MANET에서 악의적인 노드의 안전하고 효율적인 검출 방안

이 강 석[†] · 최 종 오[††] · 지 종 복[†] · 송 주 석[†††]

요 약

최근 MANET에서의 연구는 보안을 고려한 라우팅 서비스에 주목되어 왔으나 기존에 제시되었던 MANET에서의 악의적인 노드를 식별하는 방안들은 거짓 신고하는 악의적인 노드가 있을 때에는 이를 적절히 식별하고 제거하지 못하는 문제점이 있었다. 따라서 본 논문에서는 신고자와 혐의자 목록으로 구성되는 신고 메시지와 신고 테이블을 이용하여 경로 설정단계에서는 정상적으로 동작하지만 데이터 전달 과정에서는 데이터를 버리거나 내용을 변경시키는 행위, 또는 다른 노드를 거짓으로 신고하는 등의 악의적인 노드를 식별하는 효율적인 방안을 제안한다. 제안하는 방안은 DSR 과 AODV에 모두 적용 가능하다. 또한 성능분석을 위해 AODV와 제안된 알고리즘과 비교 분석하여 제안된 알고리즘이 평균 분실률 및 전송량 측면에서 현격한 성능차이를 있음을 보였다.

키워드 : 모바일 애드혹 네트워크, 악의적인 노드, 라우팅 프로토콜

A Secure and Efficient Method for Detecting Malicious Nodes in MANET

KangSeok Lee[†] · JongOh Choi[††] · JongBok Ji[†] · JooSeok Song[†††]

ABSTRACT

Lately, the MANET research has focused on providing routing services with security and previous schemes have been proposed for detecting malicious nodes in a MANET. However, they still include some problems which malicious nodes cannot be found when they falsely report other nodes as malicious. Accordingly, we propose a novel and efficient scheme for detecting malicious nodes using report messages and a report table which is consisted of node ID both for suspecting and reporting when the malicious nodes behave normally during the route discovery, but the other hand they drop and modify packets, or falsely report other nodes as malicious during the data transmission. Our proposed scheme is applicable to not only DSR but also AODV. And we provide some simulation results of our proposed scheme by comparing general AODV with our proposed scheme. Simulation results show that our proposed scheme outperforms general AODV in terms of average packet loss ratio and packet delivery ratio.

Key Words : Mobile Ad Hoc Network, Malicious Node, Routing Protocol

1. 서 론

최근 MANET(Mobile Ad hoc NETwork)은 기반시설 없이 자체적인 네트워크 구성이 가능하다는 장점 때문에 많이 연구되어 왔다. 이러한 연구의 대부분은 네트워크를 구성하는 각 요소들이 우호적이며 상호 협력적인 가정하에 무선 채널 및 라우팅에 집중되어 왔다. 하지만 실제 네트워크 환경은 우호적이며 상호 협력적인 상황만 존재하는 것이 아니므로 안전한 통신을 보장하기 위한 보안 알고리즘의 필요성이 점차 증가하였다. 또한 MANET의 고유한 특징들은 보안 알고리즘을 설계하는데 있어 다음과 같은 몇 가지 중요한 고려 요소들을 제기하고 있다.

첫째, open peer-to-peer 구조이다. MANET에서 각 이동노드는 호스트와 라우터의 기능을 동시 수행한다. 즉, 유선에서는 특정한 라우터에 보안대책을 강구할 수 있지만 MANET에서는 특정한 라우터가 없다는 것이다. 둘째, 무선 채널의 공유이다. 악의적인 노드도 무선 채널에 접속할 수 있으므로 쉽게 네트워크가 공격 당할 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 MANET의 특성에 대한 보호 방법은 사전 예방방법과 사후 조치방법으로 구분할 수 있는데 사전 예방은 라우팅 경로를 설정하는 단계에서 악의적인 노드를 식별하여 제외시키고 우호적이고 협력적인 노드들로만 경로를 설정하는 방식을 말하며, 사후 조치는 라우팅 경로를 설정하더라도 공격자에 의해 잠식되는 경우 그러한 노드를 찾아내어 적절히

