Ad-hoc 네트워크에서 악의적 노드 관리기법에 관한 연구

김일도* · 김동천**

A study on Management Mechanism of Malicious Node in Ad-hoc Networks

Il-do Kim* · Dong-cheon Kim**

요 약

Ad-hoc 네트워크가 정상적으로 동작하기 위해서는 각 노드가 동등한 권한을 갖고 상호 협조할 때 원활한 통신이 가능하다. 신뢰성을 확보하기 위해 인증된 노드로만 네트워크가 구성이 가능하지만 인증만으로 악의적 행위를 하는 노드를 완전히 배제할 수 없으므로 이들의 행위가 네트워크 전체를 위험에 빠뜨릴 수 있다. 이를 탐지 및 배제해야만 더욱 안전하고 신뢰할 수 있는 네트워크를 유지할 수 있으나 이에 대한 연구는 상대적으로 미흡한 수준이다. 따라서 신뢰 관계에 있는 노드로 구성된 네트워크에서 이기적이거나 악의적인 노드를 탐지하고 배제시켜 결과적으로 네트워크의 안전성과 신뢰성을 유지하고 처리율을 향상시킬 수 있는 방법을 제안한다.

ABSTRACT

An Ad-hoc network will operate properly and provide smooth communication when nodes cooperate mutually with each of them having equal authority. Although it is possible to form a network consisting only of authenticated nodes in order to ensure reliability, authentication by itself is not sufficient to remove malicious nodes and their activities jeopardizing the whole network. Detection and prevention of such activities are vital for maintaining a safe and reliable network, but research on this matter is relatively lacking. Hence a suggestion is made on how to detect and prevent malicious or uncooperative ones among the nodes forming a network by a relationship of mutual trust, thereby maintaining safety and stability of the network and improving its processing abilities

키워드

Ad-hoc 네트워크, 악의적 노드

Key word

Ad-hoc network, malicious nodes

* 해군사관학교 (교신저자, ikim1126@hanmail.net)
** 해군사관학교

접수일자 : 2010. 08. 27
심사완료일자 : 2010. 09. 20

Ⅰ. 서 론

미래의 전장양상은 시시각각으로 변화하는 전장을 한눈으로 가시화 하여야 하고 전투장소 및 시간에 구애됨 없이 시・공간적 제약요소를 극복하여야만 전쟁을 승리할 수 있다. 이에 따라 전쟁수행 수단이 효율적이고 상호 유기적인 협조관계를 유지하기 위해 모든 전장환경을 통합하는 네트워크 중심전으로 변화하고 있다. 이에 우리 군은 미래 전장을 주도할 통신체계 구축을 목표로 차세대 전술정보통신체계 구축을 추진중이다. 더 나아가 미래의 다양한 전장환경을 주도하기 위해 이동성을 가진 노드들 간의 멀티홉을 통해 데이터를 전달하는 Ad-hoc 네트워크 방식으로 운용될 것으로 예상한다.

Ad-hoc 네트워크는 기존의 유무선 네트워크의 고정되어 있는 기반시설 없이 이동 단말만으로 구성된 무선환경의 네트워크를 의미하는데 모든 이동 단말들은 데이터를 송수신할 뿐 아니라 수신한 데이터를 다른 단말에 전달하는 라우터의 기능까지 제공하게 된다. Ad-hoc 네트워크는 기반시설 없이 자체적으로 네트워크 구성 및 유지가 가능하므로 활용도 측면에서 우리 군에서 많은 연구가 이루어지고 있다. 그러나 유기적인 네트워크 변화와 이동성을 보장하는 특성 때문에 각종 보안 위협에 쉽게 노출될 위험에 있어 각 노드들 간 협력적인 상황하에서 좀 더 효율적인 라우팅 프로토콜을 개발하는데 중점을 두었다.

그러나 보안을 기반으로 노드 상호간에 신뢰관계가 형성되었어도 실제 네트워크의 환경은 우호적인 노드들과 상호 협력적인 상황만 존재하는 것은 아니다. Ad-hoc 네트워크의 특성중 하나인 자원 제약 요소를 피하기 위해 이기적인 행위를 하는 노드, 악의적인 목적을 가지고 데이터를 버리는 노드 등 비정상 노드들은 네트워크 전체 성능을 저하시킨다.

이에 본 연구는 내부 위협에 대한 대응방안으로 내부에서 오동작을 유발하는 악의적인 노드를 중점적으로 모니터링하여 그 결과를 기반으로 그 노드에 가중치를 부여한다. 즉, 악의적 행위를 노드 가중치 보안서버(NWSS : Node Weight Security Server, 이하 NWSS)를 운용하여 악의적 행위를 방지할 수 있는 방법을 제시한다.

