情報保護學會論文誌
第19卷 第5號, 2009. 10

Ad-hoc 네트워크에서의 효율적인 비정상행위 노드 탐지 및 관리 기법

이 윤 호,† 이 수 진‡
국방대학교

An Efficient Detection and Management Technique of Misbehavior nodes in Ad-hoc Networks

Yunho Lee,† Soojin Lee‡
Korea National Defense University

요 약

애드혹 네트워크는 통신에 참여하는 모든 노드가 서로간에 서비스를 제공하는 모바일 노드들로 구성된 네트워크이다. 하지만, 네트워크에 일부 비정상행위 노드가 존재한다면 많은 위협에 직면하게 된다. 그러므로 애드혹 네트워크의 안전성을 보장하기위해 비정상행위 노드의 탐지 및 배제가 필요하다. 이 문제를 해결하기 위해, 본 논문에서는 지역내 각 노드의 가중치를 관리하는 노드 가중치 관리 서버를 사용한다. 노드 가중치 관리서버는 비정상행위 노드가 발견되었을 경우 해당 노드의 가중치를 증가시키고, 가중치가 임계치를 초과하였을 경우, 네트워크내에서 이를 고립시키기 위해 해당 노드의 정보를 전파한다. 이 방법은 매우 효율적이고, 다수의 비정상행위 노드를 신뢰성 있게 탐지함을 보여준다.

ABSTRACT

Ad-hoc network consists f mobile nodes, which they are together in the communication. However, if some misbehaving nodes are in network, it is faced to many threats. Therefore, detection and management of misbehaving node are necessary to make confident in Ad-hoc networks. To solve this problem, we use Node Weight Management Server(NWMS), which it manage each node's weight in local area. When NWMS detect misbehaving node, it adds the node's weight and if the node's weight exceeds threshold then NWMS broadcasts the node's information to isolate in network. These mechanisms show that they are highly effective and can reliably detect a multitude of misbehaving node.

Keywords: Ad-hoc network security, Tactical Ad-hoc network, NWMS

I. 서 론

애드혹(Ad-hoc) 네트워크는 기반체계 없이 신속한 네트워크 구성 및 유지가 가능하기 때문에 군의 전술상황, 긴급 재난상황, 임시회의 구축 등 다양한 분야에 적용이 가능하다. 이에 관련 기술 분야의 연구도 활발하게 이루어졌으나 대부분의 연구가 더욱 효율적인 라우팅 프로토콜을 개발하는데 중점을 두었다. 그러나 네트워크가 가지는 각종 특성으로 인한 보안상 문제점이 발생하였고, 이를 해결하기 위해 키 관리를 통한 보안 알고리즘 등이 적용된 보안 라우팅 프로토콜에 대한 연구도 활발하게 진행되고 있다[1-3]. 하지만, 키 관리에 기반한 보안 라우팅 프로토콜이 적용되어 노드 상호간에 신뢰관계가 형성되었어도 실제 네트워크의 환경은 우호적인 노드들과 상호 협력적인 상황만 존재하는 것이 아니다. 애드혹 네트워크의 특성

접수일(2009년 5월 25일), 게재확정일(2009년 7월 7일)
† 주저자, yunholee@gmail.com
‡ 교신저자, cyberkma@gmail.com

중 하나인 자원 제약 요소를 피하기 위해 이기적인 행위를 하는 노드, 각 노드가 라우터로서의 역할을 해야 하는 점을 이용하여 악의적인 목적을 지니고 데이터를 버리는 노드, 네트워크 와해를 목적으로 하는 노드 등, 비정상행위를 하는 노드들이 존재 할 수 있으며, 이 노드의 비정상 행위는 네트워크의 전체 성능을 저하시킬 뿐만 아니라, 정상적인 노드의 에너지 소모를 가중시켜 최악의 경우 네트워크 분할의 원인이 될 수도 있다.

애드혹 네트워크를 각종 위협으로부터 보호하기 위한 방법은 정보보호를 위한 기본적인 방법과 마찬가지로 예방과 대응이다[4,5]. 예를 들어 라우팅 경로를 설정하는 단계에서 키 관리 등의 보안 알고리즘을 적용하여 악의적인 노드를 식별해내고 해당 노드를 제외시켜 상호 신뢰할 수 있는 우호적인 노드들로만 경로를 설정하는 방식이 예방이며, 대응은 사후 조치를 하는 경우로 예방을 통해 신뢰 노드로 이루어진 네트워크 구축이 되었지만 공격자에 의해 잠식(compromised)되어 내부적인 오동작을 일으키거나, 자원 제약을 극복하기 위해 이기적인 행위를 하는 노드를 찾아내고 적절한 조치를 취하는 방식이 된다.

본 논문에서는 대응에 관한 내용을 주로 다루고 있다. 기존의 대응과 관련된 대부분의 연구에서는 특정 노드가 데이터를 버리는 등의 이기적인 행위에 중점을 두고 연구[6,7]이 진행되었으며, 특정 노드가 거짓으로 다른 노드를 모함하는 경우에 대해서는 별로 연구된 바가 없다. 또한 탐지 및 관리하는 측면에서도 많은 문제점이 존재한다. 이러한 문제점을 해결하기 위해 본 논문에서는 애드혹 네트워크를 계층화시켜, 상위 계층 노드를 노드 가중치 관리서버(NWMS : Node Weight Management Server, 이하 NWMS)로 설정 운용하였고, NWMS를 통해 비정상행위 노드에 대한 가중치를 관리함으로써 좀 더 신뢰성 있는 판단이 가능하도록 하였으며 비정상행위 노드들을 정확하게 탐지 및 배제시킴으로써 네트워크를 효율적으로 관리할 수 있도록 하였다. 이러한 계층화된 애드혹 네트워크 구성은 최근 미국을 비롯한 많은 국가에서 활발히 연구중인 넓은 범위의 전술 애드 혹(Tactical ad hoc)의 개념[8,9]에서 많이 고려되고 있고, 이와 같은 특수한 목적을 위한 상황에는 계층화된 애드혹 네트워크 구성이 요구되는 상황이 발생할 수 있다. 또한 본 논문에서는 각 노드에 혐의노드 목록(suspect node list)를 두어 정상적인 노드가 부당한 가중치를 받았을 경우, 이에 대한 보상을 통해 노드의 생존성을 유지할 수 있도록 하였고, 신속한 정보 전달을 보장하기 위해 라우팅 경로 탐색 절차시 3개 이하의 다중 경로를 설정함으로써 링크 실패나 전송 실패시 다른 경로로 전달될 수 있는 방법을 제안하였다.

