韓國컴퓨터情報學會 論文誌
第15卷 第4號, 2010. 4.

2010-15-4-1-3

멀티미디어 콘텐츠의 서비스거부 방지 알고리즘 성능분석

장 희 선*, 신 현 철**, 이 현 창***

Performance Analysis of DoS Security Algorithm for Multimedia Contents Services

Jang Hee-Seon*, Shin Hyun-Chul**, Lee Hyun-Chang***

요 약

본 논문에서는 멀티미디어 콘텐츠 트래픽을 주고받는 노드들 사이에 상호 서비스 제공을 위한 정보보호 알고리즘의 성능을 분석한다. 먼저, 콘텐츠 유통에 필요한 정보보호 요소 기술들을 정의하고 멀티캐스팅 서비스를 이용하는 네트워크에서 기존 노드들의 그룹에 새로운 노드가 참여하는 경우를 가정한다. 그룹 가입을 위하여 노드는 그룹 식별자 주소가 필요하게 되며 이는 노드 스스로 생성하고 다른 노드들과의 중복성을 확인하는 과정에서 임의의 악의적인 노드에 의한 DoS(Denial of Service, 서비스거부) 공격이 발생된다. NS2를 이용한 시뮬레이션 분석결과, 새로운 주소를 생성하기 위한 난수값의 범위에 따라 주소 충돌횟수(DoS 공격의 최대 가능 횟수)와 다른 주소와 충돌되지 않는 신규 주소를 할당받기까지의 평균 시도횟수가 변하며, 네트워크의 규모에 따라 적정한 규모의 난수의 범위를 포함한 효율적인 알고리즘의 사전 설계가 필요함을 알 수 있다.

Abstract

In this paper, the performance of the DoS information security algorithm is evaluated to provide the multimedia traffic between the nodes using the multicasting services. The essence technology for information security to distribute the multimedia contents is presented. Under the multicasting services, a node participating new group needs a new address and the node compares the collision with the existing nodes, then DoS attack can be occurred between the nodes by a malicious node. Using the NS2 simulator, the number of DoS attacks, the average number of trials to generate new address, and the average time to create address are analyzed. From simulation results, the efficient algorithm with relevant random number design according to the DRM network is needed to provide secure multimedia contents distribution.

▸ Keyword : 멀티미디어 콘텐츠(Multimedia Contents), 서비스 거부 공격(DoS(Denial of Service) attack), 정보보호 성능분석(Information Security Performance Analysis)

• 제1저자 : 장희선 교신저자 : 이현창
• 투고일 : 2010. 03. 04, 심사일 : 2010. 03. 10, 게재확정일 : 2010. 04. 06.
* 평택대학교 e-비지니스및창업학과 교수 ** 백석문화대학 컴퓨터학부 교수 ***원광대학교 정보전자상거래학부 교수(교신저자)
※ 본 연구는 산학협동재단 2009년도 학술연구과제(2009-25)로 수행되었습니다.

Ⅰ. 서 론

WWW(World Wide Web)의 탄생으로 촉발된 인터넷 붐은 오늘날 생활주변에서 뿐만 아니라 기업, 정부에 이르는 모든 사회조직에 구조적인 변화를 초래하고 있다. Off-line 중심이 상거래 구조가 On-line 중심의 구조로 개편되어가고 사회조직 또한 가상공간을 활용하게 됨으로써 시공간을 초월한 가히 혁명적인 문화 패턴의 변화를 이끌어 가고 있다. 이러한 변화의 중심에는 사용자간 멀티미디어 데이터 전송기술이 필수적으로 요구되며 아울러 효율적인 멀티캐스트 서비스 제공이 중요시된다[3,9].

아울러 최근 정보화 시대로 진입하면서 인터넷과 네트워크가 차지하는 비중은 나날이 커져가고 있다. 이처럼 비중이 커짐에 따라 정보전달에 대한 위협 또한 갈수록 증가하게 되는데, 한 기관의 네트워크 망의 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 소위 유비쿼터스(Ubiquitous) 시대에서는 정보통신망의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 위협과 부작용에 대응할 수 있도록 정보통신 시스템 및 데이터의 기밀성(정보 유출 방지), 무결성(데이터 위조 및 변조 방지)을 유지하고 시스템의 가용성을 보장하는 정보보호 기술이 중요시된다[7].

