Journal of Digital Contents Society Vol. 9 No. 1 March. 2008(pp. 33-39)

Mobile Ad Hoc Network에서 시스템 보안 기법에 관한 연구

양환석*

요 약

Ad Hoc Network는 인프라스트럭처 기반의 네트워크가 아니고 노드들이 분포되어 있기 때문에 공격을 받기가 쉽다. 침입탐지시스템은 다른 노드들의 신뢰 수준을 감지하고 노드의 로컬 보안에 대한 검사와 감시 능력을 제공한다. 본 논문에서는 침입 탐지를 하는데 오버헤드를 줄이기 위해 클러스터링 기법을 적용하였다. 그리고 노드들 간의 신뢰도를 측정하기 위해 클러스터 헤드가 멤버 노드로부터 받은 신뢰 정보와 자신의 정보를 조합하여 다른 노드의 신뢰도를 평가한다. 이렇게 함으로써 네트워크내의 노드들의 대한 인증을 정확하게 수행할 수 있게 되어 안전한 데이터 전송을 제공하게 된다.

The Study of System Security Technique for Mobile Ad Hoc Network

Hwan-Seok Yang*

Abstract

Mobile Ad Hoc Network is easy to be attacked because nodes are distributed not network based infrastructure. Intrusion detection system perceives the trust values of neighboring nodes and receives inspection on local security of nodes and observation ability. This study applied clustering mechanism to reduce overhead in intrusion detection. And, in order to measure the trust values, it associates the trust information cluster head received from member nodes with its own value and evaluates the trust of neighboring nodes. Secure data transmission is received by proposed concept because the trust of nodes on network is achieved accurately.

Keywords : System Security, Intrusion Detection System, MANET(Mobile Ad Hoc Network)

1. 서론

Mobile Ad Hoc Network(MANET)는 고정된 기반 망 없이 이동 노드들로만 구성된 네트워크로서, 제한된 무선 채널을 통해 이동 노드간의 통신을 수행하는 다중 홉 무선 네트워크이다. 공중전파를 사용하는 무선통신의 고유의 속성, 고정된 인프라가 없다는 점, 그리고 노드들의 이동으로 인한 네트워크 토폴로지가 수시로 변화하는 특성 때문에 많은 보안상의 문제점을 야기시킨다. 그러므로 Mobile Ad Hoc Network에서 이러한 문제점에 대해 안전한 통신을 보장하기 위해서 기밀성, 인증, 무결성, 부인봉쇄 그리고 가용성과 같은 보안 서비스를 제공하여야 한다. 보안 시스템의 구축에 있어서 가장 핵심이 되는 부분은 침입탐지시스템과 안전한 인증 서비스를 제공하는 것이라 볼 수 있다. 전형적인 보안 모델을 가지고는 최근에 만들어진 새로운 유형의 위협들에 대한 방어가 쉽지 않다. 이러한 새로운 위협들에 대하여 방어하기 위해 신뢰 평가를 기초로 한 새로운 보안 구조들이 제안되었다. 이러한 보안 구조에서는 각 노드들이 자신과 통신하는 이웃 노드들의 신뢰를 평가한다. 노드들에 대한 신뢰 평가는 자신의 경험에 의해 이루어진다. 이렇게 평가된 신뢰를 기초로 보안 측정이나 보안 결정이 만들어진다. 이와 같은 신뢰 평가 구조에서는 통신이 거의 없는 노드에 대한 정확한 신뢰 평가를 수행하기가 상당히 어렵다. 게다가 이웃 노드들에 대한 신뢰도를 저장하기 위해서는 많은 양의 메모리가 요구된다.

※ 제일저자(First Author) : 양환석
접수일자:2008년01월31일, 심사완료:2008년02월20일
* 호원대학교
badhack@howon.ac.kr