제안하는 방법을 검증하기 위해 네트워크 시뮬레이터인 NS-2를 사용하였고, 정해진 네트워크 범위에 정상 노드와 비정상행위 노드의 포함률을 변경하며 실험하였으며, 제안한 방법을 적용하였을 경우와 적용하지 않은 순수 AODV 프로토콜[10]과의 패킷 손실률, 처리율, 오버헤드 등의 차이를 비교 분석하였다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 관련연구로 비정상행위 노드 관리에 대한 기존 연구 및 문제점을 분석하고, Ⅲ장에서는 다중 경로 설정을 통한 데이터 전송 방법과 NWMS를 이용한 비정상행위 노드의 검출 및 관리 방법을 제안하고, Ⅳ장에서는 모의실험 결과를 분석한다.

Ⅱ. 비정상행위 노드 관리에 관한 기존 연구

애드혹 네트워크를 포함한 모바일 네트워크에서의 연구는 주로 원활한 라우팅에 중점을 두고 있기 때문에 노드들이 서로간의 협력을 바탕으로 동작하는 것을 가정하고 있다. 하지만 동일 목적을 갖는 네트워크에도 내·외부의 공격 또는 자원 제약적인 환경에 의해 비정상적으로 동작하는 노드가 발생할 수 있으며, 이런 노드는 각 노드가 서로간의 필요성에 의해 분산과 협동을 전제로 동작하는 애드혹 네트워크에서 큰 문제점이 된다. 일부 노드는 자신의 수명을 연장하기 위해서 다른 노드들로부터의 서비스를 받기만하고 자신은 서비스를 지원하지 않는 이기적인 행동을 하게 된다. 또한 이기적인 행위 외에도 악의적인 목적으로 데이터를 버리거나 네트워크 와해를 시도하는 노드가 있을 수 있다. 이러한 비정상행위 노드를 탐지 및 배제하기 위한 대표적인 기존의 연구 내용은 다음과 같다.

• Watchdog & Pathrater

이는 네트워크의 모든 노드들이 자신의 주변에 있는 노드들을 감시함으로써 이기적인 노드를 탐지하는 방법에 기반을 두고 있다. Watchdog은 패킷 전달을 거부하는 노드를 감지하고 이를 바탕으로 Pathrater는 악의적인 노드를 피해 최선의 경로를 찾을 수 있도록 도와준다[6]. 하지만 이 기법의 몇 가지 문제점을 살펴보면 첫째, 이기적인 노드로 판명되었음에도 아무

런 불이익이 가해지지 않는다는 것이다. 이기적인 노드로 판명되면 Pathrater는 경로 설정시 이를 고려하여 해당 노드를 우회하는 라우팅 경로를 설정하게 되는데, 이렇게 될 경우 이기적인 노드가 처리해야 할 트래픽을 주변의 다른 노드가 처리해야하므로 오히려 이기적인 노드가 에너지를 절약할 수 있게 해준다. 둘째, 이기적인 노드는 원하는 경우 언제든지 네트워크에 참여할 수 있고 생성한 메시지는 어떠한 제약도 없이 전달될 수 있어 오히려 이기적인 노드에게 유리하게 작용할 수도 있다.

• CONFIDANT(Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks)

이 기법은 비정상적인 노드를 고립시켜 네트워크로부터 배제하는 방법을 포함한다[7]. CONFIDANT는 모니터, 신뢰관리자, 평가시스템, 경로관리자 등의 컴포넌트로 구성된다. 모니터는 인접 노드에 대한 비정상 행위를 탐지하는 역할을 수행하며, 신뢰관리자는 비정상적인 행위를 탐지했을 때 발생되는 경보 메시지에 대한 송수신을 담당하며, 이러한 경보 메시지의 수신자들을 우호적인 관계로 하고 그 리스트를 유지한다. 평가시스템은 일부 온라인 경매 시스템에서 사용되는 것으로 이는 노드에 대한 등급관리를 함으로써 악의적인 노드 리스트를 관리하고 이를 우호관계에 있는 노드와 점차 교환한다. 경로관리자는 경로상에 존재하는 노드들에 대한 평가 등을 기준으로 보안 메트릭에 따라 경로 우선순위를 재설정하고 악의적인 노드들이 포함된 경로들을 삭제한다. 하지만 이 메커니즘의 문제점은 비정상적인 노드에 대해 단지 인접해 있거나 통신을 통해 관계를 맺고 있는 우호적인 노드들과만 정보를 공유하여 새로운 통신을 요구하는 많은 다른 노드들은 이와 같은 사실을 신속히 확인할 수가 없다. 또한 각 노드의 평가관리자 컴포넌트는 특정 노드의 비정상적인 행위를 자신이 스스로 탐지하거나 라우팅 경로상에 존재하는 다른 노드로부터 보고 받게 되는데 이때 그 특정 노드를 악의적인 노드로 판단할지 여부는 각 노드에 사전 정의된 임계치에 의해 결정하게 되므로 애드혹 환경의 특성을 고려, 악의적인 노드가 이동을 하거나 네트워크 토폴로지 변화가 많이 발생하면 악의적인 노드를 판별하는데 많은 시간이 소요될 수 있다.

비정상행위 탐지 및 관리 방법과 라우팅 참여를 유도하는 방법을 제안한 기존의 연구를 분석한 결과 각각의 문제점들이 존재하며 또한 공통적인 문제점이 존재한다. 첫째는 특정 노드가 악의적인 목적을 갖고 정상적인 노드를 비정상 행위 노드로 신고할 경우에 대한 연구나 대응방법이 미흡하다는 것이다. 악의적인 노드는 패킷 드롭과 같은 비정상 행위에 대한 신고 절차를 악용하여 임의의 노드를 거짓 신고 할 수 있다. 둘째는 비정상 행위 노드가 임계치보다 낮게 행동하며 지속적으로 이동하여 비정상 행위를 계속하는 경우, 이를 해결할 방법이 없다. 셋째는 정상적으로 동작하는 노드가 임계치로 인해 고립되어 네트워크로부터 배제되는 경우이다. 그 이유는 비정상 행위에 대한 탐지 방법상 순간적인 오류로 인한 통신 실패나 통신 충돌 등으로 인한 탐지 실패 등으로 비정상행위 노드로 신고 될 수도 있기 때문이다. 이에 본 논문에서는 이러한 문제점을 해결하기 위한 새로운 비정상행위 노드 탐지 및 관리 방법을 제시하고자 한다.

