Journal of The Korea Society of Computer and Information
Vol. 18, No. 3, March 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.3.035

MANET에서 악의적 노드 탐지율 향상을 위한 협업모델 설계

신언석*, 전서인*, 박건우*, 류근호**

Collaboration Model Design to Improve Malicious Node Detection Rate in MANET

Eon-Seok Shin*, Seo-In Jeon*, Gun-Woo Park*, Keun-Ho Ryu**

요 약

MANET에서는 합법적인 노드와 비합법적인 노드 모두 네트워크에 접근이 가능함에 따라 보안 취약점을 안고 있다. MANET에 관한 대부분의 연구들은 라우팅 경로 또는 패킷 전달에 대한 공격 측면에만 중점을 두고 있으며, 특히 악의적인 노드의 다양한 공격에 효과적으로 대응하는데 한계가 있다. 이 논문에서는 MANET에서 다양한 악의적인 노드를 효율적으로 탐지하기 위한 DTecBC (detection technique of malicious node behaviors based on collaboration) 기법을 제안하였다. 제안 기법은 이웃 노드들 간의 협업관계를 기반으로 상호 메시지 교환을 통하여 악의적인 노드를 관리할 수 있도록 설계하였다.. 제안 기법의 효율성 검증을 위해 OPNET 시뮬레이션 툴을 사용하여 기존의 대표적 탐지기법인 Watchdog, CONFIDANT, SRRPPnT와 비교하였다. 평가 결과, 제안 기법은 기존 기법들에 비해 다양한 유형의 악의적인 노드 행위를 종합적으로 탐지 가능함이 확인 되었다.

▸ Keywords : MANET, 악의적인 노드, 악의적 행위 패턴, 신뢰지수, 보안 라우팅

Abstract

MANET has a weak point because it allows access from not only legal nodes but also illegal nodes. Most of the MANET researches had been focused on attack on routing path or packet forwarding. Nevertheless, there are insuffcient studies on a comprehensive approach to detect various attacks on malicious nodes at packet forwarding processes. In this paper, we propose a technique, named DTecBC (detection technique of malicious node behaviors based on collaboration), which can handle more effciently various types of malicious node attacks on MANET environment. The DTecBC is designed to detect malicious nodes by communication

• 제1저자 : 신언석 교신저자 : 전서인
• 투고일 : 2012. 12. 26, 심사일 : 2013. 1.22, 게재확정일 : 2013. 2. 12.
* 육군본부(army head quater)
** 충북대학교 전자계산학과(School of Electronic and Computer Engineering, Chungbuk National University, Chungbuk, Korea)

between neighboring nodes, and manage malicious nodes using a maintain table. OPNET tool was used to compare with Watchdog, CONFIDANT, SRRPPnT for verifying effectiveness of our approach. As a result, DTecBC detects various behaviors of malicious nodes more effectively than other techniques.

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

I. 서 론

우리 군은 이동 환경에서도 고속 대용량의 데이터 처리가 가능한 차세대 TICN체계(Tactical Information Communication Network) 구축을 추진 중이며, 이 체계에서는 MANET (Mobile Ad-hoc NETwork)이 적용될 예정이다.

MANET은 이동성을 갖는 노드로 구성되어 있으며, 기반 구조 없이 자체 네트워크 구성이 가능하고 스스로 경로를 설정하여 산악지형의 열악한 통신환경을 극복할 수 있다.

그러나 MANET은 노출된 매체, 동적인 토폴로지와 중앙에서 네트워크를 제어해 주는 중재기능이 없기 때문에 정상 노드나 악의적인 의도를 가진 노드가 모두 네트워크에 접근할 수 있는 단점을 가지고 있다. TICN체계 또한 MANET의 단점을 그대로 상속함으로써 이동노드에 악의적인 공격이 발생할 경우 정보유통의 신뢰성과 신속한 전송을 보장할 수 없다.

MANET이 가지고 있는 보안측면에서의 근본적 취약점들을 해결하기 위해 라우팅 공격이나 패킷 전송 시 악의적인 행위를 탐지하기 위한 방안 등이 연구되어 왔다 [1,2,3,4,5]. 하지만 대부분의 연구들은 외부 라우팅 경로 또는 내부 패킷 전달에 대한 공격 중 어느 한 측면에만 중점을 두고 있다.

본 논문에서는 MANET에서 다양한 악의적인 노드 행위 패턴에 대하여 이웃 노드간의 협업기반의 상호 메시지를 통하여 탐지하고, 각 노드에 대한 임계치를 설정하여 관리함으로써 악의적인 노드를 효율적으로 탐지하는 DTecBC (detection technique of malicious node behaviors based on collaboration) 기법을 제안한다.

이 논문을 효율적으로 전개하기 위하여 2장에서는 악의적인 행위 탐지 기법에 대한 기존 연구를 분석하고, 3장에서는 제안하는 기법인 DTecBC에 대하여 알아보고, 4장에서는 시뮬레이션을 통해 성능평가 및 분석하여 제안 기법의 효율성을 증명하며, 5장에서 결론을 제시한다.

II. 관련 연구

1. Watchdog 와 CONFIDANT

Watchdog은 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].

그림 1과 같이 소스노드 S로부터 패킷을 받은 노드 A는는 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.

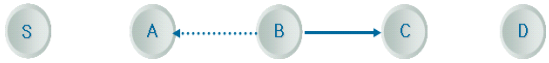


그림 1. Watchdog의 악의적인 노드 탐지 기법

CONFIDANT(Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks)는 Watchdog과 비슷하게 각 노드들이 서로를 감시하면서 악의적인 노드를 탐지하는 메커니즘이다[7]. 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.

