센서 네트워크에서 AODV 라우팅 정보 변조공격에 대한 분석

이 명 진[†] · 김 미 희[††] · 채 기 준[†††] · 김 호 원[††††]

요 약

센서 네트워크는 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크 중의 하나로 그 중요성이 점차 부각되고 있으며, 네트워크 특성상 보안 기술 또한 기반 기술과 함께 중요하게 인식되고 있다. 현재까지 진행된 센서 네트워크 보안 기술은 암호화에 의존하는 인증 구조나 키 관리 구조에 대한 연구가 주를 이루었다. 그러나 센서 노드는 쉽게 포획이 가능하고 암호화 기술을 사용하는 환경에서도 키가 외부에 노출되기 쉽다. 공격자는 이를 이용하여 합법적인 노드로 가장하여 내부에서 네트워크를 공격할 수 있다. 따라서 네트워크의 보안을 보장하기 위해서는 실행 가능한 내부 공격 및 그 영향에 대한 분석이 필요하며 이를 통해 내부 공격에 대비한 안전한 메커니즘이 개발되어야 한다. 본 논문에서는 애드혹 네트워크의 대표적인 라우팅 프로토콜이며, 센서 네트워크에서도 적용 가능한 AODV (Ad-hoc On-Demand Distance Vector) 프로토콜 분석을 통해 라우팅시 가능한 내부 공격을 모델링하고 이를 탐지할 수 있는 메커니즘을 제안하였다. 모델링한 공격은 AODV 프로토콜에서 사용하는 메시지를 변조하여 정상 노드들이 공격자를 통한 경로를 선택하게 만드는 것을 목표로 한다. 이러한 공격은 패킷스니핑 및 선택적 혹은 전 트래픽의 필터링과 변조 공격의 기본이 될 수 있다. 시뮬레이션을 통해 내부 공격이 정상 트래픽에 미치는 영향을 분석하였고, 홉수 정보를 이용한 간단한 탐지 메커니즘을 제안하였다.

키워드 : 센서 네트워크, 내부 공격 모델, 공격 탐지, AODV, 라우팅 정보 변조 공격

Analysis of the Bogus Routing Information Attacks in Sensor Networks

Myungjin Lee[†] · Mihui Kim[††] · Kijoon Chae[†††] · Howon Kim[††††]

ABSTRACT

Sensor networks consist of many tiny sensor nodes that collaborate among themselves to collect, process, analyze, and disseminate data. In sensor networks, sensor nodes are typically powered by batteries, and have limited computing resources. Moreover, the redeployment of nodes by energy exhaustion or their movement makes network topology change dynamically. These features incur problems that do not appear in traditional, wired networks. Security in sensor networks is challenging problem due to the nature of wireless communication and the lack of resources. Several efforts are underway to provide security services in sensor networks, but most of them are preventive approaches based on cryptography. However, sensor nodes are extremely vulnerable to capture or key compromise. To ensure the security of the network, it is critical to develop security mechanisms that can survive malicious attacks from "insiders" who have access to the keying materials or the full control of some nodes. In order to protect against insider attacks, it is necessary to understand how an insider can attack a sensor network. Several attacks have been discussed in the literature. However, insider attacks in general have not been thoroughly studied and verified. In this paper, we study the insider attacks against routing protocols in sensor networks using the Ad-hoc On-Demand Distance Vector (AODV) protocol. We identify the goals of attack, and then study how to achieve these goals by modifying of the routing messages. Finally, with the simulation we study how an attacker affects the sensor networks. After we understand the features of inside attacker, we propose a detect mechanism using hop count information.

Key Words : Sensor Network, Inside Attack, Attack Detection, AODV, Bogus Routing Information

1. 서 론

유비쿼터스 컴퓨팅 환경의 기본이 되는 기반 기술로서 센서 네트워킹 기술의 중요성이 점차 강조되고 있다. 센서 네트워크는 광범위하게 설치되어 있는 유무선 네트워크 인프라에 상황인지를 위한 다양한 센서를 통해 감지된 데이터를 응용 서비스 서버와 연동하는 기술이다. 이러한 센서 네트워킹 기술은 네트워크의 보안이 보장되지 않고서는 유비쿼터스 컴퓨팅 사회의 실현을 위한 기반 기술로서 실용화가 될 수 없다. 즉, 센서 네트워크의 기반 기술 개발뿐만 아니라 센서를 통해 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성·지원사업 및 한국전자통신연구원(ETRI)의 지원을 받아 수행되었음.
† 준 회 원 : 이화여자대학교 컴퓨터학과 석사
†† 정 회 원 : 이화여자대학교 컴퓨터학과 박사후과정연구원
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
†††† 정 회 원 : 한국전자통신연구원 정보보호연구단 선임연구원/팀장
논문접수 : 2006년 12월 4일, 심사완료 : 2007년 4월 20일

네트워크 상에서의 보안 메커니즘 개발이 반드시 함께 연구되어 적용되어야 한다.

센서 네트워크는 기본적인 특성으로 인해 기존 네트워크에서 보다 훨씬 많은 내부 공격 및 외부 공격이 존재하여 보안이 더욱 취약하다는 문제점을 갖는다. 특히 내부 공격의 경우 노드가 오염되어 공격자에 의해 악용될 수 있으며 이 경우 그 피해는 더욱 심각해진다. 내부 공격으로부터 네트워크를 보호하기 위해서는 먼저 내부 공격자가 센서 네트워크에 어떠한 영향을 미치는지에 대해 알아볼 필요가 있다[1]. 현재 센서 네트워크 환경에서 다양한 공격에 대한 연구가 활발하게 진행되고 있지만 내부 공격에 대한 연구는 아직 미흡하다.

본 논문에서는 애드 혹 네트워크의 대표적인 라우팅 프로토콜이며 센서 네트워크에서도 적용 가능한 AODV (Ad-hoc On-Demand Distance Vector) 프로토콜 분석을 통해 라우팅시 가능한 내부 공격을 모델링하고 또한 이를 간단하게 탐지할 수 있는 메커니즘을 제안하였다.

AODV 프로토콜에서 사용하는 메시지에서 공격자가 변경 가능한 필드를 살펴보고 필드를 변경했을 때 미칠 수 있는 영향에 대해 살펴보았다. 또한 이들 중 다른 노드들로 하여금 공격자를 통한 경로를 선택하게 만들 수 있는 필드를 선택하여 공격자를 모델링하고 이러한 공격자가 있을 때 네트워크가 받는 영향에 대한 시뮬레이션을 NS-2 시뮬레이터를 이용하여 수행하였다. 시뮬레이션을 통해 공격자가 존재할 경우, 공격자를 지나가는 트래픽 양의 변화에 대해 살펴보고, 어떤 위치에서의 공격이 효율적인지 분석해 본다. 이와 함께 공격자를 지나가는 트래픽의 패킷 전송 지연 시간의 변화도 살펴본다.

본 논문의 결과를 이용하여 센서 네트워크 보안 기술에 관한 연구를 진행할 때 내부 공격의 특성을 고려하여 내부 공격이 존재할 경우에도 안전한 프로토콜을 제안하는데 도움이 될 것으로 예상된다. 본 논문은 다음과 같은 순서로 구성되어 있다. 1장의 서론에 이어서 2장에서는 AODV 프로토콜에 대해 살펴보고 센서 네트워크에서 가능한 공격 유형에 대해 분석한다. 3장에서는 AODV를 이용한 라우팅 정보 변조 공격 모델링 방법에 대해 살펴본다. 4장에서는 공격 모델이 네트워크에 미치는 영향에 대한 분석을 위한 시뮬레이션 환경 및 시나리오를 설명하고 그 결과를 분석한 후 5장에서는 본 논문의 결론과 향후 연구 방안에 대하여 기술한다.