Ⅱ. 관련연구

2.1 Ad-hoc 네트워크의 보안 취약점

Ad-hoc 네트워크 환경은 모든 노드들이 분산되어 있고, 동적으로 상호 연결하여 역할을 수행한다. 또한 네트워크의 변화에 따라 노드마다 수행할 역할과 서비스 권한이 수시로 변화하는 특징이 있다. 각 노드는 이동성을 가지며, 무선 인터페이스를 사용하기 때문에 유선 네트워크보다 매우 유연한 네트워크의 구성이 가능하다. 하지만 이러한 특징 때문에 유선 네트워크에서 사용하던 보안 기법을 그대로 적용하기에는 다음과 같은 문제점이 존재한다[1].

첫째, 호스트들을 위한 라우터가 지정되어 있는 유선 네트워크와 달리 Ad-hoc 네트워크에서 각 노드는 호스트의 기능을 수행하면서 동시에 다른 노드들을 위해 패킷을 전달해주는 라우터 기능을 수행하게 되는데 유선에서는 네트워크를 내부와 외부로 구분해주는 라우터에 보안대책을 수립할 수 있으나 Ad-hoc 네트워크에는 이런 라우터가 없다는 문제점이 있다.

둘째, 무선 채널의 공유로 합법적인 노드와 악의적인 의도를 가진 비합법적인 노드가 모두 무선 채널에 접속할 수 있으므로 누구나 쉽게 네트워크를 공격할 수 있다. 이를 보완하기 위해 키 관리 메커니즘을 포함한 암호학적 보안 대책이 필요한 것이다.

셋째, 네트워크를 구성하는 노드의 자원이 유선 네트워크에 비해 매우 제한되어 있다는 것이다. 이동 노드의 특성상 배터리로 전원을 사용하므로 내부의 암호화 또는 외부 공격으로 인한 오버헤드가 많이 발생할 경우, 성능 제한 및 자원 고갈로 인해 네트워크에서 배제 될 수 있다.

넷째, 노드들의 이동성과 상태 변화에 따라 네트워크의 토폴로지가 동적으로 변화된다는 점이다. 하지만 노드들은 언제, 어디서나 네트워크로부터 안전한 통신 서비스를 제공받기를 원한다. 이처럼 Ad-hoc 네트워크는 그 특징으로 인한 장점이 있는 반면, 이러한 동적 변화들이 보안상 취약점으로 작용하기도 한다.

Ad-hoc 네트워크에 대한 위협은 크게 외부 위협과 내부 위협으로 구분할 수 있다[2]. 외부 위협은 네트워크 외부로부터 잘못된 라우팅 정보를 삽입하여 악용하는 위협과 이전의 라우팅 정보를 재생하여 악용하는 위협,

라우팅 정보를 변형하는 위협 등으로 분류할 수 있다. 외부 위협을 통해 공격자는 네트워크를 분할하거나 네트워크에 극심한 트래픽을 유발하여, 전체 네트워크 시스템에 장애를 일으킬 수 있다. 이러한 외부 위협은 적절한 키 관리 보안 알고리즘을 적용하는 방법과 침입탐지시스템을 이용하는 방법으로 일정부분 위협을 해소할 수 있다.

내부 위협은 네트워크 내의 훼손된 노드들이나 악의적 노드들로 인해 발생한다. 악의적인 목적으로 데이터 패킷을 자신에게 송신한 후 이를 버리거나, 자신의 에너지 소모를 줄이기 위해 데이터를 버리는 행위, 네트워크 성능 저하를 목적으로 다른 노드들에게 잘못된 정보를 제공하는 행위, 네트워크 와해를 목적으로 임의의 노드를 거짓 신고하는 행위 등이다. 이러한 내부 위협은 외부 위협과 같이 키 관리 보안 알고리즘을 적용해도 쉽게 해결되지 않는다. 내부 위협을 가하는 노드 자체가 이미 같은 보안 적용을 받고 있는 노드이기 때문이다. 이를 해결하기 위해서는 키 관리, 인증, 침입탐지 등을 통한 보안 적용 외에 악의적 노드를 관리하는 추가 보안 알고리즘이 필요하다.

본 연구에서는 내부 위협에 대한 대응 방안으로 네트워크 내 악의적 노드를 탐지 및 배제하여 네트워크 신뢰도를 향상시키는 방안을 제시한다.

