MANET 환경에서의 DDoS 공격방지 알고리즘 분석★

김동철*

요 약

본 논문에서는 MANET(Mobile Ad-hoc Network) 환경에서의 보안 요구사항과 DDoS(Distributed Denial of Service) 공격방지를 위한 보호노드(게이트웨이) 설정 알고리즘을 제시한다. 이를 위하여, 정보보호를 위한 기반기술 및 네트워크 응용기술과 보안위협을 분석하고 MANET에서 필수적으로 요구되는 보안 요구사항을 제시하며, 송신과 수신노드 사이 정보전달시 DDoS 공격을 효과적으로 방어하기 위한 보호노드 설정 알고리즘을 제시하고 성능을 분석한다. 보호노드 설정시 보호노드와 수신노드들 사이의 총링크 비용의 최대값을 최소화하는 경우와 평균비용을 최소화하는 경우로 구분하여 성능을 분석하며, 각 알고리즘의 성능을 All Enumeration 기법을 이용하여 구한 최적해와 비교, 분석한다. 분석결과, 보호노드와 수신노드들 사이의 최대비용을 이용하는 경우보다 평균비용을 이용하여 보호노드를 설정하는 경우 송신과 수신 노드들 사이의 총비용이 최소화됨을 알 수 있다.

Analysis of DDoS Prevention Algorithm in Mobile Ad-hoc Network

Kim Dong-Chul*

ABSTRACT

In this paper, the information security requirements in the mobile ad-hoc network(MANET) are presented, and the algorithm to establish the protection node(gateway) is proposed to prevent the distributed denial of service(DDoS). The information security technology and security threats in the MANET are presented, and protection node is decided to minimize the total cost through the sending nodes and receiving nodes by way of protection node. To set up the protection node, the minimization algorithms of maximum cost and the average cost between the protection node and receiving nodes are compared with the optimal solutions, in which optimal solution is found out by all enumeration method. From the results, the total cost between the sending and receiving nodes is minimized under the average cost minimization algorithm rather than the using of the maximum cost.

Keywords : MANET, DDoS, network security

접수일(2013년 2월 12일), 수정일(1차: 2013년 3월 14일), 게재확정일(2013년 3월 22일)

★ 이 논문은 2012학년도 평택대학교 학술연구비의 지원에 의하여 연구되었음.

* 평택대학교 컴퓨터학과

1. 서 론

정보기술의 급속한 발전으로 초고속 정보화시대로 진입하면서 인터넷과 네트워크가 차지하는 비중은 나날이 커져가고 있으며, 이와 함께 정보전달에 대한 위협 또한 갈수록 증가하고 있다. 한 기관의 네트워크 마비로 발생하게 되는 경제적인 피해 손실은 금액으로 표현할 수 없을 만큼 피해가 크며, 더욱이 다른 네트워크로 파급되는 위협으로 인해 발생되는 인터넷의 마비는 상상할 수 없을 만큼 그 심각성이 크다. 특히 유비쿼터스 시대[12][13][17]에서 무선 정보통신 환경에서의 데이터의 기밀성 및 무결성을 유지하고 시스템의 가용성을 보장하는 정보보호 기술이 중요시되고 있다[10][11][19].

현재 무선 이동통신 기술은 빠른 속도로 발전되고 있으며 새로운 기술의 출현과 함께 빠르게 진화되고 있다. 이러한 발전을 기반으로 스마트폰의 이용자는 계속 늘어나고 있고 스마트폰의 대중화에 따라 무선 네트워크의 사용은 쉽고 편리해졌다. 그러나 보안적인 관점에서 무선은 유선 네트워크에 비해 취약한 상태이며, 특히 향후 M2M(machine-to-machine) 통신이 보편화되어질 경우 비 인가된 디바이스들에 의한 보안 취약점이 문제가 된다. 따라서 현재 M2M 통신의 인프라로 연구되고 있는 블루투스, Zigbee, Ad-hoc 네트워크 등에서의 보안 요구사항을 제시하고 보안의 취약점 중 가장 큰 위협이 되고 있는 DDoS 공격에 대한 대응 알고리즘이 필요하다.