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.
† 준 회 원 : 연세대학교 컴퓨터과학과(석사과정)
†† 준 회 원 : 연세대학교 컴퓨터과학과(박사과정)
††† 종신회원 : 연세대학교 컴퓨터과학과 정교수
논문접수 : 2005년 3월 21일, 심사완료 : 2005년 7월 14일

조치하는 방식이다.[1]

여기서는 사후 조치 방식에 관해 살펴본다. 기존 연구들은 네트워크내의 악의적인 노드를 식별하는데 있어 단순히 악의적으로 패킷을 버리거나 변형시키는 노드를 식별하는데 중점을 두었고 정상적인 노드를 거짓으로 신고하는 악의적인 노드에 대해서는 적절한 대책이 없었다. 따라서 본 논문에서는 과거 신고 목록을 저장하는 신고 테이블을 이용하여 일차적으로 패킷을 버리거나 변형시키는 노드를 식별하는 것은 물론, 정상적인 노드를 거짓으로 신고하여 네트워크의 성능을 저하시키는 악의적인 노드를 식별하기 위한 알고리즘을 제안한다.

본 논문의 구성은 2장에서는 악의적인 노드 식별을 위한 관련연구에 대해 기술하고, 3장에서는 거짓 신고하는 악의적인 노드에 대한 검출 방안을 제시하며, 4장에서는 성능평가 및 분석, 그리고 5장에서는 결론을 맺는다.

2. 관련 연구

2.1 라우팅(경로설정)에 대한 공격

라우팅에 대한 공격은 라우팅 알고리즘대로 라우팅 정보를 전달하지 않는 모든 행위를 말한다. 예를 들어, DSR[4]에서는 공격자가 전송 패킷내에 기록되는 source route의 목록에 대해 어떤 노드의 목록을 추가/삭제하는 등의 행위를 통해 source route의 변경이 가능할 것이며 AODV[5]에서는 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[6], SAODV[7], SEAD[8]에서 각각 라우팅 정보를 보호하는 방안이 제시되었다.

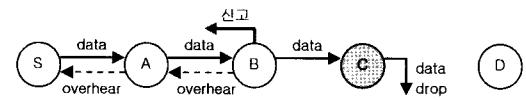
2.2 패킷 전달에 대한 공격

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[2], 이기적인 노드 관리 방안[3] 등이 있다.

2.3 Watchdog and Pathrater[2]

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 사용중인 경로에 대한 사용을 중지하고 새로운 경로설정을 하게 된다.



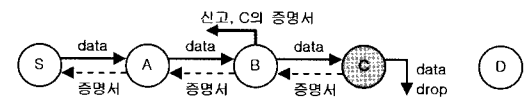
(그림 1) Watchdog and Pathrater

(그림 1)에서 노드 C가 데이터를 전달하지 않고 버리게 되면 노드 B는 노드 C의 전송을 못 듣게 되므로 이에 대해 소스 노드 S에게 노드 C가 악의적인 노드라고 신고를 하게 된다.

2.4 이기적인 노드 관리 방안[3]

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.

(그림 2)에서처럼 노드 B가 노드 C에게 데이터를 전송하면 노드 C는 노드 B에게 자신의 개인키로 암호화시킨 증명서를 보낸다. 만약 노드 C가 데이터를 노드 D에게 전송하지 않으면 노드 D로부터 ACK가 오지 않으므로 노드 B가 노드 C로부터 받은 증명서를 포함하여 소스 노드 S에게 신고를 한다. 이때 증명서는 이를 발행하는 노드인 노드 C의 개인키로 암호화 되므로 다른 노드가 임의로 발행할 수 없게 함으로써 거짓 신고의 가능성을 방지한다. 신고를 받은 소스 노드 S는 노드 C의 공개키로 복호하여 거짓신고 여부를 판단한다.



