http://dx.doi.org/10.3745/KIPSTC.2012.19C.2.083

MANET에서 협업기반의 악의적인 노드 행위 식별기법

전 서 인[†] · 류 근 호[††]

요 약

MANET은 유선 기반망이 구축되어 있지 않은 곳에서 운용되기 때문에 노출된 매체와 동적인 토폴로지, 중앙의 감시와 관리 결여 등으로 보안 측면에서 취약하다. 특히, 중앙에서 네트워크를 제어해 주는 중재자가 없기 때문에 악의적인 노드가 발생해도 그에 대한 탐지나 조치가 어렵다. 이와 같은 악의적인 노드는 Ad-hoc 관련 보안 연구 분야중 라우팅에 밀접하게 연관되어 있다. 따라서, 본 논문에서는 안전하고 효율적인 라우팅을 위해 악의적으로 행동하는 노드를 효과적으로 탐지하여 보안성을 더욱 높일 수 있는 기법을 제안한다. 이를 위해 일정기간 악의적인 행위를 수행하는 노드를 개개의 노드 및 이웃간의 협업을 통해 이중화하여 탐지하고, 각 노드에 대한 신뢰지수를 부여하여 관리함으로써 악의적인 노드 행위에 효과적으로 대응 할 수 있는 기법인 MBC(Identification technition of Malicious Behavior node based on Collaboration in MANET)을 제안한다. 제안한 방법의 효율성을 검증하기 위해 우리는 네트워크 시뮬레이션을 수행하였다. 이 시뮬레이션 수행결과는 제안한 방법이 기존 방법보다 악의적인 노드를 더 정확하고 신속하게 식별 가능함으로써 보다 효율적인 라우팅이 이루어짐을 보였다.

키워드 : 악의적인 노드, 악의적 행위 패턴, 신뢰지수, 보안 라우팅

Identification Technition of Malicious Behavior node Based on Collaboration in MANET

Seoln Jeon[†] · KeunHo Ryu[††]

ABSTRACT

MANET(Mobile Ad-Hoc Network) has a weakness from a security aspect because it operates where no wired network is built, which causes the exposed media, dynamic topology, and the lack of both central monitoring and management. It is especially difficult to detect and mitigate a malicious node because there is not a mediator which controls the network. This kind of malicious node is closely connected to the routing in the field of study of Ad-Hoc security. Accordingly this paper proposes the method on how to enhance the security for the safe and effective routing by detecting the malicious node. We propose MBC(Identification technition of Malicious Behavior node based on Collaboration in MANET) that can effectively cope with malicious behavior though double detecting the node executing the malicious behavior by the collaboration between individual node and the neighbor, and also managing the individual nodes in accordance with the trust level obtained. The simulation test results show that MBC can find the malicious nodes more accurately and promptly that leads to the more effectively secure routing than the existing method.

Keywords : Malicious Node, Malicious Behavior Pattern, Trust Level, Secure Routing

1. 서 론

최근 들어 우리 군은 고속 대용량의 데이터 처리가 가능한 차세대 전술정보통신체계(이하 TICN : Tactical Information Communication Network)[1] 구축을 추진 중이며, 이 체계에서는 Ad-hoc이 적용될 예정이다[1].

전술상황하에서 MANET(Mobile Ad-hoc NETwork)은 기반구조 없이 자체적인 네트워크 구성이 가능하고 이동성을 갖는 노드로만 데이터를 송·수신할 뿐 아니라 수신한 데이터를 다른 노드에 전달하는 라우터의 기능까지 제공하게 된다. 또한 네트워크 전이가 용이하고 멀티 홉 통신을 지원하여 지형적으로 열악한 통신환경을 극복할 수 있어서 군에서 많은 연구가 이루어지고 있다. 그러나 MANET은 유선 기반망이 구축되어 있지 않은 곳에서 운용되기 때문에 노출

※ 이 논문은 2011년도 충북대학교 학술연구지원사업의 연구비지원에 의하여 연구되었음.
† 정 회 원 : 육군본부 전산체계처 전산장교
†† 종신회원 : 충북대학교 전자정보대학 소프트웨어전공 교수
논문접수 : 2011년 11월 9일
수 정 일 : 1차 2011년 12월 30일, 2차 2012년 2월 11일
심사완료 : 2012년 2월 14일

1) TICN(Tactical Information Communication Network): 미래 네트워크중심전(NCW)에서 통합전투력 발휘 보장을 위한 고속 대용량의 전술정보통신체계

된 매체와 동적인 토폴로지, 중앙의 감시와 관리 결여 등으로 보안 측면에서 취약하다. 특히, 중앙에서 네트워크를 제어해 주는 중재자가 없어서 악의적인 노드 행위에 대하여 탐지나 조치가 어렵기 때문에 네트워크 전체에 심각한 부하와 정보유통에 치명적 문제를 발생할 수 있다. 이는 전장상황에서 정보유통의 신뢰성이 보장될 수 없다[2].

지금까지 MANET에서 라우팅 공격이나 패킷 전송시 발생 할 수 있는 여러 형태의 악의적인 행위를 효율적으로 탐지하고 대비하기 위한 많은 보안 대책이 연구되어 왔다[3,4,5]. 하지만 대부분의 연구들은 라우팅경로에 대한 공격 또는 패킷을 버리거나 변경, 거짓 신고 등의 패킷 전달에 대한 공격 중 어느 한 측면에만 중점을 두고 개개의 노드 행위를 탐지해 왔다. 이는 보다 정확하고 효율적으로 악의적인 행위에 대비 할 수 없었다.

본 논문에서는 일정기간 악의적인 행위가 이루어지는 노드를 개개의 노드 및 이웃노드와 협업을 통하여 이중 탐지하고, 악의적 행위 빈도수에 의한 신뢰단계를 구성하여 관리함으로써 악의적인 노드 행위에 효율적으로 대응 할 수 있는 MBC(Identification technition of Malicious Behavior node based on Collaboration in MANET)기법을 제안한다.

