여과기법 보안효율을 높이기 위한 센서네트워크 클러스터링 방법

Enhancing Method to make Cluster for Filtering-based Sensor Networks

김 병 희, 조 대 호*
(Byung-Hee Kim and Tae-Ho Cho)

Abstract : Wireless sensor network (WSN) is expected to be used in many applications. However, sensor nodes still have some secure problems to use them in the real applications. They are typically deployed on open, wide, and unattended environments. An adversary using these features can easily compromise the deployed sensor nodes and use compromised sensor nodes to inject fabricated data to the sensor network (false data injection attack). The injected fabricated data drains much energy of them and causes a false alarm. To detect and drop the injected fabricated data, a filtering-based security method and adaptive methods are proposed. The number of different partitions is important to make event report since they can make a correctness event report if the representative node does not receive message authentication codes made by the different partition keys. The proposed methods cannot guarantee the detection power since they do not consider the filtering scheme. We proposed clustering method for filtering-based secure methods. Our proposed method uses fuzzy system to enhance the detection power of a cluster.

Keywords: Wireless sensor network, false data injection attack. filtering scheme, fuzzy system.

I. 서론

무선 통신 기술의 발전, 저전력 회로 설계와 연산 장치의 소형화 등의 발달로 무선 센서 네트워크(WSN: Wireless sensor networks)에 대한 많은 연구가 이루어 지고 있다. 실 생활에 많은 도움을 줄 것으로 기대되는 WSN는 위험지역 감시, 공장 자동화, 지능형 빌딩, 화재 감시 등 많은 응용분야에 이용이 가능할 것으로 예상 된다 [1].

WSN의 많은 응용분야에서 관심 이벤트를 감지하고 감지 정보를 전달하는 다수의 센서 노드(sensor node)들과 센서 노드들이 감지한 정보를 수집 및 외부 네트워크와 연결하기 위한 기지국(BS: Base station)들로 구성된다. WSN의 다수를 이루고 있는 센서 노드는 하드웨어적(Hardware)인 크기의 제약으로 인해 감지(sensing), 계산(computation), 에너지(Energy), 무선 통신(wireless communication) 등에 제약사항들 가지고 있다. 또한 센서 노드는 많은 WSN 응용분야에서 광범위한 센서필드(sensor field) 내에 무작위로 배치된다. 광범위한 지역에 무작위로 배치된 센서 노드는 개개의 관리가 불가능 하며, 베터리(battery)의 교환이나 충전이 불가능 하다. 이런 WSN의 물리적, 환경적 제약으로 인해 악의적 목적을 가진 공격자(adversary)들은 배치된 센서를 물리적으로 쉽게 획득(compromising) 할 수 있으며, 획득한 센서 노드의 암호 키들을 사용하여 허위 데이터(false data)를 WSN에 삽입할 수 있다 [2]. 삽인 된 허위 데이터는 제한된 센서 노드의 에너지 자원을 고갈시킬 뿐만 아니라, 허위 경보(false alarm)를 일으켜 WSN에 혼란을 야기 시킬 수도 있다. 그림 1은 허위 데이터 삽입 공격(**False data injection attack**)을 보여준다. 허위 데이터에 의한 피해를 줄이기 위해서는, 데이터 전송 도중에 데이터의 허위 유무를 판별하여 허위 데이터를 걸러내야 하며, 걸러지지 않은 허위 데이터는 BS에서 제거 해야만 한다.

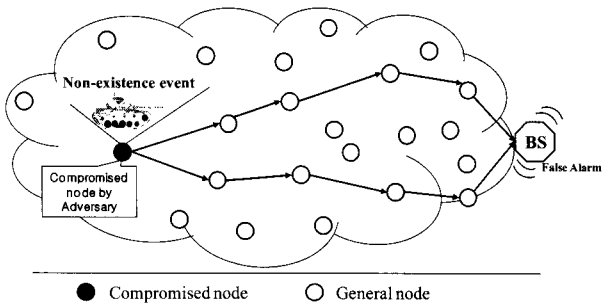

그림 1. 허위 데이터 삽입공격.