따라서 인터넷 정보통신 기술의 발전으로 인한 인터넷 사용자의 폭발적 증가와 전자상거래를 통한 디지털 콘텐츠 유통 시장의 성장 등으로 인해 급격히 증가하는 네트워크 트래픽을 수용하고 처리하기 위해 다양한 정보보호 연구들이 수행되고 있다[4,6,8]. 정보보호의 기술은 다양한 관점에서 분류가 가능하나, 크게 관리적 보안, 물리적 보안 및 기술적 보안으로 구분할 수 있다. 관리적 관점에서 는 보안 조직, 출입 관리, 교육훈련, 보안 정책이 있으며, 보안 조직에는 시스템 운영자와 망 관리자, 사용자로 나뉘어 보안 등급에 따라 시스템 사용의 차등을 부여하게 되는데, 비인가된 사용자는 크래커나 해커로 분류한다. 물리적 관점에서 보면, 시스템 자원 보안, 응용 시스템 자원 보안, OS 보안, 인터넷 보안, 네트워크 보안으로 나눌 수 있다. 끝으로 기술적 관점에서의 보안은 공통/기반 보안 기술(암호/인증, 개인 정보보호, 보안관리 기술 등)과 네트워크/응용 보안 기술(인프라 보호, 디바이스 및 서비스 보호 기술 등)로 나뉘며 주요 요소기술로는 암호, 인증, 접근제어, 개인정보 관리, 기기 보안, 콘텐츠 보안 등을 포함한다.

특히, 멀티미디어 콘텐츠의 유통에 있어서 CDN(Contents Delivery Network) 서비스는 기존의 네트워크 구조, 설비를 변경 없이 사용하면서 콘텐츠 캐싱 기술을 이용해 네트워크간의 트래픽을 효과적으로 감소시키고 적정한 수준의 보안을 유지하며 서비스의 품질을 향상시키는 방법을 제시하고 있고, 이는 향후 새로운 네트워크 서비스의 주축으로 성장될 것으로 예측되고 있다. 그리고 이를 보완하여 분산 환경에서 디지털 콘텐츠의 저작권 관리를 보호하기 위한 DRM(Digital Rights Management) 시스템에 대한 연구가 진행되고 있다[6,9]. 본 논문과 관련하여 중복 주소 탐지 기법에 대한 연구[6,7,10,11,12]에서는 기존 서비스 노드들이 주어진 환경에서 노드들 사이에 주소 할당까지의 시간과 오버헤드를 분석한 연구들이 수행되었다. 반면, 본 논문에서는 이를 확장하여 노드들이 멀티캐스팅 서비스를 이용하는 환경을 가정하고 성능분석의 초점도 기존 연구와 달리 새로운 참여노드가 할당 받는 주소와 기존 노드들이 사용하는 주소들간의 주소 충돌횟수, 충돌로 인한 재할당 횟수 및 할당 시간을 분석하고 이로부터 효율적인 알고리즘을 설계하기 위한 방안을 제시한다.

본 연구에서는 CDN/DRM 환경에서 멀티캐스팅(Multicasting) 서비스를 이용하기 위해 공동의 그룹에 가입된 노드들 사이에 상호 멀티미디어 트래픽을 송수신하는 환경과 노드 스스로 주소를 할당하는 시스템을 가정하며, 멀티캐스팅 서비스를 제공받기 원하는 참여노드의 주소와 기존 노드의 주소를 난수와 HASH(SHA(Secure Hash Algorithm)) 알고리즘을 이용하여 생성한다[10]. 여기에서 사용되는 주소는 각각의 멀티캐스팅 그룹을 구분하는 식별자, DRM 서버의 IP 주소, 노드 ID 등의 주소를 의미하며 이는 기존 유무선 네트워크에서 이용되는 DHCP(Dynamic Host Configuration Protocol)의 중앙집중적 방법[1,5]이 아니라 MANET(Mobile Ad Hoc Network)에서 노드 스스로 IP 주소를 할당하는 방식[2]을 가정한다. 각 노드가 스스로 주소를 할당하는 경우 노드별로 할당된 주소와의 충돌 여부를 확인하게 되며 각 노드별로 할당된 주소가 충돌이 발생하게 되는 경우 악의적인 노드가 이를 이용하여 DoS(Denial of Service, 서비스거부) 공격을 참여노드에게 함으로서 적절한 멀티캐스팅 서비스를 제공받지 못하게 된다. n개의 노드들이 멀티캐스팅 서비스를 이용하고 새로운 노드가 이 그룹에 가입하기 위하여 새로운 주소를 할당받는 상황을 NS2 시뮬레이션 도구를 이용하여 구축하고 기존노드들의 수와 주소를 할당받기 위해 사용되는 난수값의 범위, 그리고 주소충돌로 인한 DoS 공격의 횟수, 그리고 난수를 이용한 노드별 평균 재할당 횟수 등의 성능을 분석하며 DoS 정보위협으로부터 노드들을 보호하기 위해 필요한 성능 파라미터 값들을 비교, 분석한

다. 분석 결과를 통하여 향후 멀티미디어 트래픽을 효과적으로 전달하기 위한 멀티캐스팅 네트워크 구조와 CDN/DRM 구조를 효율적으로 설계할 수 있을 것이다.

