http://dx.doi.org/10.7236/JIIBC.2013.13.1.115
JIIBC 2013-1-17

무선 센서 네트워크에서 에너지 효율적인 시빌 공격 탐지

Sybil Attack Detection with Energy Efficiency in Wireless Sensor Networks

허준영*

Junyoung Heo

요 약 무선 센서 네트워크의 다양한 용도만큼 많은 취약점과 다양한 공격 가능성이 여러 논문에서 제기되고 있다. 여러 공격 중에서도 시빌(sybil) 공격은 공격 노드가 많은 수의 거짓 노드를 생성하여 네트워크에 잘 못된 정보를 보내는 공격이다. 사용자가 공격을 받았음을 인지하지 못하고 거짓 노드로부터 온 데이터를 사실로 오인하고 사용하게 되면 민감한 데이터일 경우 재앙이 될 수도 있다. 인증과 같은 암호화 기법으로 방어를 할 수 있지만 저전력, 저사양을 특징으로 하는 센서 노드에서는 구현이 곤란하다. 본 논문에서는 센서 네트워크에서 시빌 공격으로 생성된 거짓 노드를 탐지하는 기법을 제안한다. 제안 기법은 정상 노드의 군집과 거짓 노드의 군집 간에 네트워크가 약하다는 특징을 이용한다. 또한 센서 노드의 저전력을 고려하여 기존 에너지 고려 라우팅에 약간의 데이터를 추가함으로써 오버헤드를 최소화 하였다. 실험 결과를 통해 제안 기법이 기존 에너지 고려 라우팅에 비해 추가적인 에너지 소모가 극히 적으면서도 시빌 공격의 탐지를 90% 이상 할 수 있음을 보였다.

Abstract There are lots of vulnerability and chance to be attacked in wireless sensor networks, which has many applications. Among those attacks, sybil attack is to generate a lot of false node and to inject false information into networks. When a user uses such false information without recognizing the attack, there might be a disaster. Although authentication method can be used to protect such attack, the method is not a good choice in wireless sensor networks, where sensor nodes have a limited battery and low power. In this paper, we propose a novel method to detect sybil attack with a little extra overhead. The proposed method use the characteristics that there is a weak connection between a group of normal nodes and a group of false nodes. In addition, the method uses energy aware routing based on random routing and adds a little information into the routing. Experimental results show that the proposed method detects false node by more than 90% probability with a little energy overhead.

Key Words : 센서 네트워크, 시빌 공격, 에너지 고려 라우팅, 랜덤 라우팅

Ⅰ. 서 론

무선 센서 네트워크는 다수의 센서 노드로 구성된 무선 네트워크로 센서에서 수집한 데이터를 무선 네트워크를 통해 싱크 노드로 전송하여 정보를 수집하는 네트워크이다. 싱크에서는 수집한 정보에 따라 자동으로 반응을

*정회원, 한성대학교 컴퓨터공학과
접수일자 2013년 1월 2일, 수정완료 2013년 2월 1일
게재확정일자 2013년 2월 8일

Received: 2 January 2013 / Revised: 1 February 2013 /
Accepted: 8 February 2013
*Corresponding Author: jyheo@hansung.ac.kr
Dept of Computer Engineering, Hansung University

하거나 사용자에게 통보를 한다. 무선 센서 네트워크는 다수의 노드가 스스로 동적 네트워크를 구성하기 때문에 일부 노드가 멈추더라도 네트워크는 정상적으로 동작하는 장점이 있다. 반면에 다수의 노드가 배치되기 때문에 노드의 단가를 낮추기 위해 노드의 사양은 매우 낮고 배터리로 동작하기 때문에 저전력이 고려되어야 한다[9].

무선 센서 네트워크에는 다양한 보안 취약성이 존재하는데, 특히 시빌(sybil) 공격은 무선 센서 네트워크의 중복 메커니즘을 무력화하기 때문에 매우 위험하다. 시빌 공격은 네트워크에서 공격 노드가 많은 수의 거짓 노드를 생성하여 네트워크를 위협하는 공격이다. 거짓 노드에서는 거짓 데이터를 싱크로 전송하여 싱크에서 사용자가 거짓 데이터에 의해 중요한 판단을 하도록 한다. 이런 공격에 대해 다른 공격과 마찬가지로 인증과 같은 암호화 기법으로 시빌 공격에 대해 방어를 할 수 있지만 저전력, 저사양을 특징으로 하는 센서 노드에서는 구현이 쉽지 않다[1-4].

