동적 여과 프로토콜 적용 센서 네트워크에서의 퍼지 기반 보안 경계 값 결정 기법

A Threshold Determining Method for the Dynamic Filtering in Wireless Sensor Networks Using Fuzzy System

이 상 진*, 이 해 영, 조 대 호
(Sang-Jin Lee, Hae Young Lee, Tae Ho Cho)

Abstract : In most sensor networks, nodes can be easily compromised by adversaries due to hostile environments. Adversaries may use compromised nodes to inject false reports into the sensor networks. Such false report attacks will cause false alarms that can waste real-world response effort, and draining the finite amount of energy resource in the battery-powered network. A dynamic en-route scheme proposed by Yu and Guan can detect and drop such false reports during the forwarding phase. In this scheme, choosing a threshold value is very important, as it trades off between security power and energy consumption. In this paper, we propose a threshold determining method which uses the fuzzy rule-based system. The base station periodically determines a threshold value though the fuzzy rule-based system. The number of cluster nodes, the value of the key dissemination limit, and the remaining energy of nodes are used to determine the threshold value.

Keywords: sensor networks, false data injection attack, false reports, security, fuzzy.

I. 서론

대부분의 센서 네트워크는 조밀하게 배치된 수 많은 센서 노드들로 이루어져 있다 [1]. 이러한 센서 네트워크는 물리적 환경과 디지털 환경을 연결 할 수 있는 특징 때문에 많은 응용분야에 적용이 가능하다. 센서 노드들은 무선통신을 기반으로 서로간에 통신을 하거나, 기지 노드(base station; 이하 BS)와 직접적으로 통신을 하게 되며 [2], 적은 메모리, 제한된 배터리 용량, 컴퓨팅 성능의 제약 등 제한적인 하드웨어 자원을 가지고 있다.

일반적으로 센서 노드들은 기반시설 없이 개방된 환경에 흩뿌려져 있기 때문에, 공격자로부터 물리적 공격에 쉽게 노출 되어진다 [3]. 공격자는 훼손된 노드를 통하여 허위보고서를 네트워크 내에 주입할 수 있다 [4]. 그림 1에서 볼 수 있듯이 허위보고서 공격은 허위 경보뿐 아니라, 허위보고서가 BS까지 전송되는 과정에서 거치는 센서 노드들이 가지고 있는 제한된 에너지를 고갈시킨다. 결과적으로, 센서 네트워크 전체 수명을 단축시켜 네트워크 기능의 마비를 초래하게 된다 [5]. 이러한 허위보고서를 조기에 탐지하고 차단하기 위해서 다양한 보안기법들 [4-8]이 제안되었으며, Yu 와 Guan이 제안한 DEF (dynamic en-route filtering scheme; 이하 DEF) [8]는 그 중 하나로써, 노드에서 탐지된 이벤트 보고서를 전달하는 과정 중에 허위보고서를 탐지 및 차단할 수 있는 기법이다.

DEF에서 보안 경계 값 선택은 보안강도와 에너지 비용을 트레이드 오프 하므로 매우 중요하다. 큰 보안 경계 값은 조기에 허위보고서를 탐지 및 차단 할 수 있지만, 전달 시 발생하는 에너지량이 크다는 단점을 가지고 있고, 적은 보안 경계 값은 전달 시 발생하는 에너지량은 작지만, 많은 수의 노드가 훼손될 경우 여과 기법이 비효율적이거나 쓸모 없게 만드는 단점을 가지고 있다. 그러므로, 보안강도와 에너지 비용 사이의 적절한 트레이드 오프를 제공하는 보안 경계 값 선택이 필요하다.

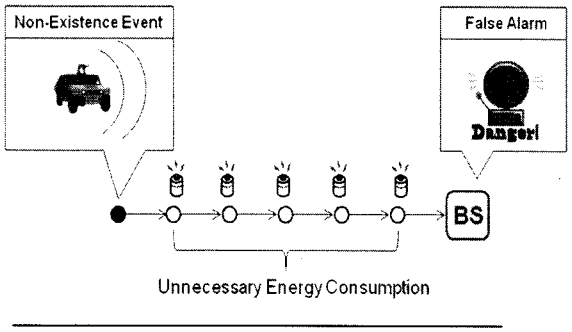


그림 1. 허위보고서 주입 공격

본 논문에서는 충분한 보안강도를 제공하면서도 에너지비용 또한 절감할 수 있는 보안 경계 값 결정 위해 퍼지 규칙 기반 시스템을 기존의 DEF에 적용시키고자 한다. 퍼지 규칙 기반 시스템은 각 클러스터의 노드 수, 키 배포제한 홉 수 및 노드의 잔여 에너지량 등의 입력 값을 통하여 보안 경계 값을 결정하게 된다.

