Wireless Ad-hoc Network에서 하이브리드 방어 메커니즘을 이용한 안전성 향상에 관한 연구

양환석*

요약

Wireless ad-hoc network는 제한된 자원과 개방된 네트워크 구조 때문에 보안상 취약점에 쉽게 노출되어 있다. 특히 노드들의 이동으로 인한 동적인 토폴로지 때문에 경로 설정 및 데이터 전송은 플러딩을 통해 이루어진다. 이러한 특성을 이용한 플러딩 공격은 네트워크 전체에 영향을 미칠 만큼 그 피해가 매우 크다. 본 논문에서는 네트워크 전역에서 분산적으로 RREQ 플러딩 공격과 데이터 플러딩 공격을 탐지하고 고립시킬 수 있는 하이브리드 방어 메커니즘을 제안하였다. 공격 노드에 대해 능동적인 탐지와 정확도를 향상시키기 위하여 네트워크 전체 트래픽의 양을 반영하였다. 그리고 의심 노드의 탐지 성능을 높이기 위하여 전체 네트워크를 일정한 영역으로 분할한 영역 기반 형태를 이용하였다. 제안한 기법의 성능 평가를 위하여 PFM, TBSS 기법과 비교실험 하였으며, 실험을 통해 제안한 기법의 우수한 성능을 확인하였다.

A Study on Improvement Security using Hybrid Defense Mechanism in Wireless Ad-hoc Network

Hwan-Seok Yang*

ABSTRACT

Wireless ad-hoc network is exposed easily to security vulnerabilities due to limited resources and open network structure. Routing and data transfer is performed through the flooding because of especially the mobility of nodes. The damage is huge as flooding attacks using these characteristics affect the whole network. In this paper, we propose hybrid defense mechanism that can detect RREQ flooding and data flooding attack in whole network and isolate. The amount of whole traffic of network is investigated in order to improve active detection and accuracy against attack nodes. The area-based shape which divides whole network to constant area to improve detection performance of suspicious nodes is used. The proposed method does comparative experiments with PFM, TBSS method in order to evaluate its performance and the superior performance of the proposed method is confirmed by the experiments.

Key Words : Wireless Ad Hoc Network, Flooding Attack, Denial of Service, Routing Attack, RREQ

*중부대학교 정보보호학과 (✉ yanghs@joongbu.ac.kr)
· 제1저자(First Author) : 양환석 · 교신저자(Correspondent Author) : 양환석
· 접수일(2013년 10월 28일), 수정일(1차 : 2013년 11월 25일), 게재확정일(2013년 12월 12일)

Ⅰ. 서 론

Wireless Ad-hoc Network는 유선 네트워크 구축이 어려운 상황에서 적은 비용으로 빠르게 무선 네트워크를 구축할 수 있는 장점이 있어 인기를 얻어왔다[1]. 네트워크를 구성하는 각 노드들은 전송 범위의 이웃 노드를 이용한 다중 홉 방식으로 통신이 이루어진다[2]. Wireless Ad-hoc Network에서는 노드들의 이동으로 인하여 네트워크 토폴로지가 수시로 변화하기 때문에 노드간의 경로를 유지하기가 어렵다[3]. 따라서 이러한 특성을 고려한 라우팅 프로토콜이 필요하다. 하지만 이러한 라우팅 프로토콜의 취약점을 이용한 플러딩 공격이 증가하고 있으며 그 피해 또한 다른 공격들에 비해 상당히 크다[4].

본 논문에서는 플러딩 공격에 대한 피해를 줄이고 능동적인 대응이 이루어질 수 있는 하이브리드 방어 메커니즘을 제안하였다. 제안한 기법에서는 분산된 방어를 통하여 공격에 빠르게 대응하기 위하여 네트워크를 영역으로 분리한 후, 영역 기반 탐지를 수행하였다. 각 노드에서는 RREQ 플러딩 공격의 탐지를 위해서 NMT(Neighbor Monitoring Table)을 이용하였으며, 데이터 플러딩 탐지를 위해 목적 노드에서는 수신한 데이터 처리율을 계산하여 의심 노드를 판단하였다. 그리고 관리 노드(Administration Node)에서는 전체 네트워크 제어 트래픽의 평균값을 계산하여 멤버 노드들에게 의심 노드를 판단하기 위한 두 개의 기준값을 전송해주며, 의심 노드들에 대한 정보를 전송하는 역할을 수행하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 플러딩 공격 탐지기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 하이브리드 방어 메커니즘에 대하여 기술하였다. 4장에서는 제안한 기법의 성능 평가를 위하여 PFM, TBSS 기법과 비교 실험하였으며 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

