애드 혹(Ad Hoc) 네트워크에서의 위치정보 기반의 웜홀(Wormhole) 탐지 기법

이규호°, 이건희, 김동규, 서정택*, 손기욱*
아주대학교, * 국가보안기술연구소
{im295°, icezzoco, dkkim}@ajou.ac.kr
{seojt, kiwook}@etri.re.kr

Wormhole Detection Method using Node Location in Mobile Ad hoc Networks

Kyuho Lee°, Gunhee Lee, Dong-kyoo Kim Jungtaek Seoo*, Kiwook Sohn*
GSIC, Ajou University, * NSRI(National Security Research Institute)

요 약

이동 애드 혹(Ad Hoc)네트워크는 노드의 참여와 이탈이 자유롭고 토폴로지의 변화가 잦기 때문에 일반 고정 유선네트워크에 비해 보안적으로 훨씬 더 많은 잠재적인 위험을 지니고 있다. 그 중 주변 노드들의 신뢰도에 대한 보장이 이루어지지 않기 때문에 멀티 홉 방식의 라우팅을 할 경우, 악의적인 중간 노드에 의해 정상적인 통신과 서비스를 방해하는 라우팅 과정에서의 공격이 일어날 수 있다. 특히 협력노드를 이용한 웜홀 공격은 단일노드에 의한 공격보다 탐지가 어렵고 그 피해도 더욱 크다. 이러한 웜홀 공격에 대응하기 위하여 본 논문에서는 네트워크에 참여한 노드들의 위치정보를 이용한 CA(central authority)에서의 경로 분석을 통해 웜홀을 탐지하는 기법을 제안하였다.

1. 서 론

이동 노드의 참여와 이탈이 자유로운 이동 애드 혹(Ad Hoc)네트워크에서는 특정한 토폴로지가 존재하지 않고, 고정된 관리 지점이 없어 네트워크 자체의 유지 및 관리에 상당한 어려움이 따른다. 따라서 무선 이동 애드 혹 네트워크에서의 안전한 통신 유지 및 관리는 여러 연구소나 산업에서 계속 연구되어 오고 있다. 특히 메시지를 전달하고 서비스를 제공하기 위한 라우팅 기술에 있어 기존의 유선 환경에서의 라우팅 기술과는 또 다른 형태의 기술이 필요하게 된다. 이러한 요구사항을 만족하기 위해서 애드 혹(Ad Hoc) 네트워크를 위한 다양한 라우팅 기술이 제안되고 실험되고 있다[1, 2].

그러나 이들 모두가 메시지의 정확한 전달에만 그 목적을 두었고 모든 노드들을 신뢰할 수 있다고 가정하였기 때문에 공격자의 다양한 공격에 노출되어 있고 보안상 상당히 취약하다. 이를 해결하기 위해서 공격자의 위협에 대응하기 위한 기술들을 추가한 CSER[3], ARAN[4], SRP[5], SEAD[6], SAODV[7] 등의 안전한 라우팅 기법들이 다양하게 연구되어 왔다.

하지만 이러한 연구들은 하나의 악의적 노드가 특정 애드 혹 네트워크나 특정 노드를 공격하는 것을 탐지하고 대응하는 것을 주요 목적으로 하고 있다. 즉 하나의 공격자 노드가 라우팅 관련 패킷을 수정하거나 가로채고 혹은 차단하여 정상적인 라우팅 과정을 수행하는 것을 방해하는 공격을 탐지, 대응하는 것에 초점을 맞추고 있다.

그러나 이러한 기법들은 하나이상의 악의적 노드들이 협력하여 공격하는 것으로부터 라우팅을 안전하게 보호하지 못한다. 협력을 이용한 공격이 단일 노드에 의한 공격보다 탐지가 어려우며, 공격이 진행 되었을 경우 더욱 큰 피해를 입힐 수 있다. 그리고 컴퓨팅 환경이 발달해 감에 따라 이동 애드 혹 네트워크를 바탕으로 하는 서비스가 점차 늘어날 것이고 그리하여 안전한 애드 혹 네트워크를 위한 연구의 필요성이 커지게 된다. 특히 네트워크 및 노드에 더욱 많은 피해를 줄 수 있는 협력 노드에 의한 공격의 탐지 및 대응을 위한 기법 연구가 더욱 요구된다.

따라서 본 논문에서는 대표적인 협력 노드를 이용한 공격인 웜홀(Wormhole) 공격에 대한 탐지 기법을 제안하고자 한다.

