애드 혹 네트워크상의 패킷 폐기 공격의 영향 분석

김상수°
국방과학연구소
plus°@add.re.kr

An Analysis on the Effect of Packet Dropping Attacks in Wireless Ad hoc Networks

SangSoo Kim°
Agency for Defense Development

요 약

본 논문에서는 무선 애드 혹 네트워크상의 패킷 폐기 공격의 영향을 분석하고 시뮬레이션을 통해 그 효과를 측정하였다. 시뮬레이션 수행 결과 RREQ 패킷을 폐기한 경우에는 네트워크에 미치는 영향이 적은 반면, RREP 및 DATA 패킷을 폐기한 경우는 네트워크의 전송 효율이 떨어졌으며, 또한 패킷을 폐기하는 악성노드가 많을수록 데이터의 전달율이 감소하고 하나의 데이터를 전송 하는데 필요한 제어 패킷의 수가 늘어남을 알 수 있었다. 시뮬레이션을 통해 분석된 결과를 바탕으로 패킷 폐기 공격의 징후를 미리 검출하거나 공격 형태를 식별하는 기초 자료로 활용가능 할 것이다.

1. 서 론

무선 애드 혹 네트워크 환경에서의 모든 노드들은 자유롭게 이동하므로 네트워크의 토폴로지는 수시로 역동적으로 변하며, 유선과는 달리 각 노드들이 중앙에 집중되어 있지 않고 분산되어 있기 때문에 본질적으로 다양한 공격에 취약하다[1][2].

애드 혹 네트워크 상에서의 공격은 크게 물리적 계층에서의 공격, MAC 계층에서의 공격 및 네트워크 계층에서의 공격으로 나눌 수 있는데, 네트워크 계층에서 발생할 수 있는 공격에는 거짓 또는 유효하지 않은 정보 전파, 패킷 불법 조작 및 전송, 불필요한 대량 패킷 전파 등의 능동적 공격과 데이터 패킷을 의도적으로 폐기하는 수동적 공격으로 나눌 수 있다[1].

본 논문은 대표적 수동적 공격 방법인 패킷 폐기에 의한 공격의 영향을 정성적인 방법 및 시뮬레이션을 통해 분석하고 그 활용 방안을 고찰하였다.

이 논문의 구성은 다음과 같다. 제 2장에서는 패킷 폐기에 의한 공격 영향을 분석하고 제 3장에서 시뮬레이션을 통해 그 피해를 측정하며, 마지막 제 4장에서 결론을 맺는다.

2. 패킷 폐기 공격의 영향 분석

애드 혹 네트워크에서 사용되는 패킷은 제어 패킷과 데이터 패킷(DATA)으로 나눌 수 있으며 제어 패킷에는 RREQ(Route Request), RREP(Route Reply), RRER(Route Error)가 있다. 패킷 폐기에 의한 공격은 이러한 네 가지의 패킷의 일부 또는 전체를 폐기하여 다른 노드들의 전송을 방해하여 전송 효율을 떨어뜨린다.

그림 1은 RREQ 패킷에 의한 공격의 영향을 나타내었다. 출발지 노드 S가 RREQ를 브로드캐스팅할 때, 악의 목적을 가진 노드 A가 S로부터 오는 RREQ를 폐기 하면, A를 지나는 경로가 목적지로 가는 최단 경로임에도 불구하고 그 대체 경로인 S-4-6-7-10-D의 경로가 사용되었다.

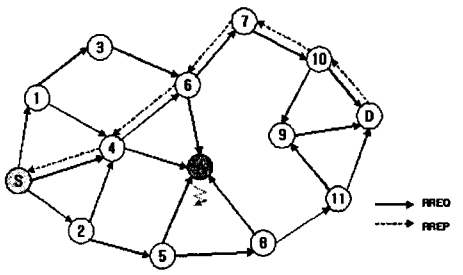

그림 1 RREQ 패킷 폐기 공격

RREQ를 폐기 하는 노드의 개수가 적은 경우는 대체 경로를 선택하면 데이터 전송에 큰 어려움이 없지만, 많은 수의 노드가 이러한 공격을 시도한다면 경로 설정이 제대로 이루어지지 않아 패킷 전송율 및 종단간 지연시간에 영향을 미치고, 최악의 경우 대체 경로를 찾지 못해 일시적으로 데이터의 전송이 불가능하게 될 수도 있다.