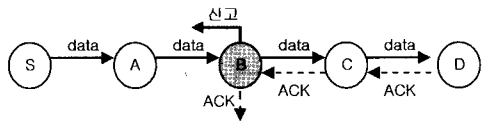
(그림 2) 증명서를 이용한 신고

2.5 기존방식의 문제점

위의 방식들은 악의적인 노드가 경로상에 포함되어 있으면서 정상적으로 동작하는 노드를 거짓으로 소스 노드 S에게 신고하는 경우 이를 식별해 낼 수 없는 문제점이 있다. 즉, Watchdog and Pathrater에서는 (그림 3)에서 노드 C가 정상적으로 패킷을 수신한 후 목적지 노드 D에게 전달하면 노드 B가 그것을 overhear하게 된다. 그러나 악의적인 노드 B는 소스 노드 S에게 노드 C가 패킷을 전달하지 않았다고 거짓 신고를 하고 동시에 목적지 노드 D로부터 수신하는ACK 마

저도 버린다면 소스 노드 S는 노드 B의 신고를 믿고 노드 C가 악의적인 노드라고 잘못 판단하게 될 것이다.

또한, 증명서를 이용한 방법에서도 악의적인 노드가 다음 노드를 거짓으로 소스 노드 S에게 신고하고 목적지 노드로부터 오는 ACK를 버린다면 소스 노드 S는 증명서가 첨부된 악의적인 노드의 신고를 받았으므로 악의적인 노드를 잘못 판단하게 된다.



(그림 3) Watchdog and Pathrater의 거짓 신고

3. 제안 알고리즘

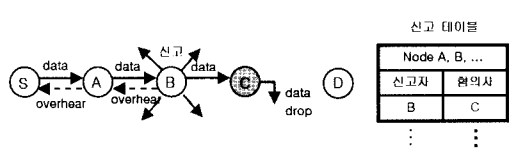
3.1 가정

각 노드는 이웃 노드의 전송을 overhear할 수 있다고 가정한다. 또한 비대칭 암호방식을 사용하는데 이를 위해 임의의 노드 i의 개인키(K_i^-)는 노드 i 자신만이 알고 있으며 공개키(K_i^+)는 모든 노드들이 알고 있다고 가정한다. 따라서 노드 i가 노드 k를 신고하는 경우 노드 i는 자신의 개인키로 암호화한 신고서, K_i^-(신고자:i, 혐의자:k)를 broadcast한다. 이를 수신하는 모든 노드는 i의 공개키를 이용하여 복호화 하여 내용을 알 수 있으며 이러한 신고는 i가 아닌 다른 노드는 i의 개인키를 알 수가 없으므로 거짓 신고서를 임의로 만들 수 없게 된다.

3.2 제안 알고리즘

제안 방식의 기본적인 동작은 다음과 같다.

네트워크내의 각 노드는 데이터를 전송 후 복사본을 버퍼에 저장하고 있으면서 다음 노드의 데이터 전송 여부를 확인한다. (그림 4)에서 노드 B는 노드 C에게 데이터를 전송한 후 복사본은 버퍼에 저장하고 있으면서 노드 C의 전송 여부를 확인하기 위해 overhear한다. 만약 일정 시간 내에 overhear되지 않으면 노드 C에 대한 failure tally를 증가시키고 tally가 threshold를 초과하면 misbehavior라고 판단하는 것은 watchdog와 동일하다. 그러나 watchdog에서는 소스 노드에게 unicast로 신고하였지만 여기서는 misbehavior를 네트워크 전체에 신고함으로써 악의적인 노드의 신속한 검출 및 제거가 가능하다.

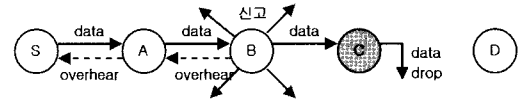


(그림 4) 제안 알고리즘

신고를 받은 노드는 자신의 신고 테이블에 동일한 신고자, 혐의자 목록이 있는지 여부를 검사해서 있다면 신고를 무시하고 버리게 되며, 만약 없다면 테이블에 새로운 목록을 추가한다. 소스 노드 S는 신고를 받으면 새로운 경로를 설정하는데 경로 설정시 신고 테이블에 있는 신고자, 혐의자 노드가 이웃노드로 포함되어 있는 경로는 제외시킨다. 각 노드는 신고횟수가 임계값 k를 넘으면 악의적인 노드라고 판단하고 네트워크에서 제외시키는데 여기서 임계값 k는 네트워크 내에 존재하는 악의적인 노드의 수라고 가정한다.

