애드혹 네트워크에서의 이웃노드 정보를 이용한 웜홀 탐지

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

Neighborhood-based Wormhole Attack Detection in Wireless Ad hoc Network

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

요 약

단말의 휴대화가 진행되고 있는 최근에서는 무선 네트워크에 대한 관심이 보다 높아지고 있다. 이러한 요구에 맞추어 기존 인프라의 도움 없이 네트워크의 구성요소들로만 네트워크를 구성하는 애드혹 네트워크 기술이 생겨났다. 하지만 애드혹 네트워크 기술이 발전함에 따라 그에 대한 공격 방법들도 날로 발발전하고 있으며, 대표적인 공격 방법 중 하나가 웜홀을 이용한 잘못된 경로의 설정이다. 공격노드는 웜홀 공격을 이용하여 다른 정상노드들의 라우팅 경로에 자신을 포함시킬 수 있고 이를 통해 패킷의 분석 및 정보의 탈취가 가능하다. 본 논문에서는 애드혹 네트워크에서의 웜홀 공격의 탐지를 위해 경로 설정시의 이웃노드들의 정보를 이용하는 방안을 제시하고 있다.

1. 서 론

무선 애드혹 네트워크(Wireless Ad hoc Network)는 이미 구축되어진 인프라의 도움 없이 무선 통신으로 연결된 노드들만으로 형성이 가능한 네트워크이다. 유선망에서의 라우터와 같은 경로 설정을 담당하는 노드가 없기에 무선 애드혹 네트워크의 모든 노드들은 라우팅 기능을 가지고 있어야 한다. 이를 위해서는 모든 노드가 라우팅 기능을 지닌 서버이자 라우팅을 이용하는 클라이언트이어야 한다. 애드혹 네트워크의 노드들은 자신의 주변에 존재하고 자신의 전송범위 안에 위치하여 인식할 수 있는 이웃 노드들과의 협력을 통하여 전송범위의 밖에 위치하고 있는 노드들과 통신을 하는 멀티홉(multi-hop) 라우팅을 사용한다.

애드혹 네트워크에서의 위와 같은 라우팅을 위해 AODV, DSR, DSDV 등의 여러 가지 라우팅 방법들이 제안되었다. 하지만 이 방법들은 공통적으로 이웃노드들에 대한 신뢰를 바탕으로 하고 있기에 악의적인 의도를 지니는 노드가 이웃노드로써 정상노드로부터 신임을 받고 있다면, 이 노드로 부터의 거짓된 정보 전송에 의하여 심각한 피해가 발생 할 수 있으며, 이중 중요한 공격 방법 중 하나가 웜홀(Wormhole) 공격이다. 웜홀 공격을 통하여 공격자는 잘못된 정보의 전송을 통해 다른 두 노드 사이에 통신 경로가 설정 될 때 자신이 중간 노드로써 포함된 경로를 선택되게 할 수 있다. 이렇게 경로를 자신이 있는 방향으로 바꿈으로써 주고받는 정보의 분석이 가능해지고 이를 통해 보다 직접적인 공격으로의 전환을 쉽게 만들 수 있다[1].

본 논문에서는 무선 애드혹 네트워크에 간접적인 피해를 입힐 수 있는 웜홀 공격을 효율적으로 탐지하고 막을 수 있는 방법을 제안하고자 한다.

2. 관련 연구

2.1 애드혹 네트워크

기존의 고정된 유선망과는 달리 무선 ad hoc 네트워크는 자체적이고 임시적인 연결성을 갖는다. 그리고 기존의 이동통신망과 구별되는 가장 큰 특징은 AP 같은 중재자의 도움이 없이 자체적으로 망 구성이 가능하고 라우터가 존재하지 않아 네트워크를 구성하고 있는 노드들 자체가 라우터의 기능을 가지고 있어야 하며, 모든 노드가 서비스 요청자인 동시에 서비스 제공자가 되어야 한다는 것이다.

