경로 요청 테이블을 이용한 러싱 공격 방지 기법

임원택°, 조은경, 김문정, 엄영익
성균관대학교 정보통신공학부
{imcliff°, iuno, tops, yieum}@ece.skku.ac.kr

Rushing Attack Prevention Scheme using Route Request Table

Won-tack Lim°, Eun-kyung Cho, Moon Jeong Kim, Young Ik Eom
School of Information and Communication Engineering, Sungkyunkwan University

요 약

무선 ad-hoc 네트워크는 이동 노드만으로 구성된 자율적이고 수평적인 네트워크이다. 무선 ad-hoc 네트워크에서의 라우팅 프로토콜은 table driven 방식과 on-demand 방식으로 나뉘는데, 이 중 라우팅 메시지의 오버헤드가 비교적 적은 on-demand 방식이 주로 사용되고 있다. 이 프로토콜은 경로를 찾기 위해서 경로 요청 메시지를 브로드캐스팅 하는데, 경로 요청 메시지는 네트워크 전체로 확산되기 때문에 이를 이용한 공격이 가능하다. 공격자는 연속적으로 경로 요청 메시지를 보냄으로써 패킷 충돌과 네트워크 큐 오버플로우 등의 장애를 일으켜 정상적인 메시지나 데이터의 전송을 방해할 수 있다. 본 논문에서는 기존의 라우팅 프로토콜에 별도의 인증 절차 없이 경로 요청 패킷의 확산을 이용한 공격을 막는 방법을 제안하고자 한다. 각각의 노드는 경로 요청 메시지의 시작 주소와 수신 시간을 경로 요청 테이블을 이용해 관리함으로써 정상적인 경로 요청 패킷과 공격자의 경로 요청 패킷을 구분한다. 수신된 경로 요청 패킷이 공격자의 패킷이라고 판단된 경우, 공격자의 패킷을 이웃 노드에 전달하지 않음으로써 전체 네트워크에 가해지는 공격을 막을 수 있다.

1. 서 론

최근 노트북, PDA, 스마트 폰과 같은 무선기기가 점차 보급되고 있다. 이러한 무선기기의 확산으로 인해 무선통신에 대한 연구가 더욱 활발하게 이루어지고 있다. 이 중 이동 노드만으로 구성된 자율적이고 수평적인 네트워크인 ad-hoc 네트워크에 대한 연구는 현재 IETF의 MANET WG을 중심으로 활발히 진행되고 있다[1].

Ad-hoc 네트워크의 라우팅 프로토콜은 table driven 방식과 on-demand 방식으로 나뉜다. 이 중 table driven 방식의 메시지 브로드캐스팅 오버헤드 문제를 해결한 on-demand 방식에 연구의 초점이 모아지고 있다. 이 라우팅 프로토콜은 트래픽이 발생할 때마다 경로 요청 패킷을 브로드캐스팅 함으로써 전송 경로를 찾아내는 방식이다.

On-demand 방식의 프로토콜은 데이터의 전송경로를 찾기 위해서 네트워크 전체에 경로 요청 패킷을 전송한다[2,3]. 만일 경로 요청이 잦아질 경우 경로 요청 패킷은 네트워크 트래픽에 부담을 줄 수 있으며, 임의의 공격자가 이를 이용해서 ad-hoc 네트워크를 공격할 수도 있다. 경로 요청 패킷을 이용한 공격 방식을 러싱 공격(rushing attack)이라고 한다[4]. 러싱 공격에는 신호의 세기를 이용한 방법, 정상적인 패킷보다 빠른 속도로 비정상적인 패킷을 전송하는 방법, 두 공격자가 받은 경로 요청패킷을 서로에게 전송하는 웜 홀 공격방법 등 여러 가지 공격 방법이 있다[5].

기존의 *on-demand* 라우팅 프로토콜에 보안 기능을 강화한 ariadne, SAODV, SRP 등의 프로토콜에서도 데이터를 전송하기 위해서 경로 요청 메시지를 보내기 때문에 러싱 공격을 피하기 어렵다[5]. 러싱 공격을 막기 위해서 고안된 기법인 RAP (Rushing Attack Prevention)는 안전한 경로를 찾기 위해 안전한 이웃 노드 찾기, 임의의 메시지 전송 등의 방법을 사용하고 있다. 하지만 인증에 필요한 별도의 패킷과 임의의 메시지를 전송하기 위해 메시지를 수집하는 시간이 오버헤드로 작용한다[5,6,7,8].