제안 알고리즘의 악의적인 노드에 대한 식별 및 조치 과정은 아래와 같이 case별로 나누어 설명한다.

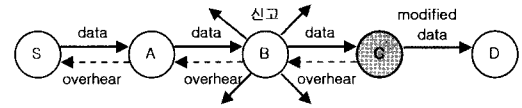
• Case 1 : 데이터를 버리는 경우



(그림 5) 데이터를 버리는 경우

(그림 5)에서 악의적인 노드 C가 데이터를 전달하지 않고 버리면 이전 노드 B가 일정 시간 내에 노드 C의 전송을 overhear하지 못하므로 노드 B는 노드 C가 데이터를 전송하지 않고 버렸다고 판단하고 악의적인 노드라고 신고한다.

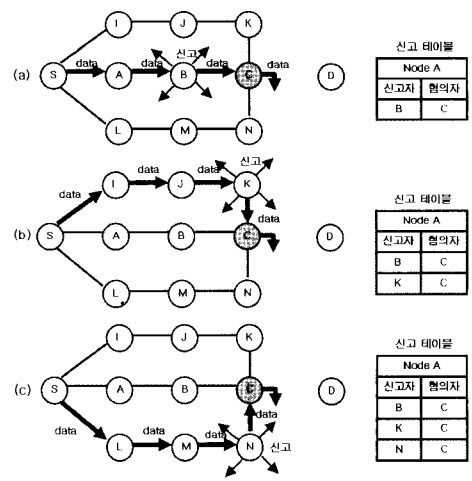
• Case 2 : 데이터를 변형시키는 경우



(그림 6) 데이터를 변형시키는 경우

(그림 6)에서 악의적인 노드 C가 노드 B로부터 받은 데이터를 임의 변경하여 전달하면 노드 B는 노드 C의 전송을 overhear해서 자신의 버퍼의 복사본과 일치하지 않으므로 노드 C를 악의적인 노드라고 판단하고 신고한다.

위의 case 1, case 2 상황에서 신고가 되면 (그림 7) (a)와 같은 신고 목록이 모든 노드들의 신고 테이블에 기록된다. 소스 노드 S는 노드 B의 신고를 받고 나서 목적지 노드 D부터



(그림 7) case 1, 2의 경우 조치

ACK가 오지 않으면 경로상에 악의적인 노드가 있는 것으로 판단하고 새로운 경로를 설정한다. 만약 새로 설정된 경로상에 악의적인 노드 C가 다시 포함될 경우 악의적인 노드 C는 역시 데이터를 버리거나 임의로 변형시킬 것이므로 (그림 7) (b), (c)와 같이 다른 노드 L, K에 의해 또다시 신고될 것이다. 즉, 악의적인 노드는 경로 설정과정에서 정상적으로 동작하여 경로에는 계속 포함되지만 데이터 전달 과정에서 데이터를 정상적으로 전달하지 않으면 다른 노드에 의해 신고되어 혐의자 목록에 계속 기록된다. 또한 네트워크 내에 악의적인 노드가 2개 존재한다면 혐의자 노드 C에 대한 목록이 3개만 되면 노드 C를 악의적인 노드로 판단한다. 이는 악의적인 노드들간 서로 협력하여 거짓 신고할 수 있는 가능성(여기서는2회)을 계산한 것이다.

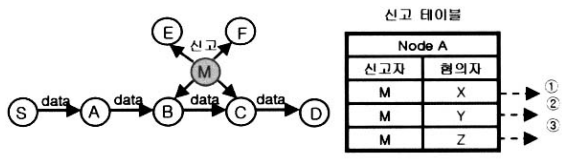
• Case 3 : 다른 노드로 위장하여 거짓 신고하는 경우

제안하는 알고리즘은 비대칭 암호방식을 사용함으로써 다른 노드로 위장하여 거짓 신고하는 것을 방지하고 있다.

