MANET에서 안전한 통신 위한 악의적 노드 검출 기법

김태은, 이영구, 이창보, 주소진, 전문석
숭실대학교 대학원 컴퓨터학과
e-mail: eunii31@ssu.ac.kr, ad3927@ssu.ac.kr,
onsmile79@nate.com, yetiblow@nate.com,
mjun@computing.ssu.ac.kr

The malicious node detecting system for secure communications in MANET

Taeeun Kim, Younggu Lee,
Changbo Lee, Sojin Joo, Moonseog Jun
Dept of Computer Science, Soongsil University

요 약

최근 MANET에서 보안적인 요소를 추가한 라우팅 연구가 활발하지만 기존에 제시된 방안들은 거짓 신고를 하는 악의적인 노드를 식별하지 못하는 문제점과 라우팅 측면에서 비효율적인 문제점이 있었다. 본 논문에서는 신고, 반박, 증명의 메시지를 이용하여 악의적인 노드의 여러 가지 공격을 차단하고 라우팅 측면에서 보다 효율적인 프로토콜을 제안한다. 제안하는 프로토콜은 여러 가지 MANET 라우팅 프로토콜에서 적용이 가능하며 라우팅 경로 선정 및 관리의 보안적인 부분을 추가하였다.

1. 서론

최근 무선 네트워크 기술의 급속한 발전과 더불어 기지국이나 AP(Access Point)와 같은 하부구조(Infrastructure)가 없는 MANET(Mobile Ad Hoc Network)에 대한 응용 범위와 빈도가 급격히 증가하고 있다. MANET의 연구는 네트워크를 구성하는 각 요소들이 상호 협력적인 가정을 하여 라우팅에 집중 되어 왔다. 하지만 실제 네트워크 환경은 상호 협력적인 상황만 존재하는 것이 아니므로 안전한 통신을 위한 보안 프로토콜이 필요하다. 또한 MANET에서 이동 노드들은 호스트와 라우터의 기능을 동시에 수행하기 때문에 보안 프로토콜을 설계 시 고려해야 한다.

이런 MANET의 특성에 대한 보호 방법은 사전 예방법과 사후 조치방법이 있다. 사전 예방법은 라우팅 경로를 설정하는 단계에서 악의적인 노드를 식별하여 제외시키고 경로를 설정하는 방식이고, 사후 조치방법은 라우팅 경로를 설정하더라도 공격자에 의해 잠식되는 경우 악의적인 노드를 찾아내어 라우팅에서 제외시키는 방식이다.[1]

본 논문에서는 사후 조치방법을 이용하여 악의 적인 노드를 식별하고 악의적인 노드가 패킷을 버리거나 변조하는 행위 이외에 정상적인 노드를 거짓으로 신고하는 행위까지 식별하여 조치하는 프로토콜을 제안한다.

2. 관련 연구

2.1 경로설정에 대한 공격

경로설정에 대한 공격은 라우팅 프로토콜의 경로 설정과정의 정보를 정상적으로 전달하지 않은 모든 행위를 뜻한다. 예를 들면, DSR(Dynamic Source Routing)[2] 라우팅 프로토콜에서 전송패킷 내에 기록되는 source route 목록의 노드를 추가, 삭제 하는 행위가 있다.

2.2 패킷 전달에 대한 공격

패킷 전달에 대한 공격은 경로설정과정에서는 정상적으로 패킷을 전달 하지만 실제 데이터 패킷은 제대로 전달하지 않는 행위를 말한다. 공격의 예로는 전달해야 할 패킷을 버리거나 변조하는 행위가 있으며 이러한 공격을 차단하기 위한 방법으로는 Watchdog and Pathrater[3], 이기적인 노드 관리 방안[4] 등이 있다.