허위 데이터 삽입 공격을 방어하기 위go 허위 데이터 검증 기법[3,4,5]들과 제안된 기법의 성능을 향상 시키기 위한 기법[6,7,8]들이 제안 되었다. 제안된 여과 기법들 중 하나인, 통계적 여과 기법(statistical en-route filtering scheme)[3]에서는 이벤트 보고서(event report)를 만들기 위해 임계 값(threshold) 이상의 이벤트 감지 노드와 서로 다른 파티션 키(partition key)가 필요하다. 만약 임계 값 이상의 이벤트 감지 노드와 서로 다른 파티션 키가 없으면 정상 이벤트 보고서를 생성하지 못하게 된다. 이는 WSN의 기능 장애를 야기하며, 정상적인 이벤트 정보를 획득하지 못하는 문제점이 발생시킨다.

센서 노드들의 에너지 효율적인 데이터 수집과 데이터 전송을 위한 클러스터링(clustering) 방법[9,10]이 제안 되었다. 클러스터링 방법은 WSN을 여러 클러스터 지역으로 나누어, 클러스터 지역 안의 센서 노드들이 협력하여 데이터를 감지고 데이터를 전송하여 중복된 데이터 전송을 제한하는 에너지 효율적인 방법이다. 하지만 제안된 클러스터링 방법은 통계적 여과 기법의 특징들을 고려하지 않아 통계적 여과 기법에 적용하기에 힘들다는 문제점이 있다. 통계적 여과 기법에 효율적인 감지 능력(Detection power)을 보장하고 정상 이벤트 보고서 생성을 위해서는 서로 다른 파티션으로

* 책임저자(Corresponding Author)
논문접수 : 2008. 7. 22. 채택확정 : 2008. 7. 30.
김병희, 조대호 : 성균관대학교 전자전기컴퓨터공학과
(bhkim@ece.skku.ac.kr, taeho@ece.skku.ac.kr)
※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0028).

구성된 임계 값 이상의 센서 노드들로 클러스터가 구성 되어야 한다.

본 논문에서는 퍼지시스템을 이용한 여과기법 보안효율을 높이기 위한 클러스터링 방법을 제시한다. 효율적인 클러스터링을 위해 퍼지시스템은 클러스터 지역의 대표노드인 클러스터 헤드(CH: cluster head)와 BS와의 거리, 파티션 정보, 그리고 클러스터 안의 센서 노드 수를 고려한다. 퍼지시스템을 이용하여 각각의 센서 노드는 클러스터링 적합도를 고려한 클러스터 지역을 선택하여 통계적 여과 기법에 적합한 클러스터 지역을 형성 할 수 있다.

본 논문의 구성은 다음과 같다. 제 2장에서는 통계적 여과 기법과 클러스터링에 대해 기술하고, 본 연구를 진행하게 된 동기를 설명한다. 제 3장에서는 여과기법 보안 효율을 높이기 위한 방법을 기술한다. 마지막 4장에서는 결론과 향후 연구 과제를 논의한다.

II. 관련 연구

이 장에서는 통계적 여과 기법과 클러스터링 방법에 대해 기술하고 본 연구를 진행하게 된 동기를 설명한다.

1. 통계적 여과 기법

통계적 여과 기법은 허위 데이터 삽입 공격과 그 대응 방안을 언급한 첫 논문이다. 허위 데이터 삽입 공격을 방어하기 위해 이벤트 보고서에 메시지 인증 코드(message authentication code)를 넣어 이벤트 보고서의 허위 유무를 판별 할 수 있도록 하였다. 통계적 여과 기법에서는 데이터의 허위 유무를 판별하기 위해 키 정보를 이용한다. 센서 노드는 센서필드에 배치되기 전, 여러 개의 파티션으로 나눠진 키 풀(key pool)에서 하나의 파티션을 선택하고 파티션에 있는 키를 랜덤으로 선택하여 메모리에 저장한다.

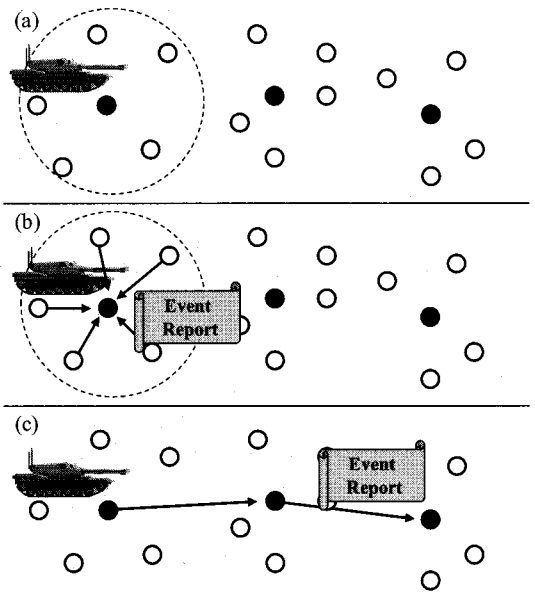

그림 2. 통계적 여과 기법에서의 이벤트 보고서 전달.

