한국군사과학기술학회지 제14권 제6호, pp. 1097~1106, 2011년 12월

학술논문 정보기술 부문

전술정보통신체계(TICN)에 적합한 침입탐지 기법

An Intrusion Detection Technique Suitable for TICN

이 윤 호* 이 수 진*
Yunho Lee Soojin Lee

Abstract

Tactical Information Communication Network(TICN), a concept-type integrated Military Communication system that enables precise command control and decision making, 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 works properly only if the participating nodes cooperate in routing and packet forwarding. However, if selfish nodes not forwarding packets of other nodes and malicious nodes making the false accusation are in the network, it is faced to many threats. Therefore, detection and management of these misbehaving nodes is necessary to make confident in Ad-hoc networks. To solve this problem, we propose an efficient intrusion detection technique to detect and manage those two types of attacks. The simulation-based performance analysis shows that our approach is highly effective and can reliably detect a multitude of misbehaving node.

Keywords : TICN(전술정보통신체계), Intrusion Detection(침입탐지), Ad-hoc Network, Misbehaving Node(비정상 행위 노드), False Accusation(거짓 지목)

1. 서 론

Ad-hoc 네트워크는 기반체계 없이 신속한 네트워크 구성 및 이동이 용이하여 군의 전술상황, 긴급 재난상황 등 다양한 분야에 적용이 가능하다. 특히, 우리 군은 1998년부터 운용중인 SPIDER 체계를 대체하기 위해 고속 및 대용량 정보전송이 가능한 차기 전술정보통신체계인 TICN을 개발하여 2013년 전력화를 목표로 추진하고 있다. TICN의 부 체계(Sub-system)중 여단급 이하의 전술통신망을 지원하는 전투무선체계는 신속한 부대 전개 및 기동을 위해 Ad-hoc 네트워크 기술 적용을 고려하고 있다. 그러나 Ad-hoc 네트워크는 기존의 유선 네트워크들과는 차별화되는 특성들 때문에 보안에 취약하다. 그리고 Ad-hoc 네트워크에 적용된 대부분의 프로토콜들이 각 노드들의 협동을 전제로 하고 있어 일부 노드들의 단순한 악의적 행위에 의해서도 네트워크 전체의 효율성이 심각하게 저하된다. 이는 [1]에서 제시된 시뮬레이션 기반의 연구 결과에서도 잘 확인할 수 있다.

Ad-hoc 네트워크의 보안문제를 해결하기 위한 연구

† 2011년 5월 17일 접수~2011년 11월 25일 게재승인
* 국방대학교(Korea National Defense University)
책임저자 : 이윤호(yunholee@gmail.com)

는 크게 예방(prevention) 차원의 접근방법과 침입탐지 및 대응 차원의 접근방법으로 구분할 수 있다. 예방 차원의 대책은 주로 단방향 해쉬 체인 기법, 암호화 기법 등을 적용한 보안 라우팅 프로토콜에 대한 연구[2~6]가 주를 이루고 있다. 즉, 노드의 신뢰성을 증명할 수 있는 비밀키를 알고 있는 노드들만 네트워크 서비스에 참여할 수 있도록 하는 접근방법이다. 그러나 이러한 예방 차원의 보안대책들은 이미 정당한 권한을 가지고 네트워크에 참여하여 비정상적인 행위를 하는 노드에 대해 효율적으로 대응할 수 없어 최근에는 제2의 방어선 개념인 침입탐지 및 대응에 대한 연구가 활발히 진행되고 있다.

Ad-hoc 네트워크에서 네트워크 성능 저하를 야기하는 비정상 행위 노드(Misbehaving Node)는 크게 이기적인 노드(Selfish Node)와 악의적인 노드(Malicious Node)로 구분할 수 있다[7]. 이기적인 노드는 자신의 자원 절약을 목적으로 행동하며 대표적인 공격 유형은 자신의 패킷은 전송하면서 다른 노드의 패킷은 전송하지 않는 패킷 드롭 공격이 해당된다. 반면 악의적인 노드는 네트워크 단절 및 인접노드 자원 고갈을 목표로 행동하며 정상 노드를 비정상 노드로 허위 지목하여 고립시키는 거짓지목 공격 등이 해당된다.

비정상 행위 노드 탐지를 위해 연구된 기존의 연구들은 대부분 이기적 노드 탐지에 중점을 두고 추진되었다. 즉, 네트워크에 참여하는 각 노드들은 주변 노드들의 행위를 계속적으로 감시하고, 특정 노드가 패킷을 전송하지 않는 비정상 행위를 탐지하면 해당 노드에 대한 평판(Reputation) 정보를 생성하여 인접 노드들에게 전파하여 우회 경로 설정 또는 네트워크에서 배제시키는 등의 대응방법에 관한 연구가 대부분이다.

하지만, Ad-hoc 네트워크에서 평판을 이용해 비정상행위 노드를 탐지하여 배제시키는 접근방법은 악의적인 거짓지목(False Accusation) 공격에 취약하다. 즉, 특정 노드에 대한 평판을 종합하기 위해 인접한 노드들이 해당 노드에 대한 평판 점수를 주고받는 과정에서 정상 노드를 비정상 노드로 지목할 수도 있으며, 이 경우 정상적인 노드들이 라우팅 과정에서 배제되어 네트워크의 전체적인 효율성이 저하될 수 있으며 극단적인 경우는 네트워크 단절을 초래할 수 있다.

