Journal of Digital Contents Society Vol. 10 No. 2 Jun. 2009(pp. 349-355)

MANET에서 안전한 서비스 제공을 위한 On-demand 라우팅 프로토콜의 성능 비교

허진경*, 양환석**

요 약

MANET(Mobile Ad hoc Network)은 infrastructure를 구성하는 것이 경제적으로 불리하거나 물리적으로 어려운 상황에서 인터넷과 같은 대형 통신망의 서비스뿐만 아니라 각 노드간의 통신의 지원에 중점을 둔 네트워크이다. MANET을 구성하는 시스템들의 보호에 있어 가장 중요한 부분은 각 노드들을 안전하게 인증하고 신뢰할 수 있는 서비스를 제공하는 것이고 이를 위해서는 잘 정의된 라우팅 기법이 필요하다. 본 논문에서는 안전한 서비스 제공을 위해서 기존의 on-demand 라우팅 프로토콜과 기존 라우팅 프로토콜의 취약성을 해결하기 위해 제시된 보안 라우팅 프로토콜과의 성능을 비교, 분석하여 향후 보안 라우팅 프로토콜의 연구 방향에 대해 논의한다.

Performance Comparison of On-demand Routing Protocol to Supply Secure Service for Mobile Ad Hoc Networks

JinKyoung Heo*, HwanSeok Yang**

Abstract

MANET is network that attach importance to not only service of large network as internet but also support of communication among each nodes because infrastructure constitution is disadvantage econ omically or difficult physically. The most important part in protection of systems constitute MANET is that authenticate each nodes securely and offer reliable service. Well defined routing technique is necessity to this. In this paper, in order to offer safe service, we compare capacity of present security routing protocol, analyze to solve weakness of existing on-demand routing protocol and existing routing protocol and argue with study course of hereafter security routing protocol.

Keywords : System Authentication, Routing Protocol, MANET(Mobile Ad Hoc Network)

1. 서론

인터넷과 이동통신 기술의 급격한 발전으로 멀티미디어 통신 서비스가 보편화되는 등 우리 환경에 큰 변화를 가져다주었다. 데이터 통신은 유선망뿐만 아니라 무선망을 통한 데이터 통신에 대한 시장 욕구가 증가되고 있다[1].

MANET(Mobile Ad hoc Network)은 물리적으로 어려운 환경에서 인터넷과 같은 대형 통신망의 서비스뿐만 아니라 각 노드간 통신의 지원에 중점을 두 네트워크로서 각 노드들은 라우터의 기능을 포함하게 되는 매우 능동적인 시스템이다[2]. MANET에서 동작하는 라우팅 프로토콜은 기존의 고정된 네트워크에서 동작하는 라우팅 프로토콜과 구별되는 몇 가지 추가된 요구 사항이 있다. 첫째, 임의의 노드에 대해 발생하는 링크의 설정이나 해제 시에도 네트워크의 동작에 심각한 영향을 미쳐서는 안 되는 분산된 동작 체제를 갖춰야 한다. 둘째, 패킷 조각들이 네트워크를 무한히 떠도는 경우를 구조적으로 막을 수 있는 프로토콜이 필요하다. 셋째, 요구 또는 필요에 따른 트래픽 패턴에 적용할 수 있는 라우팅 알고리즘이 필요하다. 넷째, 단방향 링크의 존재도 수용할 수 있는 라우팅 알고리즘

※ 제일저자(First Author) : 허진경
접수일:2009년 04월 07일, 완료일:2009년 06월 24일
* 호원대학교 사이버수사경찰학부
heojk@howon.ac.kr
** 호원대학교 사이버수사경찰학부
▣ 본 논문은 2009년 호원대학교 교내 학술연구 조성비에 의해 연구되었음

