애드혹 센서 네트워크에서 AODV 라우팅 정보변조 공격노드 탐지 및 추출기법

이재현* · 김진희 · 권경희

Method of Detecting and Isolating an Attacker Node that Falsified AODV Routing Information in Ad-hoc Sensor Network

Jae-Hyun Lee* · Jin-Hee Kim · Kyung-Hee Kwon

이 논문은 2008년도 단국대학교 대학 연구비의 지원을 받아 수행되었음

요 약

애드 혹 센서 네트워크 환경에서 사용되는 대표적인 라우팅 방식인 AODV(Ad-hoc On-Demand Distance Vector)는 무선보안 메커니즘의 부재로 라우팅 정보가 모든 노드에게 노출되어 있다. AODV방식의 문제점은 공격자가 네트워크 내부에 침입하여 임의대로 라우팅 경로를 수정하여 자신을 통과하는 경로를 최단경로로 판단하게 하는 라우팅 정보 변조공격이 가능하다는 것이다. 본 논문에서는 AODV 라우팅 정보 중 공격자가 RREQ(Route Request) 패킷의 소스 시퀀스 번호와 홉 카운트를 변조하여 사용하는 공격을 설계했다. 그리고 설계한 공격을 보안 암호화 및 인증방식이 아닌 AODV의 메커니즘 안에서 공격자를 발견하고 발견된 공격자를 고립시켜 네트워크 성능저하를 막을 수 있는 방법을 제안한다. 본 연구는 네트워크 보안을 위해 과도한 보안 알고리즘의 도입으로 생기는 오버헤드를 네트워크 메커니즘을 통하여 줄이고자 한다. 제안된 메커니즘의 성능 평가는 NS-2를 이용하였으며 정상적인 네트워크 상황, 공격 시 네트워크 상황 그리고 제안 메커니즘이 적용된 네트워크 상황하에서 목적지 노드의 데이터 총 수신량을 통하여 성능을 비교 분석하였다. 그 결과 본 논문에서 제안하는 방식을 도입하였을 경우 데이터의 총 수신량이 정상적인 네트워크 상황과 거의 동일하게 나타남을 확인하였다.

ABSTRACT

In ad-hoc sensor network, AODV routing information is disclosed to other nodes because AODV protocol doesn't have any security mechanisms. The problem of AODV is that an attacker can falsify the routing information in RREQ packet. If an attacker broadcasts the falsified packet, other nodes will update routing table based on the falsified one so that the path passing through the attacker itself can be considered as a shortest path. In this paper, we design the routing-information-spoofing attack such as falsifying source sequence number and hop count fields in RREQ packet. And we suggest an efficient scheme for detecting the attackers and isolating those nodes from the network without extra security modules. The proposed scheme doesn't employ cryptographic algorithms and authentication to reduce network overhead. We used NS-2 simulation to evaluate the network performance. And we analyzed the simulation results on three cases such as an existing normal AODV, AODV under the attack and proposed AODV. Simulation results using NS2 show that the AODV using proposed scheme can protect the routing-information-spoofing attack and the total number of received packets for destination node is almost same as the existing normal AODV.

키워드

AODV, AODV 보안(AODV Security), 애드 혹 네트워크(Ad hoc Network), 센서 네트워크(Sensor Network), 유비쿼터스(Ubiquitous)

* 단국대학교 전자계산학과

접수일자 2008. 06. 23

Ⅰ. 서 론

보안에 대한 중요성이 사회적 문제로 부각되고 있는 상황에서 애드 혹 센서 네트워크에 대한 보안 취약성은 유비쿼터스 컴퓨팅을 실용화하는데 큰 장애요소이다. 이러한 문제로 인해 애드 혹 센서 네트워크에 대한 보안 메커니즘의 개발은 반드시 필요하며 많은 연구가 진행되어야 하는 부분이다. 본 논문에서는 애드 혹 센서 네트워크에서 대표적인 라우팅 알고리즘인 AODV[1]가 라우팅 패킷의 전달과정에서 발생할 수 있는 보안 취약성을 분석하고, 그 문제를 해결할 수 있는 방안을 제안하고자 한다. AODV 라우팅 알고리즘은 라우팅 정보를 이웃 노드에게 전송 시 보안을 위한 암호화 및 인증과정 없이 패킷을 전송하므로 그 패킷에 대한 수정은 모든 노드에서 가능하다. 또한 무선 매체를 통한 네트워크 구성으로 접근성 또한 용이하다. AODV의 악의적인 내부공격은 패킷을 손실시켜 네트워크 자체를 붕괴시키는 방법이 있을 수 있으며, 또한 패킷의 내용을 변조하여 소스 노드와 목적지 노드 간의 경로가 최단경로가 되는 것을 막아 비효율적인 네트워크가 구성되게 할 수도 있다[2].

