情報保護學會論文誌
第16卷 第6號, 2006. 12

무선 Ad hoc 네트워크의 효율적인 위장 공격 방지 메커니즘에 관한 연구

홍 순 좌†, 박 현 동
국가보안기술연구소

The Study on the Effective Prevention Mechanism of Masquerade Attacks on Wireless Ad hoc Network

Soonjwa Hong†, Hyun-Dong Park
National Security Research Institute

요 약

무선 Ad hoc 네트워크는 통신 채널의 취약성, 노드의 보안 취약점, 기반 구조의 부재, 동적인 위상 변화 등의 특성으로 인해 보안 메커니즘 설계 및 구현이 기존 유선 네트워크에 비해 어려운 것으로 인식되고 있다. 기존의 연구들이 유선 네트워크의 보안을 무선 Ad hoc 네트워크로 적용하는데 많은 노력을 기울여 왔으나, 무선 Ad hoc 네트워크의 본질적인 문제로 인하여 효과적인 성과를 거두지 못하고 있다. 본 논문은 무선 Ad hoc 네트워크의 보안 분야 중에서 하나 또는 둘 이상의 협업된 위장 노드들의 대량의 위장 패킷 공격으로 인해 네트워크 자체의 생존성 및 가용성에 새로운 문제가 있음을 제기하고 그 결과를 증명한다. 또한 무선 Ad hoc 네트워크의 생존성 및 성능 향상을 위한 접근 방법으로 기존 방식의 기준을 탈피하여 무선 Ad hoc 네트워크의 특성을 반영하는 생존성 강화를 위하여 효율적인 위장 공격 방지 메커니즘을 제안한다.

ABSTRACT

Securing wireless Ad hoc network including the secure mechanism design and implementation is generally more difficult for vulnerability of channels and nodes, the absence of infrastructure, topology that change dynamically, and etc, than wire network. The efforts of early researches are based on the adaptation of securing methods for the wire network to wireless ad hoc network. However, wireless ad hoc network could not get effective study finding because network has essential problems. This paper proposes that some new problems are being came to light over the survivability and availability of the network itself, that are caused by the massive packet attack of more than one or two nodes, and proves the consequence of this phenomenon. Also, we propose an effective prevention mechanism of masquerade attacks for survivability reinforcement that escape standard of the early way by survivability of wireless Ad hoc network and approaches for performance elevation and reflect special quality of wireless Ad hoc network.

Keywords : *Ad hoc network, wireless network, survivability, masquerade packet attack*

Ⅰ. 서 론

무선 이동 Ad hoc 네트워크는 미래 유비쿼터스 컴퓨팅 환경의 네트워크 인프라 구축을 위한 핵심기

접수일: 2006년 10월 23일 ; 채택일: 2006년 12월 6일
† 주저자, hongsj@etri.re.kr

술이며, 고정 인프라가 없고, 네트워크 토폴로지가 수시로 변한다는 특성을 가지고 있다.

유비쿼터스 컴퓨팅을 향한 새롭고 다양한 응용 분야가 등장하고 실험되기 시작하면서, 무선 Ad hoc 네트워크의 보안 및 프라이버시 메커니즘에 대한 연구와 개발이 최근 들어 매우 활발하게 시작되고 있다[1].

또한 무선 Ad hoc 네트워크는 기존의 네트워크와 달리 통신 채널의 취약점, 노드의 보안 취약점, 기반구조의 부재, 동적인 위상 변화와 같은 특성들로 인해 보안 메커니즘의 설계가 어려운 것으로 인식되고 있다[2].

본 논문은 무선 Ad hoc 네트워크의 많은 보안 분야 중에서 하나 또는 둘 이상의 협업된 위장 노드들의 대량의 패킷 공격으로 인해 네트워크 자체의 생존성 및 가용성에 문제가 있음을 제안하고 증명한다. 유선 네트워크와 달리 공격 대상이 되는 희생자 노드가 생존성 및 가용성에 문제가 발생하기 이전에 중간 경로상의 노드들의 배터리 전력 소모가 급격히 발생하는 현상을 실험을 통해 증명한다[3].

또한, 보안 라우팅 프로토콜, 침입 탐지 및 차단에서 해결하기 어려운 점을 분석하여 위장 패킷의 발생범위를 제한하며, 중간 경로상에 유통되는 위장 패킷을 검출하여 전송을 방지함으로써 각 노드의 자원 소모를 최대한 감소시켜, 네트워크 전체의 생존성을 향상시킬 수 있는 메커니즘을 제안한다. 제안하는 위장 패킷 공격의 방지 메커니즘은 네트워크 구성 노드의 위장 패킷 공격에 대한 네트워크 내의 다른 구성 노드에 대한 에너지 고갈에 대처하여 생존성을 개선하고, 네트워크 내의 TCP Throughput 성능 감소를 최소화하는 것을 목적으로 하며 다음과 같은 관점에서 설계하였다.

- 기존 라우팅 프로토콜의 적용성 강화
- 비암호학적인 접근방식
- 대량 위장패킷 공격에 대한 효율적인 탐지 및 차단방식

본 논문은 II장에서 무선 Ad hoc 네트워크의 비정상 행위를 분석하고, III장에서는 위장 노드의 대량 패킷 공격으로 인하여 무선 Ad hoc 네트워크가 직면하는 새로운 문제점을 분석 및 증명한다. IV장에서는 무선 Ad hoc 네트워크의 생존성을 향상시키고자 하는 새로운 메커니즘을 제안하고, 그 성능을 분석하여 제안된 메커니즘의 타당성을 증명한다. 마지막으로 V장에서 본 논문의 결론 및 향후 연구방향을 기술한다.

II. 무선 Ad hoc 네트워크의 비정상행위

앞 장에서 논의한 바와 같이, Ad hoc 네트워크에 대한 서비스거부(DoS: Denial of Service) 공격은 네트워크에 대한 가용성 및 이에 따른 생존성을 약화시키고자하는 행위이다. 유선 네트워크에서의 DoS 공격에 대해서는 많은 연구가 이루어졌지만, 무선 Ad hoc 네트워크에서의 DoS 공격에 대한 연구는 최근에 들어서야 시작되고 있다[4-6]. 특정 호스트를 공격하여 서비스가 불가능하도록 하는 것이 유선 네트워크에서의 전형적인 DoS 공격이었으나, 무선 Ad hoc 네트워크에서는 그 특성으로 인하여 많은 새로운 유형의 DoS 공격이 가능하다. 즉, 이동 노드들의 제한된 에너지, 빈번한 이동성, 상대적으로 작은 전송 대역폭(bandwidth), Ad hoc 네트워크 특유의 라우팅 방법 등과 같이 이전의 네트워크에서는 불가능하거나 무의미 했던 유형의 행동들이 무선 Ad hoc 네트워크에서는 전송성능, 생존성 및 가용성 등의 요소에 심각한 영향을 끼칠 수도 있다. 예를 들어, Ad hoc 네트워크에서의 대부분의 라우팅 프로토콜은 브로드캐스트에 의해 경로를 탐색하므로, 라우팅 정보를 수집하거나 잘못된 정보를 전파하는 것이 상대적으로 용이하며, 제한된 에너지만을 가지고 행동하는 무선 이동 노드들의 특성에 의해 간단한 방법으로 특정 노드의 에너지를 고갈시켜서 서비스가 불가능하도록 할 수도 있다.

무선 Ad hoc 네트워크에서의 DoS 공격은 〔표 1〕에서 보는 바와 같이 적극적인 공격과 수동적인 비협조의 두 가지 형태로 분류할 수 있다. 여기에서 적극적인 공격이란, 라우팅 메커니즘이나 MAC 프로토콜을 이용하여 다른 노드들에게 잘못된 정보를 전파하거나 불필요한 트래픽을 발생시키는 등의 방법으로 네트워크 전체의 성능 및 가용성을 급격히 저하시키는 유형의 DoS 공격을 의미한다.

