Ad-hoc 네트워크 환경에서 MP-SAR 프로토콜을 이용한 악의적인 노드 검출 기법

차현종○ 한인성 유황빈
광운대학교 컴퓨터과학과
chj826○@kw.ac.kr, ishan78@kw.ac.kr, ryou@kw.ac.kr

Detecting Method of Malicious Nodes using MP-SAR Protocols in Ad-hoc Network Environment

Hyun-jong Cha○ In-sung Han Hwang-bin Ryou
Department of Computers Engineering, Kwangwoon University

요 약

기존의 무선 Ad-hoc 네트워크의 연구는 라우팅기법에 중심으로 이뤄지고 있다. 그러나 기존의 연구들은 네트워크를 구성하는 각 요소들이 우호적이며 상호 협력적인 상황을 가정하여 연구가 이루어지고 있다. 그러나 최근 연구에는 안전한 통신을 보장하기 위한 보안 알고리즘의 필요성에 집중되고 있다. 무선 Ad-hoc 네트워크에서의 악의적인 노드를 식별하는 방안들은 정상적인 노드임에도 불구하고 거짓으로 신고했을 때 확인절차 없이 경로를 재탐색하여 최적의 경로를 변경시킴으로서 최적의 전송환경을 활용하지 못하는 문제점이 있다.

본 논문에서는 다중경로 기반의 보안경로 탐색 프로토콜인 MP-SAR 프로토콜을 이용하여 보안경로에서는 악의적인 노드를 검증하고, 유효한 최단경로를 통해 데이터전송을 하는 기법을 제안하고자 한다. 제안한 기법을 적용함으로써 노드에 대한 신고가 있을 때 확인과정을 거쳐 불필요하게 경로를 재탐색하는 과정을 줄일 수 있다.

1. 서 론

최근 이동 컴퓨팅 단말기들이 보다 소형화되는 추세이다. 다양한 무선 네트워크 제품과 서비스가 제공되고 있으며, 이동 컴퓨팅 기기의 휴대성과 사용자의 이동성에 대한 연구가 활발히 진행되고 있다 사용자가 이동 중에도 네트워크 서비스를 끊임없이 제공받을 수 있도록 지원하는 환경을 이동 컴퓨팅 환경이라 한다 이러한 이동 컴퓨팅 환경에서의 무선 통신매체의 특성인 낮은 대역폭, 잦은 지연, 높은 에러율 등을 고려하고, 호스트들의 이동성 문제를 해결하기 위하여 제안된 여러 프로토콜들 중에서 IETF의 Mobile-IP가 현재 거의 표준화된 프로토콜로 인정되고 있다[1].

이동 컴퓨팅 환경은 기존에 설치된 유선망을 기반으로 하며 기지국이 관리하는 셀 영역을 벗어난 지역에 존재하는 호스트들에 대해서는 서비스 지원이 불가능한 환경이다. 이에 반해 무선 ad-hoc 네트워크 환경은 기존에 설치된 유선망의 도움 없이 이동 호스트들만으로 구성될 수 있는 임시적인 네트워크 환경이다[2][3][4].

무선 Ad-hoc 네트워크의 응용에는 전쟁이나 천재지변 등으로 기존의 유선망을 사용할 수 없을 경우 기지국 등의 서비스가 지원되지 않는 경우, 화재나 홍수 등의 긴급사태 발생 시 긴급구조 등의 특수한 목적이 있는 경우 그리고 전시장, 회의장, 판매장 등 네트워크가 일시적으로 요구되는 경우가 있다. 이러한 환경에서 Ad-hoc 네트워크를 구성하기 위해서는 참가하는 이동 호스트들이 라우터로서의 기능을 제공할 수 있어야 한다 때문에 무선 Ad-hoc 네트워크는 통신을 위한 기반시설 없이 자체적인 네트워크 구성이 가능하다는 장점 때문에 많이 연구되어 왔다.

기존의 연구들은 Ad-hoc 네트워크를 구성하는 각 요소들이 우호적이고 상호 협력적인 상황을 가정하여 무선 채널 및 라우팅에 집중되어 왔다. 하지만 실제 네트워크 환경에서는 우호적이고 상호 협력적인 상황만이 존재하는 것이 아니므로 안전한 통신을 보장하기 위한 보안 알고리즘의 필요성이 점차 증가하고 있다.

