한국군사과학기술학회지 제12권 제3호, pp. 333～343, 2009년 6월

학술논문 정보기술 부문

전술 Ad-hoc 네트워크에서의 비정상행위 노드 탐지 및 관리

Detection and Management of Misbehaving Node in Tactical Ad-Hoc Networks

장 범 근* 이 수 진**
Beomgeun Jang Soojin Lee

Abstract

Tactical Information Communication Network(TICN) is a concept-type integrated Military Communication system that enables precise command control and decision making by unifying the diversified military communication network and conveying diverse range of battle field information on real-time, at right place at right time. TICN is designed to advance into high speed, large capacity, long distance wireless relay transmission. To support mobility in battlefield environments, the application of Ad-hoc networking technology to its wireless communication has been examined. Ad-hoc network is consist of mobile nodes and nodes in the network depends on the cooperation of other nodes for forwarding of packets. In this context, some non-cooperating nodes may delay forwarding of packets or drop the packets. This may hamper the network as a whole and disrupt communication between the cooperating nodes. To solve this problem, we present a solution with a Node Weight Management Server(NWMS), which manages each node's weight according to its behavior in local area. When the NWMS detects misbehaving node, it increases the node's weight. If the node's weight exceeds a predefined threshold then the NWMS broadcasts the node's information into network to isolate the misbehaving node from the network. These mechanisms show that they are highly effective and can reliably detect a multitude of misbehaving node.

Keywords : Node Weight Management Server(NWMS), Ad-Hoc Network, Threshold, Misbehaving Node(비정상행위 노드), Weight(가중치)

1. 서 론

우리 군은 미래전에 대비 전술 C4I체계를 비롯한 응용정보체계의 막힘없는 전송 및 통신망간의 연동 요구를 만족시키고 미래 전장을 주도할 통신체계 구축을 목표로 차세대 전술정보통신체계(TICN : Tactical Information Communication Network) 구축을 추진중이다. 차세대 전술정보통신체계는 무선환경의 제약사항

† 2009년 2월 27일 접수～2009년 4월 17일 게재승인
* 육군전투지휘훈련단(BCTP)
** 국방대학교(KNDU)
책임저자 : 장범근(open3031@naver.com)

을 극복하고, 통신지원의 광역화 및 고속·대용량의 정보처리를 가능하게 함으로써 신속하게 전개되는 정보를 수직, 수평적으로 전송하여 전장 가시화와 실시간 정밀타격 등 통합전투력을 발휘하게 하는 미래의 전술통신체계이다[1].

TICN에서는 각종 정보가 하위제대로부터 상급제대까지 더욱 원활하게 유통되는 것을 지원하기 위해 체계내의 일부 무선 구간에 Ad-hoc 네트워크 기술을 적용할 예정이다. Ad-hoc 네트워크는 자가 네트워크 구성 및 유지가 가능하기 때문에 군의 전술상황, 긴급재난상황 등 다양한 분야에 적용이 가능하다. 이에 관련 기술 분야의 연구도 활발하게 이루어졌으나 대부분의 연구는 네트워크를 구성하는 각 노드들이 상호 우호적이고 협력적인 상황을 가정하여 무선 채널 접속이나 다중 홉 라우팅에 중점을 두고 좀 더 효율적인 라우팅 프로토콜을 개발하는데 중점을 두었다.

그러나 보안을 기반으로 노드 상호간에 신뢰관계가 형성되었어도 실제 네트워크의 환경은 우호적인 노드들과 상호 협력적인 상황만 존재하는 것이 아니다. Ad-hoc 네트워크의 특성중 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 비정상 행위를 하는 노드들이 존재할 수 있으며, 이러한 노드들에 의한 비정상 행위들은 네트워크의 전체 성능을 저하시킬 뿐만 아니라, 정상적인 노드의 에너지 소모를 가중시켜 최악의 경우 네트워크 분할을 유발할 수도 있다.

특히, 군에서 운용하는 Ad-hoc 네트워크 내 비정상 행위 노드의 존재는 신속하고 정확한 정보 전달 및 보고체계가 이루어져야 하는 전장환경에서 더욱 큰 문제점으로 작용할 수 있다.

Ad-hoc 네트워크를 각종 위협으로부터 보호하기 위한 대책은 예방과 대응으로 나눌 수 있다[2]. 예를 들어 라우팅 경로를 설정하는 단계에서 키 관리 등의 보안 알고리즘을 적용하여 악의적인 노드를 식별해 내고 해당 노드를 제외시킴으로써 상호 신뢰할 수 있는 우호적 노드들로만 경로를 설정하는 방식은 예방 차원의 대책이다. 이에 반해, 대응은 좀 더 능동적인 차원의 대책으로 예방을 통해 신뢰 노드로 이루어진 네트워크가 구축 되었지만 공격자에 의해 잠식(compromised)되어 내부적인 오동작을 일으키거나, 자원 제약을 극복하기 위해 이기적인 행위를 하는 경우 해당 노드를 찾아내고 적절한 조치를 취하는 방식이며, 침입탐지 시스템이 대표적인 대응책이다.

본 논문은 대응에 관한 내용을 주로 다루고 있다. 기존의 대응과 관련된 연구들은 대부분 특정 노드가 데이터를 버리는 등의 이기적인 행위 탐지에 중점을 두고 분산된 노드들 간의 협동을 통해 탐지하는 방식을 취하고 있다. 즉, 잘못된 행위를 하는 노드를 중심으로 한 주변 노드들의 모니터링 결과에 기반을 두고 비정상 행위의 발생 여부를 판단한다.

그러나 기존의 접근방법들은 네트워크에 속한 노드들의 협동을 전제로 한 탐지라고는 하지만, 특정 노드가 거짓으로 다른 노드를 모함하여 신고함으로써 정상적인 노드가 네트워크에서 배제되는 악의적인 범인지목행위(malicious accusation)가 발생할 가능성이 존재한다. 이러한 문제는 협동을 전제로 하면서도 각 노드들의 협동 탐지 결과를 제대로 종합하지 못하거나 지속적으로 관리하지 못함으로써 생기는 문제라 할 수 있지만, 대부분의 기존 연구들이 이를 간과하거나 효과적인 해결책을 제시하지 못하고 있다.