본 논문에서는 에너지 고려 라우팅을 기반으로 하여 거짓 노드 군집에 속할 가능성이 있는 노드를 탐지한다. 제안 기법은 네트워크 전체에서 정상 노드의 군집과 거짓 노드의 군집 간에 연결성이 약하다는 특징을 이용한다[5].

연결성이 약한 두 군집 간에 랜덤 라우팅 방식을 이용하여 일정한 경로를 구축한다. 랜덤 라우팅 기법을 사용하면 센서 네트워크 내에서 임의의 간선을 지나는 경로의 개수가 제한되므로, 정상 노드의 군집과 허위 노드의 군집 사이를 지나는 경로는 두 군집을 잇는 간선의 개수가 적은 만큼 제한적이다. 반면 연결성이 좋은 군집 내에서는 상대적으로 더 많은 경로가 존재하므로, 두 경로가 특정 노드에서 교차할 경우, 이 두 경로는 확률적으로 같은 군집 내의 노드만을 지날 가능성이 높다. 이 점에 착안하여 각 노드가 다른 노드들에 대해서 정상 노드인지 허위 노드인지 여부를 판단하는 알고리즘이다.

이런 판단을 위해 탐지 알고리즘을 수행하기 위해서는 센서 노드의 에너지를 많이 소비하게 되고, 탐지 주기 또한 정해야 하는 문제가 생긴다. 제안 기법은 랜덤 라우팅에 기반을 둔 에너지 고려 라우팅에 패킷 일련번호를 추가하고 특정 신뢰 노드에서 패킷의 소스가 정상 노드인지 거짓 노드인지를 확률적으로 판단한다. 이 특정 노드는 싱크 노드를 포함하여 네트워크의 적절한 위치에 배치하여 탐지를 수행한다.

실험 결과 일정 수의 신뢰 노드를 확보할 경우 거짓 노드를 탐지할 가능성이 90%이상임을 확인하였다. 높은 탐지율에도 에너지 소모량은 기존 에너지 고려 라우팅과 거의 차이가 없어 제안 기법이 기존 센서 네트워크에 오버헤드 없이 추가될 수 있음을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 소개하고 3장에서 제안 기법의 알고리즘을 설명한다. 4장에서 실험 및 결과를 보이고 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

Douceur는 P2P 네트워크에서 시빌 공격의 위험성을 논의하였다[1]. Douceur는 자원 제약 또는 노드들 간의 통신에 대한 비현실적인 가정을 도입하더라도 시빌 공격이 발생 가능함을 보였다. 최근에는 P2P 네트워크뿐만 아니라 센서 네트워크, 소셜 네트워크 등에서도 시빌 공격의 위험성이 대두대기 시작하였고, 특히 무선 센서 네트워크에서 시빌 공격을 막기 위한 다양한 기법들이 제안되었다.

Zhang 등은 단방향(one-way) 키 체인과 해시 트리를 사용하여 센서 노드를 인증하는 기법을 제안하였다[3]. 이 기법은 센서 네트워크상의 각 노드에게 고유한 비밀키를 할당하여 단방향 키 체인을 구성하고, 해시 트리를 사용하는 인증서를 배포하여 각 노드가 단방향 키 체인을 통해 인증 받는 메커니즘을 사용하였다. 이는 센서 노드에게 고유한 비밀키[10]를 할당해야 한다는 단점이 있다.

Newsome 등은 센서 네트워크상에서 시빌 공격이 가할 수 있는 피해를 분석하여 라우팅, 자원 할당, 오류 탐지 등 센서 노드의 여러 기능에 치명적인 피해를 줄 수 있음을 보였고, 정상 노드가 라디오 자원 검사를 통해 시빌 노드를 판별할 수 있는 기법을 제안하였다[4].

무선 센서 네트워크에서 시빌 공격 방어를 위한 또 다른 기법으로는 물리적인 위치와 RSSI 사이의 상호 연관 정도에 따라 K-mean 알고리즘을 사용하여 시빌 공격 을 탐지하는 방법 이다[5]. 하지만 이 기법은 시간 가변적인 RSSI 정보 때문에 정확도가 낮은 문제가 있다.

Ⅲ. 에너지 고려 라우팅 기반 시빌 탐지

그림 1은 무선 센서 네트워크에서 정상 노드 군집과 거짓 노드 군집 간의 연결 상태를 보여주고 있다. 정상 노드를 연결하는 링크의 수와 거짓 노드를 연결해주는 링크의 수에 비해 정상 노드 군집에 속해 있는 노드와 거짓 노드 군집에 속해있는 노드를 이어주는 링크의 수는 상대적으로 적다. 그림에서는 중앙 부분에 두 링크뿐이다. 즉, 거짓 노드에서 정상 노드 군집으로 들어오는 패킷 경로는 두 군집을 연결하는 두 간선을 반드시 통과해야 한다[6].