2. Ad hoc On-Demand Distance Vector 라우팅 프로토콜[2]

AODV는 라우팅 정보를 얻고자 할 때 경로를 찾는 과정을 수행하는 "On-demand Routing Protocol" 이다. 근원지 노드가 목적지 노드에게 데이터 패킷을 보내고자 할 때, 자신의 라우팅 테이블에 목적지 노드에 대한 정보가 없으면 주위 노드들에게 RREQ (Route Request) 메시지를 브로드캐스트한다. RREQ를 받은 노드는 자신의 라우팅 테이블에 목적지 노드에 대한 유효한 정보가 없으면 자신의 이웃 노드들에게 RREQ를 다시 브로드캐스트한다. 이러한 과정은 RREQ 메시지가 목적지 노드에 도착하거나 혹은 목적지 노드까지의 유효한 라우팅 정보를 가지고 있는 중간 노드에 도착할 때까지 계속된다.

RREQ를 받은 목적지 노드나 중간 노드는 근원지 노드에 대한 "Reverse Route"를 업데이트한다. 자신에게 RREQ를 보낸 이웃 노드를 근원지 노드에 대한 경로의 다음 노드로 설정한다. "Reverse Route"은 근원지 노드로 RREP (Route Reply) 메시지를 보내기 위해서 사용된다. 또한 근원지 노드에 대한 시퀀스 번호를 자신의 라우팅 테이블 안의 시퀀스 번호와 RREQ의 시퀀스 번호 중 큰 값으로 업데이트한다.

근원지 노드나 중간 노드는 RREP 메시지를 받으면 RREP 메시지를 자신에게 보내준 이웃 노드를 목적지 노드에 대한 다음 노드로 하여 "Forward Route"를 업데이트한다. RREQ 메시지를 받았을 때와 비슷하게 목적지 노드에 대한 시퀀스 번호도 자신의 라우팅 테이블 안의 값과 RREP 안의 값중 큰 값으로 업데이트한다.

RREQ 메시지와 RREP 메시지와 함께 RREP 메시지의 수신을 확인하기 위해 RREP-ACK (Route Reply Acknowledgment) 메시지도 사용된다.

또한 AODV는 경로 관리를 위해서 RERR (Route Error) 메시지도 사용한다. 만약 어떤 노드가 망가진 링크를 탐지하면, 망가진 링크를 이용하는 업스트림 노드들에게 RERR 메시지를 전송한다. 노드가 자신의 이웃으로부터 RERR 메시지를 받으면 자신의 업스트림 노드들에게 RERR 메시지를 전달한다.

결론적으로 노드들은 자신의 이웃 노드들로부터 RREQ, RREP, RRER 메시지를 받을 때마다 라우팅 정보를 업데이트 하게 된다.

3. 센서 네트워크에서의 공격 유형 분석

다음은 센서 네트워크에서 가능한 공격 유형이다.

- Bogus routing Information[3][4][5]

라우팅 메시지를 스푸핑, 변경 또는 재전송하여 라우팅을 교란시켜서 에러를 고의로 발생시키거나 라우팅 루프를 형성하거나 라우팅 정보의 전송을 지연시킴으로써 통신을 방해하는 공격이다. 예를 들어 공격자가 "자신이 목적지까지 가장 짧은 경로에 있고, 높은 전력을 가졌다" 와 같은 내용으로 다른 노드들에게 선전하는 방법으로 트래픽을 자신에게 유인할 수 있다.

이 공격으로 인해 네트워크 상에서 라우팅 효율성이 떨어지고, 루프가 형성되는 경우 토폴로지 구성에 영향을 미쳐 네트워크 분할을 유도할 수 있을 것으로 예상된다.

- Selective Forwarding[3][4][5]

특정 메시지에 대한 전달을 거부하거나 삭제하는 공격이다.

간단한 선택적 포워딩 공격의 형태로 공격자 노드가 자신에게 오는 모든 패킷의 전송을 거부하는 것이 가능하여 마치 블랙 홀처럼 행동하는 것이다. 그러나 이러한 공격은 주변 노드가 공격자 노드에게 문제가 있다는 것을 알 수 있어서 효율적으로 공격할 수 없다. 공격자 노드에 문제가 있다는 것을 감지한 노드들은 공격자를 제외한 다른 경로를 찾을 수 있다. 조금 더 복잡합 형태의 선택적 포워딩은 선택적으로 공격자에 오는 패킷을 전송한다. 모든 패킷을 공격하지 않고 선택한 몇몇 노드에서 발생하는 패킷에 대해서만 삭제하거나 수정한다. 이 같은 형태는 주변 노드들에 의해 쉽게 감지 되지 않는다.

선택적 포워딩 공격은 공격자가 확실하게 경로에 속할 때 가장 효과적이다. 따라서 이 공격을 시도하는 공격자는 경로에 자신을 속하게 하려고 라우팅 정보 변조 공격을 이용할 수 있다.

▪ Wormholes[3][4][5]

실제로는 존재하지 않는 노드 연결이 있는 것처럼 인식하게 하여 한쪽 네트워크에서 받은패킷을 다른 쪽 네트워크로 전달한다. 이 공격은 엿듣기 공격이나 선택적 포워딩과 같이 활용된다. 두개의 공격자 노드가 서로 떨어진 거리를 다른 노드들에게 실제보다 짧게 보이게 하기 위해 협력한다. 이를 위해 공격자만 사용할 수 있는 채널을 이용해 패킷을 중계하는 방법을 사용한다. 이 방법으로 실제 떨어진 거리보다 짧게 보이게 할 수 있다.

▪ Shinkholes[6]

라우팅 정보 변조 공격과 같이 사용하여 라우팅 정보를 변경하여 공격자의 노드로 모든 데이터들이 지나가도록 조작하여 엿듣기가 가능한 공격이다. 공격자는 자신이 베이스 스테이션 (혹은 싱크 노드)로 가는 최단 경로라고 광고하여 다른 트래픽들을 공격자로 이끈다. 이를 통해 공격자를 통해 가는 패킷들의 베이스 스테이션 (혹은 싱크 노드)로의 전송을 막는다. 이 공격은 다른 공격에 비해 발견하기 쉽지만, 공격이 이루어지면 네트워크를 붕괴시키기 쉽다.

▪ HELLO Floods[3][7]

멀리 있는 공격자가 강한 강도의 신호로 HELLO 패킷을 보냄으로써 가까운 곳에 위치하지 않는 공격자에게 패킷을 보내도록 하는 공격이다. 공격자로부터 HELLO 패킷을 받은 노드는 HELLO 패킷을 보낸 노드가 자신의 이웃 노드라고 판단하게 되어 공격자에게 정보를 보낸다. 이 공격으로 인해서 정상 노드들이 자신의 이웃이라고 믿고 있는 공격자에게 패킷을 보내려고 시도하게 되지만 전달되지 않거나 전달된 패킷은 공격자에 의해 삭제되어 네트워크가 혼란에 빠지게 된다.