III. 다중경로 설정을 통한 데이터 전송 및 비정상행위 노드 관리

이 장에서는 기존의 비정상 행위 노드 탐지 메커니즘의 문제점을 해결하고 네트워크 처리율을 향상시키기 위해 다중 경로 설정과 비정상노드의 탐지, 배제를 통한 처리율 향상 방안에 대해 제안한다. 여기서는 네트워크의 경로 설정 등의 에너지 소모가 비교적 적은 동작에는 참여를 하고 데이터 전송 등의 비교적 에너지 소모가 많은 동작에는 참여를 하지 않으며, 자신만의 데이터만 송신하고자 하는 노드를 이기적인 노드로 간주하였으며, 자신을 통해 경로가 설정되게 한 후, 그 경로를 통해 전송되는 데이터를 버리거나 임의로 네트워크의 성능 저하를 위해 정상적인 노드를 거짓 신고하는 노드를 악의적인 노드로 간주하였다. 본 논문에서 각 노드의 동작 환경은 다음과 같이 가정한다. 망 내에서 운용되는 상위노드를 기준으로 영역이 설정되며 영역 분할에는 상위노드와 하위노드간 공통적으로 갖는 지역키를 사용하여 중첩을 방지하고, 또한 상위노드와 각각의 하위노드가 일대일로 유지하는 노드키를 통해 악의적인 노드가 다른 노드로 위장하여 임의 노드를 신고하는 것을 방지할 수 있다. 각 노드간의 연결은 양방향 링크로 노드간에 서로 데이터를 주고받을 수 있으며 'promiscuous mode'로 동작하여 전송범위 내에 있는 인접 노드들의 전송을 엿듣기(overhear)할 수 있다. 또한 송신지 노드와 목적지 노드간에는 네트워크의 신뢰성 확보를 위해 2개 이상의 경로가 존재하며, 내·외부로부터 발생하는 위·변

조 공격 등으로부터 보호하기 위해 최초 경로 설정시 적절한 보안 알고리즘을 사용하여 신뢰된 노드들로만 구성된 상황에서 동작하며 특수 목적의 상황을 고려하여 공모 노드는 존재하지 않는다고 가정한다.

3.1 다중 경로를 통한 데이터 전송

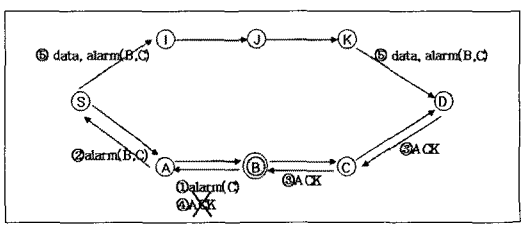
AODV 라우팅 프로토콜은 전송하고자 하는 데이터가 있을시 목적지까지의 경로를 찾기 위해 탐색 과정을 실행한다. 경로 설정 과정은 송신지 노드가 RREQ 메시지를 브로드캐스트하고 중간 노드는 자신의 라우팅 테이블과 비교하여 목적지 노드까지의 유효한 경로가 존재하면 송신지 노드로 RREP 메시지를 보내고, 유효한 경로가 존재하지 않으면, 송신지 노드와 이전 노드를 자신의 라우팅 테이블에 저장하고 RREQ 메시지를 브로드캐스트한다. 목적지 노드는 RREQ 메시지를 받으면, 송신지 노드로 RREP 메시지를 유니캐스트하고 중간 노드는 목적지 노드와 이전 노드를 라우팅 테이블에 저장하고 포워딩한다. 경로 설정 단계를 마치면 송신지 노드는 데이터를 전송한다. 하지만, 이 경로상에 이기적인 노드 또는 악의적인 노드가 존재하면 결국, 데이터의 전송은 정상적으로 이루어지지 않고 송신지 노드는 통신오버헤드가 많은 라우팅 경로 탐색 절차를 반복 수행하여 데이터를 전송하게 된다. 그러므로 이러한 문제점을 해결하기 위해 다중경로 설정을 통해 좀 더 신속하게 데이터를 전송할 수 있어야 한다. 즉, AODV 라우팅 프로토콜에서는 목적지 노드가 RREQ 메시지를 받았을 경우, 최단 거리 또는 최소 시간으로 도착한 메시지에 대해 그의 역경로를 통해 RREP 메시지를 유니캐스트로 보내어 결국 경로상의 모든 노드는 자신의 라우팅 테이블에 목적지에 대한 하나의 경로만을 유지하게 된다. 다중 경로는 목적지 노드가 RREP 메시지를 여러 개 보냄으로써 설정 할 수 있다. 본 논문에서는 송신지와 목적지 간에 경로를 3개 이하로 설정할 것을 제안한다. 제안하는 다중 경로 설정 방법은 정상적인 환경에서도 발생할 수 있는 통신 실패시 경로 재탐색을 위해 발생하는 브로드캐스트에 의한 통신 오버헤드에 비하면 오히려 효율적일 수 있다. 왜냐하면 다중 경로 설정을 위한 오버헤드는 단지 목적지 노드로부터 송신지 노드로의 유니캐스트 패킷이 2개 이하로 더 발생하여 경로상의 일부 노드의 메모리 사용 요구량이 잠시나마 3배 이하로 사용되기 때문이다.

