한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

무선 센서 네트워크의 다중 경로 라우팅에서 네트워크 수명 연장을 위한 플로딩 공격 기법

정원진[O], 조대호[*]
[O]성균관대학교 정보통신대학
[*]성균관대학교 소프트웨어대학
e-mail: wonjin12@skku.edu[O], thcho@skku.edu[*]

A Method Against Flooding attacks to Extend Network Lifetime in Multipath Routing of Wireless Sensor Networks

Won-Jin Chung[O], Tae-Ho Cho[*]
[O]College of Information and Communication Engineering, Sungkyunkwan University
[*]College of Software, Sungkyunkwan University

● 요 약 ●

무선 센서 네트워크에서 센서 노드의 취약점으로 인해 공격자는 쉽게 훼손된 노드를 만들어 센서 네트워크를 공격한다. DoS 공격에 해당하는 플로딩 공격은 노드의 에너지 손실과 경로 상의 노드의 에너지를 전부 소비시켜 네트워크 수명이 단축된다. 본 논문에서 제안 기법은 노드의 에너지가 적은 지역에서 다중경로 라우팅을 적용해 각 노드의 부하를 줄이고 네트워크 수명을 증가시키는 보안기법을 제안한다.

키워드: 무선 센서 네트워크, 네트워크 보안, 플로딩 공격

I. Introduction

무선 센서 네트워크(wireless sensor network; WSN)는 수많은 소형 센서 노드들과 기지국(base station; BS)으로 구성되어 있으며 다양한 분야에 사용된다. 하지만 센서 노드는 제한된 계산능력과 적은 에너지 그리고 무선통신을 사용하기 때문에 공격에 취약하다는 단점이 있다. 이러한 취약점을 이용하여 공격자는 노드를 쉽게 훼손을 시킨 이후 다양한 공격을 시도한다[1]. 본 논문에서는 센서 네트워크에서 발생하는 공격 중에서 서비스 거부 공격(Denial of Service)에 해당하는 플로딩 공격(flooding attack) 탐지에 대한 센서 네트워크 수명을 연장하는 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 플로딩 공격과 다중경로 라우팅을 설명한다. 3장에서는 다중 경로 라우팅을 사용하는 제안 기법을 설명하고, 기존 기법과 제안 기법의 실험 결과를 분석한다. 4장에서는 결론과 향후 연구방향을 제시한다.

II. Related works

1. 플로딩 공격

플로딩 공격은 지속적 거짓 이벤트를 발생시켜 네트워크 마비와 노드의 에너지 고갈로 센서 네트워크 수명이 단축된다. 플로딩 공격으로 소스 노드는 거짓된 이벤트를 계속 수집하고 BS로 패킷을 전달한다. 이러한 과정에서 노드들은 지속적인 에너지를 소비한다. 노드의 에너지가 플로딩 공격으로 에너지가 전부 소비되고 실제 이벤트가 발생하여도 BS로 전달하지 못한다.

2. 다중경로 라우팅

다중 경로 라우팅(multipath-based routing)은 센서 노드의 부하를 줄이기 위해 여러 개의 가용한 경로를 설정하고 BS에 패킷을 전달하는 방법이다. 다중 경로 라우팅은 설정된 경로로 패킷을 분배하여 보내거

나 패킷을 차례대로 보내어 센서 노드의 부하를 균등하게 분배할 수 있다. 이러한 방법으로 경로에 설정된 센서 노드의 에너지 효율이 증대되고 센서 네트워크의 수명을 연장할 수 있다[2].