본 논문에서는 클러스터를 기반으로 인증 기법과 침입탐지 기법을 제안하였다. Mobile Ad Hoc Network를 자신과 1-hop 거리에 있는 이웃 노드들을 기초로 클러스터를 형성한 후 클러스터 멤버 노드들에 의해 선출된 클러스터 헤드는 멤버 노드들의 신뢰 보증인과 같은 인증서 발급기관의 역할을 수행한다. 본 논문에서 각 노드들의 신뢰 평가 구조는 클러스터 헤드에 의해 제공되는 정보와 자신의 경험을 조합하여 이루어진다. 만약 특정 노드에 대한 자신의 경험이 전혀 없을지라도 클러스터 헤드에 의해 제공된 신뢰 정보를 이용하여 다른 노드를 평가할 수 있다. 즉 노드가 네트워크에 존재하는 모든 노드들에 대한 정보를 저장하고 유지할 필요가 없게 된다. 그리고 클러스터 헤드는 클러스터 내의 모든 패킷의 기록을 저장하고 패킷을 분석하여 많은 공격을 탐지할 수 있게 해준다. 그리고 클러스터 헤드와 멤버 노드가 패킷 분석을 나누어 함으로써 각 노드의 계산량을 줄이고 메모리의 오버헤드를 감소시킨다.

본 논문의 구성은 다음과 같다. 2장에서는 Mobile Ad Hoc Network에서 존재하는 공격 유형과 침입 탐지 기법에 대한 관련 연구를 살펴보고, 3장에서는 본 논문에서 제안한 방법에 대하여 설명하였다. 4장에서는 제안 방법의 성능을 평가하고 마지막으로 5장에서는 결론을 맺는다.

2. 관련연구

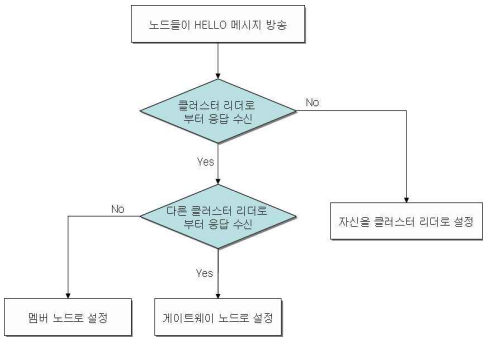
Mobile Ad Hoc Network의 특성 때문에서 도청이 쉽게 이루어 질 수 있다. 그리고 단말의 이동에 따른 보안 체계의 복잡성으로 공격은 다양하게 발생될 수 있다. Mobile Ad hoc Network 환경에서의 공격 유형은 크게 외부 공격과 내부 공격으로 나눌 수 있다 외부 공격은 비 인가된 노드들로부터 전송중인 데이터 패킷들에 대한 도청이나 정상적인 통신의 메시지 전송 흐름을 방해하는 것을 말한다. 이러한 공격의 목적은 네트워크의 혼잡과 노드들 간의 라우팅 충돌을 유발시키려는데 있다. 이에 대한 보안상의 해결책은 노드들 간의 상호 인증과 메시지 인증 코드를 이용한 전송 메시지에 대한 무결성을 보장해 주는 기법들이 있다. 내부 공격은 공격당한 이동 노드들로부터 이루어지는 공격을 말한다. 이와 같은 상황은 방어가 훨씬 더 어려워진다. 공격행위를 하는 노드는 자신의 합법적인 인증마저도 제공해 줄 수 있기 때문에 그에 대한 방어는 침입 탐지 시스템을 이용해서 악의적인 노드를 Mobile Ad Hoc Network 환경에서 배제 시키거나 경로의 중복성을 이용해서 공격행위를 회피하는 등 소수의 기법만 제기되고 있다. Ad Hoc Network에서 mobile agent를 이용한 침입 탐지 기법이 제안되었다. 이 기법은 mobile agent가 네트워크내의 침임 탐지를 하고 침입 정보를 네트워크 전체에 플러딩하는 구조를 가지고 있다. 따라서 각각의 노드들은 이 정보를 처리하고 저장해야하기 때문에 모든 노드들에게 많은 오버헤드를 발생시킨다. 그리고 노드들 간의 안전한 데이터 전송을 보장하기 위해서 Detecting Misbehaving Node가 제안되었다. 이 방법은 비정상행위를 하는 노드들을 탐지하고 이러한 노드들의 행위를 반영하는 매트릭스를 유지한다. 이 보안 기법에서는 노드들이 혼잡모드에서 다른 노드들의 행위가 정상인지를 판단하고 만약 비정상적인 행위에 대한 판단이 내려지면 해당 노드에 대한 등급을 낮춘다. 즉 매트릭스에 기록된 노드들의 등급이 높을수록 해동 노드들을 이용해서 라우터를 설정하는 것이 데이터 전송에 있어서 안전하다고 판단하는 것이다. 그러나 이 방법의 문제점은 악의적인 노드들의 협동 공격이 발생하였을 경우 이러한 노드들을 찾아내기가 어렵다는 것이다.