2.2 악의적 노드 관리의 기존 연구 및 문제점

Ad-hoc 네트워크에서의 연구는 주로 노드들이 서로 간의 협력을 바탕으로 원활한 라우팅이 이루어진다고 가정하고 있지만 동일 목적을 갖는 네트워크에도 내/외부의 공격 또는 자원 제약적인 환경에 의해 비정상적으로 동작하는 노드가 발생할 수 있다. 이런 노드는 각 노드간 유기적 협력이 필요한 Ad-hoc 네트워크에서 문제를 일으킬 수 있다. 기존에도 이러한 악의적 노드를 탐지 및 배제하기 위한 연구들이 이루어졌으며 연구 내용은 다음과 같다.

2.2.1 Watchdog & Pathrater

이는 네트워크의 모든 노드들이 자신의 주변에 있는 노드들을 감시함으로써 이기적인 노드를 탐지하는 방법에 기반을 두고 있다. Watchdog는 패킷 전달을 거부하는 노드를 감지하고 이를 바탕으로 Pathrater가 악의적인 노드를 피해 최선의 경로를 찾을 수 있도록 도와준다[3]. 하지만 Watchdog와 Pathrater에는 몇 가지 문제점이 존재한다.

첫째, 이기적인 노드로 판명되는 절차가 단순하여 특정 노드가 이기적인 노드로 오해를 받을 수 있고, 이기적인 노드로 판명되었음에도 아무런 불이익이 가해지지 않는다는 것이다. 이기적인 노드로 판명되면 Pathrater는 경로 설정 시 이를 고려하여 해당 노드를 우회하는 라우팅 경로를 설정하게 되는데, 이렇게 될 경우 이기적인 노드가 처리해야 할 트래픽을 주변의 다른 노드가 처리해야 하므로 오히려 이기적인 노드가 에너지를 절약할 수 있게 해준다.

둘째, 이기적인 노드는 언제든지 네트워크에 참여할 수 있으므로 오히려 이기적인 노드에게 유리하게 작용할 수도 있다.

2.2.2 CONFIDANT

CONFIDANT(Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks)는 Watchdog과 비슷하게 각 노드들이 서로를 감시하면서 이기적인 노드를 탐지하는 메커니즘이다[4]. 그러나 Watchdog을 이용한 메커니즘과는 달리, 악의적인 노드를 감지하고 그 노드들을 피해 메시지를 보내게 하는 것에서만 그치는 것이 아니라, 그런 노드들을 네트워크에서 고립시켜 네트워크의 서비스를 이용하지 못하도록 한다.

CONFIDANT에서는 노드에 대한 정보를 다음 두 가지로 구분한다. 이기적 행동에 피해를 입은 노드에게서 온 정보와 간접적으로 그런 정보를 확인한 노드에게서 온 정보로 구분하여 서로 다른 가중치를 둔다. CONFIDANT는 각각의 노드에 이웃 감시자와 신뢰 관리자를 설치하여 운영한다. 이웃 감시자는 정상적인 라우팅 행동에서 벗어나는 일탈 행위를 감시한다. 만약 특정 노드가 비정상적인 행동을 하게 되면 신뢰관리자에게 알람 메시지를 보내게 된다.

2.2.3 MP-SAR 프로토콜

MP-SAR 프로토콜은 보안노드를 발견할 뿐만 아니라 일반노드를 경유하는 다중경로를 발견한다[5]. 최단경로를 결정하고 선택된 일반경로는 임시적인 보안채널을 설정하도록 데이터 암호 키 교환을 한다. 그러나 검출된 노드에 대한 주기적인 관리가 없어 보안 경로가 바뀌었을 때 악의적인 노드가 네트워크에 참여할 수 있는 문

제점이 있다.

2.2.4 기존 연구의 문제점

비정상행위 탐지 및 관리 방법과 라우팅 참여를 유도하는 방법을 제안한 기존의 연구들의 문제점을 종합해 보면 다음과 같이 정리할 수 있다.

첫째, 모호한 통신 충돌로 인해 다음 노드의 전송여부 즉, 정상적인 행위인지 아닌지를 탐지하지 못하는 경우가 발생 가능하다. 그림 1과 같이 노드 A가 노드 B의 전송여부를 확인하고 있는데 노드 S가 A에게 패킷을 전송할 경우 노드 A는 노드 B가 정상적으로 전송을 했음에도 노드 B를 비정상 노드로 판단할 수 있게 된다.