▪ Sybil Attack[8][9]

하나의 노드가 다른 노드에게 여러 식별자로 인식하도록 하는 공격으로 지역적 정보를 이용하는 라우팅 (geographic routing)에서 치명적이다. 공격자 노드가 ID를 생성하는 방법은 크게 두가지로 나눌 수 있다. 하나는 ID를 단순히 만들어 사용하는 것이고, 다른 하나는 정상 노드의 ID를 훔쳐서 사용하는 것이다. 어떤 방법을 사용할 것인지는 노드가 자신의 ID를 어떻게 생성하는 지에 따라 다르다. 어떠한 메커니즘에 의해 노드 ID가 만들어 지는 센서 네트워크에서 다른 노드의 ID를 훔쳐서 사용하는 경우에는 MAC의 헤더 부분에 주소 필드에서 다른 노드의 주소를 획득할 수 있다.

Sybil 공격으로 인하여 데이터를 통합하는 네트워크나 노드들이 투표를 통해 어떤 일을 결정하거나 노드 당 자원을 할당하는 경우에 수행이 제대로 이루어 지지 못할 것으로 예상된다.

▪ DoS(Denial of Service) Attack[10][11][12]

네트워크를 무너뜨리고, 파괴하려는 공격자의 시도뿐만 아니라, 주어진 기능을 수행하기 위한 네트워크의 "Capacity"를 줄이거나 없애기 위한 모든 공격을 서비스 거부 공격이라 한다. 간단한 형태의 서비스 거부 공격은 쓸모없는 여분의 패킷을 희생자 노드에게 보내서 정상적인 네트워크 사용자들이 서비스와 자원을 접근하는 것을 막고, 희생자 노드의 자원을 고갈시킨다.

센서 네트워크에서는 각각의 계층에서 다양한 형태의 서비스 거부 공격이 수행 가능하다. <표 1>은 계층별로 가능한 공격 유형과 그에 따른 방어 기술이다[12].

이 밖에도 LR-WPAN(Low Rate Wireless Personal Area Network)[13]기반의 센서 네트워크에서는 WPAN의 MAC 헤더를 이용한 공격이나 CSMA-CA 메커니즘을 이용한 공격[14]이 가능하다.

MAC 헤더의 프레임 컨트롤 필드 중 프레임 펜딩은 송신자가 수신자에게 더 보낼 데이터가 있을 때 사용한다. 이것이 1로 설정되어 있으면 수신자는 새로운 데이터 요청 커맨드를 전송하게 된다. 공격자는 중간에서 설정된 것을 바꾸어 보낼 수 있다. 1로 설정 된 값을 0으로 보내는 경우 수신자는 자신이 받을 데이터가 있다는 것을 알 수 없고 송신자는 보낼 데이터를 계속 유보하고 있어야 한다. 반대로 0으로 설정된 값을 1로 설정하여 보내게 되면 수신자는 새로운 데이터 요청 커맨드를 전송한 뒤 응답을 기다리지만 송신자는 자신이 보낼 데이터가 없기 때문에 무시하게 된다.

공격자는 MAC 헤더의 프레임 컨트롤 필드 중 ACK Request 필드 값도 중간에서 변경할 수 있다. 1로 설정된 값을 0으로 바꾸어 보내게 되면 송신자는 ACK을 요청하였기 때문에 ACK을 기다리다가 응답이 안 오면 재시도를 하게 된다.

CSMA-CA 메커니즘에 따르면 데이터를 전송 시 채널의 상태를 2번 확인하고 2번 모두 채널이 비어 있는 경우 데이터 전송을 시작하게 되어 있다. 공격자는 채널 확인을 한번만 하여 다른 노드들 보다 채널 점유율을 높일 수 있다. 이

〈표 1〉 계층별 DoS 공격 유형 및 방어 기술

계층	공격	간단한 방어 기술
물리적 계층	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
링크 계층	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
네트워크 및 라우팅 계층	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring, redundancy
전송 계층	Flooding	Client puzzles
	Desynchronization	Authentication

에 따라 정상 노드들의 데이터 전송을 방해하고 정상 노드의 에너지를 낭비 시킬 것이라고 예상된다. 또한 전체 네트워크의 대역폭도 낭비가 될 것으로 예상된다.

이처럼 센서 네트워크에서 가능한 공격은 다양하다. 여러 공격 중 라우팅 정보 변조 공격은 다른 공격의 기본이 된다. 특히 라우팅 정보를 변경하여 다른 노드들이 공격자가 목적지 노드까지 최단 경로를 제공하는 것처럼 생각하게 만들어 목적지 노드까지의 경로상에 공격자를 위치시키는 공격을 이용하면 다른 공격들을 쉽게 적용할 수 있다. 네트워크 상에 공격자의 영향을 받는 트래픽의 양을 증가 시킬 수 있기 때문이다. 따라서 이와 같은 라우팅 정보 변조 공격이 네트워크 상에 있을 때 네트워크에 일어나는 변화에 대한 연구가 필요하다.

4. AODV 라우팅 정보 변조공격에 대한 분석 및 탐지 메커니즘

4.1. 라우팅 정보 변조공격 모델링

라우팅 경로가 설정될 때 라우팅 정보를 변조하여 이웃 노드들로 하여금 공격자를 통하면 목적지 노드로 더 빨리 갈 수 있다고 유혹하여 공격자를 포함하는 라우팅 경로를 설정하게 하는 것을 목표로 하는 라우팅 정보 변조 공격을 모델링하고 탐지할 수 있는 방법을 제안한다. 이러한 공격은 2장에서 살펴보았듯이 다른 공격들의 기본이 된다. 라우팅 경로에 공격자가 포함되면 지나가는 패킷 정보를 모두 엿들을 수 있고, 이러한 패킷 정보를 이용하여 다른 노드들의 식별자를 알아내 Sybil Attack에도 이용할 수 있다. 또한 공격자를 지나가는 특정 메시지에 대한 전달을 거부하거나 삭제하는 선택적 포워딩 공격으로 이어질 수도 있다.

AODV를 이용하여 내부 공격으로 라우팅 정보 변조 공격을 모델링 하기 위하여 공격자 모듈이 AODV에서 사용하는 메시지 중 RREQ와 RREP 메시지의 어떤 필드를 변경할지를 결정해야 한다. <표 2>는 RREQ 메시지 중 공격자가 변경할 수 있는 필드이다.

변경 가능한 필드 중 주위 노드들이 공격자를 포함하는 패스가 더 빠른 길이라 믿게 만드는 것은 RREQ ID의 증가, 홉 수(Hop Count)의 감소, 목적지 노드에 대한 시퀀스 번호(Destination Sequence Number)의 증가, 근원지 노드에 대한 시퀀스 번호(Originator Sequence Number)의 증가 이렇게 네 가지이다.