II. 보안 시스템 구조

기술적 관점에서 서비스를 이용하는 노드와 사용자 사이 멀티미디어 콘텐츠의 정보보호를 위한 주요 기술은 [그림 1]과 같다. 사용자의 접근 제어, 권한 관리, 유출방지 DRM, 데이터 암호화 기술 등이 포함되고 네트워크 서버 노드와 OS 그리고 시스템과 데이터베이스와의 정보 교환시 적용되는 기술로 나눈다.

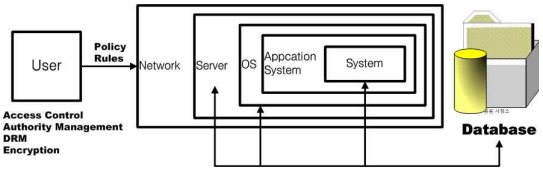

그림 1. 멀티미디어 콘텐츠 정보보호 기술
Figure 1. Security Methods for Multimedia Contents

세부적으로는 크게 공통/기반 보안 기술과 네트워크/응용 보안 기술로 나뉘며 <표 1>과 같이 요약된다. 공통/기반 보안 기술은 안전한 정보통신 환경을 구축하기 위해 필수적으로 요구되는 기술로서 차세대 IT 및 BT 환경에 적용 가능한 원천 기술(암호/인증 기술, 콘텐츠 보호 기술, 해킹/바이러스 대응 기술, 보안관리 기술 등)로 정의 된다.

표 1. 콘텐츠 정보보호 요소기술
Table 1. Technology for Contents Security

대 분 류	소 분 류	요 소 기 술
공통 기반 보안	암호/인증	암호, 인증 접근제어
	개인 정보보호 바이오 정보보호 대응	개인 정보관리 바이오 정보관리 해킹 방지 디지털 포렌직
	보안관리	위험 관리 시험 및 평가 통합 보안 관리
네트워크 응용 보안	인프라 보호	네트워크 보안 소프트인프라 보안 RFID/USN 보안
	디바이스 및 서비스 보호	기기 보안 콘텐츠 서비스 Embedded SW 웹 서비스

그리고 네트워크/응용 보안 기술은 다양한 IT 인프라, 디바이스(이동통신, Home 기기, 텔레매틱스, IPTV 등) 및 서비스(융복합, 웹콘텐츠, 의료정보 서비스 등)에 대한 안전성 및 신뢰성을 제공하기 위한 기술로서 주로 기기 보안과 서비스 보안 등의 요소기술을 포함한다.

멀티미디어 콘텐츠 정보보호 알고리즘의 성능분석을 위하여 본 연구에서는 CDN/DRM 환경에서의 멀티캐스팅 서비스를 이용하는 노드들 사이에 멀티미디어 트래픽을 주고받는 상황을 가정한다. 멀티캐스팅 서비스란 최근 UCC를 포함한 실시간 인터넷 방송, IPTV, 원격교육, 화상회의, 전자상거래, 동영상 광고, 원격 의료 서비스 등의 분야에서 송신과 수신 노드 사이 멀티미디어 데이터를 주고받는 서비스를 의미한다. 멀티캐스트 기술은 네트워크 계층의 라우팅 기술과 트랜스포트 계층의 신뢰성 제공 기술 및 멀티캐스트 응용 서비스 기술로 분류된다. 지금까지 다양한 멀티캐스트 기술이 선보여 왔으며, 멀티캐스트 통신에서는 네트워크를 통해 송신 노드가 동일한 패킷을 다수의 수신노드들에게 동시에 전달함으로써 대역폭과 지연시간 관점에서 패킷 전달의 효율을 높인다. 이는 기존 유니 캐스트 전송에서 다수의 경로 전송에 따른 대역폭 낭비를 해결하기 위한 하나의 방안으로 개발되었다. 이러한 멀티캐스트를 위해서는 서비스를 원하는 사용자가 일정한 절차를 통해 서비스 그룹에 가입하고 가입자 정보를 바탕으로 라우팅 프로토콜을 사용하여 멀티캐스트 트리를 생성하며, 이를 토대로 라우팅 테이블을 생성하고 가입자를 관리한다[6].