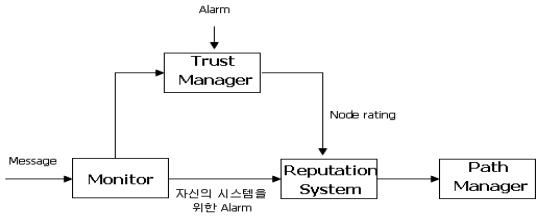


그림 2. CONFIDANT에서 제안하는 메커니즘 구조

그림 2와 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 이웃감시자로부터 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 관리한다.

2. FC 관리테이블을 이용한 탐지기법

MANET에서 악의적인 노드 탐지는 단순히 패킷을 버리거나 변경시키는 노드만을 탐지하는데 중점을 두었기 때문에 악의적인 노드에 의해 정상적인 노드가 악의적인 노드로 취급되는 경우가 많았고, 악의적인 노드들 간 서로 공모하는 노드의 탐지가 미흡하였다.

악의적인 노드가 거짓 신고 했을 때 그 사항을 저장하는 FC (forwarding counter)관리 테이블을 이용하여 식별해 내는 기법을 제안하였다[8].

이 기법은 MANET를 구성할 때 계층적 구조를 이용하여 각 노드 간 상호 인증을 통한 신뢰할 수 있는 관계를 구축한다. 네트워크가 동작함에 따라 공격자에 의해 잠식되는 노드가 발생하기 때문에 잠식된 노드를 찾아 격리 시키는 방법으로 악의적인 노드를 탐지하고 관리한다. FC 관리 테이블에는 표 1과 같이 각 노드의 거짓보고 횟수가 기록되어 있다. 거짓보고 횟수가 주어진 임계치를 초과하면 그 노드는 악의적인 노드로 규정하고 다른 노드들에게 알린다. 이 사실을 통보받은 다른 노드들도 자신의 MN테이블에 그 노드를 악의적인 노드로 등록한다. 그런 후 네트워크 내의 다른 노드들은 악의적인 노드로부터 전송된 패킷들을 모두 무시하고 자신들의 패킷 또한 그 노드로 전송하지 않는다.

표 1. FC 관리테이블 구조

보고노드의 ID	*신뢰도*	*보고 불일치 노드의 ID*	*불일치 횟수*	*거짓보고 횟수*

3. SRPPNT 기법

SRPPnT 기법은 일정기간 악의적인 행위가 이루어지는 노드를 확인하여 신뢰단계를 구성 후, 획득한 각 노드의 신뢰레벨에 따라 경로를 설정함으로써 패킷 및 라우팅 경로 설정에 대해 이루어질 수 있는 악의적인 행위를 효율적으로 대응할 수 있는 방안인 SRPPnT을 제안하였다[9]. 만약 어떠한 노드를 악의적인 노드라고 판단하게 되면 신고하는 노드는 자신의 개인키로 신고(report) 메시지를 암호화하여 네트워크 에러 메시지와 함께 브로드캐스트 한다. 신고 메시지를 받은 정상노드는 해당 메시지가 거짓 신고라는 것을 대응하기 위하여 반박(retort) 메시지를 브로드캐스트 한다. 악의적인 노드를 신고하는 메시지와 반박 메시지를 수신한 목적지 노드 또는 반박 메시지를 보낸 노드의 이웃노드들은 신고와 반박 메시지를 증명하기 위한 증명(proof) 메시지를 브로드캐스트한다.

4. 기존연구의 문제점

첫째, Watchdo기법은 정상 노드임에도 불구하고 악의적 노드로 거짓 신고 되었을 때 대처 할 수 없다는 문제가 있다. 또한 악의적 노드로 판명된 노드가 어떠한 제재도 받지 않고 네트워크상에서 지속적으로 참여, 활동할 수 있다.

둘째, CONFIDANT 기법은 실제 악의적 노드의 행위에 대한 누적 횟수는 임계치를 초과하더라도 각각의 경로에서 임계치를 초과하지 않아 악의적 노드가 고립되지 않을 수 있다. 뿐만 아니라 악의적 노드로 판정되었을 경우에도 이 정보가 우호적 관계에 있는 노드들에 한정하여 공유됨으로써 악의적 노드가 다른 경로를 통로를 통해 그 행위를 반복할 수 있다.

셋째, FC 관리테이블을 이용한 탐지기법 및 SRPPnT 기법은 악의적인 행위에 대한 임계치를 초과하지 않을 경우 탐지가 제한되고, 악의적인 노드가 다른 경로를 통해 재참여 할 수 있다는 문제점을 여전히 가지고 있다. 또한 악의적인 노드들이 서로 공모하는 경우에 대응할 수 있는 방안을 제시하지 못하고 있다.

넷째, 기존의 기법들을 사용할 경우 네트워크상 모호한 통신 충돌이 정상적인 행위인지 아닌지를 식별할 수 없는 경우가 발생할 수 있다. 따라서 악의적 노드를 탐지할 때 이러한 통신오류가 발생하는 경우를 포함하여 탐지 해야할 필요가 있다. 따라서 기존 연구들의 문제점을 개선한 새로운 보안 알고리즘이 필요하다.

III. 본 론

악의적인 행위 패턴에는 데이터 패킷을 버리거나 이웃 노드에게 잘못된 정보를 제공하는 행위, 네트워크 와해를 목적으로 임의의 노드를 거짓 신고하는 행위 등이 있다. 이러한 위협은 키 관리 보안 알고리즘을 적용해도 내부적으로 이미 동일한 보안 정책을 적용받고 있는 노드들이기 때문에 쉽게 해결되지 않는다. 기존 연구에서 살펴보았듯이 MANET에서 다양한 유형의 악의적인 행위를 종합적으로 탐지할 수 있는 기법이 필요하다.

1. 제안기법 프레임워크

DTecBC 기법은 노드들이 데이터 전송 후 다음 노드의 전송여부를 overhear 메시지를 통해 감시한다. 노드의 이상 행위가 식별될 경우, 이웃노드와 협업을 통해 악의적인 노드를 탐지하여 배제시키고, 경로를 재설정하여 데이터 송·수신함으로써 데이터 신뢰성을 향상시킨다.