2.3 Watchdog and Pathrater

Watchdog and Pathrater 방법에서 각 노드는 자신이 전송한 데이터의 복사본을 버퍼에 저장하고 다음 노드의 전송을 overhear 하여 자신의 버퍼의 데이터와 비교하여 올바른 데이터를 전송하는지 판단한다. 다음 노드가 올바른 데이터를 전송하면 버퍼의 복사본을 버리고, 다음 노드가 데이터를 전송하지 않거나 자신이 보낸 데이터와 다른 데이터를 보내는 경우 failure tally를 증가시킨다. 이 tally가 threshold를 넘어서면 다음 노드가 악의적인 노드라고 판단하여 소스 노드에게 신고한다. 신고를 받은 소스 노드는 사용 중인 경로에 대한 사용을 중지하고 새로운 경로 설정을 하게 된다.

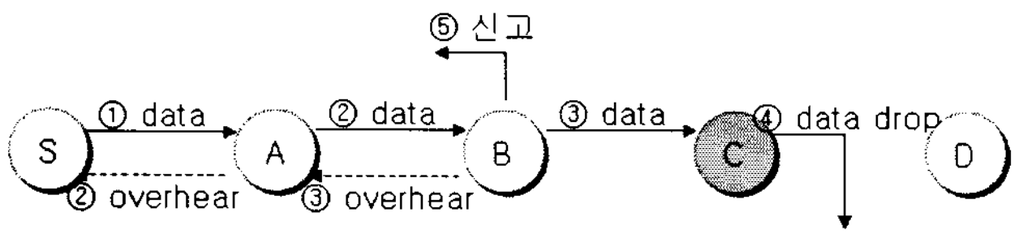

그림 1. Watchdog and Pathrater

2.4 이기적인 노드 관리 방안

이기적인 노드 관리 방안에서 각 노드는 데이터 전송 후 복사본을 저장하고 다음 노드로부터 증명서를 받는다. 목적지 노드는 데이터가 전송되면 데이터를 받았다는 ACK 메시지를 소스 노드에게 보냄으로서 데이터의 올바른 전송을 확인 한다. 만약 악의 적인 노드에 의해 ACK 메시지를 받지 못한 노드가 자신의 다음 노드를 소스 노드에게 신고한다. 증명서는 각 노드의 개인키로 암호화 되므로 다른 노드가 임의로 발행할 수 없으므로 거짓 신고의 가능성을 방지한다. 신고를 받은 소스 노드는 첨부되어온 노드의 공개키로 증명서를 복호하여 거짓신고 여부를 판단한다.

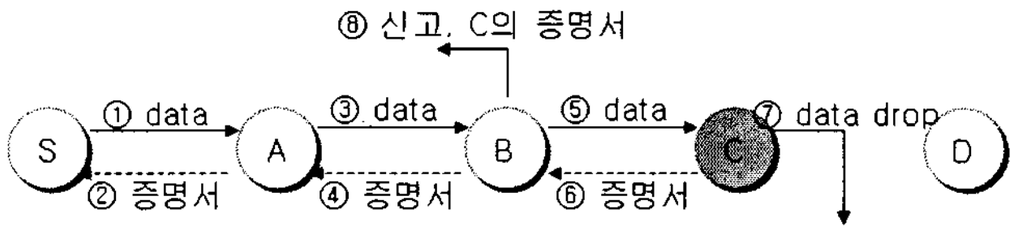

그림 2. 이기적인 노드 관리 방안

2.5 기존방식의 문제점

위의 방식들은 악의적인 노드가 메시지를 버리거나 변조하는 동작을 판단하여 차단 할 수 있지만, 정상적인 노드를 거짓으로 신고하는 경우 이를 식별해 낼 수 없는 문제점이 있다. 위의 방식들 외에도 거짓 신고를 판단하기 위한 기존의 방법들은 신고의 내용을 저장해 두고 동일한 악의적인 노드의 수차례의 거짓 신고에 의해 해당 노드를 차단한다. 이에 데이터 전송 부분에 있어 악의적인 노드를 피해가기 위해서 몇 번의 신고가 계속적으로 일어나야 하고, 데이터 전송도 그만큼 많아짐에 따라 악의적인 노드를 찾기 위해서 라우팅의 효율이 낮아질 수 있다.