센서노드 배치 후, 센서필드에 관심 이벤트(e.g., 전쟁 지역에서 적을 발견)가 발생하면(그림 2(a)), 이벤트 발생지역의 센서 노드들은 이벤트를 감지한다. 이벤트를 감지한 노드들 중 한 노드가 대표노드가 되어 이벤트 감지 노드들로부터 감지한 이벤트 정보와 함께 메시지 인증 코드를 수집한다 (그림 2(b)). 대표노드는 수집한 이벤트 정보와 메시지 인증 코드를 이용하여 이벤트 보고서(event report)를 만들고, 이를 BS로 전달한다 (그림. 2(c)). 이벤트 보고서는 다른 파티션에 속하는 키로 만들어 진 임계 값만큼의 메시지 인증 코드로 만들어 진다. 대표노드에서 만들어진 이벤트 보고서는 전송경로상에 있는 센서 노드를 통해 BS로 전달 한다. 전달노드가 이벤트 보고서를 받으면, 임계 값만큼의 서로 다른 파티션으로 만들어진 메시지 인증 코드가 있는지 확인한다. 임계 값만큼의 메시지 인증 코드가 이벤트 보고서에 포함되어 있으며, 자신이 가지고 있는 파티션 키로 생성된 메시지 인증 코드가 있는지 확인한다. 만약, 자신이 가지고 있는 파티션 키 된 메시지 인증 코드가 있다면, 이벤트 정보와 파티션 키를 이용하여 메시지 인증 코드를 만들어 이벤트 보고서의 허위 유무를 판별한다. 만약 비교한 메시지 인증 코드가 서로 다르면, 전달 받은 이벤트 보고서를 허위 이벤트 보고서로 판단하고 전달 받는 이벤트 보고서를 삭제한다. 비교한 메시지 인증 코드가 일치하거나, 자신이 가지고 있는 파티션 키로 만들어진 메시지 인증 코드가 없다면, 이벤트 보고서를 다음 전달 노드로 전달 한다. 그림 4는 전달노드에서 이벤트 보고서 검증과정을 보여준다.

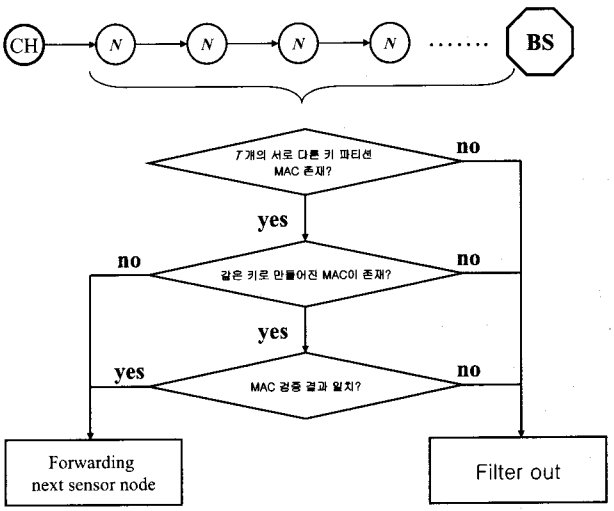

그림.3. 이벤트 보고서 허위 유무 판단 순서도.

2. 클러스터링

클러스터링 방법은 WSN의 에너지 효율적인 데이터 전송을 위해 제안된 기법이다. 클러스터링은 중복 데이터 전송을 줄이는 효율적인 라우팅 방법 중 하나로, 규모가 큰 센서네트워크에 효율적이다.

