동적 여과 기법 기반의 무선 센서네트워크에서 효율적인 키 분배를 위한 퍼지 로직 기반 결정 기법

Effective Key Disseminating Method for Fuzzy Logic Based Dynamic Filtering in Wireless Sensor Network

김 종 현*, 조 대 호*
Jong-Hyun Kim, Tae-Ho Cho

Abstract

최근 새롭게 등장한 무선 센서 네트워크는 기존의 네트워크와는 다르게 통신 인프라가 없는 환경에서도 동작이 가능한 저전력 소출력의 무선 센서간의 네트워크를 형성하고 이들간의 정보 유통이 이루어진다. 무선 센서 네트워크는 열린 환경에서 배치되기 때문에 물리적 공격에 취약하다. 공격자는 손쉽게 노드들을 포획할 수 있으며 포획된 노드를 통해 허위 보고서를 네트워크에 주입할 수 있다. 허위 보고서 삽입 공격은 허위 경보를 유발할 뿐만 아니라 네트워크의 제한된 에너지를 고갈시킨다. 이러한 허위 보고서를 조기에 탐지 및 폐기하기 위하여 Yu와 Guan은 동적 여과 프로토콜(dynamic en-route filtering scheme)를 제안하였다. 그러나 무선 센서 노드는 오직 제한된 전력 자원으로 이루어져 있기 때문에 견력보존과 전력관리가 중요시 여겨진다. 본 논문에서는 동적 여과 프로토콜에서 허위 보고서 주입 공격에 대한 충분한 보안 강도 제공과 에너지 효율성을 위한 기법을 제안한다.

Keywords : 센서 네트워크, 동적 여과 기법, 허위 보고서 삽입 공격, 퍼지 로직

I. 서 론

최근 마이크로 전자장치시스템과 무선 통신 기술의 발전은 저비용, 저전력, 다기능을 갖춘 센서 네트워크의 발전을 가져왔다. 이러한 센서 네트워크의 발전은 군사, 의료, 환경 등에서 응용이 실현 가능하게 되었다. 무선 센서 네트워크는 수많은 센서 노드들이 조밀하게 배치 되어있고 이러한 센서 노드들은 감지, 데이터 처리, 그리고 통신기능으로 구성된다[1]. 하지만 무선 센서 노드는 오직 제한된 전력 자원으로 이루어져 있으므로 센서 노드 생존기간은 배터리 생존기간과 강하게 의존된다. 무엇보다도 전장 지역과 같이 접근하기 힘든 지역에서 제한된 에너지를 사용하기 때문에 센서 노드의 에너지 효율 관점은 중요시 여겨진다[2].

센서 네트워크에서 센서 노드들은 일반적으로 열린 환경에서 독립적으로 동작하기 때문에 보안 공격에 취약하다[3]. 만약 공격자가 노드를 포획하여 허위 정보를 담은 허위 보고서를 생성해서, 이 허위 보고서를 공격자에게 포획당한 노드를 통해 센서 네트워크에 삽입할 수 있다. 이 허위 보고서 공격은 그림 1과 같이 허위 보고서를 베이스 스테이션(base station; 이하BS)에서 전달함으로써 허위 정보(false alarm)을 유발시킬 수 있을 뿐만 아니라, 센서 노드들의 제한된 에너지 자원을 고갈시킨다. 이는 센서 네트워크 전체 수명을 단축시켜 네트워크 기능의 마비를 초래하게 된다[4]. 허위 보고서의 피해를 최소화하기 위해서는 가능한 빨리 허위 보고서를 전송 중에 발견하여 걸러 내야하며, 걸러지지 않은 허위 보고서는 BS에서 발견하고 제거되어야 한다[5]. 허위 보고서 삽입 공격을 방어하기 위해 다양한 기법들 [4],[6-8]이 제안되었다. Yu와 Guan이 제안한 동적여과 기법(dynamic en-route filtering scheme; 이하 DEF)은 노드에서 감지된 이벤트 보고서를 전달 노드를 통해 전달 중 허위 보고서를 탐지 및 폐기할 수 있는 기법 중 하나이다. 하지만 DEF에서 전달 노드를 선택하고 키 배포할