이 논문을 효율적으로 전개하기 위하여 2장에서는 지금까지 연구된 MANET에서 악의적인 노드 식별기법에 대한 관련연구에 대해 살펴보고, 3장에서는 제안하는 기법인 MBC에 대해 자세히 알아보고, 4장에서는 성능평가 및 분석을 통해 MBC의 효율성을 증명 하고, 마지막으로 5장에서는 결론을 제시한다.

2. 관련 연구

MANET은 유선환경의 네트워크보다 더욱 보안의 취약성을 가진다. 그 이유는 각 노드들이 호스트로서의 서비스를 받을 뿐만 아니라 라우터로서의 역할을 동시에 수행하기 때문에 노드 중 악의적인 노드가 존재하여 라우팅 공격을 한다면 전체 네트워크를 마비시킬 수 있기 때문이다. 이러한 악의적인 노드로 인하여 최적의 경로가 이용될 수 없을 수도 있고, 네트워크에 협조하는 노드들은 이기적인 노드들을 대신하여 과중한 짐을 떠맡아 결국에는 네트워크에서 분리되는 경우도 있을 수 있다. 따라서 악의적인 노드들로 인해 네트워크 전체에 치명적인 영향을 미칠 수 있기 때문에 이들을 관리하는 메커니즘과 알고리즘이 필요하다. 지금까지 연구 된 대표적인 악의적인 노드 관리기법들을 검토하고, 장▪단점을 분석한다.

2.1 Watchdog & Pathrater

Watchdog(경비견)는 부정한 노드를 탐지하는 방법 중의 하나로 Watchdog는 패킷 전달을 거부하는 노드를 감지하는데 사용되며 메커니즘은 네트워크의 모든 노드들이 주변에 있는 노드들을 감시함으로써 악의적인 노드를 탐지하는 방법에 기반을 두고 있다[6,7.8].

(그림 1)과 같이 소스노드 S로부터 패킷을 받은 노드 A는 는 노드 B에게 패킷을 전달한다. 그러나 여기서 자신의 역할이 끝나는 것이 아니라, 노드 B가 노드 C에게 제대로 패킷을 전달하는지 까지도 감시한다. 이렇게 모든 노드에 존재하는 Watchdog이 패킷을 전달한 노드의 다음 행동까지 감시함으로써 악의적인 노드를 탐지하게 된다.

이러한 방법으로 악의적인 노드가 탐지되면 각 노드의 Pathrater(경로관리자)는 그 사실을 반영하여 악의적인 노드를 제외한 안전한 경로를 제공한다.

(그림 1) Watchdog의 악의적인 노드 탐지 기법

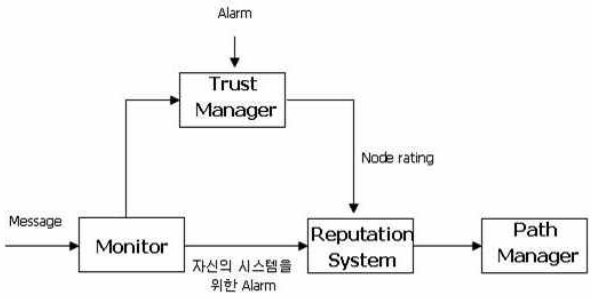
하지만 이 메커니즘에는 몇 가지 문제점이 있다. 우선 노드 A는 노드 B가 정상 노드임에도 불구하고 악의적 노드라고 거짓으로 신고를 해도 소스 노드로서는 노드 A를 무조건 믿을 수밖에 없다는 점이다. 또한, 노드 A와 노드 B가 모두 악의적인 노드인 경우, 노드 B가 노드 C에게 패킷을 전달하지 않아도 노드 A는 소스노드에게 신고하지 않을 것이다. 즉, 네트워크에 참여하는 모든 노드가 최소한 악의적인 노드는 아니라는 가정 하에서만 메커니즘이 제대로 작동할 수 있는 것이다. 또 하나의 문제점은 악의적 노드라고 판명된 노드가 어떠한 징계도 받지 않는다는 사실이다. Watchdog를 통해 악의적 노드를 탐지하면 Pathrater는 그 노드를 제외한 경로를 다시 제공된다. 그러나 악의적 노드의 관점에서 보면 그 노드는 여전히 네트워크에 참여할 수 있고 자신이 생성한 데이터를 보내는데 어떠한 제약도 받지 않는다. 결과적으로 다른 노드를 위해 데이터를 전달해 주지 않아도 되기 때문에 오히려 악의적 노드에게 더욱 유리하게 작용할 수도 있는 메커니즘인 것이다.

2.2 CONFIDANT

CONFIDANT(Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks)는 Watchdog과 비슷하게 각 노드들이 서로를 감시하면서 악의적인 노드를 탐지하는 메커니즘이다[9,10]. 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 하는 것이 이 메커니즘의 목적이다.

CONFIDANT에서는 노드에 대한 정보를 다음 두 가지로 구분한다. 악의적 행동을 직접 겪은 노드에게서 온 정보와 간접적으로 그런 정보를 들은 노드에게서 온 정보로 구별하여 서로 다른 가중치를 둔다.

(그림 2)와 같이 CONFIDANT에서 제안하는 메커니즘에서 Neighborhood Monitor(이웃감시자)는 정상적인 라우팅 행동에서 벗어나는 일탈 행위를 감시하고, 만약 특정 노드가 비정상적인 행동을 하게 되면 Trust Manager(신뢰관리자)에게 알람 메시지를 보내게 된다. 신뢰 관리자는 이웃감시자로



(그림 2) CONFIDANT에서 제안하는 메커니즘 구조

부터 들어온 알람 메세지를 필터링하고, 다른 신뢰 관리자들과 알람 메세지를 교환한다. Reputation System(평가시스템)은 다른 노드들에 관해서 관찰 또는 보고된 행동에 의해 그 노드에 대한 등급을 매기고, Path Manager(경로 관리자)는 경로에 대한 등급을 관리하며, 악의적인 노드를 포함하는 라우팅 메시지가 들어왔을 때 적절한 행동을 한다.