본 논문은 다음과 같이 구성된다. 2장에서는 허위보고서 공격 여과기법 중 하나인 DEF에 대하여 간략하게 설명하고, 3장에서는 DEF의 적절한 보안 경계 값을 위해서 제안된 퍼지기반 보안 경계 값 결정 기법을 설명한다. 마지막으로 4장에서는 결론과 향후 과제에 대해서 언급할 것이다.

II. 동적 여과 기법 (DEF)

허위 보고서를 조기에 탐지 및 차단하기 위해서 Yu 와

* 책임저자(Corresponding Author)
논문접수 : 2008. 7. 21., 채택확정 : 2008. 7.31.
이상진, 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)

Guan은 DEF [8]를 제안하였다. 기존의 기법들과 비교하여 DEF는 센서 네트워크에서의 위상 변화에 대해서 능동적으로 대처가 가능하다. DEF에서는 이벤트 탐지 노드에서 생성한 메시지 인증 코드(message authentication code; 이하 MAC)로서, 정상 보고서인지, 허위 보고서인지를 판별한다. DEF 기법은 배포 전 단계, 배포 후 단계, 검증단계의 3가지 단계로 구성되어져 있다.

배포 전 단계에서, 각 노드들은 인증키 생성을 위한 키와 인증키 전달시 이를 암호화 하기 위한 공유키 풀에서 임의로 얻어진 l+1개의 비밀 키를 적재하게 된다.

배포 후 단계에서, 모든 노드는 자신의 인증 키를 l +1개의 비밀 키를 통해 암호화 한 후 자신이 속한 클러스터 내의 대표 노드(cluesterhead; 이하 CH)에게 보낸다. 클러스트 내의 노드들에게 인증 키를 받은 CH는 이것을 조합하여 메시지 형태로 변환 후 자신의 근처 전달 노드에게 미리 정해진 홉 수만큼 배포하게 된다. 인증키 분배 메시지를 받은 각 전달 노드들은 자신이 가지고 있는 비밀 키와 같은 비밀키로 암호화된 인증키가 있는지 검사하여, 같은 비밀키가 있다면, 복호화하여 해당 인증 키를 저장하고, 없다면 다음 전달 노드에게 인증키 분배 메시지를 전달하게 된다.

마지막으로 여과단계에서는, 각 노드들은 배포 후 단계에서 분배된 인증 키를 이용하여 이벤트 내의 MAC 검증함으로써 허위보고서를 탐지 및 차단 할 수 있다.

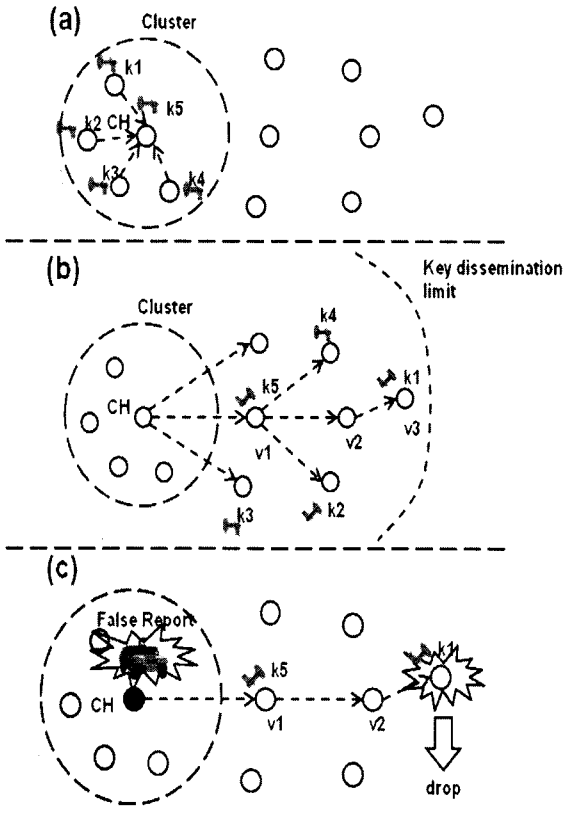


그림 2. DEF의 키 분배 및 여과과정.