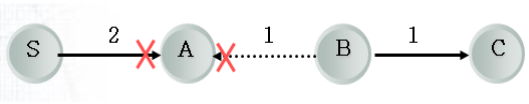

그림 1. 비정상 노드 탐지 기법에서의 문제점
Fig. 1 Problem of anormaly node detection method

둘째, 특정 노드가 악의적인 목적을 갖고 정상적인 노드를 비정상 노드로 신고할 경우에 대한 연구나 대응방법이 미흡하다. 악의적인 노드는 패킷 드롭과 같은 비정상 행위에 대한 신고 절차를 악용하여 임의의 노드를 거짓 신고 할 수 있다. 즉, 악의적인 범인 지목행위가 발생 가능하다.

셋째, 비정상 행위 노드가 임계치를 초과하지 않는 범위 내에서 지속적으로 이동해 가며 비정상 행위를 계속하는 경우, 이를 해결할 방법이 없다.

넷째, 정상적으로 동작하는 노드가 임계치 초과로 인해 고립되어 네트워크로부터 배제될 수도 있다. 그 이유는 비정상 행위에 대한 탐지 방법상 순간적인 오류로 인한 통신 실패나 통신 충돌 등으로 비정상행위 노드로 신고 될 수도 있기 때문이다. 이러한 문제점을 해결하기 위해 본 연구에서는 NWSS를 이용한 악의적 노드 탐지 및 관리 방법을 제시한다.

Ⅲ. NWSS를 이용한 악의적 행위 관리

3.1 각 노드들의 임무 및 기본 탐지 절차

먼저 악의적 노드의 탐지 및 보고는 일반 노드가 수행한다. 탐지 방법은 기존의 연구들과 마찬가지로 다음 노드에 대해 엿듣는 방법을 사용하지만 보고 및 관리 방법은 차별화 된다. 기존의 연구에서는 각각의 노드가 악의적 노드를 발견하였을 때, 이를 송신지 노드로 보고하고 송신지 노드는 스스로 사전 정의된 임계치 값을 통해 악의적 노드의 여부를 판단한다. 이를 활용한 새로운 라우팅 경로를 갱신하여 경로 상에 있는 노드에게 전파하는 방법을 사용한다.

본 연구에서 제안하는 방법은 송신 노드가 목적 노드로 데이터를 전송하는 경우 경로 상에서 악의적 노드가 확인되면, 이를 확인한 노드는 송신노드에게 이 사실을 알리게 된다. 신고를 받은 송신노드는 다중 경로를 이용한 라우팅 방법에 따라 자신의 라우팅 테이블에 존재하는 다른 경로를 통해 목적지로 데이터를 전송하며, 또한 신고 사실을 전파한다.

목적지 노드는 수신한 데이터를 버퍼에 저장하고, 신고 내용이 사실임을 판단하여 RREP(Route Reply)메시지에 악의적 노드를 포함하여 이를 송신지 노드로 전송한다. 이때 RREP메시지에서 경로를 신뢰할 수 없거나, 일방향성 경로인지를 확인할 때 사용하는 인지 요청 비트를 'A'로 설정하여 전송을 하며, 경로상의 노드들은 비정상 행위 노드에 대해 자신의 'suspect' 목록에 저장한다. RREP 메시지를 받은 송신 노드는 정상 수신을 알리는 RREP-Ack 메시지를 목적지 노드로 전송하고, 노드의 가중치를 관리하는 NWSS에 비정상 행위 노드를 신고한다. 목적지 노드는 RREP-Ack 메시지를 받으면 버퍼에 있던 데이터를 저장하고 송신지 노드와 마찬가지로 NWSS에 비정상행위 노드를 신고한다. 이로써 데이터의 송수신 및 비정상 행위 노드의 신고/전파가 완료된다.

송신지 노드와 목적지 노드로부터 신고를 받은 NWSS는 두 메시지의 도착 시간과 신고 내용을 분석하여 정상적인 신고인지 아닌지를 판단하고 정상적인 신고이면, 해당 노드의 가중치를 증가시킨다. 이러한 과정을 통해 악의적 행위 노드의 탐지 및 NWSS의 신고 접수가 수행된다. 송신지 노드와 목적지 노드가 모두 신고를 하는 것은 Ad-hoc 네트워크의 기본 운용 개념인 분산과 협동 때문이다. 즉, 원활한 통신을 위해서도 협동이 필요하지만, 비정상행위를 탐지 할 때도 이 개념이 필요한 것이다. 이러한 협동이 이루어지지 않으면 다른 노드를 비정상노드라고 신고하는 악의적인 노드를 판단해 내기가 매우 어렵다.