RREQ ID는 근원지 IP 주소와 함께 RREQ 메시지를 식별할 수 있게 한다. 이를 통해 노드는 자신이 받은 RREQ가 이전에 받았던 RREQ인지 새로운 RREQ인지를 판단할 수

〈표 2〉 공격자에 의해 변경 가능한 RREQ 메시지의 필드

RREQ 메시지 필드	가능한 변경 사항
Type	메시지 타입을 RREP, RRER로 변경 가능
RREQ ID	변경한 RREQ 메시지를 유효하다고 생각하게 증가하거나 유효하지 않다고 생각하게 감소
Hop count	다른 노드들이 "Reverse Route"을 업데이트하게 감소하거나 업데이트 메시지를 무시하게 증가
Destination IP address	다른 IP 주소로 변경
Destination Sequence Number	다른 노드들이 "Forward Route"을 업데이트하게 증가하거나 업데이트 메시지를 무시하게 감소
Originator IP Address	다른 IP 주소로 변경
Originator Sequence Number	다른 노드들이 "Reverse Route"을 업데이트하게 증가하거나 업데이트 메시지를 무시하게 감소
Flags	역으로 셋팅

있다. 주위 노드들로부터 같은 RREQ를 여러 번 받을 수 있지만 식별자를 이용하여 중복하여 받은 RREQ는 버린다. 공격자는 RREQ ID를 이용하여 다른 노드들에게 수정한 RREQ를 받아드리게 할 수 있다. 하지만 이러한 공격은 공격자가 근원지 노드의 1 홉 이내에 있을 경우에만 가능하다. 그렇지 않은 경우에는 공격자에게 RREQ 메시지를 전송한 노드도 공격자가 변경한 RREQ 메시지를 받고 자신의 라우팅 테이블을 변경하기 때문에 라우팅 루프가 발생하여 경로가 망가지게 된다. 또한 이것은 AODV의 메커니즘에 의해 쉽게 탐지가 가능하며 AODV 메커니즘에 따라 결국 공격자를 제외한 길을 선택하게 된다.

AODV 알고리즘에 따르면 RREQ 메시지를 받은 후 노드는 RREQ 메시지 안에 있는 근원지 노드에 대한 시퀀스 번호 값이 자신의 라우팅 테이블 안에 있는 값보다 크거나 시퀀스 번호 값은 같지만 RREQ 메시지 안에 홉 수 값이 라우팅 테이블 안의 값보다 작으면 근원지 노드에 대한 라우팅 정보 값을 업데이트한다. 공격자는 이를 변경하여 다른 노드들의 라우팅 테이블에 영향을 미칠 수 있다.

목적지 노드가 RREQ 메시지를 받으면 RREQ 메시지 안에 목적지 노드에 대한 시퀀스 번호 값과 자신의 라우팅 테이블 안에 값을 비교하여 둘 중 큰 값으로 시퀀스 번호를 업데이트 한다. 이를 이용하여 공격자가 RREQ 메시지 안의 목적지 노드에 대한 시퀀스 번호 값을 증가시켜서 목적지 노드가 이 값으로 업데이트하게 만들 수 있다.

공격자는 RREQ 메시지 안의 플래그의 설정을 변경할 수도 있다. 예를 들어 "D" 플래그가 설정되어 있는 RREQ 메시지라면 근원지 노드가 목적지 노드에게만 RREP 메시지를 요청한 것이지만, 플래그의 설정을 해지하여 중간노드들도 모두 RREP 메시지를 전송하게 할 수 있다. 이때 근원지 노드는 RREP 메시지가 목적지 노드로부터 온 것인지 중간 노드로부터 온 것인지 구별할 수 없다.

본 논문에서는 RREQ 메시지 안에 변경할 수 있는 필드 중 공격모델에서는 RREQ ID를 제외한 홉 수의 감소, 목적지 노드에 대한 시퀀스 번호의 증가, 근원지 노드에 대한 시퀀스 번호의 증가 이렇게 세 가지를 이용한다. RREP 메시지에는 RREQ 메시지에 없던 새로운 필드를 포함하고 있다. 라이프타임 필드는 RREP메시지에 의해 업데이트 된 라우팅 정보의 유효한 시간을 나타낸다.

RREP 메시지를 신뢰할 수 없는 노드로부터 받은 경우에는 송신자가 "A" 플래그를 설정해서 보낼 수 있는데 이런 경우 수신자는 송신자에게 메시지를 받았다는 확인으로 RREP-ACK 메시지를 보내야 한다. Prefix Size 필드는 서브넷안에서 쉽게 패스를 설정할 수 있도록 도와준다. 공격자는 이러한 필드를 이용하여 네트워크에 영향을 미칠 수 있다. RREP 메시지 안에 변경 가능한 필드 중 주위 노드들이 공격자를 포함하는 패스가 더 빠른 길이라 믿게 만드는 것은 홉 수의 감소, 목적지 노드에 대한 시퀀스 번호의 증가이다.

AODV 알고리즘에 의하면 RREQ를 받은 노드는 다음의 세가지 중 하나의 상태이다.

- 자신이 목적지인 경우
- 목적지는 아니지만 목적지까지의 라우팅 정보를 알고 있는 경우
- 목적지도 아니고 목적지까지의 라우팅 정보도 모르는 경우

RREQ 메시지를 받았을 때 목적지 노드는 아니지만 자신의 라우팅 테이블에 목적지 노드에 대한 정보가 있을 경우에는 라우팅 테이블에 있는 정보를 바탕으로 RREP 메시지를 전송하게 된다. 공격자는 이 때 자신이 가지고 있는 목적지 노드까지의 홉 수를 1이상 감소하고 시퀀스 번호도 2의 배수로 증가하여 전송하게 모델링하여 다른 노드들에게 목적지와 가까운 노드인 것처럼 위장할 수 있다. 시퀀스 번호를 2의 배수로 증가하는 이유는 AODV 알고리즘에 따라 시퀀스 번호 값이 홀수이면 유효하지 않은 정보로 판단하고 그 패킷을 버리기 때문이다.

목적지 노드도 아니고 목적지 노드에 대한 라우팅 정보가 없을 경우에는 자신이 받은 RREQ 메시지를 바탕으로 소스 IP 주소를 자신의 주소로 변경하고 RREQ의 홉 수에서 1을 증가하여 RREQ 메시지를 다시 전달하게 된다. 공격자 노드는 홉 수를 1 증가하는 대신에 1 감소하여 전송할 수 있다. 특별히 1을 감소하는 이유는 2 이상 감소하게 되면 RREQ ID를 증가했을 경우와 마찬가지로 자신에게 RREQ 메시지를 전송한 노드도 목적지 노드에 대한 경로에서 다음 노드

〈표 3〉 공격자에 의해 변경 가능한 RREP 메시지의 필드

RREP 메시지 필드	가능한 변경 사항
Type	메시지 타입을 RREQ, RRER로 변경 가능
Flags	역으로 셋팅
Prefix Size	서브넷의 prefix의 크기를 증가하거나 감소
Hop count	다른 노드들이 "Forward Route"을 업데이트하게 감소하거나 업데이트 메시지를 무시하게 증가
Destination IP address	다른 IP 주소로 변경
Destination Sequence Number	다른 노드들이 "Forward Route"을 업데이트하게 증가하거나 업데이트 메시지를 무시하게 감소
Originator IP Address	다른 IP 주소로 변경
Lifetime	RREP 메시지의 의해 업데이트 되는 라우팅 정보의 라이프타임을 줄이기 위해서 감소시키거나 늘리기 위해 증가

를 공격자로 변경하게 되기 때문이다. (AODV 알고리즘에 따르면 RREQ 메시지를 받았을 때 RREQ 메시지 안의 시퀀스 번호값이 크거나 시퀀스 번호가 같고 홉 수가 작을 때 업데이트를 하게 되어있다.) 따라서 경로 상에 루프가 생기게 되며 AODV 알고리즘에 의해 쉽게 탐지 가능하고 공격자를 제외한 경로를 설정하게 된다. 같은 이유로 시퀀스 번호 값은 변경하지 않는다.