Ad-hoc 네트워크 환경에서의 보안 알고리즘을 설계할 때 다음과 같은 점을 주의해야 한다. 첫째, 무선 Ad-hoc 네트워크는 open peer-to-peer 구조이다. 이는 각 이동 노드는 호스트와 라우터의 기능을 동시에 수행한다 그러므로 유선에서의 특정한 라우터에 보안대책을 적용할 수 있지만, Ad-hoc 네트워크에서는 보안대책을 적용할 특정한 라우터가 없다는 것이다. 둘째, 무선 채널이

공유되므로 악의적인 노드도 이 채널에 접속하여 쉽게 네트워크를 공격할 수 있다. 셋째, 네트워크의 자원이 매우 제한적이다. 배터리로 전원을 사용하는 성능이 약한 이동노드의 경우 암호화 기능을 수행하기에 충분한 자원을 가지고 있지 않아 외부로부터의 공격에 취약해질 수밖에 없다.

이러한 Ad-hoc 네트워크의 특성을 고려해 볼 때, 보안대책은 크게 사전 예방방법과 사후 조치방법으로 나뉘어서 생각을 할 수 있다. 사전 예방방법으로는 Ad-hoc 네트워크의 라우팅 경로를 설정 할 때 악의적인 노드를 제외시켜 라우팅 경로를 구성하고, 사후 조치방법으로는 데이터의 전송이 끝난 후에 악의적인 노드를 찾아내어 조치를 하는 방식이다[5].

본 논문에서는 보안성이 추가된 다중경로 라우팅을 이용한 사전 예방방법에 관해서 제안하고자 한다. 구성은 2장에서 관련연구로 다중경로 라우팅 기법과 악의적인 노드 식별에 대해서 기술하고, 3장에서는 제안하는 악의적인 노드에 대한 검출 방안을 제시하며, 4장에서 결론으로 이 논문을 마무리 한다.

2. 관련연구

2.1 다중경로 라우팅

ad-hoc 네트워크에 제안된 라우팅 프로토콜은 일반적으로 테이블 구동(table driven) 방식과 요구 기반 구동(on demand driven) 방식으로 나눌 수 있다.[6, 7]

테이블 구동 방식은 DSDV와 DSDV에서 파생된 CGSR(Clusterhead Gateway Switch Routing)과 WRP(Wireless Routing Protocol) 등으로 구분할 수 있다.

요구 기반 구동 방식은 DSR, AODV, TORA(Temporally Ordered Routing Protocol) 및 ABR(Associativity Based Routing) 등이 있다.

2.1.1 테이블 구동 라우팅 프로토콜

테이블 구동 라우팅 프로토콜은 각 노드로부터 네트워크 내의 다른 모든 노드로 일관되게 갱신되는 라우팅 정보를 유지한다.

이러한 프로토콜은 라우팅 정보를 저장하기 위하여 하나 또는 그 이상의 테이블을 필요로 하며, 네트워크 정보를 전송하여 모든 노드들이 일관된 네트워크 토폴로지에 대한 정보를 갖도록 테이블을 갱신한다.

2.1.2 요구 기반 구동 라우팅 프로토콜

요구 기반 구동 라우팅 프로토콜은 테이블 구동 라우팅 프로토콜과는 다른 접근 방식을 사용한다. 이러한 방식의 노드로의 경로가 필요하면, 네트워크 내의 경로 발견 과정을 수행한다.

이 과정은 경로가 발견되거나, 모든 가능한 경로 가능성에 대한 검사가 끝난 후에 완료된다. 이 경로는 목적지 노드로 접근 불가능하게 되거나, 경로가 더 이상 필요 없을 때까지 유지된다.

2.2 MP-SAR 프로토콜[8]

MP-SAR 프로토콜은 AOMDV 기반에서 동작하므로 AODV 기반의 SAR 프로토콜의 원활한 보안링크 연결의 한계점을 개선한 라우팅 프로토콜이다. SAR 프로토콜이 AODV 프로토콜을 기반으로 보안노드만을 발견하고 단일 보안경로채널을 설정하는데 비해, MP-SAR 프로토콜은 보안노드를 발견할 뿐만 아니라 일반노드를 경유하는 다중경로를 발견한다. 데이터 전송을 위해서 다중일반경로 중에서 최단경로를 결정하고 선택된 일반경로는 출발지 노드와 목적지 노드간의 임시적인 보안채널을 설정하도록 데이터 암호 키 교환을 한다. 최단경로의 링크가 손실될 경우, 출발지 노드는 찾았던 경로 중 최단경로를 결정하여 데이터를 전송하지만, 첫 번째처럼 키 교환을 하지 않는다. 때문에 비중첩된 최단경로를 통한 빠르고 안전한 데이터 전송을 할 수 있게 된다.