이러한 멀티캐스팅 서비스 제공 환경에서 기존 노드들과 멀티캐스팅 서비스를 원하는 참여노드들에게는 적절한 서비스 그룹의 주소를 할당해 주어야 하고 이를 토대로 라우팅 테이블을 관리하게 되며 이 라우팅 테이블을 기초로 노드들 사이에 멀티미디어 트래픽을 효과적으로 전송하게 된다. 이러한 네트워크 구조하에서 각각의 노드들에게 할당하는 주소는 크게 기존 유무선 네트워크에서처럼 중앙 집중적인 DHCP 서버를 활용하는 방식(Stateful)과 노드 스스로 주소를 할당하는 분산적인 구조(Stateless)로 나눈다. 지금까지 연구결과를 분석해보면, 중앙 집중적인 구조의 경우 노드의 수가 많아짐에 따라 주소할당의 효율성 면에서 성능이 떨어지며, 특히 MANET과 같은 모바일 환경에서 이동성을 지원해주는 멀티캐스팅 네트워크 구조하에서는 중앙 집중적인 방식이 매우 비효율적임을 알 수 있다[7,10]. 아울러 중앙 집중적인 서버에서 주소를 할당해 주는 방식은 제한된 자원의 사용으로 그 효율성이 떨어지며 특히 이동성을 지원해야 하는 환경에서는 이동성에 따라 노드가 요구하는 주소가 많아짐에 따라 이에 따른 효율성이 문제가 된다. 따라서 노드 스스로가 주소를 생성하

는 Stateless 방식이 최근 많이 사용되고 있다.

그러나 노드 스스로가 IP 주소를 생성하는 경우 이미 기존 노드들이 같은 주소를 사용하고 있는 지 확인하는 과정이 필요하다. 본 연구에서는 멀티캐스팅 서비스에 참여하고자 하는 노드가 새로운 주소를 할당 받고 기존 노드들과의 주소를 비교하는 알고리즘을 가정하며 이를 나타내면 [그림 2]와 같다.

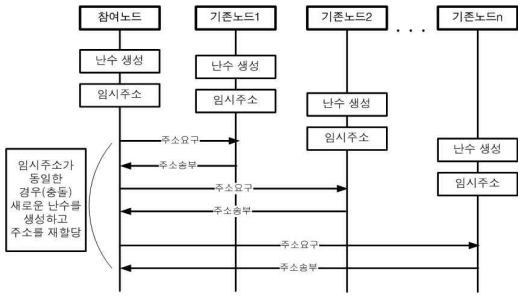

그림 2. 노드별 주소할당 흐름
Figure 2. Address Assignment Flow

노드들은 주소를 할당하기 위하여 먼저, 난수를 생성하며 이를 통하여 SHA(Secure Hash Algorithm)-1 알고리즘을 통하여 임시 주소를 할당한다. 그리고 각 노드들마다 주소를 송부 받아 비교하며 주소가 동일한 경우 충돌이 발생된 것으로 인식하여 새로운 난수를 발생하고 위의 과정을 반복하게 되며, 이 절차는 모든 노드들이 서로 충돌되지 않은 주소를 할당받을 때 까지 계속 수행된다.

노드들의 주소를 할당받기 위해 필요한 난수의 범위가 적은 경우 노드들의 주소가 충돌할 가능성이 많아지고 이로 인해 노드 사이 DoS attack의 위협이 있을 수 있다. 반대로 서비스를 요구하는 노드의 개수가 적은 경우에도 불구하고 무작정 난수의 범위를 크게 잡는다면 노드들 사이에 주소가 충돌할 가능성은 작아지나 반대로 난수값의 범위에 따른 HASH 알고리즘의 성능과 전체적인 시스템 처리시간의 성능에 영향을 미칠 수 있고 따라서 제시하고 있는 주소할당 방법에 대한 적정한 난수값의 범위 설계가 사전에 필요하다.

그리고 노드의 수가 증가함에 따라 동일한 주소를 할당하게 될 가능성이 높아지며 이와 같은 동일한 주소 할당으로 발생하게 되는 주소충돌의 횟수와 하나의 노드의 주소가 충돌이 발생한 경우 새로운 난수를 이용한 주소 할당의 반복횟수도 DoS 공격의 위협이 될 수 있다. 이는 해당 노드에서 새로운 주소를 요구받는 경우 정당한 노드가 아니면 악의적인 의도로 동일한 주소를 송부함으로서 참여노드가 서비스를 제공받지 못하게 되기 때문이다.