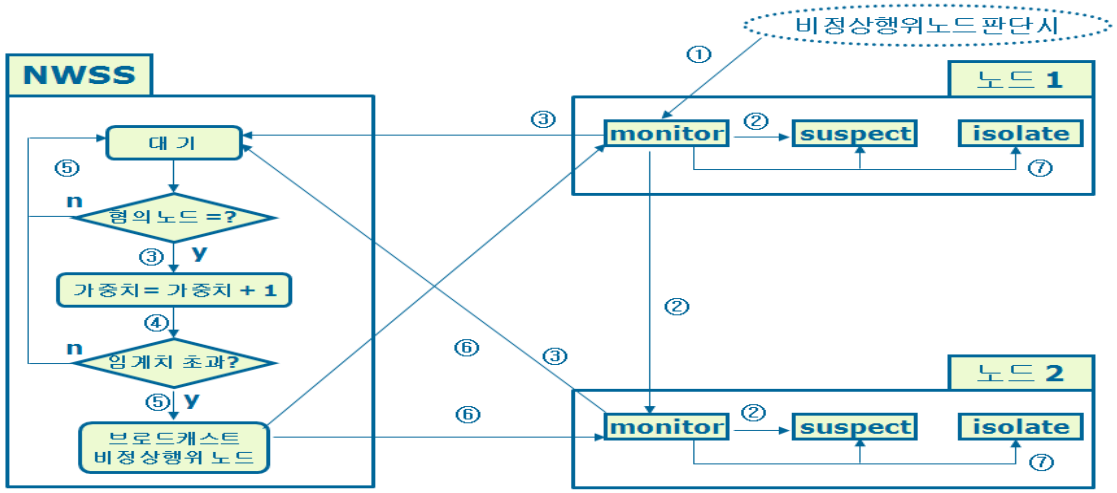

그림 2. 악의적 노드 탐지 시 동작절차
Fig. 2 Operation process of malicious node detection case

3.2 악의적 노드 판단 및 NWSS 동작절차

악의적 노드의 판단은 송신지 노드와 목적지 노드의 협동에 의해 이루어지게 된다. 하지만, 이들에 의해 NWSS에 신고가 되었다고 해서 협의노드가 완전히 네트워크에서 고립되는 것은 아니다. 아직 협의 노드가 완전히 악의적 노드로 판단되지 않았기 때문이다. 완전한 악의적 노드의 판단은 이들의 보고를 받은 NWSS에 의해 이루어진다. NWSS는 송신지 노드와 목적지 노드의 협의 노드에 대한 신고를 받고, 각각의 노드가 신고한 협의 노드가 일치하는 지를 확인한 후, 이것이 일치하면 악의적 노드로 판단하여 해당 노드에 가중치를 부여하게 된다. NWSS와 송신지, 목적지 노드의 동작 관계는 그림 2와 같다. 목적지 노드는 협의노드를 판단 후, 이를 송신지 노드와 공유하여, 협의 노드를 NWSS에 신고한다. 신고를 받은 NWSS는 일정 시간 내 도착한 두 신고를 비교하여, 협의 노드가 동일한지를 판단하고 동일한 경우 해당 노드에 가중치 1을 부여한다. Ad-hoc 네트워크는 IP 기반으로 동작한다. 그러므로 악의적인 노드는 네트워크 내 임의의 노드를 신고할 수 있다. 하지만 제안하는 방법과 같이 송신 노드와 목적 노드의 협업에 의해 악의적 노드를 판단하게 되면 이런 문제점을 해결할 수 있다.

해당 노드의 가중치가 계속 증가하면 비정상행위가 지속되는 것으로 판단할 수 있으며, 가중치가 임계치를 초과할 경우 NWSS는 이를 브로드캐스트하고, 이 메시지를 받은 각 노드는 해당 노드를 'isolate'에 등록하여 해당 노드의 메시지에 응답하지 않음으로써 노드를 고립시킨다. 임계치와 가중치를 사용하는 것은 비정상 행위로 네트워크에서 고립시키기 전에 좀 더 신중을 기하기 위함으로 정상적인 노드임에 불구하고 오인 신고 되는 경우, 이러한 노드들의 네트워크 참여를 허가하기 위함이다. 즉, 실제 비정상행위 노드와 통신상의 오류로 인해 비정상노드로 신고 받은 노드에 대한 허용치(tolerance)를 부여하는 것이다.

