MANET 환경에서 DDoS 공격 완화 기법에 관한 연구

양환석* · 유승재**

요 약

고정된 인프라스트럭쳐 없이 무선 노드로만 구성된 MANET은 높은 유연성을 제공하지만, 다양한 공격에 취약한 단점을 가지고 있다. 특히 모든 노드들이 패킷 포워딩을 수행해야 하기 때문에 DDoS 공격에 큰 취약점을 가지고 있다. 본 논문에서는 MANET에서 DDoS 공격의 피해를 완화시키고, DDoS 공격 발생시 공격자의 위치를 찾기 위한 패킷 전송 정보 관리 기법을 제안하였다. 본 논문에서는 DDoS 공격 대상을 보호하기 위하여 게이트웨이 노드를 이용하는 계층구조를 채택하였다. 소스 노드가 목적지 노드까지 경로 설정시 목적지 노드와 같은 클러스터내의 게이트웨이 노드가 반드시 포함되어야 하며, 이 게이트웨이 노드는 목적지 노드를 보호하는 기능을 수행한다. 본 논문에서 제안한 기법은 CUSUM 기법과 비교 실험하여 효율성을 확인하였고, 위치 추적에 사용할 정보 관리의 효율성을 평가하기 위해 클러스터 헤드의 메모리 사용량을 측정하였다.

A Study on DDoS Attack Mitigation Technique in MANET

Yang Hwan Seok* · Yoo Seung Jae**

ABSTRACT

MANET composed wireless nodes without fixed infrastructure provides high flexibility, but it has weak disadvantage to various attack. It has big weakness to DDoS attack because every node perform packet forwarding especially. In this paper, packet transmission information control technique is proposed to reduce damage of DDoS attack in MANET and search location of attacker when DDoS attacks occur. Hierarchical structure using gateway node is adopted for protect a target of attack in this study. Gateway node in cluster is included like destination nodes surely when source nodes route path to destination nodes and it protects destination nodes. We confirmed efficiency by comparing proposed method in this study with CUSUM and measured the quantity consumed memory of cluster head to evaluate efficiency of information control using to location tracing.

Key words : Attack Mitigation, DDoS, MANET

접수일(2012년 2월 24일), 수정일(1차: 2012년 3월 12일), 게재확정일(2012년 3월 19일)

* 중부대학교 정보보호학과
** 중부대학교 정보보호학과(교신저자)

1. 서 론

고정된 인프라스트럭처가 없이 노드들로만 구성되어 있는 MANET(Mobile Ad-hoc Network)은 다양한 분야에서 활용되고 있으며, 그 연구 분야 또한 다양하다. 그 중에서 보안 분야가 가장 활발하게 연구가 진행되고 있다[1]. 왜냐하면 MANET은 노드들의 이동으로 인한 네트워크 위상이 수시로 변화하고, 모든 노드들이 라우터 기능을 수행해야 하기 때문에 보안에 취약하다[2]. 이러한 다양한 위협 중에서 그 피해가 매우 큰 DDoS(Distributed Denial of Service) 공격은 크게 라우팅 공격과 패킷 포워딩 공격으로 나눌 수 있다[3][4]. 라우팅 공격은 정상적인 노드의 경로 설정을 방해하는 것으로서 노드들 사이의 라우팅 정보를 잘못된 정보로 바꾸어 공격을 수행한다. 반면에 패킷 포워딩 공격은 네트워크 내에 제어 패킷이나 데이터를 과도하게 발생시켜 정상 노드들이 특정 서비스를 정상적으로 제공받지 못하도록 하는 것이다.