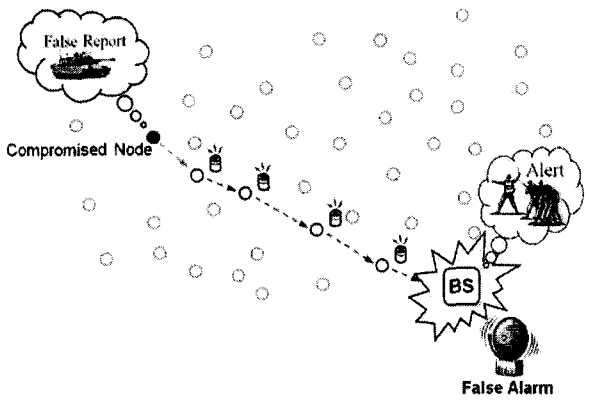


그림 1 허위보고서 삽입 공격

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

경우 전달 노드에서 키가 중복되어서 에너지가 소모되거나 키를 획득하지 못하여 보안능력을 상실 할 수 있는 단점이 있다. 그러므로 효율적인 키 배포를 위해 다음 홉의 노드 선택이 중요히 여겨진다.

본 논문에서는 키를 배포할 경우 전달 노드의 키의 중복 방지와 키를 적절히 배포하여 에너지 효율성과 적절한 보안 강도를 위해 기존 DEF에 퍼지 로직 시스템을 적용시키고자 한다. 퍼지 로직 시스템은 각 다음 홉 노드로부터의 거리, 에너지 잔여량 그리고 중복체크 등의 입력 값을 통하여 적절한 보안 경계 값을 결정하게 된다.

본 논문은 다음과 같이 구성된다. 2장에서는 DEF에 대해 간략하게 설명하고, 3장에서는 퍼지로직을 이용한 제안 기법을 설명한다. 마지막으로 4장에서는 결론과 향후 과제에 대해서 언급할 것이다.

II. 동적 여과 기법

Yu와 Guan은 허위 보고서를 조기에 탐지 및 폐기하기 위하여 동적 여과 기법[8]을 제안하였다. 동적 여과 기법은 다른 기법들과 비교하여 무선센서네트워크의 동적 위상을 잘 처리할 수 있으며, 특히 큰 규모의 무선센서네트워크에서 다른 기법들에 비해 에너지 소비가 효율적이다. DEF는 그림 2와 같이 배포 전 단계(pre-deployment phase), 배포 후 단계(pro-deployment phase), 그리고 여과 단계(filtering phase)로 구성된다. 배치 전 단계는 노드가 배치되기 전에 한번만 수행되는 반면 배치 후 단계 및 여과 단계는 여러 번 수행된다.

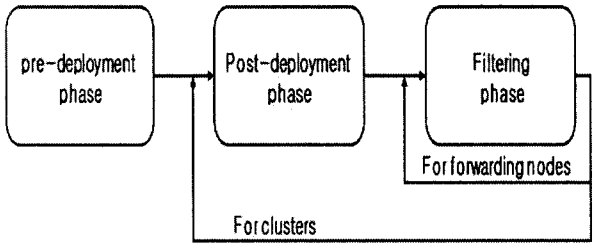


그림 2 DEF 3단계

배치 전 단계에서, 각 노드는 하나의 인증키와 인증키를 암호화하기 위해서 전역키 풀에서 임의로 선택된 1 + 1개의 비밀 키들을 적재한다. 배포 후 단계에서, 그림 3(a)와 같이 모든 클러스터 노드는 자신의 1 + 1개의 비밀키를 이용하여 자신의 인증키를 암호화 한 후 클러스터 헤드(cluster head; 이하 CH)에게 보낸다. CH는 암호화된 인증키를 보고서 형식으로 변환 후 클러스터 내의 전달 노드에게 정해 진 홉 수만큼 힐 크라임빙(Hill Climbing)방식으로 배포된다. 배포 된 인증키 보고서를 받은 각 전달 노드는 비밀키를 확인하여 같은 비밀 키를 가지고 있다면 복호화하여 인증키를 저장하고, 다음 전달노드에게 인증키 보고서를 퍼뜨린다(그림3(b)). 마지막 여과 단계에서, 허위 보고서들은 전달 노드들에게 의하여 분배된 인증 키를 이용하여 메시지 인증 코드(message authentication code; 이하 MAC)을 검증하여 탐지되어 폐기된다.

