情 報 保 護 學 會 誌
第 14 券 第 1 號, 2004. 2

유비쿼터스 네트워크에서 서비스 거부(Denial of Service) 공격의 특성 및 위험성 분석

이 병 주*, 홍 순 좌**, 이 승 형*

요 약

미래 유비쿼터스 컴퓨팅 환경의 네트워크 인프라 구축을 위한 핵심기술은 무선 ad hoc 네트워크이다. 이러한 ad hoc 네트워크에 대한 보안은 일반 네트워크와 마찬가지로 보안성, 무결성, 가용성 등이 요구되지만, 일반적으로 무선 네트워크라는 점, 고정 인프라가 없다는 점, 네트워크 토폴로지가 수시로 변한다는 점 등 때문에 보안문제는 훨씬 어려운 것으로 인식되고 있다. 본 논문에서는 보안 요구사항 중에서 가용성에 중점을 두어, 일반 네트워크와는 다른 유비쿼터스 네트워크에서의 DoS 공격의 여러 가지 유형을 분석한다. 또한 이러한 DoS 공격이 유비쿼터스 네트워크에 미치는 영향을 컴퓨터 시뮬레이션을 통해 전송성능과 생존성의 측면에서 분석한다. 본 논문의 실험결과는 같은 유형의 DoS 공격이더라도 무선 ad hoc 네트워크가 일반적인 네트워크에 비해 더 심각한 피해를 당할 수 있음을 보여준다.

Ⅰ. 서 론

미래 유비쿼터스 컴퓨팅 환경의 네트워크 인프라 구축을 위한 핵심 기술로 인식되고 있는 무선 ad hoc 네트워크는 고정의 인프라 네트워크 없이 무선의 이동 단말들이 동적으로 multi-hop 연결을 구축할 수 있는 기술이다. 이 ad hoc 네트워크는 두 개 이상의 이동 무선 단말이 각자 스스로 다른 단말과의 교신에 의해서 임시 네트워크를 구성하여 통신을 하거나 다른 패킷을 교환 혹은 전달할 수 있는 네트워크를 말한다[1]. 무선 ad hoc 네트워크의 대표적인 용도로는 전술환경에서의 군용 무선이동통신 시스템 구축과 가전 및 무선이동 단말간의 홈 네트워크 구축 등을 들 수 있다. 또한, 환경 감시, 생태계 관찰, 자연재해 예방, 그리고 ITS (Intelligent Transport System) 등에 적용이 활발히 추진되고 있는 센서(sensor) 네트워크 기술도 역시 ad hoc 네트워크의 특수한 경우로 볼 수 있다. 따라서 미래의 유비쿼터스 컴퓨팅 환경은 이러한 ad hoc 네트워크, 센서 네트워크 및 무선 네트워크가 결합하여 네트워크 인프라를 제공하게 될 것이다.

유비쿼터스 컴퓨팅을 향한 새롭고 다양한 어플리케이션이 등장하고 실험되기 시작하면서, 무선 ad hoc 네트워크의 보안 및 프라이버시 메커니즘에 대한 연구와 개발이 최근 들어 매우 활발하게 시작되고 있다. 무선 ad hoc 네트워크는 기존의 네트워크와는 여러 가지의 다른 특성들이 있어서, 일반적으로 보안 메커니즘의 설계가 어려운 것으로 평가되고 있다. 예를 들어, 무선 ad hoc 네트워크의 특징들은 각 노드들이 수시로 이동을 하므로 네트워크 토폴로지가 동적으로 변하게 되고, 모든 모드가 무선으로 전송을 하며 다른 노드에 독립적이며, 노드들은 한정된 배터리에 의해 동작하므로 네트워크의 각종 프로세스에 비협조적(non-cooperative)이 될 수 있다는 점등이다. 이러한 특성을 가진 ad hoc 네트워크에서의 보안 요구사항은 일반 네트워크와 마찬가지로 보안성, 무결성, 부인방지, 가용성 등이 있으며, 최근에 들어서 이러한 문제들에 대한 연구가 시작하는 단계에 있다.

본 논문에서는 이러한 보안 요구사항 중에서 가용성에 초점을 맞추어서 유비쿼터스 네트워크에서 발생

* 광운대학교 전자공학부({bjlee, shr}@kw.ac.kr)
** 국가보안기술연구소 선임연구원/팀장(hongsj@etri.re.kr)

할 수 있는 DoS(Denial of Service) 공격의 여러 가지 유형에 대해 분석하고, 이러한 공격이 네트워크의 전송성능과 생존성, 즉 가용성에 미치는 영향을 컴퓨터 시뮬레이션을 이용하여 평가한다. 무선 ad hoc 네트워크는 앞서 언급한 바와 같이 기존의 다른 네트워크와는 상이한 특성들을 가지고 있으므로, 새로운 유형과 내용의 DoS 공격이 가능해지며, 이러한 공격이 네트워크에 미치는 영향 또한 기존 네트워크의 경우와 상이하게 된다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 무선 ad hoc 네트워크에서의 특성 및 이에 따른 보안 요구사항을 분석하고, 이어 Ⅲ장에서는 무선 ad hoc 네트워크에서 발생할 수 있는 DoS 공격의 유형 및 이들의 특성에 대해 조사한다. Ⅳ장의 1절에서는 컴퓨터 시뮬레이션을 이용하여 무선 ad hoc 네트워크에서 DoS 공격이 발생하는 경우에 각 노드들과 전체 네트워크에 미치는 영향을 평가하고 기존 네트워크의 경우와의 차이점에 대해 분석한다. 2절에서는 mobile환경에서 같은 실험을 통해 DoS 공격의 영향을 측정하고 분석한다. 끝으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. Ad Hoc 네트워크 보안

