통계적 여과기법에서 퍼지 규칙을 이용한 적응적 보안 경계 값 결정 방법

An Adaptive Threshold Determining Method in Senor Networks using Fuzzy Logic

선 청 일*, 조 대 호
(Chung il Sun and Tae Ho Cho)

Abstract: There are many application areas of sensor networks, such as surveillance, hospital monitoring, and home network. These are dependent on the secure operation of networks, and will have serious outcome if the networks is injured. An adversary can inject false data into the network through the compromising node. Ye et al. proposed a statistical en-route filtering scheme (SEF) to detect such false data during forwarding process. In this scheme, it is important that the choice of the threshold value since it trades off security and overhead. This paper presents an adaptive threshold value determining method in the SEF using fuzzy logic. The fuzzy logic determines a security distance value by considering the situation of the network. The Sensor network is divided into several areas by the security distance value, it can each area to uses the different threshold value. The fuzzy based threshold value can reduce the energy consumption in transmitting.

Keywords: Sensor networks, statistical en-route filtering, threshold, fuzzy-logic

I. 서론

최근의 무선 통신, 전자 기기 발전은 저가의 센서 노드의 개발과 소형화에 발전을 이루었으며, 저가의 센서 네트워크 구성을 가능하게 한다. 센서 네트워크는 전장, 의료시설, 그리고 자연지역과 같은 사람의 감시가 필요한 다양한 응용 분야에 활용할 수 있다. 무선 센서 네트워크는 센싱, 계산 능력, 그리고 무선 통신능력을 가진 소형의 센서 노드와 센서 노드가 감지한 데이터를 수집하는 싱크들로 구성된다 [1]. 센서 노드들은 무선 통신 범위 내의 노드들과 직접적으로 통신하며, 범위 밖의 노드들은 다른 노드들의 메시지 전송에 의존하여 통신한다 [2]. 센서 노드는 무작위로 필드에 흩어 뿌려지고 무인의 환경에서 작동하므로, 센서 네트워크는 자가 구성 능력을 가져야 한다 [3]. 센서 네트워크의 이러한 특성으로 인하여, 센서 노드는 물리적 취약성을 가지며, 공격자에 의해 훼손, 파괴가 가능하여 보안적 문제점을 가진다. 공격자는 센서 필드에서 임의의 노드를 획득할 수 있으며, 획득한 노드를 통하여 거짓 정보를 네트워크에 삽입할 수 있다 [4]. 공격자는 거짓 정보를 네트워크에 삽입함으로써, 사용자로 하여금 잘못된 데이터의 수신으로 인한 네트워크의 상태 파악에 오류를 일으키게 하며, 센서 노드의 에너지 소모를 유발시켜 센서 네트워크의 수명을 단축시킨다 [5]. 거짓 정보 주입 공격을 방어하기 위하여 여러 가지 보안 기법이 제안되었다.

Ye 등은 이벤트 정보 전달 과정 중에 거짓 정보를 제거하기 위한 방법으로 통계적 여과 기법(Statistical en-route filtering scheme)을 제안하였다 [4]. 통계적 여과 기법에서 이벤트를 감지한 여러 노드들은 이벤트 정보와 메시지 인증 코드(Message authentication code)을 첨부하여 이벤트 보고서를 생성한다. 이벤트를 감지한 노드들 중 센싱 감도가 가장 강한 노드를 대표 노드(Center of stimulus)로 선정한다. 대표 노드는 이벤트를 감지한 노드들로부터 보고서를 전달 받아, 하나의 이벤트 보고서를 생성하는데, 이때, 일정한 개수의 보고서를 이용하여 생성한다. 사용자는 센서 네트워크 생성 전, 보안 경계 값(Threshold)을 결정하는데, 이는 대표 노드가 이벤트 보고서 생성 시, 보고서에 포함될 메시지 인증 코드의 개수를 나타낸다. 통계적 여과 기법에서의 핵심 기술은 생성된 이벤트 보고서가 베이스 스테이션으로 전달되면서, 전달 과정 중 전달 노드에 의해 보고서의 허위유무를 판단으로 보고서의 전달 및 폐기를 결정하는 것이다. 이벤트를 감지한 노드들이 이벤트 보고서에 첨부하는 메시지 인증 코드는 노드 자신이 소유한 인증키를 이용하여 생성되며, 이는 이벤트 정보에 대한 동의를 나타낸다. 생성된 이벤트 보고서는 대표 노드에게 전달되고, 대표 노드는 전달 받은 보고서를 하나의 이벤트 보고서로 생성하여 베이스 스테이션을 향하여 전달한다. 이벤트 보고서는 여러 홉을 거치면서 베이스 스테이션으로 향해 전달되며, 각 전달 노드의 올바른 MAC을 이용하여 일정한 확률로써, 보고서의 위조 유무를 판단한다. 통계적 여과 기법의 특성으로 인하여 일정한 개수의 위조 보고서는 전달 과정에서 제거되지 않고, 베이스 스테이션으로 전달된다. 그러나 베이스 스테이션은 전체 키 풀에 모든 인증키를 가지고 있으므로, 올바른 메시지 인증 코드를 생성하여 위조 보고서를 제거할 수 있다.

