한국컴퓨터정보학회 하계학술대회 논문집 제21권 제2호 (2013. 7)

확률적 투표 여과 기법의 센서 네트워크에서 에너지 효율성을 위한 경계 값 결정 기법

남수만[O], 조대호[*]
[O*]성균관대학교 정보통신대학
e-mail:{smnam[O], taecho[*]}@ece.skku.ac.kr

A Method to Decide Thresholds of False Votes for the Effectiveness of Energy Savings in Sensor Networks

Su-Man Nam[O], Tae-Ho Cho[*]
[O*]College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

무센 센서 네트워크는 개방된 환경에서 운영되기 때문에 허위 보고서와 허위 투표 삽입 공격으로부터 쉽게 노출되어 있다. 두 공격을 감지하기 위해 확률적 투표-기반 여과 기법은 보고서가 전달되는 동안 그 보고서의 투표 검증을 이용하여 허위 범위 경계 값을 통해 두 공격을 감지한다. 본 논문에서 제안 기법은 네트워크의 상황을 고려하여 센서 노드의 에너지 잔여량, 홉 수, 전달된 보고서의 수를 통해 퍼지 시스템의 입력 요소로 결정하고 나온 결과를 허위 범위 경계 값을 결정을 통해 기존 기법보다 에너지 효율을 증가시킨다. 그러므로 우리의 제안 기법은 기본 기법보다 비교했을 때 전체 네트워크 수명 연장을 기대한다.

키워드: 무선 센서 네트워크(wireless sensor network), 네트워크 보안(network security), 확률적 투표 기반 여과 기법(probabilistic voting-based filtering scheme), 퍼지 시스템(fuzzy system)

I. 서 론

인프라 기반 없이 동작하는 무선 센서 네트워크(Wireless Sensor Network; WSN)는 다수의 센서 노드와 베이스 스테이션(Base Station; BS)로 구성되며, 무선 환경에서 운영되기 때문에 악의적인 공격자로부터 다양한 공격을 당하기 쉽다[1-2]. 응용 계층에서 발생하는 허위 보고서 삽입 공격(False Report Injection Attack; FRIA)[3]과 허위 투표 삽입 공격(False Vote Injection Attack; FVIA)[4]은 불필요한 에너지 소모와 정상 보고서를 제거시킨다. 이러한 두 공격을 감지하기 위해 확률적 투표-기반 여과 기법(Probabilistic Voting-based Filtering Scheme; PVFS)이 제안되었다[4]. 본 논문에서 우리는 PVFS보다 보안 레벨을 유지하면서 에너지 효율을 증가시키는 방법을 제안한다.

II. 배경

1. 확률적 투표-기반 여과 기법

PVFS는 센서 네트워크에서 훼손된 노드에서 발생하는 FRIA과 FVIA를 동시에 감지하기 위해 제안된 기법이다[4]. 이 기법은 보고서에 vote를 첨부시켜 보고서가 전달되는 동안 허위 vote 범위 경계 값(Tf)을 통해 두 공격을 막는다. 각 노드들은 클러스터 단위로 배치되고 그 클러스터 안에서 클러스터 헤드(Cluster Head; CH)가 선출한다. 한 클러스터 구역에서 이벤트가 발생할 때 자신의 키를 통해 vote를 만들고 CH에 전달한다. 그 CH는 전달받은 vote들을 보고서에 첨부하고, 검증 노들을 선출한다. 선출된 검증 노드는 보고서를 받고 허위 vote를 검사한다. 만약 그 보고서에 허위 vote가 Tf을 넘는다면, 그 보고서는 FRIA 공격으로 제거된다. 보고서에 허위 vote가 그 범위를 안 넘는다면, FVIA 공격을 감지하고 BS에 전달한다. 따라서 PVFS는 허위 범위 경계 값을 통해 두 공격을 감지한다.

III. 본 론

본 논문에서는 네트워크 에너지 향상을 위해 세 가지 상황 매개변수(status parameter)를 입력하여 퍼지 시스템[5]을 통해 허위 범위 경계 값을 결정한다.