본 논문에서는 Mobile Ad-hoc Network(MANET) 환경에서 송신노드와 수신노드들 사이의 데이터 정보 보호를 위한 알고리즘을 제시한다. 이를 위하여 정보보호 기술과 보안 위협의 유형을 분석하고 보호노드의 설정을 통한 DDoS 공격 방지 알고리즘을 제시하며, 성능을 분석한다.

2. MANET에서의 보안

MANET은 [그림 1]에서 보는 것과 같이 중계기 역할을 하는 AP(Access Point)없이 이동 단말들로만 구성되어, 이들 노드 간에 무선으로 데이터 송수신이 이루어지는 하부 인프라 구조가 없는 네트워크를 말한다. 따라서 모든 이동 노드들은 패킷을 전달해주는 라우터 기능을 수행하여야 하며, 이로 인해 동적인 토폴로지로 올바른 라우팅 정보의 유지가 어렵고 보안 침입의 위험이 높다. MANET에서는 임의의 디바이스가 무선 통신으로 연결되며, 디바이스의 참여와 탈퇴가 자유롭게 이루어지는 환경으로 인식되고, 모든 이동 단말들이 데이터를 송신하거나 수신하는 주체임과 동시에 다른 단말을 위해 라우터로서의 기능을 병행하는 네트워크이다[1][2][3].

[그림 1] Mobile Ad-hoc Network

최근 스마트폰 시장이 활성화됨에 따라 인간이 이동 중에 ad-hoc 네트워크를 형성해 인터넷과 같은 데이터 통신 서비스를 이용하는 경우가 증가하고 있다. 따라서 실제 인간의 이동패턴에 의한 이동성 모델 환경에서 이동 ad-hoc 네트워크 라우팅 프로토콜의 성능을 평가하는 연구가 많이 이루어지고 있다[7][8][9]. 고정된 infrastructure 없이 노드들만 구성되어 있는 MANET은 다양한 분야에서 활용되고 있으며, 최근에는 국방, 항공우주 산업, 의료, 도시건설 분야, 시설물 관리 등 다양한 산업에서 도입되고 있다.

MANET의 특수한 네트워크 특성[14][15]에 따라 임의의 사용자 접근에 대한 제한이 어려우며, 악의적인 목적을 가지고 있는 디바이스의 접근에 대한 보안이 취약하다. 따라서 이러한 보안 취약점을 해결하기

위해 인증 및 암호화 키관리에 대한 연구가 이루어지고 있으며, 대표적으로 보안 라우팅 프로토콜을 포함하여 통신 경로에 대한 안전성, 참여 디바이스에 대한 인증 및 키 설립 방안에 대한 연구, 개발이 이루어지고 있다. 보안이 취약한 이유는 MANET은 노드들의 이동으로 인한 네트워크 위상이 수시로 변화하고, 모든 노드들이 라우터 기능을 수행해야 하기 때문이다.

일반적으로 정보보호는 크게 관리적 보안, 물리적 보안, 기술적 보안으로 구분되며, 여기서 기술적 관점에서의 보안은 <표 1>과 같이 공통/기반 보안 기술과 네트워크/응용 보안 기술로 나누고, 공통/기반 보안 기술은 차세대 IT 및 BT 환경에 적용 가능한 원천 기술로 정의된다[10][17].

<표 1> 정보보호 기술

항목	소분류	요소기술
공통/기반 보안	암호/인증	암호
		인증
		접근제어
	개인정보보호 및 바이오 보안	개인정보 관리
		바이오 정보관리 (얼굴, 지문, 홍채 인식 등)
	해킹/바이러스 범죄대응	해킹 및 웜/바이러스 방지
		디지털 포렌직
	보안관리	위험 관리
		시험 및 평가
		통합보안 관리
네트워크/응용 보안	인프라 보호	BcN 보안
		소프트인프라웨어 보안
		RFID/USN 보안
	디바이스 및 서비스 보호	이동통신, 지능형 로봇, u-Home 텔레매틱스, 광대역 융합
		바이오 보안 응용
		디지털콘텐츠 서비스 보안
		IT SoC 보안
		VoIP/MoIP 보안
		임베디드 소프트웨어 보안
		웹서비스 보안