이 필요하다. MANET을 위해 제안된 라우팅 방식은 크게 두 가지로 나눠진다. 평상시에 라우팅 정보를 각 노드가 수시로 탐색하고 이를 테이블에 저장, 유지하면서 필요시에 테이블을 참조하여 패킷을 전송하는 table-driven routing 방식과 경로가 요구되어질 때에만 경로를 찾는 on-demand routing 방식이 있다. Table-driven routing 방식은 모든 노드에 대한 일관되고 최신의 경로 정보를 각 노드가 유지하고 있지만, on-demand routing 방식에서는 단지 소스 노드가 요구할 때에만 경로가 설정되어진다[3]. MANET에서 사용되는 라우팅 프로토콜은 각 노드들이 라우팅 정보를 공유하고 라우팅 메시지를 broadcast하기 때문에 보안상 취약점을 가지게 된다. 만약 하나의 노드가 잘못된 라우팅 정보를 퍼뜨리게 된다면 네트워크 전체가 마비가 될 수도 있기 때문이다. 그리고 악의적인 노드가 네트워크에 쉽게 참여할 수 있고 라우팅 과정에서 많은 공격을 수행할 수가 있게 된다. 따라서 악의적인 노드의 공격을 탐지하고 방어할 수 있는 라우팅 보안 메커니즘도 반드시 필요하다. 라우팅에 대한 공격의 유형을 살펴보면 올바른 데이터가 제대로 전달되지 못하도록 하여 라우팅을 붕괴시키는 공격과 위조된 라우팅 패킷을 삽입함으로써 네트워크를 분리시키는 경우도 있다. 자원 고갈의 공격 형태는 불필요한 데이터 패킷이나 제어 패킷을 발생시켜 대역폭을 비롯한 여러 자원들이 고갈되도록 하는 공격 등이 있다.

본 논문에서는 안전한 서비스 제공을 위해서 기존의 on-demand 라우팅 프로토콜과 기존 라우팅 프로토콜의 취약성을 해결하기 위해 제시된 보안 라우팅 프로토콜의 성능을 비교 분석함으로써 안전한 라우팅 기법을 위한 향후 연구 방향을 논의 하고자 한다.

본 논문에서는 라우팅 프로토콜의 성능 평가 기준으로 라우팅 프로토콜이 얼마나 정확한 경로를 제공하는지 알아보기 위한 패킷 전달률, 네트워크의 전체적인 성능을 좌우하는 제어 패킷의 양을 성능 평가의 기준으로 정했다. 이러한 기준에 대해 일반적인 상황과 라우팅 공격중의 하나인 RREQ 플러딩 공격을 발생하여 실험하였다.

2. Ad hoc On-demand Distance Vector Routing

AODV는 network를 구성하는 노드가 빈번히 이동함으로써 링크의 위상이 자주 바뀌는 환경에서 사용되기 위한 라우팅 프로토콜로 네트워크에 참여하는 각 노드에 의해 운용되어 지며, 경로 배정에 대한 요구가 없을 때에는 동작하지 않는다. 따라서 링크의 변화를 적절한 시간 내에 감지할 수 있는 메커니즘이 제공되어야 한다[4]. Distant-Vector routing 프로토콜은 어느 한 노드의 링크가 끊겨졌을 때 여러 노드가 이 정보를 잘못 전달하여 해당 경로에 대한 무한 루프가 발생하는 문제점을 가지고 있다. 이를 보완하기 위해 AODV는 Destination sequence number 필드를 추가하였다. Destination sequence number는 경로 정보가 어떤 것이 최신인지 구별하기 위한 필드로 목적지의 노드가 하나의 경로 요청 메시지를 받을 때마다 이에 대한 응답 메시지에 그 순서 번호를 증가시켜 기입하는 것이다. 이에 의해 목적지에 대한 경로를 요청한 노드와 중간 노드들은 경로 정보 사이에 어떤 것이 가장 최신 것인지 판단할 수 있게 된다. (그림 1)과 (그림 2)는 요청 메시지와 응답 메시지의 형태를 보여준다.

Type	Reserved	Hop count
Broadcast ID		
Destination IP address		
Destination Sequence number		
Source IP address		
Source Sequence number		

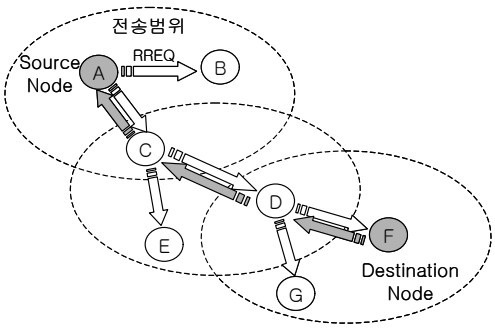
(그림 1) 라우트 요청 메시지 형태

Type	I	Reserved	Hop count
Destination IP address			
Destination Sequence number			
Life time			