무선 애드혹 네트워크는 동적인 네트워크 토폴로지를 갖는다. 수시로 네트워크의 구성 노드들이 바뀔 수 있다. 이러한 변화는 사용자의 배터리 상태나 이동성, 발생하는 트래픽에 따라 다양하게 발생한다. 이런 유동적인 네트워크 토폴로지의 변화로 인해 경로의 설정과 유지가 어렵다. 또한 기존의 유선망에서 사용하던 라우팅 프로토콜을 그대로 적용하기도 어렵다. 게다가 많은 애드혹 네트워크상의 여러 서비스들이 QoS, 패킷 처리량 등에 있어서는 유선망에서 제공하는 수준을 요구하고 있기 문에 무선 애드혹 네트워크의 기술과 다양성을 어렵게 한다. 또한 무선 네트워크를 사용하기 때문에 전송거리와 전송 대역폭의 제한이 심하고 전파의 간섭 및 다중링크로 인한 보안상의 문제점이 있기에 불안전한 링크 특성을 가지게 된다.

또한 무선 애드혹 네트워크는 분산 운영 기능을 가지고 있어서 네트워크 내에 라우터의 기능을 하거나 방화벽처럼 보안 메커니즘을 제공해 주는 서버가 없기 때문에 이러한 기능들이 네트워크 구성 노드들의 협력에 의해 분산적으로 운영 되어야 한다. 그리고 네트워크를 구성하는 노드들이 상당한 컴퓨팅 파워를 가진 머신일 수도 있지만 휴대폰이나 단말 센서와 같은 제한된 배터리

로 동작하는 노드일 수 도 있다. 이런 경우 다양한 서비스와 다른 노드들의 패킷을 전달해야 하기에 네트워크 기능에 제약으로 나타날 수 있다.

2.2 무선 애드혹 네트워크의 라우팅

무선 Ad hoc 네트워크 에서는 트래픽, 그리고 주변 환경으로 인한 링크의 연결성이 수시로 변하기 때문에 네트워크 토폴로지가 자주 변경되어 한 노드에서 다른 노드로 가는 고정적인 경로가 존재할 수 없다. 무선 애드혹 네트워크의 노드는 무선 통신을 사용하기에 제한된 전파 전송 범위를 가지고 이 때문에 멀리 떨어진 노드로의 통신은 자신의 이웃노드들과 그 노드의 이웃노드들의 메시지 전달을 이용한 멀티 홉 라우팅을 사용해야 한다. 하지만 위에 나타난 대로 노드들의 이동성으로 인하여 한 노드의 이웃 노드들은 자주 바뀌게 된다. 즉 하나의 경로가 설정되면 그것이 계속 존재할 수 없기에 주기적으로 자신의 위치를 광고하거나 메시지를 보낼 때 마다 경로를 설정하는 방법을 사용한다.

기존의 고정망에서 사용하는 RIP(Routing Information Protocol)나 OSPF(Open Shortest Path First)프로토콜들은 이동성이 적은 고정적인 네트워크 환경에서 작동하므로 계속적인 노드의 이동이 일어나는 무선 애드혹 네트워크에 사용하기에는 무리가 따른다. 따라서 기존의 라우 팅 프로토콜의 변형 또는 새로운 방식의 라우팅 프로토콜이 요구되며, 무선 애드혹 라우팅 프로토콜에 대한 연구는 무선 애드혹 네트워크의 주된 연구 대상이 되고 있다. 그 연구들의 결과로 <표 1>과 같이 AODV(Ad Hoc On-demand Distance Vector),, DSR(Dynamic Source Routing), ZRP(Zone Routing Protocol) 그리고 TORA(Temporally-Ordered Routing Algorithm) 등의 유용한 프로토콜들이 제안되었다.[2]

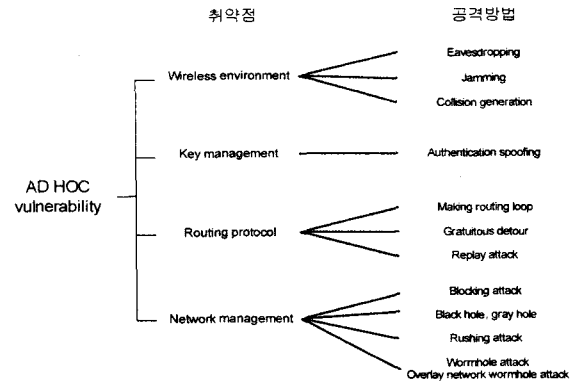
분류 방식	라우팅 프로토콜
테이블 방식	DSDV
	WRP
하이브리드	ZRP
요구 기반	AODV
	LMR
	ABR
	DSR