2.2.1 경로 발견 및 유지

RREQ 소스 라우팅 주소 정보를 추가시켜 확장하여 목적지 노드가 미리 정해진 일정 시간(즉, 프로토콜 파라미터 중 1초의 RREQ_WAITING_TIME)동안 도착한 다수의 RREQ들 중에서 보안경로와 다중일반경로를 선택하는 것이 핵심이다.

1) 출발지 노드는 목적지 노드로의 경로를 필요로 할 때 출발지 노드의 정보와 요구 보안레벨정보(보안경로 발견을 위해 필요로 하는 보안레벨)를 포함한 RREQ를 생성한다. 출발지 노드나 중간노드에서 RREQ를 전송할 때 요구 보안레벨과 출발지 라우팅 주소 정보로서 IP주소를 RREQ에 추가한다.
2) 중복으로 도착한 RREQ는 버리지 않고 수신하는 즉시 자신의 라우팅 테이블에서 라우팅 경로를 확인하여 역경로를 설정한다. 보안레벨과 중간노드 자신의 보안레벨을 비교하여 레벨이 높거나 같다면 RREQ는 암호화된 필드를 복호화한 후 소스 라우팅 리스트에 자신의 정보를 추가한다. 레벨이 낮은 경우 중간 노드는 RREQ는 암호화 되지 않은 필드에 소스 라우팅 정보를 추가하고 이웃 노드들로 브로드캐스트한다.

3) 목적지 노드는 처음 RREQ를 수신한 후 암호화된 RREQ의 필드를 확인한다. 이 필드의 소스 라우팅 리스트를 검사해 연속적으로 보안노드들로만 거쳐진 RREQ라면 보안 RREQ로 결정한다. 목적지 노드는 일정시간안에 수신된 RREQ를 확인해 다중경로들 중 최단 경로를 결정한다. 자신의 수신 순서번호가 RREQ에 포함되어 있는 수신 순서 번호보다 크거나 같으면 중간 노드에서와 같은 방법으로 역경로를 형성한다.
4) 목적지 노드는 처음 수신한 경로를 데이터 전송을 위한 주경로로 선택한 후에 주경로와 비교해 최대의 노드 비중첩성을 갖는 대체경로를 찾는다.
5) 주경로 및 대체경로에 대하여 수신 노드는 송신 노드를 향하여 각각의 RREP를 전송한다. 메시지의 응답으로 목적지 노드에서 결정된 경로정보를 포함한RREP 메시지를 출발지 노드로 보내고 RREP를 수신하는 중간노드는 목적지 노드에 대한 보안경로와 다중경로 라우팅 정보를 알게 된다.

2.3 라우팅(경로설정)에 대한 공격

라우팅에 대한 공격은 라우팅 알고리즘대로 라우팅 정보를 전달하지 않는 모든 행위를 말한다. 예를 들어, DSR에서는 공격자가 전송 패킷 내에 기록되는 source route의 목록에 대해 어떤 노드의 목록을 추가/삭제하는 등의 행위를 통해 source route의 변경이 가능할 것이며 AODV에서는 홉 수, 일련번호가 중요한 라우팅 정보이므로 공격자가 잘못된 홉 수, 일련번호를 전달하는 형태의 공격이 가능하다. 이러한 라우팅 공격은 공격자가 의도하는 특정 목적지로 전달되도록 유도할 수 있고 실제 존재하지 않는 경로가 설정되어 결국 라우팅 루프 및 네트워크 혼잡/분리까지 유발할 수 있다.

이러한 공격으로부터 라우팅 알고리즘을 보호하기 위해 Ariadne for DSR, SAODV, SEAD에서 각각 라우팅 정보를 보호하는 방안을 제시하였다.