이에 본 논문에서는 패킷 전송을 하지 않는 이기적인 노드뿐 아니라 정상 노드를 비정상 노드로 거짓 지목하는 악의적 노드를 효율적으로 탐지 및 관리를 할 수 있는 개선된 침입탐지 기법을 제안한다. 적용 네트워크 모델은 최근 미국을 비롯한 많은 국가에서 활발히 연구중이며, 우리 군도 2012년 전력화 예정인 TICN의 부체계인 전투무선체계에서 고려하고 있는 전술 애드혹 네트워크(Tactical Ad-hoc Network)[8,9]를 대상으로 한다. 일반적인 Ad-hoc 네트워크와는 달리 계층구조를 형성하는 전술 Ad-hoc 네트워크에서는 비교적 안전성과 신뢰성이 보장되고 처리능력이 뛰어난 상위 계층 노드와 하위계층 노드로 구성된다.

제안하는 기법에는 일시적인 네트워크 장애로 인해 부당한 가중치를 부여받은 노드에 대해서는 구제 알고리즘과 공모 노드 문제를 해결하기 위한 알고리즘 그리고 최적의 경로를 설정하는 방법을 추가적으로 제시하고 있다. 제안하는 기법의 효율성을 검증하기 위해 네트워크 시뮬레이터인 NS-2를 이용하여 모의실험을 실시하여 기존 기법들과 성능 비교를 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 Ad-hoc 네트워크에서 비정상 행위를 탐지 및 관리하기 위한 침입탐지 기법들을 살펴보고 문제점을 분석한다. 3장에서는 본 논문에서 제안하는 비정상 행위 노드 탐지 및 관리기법에 대해 기술한다. 4장에서는 NS-2를 이용한 모의실험 결과를 분석하고, 5장에서 결론을 맺는다.

2. 관련연구

Ad-hoc 네트워크에서 비정상 행위 노드 탐지 및 관리를 위해 연구된 논문들을 살펴보면 다음과 같다.

우선 Zhang 등은 [10]에서 Ad-hoc 네트워크에서의 침입탐지 구조 및 원리에 대해 최초로 연구하였고, 그 내용은 모든 노드들이 침입탐지를 위해 분산과 협동을 전제로 하는 구조를 취해야 한다는 개념으로 이후 연구에서도 계속적으로 적용되고 있다.

본격적인 침입탐지 기법의 연구는 Marti 등이 [11]에서 제안한 'Watchdog' 기법이다. 네트워크의 모든 노드들이 주변 노드들을 감시하여 패킷 전달을 거부하는 이기적인 노드를 탐지할 수 있는 Watchdog 모듈을 내장하고 있다. 또 다른 모듈인 Pathrater는 Watchdog의 탐지 결과를 바탕으로 악의적인 노드를 피해 최선의

경로를 찾을 수 있도록 도와준다.

CONFIDANT(Cooperative Of Nodes, Fairness In Dynamic Ad-hoc NeTworks)[12,13]은 Watchdog의 개선된 기법으로서, 비정상적인 노드 탐지 및 우회뿐 아니라 라우팅 경로설정 단계에서 고립시켜 네트워크로부터 배제하는 방법을 포함한다. CONFIDANT는 모니터, 신뢰관리자, 평가시스템, 경로관리자 등의 모듈로 구성된다. 모니터는 인접 노드에 대한 비정상 행위를 탐지하는 역할을 수행하며, 신뢰관리자는 비정상적인 행위를 탐지했을 때 발생되는 경보 메시지에 대한 송수신을 담당한다. 평가시스템은 노드에 대한 등급을 관리하고 임계치를 초과한 악의적인 노드를 식별하여 우호관계에 있는 인접 노드들에게 전파하는 역할을 담당한다. 경로관리자는 구축된 보안 매트릭에 따라 경로 우선순위를 재설정하고 비정상 노드들이 포함된 경로들을 삭제한다.

Chin-Yang 등은 [14]에서 OLSR Ad-hoc 라우팅 프로토콜을 위한 명세기반 침입탐지 기법을 제안하였다. 이 기법에서는 경로를 설정하는 과정에서 제어 메시지가 반드시 만족해야할 조건을 정의하고 이를 기반으로 각 조건을 만족하지 못했을 때 이를 이상 행위로 탐지하는 명세 모델을 제시하고 있다.

Mitrokotsa 등은 [15]에서 선택적인 패킷 드롭(Selective Packet Drop)과 같은 새로운 유형의 공격을 탐지할 수 있는 비정상 탐지(Anomaly Detection) 기법을 제안하였다. 이 방법은 신경망과 자가 학습 방법을 활용하여 MAC 계층에 대한 정상 행위 패턴 정보를 구축하여 비정상 행위에 대한 탐지에 활용한다.

Oscar 등은 [16]에서 블랙홀(Black Hole)과 같은 모든 패킷을 전송하지 않는 공격과 선택적으로 전송하는 그레이홀(Gray Hole) 공격을 탐지하기 위해 각 노드들은 이웃노드가 평소에 전송 및 수신하는 패킷의 통계적인 수치를 학습을 통해 구축하고 설정된 임계치 이하로 패킷을 전송하면 비정상 행위 노드로 탐지하는 방법을 제안하고 있다.

Jaydip Sen 등은 [17]에서 노드들 상호간의 경로설정 단계에서 주고받는 RREQ(Route REQuest) 메시지의 정상적인 포워딩을 감시하는 유한상태머신(Finite State Machine)을 작성하여 RREQ 메시지를 전송하지 않는 이기적인 노드를 탐지할 수 있는 방법을 제안하였다.