<표 1> 무선 애드혹 네트워크 라우팅 프로토콜

이렇게 많은 라우팅 프로토콜들이 개발되었지만 반사적으로 그 취약점도 많아지게 되었다. 하지만 각 프로토콜마다 경로를 설정하는 방법이 다르기에 취약점 역시 서로 다르게 나타나게 되었고, 각 프로토콜에 맞는 안전한 라우팅 방법(Secure Routing)들이 나타나게 되었다. SAODV, ARAN, Ariadne, SEAD 등의 안전한 라우팅 방법들은 서로 목표로 하고 있는 라우팅 프로토콜에서 나타나는 취약점을 해결하는 방안을 제시하고 있다. 하지만 대부분의 안전한 라우팅 방법에서도 웜홀 공격에 대하여서는 완벽한 해결책을 내놓지 못하고 있다.[3]

2.3 무선 애드혹 네트워크에서의 공격 방법

무선 애드혹 네트워크에 대한 공격은 기본적으로 라우팅 메시지나 데이터 패킷 또는 라우팅 테이블을 위조, 변경, 가로채기 혹은 메시지나 패킷을 범람시키는 방식으로 이루어 질 수 있고, 또한 네트워크에 오가는 트래픽을 도청하여 그것을 분석해 정보를 알아내는 방식 등으로 이루어 질 수 있다. 이러한 공격은 서비스 거부(Denial of Service)나 비정상적인 동작을 일으켜 네트워크에 직접적인 위해를 가하는 능동적인 공격과 네트워크에 실제 직접적인 피해를 주지는 않는 수동적 공격으로 나눌 수 있다.



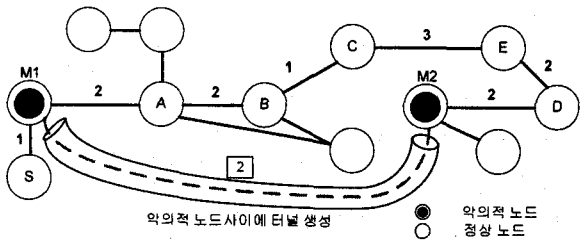
<그림 1> 애드혹 네트워크의 취약점과 공격방법

수동적인 공격은 주로 도청이나 감청 등을 지칭하며, 실질적인 피해를 주지는 않으나 네트워크에서 발생되는 정보들을 분석하여 중요한 사적인 정보를 유출시키거나 차후 더 위협적인 공격을 위한 정보 수집을 목적으로 이루어진다.

능동적인 공격은 공격 주체가 직접 네트워크에서 벌어지는 메시지의 전송에 참여해서 그것을 수정하거나 잘못된 정보를 보내는 것이다. 이는 주로 네트워크 내부의 정상노드를 가장한 노드를 이용하거나 네트워크의 외부에서 정상적인 패킷처럼 가장한 위조 패킷을 보내는 방법으로 이루어진다. 이 외에도 재밍(Jamming)이나 주파수 충돌 같은 물리적 레벨의 공격을 통해 네트워크의 기능을 마비시키는 치명적인 공격방법도 있다. 그 중 노드들 사이의 라우팅 경로를 비정상적인 터널을 통해 악의적인 노드가 포함된 경로로 설정되게 하는 웜홀 공격은 그 공격 자체는 크게 피해를 입히지 않지만 이것을 이용하여 직접적으로 피해를 입힐 수 있는 2차적인 공격이 쉽게 가능하다는 점에서 중요한 문제로 떠오르고 있다.