RREP 패킷을 폐기한 경우는 그림 2와 같다. 노드 A가 목적지 D에서 전송한 RREP를 폐기 하면 출발지 노드 S는 RREP를 수신하지 못하고 경로 찾기를 다시 수행하여 대체 경로를 찾아야 한다. 그 결과 대체 경로를 찾기까지의 지연시간일 발생하고 패킷 전송율이 떨어진다.

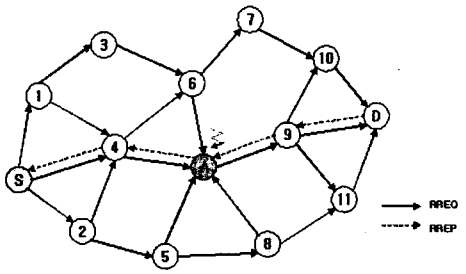

그림 2 RREP 패킷 폐기 공격

그림 3은 RRER 패킷을 폐기한 경우의 예이다. 악성 노드 A가 RERR를 폐기하면 출발지 노드 S는 기존에 설정된 경로가 유효하다고 믿고 계속해서 데이터를 보낼 것이고 중간노드인 노드 4의 버퍼에 데이터가 쌓이게 될 것이다. 만약 노드 S와 노드 A 사이에 다수의 중간 노드가 존재한다면 중간 노드에서 전송이 지연되고 데이터의 전달이 늦어질 것이다. 물론 노드들의 이동성이 높은 경우 출발지 노드는 정상적인 다른 노드에서 발생한 RERR를 전달 받아 새로운 경로 찾기를 할 가능성이 높아 별 영향이 없을 것이지만, 노드들의 이동성이 낮거나 거의 정지되어 있는 경우에는 설정된 경로상의 노드들이 이동할 가능성이 낮기 때문에 RERR를 폐기하는 공격의 피해를 입을 것이다.

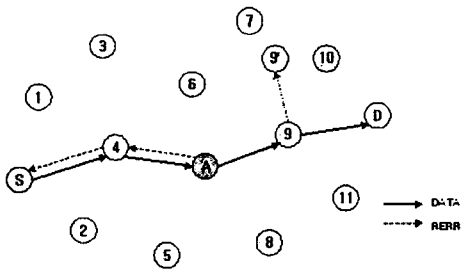

그림 3 RRER 패킷 폐기 공격

DATA 패킷 폐기를 이용한 공격의 예는 그림 4에 나타나 있다. 그림에서 S-4-A-9-D 경로가 이미 설정되어 있고 출발지 노드 S에서 데이터가 전송된다고 가정할 때, 악성 노드 A가 전달받은 데이터 패킷을 폐기하게 되면 목적지 노드 D는 재전송을 요구한다. 경로 상에 악성 노드 A가 존재하는 한 이러한 현상이 반복되어 데이터는 D로 더 이상 전달되지 않는다.

DATA 패킷이 폐기된 경우는 RREQ나 RREP 등의 제어 패킷이 폐기된 경우보다 상황은 심각하다. 왜냐하면, 데이터 패킷이 도중에 폐기되면 전달 여부를 라우팅 프로토콜로는 알 수 없기 때문이다. 노드들이 다행히 악성 노드를 제외한 경로로 데이터를 전송하면 별 문제가 없지만 악성 노드의 수가 많거나 비교적 느리게 움직이는 환경일 경우 해결할 수 있는 방법이 없다. 전송 프로토콜로 TCP를 사용할 경우 재전송할 수 있지만 UDP와 같이 재전송 매커니즘이 없는 경우 데이터는 그대로 소실된다.

