디지털산업정보학회 논문지 제10권 제4호-2014년 12월

프로파일 기반 다단계 공격 탐지 기법에 관한 연구

양 환 석*

A Study on Multi-level Attack Detection Technique based on Profile Table

Yang, Hwan Seok

〈Abstract〉

MANET has been applied to a wide variety of areas because it has advantages which can build a network quickly in a difficult situation to build a network. However, it is become a victim of malicious nodes because of characteristics such as mobility of nodes consisting MANET, limited resources, and the wireless network. Therefore, it is required to lightweight attack detection technique which can accurately detect attack without causing a large burden to the mobile node. In this paper, we propose a multistage attack detection techniques that attack detection takes place in routing phase and data transfer phase in order to increase the accuracy of attack detection. The proposed attack detection technique is composed of four modules at each stage in order to perform accurate attack detection. Flooding attack and packet discard or modify attacks is detected in the routing phase, and whether the attack by modification of data is detected in the data transfer phase. We assume that nodes have a public key and a private key in pairs in this paper.

Key Words : Attack Detection, Profile Table, Routing Protocol, MANET

Ⅰ. 서론

MANET(Mobile Ad Hoc Network)은 고정된 인프라스럭처 또는 중앙 집중 관리 없이 이동 노드로만 구성된 네트워크이다. 각각의 이동 노드들은 전송 범위내의 서로 다른 노드들과 통신하기 위하여 패킷을 송수신하는 라우터 역할을 수행해야한다. 그리고 노드들의 이동으로 인해 네트워크 토폴로지가 수시로 변화하기 때문에 경로 설정에 어려움이 있고, 이러한 특성으로 인한 보안 취약성이 매우 높다. 또한 이동 노드들의 전력, 메모리, 처리능력과 같은 자원이 제한적이기 때문에 이를 이용한 공격도 증가하고 있다[1-2]. MANET 환경에서의 특성을 이용한 수동적 공격인 도청부터 능동적 공격인 DoS 공격까지 다양한 공격이 존재한다. 수동 공격은 전송중인 패킷을 비인가된 노드가 도청 등을 시도하는 공격을 말하며, 능동 공격은 악의적인 노드가 정상적인 패킷의 흐름을 방해하는 것으로 네트워크 혼잡이나 노드들 간의 라우팅 충돌을 유발하는 공격이다. 따라서 MANET에

*중부대학교 정보보호학과 조교수

서는 제한된 자원을 이용하는 이동 노드들에 큰 부담을 주지 않으면서 정확한 공격을 탐지할 수 있는 경량화된 공격탐지 기법이 요구된다[3-4].

본 논문에서는 악의적인 노드에 의한 패킷 폐기 공격과 플러딩 공격의 효율적 탐지를 위한 프로파일 기반 다단계 공격 탐지 기법을 제안하였다. 본 논문에서 제안한 공격 탐지는 크게 경로 설정 단계와 데이터 전송 단계에서 이루어지며, 이를 위하여 Flooding Detection Module(FDM), Trust Measurement Moudle(TMM), Data Detection Module(DDM), Alert Module(AM) 4개의 모듈을 구성하였다. 경로설정 단계에서는 FDM과 TMM을 이용하여 플러딩 공격과 패킷 수정 또는 폐기 공격을 탐지하게 되며, 데이터 전송 단계에서는 DDM 모듈을 이용하여 암호화한 패킷의 유효성 검사를 실시한다. 노드가 암호화된 패킷을 수신하면 trust level 값을 1 증가시키고, 유효성에 문제가 없으면 1감소시키게 된다. 이렇게 수신하는 패킷에 대한 검사를 통해 trust level 값이 threshold 값을 초과하게 되면 악의적인 노드의 공격으로 탐지하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET의 보안 요구사항과 기존의 공격 탐지 기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 프로파일 기반 다단계 공격 탐지 기법에 대하여 설명하였다. 4장에서는 실험을 통해 제안한 기법의 성능평가를 수행하였고 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 MANET의 보안 요구사항

MANET에서는 이동 노드들의 빈번한 이동으로 인해 동적인 토폴로지와 인프라스트럭처의 부재 그리고 무선 네트워크의 보안 취약점 때문에 기존의 네트워크에 비해 많은 보안 취약점을 가지고 있다[5]. 특히 다중 홉 방식에 의한 라우팅으로 인하여 중간노드에 의해 발생할 수 있는 보안 취약점은 심각한 문제를 야기할 수 있다. 이러한 MANET의 보안 요구사항들은 가용성, 기밀성, 무결성, 부인방지, 인증 등이다.