2.4 웜홀 공격

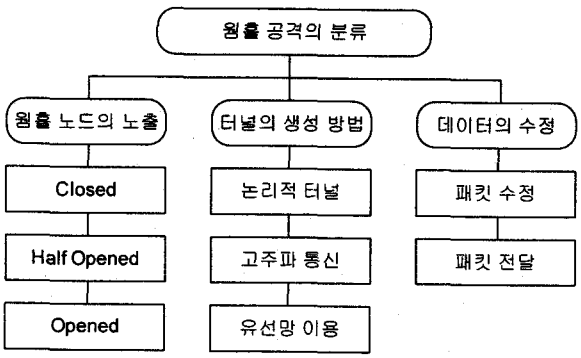
위에서 살펴보았듯이 애드혹 네트워크의 라우팅 프로토콜들은 멀티홉 기반으로 이루어지기에 결정되는 경로의 정확성을 이웃노드들에 의존할 수밖에 없다. 이러한 취약점을 이용해 웜홀 공격이 발생한다.



<그림 2> 애드혹 네트워크에서의 웜홀공격

<그림 2>는 애드혹 네트워크를 나타내고 있다. 원은 구성 노드를 나타내고, 선 위의 숫자는 노드에서 노드로 이동하는데 드는 비용을 나타낸다. 정상적인 경우라면 노드 S 에서 노드 D로의 경로는 13의 비용이 드는 S-M1-A-B-C-E-D의 경로가 선택되겠지만, 만약 악의적인 두 노드가 사전에 협의된 터널을 사용하여 자신들이 더 짧은 경로를 가지고 있다고 알린다면 S-M1-M2-D 의 경로가 최적의 경로로 선택될 것이다. 이 터널은 고속의 유선 네트워크를 사용할 수도 있고, 혹은 전송능력이 강한 무선통신을 사용하기에 실제 거리가 보다 멀더라도 정상적인 애드혹 네트워크에서의 라우팅 기법보다 목적지에 빠르게 도착 할 수 있으며, S 에게 보다 빨리 D로의 경로를 알려 줄 수 있다. 이런 방법으로 S와 D사이의 통신은 항상 공격노드에게 노출되고, 만약 그 내용이 암호화 되어있더라도 다양한 공격방법이 가능하기에 보안은 보장하기 힘든 어려움이 있다.

위에서 설명한 대로 웜홀 공격의 기본원리는 간단하지만 이를 구현한 방법에는 여러 가지가 있으며 그 구분 방법은 <그림 3>에 나타나 있다.



<그림 3> 웜홀 공격의 분류

우선 웜홀은 터널을 구성하는 두 노드가 설정되는 거짓 경로상에 나타나는지에 따라서 Closed, Half Opened, Opened로 나뉠 수 있다. Closed는 두 노드가 모두 경로에 나타나지 않을 때, Half Opened는 둘 중 한 노드만이 경로에 나타나는 경우, Opened는 두 노드 모두가 경로에 나타나는 경우를 의미한다. 그리고 터널의 생성 방법이 경로 설정 패킷의 수정을 통한 논리적인 터널일 경우, 전송 파워가 강한 안테나를 사용하여 보통의 노드들보다 빠른 전송속도를 이용한 경우, 사전에 준비된 유선 네트워크를 사용하는 경우로 나뉠 수 있다. 마지막으로 경로 설정 패킷을 수정하는지 그렇지 않은지에 따라 그 종류가 달라진다.

2.5 웜홀 공격 탐지 방법들

웜홀 공격을 탐지하기위해서는 우선 자신의 이웃 노드들에 대한 정보를 알아야 한다. 이를 탐지하기 위해 방향성 안테나[4]방법을 제안한 논문에서는 HELLO메시지를 이용하고 있다. 각 노드는 네트워크에 참가할 때 이웃 노드들을 발견하기 위해 HELLO 메시지를 사전에 분배된 키로 암호화된 메시지와 함께 전송하고 이를 받은 노드는 키를 이용한 인증을 통해 메시지를 인증하고 랜덤 챌린지(*Random challenge*)와 함께 그 응답을 보내는 방법을 사용하고 있다.