이러한 문제점을 해결하기 위해 본 논문에서는 전술통신체계의 계층화된 구조를 최대한 활용하여 상위노드(MSAP : Mobile Subscriber Access Point, 이하 MSAP)를 노드 가중치 관리서버(NWMS : Node Weight Management Server, 이하 NWMS)로 설정 운용함으로써, 각 노드들이 지역적으로 탐지한 결과를 효율적으로 관리하고 악의적인 범인지목행위를 방지할 수 있는 접근방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 Ad-hoc 네트워크의 보안 취약점을 기술하고, 3장에서는 비정상적 행위를 하는 노드들의 탐지 및 대응과 관련된 기존 연구들에 대해 살펴본다. 4장에서는 본 논문에서 제안하는 NWMS를 이용한 비정상 행위 탐지 및 관리 기법에 대해 기술하고, 5장에서는 제안된 기법에 대한 모의실험 결과를 기술한다. 마지막으로 6장에서 연구 결과를 요약하고 결론을 맺는다.

2. Ad-hoc 네트워크의 보안 취약점

Ad-hoc 네트워크 환경은 모든 노드들이 분산되어 있고, 고정된 기반구조의 지원을 받을 수 없기 때문에 모든 노드가 공평하게 역할을 나누고 그에 대해 수행해야 하는 의무와 그를 통한 서비스 권한을 갖는다는

특징이 있다. 또한 각 노드가 이동성을 가지며, 무선 매체를 사용하기 때문에 유선 네트워크보다 유연한 네트워크의 구성이 가능하다.

그러나 Ad-hoc 네트워크만이 가지는 다음과 같은 고유한 특징들로 인해 기존 유선 네트워크에서 사용하던 보안 기법을 그대로 적용할 수는 없다[2].

첫째, Ad-hoc 네트워크에서 각 노드는 호스트의 기능을 수행하면서 동시에 다른 노드들을 위해 패킷을 전달해주는 라우터 기능을 수행하게 된다. 즉, 유선 네트워크에서처럼 라우터 자체에 대해 내·외부적인 보안대책을 수립할 수 없다.

둘째, 무선 채널의 공유로 합법적인 노드와 악의적인 의도를 가진 비합법적인 노드가 모두 무선 채널에 접속할 수 있으므로 더욱 쉽게 네트워크가 공격당할 수 있는 보안 취약점을 가지고 있다.

셋째, 네트워크를 구성하는 노드의 자원이 유선 네트워크에 비해 매우 제한되어 있기 때문에 암호학적 메커니즘의 실행이나 외부 공격 등으로 인해 오버헤드가 많이 발생할 경우, 자원 고갈로 말미암아 네트워크에서 배제될 수도 있다.

넷째, 노드들의 이동성과 상태 변화에 따라 네트워크의 토폴로지가 매우 동적으로 변화한다. 그러므로 노드들은 언제, 어디서나 네트워크로부터 안전한 통신 서비스를 제공받기를 원함에도 불구하고 특정 노드는 보호받지 못하는 상태에서 공격대상이 될 수 있다.

이처럼 Ad-hoc 네트워크는 유선 네트워크와는 차별되는 고유한 특징으로 인해 많은 장점을 가지고 있긴 하지만, 또한 그러한 요소들이 보안상 취약점으로 작용하기도 한다.

Ad-hoc 네트워크에 대한 위협은 크게 외부 위협과 내부 위협으로 구분할 수 있다[3]. 외부 위협은 네트워크 외부로부터 잘못된 라우팅 정보의 삽입을 통한 위협과 이전의 라우팅 정보를 재생하여 악용하는 위협, 라우팅 정보를 변형하여 네트워크에 위험을 가져오는 위협 등으로 분류할 수 있다. 외부 위협을 통해 공격자는 네트워크를 분할하거나 네트워크에 극심한 트래픽을 유발하여, 전체 네트워크 시스템에 장애를 일으키는 결과를 초래할 수 있다. 이러한 외부 위협은 적절한 키 관리 보안 알고리즘의 적용과 침입탐지시스템을 이용하여 일정부분 해소가 가능하다.

내부 위협은 네트워크 내의 훼손된 노드들이나 이기적 노드 등 비정상행위 노드들로 인해 발생하는데, 악의적인 목적으로 데이터 패킷을 자신에게 유도한 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 알고리즘 등을 적용해도 해결이 쉽지 않다. 내부 위협을 가하는 노드 자체가 이미 같은 보안 메커니즘의 적용을 받고 있는 노드이기 때문이다. 따라서 이를 해결하기 위해서는 키 관리, 인증, 침입탐지 등의 적용 이외에도 비정상행위 노드를 관리하는 추가적인 보안 대책의 적용이 요구된다.

본 논문에서 중점적으로 다루고자 하는 내용은 내부 위협에 대한 대응 방안으로, 네트워크 내의 비정상행위 노드를 탐지 및 배제시켜 네트워크 신뢰도 및 처리율을 향상시키는 것에 목표를 두고 있다.

3. 관련 연구

Ad-hoc 네트워크를 포함한 모바일 네트워크에서의 연구는 주로 원활한 라우팅에 중점을 두고 있기 때문에 노드들이 서로간의 협력을 바탕으로 동작하는 것을 가정하고 있다. 이러한 가정은 군과 같이 동일한 목적을 달성하기 위한 조직체에서는 충분히 적용될 수 있는 가정이다.

그러나 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 Ad-hoc 네트워크에서 큰 문제점이 될 수밖에 없다. 예를 들어, 일부 노드는 자신의 수명을 연장하기 위해서 다른 노드들로부터의 서비스를 받기만 하고 자신은 서비스를 지원하지 않는 이기적인 행동을 할 수 있다. 그리고 그러한 이기적 행동은 전체 공동체를 위협할 수 있다. 또한 이기적인 행위 외에도 악의적인 목적으로 데이터를 버리거나 네트워크 와해를 시도하는 노드가 있을 수 있다.