본 논문에서 공격자 노드가 라우팅 패킷의 변조를 통해 공격자를 경유하는 경로가 최단 경로가 되게 만들어 전체 네트워크의 효율성을 저하시키는 공격을 설계하였다. 이와 같은 라우팅 정보 변조공격을 하기위해서 공격자 노드가 변조할 수 있는 라우팅 패킷의 필드는 소스 시퀀스 번호와 홉 카운트 정보이다. 네트워크상의 모든 노드들은 소스 시퀀스 번호를 이용하여 최근의 라우팅 정보를 확인할 수 있으며, 홉 카운트 정보를 이용하여 최단 경로를 확인할 수 있다. 공격자는 이 정보를 변조하여 이웃 노드에게 전송함으로써 자신을 경유하는 것이 최단 경로가 되게 이웃 노드를 속일 수 있다. 이와 같은 공격은 네트워크상에서 불필요하게 우회하는 경로를 만들고 네트워크 성능을 저하시키는 요인이 된다.

이와 같이 네트워크 성능을 저하시키는 공격을 막기 위해서는 공격자를 찾을 수 있는 방법과 발견 후 차단할 수 있는 방법이 제시되어야 한다. 본 논문에서 제안하는 방법에서 최초 공격자를 발견할 수 있는 노드는 공격자에게 RREQ 패킷을 전송한 이웃노드가 된다. RREQ의 패킷을 공격자에게 전송한 노드는 그 노드를 일정한 시간 보관하며 공격자가 다시 그 RREQ 패킷을 전달하기를 기다린다. 공격자가 전송한 RREQ 패킷의 소스 시퀀스 번호와 홉 카운트 비교를 통하여 공격자에게 RREQ 패킷을 전송한 이웃 노드는 공격자가 패킷의 라우팅 정보를 변조했는지 발견할 수 있다. 공격자를 발견한 이웃 노드는 공격자를 차단하기 위해서 공격자의 주소를 포함하는 AODV_ATTACK 패킷을 방송한다. 이 패킷을 수신한 모든 노드는 다시 이웃노드에게 방송하여 마지막에는 네트워크의 모든 노드가 공격자 노드를 설정할 수 있도록 한다. 이와 같은 메커니즘을 추가함으로써 기존의 AODV는 라우팅 변조공격에 대해서 별도의 보안 모듈을 추가하는 오버헤드를 제거할 수 있다.

본 논문의 구성은 2장에서 AODV와 보안에 대한 관련연구를 소개한다. 3장에서는 본 논문에서 제안하는 공격 모델링 방법과 공격을 방어하는 메커니즘을 제안한다. 4장에서는 모델링한 공격과 방어하는 메커니즘을 NS2를 통해 시뮬레이션하여 비교 분석하여 그 효율성을 검증한다. 마지막으로 5장에서는 본 연구에서 대한 성과를 논의하며 논문을 마무리 한다.

Ⅱ. 관련 연구

AODV 라우팅 프로토콜은 필요시 마다 경로설정을 수행하는 Reactive 방식의 무선 애드혹 센서 네트워크에 널리 사용되는 방식이다. 이 때 연결을 요청하는 노드에서 보내는 패킷이 RREQ패킷이고 이 패킷의 목적지노드가 응답하는 패킷이 RREP(Route Reply)패킷이다. 이 두 패킷의 교환에 의해서 연결은 설정된다. 그러나 이 두 패킷을 전송하는 과정에서 중간 노드들은 패킷의 필드 값을 수정할 수 있게 되고, 그로 인해 공격 노드가 아무런 방해 없이 네트워크에 침입하여 장애를 발생시킬 수 있게 된다. 본 절에서는 애드혹 센서네트워크에서 라우팅 정보변조 공격 유형을 알아보고, 공격에 대한 보안메커니즘을 알아본다.