3. 제안하는 침입탐지기법

가. 가정 사항

본 논문에서 제안하는 기법의 적용을 위해 각 노드의 동작 환경은 다음과 같이 가정한다. 첫째, TICN의 전투무선체계 하부 네트워크는 계층화 할 수 있으며 상위 계층 노드는 충분한 에너지와 안정성을 확보하고 있다. 둘째, 네트워크 내의 모든 노드들은 'promiscuous mode'로 동작하여 전송범위 내에 있는 인접 노드들의 전송을 엿듣기(Overhear)할 수 있다. 셋째, 각 노드들은 고유한 개인키를 가지고 있고, 상위 계층 노드는 지역 내 모든 노드들의 개인키를 가지고 있다.

나. 공격모델 정의

앞서 살펴본 바와 같이 우리 군에서 2012년에 도입될 TICN체계 중 소부대급에서 운용될 전투무선체계는 Ad-hoc 네트워크 프로토콜이 적용될 예정이며, 특히 이 구간에서의 발생될 수 있는 보안 취약 및 네트워크의 성능 저하를 유도할 수 있는 공격은 다양하다. 본 논문에서는 이러한 보안 취약 공격 유형 중 이기적 노드에 의한 패킷 드롭 공격과 악의적 노드에 의한 거짓 지목 공격에 대해 다루도록 한다. 먼저, Fig. 1은 이기적인 노드의 공격을 도식화 한 것으로 인접 노드의 패킷을 전송 하지 않는 형태이다. Fig. 2는 악의적인 노드에 의한 거짓 지목 공격 유형을 도식화 한 것으로 정상 노드를 마치 비정상 노드인 것으로 거짓된 알람 정보를 송신지 노드에게 전송하는 형태이다.

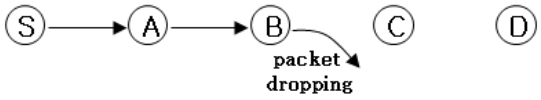

Fig. 1. 패킷 드롭 공격

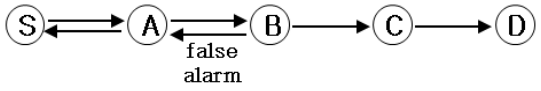

Fig. 2. 거짓 지목 공격

다. 용어 정리

우선 전술 Ad-hoc 네트워크에서는 하위 계층 노드와 상위 계층 노드로 구분한다. 하위 계층 노드는 TICN 체계에서 소부대 전투무선망을 구성하는 노드이다. 상

위 계층 노드는 하위 계층 노드로부터 수신한 정보를 바탕으로 지역 내 노드에 대한 신뢰성 값을 관리하는 가중치 관리 노드(WMN : Weight Management Node)로 설정하여 운영된다.

제안하는 침입탐지기법에서 사용되는 통신 메시지 및 각 노드에서 추가적으로 관리하는 테이블은 다음과 같다. 우선, 경로 탐색 단계에서 사용되는 메시지는 AODV의 RREQ(Route REQuest), RREP(Route REPly) 패킷에 경로 확인을 위한 필드를 추가한다[18]. *Route* 필드는 RREQ와 RREP 패킷이 경유하는 노드 주소를 순서대로 연결한 값이며, *Route_verifi_val*은 RREQ와 RREP 패킷의 경유 경로의 정확성을 확인하기 위한 것으로 각 노드의 개인키를 누적하여 지수승($g^{k_a k_b k_c} \bmod p$: k_a, k_b, k_c는 각 노드의 개인키, g와 p는 공개값)한 값이다.

- RREQ(Src_addr, Brd_id, Dest_addr, Dest_seq_#, hop_cnt, *Route, Route_verifi_val*)
- RREP(Src_addr, Dest_addr, Dest_seq_#, hop_cnt, life_time, *Route, Route_verifi_val*)

각 노드는 경로상의 인접 노드가 데이터를 정상적으로 전송하는지를 엿듣기하여 비정상 노드를 식별하면 Alarm 메시지를 이용하여 송신지 노드에게 보고하며 메시지 형식은 다음과 같다. Notify_node_addr는 보고 노드, suspect_node_addr는 비정상 행위 의심 노드를 의미한다.

- Alarm(Notify_node_addr, suspect_node_addr)

목적지 노드가 비정상 노드 탐지 알고리즘에 의해 비정상 노드를 탐지하면 해당 노드를 송신지 노드와 상위계층노드에게 통보를 한다. 이때 사용되는 Node WARNing(NWARN) 메시지의 형식은 다음과 같다.

- NWARN(Notify_node_addr, Malicious_node_addr, *Route, Route_verifi_val*)

경로상의 노드가 NWARN 메시지를 수신하면 메시지 상의 비정상 행위 의심 노드를 자신의 Suspect Node List(SNL)에 등록하여 관리하며 형식은 아래 Table 1과 같다. 여기서 count 값은 초기 1, 최대 10으로 한다. 또한 각 노드가 상위 계층 노드인 WMN으로부터 고립대상 노드를 수신하면 자신의 Isolation Node List(INL) 테이블에 등록하며 형식은 아래 Table 1, 2와 같다.

Table 1. SNL 테이블

sequence number	node ID	count

Table 2. INL 테이블

sequence number	node ID

상위계층노드인 WMN는 송신지 노드와 목적지 노드로부터 각각 비정상 행위 노드에 관한 정보를 수신하면 확인 절차 후 해당 노드를 자신의 Misbehaving Node List(MNL) 테이블에 등록하여 가중치(Weight)를 관리하며 형식은 아래 Table 3와 같고 가중치는 초기 1, 최대 5로 한다.