2.4 패킷 전달에 대한 공격

패킷 전달에 대한 공격이란 경로 설정과정에서는 정상적으로 동작하지만 실제 데이터 패킷은 제대로 전달하지 않는 행위를 말한다. 이러한 공격은 자신의 자원을 아끼기 위해 다른 노드의 데이터는 전달하지 않으면서 자신의 데이터만 보내려고 하는 이기적인 노드와 의도적으로 네트워크 성능을 저하시키기 위한 악의적인 노드에 의해 일어날 수 있다. 본 논문에서는 이를 구분하지 않고 악의적인 노드라고 부르기로 한다.

패킷 전달에 대한 공격의 형태로는 전달해야 할 패킷을 버리거나 그 내용을 임의로 변경시킬 수도 있으며 많은 양의 무의미한 패킷을 네트워크에 주입시켜 무선 채널 접속을 위한 경쟁을 높이거나 혼잡을 일으킬 수 있다. 이러한 모든 형태의 공격으로부터 네트워크를 보호하기 위한 방법으로 Watchdog and Pathrater[9], 이기적인 노드 관리 방안[10] 등이 있다.

2.5 Watchdog and Pathrater[9]

Watchdog and Pathrater에서 각 노드는 데이터를 전송 후 복사본을 자신의 버퍼에 저장하고 있으면서 다음 노드가 전송하는지 여부를 overhear한다. 만약 일정 시간 내에 overhear되면 제대로 전송되었으므로 자신의 버퍼에서 그 복사본을 버리고, 그렇지 않으면 다음 노드에 대한 failure tally를 증가시킨다. 만약, tally가 threshold를 초과하게 되면 다음 노드가 고의적으로 데이터를 버리는 것으로 판단하여 소스 노드에게 신고하고 소스 노드는 사용 중인 경로에 대한 사용을 중지하고 새로운 경로설정을 하게 된다.

2.6 이기적인 노드 관리 방안[10]

이기적인 노드 관리 방안에서 각 노드는 데이터 전송 후 복사본을 버퍼에 저장하고 있다가 데이터를 수신한 다음 노드로부터 증명서를 받음으로써 정확히 전달하였음을 확인하게 된다. 또한 목적지 노드는 데이터를 수신하면 ACK를 소스노드에게 보낸다.

3. 제안기법

위의 방식들은 악의적인 노드가 경로 상에 포함되어 있으면서 정상적으로 동작하는 노드를 거짓으로 소스 노드에게 신고하는 경우 이를 식별해 낼 수 없는 문제점이 있다. 이런 문제점을 보완하고자 악의적인 노드에 대한 신고를 검증하는 단계를 두어 거짓 신고를 걸러내는 방법을 제안하고자 한다.

3.1 가정

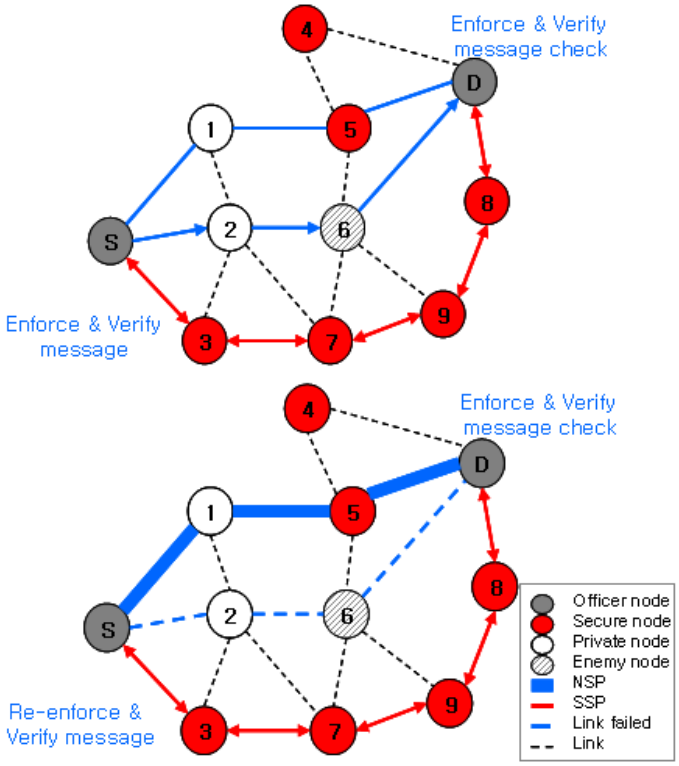
① 각 노드는 이웃 노드의 전송을 overhear할 수 있다.
② 각 노드는 자신만이 알고 있는 개인키를 가지고 있으며, 그에 대응하는 공개키는 모든 노드가 가지고 있다.
③ 악의적인 노드를 신고할 때의 신고자가 보내는 데이터를 신고서라고 하고, 이는 자신의 ID, 신고대상 노드의 ID를 포함한다.