AODV 알고리즘에 의하면 RREP를 받은 노드는 자신이 목적지 노드이면 RREP 패킷을 버리고, 목적지가 아닌 경우에는 RREQ 메시지를 받고 "Reverse Route"를 설정했던 정보를 바탕으로 RREP 패킷을 전달한다. 이 때 자신이 받은 RREP 패킷의 홉 수는 1 증가하고 소스 IP 주소를 자신으로 변경한다. 공격자일 경우에는 RREP 패킷의 홉 수를 1이상 감소하고 시퀀스 번호를 2의 배수로 증가하여 전달한다.

4.2. 홉 수를 이용한 간단한 공격 탐지 메커니즘

이 장에서는 4.1절에서 모델링한 공격자를 탐지하는 메커니즘을 제안한다. 제안하는 메커니즘에서는 두 노드의 ID를 아는 경우에 두 노드 사이의 최단 홉 수를 계산할 수 있다고 가정한다. 이러한 가정 사항은 GRID[15], GPSR[16]와 같은 위치 기반 기술에 관련된 라우팅 프로토콜에서 많이 연구되었고 지금도 연구되고 있기 때문에 무리한 가정은 아니다.

RREQ 메시지나 RREP 메시지를 받은 노드는 패킷의 목적지 노드와 자신에게 메시지를 전달한 중간 노드 사이의 최단 홉 수를 계산한다. 계산한 홉 수와 메시지 안의 홉 수를 비교하여 공격자인지 탐지한다. 만약 메시지 안의 홉 수가 계산한 것보다 작으면 자신에게 메시지를 전달한 중간 노드를 공격자라고 탐지한다. 이러한 방법을 이용하여 공격자 노드를 100% 탐지할 수 있다. 그러나 네트워크의 고장 후의 회복단계에서 관리자에 의해 새로운 노드가 투입이 되거나 고장난 노드가 교체되어 목적지까지의 기존경로보다 더 짧은 경로가 생성된 경우, 이것을 공격으로 잘못 탐지하는 경우가 발생할 수 있다. 이러한 경우 새로운 새로 생성된 최상 경로에 대한 공지나 네트워크 상황을 잘 알고 있는 관리자가 전달받은 공격 탐지 메시지를 무시하여 잘못된 탐지에 대한 피해를 줄일 수 있다.

베이스 스테이션이나 클러스터 헤드와 같은 중앙 관리 노드가 있는 센서 네트워크에서는 공격자를 탐지한 노드가 탐지 메시지를 이러한 관리 노드에게 전송하여 최종적으로 중앙 관리 노드가 공격자 노드를 판단할 수 있게 할 수 있다.

O, N1, A, N2, N3, D 라는 노드가 라우팅 경로상에 차례로 있다고 하자. O는 근원지 노드, N은 일반 노드, A는 공격자 노드, D는 목적지 노드를 의미한다. O 노드로부터 D 노드까지 RREQ 메시지를 통해 경로가 설정되는 동안 A 노드가 N1으로부터 받은 RREQ 메시지의 홉 수 부분을 변조하여 N2에게 전송하면, N2노드는 탐지 메커니즘에 의해 A가 공격자라는 탐지 메시지를 중앙 관리 노드에게 전송하고 RREQ 메시지는 N3에게 전달한다. N3와 D도 N2를 거쳐 A 노드가 변조한 RREQ 메시지를 받으면 N3는 N2가 공격자라는 탐지 메시지를 D는 N3가 공격자라는 탐지 메시지를 중앙 관리 노드에게 전송하게 된다. 이러한 탐지 메시지를 받은 중앙 관리 노드는 탐지 메시지를 종합하여 A 노드가 공격자라는 것을 판단하여 다른 노드들에게 알려 공격자 노드를 제외한 경로를 설정하게 만드는 것도 가능하다.

5. 시뮬레이션 및 결과 분석

시뮬레이션은 NS-2[17]를 기반으로 하여 기존에 카네기 멜론대학의 Monarch 그룹에서 개발한 AODV 모듈[18]을 이용하였다. <표 4>는 시뮬레이션에서 사용한 파라미터 값이다. 25개의 센서 노드가 그리드 토폴리지를 갖는 센서 네트워크를 구성하였고, 모든 시뮬레이션에서는 CBR (Constant bit rate) 트래픽을 사용하였다. 시뮬레이션 공간은 70m x 70m이고, 시뮬레이션은 100초간 지속된다. 노드의 전송 범위(15m) 안에 있는 다른 노드들은 직접적으로 라이오 신호를 수신할 수 있다. 라디오 전파 모델은 Two-Ray 모델을 사용하였다. 시뮬레이션 파라미터 값은 Ad-Hoc 네트워크 기반에서 수행되었던 AODV 프로토콜상 내부 공격자에 대한 연구[1]에서 사용한 파라미터를 참고하였다.

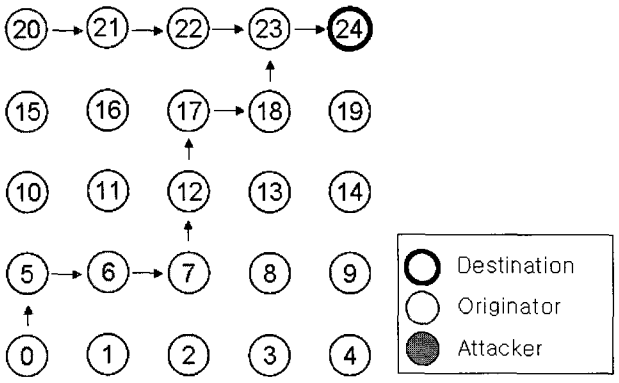
〈표 4〉 시뮬레이션 파라미터

파라미터	값
노드 수	25
내부 공격자 수	1
시뮬레이션 공간	70m x 70m
시뮬레이션 시간	100 초
라디오 전송 범위	15m
라디오 전파 모델	Two-Ray
패킷 전송률	5 pkt/sec
PHY, MAC	802.15.4

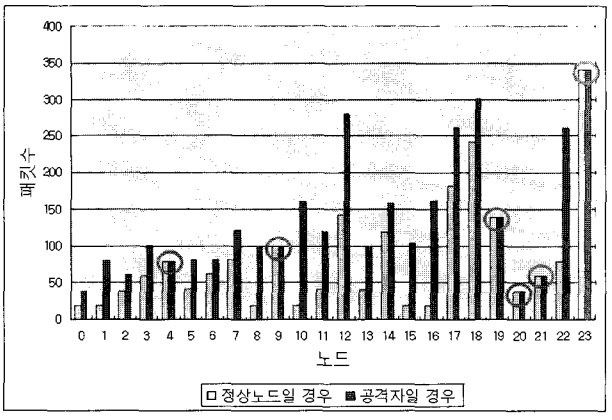
물리 계층과 MAC 계층은 삼성종합기술원과 뉴욕시립대학교에서 IEEE802.15.4를 위해 개발한 WPAN 모듈을 사용하였다. (그림 1)에서 보면 오른 쪽 위에 위치한 24번 노드가 싱크 노드이며, 0번에서 23번의 노드들은 5초마다 CBR 트래픽을 싱크 노드에게 전송한다. 싱크 노드를 제외한 0번 노드에서 23번 노드 중 어떤 노드라도 공격자가 될 수 있다. 또한 AODV 메커니즘의 특성 상 같은 목적지로의 경로는 처음 설정된 경로의 영향을 많이 받는 것으로 판단하여 이와 같은 특성이 공격자가 네트워크안에 존재할 때 어떤 영향을 미치는 지 살펴보기 위하여 시뮬레이션의 첫 트래픽은 0번이 생성한다.