그림 2는 DEF에서의 키 분배단계 및 여과과정을 나타 낸 것이다. 각 클러스터내의 센서 노드들은 자신의 인증 키를 비밀키로 암호화한 후 CH에게 보낸다(그림 2(a)). 각 센서 노드들에게 인증 키를 받은 CH는 미리 정해진 배포 홉 수만큼 인증 키를 배포한다(그림 2(b)). 그림 2(c)에서 CH를 획득한 공격자는 허위보고서 상에 해당 MAC을 첨부하고 나머지 MAC은 임의 값으로 채워 넣게 된다. v1은 CH의 MAC을 검증할 수 있는 인증 키를 가지고 있지만 공격자가 이미 해당 MAC을 획득하여 여과과정 없이 지나갈 수 있지만, 결국 v3에서 허위보고서는 해당 MAC 값을 허위로 생성하였으므로 탐지 및 차단된다.

III. 퍼지 기반 경개 값 결정 기법

3.1. 가정

센서 노드들은 배포 후 여러 개의 클러스터로 구성된다고 가정한다. 센서 노드들은 에너지 소모의 균형을 맞추기 위해서 CH는 노드간에 서로 교대로 선출 되어진다. BS는 클러스터안 의 노드 수, 키 배포 제한 홉 수, 각 노드들의 에너지량을 알 수 있다고 가정한다. 또한 BS는 방송 메시지를 인증할 수 있는 메카니즘을 가지고 있고, 모든 노드는 방송 메시지를 검증할 수 있으며, 센서 노드는 물리적 공격에 대해서 안전 하다고 가정한다.

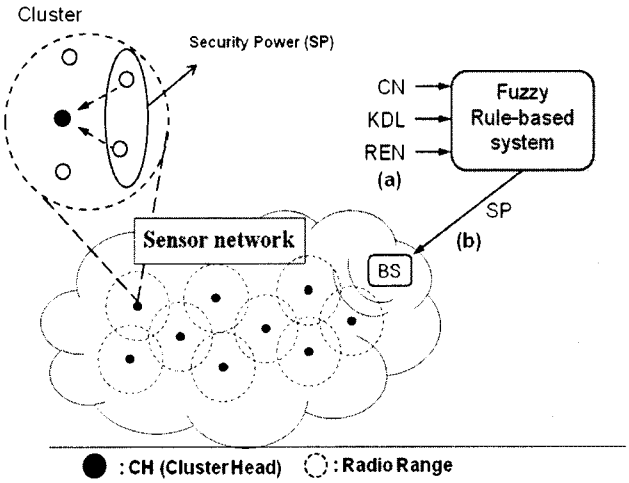


그림 3. 퍼지기반 경계 값 결정 기법

3.2. 개요

본 논문에서 제안한 경계 값 결정 기법에서 BS는 퍼지 규칙 기반 시스템을 통하여 주기적으로 보안 경계 값을 결정한다. 퍼지 시스템 입력 값으로는 각 클러스터의 노드의 수, 키 배포 제한 홉 수, 그리고 각 노드들의 잔여 에너지량이 사용된다(그림 3(a)). BS는 결정된 보안 경계 값을 해당되는 CH에게 배포하게 된다(그림 3(b)). 기존 DEF의 고정된 보안 경계 값은 이벤트 발생지역의 상태와 상관없이 값을 부여하였으나 제안한 경계 값 결정 기법은 필요 시 센서 네트워크 상황에 따라서 각기 다른 보안 경계 값을 부여하는 것이 가능하다. 이것은 제안한 기법이 기존 DEF보다 좀 더 유연한 보안 경계 값을 부여할 수 있다는 것을 의미한다. 예를 들어, 센서 노드들의 에너지가 많이 고갈된 상태에서 고정된 높은 보안 경계 값은 이벤트 보고서 생성시 많은 양의 에너지를 소비하게 되며, 이것은 센서 네트워크 수명에 영향을 미치게 된다.