반면, 네크워크/응용 보안 기술은 다양한 IT 인프라, 디바이스 및 서비스에 대한 안전성과 신뢰성을 제공하기 위한 기술을 의미한다. 여기서 접근제어란 주체(사용자 및 프로세스)가 정보 객체에 접근하려고 할 때, 주체가 가지고 있는 권한에 기초하여 접근을 허용할 것인지, 차단할 것인지를 결정하는 기술을 의미하며 크게 Discretionary Access Control(임의적), Mandatory Access Control(강제적), Roll-based Access Control(롤기반)의 유형으로 구분된다[7]. MANET 환경에서는 인프라 보호기술과 디바이스 및 서비스보호기술에 대한 사전 요구사항이 요구되며, 서비스 사용시간 노출, 위치정보 노출, 네트워크 스니핑, 단말의 취약성 노출, 서비스 사용 내용 노출 등에 대한 문제점을 해결하기 위한 연구가 수행되고 있다[4][5][6][16][18]. 예상되는 보안상의 주요 위협 문제를 요약하면 <표 2>와 같으며, MANET에서는 IP 위장, DoS 공격, 디바이스 위협 등의 보안 위협에 대한 사전 연구가 필요하다.

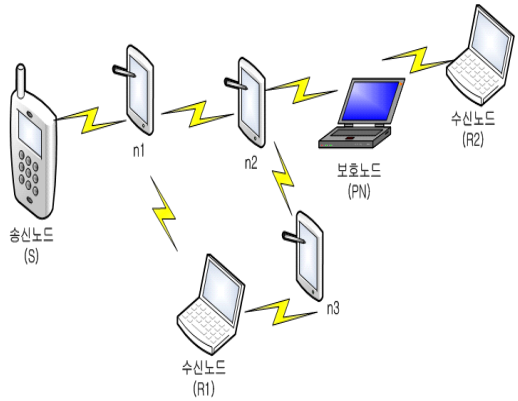
<표 2> 보안위협의 유형

분 류	보 안 위 협
신원정보 및 위치정보 노출	- 사용자의 신원 및 위치 노출 - 제 3자로의 위치정보 노출 - 도처에 존재하는 유비쿼터스 디바이스와의 정보교환시 발생
불법 접근	- 다양한 비인증 접근점 - 무선환경에서의 AP 인증없이 네트워크 접속 - 서비스 거부 공격
IP 위장	- 위장된 IP 공격 - 암호화되지 않은 전송 정보의 위협
DoS 공격	- 시스템 과부하 발생 - Ad-hoc 네트워크 구성시 발생
신호방해 공격	- 유비쿼터스 무선 디바이스간 신호 방해 공격 - 무선신호 채널의 혼선 유발
패킷 스니핑	- 패킷 캡션, 위장, 엿보기 위협 - 연동된 네트워크뿐만 아니라 내부 접속 호스트의 위협 - 무선 네트워크상에서의 패킷 스니핑 위협
트로이 목마	- 백도어 프로그램 코드 발생 - 내부 시스템의 방어 체제 침해 - 허락되지 않는 정보 획득 위협
디바이스 위협	- 다양한 디바이스의 출현으로 절도,분실,위장 - 유비쿼터스 디바이스의 인증 정보 - 디바이스의 대상 네트워크를 침해 - 과부하 공격으로 배터리 소진 - 네트워크 연결의 불가능으로 서비스거부 공격 위협

이중에서 가장 큰 취약점으로 거론되고 있는 것은 MANET에서 노드 스스로 IP 주소를 할당하는 방식을 취하는 경우 발생하며, 이 경우 노드별로 할당된 주소와의 충돌 여부를 확인하고 각 노드별로 할당된 주소가 충돌이 발생하게 될 때 악의적인 노드가 이를 이용하여 DoS(Denial of Service) 공격[14][15]을 참여 노드에게 함으로서 적절한 soure-destination 간 멀티