어떤 노드 B가 다른 노드 X인 것처럼 위장하여 거짓 신고를 하더라도 노드 B는 노드 X의 개인키를 모르므로 자신의 개인키로 암호화 한다. 그러면 이 거짓 신고를 수신한 다른 노드들은 노드 X의 신고로 알고 노드 X의 공개키로 신고 메시지를 복호화 하나 오류가 발생하므로 이 신고가 잘못된 것임을 알게 되므로 노드 B는 다른 노드로 위장하여 거짓 신고를 할 수가 없게 된다.

• Case 4 : 다른 노드를 임의로 거짓 신고하는 경우

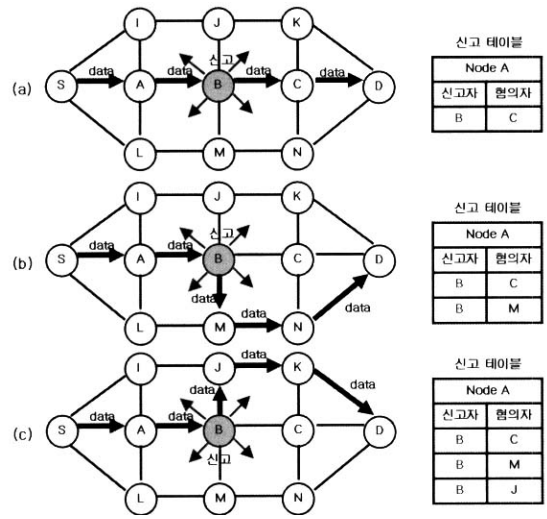
악의적인 노드 M이 경로 설정 및 데이터 전달과 무관하게 임의의 노드 X를 거짓 신고하는 경우에는 (그림 8)와 같이 각 노드의 신고 테이블에 ①과 같은 목록이 생성된다. 계속하여 악의적인 노드 M이 임의의 다른 노드를 거짓 신고할 경우 각 노드의 신고 테이블에는 ②, ③과 같은 신고 목록이 추가된다. 결국 각 노드의 신고 테이블에 신고자 노드 M의 목록이 k개 이상 기록되면 거짓 신고자로 식별되어 더 이상 네트워크의 동작에 참여할 수 없게 된다.



(그림 8) 임의 신고하는 경우

• Case 5 : 정상적인 노드를 거짓 신고하는 경우

(그림 9)에서 악의적인 노드 B가 정상적인 노드 C를 거짓 신고하는 경우, 노드 B는 노드 D로부터 오는 ACK도 버릴 것이므로 소스 노드 S는 노드 B의 신고가 거짓인지 모르고 새로운 경로를 설정한다. 그대신 모든 노드의 신고 테이블에는 (a)와 같은 목록이 추가된다. 노드 B는 새로 설정된 경로 혹은 다른 경로에서 또다시 거짓 신고할 것이므로 역시 신고 테이블에 (b), (c)와 같은 목록이 추가된다. 즉, 신고자 목록에 거짓 신고자인 노드 B의 목록만 추가되고 공통되는 혐의자가 없으므로 노드 B가 거짓 신고했음을 식별할 수 있게 된다.



(그림 9) 거짓 신고를 하는 경우

3.3 제안 알고리즘의 적용: AODV

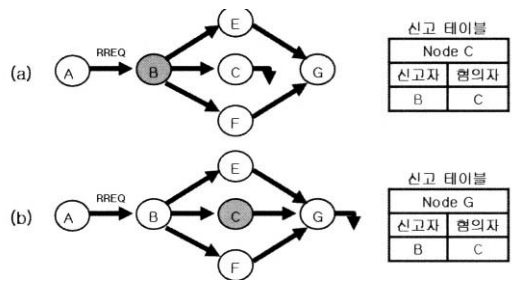
본 절에서는AODV와 DSR에 적용 방법에 대하여 알아본다.