2.1 공격유형 분석

첫 번째는 라우팅 패킷 정보를 수정하여 네트워크상의 노드들이 공격자가 원하는 작동을 수행하게 하는 방법인 Bogus routing Information[4][5] 공격이다. 이 공격은 네트워크에 트래픽을 공격자에게 집중시키게 되어 네트워크 전체적인 지연을 유발할 수 있다. 두 번째는 라우팅 정보변조 공격과 같이 사용하여 공격노드로 모든

패킷이 지나가도록 하여 패킷의 정보 엿듣기가 가능하도록 하는 공격이다. 이 공격을 통하여 공격노드는 자신이 목적지 노드로 가는 최단 경로가 되게 방송할 수 있어 네트워크의 성능을 저하시킬 수 있다[6]. 세 번째는 다른 노드의 ID를 도청하여 자신이 도청한 ID 노드인 것처럼 사용하는 방법인 Sybil Attack[9]이다. 이 공격은 공격의 운영에 따라 서비스 결과를 비정상적으로 유도할 수 있다.

2.2 보안 메커니즘

애드혹 센서 네트워크에서 라우팅 정보를 변조하는 공격을 방지하기 위해서 다양한 연구들이 발표되었다. [3]연구에서는 RREQ 패킷의 홉 수를 변조하여 공격 노드를 경유하는 것이 최단 경로가 되도록 공격 모델을 설정하였고, 최종 목적지 노드가 GRID[7]와 GPSR[7]같은 기반기술을 이용하여 자신에게 전송된 RREQ 패킷의 홉 수가 정확한지 판단함으로써 공격을 해결할 수 있는 방법을 제안하고 있다. [3]번 연구를 통해 홉 수 공격은 피할 수 있으나 목적지 노드가 소스 노드까지의 최단 홉수를 얻기 위해 GRID나 GPSR을 도입하여 네트워크의 추가적인 오버헤드가 발생할 수 있다. [8][10]는 공개키와 인증서 체인을 이용한 애드혹 네트워크 보안 메커니즘을 소개하고 있다. 1홉 떨어진 노드들은 별도의 채널을 통하여 공개키를 교환하고, 인증서는 상대방의 공개키와 정보(이름, 유효기간등)를 자신의 개인키로 해쉬 서명해서 발행한다. 이 인증서는 인증서 테이블을 통해서 관리하고, 1홉 거리의 노드들은 주기적인 인증서 교환을 수행한다. 모든 노드들은 인증서를 통하여 1홉 거리의 노드들을 정당한 노드로 인식할 것임으로 RREQ를 전송할 때 인증서를 함께 전송하는 CRREQ를 전송한다. CRREQ를 수신한 목적지 노드는 자신의 공개키가 포함된 인증서를 소스 노드에게 CRREP에 담아 보내는데 이 과정에서 중간 노드들은 상호 인증서 체인을 통하여 신뢰성을 보장받을 수 있고, 소스 노드는 최종적으로 목적지 노드의 공개키를 안전하게 수신할 수 있게 된다. 예를 들어, 노드 경로가 S - A - B - C - D 와 같이 있다면 D는 자신의 공개키를 CRREP에 담아 보내고 C는 D의 인증서를 발행했으므로 D에 대한 신뢰성을 확보하고, B는 C의 신뢰성을, A는 B의 신뢰성을 그리고 소스 노드인 S는 A의 신뢰성을 보장하므로 D가 보낸 공개키를 안전하게 수신할 수 있는 것이다. 이를 수신한 S는 CRREP-ACK을 전송함으로써 안정적인 연결설정이 이루어진다. 위 방법은 안정적으로 경로를 설정할 수 있으나 별도의 체인 및 인증서 전달과정에서 패킷에 인증서를 같이 가지고 다니므로 패킷의 크기가 증가할 것이다. 본 논문에서는 위의 방법과는 달리 추가적인 보안 기술을 사용하지 않고, AODV의 메커니즘을 통해서 해결하는 방법을 제안한다.

III. 라우팅 정보 변조공격 설계

AODV 라우팅 방식에서 라우팅 정보 변조공격은 RREQ의 RREQID, 홉수, 목적지 노드에 대한 시퀀스 번호, 소스 노드 시퀀스 번호로 가능하다. 이들 중RREQID 필드를 사용한 공격의 경우는 공격자 또한 자신이 전송한 공격 패킷을 자신이 다시 수신하게 되므로 라우팅 루프가 발생하게 된다. 이는 AODV의 메커니즘에 의해서 공격자 노드를 경유하는 경로가 아닌 다른 경로를 선택하게 되므로 공격이 발생하지 않게 된다.