(그림 2) 라우트 응답 메시지 형태

AODV는 Route Request(RREQ)와 Route Reply(RREP) 두 가지가 있다. 이 메시지는 일반적

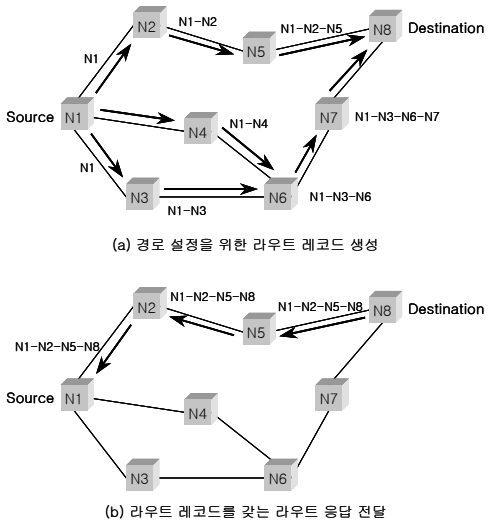
인 IP 헤더를 사용하여 UDP 기반으로 처리되며 RREQ의 전송 범위는 IP 헤더의 TTL에 의해 지정된다. 목적지로의 경로를 찾기 위해 소스는 RREQ를 전파한다. RREQ는 목적지에 도착하거나 목적지에 관한 최근의 경로 정보를 가지고 있는 중간 노드에 도달 할 때까지 계속 전파된다. 각 RREQ는 sequence number들을 사용한다. 이는 루프를 피하고 중간 노드가 경로 요청들에 대해 정확한 응답을 하기 위해 사용된다. 노드가 RREQ를 이웃들에게 전달할 때, 자신의 테이블에 요청을 처음으로 보낸 노드를 저장한다. 이 정보는 RREP를 위한 역 경로를 만들 때 사용된다. AODV는 RREP가 RREQ가 전달되어 온 경로를 거꾸로 이용하기 때문에 양방향 링크들만을 사용한다. RREP가 소스 노드로 되돌아갈 때 경로상의 노들들은 자신들의 테이블에 경로를 넣는다. 발견된 경로 정보를 테이블에 유지할 때 AODV는 타이머를 사용한다. 일정 시간 안에 그 경로 정보가 사용되지 않으면 그 정보는 무효화 된다. 이는 DSR 프로토콜과 큰 차이점이라 할 수 있겠다. AODV는 최신의 정보만을 유지하기 위하여 타이머를 사용하며 링크에 에러가 발생하였을 때 RRER을 전파하여 그 정보를 유지하고 있는 노드들에게 에러를 알리고 그 경로 정보를 무효화하게 만든다. (그림 3)은 AODV의 경로 설정 방법을 보여준다. 경로를 초기에 요구하는 노드가 A일 때 RREQ를 방송하게 되고, 이에 대한 응답을 할 수 없으면 이 메시지는 계속 전달되게 된다. 목적지 노드 또는 목적지까지의 경로를 알고 있는 노드에 의해 RREP가 unicast back되면 그 경로를 알려지게 된다.



(그림 3) AODV의 경로 설정 방법

3. Dynamic Source Routing

DSR은 모든 노드가 자기 자신을 root로 하는 shortest tree 형태를 유지한다. DSR은 경로 탐색과 경로 유지의 두 단계로 이루어진다. 소스 노드가 패킷을 목적지에 보낼 경우 먼저 캐쉬에 경로가 저장되어 있는지를 확인한다[5]. 만약 경로가 존재한다면, 그 경로를 사용하여 패킷을 전송하고, 그렇지 않다면 RREQ를 망에 전송하여 경로 탐색 절차를 실행시킨다. RREQ는 소스와 목적지의 주소 그리고 독자적인 숫자를 포함하고 있다. 경로 탐색 절차 중 각 중간 노드는 목적지로의 경로를 알고 있는지 확인하고 이를 알지 못한다면 RREQ의 route record 항에 이를 저장한다. 만약 RREQ가 목적지에 도달하게 되면 이 패킷은 route record를 가지는 RREP로 바뀌게 된다. 그와 달리 RREQ가 목적지로의 경로 정보를 가지는 중간 노드에 도착하게 되면 그 노드는 자신의 경로 캐쉬에서 목적지까지의 경로를 찾아 RREP의 route record에 추가한다. RREP를 다시 소스에게 보내기 위해서는 RREP 생성 노드는 반드시 소스로의 경로를 가지고 있어야만 하고 만약 캐쉬에 소스까지의 경로가 저장되어 있다면 캐쉬에 저장되어 있는 경로를 사용한다. DSR의 경로 설정 방법은 (그림 4)와 같다.