Table 3. MNL 테이블

sequence number	node ID	weight

라. 탐지 알고리즘

Fig. 3처럼 송신지 노드 S가 목적지 노드 D에게 경로 S-A-B-C-D를 통해 패킷을 전송하는 상황에서 2가지 공격 유형을 고려할 수 있다. 첫째, 노드 C가 패킷을 포워딩하지 않는 이기적인 노드인 경우이다. 둘째, 악의적인 노드 B가 정상 노드 C를 거짓 지목하는 경우이다. 두 경우 모두 노드 B는 송신지 노드에게 Alarm(B,C) 메시지를 보낸다. 송신지 노드는 차선의 경로(S-I-J-K-D)를 통해 데이터 패킷과 Alarm(B,C) 메시지를 재전송한다.

목적지 노드에서의 탐지 알고리즘은 Fig. 4와 같다. 즉 목적지 노드 D는 송신지 노드로부터 데이터 패킷과 함께 Alarm(B,C) 메시지를 수신하면 송신지 노드로부터 데이터 패킷을 중복 수신 여부를 확인하여 Alarm 메시지를 생성한 노드 B의 보고가 정당한지를 확인한다. 이는 데이터 패킷은 유니캐스트(Unicast)로 전송됨

으로 중복하여 수신할 수 없다는 사실을 이용한 것이다. 만약 송신지 노드 S로부터 중복된 데이터 패킷을 수신한 적이 없다면 해당 Alarm은 정당한 보고이고, 반면 중복된 데이터 패킷을 이미 수신하였다면 해당 Alarm을 발생한 노드 B는 거짓 지목 노드로 판단할 수 있다.

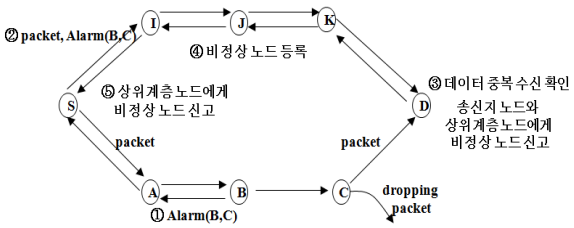

Fig. 3. 비정상 행위 노드 탐지 절차

```
## 목적지 노드가 Alarm 메시지를 수신하면
## 비정상행위 의심 노드로부터 데이터 패킷을
## 중복 수신했는지 여부 점검
Detect_Misbehavior( )
 if receive Alarm(Ni, Nj) message then
    val = check_redundant_packet_receiving(Nj)
    ## 의심노드 Nj로부터 데이터 패킷 중복수신확인
      if val == True then ## 중복수신하였다면
          Ni is false accusation node
          ## 신고한 노드가 거짓지목 행위 노드
       else        ## 중복 수신하지 않았다면
          Nj is selfish node
          ## 의심노드가 이기적인 노드
       endif
 endif
```

Fig. 4. 비정상 행위 노드 탐지 알고리즘

마. 중간노드 동작절차

목적지 노드가 비정상 행위 노드를 탐지하면 NWARN 메시지를 송신지 노드에게 전송한다. 경로상의 중간 노드의 동작 절차는 Fig. 5와 같다. 먼저 중간노드는 수신한 NWARN 메시지에 포함된 비정상 행위 노드가 자신의 SNL에 이미 존재하는지 여부를 검사하여 존재하지 않으면 신규 등록하여 count 값 1을 부여하고, 존재할 경우 1 증가시킨다 (최대값 10).

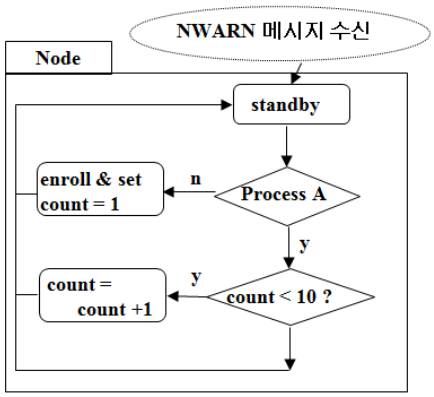

Fig. 5. 중간노드 동작절차

바. 상위계층 노드 동작절차

송신지 노드와 목적지 노드로부터 혐의 노드에 대한 정보를 수신한 상위계층노드의 동작 절차는 Fig. 6과 같다. 상위계층 노드는 일정 시간 범위 내에 도착한 두 신고를 비교하여, 혐의 노드가 동일한지 여부를 판단한다. 동일한 정보인 경우 혐의 노드가 자신의 MNL에 이미 등록된 노드인지를 확인하고 가중치 값을 1씩 증가시킨다. 만약 가중치가 임계치를 초과할 경우 지역내 노드에게 브로드캐스트하고, 이 메시지를 받은 노드들은 자신의 SNL에서 해당 노드를 삭제하고, INL에 해당 노드를 등록하여 라우팅 과정에서 배제시킨다. 그리고 상위계층노드는 정해진 시간 간격으로 인접 노드와 고립대상노드에 대한 정보를 교환한다.