센서 노드가 센서필드에 배치되면, 무선 범위, 잔여 에너지 등을 고려하여 이웃한 센서 노드들과 클러스터 지역을 형성한다. 클러스터 지역에 있는 센서 노드들 중 하나를 CH로 선출하여, 클러스터 지역의 데이터를 수집하고 전달하는 대표노드가 된다. CH의 역할은 클러스터 지역 내의 센서 노드

들이 번갈아 가며 수행하여, CH역할로 인한 에너지 소비를 줄일 수 있도록 하였다. 클러스터링 방법은 CH가 클러스터 지역내의 데이터 전송을 담당하여 중복 데이터 전송을 줄이고, 중복 데이터 충돌로 인한 전송 오류와 센서 노드의 데이터 전달 에너지를 줄이도록 하였다. 그림 3은 클러스터를 이용한 다중 홉 라우팅(multi-hop routing)방법을 보여 준다.

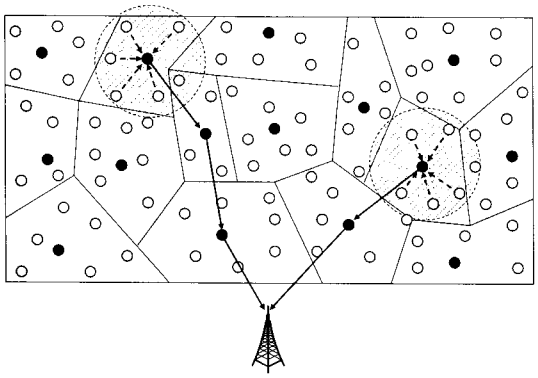

그림 4. 다중 홉 멀리 라우팅.

3. 동기

WSN의 에너지 효율적인 데이터 전송을 위해 제안된 클러스터링 방법은 통계적 여과 기법의 특성을 고려하지 않아 통계적 여과 기법에 적합한 클러스터링을 할 수 없다. 적절하기 못한 클러스터링은 통계적 여과 기법의 여과 강도를 보장하지 못하며, 클러스터 지역내의 서로 다른 파티션 키의 부족으로 정상 이벤트 보고서를 생성할 수 없는 문제점을 야기시킬 수도 있다. 따라서 클러스터링 방법을 통계적 여과 기법에 적용하기 위해서는 통계적 여과 기법의 특성을 고려한 클러스터링 방법이 요구된다. 본 논문에서는 통계적 여과 기법에 적합한 클러스터링 방법으로 센서 노드의 클러스터링 적합도를 이용한 클러스터링 방법을 제안 하고자 한다.

III. 퍼지를 이용한 클러스터링 적합도 결정 방법

이 장에서는 여과 기법 보안효율을 높이기 위한 클러스터링 적합도를 이용한 클러스터링 방법과 센서 노드의 클러스터링 적합도를 구하는 방법에 대해 기술한다.

1. 가정

WSN은 많은 센서 노드들과 BS로 구성되어 있다. 센서 노드는 센서필드에 배치 후, 클러스터 지역을 형성할 수 있는 기능을 가지고 있으며, 고유한 식별번호를 가지고 있다고 가정 한다. BS는 공격자로부터의 훼손 되지 않으며 브로드캐스트(Broadcast) 메시지를 인증할 수 있는 기능을 가지고 있다고 가정한다.

2. 퍼지를 이용한 클러스터링 방법

센서 노드의 클러스터링 적합도를 계산하기 위해, 본 논문에서는 두 개의 퍼지시스템을 이용하였으며, 클러스터링 적합도를 이용한 클러스터 지역 생성은 초기 적합도를 이용한 클러스터링 단계, 수정 적합도를 이용한 클러스터링 단계로 나누어진다.

초기 적합도를 계산하기 위해 CH로 선정된 센서노드는 주위에 있는 센서 노드들에게 거리 정보와 파티션 정보를 전달한다 (그림 5(a)). CH들로부터 받은 정보들을 이용해 각각의 센서 노드는 클러스터링 적합도를 계산하여 가장 높은 적합도를 보이는 CH를 선택하여 이를 CH에게 알린다 (그림 5(b)). CH는 센서 노드로부터 받는 정보를 이용하여 클러스터 지역 안에 센서 노드를 확인한다(그림 5(c)).