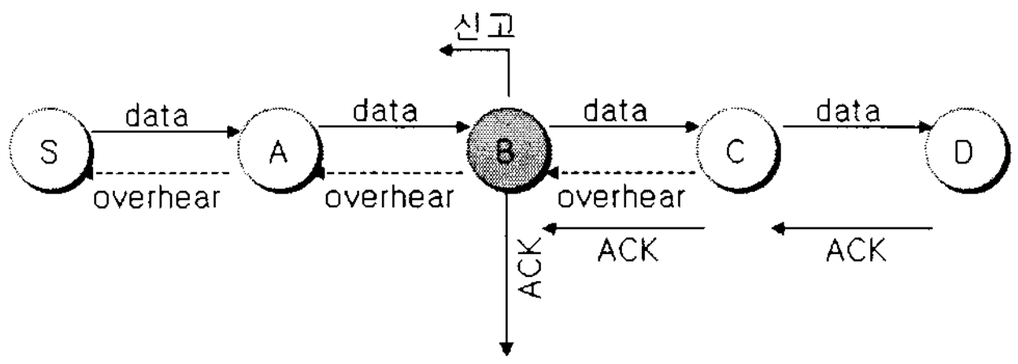

그림 3. 기존연구 방법에서 거짓 신고의 예

3. 제안 프로토콜

3.1 초기 설정

MANET에 속한 각 노드는 symmetric link를 형성하여 이웃 노드의 전송을 overhear 할 수 있다고 가정 한다. 또한 공개키 암호방식을 사용하여 노드 자신의 증명서를 발급하기 위해 개인키는 노드 자신만이 알고 있으며 공개키는 MANET을 구성하는 모든 노드들이 알고 있다고 가정한다.

신고하는 메시지의 구조는 신고할 노드, 신고하는 노드, 신고하는 메시지 악의적인 행동 타입 등이 포함된다. 반박 메시지는 자신의 이웃 노드 또는 자신을 신고하는 메시지를 수신할 때 broadcast 한다. 자신의 이웃 노드가 신고하였을 경우 수신하는 즉시 반박 메시지를 broadcast 하고, 자신의 이웃이 아닌 다른 노드가 자신을 신고하는 경우 또는 라우팅 경로 설정 중에는 반박 메시지에 자신의 이웃 노드들에게 증명 메시지를 요청한다. 증명 메시지는 목적

지 노드의 경우 자신이 수신한 메시지 또는 데이터를 전송하고 반박 메시지를 전송한 이웃노드 들은 자신의 이웃노드 목록과 메시지를 함께 전송한다.

3.2 기본 동작

제안하는 프로토콜은 거짓으로 신고를 하는 노드를 검출하기 위한 방법을 중점적으로 설명하겠다. MANET에 속한 노드는 데이터를 전송 후 전송한 데이터를 버퍼에 저장하고 다음 노드의 전달 과정을 overhear 하여 자신이 보낸 메시지와 비교한다. 만약 악의적인 노드라고 판단되는 노드를 찾게 되면 악의적인 노드를 신고하는 메시지를 신고하는 노드의 개인키로 암호화 하여 네트워크 에러메시지와 함께 broadcast 한다. 이런 신고 메시지 역시 거짓 신고를 당하는 노드가 overhear 할 수 있고 거짓 신고를 당하는 노드는 이에 대응하는 반박(retort) 메시지를 broadcast 한다. 이때, 악의적인 노드를 신고하는 메시지와 반박 메시지를 수신한 목적지 노드 또는 반박 메시지를 보낸 노드의 이웃 노드들은 신고와 반박 메시지를 증명하기 위한 증명 메시지를 broadcast 하고 모든 메시지를 수신한 소스 노드는 악의적인 노드를 결정한다.