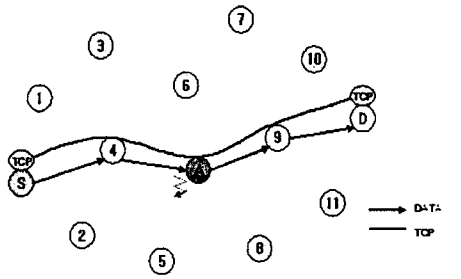

그림 4 DATA 패킷 폐기 공격

3. 시뮬레이션

애드 혹 네트워크상의 패킷 폐기에 의한 공격의 영향을 분석하기 위하여 병렬 이산 이벤트 시뮬레이션 기능을 사용하는 PARSEC[3] 기반의 Global Mobile Simulation(GloMoSim)[4] 시뮬레이터를 사용하였다. 총 600초의 시뮬레이션 시간 동안 1000x1000 미터 구간에 랜덤으로 배치된 50개의 노드를 평균 0~20 m/s 로 움직이도록 하였다. MAC 프로토콜은 802.11 DCF[5]를 사용하였으며 이동 모델은 random waypoint 모델[6]을 사용하였고, 트래픽 모델은 CBR(continuous bit rate)를 사용하여 초당 4개의 패킷으로 512 바이트의 데이터를 전송하였다.

시뮬레이션은 RREQ, RREP, DATA 패킷을 폐기하는 악성노드를 5개로 고정하고 정지 시간을 다르게 하여 패킷 전달율, 평균 종단 지연시간, 정규화된 라우팅 오버헤드에 대해서 각각을 측정하였다.

그림 5는 정상적인 경우와 RREQ, RREP, DATA 패킷을 폐기한 경우의 패킷 전달율을 비교하였는데, RREQ 패킷 폐기에 의한 영향은 거의 없었고 RREP와 DATA 패킷 폐기에 의한 영향이 비교적 컸다. 특히 DATA 패킷을 폐기한 경우 패킷 전달율이 현저하게 떨어졌는데 이는 제어 패킷의 경우는 폐기되는 제어 패킷이 재전송이나 전달 지연으로 인해 간접적으로 영향을 미친 반면, 데이터 패킷 폐기의 경우는 패킷 전달율에 직접적인 영향을 미쳤기 때문이다.

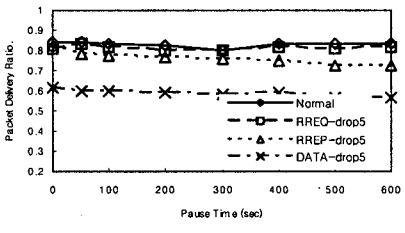

그림 5 패킷 전달율

그림 6은 정상적인 경우와 각각의 패킷을 폐기하였을 때의 종단간 지연시간을 비교한 것이다. 정상적인 경우와 RREQ 패킷을 폐기한 경우의 차이는 거의 없는 반면 RREP와 DATA 패킷을 폐기하였을 때는 종단간 지연시간이 정상적인 경우보다 감소하였다. 이는 RREP와 DATA 패킷의 폐기로 인해 전달에 성공하는 DATA 패킷의 수가 RREQ 폐기와 정상적인 경우보다 작기 때문이다.

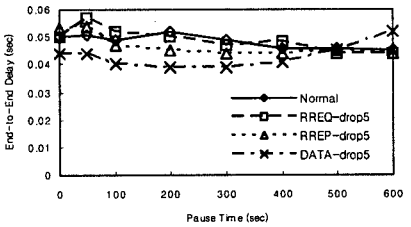

그림 6 종단간 지연시간

그림 7은 각각의 패킷의 폐기에 따르는 정규화된 라우팅 오버헤드를 비교하였다. 정상적인 경우와 RREQ 및 DATA 패킷을 폐기하는 경우는 오버헤드의 성능이 거의 비슷하였지만, RREP의 경우 오버헤드가 증가함을 볼 수 있다. 이는 RREP를 불법적으로 버리는 다수의 악성노드가 네트워크에 존재한다면 전송된 RREP는 폐기될 가능성이 높고 RREP가 폐기되면 출발지 노드는 목적지 노드로의 경로를 다시 설정해야 된다. 이러한 과정을 통해 네트워크 전체에 유입되는 RREQ 및 RREP의 양이 많아지고 라우팅 오버헤드의 수치가 높아지는 원인이 된다.