- 가용성 : 공격자의 공격에 관계없이 서비스가 지속적으로 제공되는 것을 의미하며, 노드는 항상 통신이 가능해야 한다.
- 기밀성 : MANET에서는 경로 발견을 위한 제어 메시지(RREQ, RREP 등)나 인증을 위한 키 정보가 브로드캐스트되기 때문에 기밀성 유지가 기존의 다른 네트워크에 비해 매우 중요하다. 즉, 전송되는 패킷들을 중간노드나 신뢰할 수 없는 노드로부터 보호하는 것이 필요하다.
- 무결성 : 패킷의 전달 과정에서 악의적인 공격 노드들에 의해 패킷이 변경되어 오류가 발생할 수도 있기 때문에 패킷이 전송되는 동안 변경되지 않았다는 것으로 보장해야 한다.
- 부인방지 : 잘못된 패킷을 수신한 노드는 자신이 수신한 패킷과 함께 패킷을 송신한 노드가 부인할 수 없도록 고발하고, 이를 다른 노드들에게 방송할 수 있어야 한다.
- 인증 : 서로 통신을 하는 노드들에 대해 정확히 식별할 수 있도록 해주어야만 종단 노드들 간의 통신에 일관성을 보장할 수 있다. 그렇지 못하면 공격 노드가 많은 노드들의 자원 및 정보에 쉽게 접근할 수 있게 된다.

2.2 기존 공격 탐지 기법

MANET에서의 공격 탐지는 대상에 따라 네트워크 기반 공격 탐지와 호스트 기반 탐지로 나눌 수 있으며 탐지 방식에 따라 비정상 행위 탐지와 오용 탐지

로 분류할 수 있다[6]. 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. 하지만 공격 노드가 등방향성(isotropic)이 아닌 방향성(directional)의 안테나를 가지거나 짧은 전송범위를 가질 경우 MG 기법으로는 탐지가 어렵다. 또한 공격 노드가 주변에 공격 노드의 패킷을 오버히어링할 수 있는 이웃 노드가 없는 위치에 있을 경우에는 탐지를 할 수 없는 단점을 가지고 있다[8].

SRP(Secure Routing Protocol) 기법은 MG 기법의 단점을 보완하기 위해 제안된 기법으로서 소스 노드로부터 수신된 패킷의 수를 카운팅한 후 일정시간 후에 ACK에 수신된 패킷의 수를 포함하여 다시 소스 노드에게 전송한다. 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 SRP 기법은 통신을 하는 노드들 사이에서만 ACK를 통해서 패킷을 카운트 및 초기화하기 때문에 다른 이웃 노드들의 카운터는 고려하지 않기 때문에 이웃 노드들에 대한 공격 탐지가 어려운 단점이 있다[9].

Mobile Agent를 이용한 공격 탐지 기법은 네트워크를 이동하면서 일정 범위 내의 센서들의 정보를 수집한다. 그리고 mobile agent에서 센서들의 정보를 수집하여 센서들의 에너지와 네트워크 오버헤드를 줄일 수 있다. 이러한 특징을 이용하여 센서 노드들의 정보를 mobile agent에서 수집하여 공격 탐지 알고리즘을 수행하게 된다. 하지만 센서 노드들이 전송범위가 짧고 네트워크가 큰 경우에는 적용하기가 어렵다[10].