3.3 제안 프로토콜의 악의적 노드 신고과정

· *Case 1* : 악의적인 노드의 데이터 버림 및 변경

악의적인 노드가 데이터를 버리거나 변경하는 경우 악의적 노드의 전송을 overhear 한 노드가 악의적인 노드를 신고하게 된다. 이때, 신고 메시지를 받은 목적지 노드는 증명 메시지를 소스 노드로 보내 신고를 증명한다.

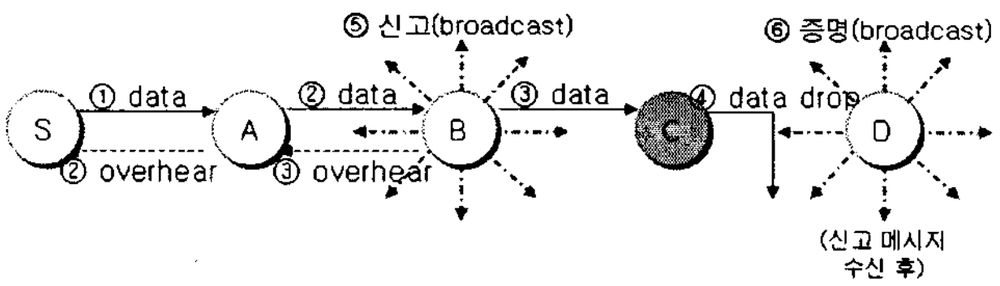

그림 4. Case 1의 데이터 버림의 예

(그림 4)의 경우 신고 메시지와 증명 메시지를 받은 소스 노드는 신고 메시지의 신고 된 메시지와 증명노드가 보낸 메시지를 비교하여 노드 C가 메시지를 보내지 않았다는 것을 확인 하고 C를 악의적 노드라고 알리고 네트워크 동작에서 제외시킨다.

· *Case 2* : 다른 노드로 위장하여 거짓신고

어떠한 노드를 신고하기 위해서 공개키 암호화 방식을 사용하고, 노드 고유의 개인키로 암호화 하여 신고, 반박, 증명 메시지를 생성해서 전송해야 하기 때문에 다른 노드로 위장하여 거짓신고를 하는 것을 차단 할 수 있다.

· *Case 3* : 다른 노드를 임의로 거짓 신고

악의적인 노드가 자신의 이웃이 아닌 전혀 상관없는 다른 임의의 노드를 거짓으로 신고할 경우 목적지 노드의 증명 메시지로 목적지 노드가 데이터를 수신한 것을 확인 할 수 있고, 신고를 당한 노드의 반박 메시지로 그의 이웃 노드들이 증명 메시지를 보냄에 따라 임의의 거짓 신고를 막을 수 있다.

· *Case 4* : 정상적인 노드를 거짓 신고하는 경우

(그림 5)의 경우 노드 C는 정상적으로 목적지 노드에게 데이터를 보냈지만 악의적인 노드 B는 목적지 노드에게서부터 전송된 ACK 메시지를 버리고 노드 C를 악의적인 노드라고 신고한다. 이때, 노드 B의 신고 메시지를 수신한 노드 C는 자신이 악의적인 노드가 아님을 반박하는 반박 메시지를 네트워크로 broadcast 하게 된다. 또한, 신고 메시지를 수신한 목적지 노드 역시 증명 메시지를 broadcast 하게 된다. 신고, 반박, 증명 메시지를 모드 수신한 소스 노드는 신고 메시지에 신고 된 메시지가 증명 메시지에 첨부되어 있다면 노드 C는 목적지 노드에게 메시지를 전송 하였다고 판단하고 노드 B를 악의적으로 거짓 신고를 한 노드라고 네트워크에 알리고 네트워크 동작에서 노드 B를 제외시킨다.