3. 제안한 방법

3.1 클러스터 형성

본 논문에서 클러스터는 자신과 1-hop 거리에 있는 이웃 노드들을 기초로 형성된다. 이렇게 형성된 클러스터 내에서 신뢰도 값과 연결수 값을 조합하여 가장 높은 값을 갖는 노드가 클러스터 헤드(CH)가된다. 여기서 신뢰도 값이란 이웃 노드가 자신의 패킷을 성공적으로 전달해 준 비율을 의미한다. 만약 이렇게 선택된 클러스터 헤드가 이미 다른 클러스터의 멤버라면 두 번째로 높은 값을 갖는 노드를 클러스터 헤드로 선택된다. 클러스터 헤드가 선출되면, 인접해있는 클러

스터들과 통신을 유지해 주는 게이트웨이 노드, 그리고 멤버 노드가 설정된다. (그림 1)은 앞에서 설명한 클러스터 형성을 위한 노드들의 초기화 과정을 보여주고 있다.



(그림 1) 노드들의 초기화 과정

클러스터가 형성되면 클러스터 헤드는 멤버 노드들에 대해 보증인의 역할을 담당하게 된다. 즉, 멤버 노드들은 클러스터 헤드에게 자신의 인증서를 요구하게 된다. 멤버 노드들은 이 인증서를 이용하여 다른 노드들과 통신을 수행할 수 있게 된다.

3.2 노드간의 인증 기법

클러스터 헤드는 클러스터내의 모든 노드들에 대해서 인증서를 발급해준다. 게이트웨이 노드 A에 대해서 다음과 같은 정의되는 인증서를 발급해준다.

GwCert := { Node(A), Trust_Value,
PubKey(CH), Validity(t), Status("Gw"),
Sign(CH'id, Create time) }

여기서, 신뢰도 값은 CH가 멤버 노드들로부터 노드 A에 대한 패킷 전달 비율에 대한 정보를 수집한 값이 된다. Validity(t)는 유효 기간으로서 유효 기간이 지나면, 노드는 클러스터 헤드에서 새로운 인증서를 요구하게 된다. 멤버 노드도 같은 형식의 인증서를 발급받게 된다. 멤버 노드의 인증서는 다음과 같이 정의한다.

MnCert := { Node(B), Trust_Value,
PubKey(CH), Validity(t), Status("Mn"),
Sign(CH'id, Create time) }

3.3 노드의 이동

새로운 노드가 클러스터 안으로 들어오는 경우는 두 가지 경우가 있다. 첫 번째 하나의 클러스터에서 다른 클러스터로 이동하는 경우와 두 번째로 처음으로 네트워크에 진입하는 경우이다. 첫 번째 경우에 새롭게 클러스터에 들어온 노드는 자신이 이전 클러스터 헤드로부터 받았던 인증서를 현재 클러스터 헤드에게 전달한다. 이 인증서를 가지고 현재 클러스터 헤드로부터 인증을 받고 새로운 멤버 노드의 초기 신뢰도 값을 확립한다. 두 번째 경우에 클러스터 헤드는 노드에 대한 신뢰도 값을 구하기 위해 정보를 모은다.

하나의 클러스터로부터 이동하는 노드는 자신의 클러스터 헤드에게 Out 메시지를 송신하면 된다. 이 메시지를 수신한 후에 클러스터 헤드는 노드에 관한 정보를 삭제하면 된다.

OutMsg := { Node(N), PubKey(CH),
Validity(t), "Out" }

3.4 침입탐지 시스템

침입탐지시스템은 컴퓨터 혹은 네트워크에 침입 시도를 탐지하는데 사용된다. Mobile Ad Hoc Network는 중앙 집중화된 관리나 표준화된 지원 서비스의 도움 없이 무선 이동 노드들로만 구성되어있기 때문에 분산된 방식의 침입탐지시스템을 사용해야만 한다.