본 논문에서 제안하는 기법에서는 경로 요청 패킷을 수신할 때마다 시작 주소와 수신 시간을 저장함으로써 비정상적으로 빠른 주기의 경로 요청 패킷을 공격 패킷으로 구분한다. 수신된 패킷이 공격 패킷이라고 판단될 경우 경로 요청 패킷을 브로드캐스팅하지 않음으로써 별도의 인증절차 없이도 러싱 공격을 막아낼 수 있다. 또한 인증에 필요한 패킷이나 시간의 지연이 없기 때문에 기존의 해결 방식이 가지는 오버헤드를 크게 줄일 수 있다.

본 논문의 2장에서는 경로 요청 패킷을 이용한 러싱 공격과 이 공격을 막기 위해 기존에 연구됐던 RAP 방식을 살펴보고 3장에서는 경로 요청 테이블을 이용해 경로 요청 패킷의 수신 시간을 관리함으로써 러싱 공격을 막는 법을 제안한다. 4장에서는 결론과 향후 연구방향에 대해서 설명한다.

2. 관련연구

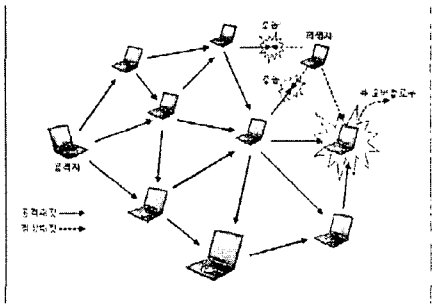
본 절에서는 제안 기법이 해결하고자 하는 공격방식인 러싱 공격과, 이 러싱 공격을 막기 위해 연구 되었던 RAP 기법에 대해서 알아본다.

2.1 러싱 공격(Rushing attack)

러싱 공격은 on-demand 라우팅 프로토콜의 특성을 이용해서 DoS(Denial-of-Service)공격 방식과 유사한 효과를 내는 공격방식이다. On-demand 라우팅 프로토콜은 경로를 찾기 위해서 반드시 경로 요청 패킷을 전체 네트워크에 브로드캐스팅 해야 한다. 경로 요청 패킷은 유일하게 전체 네트워크에 확산될 수 있는 패킷이므로, 이 패킷이 많아지게 되면 네트워크 전체의 성능에 커다란 영향을 미칠 수 있다. 러싱 공격은 경로 요청 패킷의 이와 같은 특성을 이용해서 네트워크의 성능을 저하시키거나 정상적인 패킷의 원활한 전송을 방해하는 공격 방식이다.

러싱 공격에는 신호의 세기를 이용한 방법, 정상적인 패킷보다 빠른 속도로 비정상적인 패킷을 전송하는 방법, 두 공격자가 받은 경로 요청 패킷을 서로에게 전송해서 경로상의 터널을 형성하는 웜 홀 공격방법 등 여러 가지 공경 방법이 있다[5].

(그림 1)에서 공격자는 짧은 주기로 계속해서 시퀀스 번호와 목적지 주소를 바꾸어가면서 경로 요청 패킷을 전송한다. 만일 네트워크에 목적지 주소를 가진 호스트가 없다면 경로 요청 패킷은 네트워크 전체로 확산될 것이다. 비록 경로 요청 패킷은 크기가 크지 않지만 빠른 주기로 확산된다면 네트워크 트래픽의 상당량을 차지하게 된다.

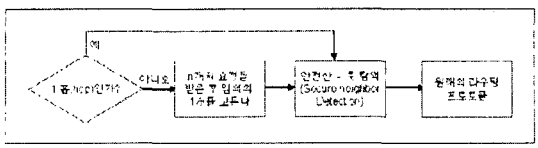


(그림 1) 러싱 공격(Rushing Attack)의 결과

만일 이 때 다른 정상적인 노드가 정상적인 패킷을 전송하려고 한다면 네트워크를 가득 메우고 있는 경로 요청 패킷에 의해 정상적인 패킷이 충돌(collision)하거나 호스트의 큐가 가득 차게 돼서 패킷을 처리할 수 없게(queue overflow)되는 등 비정상적인 동작이 야기 될 수 있다.