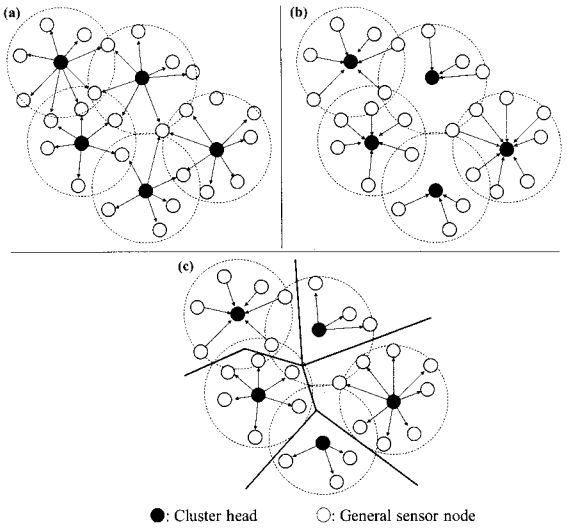

그림. 5. 초기 클러스터링 적합도를 이용한 클러스터링.

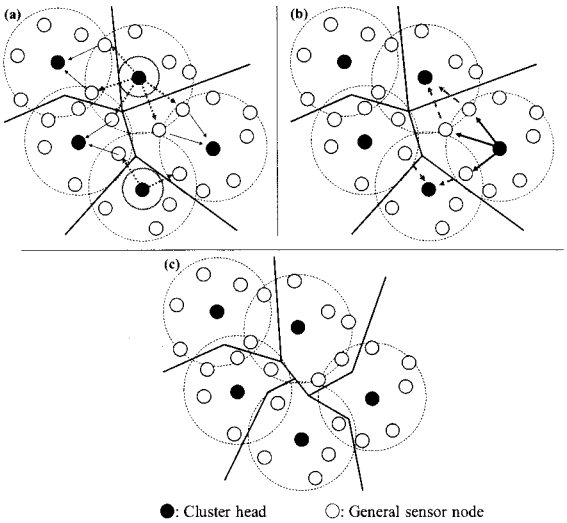

그림. 6. 수정 클러스터링 적합도를 이용한 클러스터링.

초기 적합도를 이용한 클러스터링 후, 각각의 CH는 클러스터 지역에 이벤트 보고서를 생성 할 수 충분한 수의 센서 노드가 있는지를 확인한다 (그림 6(a)). 만약 정상 이벤트를 생성할 수 있는 충분한 수의 센서 노드가 클러스터 지역에 없다면, 이를 주변 센서 노드에게 알려 수정 클러스터링 적합도 계산을 요청한다(그림 6(b)). 수정 클러스터링 적합도 계산 요청 받은 센서노드는 수정 적합도를 계산하여, 자신이 속한 클러스터 지역의 클러스터링 적합도 보다 높으면 센서 노드는 클러스터 지역을 수정 하고 이를 CH에 알린다 (그림 6(c)).

3. 클러스터링 적합도를 구하기 위한 퍼지입력 매개변수

센서 노드의 클러스터링 적합도를 구하기 위해 두 개의 퍼지 시스템을 사용하였다. 초기 클러스터링 적합도를 계산하기 위해 퍼지시스템은 CH와 BS와의 거리(Hops) 그리고 CH에서 BS사이의 전송 노드들이 가지고 있는 파티션 정보(WPI: weight of partition information)를 고려하였다. 수정 클러스터링 적합도를 계산하기 위해 클러스터 지역내의 센서 노드 수(NSC: number of the sensor nodes)와 초기 클러스터링 적합도(PFV: pre-fitness value)를 이용하였다. 그림 7은 클러스터링 적합도를 구하기 위한 퍼지시스템과 매개변수를 보여준다.

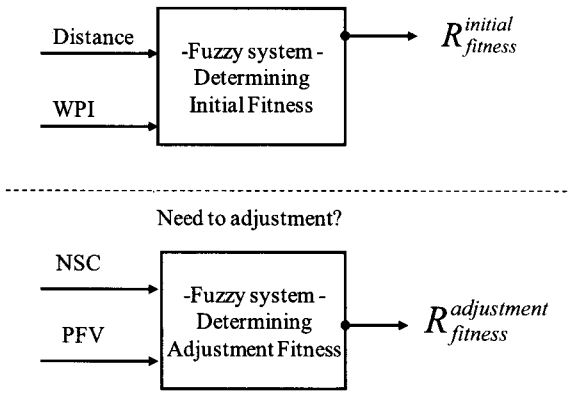

그림. 7. 클러스터링 적합도를 구하기 위한 퍼지시스템.