2장에서는 웜홀 공격 탐지와 관련한 이전 연구에 대하여 알아보고 3장에서는 웜홀 공격에 대하여 알아본다. 4장에서는 본 논문을 통해 제안하는 웜홀 탐지 기법에 대하여 논의하고 5장에서는 제안된 기법에 대한 분석, 6장에서는 결론과 향후 연구 방향에 관하여 언급한다.

2. 관련 연구

무선 네트워크에서의 웜홀 공격은 Dahill[8], Hu[9], 그리고 Papadimitratos[5]에서 소개 되었으며, 웜홀 공격을 탐지하고 대응하기 위한 여러 연구가 이루어져 왔다.

웜홀 공격에 대응하기 위한 초기 제안들은 오직 신뢰성를 인정받은 노드들에 의해 확인될 수 있는 암호학적으로 보호된 비트들을 이용하였다. 이 기법은 암호키를 모르는 외부의 공격자로부터만 보호될 수 있다.

Packet Leashes[9]에서는 패킷에 부가적인 정보들(leashes)을 추가함으로써 그 패킷이 전송될 수 있는 최대 거리를 제한하여 웜홀을 막는 방법을 제안하였다.

Geographic leashes는 위치정보를 이용하여 패킷 수신자가 전송자로부터 합당한 거리내에서 패킷을 받는지 아닌지 판단한다. 이를 위해서 모든 노드는 자신의 지리적 위치정보를 알고 있으며, 클럭 정보가 어느 정도 동기화 되어 있어야 한다. Temporal leashes는 패킷의 유효시간을 설정함으로써 최대 전송 거리를 제한하는 방법이다. 패킷이 전송되기 전에 패킷의 라이프 타임을 결정하고 만약 패킷이 라이프 타임이 지난 시점에 도착하면 웜홀을 의심한다. 모든 노드는 정밀한 클럭 동기화가 되어야 한다. Geographic leashes와 Temporal leashes는 둘 다 각 패킷에 leashes를 보호하기 위한 인증 데이터가 추가 되어야 하고 따라서 오버헤드가 늘어난다. 게다가 해쉬 트리 기반의 인증 기법을 사용하기 때문에 각 노드는 많은 저장 공간을 필요로 한다.

SECTOR[10]에서는 어떠한 클럭 동기화를 필요로 하지않는 웜홀 탐지 기법을 제안하고 있다. 이 기법은 특정 비트를 교환하기 위한 별도의 하드웨어를 사용하여 한 노드가 다른 노드와 비트를 교환한 후 그 비트의 왕복 시간을 계산하여 실제 두 노드 사이의 거리를 구한다. 그 거리가 이웃 노드가 될 수 있는 거리 이상이면 웜홀로 의심을 한다.

Hu와 Evans[11]는 웜홀을 방지하기 위해서 directional antenna를 사용한다. 각 노드는 다른 모드들과 비밀 키를 나누어 가지고 있고, directional antenna를 사용하여 모든 방향으로 암호화된 메시지를 브로드캐스트 하여 응답이 오면 그 방향에 실제 자신의 이웃 노드가 존재하는 것으로 간주하고 이웃 노드 리스트를 갱신한다. 이 방법은 웜홀을 통해 실제 멀리 떨어진 노드가 이웃인 것처럼 속이는 것을 방지할 수 있으나 모든 노드가directional antenna라는 하드웨어가 탑재되어 있어야 한다.

LiteWorp [12]은 네트워크 전반에 분포되어 있는 Guard라고 하는 선택된 노드에 의한 모니터링을 이용한다. Guard는 웜홀을 탐지하기 위해서 A가 C와 통신하기 위해 B에게 패킷을 전달했는데 B가 패킷을 전달하지 않는 행위 등을 모니터링하여 웜홀을 탐지한다. 그러나 악의적으로 잘못된 행위를 일으켜 정상 노드를 비정상으로 모니터링 되게 할 수 있는 취약한 점이 있다.

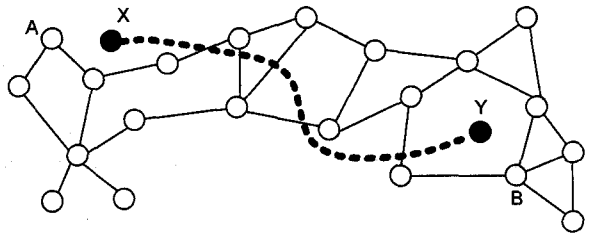
[13]에서는 지역 브로드캐스트 키를 사용하여 웜홀을 지나간 브로드캐스트 패킷은 확인 할 수 없도록 하여 웜홀을 탐지하고 대응한다.

