IPv6 Multicast 네트워크에서 QoS 적용과 Security보장을 위한 최적화 연구

김영래*, 이효범**, 민성기**
*고려대학교 컴퓨터정보통신대학원 정보통신공학과
**고려대학교 정보통신대학 컴퓨터학과
{kkyyjj66, embryo81, sgmin}@korea.ac.kr

A study on Optimization of Using QoS and Ensuring the Security in IPv6 Multicast Network

Young-Rae Kim*, Hyo-Beom Lee**, Sung-Gi Min**
*Graduate School of Computer & Information Technology, Korea University
**Dept. of Computer Science & Engineering, Korea University

요 약

TPS(Triple Play Service)를 통한 IP-TV,인터넷, 전화 등이 통합되는 추세에서, IPv6 상용네트워크가 수 년 안에 구축될 필연성을 공감하고 있다. 그러나 [1] 현재 IP-TV 서비스에서 Delay, Jitter,전송장애 등 QoS 에 대한 사용자 불만이 계속 발생하고 있다. 또한 현재 서비스중지 (DoS : Denial of Service)를 유발하는 [2] 인터넷 침해 사고가 월 평균 2157건 이상 발생하는 등, Security Issue의 증가 문제가 지속 되고 있다. IPv4/IPv6 듀얼 스택 멀티 캐스트 네트워크를 구현하여, 라우팅, 멀티캐스트(PIM-SM), QoS, Security 이슈에 대한, 최적의 방안을 도출하여, 라우팅 구현시 IPv6 라우팅 프로토클 간에 재분배(Redistribution) 장애 해결책, IPv6 특성에 따른 멀티캐스트 그룹주소 지정시의 장애 대책을 제시하였고, QoS 에서는 기존의 QoS 정책의 문제점과 IPv6의 고유한 패킷 구조의 장점을 활용한 Adaptive QoS 방법을 제시하고, IPv6 멀티캐스트 서비스 중지 공격 유형을 정의하여, 최적화된 IPv6 멀티캐스트 구성 모델을 제시 하였다. 결론적으로 구현된 시스템에서 IPv6 패킷 분석을 통해서 최적화된 경로 통신 및 차별화된 IPv6 패킷의 QoS 방안을 제시하였으며, 서비스 중지공격을 대응하는 Security 보장성을 갖고 있음을 검증하여, 향후 상용화된 IPv4/IPv6 네트워크 구현을 위한 최적화 방안을 제시 하였다.

1. 서론

인터넷이 1994년 KORNET 를 통한 상용서비스를 시작한 이후, 2000년도12월에 [3] 디지탈화 된 동영상을, 인터넷으로 멀티캐스트 하는 서비스를 최초로 두루넷에서 시도하였다. PIM-DM 으로 서비스를 준비하여, PIM-SM 으로 서비스를 1년 정도 지속한 후 컨텐츠의 부족과 가입자 대역폭의 QoS 보장 문제로 중단하였다. 멀티캐스트가 국내 처음 시도 된지 6년이 지난 후, 가입자 대역폭 확장과 네트워크 장비의 성능이 좋아지면서, 2007년 7월부터는, [4] KT와 하나로 텔레콤에서는 멀티캐스트 기반의 IP-TV를 다시 시작하였으며, 2008년 9월부터는 지상파 방송의 재전송 및 PP(program provider) 방송도 송출이 가능할 예정이어서, 멀티캐스트 트래픽은 폭증할 것으로 예상된다. 인터넷의 빠른 확산속도 만큼 인터넷 침해 사고도 증가 하여, 2007년 한해 27,728 건의 인터넷 침해 사고가 발생하였고, 재산상의 직접적인손실이나 서비스 중지 공격(DoS) 등을 시도하는 중국을 대표로 하여, 유입되는 해킹 및 웜 트래픽은 매월 12.1 % 이상씩 증가 하고 있다. 이때 사용자의 권리는 서비스 품질 과 Security 보장이며, 이를 위해서 본 논문에서, "IPv4/IPv6 멀티캐스트 관점"에서 관련서비스에 대한 품질과 Security를 보장하는 안전한 시스템구현을 실현하기 위한 구성 요소인 라우팅, 멀티캐스트, QoS, Security 에 대한 최적화 방안을 제시하였다.본 논문의 구성은 다음과 같다. 제2장에서는 IPv4와 IPv6에서 각각 정의된 기술간의 변경사항을 살펴보고, 제3장에서는 IPv4/IPv6 멀티캐스트 네트워크에서 발생되는 문제점과 해결책을 제안한다, 제4장에서는, 관련 실험 시스템을 구축후 개선방안을 적용하여 서비스 품질을 검증 평가하고, 제5장에서는 결론을 내리고자 한다.