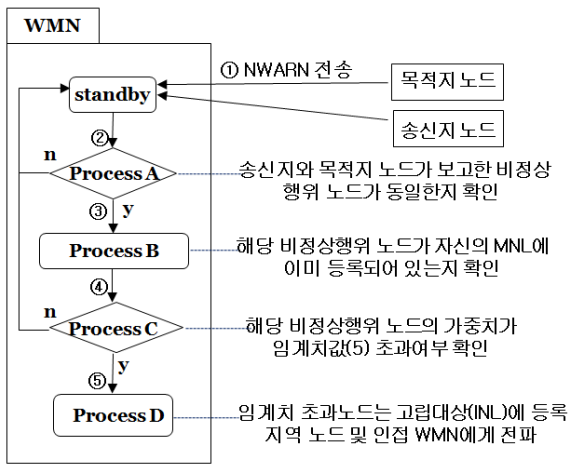

Fig. 6. 상위계층 노드 동작절차

사. 공모 노드 탐지

제안하는 라우팅 프로토콜에서는 송신지 노드와 목적지 노드가 상위계층 노드인 WMN에 거짓지목 행위 노드를 보고한다. 하지만 네트워크 내에 2개의 악의적 노드가 공모하여 특정 노드를 허위로 보고할 수 있다. 본 논문에서는 이와 같은 공모노드 문제를 해결하기 위해 이산대수 문제의 어려움에 근거를 두고 있는 ElGamal 암호 방식을 응용한 해결방법을 사용한다. 즉 식 $y_a = g^{k_a} \bmod p$에서 g, p는 공개된 값이고 k_a가 주어지면 y_a는 쉽게 확인이 가능하지만 그 반대는 매우 어렵다는 사실을 이용한다.

경로 탐색 단계에서 RREQ 메시지를 수신한 각 노드들은 Route 필드에 자신의 주소 정보를 추가하고 Route_verifi_val 필드에 자신의 개인키를 지수승하여 전송한다. 즉 Fig. 2의 A 노드가 송신지 노드 S로부터 RREQ 메시지를 수신하면 Route 필드는 S-A가 되고, Route_verifi_val 필드에는 $g^{k_s k_a} \bmod p$가 된다. 이와 같은 방식을 통해 RREQ와 RREP 메시지를 송신지 노드와 목적지 노드가 수신하면 해당 경로의 주소 체인과 경로 확인 값을 획득할 수 있게 된다. 만약 송신지 노드와 목적지 노드가 악의적인 노드를 식별하면 이 값을 NWARN 메시지와 함께 WMN에게 통보하게 된다. WMN는 전체 노드에 대한 개인키를 보유하고 있어 경로 확인 값을 주소 체인과 비교하여 두 노드의 공모에 의한 허위 보고 행위를 식별할 수 있게 된다.

아. 최적 경로 설정

본 논문에서는 패킷 전송 실패 또는 경로상의 비정상 노드에 의한 통신 장애 시 신뢰도가 높은 재전송 경로 설정을 위해 각 노드가 유지하고 있는 SNL 테이블의 노드 신뢰도 정보를 활용한다. 전통적인 AODV 라우팅 프로토콜에서는 목적지 노드가 송신지 노드로부터 다수 경로를 통해 RREQ 메시지를 수신할 때, 일정 시간 내에 도착한 RREQ 메시지 중 홉 수가 작은 경로의 이웃 노드에게 RREP 메시지를 전송하여 경로를 설정하였다. 하지만 제안하는 기법의 프로토콜은 최적의 라우팅 경로 선정을 위해 기존의 AODV 프로토콜[18]을 개선하여, 목적지 노드가 RREQ 메시지를 수신하면 홉 수와 함께 메시지에 포함된 경로상의 중간 노드가 자신의 SNL 테이블에 포함되어 있는지 여부를 확인하여 해당 노드의 count 값을 함께 고려한다. 최적 경로 선택 시 사용하는 식은 아래와 같고 이 식을 통해 구해진 경로신뢰도(PT : Path Trust) 값이 가장 작은 경로를 선정한다. 이 식에서 $\sum N_{count} * 0.05$의 의미는 경로상의 노드중 자신의 SNL 테이블에 포함되어 count 값이 최대치에 해당되는 노드가 2개가 넘으면 홉 수가 '1' 증가하는 효과를 나타낸다.

$$PT = hop\_count + \sum N_{count} * 0.05$$

자. 구제 알고리즘

일시적인 통신상의 오류 등으로 인해 정상적인 노드가 부당한 가중치를 부여받은 경우 이에 대한 구제 방법이 필요하다. 본 논문에서는 정상적인 패킷 전송에 참여하는 노드에 대해 부당한 가중치 값을 줄여주는 구제 방식을 가지고 있다. Fig. 7은 노드가 자신의 SNL에 등록된 인접 노드의 정상 동작을 탐지할 경우 이를 구제하는 동작절차를 도식하고 있다. 즉, 자신의 SNL에 포함된 노드가 정상적인 패킷 전송을 할 경우 count 값을 1씩 줄이고 그 노드에 대해 WMN에게 보고한다. WMN는 해당 노드 weight 값을 확인하여 0이 아닐 경우 0.1 감소시키고, weight 값이 0이 되면 모든 노드들에게 브로드케스트하여 해당 노드를 SNL에서 삭제되도록 한다.

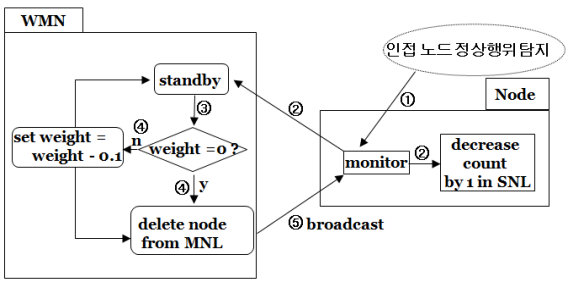

Fig. 7. 정상노드 구제 동작 절차

4. 모의실험 결과

가. 실험환경 및 시나리오

모의실험은 NS-2를 사용하였으며 Ad-hoc 네트워크에 적용될 라우팅 프로토콜은 AODV 알고리즘을 따르도록 설계하였다. 주요 실험내용은 비정상 행위 노드가 Ad-hoc 네트워크에 미치는 악영향에 대해 실험을 통해 분석하였다. 그리고 비정상 행위 노드 수 변화에 따라

본 연구에서 제안하는 탐지 기법과 대표적인 Ad-hoc 네트워크 침입탐지기법인 Watchdog, CONFIDANT와 네트워크 패킷 처리율을 비교하여 성능 분석을 실시하였다. 라우팅 오버헤드 분석은 수학적 분석 및 실험을 병행하였다. 모의실험을 위한 설정 값은 Table 4와 같다.