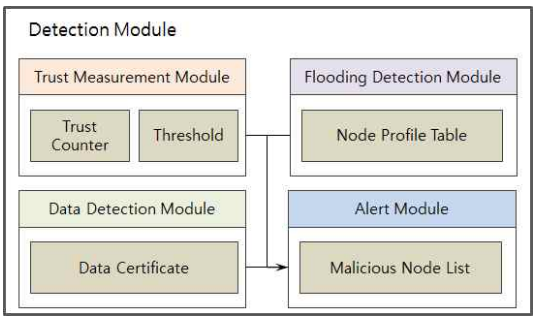
Ⅲ. 제안한 공격 탐지 기법

본 장에서는 MANET에서의 악의적인 노드들의 공격 탐지를 위한 프로파일 기반 공격 탐지 기법에 대하여 설명한다. 제안한 기법은 정확한 공격 탐지를 위하여 4개의 모듈로 구성하였다.

3.1 초기화

MANET에서 악의적인 노드들의 공격 형태는 매우 다양하지만 대부분은 패킷의 수정, 폐기 또는 대량 전송의 형태를 띠고 있다. 따라서 본 논문에서 제안한 공격탐지 알고리즘은 악의적인 노드들이 패킷을 폐기하거나 플러딩 공격과 같은 대량으로 패킷을 전송하는 공격을 탐지하기 위해 설계하였다. 이러한 목적을 달성하기 위해 제안한 공격 탐지 기법은 크게 Flooding Detection Module(FDM), Trust Measurement Moudle(TMM), Data Detection Module(DDM), Alert Module(AM)로 이루어져 있다. FDM은 플러딩 공격을 탐지하기 위한 모듈로서 노드 자신의 1-hop 이웃 노드들에 대한 정보를 유지하기 위한 프로파일 테이블을 관리하게 된다. 네트워크에 참여하는 모든 노드들은 초기화 단계에서 자신의 1-hop 이웃 노드들에 대한 정보를 프로파일 테이블에 저장하게 된다. 그리고 일정 시간동안 1-hop 이웃 노드들로부터 수신한 RREQ 패킷에 대한 정보를 저장하고, threshold table을 값과 비교하여 이를 초과하게 되면 플러딩 공격을 탐지하게 된다. TMM은 이웃 노드들의 신뢰도를 측정하기 위한 turst counter와 threshold table을 가지고 있으며, trust counter는 이웃 노드들이 수신한 제어 패킷을 이웃 노드에게 전달하는 검사하여 그 정보를 유지하는 테이블이고 threshold table은 클러스터 헤드로부터 수신한 RREQ 제어패킷과 신뢰도의 기준값을 저장하는 테이

블이다. 마지막으로 AM은 악의적인 노드 탐지시 클러스터 헤드에게 노드에 대한 정보를 전송하여 해당 노드를 네트워크에서 배제시키고, 악의적인 노드들에 대한 정보를 저장하는 블랙 리스트 테이블을 관리하고 있다. 본 논문에서 제안한 프로파일 기반 다단계 공격 탐지 구조는 <그림 1>에서 보여주고 있다.



<그림 1> 제안한 공격 탐지 구조

3.2 공격 탐지 방법

본 논문에서는 클러스터 구조를 이용하여 네트워크에 참여하는 노드들에 대한 신뢰를 평가한다. 클러스터를 형성한 후 선출된 클러스터 헤드 노드가 인증서 발급기관의 역할을 담당하게 된다. 클러스터 헤드 선출 방법은 노드들의 연결 수를 기준으로 선출하게 된다. 클러스터 헤드는 멤버 노드들에게 인증서를 발급해주고, 멤버 노드들은 인증서를 이용하여 데이터 전송을 하게 된다.

악의적인 노드들에 의한 공격은 경로설정 단계에서 공격과 데이터 전송 단계에서의 공격으로 나눌 수 있다. 이 단계에서는 FDM과 TMM 두 개의 모듈에서 경로설정 단계의 공격 탐지 과정과 DDM과 TMM에서 데이터 전송 단계의 공격 탐지 과정에 대하여 설명한다.