1. Ad Hoc 네트워크의 보안 특성

무선 ad hoc 네트워크에 대한 보안은 다음과 같은 면에서 기존의 네트워크 보안 보다 어려운 문제로 인식되고 있다[2,3,5]. 먼저, 일반적으로 무선 네트워크는 유선의 경우보다 보안에 취약하며, 이러한 무선 네트워크에 대한 공격은 수동적인 도청에서부터 능동적으로 신호 간섭을 일으키거나 시스템의 동작을 방해하는 여러 가지 유형이 있을 수 있다. 하나의 이동 노드가 ad hoc 네트워크에서 다른 노드들에 대해 능동적으로 공격을 하는 경우에, 다음에 언급할 많은 보안 요구사항들, 즉, 비밀성, 무결성, 가용성 등이 심각하게 위협받을 수 있다. 두 번째로, 무선 ad hoc 네트워크는 infrastructure가 없으며, 네트워크 노드들 사이의 관계가 매우 동적이고 일시적이므로, 노드들 사이의 보안 메커니즘의 설계가 어렵다. 즉, 무선 ad hoc 네트워크는 유선 네트워크의 방화벽과 같은 명확한 방어선이 없으므로, 모든 노드가 직간접적인 공격에 대비하는 메커니즘이 설계되어야 한다. 한편으로 많은 경우에 무선 ad hoc 네트워크는 이러한 분산 구조를 갖는 것이 생존성(survivability)을 높일 수 있다. 예를 들어, 전장과 같은 적대적인 지역에 네트워크가 배치되는 경우에 해킹을 당하거나 물리적으로 공격을 받을 위험이 매우 높다. 따라서 이러한 경우에 중앙 관리 방식의 네트워크에서는 중앙 노드에 대한 해킹은 네트워크 전체에 문제를 야기한다.

세 번째로, 무선 노드들이 지속적으로 이동 하므로, 네트워크의 토폴로지와 노드들 간의 연결성이 수시로 변화한다. 그러므로 예를 들어 어떤 노드가 해킹당한 것으로 판명되는 경우에 이동하는 노드들 간의 신뢰관계도 동적으로 변하게 된다. 일반적으로 이동 노드들은 여러 ad hoc 네트워크에 수시로 가입과 탈퇴를 하므로, 이러한 네트워크에서의 보안 메커니즘은 이러한 점을 고려하여 동적으로 설계되어야 한다. 또한, 어떤 노드가 해킹을 당하는 경우에 큰 규모의 ad hoc 네트워크에서 이 노드를 추적하기는 매우 어려우므로, 모든 노드는 기본적으로 다른 노드에 대한 신뢰 없이 동작할 수 있어야 한다.

2. Ad Hoc 네트워크의 보안 요구사항

무선 ad hoc 네트워크에 대한 보안 요구사항은 일반적인 다른 네트워크와 다르지 않다. 즉, 일반적인 보안 시스템에서 고려하여야 하는 인증 (authentication), 비밀성 (confidentiality), 무결성 (integrity), 부인방지(non-repudiation), 접근통제(access control) 및 가용성(availability) 등이 무선 네트워크에서 마찬가지로 보장되어야 하는 보안 요구사항들이다. 먼저 인증은 통신을 하고자 하는 상대 노드의 신분을 확인하는 것인데, 이러한 인증이 필요한 경우에, 예를 들면 CA의 역할을 노드가 있어서 이를 확인해 주어야 한다. 그러나 무선 ad hoc 네트워크에서는 infrastructure의 부재와 노드들 사이의 일시적이고 동적인 관계로 인하여 이러한 인증이 매우 힘들게 된다[4].

비밀성(confidentiality)은 특정 정보가 비인가자에게 누출되지 않도록 하는 것으로써, 이는 ad hoc 네트워크에서 매우 중요한 요소가 될 수 있다. 예를 들어, 군사적인 목적으로 ad hoc 네트워크가 사용되어 전장에 적용이 된다면, 전략적 혹은 전술적 군사기밀들에 대한 비밀은 통신 중에 철저히 유지 되어야 하며, 또한 라우팅 정보 역시 철저한 비밀이 요구되는데, 이는 그 정보가 네트워크의 구성 및 각 이동 노드의 위치를 알려줄 수 있기 때문이다. 또한, 홈 네트워크의 구축에 ad hoc 네트워크가 적용되는 경우에는 개인의 사생활 정보가 외부로 유출되지 않도록 보장이

되어야 한다. 무결성(integrity) 역시 마찬가지 관점에서 전장, 홈 네트워크, 센서 네트워크 등의 ad hoc 환경에서 자료의 불법적인 변경이 불가능하도록 하도록 보장되어야 한다. 부인방지(non-repudiation)는 데이터의 송신자가 전송사실을 부인하지 못하도록 하는 것인데, 이는 ad hoc 네트워크에서 해킹을 당한 노드를 식별하는데 다음과 같이 적용될 수 있다[5]. 만일 노드 A가 노드 B로부터 에러가 있는 메시지를 받았는데 노드 B가 이를 보낸 사실을 부인한다면, 노드 A는 노드 B가 해킹 당한 것으로 판단하고 이 사실을 다른 이동 노드들에게 알려서 네트워크에서 분리를 시킬 수 있다.

마지막으로 가용성(availability)은 서비스 거부(DoS: Denial of Service) 공격에 대하여 네트워크의 생존성을 유지하는 것으로써, 본 논문에서 집중적으로 분석하고자 하는 무선 ad hoc 네트워크의 보안 요구사항이다. 무선 네트워크에서의 DoS 공격은 다양한 계층에서 이루어질 수 있다. PHY와 MAC에서는 재밍(jamming) 이나 불법적인 프레임의 송신으로 다른 이동 노드들의 통신을 방해하고, 전송률을 저하시키거나, 에너지를 고갈시킬 수 있다. 특히 무선 이동 노드들은 일정량의 배터리에 의존하기 때문에 다른 노드들의 에너지 절약 모드를 방해하거나 불필요한 전송에 의해 서버노드 및 중간 노드들의 에너지를 고갈시키는 것은 매우 큰 문제로 인식되고 있다[6]. 네트워크 계층에서는 ad hoc 라우팅 정보를 조작 혹은 변조하거나 패킷의 전달을 거부하는 등의 방법으로 네트워크 전체의 성능을 크게 저하시킬 수 있다. 상위 계층의 경우에도 응용 프로그램 등을 공격함으로써 시스템의 서비스를 마비시킬 수 있다.

Ⅲ. Ad Hoc 네트워크에서 DoS 공격 유형

앞장에서 논의한 바와 같이, ad hoc 네트워크에 대한 DoS 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[7,8,9,10]. 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 등은 이전의 네트워크에서는 불가능하거나 무의미했던 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 방법에 의해 특정 노드의 에너지를 고갈시켜서 서비스가 불가능하도록 할 수도 있다.