5.1. 라우팅 정보 변조 공격이 네트워크에 미치는 영향 분석

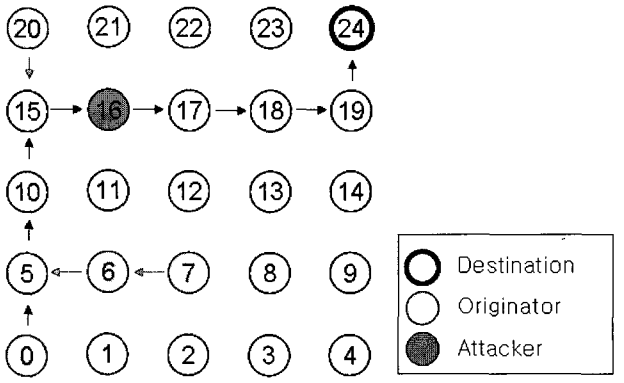
(그림 1)는 공격자가 없을 경우 0번에서 24번으로 가는 경로에 대한 그림이다. 0번에서 24번으로 가는 경로가 0번, 5번, 6번, 7번, 12번, 17번, 18번, 23번, 24번으로 설정된 것을 볼 수 있다. 이 경로 위에 있는 노드들은 자신이 24번으로 CBR



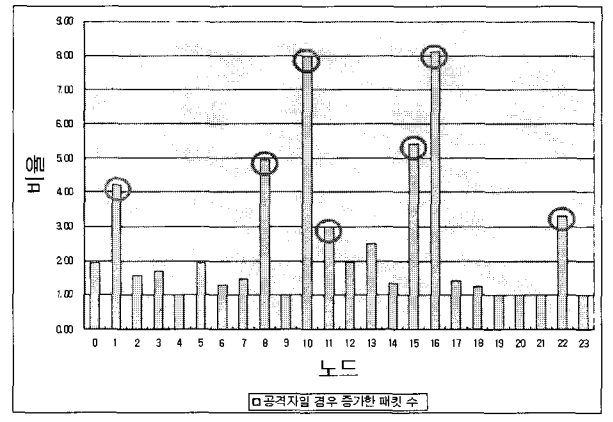
(그림 1) 정상적인 환경에서의 경로 설정



(그림 2) 정상일 경우와 공격자일 경우에 노드를 지나가는 패킷 수



(그림 3) 16번 노드가 공격자일 경우 경로 설정



(그림 4) 공격자 노드일 때 지나가는 패킷의 증가율

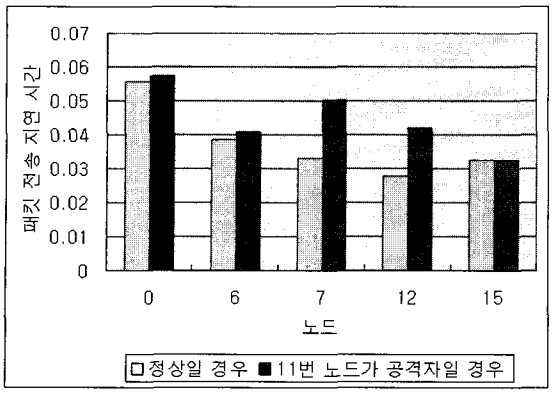
트래픽을 보내야 할 때 이 경로를 그대로 사용하게 된다.

(그림 2)은 0번 노드에서 23번 노드까지 각 노드에 대하여 공격자일 경우와 정상일 경우에 대한 노드를 거쳐가는 패킷 수를 측정한 그래프이다. 거의 모든 노드가 공격자일 경우 지나가는 패킷 수가 크게 증가한 것을 볼 수 있다. 동그라미 표시가 되어 있는 노드들(4번, 9번, 19번, 20번, 21번 23번)의 경우에는 정상일 경우와 공격자일 경우에 노드를 지나가는 패킷 수에 변화가 없다. 여섯 노드는 두 가지 그룹으로 나눌 수 있다. 첫 번째 그룹은 목적지 노드에서 1홉 거리에 있는 19번 노드와 23번 노드이다. 싱크 노드인 24번 노드로 가기 위해서는 19번 노드나 23번 노드를 거쳐야 한다. 따라서 공격자일 경우와 그렇지 않을 경우에 차이가 나타나지 않는 것으로 보인다. 두 번째 그룹은 오른쪽 아래의 4번 노드와 9번 노드 왼쪽 위에 있는 20번 노드와 21번 노드이다. AODV 메커니즘에 따르면 RREQ 메시지를 받았을 경우 자신이 목적지가 아니더라도 목적지로의 라우팅 정보를 알고 있으면 RREP 메시지를 전송하게 되어 있다. 그래서 같은 목적지에게 여러 노드가 패킷을 전송하는 네트워크의 경우에는 처음 결정된 경로에 영향을 많이 받게 된다. 시뮬레이션 시나리오에 따르면 0번 노드부터 CBR 트래픽을 전송하기 때문에 0번 노드가 선택한 경로의 영향을 많이 받게 되는 것이다. 따라서 0번 노드에서 24번 노드로의 대각선에서 멀리 떨어져 있는 노드들의 경우 정상일 경우에 그 노드를 지나가는 패킷의 수는 적게 된다. 또한 이러한 노드가 공격자일 경우에도 영향을 미칠 수 있는 주위 노드의 수가 다른 노드들에 비해 적기 때문에 공격자일 경우에도 큰 영향을 미칠 수 없게 된다.

(그림 3)은 16번 노드가 공격자일 경우에 경로 설정에 관한 그림이다. 정상적인 환경에서 경로를 설정하는 것과 달리 16번 노드가 공격자일 경우에는 0번 노드에서 24번 노드로 가는 경로가 16번 노드를 포함한 0번, 5번, 10번, 15번, 16번, 17번, 18번, 19번, 24번으로 설정되는 것을 볼 수 있다. 이는 이후에도 영향을 미쳐서 6번 노드나 7번 노드, 20번 노드가 24번으로 CBR 트래픽을 보내려 할 때 16번 노드를 포함한 경로를 설정하게 만들게 된다.

이렇게 각 노드가 공격자일 경우 0번 노드에서 처음으로 보내는 CBR 트래픽의 경로에 공격자 노드가 포함될 가능성이 높아지게 된다. 이에 따라 이후에 같은 싱크노드로 향하는 트래픽에 공격자가 영향을 미칠 수 있는 가능성이 더욱 커지게 된다.

(그림 4)는 정상 노드일 경우에 비해 공격자일 경우에 노드를 지나가는 패킷의 증가율에 대한 그래프이다. 11번 노드의 경우, 정상적인 환경에서는 11번 노드를 지나가는 패킷의 수가 40이고 공격자일 경우에는 지나가는 패킷의 수가



(그림 5) 11번 노드가 공격자일 경우 주변 노드들의 패킷 전송 지연 시간

120이다. 이 때의 패킷의 증가율은 3배가 되는 것이다.

3배 이상의 증가율을 보이는 노드는 1번, 8번, 10번, 11번, 15번, 16번, 22번이다. 이 노드들의 공통점을 찾아보면 정상적인 환경에서 0번에서 24으로 가는 경로의 주변 노드들 이라는 것이다.

