MANET에서 계층 구조를 이용한 공격 탐지율 향상 연구

양환석*

요약

최근 들어 무선 네트워크의 활용 범위가 빠르게 증가함에 따라 네트워크 보안의 대상이 넓어지고 위협의 수가 증가하고 있는 실정이다. 그리고 노드들의 이동으로 인한 동적인 토폴로지와 중앙 통제를 할 수 없는 MANET의 특성 때문에 기존의 보안 메커니즘이 그대로 적용될 수 없는 문제를 가지고 있다. 본 논문에서는 네트워크에 참여하는 전체 노드들을 중앙에서 관리하며, 분산적인 침입탐지를 수행하여 신뢰성을 향상시킬 수 있는 계층 구조 침입탐지기법을 제안하였다. 각 클러스터 헤드에서는 오용탐지를 수행하고, 게이트웨이 노드에서는 비정상행위 탐지를 수행하게 된다. 그리고 클러스터 헤드에서는 공격 노드의 위치를 탐지하기 위하여 RDHT, CMT 테이블을 관리하게 된다. 제안한 기법의 성능 평가를 위하여 ZBIDS, MCBIDS 기법과 비교실험을 하여 제안한 기법의 우수한 성능을 확인하였다.

A Study for Attack Detection Rate Improvement using Hierarchical Structure in MANET

Hwan-Seok Yang*

ABSTRACT

Recently, as the use range of wireless networks rapidly increase the target of network security become wider and the number of threat is increasing. Existing security mechanisms have problems which cannot be applied as it is because of dynamic topology by the movement of nodes and characteristic of MANET which cannot do the central control. In this paper, we proposed hierarchical structure intrusion detection technique that manages the whole nodes in the center and can improve reliability by performing distributed intrusion detection. The misuse detection is performed in each cluster head and anomaly detection is performed in the gateway. And RDHT, CMT is managed to detect the location of attack node in the cluster head. ZBIDS, MCBIDS technique with the proposed technique was compared to evaluate the performance of proposed technique and superior performance of the proposed technique was confirmed through the experiment.

Key Words : Intrusion Detection, Mobile Ad-hoc Network, Cluster Technique, CART Algorithm, Hierarchical Structure

* 중부대학교 정보보호학과 (✉ yanghs@joongbu.ac.kr)
· 제1저자(First Author) : 양환석 · 교신저자(Correspondent Author) : 양환석
· 접수일(2013년 7월 16일), 수정일(1차 : 2013년 7월 27일), 게재확정일(2013년 8월 8일)

Ⅰ. 서 론

지금까지 MANET(Mobile Ad-hoc Network)에 대한 연구는 다양한 분야에서 활발하게 진행되고 있다. 그 중에서 보안 분야에 대한 연구가 특히 활발히 진행되고 있다. 왜냐하면 어떠한 네트워크 장치의 도움 없이 이동 노드로만 구성되어 있기 때문에 중앙에서 네트워크 전체를 관리할 수 있는 구조가 아니기 때문이다. 또한 노드들의 이동으로 인한 동적인 네트워크 토폴로지와 대역폭 제약 그리고 이동 노드들의 제한된 자원 등의 특성이 공격 대상이 되기 때문이다[1-2]. 따라서 이러한 특성을 이용한 공격을 차단하기 위한 침입탐지시스템이 반드시 설치되어야만 한다. 그러나 기존의 유.무선 네트워크에서 사용하던 침입탐지시스템의 구조가 그대로 적용될 수가 없고, MANET의 특성에 맞게 수정되어야 한다[3].

본 논문에서는 노드들의 이동에도 공격에 대한 정확한 탐지가 이루어질 수 있는 계층형 분산 침입탐지 구조를 제안하였다. 제안한 기법은 MANET을 클러스터로 구성한 후, 각 클러스터를 관리하는 클러스터 헤드를 선출한다. 그리고 선출된 클러스터 헤드들 중에서 최상위 클러스터 헤드를 선출한다. 최상위 클러스터 헤드는 클러스터 헤드에서 오용 탐지를 위해 사용할 rule DB를 관리하고, 게이트웨이 노드에서는 CART(Classification and Regression Tree) 기법을 이용한 비정상행위 탐지가 이루어진다. 또한 각 클러스터 헤드에서는 침입탐지시 공격자의 위치 추적에 도움을 주기 위하여 RDHT(Received Data History Table)와 CMT(Cluster Member Table)을 관리하도록 하였다. .