〔표 1〕 무선 ad hoc 네트워크에서 DoS 공격 유형의 분류

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

무선 ad hoc 네트워크에서의 DoS 공격은 적극적인 공격과 수동적인 비협조의 두 가지 형태로 분류할 수 있다. 여기에서 적극적인 공격이란, 라우팅 메커니즘이나 MAC 프로토콜을 이용하여 다른 노드들에게 잘못된 정보를 전파하거나 혹은 불필요한 트래픽을 발생시키는 등의 방법으로 네트워크 전체의 성능 및 가용성을 급격히 저하시키는 유형의 DoS 공격을 의미한다. 한편, 이동 노드가 라우팅 정보의 전달과 공유에 참여하지 않거나, 혹은 MAC 프로토콜의 access 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. 이 장에서는 이러한 두 유형의 DoS 공격에 대해 분석한다.

1. 적극적인 DoS 공격

〔표 1〕에서와 같이 적극적인 DoS 공격은 네트워크 계층과 MAC 계층의 두 경우로 분류할 수 있다. Ad hoc 네트워크의 네트워크 계층에서 가능한 DoS 공격은 예를 들어 다음과 같은 방법이 있을 수 있다.

a) 이동 노드가 특정 전송경로에 참여하여 일부 데이터 패킷을 의도적으로 폐기하면, 특히 TCP를 사용하는 플로우의 경우에는 심각한 전송성

능의 저하를 겪을 수 있다[7].

b) 이동 노드가 거짓 라우팅 정보를 다른 노드에게 전파하면, 패킷의 전송실패가 급증하게 된다.

c) 오래되어 유효하지 않은 라우팅 정보를 replay 하는 경우에도 마찬가지로 급격한 성능의 저하가 올 수 있다.

d) 전달하는 모든 패킷의 TTL의 값을 줄이면 목적지에 가기 전에 폐기된다.

e) 많은 양의 불필요한 패킷을 먼 거리의 목적지로 전송을 하면, 중간의 무선 노드들은 계속되는 패킷의 전달(수신 및 송신)로 인하여 에너지가 고갈되는 현상이 발생할 수 있으며, 이는 네트워크 전체의 가용성과 생존성을 급격히 저하시키게 된다.

위에서 예로 열거한 여러 가지의 공격 유형들은 공통적으로 네트워크에 혼잡(congestion)을 발생시켜서 다른 노드들의 전송을 방해하거나 효율을 저하시킨다. 이는 폐기되거나 잘못 전달된 패킷들의 재전송에 의해 발생할 수 있으며, 특히 마지막의 경우에는 노드들의 에너지가 감소하여 패킷전달을 담당할 충분한 수의 무선 노드가 존재하지 않는 경우에 발생할 수 있다. 이러한 유형의 DoS 공격에 대해서는 다음 장의 시뮬레이션에 의해 그 영향을 분석할 것이다.

두 번째로, MAC 계층에서는 다음과 같은 방법으로 DoS 공격을 수행할 수 있다.

a) 대부분의 무선 ad hoc 네트워크에서는 MAC에서 단일 채널의 사용을 가정하고 있으므로, 어떤 노드가 계속적인 채널 busy 신호를 전송한다면 모든 이웃 노드들은 통신이 불가능하므로, 이는 이 노드들에 대한 강력한 DoS 공격에 해당된다.

b) 특정 노드가 불필요한 프레임을 계속하여 전달하도록 한다면, 해당 노드는 에너지가 고갈되어 통신이 불가능한 상태에 이르게 된다.

이와 같이 MAC 계층에서의 DoS 공격은 이웃 노드들의 통신을 불가능하게 하거나 에너지를 급속하게 고갈시키는 등의 방법으로, 전송 범위 안에 있는 무선 모드들에 대해 행하는 공격이다. 따라서 DoS 공격의 영향은 전체 네트워크의 일부 지역에만 국한되지만, 몇 몇 노드가 네트워크에 잠입하여 MAC 계층 공격을 하는 경우에는 네트워크 계층에서의 공격과 마찬가지로 시스템 전체의 전송 성능을 감소시키고 에너지를 고갈시켜서 가용성을 급속하게 저하시킬 수 있다.

2. 비정상 행위에 의한 간접 DoS 공격

무선 ad hoc 네트워크를 위해 개발된 모든 라우팅 메커니즘 및 MAC 프로토콜은 무선 이동 노드들의 자발적인 협조(cooperation)를 기본적인 가정으로 하고 있다. 예를 들어, ad hoc 네트워크의 한 노드가 자신의 에너지를 절약하기 위하여 라우팅 정보의 전파 혹은 전달을 하지 않는 행위는 네트워크에 직접적인 연향을 끼치지는 않지만 간접적으로 네트워크의 전송 성능을 저해하고 다른 노드들의 에너지 소모를 촉진하는 결과를 낳는다. 또한, IEEE 802.11 MAC 프로토콜의 경우에, 주위에서 RTS(Request to Send)나 CTS(Clear to Send)와 같은 메시지를 받는 경우에는 정해진 시간동안 데이터의 전송을 중단하여야 하는데, 어떤 노드가 이를 무시하고 자신의 데이터를 먼저 전송하기 위해 신호를 전송하면 그 노드 주위에서 다른 노드들은 프레임의 전송이 불가능한 서비스 거부 상태가 되며, 이와 같은 경우도 간접적인 DoS 공격으로 볼 수 있다.

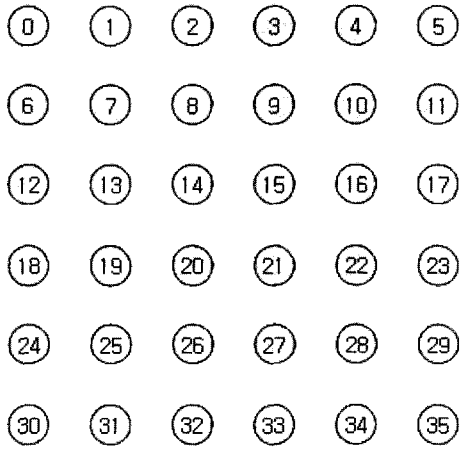
이 중에서 네트워크 계층에서의 비정상 행위는 주로 자신의 에너지를 절약하기 위해서 자신이 속한 네트워크의 라우팅 메커니즘에 비협조적(non-cooperative)으로 행동하는 경우이며, Michiardi와 Molva[9]는 네트워크 계층에서의 비정상행위 노드들을 다음과 같이 두 가지로 분류하였다. 첫째 유형은 에너지 절약을 위하여 자신이 수신자나 송신자가 아닌 모든 데이터 패킷의 전달을 거부하고, 라우팅 정보 수집을 위한 프로세스, 즉 경로 탐색과 경로 유지보수에만 참여하는 노드들이다. 이러한 유형의 노드들은 다른 노드들의 데이터 전송을 하지 않음으로써 자신의 에너지를 절감하게 되나, 이로 인해 다른 노드들의 평균 전송성능 및 효율을 저하시키게 된다. 두 번째 유형은 라우팅 프로세스의 route discovery에도 참여하지 않는 노드들이다. 따라서 다른 노드들은 이 노드의 존재를 모르게 되며, 이로 인해 ad hoc 네트워크 노드들의 경로 탐색에 상당한 지장을 주어서 첫 번째 유형 보다 시스템에 더 심각한 영향을 끼칠 수 있다. 물론 이러한 유형의 노드들은 더 많은 에너지를 절약할 수 있게 된다.