(a) 경로 설정을 위한 라우트 레코드 생성

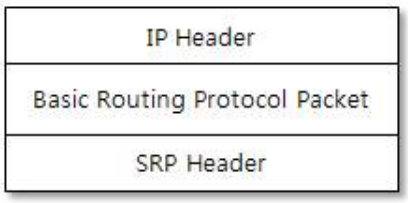
(b) 라우트 레코드를 갖는 라우트 응답 전달

(그림 4) DSR의 경로 설정 방법

DSR은 경로 유지를 위해 RERR(Route Error Packet)과 acknowledgement를 사용한다. 노드에서 에러를 발견하면 RERR를 생성하고 캐쉬에서 에러나 간 홉을 제거한다. Acknowledgement 패킷들은 경로 링크의 올바른 전송 상태를 입증하기 위해 사용된다[6][7].

4. Secure Routing for Mobile A d hoc networks

P. Papadimitrator와 Zygmunt J.Hass에 의해 제안된 보안 라우팅 프로토콜인 SRP는 종단간 보안 통신을 제공할 목적으로 만들어졌다[8]. 이 방법은 소스 노드와 목적지 노드 사이에 SA(Security Association)만 설정되면 그 중간 노드들은 무조건 패킷을 전달하는 방식이다. 즉, 경로상에 악의적인 노드가 존재한다 하더라도 안전한 통신을 제공할 수 있다는 것이다. 보안 라우팅 프로토콜인 SRP의 경로 설정 방법은 다음과 같다. 먼저 종단간 노드 사이에 SA가 존재한다고 가정한다. 또한 종단간 두 노드는 비밀키를 공유한다. 먼저 소스 노드는 query sequence number와 random query identifier 쌍에 의해 구분되는 경로 요청 패킷을 발생시킨다. 이 패킷을 수신한 중간 노드들은 자신의 IP주소를 추가하여 다음 이웃 노드에게 전달하게 된다. 경로 요청 패킷을 수신한 목적지 노드는 MAC(Message Authentication Code) 값을 계산하여 중간 노드들에 의한 패킷 변조여부를 확인하게 된다. 만약 이상이 없으면 MAC 값을 다시 계산하여 경로 응답 패킷을 소스 노드에게 전달하게 된다. 이 방법은 소스 노드와 목적지 노드 사이에 악의적인 노드가 존재한다 하더라도 두 노드간의 비밀 공유키를 알 수 없기 때문에 패킷의 내용을 변조할 수 없다. 만약 변조한다 하더라고 올바른 MAC 값을 계산할 수 없기 때문에 종단간 노드에서 변조된 패킷을 삭제하게 된다. 또한 MAC 값을 계산하는데 많은 처리과정이 필요하지 않기 때문에 비교적 간단하게 메시지의 무결성을 제공할 수 있다. 그러나 경로상의 존재하는 악의적인 노드가 패킷을 복사하여 전송할 경우 목적지 노드에 의해서 삭제될 수는 있지만 그 패킷을 전달하는 중간 노드들의 자원 낭비를 막을 수 없는 단점을 가지고 있다. (그림 5)는 보안 라우팅 프로토콜인 SRP 패킷의 구조를 보여주고 있다.



(그림 5) SRP 패킷

5. 실험 및 결과

5.1 실험 환경

본 장에서는 MANET의 On-demand 라우팅 프로토콜과 보안 라우팅 프로토콜인 SRP의 보안의 취약성 부분에 대한 성능 평가를 위해 다음과 같은 환경에서 실험하였다. 무선 전송 모델은 two-ground(1/r4)이며, 이동성 모델인 random way-point model이다. 이 모델은 제한한 속도로 임의의 위치로 이동한 후 임의의 시간 동안 정지하고, 다시 임의의 위치로 이동하는 모델을 말한다. 그리고 MANET을 구성하는 노드들은 균등하게 본포하고 있으며, 제한된 방향성을 가진 공간보다는 사용자가 자유롭게 움직일 수 있는 개방된 환경에서 동작한다고 가정한 것이다. 이러한 가정하에 한정된 네트워크의 크기와 노드 수 사이에서 라우팅 프로토콜이 얼마나 정확한 경로를 제공하는지 알아보기 위한 패킷 전달률, 네트워크의 전체적인 성능을 좌우하는 제어 패킷의 양을 성능 평가의 기준으로 정했다. 이러한 기준에 대해 일반적인 상황과 라우팅에 대한 공격중의 하나인 RREQ 플러딩 공격을 발생한 경우를 실험하였다.