따라서 본 연구에서는 시뮬레이션을 통하여 노드의 수에 따른 적정한 난수값의 범위와 동일한 주소 할당으로 발생하게 되는 DoS 공격의 위협 횟수 그리고 노드별 평균 주소 재할당 횟수를 비교함으로서 멀티미디어 콘텐츠의 상호 전달에서의 정보보호 방안을 제시한다.

III. 성능분석

멀티미디어 콘텐츠의 정보보호 시스템 성능평가를 위하여 [그림 3]과 같은 네트워크 구조를 가정한다. 기본적으로 멀티캐스팅 서비스를 주고받는 기존 노드에서 하나의 참여노드가 멀티캐스팅 서비스를 제공받고자 하는 경우를 가정한다. 이를 위하여 참여노드에게 새로운 멀티캐스팅 주소(예를 들어 노드 식별자, 방문노드 주소, IP 주소, 인증 주소 등)를 할당하는 경우 기존 노드들에게 사용하지 않는 주소를 할당해주어야 한다. 이 경우 DHCP 방법이 아닌 MANET 환경에서와 마찬가지로 노드 스스로 난수와 HASH 함수를 이용하여 주소를 할당받는 경우를 가정하여 주소 중복 탐색의 경우 발생할 수 있는 주소의 충돌 횟수(DoS 공격의 발생할 가능성이 있는 빈도수)와 주소 할당시 중복으로 인한 주소 재할당 횟수와 같은 성능 치수들을 평가한다.

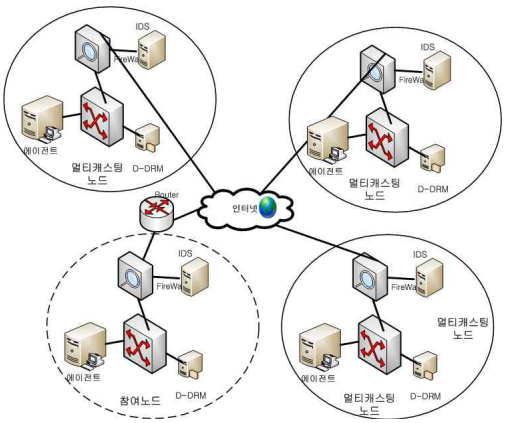

그림 3. 네트워크 구조
Figure 3. Simulation Network

노드들에게 임시 주소와 인증 주소를 할당하기 위한 방법들은 많이 있지만 본 연구에서는 SHA-1의 HASH 함수를 이용하며 주소 할당 알고리즘의 처리 절차를 요약하면 [그림 4]와 같다.

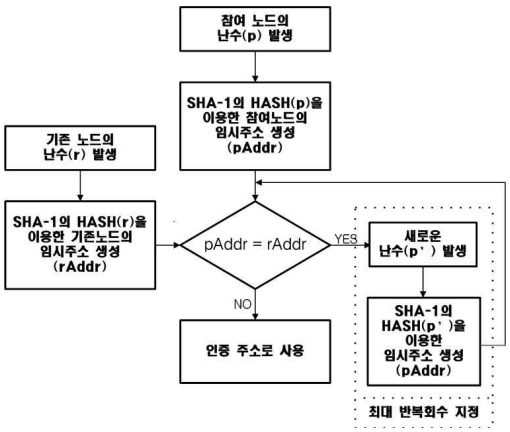

그림 4. 주소 할당 방법
Figure 4. Address Assignment Algorithm

제시된 알고리즘의 효율성을 평가하기 위한 성능분석을 위해 NS2 시뮬레이션을 수행하며 기본적인 사전 주요 가정을 요약하면 다음과 같다.

(1) 각각의 D-DRM 서버(멀티미디어 콘텐츠 정보보호 자동분석 에이전트)가 속한 도메인들에게 하나의 임시주소(예: Gateway 노드 식별자, 인증 주소, 방문노드 주소, IP 주소, 멀티캐스팅 등을 위한 주소)를 할당하며 이 주소를 통하여 해당 도메인의 콘텐츠를 이용한다.
(2) 주소 할당은 사전에 생성된 난수(0과 자연수)와 SHA-1의 HASH 함수를 이용하여 생성한다. 그리고 주소 할당시 DHCP 방법이 아닌 분산형 주소할당방식을 이용하여 노드 자체의 주소할당방식을 채택한다.
(3) 멀티캐스팅 서비스를 이용하기 위해 참여노드는 기존 노드들의 임시주소들을 검색하며 이 경우 임의의 노드에서 주소 충돌로 인해 DoS 공격을 받을 수 있다. 이 경우 최대 반복횟수를 지정([그림 4]에서 점선 부분)하며 새로운 난수와 HASH 함수를 이용하여 생성된 주소가 참여노드의 주소와 최대 반복횟수 만큼 동일한 경우 서비스를 제공(인증이 실패됨)하지 않는다.