최근에 Kyasanur와 Vaidya[10]은 MAC 계층에서 발생할 수 있는 ad hoc 네트워크 노드들의 비정상 행위를 다음과 같이 예로 들었다. IEEE 802.11 MAC의 경우에 송신자는 RTS 메시지를 전송하고 수

신자가 CTS 메시지로 회신하면, 이 두 노드에 의해 채널이 예약되어 전송이 시작된다. 송신자는 DATA를 보내고 수신자는 즉시 ACK로 확인을 하는데, 이에 성공하면 CW(Congestion Window)의 값을 최소값으로 설정하고, ACK를 받는데 실패하거나 RTS에 대한 CTS의 수신에 실패하면 자신의 CW 값을 두 배로 증가하게 된다. 이 CW 값은 채널이 비는 경우에 누가 먼저 전송을 시작할 수 있는지, 즉 누구의 backoff가 더 작은지를 확률적으로 정해주는 척도이기 때문에, CW 값이 작을수록 데이터를 전송하게 될 확률이 증가한다. 이러한 메커니즘을 악용하게 되면 여러 가지 방법으로 채널을 선점하는 것이 가능해 진다. 예를 들어, ACK나 CTS의 수신 실패 후에도 CW 값을 증가시키지 않거나, 혹은 채널이 비는 경우에 backoff 값을 비정상적으로 작게 설정하게 되면, 다른 노드들에 비해 채널을 사용하게 될 확률이 급격히 증가하며, 이에 따라서 다른 정상 노드들의 전체 전송 성능은 급감하게 되어 DoS 공격의 효과를 낸다.

Ⅳ. DoS 공격의 영향 분석

이 장에서는 앞장에서 논의한 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 wireless subnet 및 ad hoc networking을 위한 새로운 component를 추가한 CMU Monarch extensions[11]을 사용하였다. 먼저 시뮬레이션을 위한 ad hoc 네트워크의 토폴로지는 [그림 1]과 같이 가로 세로 각각 6개씩의 무선 이동노드를 배치하여 실험을 하였다. 36개의 노드 모두 IEEE 802.11 MAC을 사용하고, 라우팅 프로토콜은 DSR(Dynamic Source Routing)을 적용하였다. 노드 사이의 거리는 실험 시나리오에 따라 100m에서 200m까지 가변시켰다. 참고적으로 각 노드의 전송 범위(transmission range)는 반경 250m 씩이다. 1절의 실험은 무선 ad hoc 노드의 위치를 실험 기간동안 변동시키지 않은 고정된 노드의 환경에서 수행한 결과이고, 2절의 실험은 mobile 환경에서 노드가 일정 범위 내에서 이동하는 random topology 환경에서 실험한 결과의 고찰이다.