이웃노드의 탐지 못지않게 중요한 것은 노드의 위치정보이다. Packet Leashes[5]에서는 노드들의 위치정보를 기반으로 웜홀 공격을 탐지하고 있다. 경로 설정 패킷 안에는 그때까지 지나온 노드들의 위치정보와 해당 노드에서 패킷을 전송 했을 때의 시간정보가 담겨 있다. 목적지 노드에서는 이 정보들을 바탕으로 각각의 노드와 노드사이에서 패킷이 전송된 속도를 계산해 낼 수 있고, 이를 미리 정해놓은 최대 속도와 비교하여 만약 그 값을 넘어선다면 비정상적인 터널을 이용한 웜홀 공격으로 판단하고 있다. 이와는 별도로 패킷의 라이프타임을 설정하여 실제 전송되는 거리를 제한하고 있다. 하지만 이 방법은 시간을 중요한 요소로 사용하고 있기에 모든 노드들이 동기화 되어 있어야 한다는 단점을 지니고 있다.

DelPHI[6]에서는 경로 설정 패킷이 전달될 때에 각 노드들은 패킷을 받은 시간을 경로설정 패킷에 덧붙이고, 이를 계산하여 노드 사이의 RTT(Round Trip Time)을 구하여 구간별 집중도를 분석함으로써 웜홀 공격을 탐지해 내고 있다. 하지만 이 역시 노드들 사이의 동기화가 이루어져 있어야 한다는 어려움이 있다.

주변노드들의 행동을 모니터링 하여 웜홀을 탐지하는 방법으로는 LITEWORP[7]가 있다.LITEWORP에서는 이웃 노드들과 그리고 두 홉 거리에 있는 노드들에 대한 이웃노드 리스트를 유지한다. 이 이웃노드 리스트를 이용하여 공격 노드가 RREQ나 RREP의 이웃 노드를 수정한다면 탐지해 낼 수 있다. 하지만 이 방법은 이웃노드 리스트의 생성 시 해당 정보에 대한 확인 방법이 없기에 공격 노드가 사전에 거짓 이웃 정보를 전파하는 경우 웜홀의 탐지가 불가능하다.

또 다른 방법으로는 이웃 노드들의 이상행동을 감지하는 것이 있다. 이것은 DSR 라우팅 프로토콜에서만 사용가능하다. 각 노드는 경로설정 패킷을 전송한 뒤 자신의 주변노드들이 그것을 전송하는 것을 살펴본다. 만약 A 노드가 지금까지의 경로를 S-U-A 라고 설정하고 B 노드에게 전달했다면 B노드는 경로를 S-U-A-B 로 설정하고 보내야 한다. 그러나 만약 B노드가 웜홀 공격 노드라면 이 값을 다른 이름으로 바꾸게 될 것이고 A 노드는 모니터링을 통해 경로가 조작되었음을 판단하는 방법이다.[8] 하지만 이 방법은 웜홀 공격 노드가 경로를 수정할 경우는 정상적으로 탐지할 수 있으나 비정상적인 터널을 통하여 경로의 수정이 없이 웜홀을 생성한 경우