DTecBC 기법은 그림 3과 같이 4개의 모듈로 동작한다. 감시 모듈은 의심 가는 노드의 행위를 신고하며 협업 모듈을 통하여 악의적인 노드를 탐지한다. 신뢰관리 모듈은 임계치를 초과하는 노드는 악의적인 노드로 확정하고 신뢰지수를 감소시키며 관리테이블을 유지한다. 경로발견 모듈은 신뢰기반의 라우팅 경로를 재설정한다.

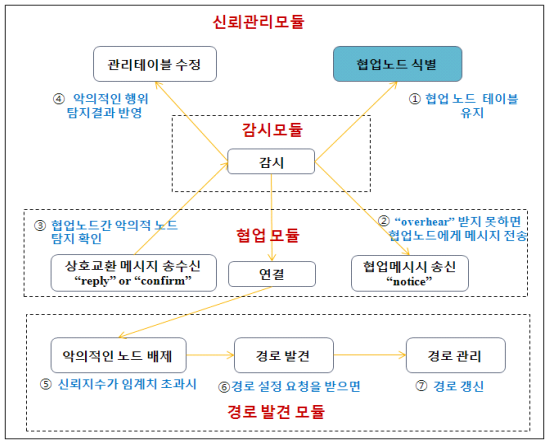


그림 3. DTecBC에서 제안하는 프레임워크

협업기반의 악의적인 노드 탐지를 위해 용어, 테이블 구조 및 메시지 형식을 다음과 같이 정의한다.

〔정의 1〕 MANET에 속한 전체 노드 N은 N={nid, nid+1, … nid+k} 으로 정의한다. 노드의 집합 N에서 정상노드는 정상적으로 라우팅 경로에 참여하는 노드로 NN (normal node)이라 한다. 악의적인 노드는 데이터 버림 및 변경, 정상노드를 거짓 신고, 거짓 반박 행위 등에 대해 탐지된 노드이며 MN (malicious node)이라 한다. 이웃노드 간 협업노드는 정상노드와 같이 라우팅경로에는 포함되지 않은 한 홉 떨어진 이웃한 노드이며 CN (collaborattion node)이라 한다.

〔정의 2〕 협업을 위한 테이블의 구조는 아래와 같다.

(1) 악의적 행위 관리 테이블

표 2는 악의적 행위 관리 테이블 (MBMT : malicious behavior manage table)은 각 노드의 악의적인 행위 횟수와 신뢰정보를 관리하는 테이블이다.

표 2. MBMT 관리테이블

seq#	node_id	malicious behavior pattern				count	trust level
		drop	false report	modified data	refutation		

(2) 협업노드 관리 테이블

표 3은 협업노드 관리 테이블 (CMT : collaboration node manage table)은 라우팅 경로 설정 시 이웃노드에 대한 정보를 사전에 등록하여 협업에 활용하기 위한 정보이다.

표 3. CMT 관리테이블

seq#	node_id	collaboration node_id

(3) 배제노드 관리 테이블

표 4는 배제노드 관리 테이블 (EMT : exclution node manage table)은 악의적인 노드 행위가 따라 경로 설정 시 지정된 임계치를 초과했을 경우 배제노드 테이블에 등록된다.

표 4. EMT 관리테이블

seq#	node_id	ex_check

〔정의3〕 협업을 위한 메시지는 아래와 같이 정의한다.

(1) nm (notice message)

nm은 악의적인 행위로 의심되는 노드를 확인하기 위하여 협업노드에게 보내는 메시지이다. 형식은 notice (notify

_node_id, suspect_node_id, next_node_id) 로 정의한다.

(2) rm (reply message)

협업노드는 악의적인 노드 행위를 확인하여 notice message 보낸 노드에게 reply message를 보낸다. 메시지 형식은 reply (node_id, receive_status)로 정의한다.

(3) cm (confirm message)

cm 메시지는 정상노드가 악의적인 노드로 거짓 신고 되었을 경우, 소스노드로부터 notice message 수신시 협업노드에게 전송할 때 사용하는 메시지이다. 메시지 형식은 confirm (node_id, reported_node_id, verify_check)으로 정의한다.

(4) frm (false report message)

frm 메시지는 정상노드를 거짓 신고할 때 사용된다. 메시지 형식은 false_report (node_id, report_node_id)로 정의한다.

(5) mnm (modify_notice message)

mnm 메시지는 최종적으로 데이터를 받은 목적지 노드가 협업관계에 있는 이웃노드에게 전송받은 데이터 변경여부를 확인하기 위해 사용한다. 메시지 형식은 modify_notice (node_id, source_node_id, data_info)로 정의한다.

(6) mrm (modify_reply message)

mnm을 받은 협업노드는 데이터 변경여부를 이웃노드와 협업하여 mrm을 보낸 노드에게 전송할 때 사용하는 메시지이다. 메시지 형식은 Modify_reply (node_id, data_info, modify_status)로 정의한다.

(7) rfm (refutation message)

rfm 메시지는 노드가 악의적인 노드로 신고 될 때 이를 반박하기 위해 사용된다. 메시지 형식은 refutation (reported_node_id, report_node_id)으로 정의한다.

2. 탐지 알고리즘

악의적인 행위가 발생하면 이웃노드와 협업을 통해 탐지한다. 탐지된 노드는 관리테이블의 임계치를 증가시키고 신뢰지수를 감소시킨다. 악의적인 행위 횟수가 임계치를 초과하면 악의적인 노드로 확정한다. 또한 악의적인 노드가 확정되면 라우팅 경로를 재설정하게 된다. 경로 재설정 시 각 노드의 신뢰지수가 신뢰지수에 대한 임계치보다 크지 않으면 경로 설정 시 배제시키고 임계치보다 크면 라우팅에 포함시킨다. 이에 대한 탐지 알고리즘 1과 같다.