본 논문에서는 DDoS 공격의 피해를 완화시키고, 공격자 위치 추적에 도움이 되는 패킷 전송 정보의 관리 방법을 제안하였다. 소스 노드가 목적지 노드와 경로를 설정할 때 목적지 노드와 같은 클러스터에 속한 게이트웨이 노드를 반드시 경로에 포함되도록 하였다. 이 게이트웨이 노드가 목적지 노드로 가는 모든 패킷을 감시하여 의심스러운 패킷이 발견된다면 이를 차단하는 역할을 수행하는 것이다. 그리고 경로가 설정된 후 패킷을 전송하는 모든 노드들은 패킷 전송 정보를 자신의 클러스터 헤드에게 전송한다. 이 정보는 공격자의 위치를 찾아내기 위해 사용되며 클러스터 헤드에 의해 관리된다. 본 논문에서는 게이트웨이 노드들이 공격 탐지 기능을 가지고 있다고 가정하였다.

본 논문의 구성은 다음과 같다. 2장에서는 DDoS 공격 탐지 및 역추적 기법에 대하여 살펴보고 3장에서는 DDoS 공격의 피해를 완화시킬 수 있는 제안한 기법에 대하여 기술하였다. 4장에서는 제안한 기법의 성능을 평가하고 5장에서는 결론을 맺는다.

2. 관련연구

2.1 DDoS 탐지 기법

MANET에서 이용되는 DDoS 탐지 기법은 탐지 시스템의 위치에 따라 victim 기반 탐지와 소스 기반 탐지로 나눌 수 있다[5]. Victim 기반 탐지 기법은 탐지 시스템이 victim 근처에 위치해 있다. 이 방법은 빠르게 공격을 탐지할 수 있는 장점을 가지고 있다. 그러나 공격 경로의 혼잡을 완화시킬 수 없는 단점을 가지고 있다. Victim 기반 탐지 기법에서 주로 사용하는 기법은 기계 학습과 통계 모델이다. TRA(Traffic Rate Analysis)는 TCP 패킷에서 플래그의 분산 비율을 측정하는 방법으로서 공격이 발생했을 때 트래픽 패턴을 검사하기 위하여 기계 학습 방법을 적용한다. 이 시스템에서 DDoS 탐지는 신경망 모델과 베이지안 분류기를 기초로 한다. 통계 모델을 이용한 공격 탐지 기법인 CUSUM(Cumulative Sum) 알고리즘은 SYN과 SYN-ACK 패킷에 대한 모델을 이용하였다. 수집된 SYN 패킷의 수가 SYN-ACK 패킷보다 많다면 CUSUM 값은 양수가 된다. CUSUM 값이 크다면 SYN-ACK 패킷과 쌍을 이루지 못하는 SYN 패킷이 많다는 것이고, 즉 DDoS 공격이 발생했음을 의미한다. 소스 기반 탐지는 공격자의 위치에 가깝게 위치하게 한다. 그러므로 탐지 시스템의 위치는 경계 라우터에 위치한다. 널리 알려진 소스 기반 탐지 시스템인 D-WARD는 공격자를 탐지하기 위하여 게이트웨이 라우터에 위치하고 트래픽 흐름을 제한하였다. D-WARD는 트래픽 통계를 이용하여 비정상 트래픽을 탐지한다. 비정상 트래픽이 탐지되면 공격 트래픽의 유입을 제한하기 위하여 소스 라우터의 트래픽을 조정하는 방법을 사용한다.

2.2 DDoS 역추적 기법

역추적 기법은 크게 ICMP 메시지를 사용한 기법, 로깅을 이용한 기법, PPM을 적용한 기법으로 나눌 수 있다. IP의 역추적을 위해 IETF가 제안하는 ICMP 기반의 iTrace-CP 방법이 있다[3]. iTrace-CP 기법은 ICMP 메시지를 생성하여 목적지 까지 IP 패킷과 함께 동일한 경로를 사용하여 전달된다. 패킷이 목적지까지 가는 모든 경로 정보를 ICMP 메시지에 저장함으로써 역추적을 가능하게 하는 것이다. 이 기법의 단점은 공격자의 위치를 역추적하기 위해서는 ICMP 메시지를 수집해야 하며, 따라서 공격자의 위치가 이동