실험 결과를 살펴 보면, 정상적인 환경에서 처음 설정되는 경로 주변에 위치한 노드들이 공격자로 활동하게 될 경우 공격자가 아닐 때에 비해서 노드들을 지나가는 트래픽의 양이 눈에 띄게 증가하는 것을 알 수 있다.

(그림 5)는 공격자인 노드 주변에 위치한 노드들의 패킷 전송 지연 시간에 대한 그래프이다. 11번 노드가 공격자일 경우 0번 노드에서 24번 노드로 가는 경로는 11번 노드를 포함하는 0번, 5번, 10번, 11번, 16번, 17번, 18번, 19번, 24번으로 설정된다. 11번 노드 주변 노드들 중 이 경로에 속하지 않은 6번, 7번, 12번, 15번 노드의 패킷 전송 지연 시간을 살펴보면 다음과 같다. 7번과 12번 노드의 경우 정상일 경우에 비하여 11번 노드가 공격자일 경우에 패킷 전송 지연

	최대	평균
증가한 패킷 수	8.1	2.56
패킷 증가율	142	55
패킷 전송 지연 시간	0.017 초	0.0089 초

(그림 6) 시뮬레이션 종합 분석 표

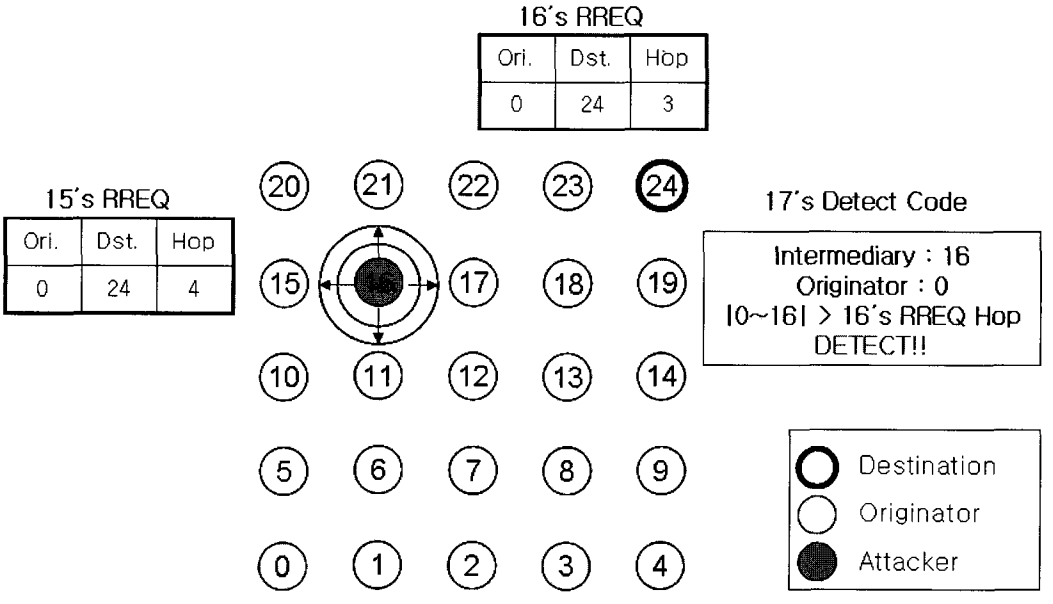
시간이 다른 노드들보다 많이 길어진 것을 볼 수 있다. 이것은 7번과 12번 노드의 경우 11번을 통하여 24번으로 가는 경로가 최단 경로가 아니기 때문이다. 11번 노드를 통하여 24번 노드로 가는 경로가 최단인 주변 노드들도 패킷 전송 지연 시간이 조금씩 길어진 것을 볼 수 있는데 이것은 11번 노드로 트래픽이 몰리기 때문인 것으로 보여진다.

시뮬레이션의 경우에는 네트워크의 규모가 작고, 트래픽 양이 많지 않기 때문에 정상적인 환경과 공격자가 있는 환경에서 패킷 전송 지연 시간 차이가 크지 않지만 실제적인 네트워크에서는 공격자가 존재할 경우 패킷 전송 지연 시간의 차이가 클 것으로 예상된다.

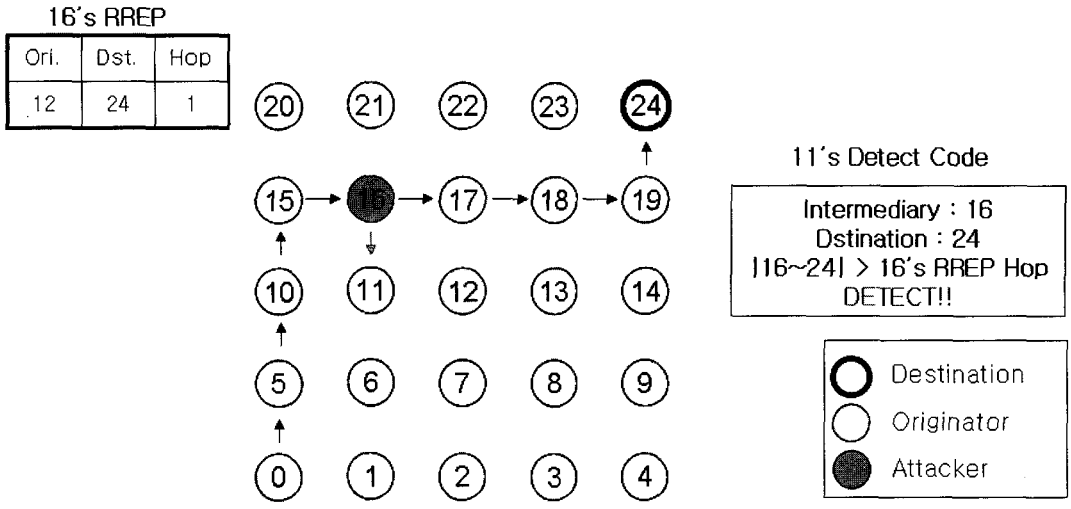
(그림 6)은 시뮬레이션 결과를 종합적으로 분석한 표이다.

5.2. 탐지 메커니즘 적용시 네트워크에 미치는 영향 분석

(그림 7)은 RREQ 메시지를 변조하는 공격자가 있을 때 공격자 탐지 메커니즘을 적용했을 경우의 네트워크 상황이다. 0번에서 24번으로 경로를 찾기 위해서 RREQ를 전송하는 과정이다. 공격자인 16번 노드가 15번 노드로부터 받은 RREQ 메시지 안의 홉수를 1 감소하여 전달한다. 이를 받은 17번 노드는 자신에게 RREQ 메시지를 전달한 16번 노드와 목적지 노드인 24번 노드 사이의 최단 홉수를 계산하고 자신이 받은 RREQ 메시지 안의 홉수와 비교하여 16번 노드가 공격자라는 것을 탐지할 수 있다.