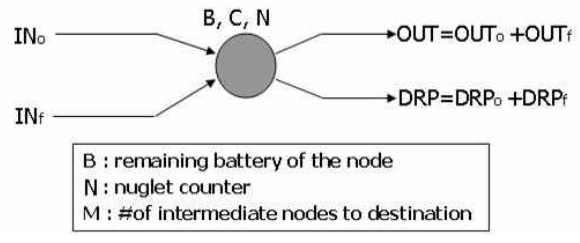
하지만 이 메커니즘의 문제점은 각 노드는 설정된 임계치 이하로 동작할 수 있으며, 또한 서로 다른 경로에 포함되어 악의적 행위를 할 경우 실제 악의적 행위 누적 횟수는 임계치를 초과하지만 각각의 경로에서는 임계치를 초과하지 않아 네트워크에서 고립되지 않을 수도 있다. 또한 악의적 노드로 판정되었을 때 공유는 우호관계에 있는 노드로만 한정되어서 다른 경로에 이동하여 같은 행위를 반복할 수 있다.

2.3 Nuglets

앞서 언급한 연구에[6,7,8,9,10] 대한 매커니즘은 이미 악의적 행동을 한 노드들에 대한 대처방법이라면 Nuglets는 처음부터 부정행위를 하지 않도록 유도하는 방법을 제안하고 있다.

(그림 3)과 같이 Nuglets은 Ad-hoc 네트워크 환경에서의 두가지 중요한 점을 강조하였는데 첫째, 노드들이 네트워크 작업(주로 다른 노드들을 위해 피킷을 전달해 주는 작업)에 협조하도록 하려면 반드시 일종의 보상이 주어져야 한다는 점과, 둘째 어떤 노드가 네트워크에 과중한 짐을 지우려 할 경우, 그 노드는 그에 따른 손실이 있어야 한다는 것이다. 이를 실제로 구현하기 위해 Nuglets counter개념을 도입하였다.

노드가 자신이 생성한 패킷을 보내는 경우 Nuglets counter가 감소하고, 다른 노드가 생성한 패킷을 중간에서 전달할 경우 Nuglets counter는 증가하게 된다 만약 노드가



(그림 3) Nuglets 카운터 구조

자신이 생성한 패킷을 보내려 하는 경우에는 목적지까지 도착하기 위해 중간에 거쳐야 할 노드 수가 계산된다. 송신노드의 Nuglets counter가 중간에 거쳐야할 노드 수보다 크거나 같은 경우에만 패킷을 보낼 수 있고 Nuglets counter는 그 수만큼 감소하게 된다. 그리고 노드가 임의로 Nuglets counter를 조작하는 것을 방지하기 위해 Nuglets counter는 각 노드에 존재하는 변경방지 보안모듈에 의해 보호된다.

이 매커니즘은 노드가 협조를 할수록 네트워크 전체뿐만이 아니라 자기 자신에게도 이익이 된다는 것이 장점이지만 또한 몇가지 문제점이 있다.

우선 패킷을 보내고자 하는 노드가 목적지까지의 중간 노드수를 추정하는데 있어서 어려움이다. Ad-hoc 네트워크 특성상 잦은 노드들의 이동으로 예정된 경로보다 더 긴 경로로 갈수도 있고 그렇게 되면 Nuglets counter가 충분치 않아 그패킷은 버려진다.

또한 중간 노드들이 Nuglets counter만 가져가고 실제로 패킷을 전달해 주지 않는 경우도 문제가 될수 있다. 게다가 Nuglets counter은 패킷을 전달하는 것에만 그 목적이 있으므로 패킷을 변조해 보내는 경우에는 대처할 수 없다.

3. 협업기반 악의적인 노드 탐지 기법

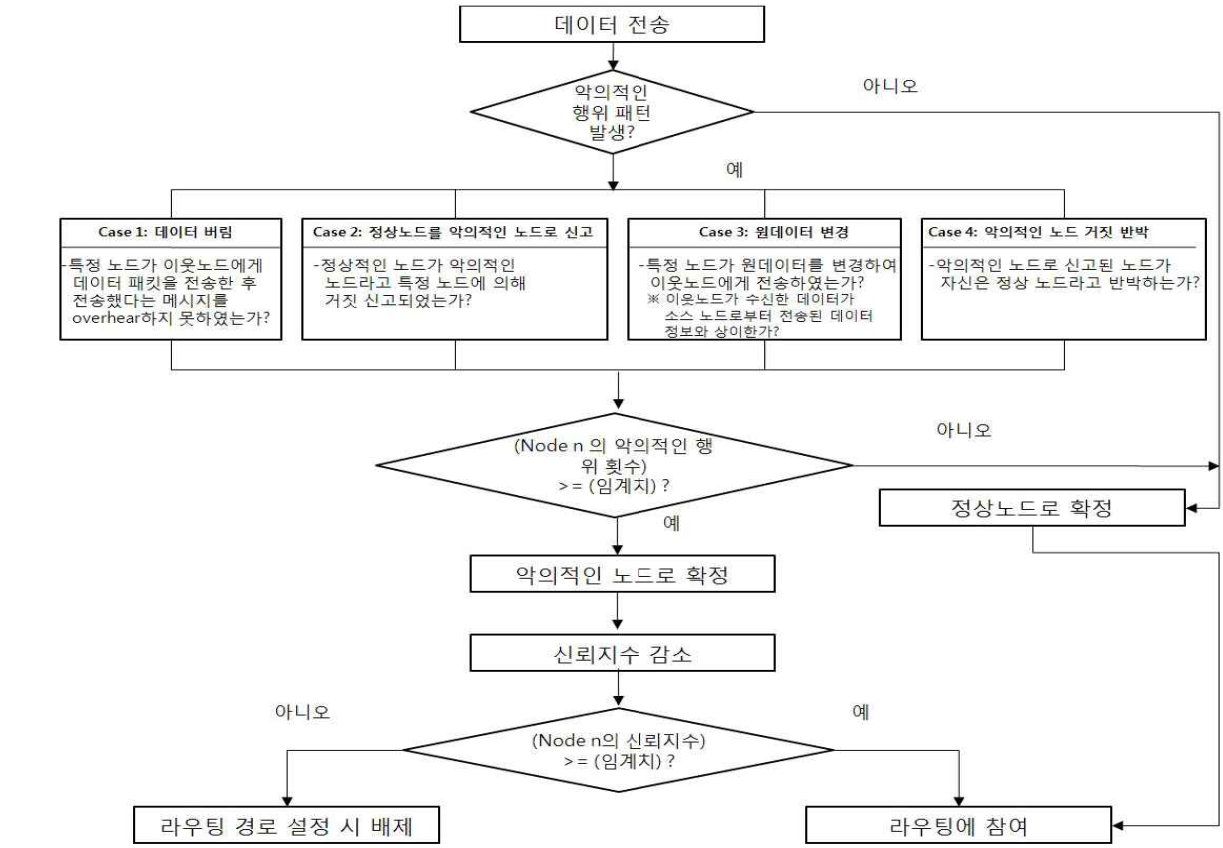
MANET에서 안전하고 효율적인 라우팅을 위해 악의적으로 행동하는 노드를 효과적으로 탐지하여 보안성을 더욱 높일수 있도록 MBC(Identification technition of Malicious Behavior based node on Collaboration in MANET)을 제안하며, 절차는 (그림 4)와 같다. MBC는 이웃노드들과 협업을 기반으로 각 노드들의 악의적인 행위를 탐지하고 각 노드에 대하여 노드의 빈도수에 의한 각 노드의 신뢰단계를 구성하여 관리함으로써 악의적인 행위에 효율적으로 대응할 수 있다. 또한 각 노드가 관리 및 유지하고 있는 신뢰지수를 바탕으로 라우팅 경로를 설정한다. 즉, 악의적인 노드를 탐지하기 위해 이웃 노드들은 경로 상 협업관계를 맺고 있으며 식별된 악의적인 행위들은 신고, 증명 메시지 등을 통해 관리 테이블에 저장되며 저장된 정보를 통해 최종 악의적인 노드 식별 및 라우팅 참여 여부를 결정하게 된다.