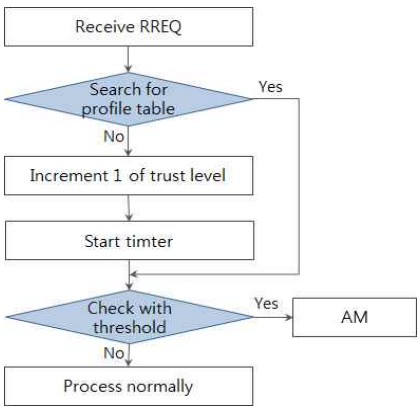
MANET에서 모든 노드들은 경로설정을 위하여 자신의 이웃 노드들에게 RREQ 패킷을 방송하게 된다. 각각의 노드에서는 RREQ 패킷을 수신하게 되면 해당 정보를 프로파일 테이블을 검색한다. 만약에 해당 노드에 대한 정보가 존재하지 않는다면 프로파일 테이블에 저장하고 TR(Timer of RREQ)를 초기화한 후 시작한다. 그리고 해당 RREQ 패킷에 대한 모니터링을 시작하게 된다. 만약 해당 RREQ 패킷의 정보가 프로파일 테이블에 존재하게 된다면 해당 패킷의 수신된 양이 threshold값을 넘었는지 TMM의 값과 비교 판단하게 된다. 만약 threshold값을 초과하게 된다면 해당 패킷은 악의적인 노드로 판단하여 해당 정보를 AM 모듈로 전달하게 된다. <그림 2>는 profile table의 구조를 보여주고 있다.

Node ID	Receive Time	Counter	Timer	Flag
D	09:10:12	12	12	M
A	09:14:54	0	5	N
...	...	...	...	...
F	09:19:23	-2	0	M

<그림 2> Profile Table 구조

경로설정 시 악의적인 노드들의 또 다른 공격유형은 패킷의 폐기 또는 수정을 하는 공격이 있다. TMM은 이러한 공격을 탐지하기 위하여 노드가 이웃 노드들로부터 RREQ 패킷을 수신하면, 해당 패킷에 대한 turst counter를 초기화한다. Trust level은 패킷을 수신하면 1을 증가시키고, 패킷을 전송하면 1을 감소하게 된다. 이 turst level 값이 높은 값을 갖게 되면 해당 노드는 패킷을 폐기시키는 악의적인 행동을 하는 노드로 판단할 수 있고, 음수 값을 갖게 되면, RREQ 패킷을 수정하여 전송하는 공격을 수행하는 것으로 판단할 수 있다. 만약 노드 A로부터 RREQ 패킷을 수신하게 된다면, 해당 노드에 대한 trust level값이 0으로 초기화 된 후에 값을 1 증가시킨다. 그리고 timer

를 시작시킨다. 만약에 수신한 패킷을 timer가 완료될 때까지 패킷을 전송하지 않으면 trust level값을 1 증가시킨다. 만약 그렇지 않다면 turst level을 1 감소시킨다. 그리고 마지막으로 trust level 값을 threshold 값과 비교하여 크다면 해당 노드를 악의적인 노드로 판단하고 노드 정보를 AM으로 전송하게 된다. Threshold값은 노드들의 이동으로 인한 제어 패킷의 전송이 정상적으로 이루어질 수 없는 경우도 발생하기 때문에 클러스터 헤드에서 클러스터의 제어 패킷의 양을 노드수로 나누어 주기적으로 계산이 이루어진다. <그림 3>은 TMM을 이용한 공격 탐지 과정을 보여주고 있다.



<그림 3> TMM 공격 탐지 과정

소스 노드와 목적 노드까지의 경로가 설정이 되면, 소스 노드는 목적 노드까지의 경로와 홉에 관한 모든 정보를 가지고 있다. 이 단계에서 노드가 데이터 패킷을 다음 홉에 전달할 때, 노드는 다음 홉으로부터 수신한 패킷의대한 인증을 수행한다. 이 인증은 노드가 데이터 패킷을 수정하지 않고 정확하게 전달했는지 검사하는 것이다. 만약 경로상에 있는 노드가 유효한 인증을 받을 수 없다면 해당 노드는 악의적인 노드로 탐지되며, 해당 노드의 정보를 AM 모듈로 전달하게 된다. 수신한 패킷의 유효성 검사는 다음과 같다.