이러한 문제들을 해결하기 위한 기존 연구들 중 대표적인 접근방법은 다음과 같다.

가. Watchdog & Pathrater

네트워크 내의 모든 노드들이 자신의 주변에 있는 노드들을 감시함으로써 이기적인 노드를 탐지하는 접

근방법이다. Watchdog는 패킷 전달을 거부하는 노드들을 탐지하고, Pathrater는 탐지된 결과를 바탕으로 악의적인 노드를 배제한 최선의 경로를 찾는다[4].

그러나 Watchdog과 Pathrater에는 몇 가지 문제점이 존재한다.

첫째, 특정 노드가 이기적인 노드로 판명되었음에도 아무런 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 있으므로 오히려 이기적인 노드에게 유리하게 작용할 수도 있다. 즉, 이기적인 노드들이 생성하는 메시지들이 어떠한 제약도 없이 주변의 노드들에게 전달될 수 있기 때문이다.

나. CONFIDANT

CONFIDANT(Cooperation Of Nodes : Fairness In Dynamic Ad-hoc NeTworks)는 비정상적인 노드를 고립시켜 네트워크로부터 배제하는 방법이다[5].

CONFIDANT는 모니터, 평가시스템, 경로관리자, 신뢰관리자 등의 네 가지 컴포넌트로 구성된다. 모니터는 인접 노드에 대한 비정상 행위를 탐지하는 역할을 수행하며, 신뢰관리자는 비정상적인 행위를 탐지했을 때 발생되는 경보 메시지에 대한 송수신을 담당하면서 이러한 경보 메시지의 수신자들을 우호적인 관계로 설정하고 그 리스트를 유지한다.

평가 시스템은 일부 온라인 경매 시스템에서 사용되는 것으로 이는 노드에 대한 등급관리를 함으로써 악의적인 노드 리스트를 관리하고 이를 우호관계에 있는 노드와 교환한다. 경로 관리시스템은 경로 상에 존재하는 노드들에 대한 평가 등을 기준으로 사전에 정의된 기준에 따라 경로 우선순위를 재설정하고 악의적인 노드들이 포함된 경로들을 삭제한다.

이러한 CONFIDANT의 문제점은 비정상적 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 없다는 점이다.

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 Ad-hoc 환경의 특성을 고려, 악의적인 노드가 이동을 하거나 네트워크 토폴로지 변화가 많이 발생하면 악의적인 노드를 판별하는데 많은 시간이 소요될 수도 있다.

다. 기존 연구들의 문제점 분석

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. 즉, Fig. 1과 같이 노드 A가 노드 B의 전송여부를 확인하고 있는데 노드 S가 A에게 패킷을 전송할 경우 노드 A는 노드 B가 정상적으로 전송을 했음에도 노드 B를 비정상행위 노드로 판단할 수 있게 된다.

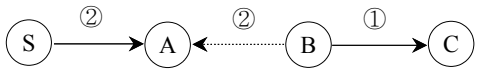


Fig. 1. 비정상행위 노드 탐지 기법에서의 문제점

둘째, 특정 노드가 악의적인 목적을 갖고 정상적인 노드를 비정상 행위 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 범인지목행위가 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 인한 탐지 실패 등으로 비정상행위 노드로 신고 될 수도 있기 때문이다.

이러한 문제점을 해결하기 위해 본 논문에서는 전술통신체계의 계층화된 네트워크 특성을 최대한 활용한 새로운 개념의 비정상행위 노드 탐지 및 관리 방법을 제시한다.

4. NWMS를 이용한 비정상행위 탐지 및 관리

본 논문에서는 비정상행위 노드 관리를 위해 전술 통신체계 내의 상위 계층 노드(MSAP)를 NWMS로 활용하여 자신이 관할하는 지역 내 노드들에 대한 가중치를 관리함으로써 네트워크가 운용되면서 점차적으로 처리의 효율성을 높이는 접근방법을 채택하였다.

즉, 기존 탐지 및 신고 방법에서 한 노드가 임의의 다른 노드에 대해 잘못된 판단을 하고 이를 전파함으로써 발생 가능했던 문제점을 줄이기 위해 비정상행위 노드에 대한 판단을 각각의 노드가 수행하는 것이 아니라 지역노드를 관리하는 MSAP가 수행하는 것이다. MSAP에 탑재되는 NWMS는 각각의 노드로부터 보고되는 정보를 통합 관리함으로써 좀 더 신중하게 비정상행위 노드를 판단하여 이를 지역노드들에게 전파한다.

가. 각 노드들의 임무 및 기본적인 탐지 절차

전술통신체계 상의 상위계층 노드와 일반 노드가 비정상행위 노드를 탐지 및 관리하는 과정에서 수행하는 임무는 다음과 같다.

먼저 비정상행위 노드의 탐지 및 보고는 일반 노드들이 수행한다. 송신 노드가 목적 노드로 데이터의 전송을 시도하는 경우 경로 상에서 비정상행위를 하는 노드가 확인되면, 이를 송신노드 및 NWMS에게 보고한다. 보고를 받은 NWMS는 보고메시지에 포함된 신고 노드와 혐의 노드 모두에 대해 가중치 '1'을 부여한다. 여기서 신고 노드의 가중치도 증가시키는 이유는 3장에서 언급한 바와 같이 임의 노드가 악의적으로 다른 노드들에 대해 지속적인 거짓 신고를 할 경우에 대비한 것으로서, 본 논문에서 제안된 접근방법이 기존 연구들과 가장 크게 차별화되는 점이다.

이러한 접근방법이 적용되면 악의적인 노드가 지속적으로 거짓 신고를 했을 때 가중치가 증가하여 결국 설정된 임계치를 초과하게 되고 이를 NWMS가 각 노드에게 전파한다. 각 노드는 NWMS가 전파한 정보를 자신의 관리테이블에 저장하고 라우팅 경로 설정 시 배제하거나 해당 노드로부터의 RREQ 패킷을 무시하는 등의 방법으로 해당 노드를 고립시킬 수 있다.

