https://doi.org/10.33778/kcsa.2019.19.5.019

무선 네트워크 환경에서 영역기반 침입탐지 기법에 관한 연구

양환석*

요 약

MANET은 이동 노드로만 구성되어 있기 때문에 기존의 유선 환경에서의 라우팅 프로토콜을 그대로 적용할 수 없다. 따라서 이러한 특성이 고려된 라우팅 프로토콜이 필요하다. 특히 라우팅 단계에서 악의적인 노드들을 배제하지 못한다면 네트워크 성능은 크게 떨어질 수 밖에 없다. 본 논문에서는 라우팅 성능을 향상시키기 위해 영역기반 침입탐지 기법을 제안하였다. 제안한 기법에서는 전체 네트워크를 일정한 영역으로 분할한 후 영역관리 노드를 이용하여 영역내 공격 탐지가 이루어지도록 하였으며, 멤버 노드로부터 수신한 완료 메시지를 이용하여 서로간 협업을 통해 경로상에 존재하는 공격 노드를 탐지할 수 있는 방법을 제안하였다. 그리고 탐지한 공격노드 정보를 블록체인에 저장하여 공유함으로써 네트워크에 참여하는 모든 노드들이 공격노드 정보를 공유할 수 있도록 하는 방법을 적용하였다. 제안한 기법의 성능 평가는 기존의 보안 라우팅 기법들과 비교 실험하였으며, 실험을 통해 제안한 기법의 우수한 성능을 확인할 수 있었다.

A Study on Zone-based Intrusion Detection in Wireless Network Environments

Hwanseok Yang*

ABSTRACT

It is impossible to apply the routing protocol in the wired environment because MANET consists of only mobile nodes. Therefore, routing protocols considered these characteristics are required. In particular, if malicious nodes are not excluded in the routing phase, network performance will be greatly reduced. In this paper, we propose intrusion detection technique based on region to improve routing performance. In the proposed technique, the whole network is divided into certain areas, and then attack detection within the area using area management node is performed. It is a proposed method that can detect attack nodes in the path through cooperation with each other by using completion message received from member nodes. It also applied a method that all nodes participating in the network can share the attack node information by storing the detected attack node and sharing. The performance evaluation of the proposed technique was compared with the existing security routing techniques through the experiments and the superior performance of the proposed technique was confirmed.

Key words : Intrusion Detection, Block chain, Region-based Architecture, Mobile Ad-hoc Network

접수일(2019년 12월 5일), 게재확정일(2019년 12월 26일)

* 중부대학교 정보보호학과

1. 서 론

이동 노드로만 네트워크를 구성하는 MANET은 최근 많은 분야에 응용되고 있으며, 중앙의 어떠한 통제도 없기 때문에 네트워크를 구성하는데 유연하다는 장점을 갖고 있다. 따라서 무선 전송 범위 내의 노드들끼리 hop-by-hop 방식으로 데이터 전송이 이루어지기 때문에 모든 노드가 라우터 역할을 수행해야 한다[1][2]. 하지만 노드들의 이동으로 인한 동적인 토폴로지와 무선 매체의 개방성으로 인해 많은 보안 취약점을 가지고 있다[3]. 만약 라우팅 과정에 악의적인 노드를 배제하지 못한다면 전송 데이터에 무결성을 보장하기 어렵고 네트워크 성능이 크게 떨어지거나, 네트워크가 마비될 수 있는 큰 피해를 입을 수도 있다[4].