3.2 비정상행위 노드 탐지 및 관리

비정상 행위 노드 탐지 기법에 관한 기존 연구[5,6]에서도 탐지 성능의 차이는 있었지만 비정상행위를 하는 노드들을 탐지 및 관리할 수 있었다. 하지만 기존 연구에서의 가장 큰 문제점은 이러한 탐지 및 관리 메커니즘을 악용하여 다른 정상적인 노드를 비정상행위 노드로 신고하여 네트워크에 참여하지 못하게 하는 점이다. 이는 방법이 다를 뿐 유·무선 네트워크 환경에서 발생할 수 있는 공격방법인 서비스 거부 공격(DoS : Denial of Service)과도 같은데, 애드혹 네트워크에서는 각 노드가 다른 노드를 위해 라우팅 서비스를 지원해야 하므로 이는 더 큰 문제점이 아닐 수 없다. 이러한 문제점을 해결하기 위해 이번 절에서는 상위 노드인 NWMS를 이용하여 비정상행위 노드들을 정확하고 신속하게 탐지하여 네트워크에서 배제시킴으로 네트워크의 효율성을 향상시킬 수 있는 방법에 대해 구체적으로 제시하겠다. 우선 기존 연구를 통해 악의적인 의도로 정상 노드를 신고하는 노드가 존재시의 문제점을 구체화해 보겠다.

3.2.1 악의적인 범인 지목행위(Malicious Accusation)

[그림 1]에서와 같이 악의적인 노드 B는 경로상의 노드 C를 네트워크에서 배제시키려는 목적으로 송신지 노드 S가 목적지 노드 D로 보낸 데이터를 노드 C가 정상적으로 전달했음에도 불구하고 전달하지 않은 것으로 송신지 노드 S에 이를 신고한다. 이때 목적지노드 D는 정상적으로 데이터를 받았으므로 ACK 메시지를 보내게 된다. 하지만, 노드 B는 자신의 행위를 숨기기 위해 이를 버린다. 소스 노드 S는 B의 신고를 받았으므로 S-I-J-K-D 경로로 데이터를 다시 보내며, 노드 C가 비정상행위를 했다고 전파하며, 결국 정상노드 C가 네트워크로부터 배제될 수 있다. 이처럼 기존의 연구에서는 악의적인 범인 지목 행위에 대한 대응 방법이 없었거나 미흡하였다. 이에 본 논문에서



[그림 1] 악의적인 범인 지목행위

는 이러한 비정상행위를 관리할 수 있는 방법을 제안한다.

3.2.2 비정상행위 노드 탐지 방법

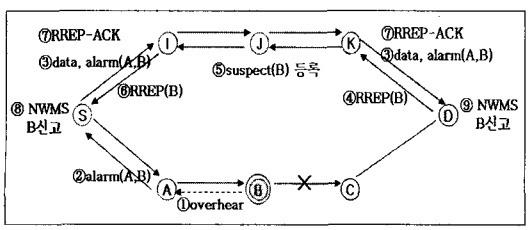
이번 절에서는 경로상의 비정상 노드가 패킷을 버릴 경우와 악의적인 노드가 정상노드를 범인으로 지목하는 경우에 대한 해결방안을 제안한다. 제안하는 방법은 데이터 전송시 비정상행위 노드를 신고하는 노드의 진실성 판단은 송신지 노드와 목적지 노드 상호간의 협업에 의한 이뤄진다. 최종적인 판단은 송·수신 노드로부터 각각 보고를 받는 상위 계층 노드인 NWMS에 의해 이뤄지고 그 결과를 지역 노드들에게 전파하는 방식으로 진행된다. 또한 노드가 정상적으로 데이터를 포워딩 했음에도 불구하고 모호한 통신 충돌 등에 의해 비정상행위 노드로 판단될 수 있으므로 각 노드에 혐의노드 목록을 유지하여 오인된 노드를 구제할 수 있는 기법에 대해서도 제시한다.

1) 경로상의 비정상 노드가 패킷을 버릴 경우

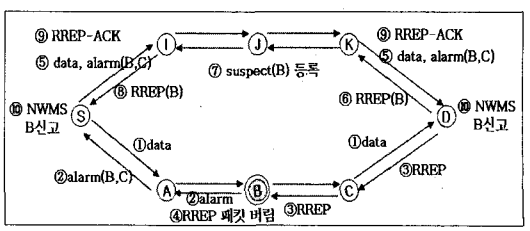
〔그림 2〕와 같이 송신지 노드 S가 목적지 노드 D로 데이터를 보낼 때, 경로상의 노드 B가 이를 버릴 경우 이전 노드 A는 이를 엿듣기(overhear)하여 송신지 노드 S로 신고한다. 신고를 받은 송신지 노드 S는 차선의 경로(S-I-J-K-D)를 이용하여 데이터를 재전송하고, B의 행위에 대한 A의 신고 사실을 전송한다. 목적지 노드 D는 S로부터 접수된 데이터와 신고내용을 바탕으로 이전의 중복 데이터 접수여부를 확인 후, 노드 A의 신고가 사실임을 판단하여 혐의 노드 B의 정보를 포함하여 RREP 메시지를 송신지 노드로 보낸다. 이 RREP 메시지를 전달하는 경로상의 중간 노드들은 혐의 노드 B를 혐의노드 목록에 등록한다. 송신지 노드 S는 RREP 메시지를 받음으로써 A의 신고가 사실임을 확인한다. 송신지 노드 S는 RREP-Ack 메시지를 목적지 노드 D로 보내 메시지를 정상적으로 받았음을 확인시킨다. 이 과정을 통해 송신지 노드와 목적지 노드는 혐의 노드가 B라는 것을 확인하였고 이를 NWMS에 보고한다. 보고를 받은 NWMS의 동작 절차는 3.2.2.3절의 〔그림 4〕를 통해 설명한다.