제안된 클러스터링 알고리즘은 네트워크에 들어오는 모든 트래픽을 클러스터 헤드와 멤버 노드 나누어 분석한다. 이 방식은 각 노드들의 계산량을 줄이고 메모리의 오버헤드를 감소시킨다. 만약 클러스터 헤드에 의해 어떤 의심스러운 해동이 탐지되면 클러스터 헤드는 멤버 노드와 게이트웨이 노드를 통해 이웃 클러스터에게 이러한 행동을 통보하게 된다. (그림 2)는 본 논문에서 제안한 침입탐지 단계를 보여주고 있다.

(그림 2) 침입탐지 단계

그림에서 첫 번째 학습단계에서 수집된 정보는 정상적인 트래픽에 대한 threshold 값을 파악하기 위하여 침입정보 단계로 전달된다. 다음 단계에서는 threshold 값이 침입활동 검사에 이용된다. 만약 비정상적인 행동이 탐지되면 침입정보 전달 단계에서 다른 노드들에게 이를 통보하게 된다.

클러스터 헤드는 클러스터 내에서 전송되는 모든 패킷의 기록을 남긴다. 여기에는 송신, 순신, 전달된 패킷의 수와 정보를 담고 있으며 이러한 패킷은 데이터 패킷 또는 제어 패킷일 수도 있다. 제어 패킷은 AODV의 RREQ, RREP, RERR과 HELLO들이다. 이러한 로그는 blackhole, wormhole, sleep deprivation, 의심스러운 플러딩과 같은 많은 공격을 탐지할 수 있게 해준다. 멤버 노드와 게이트 노드들은 추가 또는 삭제된 경로의 수와 같은 자세한 경로 정보를 갖고 있다. 이러한 정보는 DoS와 같은 공격을 검출하는데 이용된다.

만약 오용행위 서명 기법을 사용한다면 모든 노드들은 학습 처리를 포함한 침입탐지 베이스와 같은 데이터베이스를 유지해야만 한다. 침입을 야기하는 모든 서명은 데이터베이스에 유지되어야만 한다. 비정상행위 탐지 기법은 비정상적인 행동에 대한 잘 정의된 적절한 threshold 값을 가지고 있어야만 한다. 효율적인 검출 처리는 오용행위 서명 또는 비정상행위에 대해 사용되어진다. 서명 데이터베이스나 비정상행위의 값은 수동 또는 다른 네트워크의 노드들로부터 업데이트될 수 있다. 이전 단계의 threshold 값은 비정상행위에 대한 정확한 threshold 값을 예측하기 위해 사용된다. 이 값은 Mean and Standard Deviation Model을 이용하였다.

노드들이 학습되었을 때 정상적인 행동의 트래픽 패턴을 분석하고 비교함으로써 침입을 탐지할 수 있다. 클러스터 헤드는 트래픽을 캡처하고 정상적 트래픽 행동과 비교한다. 만약 데이터에서 비정상행위가 탐지되면 클러스터 헤드는 멤버노드와 이웃 클러스터에게 이 정보를 알리고 감시 수준은 높인다. 그리고 공격의 유형과 공격자를 확인하기 위해 보다 자세하게 패킷을 분석한다. 만약 침입자가 같은 클러스터내에 속하지 않았다면 클러스터 헤드는 이웃 클러스터 헤드에게 침입자의 정보를 전달하게 된다.

어떤 침입에 대한 탐지는 크게 세 가지 경우로 나눌 수 있다. 첫 번째 멤버 노드가 침입을 탐지하는 경우 두 번째는 클러스터 헤드가 탐지하는 경우 세 번째는 이웃 클러스터에게 탐지 정보를 받는 경우이다. 첫 번째 멤버 노드가 침입을 탐지하는 경우에는 클러스터 헤드에게 이 정보를 알리고 이 정보를 받은 클러스터 헤드는 침입 활동에 대해 좀 더 자세히 패킷을 분석하여 다른 노드들에게 정보를 제공한다. 나머지 두 가지 경우에는 클러스터 헤드가 게이트웨이 노드를 통해 네트워크 전역에 침입 정보를 전달해 주면 된다.

4. 실험 및 결과

4.1 실험 환경

본 논문에서 제안한 방법의 성능 분석을 위하여 다음과 같은 환경에서 실험하였다.