3. 웜홀 공격(Wormhole Attack)

협력 노드를 이용한 대표적인 공격인 웜홀 공격은 특히 라우팅과 관련하여 위험성을 가지고 있다. 애드 혹 네트워크 라우팅 프로토콜이 정상적으로 동작하지 못하게 하여 네트워크의 노드들이 통신을 하는 것을 방해한다.

3.1 웜홀 공격

웜홀은 네트워크 안에 형성된 일종의 터널이다. 이 터널을 통해 실제 두 홉 이상 떨어져있는 노드들은 여러 홉 거리가 아닌 1 홉 거리가 된다. 즉 웜홀을 이루는 공격 노드들은 실제 한 홉 이상 멀리 떨어져 있지만, 이들 사이에 형성된 터널을 이용하여 한 홉 거리에 있는 것처럼 행동한다. 따라서 공격자는 정상의 여러 홉을 거치는 경로보다 공격 노드가 포함된 더 좋은(홉 수가 작거나, 빠른) 경로를 따라 패킷이 이동하도록 하는 것이 가능하다.



[그림 1] 기본적인 웜홀의 예

[그림 1]은 간단한 웜홀을 보여 준다. A는 B에게 패킷을 보내려고 한다. 이때 A로부터 패킷을 받은 X는 그 패킷을 X와 Y사이에 형성된 웜홀 터널을 통해 Y로 보낸다. 패킷을 받은 Y는 그 패킷을 B에게 보낸다. 웜홀이 없을 경우, A와 B사이의 정상적인 경로를 따라 여러 홉을 거쳐 패킷이 이동되어야 하지만 이 경우 웜홀을 통해 아주 빠르게 패킷이 전달된다.

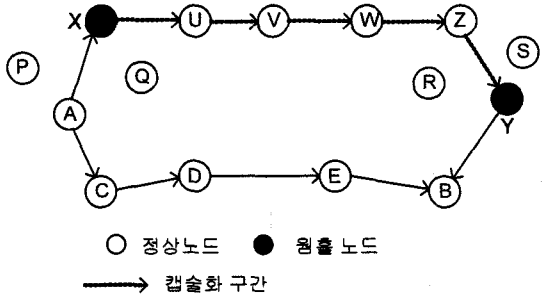
공격자가 네트워크의 매우 위협적인 위치에 웜홀을 생성하여 이를 악용한다면, 경로 설정 과정에서 웜홀이 경로에 포함되게 할 수 있고, 포착되기 어렵게 특정메시지를 선택적으로 차단하거나 변경시킬 수 있다.

3.2 웜홀의 분류

웜홀은 그것을 형성하는 방법에 따라 캡슐화를 이용하는 방법, 외부채널을 이용하는 방법, 강한 전파를 이용하는 방법, 패킷을 중계하는 방법으로 분류될 수 있다.

3.2.1 캡슐화 이용 웜홀

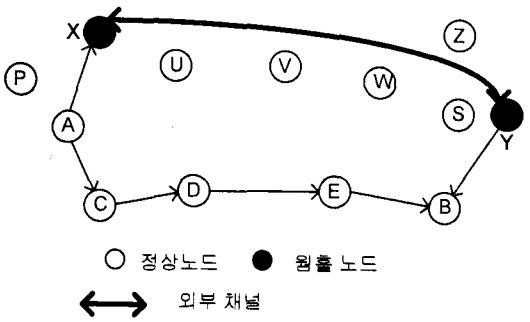
웜홀을 형성한 한쪽의 공격 노드가 주변의 경로요청 메시지를 들으면 그 메시지를 일반 데이터 패킷 포맷의 페이로드(payload)부분에 넣어 캡슐화 하여 웜홀의 반대쪽 공격 노드에게 일반 데이터처럼 전달한다. 웜홀의 반대쪽 노드가 그 데이터를 받으면 페이로드 부분에서 경로요청 메시지를 획득하여 그것을 다시 일반 경로탐색 과정처럼 경로요청 메시지의 목적지로 브로드캐스팅을 한다.