본 논문에서 설계한 공격방식은 RREQ 패킷의 소스 시퀀스 번호와 홉 수를 이용한 지연공격방법이다. 소스 시퀀스 번호는 송신 노드가 전송한 패킷이 가장 최신 패킷임을 구별하는데 사용되므로 소스 시퀀스를 공격자 노드가 수신한 번호보다 높게 변조하여 전송하면 이를 수신한 노드들은 공격자 노드가 전송한 RREQ 패킷의 내용을 최신의 정보로 판단하여 라우팅 테이블에 반영할 것이다. 또한 홉 수는 현재 전송되는 경로의 길이를 나타내는 값이므로 공격자 노드가 이 값을 수신한 패킷의 값보다 작게 변조하여 전송하면 이 패킷을 수신한 노드들은 공격자를 경유하는 경로가 최단경로라고 인식하여 라우팅 테이블을 수정할 것이다.

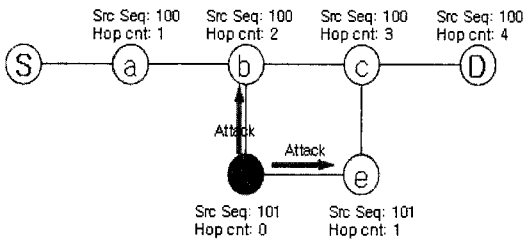

그림 1. AODV 지연공격 전
Fig. 1. Before AODV delay attac

위의 그림 1에서 보면 송신노드 S에서 목적지 노드 D까지 정상적인 경로를 보면 S-ⓐ-ⓑ-ⓒ-D로 4홉의 길이를 가지게 된다.

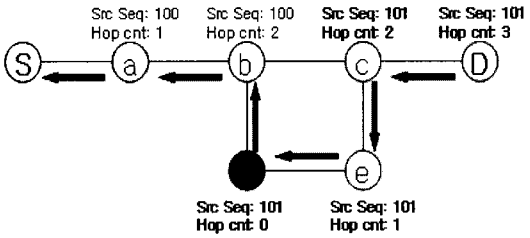

그림 2. AODV 지연공격 후
Fig. 2. After AODV delay attack

그러나 악의적인 공격노드F가 소스 시퀀스 버호를 1 증가하고 홉 수를 0으로 감소하여 변조된RREQ패킷을 전송하게 되면 목적지노드 D가 보낸 RREP에 의해 그림 2와 같이 S-ⓐ-ⓑ-ⓕ-ⓔ-D의 경로가 설정되고 경로길이는 6홉으로 증가하게 된다. 이러한 공격은 네트워크 전체의 전송지연을 유발하여 네트워크 성능저하의 원인이 된다.

Ⅳ. 공격에 대한 해결방안

본 논문에서는 라우팅 정보 변조공격을 통한 네트워크 지연공격을 효과적으로 해결하기 위해서 2가지 메커니즘을 AODV 알고리즘에 추가적으로 적용하였다. 첫 번째는 공격 노드가 공격을 시작했을 때, 최대한 신속하게 공격 노드를 발견하는 방법이고, 두 번째는 발견된 공격 노드를 어떻게 네트워크로부터 고립시키는 가에 대한 방법이다.

4.1 공격노드 발견

공격노드가 RREQ 패킷을 변조하여 공격을 시작하면, 그 패킷을 수신하는 이웃 노드들이 첫 번째 공격의 대상이 될 것이다. 그러나 그 이웃들 중에는 공격 노드에게 RREQ 패킷을 전송한 노드가 포함되어 있을 것이고, 만약 공격 노드에게 RREQ 패킷을 전송한 노드가 전송한 패킷의 정보를 일정시간 가지고 있다면 공격 노드가 변조한 패킷의 정보와 비교를 통하여 자신에게 RREQ 패킷을 전송한 노드가 공격 노드인지 정상적인 노드인지 판단할 수 있을 것이다.

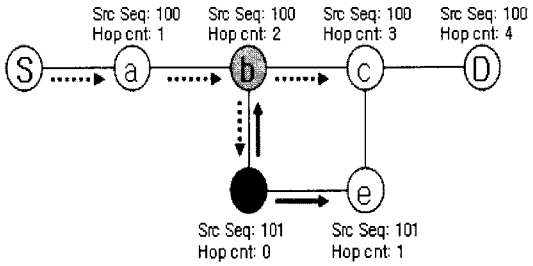

그림 3. 공격노드 발견
Fig. 3. Discover attacker node

그림 3에서 노드 ⓑ는 RREQ 패킷을 전송한 후 RREQ-List에 전송한 패킷을 일정시간 보관한다.

노드 ⓑ의 RREQ 패킷을 수신한 공격 노드 ⓕ는 소스 시퀀스 번호와 홉수를 변조하여 다시 RREQ패킷을 포워딩 할 것이다. 노드 ⓑ는 공격 노드 ⓕ가 전송한 패킷이 정당한 것인지 검증하기 위하여 그림 4와 같은 절차를 수행한다.