만약 통신상의 오류 등으로 인해 정상적인 노드가 부당한 가중치를 부여 받았다면 이에 대한 구제 방법이 존재해야 한다. 그래서 각 노드에 'suspect'를 유지함으로써 경로상의 인접 노드가 정상적으로 동작할 경우, 이를 통해 가중치를 줄이는 방법을 사용한다. 'suspect'에 있는 노드 정보는 라우팅 경로 설정과는 무관하며, 부당하게 가중치를 부여 받은 노드에 대한 구제에만 사용되게 된다.

'suspect'는 앞서 언급한 것과 같이 정상 노드임에도 불구하고 악의적 노드로 부당한 가중치를 부여받은 노드에 대한 구제에 사용된다. 한 노드가 라우팅 경로상의 다음 노드를 'suspect'에 가지고 있을 경우, 데이터 전송 시 그 노드가 정상적으로 라우팅에 참여한다면 'suspect'

를 보유하고 있는 노드는 해당 노드의 값을 '1'씩 줄이고 그 노드에 대해 NWSS에 보고한다. 보고를 받은 NWSS는 해당 노드의 가중치를 확인하고 '0'이 아닐 경우 해당 노드에 대한 가중치를 '0.1' 만큼 감소시키고, '0'일 경우 보고한 노드에게 'suspect' 목록에서 해당 노드의 정보를 지울 것을 지시한다. 지시를 받은 노드는 suspect 목록에서 해당 노드의 정보를 삭제한다. 노드가 목적지 노드로부터 전송된 혐의 노드를 포함한 RREP 메시지를 수신하였을 경우 자신의 suspect 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. 부당하게 가중치를 받은 노드에 대한 구제 절차로 한 노드가 정상행위를 확인하였을 경우 한 노드는 다음 노드의 행위를 감시할 때 'suspect' 목록을 참조한다. 다음 노드가 정상 동작을 하였을 경우 'suspect' 목록에 있으면 NWSS에 보고하고 해당 노드의 count를 '1'만큼 감소시킨다.

제안하는 방식에서는 통신 오버헤드를 줄이기 위하여 신고 및 보고 제어 패킷은 유니캐스트로 처리하며, 비정상행위 노드가 NWSS에서 판별되었을 경우에만 신속한 공유를 위해 브로드캐스트로 전파하였다. 이는 비정상행위 노드의 탐지시간을 줄이고, 탐지율을 높이는데도 효과적이다. NWSS는 가중치가 '0'이 된 노드에 대해 'suspect' 관련 보고가 들어올 경우 이를 삭제 지시하여 노드의 불필요한 패킷이 발생하는 것을 방지하며, 각 노드는 'suspect' 목록의 노드 count가 '0'이 되거나 NWSS로부터 특정 비정상행위 노드에 대한 전파를 받았을 경우 'suspect' 목록에서 해당 노드의 정보를 삭제하여 통신 오버헤드 및 메모리 사용량을 줄일 수 있다.

Ⅳ. 성능분석

4.1 실험환경 및 시나리오

모의실험은 NS-2를 사용하였으며 라우팅 프로토콜은 AODV상에서 비교가 가능하도록 실험하였다. 주요 실험내용은 노드 수 변화에 따른 네트워크 처리율, 비정상행위 노드 포함율에 따른 손실율에 대해 비교 분석하였다. 모의실험을 위해 설정되는 주요 설정 값은 표 1과 같다.

표 1. 모의실험 주요 설정 값
Table. 1 Main setup value for simulation

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

실험은 좀 더 다양한 결과를 산출하기 위해 네트워크 내에 정상적인 노드 수와 악의적 노드 수를 변경시켜 가며 실시하였으며, 데이터 전송 시 다음 노드로 정상적으로 포워딩 하지 않고 이를 버렸을 경우 이전 노드가 이를 탐지하여 NWSS에 보고하고, NWSS는 이에 대한 관리 및 해당 노드의 가중치가 임계치 초과시 이를 전파하여 악의적 노드를 배제시키는 방식으로 진행하였다.

4.2 악의적 행위 노드수에 따른 패킷 처리량

추가자료 네트워크 내 비정상행위 노드가 각각 25, 50개가 존재할 경우 AODV와 제안하는 방법의 패킷 처리량을 보여준다. 트래픽 발생주기가 100ms이므로 100초당 발생하는 패킷의 수는 최대 1000개가 된다. 그림 3에서 볼 수 있듯이 패킷 처리량은 100초 단위로 종합되었으며, AODV의 경우 평균 40~60%의 처리율을 나타내고 있으며, 제안된 방법에서는 악의적 노드가 25개일 경우와 50개일 경우 시간의 흐름에 따른 처리량이 변화를 확인할 수 있다.