시뮬레이션 수행시 동일한 하나의 파라미터 환경에서 신뢰도를 높이기 위하여 참여노드의 주소에 대하여 총 200번의 시뮬레이션을 수행하고 이에 대한 평균값을 기준으로 평가한다. 먼저, 기존 노드의 수에 따른 가능한 주소의 충돌 횟수를 나타내면 [그림 5]와 같다. 여기에서는 난수의 값(자연수)의 크기에 따른 충돌 횟수를 나타내었으며, 이는 참여노드의 주소와 기존 노드의 충돌로 인해 발생할 수 있는 횟수로 산출하였고 따라서 주어진 노드의 수에서 최대로 발생 가능한 DoS 공격의 수로 평가할 수 있다. 즉, 난수값의 범위가 2인 경우 0과 자연수 1을 이용한 난수 발생을 의미한다. [그림 5]의 결과로부터 난수 값의 범위가 2이내일 때는 노드의 수가 많아짐에 따라 많은 주소 충돌(DoS 공격)이 예상되며 이는 20이내의 경우와 비교할 때 평균 7배의 횟수가 증가됨을 의미한다.

멀티캐스팅 서비스를 제공하기 위해서는 소스와 노드 사이에 사전 주소할당이 신속하게 이루어져야 한다. 이를 위해서는 멀티캐스팅 서비스를 제공받기 위해 참여하는 노드와 기존 노드가 중복되지 않는 임시 주소를 할당받아야 한다. 따라서 멀티캐스팅 서비스에 참여하고 있는 노드들의 수에 따른 주소 할당 시간의 평가가 전체 서비스 성능에 주요한 평가 요소가 된다.

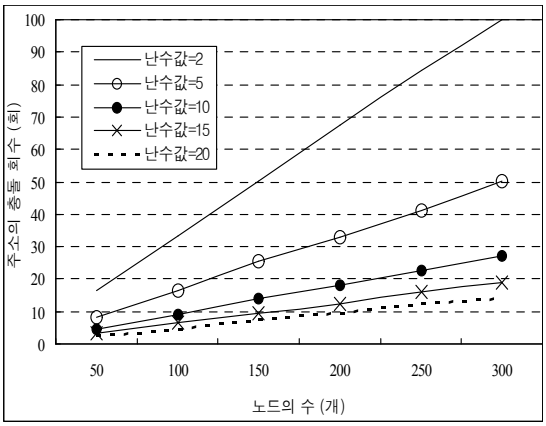

그림 5. 주소의 충돌 횟수
Figure 5. The Number of Collisions

[그림 6]은 노드의 수와 할당된 난수의 값에 따른 주소 할당 시간을 나타낸다. 시뮬레이션 컴퓨터는 Pentium 4 CPU 2.4GHz을 사용하였으며, 비교의 편의상 각각의 평가에서 HASH(난수) 알고리즘의 시간은 동일하므로 이는 시간의 합에서 제외한다. 결과에서 보듯이 노드의 수가 증가함에 따라 주소할당시간은 증가함을 알 수 있으나 난수 값이 주소할당시간에는 큰 영향을 미치지 않음을 알 수 있다. 이는 난수값의 범위로 인하여 각각의 멀티캐스팅 서비스를 제공하기 위한 도메인의 주소 할당시간에는 영향을 미치지 않으며 따라서 주소 충돌로 인한 DoS 공격 가능성을 고려한 난수값의 범위를 선택하는 것이 바람직함을 알 수 있다. 예상대로 주소 할당 시간은 충돌 횟수에 의존하며, 노드의 수와 난수값의 범위에 따라 선형적으로 증가하지만, [그림 6]의 결과에서 약간의 굴곡점이 있는 이유는 시뮬레이션을 수행하는 운영체제 처리시간의 오차로 인해 발생되는 것으로 예측된다.

기존노드 주소와의 중복성으로 인해 새로운 주소를 할당 받는 경우에도 DoS 공격의 위협이 있으며 따라서 이에 대한 분석도 필요하다. [그림 7]은 노드의 수에 따른 노드별 평균 주소 재할당 횟수를 나타낸다. 마찬가지로 난수값의 범위가 2인 경우에는 너무나 많은 재할당 횟수가 발생하므로 DoS 공격으로부터 시스템을 안전하게 보호하기 위해서는 적절한 난수값 범위 설정이 필요함을 알 수 있으며, 비교 결과 난수값이 20인 경우에 비하여 2인 경우는 평균적으로 9배 이상 서비스를 제공하기 위하여 주소 재할당이 필요함을 알 수 있다.