알고리즘 1. 협업기반 탐지 알고리즘

```
Algorithm : Malicious Node Detection
Input : packet, overhear, malicious behavior pattern
Output : Malicious Node
Begin
 malicious behavior pattern = detect malicious behavior
 pattern from  data packet;
 case malicious behavior of
   drop data :          //데이터 버림의 경우
    broadcast notice message to Collaboration Node
      if did not receive overhear message from Target
Node then
         increment Target Node's MBMT.drop count
         decrement Target Node's MBMT.trust_level
    false report :       //거짓 신고의 경우
      if check_nomal_node(Target Node, Collaboration
Node) !=                          Normal Node then
         increment Target Node's MBMT.false report
count
         decrement Target Node's MBMT.trust_level
      end if
    modify data :        //데이터 변경의 경우
      if compare to buffered_data(data packet) != data
packet then
         increment Target Node's MBMT.modified count
         decrement Target Node's MBMT.trust_level
      end if
     refutation :        //거짓 반박의 경우
      if check refutation_node(Target Node, Collaboration
Node) !=                  Normal Node then
        increment Target Node's MBMT.refutation
count
        decrement Target Node's MBMT.trust_level
      end if
   end case
 if Target Node's MBMT.count 〉threshold then
                          //악의적 행위 횟수와 임계치 비교
    Target Node = Malicious Node  // 악의적 노드로 판단
    else Target Node = Normal Node  // 정상 노드로 판단
 end if
 if TN's MBMT.trust_level 〉Route Path's trust_level
then
             //경로 설정을 위한 신뢰지수 임계치 값과 비교
     exclude Target Node to Route Path
   else Include Target Node to Route Path
 end if
End
```

3. 악의적인 노드 탐지 절차

3.1 악의적인 노드가 데이터를 버리는 경우

노드 N2가 데이터를 버리고, 노드 N1은 overhear 메시지를 받지 못한 상태에서 노드 N1이 N2의 악의적 행위를 확인하는 절차는 그림 4와 같다.

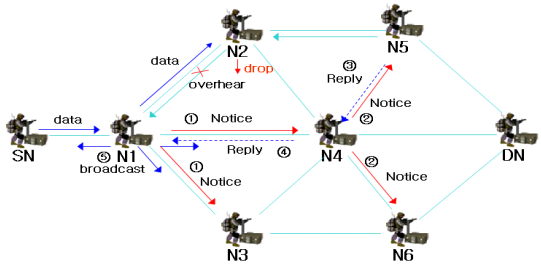


그림 4. 데이터를 버리는 악의적인 노드 확인

① 노드 N1은 협업관계의 이웃노드 N3, N4에게 notice message를 전송: notice (N1, N2, N5)

② 노드 N3는 노드 N5의 이웃노드가 아니므로 notice message를 무시, 노드 N4는 노드 N5의 협업노드 이므로 노드 N5에게 notice message 전송: notice (N4, N2, N5)

③ notice message를 받은 노드 N5는 노드 N2로부터 데이터를 받지 않았다는 정보를 노드 N4에게 reply message를 전송 : reply (N5, 1)

④ 노드 N4는 노드 N5로부터 받은 reply message를 노드 N1에게 포워딩

⑤ 노드 N1는 노드 N4로부터 받은 reply message 정보를 확인하여receive_status가 "1"이면 노드 N2를 악의적인 행위로 등록, 그리고 각 노드의 MBMT의 count를 증가시키고 trust_level은 감소시킴

3.2 정상노드를 악의적인 노드로 신고하는 경우

노드 N2는 노드 N5가 정상적으로 데이터를 전송하였으나 노드 N5를 거짓 신고할 경우 노드 N1이 협업을 통하여 탐지 절차는 그림 5와 같다.

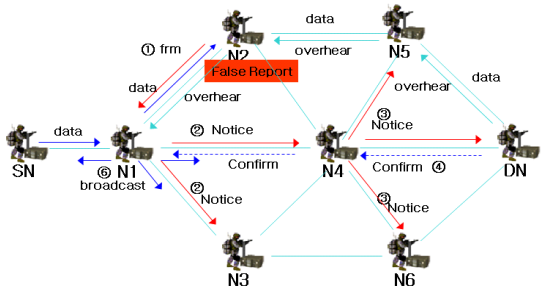


그림 5. 정상 노드를 거짓 신고하는 악의적인 노드 확인

① 노드 N2는 노드 N5 악의적인 노드라고 신고 : false_report (N2, N5)

② 노드 N1은 이웃노드 N3, N4에게 message를 전송 : notice (N1, N5, DN)

③ 노드 N3은 노드 N5의 이웃노드가 아니므로 notice message를 무시, 노드 N4는 협업관계에 있는 이웃노드 N5와 노드 DN에게 notice message 전송 : notice (N4, N5, DN)

④ 노드 N5는 notice message를 무시하고, 노드 DN은 노드 N5로부터 정상적으로 전송받았다는 정보를 노드 N4에게 confirm message를 전송 : confirm (DN, N5, 1)

⑤ 노드 N4는 노드 DN의 message를 노드 N1에게 전송 : confirm (N4, N5, 1)

⑥ 노드 N1는 노드 N4로부터 받은 message 정보를 확인하여 verify_check가 "1"이면 노드 N2를 악의적인 노드 행위로 등록한다.

3.3 원(original) 데이터를 변경해서 보내는 경우

노드 N2의 데이터 변경 후 탐지하는 절차는 그림 6과 같다.