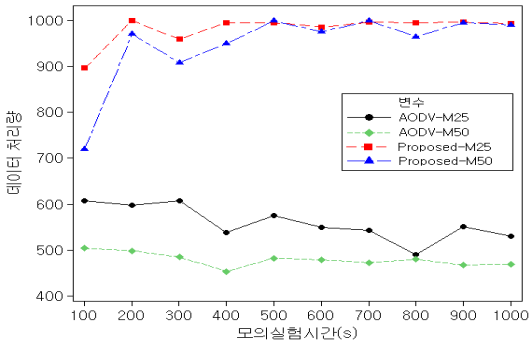

그림 3. 악의적 노드수 변화에 따른 패킷 처리량
Fig. 3 Packet processing quantity due to variation of malicious node number

4.3 노드 수 증가 대비 손실 패킷 수

총 노드 수 대비 비정상행위 노드가 각각 10, 30% 존재할 경우 노드 수가 증가함에 따른 손실 패킷 수를 보이고 있다. 그림 4에서도 알 수 있듯이 총 노드 수가 증가할수록 손실되는 패킷 수도 증가함을 알 수 있다. 그 이유는 포함율은 일정하나 총 노드 수가 증가함에 따라 그만큼 비정상행위 노드가 많이 존재 하기 때문이다. 하지만 AODV의 경우 총 노드 수가 증가할수록 손실되는 패킷 수가 크게 증가하는 반면, 제안 방법이 적용될 경우는 총 노드 수와 비정상행위 노드 수가 증가해도 시간이 경과할수록 비정상행위 노드가 탐지 및 배제가 이루어지기 때문에 큰 변화가 없다. 또한 비정상행위 노드가 10%일 경우와 30%일 경우 약간의 차이가 발생하는데, 이는 실험 초기 즉, 비정상행위 노드가 탐지 및 배제가 되기 전에 손실되는 패킷량의 차이가 반영된 것이다.

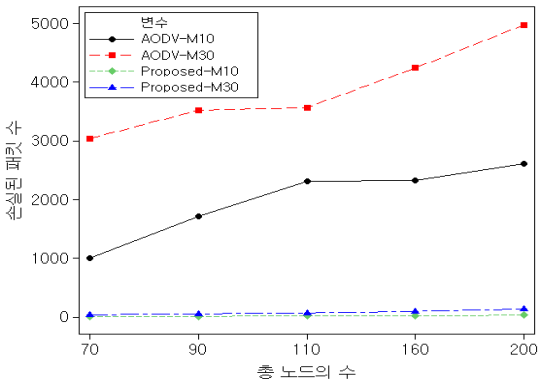

그림 4. 악의적 노드 포함율에 따른 손실 패킷 수
Fig. 4 Lossin packet number by malicious node contain rate

4.4 라우팅 오버헤드

본 연구를 통해 제안하는 방식이 적용될 경우 당연히 기존 라우팅 프로토콜에 비해 오버헤드가 약간 늘어날 수 밖에 없다. 그 이유는 제안하는 방법이 적용되지 않은 프로토콜에서는 악의적 노드의 탐지 및 관리를 위한 제어 패킷이 발생하지 않으며 그에 따라 평균 전송률 또한 큰 변화가 없는 반면 제안 방법이 적용된 경우는 모의실험 시간동안 탐지 및 전파를 위한 매우 작은 크기의 제어 패킷이 발생하기 때문이다. 추가적으로 발생하는 패킷은 악의적 노드를 유니캐스트로 신고하는 패킷과 NWSS가 악의적 노드라고 판단하였을 때 지역 내 노드로 전파하는 브로드캐스트 패킷이 추가되는 것이다. 신고 및 비정상행위 노드 전파 시 발생되는 오버헤드는 식 (1),(2),(3)과 같이 표현할 수 있다.

초당 패킷 발생수를 t, 평균 라우팅 경로 포함 노드 수를 p, 패킷 사이즈를 NP_{size}, 총 노드수를 N, 악의적 노드 수를 M, 신고 및 전파 제어 패킷 사이즈를 CP_{size}, 임계치를 threshold, 모의실험 시간을 T, 신고노드로부터 NWSS까지의 경로에 포함되는 평균 노드수를 n 이라고 할 경우,