되는 경우에는 추적이 쉽지 않다는 것이다. 두 번째로 로깅을 이용한 기법으로는 Hotspot-based Traceback, SWAT(Small World-based Attacker Traceback) 등이 있다[6]. Hotspot-based traceback 기법은 Bloom filter에 감시된 패킷의 TTL(Time-to-Live) 정보를 저장할 수 있는 TBF(Tagged Bloom Filter)를 이용한 역추적 기법이다. Bloom filter는 매우 간단한 비트-벡터를 사용하여 입력 값이 특정 집합에 속하는 요소인지를 판단해주는 필터이다. 마지막으로 PPM을 사용한 기법으로 Contact-based Traceback 기법과 ZSBT 기법이 있다[7]. Contact-based Traceback 기법은 PPM 기법을 그대로 무선 네트워크에 적용한 기법으로 sink 노드와 contact들 사이의 메시지 교환을 통해 역추적을 수행한다. 그리고 ZSBT 기법은 전체 네트워크를 zone으로 나눈 후, 특정 노드를 지나는 패킷에 IP 주소 대신에 노드가 속한 zone-id를 추가하는 기법이다. 그리고 나머지 과정은 유선 환경에서의 PPM 기법과 거의 유사하다. <표 1>은 역추적 기법들의 장단점을 보여주고 있다.

<표 1> 역추적 기법의 특징 비교

기 법	장 점	단 점
ICMP	· 경로 재구성 용이 · ICMP 메시지에 모든 경로 저장	· ICMP 패킷이 필터 되는 경우 발생
PPM	· 오버헤드가 상당이 적음 · 일정한 확률로 패킷에 정보 마크	· 역추적을 위한 최소한의 패킷 필요 · 패킷 단편화시 역추적 불가능
Logging	· 모든 패킷에 정보 저장 · 공격 완료된 후 역추적 가능	· 공격 경로 재구성을 위한 많은 오버헤드 발생 · 많은 로그 정보의 관리

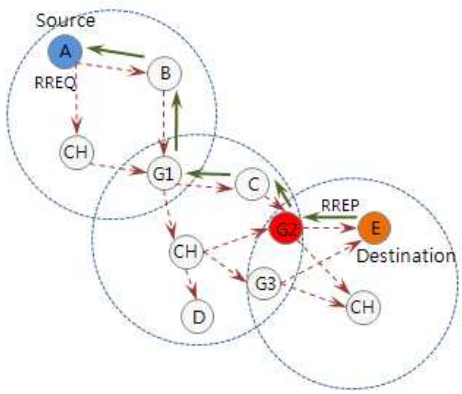
3. DDoS 공격의 완화

3.1 노드 초기화

본 논문에서는 계층적 구조를 이용하기 위하여 네트워크를 구성하고 있는 노드들을 클러스터로 형성한다. 다음 단계로 노드들은 자신의 상태를 결정하기 위해 자신의 링크 수를 방송한다. 링크 수가 가장 높은 노드가 클러스터를 관리하는 클러스터 헤드가 된다. 링크수가 높은 노드를 이용하는 것은 주변의 많은 이웃 노드로부터 정보를 수신할 수 있기 때문이다. 그리고 인접한 다른 클러스터의 노드와 통신이 가능한 노드가 게이트웨이 노드가 된다. 이렇게 노드들의 상태가 결정이 되고난 후에 소스 노드로부터 목적지 노드까지의 경로가 설정될 때 목적지 노드가 속한 클러스터의 게이트웨이 노드가 목적지 노드를 보호하는 보호 노드 역할을 수행하게 된다.