3.1 악의적인 노드 탐지

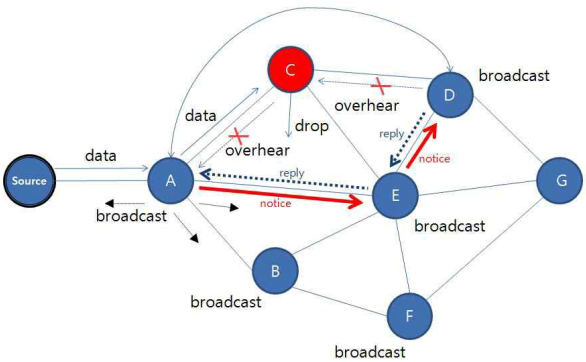
3.1.1 악의적인 노드가 데이터를 버리는 경우

악의적인 노드가 전송받은 데이터를 버리고 전송노드에게 overhear하지 않을 경우, 전송노드는 전송받은 노드의 overhear전송여부와 전송노드와 협업관계에 있는 이웃노드들에게 정보를 상호교환(notice, reply)함으로써 악의적인 행위를 이중적으로 감시하게 된다.

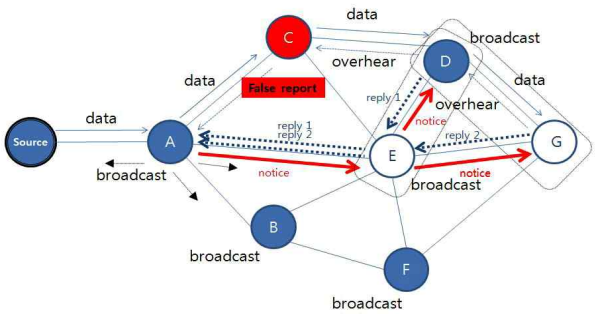
(그림 5)의 경우 소스노드로부터 데이터를 전송받은 노드 A는 노드 C에게 데이터를 전송 후 일정기간 동안 노드 C가 노드 D에게 메시지를 전송했다는 내용을 overhear하지 못할 경우 노드 C를 악의적인 노드라고 판단한다. 또한 노드 A는



(그림 4) 협업기반 악의적인 노드탐지 절차



(그림 5) 데이터를 버리는 악의적인 노드 확인



(그림 6) 정상적인 노드를 거짓 신고하는 악의적인 노드 확인

경로 상 협업관계에 있는 이웃 노드, 즉 노드 E에게 상호 정보교환 메시지(notice, reply)를 통해 노드 C가 악의적인 노드라는 것을 확신하게 된다. 이때 이웃노드들에게 control 패킷을 통해 노드 C가 악의적인 행위를 했음을 broadcast하고 각 노드들은 악의적인 행위패턴 정보, 즉 노드 C가 데이터를 버렸다는 정보를 관리테이블에 등록하고 관리한다.

3.1.2 정상노드를 악의적인 노드로 신고하는 경우

정상노드가 데이터를 전송하고 overhear 보냈으나 악의적인 노드가 Ack를 버리고 정상노드를 거짓으로 신고하게 되면 악의적인 노드로 간주된 정상노드의 경로를 우회하여 상대적으로 먼 경로로 데이터가 전송될 수 있다. 이러한 결과는 더 많은 자원소모를 야기하기 된다.

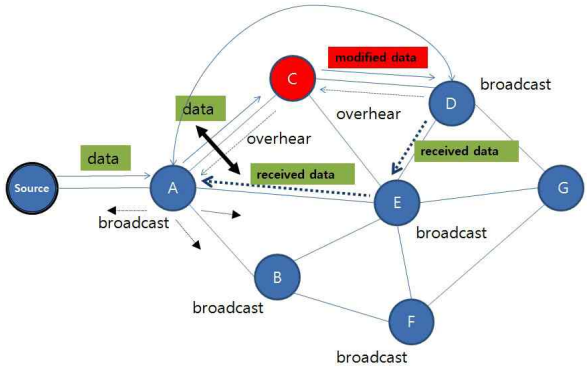
(그림 6)에서 노드 D는 정상적으로 목적지까지 데이터를 전송하였으나 노드 C가 Ack를 버리고 노드 D를 거짓신고를 한다. 이럴 경우 신고 받은 노드 D는 자신의 거짓신고를 반박하며 정상노드라는 것을 broadcast한다. 그러면 노드 A는 노드 C의 거짓신고 여부를 확인하기 위해 협업관계에 있는 이웃노드 노드 E와 D에게 정상적으로 데이터를 받았는지 상호 정보교환를 통하여 노드 C의 행위를 확인하게 된다. 또한 목적지 노드 G도 정상적으로 데이터를 받았다는

메세지(reply)를 노드 A에게 보내된다. 결국 노드 A는 이웃 노드들 간 협업된 메세지를 통하여 노드 C가 거짓 신고한 것을 확인한다. 그리고 이웃노드들에게 control 패킷을 보내서 노드 C가 악의적인 행위를 했음을 broadcast하고 각 노드들은 이웃노드들에 대한 관리테이블을 유지하게 된다.