통계적 여과 기법에서는 대표 노드가 이벤트 보고서를 생성할 때, 주변 노드들로부터 보고서 생성 시 필요한 메시지 인증 코드를 보안 경계 값만큼 모은다. 보안 경계 값은 사용자에 의해 결정되며, 센서 네트워크가 유지되는 동안 고정된 값을 가지게 된다. 이벤트 보고서에 첨부되는 메시지 인증 코드의 개수가 많아지면, 보고서 검증 시 위조의 판별을 통한 제거의 확률이 높아지는 반면에, 에너지 소모는 증가한다.

* 책임저자(Corresponding Author)
논문접수 : 2008. 7. 21., 채택확정 : 2008. 7. 31.
선청일, 조대호 : 성균관대학교 정보통신공학부
(cisun@ece.skku.ac.kr, taecho@ece.skku.ac.kr)
※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0701-0028)

고정된 보안 경계 값을 가지므로 인한, 불필요한 노드의 에너지 소모가 발생하기도 한다. 이러한 문제점을 보안하기 위해 본 논문에서는 퍼지 규칙을 이용한 전체 네트워크의 상황을 고려하여 에너지 소모를 줄이기 위한 적응적 보안 경계 값 결정 방법을 제안한다. 제안에서 센서 네트워크는 일정한 홉 수에 의해 지역 분할되며, 각기 다른 지역에 속한 노드들은 다른 보안 경계 값을 가짐으로써, 불필요한 에너지 소모를 줄일 수 있게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 통계적 여과 기법에 대한 간략한 소개를 하고, 3장에서는 제안한 기법에 대해 자세히 설명한다. 마지막으로 4장에서는 결론 및 향후 과제에 대해 설명한다.

II. 관련연구

통계적 여과 기법에서, 베이스 스테이션은 전체 키 정보를 담은 전체 키 풀을 가진다. 전체 키 풀은 m개의 키로 구성되어 있으며, 사용자에 의해 P개의 구획으로 나누어 진다. 각 구획은 m/P 개의 서로 다른 키들로 구성되며, 각 키들은 고유의 키 인덱스를 가진다. 센서 노드가 네트워크에 배치되기 전에 사용자는 임의로 한 구획을 선택하고, 선택된 구획에서 일정한 수의 키들을 임의적으로 노드에게 적재한다 [4]. 센서 필드에서 실제 이벤트가 발생하면, 이벤트를 탐지한 노드들 중 감지 강도가 가장 강한 노드가 대표 노드로 선정된다. 대표 노드는 이벤트를 감지한 주변 노드들의 보고서를 전달받아 하나의 이벤트 보고서를 생성하는 역할을 한다. 이벤트를 감지한 모든 노드들은 $\{L_E, t, E\}$ 형태의 메시지를 생성한다. L_E는 이벤트의 위치, t는 감지 시간, 그리고 E는 이벤트의 종류를 나타낸다 [4]. 생성한 메시지를 주변 노드에게 브로드캐스트하여 이벤트를 감지한 노드들이 동일한 이벤트에 대해 탐지 여부를 비교한다. 이벤트 감지 노드들은 자신이 가진 키들 중 하나의 키를 임의로 선택하고, 이 키를 이용하여 메시지를 일방향 암호화 방식을 이용하여 암호하여 메시지 인증 코드를 생성한다. 메시지 인증 코드 생성 후, 이벤트 감지 노드는 $\{i, M_i\}$ 키 인덱스와 생성한 메시지 인증 코드를 대표 노드에게 전달한다. 대표 노드는 보안 경계 값(T)만큼의 서로 다른 구획의 키 인덱스로 생성된 메시지 인증 코드를 임의로 선택한다. 선택된 메시지 인증 코드를 이용하여 최종 이벤트 보고서를 다음과 같은 형태로 생성한다.

$$\{L_E, t, E, i_1, M_{i1}, i_2, M_{i2}, \ldots, i_T, M_{iT}\} \quad (1)$$

최종 이벤트 보고서에서 보안 경계 값(T)의 결정은 네트워크의 보안 강도와 에너지 소모에 있어 상충 관계에 있다. 보안 경계 값의 값보다 적은 개수의 메시지 인증 코드가 첨부되거나, 서로 같은 구획의 키 인덱스를 사용하여 생성된 다른 메시지 인증 코드가 첨부되면 이 보고서는 전달되지 않는다. 최종 보고서가 생성되기 위해서는 다음과 같은 조건을 만족해야 한다.