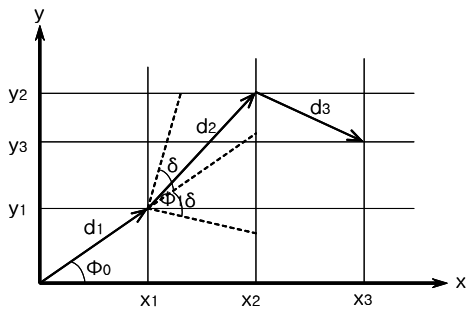
<표 1> 기본 실험 환경

무선 전송 모델	Two- Ground(1/r4)
MAC	IEEE 802.11 DCF
이동성 모델	Random way-point model
트래픽	TCP / UDP

위의 표에서 무선 전송 모델은 비교적 근거리에서는 $1/r^2$에 비례하며, 원거리는 근사적으로 $1/r^4$에 비례한다. 여기서 r은 거리를 의미한다. 그리고 이동성 모델인 random way-point model

은 제한한 속도로 임의의 위치로 이동한 후 임의의 시간 동안 정지하고, 다시 임의의 위치로 이동하는 모델을 말한다.

성능 평가를 위해 사용한 이동 노드들의 이동성 모델은 제한적인 2차원 모델에서 이동 방향을 모든 방향으로 방향 제한을 없앤 모델을 사용한다. 이것은 Mobile Ad Hoc Network에서 사용자는 균등하게 분포하고 있으며, 제한된 방향성을 가진 공간보다는 사용자가 자유롭게 움직일 수 있는 개방된 환경에서 동작한다고 가정한 것이다. 이러한 가정 하에 경로 설정, 클러스터 형성의 오버헤드, 제어 패킷의 양으로 성능 평가의 기준을 정했다.



(그림 3) 노드의 이동 방향 결정

(그림 2)에서는 이동 노드의 초기 진행 방향을 나타내며, 노드는 정해진 방향에 따라 정해진 속도록 임의의 시간동안 이동한 후에 그림과 같이 새로운 이동방향을 결정하게 된다. 그리고 노드들의 이동속도는 식 (1)과 같이 가우시안 확률밀도 함수에 의해서 만들어진 초기 속도와 속도의 증감은 식 (2)에서 현재 속도의 100%의 범위에서 균등 분포를 나타내는 모델을 이용하였다.

$$S_0 = G(e,\sigma) \quad (1)$$

$$S_i = U[S_{i-1}\times 0.9, S_{i-1}\times 1.1] \quad (2)$$

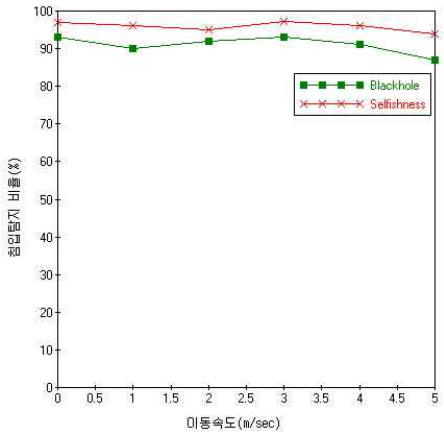
4.2 실험 결과

실험 평가를 위해 패킷의 크기는 64바이트, pause time은 30초로 하였다. 그리고 전송 범위는 150m로 하였으며 네트워크 크기에 따라 10번의 실험을 반복하였으며, 각 실험 시간은 600초로 하였다. 실험에 사용한 노드의 수는 네트워크의 크기에 따라 다르게 설정하였다. <표 2>는 실험에 사용한 노드 수에 따른 네트워크의 크기를 보여주고 있다.

<표 2> 노드 수에 따른 네트워크 크기

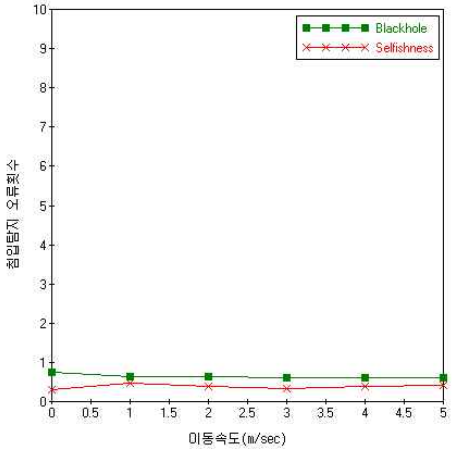
노드수	네트워크 크기
15	300m × 300m
25	500m × 500m
50	700m × 700m

침입탐지 실험을 위해 blackhole과 selfishness를 이용하였다. 각 공격은 임의로 발생시켰으며 실험 시간 동안 10번 발생시켰다. 각 노드들은 학습단계에서 얻은 threshold 값을 이용하여 침입탐지를 하였다. (그림 4)는 침입탐지 비율을 보여주고 있다.