캐스팅과 같은 정보전달 서비스가 불가능하게 된다. 이와 같이 다양한 위협 중에서 그 피해가 매우 큰 DDoS(Distributed DoS) 공격은 크게 라우팅(routing) 공격과 패킷 포워딩(packet forwarding) 공격으로 나눌 수 있다. 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. 지금까지 MANET 환경에서 DDoS 공격을 완화하기 위하여 송신노드(소스) 노드에서 목적지(수신) 노드까지의 경로 설정시 목적지 노드와 동일한 클러스터에 속한 노드들 중 하나의 보호노드(PN: Protection Node, 게이트웨이)를 선택하여 보호노드가 목적지 노드까지 전달되는 트래픽의 게이트웨이 노드의 역할을 수행하며, 의심스러운 노드로 부터의 패킷이나 위협적인 패킷을 폐기하게 된다. 본 논문에서는 미래 다양한 디바이스들간의 정보교환의 인프라로 활용될 수 있는 MANET 환경에서 보안에 가장 취약한 DDoS 공격을 완화시키기 위해 게이트웨이 역할을 수행하는 보호노드 결정 알고리즘을 제안하며 시뮬레이션을 통하여 알고리즘의 성능을 분석한다.

[그림 2]는 보호노드를 이용한 데이터 송수신 과정을 나타낸다. 송신과 수신 노드들 사이의 데이터 정보를 보호하기 위하여 보호노드 PN을 이용하는 경우, 송신노드는 사전에 Routing Table를 이용하여 설정된 경로를 따라 수신노드 R1과 R2에 데이터를 송신한다.



[그림 2] 보호노드를 이용한 데이터 송수신

그림에서 수신노드 R1은 S-n1-n2-PN-n2-n3-R1(또는 노드간 홉수 및 지연시간 등의 비용을 고려하여 S-n1-n2-PN-n2-n1-R1이 될 수도 있음)을 통하여 데이터를 수신한다. 그리고 수신노드 R2는 S-n1-n2-PN-R2의 라우팅 경로를 이용하여 S가 보내는 데이터를 안전하게 수신한다. [그림 2]에서 보듯이 송신과 수신노드들 사이의 라우팅 테이블이 어떻게 설정되느냐와 어떤 노드를 보호노드로 설정하느냐에 따라 송신과 수신 노드들 사이의 비용(홉수, 거리, 지연시간, 링크 가중치, 거리 변이 등)이 달라진다.

3. 알고리즘

N개의 노드들 중 보호노드를 설정하기 위하여 다음과 같은 두 가지 알고리즘을 고려한다.

(1) Minimum of Maximum Cost(MMC): 데이터 수신노드들까지의 최대 비용(지연시간, 홉수, 대역폭, 거리, 지연시간의 변이, 가중치 등)을 최소화하는 노드를 보호 노드로 지정한다.

(2) Minimum of Average Cost(MAC): 수신노드들까지의 평균비용을 최소화하는 노드를 보호노드로 지정한다.

즉, MMC에서는 각 노드들에 대하여 수신 노드들까지의 비용을 구하고 이 값이 최대가 되는 비용을 구한 후 모든 노드들 중 이 값이 최소가 되는 노드를 보호노드로 설정한다. 반면, MAC에서는 수신 노드들까지의 평균 비용을 구하고 이 값이 최소가 되는 노드를 보호노드로 정한다.

알고리즘의 성능을 분석하기 위하여 다음을 가정한다.

(1) 전체 노드의 수는 400개이고 노드와 노드 사이의 비용은 0과 1사이의 uniform 분포를 따른다. 총비용은 송신노드-보호노드-수신노드들 사이의 링크 비용의 합이다.

(2) 송신노드와 수신노드는 사전에 결정되며, 보호노드와 수신노드들 사이의 경로는 라우팅 테이블로부터 결정되어 있다.

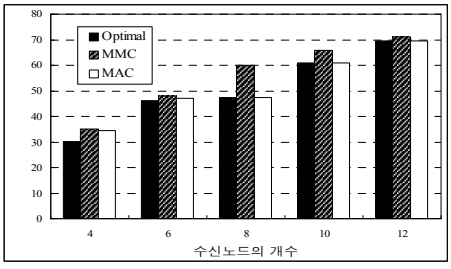
그리고 주요 수행 알고리즘을 요약하면 다음과 같다.