III. The Proposed Scheme

WSN에서 플로딩 공격 탐지 기법은 탐지를 위해 BS까지 다량의 패킷들이 전달된다. 이러한 과정에서 해당 경로에 있는 센서 노드들의 에너지가 고갈될 수 있다. 따라서 제안 기법은 다중 경로 라우팅을 사용하여 각 센서 노드의 에너지 소비를 줄이고 센서 네트워크의 수명 연장을 목표로 한다. 플로딩 공격 탐지는 ad-hoc network에서 제안한 Flooding Attack Prevention(FAP)을 변형하여 사용 한다[3]. 제안 기법은 플러딩 공격이 발생하면 소스 노드는 데이터를 수집하고 클러스터 헤더에 전달한다. 이후 클러스터 헤더는 소스 노드 ID가 블랙리스트에 포함된 노드인지 확인하고 포함되지 않으면 패킷을 다중 경로 라우팅으로 BS로 전달한다. 수집된 패킷은 이전 패킷과 비교하여 같은 소스 노드 ID와 패킷 전송 시간이 1초 정도 차이 날 경우 공격 변수를 증가시킨다. 공격 변수가 임계값보다 클 경우 플로딩 공격으로 의심하고 소스 노드에서 전달되는 패킷을 차단하고 소스 노드 ID를 블랙리스트로 추가한다.

실험에서 사용한 센서 네트워크의 필드 크기는 200×200이며 사용된 노드의 수는 125개이며 그중 25개는 클러스터 헤더이다. 센서 노드는 1byte의 메시지를 송수신할 때 각 16.25㎲, 12.25㎲의 에너지를 소모한다. 메시지의 크기는 29 bytes로 설정한다. FAP 알고리즘과 같이 임계값은 15로 설정한다.

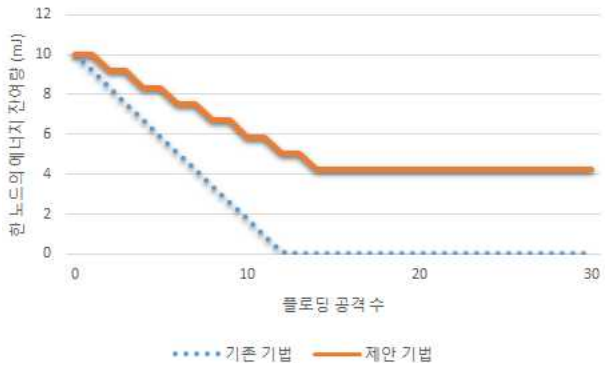

Fig. 1. 플러딩 공격 횟수에 따른 한 노드의 에너지 잔여량

Fig.1은 플로딩 공격 경로에 포함된 한 센서 노드 에너지 소모량을 보여준다. 위 실험을 통하여 에너지가 전부 고갈된 센서 노드의 수는 제안 기법인 경우 훼손된 노드와 같은 셀에 있는 클러스터 헤더, 그리고 BS 이전 클러스터 헤더 총 2개의 센서 노드의 에너지가 고갈된다. 기존기법인 경우 제안 기법에서 고갈된 센서 노드들을 포함하고, 경로에 포함된 클러스터 헤더 에너지가 추가로 고갈되어 총 8개의 센서 노드의 에너지가 전부 소모되었다.

IV. Conclusions

본 논문에서는 WSN에서 발생하는 플로딩 공격을 탐지하는 과정에서 다중경로 라우팅을 사용하여 각 센서 노드의 소모에너지를 분배하는 기법을 제안한다. 각 센서 노드의 에너지 효율 증대와 네트워크 수명을 연장에 기여한다. 향후 연구는 기존 기법과 제안 기법에서 고갈된 노드들의 에너지 소모를 감소시킬 수 있는 추가적인 연구가 필요할 것이다.

Acknowledgments

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임
(No. NRF-2015R1D1A1A01059484)

References

[1] D.R. Raymond, and S.F. Midkiff, ”Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses,” IEEE Pervasive Computing, Vol. 7, No. 1, pp. 74-81, Jan. 2008.

[2] M. Radi, B. Dezfouli, K.A. Dakar, and M. Lee “Multipath routing in wireless sensor networks: survey and research challenges,” Sensors, Vol. 12, No. 1, pp. 650-685, Jan. 2012.

[3] Y. Ping, H. Yafei, Z. Yiping, Z.Shiyong, and D. Zhoulin, ”Flooding attack and defence in ad hoc networks,” Journal of Systems Engineering and Electronics, Vol. 17, No. 2, pp. 410-416, Jan. 2006.