2.2 RAP(Rushing Attack Prevention)

RAP는 러싱 공격을 막기 위한 방법으로 기존의 on-demand 프로토콜에 쉽게 이식할 수 있는 장점을 가지고 있다. 이 방법은 여러 가지 러싱 공격 기법을 막기 위해 고안되었다. RAP는 (그림 2)에서 보는 바와 같이 대표적으로 안전한 이웃 탐색(secure neighbor detection)과 임의의 메시지 포워딩(randomized message forwarding)기법을 사용해서 러싱 공격을 막아낸다.



(그림 2) RAP(Rushing Attack Prevention)

안전한 이웃 탐색은 경로 요청 패킷을 통해서 암묵적으로 이웃의 존재를 탐색하는 기존의 on-demand 방식의 프로토콜과 달리 능동적으로 이웃의 존재를 식별하고 인증해 줌으로써 안전한 이웃을 통해서 경로를 생성하는 방식이다. 탐색은 이웃을 알고 싶어하는 노드가 이웃의 정보를 요청하는 단계, 이웃의 정보 요청에 응답하는 단계, 그리고 이웃의 정보를 확인해 주는 단계의 세 단계로 진행된다. 처음 두 단계에서는 각자의 노드의 키를 생성하고, 모든 단계에서는 그 키를 이용해서 서명을 함으로써 서로가 안전한 이웃임을 확인할 수가 있게 된다.

임의의 메시지 포워딩 기법은 반복적인 경로 요청 패킷에 의한 공격을 막기 위한 방법이다. 일반적인 on-demand 라우팅 프로토콜에서는 경로 요청 패킷을 받게 되면 즉각적으로 패킷을 포워딩한다. 따라서 연속적인 패킷을 받게 되면 네트워크에 부담을 줄 수 있다. RAP 에서는 이러한 현상을 막기 위해 경로 요청 패킷을 받게 되면 일정 기간 동안 경로 요청 패킷을 담아 두었다가 임의의 경로 요청 패킷을 포워딩 한다. 이러한 기법을 사용함으로써 연속적인 경로 요청 패킷을 이용한 러싱 공격을 막을 수 있다.

3. 제안기법

3.1 개요

정상적인 ad-hoc 네트워크 환경에서 수십 ms 단위로 경로만을 탐색하는 일은 매우 드물다. 따라서 짧은 주기로 경로 요청 패킷을 전송하는 호스트의 패킷은 공격자의 패킷으로 간주할 수 있다. 따라서 각각의 호스트가 경로 요청 패킷을 받은 시간을 관리하게 된다면 정상 패킷과 공격 패킷을 구분할 수 있다. 또 이를 통해서 공격 패킷을 무시함으로써 공격 패킷이 네트워크 전체로 전파되는 것을 막을 수 있다.

이러한 방법은 간략한 테이블과 타이머로써 구현이 가능하며 별도의 패킷을 발생하지 않으므로 기존의 프로토콜에 탑재한다고 해도 오버헤드가 거의 발생하지 않는 장점을 가진다.

3.2 경로 요청 테이블

경로 요청 테이블은 (그림 3)과 같이 경로 요청 패킷을 받은 시간과 시작 주소를 저장하는 테이블이다. 이 테이블에 있는 항목을 근거로 정상적인 패킷과 공격자의 패킷을 구분한다.

Source Address	Recv Time(ms)
192.168.1.35	241512
192.168.1.122	241740
...	...

(그림 3) 경로 요청 테이블의 예

테이블은 경로 요청 패킷의 시작 주소와 수신 시간을 저장한다. 이 테이블은 일종의 캐시역할을 하게 된다. 일정시간 Δt 동안만 패킷의 정보를 저장하기 때문이다. Δt는 이 제안 기법에서 중요한 역할을 하는 시간으로, 정상적인 경로 요청 패킷과 공격 패킷을 구분하는 기준이 되는 시간이다.