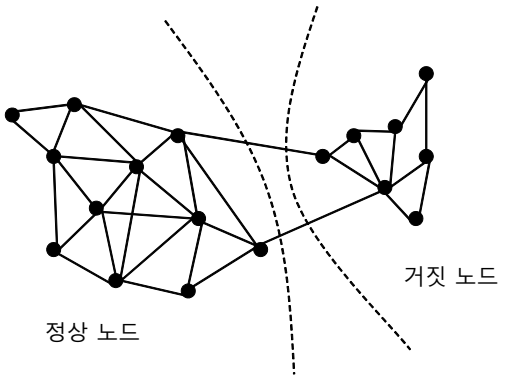

그림 1. 정상 노드와 공격/거짓 노드
Fig. 1. Normal node and attack/false node

에너지 고려 랜덤 라우팅[7]은 패킷의 경로를 결정 할 때 전송에 필요한 에너지와 노드의 잔여 에너지를 고려하여 랜덤하게 다음 전송 노드를 선정하는 방식이다. 따라서 동일한 소스의 패킷이 일정 횟수 이상 연속적으로 같은 링크를 지난다면 링크의 좌우 군집의 연결이 매우 약하다고 판단하여 이 패킷의 소스가 거짓 노드일 가능성이 높다고 판단한다. 이 판단을 위해 패킷에 일련번호를 추가하여 패킷이 얼마나 연속적으로 같은 링크를 지나고 있는지 판단한다.

정상 노드와 거짓 노드 군집에 하나의 링크가 아니라 상대적으로 적은 수의 링크로 연결되는 것이므로 이를 판단하기 위해 정상적인 노드 군집에서 가능한 평균적인 링크 수(한 노드가 패킷을 보낼 수 있는 이웃 노드의 수를 의미함, *Normal_Link_Num*)를 설정한다. 만일 *Normal_Link_Num*이 3이고 이웃 노드를 선택할 확률이 동일하다면 확률적으로 패킷 세 개중에 하나가 한 링크로 지나가게 된다. 패킷 두 개가 연속으로 한 링크로 지날 확률은 1/9이 되고, 이는 정상적인 노드로부터 온 패킷일 확률이 1/9이란 것을 의미한다.

에너지 고려 랜덤 라우팅은 다음과 같은 식으로 이웃 노드 선택 확률이 계산된다.

$$\overline{C_{i,j}} = \overline{C_j} + E_{i,j} \tag{1}$$

$\overline{C_{i,j}}$는 노드 i에서 노드 j를 통해 싱크 노드까지 패킷을 전송하는데 필요한 기대 에너지를 의미한다. $\overline{C_i}$는 패킷을 노드 i에서 싱크 노드까지 보내는데 필요한 기대 에너지 비용으로, 싱크 노드의 경우 $\overline{C_{sink}} = 0$이다. $E_{i,j}$, 각각 노드 i와 노드 j 사이에서 단일 홉 통신의 에너지 비용을 의미한다.

$$E_{i,j} = (d_{i,j}^3)^{\alpha} / B_j^{\beta} \tag{2}$$

여기에서 $d_{i,j}$는 노드 i와 노드 j간의 거리를 의미한다. B_j는 노드 j의 에너지 잔량으로 초기 에너지에 일반화한 값이다. α와 β는 가중치 요소이다.

노드 i의 라우팅 테이블(*RT*)에 있는 모든 이웃 노드에 대해 다음과 같이 라우팅 확률($P_{i,k}$)을 계산한다. 라우팅 테이블에 있는 모든 이웃 노드 k에 대해

$$P_{i,k} = \frac{1/\overline{C_{i,k}}}{\sum_{m \in RT} 1/\overline{C_{i,m}}} \tag{3}$$

$P_{i,k}$는 노드 i가 노드 k를 패킷 전달할 다음 노드로 선택할 확률이다. 그래서 에너지를 적게 소모하는 이웃 노드가 선택될 가능성이 높아지게 된다.