[그림 2] 캡슐화 이용 웜홀

3.2.2 외부채널이용 웜홀

이 웜홀은 두 공격 노드 사이에 외부채널을 형성하는 방법이다. 이 외부채널은 긴 거리를 가진 방향성 있는 무선 링크일 수 있고, 직접 연결된 유선링크일 수 있다. 이 방법은 위의 캡슐화 방법에 비해 외부 채널 형성을 위한 특별한 하드웨어가 필요하다는 점이 다르다. 이 웜홀을 이용한 공격도 A의 B에 대한 경로 요청 메시지를 외부 채널을 통해 실제 여러 홉 떨어져있는 X와 Y가 1홉인 것처럼 보이게 함으로써 정상 경로인 A-C-D-E-B보다 A-X-Y-B가 최종 경로로 선택되게 한다.



[그림 3] 외부채널을 이용한 웜홀

3.2.3 강한 전파이용 웜홀

이 방법은 공격 노드가 경로요청 메시지를 받으면, 그 메시지를 일반 노드보다 훨씬 높은 파워로 브로드캐스팅 한다. 이 높은 파워의 브로드캐스트는 보통의 파워를 가진 것보다 채택될 가능성이 높다. 공격 노드의 브로드캐스팅을 들은 노드는 일반 경로탐색 과정을 따라 목적지를 향해 다시 브로드캐스팅 한다. 이 웜홀 형성 방법은 또 다른 협력 노드의 참여 없이 하나의 공격 노드만으로 가능하며, 그 노드가 최종 경로에 포함될 기회를 증가시킨다. 이 방법은 일반 노드가 자신이 받을 수 있는 시그널 파워의 최대치를 설정해 놓는 간단한 방법으로 대처할 수 있다.

3.2.4 패킷 중계이용 웜홀

이 방법도 하나의 공격 노드만으로 가능한 방법이다. 서로 이웃 노드가 아닌 A, B노드가 서로를 이웃으로 착각하게 만들기 위해, A와 B사이의 공격 노드가 패킷을 단순히 중계한다. 따라서 A와 B는 서로 1홉 사이에 있는 것으로 믿게 된다.

4. 제안하는 웜홀 탐지 기법

웜홀로 인해 실제 여러 홉의 거리로 멀리 떨어진 두 노드가 라우팅 과정에서 1홉의 거리가 되어 정상적인 라우팅을 방해하고 경로가 웜홀을 지나도록 설정되어질 가능성이 커지게 된다. 본 논문에서 제안하는 기법은 해당 네트워크에 CA(central authority)두어 각 노드들의 위치정보를 기반으로 하여 라우팅 과정이 끝난 후 선택된 경로에 대한 정당성 여부를 판단한다. 선택된 경로 상의 노드들 사이의 거리 중 정상적인 범위 이상의 것이 발견되면 그 경로 상에 웜홀이 있는 것으로 간주하고 탐지한다.

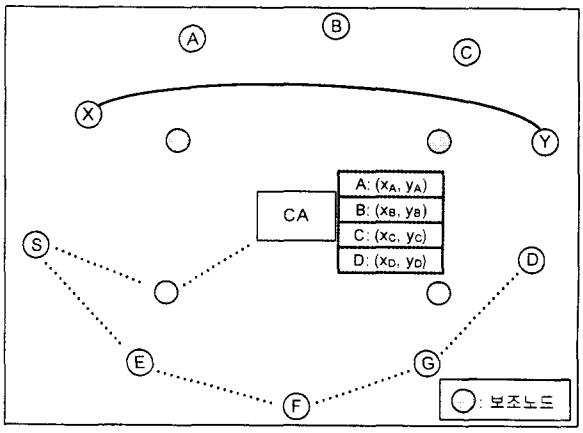
4.1 가정

이 기법은 다음을 가정한다.

- 라우팅 프로토콜은 DSR[2]을 사용하는 것으로 가정한다.
- 해당 네트워크에 CA를 두어 각 노드의 위치정보를 관리한다. 이때의 위치정보는 2차원 좌표인 (x, y)를 사용한다고 가정한다.
- 네트워크의 각 노드들은 CA와 secret key를 공유하고 있다.
- 네트워크에 노드가 새로 진입 시 또는 노드가 이동하여 새로운 위치로 갈 때마다 노드의 위치정보를 CA에게 전달한다.