3.3 기본동작

이 기법을 수행하기 위해서는 몇 가지 가정이 필요하다. 무선 ad-hoc 네트워크의 모든 노드들은 단말기로써의 역할 뿐만 아니라 라우터의 역할을 할 수 있어야 한다. 러싱 공격은 on-demand 방식의 라우팅 프로토콜의 보안 취약성을 이용한 공격이기 때문이다. 그리고 라우팅을 담당하는 중간 노드는 경로 요청 패킷을 받았을 때 시간 지연 없이 즉각 패킷을 이웃 노드에게 브로드캐스팅 해야 한다. 만일 경로 요청 패킷을 받은 후 시간 지연을 두고 다음 패킷을 처리하게 되면 러싱 공격 자체가 성립이 되지 않기 때문이다. 러싱 공격을 막기 위해서 고정된 값의 시간 지연을 두는 것은 모바일 노드가 많은 상황에서는 오히려 경로 요청 패킷의 처리를 방해해서 네트워크의 전체적인 성능을 떨어뜨릴 수 있다.

테이블의 항목을 관리하기 위해서 각각의 노드들은 ms 단위로 시각을 측정할 수 있는 클럭을 가지고 있어야 하고, 공격 패킷을 구분할 기준 시간인 Δt가 미리 정해져 있어야 한다.

경로 요청 패킷을 받은 노드는 해당 패킷의 시작 주소를 경로 요청 테이블에서 검색한다. 만약 시작 주소가 테이블에 존재하지 않는다면 해당 패킷의 시작 주소와 패킷을 받은 시각을 테이블에 저장한다. 이 경우 경로 요청 패킷은 정상적인 패킷으로 간주되어 이웃 노드로 브로드캐스팅 된다.

경로 요청 패킷의 시작 주소가 경로 요청 테이블에 존재한다면 해당 패킷을 받은 시각으로 정보를 갱신한다. 이 경우에 지정된 시간 이내에 같은 노드에서 경로 요청 패킷이 전송되었으므로 이 패킷은 공격 패킷으로 간주된다. 따라서 이 패킷은 이웃 노드로 브로드캐스팅 되지 않는다.

각각의 항목이 추가될 때마다 항목에는 Δt만큼의 타이머가 동작하게 된다. 만일 이 타이머가 시간이 다 되게 되면 해당 항목은 테이블에서 사라지게 된다.

3.4 알고리즘

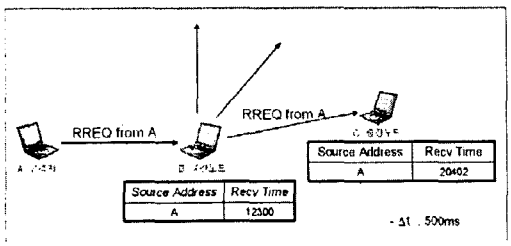
경로 요청 테이블을 이용해서 러싱 공격을 막아내는 동작 과정을 (알고리즘 1)에서 보인다.

```
if(a route request packet is received) {
  Search a source address of received packet in the table;
  if(a source address is in the table) {
    Modify a arrival time;
    Set up timer again;
  }
  else {
    Insert a source address and a arrival time into Table;
    Set up timer;
    Broadcast a route request packet to neighbors;
  }
}
```

(알고리즘 1) 경로 요청 테이블 검색을 이용한 러싱 공격 방지기법

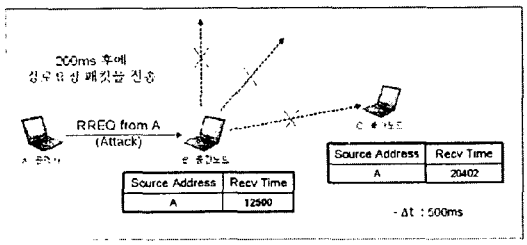
3.5 시나리오

경로 요청 테이블을 이용해서 러싱 공격을 막으려면 우선 정상 패킷과 공격 패킷을 구분 지을 수 있는 기준 시간을 정해 놓아야 한다. 본 시나리오에서는 Δt를 500ms로 가정하고 설명한다.