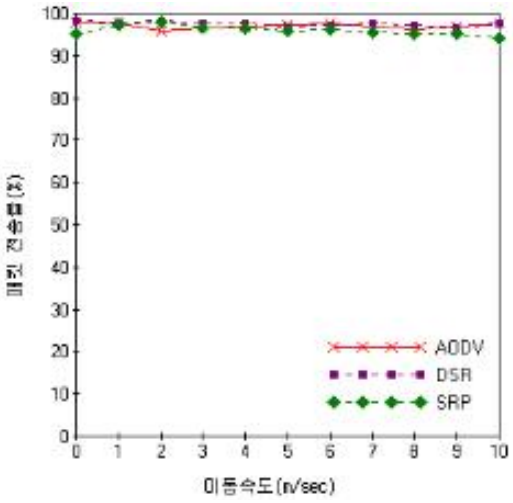
5.2 실험 결과

실험 평가를 위해 64바이트, pause time은 15초로 하였다. 그리고 데이터 전송 범위는 100m로 하였으며 네트워크 크기에 따라 10번 실험을 반복하였으며 각 시뮬레이션에는 300초의 시간이 주어졌다. 실험에 사용한 노드의 수는 네트워크의 크기에 따라 다르게 설정하였다. 표 2는 노

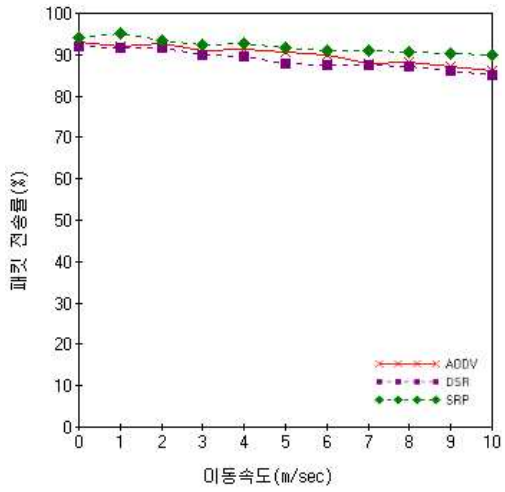
드 수에 따른 네트워크 크기를 보여주고 있다.