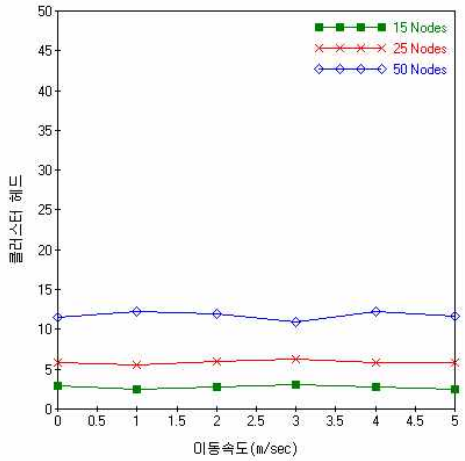


(그림 4) 침입탐지 비율

(그림 5)에서는 침입탐지 오류비율을 보여주고 있으며 selfishness는 0.36%, blackhole은 0.61%의 결과를 보여주었다. (그림 6)에서는 네트워크의 안정성, 즉 클러스터간의 연결 수준과 클러스터들의 안정성을 확인하기 위해서 클러스터 헤드의 평균수를 측정하였다.



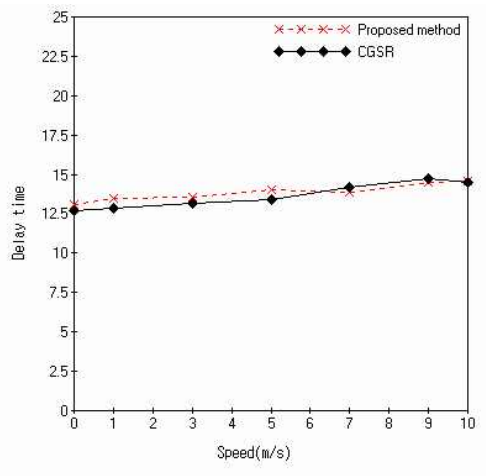
(그림 5) 침입탐지 오류 비율



(그림 6) 클러스터 헤드의 수

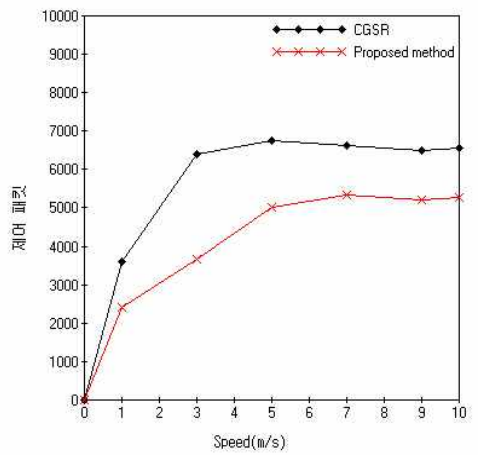
(그림 6)에 나타났듯이 클러스터 헤더들의 수는 네트워크 전체의 노드 수와 이동 속도에 큰 영향을 받지 않고 일정한 비율을 유지하였다. 각 실험에서 클러스터 헤더들의 수는 전체 노드들의 수의 평균 23%를 유지하였다. 여기에서 클러스터 헤드의 수는 전송 반경에 따라 달라질 수 있다. 하지만 네트워크 크기나 노드의 수가 서로 다르더라도 클러스터 헤드의 비율이 일정한 비율로 유지되는 것이 중요하다. 왜냐하면 이러한 일정한 비율이 곧 네트워크의 안정성을 나타내기 때문이다. 본 논문에서 제안한 방법은 클러스터 헤드는 자신의 이웃 노드들로부터 자신이 알고 있는 이웃 노드에 대한 신뢰도 값을 받게 된다. 이때 중복된 노드들에 의한 신뢰도 값을 받는다면 이 신뢰도 값의 평균값을 그 노드의 신뢰도 값으로 설정한다. 따라서 클러스터 헤드가 목적지 노드까지의 경로를 찾기 위해 RREQ 패킷을 수신하면 클러스터 헤드는 중간 노드들의 신뢰도 값을 검사한다. 만약 최단의 경로를 얻는다 하여도 만약 그 경로의 중간 노드가 신뢰도 값이 낮다면 다른 경로를 찾기 위해 RREQ 패킷을 재전송한다. 이렇게 함으로써 안전한 데이터 전송을 할 수 있게 된다. 그리고 노드들의 데이터 전송률이 높아져야 높은 신뢰도 값을 가질 수 있기 때문에 selfish 노드의 수가 적어지고 각 노드들의 상호협력을 조장할 수 있게 된다.