본 논문의 구성은 다음과 같다. 2장에서는 침입탐지 시스템의 고려 요소와 기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 계층 구조를 이용한 침입탐지 기법에 대하여 기술하였다. 4장에서는 제안한 기법의 성능 평가를 위하여 ZBIDS, MCBIDS 기법과 비교 실험 하였으며 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 침입탐지 고려 요소

MANET은 기존의 유.무선 네트워크와는 다른 특징을 가지고 있기 때문에 침입탐지시스템을 구축하기 위해서는 이러한 특성들을 고려해야만 한다[4]. 먼저 비정상행위 탐지를 위해서는 정상 프로파일이 구축되어 있어야만 한다. 하지만 노드들의 이동으로 인하여 정상 프로파일 구축이 쉽지 않고 위상이 동적으로 변화하기 때문에 이에 대해 적절히 대처할 수 있어야 한다. 그리고 노드들이 사용할 수 있는 자원은 제한적이기 때문에 침입탐지시스템은 효율적인 자원의 사용을 고려해야 한다. 또한 침입탐지시스템이 설치되어야 할 위치가 고려되어야 한다. 이동 노드로만 구성되어 있는 MANET은 트래픽이 특정한 지점을 거치거나 집중되지 않는다. 따라서 네트워크내의 모든 트래픽을 감시하고 정확한 침입탐지를 위해서는 침입탐지시스템의 설치 위치도 중요하다고 할 수 있다[5].

2.2 기존의 침입탐지 기법

전체 네트워크를 중복되지 않는 영역(zone)으로 분할한 후 각 영역내의 데이터 수집과 영역들 간의 데이터 수집을 통해 침입탐지를 수행하는 ZBIDS(Zone Based IDS) 기법이 있다[6]. 이 기법에서는 각각의 노드들에서 IDS 에이전트가 실행하며, 각 IDS 에이전트에서는 침입탐지를 위한 데이터 수집, 로컬 탐지 그리고 전역탐지를 수행하게 된다. 각 IDS 에이전트에서는 공격 탐지를 위한 정보 수집을 주기적으로 실행하며, 정보의 유사성을 판단하여 침입경보를 생성한다. ZBIDS 기법은 전체 네트워크를 작은 영역으로 나누어

브로드캐스트로 인한 오버헤드를 감소시켜주는 장점을 가지고 있다[7].

다중 계층 클러스터 기반(Multi-layer Cluster Based IDS) 기법은 노드들에 의해 침입 데이터를 수집한 후, 수집한 데이터를 줄여 분석되어 클러스터 헤드에게 전달되는 기법이다[8]. 이 기법은 클러스터 헤드 모듈과 클러스터 멤버 모듈로 이루어져 있다. 클러스터 헤드 모듈은 클러스터 헤드에서만 실행되며 클러스터 멤버 노드들의 관리를 책임지며, 클러스터 멤버 모듈은 모든 노드에서 실행되고 멤버 노드들에 의해 지역적으로 수집된 데이터를 유지하며, 클러스터 헤드의 요청시 정보를 제공한다. 이 기법은 클러스터 헤드들 서로가 협력적 침입탐지를 수행할 수 있는 장점을 가지고 있다.

III. 제안한 기법

본 장에서는 계층 구조를 이용하여 네트워크의 모든 노드들에 대한 감시와 침입탐지 성능을 향상시킬 수 있는 기법에 대하여 기술한다.