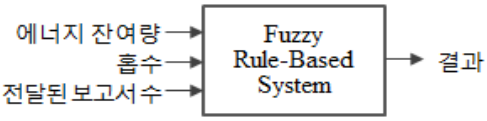


그림 1. 퍼지 기반 제안 기법

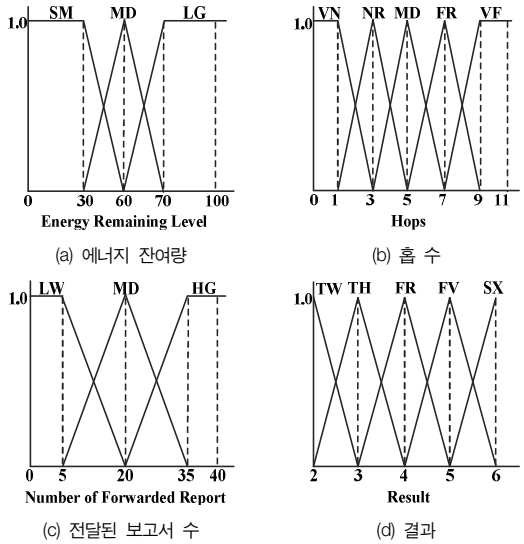
그림 1은 제안 기법의 입력과 출력에 대해서 보여준다. 퍼지 시스템의 입력은 에너지 잔여량 (한정된 자원을 효과적으로 관리), 홉 수(BS로부터 해당 CH까지의 거리), 그리고 전달된 보고서 수 (보고서 발생 양)을 나타내고, 경계 값을 출력한다.

퍼지 변수의 입력 요소는 다음과 같다.

- 에너지 잔여량(ER)={Small (SM), Middle (MD), Large (LG)}
- 홉 수(HC)={Very Near (VN), Near (NR), Middle (MD), Far (FR), Very Far (VF)}
- 전달된 보고서 수(NR)={Low (LW), Middle (MD), High (HG)}

퍼지 변수의 출력 요소는 다음과 같다.

- 결과={Two (TW), Three (TH), Four (FR), Five (FV), Six (SX)}



(a) 에너지 잔여량 (b) 홉 수

(c) 전달된 보고서 수 (d) 결과

그림 130. Fuzzy membership Functions

우리는 45개의 퍼지 규칙들을 정의하였고, 특정 규칙에 대해 표 1과 같이 정의하였다.

표 2. Fuzzy if-then rules

번호	입력			출력
	ER	HC	NR	RS
1	SM	VF	LW	FV
23	MD	MD	MD	FR
45	LG	VF	HG	TH

III. 결 론 및 향후 계획

WSN의 응용 계층에서 발생하는 FRIA과 FVIA은 악의적인 공격자로부터 발생하기 쉽다. 이러한 공격을 감지하기 위해 PVFS는 제안되었다. 본 논문에서는 기존 PVFS의 네트워크 운영전에 결정되는 허위 vote 범위 경계 값을, 제안 기법에서는 퍼지 시스템을 기반으로 그 경계 값을 결정하였다. 그래서 우리는 동적인 보안 경계 값을 효과적으로 결정 위해, 센서 노드의 에너지 잔여량, 홉 수, 전달된 보고서 수를 입력받아 그 경계 값을 출력했다. 그러므로 우리는 센서 네트워크의 불필요한 에너지 소모를 막고, 전체 네트워크의 수명 연장을 기대한다.

Acknowledgement

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2013R1A2A2A01013971)

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.102-114, Aug. 2002.

[2] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad hoc Networks, vol.3, no.3, pp.325-349, May 2005.

[3] H. Y. Lee and T. H. Cho, "A scheme for adaptively countering application layer security attacks in wireless sensor networks," IEICE Trans. Commun., vol.E93-B, no.7, pp.1881-1889, 2010.

[4] F. Li, A. Srinivasan, and J. Wu, "PVFS: A probabilistic voting-based filtering scheme in wireless sensor networks," Int. J. of Security and Network, vol.3, no.3, pp.173-182, 2008.

[5] FFLL, http://ffll.sourceforge.net/.