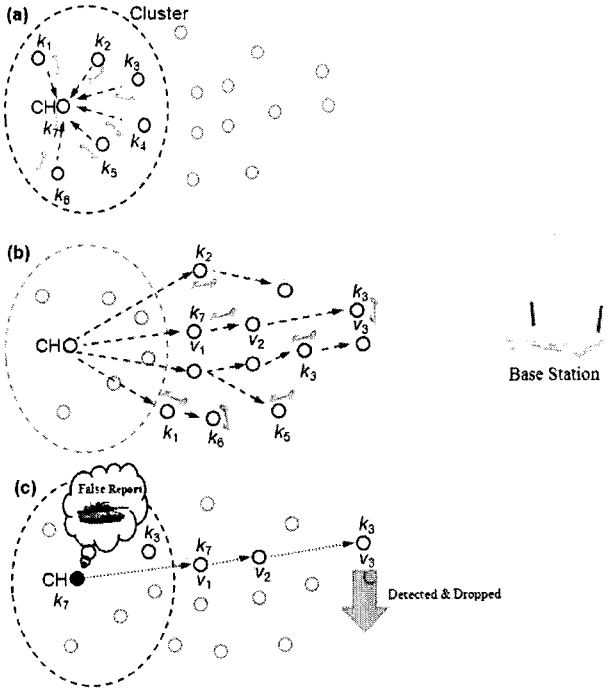


그림 3 DEF의 키 분배 및 여과 단계

그림 3(c)에서 공격자가 CH를 포획하였다고 생각해보자. 공격자는 전달 노드 v1과 공유하는 인증키 k7을 획득하였고 v2는 인증키가 없으므로 검증 없이 다음 전달 노드 v3에게 전달된다. 하지만 v3에서의 k3는 획득되지 않았기 때문에 허위 보고서는 v3에 의하여 탐지되어 폐기될 것이다.

III. 퍼지 기반 경계 값 결정 기법

1. 가정

각 노드들은 배치 후 여러 개의 클러스터로 구성되어진다고 가정한다. CH는 노드간의 에너지 잔여량의 균형을 위해서 서로 교대로 선출된다. BS는 클러스터내의 노드 수, 키 배포 제한 홉 수, 각 노드들의 에너지량을 알 수 있다. 또한 BS는 방송 메시지를 인증할 수 있는 메커니즘을 가지고 있고, 모든 노드는 방송 메시지를 검증할 수 있으며, 센서 노드는 물리적 공격에 대해서 안전 하다고 가정한다. 마지막으로 DEF에서는 GPSR/GEAR[9] 프로토콜을 사용한다고 가정한다.

2. 개요

본 논문에서는 적절한 보안경계 값(이하 FK)를 선택하기 위해 DEF내에 퍼지 로직 기반 시스템을 적용하였다. 퍼지로직은 1960년대 중반 Lotfi-Zadeh [10]이 소개하였고 오직 참 그리고 거짓만을 선택할 수 있는 디지털 장치의 특성을 보안하기 위한 기법으로 IF-THEN 규칙을 통하여 명확하게 이분화되지 않는 상황에서 적절한 결과 값을 도출해내기 위한 방법 중 하나이다[11]. 키 배포 시 노드의 키 중복(이하 COK), 노드가 상태(이하 CNC), 노드의 에너지 잔여량(이하 NEL), 그리고 이웃 노드까지의 거리(이하 DN)을 입력 값들로 도출 된 적절한 보안 경계 값은 그림

4같이 BS에게 전달되고 BS는 각각의 CH들에게 전달된다. 위상의 변화와 주기로 인한 키를 재 배포할 경우 각 전달 노드들은 입력 값들로부터 도출된 결과 값으로 이웃노드를 선택하고 이러한 과정은 키 재배포시마다 반복된다. DEF에서 FK는 키를 배포 하기 위한 다음 홉 노드들의 선택 값(이하 q)보다 커질 수 없다.