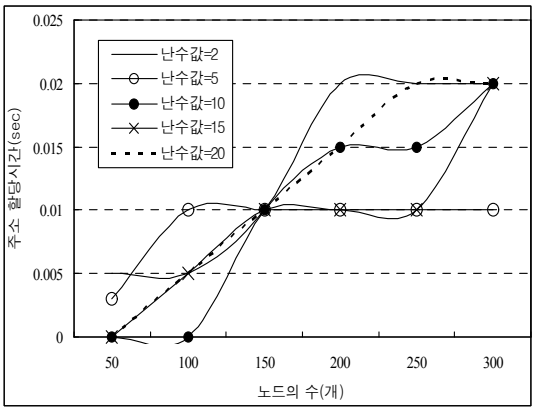

그림 6. 주소할당 시간
Figure 6. Address Assignment Time

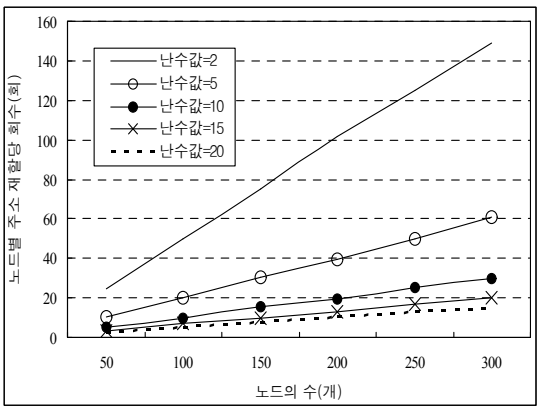

그림 7. 주소 재할당 횟수
Figure 7. The Number of Reassignments

성능분석을 통하여 주소할당을 위해 사용되는 난수값의 크기에 따른 주소충돌 횟수, 시간 및 재할당 횟수를 분석하였다. 사전에 예상했던 대로 난수값의 크기가 커짐에 따라 주소 충돌과 재할당 횟수가 감소하지만, 주소 할당 시간에는 크게 영향을 미치지 않음을 알 수 있다. 효율적인 알고리즘 설계를 위한 난수값의 설계가 필요하다. 예를 들어, 노드가 300개인 경우, 난수가 2에서 20개로 10배가 증가하면, 주소 충돌의 횟수는 86.1%가 감소하지만 재할당은 90.2%의 감소 효과가 있다. 이와 같이 모든 자원 사용(난수)에 대한 감소 효과를 측정하고 평가하여 적절한 알고리즘의 설계가 이루어져야 한다.

IV. 결 론

정보화 사회로의 진입이 가속화됨에 따라 멀티미디어 데이터 전송이 많아지고 있으며 아울러 공동의 그룹 내에서 노드들 상호 사이의 멀티캐스팅 서비스를 이용하는 사용자들이 증가하고 있다. 이러한 서비스 이용의 환경 속에서 미래에는 멀티미디어 콘텐츠의 유통이 많아질 것이며 이에 대한 정보보호의 기술들이 중요하게 되었다. 특히 유비쿼터스 환경에서는 사용자와 네트워크 사이 그리고 네트워크 내에서의 데이터베이스와의 정보교환에 대한 효율적인 정보 보호 기술이 시대의 요구에 따라 발전하고 있다. 이 중에서 사용자들 상호 멀티미디어 콘텐츠의 유통에 대한 정보보호 기술에 대하여 많은 연구가 CDN/DRM 분야에서 제시되고 있다. 본 논문에서는 멀티캐스팅 서비스를 이용하는 임의의 노드들에서 멀티미디어 콘텐츠를 전송하는데 있어서 주요 정보보호 기술 알고리즘에 대한 성능을 분석하였다. 제시된 알고리즘에서는 기존의 멀티캐스팅 그룹에 가입하려는 하나의 노드가 임의의 난수값을 이용하여 새로운 주소(멀티캐스팅 노드 식별자, 노드 주소, 그룹 식별자 등)를 할당하고 기존 노드들과의 주소 충돌을 비교하는 흐름 속에서 임의의 악의적인 노드들의 DoS 공격의 횟수(주소 충돌의 횟수)를 분석하였다. 아울러 난수값의 범위와 서비스 노드의 수, 주소 충돌까지의 시스템 소요시간 등을 분석함으로서 미래 멀티미디어 콘텐츠의 유통에 대한 정보보호 알고리즘의 사용 가능성을 타진하였다.