이와 대조적으로, 제안한 기법은 클러스터 안의 노드 수, 키 배포 제한 홉 수, 각 노드들의 에너지량의 입력 값을 고려하여 보안 경계 값을 결정하기 때문에, 상황에 맞는 적절한 SP 값 설정이 가능하다.

3.3. 경계 값 결정 기법을 위한 입력 값

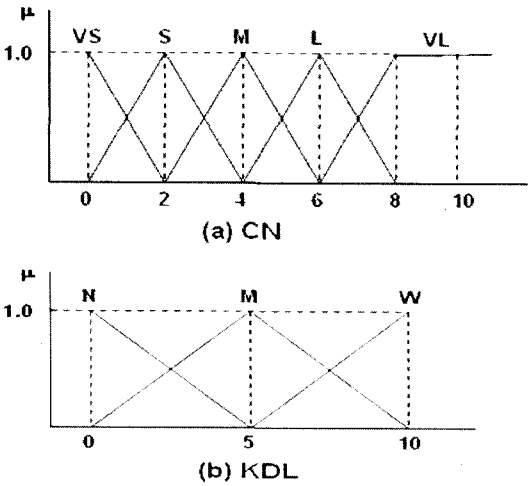
DEF에서 보안 경계 값(이하 SP)은 각 클러스터내의 노드 수(이하 CN)보다 커질 수 없다. 각 보고서에 붙는 MAC들은 클러스터내의 노드들의 인증 키들로 생성되어진다. 만약 6개의 노드로 구성된 클러스터가 있다면, 보고서는 0~6 까지의 MAC을 포함할 수 있다. 그러므로 SP는 CN을 고려하여 결정돼야 한다. CN의 값은 노드의 에너지 고갈이나 훼손으로 인한 재 배치 등으로 변경될 수 있다.

큰 값의 인증키 배포제한 홉 수(이하 KDL)은 센서 네트워크 내에 많은 수의 노드들이 인증 키를 가질 확률이 높아진다는 것을 의미하고, 이것은 허위보고서 여과 확률이 높아진다는 것을 뜻한다. 높은 SP값이 설정된다 할지라도 KDL값이 낮으면 KDL값이 높았을 때 보다 낮은 확률로 허위보고서를 여과하게 될 것이다. 그러므로 KDL 또한 SP 선택 시 고려해야 할 사항이다.

센서 네트워크는 한정적인 자원을 가지고 동작하므로 에너지는 반드시 고려해야 할 요소 중 하나이다. 각 노드들의 에너지 잔여량(이하 REN)이 거의 다 고갈된 상태에서의 높은 SP 값은 전체 센서 네트워크 동작에 장애가 되므로, 차라리 SP 값을 낮게 설정하거나 SP 값을 0으로 설정하여 네트워크의 수명을 연장시키는 것이 더욱 더 바람직하다. 그러므로 SP 결정 시 REN 또한 반드시 고려해야 한다.

4. 퍼지 규칙 설계

그림 4.(a),(b), 그리고 (c)는 제안된 퍼지 규칙 시스템의 3가지입력 변수(CN, KDL, 및 REN)에 대한 멤버십 함수이다



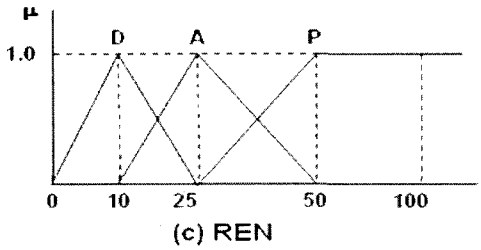


그림 4. 퍼지 입력 값 멤버십 함수.

다음은 퍼지 입력 변수들의 명칭들을 나타낸다.