• DISTANCE: 클러스터링 적합도를 고려할 때, CH와 BS와의 거리를 고려해야 한다. BS와 거리가 가까울수록 데이터 전송 에너지를 줄일 수 있기 때문이다.
• WPI: 여과 효율을 보장하기 위해서는 전송노드가 가지고 있는 파티션 정보 역시 고려 되어야 한다. 만약 전송 노드들이 같은 파티션 키를 가지고 있지 않다면, 허위 이벤트 보고서는 여과 과정 없이 BS로 전달 되기 때문이다.
• NSC: 클러스터안의 센서노드 수 역시 고려 되야 할 사항이다. 클러스터 지역 안의 충분한 센서노드가 없다면 이벤트 보고서를 만들 수 없기 때문이다. 클러스터 생성 후, 클러스터 지역에 충분한 센서 노드가 없다면, 부분적인 재 클러스터링 과정이 필요하다.
• PFV: 초기 클러스터링 적합도 역시 고려 되어야 한다. 수정 클러스터링 적합도 계산을 요청한 클러스터 지역의 클러스터링 적합도에 가중치를 부여가 필요하기 때문이다. 또한 수정 클러스터링 적합도를 요청한 CH가 둘 이상일 때, 보다 적합한 클러스터 지역을 선택하기 위해 고려 되어야 한다.

4. 퍼지 매개변수 정의와 퍼지 룰

퍼지 입력 매개 변수를 이용한 센서노드의 클러스터링 적합도를 구하기 위해 두 개의 퍼지시스템을 사용하였다. 초기 클러스터링 적합도를 구하기 위해 사용하는 퍼지 입력 변수들의 명칭들은 다음과 같이 표현된다.

• DISTANCE = {VS(Very Short), S(Short), M(Middle), L(Long), VL(Very Long)} (Fig. 7(a))
• WPI = {VL(Very Low), L(Low), M(Middle), H(High), VH(Very High)} (Fig. 7(b))

초기 클러스터링 적합도 결과 값 변수들의 명칭들은 다음과 같이 표기 한다.

• INITIAL_FITNESS = {VL(Very Low), L(Low), E(Enough), G(Good), VG(Very Good)} (Fig. 7(c))

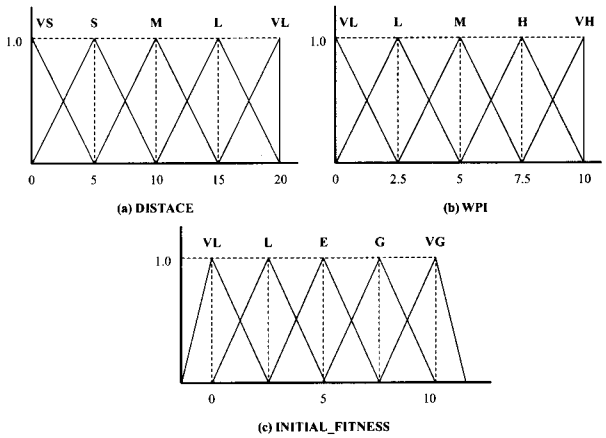

그림. 8. 초기 클러스터링 적합도를 구하기 위한 퍼지 멤버쉽 함수.

수정 클러스터링 적합도를 구하기 위해 퍼지시스템은 클러스터 지역 내의 노드 수(NSC: Number of the Sensor Nodes), 이전 클러스터링 적합도(PFV: Value of Pre-Fitness)를 이용한다. 퍼지 입력 변수들의 명칭들은 다음과 같이 표현된다.

• NSC = {VS(Very Short), S(Short), M(Middle), L(Long), VL(Very Long)} (Fig. 8(a))
• PFV = {VL(Very Low), L(Low), M(Middle), H(High)} (Fig. 8(b))

초기 클러스터링 적합도 결과 값 변수들의 명칭들은 다음과 같다.

• ADJUSTED_FITNESS = {L(Low), E(Enough), G(Good)} (Fig. 8(c))

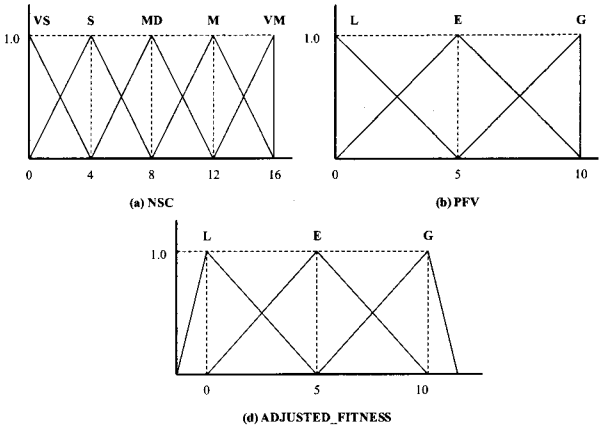

그림. 8. 수정 클러스터링 적합도를 구하기 위한 퍼지 멤버쉽 함수.