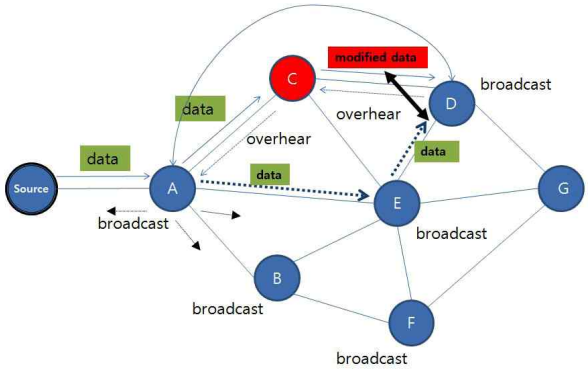
만일 소스노드-A노드-B노드-목적지 노드와 같은 경우, 소스 노드가 A노드로 패킷을 전송하고, A노드가 B노드로 수신한 패킷을 전송하는 경우에 A노드로부터 전송되는 패킷을 소스 노드가 overhear하지 못할 수 있다. 이때, 정상노드가 악의적인 노드로 간주될 수 있는 문제점이 있다. 이와 같은 문제점을 방지하기 위해 RTS(Request To Send)/CTS(Clear To Send)를 사용한다. RTS는 소스노드에서 다음노드에게 보낼 데이터가 있다고 요청하는 것이고, CTS는 그에 대한 응답이다. 즉, RTS/CTS 절차를 사용하면 CTS를 받은 노드만 데이터 전송을 할 수 있기 때문에 소스노드가 동시에 패킷을 송수신하는 문제를 해결함으로써 정상노드가 악의적인 노드로 간주되는 문제점을 해결한다.

3.1.3 원(Source)데이터를 변경해서 보내는 경우

원(source) 데이터를 변경해서 보내는 악의적인 노드를 확인하는 방법은 많은 제한사항이 있었다. 그러나 이웃노드들과의 협업관계를 유지하면서 전송노드가 데이터를 확인하는 방법과 수신노드에서 받은 데이터를 확인하는 방법을 통하여 원(source)데이터를 변경하는 악의적 노드를 탐지할 수가 있다.



(a) 전송노드 A가 확인 및 통보



(b) 수신노드 D가 확인 및 통보

(그림 7) 원(Source)데이터를 변경하는 악의적 노드 확인

(그림 7)에서 노드 A는 노드 C에게 데이터를 전송하고, 노드 C는 데이터를 변경하여 노드 D에게 전송하였을 경우 전송노드가 확인하는 방법은 (그림 7(a))와 같이 노드 A는 데이터를 전송 후 원 데이터를 버퍼에 저장하고 다음노드와 연결된 노드 E와 협력관계를 유지하게 된다.

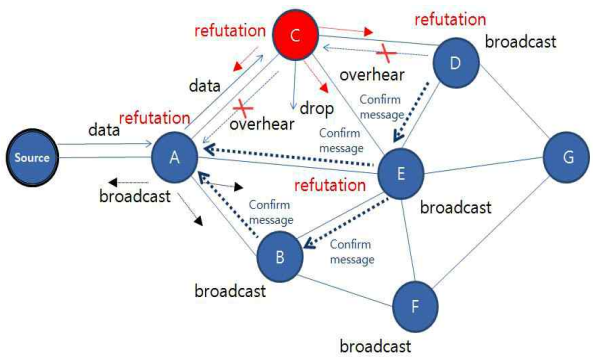
즉 노드 E는 노드 A입장에서 볼 때 노드 D와 연결되어 있는 노드이기 때문이다. 노드 D는 노드 C로부터 받은 데이터 정보를 노드 E에게 보내고 노드 E는 노드 A에게 정보를 보내게 된다. 전송노드 A는 노드 C에게 전송한 데이터와 노드 E로부터 받은 정보를 상호 비교하여 노드 C가 데이터를 변경한 것을 판단한다. 이웃노드들에게 노드 C의 행위를 broadcast 하고 이웃노드들은 노드 C의 행위에 대한 관리테이블을 유지하게 된다.

또한 수신노드가 확인하는 방법은 (그림 7(b))와 같이 노드 A는 노드 C로 데이터를 전송하면서 대체경로인 A-E-D를 통해 원 데이터 전송과 관련된 정보를 알려준다. 그러면 수신노드 D는 노드 C로부터 받은 데이터와 이웃노드 E로부터 받은 데이터를 상호 비교하여 상이할 경우 노드 C를 악의적인 노드로 판단한다. 그리고 이웃노드들에게 노드 C의 행위를 broadcast 하고 이웃노드들은 노드 C의 행위에 대한 관리테이블을 유지하게 된다.

3.1.4 악의적인 노드로 신고될 때 거짓반박하는 경우

악의적인 노드가 자신의 악의적인 행위에 대해 신고를 당했을 경우 이를 거짓으로 반박 할 수 있다.

(그림 8)에서 노드 A노드 C로 데이터를 전송하였으나, 노드 C는 데이터를 버림으로써 악의적인 노드로 신고를 당하였다. 그러나 노드 C는 정상적으로 데이터를 전송했다고 반박하는 경우가 발생 할 수 있다. 이때 노드 A는 협업관계에 있는 이웃노드 E와 노드 D에게 데이터를 정상적으로 받았는지 확인하기 위하여 메세지를 상호교환(notice, reply)함으로써 노드 C가 거짓 반박하고 있다는 것을 확인 할 수 있다. 이때 이웃노드들에게 노드 C가 악의적인 행위를 했음을 broadcast하고 각 노드들은 악의적인 행위패턴 정보, 즉 노드 C가 데이터를 버렸다는 정보를 관리테이블에 등록하고 관리한다.