- 보고서 내에 보안 경계 값(T) 만큼의 $\{i, M_i\}$ 쌍이 존재하는가
- 키 인덱스 i가 서로 다른 구획에서 존재하는가

생성된 최종 보고서는 여러 홉을 거치면서 베이스 스테이션을 향하여 전달된다. 전달 경로 상에 존재하는 각 전달 노드들은 최종 보고서 내의 키 인덱스와 동일한 키 인덱스를 소유하고 있다면, 이벤트 감지 노드들과 동일한 방식으로 메시지 인증 코드를 생성하여, 최종 이벤트 보고서내에 첨부된 메시지 인증 코드와 비교한다. 만약 비교한 값이 다르다면, 보고서에 첨부된 메시지 인증 코드를 위조로 판단하여 보고서를 제거한다. 메시지 인증 코드의 값이 동일하면, 다음 홉의 전달 노드에게 전송하며, 이는 보고서가 베이스 스테이션에게 전달될 때까지 진행된다.

공격자는 네트워크에 배치된 노드를 획득하여 위조 보고서를 삽입할 수 있다. 획득한 노드를 통하여 허위 메시지 인증 코드를 생성하고, 이를 이용하여 위조 보고서를 생성 및 삽입한다. 훼손된 노드에 삽입된 위조 보고서는 베이스 스테이션으로 향하여 전달되는데, 전달 과정에서 전달 노드에 의해 여과될 수 있다. 전달 노드가 소유한 키를 이용하여 허위로 생성된 메시지 인증 코드와 비교하여 일정한 확률로 위조 보고서를 여과시킬 수 있다. 만약, 위조 보고서가 전달 과정에서 여과되지 않는다면, 베이스 스테이션에서 제거된다. 베이스 스테이션은 전체 키 풀에 모든 키 정보를 알고 있으므로, 허위로 생성된 메시지 인증 코드와 비교하여 보고서의 허위 유무를 판단하고 제거한다.

III. 제안

3.1 가정

본 논문에서는 네트워크 상의 노드의 밀집도는 충분하다고 가정한다. 또한, 전달 경로는 사용자의 요청 혹은 네트워크의 토폴로지 변화에 따라 베이스 스테이션이 전달하는 조작 메시지에 의해 설립된다. 베이스 스테이션은 네트워크의 모든 전달 경로과 홉 수를 알 수 있다.

3.2 동기

통계적 여과 기법에서 전달 노드는 일정한 확률에 따라 보고서의 허위 유무의 검증을 수행하므로 필요 이상의 여과 연산을 수행하거나 한 번도 수행하지 않을 수 있다. 또한, 통계적 여과 기법의 특성상 허위 보고서는 여러 홉을 거쳐 여과 연산을 할 경우, 검증 및 폐기의 확률이 높아진다. 베이스 스테이션에서 근접한 지역에서 허위 보고서가 생성될 경우, 홉 수가 짧은 경로를 통해 전달되기 때문에 전달 과정 중에 여과될 확률은 낮아진다. 따라서, 베이스 스테이션에 근접한 노드에서 발생한 허위 보고서는 노드의 검증 및 전달로 인한 에너지 소모를 유발시킨다. 통계적 여과 기법은 사용자에 의해 결정된 보안 경계 값은 고정된 값을 가지므로, 필요치 않은 노드의 에너지 소모를 유발하여 전체 네트워크의 수명을 줄인다. 따라서, 네트워크의 상황을 고려하여 적응적 보안 경계 값을 설정하는 것이 효율적이다.