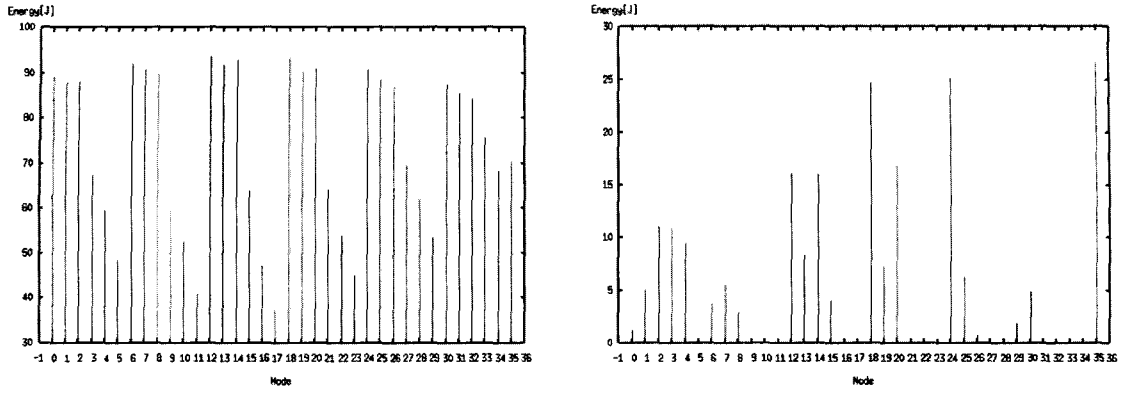
[그림 1] 시뮬레이션 토폴로지

1. 고정된 노드들 사이에서 DoS 공격의 영향

1.1 DoS 공격에 의한 노드 에너지 고갈

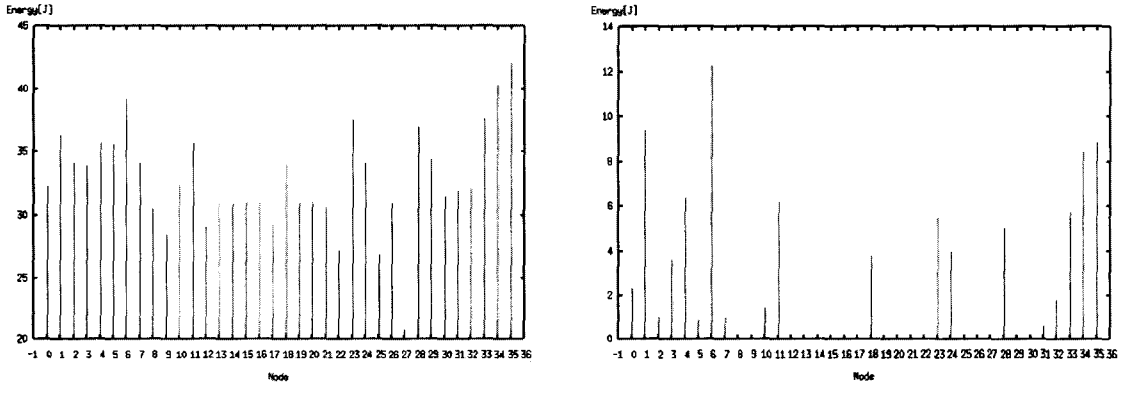
먼저, 3장에서 논의한 적극적인 DoS 공격의 유형 중에서 불필요한 전송에 의한 에너지 감소 효과를 분석한다. 전술한 바와 같이, 많은 양의 불필요한 패킷을 먼 거리의 목적지로 전송을 하면, 중간의 무선 노드들은 계속되는 패킷의 전달(수신 및 송신)로 인하여 에너지가 고갈되는 현상이 발생할 수 있으며, 이는 네트워크 전체의 가용성과 생존성을 급격히 저하시키게 된다. [그림 1]의 ad hoc 네트워크에서 각 모퉁이의 0번, 5번, 30번 노드가 DoS 공격을 수행하는 노드들이고, 이들이 동시에 35번 노드에 대해 UDP 트래픽을 발생하여 전송하도록 하였다. 이는 유선 네트워크에서의 UDP flooding 공격에 해당하는 것이다. 각 노드의 최초 에너지는 100J이고 패킷의 송신에 2watts, 수신에 1watt의 파워가 소모된다고 가정하였다. 이러한 공격의 결과가 다음의 [그림 2]와 [그림 3]에 나타나 있다.

[그림 2]의 경우에는 각 노드들 간의 간격이 각각 200m로 설정하여 시뮬레이션을 수행한 후에 100초 후, 그리고 200초 후에 각 노드에 남아있는 에너지의 양을 측정한 것이다. 노드들의 전송범위가 반경 250m 이므로, 한 노드의 데이터를 전송할 때는 하나의 이웃 노드만이 데이터를 받게 된다. 예를 들어, 0번 노드가 보내는 패킷들은 0-1-2-3-4-5-11-17-23-29-35의 경로를 따라서 전송이 되며, 5번 노드가 보내는 패킷 역시 5-11-17-23-29-35의 경로를 통해 전달이 된다. 그러므로 100초 후의 그래프에서 볼 수 있듯이, 0번 노드가 보내는 패킷과 5번 노드가 보내는 패킷을 모두 송수신 하여야 하는 노드들(5,11,17,23,29번)의 에너지가 다른 노드들에 비하여 급격히 감소하였음을 알 수 있다. 이에 비해, 30번 노드가 공격하는 패



(a) (b)

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



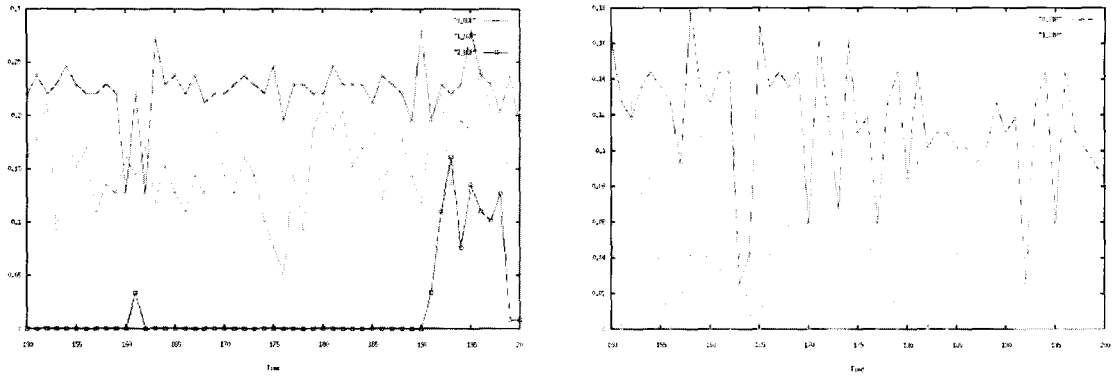
(a) (b)

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

킷의 전송경로 30-31-32-33-34-35에 있는 노드들의 에너지는 상대적으로 많이 남아 있다. 이 ad hoc 네트워크에서 사용하는 DSR 라우팅 메커니즘은 기본적으로 경로 설정과 경로의 유지보수에 패킷의 브로드캐스팅을 적용하기 때문에 전송경로에 상관없는 노드들도 라우팅 프로세스에 의해 에너지가 감소하며, 또한 그에 무관한 노드들이더라도 단순히 이웃 노드의 전파를 수신하는 것에 의해 에너지가 감소한다.

그림에서, 200초 후에는 일부 노드를 제외한 대부분의 노드들의 에너지가 고갈되었음을 나타낸다. 즉, 3개 노드가 특정 노드에 대해 UDP 패킷을 전송하는 DoS 공격을 수행함에 따라서 네트워크 노드들의 에너지가 급감하여 가용성(availability)을 저해하는 효과를 내게 된다. 이는 유선 네트워크에서는 실현이 불가능한 DoS 공격의 효과이다. 즉, 유선 네트워크의 경우에는 공격 대상이 되는 노드가 가장 많은 피해를 보는 것이 일반적이다. 그러나 〔그림 2〕의 실험결과에 의하면 무선 ad hoc 네트워크의 경우에는 공격대상 노드보다 공격자와의 전송경로 상에 있는 노드들의 피해가 훨씬 심각함을 보여주고 있으며, 이는 같은 DoS 공격을 수행하더라도 ad hoc 네트워크의 경우에 더 심각한 피해를 당할 수 있음을 보여주는 것이다.