3.1 네트워크의 계층 구조

MANET을 구성하는 모든 노드들에 대한 철저한 감시와 데이터 전송 정보의 관리를 용이하게 함으로써 침입탐지의 성능을 향상시킬 수 있는 계층 구조인 클러스터를 이용하였다. 네트워크를 구성하는 전체 노드들을 클러스터 형태로 구성한 후, 신뢰도 값을 기준으로 클러스터를 관리할 클러스터 헤드를 선출하게 된다. <그림 1>은 네트워크 계층 구조의 형태를 보여주고 있다.

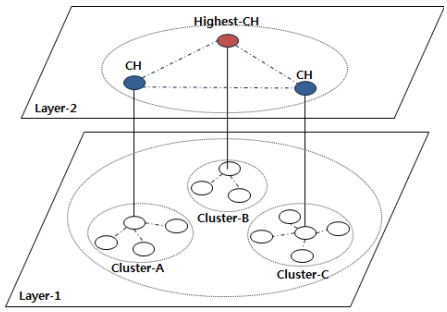

그림 1. 네트워크의 계층 구조
Fig. 1. Hierarchical Structure of Network

선출된 클러스터 헤드는 각 클러스터의 멤버 노드들에 대한 정보를 관리하기 위한 CMT와 공격 탐지시 공격자의 위치 추적에 도움을 줄 수 있는 RDHT를 관리한다. 그리고 선출된 클러스터 헤드들 중에서 링크 수와 신뢰도 값을 조합하여 최상위 클러스터 헤드를 선출한다. 최상의 클러스터 헤드는 침입탐지시스템에서 오용 탐지를 위해 사용할 rule DB를 관리하고, 최신 공격 정보에 대한 rule을 침입탐지시스템에게 전달해 준다.

3.2 테이블 관리

클러스터 관리를 위해 선출된 클러스터 헤드는 클러스터로 들어오고 나가는 멤버 노드들을 관리하기 위하여 CMT와 RDHT를 관리한다. <그림 2>는 CMT의 구조를 보여주고 있다.

Node-ID	In-Time	Out-Time	Trust-Value	Status
N-1	09:01:20	09:17:01	3	Mn
N-2	09:03:04	-	5	Gw
⋮	⋮	⋮	⋮	⋮

그림 2. CMT 구조
Fig. 2. CMT Structure

이 CMT에는 각 멤버 노드들이 클러스터에 들어오고 나간 시간 그리고 신뢰도 값 등의 정보가 저장되어

있다. 이 테이블에 저장된 멤버 노드들의 정보는 공격 발생시 해당 노드에 대한 정보 수집을 위해 사용된다.

침입탐지시스템에 의해 공격이 탐지되었을 때 이에 대한 적절한 대응도 매우 중요하다. 따라서 침입탐지시 공격 노드에 대한 정보를 수집하고, 추적하는데 도움을 주기 위하여 클러스터 헤드에서는 RDHT를 유지하게 된다. RDHT는 클러스터내의 멤버 노드들이 자신이 데이터 수신을 완료하였을 때, 그 정보를 클러스터 헤드에게 전송해준다. 패킷을 수신할 때마다 정보를 클러스터에게 저장하게 된다면 그 양이 방대하게 커져 클러스터 헤드에게 큰 오버헤드가 발생하게 된다. 따라서 데이터 수신이 완료되었을 때만 그 정보를 전달하게 하였다. 이 정보를 관리함으로써 해당 노드가 공격을 당했을 때, 어느 노드로부터 패킷을 수신하였는지 파악할 수 있으며, CMT에 저장된 값을 이용하여 어느 클러스터에 속해있는지 탐지해낼 수 있게 된다. 따라서 공격 노드를 네트워크에서 완전히 배제시킬 수 있게 된다. <그림 3>은 RDHT의 구조를 보여주고 있다.