본 논문에서는 공격노드들에 대한 효율적인 침입탐지를 위해 영역기반 침입탐지 기법과 공격노드 정보를 블록체인에 저장하여 공유할 수 있는 방법을 제안하였다. 제안한 기법은 공격노드 탐지 정확도를 높이기 위하여 영역을 기반으로 노드들 간의 협업을 통한 탐지가 이루어질 수 있는 방법을 제안하였다. 영역 기반 탐지는 전체 네트워크의 부하를 줄일 수 있었으며, 각 영역내 관리를 위해 영역관리 노드를 선출하였다. 영역관리 노드는 멤버 노드들로부터 수신한 완료 메시지를 이용하여 공격노드 탐지를 수행하였다. 그리고 노드들간 송수신 패킷 정보들에 대한 교환을 통해 공격노드들을 탐지하였다. 영역관리 노드들은 협업 탐지를 위해 영역정보 테이블을 관리하였다. 그리고 공격노드들의 정보를 블록에 저장하기 위해 관련 정보를 블록 헤더에 추가할 수 있는 구조를 적용하였다. 공격노드에 대한 정보를 블록체인에 저장하기 위해 트랜잭션 생성, 블록 패키징, 검증의 과정을 거치게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대하여 살펴보고 3장에서는 본 논문에서 제안한 영역기반 침입탐지 기법에 대해 기술하였다. 4장에서는 제안한 기법의 성능 평가를 위해 실험하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 보안요구 사항

노드들의 빈번한 이동으로 인해 동적인 토폴로지와 고정된 인프라 부재 그리고 무선 매체의 개방성이 갖는 보안 취약점 때문에 많은 보안 취약점을 가지고 있다[5]. 특히 다중 홉 방식에 의한 라우팅으로 인하여 중간노드에 의해 발생할 수 있는 라우팅 취약점은 심각한 문제를 야기할 수 있다. 이러한 MANET의 보안 요구사항들은 가용성, 기밀성, 무결성, 부인방지, 인증 등이다. 라우팅 프로토콜의 취약점을 이용한 공격은 크게 패킷을 도청 또는 감청을 통해 정보를 탈취해가는 passive 공격과 패킷의 주입이나 삭제 또는 변경을 통해 패킷 전송이 불가능하게하고, 네트워크 전체를 마비시킬 수 있는 active 공격이 있다[6].

2.2 침입탐지 기법

침입탐지 기법의 종류는 탐지 대상에 따라 네트워크 기반 공격 탐지와 호스트 기반 탐지로 나눌 수 있으며 탐지 방식에 따라 비정상 행위 탐지와 오용 탐지로 분류할 수 있다. MG(Mutual Guarding) 기법은 이웃 노드들이 송신하는 패킷들에 대한 오버히어링을 이용하여 공격을 탐지하는 기법이다[7]. 만약 이웃 노드로부터 오버히어링 한 패킷의 정보가 이웃 노드의 ID가 아니거나 자신의 ID인 경우 비정상 행위로 판단하게 된다. 즉, 센서 노드의 오버히어링 특성을 이용하여 이웃 노드를 관찰하여 비정상 행위를 탐지한다.

SRP(Secure Routing Protocol) 기법은 MG 기법의 단점을 보완하기 위해 제안된 기법으로서 수신된 패킷 수를 카운팅한 후 일정시간 후에 ACK에 수신된 패킷 수를 포함하여 다시 소스 노드에게 전송한다[8]. 만약 수신된 패킷의 수가 송신한 패킷의 수보다 많을 경우 소스 노드는 자신의 ID를 이용하여 패킷을 전송을 하는 공격 노드가 있는 것을 탐지하고 경고 메시지를 방송하게 된다. 하지만 이웃 노드들의 카운터는 고려하지 않기 때문에 이웃 노드들에 대한 공격 탐지가 어려운 단점이 있다[9].

3. 영역기반 침입탐지 기법

3.1 영역기반 침입탐지 구조

본 절에서는 라우팅 프로토콜의 취약점을 이용한 공격들에 대한 탐지 기법에 대하여 설명한다. 전체 네트워크를 일정한 크기의 영역으로 분할한 후 분할된 영역을 기반으로 한 침입탐지를 실시함으로써 네트워크의 부하를 줄이면서 효율적인 침입탐지를 수행할 수 있게 하였다. 각 영역에는 영역관리 노드를 지정하였고, 영역관리 노드는 영역내 모든 멤버 노드들에 대한 정보 수립 및 공격노드 탐지시 이들에 대한 정보를 트랜잭션으로 발생시켜 이를 블록체인에 저장하게 함으로써 공격노드들에 대한 정보를 공유할 수 있도록 함으로써 이들의 네트워크 참여를 배제시킬 수 있도록 하였다. 영역내 멤버 노드들은 경로 설정 후 패킷 송신을 완료했을 때나 수신을 완료했을 때 해당 정보를 영역관리 노드에게 전송한다. 영역관리 노드는 멤버 노드들로부터 수신한 정보를 영역정보 테이블(Zone Information table)에 저장하게 된다. (그림 1)은 본 논문에서 사용한 영역정보 테이블의 구조를 보여주고 있다.