악의적인 노드가 네트워크 경로설정 과정에 참여하지 못하게 하는 방법은 (그림 10) (a)처럼 노드 A가 RREQ를 broadcast하면 악의적인 노드 B도 RREQ를 수신한 후 rebroadcast하게 되는데 이를 수신한 정상적인 노드 C, E, F는 노드 B의 RREQ를 수신한 후 자신의 신고 테이블을 확인하여 노드 B가 악의적인 노드임을 알고 수신한 RREQ는 더 이상 전달되지 못하도록 함으로써 노드 B가 경로에 포함되지 못하도록 한다.

신고자/혐의자 쌍이 한번 이상 네트워크에 신고는 되었으나 악의적인 노드가 정확히 식별되지 않은 경우에는 (그림 10) (a)에서 모든 노드의 신고 테이블에 신고 목록이 기록되어 있고 만약 신고자 노드 B가 악의적인 노드인 경우, 즉, 악의적인 거짓 신고자인 경우라면 노드 B는 RREQ를 broadcast하고 노드 E, C, G는 이것을 수신하지만 정상적인 노드 C는 노드 B로부터 수신한 RREQ에 의한 경로가 설정될 경우 신고 목록에 해당되는 것을 알고 버린다. 대신 노드 E, F는 노드 B에게서 받은 RREQ를 rebroadcast하여 경로가 설정되도록 한다.

만약, (그림 10) (b)처럼 노드 C가 악의적인 노드라면 노드 B가 broadcast한 RREQ를 버리지 않고 rebroadcast하여 노드 B-C 쌍이 경로에 다시 포함되도록 시도할 것이다. 왜냐하면 새로운 경로에 악의적인 노드인 C가 다시 포함되어 노드 B로부터 오는 데이터를 버리더라도 노드 B의 신고를 네트워크에서 무시하게 되도록 유도할 것이기 때문이다. AODV에서 이런 경우의 악의적인 노드를 제외시키기 위해서는 추가 알고리즘이 필요하다. 즉, RREQ에 이전 노드의 주소 필드를 추가함으로써 RREQ를 받은 노드가 자신에게 RREQ를 보낸 노드와 그 노드의 이전 노드를 알 수 있게 함으로써 해결이 가

능하다. (그림 10) (b)에서 악의적인 노드 C가 노드 B로부터 받은 RREQ를 버리지 않고 계속 전달할 경우, 노드 G가 노드 C로부터 RREQ를 받았을 때 노드 C의 이전 노드가 노드 B라는 것을 알 수 있으므로 노드 G는 신고 테이블을 참고하여 노드 B-C 쌍이 경로에 포함되지 않도록 하기 위해 노드 C로부터 받은 RREQ를 전달하지 않고 버린다.



(그림 10) 제안 알고리즘의 적용

3.4 제안 알고리즘의 적용: DSR

소스 라우팅 방식인DSR에서 이미 식별된 악의적인 노드를 제외시키는 방법은 AODV와 같이, (그림 10) (a)에서 악의적인 노드 B가 RREQ를 broadcast하면 이를 수신한 노드 C, E, F는 자신의 신고 테이블을 보고 노드 B가 악의적인 노드라는 것을 알고 더 이상 전달하지 않는다.

신고자/혐의자 노드 중 악의적인 노드가 정확히 식별되지 않은 경우에도 (그림 10) (a)처럼 악의적인 노드 B로부터 RREQ를 수신한 노드 C, E, F 중 노드 C는 노드 B로부터 수신한 RREQ에 의한 경로가 설정될 경우 신고 목록에 해당되는 것을 알고 버린다. 대신 노드 E, F는 노드 B에게서 받은 RREQ를 rebroadcast하여 경로가 설정되도록 한다.

또한 (그림 10) (b)처럼 혐의자 노드 C가 악의적인 노드인 경우에도 노드 C가 rebroadcast한 RREQ를 수신한 노드 G는 소스 라우팅 정보를 보고 노드 B-C 쌍이 경로상에 포함될 것을 알아 RREQ를 전달하지 않는다.