DoS 공격의 일종인 플러딩 공격은 공격 노드가 네트워크 또는 노드들의 유용한 자원을 소모시키기 위하여 잘못된 많은 패킷을 전송하는 공격으로서, on-demand 방식의 모든 라우팅 프로토콜에서 나타날 수 있다[5]. RREQ 플러딩 공격은 경로 발견시 잘못된 주소의 RREQ 패킷을 대량으로 브로드캐스트하여 플러딩 설정을 초과시켜 자원을 소모시키는 공격이고, 데이터 플러딩 공격은 경로가 설정된 목적 노드들에게 위조된 데이터 패킷을 대량으로 전송하는 방법이다[6].

PFM(Prevention of Flooding attack in MANET) 기법은 플러딩 공격의 피해를 줄이기 위하여 신뢰 함수를 이용하였다[7]. 이 기법에서는 각 노드들의 신뢰 값에 따라 stranger, acquaintance, friend 세 가지로 분류하였다. Stranger는 신뢰할 수 없는 노드를 의미하고, friend는 신뢰하는 노드를 의미하며 acquaintance는 그 사이의 신뢰 값을 갖는 노드이다. 어떤 노드가 RREQ 패킷을 수신하게 된다면 노드의 관계를 검사한다. 만약 stranger에 속하게 된다면 노드로부터 수신한 패킷을 폐기하고, 해당 노드를 블랙리스트로 설정한다. 이 기법에서는 이동 속도가 빨라지면 성능이 떨어지는 단점을 가지고 있다.

TBSS 기법은 PFM 기법의 확장된 기법으로서 PFM 기법에서 노드들이 이동이 빨라지면 노드들에 대한 관계 계산이 어려워져지는 단점을 보완하기 위하여 지연 큐 개념을 도입하였다[8]. 즉, 노드들의 빠른 이동 속도에도 노드들에 대한 관계 계산의 정확도를 높이기 위하여 이웃 노드의 관계 유형이 acquaintance이고 기준값보다 작은 경우에 해당 노드의 패킷은 전달해 주지만 노드를 지연 큐에 삽입한 후, 일정시간 해당 노드의 패킷과 행동을 분석한 후 공격자인지 정상인지를 검사하였다.

III. 제안한 기법

본 장에서는 RREQ 플러딩 공격과 데이터 플러딩 공격을 효율적으로 차단할 수 있는 하이브리드 방어 메커니즘에 대하여 기술한다.

3.1 시스템 모델

네트워크를 구성하는 전체 노드들로부터 발생하는 패킷들에 대한 실시간 감시가 원활하게 이루어질 수 있는 영역 기반 형태를 이용하였다. 전체 네트워크를 일정한 크기의 영역으로 분할한 후 각 영역을 담당하는 관리 노드를 선출하였다. 선출된 관리 노드는 영역 내의 RREQ 플러딩 공격 탐지를 위하여 멤버 노드들로부터 수신한 RREQ 정보를 수신하며, 각 영역의 관리 노드들은 주기적인 간격으로 관리 영역의 평균 제어 메시지 양을 주고받는다. 본 논문에서 사용한 영역 기반 네트워크의 구조를 <그림 1>에서 보여주고 있다.

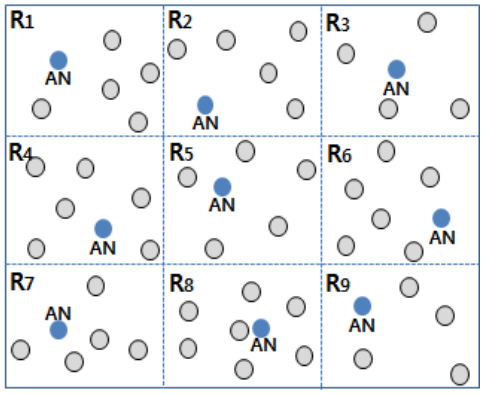

그림 1. 영역 기반 네트워크의 구조
Fig. 1. Structure of Network based Region

관리 노드는 RREQ 플러딩 공격 탐지를 위하여 멤버 노드들로부터 일정 시간 간격으로 각 노드들로부터 수신한 RREQ 정보를 RMT(Region Management Table)에 저장한다. 이렇게 수신한 RREQ 양을 측정한 후 평균값을 멤버 노드들에게 전송한다. 그리고 RMT 테이블에는 의심스러운 노들에 대한 정보 역시 저장된다. 그리고 멤버 노드에서는 자신의 이웃 노드로부터 수신한 RREQ 패킷을 수신할 때마다 자신이 관리하는 NMT에 그 정보를 저장한다. 여기에는 각 RREQ 생성 노드에게 수신된 RREQ 개수를 유지한다. 이렇게 RREQ 패킷을 수신할 때마다 평균값과 검사가 이루어져 그 이상의 패킷을 생성한 노드는 의심노드로 결정하여 관리 노드에게 통보하게 된다. 그리고 각 멤버 노드에서는 데이터 플러딩 공격 여부를 계산하기 위하여 NMT에 각 노드들에게 수신한 데이터 패킷에 대한 정보도 저장한다. <그림 2>는 RMT와 NMT의 구조를 보여주고 있다.