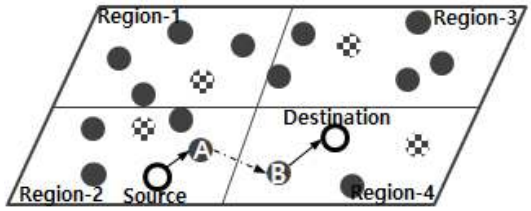
Zone ID	Node ID	Flag	Destination Node	Data Size(Kb)	Time
Z_1	N-2	R	N-7	1,430	13:11:20
Z_4	N-9	S	N-16	824	13:31:09
Z_2	N-1	R	N-2	4,570	12:58:36
Z_3	N-12	R	N-7	16,478	12:48:47

(그림 1) 영역정보 테이블 구조

본 논문에서는 라우팅 설정시 취약점 공격에 대비하기 위하여 다음과 같은 기법을 적용하였다. 노드들간 패킷 송신 또는 수신이 완료되었을 때 그 결과에 대해 영역관리 노드에게 완료 메시지를 전송한다. 완료 메시지의 내용은 영역정보 테이블에 포함되어 있는 내용에 전송 경로, 전송 시간이 포함되어 있다.

3.2 영역기반 침입탐지

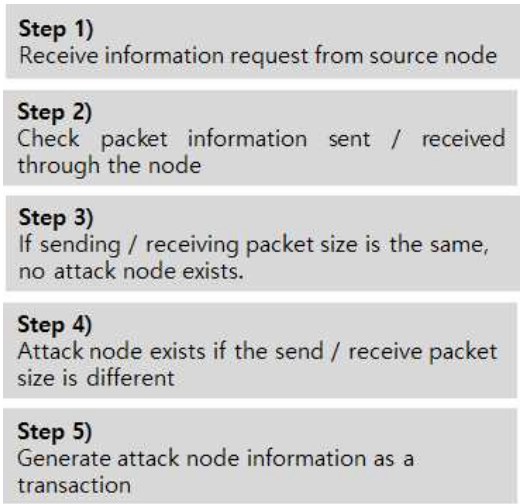
영역내 악의적인 공격노드를 탐지하기 위해서 데이터를 송수신하는 모든 노드들은 영역관리 노드에게 완료 메시지를 전송한다. 이 정보를 수신한 영역관리 노드는 단위 시간 간격으로 소스 노드에서 송신한 패킷의 양과 목적 노드에서 수신한 패킷의 편차를 계산하여 존 내의 평균값을 계산한다. 이 평균값을 기준으로 하여 각 노드들 사이의 편차가 영역내 평균값보다 큰 값을 갖는지 검사를 한다. 만약 평균값보다 큰 값을 갖는 노드가 탐지된다면, 해당 패킷이 전송되는 경로에 공격노드가 존재하는 것으로 판단하고, 완료 메시지내의 전송 경로 정보에 존재하는 중간 노드들에 대한 정보를 이웃 영역의 영역관리 노드에게 전송하여 중간 노드들에 대한 검사를 실시하여 공격노드를 탐지한다.