노드가 자신의 이전 홉으로부터 데이터 패킷을 수신하면, 수신한 패킷의 인증이 이루어지고 이전 홉에게 전달한다. 만약 노드 A가 데이터 D를 노드 B에게 전달한다면 노드 A는 랜덤 값 r을 해시함수를 이용해 해시 값$H(r)$을 생성한다. 그리고 노드 A는 r과 데이터 D를 노드 B의 공개키 PN_B로 암호화한 $E_{PN_B}(r \| A)$를 생성한다. 노드 A는 $H(r)$와 $E_{PN_B}(r \| A)$를 노드 B에게 송신하게 된다. 노드 B는 수신된 $E_{PN_B}(r \| A)$를 개인키 PR_B로 복호화하여 r과 A를 복구한다. 그리고 노드 B는 복구한 r에 해시함수를 적용하여 $H(r)$를 계산하여 자신이 구한 해시함수 값과 노드 A가 보내준 $H(r)$값을 비교하여 인증을 하게 된다.

노드 B가 노드 A로부터 데이터 패킷을 수신하면 trust level을 1 증가시키고, timer를 시작시킨다. 그리고 노드 B는 노드 A로부터 수신한 데이터의 인증을 실시한 후 노드 A에 정보를 전송한다. 이와 같은 방법으로 수신한 데이터의 유효성을 검사하여 데이터의 유효성에 문제가 없다면 trust level값을 1씩 감소시키고, 그렇지 않다면 1씩 증가시키게 된다. 마지막으로 trust level값을 threshold값과 비교하여 공격 노드를 판단하게 된다.

위의 공격탐지 과정에서 악의적인 노드가 탐지되면 노드 정보를 AM 모듈로 전송하게 된다. AM 모듈에서는 노드 정보를 MNL(Malicious Node List)에 저장하고 클러스터 헤드에 전송하게 된다. 이를 수신한 클러스터 헤드들은 해당 노드에게 발급한 인증서를 폐기하고, 이웃 클러스터 헤드에게 정보를 전송하게 된다. 따라서 악의적인 노드들은 더 이상 네트워크에 참여하게 할 수 없게 된다.

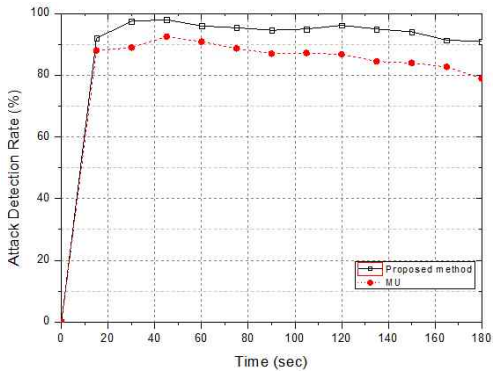
Ⅳ. 성능분석

4.1 실험 환경

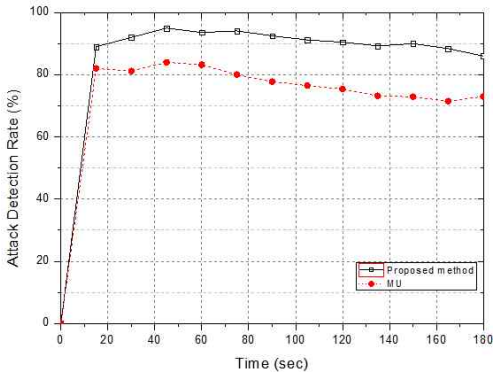
본 논문에서 제안한 프로파일 기반 다단계 공격 탐지 기법의 성능평가를 위하여 ns-2 시뮬레이터를 이용하였다. 그리고 악의적인 노드들은 일정 시간동안 패킷을 포워딩 하지 않거나 폐기하고, 플러딩 공격을 실행하였으며, 이를 위하여 AODV 프로토콜을 수정하였다. 실험에 사용한 환경변수 값은 <표 1>에서 보여주고 있다.