<표 1 > 네트워크 크기

노드수	네트워크 크기
20	400m × 400m
40	800m × 800m



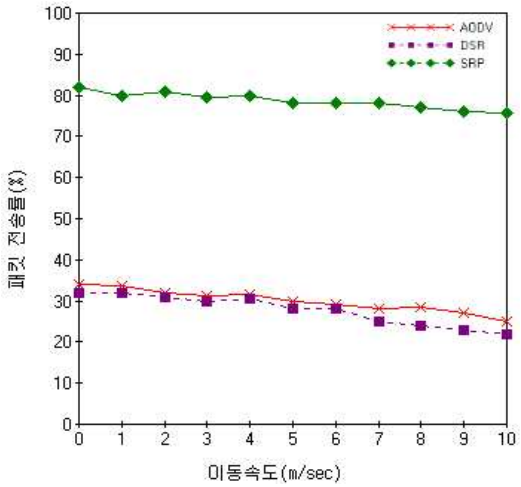
(a) 20 노드



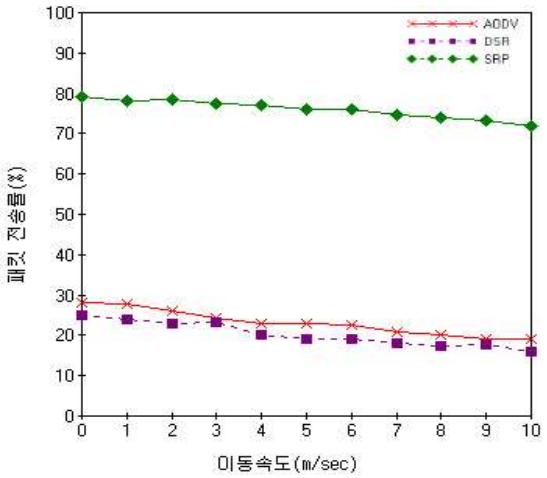
(b) 40 노드

(그림 6) 안전한 네트워크에서의 패킷 전송률

(그림 6)은 라우팅 프로토콜의 정확한 경로 제공을 측정하기 위해서 노드의 수를 변화시키면서 AODV와 DSR 그리고 보안 라우팅 프로토콜인 SRP를 각각 적용하여 패킷 전송률 구하였다. 여기서는 공격 노드가 존재하지 않는 네트워크는 안전하다는 가정 하에서 실험하였다. 그림에서 알 수 있듯이 네트워크가 안전한 상황에서는 보안이 고려되지 않은 AODV와 DSR 그리고 보안 라우팅 프로토콜인 SRP가 거의 비슷한 성능을 나타내고 있다. 다만 노드들의 이동 속도가 빨라질수록 패킷 전송률이 조금씩 떨어지는 것은 확인할 수 있다.



(a) 20 노드



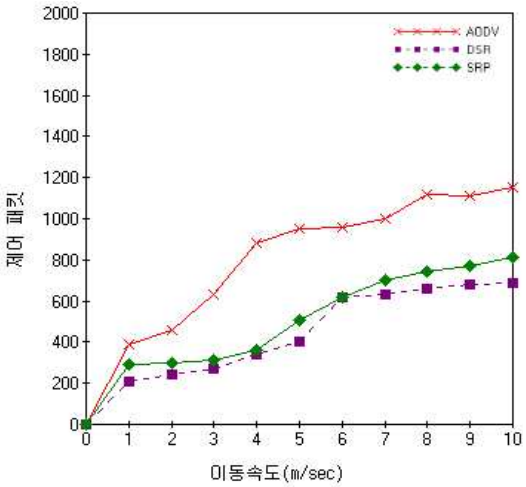
(b) 40 노드

(그림 7) RREQ 플러딩 공격시 패킷 전송률

(그림 7)은 RREQ 플러딩 공격을 발생시킨 경

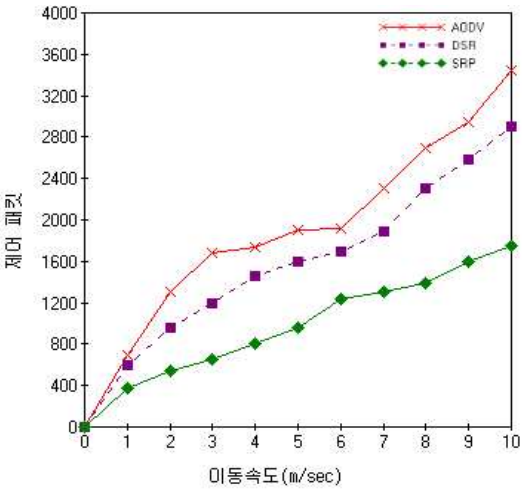
우의 패킷 전송률 측정하였다. 보안이 고려되지 않은 AODV와 DSR은 패킷 전송률이 급격하게 떨어졌다. 두 프로토콜은 공격 노드의 잘못된 RREQ를 전달받음으로써 올바른 경로를 탐색하여 제공하지 못하였기 때문에 패킷 전송률이 급격하게 저하되었다. 그러나 보안 라우팅 프로토콜인 SRP는 두 라우팅 프로토콜에 비해서는 성능이 많이 떨어지지는 않았지만 이 기법은 노드에 2개 이상의 경로가 설정되면 동작하지 않기 때문에 지연 시간은 길어졌다.

(그림 8)은 네트워크가 안전하다는 가정하에서 노드의 수가 20개인 경우의 네트워크 전역의 제어 패킷의 양을 측정하였다. 무선 네트워크의 대역폭이 낮기 때문에 제어 패킷이 많아지지만 네트워크의 전체적인 성능이 떨어지게 된다. 그림에서 알 수 있듯이 DSR은 AODV에 비해 제어 패킷의 양이 적다. 왜냐하면 DSR은 자신의 캐쉬에 있는 경로의 정보가 유효하지 않을 경우에만 경로 검색을 수행하기 때문이다. 그리고 보안 라우팅 프로토콜인 SRP 역시 종단간 SA를 설정하여야 하기 때문에 제어 메시지의 양이 DSR에 비해서 많게 나타났다.