Node-ID	Source-Node	Cluster-ID	Received-Time	Data Size
N-1	N-7	Cluster-C	09:12:30	84
N-4	N-24	Cluster-B	09:32:15	675
⋮	⋮	⋮	⋮	⋮

그림 3. RDHT 구조
Fig. 3. RDHT Structure

3.3 침입탐지

본 논문에서 제안한 계층 구조 침입탐지 기법에서는 두 단계의 침입탐지가 이루어진다. 먼저 클러스터 헤드에서는 최상위 클러스터 헤드로부터 수신한 rule DB를 이용하여 오용 탐지를 실시하게 된다. 만약 공격이 탐지되면 이웃 클러스터 헤드에게 공격 정보를 제공하고 이를 수신한 클러스터 헤드는 자신이 관리하는 두 개의 테이블을 이용하여 공격 노드를 추적하고, 이에 대응하게 된다. 그리고 클러스터 사이에 존재하면서 많은 패킷을 전달해주는 게이트웨이 노드에서 비정상행위를 탐지하게 된다. 먼저, 게이트웨이 노드에서는 수신한 패킷들에 대한 정확한 비정상행위 탐지를 위해 여러 개의 후보 트리를 생성한 후에 그 중에서 최적의 트리를 찾아내는 CART 알고리즘을 이용하였다. CART 알고리즘은 이산형 목표 변수인 경우 지니 지수(Gini index)를 이용하여 이진 분리를 수행하게 된다. 노드 t에서 지니 지수는 식 1과 같이 표현된다.

$$G(t) = \sum_{i=1}^{r} P(i)(i - P(i)) \quad (1)$$

여기서 r은 수신한 패킷의 정상과 비정상 구분을 나타내며, $P(i)$는 주어진 데이터 중 클래스 i에 분류될 확률을 의미한다.

위의 지니 지수를 가장 잘 감소시켜주는 예측 변수와 그 변수의 최적 분리를 자식 노드로의 선택은 식 2에 의해 계산된다.

$$\triangle G(t) = G(t) - p_R \cdot G(t_R) - p_L \cdot G(t_L) \quad (2)$$

여기서 p_R과 p_L은 노드 t에서 t_R과 t_L로 구분될 확률을 나타낸다.

이와 같은 방법으로 불순도가 가장 작은 자식노드를 형성하여 정확한 탐지가 이루지게 된다. 게이트웨이 노드에서 공격이 탐지되게 되면 자신의 클러스터 헤드에게 공격 정보를 전달하여 공격에 대한 대응을 하게 된다. <그림 4>는 본 논문에서 제안한 침입탐지 과정을 보여주고 있다.

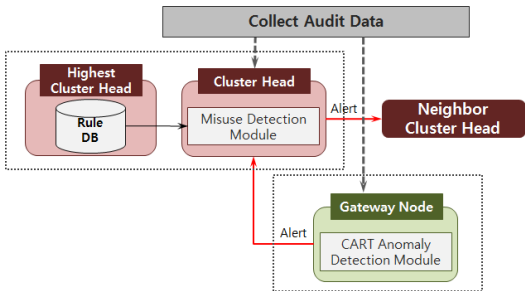

그림 4. 침입탐지 과정
Fig. 4. Intrusion Detection Process

Ⅳ. 모의실험 및 결과

4.1 모의실험 환경

본 논문에서 제안한 계층 구조 침입탐지시스템의 성능을 평가하기 위하여 ZBIDS 기법, MCBIDS 기법과 비교 실험하였다. 모의실험을 위해 ns-2 시뮬레이터를 이용하였고 실험에 사용한 환경 변수 값은 <표 1>과 같다. 그리고 본 논문에서는 각 노드들의 자원 소모에 대해서는 고려하지 않고 실험하였다.

표 1. 모의실험에 사용한 환경변수
Table 1. Simulation parameters

Parameter	Values
Network size	1000m × 1000m
Mobility model	Random waypoint
Number of nodes	100
Speed of Mobile node	0 ~ 10 m/s
Transmission range	200m
Bandwidth(MB)	2
Attacks	15
Pause time(Sec)	20

4.2 결과

본 논문에서 제안한 침입탐지 기법의 성능의 기준은 침입탐지의 중요한 요소인 공격 탐지율, 공격 노드 위치 탐지율, TPR(True Positive Rate)과 FPR(False Positive Rate)을 측정하였다. TPR과 FPR은 식 3과 식 4로 계산된다.