Time Slot	Node Addr	RREQ Cnt	Data Cnt	Min_Limit	Max_Limit

(a) NMT(Neighbor Monitoring Table)

Node Addr	RREQ Flag	Data Flag	TimeOut	Status

(b) RMT(Region Management Table)

그림 2. NMT와 RMT 구조
Fig. 2. Structure of NMT, RMT

3.2 하이브리드 방어 메커니즘

본 논문에서는 RREQ 플러딩 공격과 데이터 플러딩 공격을 막기 위한 하이브리드 방어 메커니즘을 제안하였다. 먼저 RREQ 플러딩 공격은 특정 노드를 목표로 하여 가짜 RREQ를 무작위로 전송하고, 데이터 플러딩 공격은 특정 노드에 피해를 주기 보다는 전체 네트워크를 방해하기 위하여 다중 홉을 통해 많은 데이터 패킷을 송신한다. 그리고 데이터 플러딩 공격은 경로를 설정한 후에 이루어지게 된다. 따라서 본 논문에서는 관리 노드로부터 수신한 RREQ 최대값과 최소값을 이용하여 멤버 노드에서 의심스러운 노드의 탐지와 데이터를 수신한 목적 노드에서 처리된 패킷 양을 계산하여 데이터 플러딩 공격을 탐지하는 하이브리드

탐지 과정을 거치게 된다. 먼저, 관리 노드는 영역내의 멤버 노드들로부터 수신한 RREQ의 평균값과 이웃 영역 관리 노드들로부터 수신한 RREQ의 평균값을 계산하여 큰 값은 MAX_Limit로 작은 값은 MIN_Limit로 설정하여 NMT에 저장하고, 이 값을 멤버 노드에게 전송한다. 네트워크내의 멤버 노드들은 단위 시간 동안 이웃 노드들로부터 수신한 RREQ 개수를 카운트하여 그 값이 Min_Limit 값 미만이면 정상, Min_Limit과 Max_Limit 사이면 감시, Max_Limit을 초과하면 의심 노드로 판단한다. 의심 노드로 판정된 노드 정보를 관리 노드에 전송하면, 관리 노드에서는 멤버 노드들과 이웃 관리 노드들에게 해당 정보를 전송한다. 의심 노드부터 생성되는 RREQ 패킷에 대하여 이웃하는 모든 노드들이 RREQ_Timeout 시간동안 무시하게 된다. 이러한 분산된 방어를 통해 RREQ 플러딩 공격의 피해를 막을 수 있게 된다.

경로 설정 후에 이루어지는 데이터 플러딩 공격 탐지는 목적 노드에서 소스 노드가 송신한 패킷 처리율을 계산하여 이루어진다. 즉, 목적 노드는 t_i에서 t_{i+1} 시간동안 수신한 모든 데이터 패킷의 평균(D_{avg}) 값과 특정 소스 노드가 송신한 패킷(S_D)과 그 노드로부터 수신한 패킷(R_D)의 차를 계산하여 데이터 플러딩 공격의 기준값을 식 1과 같이 계산한다.

$$T_{value} = v(S_D - R_D) + D_{avg} \quad (1)$$

만약 목적 노드에서 수신한 패킷 양이 기준값보다 크다면 데이터 플러딩 공격 노드로 판단하여 해당 노드에 대한 정보를 관리 노드에 통보하고 의심 노드로부터 수신되는 모든 패킷을 무시하게 된다. 관리 노드에서는 의심 노드의 고립을 위해 모든 멤버 노드와 이웃 멤버 노드에게 정보를 전송하는 과정을 수행한다. 본 논문에서 제안한 하이브리드 방어 과정을 <그림 3>에서 보여주고 있다.