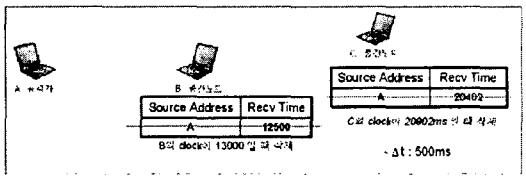
(그림 4) 공격 시작과 경로 요청 테이블에 경로 요청 패킷 정보 등록

(그림 4) 에서 A는 공격자, B와 C는 각각 라우터의 역할을 하는 중간 노드이다. 공격자는 목적지 주소를 바꾸어 가면서 ad-hoc 네트워크 전체로 경로 요청 패킷을 확산시키려 한다. 공격자의 첫 번째 공격 패킷을 받은 중간 노드 B는 경로 요청 테이블에 공격자의 주소와 패킷을 받은 시간을 저장한다. 경로 요청 테이블에는 공격자의 주소가 없으므로 정상적인 패킷으로 간주, C로 브로드캐스팅 한다. B로부터 패킷을 받은 C도 경로 요청 테이블에 A의 주소와 패킷을 받은 시간을 저장하고 다시 이웃 노드에게 패킷을 브로드캐스팅 한다.



(그림 5) 공격 패킷의 인식과 공격 패킷의 재확산 방지

(그림 5)에서 공격자 A가 빠른 주기로 다음 패킷을 네트워크에 확산시키기 위해 이웃 노드인 B에게 20ms 후에 브로드캐스팅 한다. B는 경로 요청 패킷의 시작 주소를 경로 요청 테이블에서 검색한다. 검색 결과 경로 요청 테이블에 공격자 A의 주소가 있으므로 이번 패킷은 공격 패킷으로 간주한다. 우선 이번 패킷을 받은 시간으로 경로 요청 테이블의 항목을 갱신한다. 수신된 패킷이 공격 패킷으로 간주 되었으므로 이 패킷은 이웃 노드에게 브로드캐스팅 되지 않는다. 이 동작은 테이블에서 공격자의 항목이 사라지지 않는 한 계속 된다. 이러한 과정을 통해서 러싱 공격으로 전체 네트워크가 공격당하는 것을 막게 된다.



(그림 6) 경로 요청 테이블 항목 삭제

(그림 6)에서 보는 바와 같이 경로 요청 테이블에 있는 정보는 패킷을 받은 각각의 시간(B는 12500, C는 20402)으로부터 500ms가 지났을 때 삭제된다.

4. 결론 및 향후 연구과제

본 논문에서는 경로 요청 테이블과 경로 요청 패킷을 관리하는 알고리즘을 사용해서 경로 요청 러싱 공격을 막는 방법을 제안하였다. 이 방법은 기존의 on-demand 방식의 라우팅 프로토콜에서 큰 변화를 주지 않고 공격을 막아낼 수 있으므로 경로 요청 패킷을 이용하는 대부분의 on-demand 방식의 라우팅 프로토콜에도 적용될 수 있다.

향후 연구에서는 시뮬레이션이나 실제 ad-hoc 네트워크에서의 실험을 통해서 정상적인 네트워킹에 지장을 주지 않으면서 러싱 공격을 막을 수 있는 적당한 Δt 값을 결정해야 할 것이다. 또한 목적지 주소뿐만 아니라 시작 주소도 함께 바꾸어 공격해 올 경우 제안방식으로는 막아낼 수 없으므로 MAC address를 이용한 해결방안의 연구가 필요하다.

참고문헌

[1] J. Z. Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing," In Proceedings of ICII 2001 International Conference on Info-tech and Info-net, Vol. 3, pp. 316-321, 2001.

[2] C. E. Perkins, "Ad-hoc on-demand distance vector routing," in MILCOM '97 panel on Ad Hoc Networks, Nov. 1997.

[3] David B. Johnson and David A. Maltz. "Dynamic Source Routing in Ad Hoc Wireless Networks," In Mobile Computing, chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996.

[4] Baruch Awerbuch, "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks," Technical Report. March 2004.

[5] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Technical Report TR01-384, Department of Computer Science, Rice University, June 2002.

[6] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," In Proceedings of theEighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, September 2002.

[7] Manel Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," In Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), September 2002.

[8] Panagiotis Papadimitratos and Zygmunt J. Haas. "Secure Routing for Mobile Ad Hoc Networks," In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.