신뢰 노드는 정상 노드임을 인정받은 노드로 위의 확률을 사용하여 거짓 노드를 탐지하는 노드이다. 싱크 노드도 당연히 신뢰 노드에 포함된다. 신뢰 노드는 자신이 가지고 있는 라우팅 테이블의 각 노드 선택 확률 $P_{i,k}$를 기반으로 하여 다른 이웃 노드의 확률을 추정한다. 즉 신뢰 노드에서 이웃 노드가 5개 A, B, C, D, E, F이고 각각에 대해 선택 확률(PA, PB, PC, PD, PE)이 계산되어 있다면 그 이웃 노드들도 해당 확률로 패킷을 보내 올 것으로 예측한다. 물론 이 확률이 실제 이웃 노드가 패킷을

보내올 확률과 차이가 있을 수 있다. 만일 F가 거짓 노드라면 신뢰 노드가 기대하는 PF의 확률 보다 훨씬 높은 확률로 F에서 패킷이 전달된다. 거짓 노드의 경우 싱크로 패킷을 보내기 위해 반드시 신뢰 노드를 거쳐야 하기 때문이다.

Ⅳ. 실험 및 결과

제안 기법의 성능을 측정하기 위해 GloMoSim[8] 시뮬레이터를 사용하였다. GloMoSim은 무선 통신을 위한 매우 빠르고 효율적인 이벤트 기반 시뮬레이터이다. 또한 구체적인 전달 모델, 라디오, MAC 레이어를 가지고 있다. 표 1은 구체적인 실험 환경에 대한 파라미터이다.

표 1. 실험 파라미터
Table 1. Simulation Parameters

MAC 레이어	802.11 (Simplified DCF)
물리(라디오) 레이어	RADIO-ACCNOISE
전달 모델	TWO-RAY
대역폭 (Kb/s)	200
패킷 크기 (bits)	256
필드 크기 (m × m)	100 × 100
센서 노드 수	100 (정상 노드 90, 거짓 노드 10)
노드 배치	랜덤 배치 싱크는 필드 중앙에 배치
무선 송신 거리 (m)	25
초기 에너지 (J)	0.1

모든 센서 노드들은 매초마다 싱크 노드로 데이터를 전송한다. 이 때 0번부터 패킷에 일련번호를 붙여서 전송을 한다. 에너지 비용 $E_{i,j}$에서 α와 β 는 각각 1과 50을 사용하였다.

전체 100개의 노드 중 거짓 노드는 10개로 하였고, 정상 노드 군집과의 연결은 두 개로 제한하였다. 즉, 거짓 노드에서 싱크로 데이터를 보내기 위해서는 두 링크 중 하나를 반드시 지나가도록 하였다.

비교를 위해 기존 에너지 고려 라우팅(EAR)과 제안 기법(EAR-S)을 실험하였다. 그림 2는 노드 평균 잔여 에너지량을 비교한 그래프이고, 그림 3은 신뢰 노드에서 거짓노드마다 거짓 노드로 판단할 확률을 나타낸 것이다.

그림 2에서 알 수 있듯이 기존 에너지 고려 라우팅(EAR)과 비교하여 제안 기법(EAR-S)의 에너지 사용량이 비슷함을 알 수 있다. 패킷 전송 수에 따라 비례하여 에너지가 줄어들지 않는 이유는 에너지가 고갈 되어 죽어 버리는 노드가 생겨서 다른 노드가 에너지를 더 소모해버리기 때문이다.

그림 3에서 신뢰 노드에서 판단한 거짓 노드의 거짓일 확률을 보면 10개의 거짓 노드에 대해 대부분 0.9 이상의 확률을 보이고 있다. 즉, 90% 이상의 확률로 거짓 노드 탐지가 가능함을 알 수 있다.

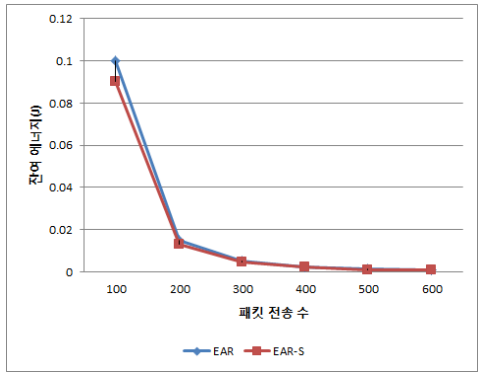

그림 2. 노드 평균 잔여 에너지량
Fig. 2. Average residual energy of nodes

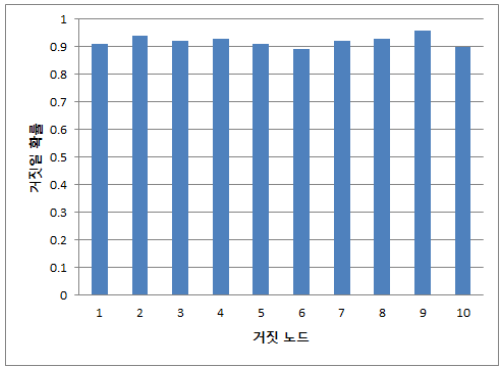

그림 3. 거짓 노드일 확률
Fig. 3. Probability of false node

Ⅴ. 결 론

무선 센서 네트워크의 다양한 용도만큼 많은 취약점과 다양한 공격 가능성이 여러 논문에서 제기되고 있다. 여러 공격 중에서도 시빌(sybil) 공격은 공격 노드가 많