〔그림 3〕의 경우에는 각 노드들 간의 거리를 100m로 줄여서 같은 내용의 실험을 반복한 결과이다. 노드들 간의 거리가 줄면서 한 노드의 전송범위에 여러 개의 노드가 들어가기 때문에 UDP 패킷의 전송 경로가 〔그림 2〕의 경우처럼 노드의 배열을 따라 직선으로 형성되지 않고, 네트워크를 가로질러서 형성된다. 즉, 네트워크의 모든 노드들이 패킷의 수신과 송신에 참여하게 됨에 따라 100초 후에는 (a)에서 보듯이 거의 모든 노드들이 에너지 감소를 겪게 된다. (b)는 150초 후에 각 노드에 남아있는 에너지를 측정하여 나타낸 그래프인데, 〔그림 2〕의 경우보다 노드들의 에너지가 훨씬 빠른 시간 안에 고갈되었음을 알 수 있다. 이



(a) (b)

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

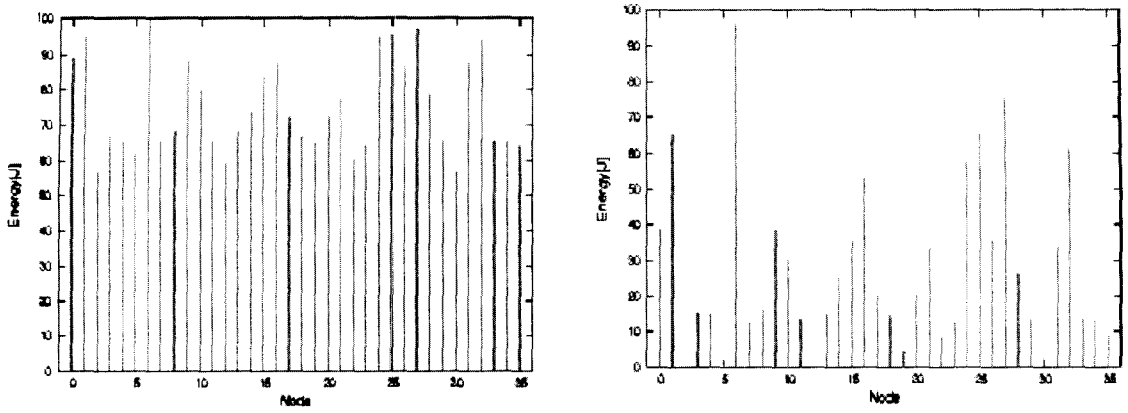
는 노드들 간의 간격이 좁아짐에 따라서 한 노드가 패킷을 전송할 때 영향을 받는 노드의 수가 증가하기 때문이다. 예를 들어, 〔그림 1〕의 토폴로지에서 0번 노드가 패킷을 전송하는 경우에 노드 간격이 200m인 경우에는 1번과 6번의 두 노드만이 이를 수신한다. 그러나 〔그림 3〕의 경우처럼 노드 간격이 100m로 줄어들면 1,2,6,7,8,12,13번의 7개 노드가 패킷을 수신하게 되어, 이들이 패킷을 다시 전송을 안 하더라도 에너지를 소모하게 된다. 이 결과에서 알 수 있듯이, ad hoc 네트워크에서 이동 노드들이 밀집해있거나, 각 노드의 전송반경이 큰 경우에는 이러한 DoS 공격에 의한 피해가 훨씬 심각해진다.

1.2. TCP Throughput 감소

다음으로는 일부 노드들이 DoS 공격을 함에 따라 다른 노드들의 throughput이 어떤 영향을 받는지에 대한 실험이다. 〔그림 1〕의 네트워크에서 5번 노드와 30번 노드가 각각 35번 노드에게 UDP flooding 공격을 하는 동안에 18번 노드가 23번 노드에게 TCP 트래픽을 전송하도록 하였다. (a)에서 세 개의 그래프는 위에서부터 각각 UDP flooding이 없는 경우, 5번 노드만 UDP 패킷을 전송하는 경우, 그리고 5번과 30번 모두 DoS 공격에 참여하는 경우에 대해서 TCP 트래픽의 throughput을 측정한 것이다. UDP flooding이 없는 경우에 비해서 5번 노드가 DoS 공격을 하는 경우에는 TCP의 throughput이 감소함을 알 수 있는데, 이는 TCP 트래픽의 전송경로와 UDP 트래픽의 전송경로가 23번 노드에서 일부 중첩되기 때문에 TCP throughput이 감소하는 것이다. 30번 노드까지 DoS 공격에 가담을 하는 경우에는 TCP 트래픽의 throughput이 심각하게 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. 그림에서 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.

이 실험에서도 마찬가지로 유선 네트워크에서와는 다른 무선 ad hoc 네트워크에서 DoS 공격의 영향을 살펴볼 수 있다. 즉, 유선 네트워크에서는 일반적으로 DoS 공격이 진행되더라도, 이와 다른 전송경로를 사용하는 트래픽의 경우에는 아무런 영향을 받지 않는다. 그러나 〔그림 4〕의 결과에서 보듯이, 무선 ad hoc 네트워크에서는 DoS 패킷들이 전송경로가 다르더라도 다른 트래픽의 throughput에 심각한 영향을 끼침을 알 수 있다. 따라서 같은 형태의 DoS 공격이더라도 유선 네트워크의 경우 보다 무선 ad hoc 네



(a) (b)

〔그림 5〕 DoS 공격에 의한 에너지 소모: 전송범위 250m, (a) 50초 후, (b) 100초 후

트워크의 경우에 네트워크 전체의 전송 성능 및 가용성에 훨씬 심각한 영향을 미침을 알 수 있다.

2. Mobile 환경에서 DoS 공격의 영향

이 장에서는 앞장에서의 시뮬레이션과 동일한 조건하에서 36개의 노드들에 임의의 이동성(random mobility)을 부여하였다. 따라서 시뮬레이션 시간동안 각 노드들은 일정한 범위 내에서 지속적으로 이동하며 토폴로지(topology)를 변화시킨다. 실험 시나리오에서는 노드들의 전송 범위(transmission range)를 150m와 250m로 설정하여 시뮬레이션을 수행하였다. 이 장에서도 앞장에서와 동일하게 적극적인 DoS 공격의 영향을 에너지 감소효과와 throughput의 영향 두 가지 측면에서 살펴본다.