$$TPR = \frac{TP(True\ \ Positive)}{TP + FN(False\ \ Negative)} \quad (3)$$

$$FPR = \frac{FP(False\ \ Positive)}{FP + TN(True\ \ Negative)} \quad (4)$$

<그림 5>에서는 공격 탐지율의 결과를 보여주고 있다. 그림에서 나타나듯이 제안한 기법의 공격 탐지 성능이 노드들의 이동 속도에 큰 영향을 받지 않으면서 우수하게 나타났다. ZBIDS는 노드들의 이동이 많이짐에 따라 공격 노드에 대한 감시가 지속적으로 이루어지지 않아 공격 탐지율이 떨어졌다. MCBIDS 기법은 클러스터 헤드간의 협력적 침입탐지가 잘 이루어졌지만 지역적으로 수집된 정보가 전역적 침입탐지에 원활히 활용되지 못하여 노드들의 이동이 많아질수록 성능이 다소 떨어졌다. 하지만 제안한 기법에서는 각 클러스터내에 있는 클러스터 헤드와 게이트웨이 노드에서 침입탐지가 분산되어 수행되기 때문에 노드들의 이동에 크게 영향을 받지 않았다.

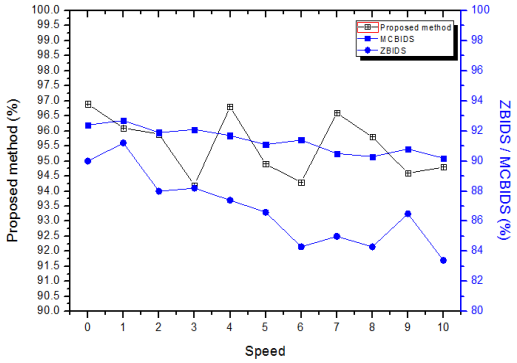

그림 5. 공격 탐지율
Fig. 5. Attack detection rate

<그림 6>은 제안한 기법과 ZBIDS, MCBIDS 기법의

TRP과 FPR을 측정한 결과를 보여주고 있다. ZBIDS는 노드들의 이동이 많아짐에 따라 zone의 이동이 빈번히 발생함에 따라 IDS agent들 간의 협업이 제대로 이루어지지 않아 오탐율이 증가 하였다. MCBIDS에서도 노드들의 이동이 증가할수록 지역적으로 수집된 감사 데이터들의 원활한 교환이 이루어지지 못해 오탐율이 증가하였다. 그러나 제안한 기법에서는 최상위 클러스터 헤드로부터 최신의 공격 rule을 이용한 침입탐지와 게이트웨이 노드들 간의 협력적 공격 탐지가 원활하게 이루어져 우수한 성능을 보여주었다.

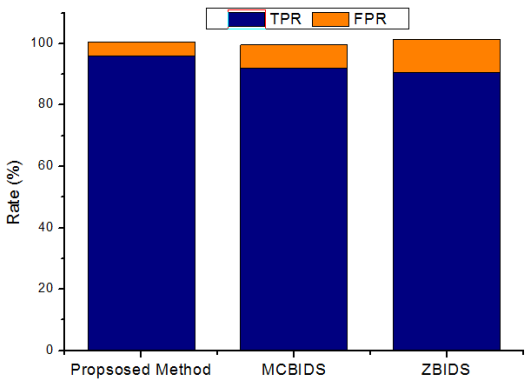

그림 6. TPR과 FPR 측정 결과
Fig. 6. Measurement results of TPR and FPR

<그림 7>은 공격이 탐지되었을 때 공격 노드의 위치를 정확히 알아내는 비율을 보여주고 있다. 클러스터 헤드에서 관리되는 두 개의 테이블 RDHT와 CMT에 의해 공격 노드가 공격 시도 후 이동을 하더라도 정확하게 위치를 탐지해낼 수 있었다. 특히 모든 멤버 노드들은 자신이 데이터 수신을 완료하게 되면 그 결과를 클러스터 헤드에게 전달하기 때문에 어느 노드에 의해 공격이 시도되었는지 정확히 알아낼 수 있으며, CMT 테이블에 의해 공격 노드가 현재 어느 위치에 있는지 쉽게 탐지할 수 있게 된다. 단, 공격 탐지시 공격 노드의 신분을 정확히 밝히는 것이 공격 위치 탐지의 중요한 요소가 된다.