Table 4. 설정값

설정 환경	설정값
모의실험 시간	1000 sec
지역 크기	1000 m × 1000 m
신호발생 주기	100 ms
전체 노드 수	500
비정상 행위노드	전체 노드 수의 10, 20%
거짓지목행위노드	비정상 행위 노드의 50%
노드 이동 속도	5 m/s
weight값 임계치	5
전파 범위	200 m

통신 오버헤드 감소를 위해 신고 및 보고 제어 패킷은 유니캐스트로 처리하며, 상위계층 노드인 WMN가 비정상 행위 노드를 최종 판별하여 고립시킬 경우에만 브로드캐스트로 전파하도록 설계하였다. 본 실험에서 설정된 MNL의 weight 값 증가율 1, 임계치 5와 각 노드 SNL의 count 값 증가율 1, 감소율 1, 최대값 10은 여러 번의 실험을 통해 도출한 값이며 향후 추가 실험을 통해 개선의 여지는 있다. 트래픽 발생주기가 100ms이므로 100초 당 발생하는 패킷 수의 최대치는 1000개이며 100초 단위로 패킷 처리량을 누적하여 측정하였다.

나. 실험결과

1) 비정상 행위 노드 영향분석

Fig. 8은 비정상 행위 노드가 Ad-hoc 네트워크에 미치는 영향에 대해 실험을 통해 분석한 내용이다. 즉, i) 네트워크 내에 모든 노드가 정상적인 노드로만 구성되고 표준 AODV 라우팅 프로토콜을 사용하는 경우, ii) 여기에 패킷을 드롭하는 이기적인 노드의 비율이 전체 노드의 10%인 경우, iii) 거짓 지목하는 악의적인 노드 비율이 전체 노드의 10%인 경우에 대해 각각 실험을 통해 패킷 처리율을 측정하였다.

실험 결과를 분석해보면 이기적인 노드의 포함 비율이 10%인 경우 정상적인 네트워크 환경에 비해 패킷 전송 성공률이 대략 10% 정도 감소함을 확인할 수 있다. 하지만 악의적인 거짓 지목 노드의 포함 비율이 10%인 경우에는 실험 시간이 경과할수록 패킷 전송율이 급격히 낮아지는 것을 확인할 수 있었다. 즉 Ad-hoc 네트워크의 정상적인 성능 발휘를 위해서는 이기적인 노드뿐만 아니라 악의적인 거짓 지목 행위 노드에 대해 탐지 및 대응 메커니즘이 필요하다. 특히 Ad-hoc 네트워크 성능에 이기적인 노드보다 거짓 지목행위 노드가 더 치명적임을 실험을 통해 확인할 수 있다.

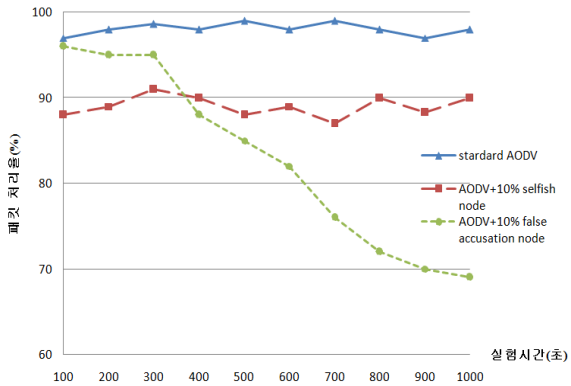

Fig. 8. 비정상 행위 노드에 따른 네트워크 영향 분석

2) 비정상 행위 노드 수 변화에 따른 패킷 처리율

Fig. 9, 10은 네트워크내의 비정상 행위 노드의 비율을 각각 10%, 20%로 증가시킴에 따라 Watchdog, CONFIDANT 그리고 제안하는 기법의 패킷 처리 성능 결과를 보여준다. 실험 결과를 종합적으로 분석해 보면 제안하는 기법은 네트워크 내에 비정상 행위 노드가 증가하더라도 시간이 증가함에 따라 이기적 노드뿐만 아니라 악의적인 거짓지목 행위 노드까지 탐지하여 네트워크로부터 이들을 배제시킬 수 있어 가장 뛰어난 성능을 보였다.

Watchdog은 알고리즘 특성상 패킷을 버리는 이기적 노드를 탐지하여 이들을 우회할 수 있는 기능만을 가지고 있다. 따라서 비정상 행위 노드의 비율이 증가할수록 패킷 처리량이 줄어들지만 악의적인 거짓지목 행위 노드로부터 영향을 받지 않기 때문에 일정한 패킷

처리 성능을 보장받을 수 있다. 반면, CONFIDANT 탐지 알고리즘은 이기적 노드를 탐지하여 네트워크로부터 고립시킬 수 있지만 악의적인 거짓지목 행위 노드에 대해 전혀 고려가 되지 않았다. 실험 결과에서 보듯 CONFIDANT는 초기에는 이기적 노드들을 탐지하여 네트워크로부터 배제시켜 성능이 좋아지지만 시간이 경과할수록 악의적 노드에 의해 정상 노드가 네트워크로부터 배제됨에 따라 급격한 성능 저하 현상을 보이게 된다. 즉 단순한 이기적 노드에 대해서는 적절한 탐지 및 배제가 가능하지만 악의적인 거짓지목 행위에 치명적인 피해를 받게 된다.