(그림 2) 라우팅 취약점에 의한 공격

(그림 2)에서 만약 공격 노드 A가 이웃 노드 B에 대한 잘못된 정보를 소스 노드에게 전달하고 노드 B는 노드 A가 의심스럽다는 정확한 정보를 목적 노드에게 전달하였을 때, 각 노드들이 이를 그대로 받아들인다면 두 개의 영역은 서로 단절되는 문제가 발생할 수 있게 된다. 따라서 이러한 문제를 차단하고 공격 노드를 정확하게 탐지하기 위해서는 멤버 노드로부터 수신한 정보를 그대로 받아들이지 않고, 소스 노드는 자신의 속한 영역관리 노드에게 정보 확인을 요청한다. 소스 노드로부터 요청을 수신한 영역관리 노드는 경로에 해당 노드가 포함되어 있는 경로를 이용하여 데이터를 송신하는 소스 노드의 송신 패킷 값과 목적 노드가 속해있는 영역의 영역관리 노드에게 소스 노드로부터 수신한 패킷 값을 비교하게 된다. 만약 두 개의

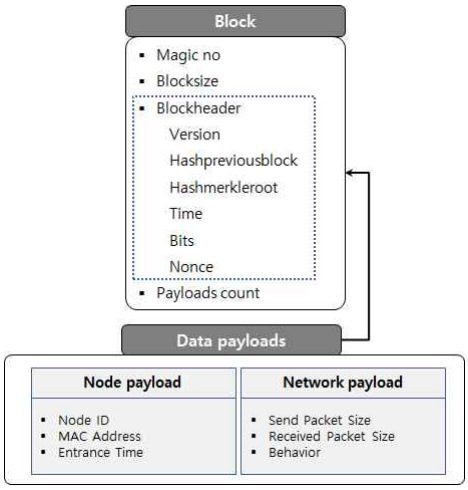
값이 같다면, 중간 노드들이 모든 패킷들을 정상적으로 포워딩 했다는 것을 의미한다. 따라서 소스 노드에게 해당 노드는 정상 노드임을 통보해주면 된다. 그러나 두 개의 값이 같이 않다면, 해당 노드를 의심스러운 노드로 판단하여, 소스 노드에게 이를 알리고 해당 노드에 대한 정보를 블록체인에 저장하기 위하여 트랜잭션을 생성하여 영역관리 노드에게 전달하면 된다. (그림 3)는 위에서 설명한 공격 노드 탐지 과정을 보여주고 있다.



(그림 3) 공격 노드 탐지 과정

3.3 블록체인 생성 및 교환

영역기반 침입탐지를 통해 발견된 공격노드들에 대한 정보를 네트워크 전역의 모든 노드에게 제공함으로써 공격 노드들의 네트워크 참여를 배제시키기 위해서 블록체인을 적용하는 방법에 대하여 기술한다. 본 논문에서는 공격 노드들의 정보를 블록체인에 저장하기 위해 새로운 블록체인을 설계하였다. 공격 노드의 정보를 저장하기 위해 블록헤더내 머클트리 루트 새로운 데이터 payload를 적용하였다. (그림 4)는 공격 노드 정보를 위한 데이터 payload를 적용한 블록헤더 구조를 보여주고 있다.



(그림 4) 공격 노드 정보를 적용한 블록헤더

공격노드 정보를 블록체인으로 생성하기 위한 과정은 크게 트랜잭션 생성, 블록 패키징, 검증 및 배포의 3 단계로 이루어진다. 트랜잭션 생성 단계는 영역관리 노드가 공격노드에 대한 탐지가 이루어지면 해당 노드에 대한 정보를 트랜잭션으로 생성한다. 각 영역관리 노드에서 생성된 트랜잭션은 영역관리 노드들 중에서 선출된 인증 노드에게 전달된다. 트랜잭션을 전달받은 인증 노드는 카프카 분산 메시징 방식을 이용하여 해당 트랜잭션을 순서대로 정렬한 후 최신 블록을 생성한다. 마지막 과정인 검증 및 배포 단계는 인증 노드가 생성한 최신 블록을 각 영역의 영역관리 노드들에게 전달하고, 최신 블록을 전달받은 영역관리는 해당 블록이 올바르게 생성되었는지 검증하기 위해 해당 블록을 자신의 영역내 노드들에게 배포해준다. 최신 블록에 포함된 결과값이 정상 여부 검사와 보증 정책 검증 작업을 수행한 후 자신의 로컬 저장소에 저장된 블록체인에 최신 블록을 추가하고 업데이트한다. 이러한 과정을 통해 블록을 생성 및 배포할 수 있게 된다.