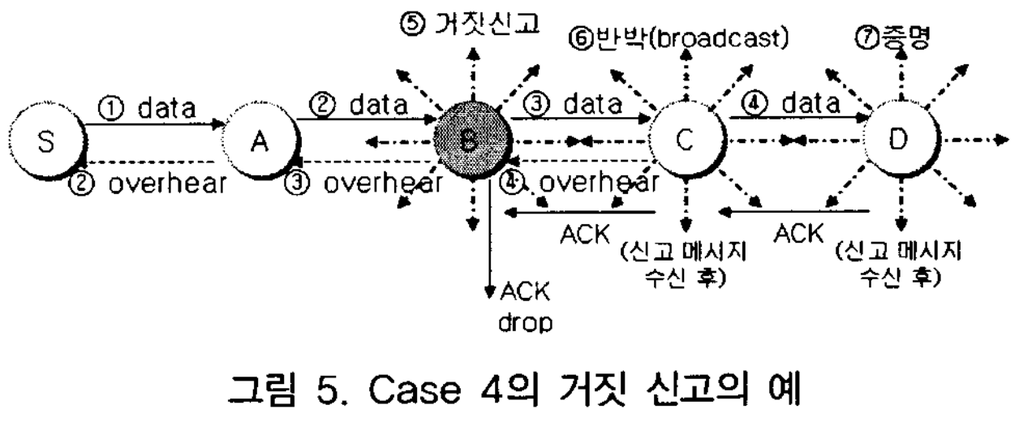

그림 5. Case 4의 거짓 신고의 예

· *Case 5* : 악의적인 노드의 거짓 반박

Case 1과 같은 상황에서 악의적인 노드가 자신의 데이터 버림 또는 변경을 들켜 신고를 당했을 때 자신이 악의적인 노드가 아님을 반박할 수 있다. 하지만 노드 B가 신고한 메시지와 목적지 노드가 수신한 메시지가 다르게 되어 노드 C의 거짓 반박은

무효가 되고 역시 노드 C가 악의적인 노드로 네트워크에 알려지게 되고 네트워크 동작에서 제외된다.

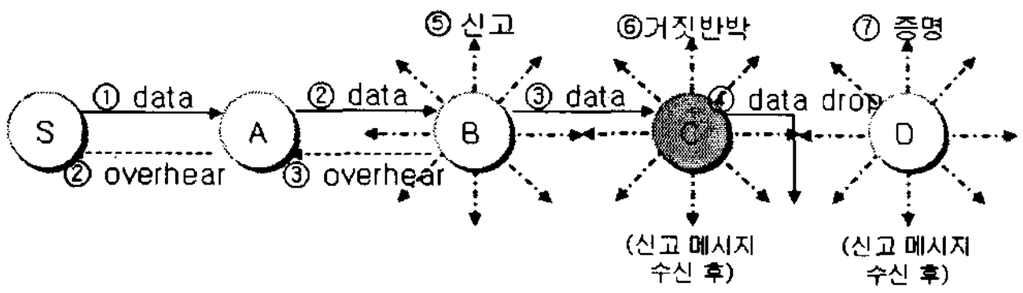

그림 6. Case 5의 거짓 반박의 예

4. 성능평가 및 안전성

4.1 라우팅 측면의 신속성

기존 연구되었던 방법에서 보여줬던 악의적인 노드의 몇 차례의 악의적인 행동을 테이블에 저장해 두었다가 threshold를 초과하였을 경우 해당되는 노드를 악의적 노드로 보고 네트워크 동작에서 제외하기 때문에 threshold를 초과하기 위해 악의적인 노드에게 수차례의 메시지를 계속 보냄으로써 라우팅의 신속함이 떨어지게 된다. 하지만 제안하는 프로토콜 에서는 악의적인 노드의 한 번의 행위에 반박과 증명이라는 시스템을 활용하여 여러 번의 중복되는 소스 노드의 전송 과정을 거치지 않고 악의적인 노드를 판별해낼 수 있어 더욱 신속하게 올바른 라우팅 과정을 수행 할 수 있다.