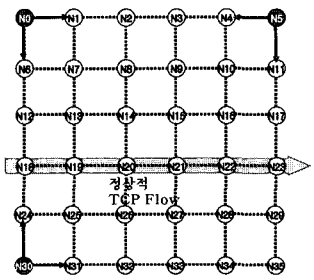
〔표 1〕 무선 Ad hoc 네트워크에 대한 공격 분류

계층 / 공격유형	네트워크 계층	MAC 계층
Active attack	라우팅 메커니즘에 대한 DoS 공격	MAC 프로토콜을 이용한 DoS 공격
Mis-behaving	라우팅 메커니즘에 대한 비협조 및 무시	MAC 프로토콜을 역이용하는 행위

한편, 이동 노드가 라우팅 정보의 전달과 공유에 참여하지 않거나, 혹은 MAC 프로토콜의 접근 규칙을 위반하여 불공정하게 네트워크를 사용하는 등의 행위는 다른 노드들을 직접적으로 공격하는 행위는 아니지만, 결과적으로 네트워크의 전송효율을 저하시키고 불필요한 에너지를 사용하게 하여 간접적으로 DoS 공격의 효과를 내게 된다.

Ⅲ. 무선 Ad hoc 네트워크의 새로운 문제점 분석

이미 논의된 무선 Ad hoc 네트워크에 대한 DoS 공격 유형 중에서 적극적인 DoS 공격이 시스템에 미치는 영향을 시뮬레이션에 의해 고찰하고 분석한다. 시뮬레이션 도구는 ns-2의 시뮬레이션 환경에 무선 서브넷 및 Ad hoc 네트워킹을 위한 새로운 구성요소를 추가한 CMU Monarch extensions[7]을 사용하였다. 먼저 시뮬레이션을 위한 Ad hoc 네트워크는 [그림 1]과 같이 가로 세로 각각 6개씩의 무선 이동노드를 배치하여 실험을 하였다.

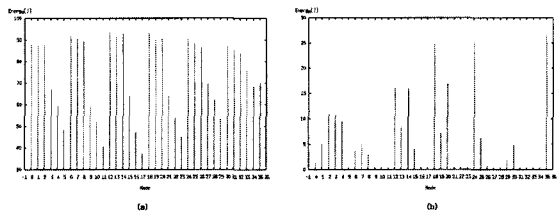


[그림 1] 실험 대상의 토폴로지

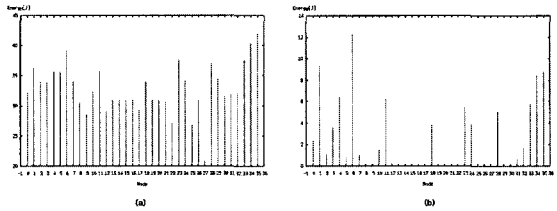
36개의 노드 모두 IEEE 802.11 MAC을 사용하고, 라우팅 프로토콜은 DSR(Dynamic Source Routing)을 적용하였다. 각 노드들의 위치는 시뮬레이션 기간 중에 고정시켰으며, 노드 사이의 거리는 실험 시나리오에 따라 100m에서 200m까지 가변시켰다. 참고적으로 각 노드의 전송 범위(transmission range)는 반경 250m 씩이다.

3.1 무선 Ad hoc 네트워크의 생존성 문제

[그림 1]의 Ad hoc 네트워크에서 0번, 5번, 30번 노드가 DoS 공격을 수행하는 노드들이고, 이들이 동시에 35번 노드에 대해 TCP 트래픽을 발생하여 전송하도록 하였다. 이는 유선 네트워크에서의 TCP flooding 공격에 해당하는 것이다. 각 노드의 최초 에너지는 100J이고 패킷의 송신에 2watts, 수신에 1watt의 파워가 소모된다고 가정하였다. [그림 2]는 노드간 거리를 200m로 가정하고 Dos 공격 후의 소모되는 에너지의 잔량을 보여주고 있으며, [그림 3]은 100m로 가정하였을 때의 결과이다. 노드간의 거리가 짧을수록 DoS 공격에 의한 노드의 에너지 소모가 더 크게 발생한다.



[그림 2] DoS 공격에 의한 에너지 소모: 노드간 간격 200m, (a) 100초 후, (b) 200초 후



[그림 3] DoS 공격에 의한 에너지 소모: 노드간 간격 100m, (a) 100초 후, (b) 150초 후

3.2 무선 Ad hoc 네트워크의 TCP Throughput 문제

[그림 4] (a)에서 세 개의 그래프는 위에서부터 각각 TCP flooding이 없는 경우, 5번 노드만 TCP 패킷을 전송하는 경우, 그리고 5번과 30번 모두 DoS 공격에 참여하는 경우에 대해서 TCP 트래픽의 throughput을 측정한 것이다. TCP flooding이 없는 경우에 비해서 5번 노드가 DoS 공격을 하는 경우에는 TCP의 throughput이 감소함을 알 수 있는데, 이는 TCP 트래픽의 전송경로와 TCP 트래픽의 전송경로가 23번 노드에서 일부 중첩되기 때문에 TCP throughput이 감소하는 것이다. 30번 노드까지 DoS 공격에 가담을 하는 경우에는 TCP 트래픽의 throughput이 심각

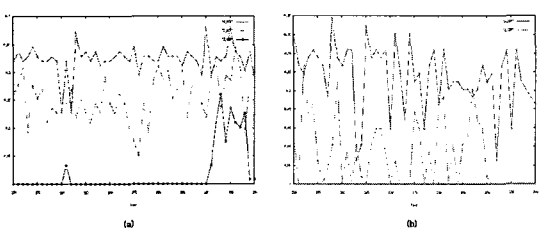
하게 저하됨을 볼 수 있는데, 이는 30번 노드에서 전송되는 UDP 패킷들이 TCP 트래픽의 전송경로와 평행하게 전달이 됨으로 인해서 TCP 패킷의 전송을 방해하기 때문이다. 즉, 노드 사이의 거리가 100m이므로, 예를 들어 31번 노드가 UDP 패킷을 18,19,20번 노드 모두 이의 전송범위에 포함되어 전송이 불가능해지는 것이다.

(b)에서는 노드간의 거리를 200m로 늘인 상황에서 앞에서와 같은 내용의 시뮬레이션을 수행하였다. 그림 4에서 두 개의 그래프는 위에서부터 UDP flooding이 없는 경우와 5번 노드가 DoS 공격을 하는 경우에 각각 18번과 23번 노드 사이의 TCP throughput을 나타낸다. UDP flooding이 없는 경우에 (a)와 비교하면 TCP throughput이 절반 정도로 감소함을 알 수 있는데, 이는 노드간의 거리가 멀어짐으로 인해서 송신자와 수신자 사이의 전송경로(hop 수)가 2배로 증가하기 때문이다. 또한 (a)의 경우와 마찬가지로, 5번 노드가 35번 노드에 대해 DoS 공격을 하는 경우에 전송경로의 중첩으로 인하여 TCP 트래픽의 throughput이 감소함을 볼 수 있다.

Ⅳ. 효율적인 위장 공격 방지 메커니즘

4.1 기존 방식의 문제점 및 제안방향

무선 Ad hoc 네트워크에 대한 DoS 공격의 특성은 기존 유선 네트워크에 비해 공격의 대상이 되는 희생자 노드보다 전송 중간경로 상의 노드들의 피해가 심각하고, 피해가 전체 네트워크에 걸쳐 발생하며, 다른 전송경로의 throughput에도 영향을 미친다.



(그림 4) DoS 공격에 의한 throughput 감소효과 (a) 노드간 100m (b) 노드간 200m

특히 이동 노드들이 밀집해 있고, 넓은 전송 범위를 유지하며, 희생자 노드까지 많은 hop 수가 있는 경우에는 무선 Ad hoc 네트워크의 에너지 소모가 커지므로 생존성 보장이 보다 더 어렵게 된다. 기존 무선 Ad hoc 네트워크 보안 관련 연구 분야 및 각각의 문제점은 (표 2)와 같다.