2) 악의적인 노드가 정상적인 노드를 신고하는 경우

다음은 기존 연구에서 다루지 않았거나 해결 방법에 문제가 있었던 악의적의 노드가 정상노드를 신고하는 경우이다. 〔그림 3〕과 같이 송신지 노드 S는 목적지 노드 D로 데이터를 전송한다. 이때, 경로상의 악의적인 노드 B는 데이터 패킷을 버리지 않고 다음 노드 C에 전달한다. 그리고 난 후 노드 B는 C가 데이터를 전달하지 않은 것처럼 송신지 노드 S에 신고한다. 물론 노드 D는 정상적으로 메시지를 접수한 후 RREP 패킷을 유니캐스트한다. 하지만 노드 B는 자신의 행위를 숨기기 위해 이를 버린다. 신고를 받은 노드 S는 노드 B의 신고사실과 데이터를 차선의 경로(S-I-J-K-D)를 통해 재전송한다. 신고 노드는 B이고 혐의 노드는 C가 된다. 이때 목적지 노드 D는 송신지 노드 S로부터 데이터를 중복으로 받게 될 것이다. 즉, 목적지 노드 D는 최선의 경로와 차선의 경로 모두를 통해 데이터 패킷을 받는다. 하지만 데이터 패킷은 유니캐스트 패킷이므로 중복해서 받을 수 없고 이를 통해 목적지 노드 D는 신고노드가 거짓 신고 한 것임을 알 수 있다. 노드 D는 노드 B가 거짓 신고한 것임을 송신지 노드에게 전달하고, 중간 노드들은 이를 혐의노드 목록에 등록한다. 송신지 노드 S는 D의 메시지를 통해 혐의 노드가 B라는 것을 확인하고 이를 정상적으로 받았음을 RREP-Ack 메시지를 통해 알린 후 이 사실을 NWMS에 신고한다. 이처럼 비정상행위 노드 여부의 판단은 송신지 노드와 목적지 노드의 협업에 의해 이루어지게 된다. 하지만, 이들에 의해 NWMS에 신고가 되었다고 해서 혐의노드가 완전히 비정상행위 노드로 판단되어 네트워크에서 고립되는 것은 아니다. 완



〔그림 2〕 경로상의 비정상 노드가 패킷을 버릴 경우



〔그림 3〕 악의적인 노드가 정상적인 노드를 신고하는 경우

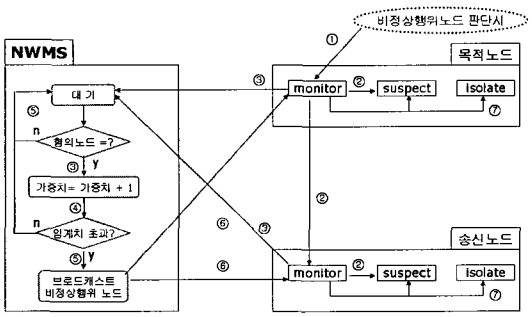
전한 비정상 노드의 판단은 이들의 보고를 받은 NWMS에 의해 이루어진다. NWMS는 송신지 노드와 목적지 노드의 협의노드에 대한 신고사실의 일치여부를 확인한 후 가중치 부여를 결정하고, 협의 노드가 특정 임계치를 초과하면 네트워크로부터 고립시키기 위한 메시지를 브로드캐스트하게 된다.

3) NWMS의 동작원리

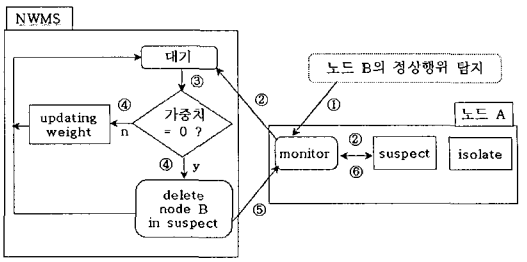
NWMS와 송신지, 목적지 노드의 동작 관계는 〔그림 4〕와 같다. 우선 목적지 노드는 협의노드를 판단하고 이를 송신지 노드에 전파한 후 NWMS에 신고한다. 송신지 노드는 목적지 노드의 판단결과를 바탕으로 NWMS에 신고를 한다. 신고를 받은 NWMS는 일정 시간내 도착한 두 신고를 비교하여, 협의 노드가 동일한지를 판단하고 동일 할 경우 해당노드에 가중치 1을 부여한다. 해당 노드의 가중치가 계속 증가하면 비정상행위가 지속되는 것으로 판단 할 수 있으며, 가중치가 임계치를 초과할 경우 NWMS는 이를 브로드캐스트하고, 이 메시지를 받은 각 노드는 해당 노드를 고립(isolate) 목록에 등록하여 해당 노드로부터의 메시지에 응답하지 않음으로써 노드를 고립시킨다. 임계치와 가중치를 사용하는 것은 비정상행위로 네트워크에서 고립시키기 전에 좀 더 신중을 기하기 위함으로 정상적인 노드임에 불구하고 오인 신고되는 경우, 이러한 노드들의 네트워크 참여를 허가하기 위함이다. 즉, 실제 비정상행위 노드와 통신상의 오류로 인해 비정상노드로 신고받은 노드에 대한 허용치(tolerance) 값을 부여하는 것이다.

4) 부당한 가중치를 받은 노드의 구제 절차

만약 통신상의 오류 등으로 인해 정상적인 노드가 부당한 가중치를 부여 받았다면 이에 대한 구제 방법



〔그림 4〕 협의노드의 신고와 NWMS의 동작 절차



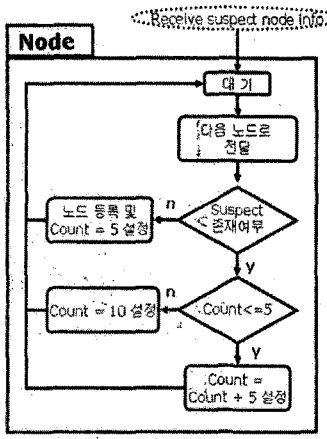
〔그림 5〕 협의노드 목록에 포함된 노드의 정상 동작시 구제절차

이 존재해야 한다. 본 논문에서는 각 노드에 협의노드 목록을 유지함으로써 경로상의 인접 노드가 정상적으로 동작할 경우 가중치를 줄이는 방법을 사용한다. 협의노드 목록에 있는 노드 정보는 라우팅 경로 설정과는 무관하며, 부당하게 가중치를 부여 받은 노드에 대한 구제에 사용되게 된다. 〔그림 5〕는 노드의 협의노드 목록에 등록된 특정 노드가 정상 동작하는 것을 확인했을 때의 동작절차를 나타낸다.