에는 탐지해 낼 수 없다는 단점이 있다

3. 제안 기법

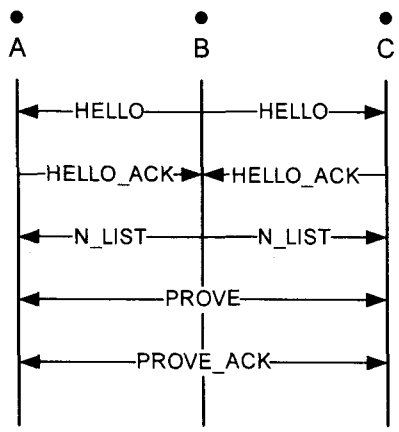
3.1 필요한 가정

본 논문에서 제안하고자 하는 웜홀 탐지 방법을 사용하기 위해서는 네트워크 환경에 있어서 몇 가지 가정이 필요하다. 모든 노드는 GPS(Global Positioning System)나 사용자 입력 방식 등을 통해 자신의 지리적 위치를 알고 있어야 하며, 정적인 네트워크여야 한다. 즉 노드의 위치가 변경될 수 없고 위치를 이동하기 위해서는 네트워크에서 탈퇴 한 뒤 다시 참가하는 방식을 취하여야 한다. 또한 노드들 사이의 링크는 양방향으로 이루어져서 A라는 노드가 B노드의 통신 내용을 들을 수 있다면 B노드도 A노드의 통신을 들을 수 있어야 한다. 그리고 이 전송범위는 모든 노드에 있어서 동일한 값을 가진다. 모든 노드는 한 노드에서 다음 노드로 메시지가 전송되는 최대 시간에 대한 임계값 T_t를 공통적으로 가지고 있어야 한다. 이 T_t는 두 노드 사이의 패킷전송 최대 시간을 의미하며, 만약 패킷이 전송된 시간으로부터 Tt시간 후에 도달하게 되면 해당 패킷을 폐기한다. 각 노드는 자신의 전송범위 내에 존재하는 노드들을 감지할 수 있다. 경로 설정에 있어서 어떠한 라우팅 프로토콜이라도 사용될 수 있지만 라우팅 패킷의 메시지 부분에는 해당 RREQ, RREP 패킷을 보낸 노드의 아이디, 위치정보와, 이전 노드의 아이디, 위치정보가 포함되어 있어야 한다.

3.2 이웃 노드의 탐색

본 논문에서 제안하고 있는 웜홀 탐지 방법은 공격노드가 웜홀을 이용하여 비용이 적게 드는 경로를 만들기 위해서는 자신의 이웃노드에 대한 정보를 속여야만 한다는 점에 착안하고 있다.

네트워크의 모든 노드는 자신의 이웃 노드 리스트를 가진다. 이 리스트에는 자신의 이웃 노드들의 아이디와 위치정보가 담겨 있다.

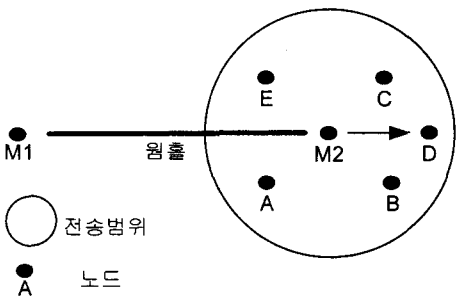


<그림 4> 이웃 노드 탐지 과정

<그림 4>는 A와 C라는 노드가 이웃노드인 관계에 있을 때 B노드가 A와 C의 이웃노드로 네트워크에 참가하는 모습을 나타내고 있다. B 노드는 네트워크에 처음 참가하거나 자신의 위치를 이동한 뒤에 네트워크에 재 참가 할 때 자신의 주변노드들에게 HELLO 패킷을 브로드캐스트(broadcast)한다. 이 패킷을 받은 B의 인근노드 C는 응답으로 자신의 이웃노드 리스트를 보낸다. 이 과정은 A에게도 마찬가지로 적용된다. B는 이렇게 이웃노드들로부터 받은 리스트들을 취합하고, 이를 다시 주변 노드들에게 브로드캐스트한다. 이 과정을 통하여 노드 A와 C는 B의 이웃노드들에 대한 리스트를 얻을 수 있고 해당 노드들의 아이디와 실제 위치를 알 수 있다. 그리고 이 리스트의 신뢰도를 검사하기 위해 리스트에 있는 노드들 중 자신의 전송범위 안에 있는 노드들을 추려내어 PROVE 패킷을 전송함으로써 실제 그 위치에 있는지를 검사한다. <그림 5>에서는 A가 C에게 PROVE 패킷을 보내고 있다. 만약 PROVE 패킷에 대한 응답을 패킷의 최대 왕복 시간인 2 X T_t 시간 내에 받지 못하거나 지정된 위치에 해당 노드가 존재하지 않는다면 노드 A는 노드 B와 리스트에 지정된 노드인 C를 이상노드로 판단하고 이웃 노드들에게 경보 메시지를 보낸다. 이렇게 함으로써 악의적인 노드가 자신의 이웃에 있지 않은 노드를 이웃으로 알리는 것을 방지할 수 있다.