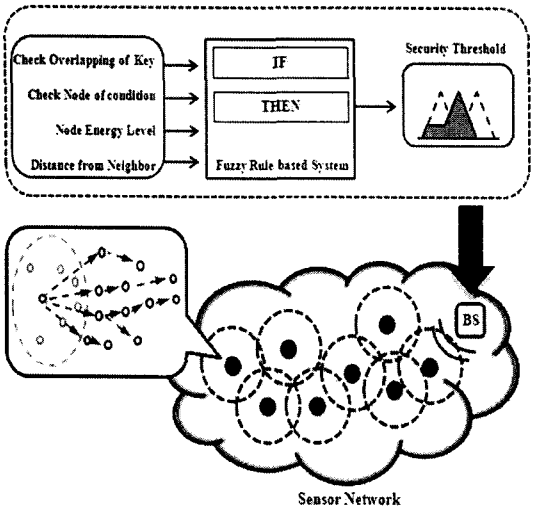


그림 4 제안된 퍼지 기반 기법의 개요

3. 경계 값 결정을 위한 입력 값

FK는 DEF에서 키 배포 시 다음 홉의 노드에 키의 중복성, 노드의 상태, 에너지 잔여량과, 노드간의 거리를 고려하여 키 배포를 위한 적절한 노드를 선택할 수 있다. 높은 보안 경계 값(이하 FK)는 q범위 내에서 최대한 많은 수의 노드들에게 키를 배포한다. 예를 들어 미리 정해진 q값이 4일 경우 그리고 FK의 값이 VL일 경우 다음 홉 4개의 노드들에게 키를 배포할 수 있다. 하지만 입력 값 중에서 다음 홉 노드의 키 중복 확인(이하 COK)값이 중복(이하 Y)일 경우 아무리 노드의 에너지 잔여량(이하 NEL)의 값이 높고(이하 AH) 그리고 다음 홉 이웃 노드까지의 거리(이하 DN)의 값이 높을(이하 VS) 경우라도 그 키 중복된 노드에게 키를 배포하지 않는다. 또한 다음 홉 노드의 노드 상태 확인(이하 CNC)값이 D이거나 S일 경우 아무리 노드의 에너지 잔여량(이하 NEL)의 값이 높고(이하 AH) 그리고 다음 홉 이웃 노드까지의 거리(이하 DN)의 값이 높을(이하 VS) 경우라도 작동되지 않는 노드에게 키를 배포하지 않는다.

4. 퍼지 로직 설계

다음 그림은 제안된 퍼지 로직 시스템의 입력 값 4가지 (COK, CNC, NEL, DN)에 대한 맴버쉽 함수이다.

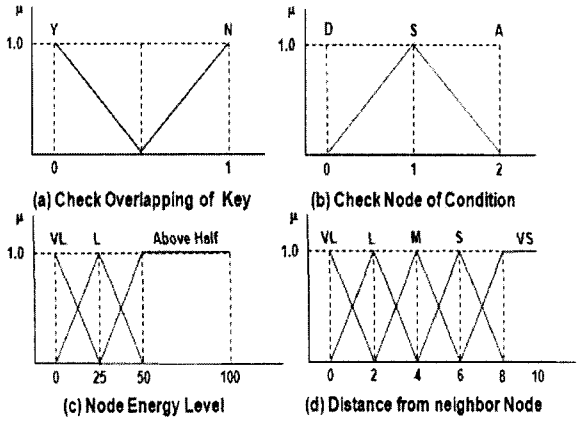


그림 5 퍼지 입력 값 멤버쉽 함수

다음은 퍼지 입력 변수들의 명칭을 나타낸다.