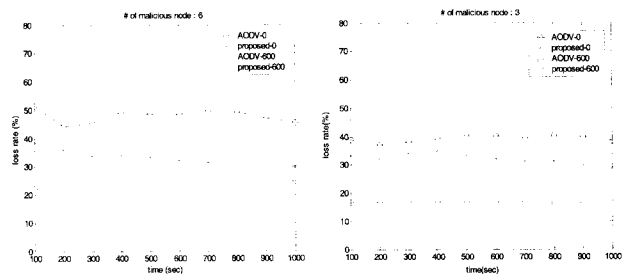
4. 성능평가 및 분석

시뮬레이션은 ns-2를 사용하였으며 DSR에서는 제안 알고리즘 구현이 간단하여 AODV 에 대해서만 실험하였다. 시뮬레이션은 AODV와 제안 알고리즘을 평균 분실률, 평균 전송량, 그리고 상대적인 오버헤드 측면에서 비교 분석하였으며, 주요 변수 값은 <표 1>과 같다.

〈표 1〉 주요 변수 값

네트워크 사이즈	1000 * 1000 (m)
노드의 수	60
악의적인 노드의 수	3, 6
시뮬레이션 시간	1000 sec
Pause time	0, 600 sec
트래픽	UDP/CBR

4.1 평균 분실률



(a) 악의적인 노드가 6개인 경우 (b) 악의적인 노드가 3개인 경우

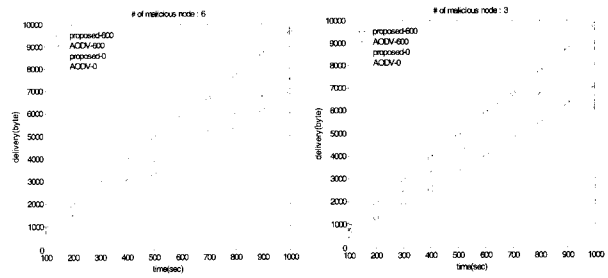
(그림 11) 평균 분실률 비교

(그림 11) (a)는 악의적인 노드가 6개이고 pause time이 각 0초, 600초인 경우 AODV와 제안 알고리즘의 평균 분실률을 나타낸다. 그림에서와 같이 AODV보다 제안 방식의 분실률이 10(%)~20(%) 정도 감소한다. 그리고 시간이 경과할수록 AODV와 제안 방식의 분실률의 격차가 더욱 커지는 것을 볼 수 있는데 이는 악의적인 노드들이 시간 경과에 따라 식별, 제외되기 때문이다. 또한 이동성이 심한 경우 분실률이 더 커지는데 이는 악의적인 노드들이 이동하면서 다른 새로운 경로에 포함될 확률이 높아지게 되기 때문이다.

(그림 11) (b)는 악의적인 노드의 숫자가 3개인 경우인데 6개인 경우보다 평균 분실률이 감소한다. 이는 네트워크 내에 악의적인 노드가 상대적으로 작으므로 당연하다.

4.2 평균 전송량

(그림 12)는 (그림 11)과 동일한 환경에서 평균 전송량을 나타낸다. AODV보다 제안한 방식이 분실률이 적은 만큼 전송량이 더 많다는 것을 알 수 있으며, 악의적인 노드가 6개인 경우보다 3개인 경우 더 많은 양을 전송할 수 있다는 것을 알 수 있다. 그리고 이동성이 적은 경우 분실률은 더 낮으며, 전송량은 더 많아지는데 이는 악의적인 노드가 새로운 경로에 참여할 기회가 증가하게 되어 분실률을 높이고 전송량을 줄이게 되는 것이다. 또한 시간이 경과할수록 전송량 차이가 나는 것은 네트워크내의 악의적인 노드가 시간 경과에 따라 식별, 제거되기 때문이다.