<표 2> 실험에 사용한 환경 변수

Parameter	Value
Network Size	1000 × 1000
Number of Nodes	100
Pause Time(Sec)	5
Traffic Model	CBR
Packet Size	512
Malicious Node	10



(a) 패킷 폐기 공격



(b) 플러딩 공격

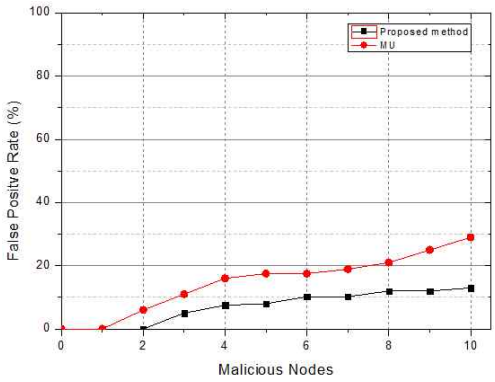
<그림 5> 공격 종류에 따른 공격 탐지율

4.2 실험 결과

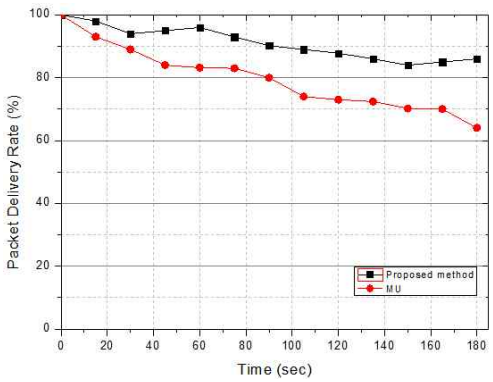
이 장에서는 제안한 공격 탐지 기법의 성능 측정 결과에 대하여 설명하며, 성능 측정은 MU 기법과 비교 실험하였다. 성능 측정을 위해 사용한 성능 평가 기준은 공격 탐지율, 공격 오탐율, 패킷 전달 비율로 설정하였다.

<그림 5>에서는 패킷을 포워딩 하지 않거나 폐기하는 공격과 플러딩 공격 탐지에 대한 측정 결과를 보여주고 있다. MU 기법은 패킷 폐기 같은 공격은 이웃 노드들에 대한 오버히어링을 통해 탐지가 이루어졌으나, 플러딩 공격에 대한 성능은 상당히 떨어지는 결과를 보여주었다. 반면에 제안한 기법은 노드가 RREQ 패킷을 수신하였을 때, 프로파일 테이블을 이용하여 해당 노드로 부터의 수신한 RREQ 패킷의 정보를 저장하고, TMM의 threshold value를 비교하여 공격을 탐지하기 때문에 우수한 성능보여주고 있다. 특히 노드들의 이동에도 공격 탐지율은 큰 차이를 보이지 않았다.

<그림 6>에서는 정상 노드를 공격 노드로 잘못 탐지한 결과를 보여주고 있다. MU 기법은 노드들의 이동 속도가 빨라져 오버히어링이 정상적으로 이루어지지 않는 경우 제대로 공격 탐지가 제대로 되지 않아, 노드들의 이동 속도가 빨라질수록 오탐율이 증가하는 결과를 보여주었으며, 제안한 기법은 악의적인 노드들로부터 수신한 패킷들에 대한 trust count가 이



<그림 6> 공격 오탐율 비교



<그림 7> 패킷 전달 비율 측정 결과

루어지기 때문에 오탐률이 낮은 결과를 보여주었다. 다만, 노드들의 이동으로 인해 일정시간이 초과되는 경우 해당 노드에 대한 정보가 프로파일 테이블에서 초기화가 되어 탐지율이 다소 떨어지는 결과를 보였다.

<그림 7>은 소스 노드에서 전달한 전체 패킷들 중에 목적 노드가 수신한 패킷의 양을 측정한 결과를 보여주고 있다. 이 성능 기준은 공격 탐지율과 비례하며, 악의적인 노드를 탐지하여 네트워크에서 배제가 잘 이루어져야 패킷 전달 비율이 높게 나타난다. MU 기법은 노드들의 이동이 많지 않은 경우에는 패킷 전달 비율이 높았지만 노드들의 이동이 빨라질수록 패킷 전달 비율이 낮은 결과를 보여주었다. 제안한 기법은 실험시간 동안 약 85% 이상의 패킷 전달 비율을 보여주는 것으로 측정되었다.