4. 실험 및 결과

4.1 실험 환경

본 논문에서 제안한 영역기반 침입탐지 기법의

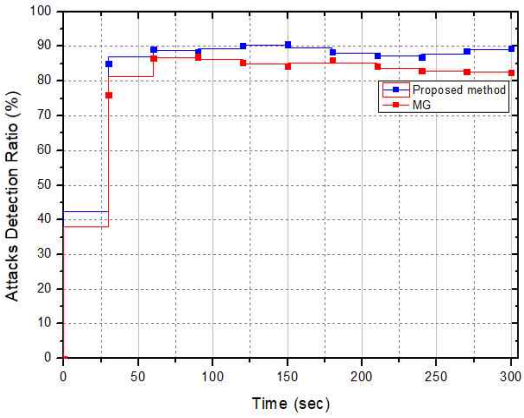
성능 평가를 위하여 NS-2 시뮬레이터를 이용하여 다음과 같은 환경에서 실험을 진행하였다. 먼저, 10개의 악의적인 노드가 패킷을 전달하지 않거나 폐기하도록 공격을 수행하였다. 실험시간은 300초로 하였으며, 노드들의 전력 소모는 고려하지 않았다. <표 1>은 실험에 사용한 환경변수를 보여주고 있다.

<표 1> 실험에 사용한 환경 변수

Parameter	Values
Number of Nodes	100개
Network Size	1500 × 1500
MAC Protocol	IEEE 802.11 DCF
Routing Protocol	AODV
Pause Time(sec)	20
Transmission range	100m

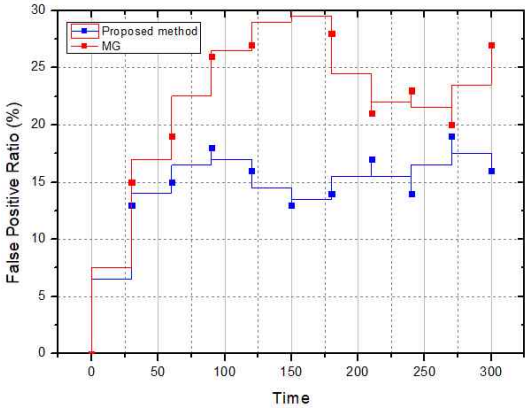
4.2 실험 결과 분석

이 절에서는 제안한 침입탐지 성능 측정을 위해 MG 기법과 비교실험 하였으며, 성능 평가 기준은 공격 탐지율, 오탐율, TPS(Transaction per Second)로 하였다.



(그림 5) 공격 탐지율 결과

<그림 5>에서는 공격탐지에 대한 측정 결과를 보여주고 있다. MG 기법은 노드들의 이동이 많아지게 되면서 이웃 노드들에 대한 패킷 오버히어링이 원활하게 이루어지지 못하여 탐지 성능이 다소 낮게 나타났다. 반면에 제안한 기법에서는 영역을 관리하는 영역관리 노드가 멤버 노드로부터 수신한 수신 완료 메시지의 원활한 교환 및 측정을 통해 정확한 공격 탐지가 이루어짐을 확인할 수 있었다. 특히 노드들의 이동에도 공격 탐지율은 큰 차이를 보이지 않았다.



(그림 6) 오탐율 측정 결과

<그림 6>에서는 정상 노드를 공격 노드로 잘못 탐지한 결과를 보여주고 있다. MG 기법은 노드들의 이동 속도가 빨라짐에 따라 오버히어링이 원활하게 이루어지지 않아 오탐율이 증가하는 결과를 보여주었으며, 제안한 기법은 영역 내부의 모든 노드들이 수신한 패킷 양의 편차와 각 멤버 노드에서 의심노드 판단을 위해 사용하는 기준값을 이용하기 때문에 좋은 성능을 보였다.