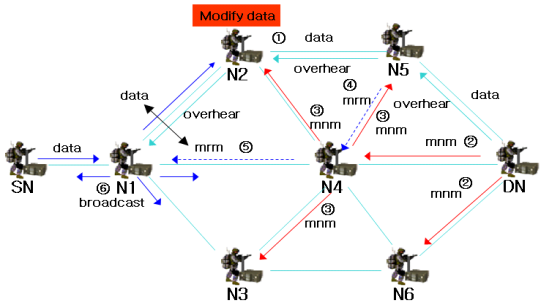


그림 6. 원(original)데이터를 변경하는 악의적인 노드 확인

① 노드 N1은 노드 N2에게 데이터를 전송하고 버퍼에 저장하고, 노드 N2는 데이터 변경 후 최종 목적지 노드 DN까지 전송

② 목적지 노드 DN은 데이터 변경여부를 확인하기 위하여 협업관계의 이웃 노드 N4, N6에게 확인 message를 전송 : modify_notice (DN, A, data_info)

③ 노드 N6은 경로 상 이웃노드가 아니므로 무시, 노드 N4는 협업노드이므로 노드 N5, N3, N2에게 message를 전송 : modify_notice (N4, N1, data_info)

④ 경로 상 이웃노드 아닌 노드는 무시, 노드 N2와 노드 N4는 전송받은 데이터 정보를 노드 N4 에게

message를 전송: Modify_reply (N2/N4, data_info)

⑤ 노드 N4는 노드 DN로부터의 데이터정보와 노드 N2, N4로부터 받은 데이터정보를 비교하여 노드 N2가 데이터를 변경하여 보낸 것을 확인하고 최초 데이터 전송노드인 N1에게 전송

⑥ 노드 N1는 노드 N2가 데이터를 변경한 악의적 행위로 등록하고 브로드캐스트, 그리고 각 노드의 MBMT의 count를 증가시키고 trust_level은 감소시킨다.

3.4 악의적인 노드가 거짓 반박하는 경우

노드 N1이 협업을 통해 N2의 거짓 반박을 확인하는 절차는 그림 7과 같다.

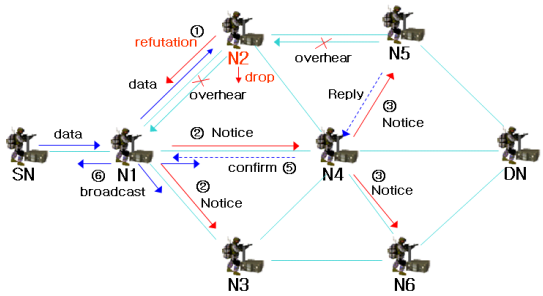


그림 7. 거짓 반박하는 악의적인 노드 확인

① 노드 N2는 악의적인 노드가 아니라고 반박 : reputation (N2, N1)

② 노드 N1는 협업관계의 이웃노드 N3, N4에게 notice message를 전송: notice (N1, N3, N5)

③ 노드 N3은 노드 N5의 이웃노드가 아니므로 notice message를 무시, 노드 N4는 노드 N5의 협업관계에 있는 이웃노드 이므로 노드 N5에게 notice message 전송 : notice (N4, N2, N5)

④ notice message를 받은 노드 N5는 노드 N2로부터 데이터를 받지 못했다는 정보를 노드 N4에게 reply message를 전송 : reply (N5, 1)

⑤ 노드 N4는 노드 N5로부터 받은 message를 확인하여 노드 N2의 행위에 대하여 확인 메시지 전송 : confirm (N4, N2, 1)

⑥ 노드 N1는 노드 N4로부터 받은 message 정보를 확인하여 verify_check 가 "1"이면 노드 N2가 거짓 반박이라고 결정, 그리고 각 노드의 MBMT의 count를 증가시키고 trust_level은 감소시키고, 노드 N2가 최초 설정된 신뢰지수 7을 초과했으므로, 배제테이블에 등록한다.

4. 신뢰기반 라우팅 경로를 통한 데이터 전송

각 노드의 신뢰지수를 기반으로 라우팅 경로를 설정하는 과정은 알고리즘 2와 같다. 우선 이전 노드는 주변 이웃노드들에게 RREQ 메시지를 송신하게 되며, 이때 이웃노드들의 신뢰지수를 확인하여 설정한 신뢰지수에 대한 임계치를 충족하는지 확인한다. 즉, 경로 설정 시 임계치로 설정한 신뢰지수(Mtv)와 이웃노드들의 신뢰지수(tv)를 비교하여 임계치 이상의 신뢰지수를 갖는 이웃노드들을 탐색한다. 이전 노드는 탐색된 이웃노드들 중 최대값을 갖는 노드를 선택하여 RREQ 패킷을 송신하게 되며, 목적지 노드까지 반복 수행하게 된다.

RREQ 패킷이 최종 목적지에 도착하면 목적지 노드는 소스 노드까지 역 경로를 이용하여 RREP 패킷을 유니캐스팅함으로써 최종적으로 라우팅 경로를 설정한다.

알고리즘 2. 경로 재설정 알고리즘

```
Algorithm : Route reestablish(RREQ, Mtv)
Input : RREQ, current node, Mtv  //최대 신뢰지수값
Output : RREP
Begin
 receive RREQ from Neighbor Node  //이웃노드 RREQ패킷 수신
 if current node.addr == RREQ.targetnode then unicast
    RREP to RREQ.seq
   //목적지 노드인경우  최근 수신 노드의 순서번호로 유니캐스팅
 else
   set Mtv to get MAX(Trust_value) from Neighbor Node
                        //이웃노드의 tV에 Max값을 구함
  for each current node on Neighbor Node
      if current node's trust_value == Mtv then
                              //노드의 신뢰지수 비교
       send RREQ to Neighbor Node
                          //RREQ패킷을 이웃노드에게 전송
     end if
   end for
 end if
End
```

IV. 성능평가 및 분석

OPNET 시뮬레이션 툴을 이용하여 기존 기법과 비교하면서 결과를 분석 검증하였다. 이 실험에서는 악의적인 노드 수의 증가, 임계치 증가, 악의적 행동을 할 확률 변화 등 다양한 환경을 설정하여 악의적인 노드 탐지수와 라우팅 측면의 신속성을 위한 전송 지연시간, 패킷 오버헤드 등을 고려하였다.