3.3 웜홀 공격 탐지

위의 이웃노드 탐지 방법을 통해 노드는 자신의 이웃 노드들의 위치를 알 수 있다. 각 노드는 이 정보를 이용하여 자신의 이웃노드들이 이상행동을 하는지를 감시해야 한다.



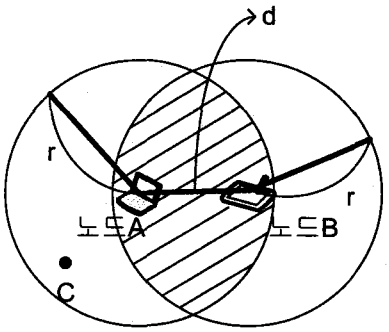
<그림 5> 웜홀을 이용한 메시지 전달

<그림 5>는 인근 노드 모니터링의 전반적인 방법을 나타내고 있다. 기본적으로 각 노드는 자신의 전송범위 내에 있는 노드가 보내거나 전달하는 RREQ, RREP 메시지를 청취한다. 노드 M1과 M2는 웜홀 공격 노드로써 사전에 정의된 터널을 이용하여 빠른 속도로 메시지를 주고받을 수 있다. 만약 M2가 D에게 S-M1-M2 라는 경로를 전달하려 한다면 3.1의 가정에 따라 M2는 M1의 위치를 메시지에 담아 보내야 한다. 무선 애드혹 네트워크의 특성상 이 메시지는 D 뿐만이 아니라 M2의 이웃 노드들에게 전해지고, 해당 노드들은 자신이 가지고 있

는 이웃노드 리스트에 들어있는 정보와 비교를 하여 경로에 포함되어 있는 노드들의 위치가 올바른지를 검사한다. 위의 경우 M1의 위치가 이웃노드들의 전송 범위 안에 있지 않고, 만약 그 위치를 속여서 전송한다면 이웃노드들의 실제 위치검사로 그 진위여부를 파악할 수 있고, 실제 M1의 위치를 그대로 전송한다면 단순한 거리계산으로 M1이 M2의 이웃이 아님을 알 수 있음으로 웜홀 공격이 실행되고 있음을 알 수 있게 된다.

4. 제안 기법 분석

3절을 통해 웜홀 공격이 발생하였을 때 그것을 어떻게 탐지하는 지에 대해 알아보았다. 4절에서는 본 논문에서 제안한 방법의 성능에 대해 분석하고 있다.



<그림 6> 웜홀의 탐지가 가능한 범위

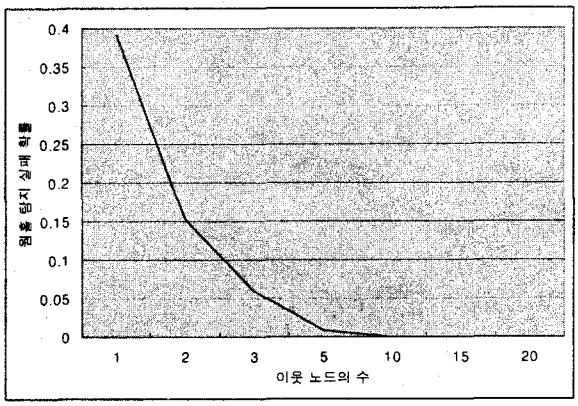
3절에서 제안한 웜홀 탐지 기법은 이웃노드들에 대한 정보교환을 바탕으로 하고 있다. 이는 웜홀 공격을 시도하는 노드의 이웃노드들이 존재해야 공격을 탐지 해 낼 수 있다는 것이다. <그림 6>에서 r은 각 노드 전송 범위의 반지름, d는 두 노드사이의 거리를 나타낸다. 만약 노드 A가 웜홀을 생성하였을 경우 B에게는 웜홀을 생성한 상대 노드의 위치를 자신의 이웃 노드인 것처럼 위장해야 한다. 그 위치는 <그림 6>에서의 C 위치이다. 이 경우 노드 B가 탐지할 수 없기 위해서는 <그림 6>에서의 사선으로 표현된 부분에 C가 위치하지 않아야 한다. 즉 위의 그림에서 노드 A가 노드 B에게 탐지되지 않고 웜홀을 생성할 확률은 노드 A의 넓이와 사선으로 표현된 부분의 넓이를 확률로 표현한 값과 같다. 그런데 여기서 최악의 경우는 <그림 6>에서 사선으로 표현되는 부분이 가장 작은 경우인 d와 r의 값이 같을 때이므로 이것을 가정한다면 식은