임의의 노드에서 악의적인 노드를 신고할 때 신고서를 암호화해서 broadcast한다. 이를 받은 노드들은 송신노드의 공개키로 복호화를 하여 신고서를 볼 수 있다 또한 이 신고서는 개인키로 암호화를 하기 때문에 다른 노드에서 거짓으로 신고서를 만들 수가 없다

④ 각 노드는 보안레벨을 가지고 있다
⑤ 네트워크의 구성은 AOMDV를 기반으로 하는 MP-SAR 프로토콜을 사용한다
⑥ 노드 간의 링크들은 양방향 통신이 가능하다

3.2 제안 알고리즘

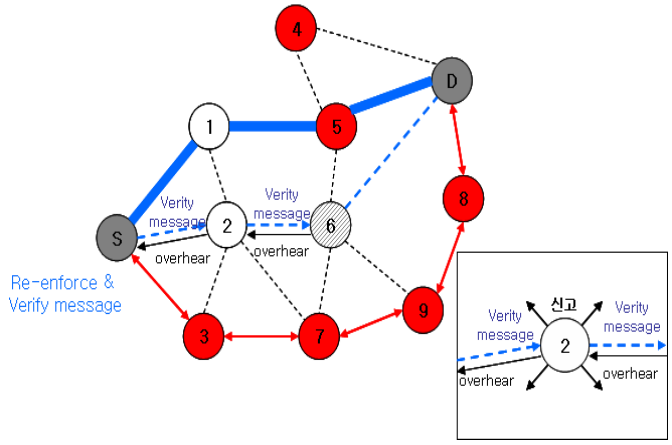
제안 방식의 기본적인 동작은 다음과 같다



[그림 1] MP-SAR의 경로 설정 단계

AOMDV를 기반으로 MS-SAR 프로토콜에 의해 [그림 1]과 같이 보안경로 SSP(Security Shortest Path)와 일반 다중경로 NSP(Normal Shortest Path)가 탐색되었고, 다중경로 중 최단 경로로 [S,2,6,D] 경로가 선택되었지만 데이터 전송을 위한 초기단계에서 검증 메시지를 전송하는 중 선택된 경로에서 온 메시지의 오류가 발견되었다 따라서 다음 NSP인 [S,1,5,D] 경로가 검증이 완료되어 데이터 전송 경로를 강화하여 데이터 전송이 이루어진 상태이다.

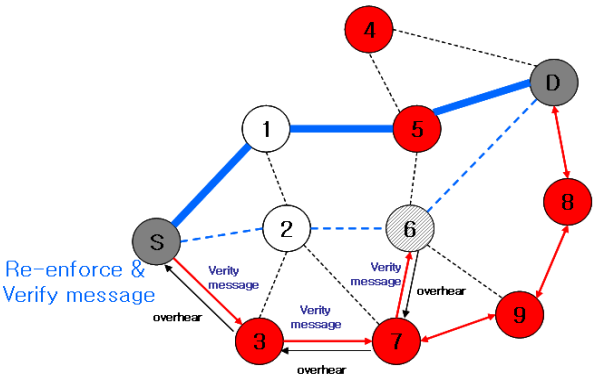
강화된 전송경로로 데이터가 전송하면서 동시에 오류를 발견된 [S,2,6,D] 경로에 대해서 오류가 있거나 악의적인 노드를 검출하기 위해서 오류가 발생한 경로로 검증 메시지를 보낸다. 보내진 메시지는 Watchdog and Pathrater기법을 이용한다