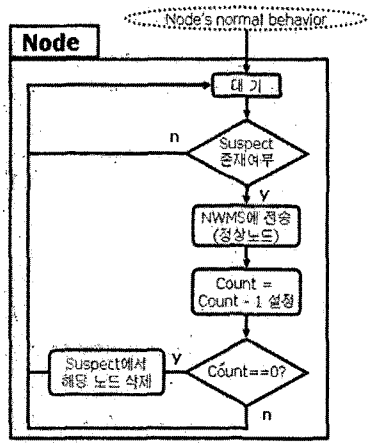
①,②와 같이 한 노드가 라우팅 경로상의 다음 노드를 협의노드 목록에 가지고 있을 경우, 데이터 전송시 그 노드가 정상적으로 라우팅에 참여한다면 협의노드 목록에 있는 노드는 해당 노드의 값을 '1'씩 줄이고 그 노드에 대해 NWMS에게 보고하고, NWMS는 ③과 같이 해당 노드의 가중치를 확인하고 '0'이 아닐 경우 ④처럼 해당 노드에 대한 가중치를 '0.1' 만큼 감소시키고, '0'일 경우 ⑤와 같이 보고한 노드에게 협의노드 목록에서 해당 노드의 정보를 지울 것을 지시한다. 지시받은 노드는 ⑥과 같이 협의노드 목록에서 해당 노드의 정보를 삭제하게 된다.

5) 외부 이벤트에 대한 노드 자체의 동작절차

〔그림 6〕은 통신 경로상의 노드가 목적지 노드로부터 전송된 협의 노드를 포함한 RREP 메시지를 수신하였을 경우의 동작 절차이다. 이 메시지를 수신하면 자신의 협의노드 목록에 해당 노드의 정보가 있는지를 검사한다. 검사 결과 존재하지 않으면 count '5'를 부여하며 해당 노드를 등록하고, 존재할 경우 count값을 비교하여 5보다 작으면 그 값에 5를 더하고 그렇지 않으면 최대값인 '10'을 부여한다. 〔그림 7〕은 부당하게 가중치를 받은 노드에 대한 구제 절차로 인접 노드가 정상행위를 확인하였을 경우의 동작 절차이다. 한 노드는 다음 노드의 행위를 감시할 때 협의노드 목록을 참조한다. 다음 노드가 정상 동작하였을 경우 이를



〔그림 6〕 혐의노드 신고 메시지 수신지 동작



〔그림 7〕 인접 노드의 정상 행위 탐지시 동작

NWMS에 보고하고 자신이 보유중인 혐의노드 목록의 해당 노드 count를 '1'만큼 감소시키는 방식으로 진행된다.

IV. 모의실험 결과

이 장에서는 본 논문에서 제안하는 방법을 모의실험을 통해 그 결과를 분석한다. 모의실험 분석은 네트워크 처리율, 패킷 손실률, 라우팅 오버헤드, 비정상 행위 노드 탐지율을 중심으로 분석한다. 제안하는 방식에서는 통신 오버헤드를 줄이기 위해 신고 및 보고 제어 패킷은 유니캐스트로 처리하며, 비정상행위 노드가 NWMS에서 판별되어 고립시킬 경우에만 신속한 정보공유를 위해 브로드캐스트로 이를 전파한다.

〔표 1〕 모의실험을 위한 주요 설정값

설정 환경	설정값
모의실험 시간	1000 sec
지역 크기	1000 m X 1000 m
신호발생 주기	100 ms
총 노드의 수	기본 250
노드 이동 속도	5 m/s
임계치	5
전파 범위	200 m

4.1 실험환경 및 시나리오

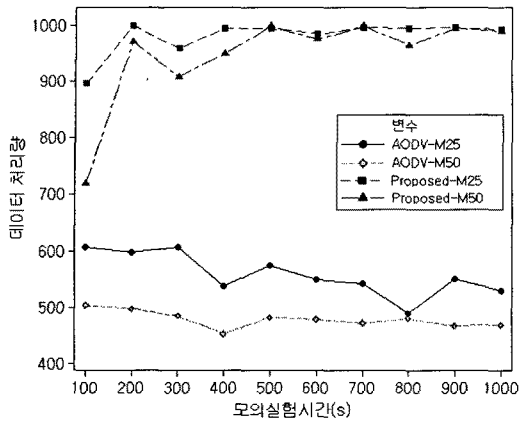
모의실험은 NS-2를 사용하였으며 라우팅 프로토콜은 On-demand 프로토콜인 AODV상에서 비교가 가능하도록 실험하였다. 주요 실험내용은 노드 수 변화에 따른 네트워크 처리율, 비정상행위 노드 포함률에 따른 손실률, 통신 오버헤드, 비정상행위 노드 탐지율에 대해 비교 분석하였다. 모의실험을 위해 설정되는 주요 설정 값은 〔표 1〕과 같다.

실험은 좀 더 다양한 결과를 산출하기 위해 네트워크 내에 정상적인 노드의 수와 비정상행위 노드의 수를 변경시켜가며 실시하였으며, 데이터 전송시 다음 노드로 정상적으로 포워딩하지 않고 이를 버렸을 경우 이전 노드가 이를 탐지하여 NWMS에 보고하고, NWMS는 이에 대한 관리 및 해당 노드의 가중치가 임계치 초과시 이를 전파하여 비정상 행위 노드를 배제시키는 방식으로 진행하였다. 본 실험에서 설정된 NWMS의 가중치 증가율 '1', 임계치 '5', 각 노드의 혐의노드 목록 가중치 증가율 '5', 감소율 '1', 최대값 '10'은 여러 번의 실험을 통해 도출한 최적의 값이며 향후 추가 실험을 통해 개선의 여지는 존재한다.

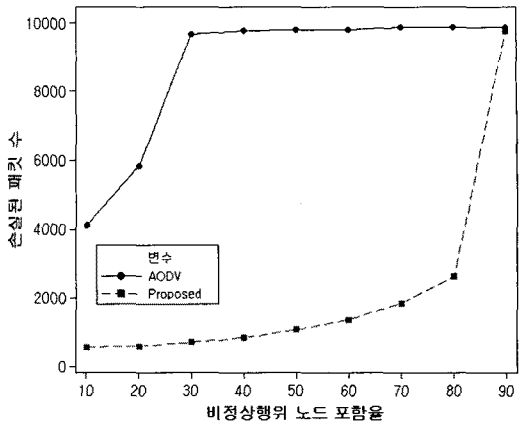
4.2 실험 결과

4.2.1 비정상행위 노드수 변화에 따른 패킷 처리량

〔그림 8〕은 네트워크내의 비정상행위 노드가 각각 25, 50개가 존재할 경우 AODV 프로토콜과 제안하는 방법의 패킷 처리량을 보여준다. 트래픽 발생주기가 100ms이므로 100초 당 발생하는 패킷의 수는 최대 1000개가 된다. 그림에서 볼 수 있듯이 패킷 처리량은 100초 단위로 종합되었으며 AODV의 경우 평균 40~60%의 처리율을 보였다. 반면 제안한 방법에서는