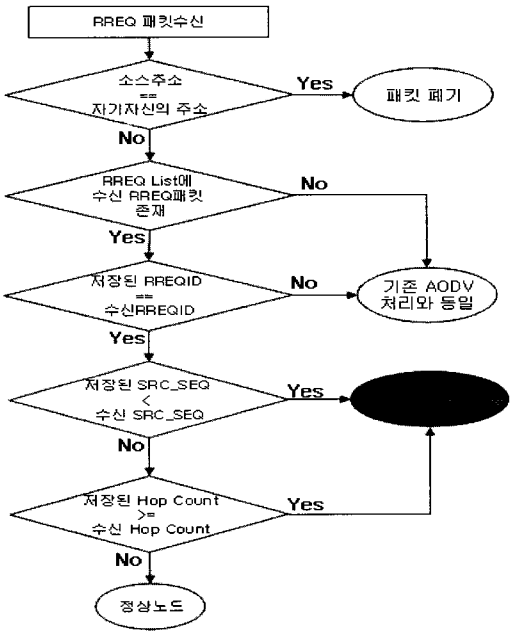

그림 4. 공격노드 검사
Fig. 4. Check attacker node

그림 4에서 최초 RREQ패킷을 수신하면 기존의 AODV와 동일하게 패킷을 전송한 최초 소스가 자신인지 확인하여 자신이 보낸 패킷과 같다면 패킷을 폐기하고 RREQ 수신절차를 끝내고, 그렇지 않으면 현재 수신한 패킷이 내가 전송했던 패킷인지 확인을 위해 RREQ-List를 검색한다. 이 검색은 패킷의 RREQID, 소스 주소, 목적지 주소를 사용한다. 만약 RREQ-List에 패킷이 존재한다면 이 패킷은 자신이 전송한 패킷을 다시 이웃 노드가 전송한 것임으로 공격노드 검사가 수행될 것이고, 아니라면 기존의 AODV와 동일하게 패킷이 처리 될 것이다.

공격노드 검사를 수행하게 된다면 우선 전송된 패킷의RREQID가 동일한지 확인한 후 소스 시퀀스가 저장된 값보다 작거나 또는 홉수가 저장된 값보다 같거나 큰 값을 갖는지 확인하여 그 패킷을 전송한 노드가 공격노드인지 판단한다. 이와 같이 공격 노드를 이웃 노드를 통하여 발견하게 함으로써 공격이 시작한 후 바로 공격 노드를 발견 할 수 있다.

4.2 공격노드 고립

네트워크의 모든 노드들은 공격 노드를 고립시키기 위해서 각 노드마다 Attacker List를 만들어 관리한다. 만일 공격 노드가 발생하면 공격 노드의 주소를 각 노드들의 Attacker List에 등록하여 노드들이 AODV 패킷을 수신할 때 패킷의 이웃 송신자가 공격 노드인지 판단할 수 있다. 따라서 각 노드는 공격 노드의 패킷이라고 판단된 패킷을 폐기함으로써 공격 노드로 하여금 자신을 경유하는 2홉 이상의 노드들과의 연결을 차단하여 공격노드를 고립시킬 수 있게 하였다.

공격 노드를 발견한 노드가 네트워크의 다른 노드들에게 공격 노드의 주소를 알리기 위한 방법으로 새로운 형식의 AODV 패킷을 추가하였다. 네트워크에서 공격 노드를 격리시키기 위해 추가한 패킷은 ADISC(Attack DISCovery)이다. ADISC 패킷은 그림 4에서 노드 ⓕ가 공격 노드로 확정되는 단계에서 만들어지고 방송된다. ADISC 패킷을 통하여 공격 노드 주소는 네트워크상의 모든 노드들에게 방송될 것이고, 이 패킷을 수신한 노드들은 공격 노드를 자신의 공격리스트(Attacker List)에 등록한다. ADISC 패킷의 주요 구성요소로는 수신 패킷구분을 위한 패킷타입으로 ATTACKER를 추가하여 사용하였고 네트워크 노드들의 ADISC패킷중복 수신을 방지하기 위해 ADISCID 필드가 있으며, 공격 노드를 발견한 노드의 주소 필드와 공격 노드의 주소로 구성되어있다.