4.2 웜홀 탐지 모델

본 논문에서 제안한 애드 혹 네트워크에서의 웜홀 탐지 기법을 설명하기 위한 네트워크 모델은 [그림 4]과 같다. CA는 각 노드들과 Key를 공유하고 있고, 각 노드의 위치정보를 가지고 있다. 토폴로지 내부 어디에서도 CA와 통신 가능하도록 CA는 네트워크의 가운데 위치하고 있으며 그 주위로 패킷 포워딩을 위한 보조 노드들이 위치하고 있다. 보조노드는 자신에게 오는 패킷을 전달하는 중간노드로서의 역할만을 하고 CA는 중간노드로서 패킷 전달의 역할은 하지 않고 웜홀 탐지를 위한 각 노드와의 통신과 관계된 패킷만 처리한다. X, Y 노드는 터널을 형성하고 있는 웜홀 공격에 이용되는 공격자 노드이다.



[그림 4] 웜홀 탐지 모델

4.3 웜홀 탐지 과정

각 노드 ID들은 네트워크에 진입시 또는 이동하여 위치를 옮긴 후 CA와 공유하고 있는 키 K_n를 이용하여 자신의 위치정보 암호화한 $E_{Kn}[ID_n, x_n, y_n]$를 CA에 전달한다(여기서 ID_n은 n번 노드를 의미하며 x_n, y_n는 그 노드의 (x, y) 좌표정보를 의미한다.). 그리하여 CA는 네트워

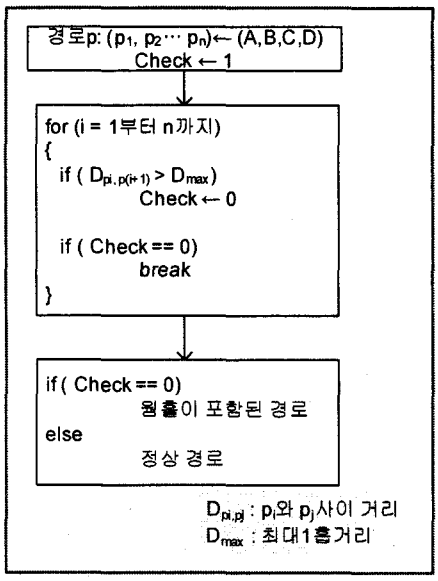
크 내의 모든 노드들의 위치정보를 가지게 된다.

그 뒤 출발지 노드S가 목적지 노드D와 통신하기 위해 DSR 라우팅 과정을 따라 경로를 결정하게 되면, 노드 S는 목적지 D까지의 전체경로(S-…-D)를 얻게 되고 그렇게 얻은 경로정보를 CA와 공유하고 있는 키 K_s을 이용하여 암호화한 $E_{Ks}[ID_n$, 전체경로(S-…-D)]를 CA에게 보낸다.

CA는 노드S로부터 받은 전체경로를 자신이 가지고 있는 위치정보를 이용하여 [그림 4]와 같은 과정을 따라 전체경로에 포함된 노드들 사이의 1홉 거리를 계산하여 네트워크에서 허용하는 최대 1홉 거리보다 큰 것이 있으면 그 경로 상에 비정상적인 웜홀이 있다고 탐지한다. (x_i, y_i), (x_j, y_j)에 위치하는 두 노드 i, j사이의 거리는 아래의 식을 이용하여 구할 수 있다.

$$D_{i,j} = \sqrt{(x_i - x_j)^2 - (y_i - y_j)^2}$$

노드S는 CA로부터 그 경로에 웜홀이 없다는 메시지를 되돌려 받으면 그때부터 노드D와의 통신을 시작한다.



[그림 6] CA에서의 경로분석 과정

5. 탐지 기법 분석

제안한 웜홀 탐지 기법을 이용하여 웜홀이 어떻게 탐지되는지 사례를 들어 분석해본다.

사례 1: [그림 4]에서 노드S와 D사이의 정상 경로는 (S, E, F, G, D)이다. 그러나 S와 D사이의 경로를 설정하려고 할 때, 웜홀 노드 X, Y사이의 터널로 인해 정상경로가 아니라 웜홀 노드가 포함된 경로인 (S, X, Y, D)가 선택된다. 그러나 이 경우 노드S가 선택된 경로를 CA에게 보내면 CA는 X, Y사이의 거리가 최대1홉거리보다 크기 때문에 웜홀이 포함된 경로로 판단하게 된다.

사례 2: 노드S와 D사이의 경로 설정 시 웜홀 노드 X, Y가 라우팅 과정을 따르지 않고 둘 사이의 터널로 단순히 중계했을 경우 정상경로가 아닌 (S, D)가 경로로 선택된다. 그러나 노드S가 선택된 경로를 CA에게 보내면 CA는 거리 계산을 통해 S와 D는 이웃이 아님을 알 수 있고 웜홀이 탐지된다.