나. 부당한 가중치 적용 노드 구제 방법

전술한 기본적인 탐지 및 관리 절차를 적용함에 있어 여전히 악의적인 노드에 의해 부당하게 가중치를 부여 받게 되는 노드가 발생할 수도 있다. 그러므로 이런 노드에 대한 구제를 위해 네트워크 내의 각 노드는 'suspect'라는 필드를 추가적으로 가지며, 여기에는 신고한 노드와 혐의 노드의 정보를 유지한다. 'suspect'에 있는 노드 정보는 라우팅 경로 설정에는 관여하지 않으며 부당하게 가중치를 부여 받은 노드에 대한 구제에만 사용되게 된다.

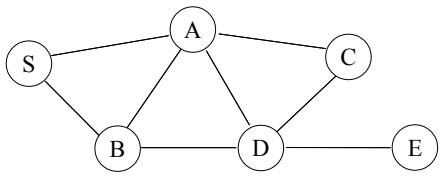


Fig. 2. 이기적 노드 탐지 예

Fig. 2를 예로 설명하면 송신 노드가 S, 목적 노드가 C라고 하면 먼저 S는 C에 대한 경로를 찾기 위해 RREQ 패킷을 브로드캐스트한다. C까지의 도달 경로는 S-A-C와 S-B-D-C가 된다. 첫 번째 경로인 S-A-C를 통해 패킷이 도착하면 노드 C는 역경로를 통해 응답을 하게 된다. 두 번째 경로인 S-B-D-C에서 노드 D가 노드 C에 대한 경로 정보를 캐쉬에 저장하고 있다면 RREQ 패킷은 노드 C까지 전달되지 않고 노드 D가 바로 노드 S로 응답할 것이다.

이 경우, 만약 노드 D가 악의적인 의도로 정상적인 정보 유통을 방해하기 위해 자신이 포함된 경로로 데이터를 보내도록 유도한 후, 실제 전송되는 데이터를 노드 C로 전달하지 않는다면 노드 B는 노드 D의 전달여부를 감시하고 있다가 이를 송신 노드인 S에게 알리면서 동시에 상위 노드인 NWMS로 보고한다. 노드 S는 이 사실을 확인하면, 다시 첫 번째 경로를 통해 목적지 노드로 데이터를 보내면서 동시에 노드 D에 대한 정보를 같이 보내게 된다. 이때 혐의 노드 D를 탐지한 노드 B의 'suspect'에는 노드 D의 정보가 포함되고, 경로상의 각 노드의 'suspect' 목록에는 노드 B와 D의 정보가 모두 추가된다.

그러나 만약 노드 D가 정상적으로 데이터를 포워딩했는데 노드 B가 이를 오탐했거나 악의적으로 노드 D가 포워딩하지 않은 것처럼 신고를 한다면 부당하게 노드 가중치 관리 서버에 가중치가 누적되고, 이렇게 누적된 가중치로 인해 네트워크로부터 배제될 수도 있을 것이다. 그러므로 부당하게 부과된 가중치에 대해서는 반드시 보상이 필요하며, 이를 위해 제안하는

방법에서는 각 노드가 유지한 'suspect' 목록과 함께 Ad-hoc 네트워크의 기본적인 특성을 이용한다.

Ad-hoc 네트워크 내에 존재하는 임의의 한 노드는 다양한 경로의 중간 노드로 포함될 수 있으며, 시간이 경과함에 따라 기존의 실패했던 라우팅 경로가 다시 사용될 수도 있을 것이다. 그리고 라우트 캐쉬 정보는 시간이 지나면 갱신되기 때문에, 이전에 사용된 경로든 새로운 경로든 노드 D가 정상적으로 동작을 하면 이를 탐지하던 이전 노드는 자신의 'suspect' 목록을 비교하여 해당 정보가 있으면 'suspect' 내의 해당 노드의 값을 '1' 만큼 감소시키고 상위 NWMS로 이를 보고한다. 'suspect'내의 해당 노드의 값 처리에 대해서는 Fig. 4(a)의 동작절차 설명 시 추가한다.

신고 노드로부터 보고를 받은 NWMS는 해당 노드에 대해 '0.1'씩 가중치를 감해주게 된다. 즉, 부당하게 가중치를 부여받은 노드도 지속적으로 정상적인 동작을 수행하면 부당한 가중치가 감소하게 된다.

이러한 방법은 각 노드가 네트워크에서 동작함에 있어 일시적인 오동작에 대한 허용치(tolerance)를 부여함으로써 네트워킹에 대한 참여율이 높아지도록 권장하는 방법이기도 하다. 따라서 이 방법을 적용하면 지속적으로 신뢰도와 처리율이 향상되며, 이는 차후 5장에서 실험을 통해 증명한다.

다. NWMS의 내부 구성 형태 및 동작 절차

Fig. 3은 노드와 NWMS의 내부 구성 형태 및 동작 절차를 보여주고 있다. 그림에서와 같이 각 노드는 monitor, suspect, isolate로 구성된다. 먼저 ①에서 한 노드의 monitor가 비정상 행위를 탐지하였을 경우, ②와 같이 monitor는 자신의 suspect에 이를 추가하는 동시에 경로상의 이전 노드와 NWMS에 이를 보고한다. 이 때 한 노드의 suspect 목록에 특정 노드를 등록시킬 경우 기본값으로 '5'를 부여하고 중복 신고될 경우 '5'를 더하며, 최대값은 '10'으로 설정된다.