3.2 보호 노드의 선택

소스 노드가 목적지 노드와 경로를 설정하기 위하여 RREQ(Route Request) 패킷을 방송한다. RREQ 패킷을 수신한 목적지 노드와 같은 클러스터에 존재하는 게이트웨이 노드들은 자신이 보호 노드 역할을 수행하는 태그 값을 설정한 후 RREQ 패킷을 목적지 노드에 전송한다. 목적지 노드는 여러 게이트웨이 노드들로부터 수신한 RREQ 패킷 중 하나를 선택하여 RREP 패킷을 송신한다. (그림 1)은 보호 노드가 선택되는 과정을 보여주고 있다.



(그림 1) 보호 노드 선택

(그림 1)에서 보듯이 목적지 노드 E는 자신과 같은 클러스터에 속한 게이트웨이 노드 G2와 G3로부터 RREQ 패킷을 수신한다. 목적지 노드 E가 게이트웨이 노드 G2를 선택하여 경로를 설정하면 게이트웨이 노드 G2는 보호 노드 역할을 수행하게 된다. 따라서 목적지 노드 E로 가는 전체 트래픽은 보호 노드 G2를 거쳐야 하기 때문에 의심스러운 노드로 부터의 패킷

은 이 보호 노드 G2에 의해 폐기된다. 게다가 의심스러운 노드로 부터의 새로운 RREQ 역시 보호 노드 G2에 의해 폐기된다. 이러한 방식으로 DDoS 공격 에이전트가 새로운 경로를 생성하는 것을 막을 수 있다.

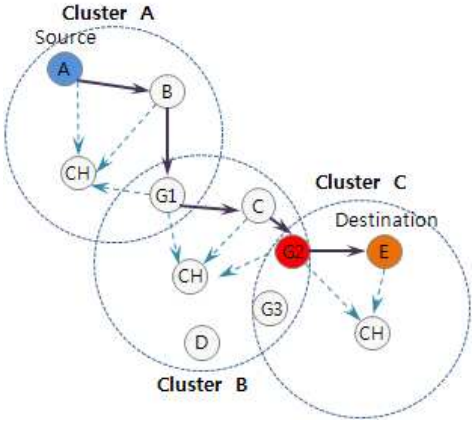
3.3 전송 정보 수집

DDoS 공격이 발생하였을 때 공격자의 위치를 알아내는 일은 쉽지가 않다. 특히 이동 노드로 구성되어 있기 때문에 공격이 탐지되었을 때 역추적이 어렵고 경로 정보의 신뢰성에 대한 문제가 있다. 따라서 정확한 역추적을 위한 경로 정보의 유지를 위해 노드들은 패킷 전송시, 자신이 속한 클러스터 헤드에게 (그림 2)와 같은 구조의 전송 정보를 송신한다.

Own IP Address	
Destination IP Address	
Hash Value	TTL

(그림 2) 전송 정보 구조

(그림 3)은 소스 노드 A가 목적지 노드 E에게 패킷을 전송할 때, 패킷을 전달하는 중간 노드들이 경로 정보를 클러스터 헤드에게 전송하는 과정을 보여주고 있다. 공격이 발생하였을 때 이렇게 수집된 경로 정보를 기초로 하여 공격자의 위치를 추적하게 된다.



(그림 3) 경로 정보 전송

그림 3에서 클러스터 A의 클러스터 헤드는 멤버 노드 A, B, G1 으로부터 수신한 전송 정보는 그림 4와 같다.

노드 A	A	B	Hash	TTL
노드 B	B	G1	Hash	TTL
노드 G1	G1	C	Hash	TTL

(그림 4) 역추적 경로 정보

그림 4에서와 같이 클러스터 헤드는 수신한 경로 정보를 근거로 패킷을 재구성하여 저장한다. 즉 클러스터 헤드는 (A, G1, Hash, TTL)의 경로 정보를 저장한다. 같은 방법으로 클러스터 헤드간의 경로 정보를 계산하면 패킷 전송 경로를 역추적 할 수 있게 된다.