은 수의 거짓 노드를 생성하여 네트워크에 잘 못된 정보를 보내는 공격이다. 사용자가 공격을 받았음을 인지하지 못하고 거짓 노드로부터 온 데이터를 사실로 오인하고 사용하게 되면 민감한 데이터일 경우 재앙이 될 수도 있다. 인증과 같은 암호화 기법으로 방어를 할 수 있지만 저전력, 저사양을 특징으로 하는 센서 노드에서는 구현이 곤란하다.

본 논문에서는 센서 네트워크에서 시빌 공격으로 생성된 거짓 노드를 탐지하는 기법을 제안한다. 제안 기법은 정상 노드의 군집과 거짓 노드의 군집 간에 네트워크가 약하다는 특징을 이용한다. 또한 센서 노드의 저전력을 고려하여 기존 에너지 고려 라우팅에 약간의 데이터를 추가함으로써 오버헤드를 최소화 하였다. 실험 결과를 통해 제안 기법이 기존 에너지 고려 라우팅에 비해 추가적인 에너지 소모가 극히 적으면서도 시빌 공격의 탐지를 90% 이상 할 수 있음을 보였다.

향후 정상 노드 군집과 기존 노드 군집의 연결 강도와 신뢰 노드 수에 따른 탐지 확률을 계산하여 신뢰 노드의 수와 위치를 결정하는 방법을 추가하여 연구를 확장할 계획이다.

참 고 문 헌

[1] John R. Douceur, The Sybil Attack, in proc. of 1st international workshop on peer-to-peer systems, pp. 251-260, 2002.

[2] A. Pathan, H. Lee, and Choong Seon Hong, Security in wireless sensor networks: issues and challenges, in proc. of the 8th international conference on advanced communication technology, pp. 1043-1048, 2006.

[3] Q. Zhang, P. Wang, D. Reeves, and P. Ning, Defending against Sybil Attacks in Sensor Networks, in proc. of IEEE international conference on distributed computing systems workshops, pp. 185-191, 2005.

[4] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, in proc. of the 3rd international symposium on information processing in sensor networks, pp. 259-268, 2004.

[5] J. Yang, Y. Chen, and W. Trappe, Detecting sybil attacks in wireless and sensor networks using cluster analysis, Mobile Ad Hoc and Sensor Systems (MASS 2008), pp. 834-839, 2008.

[6] H. Yu, M. Kaminsky, P. B. Gibbons, and Abraham Flaxman, Sybilguard: defending against Sybil attacks via social networks, in proc. of the conference on applications, technologies, architectures, and protocols for computer communications, pp. 267-278, 2006.

[7] Shah, R., Rabaey, J. “Energy aware routing for low energy ad hoc sensor networks,” Proc. of IEEE Wireless Communications and Networking Conference(WCNC), 2002.

[8] X. Zeng, R. Bagrodia, and M. Gerla, “GloMoSim: a library for parallel simulation of large-scale wireless networks,” ACM SIGSIM Simulation Digest, vol. 28, no. 1, pp. 154 - 161, 1998.

[9] I. S. Choi, Y. W. Cha, C. H. Kim, I. K. Cho, "Design and Implementation of Management Protocol and Web Services for Sensor Network", Journal of Korean Institute of Information Technology, vol 9, issue 7, pp. 93-104, Jul 2011

[10] S. K. Sung, "A Study on the Activation Technique of Detection nodes for Intrusion Detection in Wireless Sensor Networks", Journal of the Korea Academia-Industrial cooperation Society, v.12, no.11, pp. 5238-5244, 2011

※ 본 연구는 한성대학교 연구장려금 지원과제임.

저자 소개

허 준 영(회원)

- 1998년 : 서울대학교 컴퓨터공학과 졸업(학사).
- 2009년 : 서울대학교 컴퓨터공학부 졸업(박사).
- 2009년 ~ 현재 : 한성대학교 컴퓨터공학과 조교수.

<주관심분야 : 운영체제, 무선 센서 네트워크, 임베디드 시스템, 결함허용 시스템>