보고를 받은 이전 노드는 신고 노드와 혐의 노드를 마찬가지로 suspect에 추가하고, NWMS는 신고 노드와 혐의 노드 모두의 가중치를 '1'씩 증가시킨다. 그 다음 ⑤와 같이 해당 노드의 임계치 초과 여부를 판단한 후 초과하지 않았을 경우 다시 준비 상태로 돌아가고 초과하였을 경우 ⑥과 같이 해당 노드를 브로드캐스트하여 노드들에게 알린다. NWMS의 전파를 받은 각 노드는 ⑦과 같이 suspect 목록에서 해당 노드의 정보를 삭제하고 isolate에 추가하여 해당 노드를 우회하고, 해당 노드로부터 송신되는 패킷을 무시하여 해당 노드를 고립시킨다.

Fig. 4는 외부 이벤트에 대한 노드의 동작절차를 보여주고 있다. 그 중 Fig. 4(a)는 한 노드가 다른 노드

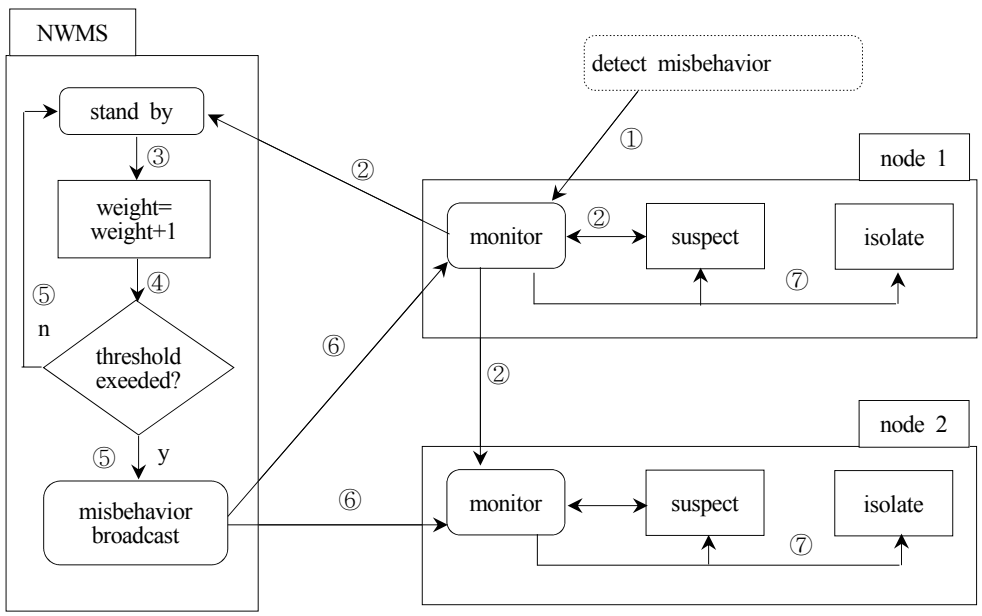


Fig. 3. 비정상행위 노드를 탐지 했을 경우의 동작 절차

의 비정상행위를 탐지했을 경우의 동작 절차이다. 우선 비정상행위를 탐지하면 NWMS에 보고하고 자신의 suspect 목록에 해당 노드의 정보가 있는지를 검사한다. 검사 결과 존재하지 않으면 count 값으로 '5'를 부여하며 해당 노드를 등록하고, 이미 존재할 경우 count 값을 비교하여 5보다 작으면 그 값에 5를 더하고 그렇지 않으면 최대값인 '10'을 부여한다.

Fig. 4(b)는 부당하게 가중치를 받은 노드에 대한 구제 절차로 한 노드가 정상행위를 확인하였을 경우의 동작 절차이다. 한 노드는 다음 노드의 행위를 감시할 때 suspect 목록을 참조한다. 다음 노드가 정상동작 하였을 경우 suspect 목록에 있으면 NWMS에 보고하고 해당 노드의 count를 '1'만큼 감한다.

이러한 과정이 지속적으로 반복되면, 전술한 바와 같이 거짓 신고를 하는 악의적인 노드를 통제하기 위해 탐지된 노드와 함께 가중치를 부여받은 신고 노드들이나 악의적인 노드에 의한 거짓 신고로 부당한 가중치를 받은 노드들, 그리고 통신 오류 등에 의해 부당한 가중치를 받은 노드들이 충분히 보상을 받을 수 있게 된다. 그 이유는 그 정상 노드에 대한 suspect 정보를 주변의 다른 노드들도 보유하고 있으므로 또 다른 경로가 설정되어 데이터가 전송될 경우 부당한 가중치를 받은 노드들이 정상적으로 동작하면 이같은 보상 행위는 계속 이루어지기 때문이다.

제안하는 접근방식에서는 통신 오버헤드를 줄이기 위해 신고 및 보고 제어 패킷은 유니캐스트로 처리하며, 비정상행위 노드가 NWMS에서 판별되었을 경우에만 신속한 공유를 위해 전파시 브로드캐스트를 하였다. 이는 비정상행위 노드의 탐지시간을 줄이고, 탐지율을 높이는데도 효과적이다.

또한 NWMS는 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 NWMS로부터 특정 비정상행위 노드에 대한 전파를 받았을 경우 suspect 목록에서 해당 노드의 정보를 삭제하여 통신오버헤드 및 메모리 사용량을 줄일 수 있다.

요컨대 본 논문에서 제안하는 메커니즘을 적용할 경우 악의적이거나 이기적인 노드는 정상 동작 노드에 비해 여러 면에서 불리할 수밖에 없다. 그 이유는 악의적인 의도로 특정 노드가 임의의 다른 노드를 네트워크에서 탈퇴시키려고 한다면 그 임의의 노드가 탈