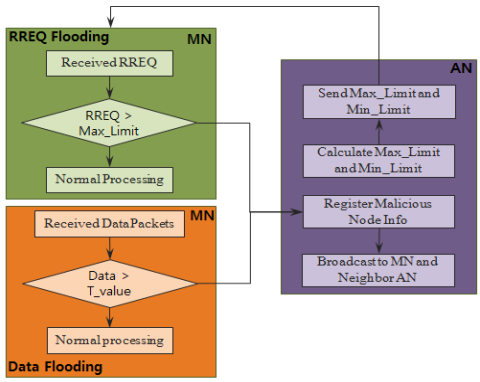

그림 3. 제안한 하이브리드 방어 메커니즘
Fig. 3. Proposed Hybrid Defense Mechanism

Ⅳ. 모의실험 및 결과

4.1 모의실험 환경

본 논문에서 제안한 하이브리드 방어 메커니즘은 ns-2 시뮬레이터를 이용하였으며, 성능 평가를 위해서 PFM 기법, TBSS 기법과 비교 실험하였다. 실험 시간 300초 동안 20번의 공격을 발생시켰으며, 노드들의 전력 소모는 고려하지 않았다. <표 1>은 실험에 사용한 환경 변수 값을 보여주고 있다.

표 1. 모의실험에 사용한 환경변수
Table 1. Simulation parameters

Parameter	Values
Network size	1000m × 1000m
Mobility model	Random waypoint
Number of nodes	50
Routing Protocol	AODV
Transmission range	200m
Traffic	CBR
Attack Nodes	10
Pause time(Sec)	20

4.2 결과

본 논문에서 제안한 기법의 성능 평가기준은 공격 노드 수에 따른 플러딩 공격 탐지율과 신뢰도 평가를 위해 FPR(False Positive Rate) 그리고 네트워크 성능을 측정할 수 있는 RREQ 패킷 양으로 하였다.

<그림 4>에서는 플러딩 공격에 대한 제안한 기법과 TBSS 기법, PFM 기법의 공격 탐지율을 보여주고 있다. 그림에서 보여주듯이 PFM 기법은 노드들의 이동 속도에 따라 탐지율이 크게 떨어졌으며, TBSS 기법은 노드들의 이동 속도가 빨라져도 탐지율이 향상은 되었으나, 노드들의 관계 계산에 시간이 걸려 성능이 다소 떨어지는 결과를 보였다. 제안한 기법은 멤버 노드들의 협력과 관리 노드에서 전체적인 트래픽 감시가 원활이 이루어져 이동 속도에 상관없이 안정된 성능을 보여줌을 확인할 수 있었다.

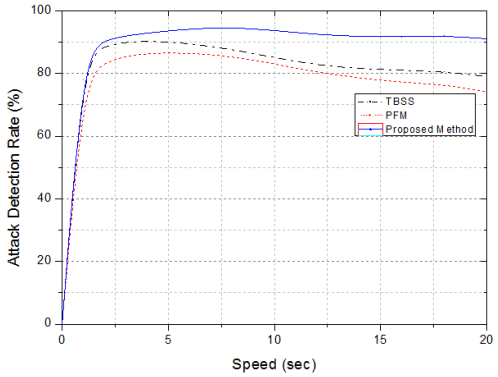

그림 4. 공격 탐지율
Fig. 4. Attack detection rate

각 기법들의 신뢰도 평가의 척도가 되는 FPR 측정 결과는 <그림 5>에서 보여주고 있다. PFM은 이동 속도 증가에 따른 정확한 신뢰 평가가 이루지지 않았기 때문에 결과가 좋지 않았고, TBSS 기법은 이동 속도에 따른 신뢰 함수의 정확도가 떨어져 결과가 다소 좋지 않았다. 제안한 기법에서는 공격 노드를 판단하는 기준값에 전체 네트워크의 트래픽을 반영하였기 때문에 가장 좋은 성능을 보여주었다.