<표 2> 영역관리노드에서 생성한 트랜잭션

Time	0	60	120	180	210	270	300
TPS	0	6	9	7	8	11	9

<표 2>에서는 공격탐지가 이루어졌을 때 공격노드에 대한 정보를 네트워크의 모든 노드들과 공유하기 위해 영역관리 노드에서 트랜잭션을 생성한 후 합의를 통해 그 정보를 블록체인에 저장하기 위한 성능을 측정하는 것으로서 영역관리 노드에서 생성되는 트랜잭션 처리 성능(TPS)을 보여주고 있다.

5. 결 론

본 논문에서는 이동 노드로만 구성된 MANET

환경에서 영역기반 침입탐지 기법을 제안하였다. 제안한 기법에서는 침입탐지의 효율성을 높이고 부하를 줄이기 위하여 전체 네트워크를 일정한 영역으로 나눈 후 영역관리노드를 이용한 침입탐지를 제안 하였다. 침입탐지의 정확도를 향상시키기 위하여 멤버 노드들의 협력을 기반으로 한 탐지를 수행하였다. 이를 위해 영역내 모든 노드들이 수신한 패킷의 편차를 기준값으로 이용하였다. 이렇게 탐지된 공격 노드들에 네트워크 참여를 배제시키기 위해 공격노드들에 정보를 블록체인에 저장하여 이를 배포하는 기법을 적용하였다. 이를 위해 공격 노드의 정보를 저장하기 위해 블록헤더내 머클트리 루트에 2개의 새로운 데이터 payload를 적용하였다. 트랜잭션 생성은 영역관리노드에 의해 이루어지며, 블록 패키징, 검증 및 배포의 과정을 거치게 된다. 실험을 통해 본 논문에서 제안한 침입탐지 기법은 공격 탐지율과 오탐율 그리고 TPS의 우수한 성능을 확인할 수 있었다.

참고문헌

[1] Nishani, L., Biba, M., “Machine learning for intrusion detection in MANET,” a state-of-the-art survey. J Intell Inf Syst 46, pp. 391-407, 2016.

[2] Shurman M.AI, Yoo S.M., Park S., “ Black Hole Attack in Wireless Ad Hoc Networks.,” In: Proceedings of ACM 42nd Southeast Conference (ACMSE 04), pp. 96-97, Alabama (2004).

[3] Kim G, Han Y, Kim S., “A cooperative-sink-hole detection method for mobile ad hoc networks,” .AEU-Inter-national Journal of Electronics and Communications, ;64(5), pp. 390 - 397, 2010.

[4] Cho JH, Chen IR. Performance analysis of hierarchi-cal group key management in-tegrated with adaptiveintrusion detection in mobile ad hoc networks.Per-formance Evaluation, 68(1), pp. 58 - 75, 2011.

[5] Mechtri L, Tolba FD, Ghanemi S., “MASID: multi-agent system for intrusion detection in MANET.,” InProceedings of Ninth IEEE International Conferenceon Information Technology : New Generations(ITNG), Las Vegas, Nevada, USA, April 2012, pp. 65 - 70.

[6] Al-Roubaiey, A. Sheltami, T., Mahmoud, A., Shakshuki, E., Mouftah, H., “AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement,” Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, Vol. 3, No. 1, pp. 634-640, 2010.

[7] Mohanapriya M, Krishnamurthi I., “Modified DSR protocol for detection and removal of selective black hole attack in MANET.,” Computers & Electrical Engineering, 40(2), pp. 530 - 538, 2013.

[8] Kumar G, Kumar K., “An information theo-retic ap-proach for feature selection.,” Security and Communi-cation Networks, 5(2), pp. 178 - 185, 2013.

[9] Lin HC, Sun MK, Huang HW, Tseng CY, Lin HT., “A specification-based intrusion detection modelfor wireless ad hoc networks.,” In Proceedings of Third IEEE International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA), Kaohsiung, Taiwan, September, pp. 252 - 257, 2012.

〔저자소개〕

양 환 석 (Hwan-seok Yang)
1998년 2월 조선대학교 이학석사
2005년 2월 조선대학교 이학박사
2007년 3월 호원대학교 연구교수
2011년 9월 ~ 현재 중부대학교 정보보호학과 부교수
email : yanghs@joongbu.ac.kr