4. 실험 및 결과

4.1 노드 초기화

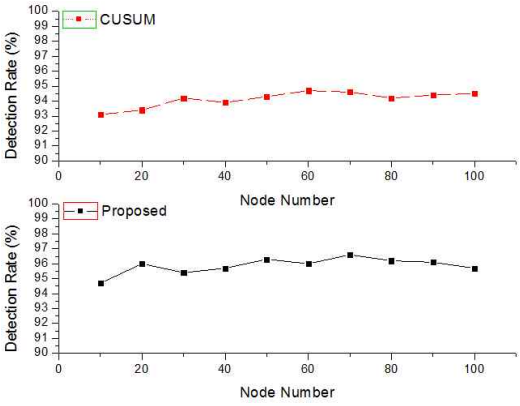
본 장에서는 제안한 기법의 효율성을 평가하기 위해 CUSUM 기법과 공격 탐지율을 비교 실험하였다. 성능 평가 기준은 공격 탐지율과 보호 노드에서 의심스러운 공격 패킷 드롭율로 하였다. 그리고 공격자 위치 추적을 위해 패킷 전송 정보를 수집하는 클러스터 헤드의 오버헤드를 측정하기 위해 메모리 사용량을 측정하였다. 실험에 사용한 환경은 <표 2>와 같고, ns-2 시뮬레이터를 사용하였다. 실험에 사용한 노드의 수는 100개이고, 각 실험 시간은 600초로 하였으며, TCP-SYN 공격 트래픽을 임의로 발생시켰다. 본 논문에서 각 노드들의 전력 소모는 고려하지 않았다.

<표 2> 실험 환경

매개변수	값
네트워크 크기	1500m × 1500m
트래픽	CBR
이동성 모델	Random way point
이동 속도	0 ~ 10 m/s

4.2 실험 결과

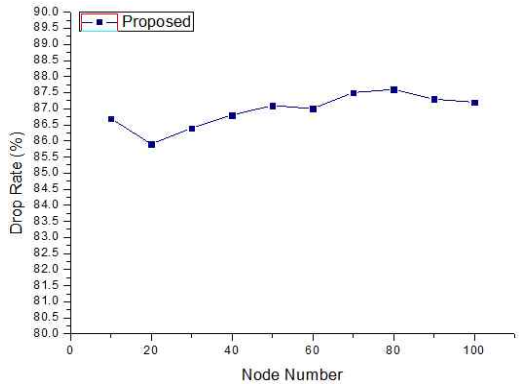
본 논문에서 제안한 기법과 CUSUM 기법의 공격 탐지율을 측정하여 (그림 5)에서 보여주고 있다. 그림에서 보듯이 제안한 기법은 네트워크내의 노드 수에 큰 영향을 받지 않고 안정되고 높은 탐지율을 보였다. 이러한 이유는 네트워크내의 보호 노드가 일정한 비율을 유지하였고 따라서 보호 노드에 의해 공격 패킷이 일부 폐기되었기 때문에 안정된 공격 탐지 성능을 낼 수 있었다.



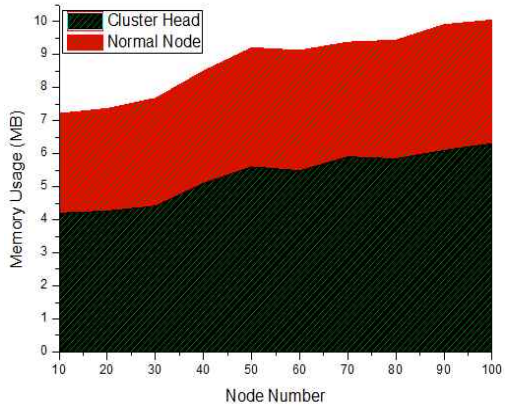
(그림 5) 공격 탐지율

의심스러운 공격 패킷이 보호 노드들에 의해 폐기되는 드롭율은 (그림 6)에서 보여주고 있다. (그림 6)에서 보듯이 노드의 수가 증가하더라도 보호 노드에 의한 패킷 드롭율은 거의 비슷한 성능을 보여주고 있으며 이것은 경로 설정시 선택된 보호 노드들이 안정된 역할을 수행하고 있음을 의미한다. 즉 공격 발생시 공격 대상이 되는 노드들의 공격 피해를 완화시켜주는 역할을 수행하는 것을 의미한다.