실험 환경은 정해진 1000m x 1000m 크기의 네트워크 필드에 100개의 이동 노드들이 데이터 송·수신이 가능한 속도로 랜덤하게 이동성을 부여한 후 0~900초 동안 시뮬레이션을 수행하였다. 표 5와 같이 설정하여 성능 평가 및 분석을 실시하였다.

표 5. 시뮬레이션 주요 환경 설정값

지역크기	1000*1000(m)
노드 수	1000ms
악의적 노드 수	5 ~ 30개
임계치	1 ~ 5회
악의적인 행동을 할 확률	20 ~ 100%
이동속도	- Pause Time : 0 ~ 900 sec - Speed : min 0, max 30m/s

1. 악의적인 노드 탐지율

1.1 악의적인 노드수 증가

그림 8은 데이터를 버릴 경우에 대하여 악의적인 노드 수를 5개, 15개, 30개로 증가시켜 가면서 악의적 노드 탐지율을 평가한 결과이다.

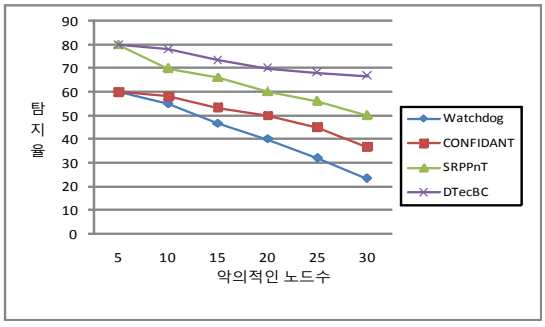


그림 8. 악의적인 노드 수 증가에 따른 탐지율

DTecBC는 기본적으로 임계치를 설정하여 이웃노드와 협업을 유지하면서 악의적 노드 행위에 대하여 상호 메시지 교환을 통하여 탐지 후 악의적 행위패턴을 관리테이블 등록하고, 공유함으로써 기존방법보다 탐지율이 좋아지는 것을 알 수 있다. 그러나 악의적인 노드 수가 많아질수록 탐지수는 증가하나 전체 탐지율은 서서히 낮아지는 것을 확인하였다.

1.2 임계치 증가

표 6은 데이터를 변경한 경우에 대하여 임계치를 1회, 3회, 5회로 증가시켜 가면서 악의적인 노드 탐지율을 평가한 결과이다.

표 6. 임계치 변화에 따른 악의적인 노드 탐지 수

임계치변화 (악의노드 15개)	*Watchdog*			*CONFIDANT*			*SRPPnT*			*DTecBC*		
	1회	*3회*	*5회*	*1회*	*3회*	*5회*	*1회*	*3회*	*5회*	*1회*	*3회*	*5회*
탐지수	11	11	12	11	12	11	12	13	12	13	13	13
탐지율(%)	40	53.3	46.7	46.7	60	53.3	53.3	66.7	60	53.3	73.3	66.7
오인탐지수	5	3	5	4	3	3	4	3	3	5	2	3

임계치에 따라 정상적인 노드가 악의적인 노드로 중복 및 오인 탐지되는 비율 즉 탐지율의 정확도에 영향을 미치는 것을 알 수 있다 임계치를 1회로 설정하였을 때 보다 임계치를 3회로 설정하였을 때 3개의 알고리즘 모두 탐지율이 증가하다가 임계치를 5회로 설정하였을 때는 다시 탐지가 감소하는 것을 볼 수 있다. 즉, 적정 임계치를 3회로 부여하는 것이 악의적인 노드 탐지 정확성을 향상되는 것을 확인 할 수 있다.

DTecBC는 이웃노드 간 협업을 통하여 탐지함으로써 기존 알고리즘보다 성능 20%이상 향상된 것을 확인하였다. 적정 임계치를 두는 것이 정상노드의 통신오류 등 비정상 행위가 발생할 수 있기 때문에 악의적인 노드를 정확히 파악하는 데는 긍정적인 영향을 미친다는 것을 확인하였다.

1.3 악의적인 행위 할 확률 증가

최근 노드가 지능화되어 필요에 따라 자신이 악의적인 노드라는 것을 숨기기 위해 자신에게 데이터 패킷이 올 때마다 매번 악의적인 행위를 하지 않는다. 따라서 정상적인 노드 입장에서 악의적인 노드를 탐지하기가 보다 어려워진다. 이와 같이 지능화된 악의적인 노드를 탐지할 수 있는 성능을 확인하기 위해 악의적인 행위를 수행할 확률을 변화시키면서 평가를 실시하였다.

표 7. 악의적 행위를 할 확률 변화에 따른 노드 탐지수

확률변화 (악의노드 15개)	*Watchdog*			*CONFIDANT*			*SRPPnT*			*DTecBC*		
	20%	*50%*	*100%*	*20%*	*50%*	*100%*	*20%*	*50%*	*100%*	*20%*	*50%*	*100%*
탐지수	9	10	11	10	10	11	12	13	13	13	13	13
탐지율(%)	26.7	33.3	46.7	33.3	46.7	53.3	46.7	46.7	66.7	53.3	60	73.3
오인탐지수	5	5	4	5	3	3	5	6	3	5	4	2

표 7과 같이 확률이 높아질수록 탐지율이 증가하고 확률이 낮아질수록 탐지율이 감하는 것을 확인할 수 있다. 하지만 DTecBC는 악의적 행동을 할 경우에는 이웃 간 협업을 통하여 적정 탐지율을 유지하면서 확률이 낮아질 경우에도 50% 수준의 탐지율을 나타내고 있다.