〔그림 8〕 비정상행위 노드수 변화에 따른 패킷 처리량

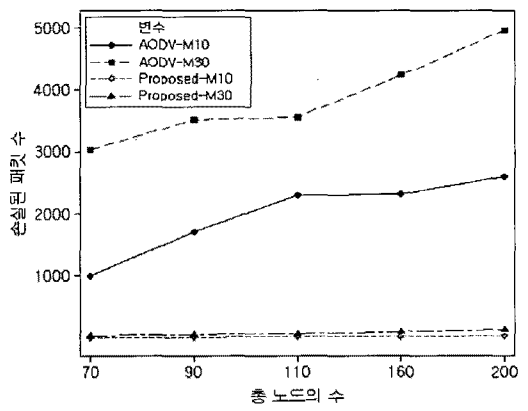


〔그림 10〕 비정상행위 노드 포함률에 따른 손실 패킷 수

비정상 노드가 25개일 경우와 50개일 경우 모두 일정 시간(200초)이 경과한 이후에는 90% 이상의 처리율을 보장해 주었다. 이는 제안하는 기법이 조기에 비정상행위 노드를 탐지 및 배제시키며 네트워크를 효과적으로 잘 관리해줌을 보여주는 결과이다.

4.2.2 노드수 증가 대비 손실 패킷 수

〔그림 9〕에서는 총 노드수 대비 비정상행위 노드가 각 각 10, 30% 존재할 경우 노드수가 증가함에 따른 손실 패킷수를 보이고 있다. 그림에서도 알 수 있듯이 AODV의 경우 총 노드의 수가 증가할수록 손실되는 패킷 수도 증가함을 알 수 있다. 그 이유는 포함률은 일정하나 총 노드수가 증가함에 따라 그만큼 비정상행위 노드가 많이 존재하기 때문이다. 하지만, 제안하는 방법에서는 비정상 노드의 포함비율에 관계없이



〔그림 9〕 노드 수 증가 대비 손실 패킷 수(10, 30%)

총 노드수와 비정상행위 노드수가 증가해도 시간이 경과할수록 비정상 행위 노드가 탐지 및 배제가 이루어지기 때문에 손실되는 패킷의 수는 적정수준에서 일정하게 유지됨을 실험을 통해 확인하였다.

4.2.3 비정상행위 노드 포함률에 따른 손실 패킷 수

〔그림 10〕은 네트워크 내에 비정상행위 노드 포함률에 따른 패킷 손실량에 대한 실험 결과이다. 순수 AODV 프로토콜의 경우 비정상 행위에 대한 대책이 없어 비정상행위 노드가 약 30% 이상 존재할 경우 손실률이 98% 이상을 유지한다. 하지만 제안하는 방법을 적용시 시간이 경과할수록 손실 패킷수는 많아지나 비교적 서서히 증가한다. 그 이유는 네트워크 내에 비정상행위 노드가 많이 존재하면 최초 패킷 손실률은 높지만 오히려 비정상행위 노드의 탐지 및 배제는 더욱 빠르고 활발하게 이루어지기 때문이다. 그렇기 때문에 비정상행위 노드가 많이 포함되어 있어도 패킷의 손실률은 큰 차이가 발생하지 않는다. 하지만 비정상행위 노드의 포함률이 80%를 초과하면서부터 급격하게 손실률이 증가하게 된다. 이는 비정상행위 노드가 탐지 및 배제되면서 남게 되는 정상적인 노드의 수가 적어지기 때문이다.

4.2.4 비정상행위 노드 탐지 성능

비정상행위 노드의 탐지 시간이나 수량에 있어 본 논문에서 제안하는 방식을 적용할 경우 기 연구되었던 비정상행위 노드 탐지 및 배제 방법인 CONFIDANT

에 비해 성능이 우수하다. 이유는 기존 방식의 경우, 라우팅 경로 상에서 비정상 행위 노드 탐지시 경로 상에 존재하는 노드들만 이 정보를 공유하게 된다. 만약 비정상행위를 한 노드가 임계치를 초과하지 않고 다른 경로로 이동하여 또다시 비정상행위를 해도 기존의 임계치 값이 적용되지 않아 계속해서 네트워크 내에서 통신 참여가 가능하다. 하지만 제안하는 기법에서는 NWMS를 통해 노드의 이동과 관계없이 비정상행위에 대한 지속적인 관리가 이루어지기 때문에 탐지 및 배제가 신속히 이뤄진다.

4.2.5 라우팅 오버헤드

기존 라우팅 프로토콜에 비해 제안한 방법이 적용될 경우 통신 오버헤드는 증가한다. 그 이유는 비정상행위 노드의 탐지 및 관리를 위한 제어 패킷이 발생하기 때문이다. 추가적으로 발생하는 패킷은 송신지 노드에서 목적지 노드로 메시지 정상 수신 여부 확인을 위해 발송하는 RREP-Ack 패킷, 비정상행위 노드를 유니캐스트로 신고하는 패킷, NWMS가 비정상행위 노드라고 판단하였을 때 지역내 노드로 전파하는 브로드캐스트 패킷이다. 신고 및 비정상행위 노드 전파시 발생되는 통신 오버헤드를 구하는 식은 (1),(2),(3),(4)와 같이 표현할 수 있다.