(표 2) 기존 연구 분야의 한계점

기존 연구	한계점
호스트 기반의 IDS를 적용하여 비정상 행위 및 패킷 탐지 연구 분야[13-14]	각 분야가 개별적인 연구를 해옴으로써 유선 네트워크의 IPSEC 사례가 반복됨 호스트 기반의 IDS는 탐지율이 100% 신뢰할 수 없으며, 처리하는데 Overhead가 높음
Secure 라우팅 프로토콜 제안을 통한 보안성 강화를 통한 연구 분야[9-12]	Secure Routing 프로토콜과 인증/암호 프로토콜은 암호학적인 키 관리에 의존적이므로 높은 Overhead의 중앙집중형의 인프라 구조를 요구
암호학적인 인증 및 암호 프로토콜 적용하는 연구 분야[17-21]	Ad hoc은 노드의 이동성 및 연결성이 빈번하므로 중앙 집중적인 구조는 한계를 보임

가용성 및 생존성 분야는 MAC 계층 이하에서 배터리 파워 소모 관련 연구가 대부분이며, 생존성 향상 연구가 노드에 집중되고 있으므로 전체 네트워크 생존성 보장 연구는 없는 실정이다[15,16].

노드별로 연결 및 비연결이 용이하므로 공격자 및 불법 패킷의 탐지가 어려우며, 위장 패킷의 flooding 공격은 유선과 달리 네트워크 노드의 전력소모를 극대화하여 생존성 보장에 어려움을 발생하는 Ad hoc 네트워크의 생존성 보장의 새로운 이슈이다[8]. 그러나 정상 패킷에 대한 Power- guaranteed 분야의 기술 연구는 생존성 보장이라는 측면에서 한계를 가질 수 있다. 따라서 본 논문에서 제안하고자 하는 효율적인 위장 공격 방지 메커니즘의 기본적인 연구방향은 다음과 같다.

- 키관리와 같은 인프라를 가능한 배제
- 기존의 라우팅 프로토콜에 손쉽게 적용할 수 있는 메커니즘 제안
- 무선 Ad hoc에 주로 사용되는 소스 기반의 라우팅(on-Demand) 방식(DSR, AODV)은 Packet flooding을 기본으로 함
- Packet flooding에 대한 새로운 구조를 제안하여 기존의 라우팅 프로토콜의 적용성을 용이하게

하며 불법적인 위장 패킷을 최소화하여 생존성을 강화 시키는 방향 연구
- 무선 Ad hoc 네트워크내의 위장 공격에 대한 네트워크 생존성 향상

4.2 위장 패킷 탐지 및 차단을 위한 제안

본 논문에서 제안하는 메커니즘은 무선 Ad hoc 네트워크의 특정 노드를 공격자로 설정하고 공격 대상인 희생자 노드에 위장 패킷을 대량으로 플러딩하여 공격하는 것을 가정한다. 4.3절 및 4.4절에서 제안되는 메커니즘은 위장된 패킷을 탐지하고 차단하는 것을 목표로 하며, 궁극적으로 제 3 장에서 증명된 네트워크 생존성 문제점을 해결하는 것을 목적으로 한다.

본 절은 다음과 같은 구성요소의 데이터 구조를 제안하며, 4.3절 및 4.4절의 메커니즘에 적용된다.
- 송신 불필요 노드 리스트(*NoRcvNodeList*) : 수신된 패킷의 전송을 위하여 다음 경유 노드에서 제외해야 하는 노드들의 집합
- 이웃 노드 테이블(*NNT*: Neighbor Node Table) : 전송 범위 내에 있는 노드들의 정보
- 패킷 구조 : *NoRcvNodeList*, *NNT* 정보가 반영되어 재구성된 패킷 구조

4.2.1 이웃 노드 테이블(NNT)

이웃 노드 테이블은 각 노드가 전송 범위 내에 있는 이웃 노드들의 정보를 유지 관리하는 테이블이고 다음과 같이 표현하며, 주기적으로 이웃 노드와 통신을 통해 갱신하여 최신 정보로 유지하는 것을 가정한다.

$NNT_i = \{ Node_{i1}, \ldots, Node_{in} \}$
i : 현재 노드 번호
n : i'th 노드가 전송 가능한 이웃 노드의 갯수

무선 Ad hoc 네트워크는 노드의 이동성이 빈번하므로 *NNT*의 정확성은 네트워크의 *NNT* 갱신 주기 T_{NNT}값에 의존적이다.
- T_{optNNT} : 주어진 Ad hoc 네트워크의 이상적인 *NNT* 갱신 주기
- ***Mobility***(Nodes) : 네트워크 구성 노드들의 이동성
- $T_{optNNT} \propto$ ***Mobility***(Nodes)
- $(T_{optNNT} \gg T_{NNT}) \propto (1/$***Reliability***$(NNT))$, *NNT*의 신뢰성이 떨어지므로 라우팅 경로 설정 시 비정확한 경로 생성으로 네트워크 성능을 저하시킴
- $(T_{optNNT} \ll T_{NNT}) \propto$ ***Reliability***(NNT), T_{NNT}가 작으면 *NNT*의 신뢰성은 증가, *NNT* 갱신의 네트워크 부하 증가

T_{optNNT}의 설정은 네트워크 특성에 따라 결정할 수 있고 정확한 값을 설정하는 방법은 추후 연구 분야로 제안하며, 본 논문의 연구 범위에서는 제외한다. 〔그림 1〕의 실험 대상이 되는 무선 Ad hoc 네트워크의 구조에서 구성되는 *NNT*는 〔표 3〕과 같다.

〔표 3〕 이웃 노드 테이블

노드	인접노드번호	노드	인접노드번호	노드	인접노드번호	노드	인접노드번호
N_0	1,6	N_9	3,8,10,15	N_{18}	12,19,24	N_{27}	21,26,28,33
N_1	0,2,7	N_{10}	4,9,11,16	N_{19}	13,18,20,25	N_{28}	22,27,29,34
N_2	1,3,8	N_{11}	5,10,17	N_{20}	14,19,21,26	N_{29}	23,28,35
N_3	2,4,9	N_{12}	6,13,18	N_{21}	15,20,22,27	N_{30}	24,31
N_4	3,5,10	N_{13}	7,12,14,19	N_{22}	16,21,23,28	N_{31}	25,30,32
N_5	4,11	N_{14}	8,13,15,20	N_{23}	17,22,29	N_{32}	26,31,33
N_6	0,7,12	N_{15}	9,14,16,21	N_{24}	18,25,30	N_{33}	27,32,34
N_7	1,6,8,13	N_{16}	10,15,17,22	N_{25}	19,24,26,31	N_{34}	28,33,35
N_8	2,7,9,14	N_{17}	11,16,23	N_{26}	20,25,27,32	N_{35}	29,34

4.2.2 프로토콜 패킷 구조 제안

4.2.2.1 데이터 구조

기존의 패킷 구조 중에서 DSR 프로토콜에서 사용되는 패킷 P의 구조는 다음과 같이 표현할 수 있다.

$P = \{(S, D), \{H_1 \ldots H_L\}\}$,
S: 소스 주소, D: 목적지 주소, H_i : i번째 홉 노드($1 \le i \le L$)

본 논문에서 제안되는 메커니즘을 위해 적용하고자 하는 패킷 구조는 다음과 같다.

$P = \{(S, D), \boldsymbol{NNT_c}, \boldsymbol{NoRcvNodeList}, \boldsymbol{HopNodeList}\}$

HopNodeList는 중간 경로의 노드들의 IP 주소 집합으로 기존의 DSR 등의 프로토콜에서 사용되고 있는 중간 경로의 홉 노드를 가변적으로 표현하며, 다음과 같이 표현된다.

$\boldsymbol{HopNodeList} = \{H_1, \ldots, H_n\}$,
n : 패킷에 저장되는 노드 주소들의 크기

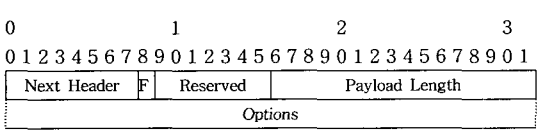
기존 패킷 구조에 새롭게 제안된 요소는 $\boldsymbol{NNT_c}$와 ***NoRcvNodeList***이다. $\boldsymbol{NNT_c}$는 현재 패킷을 전송한 노드의 NNT이며, ***NoRcvNodeList***는 해당 패킷을 이미 수신하여 재전송이 불필요하다고 판단되는 노드들의 리스트로 다음과 같이 표현된다.