ADISC 패킷을 수신한 노드는 패킷형식을 판단한 후 그 형식이 AODVTYPE_ATTACKER일 경우에 먼저 해당패킷이 중복된 패킷이 아닌지를 판단하기 위하여 ADISCID 리스트를 검사한다. 만약 존재한다면 이미 해당 공격 노드가 등록되어 있으므로 패킷을 폐기하고 그렇지 않다면 패킷에 있는 공격 노드 주소를 Attacker List에 등록한다. 이와 같은 방법으로 공격 노드를 네트워크상에서 고립시키면 공격으로 발생한 네트워크 성능을 빠르게 회복할 수 있게 된다.

V. 시뮬레이션

4.1 시뮬레이션 환경

본 논문에서 모델링한 네트워크 지연공격과 제안한 AODV알고리즘을 분석하기 위하여 NS2[12]를 이용하였다. 그리고 시뮬레이션을 위한 환경은 다음과 같다. 네트워크 프로토콜은 TCP Reno를 사용하였고, 패킷의 송수신 방법은 반이중(half-duplex)을 가정한다. 시뮬레이션 공간은 670m*670m로 하였고, 각 노드의 전송범위는 250m로 하였다. 트래픽은 CBR(Constant Bit Rate)과 TCP를 사용하였다. 거리에 따른 신호세기 감소는 Free space 모델과 Two-ray Ground 모델로 구성하였고, 물리계층은 802.11 전송방식인 DSSS(Direct Sequence Spread Spectrum)이며 채널 접근방식은 CSMA/CA를 사용한다.

시뮬레이션은 두 개의 노드에 대한 패킷 수신량을 통하여 네트워크의 지연상황을 예측하도록 하였다. 첫 번째 노드는 목적지 노드이다. 목적지노드의 패킷 수신량을 기존의 정상적인 AODV인 경우, 지연공격을 모델링한 경우 그리고 지연공격 방어하기위해 제안한 AODV인 경우로 나누어 비교하였다. 두 번째 노드는 공격 노드의 패킷 수신량을 기존의 정상적인 AODV, 지연공격을 모델링한 경우 그리고 지연공격을 방어하기 위해 제안한 AODV의 경우로 나누어 비교하였다.

시뮬레이션을 위한 네트워크 구성은 그림 5와 같으며, 50초, 100초, 200초로 시간을 변경하면서 공격노드와 목적지노드의 패킷 수신량의 변화를 확인하였다. 그

리고 시뮬레이션을 위해 네트워크 안에 노드의 개수는 50개로 설정했으며 각 노드의 위치는 랜덤하게 설정하였고, 송신 노드의 수는 1개 이상으로 랜덤하게 설정하여 3가지(50s, 100s, 200s) 경우에 동일하게 적용하였다. 목적지 노드는 2번 노드로 설정하여 모든 송신 노드는 2번 노드와 경로를 설정하고 패킷을 전송하게 된다. 그리고 공격 노드는 13번 노드로 설정하여 13번 노드에서 변조한 RREQ 패킷을 전송하게 하였다.

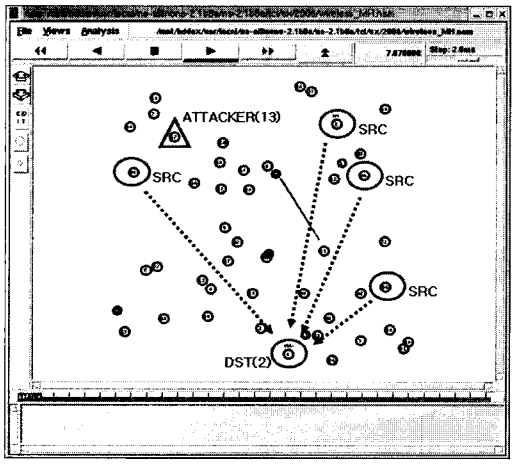

그림 5. 노드 구성
Fig. 5. Node organization

4.2 실험결과 분석

그림 6는 목적지 노드인 2번 노드의 패킷 수신량을 나타내고 있다. 기존의 방식(Normal AODV)인 경우 패킷이 시간의 변화에 따라 657Kb, 1400Kb, 2957Kb로 목적지 노드의 패킷 수신량이 증가하는 것을 볼 수 있다. 그러나 13번노드에 의해 공격이 시작된 경우(Attacked AODV)는 패킷 수신량이 530Kb, 875Kb, 2239Kb로 각각 19%, 37.5%, 24.3% 감소하는 것을 볼 수 있다. 이런 결과는 라우팅 정보 변조공격으로 인해 송신 노드들에서 목적지 노드까지의 경로가 정상인 경우보다 우회하여 설정되었기 때문이다. 그리고 본 논문에서 제안하는 방식(Recovery AODV)의 경우 패킷 수신량은 598 Kb, 1359Kb, 2880Kb로 정상적인 경우보다 시간대별로 9%, 2.9%, 2.6% 의 감소율을 보이고 있다. 따라서 제안하는 방식을 이용했을 경우 라우팅 정보 변조공격을 차단하고 시간이 지남에 따라 정상적인 경우에 유사한 네트워크 성능을 가짐을 확인하였다.