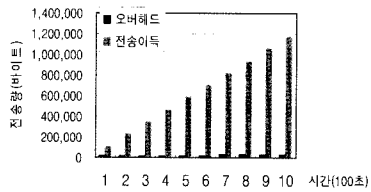
(a) 악의적인 노드가 6개인 경우 (b) 악의적인 노드가 3개인 경우

(그림 12) 평균 전송량 비교

4.3 오버헤드

(그림 13)은 AODV와 제안 방식의 상대적인 전송이득과 오

버헤드를 비교한 것이다. 오버헤드는 제안 방식의 제어 패킷 양에서 AODV의 제어 패킷 양을 뺀 값이며 전송이득은 제안 방식의 전송량에서 AODV의 전송량을 뺀 값이다. 패킷 단위로 비교하면 AODV에 비해 제안 방식이 더 많은 제어 메시지를 발생시킨다. 이는 악의적인 노드가 식별되었을 때 신고 메시지를 네트워크에 broadcast하기 때문이다. 그러나 제어 패킷은 크기가 수십 byte 이고 데이터 패킷은 수백 byte이므로 네트워크 전체적인 전송 측면에서 제안 방식이 작은 오버헤드를 통해 많은 전송이득이 있는 것을 알 수 있다.



(그림 13) 상대적인 전송이득 및 오버헤드

5. 결 론

MANET은 그 특성상 보안에 취약할 뿐만 아니라 공격으로 데이터가 손실되었을 경우 그 피해가 매우 심각하다. 따라서 어느 정도의 오버헤드를 감수하더라도 적극적이고 안전한 보안 대책이 강구되어야 한다.

본 논문에서는 MANET에서 신고자와 혐의자로 구성되는 신고 메시지와 신고 테이블을 이용하여 경로 설정 시에는 정상적으로 동작하지만 데이터 전달과정에서는 비정상적으로 동작하는 악의적인 노드를 식별, 제거하기 위한 알고리즘을 제안하였다. 특히, 거짓 신고하는 악의적인 노드를 식별하고 제거하기 위해 네트워크내에 k개의 악의적인 노드가 있을 경우 k개 이상의 신고 목록이 기록되면 비로소 악의적인 노드라고 판단하도록 하여 악의적인 노드를 효율적으로 식별, 제거할 수 있도록 하였으며 AODV 및 DSR에 적용 가능한 방안을 제시하였다. 또한 시뮬레이션을 통하여 제안한 방식이 AODV 에 비해 평균 분실률, 전송량 측면에서 현격한 성능 향상을 보였다.

참 고 문 헌

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

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

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

[4] J.Broch, D.Johnson & D.Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", http://ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, IETF Internet draft, 15 April, 2003, Work in progress.

[5] S.R.Das & C.E.Perkins, "Ad hoc On-Demand Distance Vector(AODV) Routing for Mobile Ad Hoc networks", http://www.ietf.org/rfc/rfc3561.txt, July, 2003.

[6] Y. Hu, A. Perring, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", ACM MOBICOM, 2002.

[7] M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols", ACM WiSe, 2002.

[8] Y. Hu, D. Johnson, and A. Perring, "Sead: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", IEEE WMCSA, 2002.

[9] H. Yang, X. Meng, and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks", ACM WiSe, 2002.

[10] L. Zhou, and Z. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, Vol.13, No.6, 1999

이 강 석

e-mail : navalee@emerald.yonsei.ac.kr
1999년 해군사관학교 전산과학과(학사)
2004년~현재 연세대학교 컴퓨터과학과 석사과정
관심분야 : 무선네트워크, 네트워크 보안

최 종 오

e-mail : jochoi@emerald.yonsei.ac.kr
2002년 국방대학교 전산학과(석사)
2003년~현재 연세대학교 컴퓨터과학과 박사과정
관심분야 : 센서네트워크, IPv6, 암호학

지 종 복

e-mail : rdrstby@emerald.yonsei.ac.kr
1998년 공군사관학교 전자공학과(학사)
2004년~현재 연세대학교 컴퓨터과학과 석사과정
관심분야 : 무선네트워크, 네트워크 보안

송 주 석

e-mail : jssong@emerald.yonsei.ac.kr
1976년 서울대학교 전기공학과(학사)
1979년 한국과학기술원 전기전자공학(석사)
1988년 Univ. of California at Berkeley, 컴퓨터과학(박사)
1988년~1989년 Assistant Professor in Naval Postgraduate School
1989년~현재 연세대학교 컴퓨터과학과 정교수
관심분야 : Information Security, Cryptography, Protocol Engineering