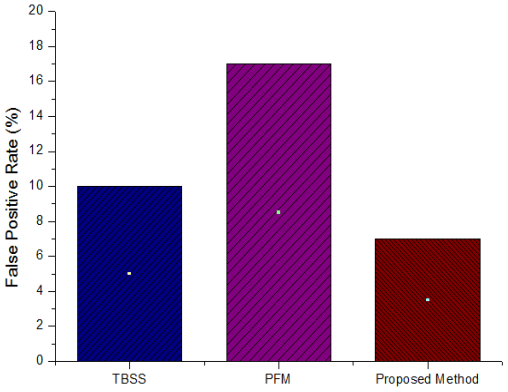

그림 5. FPR 측정 결과
Fig. 5. Measurement results of FPR

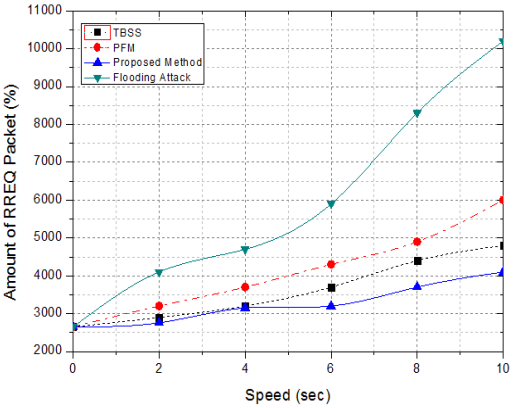

그림 6. RREQ 패킷 양 측정 결과
Fig. 6. Amount of RREQ Packets

네트워크에 제어 패킷의 양이 많을수록 대역폭 소모가 증가하기 때문에 전체 네트워크의 성능은 떨어질 수밖에 없다. <그림 6>에서는 공격 탐지 기법이 적용되지 않은 공격 노드에 의한 RREQ 패킷의 양을 보여주고, 제안한 기법과 PFM 기법, TBSS 기법이 각각 적용되었을 때 RREQ 패킷의 양을 측정한 결과를 보여

주고 있다. 그림에서 볼 수 있듯이 위 결과는 공격 탐지율과 반비례하였으며, 제안한 기법이 가장 우수한 결과를 보여주고 있다.

V. 결 론

본 논문에서는 RREQ 플러딩 공격과 데이터 플러딩 공격에 능동적으로 대응할 수 있는 하이브리드 방어 메커니즘을 제안하였다. 제안한 기법에서는 효율적인 공격 탐지를 위하여 전체 네트워크를 일정 영역으로 분할한 후 노드들 간의 협력적 방법을 이용하였다. 관리 노드는 RREQ 플러딩 공격 탐지시 이용되는 두 개의 기준값을 계산할 때, 전체 네트워크 트래픽 양을 반영하여 공격 탐지의 정확도를 향상시킬 수 있었으며, 각 멤버 노드에서는 이웃 노드들의 정보를 NMT 테이블에 저장 및 관리하고 분산적인 공격 탐지를 수행하여 네트워크 안정성을 높일 수 있었다. 그리고 데이터 플러딩 공격 탐지를 위하여 데이터를 수신한 목적 노드에서 데이터 처리율을 계산한 후 관리 노드로부터 수신한 기준값과 비교하였다. 공격 탐지를 위해 사용되는 기준값들은 관리 노드에서 의해 계산되며, 공격 탐지는 각 멤버 노드에서 분산적으로 수행함으로써, 모든 노드들의 자원 활용률을 극대화할 수 있었다. 본 논문에서 제안한 하이브리드 방어 메커니즘 기법의 우수한 성능은 실험을 통하여 확인할 수 있었다.

참고문헌

[1] P. Albers, O. Camp, J.-M. Percher, B. Jouga, L. Mé, R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches ," *in Proceedings of the First International Workshop on Wireless Information Systems*, 2002.

[2] Meenakshi Patel, Sanjay Sharma, " Detection and prevention of Routing Attacks in MANET using AODV," *International Journal of Advanced Research in Computer Science and Electronics Engineering*, Vol. 1, Issue 1, pp.39-44, 2012.

[3] P. Michiardi, R. Molva,"Ad hoc networks security," *IEEE Press Wiley*, New York, 2003.

[4] Yongguang Zhang, Wenke Lee, Yi-An Huang, "Intrusion detection techniques for mobile wireless networks", *Wireless Networks*, Vol. 9, No. 5, pp.545-556, 2003.

[5] K. Bhuvaneshwari and F. S. Devaraj, "PDS-A Profile based Detection Scheme for flooding attack in AODV based MANET," *International Journal of Security, Privacy and Trust Management,*, Vol. 2, No. 3, pp.17-28, 2013.

[6] S. Kannan, T. Maragatham, S. Karthik and V.P. Arunachalam, "A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols," *International Business Management*, Vol. 5, Issue. 3, pp.178-183,2011.

[7] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka and T. Rama Rao, "Prevention of flooding attack in mobile ad hoc network," *International Conference on Advances in Computing,* pp.365-373, 2005.

[8] Shishir K. Shandilya, Sunita Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET," *International Journal of Computer Applications*, Vol. 5, No. 12, pp.4-8, 2010.

저자소개

양환석(Hwan-Seok Yang)

1998년 조선대학교 대학원 전산통계학과(이학석사)
2005년 조선대학교 대학원 전산통계학과(이학박사)

2011년~현재 중부대학교 정보보호학과 조교수
※관심분야 : 정보보호, 모바일 보안, 시스템 보안