$\boldsymbol{NoRcvNodeList} = \{N_1, \ldots, N_l\}$

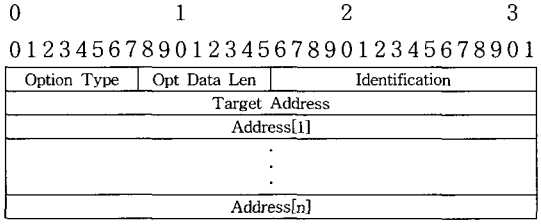
NoRcvNodeList는 패킷의 시작 노드, 현재 패킷의 송신 노드, 이미 패킷을 수신한 노드 3 종류의 노드를 포함한다.

4.2.2.2 DSR 프로토콜의 패킷 구조

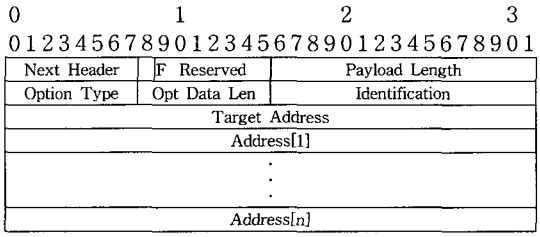
DSR 라우팅 프로토콜의 기본적인 구조는 다음의 DSR Options Header의 고정된 영역과 Options 필드의 확장으로 구성된다[22].



DSR 패킷 중에서 위장 공격에 사용되는 플러딩 패킷은 ***Route Request option***에 해당되므로, 본 논문에서는 이 option에 대한 패킷 구조만을 다루기로 한다.

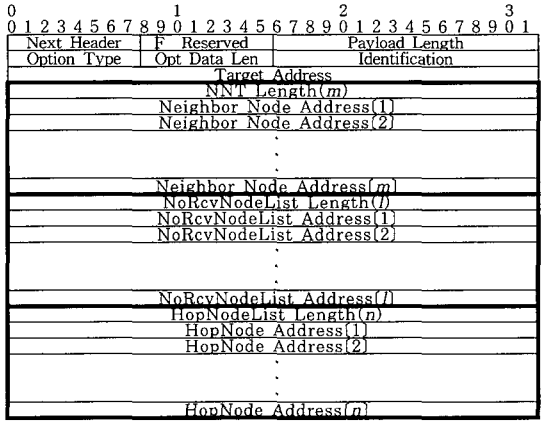


앞에서 정의한 DSR Options Header의 Options에 ***Route Request option***을 확장한 패킷 구조는 다음과 같다.



4.2.2.3 DSR 프로토콜의 패킷 구조의 변경

본 논문에서 제안되는 메커니즘의 추가 요소를 적용하여 Route Request option에 패킷 구조를 확장 및 재구성한 결과는 다음과 같다.



4.3 패킷 생성 및 전달 메커니즘

패킷 생성 및 전달 메커니즘은 초기의 패킷 생성과 패킷 전달 메커니즘으로 구성되며, 이에 요구되는 전제 사항으로 노드 구분은 N_s : 시작지 노드(source node), N_d : 목적지 노드(destination node), N_r : 중간 연계 노드(relay node), N_i : i번째 노드의 4종으로 구분하며, 이웃 노드 테이블(NNT_i)는 노드 N_i 의 이웃 노드 테이블로서 다음과 같이 표현한다.

$$NNT_i = \{N_{i1}, \ldots, N_{in}\},$$

n은 네트워크 내에서 가장 큰 이웃노드를 가진 노드의 이웃 노드 수이다.

4.3.1 패킷 생성 메커니즘

기존의 라우팅 프로토콜에서 패킷 플러딩 절차를 변경한 메커니즘으로, 패킷을 생성할 때 *NoRcvNodeList*를 4.2.2절에서 제안한 패킷 구조에 적용한다. 기존 라우팅 프로토콜은 *NoRcvNodeList*를 생성하여 패킷을 재구성하는 부분만 추가하여 구현될 수 있다.

다음 〈메커니즘 1: 패킷 생성〉에 따라 새로운 패킷을 생성하고 전파한다. [단계 1]은 기존 라우팅 프로토콜과 동일하며, [단계 2]에서는 이 패킷을 수신한 노드가 재전송을 판단할 때 불필요한지 여부를 판단하는 *NoRcvNodeList*를 생성하는 단계이다. 즉, 초기 생성 시 *NoRcvNodeList*에는 소스 노드인 N_s만 추가된다. [단계 3]에서는 *HopNodeList*에 자신인 소스 노드 N_s를 추가하며, [단계 4]에서는 [단계 1], [단계 2], [단계 3]에서 생성된 데이터를 조합하여 패킷을 생성한 후, 그 패킷을 이웃 노드들에게 전송한다.

< 메커니즘 1 : 패킷 생성 >

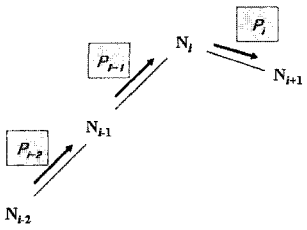
[단계 1] 시작지 N_s는 목적지 노드 N_d를 선택
- $S = N_s$, $D = N_d$

[단계 2] 이 노드에서 생성한 패킷의 재전송 불필요 노드 계산
- $NoRcvNodeList_{new} = \{N_s\}$

[단계 3] *HopNodeList*에 시작지 노드를 추가
- $HopNodeList_{new} = \{\} + \{N_s\} = \{N_s\}$

[단계 4] 패킷 생성 및 전송
- 노드 N_s는 $NoRcvNodeList_{new}$, $HopNodeList$가 갱신된 다음과 같은 패킷을 생성하고, 자신의 전송 범위에 해당되는 노드로 이 패킷을 전송

$P = \{(N_s,N_d), NNT_s, NoRcvNodeList_{new}, HopNodeList_{new}\}$



〔그림 5〕 패킷 릴레이의 예

< 메커니즘2 : 패킷 전달 >

[단계 1] 현재의 노드 N_c는 자신에게 전송된 패킷 $P(N_{i-1},N_i)$을 수신한다.
N_i : 패킷을 수신한 현재 노드(current node)
N_{i-1} : 패킷을 전송한 이전 노드(previous node)

[단계 2] 현재 노드 N_i가 $NoRcvNodeList_{i-1}$에 포함되어 있는가를 비교
if ($N_i \in NoRcvNodeList_{i-1}$)
then 현재 패킷 $P(N_{i-1},N_i)$ 폐기 & exit
else go to [단계 3]

[단계 3] $P(N_{i-1},N_i)$의 재전송 불필요 노드 계산
$NoRcvNodeList_i = NoRcvNodeList_{i-1} + \{N_i\} + NNT_{i-1}$
$= NoRcvNodeList_{i-1} + \{N_i\} + \{N_{(i-1)1}, \ldots, N_{(i-1)m}\}$

[단계 4] *HopNodeList*에 자신을 추가
$HopNodeList_i = HopNodeList_{i-1} + \{N_i\}$

[단계 5] 패킷 갱신 및 전송
현재 노드 N_i는 다음과 같이 패킷을 생성하고, 자신의 전송 범위에 해당되는 노드로 이 패킷을 전송
$P = \{(N_s,N_d), NNT_i, NoRcvNodeList_i, HopNodeList_i\}$

4.3.2 패킷 전달 메커니즘

패킷 릴레이는 수신된 패킷을 다음 노드에게 전송하는 방식을 의미하며, [그림 5]는 패킷의 릴레이에 대한 예제를 보여준다. N_{i-2}가 패킷 P_{i-2}을 N_{i-1}로 전송하고, N_{i-1}가 패킷 P_{i-1}을 N_i로 전송하고, N_i는 패킷 P_i를 N_{i+1}로 전송하는 과정이다.