2. 데이터 전송 지연율

2.1 악의적인 노드수 증가

데이터 전송 지연 시간은 전송노드에서 목적지노드까지 데이터를 전송하는데 소요되는 시간을 나타낸다. 그림 9는 악의적인 노드 수 증가에 따른 데이터 전송지연 시간을 나타내는 것으로 악의적인 노드가 5개일 경우 DTecBC가 Watchdog, CONFIDANT, SRPPnT에 비해 각각 7%, 3%, 1% 전송지연이 감소하는 것을 확인하였다.

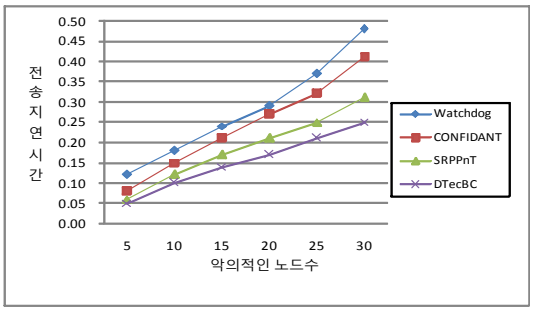


그림 9. 악의적인 노드 수 증가에 따른 전송지연시간

2.2 임계치 증가

그림 10는 임계치 증가에 따른 데이터 전송지연 시간을 나타내는 것으로 임계치 변화에 따라서도 전송지연이 차이가 나는 것을 확인하였다. 악의적인 노드가 5개이면서, 각 노드들의 임계치가 1회일 경우에는 DTecBC가 Watchdog, CONFIDANT, SRPPnT에 비해 각각 25%, 10%, 2% 전송지연이 감소되었다. 임계치가 3회일 경우에는 각각 18%, 5%, 2% 전송지연이 감소되는 것을 확인 할 수 있었으며 임계치가 5회일 경우에는 각각 19%, 7%, 3% 전송지연이 감소하는 것을 확인하였다.

또한 악의적인 노드수를 15개, 30개로 증가시키면서 임계치 변화에 따른 전송지연을 확인한 결과, DTecBC가 기존알고리즘보다 평균 2~25%이상 향상된 것을 확인 할 수 있다.

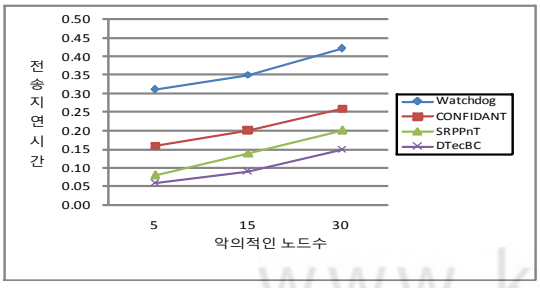


그림 10. 임계치 증가에 따른 전송 지연시간

데이터 전송 지연에 대한 측면은 네트워크에 존재하는 노드들 중 얼마나 신뢰할 수 있는 노드들로 경로를 구성하고, 실제 데이터를 주고받는데 참여하는 지가 큰 영향을 미치는 것을 확인 할 수 있다. 특정 임계치 이상의 신뢰할 수 있는 노드들로 이루어진 네트워크에서는 전송지연이 감소하고 악의적인 노드들의 분포도가 높아 악의적인 행위가 다수 발생하는 신뢰지수가 낮은 네트워크일수록 전송지연이 크게 발생하는 것을 알 수 있다. 따라서 단순 네트워크 측면에서의 전송지연을 감소시키려는 노력뿐만 아니라 보안 측면에서 어떻게 하면 신뢰할 수 있는 노드들을 식별하여 실제 경로 설정에 참여시키기 위한 노력도 반드시 고려되어야 할 부분이다.

DTecBC는 이웃 간의 협업을 통하여 악의적인 노드를 탐지해 내고, 신뢰지수에 의하여 경로를 재설정함으로써, 임계치의 변화에 영향을 받지 않고 지속적으로 악의적인 노드를 보다 정확하게 탐지함으로써 전송지연이 기존 알고리즘에 비해 감소하는 것을 알 수 있다.

3. 패킷 오버헤드

그림 11에 나타나듯이 라우팅 시 발생하는 패킷 오버헤드를 비교한 것을 보면 DTecBC가 평균 CONFIDANT에 비해 15%, Watchdog에 비해 30%, SRPPnT에 비해 7% 패킷 오버헤드가 큰 것을 확인하였다.

DTecBC는 악의적인 노드 활동성이 감소하기 때문에 경로 재설정과정에서 발생되는 제어패킷의 오버헤드는 감소한다. 즉 일반적으로 MANET에서 사용하는 경로 설정을 위한 제어패킷만을 고려하면 DTecBC가 기존의 Watchdog와 CONFIDANT보다 패킷 오버헤드는 오히려 감소한다. 하지만 SRPPnT와 DTecBC의 경우 보다 정확한 악의적인 노드를 탐지하기 위해 부가적인 관리 메시지를 주고받기 때문에 오버헤드가 증가하게 된다. 특히, DTecBC의 경우 이웃노드와 협업관계를 유지하고 관리하기 위한 관리테이블, 배제테이블, 상호교환 메시지 패킷 오버헤드가 증가하는 것을 확인 하였다.

