의 규칙들의 일부이다. 검증 확률은 거리와 네트워크내의 허위 보고서 비율로 기반으로 결정을 한다.

표 1. 퍼지 규칙

Rule#	Distance	FTR	PV
01	VL	S	Full
02	VL	M	Half
03	VL	L	Quarter
04	M	S	Full
05	M	M	Half
06	M	L	None

IV. 결론 및 향후 과제

본 논문에서는 동적 전달 중 여과 프로토콜의 동작과정을 설명하였다. 동적 전달 중 프로토콜에서는 클러스터 노드에서 기지 노드까지의 각각의 전달 노드들이 모두 보고서를 검증하지만, 제안 기법은 퍼지 규칙 기반 시스템을 이용하여 검증 확률을 거리와 네트워크 내 허위 보고서의 비율로 구하여 검증 확률을 조절하는 기법을 제한 하였다. 검증 확률을 이용하여 검증 노드 수를 줄이면 각각의 모든 전달 노드들이 보고서들을 검증할 필요 없이 검증 노드만 보고서를 검증하기 때문에 에너지 효율을 높일 수 있을 것이다 예상 된다.

향후 과제로는 본 논문에서 제안한 퍼지 규칙 기반 시스템으로 도출된 검증 확률로 검증 노드들의 수를 조절하여 기존의 동적 전달 중 여과 기법과 비교 하여 성능을 증명 할 수 있는 시뮬레이션을 수행할 것 이다. 또 한 본 논문에서 제안한 퍼지 규칙 기반 시스템의 입력 값이 외에 다른 입력 값들을 고려 한 후 시뮬레이션을 수행해 더 효율적인 검증 확률을 찾아 더 좋은 결과 값을 도출해 내는 것이다.

참고문헌

[1] Yu Z, Guan Y. A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks. In *Proc. SenSys*, 2005, pp.294-295.

[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] H.Y. Lee and T.H. Cho, "Fuzzy-Based Adaptive Threshold Determining Method for the Interleaved Authentication in Sensor Networks", Lect. Notes Artif. Int., vol.4293, pp.112-121, Nov. 2006.

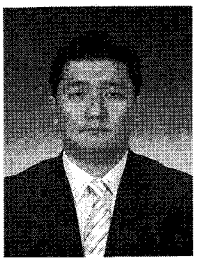
[4] Zhu S, Setia S, Jajodia S, Ning P. An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks. In *Proc. S&P*, 2004, pp.259-271.

[5] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci., "A Survey on Sensor Networks, IEEE Communications Magazine," vol. 40, no. 8, pp. 102-116, 2002.

[6] B.H. Kim, H.Y. Lee, and T.H. Cho, "Fuzzy Key Dissemination Limiting Method for the Dynamic Filtering-Based Sensor Networks", Lect. Notes Comput. Sc., vol.4681,pp.263-272,Aug. 2007.

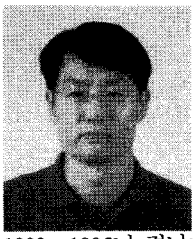
[7] Perrig A, Szewczyk R, Tygar J D, Wen V, Culler D E. SPINS: Security Protocols for Sensor Networks. *Wirel. Netw.*, 2002, 8(5): 521-534.

[8] 이해영, 조대호, "유비쿼터스 센서 네트워크에서 동적 여과를 위한 퍼지 로직 기반 경계 값 결정 기법,"디지털산업정보학회 추계학술대회, 한성대학교, pp. 1-7, 2007 년 12 월.



한 만 호

2008년 건양대학교 정보전산학과 졸업.
2008년~현재 성균관대학교 정보통신공학부 전자전기컴퓨터공학과 석사과정.
관심분야는 센서 네트워크 보안, 모델링 및 시뮬레이션



조 대 호

1983년 성균관대학교 전자공학과 학사.
1987년 Univ. of Alabama 전자공학과 석사.
1993년 Univ. of Arizona 전자 및 컴퓨터공학과 박사.
1993~1995년 경남대학교 전자계산학과 전임강사.
1995~1999년 성균관대학교 전지전자 및 컴퓨터공학부 조교수.
1999~2002년 성균관대학교 전기전자 및 컴퓨터공학부 부교수.
2002~2004년 성균관대학교 정보통신공학부 부교수.
2004~현재 성균관대학교 정보통신공학부 교수.
관심분야는 USN 모델링 및 시뮬레이션, 지능 시스템, 네트워크 보안.

이 해 영

2003년 성균관대학교 정보통신공학부 학사.
2003년~현재 성균관대학교 정보통신공학부 컴퓨터학과 박사 과정.
관심분야는 무선센서 네트워크, 지능 시스템, CAD, 인공지능, 모델링 및 시뮬레이션.