4.2 정확한 악의적 노드 판별

MANET에서의 기존의 악의적인 노드를 판별하고 차단하는 알고리즘들은 악의적인 노드의 계속적인 데이터 버림, 데이터 변조 또는 거짓 신고에 대해서 threshold를 초과할 경우 그 노드를 악의적인 노드라고 판별하여 네트워크의 동작에서 제외시킨다. 하지만 실제 네트워크에서 적용할 때 악의적인 노드는 악의적인 행동을 연속적으로 계속하지는 않을 것이다. 따라서 제안하는 프로토콜을 사용하여 한 번의 악의적인 노드의 올바르지 않은 행동을 차단함으로써 더욱 효과적으로 악의적인 노드를 판별할 수 있다.

4.3 프로토콜의 적용

제안한 프로토콜은 MANET의 데이터 전송 과정에서의 악의적인 노드의 검출에 적용하는 것 이외에도 DSR이나 AODV(Ad hoc On-demand Distance Vector routing)[5]같은 라우팅 프로토콜의 라우팅 경로설정 과정에서도 적용이 가능하다.

라우팅 경로 설정 단계에서 보내지는 RREQ 메시지 또는 RREQ 메시지를 수신한 목적지 노드의 응답 메시지인 RREP 메시지를 악의적인 노드가 버리거나 변경하여 전달하였을 경우에도 악의적인 노드를 신고하고 차단하여 라우팅 경로 설정에서 나오는 악의적인 노드의 행동을 막을 수 있다.

4.4 안전성

제안하는 프로토콜의 안전성은 악의적인 노드에 의해 네트워크에 잘못된 정보가 퍼질 수 있는 상황을 방지해서 목적지 노드까지의 올바른 메시지를 전송해줄 수 있고, 악의적인 노드에 의해 좋지 않은 라우팅 경로를 사용할 수 있게 되는 경우와 계속 되는 메시지를 보내는 경우에는 네트워크를 구성하는 각 노드의 많은 자원을 소모하게 되는데 이를 방지함으로써 네트워크의 불필요한 자원 소모를 막을 수 있다.

5. 결론

MANET은 하부구조가 없는 특성상 무선으로 노드들 간에 데이터를 송수신하기 때문에 보안에 취약하고 악의적인 노드의 공격에 데이터가 손실되었을 경우나 라우팅 경로가 회손 되었을 경우에 그 피해가 심각하다. 따라서 본래 네트워크의 효율을 전부 살릴 순 없지만 최소한의 오버헤드를 감수하는 보안적인 연구를 활발히 해야 할 것이다.

본 논문에서는 악의적인 행동을 하는 노드와, 악의적인 노드를 신고하는 신고노드, 또 악의적인 누명을 쓰고 반박을 하는 반박노드 마지막으로 이 신고를 받고 소스 노드에게 악의적인 노드를 증명하는 증명노드로 나누어서 네트워크에서 악의적인 행동을 하여 네트워크의 효율을 떨어트리는 노드를 신속하게 찾고 처리할 수 있는 시스템을 제안하여 기존의 제시되었던 알고리즘 보다 더 빠르고, 정확하고 안전하며 다양한 라우팅 프로토콜에 적용이 가능하여 보안적인 요소가 꼭 필요한 MANET에서 안전한 통신을 가능하게 하였다.

참고문헌

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

cations, 2004
[2] J.Broch, D.Johnson & D.Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," http://ierf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, IETF Internet, 15 April, 2003, Work in progress
[3] S.Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," ACM MOBICOM, 2000.
[4] Gajin Na et al, "Secure Mechanism to manage selfish nodes in Ad hoc Network," JCCI, 2004.
[5] S.R.Das & C.E.Perkins, "Ad hoc On-Demand Distance Vector Routing for Mobile Ad Hoc networks," http://www.ierf.org/rfc/rfc3561.txt, July, 2003.