Ⅴ. 결론

MANET에서 공격 탐지는 다른 네트워크에 비해 그 중요성이 매우 높다. 왜냐하면 MANET은 이동 노드로만 구성되어 있고, 중앙 집중 관리가 이루어지고 있지 않기 때문에, 전체 네트워크를 마비시킬 수 있는 라우팅 공격이 발생하게 된다면 그 피해는 엄청나게 클 수밖에 없다. 따라서 본 논문에서는 공격 탐지의 성능을 향상시키기 위하여 다단계 공격 탐지 기법을 제안하였다. MANET을 구성하는 이동 노드들은 데이터 전송을 하기 위해서는 제어 패킷을 이용하여 경로 설정을 수행한 후, 경로가 확립되면 데이터 전송을 수행하게 된다. 따라서 제안한 공격 탐지 기법은 경로 설정 단계에서의 플러딩 공격과 패킷 수정 및 폐기 공격의 탐지가 이루어지고, 데이터 전송 단계에서 데이터 변조 공격을 탐지하게 된다. 플러딩 공격과 패킷 수정 및 폐기 공격의 탐지를 위해 FDM과 TMM을 이용하였다. 즉, 각 이웃 노드들에 대한 프로파일 테이블과 trust counter를 이용하여 수신한 제어 패킷에 대한 공격 여부를 판단함으로서 라우팅 공격에 대한 탐지의 성능을 높일 수가 있었다. 그리고 데이터 변조 공격의 탐지를 위해서 노드가 암호화가 된 패킷을 수신하였을 때 trust counter 값을 1 증가시키고, 해당 패킷에 대한 유효성 검사 실시에서 이상이 없는 경우에 trust counter 값을 1 감소시킨다. 이와 같은 과정을 반복함으로써 노드가 수신한 패킷에 대한 변조 여부를 탐지하게 됨으로써 공격 탐지의

성능을 높일 수 있다. 본 논문에서는 제안한 공격 탐지 기법을 성능을 평가하기 위하여 MU기법과 비교 실험하여, 우수한 성능을 확인하였다.

참고문헌

[1] Zhou, L. and Haas, Z. J., "Securing ad hoc networks," IEEE Network, 2008, Vol. 13, Issue 6, pp. 24-30.

[2] A. Agah, S. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks : A non-cooperative game approach," in 3rd IEEE International Symposium on Network Computing andApplications, (NCA 2004), Boston, MA, August 2004, pp. 343-346.

[3] 신대철, 김홍윤, "침입탐지 알고리즘 성능 최적화 및 평가 방법론 개발," 디지털산업정보학회지, 제8권, 제1호, 2012, pp. 125-137.

[4] A. Hasswa, M. Zulker, and H. Hassanein, "Routeguard: an intrusion detection and response system for mobile ad hoc networks," Wireless And Mobile Computing, Networking And Communication, 2005, Vol. 3, pp. 336-343.

[5] V. Bhuse, A. Gupta, "Anomaly intrusion detection in wireless sensor network," Journal of High Speed Networks, 2006, Vol. 15, Issue 1, pp. 33-51.

[6] Shakshuki, E., Kang, N., Sheltami, T., "EAACK - A Secure Intrusion Detection System for MANETs," IEEE Transactions on Industrial Electronics, 2013, Vol. 60, No. 1, pp. 1089-1098.

[7] 최희식, 박재표, 전문석, "SIP 플러딩 탐지 차단 실험방법에 대한 연구," 디지털산업정보학회지, 제7권, 제2호, 2011, pp. 39-46.

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

[9] Chong Eik Loo, Mun Yong Ng, Christopher Leckie, Marimuthu Palaniswami. Intrusion Detection for Routing Attacks in Sensor Networks, International Journal of Distributed Sensor Networks, 2006, Vol. 2, Issue 4, pp. 313 -332.

[10] 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, 2010, Vol. 3, No. 1, pp. 634-640.

■ 저자소개 ■

양 환 석
Yang, Hwan Seok

2011년 9월~현재
중부대학교 정보보호학과 조교수
2005년 2월 조선대학교 전산통계학과(이학박사)
1998년 2월 조선대학교 전산통계학과(이학석사)
1996년 2월 호원대학교 전산계산학과(이학사)

관심분야 : 정보보호, 침입탐지시스템, MANET
E-mail : yanghs@joongbu.ac.kr

논문접수일: 2014년 11월 2일

게재확정일: 2014년 11월 17일