신고 노드가 NWSS에 유니캐스트로 신고 시 발생하는 오버헤드(U)는

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

NWSS가 악의적 노드를 브로드캐스트시 발생하는 오버헤드(B)는

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

실험 시간동안 발생하는 총 통신량 대비 오버헤드(O)는

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

신호의 발생주기가 100ms, 패킷 사이즈는 128Byte, 총 노드 수 250, 악의적 노드 수 10, 신고 및 전파 제어 패킷 사이즈 20Byte, 임계치 5, 모의실험 시간 1000s, 라우팅 경로에 포함되는 평균 노드 수를 5, 신고노드로부터 NWSS까지의 경로에 포함되는 평균 노드 수를 7 이라고 할 경우, 신고노드로부터 NWSS에 유니캐스트로 신고 시 발생한는 오버헤드는

= 7 X 20 X 5 X 10 = 7000 Byte

NWSS가 악의적 노드를 브로드캐스트 시 발생하는 오버헤드는

= 10 X 20 X 250 = 50000 Byte

실험 시간동안 발생하는 총 통신량 대비 오버헤드(O)는

= $$\frac{7000+5000}{1000 \times 10 \times 5 \times 128}$$ = 0.0089 이다.

즉, 악의적 노드의 탐지 및 배제를 위해 추가적으로 발생하는 오버헤드는 총 통신량 대비 약 0.89%이나 패킷 처리량은 적용하지 않았을 경우보다 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 비정상행위가 탐지 및 배제되므로 전송률이 크게 증가한다. 즉, 제

어 패킷은 시간 경과에 따라 함께 증가하는 것이 아니며 악의적 노드의 탐지시마다 적은 양의 패킷이 발생하게 된다. 하지만 이러한 오버헤드는 악의적 노드의 탐지 및 배제를 통해 네트워크 전반의 처리율이 향상되는 것을 고려 시 그 영향은 극히 적다.

V. 결 론

Ad-hoc 네트워크는 고정된 인프라가 존재하지 않는다는 점과 연산 능력 및 배터리가 작은 이동성 있는 노드들로만 구성된다는 점 때문에 기존의 보안 메커니즘을 그대로 적용할 수 없다. 또한 통신의 참여 대상이 다수의 노드들로, 분산과 협동의 개념에서 네트워크가 구성되기 때문에 보안에 더욱 어려움을 지닐 수밖에 없는 환경이다. 이에 네트워크를 구성하는 각 노드는 서로 신뢰할 수 있어야 하나, 모든 노드가 정상적으로 동작하지는 않는 문제점이 존재한다. 이에 본 연구에서는 이러한 비정상적으로 동작하는 노드를 신속히 탐지 및 배제에 중점을 두었다.

본 연구에서는 지역 내 각 노드들의 가중치를 관리하는 NWSS 서버를 활용하고 부당하게 가중치를 부여받는 노드들의 생존성을 유지하기 위해 가중치를 감해주는 알고리즘이 적용되었다. 또한 기존의 연구에서 간과하였던 정상노드를 비정상노드로 신고하는 악의적인 노드에 대한 관리 방법도 제안하였다.

본 연구에서 제안하는 방법에 따른 모의실험 결과, 비정상적인 행위를 하는 노드에 대한 효과적인 탐색 및 관리를 통해 네트워크 전반의 생존성 및 데이터 처리율이 향상되는 것을 확인할 수 있었다. 본 연구는 보안성이 강화된 차세대 전술정보통신체계 구축에 기여할 것으로 판단되며, 추가적으로 Ad-hoc 네트워크에서의 침입탐지 연구와 연계하여 각종 위협에 종합적으로 대응을 할 수 있는 시스템 연구에도 도움이 될 수 있을 것으로 판단된다. 그러나 비정상행위 노드는 불특정하게 발생하므로 다양한 비정상행위 노드 수에 대한 타 라우팅 프로토콜에 대한 비교 연구도 수행할 가치가 있을 것이다.

참고문헌

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

[2] D. Nguyan, L.Zhao, P.Uiswang and J.Plat, "Security Routing Analysis For Mobile Ad-hoc Networks" Interdisciplinary Telecommunications program of Colorado univ, spring 2000

[3] S. Marti et al., "Mitigating routing misbehavior in Mobile Ad Hoc networks," ACM MOBICOM, 2000.

[4] Sonja Buchegger and Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-hoc NeTworks," ACM MobiHOC, 2002.

[5] In Sung Han et al., "Multi-Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network," ichit, pp.620-626, 2006 International Conference on Hybrid Information Technology-Vol 1, 2006.

저자소개

김일도(Il-do Kim)

고려대학교 전산학과 박사
해군사관학교 교수

※관심분야 : 데이터베이스 보안, NCW 보안, 센서네트워크 보안

김동천(Dong-cheon Kim)

국방대학교 전산정보학과 석사
해군사관학교 전임강사

※ 관심분야 : 침입탐지 시스템, 노드 인증