3.3 개요

제안한 기법은 기존의 통계적 여과 기법과 비교하여 보안 경계 값이 유동적이며, 네트워크의 상황을 고려한다는 점에서 차이점을 가진다. 통계적 여과 기법에서는 네트워크가 설정되기 위해 사전에 보안 경계 값을 사용자에 의해 결정된다. 반면에, 제안한 기법에서는 초기에 사용자에 의해 설정된 보안 경계 값과 네트워크의 상황을 고려하여 새로운 보안 경계 값을 설정한다. 제안 기법에서는 지역 분할 단계와 적응적 보안 경계 값 설정 단계의 과정을 두어 진행한다. 지역 분할은 통계적 여과 기법에서 고정된 보안 경계 값을 가짐으로써 불필요하게 소비되는 노드의 에너지 소모를 막는다. 지역 분할을 통해 베이스 스테이션과 근접한 지역의 노드들과 먼 지역에 배치된 노드들이 다른 보안 경계 값을 가진다. 베이스 스테이션과 근접한 지역에서 이벤트 발생 시, 이 지역에 속한 대표 노드는 사용자가 설정한 보안 경계 값보다 적은 수의 메시지 인증 코드를 최종 보고서에 첨부함으로써, 보고서 생성 및 전달 시, 불필요한 에너지 소모를 줄인다. 반면에, 베이스 스테이션과 먼 지역에서 발생한 이벤트를 감지한 노드들은 사용자가 설정한 보안 경계 값과 동일한 개수의 메시지 인증 코드를 보고서에 첨부하여 네트워크의 보안 강도를 높인다. 지역 분할 단계에서는 네트워크의 전달 경로가 설정 된 후, 모든 노드는 자신의 홉 수가 담긴 제어 메시지를 베이스 스테이션에게 전달 경로로 전송한다. 베이스 스테이션은 모든 노드로부터 홉 수를 전달받은 후, 수식 (1)을 이용하여 지역 분할을 위한 계산을 수행한다.

$$P = \frac{d_{\max}}{\frac{T}{2}+1} \qquad (2)$$

$d_{\max}$는 전달 경로 상의 최대 홉 수이고, T는 초기에 사용자에 의해 결정된 보안 경계 값이다. P는 지역 분할을 위한 보안 거리 값이며, 이 값을 이용하여 네트워크를 분할한다. 베이스 스테이션은 네트워크 분할을 진행하여 조작 메시지에 분할 정보를 테이블로 저장하여 모든 노드에게 브로드 캐스팅한다. 표1은 베이스 스테이션이 지역 분할을 수행한 뒤, 조작 메시지에 포함할 지역 분할 정보를 나타낸다.

표 1. 지역 분할 정보 테이블

Area	Range	보안 경계 값
$Area_1$	$0 < Area_1 \le P$	T_{Area2}-1
$Area_2$	$P < Area_1 \le 2P$	T_{Area3} - 1
$Area_{n-1}$	$Area_{n-2} < Area_{n-1} \le Area_{n-2} + P$	T
$Area_n$	$Area_{n-1} < Area_n$	T

분할 정보를 담은 메시지를 수신한 노드들은 자신의 홉 수와 분할 정보 테이블의 홉 수를 비교하여 보안 경계 값 및 자신의 속한 지역의 정보를 재설정한다. 새롭게 설정된 보안 경계 값은 이벤트 발생 시, 해당 노드가 대표 노드로 설정되었을 때 주변 노드로부터 수신하는 메시지 인증 코드들의 개수를 결정한다.

적응적 보안 경계 값 설정 단계는 네트워크 생성 후 일정 시간이 흐른 뒤, 네트워크 상황을 고려하여 퍼지 규칙을 통한 보안 경계 값 재설정 단계이다. 네트워크의 생성 후, 일정 시간이 지나면 노드의 에너지 소모가 일어나고 분할 지역마다 에너지 소모량이 달라지게 된다. 베이스 스테이션은 모든 노드에게 노드의 잔여 에너지량을 요청한다. 모든 노드는 자신의 잔여 에너지 량을 베이스 스테이션으로부터 수신한 요청 메시지에 첨부하여 전달한다. 베이스 스테이션은 각 노드들로부터 수신한 잔여 에너지 정보량과 네트워크 상황을 인자로 하여 퍼지 함수를 사용해 지역 분할 시 사용되는 보안 거리 값을 계산한다. 재 계산된 보안 거리 값을 이용하여 새로운 분할 정보 테이블을 생성하고, 네트워크의 브로드 캐스팅한다. 새로운 분할 정보를 수신한 각 노드들은 이전의 설정된 보안 경계 값 및 지역 정보를 새로운 값을 재 설정한다.