- COK = { Y (Yes) , N (No) }
- CNC = { D (Death), S (Sleep), A (Activity) }
- NEL = { VL (Very Low), L(Low), AH(Above Half)
- DN = { VS (Very Short), S (Short), M (Medium), L (Long), VL (Very Long)

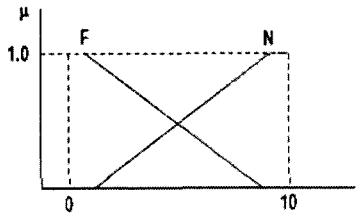


그림 6 퍼지 출력 값 멤버쉽 함수

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

- FK = { F (Forward key), N (None) }

표1은 퍼지 규칙들의 일부이다. 기본적으로 퍼지 규칙 기반 시스템은 COK와 CNC를 기반으로 FK를 결정한다. 입력 값 NEL과 DN의 값이 크다고 해도 COK값이 Y이고 CNC값이 D 또는 S일 경우 FK값은 N를 선택한다. 하지만 COK와 CNC값이 만족될 경우 나머지 NEL과 DN으로 F를 선택하게 된다.

표 1 퍼지 규칙

Rule No.	IF				THEN
	COK	CNC	NEL	DN	FK
01	Y	D	L	VL	N
06	Y	D	AH	VS	N
13	Y	A	AH	S	N
22	N	D	AH	S	N
27	N	S	AH	S	N
35	N	A	L	S	F

VI. 결론 및 향후 과제

본 논문에서는 동적 여과 기법의 동작과정을 설명하였다. DEF에서 보안 경계 값 결정은 에너지 비용과 보안 강도에서 트레이드 오프 하므로 매우 중요하다. 기존의 DEF 상에서 고정된 보안 경계 값은 네트워크 상황에 맞는 적절한 보안 경계 값 선택이 불가능하였다. 본 논문에서는 네트워크 상황에 맞는 효율적인 보안 경계 값을 도출하고자 퍼지 로직 기반 보안 경계 값을 결정하는 기법을 제안하였다. 향후 과제로 제안된 퍼지 로직 시스템으로 도출된 FK 값이 본래의 DEF와 비교하여 얼마나 효율적인 성능을 보이는지 시뮬레이션을 보여주고 분석할 것이다. 그리고 본 논문에서 보여준 FK을 좀 더 효율적으로 도출하기 위한 입력 값 및 다른 방식을 찾아보고자 한다.

이 논문은 교육과학기술부의 재원으로 시행하는 한국 과학 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] D. Culler, D. Estrin, and M. Srivastava, "Overview of Sensor Networks, "*IEEE Computer*, vol. 37, no. 8, pp. 41-49, Aug. 2004.

[3] 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.

[4] F. Ye, H. Luo, and S. Lu, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839-850, Apr. 2005.

[5] 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.

[6] Yu, Z. Guan, Y. (2005), "A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks", Proc. of SenSys, pp. 294-295, *ACM*.

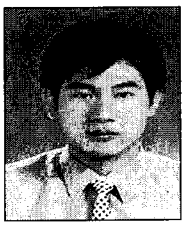
[7] Yang, H., Lu, S. (2004), "Commutative Cipher Based En-route Filtering in Wireless Sensor Networks", Proc. of VTC, pp. 1223-1227, *IEEE*.

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

[9] Y. Yu, R. Govindan, and D. Estrin, "Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks", in *UCLA Computer Science Department* Technical Report UCLA/CSD-TR-01-0023, May 2001

[10] A.A. Elsamiee, The development of AWS AND introductory to the IWS, intelligent weather system, in: *TECO 2006 - WMO Technical Conf*, 2006.

[11] M. Yusuf, T. Haider, Energy-aware fuzzy routing for wireless sensor networks, in: *IEEE International Conf on Emerging Technologies*, 2005.



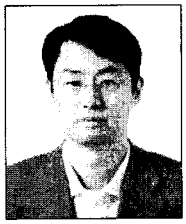
김 종 현

2009년 단국대학교 컴퓨터과학과 졸업

2009년~현재 성균관대학교 정보통신학부 전자전기컴퓨터공학과석사과정

<관심분야> 정보보호, 무선센서 네트워크, 지능시스템

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



조 대 호

1983년 성균관대학교 전자공학과 학사.

1988년 Univ. of Alabama 전자공학과 석사.

1993년 Univ. of Arizona 전자및컴퓨터공학과 박사

<관심분야> USN 모델링 및 시뮬레이션, 지능시스템, 네트워크 보안.

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