정의된 퍼지 매개 변수를 퍼지 시스템에 적용하기 위해서는 퍼지 룰(fuzzy rules)을 정의 하였다. 표 1은 클러스터링 적합도를 구하기 위한 퍼지 룰을 보여준다.

표 1. 퍼지 If-then 룰.

RULE	IF		THEN
	DISTANCE	WPI	IINITIAL_FITNESS
1	VS	L	L
2	S	M	L
3	M	H	G
4	L	L	L
5	VL	M	E
RULE	NSC	PVF	ADJUSTED_FITNESS
6	VF	G	VL
7	F	G	VL
8	M	E	E
9	M	L	G
10	VM	L	G

IV. 결론 및 향후 과제

기존의 클러스터링 방법은 여과기법의 특성을 고려하지 않아 여과 효율을 보장하지 못하며, 정상 이벤트를 발상하지 못 하는 문제점이 발생한다. 본 논문에서는 이러한 문제점들을 해결하기 위하여 퍼지를 이용하여 여과기법 보안효율을 높이기 위한 센서네트워크 클러스터링 방법을 제안 하였다. 여과기법의 보안효율을 높이기 위한 클러스터링을 위해 노드의 클러스터링 적합도를 사용하여 클러스터링을 하였다. 클러스터링 적합도를 계산하기 위해, 퍼지 시스템은 BS와 CH의 거리, 전달노드의 파티션 정보, 그리고 클러스터 지역 안의 센서노드 수를 고려하였다. 향후 과제로는 제안된 방법의 효율성 분석을 위한 시뮬레이션을 수행하는 것이다. 그리고 시뮬레이션 결과의 비교분석을 통하여 제안한 기법의 효율성을 증명하고, 센서노드를 이용한 시뮬레이션을 수행하여 실제로 적용 가능한 분야를 제시하고자 한다.

참고문헌

[1] J. N. Al-Karaki, and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEE Wirel. Commun.*, vol. 11, no. 6, pp. 6-28, December, 2004.

[2] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," *ACM, In Proc. Of SenSys*, pp. 255-265, 2003.

[3] F. Ye, H. Luo, and S. Lu, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," *IEEE J. Sel. Area Comm.* vol. 23, no. 4, pp. 839-850, 2005.

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

[5] F. Li, and J. Wu, "A Probabilistic Voting-Based Filtering Scheme in Wireless Sensor Networks," *In Proc. The International Wireless Communications and Mobile Computing Conference*, pp. 27-32, 2006.

[6] 김상률, 조대호, "통계적 여과 기법기반의 센서 네트워크를 위한 퍼지로직을 사용한 보안 경계 값 결정 방법," 한국시뮬레이션학회 논문지, vol. 16, no. 2, pp. 27-35, June 2007.

[7] 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. 261-272, August, 2007.

[8] B. H. Kim and T. H. Cho, "Efficient Selection Method of Message Authentication Codes for Filtering Scheme in Sensor Netwroks," *In Pro. Of ICUIMC*, pp. 528-531, January, 2008.

[9] C. C. Huang and M. H. Guo, "Weight-Based Clustering Multicast Routing Protocol for Mobile Ad Hoc Networks," *Internet Protocol Tec.*, vol. 1, no. 1, pp. 10-18, 2003.

[10] Y. Ossama and F. Sonia, "A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks," *IEEE Trans. Mobile Com.*, vol. 3, no. 4, pp. 366-379, December. 2004.

김 병 희

2007년 동서대학교 정보통신공학과 졸업. 2007년~현재 성균관대학원 석사과정 재학중. 관심분야는 센서네트워크 보안, 네트워크 보안, 와이브로 등임.

조대호

1983년 성균관대학교 전자공학과(공학사). 1987년 Univ. of Alabama 전자공학과(공학석사). 1993년 Univ. of Arizona 전자 및 컴퓨터공학과(공학박사). 1995~현재 성균관대학교 정보통신공학부 교수. 관심분야는 USN, 모델링 및 시뮬레이션, 지능 시스템, 네트워크 보안 등임.