(그림 7)은 소소 노드에 의해 생성된 데이터 패킷이 목적지 노드에 도달하는데 걸린 평균 지연시간이다. 본 논문은 빠른 데이터 전송 보다는 안전한 데이터 전송과 네트워크의 안정성을 목적으로 설계되었기 때문이다.



(그림 7) 평균 지연 시간

(그림 8)에서 보여주는 제어 패킷의 양은 <표 2>에서 보여준 노드의 수가 50개인 경우에 대해서만 실험한 결과를 보여주고 있다. 무선 통신은 대역폭이 낮기 때문에 제어 메시지의 양이 많아지면 네트워크의 전체적인 성능이 저하되게 된다. 특히 클러스터 헤드에 의해 설정되는 경로상에 존재하는 중간 노드들의 신뢰성이 높이 때문에 경로의 수정 횟수가 적게 나타났다.



(그림 8) 제어 패킷의 양

5. 결론

본 논문에서는 Mobile Ad Hoc Network에서 클러스터를 기반으로 노드들의 인증 기법과 침입탐지 기법을 제안하였다. Mobile Ad Hoc Network의 매우 동적인 토폴로지와 다양한 링크의 품질에 적응이 필요하다. 따라서 클러스터를 형성하고 클러스터 헤드가 선출될 때 노드들은 자신의 이웃 노드에 대한 신뢰도 값을 클러스터 헤드에게 통보함으로써 클러스터 헤드는 노드에 관한 직접적인 경험이 없다하여도 노드의 신뢰값을 평가하고 인증할 수 있게 된다. 그리고 클러스터 헤드는 클러스터 내의 모든 패킷의 기록을 저장하고 패킷을 분석하여 많은 공격을 탐지할 수 있게 해준다. 그리고 클러스터 헤드와 멤버 노드가 패킷 분석을 나누어 함으로써 각 노드의 계산량을 줄이고 메모리의 오버헤드를 감소시킨다. 본 논문에서 제안한 방법으로 다양한 공격을 탐지하고 안전한 데이터 전송이 이루어짐을 확인할 수 있었다. 향후 연구로 클러스터 리더를 선출하는 최적의 알고리즘에 대한 많은 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] Charles E. Perkins, "Ad hoc Networking", Addison Wesley, 2001.

[2] L. Venkatraman and D.P. Agrawal, "A Novel Authentication scheme for Ad Hoc Networks", Wireless Communications and Networking Conference, 2000.

[3] Y. Desmedt and S. Jajodia, "Redistributing secret shares to new access structures and its applications", George Mason Univ., Tech. Rep., 1997.

[4]. L. Zhou and Z. J. Hass, "Securing ad hoc networks", IEEE Network, vol. 13, no. 6, pp.24-30, 1999.

[5] A. Bayya, S. Gupte, Y. Shukla, and A. Garikapati, "Security in Ad hoc networks", CS 685, Computer Science Department University of Kentucky.

[6]. H. Lo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing ad hoc wireless networks", in Proc. 7th IEEE Symp. On Comp. and Communication (ISCC), Taormina, 2002.

[7] FH Wai, YN Aye, NH James, "Intrusion Detection in Wireless Ad-Hoc Networks", 2003.

[8] Dorothy E. Denning, "An intrusion-detection Model. IEEE Transactions on software enginnering", February 1987.

양 환 석

1998년 : 조선대학교 전산통계학과 대학원 (이학석사)

2005년 : 조선대학교 전산통계학과 (이학박사)

2007년～현 재 : 호원대학교 사이버수사경찰학부 연구교수

관심분야 : 시스템 보안(System Security), 네트워크 보안(Network Security), 정보보호(Personal Information)