실험결과에서 살펴보듯이 Ad-hoc 네트워크에서의 비정상 행위 노드 탐지를 위한 알고리즘 설계에 있어서 반드시 악의적인 거짓지목 행위에 대한 고려가 필수적이라 할 수 있다.

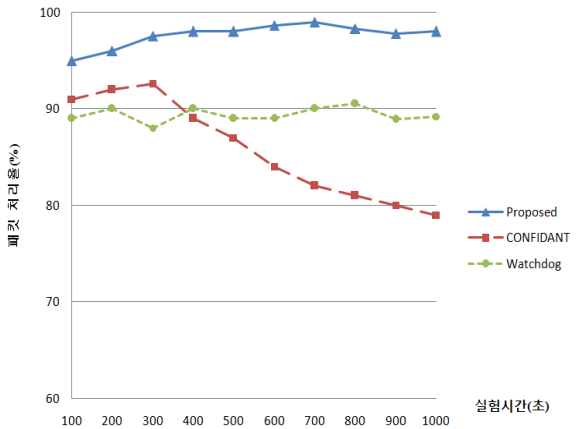

Fig. 9. 패킷 처리율 분석(비정상행위 노드 비율: 10%)

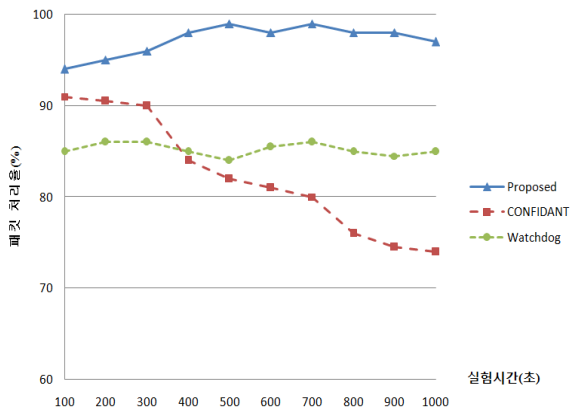

Fig. 10. 패킷 처리율 분석(비정상행위 노드 비율: 20%)

3) 네트워크 오버헤드 분석

제안한 기법은 비정상 행위 노드의 탐지 및 관리를 위한 제어 패킷이 추가적으로 발생하기 때문에 기존 라우팅 프로토콜에 비해 통신 오버헤드는 다소 증가한다. 추가적으로 발생하는 패킷은 목적지 노드가 비정상행위 노드를 송신지 노드에게 신고하는 패킷, 송신지 노드와 목적지 노드가 비정상 행위 노드를 상위 계층 노드인 WMN에게 보고하는 패킷, 상위 계층 노드가 고립 대상 노드를 선정하여 지역내 노드들에게 브로드캐스트하는 패킷이다. 신고 및 비정상 행위 노드 전파시 발생되는 통신 오버헤드를 구하는 식은 (1), (2), (3), (4)와 같이 표현할 수 있다.

초당 패킷 발생수를 t, 평균 라우팅 경로 포함 노드수를 p, 데이터 패킷 사이즈를 NP_{size}, 총 노드수를 N, 비정상 행위 노드수를 M, 전체 실험시간 동안 평균적인 비정상 행위 발생 횟수를 r, 신고 및 제어 패킷 사이즈를 CP_{size}, 모의실험 시간을 T, 신고노드로부터 WMN까지의 경로에 포함되는 평균 노드수를 n이라고 할 경우, 송신지 노드와 목적지 노드 사이에 NWARN 패킷 전송을 위한 오버헤드(V)는

$$V = p \times CP_{size} \times M \times r \quad (1)$$

송신지 및 목적지 노드가 WMN에게 혐의노드 신고시 발생하는 오버헤드(U)는

$$U = n \times CP_{size} \times M \times r \times 2 \quad (2)$$

WMN가 비정상 행위 노드를 브로드캐스트시 발생하는 오버헤드(B)는

$$B = M \times CP_{size} \times N \quad (3)$$

실험시간동안 발생하는 총 통신량 대비 오버헤드(O)는

$$O = \frac{V + U + B}{T \times t \times p \times NP_{size}} \quad (4)$$

로 표현할 수 있다. Fig. 11는 비정상 행위 노드의 탐지 및 배제를 위해 추가적으로 발생한 패킷 유통량에 대해 실험을 통해 분석한 결과 그래프이다. 즉, 본 논문에서 제안하는 탐지 기법을 적용할 경우 추가적인

통신 오버헤드는 약 2~5%이다. 하지만 패킷 처리량은 앞에서 살펴보았듯이 기존 방식에 비해 10~20% 이상 향상되며 시간이 경과할수록 격차는 점점 더 커지는 것을 알 수 있었다. 또한 제안하는 기법에서 발생되는 제어 패킷은 시간 경과시 비정상 행위 노드가 고립됨에 따라 점차 감소함을 알 수 있다. 따라서 추가적인 통신 오버헤드는 비정상 행위 노드의 탐지 및 배제를 통해 네트워크 전반의 처리율이 향상되는 것을 고려할 때 그 영향은 제한적이다.