현재 노드인 N_i가 수신한 패킷 P_{i-1}의 $NoRcvNodeList_{i-1}$, 즉 N_{i-1}이 생성한 재송신 불필요 노드는 다음과 같이 계산되어 전송되어 온 것이다.

$$NoRcvNodeList_{i-1} = Source + Sender(N_{i-1}) + NeighborNodes_{i-2}$$

$NoRcvNodeList_{i-1}$에 N_i가 포함되어 있다면 이 패킷(P_{i-1})을 이미 수신하여 재전송한 경우가 있으므로, 다른 경로를 통하여 전파되어온 동일한 패킷으로 판단할 수 있으므로 폐기할 수 있다. 즉, $NoRcvNodeList_{i-1}$에는 P_{i-1}을 재전송할 필요가 없는 노드들의 집합이다.

Source는 현 패킷의 시작지 노드, ***Sender***는 이 패킷을 전송한 노드(N_{i-1})이며, ***Neighbor Nodes***$_{i-2}$는 P_{i-2}을 전송한 N_{i-2}의 이웃 노드들로써 NNT_{i-2}에 해당된다. 즉, ***NoRcvNodeList***$_i$는 패킷을 수신한 노드들이 패킷을 폐기할 것인가를 판단할 때 사용하는 정보이다.

수신된 패킷의 목적 노드가 아닌 중간 노드의 역할을 정의하는 절차는 〈메커니즘 2: 패킷 수신·전달〉과 같다. 수신된 패킷의 목적 노드 N_d가 자신일 경우, 정해진 라우팅 프로토콜에 따라 RREP 패킷을 전송한다.

4.4 위장 패킷 탐지·차단 메커니즘

수신된 패킷의 위장 여부에 대한 탐지 및 차단 절차는 〈메커니즘 3: 위장 패킷 탐지·차단〉과 같다.

수신된 패킷의 *HopNodeList*에 하나의 노드만 있을 경우 직전에 생성되어 온 시작 패킷으로 판단할 수 있으며, 그 노드는 소스 노드 N_s와 동일해야 한다. 만일 서로 다른 값이라면 패킷이 위장된 것으로 판단하고 패킷을 폐기하고 이후 절차를 중단한다.

수신된 패킷의 *HopNodeList*에 둘 이상의 노드가 있는 경우 이전 노드로부터 재전송되어 온 것으로 판단할 수 있으며, 〔단계 2〕로 진행하여 패킷의 수신 범위를 검증한다.

< 메커니즘 3 : 위장 패킷 탐지·차단 >

[단계 1] 수신된 패킷의 종류 검사 시작 패킷 검증
- 시작 패킷인 경우
  HopNodeList에 하나의 노드만 있고, 소스(N_s)와 일치하지 않은 경우 패킷 전송을 중단하고 패킷을 폐기 후 중단
- 중간 패킷인 경우
  HopNodeList가 2개 이상으로 구성된 패킷일 경우 [단계 2]로 진행

[단계 2] 중간 패킷의 패킷 수신 범위 검증
- ***HopNodeList***의 마지막 노드 N_{i-1}는 패킷의 송신 노드로서,
- 패킷을 수신한 현재 노드(N_i)는 자신의 NNT_i와 비교하여 수신 가능한 패킷인지 검증 수행, 즉 N_{i-1}이 NNT_i에 포함되어 있는가를 검사
- 없다면 수신 불가능한 패킷인 경우로 패킷 폐기하고 진행을 중단
- 있다면 수신 가능한 패킷인 경우로 <메커니즘 2>에 따라 패킷을 생성하여 전송절차 수행

HopNodeList의 마지막 노드 N_{i-1}는 패킷의 송신 노드로서, 패킷을 수신한 현재 노드(N_i)는 자신의 NNT_i와 비교하여 수신 가능한 패킷인지를 검증한다. 즉, 송신 노드 N_{i-1}이 NNT_i에 포함되어 있는가를 검사하는 것으로, N_{i-1}이 NNT_i에 포함되지 않았다면 송신 노드가 위장되어 있는 패킷으로 판단하여 해당 패킷을 폐기하고 더 이상 진행하지 않는다. 반대로 있다면 정상 패킷으로 판단하여 〈메커니즘 2〉의 절차에 따라 패킷을 재 생성하여 전송절차를 수행한다.

4.5 제안 메커니즘 검증

본 논문에서 제안된 위장 패킷 탐지/차단 메커니즘의 정확성 및 효율성 검증을 위하여 위장 공격 패킷 시나리오를 설정하고, 제안된 알고리즘이 위장 패킷을 탐지하고 차단하는 능력을 검증하며, 전체 네트워크에서 위장 패킷을 발생 시키는 범위를 제한하는 능력의 효율성을 검증한다.

4.5.1 위장 패킷 공격 시나리오

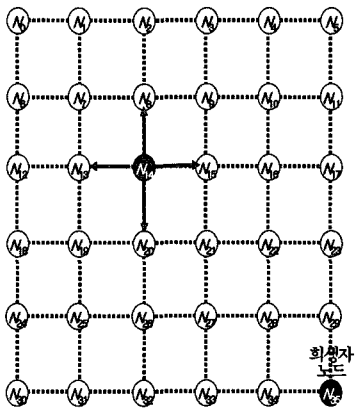
〔그림 1〕에서 노드 N_{14}를 공격자로, 노드 N_{35}를 희생자로 선정한 공격 상황을 가정하여 위장 패킷 공격을 한다. 〔표 3〕은 노드별로 구성되는 이웃 노드 테이블이다. 공격 노드인 N_{14}는 플러딩 패킷을 전파하며, 소스 주소는 자신이 아닌 것으로 위장하며, 목적지 주소는 희생자 노드인 N_{35}로 한다. 즉, N_{14}를 제외한 35개의 소스 주소를 갖는 위장 패킷을 생성하여 플러딩한다. 이때 공격하는 방법은 다음 두 가지로 나누어 볼 수 있다.

[공격 시나리오 1]

공격자 노드가 위장 패킷에 소스만을 위장하고, ***HopNodeList***를 위장하지 않은 경우로, 예를 들면 공격 노드 14가 패킷을 처음 전송하는 것으로 위장하는 경우가 해당된다.

[공격 시나리오 2]

공격자 노드가 위장 패킷에 소스와 ***HopNode List***를 동시에 위장하는 경우로, 예를 들면 공격 노드 14가 수신된 패킷을 중간 경로로 사용되어 전송하는 것으로 위장하는 경우가 해당된다.



〔그림 6〕 공격 시나리오 네트워크 위상

공격 시나리오 1에 따른 패킷의 경우의 수는 다음과 같다.

- 노드 N_{14}가 전파할 수 있는 패킷은 동일한 패킷에 대해 다음과 같이 4종류 나눌 수 있다.

  $P(14, 8) = \{(N_s, N_{35}), NNT_{14}, NoRcvNodeList, HopNodeList\}$

  $P(14,13) = \{(N_s, N_{35}), NNT_{14}, NoRcvNodeList, HopNodeList\}$

  $P(14,15) = \{(N_s, N_{35}), NNT_{14}, NoRcvNodeList, HopNodeList\}$

  $P(14,20) = \{(N_s, N_{35}), NNT_{14}, NoRcvNodeList, HopNodeList\}$
- N_S는 위장된 소스 노드, $(0 \le s \le 35,\ 14$제외$)$
- $HopNodeList = \{ s \}$

공격 시나리오 2에 따른 패킷의 경우의 수는 다음과 같다.

- 노드 N_{14}가 전파할 수 있는 패킷 형태는 시나리오 1과 동일하며, 다음 값만 다르다.
- $HopNodeList = \{s, h_1, \ldots, h_m\}$, h_i : i번째 홉 노드

공격 시나리오 1, 2에서 소스 노드 N_s는 위장된 것으로 네트워크 구성 노드들 모두가 위장 대상이 된다. 일반적으로 공격자 노드는 자신을 제외한 노드로 위장을 수행하므로 앞에서 제안된 네트워크에서 위장된 소스 노드는 다음과 같이 표현할 수 있다.

$$N_s \in \{ N_0, \ldots, N_{35} \} - N_A$$

4.5.2 위장 패킷 공격에 대한 대응 능력 분석

앞에서 제안된 메커니즘에 대한 성능 분석을 위해 다음과 같은 기준을 적용할 수 있다.