NS2를 이용한 시뮬레이션 분석 결과, 난수값의 2개 이내로 적게 사용하는 경우 주소 충돌의 횟수가 다른 경우에 비하여 너무 높게 발생함을 알 수 있고, 이는 그 범위가 20인 경우와 비교하여 7배나 많은 충돌이 발생되었다. 그리고 새로이 할당받은 주소가 기존 노드의 주소와 중복되는 경우 새로운 주소를 할당받으며 이의 횟수를 평가한 결과 마찬가지로 2개 이내의 난수 범위는 바람직하지 않으며 사용되는 콘텐츠의 DRM 시스템의 규모에 따라 적절한 난수 범위를 제시하여야 함을 알 수 있었다. 난수값의 범위에 따라 시스템의 서비스 개시까지의 소요 시간에 영향을 미치는지에 대한 평가 결과, 이는 해당 멀티캐스팅 도메인의 주소 할당시간과 난수값의 범위에는

큰 영향을 미치지 않으며 결국, 난수값의 범위는 주소 충돌의 횟수와 주소 재할당 횟수에 영향을 미치며, 따라서 제공되는 DRM 시스템의 규모에 따라 적정한 알고리즘 설계가 필요함을 알 수 있다.

분석한 시뮬레이션에서는 멀티캐스팅 서비스만을 가정하여 노드들 사이에 정보 보호 알고리즘의 성능을 분석하였으나, 향후 제시된 알고리즘을 사용하여 멀티캐스팅 서비스 외에도 다른 노드들과의 융복합 서비스 및 다른 기기를 사용한 서비스를 상호 교환하는 환경과 HASH 알고리즘 외에도 콘텐츠의 유통에 보다 효율적인 알고리즘의 개발이 필요하다.

참고문헌

[1] C. Bernardos and M. Calderon, "A DHCP-based IP Address Autoconfiguration for MANETs," International Conference on Ubiquitous Computing: Applications, Technology and Social Issues, 2006.

[2] H. Zhou, L. Ni and M. Mutka, "Prophet Address Allocation for Large Scale MANETs," IEEE INFOCOM, 2003.

[3] J. Novak and S. Northcutt, "Network Intrusion Detection," New Riders Publishing, 2003.

[4] R. Lippmann, J.W. Haines, D.J. Fried, J. Korba and K. Das, "The 1999 DARPA offline Intrusion Detection Evaluation," Computer Networks, Vol.34, No.4, pp.579-595, 2000.

[5] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131, March 1997.

[6] 김점구, 김태은, "CDN 환경에서 콘텐츠 보안 방법 연구," 정보보안 논문지, 제8권, 제3호, 51-56쪽, 2008년 9월.

[7] 박유미, 김윤정, "침입탐지 시스템의 탐지모듈 성능개선 방안에 대한 연구," 정보보안 논문지, 제 3권, 제 4호, 15-22쪽, 2003년 12월.

[8] 이영석, "능동 네트워크 기반의 능동 보안관리 시스템," 한국통신학회논문지, 제 29권, 제 4C호, 559-569쪽, 2004년 4월.

[9] 이창열, "MPEG-21 기반 방송 콘텐츠 유통 프로토타입 시스템 개발," 한국전자통신연구원 연구보고서, 2000년 12월.

[10] 임정미, 박창섭, "MANET 환경에서 중복 주소탐지에 대한 DoS 공격을 방지하는 보안기법과 성능평가," 멀티미디어 학회 논문지, 제 12권, 제 8호, 1099-1108쪽, 2009년 8월.

[11] 나재훈, "IPTV 컨버전스 환경에서 콘텐츠 보안 기술 동향," 정보보호학회지, 제 19권, 제 3호, 18-21쪽, 2009년 6월.

[12] 정윤수, 김용태, 박길철, 이상호, "RFID를 이용한 IPTV 사용자의 경량화 인증 프로토콜," 한국정보보호학회논문지, 제 19권, 제 2호, 105-115쪽, 2009년 4월.

저 자 소 개

장 희 선

KAIST 산업공학과(공학박사)

현재 : 평택대학교 e-비즈니스및창업학과 교수

관심분야 : 트래픽 엔지니어링

신 현 철

서울산업대학교 전자계산학과(공학사)

광운대학교 전자계산학과(공학석사)

원광대학교 컴퓨터공학과(공학박사)

현재 : 백석문화대학 컴퓨터학부 교수

관심분야 : 정보통신, 이동성관리

이 현 창

홍익대학교 이학박사

현재 : 원광대학교 정보전자상거래학부 교수

관심분야 : 웹정보시스템, 데이터웨어하우징, 시맨틱웹, 온톨로지, 유비쿼터스