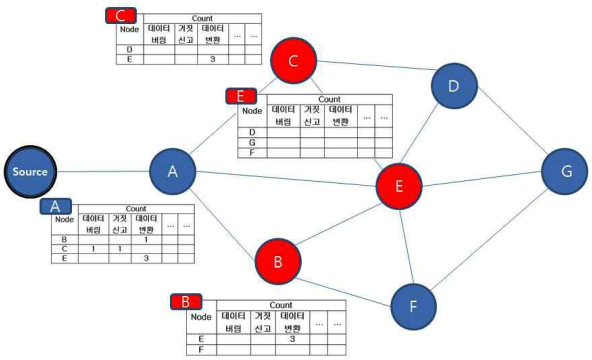
(그림 8) 거짓 반박하는 악의적인 노드 확인

3.2 신뢰기반 라우팅 경로를 통한 데이터 전송

3.2.1 탐지 정보 유지

악의적인 행위 패턴을 탐지하는 과정에서 각 노드는 포워드한 인접노드에 대하여 관리테이블을 유지하고 있고, 악의적 행위 패턴에 대하여 count 정보를 관리하고 있다.

이와 같은 정보는 라우팅 경로설정시 RREQ 패킷에 신뢰지수(Trust_value)로 반영될 수 있도록 하였다. 예를 들어 노드의 악의적인 행위 패턴에 대한 관리테이블의 count정보는 (그림 9)와 같이 데이터 버림, 거짓신고, 데이터 변경등 악의적인 행위에 대한 카운트가 되고 신뢰지수의 임계치(Threshold_count)값이 적용이 되어 경로를 설정한다.



(그림 9) 악의적 행위 패턴 관리정보테이블

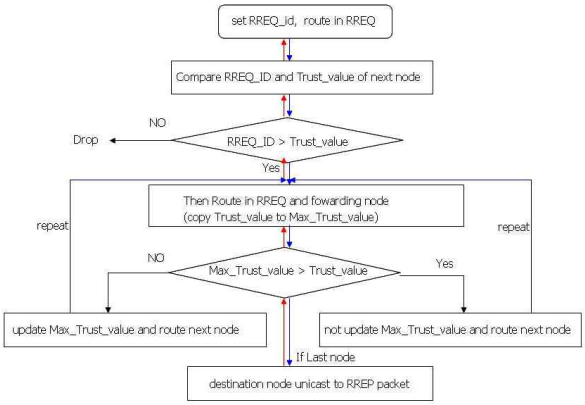
라우팅 경로를 설정할 때 각 노드는 RREQ 메세지에 악의적 행위 패턴에 대한 임계치(Threshold_coun)와 이웃노드들에 대한 신뢰지수(Trust_value)를 유지하여 라우팅 경로를 설정한다. RREQ 메시지 포맷은 <표 1>과 같다.

〈표 1〉 RREQ Message Format

항 목	용 도
Msg_Type	메시지 종류를 표시함(0x0a: RREQ)
Len	메시지의 총 길이를 표시함
TTL	Time To Live, 최대 홉수 (노드 경유시 1씩 감소)
LQI	IEEE 802.15.4에 기술된 LQI 값
Target.Addr.Type	0x02=2byte 단축주소, 0x03=8 byte 확장주소
Target.Addr	목적지 주소
Orign.Addr.Type	0x02=2byte 단축주소, 0x03=8byte 확장주소
Orign.Addr	송신지 주소
Orign.Seq	가장 최근 수신한 목적지 노드의 순서번호
Orign.HopCnt	경유한 노드의 홉수
Threshold_count	악의적 행동에 대한 임계치
Threshold_trust	경로설정시 요구되는 노드 신뢰지수 임계치
Trust_value	이웃노드들에 대한 신뢰지수
Max_Trust_value	이웃노드들에 대한 최대 신뢰지수

3.2.2 신뢰기반의 라우팅 경로설정 및 데이터 전송

(그림 10)은 라우팅 경로설정 과정을 나타낸다. 경로 설정 방법은 우선 이웃노드들은 RREQ 메시지를 수신하면 가장 먼저 신뢰지수를 충족하는지 확인한다. 설정된 신뢰지수와 각 노드의 신뢰지수 값을 비교 한 후 충족되지 않으면 패킷은 버려지고, 충족되면 다음노드로 포워딩 한다. 그런 다음 신뢰지수 값을 이전노드가 가지고 있는 최대값으로 업데이트 한다. 이와 같은 과정을 목적지 노드까지 반복한다. 최종적으로 소스 노드로부터 목적지 노드까지 갈 수 있는 다수의 경로 중 신뢰지수의 합이 최대인 경로가 설정되게 되며, 해당 경로를 통해 RREP패킷을 역방향으로 소스노드까지 전송해 가면서 신뢰기반의 최종 라우팅 경로를 설정하여 데이터를 전송하게 된다.



(그림 10) 신뢰기반의 경로 설정 절차

4. 성능 평가 및 분석

성능 평가 및 분석을 위해 비주얼 C++를 이용하여 프로그램 구현을 통해 시뮬레이션을 실시하였다.

시뮬레이션을 위한 주요 환경설정 값은 <표 2>와 같이 노드수는 100개로 하였으며 이중 악의적인 노드 수는 20개로 설정하였다. 악의적인 행위에 대한 임계치는 3으로 설정하였다. 임계치가 3이라는 것은 악의적인 행동을 3번했을 경우 악의적인 노드로 판단하고 경로설정에서 제외되는 수치이다. 악의적인 노드로 설정된 20개의 노드가 악의적인 행위를 할 확률을 50%로 설정하였다. 성능평가는 악의적인 행위 패턴 유형별 즉 데이터를 버리거나 변경한 경우, 정상노드가 악의적인 노드로 신고한 경우, 악의적인 노드로 신고될 때 이를 반박하는 경우 각각에 대하여 악의적인 노드 탐지율에 대하여 평가를 하고, 또한 전송지연 시간을 평가하였다. 기존방법인 Watchdog&Pathrater, CONFIDENT 및 Nuglet와 성능을 비교하여 분석 하였다.