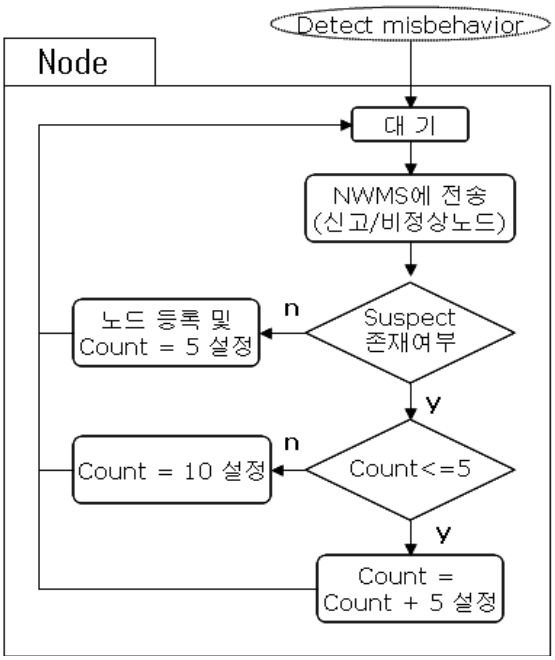
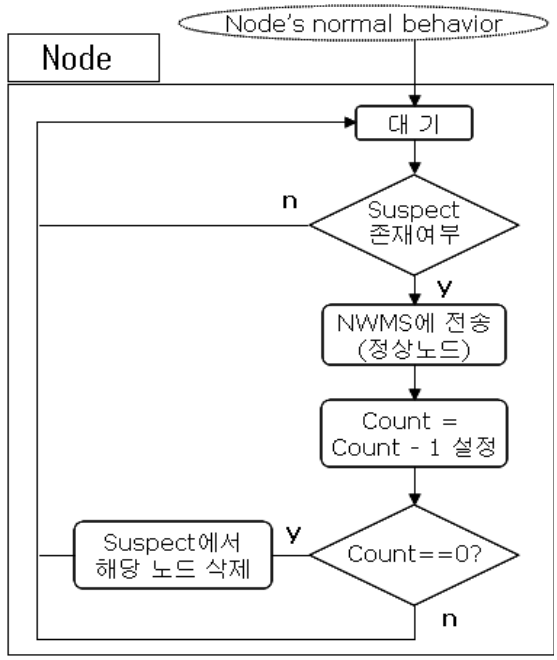


Fig. 4. a) 노드가 비정상행위를 탐지했을 때의 동작 절차



b) 노드가 정상행위를 탐지했을 때의 동작 절차

퇴될 확률보다 자신이 먼저 탈퇴될 확률이 높기 때문이다. 또한 기존의 연구에서는 비정상 행위 노드가 지정되는 임계치를 알고 있을 경우 위치를 이동하며 임계치보다 낮게 동작하는 행위가 가능할 수 있었으나 제안하는 접근방법에서는 각 노드가 NWMS에 설정된 값을 알 수 없기 때문에 이러한 지능적인 공격행위를 방지할 수 있다.

5. 모의 실험 및 분석

이 장에서는 본 논문에서 제안하는 방법에 대한 모의실험의 결과를 분석한다. 모의실험 분석은 네트워크 처리율, 패킷 손실율, 라우팅 오버헤드, 비정상 행위 노드 탐지율을 중심으로 분석한다.

가. 실험환경 및 시나리오

모의실험은 NS-2를 사용하였고 라우팅 프로토콜은 On-demand 프로토콜인 AODV 상에서 비교가 가능하도록 실험하였다. 주요 실험내용은 노드 수 변화에 따른 네트워크 처리율, 비정상행위 노드 포함율에 따른 손실율 등이며, 추가로 오버헤드, 비정상행위 노드 탐지율에 대해 분석하였다. 모의실험을 위해 설정되는 주요 설정 값은 Table 1과 같다. 실험은 다양한 결과 도출을 위해 네트워크 내 정상적인 노드의 수와 비정상행위 노드의 수를 변경시켜가며 진행하였다.

Table 1. 모의실험을 위한 주요 설정 값

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

나. 비정상행위 노드 수에 따른 패킷 처리량

네트워크 내 비정상행위 노드가 각각 25, 50개가 존재할 경우 AODV 프로토콜과 제안하는 방법의 패킷 처리량을 측정하였다. 트래픽 발생주기가 100ms이므로 100초당 발생하는 패킷 수는 최대 1000개가 된다. 패킷 처리량은 100초 단위로 종합되었으며, Fig. 5에서 볼 수 있듯이 AODV의 경우 평균 40~60%의 처리율을 나타내고 있지만, 제안된 방법에서는 비정상 행위 노드가 네트워크 내에 존재하더라도 일정시간(200초)이 경과한 이후에는 90% 이상의 처리율을 보장해 주었다.

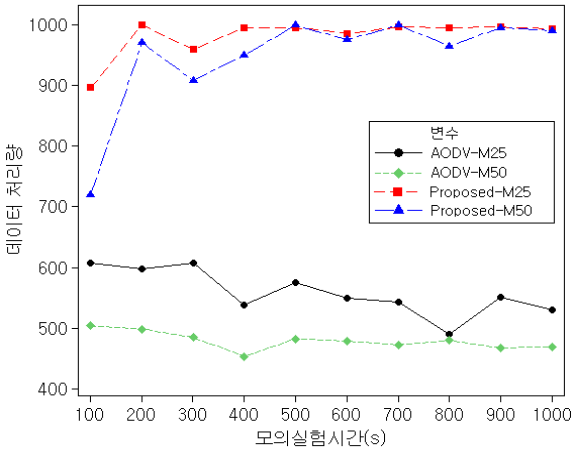


Fig. 5. 비정상행위 노드 수 변화에 따른 패킷 처리량

이는 전술한 바와 같이 본 논문에서 제안하는 접근방법이 조기에 비정상행위 노드를 탐지해 내고 효과적으로 관리하여 주고 있음을 잘 보여주는 결과이며, 비정상행위 노드 수가 2배 이상 증가시켜 실험을 실시해 본 결과 해당 노드들이 탐지되고 배제되는 시간은 조금 더 소요되긴 했지만, 시간이 경과할수록 90% 이상의 패킷 처리율을 보여줌을 확인하였다.

나. 노드수 증가 대비 손실 패킷 수

Fig. 6에서는 총 노드 수 대비 비정상행위 노드가 각각 10%, 30% 존재할 경우 노드 수가 증가함에 따른 손실 패킷 수를 보여주고 있다.