사례 3: 위의 사례1에서 웜홀 노드 X, Y가 X와 Y의 사이가 1홉 거리이내에 있도록 자신의 위치를 속여서 CA에 알릴 경우, 노드S와 D사이에 설정된 경로인 (S, X, Y, D)를 CA가 분석할 때 X와 Y사이의 거리는 정상으로 판단될 수 있지만 X와 Y가 가까워진 대신 S와 X 또는 Y와 D의 거리가 멀어지게 되어 경로 상에 비정상노드가 있는 것으로 탐지되게 된다.

사례 4: [그림 4]에서 노드S와 B사이의 경로 설정 시 공격자 노드 X가 라우팅관련 패킷을 단순히 중계하여 (S, A, B)라는 경로를 설정하면 S는 A와 이웃이라고 착각하게 된다. 이때에도 CA는 노드S로부터 받은 경로의 분석을 통해 S와 A사이의 거리가 최대 1홉 거리 이상인 것을 알 수 있고 그 사이에 공격자 노드가 있다고 탐지한다.

6. 결론 및 향후방향

애드 혹 네트워크를 이용한 서비스 제공에 있어서 안전한 메시지 전달 및 서비스 유지를 위한 안전한 라우팅의 보장은 매우 중요한 사안이다. 특히 공격자가 협력 노드를 이용한 웜홀을 형성하여 정상적인 라우팅을 방해하고 네트워크에 위협을 가하는 행위는 하나의 노드에 의한 공격 보다 정확한 탐지가 어려우며, 그 피해도 더욱 크다. 따라서 안전한 애드 혹 네트워크를 위하여, 악의적 협력 노드를 이용하는 웜홀 공격의 탐지 및 대응을 위한 연구가 더욱 필요하다.

본 논문에서 제안한 라우팅 과정에서의 웜홀 탐지 기법은 웜홀 공격으로 인한 피해를 감소시키기 위해, 네트워크에 참여한 노드들의 위치정보를 기반으로 하여 CA(central authority)에서 DSR라우팅 결과를 분석하고 그 결과를 바탕으로 경로상의 웜홀 여부를 판단한다.

네트워크의 주 구성원인 리소스 제한적인 이동 노드에서의 처리 부담을 줄이기 위해 라우팅 과정 이외의 웜홀 탐지와 관련한 과정은 모두 CA에서 처리하고 그 결과만 각 노드와 교환하도록 하였으나, 네트워크 규모가 커지고 각 노드간 통신 세션이 아주 빈번하게 이루어진다면, 한 CA에서의 오버헤드가 매우 커질 것이다. 따라서 CA에서의 부담을 줄이기 위한 분산 CA의 활용이 필요하고 이에 대한 논의는 향후 연구 과제이다.

7. 참고 문헌

[1] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing", In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100,

New Orleans, LA, February 1999.
[2] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", in Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.
[3] B. Lu, U. W. Pooch, "Cooperative Security-Enforcement Routing in Mobile Ad Hoc Networks", Mobile and Wireless Communications Network, 4th International Workshop, pp. 157- 161, 2002
[4] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. B. Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 2002
[5] P. Papadimitratos and Z.J. Hass, "Secure Routing for Mobile Ad hoc Networks", Proceeding of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 02), 2002
[6] Y. C. Hu, D. B. Johnson, A. Perrig "SEAD: Secure Efficient Distance Vector Routing For Mobile Wireless Ad Hoc Networks", Mobile Computing Systems and Applications, Proceedings 4th IEEE Workshop, pp.3-13, 2002
[7] M. C. Zapata "Secure Ad hoc On-Demand Distance Vector Routing", ACM SIGMOBILE Mobile Computing and Communications Review, Vol 6, issue 3, New work, USA, pp.106-107, 2002
[8] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad-hoc networks", Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, 2001
[9] Y. C. Hu, A. Perrig, and D. B. Johnson. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", In Proceedings of IEEE INFOCOM 2003, pp.1976-1986, 2003
[10] S. Capkun, L. Buttyan, and J. P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop WirelessNetworks", in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN 03), pp.21-32, 2003.
[11] L. Hu and D. Evans "Using Directional Antennas to Prevent Wormhole attacks", In Proceedings of Network and Distributed System Security Symposium, pp.131-141, 2004
[12] Khalil, I. Saurabh Bagchi Shroff, N.B., "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks", In Proceedings of the International Conference on Dependable Systems and Networks,(DSN'05), pp.612-621, 2005
[13] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks", ACM Journal on Wireless Networks, 2005