$$2\left(\frac{1}{3}\pi r^2 - \frac{1}{2}r^2\sin(120)\right)\times\frac{1}{\pi r^2} = \frac{2}{3} - \frac{\sin(120)}{2\pi}$$

이 된다. 이는 A의 실제 이웃노드가 1개일 때를 가정한 것이고 만약 A의 이웃노드가 n개라면 웜홀 공격이 탐지되지 않을 확률은 다음과 같다.

$$\left(\frac{2}{3} - \frac{\sin(120)}{2\pi}\right)^n$$

<그림 7>은 이것을 n 값에 따른 확률을 도표로 정리한 것이다.



<그림 7> 이웃 노드 수에 따른 웜홀 탐지 확률

위의 <그림 7>에서 알 수 있듯이 이웃 노드의 개수가 2개가 넘어가는 시점부터 웜홀 공격 탐지 실패 확률이 크게 감소되고 있다. 이는 이웃노드가 2개 이상일 경우 이웃 노드들로 인하여 자신의 전송범위가 대부분 감지되고 있기 때문이다.

5. 결론 및 향후 과제

지금까지 애드혹 네트워크에서 발생할 수 있는 웜홀 공격에 대한 탐지방법에 대해 설명하였다. 현재의 통신 시장이 무선을 지향하고 있으며, 고정된 네트워크보다는 휴대전화, 노트북, PDA등을 통한 무선의 노드들 사이의 네트워크 구성이 필요한 시대로 접어들고 있기에 애드혹 네트워크는 그 필요성이 어느 때 보다도 커지고 있는 추세이다. 이에 따라 애드혹 네트워크에 대한 여러 공격방법들이 나오고 있고, 공격방법들에 대한 뚜렷한 해결책이 제시되지 못한 것들 중 하나가 웜홀 공격이다.

본 논문에서는 그 해결책으로 이웃 노드 정보를 이용한 웜홀의 탐지방법을 제안하고 있으며, 이 방법은 이웃노드와 두 홉 거리 노드의 위치정보 이외에는 어떠한 다른 정보가 필요하지 않기에 다른 탐지 방법보다 경제적이라는 장점이 있다. 그리고 이웃 노드가 많은 밀집된 네트워크의 경우 상당히 높은 탐지율을 기대할 수 있다.

다만 제안된 시스템 상에서는 경로의 탐색이 이루어질 때마다 모든 RREQ, RREP 패킷의 검사가 이루어 져야 하기 때문에 각 노드에 상당한 부하가 걸릴 위험이 있으며 이는 앞으로 해결해 나가야 할 과제이다.

6. 참고문헌

[1] L. Zhou and Z. J. Haas. "Securing ad hoc networks. IEEE Network", 13(6):24-30, 1999.

[2] Milanovic N., Malek M., Davidson A., Milutinovic V. "Routing and Security in Mobile Ad Hoc Networks", IEEE Computer, February 2004.

[3] Yih-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy Volume 2 Issue 3 28-39, May 2004

[4] R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya. "Using directional antennas for medium access control in ad hoc networks". In Proc. of ACM MOBICOM, Sept. 2002.

[5] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", In Proceedings of IEEE INFOCOM 2003, pp.1976-1986, April 2003

[6] Hon Sun Chiu, King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", In Proceedings of Wireless Pervasive Computing 2006 1st International Symposium, pp.1-6, Jan 2006

[7] Issa Khalil, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05) - Volume 00, 2005

[8] Asad Amir Pirzada, Chris McDonald, "Detecting and Evading Wormholes in Mobile Ad-hoc Wireless Networks", International Journal of Network Security Vol.3, pp.191-202, 2006