그림에서도 알 수 있듯이 순수 AODV의 경우 총 노드 수가 증가할수록 손실되는 패킷 수가 크게 증가한다. 그 이유는 총 노드수가 증가함에 따라 그만큼 네트워크 내에 비정상행위 노드가 많이 존재하기 때문이다. 반면, 제안 방법이 적용될 경우에는 총 노드수와 비정상행위 노드수가 증가하더라도 시간이 경과할수록 비정상행위 노드에 대한 탐지 및 배제가 효율적

으로 이루어지기 때문에 패킷 손실량에는 큰 변화가 없다.

비정상행위 노드가 10% 일 경우와 30%일 경우 손실 패킷 수에 약간의 차이가 발생하는데, 이는 실험 초기 즉, 비정상행위 노드에 대한 탐지 및 배제가 진행되기 이전에 손실되는 패킷량의 차이가 반영된 것이다.

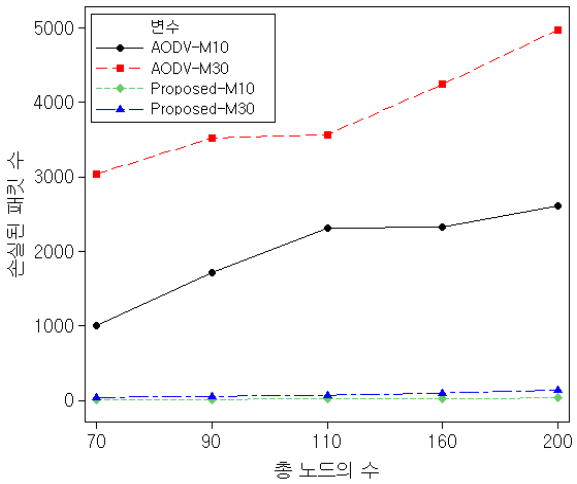


Fig. 6. 노드 수 증가 대비 손실 패킷 수 (10, 30% 포함시)

다. 비정상행위 노드 포함율에 따른 손실 패킷 수

Fig. 7은 네트워크 내 비정상행위 노드 포함율에 따른 패킷 손실량을 보여주고 있다.

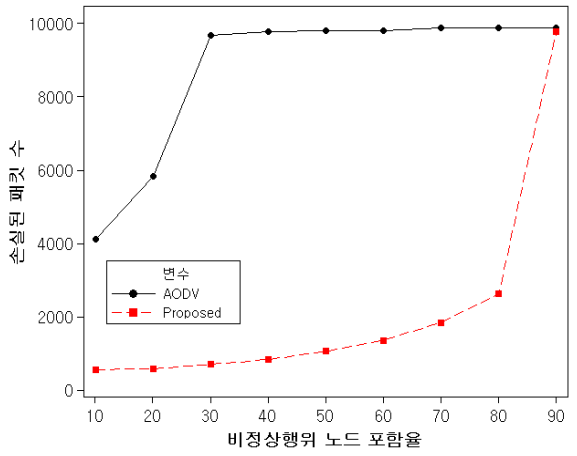


Fig. 7. 비정상행위 노드 포함율에 따른 손실 패킷 수

순수 AODV 프로토콜의 경우 비정상행위에 대한 대책이 없어 비정상행위 노드가 약 30% 이상 존재할 경우 손실율이 98% 이상을 유지한다. 그러나 제안하는 방법을 적용시에는 시간이 경과할수록 손실 패킷수가 많아지기는 하나 비교적 서서히 증가한다. 그 이유는 네트워크 내에 비정상행위 노드가 많이 존재하면 최초 패킷 손실율은 높지만 오히려 비정상행위 노드의 탐지 및 배제는 더욱 빠르고 활발하게 동작하기 때문이다.

그러나 비정상행위 노드의 포함율이 80%를 초과하면서부터 급격하게 손실율이 증가하게 된다. 이는 비정상행위 노드가 탐지 및 배제되면서 남게 되는 정상적인 노드의 수, 즉 네트워크 내에 존재하는 노드의 수가 적어지기 때문에 네트워크 형성에 문제가 발생함으로써 초래되는 패킷 손실이다. 실제 실험 결과를 분석해보면 포함율 80%시 실험시간 종료 후에 검출되는 비정상행위 노드는 약 148개였다.

본 모의실험에서는 이를 증명해 보기 위해 총 노드 수의 약 20%인 50개와 60개, 70개의 정상적인 노드만을 배치하여 테스트 해 보았으며 그 결과, 60개에서는 약 46%의 손실율이 발생하였고 70개 이상에서는 손실율이 발생하지 않았으며 50개 이하에서는 정상적인 통신이 이루어지지 않는 것을 확인할 수 있었다.

라. 비정상행위 노드 탐지 성능

비정상행위 노드의 탐지 시간이나 수량에 있어 본 논문에서 제안하는 접근방식을 적용할 경우 기 연구되었던 비정상행위 노드 탐지 및 배제 방법인 CONFIDANT에 비해 빠르고 더 많이 탐지할 수 있다는 것을 알 수 있다. 그 이유는 CONFIDANT의 경우, 라우팅 경로상에서 발생하는 비정상행위 탐지시 경로상에 존재하는 노드들만 해당 정보를 공유함으로 특정 경로 상에서 비정상행위 과다로 임계치가 초과하였다 하더라도 다른 경로에서는 비정상행위 노드로 분류되지 않을 수도 있기 때문이다.

또한, 임계치를 알고 있는 노드가 A라는 경로에서 비정상행위를 하고 임계치를 초과하지 않은 상태에서 지역을 이동하여 다른 경로에 참여하고 또다시 비정상행위를 해도 이 역시 비정상행위 노드로 분류되지 않는 경우가 발생하기 때문이다.

그러나 제안하는 접근방법에서는 NWMS를 통해 노드의 이동과 관계없이 비정상행위에 대한 지속적인 관리가 이루어지기 때문에 탐지 시간이 짧아질 수 있으

며, 탐지되는 수도 많을 뿐만 아니라 네트워크가 운영되는 시간 동안 지속적인 탐지가 가능하다. 이러한 특징은 지속적인 신뢰성이 요구되는 전장환경 하에서 적합한 접근방법이라고 하겠다.