[그림 2] Watchdog을 이용한 악의적인 노드 검출

[그림 2]와 같이 검증 메시지를 다음 노드에 보내기 전에 버퍼에 메시지를 저장하고, 다음 노드에게 메시지를 보낸다. 다음 노드가 메시지를 다음 노드에게 올바른 메시지를 보내는지 overhear를 해서 원래의 메시지와 같다면 버퍼에 저장된 내용을 삭제한다, 만약 다르다면 다음 노드가 고의로 데이터를 변경시켜 보내는 것으로 판단한다. 또한 일정시간 내에 데이터를 보내는 것을 감지하지 못한다면, 고의로 데이터를 버리는 것으로 판단한다. 이러한 고의로 데이터를 변경 또는 버리는 노드를 악의적인 노드로 주위 노드에 broadcast하고, 소스노드에 알린다. 이러한 악의적인 노드의 신고는 각 노드의 개인키로 신고자와 행위자의 정보가 포함된 신고테이블을 암호화해서 신고를 하게 된다

Watchdog and Pathrater로 악의적인 노드를 발견했다고 해도 신고자가 고의로 정상적인 노드를 악의적인 노드라고 신고하는 경우가 있다 이러한 경우를 대비해서 신고에 대한 신뢰성을 검증을 위해 그림 3과 같이 MP-SAR로 확보된 보안경로(SSP)를 이용해서 이전과 같은 악의적인 노드를 검출하는 과정을 거친다 만약 보안경로(SSP)를 이용한 검증에서 신고된 노드가 악의적인 노드가 아니라는 것으로 판단된다면, 신고를 한 노드를 고의로 정성적인 노드를 악의적인 노드라고 신고한 것으로 간주한다.



[그림 3] 보안경로를 이용한 악의적인 노드 검증

이렇게 판명된 악의적인 노드의 정보(ID)는 링크 내의 모든 노드가 저장하고 있다가 후에 소스노드가 바뀌고 라우팅 계산을 할 때 악의적인 노드가 거치는 경로를 제외하고 라우팅을 계산한다.

4. 결론

본 논문에서는 다중경로에서의 보안경로를 확보하고 다중일반경로 중 최단 경로로 데이터를 전송하는 MP-SAR 라우팅 프로토콜을 이용하였다. MP-SAR 프로토콜을 기반으로 일반경로와 보안경로를 이용한 데이터를 전송하는 동시에 악의적인 노드가 있다는 신고가 들어오면 보안경로를 통한 검증으로 검출에 대한 신뢰도를 높였다. 또한 네트워크 환경 측면에서는 재탐색과 같은 불필요한 작업을 중복하지 않기 때문에 기존 방법보다 자원을 절약할 수 있다. 제안하는 방법에서는 악의적인 노드의 검출에 대한 신뢰성을 높였으나, 검출된 노드에 대한 주기적인 관리가 없어 보안 경로가 바뀌었을 때 악의적인 노드가 네트워크에 참여할 수 있는 문제점이 있다. 향후에는 검출된 노드를 관리하여 다른 경로를 통해 네트워크에 참여하지 않도록 연구할 것이다.

5. 참고 문헌

[1] Charles E. Perkins, editor. IP mobility support Internet Draft, August 1995. Work in progress.

[2] S. Corson, J. Macker, "Mobile ad hoc Networking(MANET)," Internet Draft, Oct. 1998.

[3] Charles E. Perkins, "Mobile Ad Hoc Networking Terminology," Internet Draft, Nov. 1998.

[4] S. Corson, J. Macker, S. Batsell, "Architectural Considerrations for Mobile Mesh Networking," http://tonnant.itd.nrl.navy.mil/mmnet/mmnetRFC.txt, May 1996.

[5] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, "Security in Mobile Ad Hoc Networks : Challenges and Solutions", IEEE Wireless Communications, 2004.

[6] Andrew S. Tanenbaum, "Computer Networks," Prentice-Hell International Inc., Second Edition, pp.345-374, 1996.

[7] C.E Perkins and P.Bhagwat, "Routing over Multi-hop Wireless Network of Mobile Computers, "SIGCOMM'94 : Computer Communications Review, pp.234-244, Oct., 1994.

[8] In Sung Han, Hwang-Bin Ryou, Seok-Joong Kang, "Multi-Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network," ichit, pp.620-626, 2006 International Conference on Hybrid Information Technology-Vol 1(ICHIT'06), 2006.

[9] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", ACM MOBICOM, 2000.

[10] gajin Na et al, "Secure Mechanism to manage selfish nodes in Ad hoc Network", JCCI, 2004.