(그림 7) RREQ 메시지 변조 탐지



(그림 8) RREP 메시지 변조 탐지

(그림 8)은 16번 노드가 공격자인 네트워크에서 0번에서 24번 노드로의 경로가 0번, 5번, 10번, 15번, 16번, 17번, 18번, 19번, 24번으로 설정되어 있는 상황이다. 이때 12번 노드가 24번 노드로 CBR 트래픽을 전송하고자 RREQ 메시지를 브로드캐스트하면 이를 받은 11번 노드가 다시 RREQ 메시지를 전송한다. 이를 받은 공격자 노드는 자신이 24번까지의 경로를 알고 있기 때문에 RREP 메시지를 생성하게 된다. RREP 메시지를 생성할 때 24번 노드까지의 홉 수를 1 이상 감소하여 전송한다. 변조한 RREP 메시지를 11번 노드에게 전송하면 이를 받은 11번 노드는 자신에게 RREP 메시지를 보낸 16번 노드와 24번 노드 사이의 최단 홉 수를 계산하고 RREP 안에 포함된 홉 수를 비교하여 16번 노드가 공격자 노드라고 탐지할 수 있다.

6. 결 론

본 논문에서는 애드 혹 네트워크의 대표적인 라우팅 프로토콜이며 센서 네트워크에서도 적용 가능한 AODV 프로토콜 분석을 통해 라우팅시 가능한 내부 공격을 모델링하고 이를 탐지할 수 있는 메커니즘을 제안하였다.

AODV 프로토콜에서 사용하는 메시지에서 공격자에 의해 변경 가능한 필드를 살펴보고 필드를 변경했을 때 미칠 수 있는 영향에 대해 살펴보았다. 또한 이들 중 다른 노드들로 하여금 공격자를 통한 경로를 선택하게 만들 수 있는 필드를 선택하여 정상 노드들이 공격자를 통한 경로를 선택하게 만드는 것을 목표로 하는 공격자를 모델링하고 이러한 공격자가 있을 때 네트워크가 받는 영향에 대한 시뮬레이션을 NS-2 시뮬레이터를 이용하여 수행하였다.

모델링한 공격자가 네트워크 내에 존재할 때와 아닐 때에 대하여 공격자를 지나가는 트래픽 양을 측정하고 트래픽양의 변화를 분석하여 공격자에게 네트워크 트래픽이 몰리는 것을 알 수 있었다. 이와 함께 트래픽의 패킷 전송 지연 시간의 변화에 대한 시뮬레이션도 수행하여 공격자를 통한 경로를 선택하게 되었을 때 전송 지연이 얼마나 길어지는 지에 대한 결과도 얻을 수 있었다. 이러한 시뮬레이션 결과를 통해 내부 공격자의 특징을 분석하고 내부 공격자가 네트워크에 미치는 영향에 대한 연구를 진행하였다.

본 논문의 결과를 이용하여 센서 네트워크 보안 기술에 관한 연구를 진행할 때 내부 공격의 특성을 고려하여 내부 공격이 존재할 경우에도 안전한 프로토콜을 제안하는데 도움이 될 것으로 예상된다.

참 고 문 헌

[1] Ning, P., Sun, K., "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocol," Proc. of Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, 2003.

[2] Perkins, C., Delding-Royer, E., Das, S., "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, 2003.

[3] Karlof, C., Wagner, D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," First IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.

[4] Li, M., "Secure Routing Protocols in Wireless Sensor Networks," CSCE 990, UNL, Nov., 2004.

[5] 김신효, 강유성, 정병호, 정교일, "u-센서 네트워크 보안 기술 동향", 전자통신동향분석, 제20권 제1호, Feb., 2005.

[6] Benjamin, J., Culpepper, H., Tseng, C., "Sinkhole intrusion indicators in DSR MANETs," Proc. First International Conference on Broad band Networks, pp.681-688, 2004.

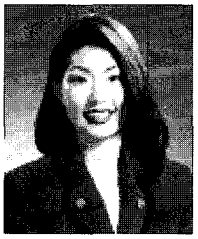
[7] Wood, A.D., Stankovic, J.A., Stankovic, "Denial of service in sensor network," Computer IEEE, Volume 35, pp.54-62, Oct., 2002.

[8] Douceur, J., "The Sybil Attack," 1st International Workshop on Peer-to-Peer Systems 2002.

[9] Newsome, J., Shi, E., Song, D., Perrig, A., "The sybil attack in sensor networks: analysis & defenses," Proc. of the third international symposium on Information processing in sensor networks, ACM, pp.259-268, 2004.
[10] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L.,, Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies," Proc. of DARPA Information Survivability Conference and Exposition, Volume 1, pp.26-36, Apr., 2003.
[11] Wang, B.T., Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks," Canadian Conference on Electrical and Computer Engineering, Volume 2, pp.901-904, May, 2004,
[12] Wood, A.D., Stankovic, J.A., "Denial of service in sensor network," Computer IEEE, Volume 35, pp.54-62, Oct., 2002.
[13] IEEE 802.15.4-2003 IEEE Standard for Information Technology-Part 15.4: Wireless Medium Access Control (MAC) and Physical layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANS), 2003.
[14] Misic, V.B., Jun Fang, Misic, J., "MAC layer security of 802.15.4-compliant networks," Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.
[15] Karp, B., Kung, H., "GPSR: Greedy Perimeter stateless Routing for Wireless Networks," MobiCom, 2000.
[16] Liao, W.H., Tseng, Y.C., Sheu, J.P., "GRID: A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks," Telecommunication Systems, 18(1):pp.37-60, 2001.
[17] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns
[18] Wireless and Mobility Extensions to ns-2, http://www.monarch.cs.cmu.edu/cmu-ns.html

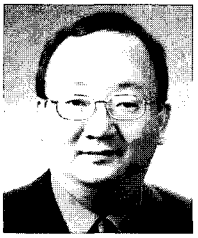
이 명 진

e-mail : maya012@ewhain.net
2005년 이화여자대학교 컴퓨터학과 학사.
2007년 이화여자대학교 컴퓨터학과 석사.
관심분야 : 네트워크 보안, 센서 네트워크 보안, 유비쿼터스 네트워크 보안



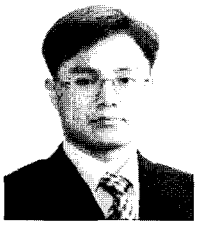
김 미 희

e-mail : mihui@ewhain.net
1997년 이화여자대학교 전자계산학과 (학사)
1999년 이화여자대학교 컴퓨터학과(석사)
1999년 (주)인티 연구원
1999년~2003년 한국전자통신연구원 연구원
2007년 이화여자대학교 컴퓨터학과(박사)
2007년~현 재 이화여자대학교 컴퓨터학과 박사후과정연구원
관심분야 : 네트워크 보안, NEMO(NEtwork MObility) 보안, 센서 네트워크 보안, 유비쿼터스 네트워크 보안



채 기 준

e-mail : kjchae@ewha.ac.kr
1982년 연세대학교 수학과(학사)
1984년 미국Syracuse University 컴퓨터학과(석사)
1990년 미국 North Carolina State University 컴퓨터공학과(박사)
1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수
1992년~현 재 이화여자대학교 컴퓨터학과 교수
관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능분석, 센서 네트워크, 홈 네트워크, 유비쿼터스 컴퓨팅



김 호 원

e-mail : khw@etri.re.kr
1993년 경북대학교 전자공학과 졸업(학사)
1995년 포항공과대학교 전자전기공학과 석사(공학석사)
1999년 포항공과대학교 전자전기공학과 박사(공학박사)
2003년 7월~2004년 6월 독일 Ruhr University Bochum, Post Doc. 과정
1998년 12월~현 재 한국전자통신연구원 정보보호연구단 선임연구원/팀장
관심분야 : RFID 정보보호 기술 및 USN 정보보호 기술, 타원곡선 및 초타원곡선 암호이론, VLSI 설계