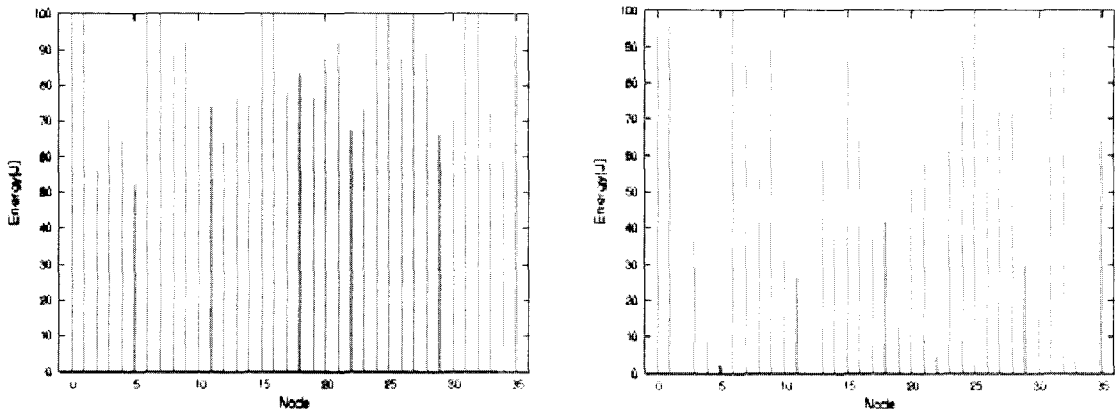
2.1. DoS 공격에 의한 노드 에너지 고갈

이 장에서의 시뮬레이션에서는 2번, 5번, 30번 노드가 UDP 트래픽을 발생하여 DoS 공격을 수행하는 노드들이고, 35번 노드가 DoS의 공격을 받는 노드의 역할을 수행하게 된다. 각 노드들의 최초 에너지는 100J이고 송신에 2Watts, 수신에 1Watt의 파워가 소모된다.

〔그림 5〕의 경우에는 각 노드들의 전송 범위를 250m로 설정하여 시뮬레이션을 수행시키고 50초 후, 100초 후에 각 노드에 남아있는 에너지의 양을 측정한 결과이다. 앞장에서 노드들이 일정한 간격으로 고정되어 있는 경우처럼 송신 노드들에 의해서 생성된 패킷들은 일정한 경로에 놓인 노드를 통해 전송되는 것이 아니라 노드들의 이동에 따라 전송에 참여하는 노드들이 변하게 된다. 따라서 앞 장에서와 같이 일정한 경로에 위치한 노드들의 에너지 고갈이 현저하게 나타나지는 않는다. 에너지의 급격히 고갈은 서로 근접하여 있는 노드들에서 나타난다. 만약 시뮬레이션의 실행과 더불어 다른 노드들과 멀리 떨어진 위치로 이동한 경우에는 패킷을 생성하는 노드의 전송범위를 벗어나 패킷의 전송에 참여하지 못하게 된다.

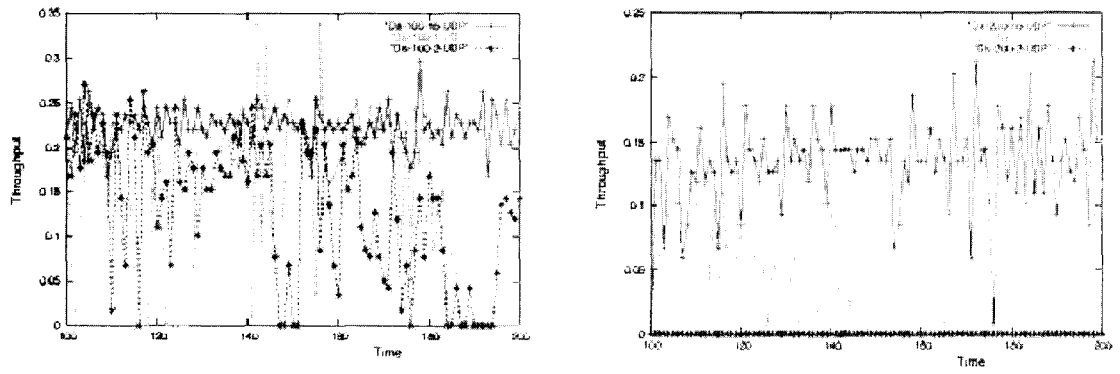
100초 후에는 몇 개의 노드를 제외하고는 대부분 노드들의 에너지가 급격히 감소하였다. 이러한 에너지의 고갈은 노드들을 일정한 거리에 고정하였을 경우보다 더 급격하다. 노드들의 이동성이 제공되면서 노드들의 간격의 변화와 전송에 참여하는 노드들이 변화로 더 급격한 에너지의 고갈과 더 많은 노드들에 영향을 준다. 따라서 이동성이 제공되는 ad hoc 네트워크의 경우 이동성을 제공하지 않는 경우보다 DoS 공격은 더 심각한 피해를 입힐 수 있다.

〔그림 6〕의 경우에는 각 노드들의 전송 범위를 150m로 줄여서 실험을 반복한 결과이다. 전송 범위가 150m로 줄어들면서 패킷의 수신과 송신에 참여할 수 있는 노드의 수가 줄어들게 된다. 50초 후에는 (a)에서 보듯이 에너지의 감소 폭이 작다. 150초 후에 남아있는 에너지의 양을 나타내는 (b)의 그림을 보면, 앞의 실험과 비교하여 볼 때 더 많은 시간이 지났음에도 남아있는 에너지의 양이 더 많음을 볼 수 있다. 이는 각 노드들의 전송 범위가 줄어들면서 한 노드가 패킷을 전송할 때 영향을 받는 노드의 수가 감소하기 때문이다. 이렇듯 ad hoc 네트워크에서 노드의 이동성, 밀집도 그리고 전송 반경이 DoS 공격에 대한 피해정도에 영향을 주게 된다. 이와 같은 특징은 네트워크의 구성이 유선이 아닌 무선임으로 인해서 발생하



(a) (b)

〔그림 6〕 DoS 공격에 의한 에너지 소모: 전송 범위 150m, (a) 50초 후, (b) 150초 후



(a) (b)

〔그림 7〕 DoS 공격에 의한 throughput 감소효과: (a) 전송범위 250m (b) 전송범위 150m

는 것으로 유선이었다면 DoS 공격으로 별 영향을 받지 않을 수도 있는 공격에도 무선 상황이어서 큰 영향을 받는다.

2.2. TCP Throughput 감소

토폴로지가 변하는 네트워크 상에서의 DoS 공격이 throughput에 끼치는 영향을 살펴보는 실험이다. 이번 실험에서는 11번, 30번 노드가 35번 노드에게 UDP flooding 공격을 하는 동안에 18번 노드와 23번 노드 사이에 TCP 트래픽을 전송하도록 하였다.

〔그림 7〕의 각 그래프는 위에서부터 각각 UDP flooding이 없는 경우, 11번 번 노드만 UDP를 전송하는 경우 그리고 11번과 30번 노드가 DoS 공격에 참여하는 경우에 대한 TCP 트래픽의 throughput를 보여준다.