- 위장 패킷 생성 범위의 제한
- 위장 패킷 생성의 어려움 증대
- 위장 패킷 공격에 대한 탐지 능력 향상

공격자 노드는 위장 패킷을 생성하여 희생자 노드에 위장 공격을 감행하게 되며, 이에 대한 피해는 유선 네트워크와 달리 무선 Ad hoc 네트워크는 네트워크의 생존성 문제에 연결된다. 공격자 노드 N_A는 자신을 제외한 다른 노드로 위장하여 패킷을 전송하게 된다.

N_A를 N_{14}로 볼 때, N_{14}에서 위장 패킷의 전송 가능 노드는 $NNT_{14} = \{8, 13, 15, 20\}$의 노드들이 해당된다. 제안된 메커니즘에 의해 공격자 노드 N_{14}가 생성할 수 있는 패킷의 위장 범위(SR: Spoofed Range)는 다음과 같다.

- N_{14}에서 N_8로 위장 패킷을 전송할 때의 위장 범위

  $SR_{14}(N_8) = NNT_8 - N_{14} = \{2,7,9,14\} - 14 = \{2, 7, 9\}$
- N_{14}에서 N_{13}으로 위장 패킷을 전송할 때의 위장 범위

  $SR_{14}(N_{13}) = NNT_{13} - N_{14} = \{7,12,14,19\} - 14 = \{7,12,19\}$
- N_{14}에서 N_{15}로 위장 패킷을 전송할 때의 위장 범위

  $SR_{14}(N_{15}) = NNT_{15} - N_{14} = \{9,14,16,21\} - 14 = \{9,16,21\}$
- N_{14}에서 N_{20}으로 위장 패킷을 전송할 때의 위장 범위

  $SR_{14}(N_{20}) = NNT_{20} - N_{14} = \{14,19,21,26\} - 14 = \{19,21,26\}$

개별적인 현재 수신 노드 N_C에 대한 N_A의 위장 범위는 다음과 같이 일반화 할 수 있다.

$$SR_{NA}(N_C) = NNT_c - N_A$$

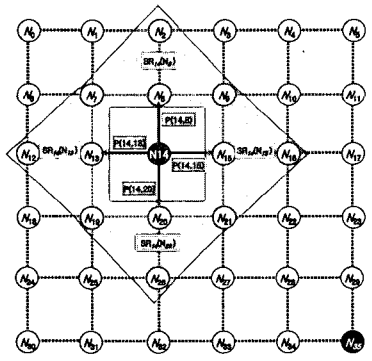
N_A가 위장할 수 있는 전체 수신 노드에 대한 N_A의 위장 범위는 다음과 같이 일반화 할 수 있다(〔그림 7〕).

$$SR_{NA}(\{N_C\}) = \bigcup_{c \in NNT_A} SR_{NA}(N_C) - N_A$$

즉, $SR_{14}(\{N_C\}) = \bigcup_{c \in NNT_{14}} SR_{14}(N_C) - \{14\}$

$= \{2,7,9\} \cup \{7,12,19\} \cup \{9,16,21\} \cup \{19,21,26\}$

$= \{2,7,9,12,16,19,21,26\}$



〔그림 7〕공격자 노드 N14의 전체 위장 범위

공격자 노드는 패킷의 위장범위가 자신을 제외한 35개의 노드에서 8개의 노드로 제한된다. 즉, 위장의 범위가 23%내의 노드로 제한되므로 공격의 파급효과가 네트워크의 생존성에 미치는 범위도 매우 작아짐을 확인할 수 있다. 〔표 4〕는 구성 노드 수를 6x6에서 nxn로 증가시켰을 때의 위장영역 비율을 계산한 표이다. 공격자 노드가 위장 가능한 노드 수는 상수 값(8)으로 고정되므로 전체 네트워크의 구성 노드 수가 증가하게 되면 위장영역 비율이 상대적으로 작아지며, 충분히 n이 클 경우 위장영역 비율은 무시할 수준까지 도달하므로 전체 네트워크 관점에서 생존성 및 가용성의 향상을 기대할 수 있다.

〔표 4〕 구성 노드에 대한 위장영역 비율

구성 노드 수(n)	위장노드 수	위장영역 비율
36(6x6)	8	8/36≒0.23
49(7x7)	8	8/49≒0.16
64(8x8)	8	8/64≒0.13
81(9x9)	8	8/81≒0.099
. . .	. . .	. . .
225(15x15)	8	8/225≒0.035
. . .	. . .	. . .
n($\sqrt{n} \times \sqrt{n}$)	8	8/n≒0

4.5.3 제안 메커니즘의 성능 검증

4.5.3.1 노드별 전력 소모율 계산

본 절에서는 4.5.3절의 공격 시나리오를 기준으로 제안된 메커니즘의 성능 및 효율성을 검증한다. 제 3 장에서 증명했듯이 공격자 노드가 희생자 노드를 목표로 위장 패킷을 대량으로 플러딩하는 경우 기존의 라우팅 프로토콜에서는 무조건적으로 주위의 노드로 수신된 패킷을 전파하며, 그 결과 중간 경로상의 노드들의 전력 소모를 극대화하여 네트워크 생존성에 치명적인 현상을 초래하였다.

근거리 무선 데이터 통신 기술은 블루투스, IEEE802.11, Home RF 및 IrDA가 있으며 상호 경쟁적인 관계이나, 현재 블루투스가 가장 앞서나가고 있는 상황이다. 예를 들면 세계 이동통신 시장의 40% 이상을 차지하고 있는 Ericson과 Nokia 2개사가 적극적으로 탑재할 것임을 명확히 하고 있다[23]. 이와 같은 4개 무선 데이터 통신 기술별로 요구되는 전력 소모를 비교하면 〔표 5〕와 같다.

〔표 5〕 무선 이동통신 기술의 전력소모 비교

방식명	Bluetooth	IEEE802.11	Home RF	IrDA
최대 소비 전력 및 전류	송신 : 30 mA 대기 : 0.3 mA	최대 1watt 정도	미공개	수 mA

패킷 1개당 노드의 전력소모 비율은 일반적으로 수신 보다 송신의 소모가 높게 나타난다. 다음과 같이 패킷 송수신 시 요구되는 전력 소모 요소를 다음과 같이 가정한다.

- $Power$(tx):송신 소모 전력(transmit power)
- $Power$(rx):수신 소모 전력(receiving power)
- $Power$(rc):라우팅 처리 전력 소모(routing computation power)

휴대 단말기의 경우 일반적 전력 소모 계산은 다음과 같다.

$Power(rx) = V \cdot (I_{modem} + I_{RX})$,

$Power(tx) = V \cdot (I_{modem} + I_{TX} + I_{PA})$

V는 요구되는 전압이며, I_{modem}은 모뎀에서 요구되는 전류, I_{RX}는 수신시 요구되는 전류, I_{TX}는 송

신시 요구되는 전류, I_{PA}는 송신시 동작하는 파워 앰프에 요구되는 전류이다. 최적의 통신 환경을 가정했을 때 V를 $3.3V$, I_{modem}을 $100mA$, I_{RX}와 I_{TX}는 $30mA$, I_{PA}를 $60mA$로 적용할 수 있으며, 이때의 $Power$(rx)와 $Power$(tx) 값은 다음과 같다.

$Power(rx) = 3.3\cdot(100+30) = 429mW$

$Power(tx) = 3.3\cdot(100+30+60) = 627mW$

단말기와 기지국간의 거리가 멀어지거나 통신 환경이 열악하게 되면 송신 출력을 높이기 위해 파워 앰프 전류 I_{PA}를 증가시킨다. I_{PA}값이 $100mA$일 때 $Power$(tx)는 $759mW$, I_{PA}값이 $200mA$일 때 $Power$(tx)는 $1,089mW$, I_{PA}값이 $300mA$일 때 $Power$(tx)는 $1,419mW$, I_{PA}값이 $450mA$일 때는 일반적으로 최대 기지국과 송신하기 위한 최대 전류로 볼 수 있으며 이때 $Power$(tx)는 $1,914mW$이다.