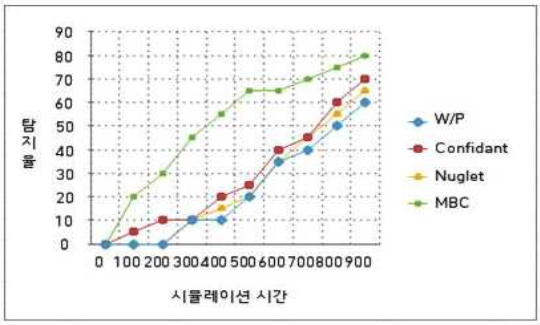
〈표 2〉 시뮬레이션 주요 환경 설정값

설정환경	설정값
지역크기	1000*1000(m)
노드수	100
악의적 노드수	20
임계치	3
악의적인 행동을 할 확률	50%
이동속도	- Pause Time : 0 ~ 900 sec - Speed : min 0, max 30m/s

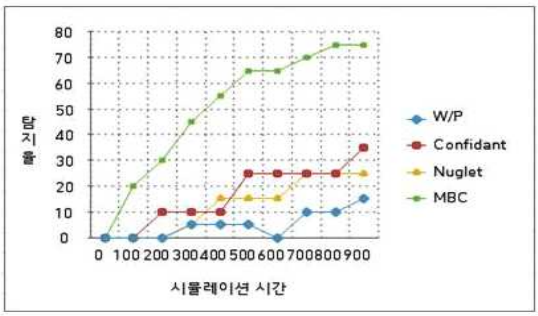
4.1 악의적인 노드 탐지

(그림 11)의 (a)는 데이터를 버릴 경우, (b)는 정상 노드를 악의적인 노드로 신고한 경우, (c)는 악의적인 노드로 신고될 때 이를 반박하는 경우에 대한 노드 탐지율을 평가한 결과이다. 각각의 경우에 대해 MBC가 기존의 방법들 보다 성능이 우수한 것으로 나타나는 것을 알 수 있다. 즉, MBC는 네트워크 수명주기 동안 임계치 이하로 계속하여 악의적인 활동을 하는 노드에 대하여 이웃간의 협업을 통해 악의적 행위를 탐지하고 관리테이블을 이용하여 관련 정보를 상호 공유함으로써 기존방법보다 더 많은 수의 악의적인 노드가 탐지되는 것을 알 수 있다.

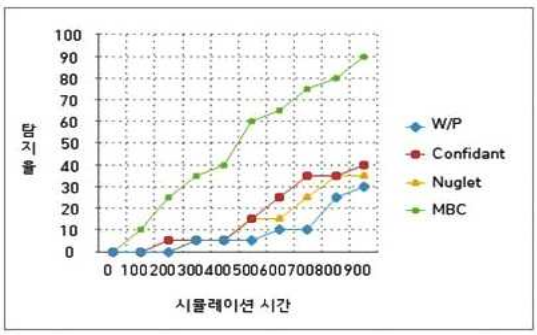
데이터 유통을 방해할 목적으로 정상노드를 악의적인 노드로 신고했을 경우에 기존에 연구되었던 방법들은 정상노드를 신고 한 악의적인 노드가 임계치를 초과하지 않았을 경우에는 신고를 당한 정상노드를 악의적인 노드로 판단할 수밖에 없었다. 또한, 악의적인 노드가 자신의 행위에 대하여 거짓반박 하여 정상노드로 간주되는 경우 기존의 방법에서는 악의적인 노드가 임계치 이하일 경우에 거짓반박을 믿을 수밖에 없었다. 그러나 MBC는 이웃간의 협업을 통하여 반박에 대한 상호교환메시지(notice, reply, confirm)를 통하여 악의적인 노드의 거짓반박을 확인함으로써, 악의적인 노드 탐지율을 약 20~40% 높일 수 있는 것을 확인 할 수 있다.



(a) 데이터를 버릴 경우 노드 탐지 수



(b) 정상노드를 거짓 신고 한 노드 탐지 수

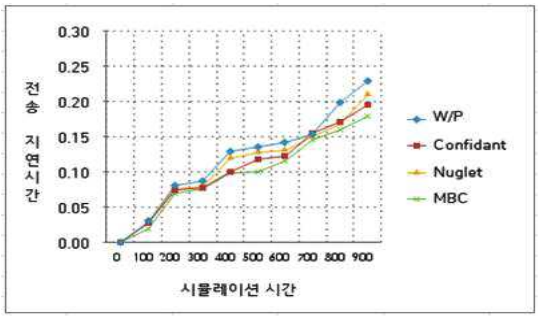


(c) 거짓 반박하는 악의적 노드 탐지 수

(그림 11) 악의적인 행위에 대한 노드 탐지율

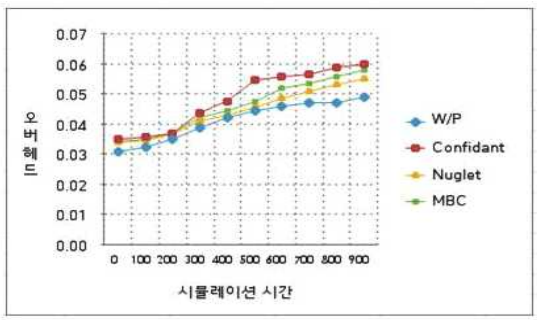
4.2 데이터 전송지연 및 오버헤드

(그림 12)는 데이터 전송지연 시간을 나타내는 것으로 MBC가 기존 방법들보다 전송지연이 평균 20% 낮게 발생하는 것을 확인할 수 있다. 특히, 시간이 지날수록 Watchdog&Pathrater, CINFIDENT 및 Nuglet 보다 전송지연 시간이 더 크게 줄어드는 것을 확인 할 수 있다. 기존 연구들은 일정 시간동안 악의적인 행위가 발생함에도 불구하고 악의적인 노드로 판별하지 못하는 경우가 다수 발생하게 되지만, MBC는 인접노드와 협업을 통해 악의적인 행위를 탐지함으로써 수차례 반복되는 소스 노드의 재전송 과정을 최소화함으로써 전송지연 시간을 감소시킬 수 있기 때문이다.