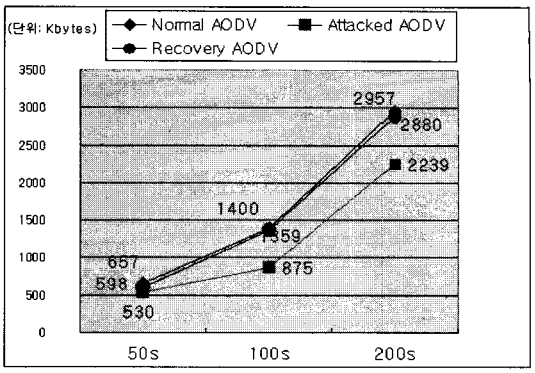

그림 6. 목적지노드(Node 2) 패킷 수신량
Fig. 6. Total number of packet received for destination node(Node2)

그림 7은 공격노드인 13번 노드의 패킷 수신량을 시간대별로 나타내고 있다. 13번 노드의 수신량을 분석하면, 정상적인 경우 시간대별 패킷 수신량은 0Kb, 6Kb, 7Kb로 나타난다. 50초까지는 13번을 경유하는 패킷이 존재하지 않고, 그 이후에는 새로운 송신 노드의 출현 및 라우팅 타임아웃에 의해 13번 노드가 라우팅 경로에 포함되어 패킷을 수신하게 된다.

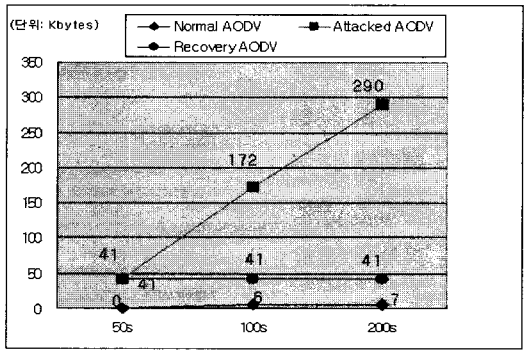

그림 7. 공격노드(Node 13) 패킷 수신량
Fig. 7. Total number of packet received for attacker node(Node13)

정상적인(Normal AODV) 경우13번 노드의 패킷 수신량은 10Kb 미만으로 현저히 낮게 나타나지만, 13번 노드가 공격(Attacked AODV)를 수행하는 경우에는 패킷의 수신량이 41Kb, 172Kb, 290Kb로 급격하게 증가하는 것을 확인할 수 있다. 이런 결과는 13번 노드가 소스 시퀀스와 홉수를 변조하여 이웃 노드들에게 자신을 경유하

는 것이 최단경로라고 속임으로써 발생하는 결과이다.

공격노드인 13번 노드를 고립할 수 있는 Recov ery AODV방식의 경우에는 시간대별로 수신 패킷량이 41Kb로 동일하게 나타나고 있다. 이는 최초 공격 노드인 13번 노드는 RREQ 패킷을 수신한 후에 변조한 패킷을 이웃 노드들에게 방송 한다. 이때 13번 노드의 이웃 노드 중 한 노드가 13번 노드가 공격 노드임을 발견할 것이다. 그러나 13번 노드의 변조 패킷은 이미 목적지 노드에게 전달되고 RREP는 기존의 AODV와 동일하게 작동한다. 따라서 첫 번째 공격경로는 성공을 할 것이다. 그러나 타임아웃으로 인한 경로 재설정 또는 새로운 경로설정을 수행하려 할 경우에는 이미 공격 노드로 Attacker list에 등록이 되어 있으므로 모든 노드와의 패킷교환이 불가능하게 된다. 따라서 더 이상 13번을 경유하는 패킷은 존재하지 않게 되고 41Kb에서 더 이상 패킷 수신량은 증가하지 못한다.

VI. 결론

본 논문에서는 기존에 애드혹 센서 네트워크에서 널리 사용되고 있는 AODV 라우팅 알고리즘을 분석하여 패킷 변조를 통한 라우팅 정보변조 공격에 대해서 살펴보았고, AODV의 패킷 변조공격의 취약점을 보안할 수 있는 메커니즘을 제안하였다. 기존의 AODV 보안은 키 분배 및 인증방식을 이용한 보안 메커니즘에 의존하여 연구되었으나 이러한 방식들은 저전력 과 낮은 Bandwidth를 사용하는 애드혹 센서 네트워크 환경에서는 실용성이 낮다.