초당 패킷 발생수를 t, 평균 라우팅 경로 포함 노드수를 p, 패킷 사이즈를 NP_{size}, 총 노드수를 N, 비정상행위 노드수를 M, 신고 및 전파 제어 패킷 사이즈를 CP_{size}, 임계치를 threshold, 모의실험 시간을 T, 신고노드로부터 NWMS까지의 경로에 포함되는 평균 노드수를 n 이라고 할 경우, 송신지 노드가 목적지 노드로 메시지 정상 수신을 확인하기 위한 RREP-Ack 패킷 전송을 위한 오버헤드(V)는

$$V = p \times CP_{size} \times M \quad (1)$$

신고노드가 NWMS에 유니캐스트로 신고시 발생하는 오버헤드(U)는

$$U = n \times CP_{size} \times threshold \times M \quad (2)$$

NWMS가 비정상행위 노드를 브로드캐스트시 발생하는 오버헤드(B)는

$$B = M \times CP_{size} \times N \quad (3)$$

실험시간동안 발생하는 총 통신량 대비 오버헤드(O)는

$$O = \frac{V + U + B}{T \times t \times p \times NP_{size}} \quad (4)$$

로 표현할 수 있다. 이번 실험 환경에서 비정상행위 노드의 탐지 및 배제를 위해 추가적으로 발생한 평균 통신 오버헤드는 총 통신량 대비 약 0.97%였다. 하지만 패킷 처리량은 그림8과 같이 기존의 방식에 비해 2배 이상 향상되는 것을 알 수 있다. 기존의 프로토콜에서는 시간의 경과와 상관없이 지속적인 데이터 전송 패킷 손실이 발생하는 반면 제안하는 방법이 적용될 경우 시간이 경과할수록 비정상행위 노드가 탐지 및 배제가 이뤄짐으로 전송률이 크게 증가한다. 또한 제안하는 기법에서 발생되는 제어 패킷은 시간 경과에 따라 일정하게 증가하는 것이 아니며 비정상행위 노드의 탐지시 적은 양의 패킷을 발생한다. 이러한 오버헤드는 비정상행위 노드의 탐지 및 배제를 통해 네트워크 전반의 처리율이 향상되는 것을 고려할 때 그 영향은 극히 미미하다.

V. 결 론

애드혹 네트워크는 고정된 인프라가 존재하지 않는다는 점과 연산 능력 및 배터리 용량이 적은 이동성 있는 노드들로만 구성된다는 점 때문에 기존의 보안 메커니즘을 그대로 적용할 수 없다. 또한 통신의 참여 대상이 알 수 없는 다수의 노드들이지만 서로간의 협조 관계를 전제로 네트워크가 구성됨으로 보안 취약성이 존재한다. 이에 본 논문에서는 네트워크 내의 비정상행위 노드를 신속히 탐지 및 배제할 수 있는 기법을 제시하였고 실험을 통해 그 효율성을 입증하였다. 일반적으로 전술 통신용 애드혹 네트워크는 전통 애드혹 네트워크와 다음의 면에서 차별된다. 우선 최초 통신의 참여 대상이 신뢰성 있는 노드들로 구성될 수 있다는 것이고, 또한 사용되는 노드의 특성상 일정부분 계층화도 가능할 것이라 판단되었기에 본 논문에서는 상위계층 노드를 지역내 각 노드들의 가중치를 관리하는 NWMS로 활용하였다. 또한 부당하게 가중치를 부여받는 노드들의 생존성을 유지하기 위해 가중치를 감해주는 알고리즘이 적용되었다. 그리고 기존의 연구에서 간과하였던 정상노드를 비정상노드로 신고하는 악의적인 노드에 대한 관리 방법도 제안하였다.

본 논문에서 제안하는 방법에 따른 모의실험 결과, 비정상적인 행위를 하는 노드에 대한 효과적인 탐색 및 관리를 통해 네트워크 전반의 생존성 및 데이터 처리율이 향상되는 것을 확인 할 수 있었다. 향후에는 본 논문에서 제안하는 기법이 애드혹 네트워크에서의 침입탐지 연구와 관련하여 각종 위협에 대해 효과적인 탐지가 가능한지 추가적인 실험 및 연구를 진행할 예정이다.

참 고 문 헌

[1] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing Pairwise Keys for Secure Communication in Ad hoc Networks: A Probabilistic Approach," Proceedings of the 11th IEEE Conference on Network Protocols(ICNP'03), pp. 326-335, Nov. 2003.

[2] M.G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," In Proceeding of the 2002 ACM workshop on wireless security, pp. 1-10, Sep. 2002.

[3] N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks," Computer Communication, pp. 1627-1637, Nov. 2000.

[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, pp. 24-30, Nov. 1999.

[5] C.K. Toh, Ad Hoc Mobile Wireless Networks: Protocol and Systems, Prentice Hall PRT, Dec. 2001.

[6] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceeding of the 6th International Conference on Mobile Computing and Networking, pp. 255-265, Aug. 2000.

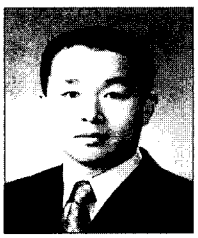
[7] S. Buchegger and J.L. Boudec, "Performance analysis of the CONFIDANT Protocol," Proceeding of the 3rd ACM International Symposium on Mobile ad hoc networking & computing, pp. 226-236, June 2002.

[8] C.K. Toh, C. Lee, and N.A. Ramos, "Next-Generation Tactical Ad Hoc Mobile Wireless Networks," Technology Review Journal, pp. 103-113, Apr. 2002.

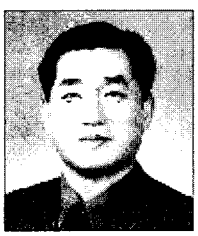
[9] J. Brand and G. Hartwig, "Management of tactical ad hoc networks with C2 data models," Military Communication Conference 2001 IEEE, pp. 915-922, Aug. 2001.

[10] C.E. Perkins, E.M. Royer, and S.R. Das, "Ad hoc on-demand distance Vector(AODV) routing," IETF Internet draft, MANET working group, Jan. 2002.

〈著者紹介〉



이 윤 호 (Yunho Lee) 학생회원
1999년 2월: 육군사관학교 전자공학과 졸업
2005년 2월: 서울대학교 컴퓨터공학과 석사
2009년 1월 ~ 현재: 국방대학교 전산정보학과 박사과정
〈관심분야〉 침입탐지 시스템, XML, 데이터베이스 보안



이 수 진 (Soojin Lee) 정회원
1992년 2월: 육군사관학교 전산학과 졸업
1996년 2월: 연세대학교 컴퓨터과학과 석사
2006년 2월: 한국과학기술원 전산학과 박사
2006년 3월 ~ 현재: 국방대학교 전산정보학과 교수
〈관심분야〉 침입탐지 시스템, 모바일 웹 보안, 네트워크 보안