(그림 8) 안전한 네트워크에서 제어 패킷의 양

(그림 9)는 RREQ 플러딩 공격시 네트워크 전역의 제어 패킷의 양을 보여주고 있다. 그림에서도 나타나듯이 공격자의 RREQ 제어 패킷에 의해 라우팅 프로토콜이 목적지 노드까지의 올바른 경로를 탐색하기가 쉽지 않기 때문에 제어 패킷의 양이 크게 증가한 것을 확인할 수 있다. 그러나 보안 라우팅 프로토콜인 SRP 경우에는 제어 패킷의 양이 증가하기는 하였지만 보안이 고려되지 않은 라우팅 프로토콜에 비해서는 현저하게 적음을 알 수 있다. 즉, 보안 라우팅 프로토콜은 다른 두 개의 라우팅 프로토콜에 비해서 효율성 및 성능 모두에서 훨씬 뛰어난 기능을 갖고 있음을 확인할 수 있었다.



(그림 9) RREQ 플러딩 공격시 제어 패킷의 양

6. 결론

본 논문에서는 보안 프로토콜이 갖추어야 할 요건들을 알아보기 위해서 기존의 on-demand 라우팅 프로토콜과 기존 라우팅 프로토콜의 취약성을 해결하기 위해 제시된 보안 라우팅 프로토콜인 SRP의 성능을 비교 분석하였다. 네트워크가 안전하다고 가정한 경우에는 보안이 고려되지 않은 AODV와 DSR, 그리고 보안 라우팅 프로토콜인 SRP가 거의 비슷한 성능을 보였다. 그러나 네트워크 내에 공격이 존재하는 경우는 보안이 고려되지 않은 AODV와 DSR 라우팅 프로토콜의 성능이 현저하게 떨어지는 것을 확인할 수 있었다. 향후 보안에 취약한 MANET에서 라우팅 프로토콜 설계시 다양한 공격에도 안전하고 신뢰성 있는 라우팅을 제공하기 위한 연구가 이루어져야 할 것이다.

참고문헌

[1] Eva Gustafsson, Ericsson, Editor, Requirements on Mobile Ip from a cellular Perspective, draft-ieft-mobileip-cellular-requirements-02.txt, June. 1999.

[2] C. K. Toh, "Ad Hoc Network Wireless Networks," Protocols and System, Prentice Hall PTR, 2002.

[3] David Maltz, Josh Broch, Jorjeta Jetcheva, and David Johnson. The effects of on-demand behavior in routing protocols for multi-hop wireless ad hoc networks. IEEE Journal on Selected Areas in Communication, 1999.

[4] Charles Perkins, "Ad Hoc On Demand Distance Vector (AODV) Routing", Internet-Draft, draft-ietf-mant-aodv-00.txt, November, 1997.

[5] J. Broch, D. Johnson, and D. Maltz. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet-Draft, draft-ietf-mant-dsr-03.txt, Oct. 1999.

[6] D. Johnson and D. Maltz. Dynamic source routing in ad hoc wireless networks. In T. Imielinski and H. Korth, editors, Mobile Computing, chapter 5. Kluwer Academic, 1996.

[7] Mainak Chatterjee, Sajal K. Das and Damla Trugut, "An On-demand Weighted clustering Algorithm (WCA) for Ad hoc Networks," IEEE GLOBECOM. pp 1697-1701, 2000.

[8] P. Papadimitratos and Z. J. Hass, "Secure Routing for Mobile Ad Hoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January pp 27-31, 2002.

양 환 석

1996년 : 호원대학교 전자계산학과 (이학사)

1998년 : 조선대학교 전산통계학과 대학원 (이학석사)

2005년 : 조선대학교 전산통계학과 (이학박사)

2007년～현재: 호원대학교 사이버수사경찰학부 연구교수

관심분야 : 시스템 보안(System Security), 정보보호(Personal Information), 침입탐지시스템(IDS) 등

허 진 경

1998년 : 호원대학교 전자계산학과 (이학사)

2000년 : 조선대학교 전산통계학과 대학원 (이학석사)

2004년 : 조선대학교 전산통계학과 (이학박사)

2006년～2008년 8월 : 호원대학교 사이버수사경찰학부 연구교수

2008년 9월 ~ 현재 : 호원대학교 사이버수사경찰학부 전임강사

관심분야 : 웹어플리케이션 보안(Web Application Security), 정보보호(Personal Information), 분산처리(Distributed Computing) 등