(a)의 경우는 각 노드의 전송 범위를 250m로 한 경우이다. 앞장에서의 실험 결과와 동일하게 UDP flooding이 증가하면서 TCP의 throughput가 감소된다. 그러나 이전의 실험과는 달리 throughput의 결과를 보면 각 UDP flooding으로 인한 영향이 뚜렷하게 나타나지 않고 0.15에서 0.25의 범위에 걸쳐 중첩되는 것을 볼 수 있다. 이는 각 노드들에게 이동성이 제공되면서 앞 장에서와는 달리 노드 11번과 30번에 의한 UDP flooding의 전송경로가 18번 노드와 23번 노드 사이의 TCP 트래픽 전송경로의 방향과 평행함으로 인한 방해가 뚜렷하지 않기 때문이다.

(b)는 각 노드의 전송 범위를 150m로 감소시킨 후 실험을 반복한 결과이다. UDP flooding이 없는 경우는 (a)의 경우에 비해 절반 정도로 떨어진 것을 볼 수 있다. 이는 전송 범위가 줄어들면서 TCP 트래픽의 전송경로가 증가하기 때문이다. UDP flooding이 증가하면서 throughput는 급격한 감소를 보이다

우에는 throughput이 0이 되는 것을 볼 수 있다.

이 실험에서는 노드에 이동성이 주어질 경우에는 고정된 토폴로지에서와는 달리 일정한 경로가 주어지지 않기 때문에 DoS에 의한 공격으로 더 심각한 피해를 끼칠 수 있다. 또한 각 노드들의 전송 범위에 따라 전송 성능 및 가용성에 심각한 영향을 미칠 수 있다.

V. 결 론

본 논문에서는 유비쿼터스 네트워크의 보안 요구사항들과, 이 중에서 가용성을 저해하는 DoS 공격의 여러 가지 유형에 대해 분석하고, 이러한 공격이 네트워크의 전송성능과 생존성에 미치는 영향을 컴퓨터 시뮬레이션을 이용하여 분석하였다. 무선 ad hoc 네트워크는 기존의 다른 네트워크와는 상이한 여러 가지 특성들로 인하여, DoS 공격이 네트워크에 미치는 영향 또한 기존 네트워크의 경우와 상이함을 발견하였다.

무선 ad hoc 네트워크의 성능을 결정짓는 중요한 요소인 에너지 소모 측면에서 공격대상 노드보다 공격자와의 전송경로 상에 있는 노드들의 피해가 훨씬 심각함을 확인하였다. 이는 같은 DoS 공격을 수행하더라도 ad hoc 네트워크의 경우에 더 심각한 피해를 당할 수 있음을 보여주는 것이며, 유선 네트워크에서는 실현이 불가능한 DoS 공격의 효과이다. Ad hoc 네트워크에서 이동 노드들이 밀집해있거나, 각 노드의 전송반경이 큰 경우에는 이러한 DoS 공격에 의한 피해가 훨씬 심각해진다. 또한 전송성능의 측면에서도, 무선 ad hoc 네트워크에서는 DoS 패킷들이 전송경로가 다르더라도 다른 트래픽의 throughput에 심각한 영향을 끼침을 확인하였다. 이상의 결과에서, 같은 형태의 DoS 공격이더라도 유선 네트워크의 경우 보다 무선 ad hoc 네트워크의 경우에 네트워크 전체의 전송 성능 및 가용성에 훨씬 심각한 형향을 미침을 알 수 있다.

미래의 유비쿼터스 컴퓨팅 환경은 센서 네트워크 및 무선 네트워크를 포함하는 무선 이러한 ad hoc 네트워크가 네트워크 인프라를 제공하게 될 것이며, 최근 들어 '유비쿼터스 컴퓨팅을 향한 새롭고 다양한 어플리케이션이 등장하고 실험되기 시작하면서, 이와 더불어 무선 ad hoc 네트워크의 보안 및 프라이버시 메커니즘에 대한 연구와 개발이 매우 활발하게 시작되고 있다. 향후에 본 논문에서 다루지 못한 여러 가지 공격 유형 및 위험성에 대한 분석과 더불어서 이에 대한 대처 방안과 메커니즘을 개발하여야 한다.

참고문헌

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

[2] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," IEEE ICNP, Nov. 2001

[3] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," ACM Mobicom, Aug. 2000

[4] K. Wrona, "Distributed security: ad hoc networks & beyond," PAMPAS Workshop, Sep. 2002

[5] L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Network, pp. 24-30, Nov/Dec. 1999

[6] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ubiquitous computing," IEEE Security & Privacy, pp. 22-26, 2002. Avaliable at http://www.computer.org/computer/sp

[7] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks," IEEE MILCOM, Oct. 2002

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

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

[10] P. Kyasanur and N. Vaidya, "Diagnosing and penalizing MAC layer misbehavior in wireless networks," Technical Report, Dept. of ECE, UIUC, Dec. 2002. Available at http://www.crhc.uiuc.edu/~nhv/

[11] The CMU Monarch project's wireless and mobility extensions to ns, Snapshot Release 1.1.1, Carnegie mellon University, Aug. 1999. Available at http://www.isi.edu/nsnam/ns/

〈著 者 紹 介〉

이 병 주(Byungjoo Lee)

1997년~2002년 : 광운대학교 컴퓨터공학과(공학사)
2002년~2004년 : 광운대학교 전파공학과(공학석사)
2004년~현재 : 광운대학교 전파공학과 박사과정
〈관심분야〉 무선 LAN/PAN, 무선 네트워크 및 보안

홍 순 좌 (Soonjwa Hong)
종신회원

1989년 : 숭실대학교 전산학과(이학사)
1989년~1991년 : 숭실대학교 전산학과(이학석사)
1991년~2000년 : 국방과학연구소 선임연구원
2000년~현재 : 국가보안기술연구소 선임연구원/팀장
〈관심분야〉 유비쿼터스 컴퓨팅 보안, 사이버테러 대응기술

이 승 형 (Seung Hyong Rhee)
종신회원

1984년~1988년 : 연세대학교 전자공학과(공학사)
1988년~1990년 : 연세대학교 전자공학과(공학석사)
1995년~1999년 : University of Texas at Austin, Dept. of ECE(Ph. D.)
1990년~1995년 : 국방과학연구소 연구원
1999년~2000년 : 삼성종합기술원 전문연구원
2000년~현재 : 광운대학교 전자공학부 조교수
〈관심분야〉 무선 LAN/PAN, 무선 네트워크 및 보안