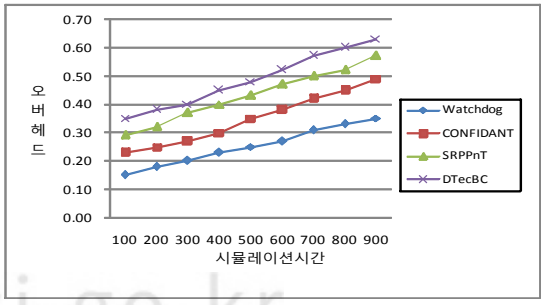


그림 11. 패킷 오버헤드

제안하는 방식이 제어패킷을 추가적으로 사용할하기 때문에 기존 알고리즘에 비해 오버헤드가 증가할 수밖에 없다. 하지만 패킷 오버헤드 증가와 악의적인 노드의 정확한 탐지에 의한 데이터 전송 신뢰성 보장 측면에서의 trade-off 적인 부분을 고려해 볼 때 특히, 군 환경에서는 비록 통신 오버헤드가 다소 증가하더라도 보안 측면을 강조하여 데이터 송수신의 신뢰성을 보장하는 것이 더 중요할 것으로 판단된다. 뿐만 아니라 추가적인 제어 패킷 사용을 통해 보다 최적의 경로를 설정함으로써, 빈번하게 경로를 재설정함으로써 브로드캐스트 되는 일반적인 패킷 오버헤드를 감소시킬 수 있다는 사실 또한 간과해서는 안 될 것이다.

V. 결 론

현재까지 연구된 탐지 기법들은 다양한 유형의 악의적인 행위들을 종합적으로 대처하는데 제한이 있었다. 따라서 다양한 유형의 악의적인 행위와 악의적인 노드들 간의 공모에 보다 효율적으로 대처함으로써 보안 측면에서의 신뢰성 향상을 위하여 협업 기반의 탐지 기법인 DTecBC를 제안하였다.

DTecBC 기법은 악의적인 노드를 확인하는 과정에서 이웃 노드와 협업관계를 맺고 상호 신뢰 하에 악의적인 행위를 하는 노드를 탐지한다. 이를 위해, 각 노드들은 악의적인 노드에 대한 관리 테이블을 유지하도록 설계하였다. 성능 평가를 위해 제안 기법을 기존의 악의적 노드 탐지 기법인 Watchdog, CONFIDANT, SRPPnT기법과 비교하여 평가하였다. 그 결과, 제안 기법이 기존 기법보다 악의적인 노드에 대한 높은 탐지율과 낮은 데이터 전송 지연율을 보이는 등 MANET에서 발생 할 수 있는 악의적인 행위 유형에 효율적으로 탐지함을 확인하였다. 그러나 이웃노드 간 협업을 위해 상호 메시지 교환과 관리테이블 추가함으로 인해 네트워크상 패킷 오버헤드가 기존 기법보다 다소 높게 발생하였다. 향후 패킷 오버헤드를 감소시키기 위한 연구가 진행 되어야 한다.

참고문헌

〔1〕 D.Elma, G., Nils, A., Pete, M. and Jens, T., "Detecting black hole attacks in tactical MANET using topology graphs", In Proceedings of the 32nd IEEE conference on local compute networks, pp.1043-1052, 2007.

〔2〕 Hong, D., "Routing Security in ad hoc Networks", IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol.40, No.10, pp.70-75, 2

〔3〕 Jinsub, K., Dan, S., Rommie, H., Roshan, K. and Lang, T., "Timing-based localization of in-band wormhole tunnels in MANETs", In Proceedings of the 3rd ACM conference on Wireless network security, pp.1-12, 2010.

〔4〕 Yang, H., Luo, H., Ye, F. and Zhang, L., "Security in Mobile ad hoc Networks : Challenges and Solutions", IEEE Wireless Communications, Vol.11, Issue.1, pp.38-47, 2004.

〔5〕 Zapata, M. G. and Asokan, N., "Securing ad hoc routing protocols", In Proceedings of the 1st ACM workshop on Wireless security. pp.1-10, 2002.

〔6〕 Abdul, H. A. and Zuriati, A. Z.,"Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile ad hoc Networks", European Journal of Scientific Research, Vol.31, No.4, pp.566-576, 2009.

〔7〕 Usop, N. S., Abdullah, A. and Abidin, A. F., "Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment", IJCSNS International Journal of Computer Science and Network Security, Vol.9, No.7, pp.261-268, 2009.

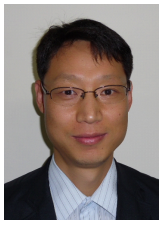
〔8〕 Hwang Y. C., Kim J. I. and Kim, J. S, "Malicious Node Detection Mechanism of Consideration Compromised Node in MANET", KIIT, Vol.7, No.5, pp.113-124, 2009.

〔9〕 Park, S. S., Park, G. W., Ryu, K. H, and Lee, S. H, "A Secure Routing Protocol in MANET based on Malicious behavior Pattern of Node and Trust Level", KSCI, Vol.14, No.5, pp.103-117, 2009.

저 자 소 개

신 언 석

- 1983: 육군사관학교 전자계산학과 이학사
- 1990: 미해군대학원 공학석사
- 1997: 충북대학교 대학원 박사수료
- 현재 : 육군본부 전산체계처장
- 관심분야 : SNS, 지식기반서비스
- Email : shines39@hanmail.net



전 서 인 (Seo In Jeon)

- 1993: 서원대학교 수학교육과 이학사
- 2002: 경북대학교 대학원 공학석사
- 2012: 충북대학교 대학원 공학박사
- 현재: 육군본부 전산장교
- 관심분야 : 센서네트워크, DB보안
- Email : jsi0198@naver.com

박 건 우 (Gun Woo Park)

- 1997: 충남대학교 컴퓨터과학과 학사
- 2007: 연세대학교 대학원 공학석사
- 2011: 국방대학교 대학원 공학박사
- 현재: 육군본부 전산장교
- 관심분야 : 소셜네트워크
- Email : pgw4050@hanmail.net

류 근 호 (Keun Ho Ryu)

- 1976: 숭실대학교 전산학과 이학사
- 1980: 연세대학교 공학대학원 전산전공 공학석사
- 1988: 연세대학교 대학원 전산전공 공학박사
- 현재: 충북대학교 전자정보대학 교수
- 관심분야 : 시공간데이터베이스, DB보안, 데이터마이닝, Bioinformatics
- Email : khryu@dblab.chungbuk.ac.kr