마. 라우팅 오버헤드

제안하는 접근방법이 적용될 경우 당연히 기존 AODV 라우팅 프로토콜에 비해 오버헤드는 늘어날 수 밖에 없다. 그 이유는 제안하는 방법이 적용되지 않은 프로토콜에서는 비정상행위 노드의 탐지 및 관리를 위한 제어 패킷이 발생하지 않으며 그에 따라 평균 전송률 또한 큰 변화가 없는 반면 제안 방법이 적용된 경우는 비정상행위 노드 탐지 및 정보 전파를 위해 매우 작은 크기의 제어 패킷이 지속적으로 발생하기 때문이다.

추가적으로 발생하는 패킷은 비정상행위 노드를 유니캐스트로 신고하는 패킷과 NWMS가 비정상행위 노드라고 판단하였을 때 지역 내 노드로 전파하는 브로드캐스트 패킷 2가지이다. 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*, 비정상행위 노드 수를 *M*, 신고 및 전파 제어 패킷 사이즈를 CP_{size}, 임계치를 *threshold*, 네트워크 운영 시간을 *T*, 신고 노드로부터 NWMS까지의 경로에 포함되는 평균 노드수를 *n* 이라고 할 경우, 신고 노드가 NWMS에 유니캐스트로 신고시 발생하는 오버헤드(U)는

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

NWMS가 비정상행위 노드를 브로드캐스트시 발생하는 오버헤드(B)는

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

네트워크 운영 시간 동안 발생하는 총 통신량 대비 오버헤드(O)는

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

으로 표현할 수 있다.

이러한 분석결과에 근거하여 모의실험에 적용된 환경을 기준으로 비정상행위 노드의 탐지 및 배제를 위해 추가적으로 발생하는 오버헤드를 계산해 본 결과, 실험시간 1000sec 동안 발생한 총 통신량 대비 약 0.89%의 오버헤드 증가가 있었다.

그러나 패킷 처리량은 Fig. 5에서 보는 바와 같이 적용하지 않았을 경우보다 2배 이상 향상되었다. 또한, 기존의 프로토콜에서는 시간의 경과와 상관없이 지속적인 데이터 전송 패킷 손실이 발생하는 반면 제안하는 방법이 적용될 경우 시간이 경과할수록 비정상행위가 탐지, 배제되므로 전송률은 크게 증가한다.

6. 결 론

Ad-hoc 네트워크는 고정된 인프라가 존재하지 않는 상황에서도 네트워크 내 노드들 간의 협동을 통해 스스로 네트워크를 구성할 수 있고, 이동성을 지원한다는 장점으로 인해 다양한 분야에 응용되고 있으며, 우리 군도 미래 전술정보통신체계인 TICN을 구축함에 있어 Ad-hoc 네트워킹 기술의 적용을 검토하고 있다.

그러나 Ad-hoc 네트워크는 대부분의 프로토콜들이 분산과 협동을 전제로 하고 있으며, 이동 노드들의 자원 제약적 특성으로 인해 많은 보안 위협에 직면할 수 있어, 기밀성 · 무결성 · 가용성 및 신뢰성이 극도로 요구되는 전장환경에서 효율적인 보안대책의 적용 없이 운용하는 것은 불가능하다.

이에 본 논문에서는 전술 통신용 Ad-hoc 네트워크에 적용 가능한 보안대책을 제안하였다. 보안대책을 제안함에 있어서는 예방책보다는 능동적인 대응에 중점을 두고, 네트워크 내에서 비정상적인 행위를 하는 악의적 노드들을 조기에 탐지 및 배제할 수 있도록 설계하였다. 그리고 전장환경에 대한 적용 가능성을 높이기 위해 TICN의 계층화된 네트워크 구조를 최대한 활용하였다.

우선 TICN의 상위계층 노드인 MSAP를 NWMS로 설정하여 각 노드들의 비정상행위 여부에 따라 부여되는 가중치를 관리하고 종합적인 판단을 수행하도록 하였으며, 악의적인 범인지목행위 또는 일시적인 네트워크 오류 등으로 인해 부당하게 가중치를 부여받는 노드들의 생존성을 유지하기 위해 가중치를 보상해 줄

수 있는 알고리즘도 적용하였다. 또한 기존의 연구에서 간과하였던 정상노드를 비정상노드로 신고하는 악의적인 노드에 대한 관리 방법도 제안하였다.

제안하는 방법에 대한 모의실험 결과, 비정상적인 행위를 하는 노드에 대한 효과적인 탐색 및 관리를 통해 네트워크의 전반적인 데이터 처리율이 향상되면서도 원본 AODV 프로토콜에 비해 라우팅 오버헤드가 크게 증가하지 않음을 확인할 수 있었다.

본 논문에서 제안하는 비정상행위 노드 탐지 및 관리 방법은 TICN의 특성을 기반으로 설계되었기 때문에 향후 보안성이 강화된 TICN 구축에 크게 기여할 수 있을 것으로 판단되며, 향후 전술 통신용 Ad-hoc 네트워크에서의 침입탐지 시스템 연구와 연계된다면 전장환경 하에서 발생 가능한 각종 위협에 종합적으로 대응을 할 수 있는 시스템 개발에도 도움이 될 수 있을 것이다.

References

[1] 합참, 군 전술종합정보통신체계 운영 개념서, 2006.

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

[3] 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.

[4] Sergio Marti and T. J. Giuli and Kevin Lai and Mary Baker, “Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks”, Mobile Computing and Networking, 2000.

[5] Sonja Buchegger and Jean-Yves Le Boudec, “Performance Analysis of the CONFIDANT Protocol : Cooperation of Nodes - Fairness in Distributed Ad-hoc NeTworks”, In Proceedings of IEEE/ACM Workshop on Mobile Ad-Hoc Networking and Computing(MobiHOC), Lausanne, CH, June 2002.