Ad-hoc 네트워크에서 악의적 노드 관리기법에 관한 연구

김일도* · 김동천*
*해군사관학교

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

Il-do Kim* · Dong-cheon Kim*
*Naval Academy

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 신뢰성를 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 conisting 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

Ⅰ. 서 론

Ad-hoc 네트워크는 이동 단말만으로 구성되기 때문에 각종 보안 위협에 쉽게 노출될 위험에 있다. Ad-hoc 네트워크의 특성중 하나인 자원 제약 요소를 피하기 위해 이기적인 행위를 하는 노드, 악의적인 목적으로 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. 각 노드는 이동성을 가지며, 무선 인터페이스를 사용하기 때문에 유선 네트워크보다 매우 유연한 네트워크의 구성이 가능하지만 이러한 특징 때문에 유선 네트워크에서 사용하던 보안 기법을 그대로 적용하기에는 다음과 같은 문제점이 존재한다[1].

첫째, 무선 채널의 공유로 합법적인 노드와 악의적인 노드가 모두 무선 채널에 접속할 수 있으므로 누구나 쉽게 네트워크를 공격할 수 있다.

둘째, 네트워크를 구성하는 노드의 자원이 유선 네트워크에 비해 매우 제한되어 있다는 것이다.

셋째, 노드들의 이동성과 상태 변화에 따라 네트워크의 토폴로지가 동적으로 변화된다는 점이다.

Ad-hoc 네트워크에 대한 위협은 크게 외부 위협과 내부 위협으로 구분할 수 있다[2]. 외부 위협은 적절한 키 관리 보안 알고리즘을 적용하는 방법과 침입탐지시스템을 이용하는 방법으로 일정부분 위협을 해소할 수 있으므로 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 네트워크를 포함한 모바일 네트워크에서의 연구는 주로 노드들이 서로간의 협력을 바탕으로 원활한 라우팅이 이루어진다는 가정하에 Watchdog & Pathrater[3]와 CONFIDANT[4] 등의 메커니즘이 연구되었다.

하지만 동일 목적을 갖는 네트워크에도 내/외부의 공격 또는 자원 제약적인 환경에 의해 비정상적으로 동작하는 노드가 발생할 수 있다. 이러한 비정상행위 탐지 및 관리 방법과 라우팅 참여를 유도하는 방법을 제안한 기존의 연구들의 문제점은 다음과 같다.

첫째, 모호한 통신 충돌로 인해 다음 노드의 전송 여부 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.

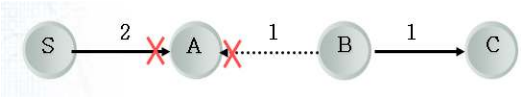

그림 1. 비정상 노드 탐지 기법에서의 문제점

둘째, 특정 노드가 악의적인 목적을 갖고 정상적인 노드를 비정상 노드로 신고할 경우에 대한 연구나 대응방법이 미흡하다.

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.

이러한 문제점 해결을 위해 본 연구는 NWSS를 이용한 악의적 노드 탐지 및 관리 방법을 제시한다.

III. 악의적 노드 판단 및 NWSS 동작절차

악의적 노드의 판단은 송신지 노드와 목적지 노드의 협동에 의해 이루어지게 된다. 하지만, 이들에 의해 NWSS에 신고가 되었다고 해서 혐의노드가 완전히 네트워크에서 고립되는 것은 아니다. 아직 혐의노드가 완전히 악의적 노드로 판단되지 않았기 때문이다. 완전한 악의적 노드의 판단은 이들의 보고를 받은 NWSS에 의해 이루어진다. NWSS는 송신지 노드와 목적지 노드의 혐의 노드에 대한 신고를 받고, 각각의 노드가 신고한 혐의 노드가 일치하는 지를 확인한 후, 이것이 일치하면 정상적인 노드로 판단하여 해당 노드에 가중치를 부여하게 된다. 목적지 노드는 혐의노드를 판단 후, 이를 송신지 노드와 공유하여, 혐의 노드를 NWSS에 신고한다.

신고를 받은 NWSS는 일정 시간 내 도착한 두 신고를 비교하여, 혐의 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 오인신고 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 suspect를 유지함으로써 경로상의 인접 노드가 정상적으로 동작할 경우, 이를 통해 가중치를 줄이는 방법을 사용한다. suspect에 있는 노드 정보는 라우팅 경로 설정과는 무관하며, 부당하게 가중치를 부여 받은 노드에 대한 구제에만 사용되게 된다. suspect는 앞서 언급한 것과 같이 정상 노드임에도 불구하고 악의적 노드로 부당한 가중치를 부여받은 노드에 대한 구제에 사용된다. 한 노드가 라우팅 경로상의 다음 노드를 suspect에 가지고 있을 경우, 데이터 전송시 그 노드가 정상적으로 라우팅에 참여한다면 suspect를 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 '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 정상동작을 하였을 경우 suspect 목록에 있으면 NWMS에 보고하고 해당 노드 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 0이 된 노드에 대해 suspect 관련 보고가 들어올 경우 이를 삭제 지시하여 노드의 불필요한 패킷이 발생하는 것을 방지하며, 각 노드는 suspect 목록의 노드 count가 0이 되거나 NWMS로부터 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 On-demand 프로토콜인 AODV(Ad-hoc On-demand Distance Vector)상에서 비교가 가능하도록 실험하였다.

표 1. 모의실험 주요 설정 값

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.

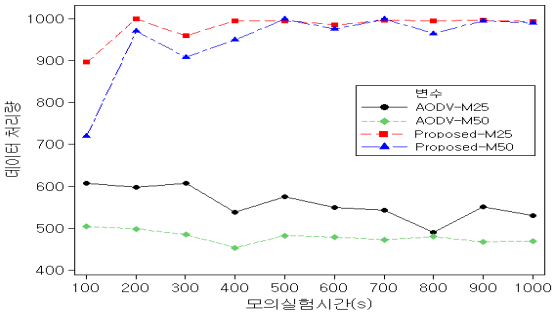

그림 2. 악의적 노드 수 변화에 따른 패킷 처리량

4.3 노드 수 증가 대비 손실 패킷 수

총 노드 수 대비 비정상행위 노드가 각각 10, 30% 존재할 경우 노드 수 증가에 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 존재하기 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.

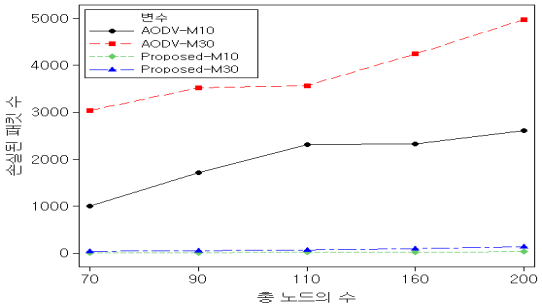

그림 3. 악의적 노드 포함율에 따른 손실 패킷 수

V. 결 론

본 연구에서는 지역 내 각 노드들의 가중치를 관리하는 NWSS 서버를 활용하고 부당하게 가중치를 부여받는 노드들의 생존성을 유지하기 위해 가중치를 감해주는 알고리즘이 적용되었다. 본 연구에서 제안하는 방법에 따른 모의실험 결과, 비정상적인 행위를 하는 노드에 대한 효과적인 탐색 및 관리로 네트워크 전반의 생존성 및 데이터 처리율이 향상되었다.

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] 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.

[4] 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