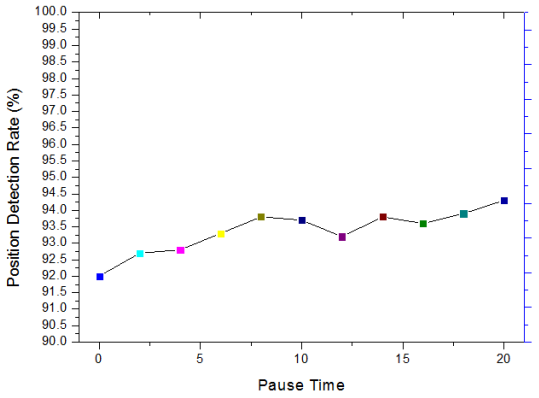

그림 7. 공격 노드 위치 탐지율
Fig. 7. Attack node position detection rate

V. 결 론

본 논문에서는 협력적 방법을 통한 침입탐지의 성능을 향상시키고, 네트워크의 신뢰성을 높이기 위하여 계층 구조 침입탐지기법을 제안하였다. 네트워크를 구성하는 노드들의 신뢰값을 기준으로 클러스터 헤드를 선출하고, 선출된 클러스터 헤드들 중에서 링크수와 신뢰값을 조합하여 최상위 클러스터 헤드를 선출한다. 최상위 클러스터 헤드는 오용탐지를 위한 최신 rule DB를 관리하고 각 클러스터 헤드에서 오용탐지를 수행하게 된다. 그리고 클러스터 사이에서 패킷을 전달해주는 게이트웨이 노드에서 CART 알고리즘을 이용한 비정상행위를 탐지하여 분산적이고 협력적인 방법으로 침입탐지를 수행하여 침입탐지 성능을 향상시킬 수 있었다. 또한 클러스터 헤드에서는 RDHT와 CMT 테이블을 이용하여 공격자의 위치를 정확하게 확인할 수 있었다. 제안한 계층 구조 침입탐지 기법의 성능은 실험을 통하여 확인할 수 있었다.

참고문헌

[1] Y.-C. Hu, A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security and Privacy Magazine*, Vol. 2, No. 3, pp.28-39, 2004.

[2] P. Albers, O. Camp, J-M. Percher, B. Jouga, M. Ludovic, and R. Puttini, "Sercurity in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," *Proc. of the First Interantional Workshop on Wireless Information Systems*, pp.1-12, 2002.

[3] Bhuvaneshwari K, A. Francis Saviour Devaraj, "Examination of impact of flooding attack on MANET and to accentuate on Performance degradation," *International Journal of Advanced Networking and Applications*, Vol. 4, Issue 04, pp.1652-1656, 2013.

[4] Denning D E, "An Intrusion Detection Model," *IEEE Transactions on Software Engineering*, Vol. 51, No. 8, pp.12-26, 2003.

[5] A. Agah, and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," *International Journal of Network Security*, Vol. 5, No. 2, pp.145-153, 2007.

[6] Sun B and Wu K, "Zone-based Intrusion Detection System for Mobile Ad Hoc Networks," International Journal of Ad Hoc and Sense Wireless Networks 2:3, 2006.

[7] S. Sen and J, A. Clark, "Intrusion Detection in Mobile Ad Hoc Networks," Guide to Wireless Ad Hoc Networks, Computer Communications and Networks, pp. 441-442, 2009.

[8] D. Sterne and R. Guha, "A General Cooperative Intrusion Detection Architecture form MANETs," *Proceedings 36th IEEE IWIA*, pp.57-70, 2005.

저자소개

양환석(Hwan-Seok Yang)

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

E-mail : yanghs@joongbu.ac.kr
2011년~현재 중부대학교 정보보호학과 조교수
※ 관심분야 : 정보보호, 모바일 보안, 시스템 보안