- CN = {VS (Very Small), S (Small), M (Medium), L (Large), VL (Very Large)}
- KDL = {N (Narrow), M (Medium), W (Wide)}
- REN = {D (Deficiency), A (Average), P (Plenty)

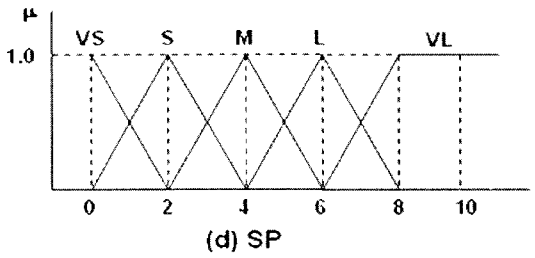


그림 5. 퍼지 출력 값 멤버십 함수.

그림 5는 제안된 퍼지 규칙 시스템의 출력 변수에 대한 멤버십 함수이며, 각 명칭들은 다음과 같다.

SP = {VS, S, M, L, VL}

퍼지 규칙 시스템은 3가지 입력 파라미터 값을 이용하여 상황에 맞는 출력 값 SP를 결정한다. 표 1은 제안된 기법의 퍼지 규칙 중 일부를 나타낸 것이다.

표 1. 퍼지 규칙

Rule #	IF			THEN
	CN	KDL	REN	SP
01	VL	W	D	S
02	VL	W	P	L
03	VL	M	D	VS
04	VL	M	P	M
05	VL	N	D	VS
06	VL	N	P	VL

기본적으로 SP는 CN과 KDL을 기반으로 SP 값을 결정한다. 하지만 REN이 충분하지 못하다면 SP를 낮은 값으로 설정하게 된다. 에너지 고갈로 인해 동작이 마비되는 것 보다는 보안강도를 낮추어서 네트워크 전체 수명을 연장하는 것이 더 효율적이기 때문이다.

IV. 결론 및 향후 과제

DEF에서 보안 경계 값 결정은 에너지 비용과 보안강도 사

이에서 트레이드 오프 하므로 매우 중요하다. 기존의 DEF상에서 고정된 보안 경계 값은 네트워크 상황에 맞는 적절한 보안 경계 값 선택이 불가능하였다. 본 논문에서는 네트워크 상황에 맞는 효율적인 보안 경계 값을 도출하고자 퍼지 규칙 기반 보안 경계 값을 결정 기법을 제안하였다. 향후 과제로 제안된 퍼지 규칙 기반 시스템으로 도출된 SP 값이 본래의 DEF와 비교하여 얼마나 효율적인 성능을 보이는지를 분석하기 위한 시뮬레이션을 수행할 것이며, 본 논문에서 제안한 입력 값 이외에 다른 요소들도 입력 값으로 선택하여 좀 더 효율적인 SP값을 결정할 수 있는 것들을 찾아내 보고자 한다.

참고문헌

[1] 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.

[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] Przydatek I, Song D, Perrig A. SIA: Secure Information Aggregation in Sensor Networks. In Proc. SenSys, 2003, pp.255-265.

[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] Ye F, Luo H, Lu S. Statistical En-Route Filtering of Injected False Data in Sensor Networks. *IEEE J. Sel. Area Comm.*, 2005, 23(4): 839-850.

[6] Yang H, Lu S. Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks. In *Proc. VTC*, 2003, pp.1223-1227.

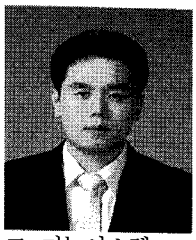
[7] F. Li and J. Wu, 'A probabilistic voting-based filtering scheme in wireless sensor networks,"Proc. IWCMC, pp.27–32, July 2006.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

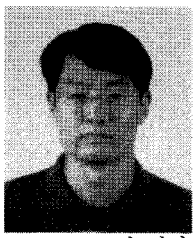


이 상 진

2007년 백석대학교 정보통신공학부 학사.

2008년~현재 성균관대학교 정보통신공학부 전자전기컴퓨터공학과 석사과정.

관심분야 : 정보보호, 무선센서 네트워크, 지능시스템



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.

관심분야 : USN 모델링 및 시뮬레이션, 지능 시스템, 네트워크 보안.

이 해 영

2003년 성균관대학교 정보통신공학부 학사.

2003년~현재 성균관대학교 정보통신공학부 컴퓨터공학과 박사과정.

관심분야 : 무선센서 네트워크, 지능 시스템, CAD, 인공지능, 모델링 및 시뮬레이션.