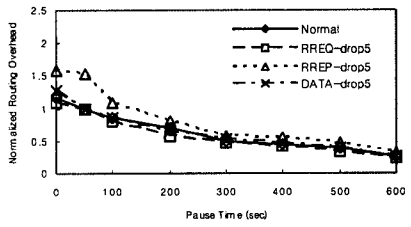

그림 7 라우팅 오버헤드

4. 결 론

패킷 폐기에 의한 공격의 영향을 분석하고 시뮬레이션을 통해 패킷 전달율, 평균 종단간 지연시간, 정규화된 라우팅 오버헤드를 측정하였다. 시뮬레이션 수행결과 RREQ 패킷을 폐기하는 악성노드가 존재하는 경우 패킷 전달율과 종단간 지연시간 및 정규화된 라우팅 오버헤드 모두 정상적인 경우와 별로 차이가 나지 않았다. 이로써 악성노드의 개수가 적은 환경에서 RREQ 패킷 폐기로 인한 공격의 효과는 미미했다.

RREP 패킷 폐기에 의한 공격의 효과는 정상적인 경우와 차이가 없지만 악성노드의 개수가 증가할수록 RREP의 폐기율이 높아서 경로 재설정을 할 확률이 높아지기 때문에 라우팅 오버헤드의 값이 증가할 것이다. DATA 패킷의 폐기로 인한 결과는 RREQ, RREP를 폐기하는 경우와는 달리 패킷 전달율이 급격하게 감소했고 정규화된 라우팅 오버헤드의 값이 증가하였다.

패킷 폐기에 의한 공격의 피해 정도는 어떠한 패킷을 폐기 하느냐와 악성노드의 개수가 얼마나 되는가에 따라 결정된다고 볼 수 있다. 다수의 노드 중 하나의 노드만 비정상적인 행동을 하는 경우는 네트워크 전체에 미치는 영향이 미비하여 탐지 하기는 힘들지만, 많은 노드들이 공격에 참여하는 경우는 각 패킷 종류마다 나타나는 특성이 다르기 때문에 이를 이용해서 패킷 폐기에 의한 공격을 미리 검출하거나 공격 형태를 식별하는 기초 데이터로 활용할 수 있을 것이다.

참고문헌

[1] 심학섭, 김태윤, "이동 Ad Hoc 네트워크에서의 보안 취약점에 대한 연구", 제 18회 한국정보처리학회 추계학술발표대회 논문집 제 9권 제 2호, 2002.11.

[2] 이승형, 홍순좌, 최헌준, "무선 Ad Hoc 네트워크에서의 서비스 거부(Denial of Service) 공격의 위험성 분석", 제 15회 정보보호와 암호에 관한 학술대회 논문집, pp. 660-669, 2003. 9.

[3] R. Bagrodia, R. Meyer, M. Takai, Y. Chen, X. Zeng, J. Martin, and H. Y. Song, "PARSEC: A Parallel Simulation Environment for Complex Systems", IEEE Computer, vol. 31, no. 10, pp. 77-85, Oct. 1998.

[4] UCLA Parallel Computing Laboratory and Wireless Adaptive Mobility Laboratory, GloMoSim: A Scalable Simulation Environment for Wireless and Wired Network Systems, http://pcl.cs.ucla.edu/projects/domains/glomosim.html.

[5] IEEE Computer Society LAN MAN Standards Committee, Wireless LAN Medium Access Protocol (MAC) and Physical Layer (PHY) Specification, IEEE Std 802.11-1997. The Institute of Electrical and Electronics Engineers. New York, NY, 1997.

[6] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, pp. 183-97, Oct. 1996.