$Power$(rc)는 노드에서 필요한 연산을 수행하는데 요구되는 전력소모량으로써 최근 하드웨어 기술의 발전으로 연산에 소요되는 전력은 무시할 만한 수준이며 패킷 송수신에 비해서는 상대적으로 매우 작다. 각 요소별 상대적 크기를 다음과 같이 가정할 수 있다.

$Power(tx) = a\cdot Power(rx),\ (1.5\le a\le 3),\ Power(rc) \ll Power(rx)$

제안된 메커니즘은 다음과 같은 동작이 요구되므로, 노드별로 다음과 같은 추가 전력 소모 요인이 발생한다.

- $Power$(nu) : 주기적 NNT 갱신(update)
- $Power$(pc) : 패킷 재구성(packet reconstruct- ion)
- $Power$(fc) : 위장 패킷에 대한 식별 및 차단 (filtering capability)

전력 소모 측면에서 보면 $Power$(pc), $Power$(fc)는 $Power$(rc)의 일부로써 무시할만한 수준이며, $Power$(nu)는 NNT의 갱신 주기에 따라 전력 소모의 증가 요인이 될 수 있다. 이때 $Power$(nu)에 요구되는 전력 소모는 다음과 같다.

$Power(nu) = Power(tx) + Power(rx)$

전력 소모율을 계산하기 위해 다음과 같은 가정을 둔다.

- $Power(tx) = a\cdot Power(rx) = 2\cdot Power(rx),\ (a=2, Power(rx)=\boldsymbol{w})$
- $PoN_{old}(N_i)$: 제안된 메커니즘 적용전 노드 N_i의 전력 소모량
- $PoN_{new}(N_i)$: 제안된 메커니즘 적용후 노드 N_i의 전력 소모량

[그림 3]에서 공격 노드인 N_{14}가 N_{35}를 공격하는 상황을 가정하고, N_{14}는 자신을 제외한 노드를 소스로 위장하여 순차적으로 증가하는 것을 가정한다. 즉, 소스 주소는 N_{14}(공격자 자신), N_{35}(희생자), N_{14}의 이웃노드(N_8, N_{13}, N_{15}, N_{20})을 제외한 30개의 주소가 위장된 패킷을 생성하여 주위로 전파한다. N_{14}의 주위 노드인 N_8, N_{13}, N_{15}, N_{20} 노드는 무조건 패킷을 수신하여 주변의 노드로 재전파하게 되며, 30개의 패킷에 대해 다음과 같은 전력 소모가 발생하게 된다.

$$PoN_{old}(N_8) = 30\cdot(Power(rx)+Power(tx)+Power(rc))$$
$$= 30\cdot\boldsymbol{w}+30\cdot(2\cdot\boldsymbol{w})+30\cdot Power(rc)$$
$$\fallingdotseq 90\cdot\boldsymbol{w}$$

N_{13}, N_{15}, N_{20}의 경우도 동일한 전력 소모가 예상된다. 제안된 메커니즘의 위장 패킷 탐지 및 차단 능력을 노드에 적용하였을 경우 다음과 같은 에너지 소모가 발생한다. 수신된 패킷 30개중에서 N_{14}의 이웃노드인 N_8, N_{13}, N_{15}, N_{20}의 이웃 노드 8개에 대해서만 정상 패킷으로 식별하여 전송하게 된다.

$$PoN_{new}(N_8) = 30\cdot Power(rx)+8\cdot Power(tx)+30\cdot Power(rc)+1\cdot Power(nu)$$
$$=30\cdot\boldsymbol{w}+8\cdot(2\cdot\boldsymbol{w})+30\cdot Power(rc)+(Power(tx)+Power(rx)) \fallingdotseq 53\cdot\boldsymbol{w}$$

여기서 노드들의 라우팅 연산, 패킷 재구성, 위장 패킷 탐지 및 차단 등은 전력 소모 측면에서 무시할

만한 수준에 있으므로 제외하는 것으로 가정한다. 제안된 메커니즘의 전력 소모 감소율은 70%의 개선 효과를 볼 수 있다.

$$PoN_{old}(N_8)/PoN_{new}(N_8) = 1.7$$

전체적으로 위장 패킷을 제한하여 주위의 노드로 전파하므로 주위의 노드인 N_9의 경우 다음과 같이 더 효율적인 전력 소모를 하게 된다.

$$PoN_{old}(N_9) = 90 \cdot Power(\mathrm{rx})$$
$$PoN_{new}(N_9) = 8 \cdot Power(\mathrm{rx}) + 8 \cdot Power(\mathrm{tx}) + 30 \cdot Power(\mathrm{rc}) + 1 \cdot Power(\mathrm{nu})$$
$$= 8 \cdot \boldsymbol{w} + 8 \cdot (2 \cdot \boldsymbol{w}) + 30 \cdot Power(\mathrm{rc}) + (Power(\mathrm{tx}) + Power(\mathrm{rx})) \fallingdotseq 23 \cdot \boldsymbol{w}$$
$$PoN_{old}(N_9)/PoN_{new}(N_9) = 3.9$$

결과적으로 공격자의 이웃 노드들에 비해 중간 경로상의 노드들의 전력소모 효율이 더 높게 나타난다. 즉, 3 장에서 증명한 결과인 DoS 등의 위장 공격으로 인한 무선 Ad hoc 네트워크의 생존성 문제점을 개선할 수 있다. 반면에 *NNT* 최신 정보 유지를 위한 주기적 갱신 및 패킷 재구성에 요구되는 지연 시간 등의 정확한 적용 연구가 요구된다.

4.5.3.2 DoS 위장 공격에 대한 성능 분석

〔표 6〕은 기존 DSR 라우팅 프로토콜을 적용했을 때, 각 노드별로 예상되는 에너지 잔존량과 제안된 메커니즘을 기존 라우팅 프로토콜에 적용했을 때를 가정하여 예상되는 에너지 잔존량을 비교한 결과이다. 고정된 위상이 임의의 위상에서보다 에너지 향상 비율이 상대적으로 높게 나타났다. 그 이유는 고정된 위상은 각 노드의 전송 범위가 지속적으로 유지되므로 생성된 패킷 전부가 네트워크에 유통되므로 상대적으로 임의의 위상에서 보다 공격에 대한 효율성이 높게 나타났다는 것을 알 수 있다.

〔표 7〕은 TCP throughput의 경우에도 유사한 결과를 보여주고 있다. 고정된 위상일 때가 임의의 위상일 때보다 성능향상이 높음을 알 수 있다. 이와 같은 이유는 에너지 잔존량일 때의 경우와 유사하다.

〔표 6〕 제안 메커니즘 적용 전/후 에너지 잔량 비교

	노드 간격 (m)	경과 시간 (초)	노드 구분	제안 메커니즘 적용전 노드 평균 에너지 잔량(Joul)	제안 메커니즘 적용후 노드 평균 에너지 잔량(Joul)	에너지 잔량 향상률
고정된 위상	200	100	전체 노드	76.42	79.26	3.7%
			공격노드 제외	75.82	78.92	4.1%
			공격노드 주위	84.17	86.32	2.6%
		150	전체 노드	41.17	58.71	42.6%
			공격노드 제외	41.09	60.23	46.6%
			공격노드 주위	45.67	69.06	51.2%
	100	100	전체 노드	33.05	50.67	53.3%
			공격노드 제외	32.63	51.85	58.9%
			공격노드 주위	35.67	53.50	50.0%
		150	전체 노드	2.42	25.08	937.6%
			공격노드 제외	2.55	27.26	971.1%
			공격노드 주위	6.33	33.00	421.1%
임의의 위상	200	100	전체 노드	25.71	43.58	69.5%
			공격노드 제외	26.87	46.36	72.5%
			공격노드 주위	41.78	53.07	27.0%
		150	전체 노드	19.29	32.68	69.5%
			공격노드 제외	26.87	34.77	29.4%
			공격노드 주위	31.34	53.07	69.3%
	100	100	전체 노드	56.47	64.97	15.0%
			공격노드 제외	57.95	67.57	16.6%
			공격노드 주위	56.53	66.05	16.8%
		150	전체 노드	33.42	50.44	50.9%
			공격노드 제외	35.76	55.02	53.9%
			공격노드 주위	35.27	50.04	41.9%