(그림 12) 전송 지연시간

그러나 (그림 13)에 나타나듯이 MBC는 이웃 노드들과의 협업을 수행하기 위해 notice, reply 메시지를 control 패킷 필드에 추가함으로써 Watchdog&Pathrater와 Nuglet 보다 각각 10%, 5% 패킷 오버헤드가 증가하는 것을 확인 할 수 있다. 하지만 Confidant 보다는 5% 낮은 오버헤드를 나타내는 것을 확인할 수 있다. 결과적으로 악의적인 노드 탐지율과 데이터 전송 지연율이 향상된 정도에 비해 오버헤드의 증가는 상대적으로 매우 작기 때문에, 보안 측면에서 고려해 볼 때 MANET 환경에서 발생 할 수 있는 라우팅 공격 양상에 효율적으로 대처할 수 있는 방법임을 알 수 있다.



(그림 13) 패킷 오버헤드

5. 결 론

현재 우라 군은 노드와 노드간의 Ad-hoc 네트워크를 사용하는 TICN을 도입할 필요성이 증대되고 있다. Ad-hoc 네트워크는 그 특성상 유선 네트워크에 비해 악의적 노드 공격에 매우 취약하므로 우리는 다양한 공격을 보다 안전하게 대처할 수 있는 MBC기법을 제안하였다. 제안한 MBC기법은 악의적인 노드 확인 과정에서 이웃노드와 협업관계를 맺고 상호 신뢰하에 악의적인 행위를 하는 노드를 이중적으로 감시하여 탐지한다. 그리고 탐지 후에 이웃노드에게 악의적인 노드를 관리할 수 있는 관리 테이블을 유지하도록 설계하였다. 즉, 제안하는 기법은 협업과 상호 신뢰지수를 기반으로 악의적인 노드를 식별하고 식별된 노드를 라우팅 경로에서 배제 시킨 후 라우팅경로를 설정하여 데이터를 전송한다. 우리가 제안한 MBC기법을 기존방법과 비교하기 위하여 시뮬레이션을 수행하였다. 그 결과 기존방법보다 악의적인 노드 탐지율이 향상되었고 전송 지연율이 감소함으로써 MANET에서 발생 할 수 있는 라우팅 공격 양상에 효율적으로 대처함을 확인하였다.

이 논문에서 제안한 기법은 악의적 노드를 효율적으로 탐지함을 확인하였으나, 관리테이블의 새로운 속성 추가에 따른 오버헤드가 발생한다. 또한 선의의 협업관계가 이루어지지 않을 경우 문제가 발생할 수 있으므로 이에 대한 후속 연구가 수행되어야 한다.

참 고 문 헌

[1] 배달형, 조용건, “NCW 컴퓨터네트워크작전(CNO)의 작전적 원리와 한국군의 발전방향”, 국방연구, 2009.

[2] H. Yang and H. Luo and F. Ye and S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications, 2004.

[3] 황윤철, “MANET에서 비정상 노드를 효율적으로 탐지하기 위한 보안 설계”, 한국통신학회논문지 제35권 제3호(네트워크 및 서비스), pp.373-563, 2010.

[4] 김재홍, 김세헌, “MANET에서 wormhole 공격의 탐지 및 방지를 위한 알고리즘에 대한 연구”, 한국경영과학회 추계학술대회 및 정기총회, pp.494-497, 2008.

[5] H. Jhaveri and D. Patel and D. Parmar and I. Shah, “MANET Routing Protocols and Wormhole Attack against AODV”, IJCSNS International Journal of Computer Science and Network Security, Vol.10, No.4, Apr., 2010.

[6] C. Komala and S. Srinivas and S. Padmashree and E. Elevarasi, “Wireless Ad hoc Mobile Networks”, National Conference on Computing Communication and Technology, pp.168-174, 2010.

[7] A. H. A. Rahman and Z. A. Z.ukarnain, “Performance Comparison of AODV,DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks”, European Journal of Scientific Research, pp.566-576, 2009.

[8] S. K. B.V and V. A.L, “Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism, International Journal of Scientific & Engineering Research, Vol.1, Issue3, Dec., 2010.

[9] N. S. M. Usop and A. Abdullah and A. F. Abidin, “PerformanceEvaluation of AODV,DSDV & DSR Routing Protocol in Grid Environment”, IJCSNS International Journal of Computer Science and Network Security, pp.261-268, 2009.

[10] H. Rutvij and D. Ashish and D. Jatin, “MANET Routing Protocols and Wormhole Attack against AODV”, IJCSNS International Journal of Computer Science and Network Security, Vol.10, No.4, Apr., 2010.

전 서 인

e-mail : jsi0198@naver.com

1993년 서원대학교 수학교육학과(이학사)

2002년 경북대학교 컴퓨터공학과(공학석사)

2008년 충북대학교 전자계산학과(박사수료)

2009년～현 재 육군본부 전산체계처 전산장교

관심분야 : 센서네트워크, 시공간DB, 데이터마이닝, DB보안

류 근 호

e-mail : khryu@dblab.chungbuk.ac.kr

1976년 숭실대학교 전산학과(이학사)

1980년 연세대학교 전산전공(공학석사)

1988년 연세대학교 전산전공(공학박사)

1976년～1986년 육군군수지원사 전산실 (ROTC 장교), 한국전자통신연구원(연구원) 한국방송통신대학교 전산학과(조교수) 근무

1989년～1991년 Univ. of Arizona Reaearch Staff(TempIS 연구원, Temporal DB)

1986년～현 재 충북대학교 전자정보대학 소프트웨어전공 교수

관심분야 : 시간데이터베이스, 시공간데이터베이스, DB보안 Temporal GIS, 지식기반정보검색시스템, 데이터마이닝, Biomedical 및 Bioinformatics