(1) 보호노드 결정시 노드간 비용은 변하지 않으며, 보호노드와 수신노드들 사이의 비용이 동일한 경우 홉수(노드들의 수)가 최소화되는 경로를 선택한다.

(2) 각 알고리즘의 성능을 비교하기 위하여 최적(Optimal)의 해를 구한다. 최적해는 각각의 노드를 보호노드로 가정하여 설정하는 경우 비용이 최소가 되는 노드를 선택한다.

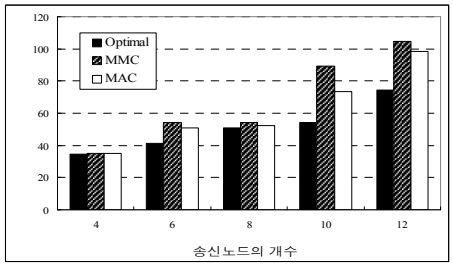
4. 성능분석

알고리즘의 성능을 분석하기 위하여 송신과 수신노드의 수를 변화시키면서 시뮬레이션을 수행하였다. [그림 3]은 송신노드(소스)의 수를 5개로 가정하고 수신노드 수의 변화에 따른 총비용을 나타낸다. 수신노드의 수가 증가함에 따라 노드들 사이의 경로의 증가로 총비용이 증가하며, 최적해에서 비용이 최소가 되고 MAC가 MMC보다 총비용이 작음을 알 수 있다. 수신노드의 수를 5개로 고정하고 송신노드의 수의 변화에 따른 총비용은 [그림 4]와 같다. 마찬가지로 송신노드의 수가 증가하면서 총비용이 증가하고 MAC의 성능이 우수함을 알 수 있다.

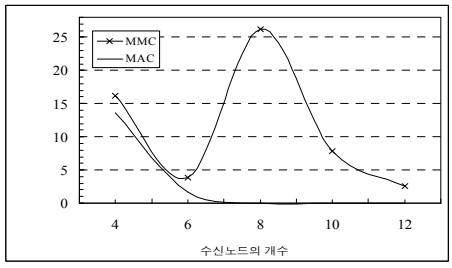


[그림 3] 수신노드의 수에 따른 총비용

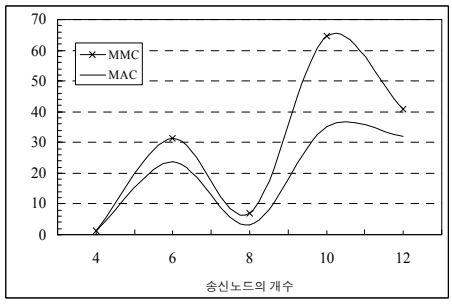
최적해와의 차이를 분석하기 위하여 알고리즘과 최적해 사이의 상대적인 총비용의 차이 ($\Delta = (measure - optimal)/optimal \times 100(\%)$) 를 나타내면 [그림 5]~[그림 6]과 같다. Δ 값은 항상 0이상이며, Δ 값이 작을수록 최적해와 가깝고, 값이 클수록 총비용이 큼을 나타낸다. 최적해와의 비교에서도 MAC 알고리즘의 성능이 MMC에 비해 우수하다. 따라서 각 노드에서 수신노드들까지의 평균비용이 최소가 되는 노드를 보호노드로 정하여 DDoS 공격을 방어하는 것이 바람직하다.



[그림 4] 송신노드의 수에 따른 총비용



[그림 5] 수신노드의 수에 따른 비용차이



[그림 6] 송신노드의 수에 따른 비용차이

결과에서 송신노드의 개수가 8인 경우 발생된 네트워크의 구조와 노드 사이의 거리 값(비용)에 대한 랜덤값의 변이로 다른 경우보다 그 차이가 다름을 알 수 있으나 일반적인 추이는 큰 변화가 없음을 알 수 있다.