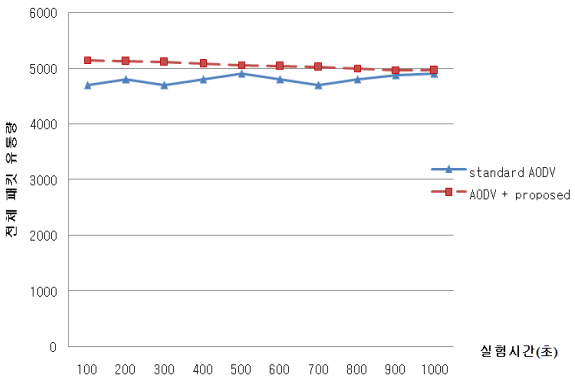

Fig. 11. 네트워크 오버헤드 분석

5. 결 론

향후 우리 군에 도입될 TICN체계에 적용될 Ad-hoc 네트워크 기술은 고정된 인프라가 존재하지 않는다는 점과 연산 능력 및 배터리 용량이 적은 이동성 있는 노드들로만 구성된다는 점 때문에 기존의 보안 메커니즘을 그대로 적용할 수 없다. 그리고 통신에 참여하는 다수의 노드들은 서로간의 협조 관계를 전제로 네트워크가 구성됨으로 보안 취약성이 존재한다. 또한 기존에 제시된 탐지 기법들이 악의적인 거짓지목 행위 노드에 대한 고려가 전혀 되지 않았다는 문제점을 가지고 있다. 이에 본 논문에서는 일반적인 비정상 행위 노드 중 이기적 행위 노드뿐만 아니라 악의적인 거짓지목 행위 노드에 대해서도 동시에 탐지 및 배제할 수 있는 기법을 제시하였고 실험을 통해 그 효율성을 입증하였다.

또한 각 노드들이 관리하는 SNL를 활용하여 경로 설정 단계에서 신뢰할 수 있는 최적의 경로 설정이 가능하도록 하였으며, 공모 노드에 의한 취약점 해결을 위해 ElGamal 방식을 응용한 해결 방법과 부당하게 가중치를 부여받는 노드들의 생존성 유지를 위해 가중치를 감해줄 수 있는 알고리즘을 추가로 제시하였다.

본 논문에서 제안하는 방법에 따른 모의실험 결과, 이기적인 노드뿐만 아니라 악의적인 거짓지목 행위 노드에 대해서도 기존의 탐지기법에 비해 뛰어난 탐지 및 배제가 가능하다는 것을 확인 할 수 있었으며 본 연구 결과는 향후 우리 군에서 TICN 체계 도입시 성능 및 보안 향상에 기여할 수 있을 것으로 기대한다. 향후에는 추가적인 공격 유형에 대한 침입탐지 기법에 대한 연구를 진행할 예정이다.

References

[1] P. Michiardi, and R. Molva, “Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks”, European Wireless Conference, 2002.

[2] Panagiotis Papadimitratos, and Zygmunt J. Hass, “Secure Routing for Mobile Ad Hoc Networks”, in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference(CNDS 2002), San Antonio, TX, Jan. 2002.

[3] Y. Hu, A. Perring, and D. Johnson, “Ariadne : A Secure On-Demand Routing Protocol for Ad Hoc Network”, in Proceedings of ACM MobiCom ’02, 2002.

[4] G. Zapata, “Secure Ad Hoc On-Demand Distance Vector(SAODV) Routing”, in IETF Draft, http://www.ietf.org/internet-draft/draft-guerrero-manet-saodv-00.txt, 2001.

[5] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks”, in Proceedings of IEEE ICNP ’02, 2002.

[6] F. Kargl, and A. Geiss, “Secure Dynamic Source Routing”, in Proceedings of HICSS 38, 2005.

[7] Jaydip Sen, “A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks”, CoRR, 2010.

[8] C. K. Toh, C. Lee, and N. A. Ramos, “Next-Generation Tactical Ad Hoc Mobile Wireless Networks”, in Technology Review Journal Spring, pp. 103~113, 2002.

[9] J. Brand, and G. Hart Wig, “Management of Tactical Ad Hoc Networks with C2 Data Models”, Military Communication Conference 2001 IEEE, pp. 915～922, Aug. 2002.

[10] Y. Zhang, and W. Lee, “Intrusion Detection in Wireless Ad-Hoc Networks,” in Mobile Computing and Networking, pp. 275～283, 2000.

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, in Proceeding of the 6th International Conference on Mobile Computing and Networking, pp. 255～265, Aug. 2000.

[12] S. Buchegger, J-Y. L. Boudec, “Nodes Bearing Grudges : Towards Routing Security, Fairness and Robustness in Mobile Ad Hoc Networks”, in Euromicro Workshop on Parallel, Distributed amd Network-based Processing, pp. 403～410, Jan. 2002.

[13] S. Buchegger, and J. L. Boudec, “Performance Analysis of the CONFIDANT Protocol,” in Proceeding of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, pp. 226～236, 2002.

[14] Chin-Yang Tseng, Poornima Balasubra-manyam, Calvin Ko, and Karl Levitt, “A Specification-Based Intrusion Detection Model for OLSR”, LNCS 3858, pp. 330～350, 2006.

[15] Aikaterini Mitrokotsa, Rosa Mavropodi, and Christos Douligeris, “Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks”, International Conference on Intelligent Systems and Computing : Theory and Applications, July, 2006.

[16] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou, “Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-hoc Networks”, Journal of Internet Engineering, Vol. 2, No. 1, June, 2008.

[17] Jaydip Sen, and Kaustav Goswami, “An Algorithm for Detection of Selfish Nodes in Wireless Mesh Networks”, in Proceedings of the International Symposium on Intelligent Information Systems and Applications, pp. 571～576, Oct., 2009.

[18] C. E. Perkins, E. M. Royer, and S. R. Das., “Ad Hoc On-Demand Distance Vector(AODV) Routing”, IETF, MANET Working Group, Oct. 1999.