DDoS 공격시 공격자의 위치를 알아내기 위해 패킷을 전송하는 중간 노드들은 패킷 전송 정보를 클러스터 헤드에게 전송해야 한다. 따라서 이 정보를 수신한 클러스터 헤드의 메모리 사용량을 측정하여 클러스터 헤드에게 얼마나 많은 부하가 발생하는지 측정하였다.



(그림 6) 보호 노드의 패킷 드롭율



(그림 7) 클러스터 헤드 메모리 사용량

(그림 7)에서 보듯이 클러스터 헤드의 평균 메모리 사용량은 5.2M로 일반 노드들과 비교했을 때 크게 높지 않았다. 따라서 공격자의 위치를 찾아내기 위해 클러스터 헤드에서 저장하는 경로 정보는 오버헤드는 크지 않았고 이 정보를 이용하면 효율적인 역추적을 수행할 수 있다.

5. 결 론

이동 노드로만 구성된 MANET은 다양한 공격의 위협에 노출이 되어 있다. 그 중에서도 피해가 가장 큰 공격이 DDoS 공격이다. 본 논문에서는 보호 노드를 사용하여 DDoS 공격의 피해를 최소화시키고 공격

자의 위치를 찾아내기 위해 패킷 전송 정보를 관리하는 기법을 제안하였다. 제안한 기법은 데이터 전송을 위해 소스 노드가 경로 설정을 할 경우 목적지 노드와 같은 클러스터 내의 게이트웨이 노드가 반드시 경로에 포함되어 목적지 노드를 보호하는 기능을 수행하게 하였다. 그리고 이렇게 설정된 경로를 이용해 데이터를 전송하는 모든 노드들은 자신의 클러스터 헤드에게 패킷 전송 정보를 송신하였다. 실험을 통해 제안한 기법의 효율성을 확인하였다.

참고문헌

[1] L. Zhou and Z. Haas, Securing Ad Hoc Networks, IEEE Network Magazine Vol. 13 No. 6, pp.24-30, 1999.

[2] M. Caralho, "Security in Mobile Ad Hoc Networks," IEEE Security & Privacy, March/April 2008.

[3] I. Aad, J. P. Hubaux, E. W. Knightly, " Impact of Denial of Service Attacks in MANETs" IEEE/ACM Transactions on Networking(TON), vol. 16(4), pp. 791-802, 2008.

[4] Y. Liu and L. Shen, "Defense of DoS Attack Focusing on Protecting Resource in Mobile Ad Hoc Networks," Computer knowledge and Technology 2007 3(16), 2007.

[5] S. Noh, C. Lee, K. Choi, and G. Jung, "Detecting distributed denial of Service (DDoS) attackts through inductive learning," In Proceedings of the 4th International Conference on Intelligent Data Engineering and Automated Learning(IDEAL'03), pp. 286-295, Mar. 2003.

[6] H. Burch, "Tracing anonymous packets to their approximate source," In Proceedings of the 14th USENIX Conference on System Administration, pp. 319-328, Dec. 2000.

[7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson,"Practical network support for IP traceback," ACM SIGCOMM Computer Communications Review, vol. 30, no. 4, pp. 295-306, Aug. 2000.

[저 자 소 개]

양 환 석 (Hwan-seok Yang)

1996년 2월 호원대학교 이학사
1998년 2월 조선대학교 이학석사
2005년 2월 조선대학교 이학박사
2011년 9월 ~ 현재 중부대학교 정보보호학과 전임강사

email : yanghs@joongbu.ac.kr

유 승 재 (Seung-jae Yoo)

1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 부교수

email : sjyoo@joongbu.ac.kr