5. 결 론

이동통신에 대한 수요의 증가와 함께 데이터 트래픽이 증가하고, 미래 MANET 인프라에서의 M2M 통신으로 디바이스간 상호 정보교환이 증가하게 되며, 이에 따른 보안 요구사항의 제시와 DDoS 공격방지를 위한 알고리즘 개발이 요구된다. 본 논문에서는 MANET 환경에서의 보안 요구사항과 DDoS 공격 방지를 위한 보호노드 (protection node, gateway) 설정 알고리즘을 제시하고 그 성능을 분석하였다. 보호노드의 설정을 위하여 보호노드와 각 수신노드들 사이의 최대비용을 이용하는 것 보다 평균비용을 이용하는 경우가 비용이 최소가 됨을 알 수 있었다. 향후 보호노드에서의 정보보호 요구사항의 제시와 함께, 보다 다양한 MANET 정보통신 서비스 환경에서의 시뮬레이션 성능분석이 요구된다.

참고문헌

[1] C.E. Perkins, Ad Hoc Networking, Addison-Wesley Pub., 2001.

[2] C. Siva Ram Murthy and B.S. Manoj, Ad Hoc Wireless Networks, Prentice Hall, 2004.

[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, No.4, 2008.

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

[5] M. Caralho, "Security in Mobile Ad Hoc Networks," IEEE Security & Privacy, 2008.

[6] Y. Liu and L.Shen, "Defense of DoS Attack Focusing on Protecting Resource in Mobile Ad Hoc Networks," Computer Knowledge and Technology, Vol.3, No.16, 2007.

[7] 김정훈, 정준우, 김중빈, 임재성, "생존성 향상을 위해 신뢰성 및 저피탐을 보장하는 멀티캐스팅 MAC 프로토콜 기법," 한국통신학회논문지, 제35권, 제11호, pp.1685-1695, 2010.

[8] 문종식, 변상구, 이임영, "Ad-hoc 네크워크에서 식별자를 이용한 인증 아이디에 관한 연구," 멀티미디어학회 논문지, 제13권, 제8호, pp.1202-1211, 2010.

[9] 모상만, "정적 애드혹 네트워크 멀티캐스트에서 지연시간과 에너지 소비의 트레이드오프를 위한 적응 오버레이 트리," 정보처리학회논문지C, 제16-C권, 제6호, pp.791-800, 2009.

[10] 방송통신위원회, "개인정보의 기술적, 관리적 보호조치 기준 해설서," 2010.

[11] 서동일, 정종수, 조현숙, "미래 인터넷 정보보호 요구사항," 인터넷정보학회지, 제10권, 제4호, pp.9-79, 2009.

[12] 손병희, 장종찬, "유비쿼터스 개론: 개념과 기술," ITC, 2009.

[13] 양순옥, 김성석, 정광식, "유비쿼터스 컴퓨팅 개론," 한빛미디어, 2008.

[14] 양환석, 유승재, "MANET 환경에서 DDoS 공격 완화 기법에 관한 연구," 정보보안논문지, 제12권, 제1호, pp.3-8, 2012.

[15] 양환석, 유승재, 양정모, "Distributed Mobile Agent를 이용한 침입탐지 기법," 융합보안 논문지, 제12권, 제6호, pp.69-75, 2012.

[16] 오제준, 강남희, 김용혁, 김영한, "커뮤니티 그룹 통신을 위한 효율적인 데이터 전달 트리 구성 방안," 전자공학회 논문지, 제44권, pp.55-63, 2007.

[17] 윤석규, 장희선, "u-City에서의 정보보안 설계 방안," 정보보안 논문지, 제11권, pp.37-42, 2011.

[18] 진병욱, 조인희, 한민기, 전문석, "이동 Ad-Hoc 네트워크에서 임시 인증서를 사용한 사용자 식별 및 인증 프로토콜," 한국산학기술학회 춘계 학술발표 논문집, pp.263-267, 2011.

[19] 한국인터넷진흥원 개인정보보호 실태, http://isis.kisa.or.kr.

[저 자 소 개]

김 동 철 (Dong-Chul Kim)

Brigham Young University 박사
평택대학교 컴퓨터학과 교수
관심분야 : 컴퓨터네트워크
QoS 관리
분산 시스템
네트워크 성능분석