3.4 인자

새로운 보안 거리 값 결정을 위한 퍼지 함수의 인자로는 1) 각 노드의 홉 수 (H: HOPS), 2) 각 노드의 잔여 에너지량 (E: NODE ENERGY), 3) 분할 지역 내 허위 보고서 비율 (FTR: FALSE TRAFFIC RATIO)이 있다.

노드의 잔여 에너지가 적거나 노드의 홉 수가 작은 경우, 또는 해당 노드가 속한 분할 지역 내 허위 보고서 비율이 낮은 경우, 보안 거리 값은 작아진다. 반면에, 노드 에너지가 충분하고 홉 수가 크며, 분할 지역 내 허위 보고서 비율이 크다면 보안 거리 값은 커지게 된다.

3.5 퍼지 규칙

제안한 기법에서 각 노드의 잔여 에너지 와 분할 지역 내 허위 보고서 비율은 기준에 따라 크고 작음을 다르게 판단할 수 있으며, 오차를 가질 수 있다. 이러한 불확실성과 애매성을 가진 계산을 수행하기 위해서 퍼지 논리를 이용한다. 제안한 기법에서 퍼지 함수의 인자와 결과 값에 대한 멤버십 함수는 다음과 같다.

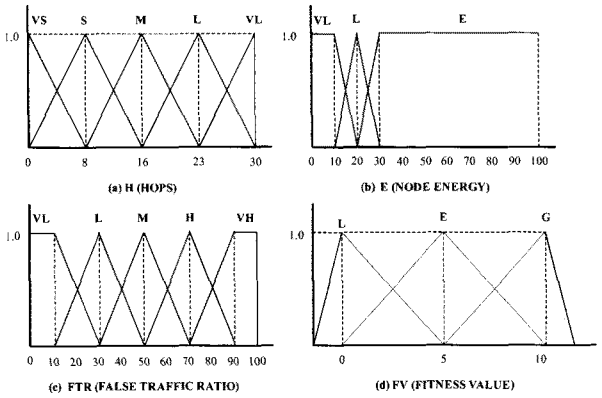


그림 1. 멤버십 함수

그림 1의 멤버십 함수에서 (a) H 의 최대 값은 네트워크의 최대 홉 수를 넘을 수 없으며, 최대 값은 최대 홉 수와 동일하다.

IV. 결론

본 논문에서는 허위 보고서 삽입 공격에 대응하는 여과 기법 중 하나인 통계적 여과 기법에 동작 과정을 분석하고 고정된 보안 경계 값을 가지는 방식의 문제점을 보완하는 적응적 보안 경계 값 결정 방법을 제안하였다. 네트워크의 상황을 인지하고 이를 고려한 적응적 보안 경계 값을 가짐으로써, 전달 노드 및 대표 노드의 불필요한 에너지 소모를 줄일 수 있다. 향후 과제는 제안한 방식의 성능을 증명할 수 있는 시뮬레이션을 수행하고, 기존의 여과 방식들과 비교하여 효율성을 비교하는 것이다.

참고문헌

[1] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci., "A Survey on Sensor Networks,'IEEE Wireless Communication Magazine, Vol. 40, no. 8, pp. 102-116, 2002.

[2] R Guorui Li, Jingsha He, and Yingfang Fu, "Analysis of an Adaptive Key Selection Scheme in Wireless Sensor Networks", LNCS 4490, pp. 409-416, 2007

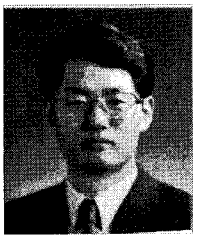
[3] Yang and S. Lu, "Commutative Cipher based En-Route Filtering in Wireless Sensor Networks", Proc. of VTC, pp. 1223-1227, Sep. 2003.

[4] 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, Apr. 2005.

[5] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Network: A Predistribution and Local Collaboration-base Approach", Proc. of INFOCOM., pp. 503-514, Mar. 2005.

선 청 일

2007년 경원대학교 소프트웨어학부 졸업.
2007년~ 현재 성균관대학교 정보통신공학부 석사과정 재학 중.
관심분야는 유비쿼터스, 센서 네트워크, 모델링 시뮬레이션, 센서 네트워크 보안



조 대 호

1983년 성균관대학교 전자공학과 (공학사).
1987년 University of Alabama 전자공학과 (공학석사).
1993년 University of Arizona 전자 및 컴퓨터 공학과 (공학박사).
1995년~현재 성균관대학교 정보통신공학부 교수
관심분야는 유비쿼터스 센서 네트워크, 모델링 및 시뮬레이션, 지능 시스템, 네트워크 보안