〔표 7〕 제안 메커니즘 적용 전 · 후 throughput 비교

	노드 간격 (m)	제안 메커니즘 적용전 평균 throughput			제안 메커니즘 적용후 평균 throughput			throughput 향상 비율		
		Type1	Type2	Type3	Type1	Type2	Type3	Type1	Type2	Type3
고정된 위상	100	0.228	0.157	0.022	0.289	0.204	0.089	26.6%	30.3%	306.4%
	200	0.118	0.031	0.000	0.162	0.080	0.117	37.0%	162.0%	∞
임의의 위상	100	0.065	0.016	0.000	0.075	0.040	0.025	15.8%	151.6%	∞
	200	0.115	0.068	0.045	0.127	0.076	0.051	10.0%	13.0%	13.8%

V. 결 론

이동성이 빈번한 Ad hoc 네트워크 구조에서 인증 및 암호를 적용하기 위해서는 키 인프라구조가 요구되므로 자원이 제약되고 위상변화가 빈번한 무선 Ad hoc 네트워크에 적용하는 것은 현실적으로 어려움이 많이 있다.

본 논문에서는 무선 Ad hoc 네트워크의 많은 보안 분야 중에서 대량의 위장 패킷 공격으로 인해 네트워크 자체의 생존성 및 가용성에 문제가 있음을 제기하였으며, 유선 네트워크와 달리 공격 대상이 되는 희생자 노드가 생존성 및 가용성에 문제가 발생하기 이전에 중간 경로상의 노드들의 배터리 전력 소모가 급격히 발생하는 현상을 시뮬레이션 실험을 통해 증명하였다.

또한, 앞에서 살펴본 보안 라우팅 프로토콜, 침입 탐지 및 차단 등과 같은 기존의 연구들에서 해결하지 못한 한계점을 극복하기 위해 위장 패킷의 발생 범위를 제한하며, 중간 경로상에 유통되는 위장 패킷을 검출하여 전송을 방지하고 각 노드의 자원 소모를 최대한 감소시킴으로써, 네트워크 전체의 생존성을 향상시킬 수 있는 효율적인 위장 공격 방지 메커니즘을 제안하였다.

본 논문에서 제안한 메커니즘은 기존의 보안 라우팅 프로토콜, 침입 탐지 및 차단에 비해 생존성 강화 측면에서 효율적인 성능을 보여주는 반면에, 패킷 구조에 새로이 부가된 *NNT*, *NoRcvNodeList*의 유지를 위한 오버헤드가 존재한다. 또한 제안된 메커니즘은 기존의 라우팅 프로토콜의 변경을 요구하므로, 변경된 라우팅 프로토콜의 성능보장 및 추가적으로 요구되는 오버헤드를 최소화 할 수 있는 연구가 수행되어야 할 것으로 예상된다.

참 고 문 헌

[1] C-K Toh, "Ad hoc Mobile Wireless Networks", Prentice Hall PTR 2002.

[2] Levente Buttyan, Jean-Pierre Hubaux, "Report on a working session on security in wireless Ad hoc networks", *ACM SIGMOBILE Mobile Computing and Communications Review*, Volume 7 Issue 1, January 2003.

[3] Soonjwa Hong, Seung Hyong Rhee, Jae-Cheol Ryou, "Simulation-Based Analysis of DoS Attacks in Wireless Ad hoc Networks", *IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS*, Vol.E87-D No. 10 pp. 2415-2418, October 2004.

[4] A. Wood and J. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, pp. 48-56, Oct. 2002.

[5] P. Michiardi and R. Molva, "Simulation- based analysis of security exposures in mobile Ad hoc networks," *European Wireless Conference*, Feb. 2002.

[6] P. Kyasanur and N. Vaidya, "Diagnosing and penalizing MAC layer misbehavior in wireless networks," *Technical Report, Dept. of ECE, UIUC*, Dec. 2002.

[7] The CMU Monarch project's wireless and mobility extensions to ns, Snapshot Release 1.1.1, Carnegie mellon University, Aug. 1999.

[8] HyoJun Lim, Chong-kwon Kim, "Flooding in Wireless Ad hoc Networks", *Computer Communications*, Vol. 24, February 2001.

[9] Manel, G.Z., "Secure Ad hoc On-demand Distance Vector Routing", *IETF internet Draft draft-guerrero-manet-saodv-00.txt (work in progress)*, 2001.

[10] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *In Proceedings of the 8th annual international conference on Mobile computing and networking*, pp. 12-23.ACM Press, 2002.

[11] Y.-C. Hu, D. B. Johnson, and A. Perrig. "Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks", *In Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*, page 3, 2002.

[12] U. Lu, B.; Pooch. "Cooperative security-enforcement routing in mobile ad hoc networks", *Mobile and Wireless Communications Network*, 2002.

[13] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. *In Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 275-283, ACM Press, 2000.

[14] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasit-tiporn, J. Rowe, and K. Levitt. "A specification-based intrusion detection system for aodv", *In Proceedings of the 1st ACM workshop on Security of Ad hoc and sensor networks*, pp. 125-134, ACM Press, 2003.

[15] Amin Vahdat, Alvin Lebeck, Carla Schlatter Ellis, "Every joule is precious: the case for revisiting operating system design for energy efficiency", *Proceedings of the 9th workshop on ACM SIGOPS European workshop*, September 2000.

[16] Sung Park, Mani B. Srivastava, "Dynamic battery state aware approaches for improving battery utilization", *Proceedings of the 2002 international conference on Compilers, architecture, and synthesis for embedded systems*, October 2002.

[17] Mathias Bohge, Wade Trappe, "An authentication framework for hierarchical ad hoc sensor networks", *Proceedings of the 2003 ACM workshop on Wireless security*, September 2003.

[18] Andre Weimerskirch, Dirk Westhoff, "Identity certified authentication for ad-hoc networks, *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, October 2003.

[19] He Huang, Shyhtsun Felix Wu, "An approach to certificate path discovery in mobile Ad Hoc networks", *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, October 2003.

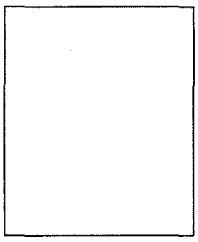
[20] Jim Binkley, William Trost, "Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems", *Wireless Networks 7*, pp. 139-145, 2001.

[21] Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei, "Random key-assignment for secure Wireless Sensor Networks", *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, October 2003.

[22] D. B. Johnson, D. A. Maltz, and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks(DSR)", *IETF MANET Working Group Internet draft*, July 2004.

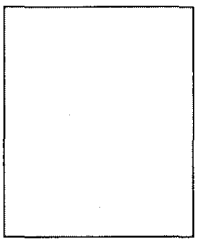
[23] 박용우, "블루투스 기술발전에 따른 국내기업의 대응전략", 정보통신정책, 제13권 14호 통권283호, pp. 1-26, 2002년 8월.

〈著者紹介〉



홍 순 좌 (Soonjwa Hong) 정회원

1989년 2월:숭실대학교 전자계산학과 졸업
1991년 2월:숭실대학교 전자계산학과 석사
2005년 2월:충남대학교 컴퓨터과학과 박사
1991년~2000년:국방과학연구소 선임연구원
2000년~현재:국가보안기술연구소 팀장/선임연구원
<관심분야> 컴퓨터 보안, 유/무선 통신 보안



박 현 동 (Hyun-dong Park) 정회원

1995년 2월:충남대학교 컴퓨터과학과 졸업
1997년 2월:충남대학교 컴퓨터과학과 석사
1997년 2월:충남대학교 컴퓨터과학과 박사
2000년~2002년 국가보안기술연구소 선임연구원
2002년~2004년:대덕대학 전임강사
2004년:충남대학교 전기정보통신공학부 연구교수
<관심분야> 무선LAN/PAN, 무선네트워크 및 보안