제안하는 AODV 방식의 장점은 별도의 보안 모듈을 도입하지 않고 AODV 메커니즘 안에서 공격노드를 발견하고 그 노드를 고립시키는 것을 가능하게 한다는 것이다. 기존의 AODV 라우팅 알고리즘에 RREQ List와 ADISC 패킷을 추가하여 사용함으로써 추가적인 비용부담도 크지 않다. 그리고 네트워크 지연공격을 설계하고, 그에 대한 공격을 방어하는 방식으로 성능평가를 한 결과, 공격노드를 고립시킨 후 목적지 노드의 총 패킷 수신량은 정상적인 AODV에서의 총 패킷 수신량과 유사하게 나타남을 확인하였다.

본 논문에서는 네트워크 보안에 대한 연구에 있어서 보안기술연구에 의존하기보다는 네트워크 메커니즘을 이용하여 효과적으로 보안문제를 해결하고자 하였고 그 결과 패킷변조를 통한 네트워크 공격을 막을 수 있었다.

참고문헌

[1] Larry L.Peterson, Bruce S. Davie, Compuer Networks "Computer Networks : A Systems Approach", Morgan Kaufmann, 1999

[2] 서 현 곤, 김 기 형, "애드 혹 네트워크 네트워크에서 AODV 에 기반한 효율적인 경로 복구 기법", KNOM Review 제6권 제1호, pp1~8, 2003.6.

[3] 이 명진, 김 미희, 채 기준, 김 호원, "센서 네트워크에서 AODV 라우팅 정보 변조공격에 대한 분석", 정보처리학회 논문지 C 제14-C권 제 3호, pp 0229 - 0238, 2007,6

[4] 김 종 천, 김 영 용, "AD Hoc 통신망 프로토콜 개발동향", Telecommunications Reviw, vol.12, no. 3, 2002

[5] 김 한 식, 박 현 희, 강 병 석, 백 상 헌, 강 철 희, "모바일 애드혹 네트워크에서 안전한 라우팅을 위한 경로 조사 기법",한국통신학회 '07 하계 학술 발표 논문집, 2007.7

[6] M. G. Zapata and N. Asokan, "Security ad hoc routing protocols," ACM Wise2002, vol.10, no.1 , pp.1-10, Sept. 2002

[7] S. j. Lee, B.h. Han, and M.h, Shin, "Robust routing in wireless ad hoc networks," in proc. ICCP2002, vol. 6, pp. 73-78, Aug. 2002.

[8] K. Sanziri, B. Dahill, B. N. Levine, and E. M. B. Royer, "A secure routing protocol for ad hoc networks," in proc. ICNP2002, vol. 10, no. 10, pp. 78-87, November. 2002.

[9] Hu, Y. -C., Johnson, D. B. and Perrig, A, "Sead: Secure efficient distance vector routing in mobile wireless Ad Hoc networks", Proc. of Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp. 3 -13 , 2002

[10] K. Sanzgiri et al, "A Secure Routing Protocol for Ad Hoc Networks", ICNP IEEE Press, 2002.

[12] http://www.ietf.org/rfc/rfc3561.txt

저자소개

이재현(Jae-Hyun Lee)

2000년 단국대학교 전자계산학과 졸업(이학사)
2003년 단국대학교 대학원 전자계산학과(이학석사)
2007년 : 단국대학교 전자계산학과 박사수료
※관심분야 : ad hoc 네크워크, IPv6, RFID

김진희(Jin-Hee Kim)

1999년 한국방송통신대학교 전자계산학과(이학사)
2001년 단국대학교 전자계산학과 컴퓨터과학(이학석사)
2007년 단국대학교 전자계산학과 컴퓨터과학(이학박사)
※관심분야 : 컴퓨터 네트워크, TCP/IP, 이동 컴퓨팅

권경희(Kyung-Hee Kwon)

1976년 고려대학교 물리학과 (이학사)
1986년 Old Dominion Univ. Dept. of Computer Science(M.S.)
1992년 Louisiana State Univ. Dept. of Computer Science (Ph.D.)
1979년~1984년 : 산업연구원 연구원
1993년~현재 : 단국대학교 교수
※관심분야 : 컴퓨터 네트워크, 알고리즘 분석 및 설계, 웹 공학, 이동 컴퓨팅