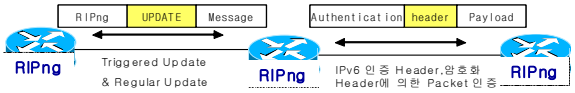
2. IPv4/IPv6기술의변경사항

IPv4 와 IPv6 프로토클은 각각 독립적으로 운영되는 프

로토클이지만, 서비스 관점에서, 사용자에게는 동일한 목적의 어플리케이션이 사용될 수 있도록 하는 프로토클이다. 그러나 패킷구조가 IPv4에서 IPv6 로 정의 될 때 적지 않은 부분이 수정, 개선되고 기능이 확장되어, 차이가 발생하는 부분이 발생 하게 된다.

2.1 IPv4/IPv6 라우팅 프로토클

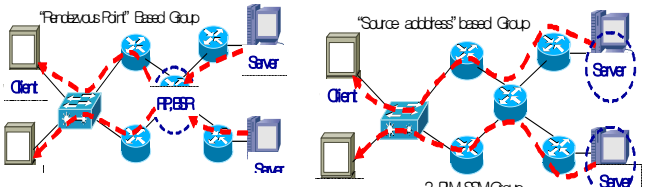
RIP에서 발전된 IPv6 표준인 [5]RIPng 에서는 triggered update 를 1~5 sec 이하의 random timer 를 설정하여 시행하며, time out 이전에 30초 간격의 regular update가 시행되었더라도 triggered update 를 시행하도록 한다. OSPFv3 에서는 기존 OSPFv2 에서 Equal Cost 에서 NextHop 주소를 작은 것을 우선하여 선택하도록 한 것을 개선하여, Routerid 를 1차 비교하여 작은 값을 선택하고, 동일한 값 일 때는 2차로 Hello packet에 포함된 interface ID를 이용해서 경로를 선택한다.



<그림 1> IPv6 라우팅에서 수정개선사항

2.2 IPv4/IPv6 멀티캐스트 프로토클

IPv6 멀티캐스트는 IPv4 멀티캐스트와 완전히 독립적으로 동작하지만 멀티캐스트 서비스를 위한 동일한 기능을 수행하며, [6] IPv6 에서의 차이점은 Group Management 기능과 멀티 캐스트 그룹의 다양성이다.

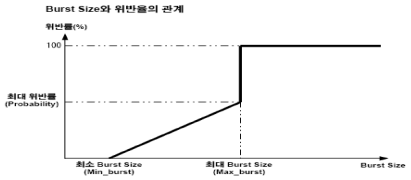


<그림 2> IPv4/IPv6 PIM-SM/SSM 프로토클의 차이점

그룹관리를 위해서는 MLD(Multicast Listener Discovery) 프로토클을 사용하는데, MLDv1 표준은 기존의 IPv4 의 IGMP기본기능과 같이 Group 의 참가 조회 및 이탈을 관리하며, MLDv2는 멀티 캐스트 네트워크의 효율적인 관리를 위하여 Filter mode를 통해서 Source주소의 Filtering 기능을 갖고 있어서 그룹관리의 효율성을 강화 하였다.

2.3 IPv4/IPv6 QoS 프로토클

All-IP 로 이행하는 과정에서, 기존의 IPv4 에서 QoS 보장은 IP precedence, Source 주소,Destination 주소 등을 검출하여 제어하였다. IPv6 에서도 기존과 같은 방식으로 QoS 제어는 가능하지만, 효과적인 QoS를 적용하기 위해서 Flow Label도 사용하도록 권장되며, [7]Flow Label을 이용하면, Source 에서 Application에 따라서 다양한 Label을 지정할 수 있어 응용이 다양하다. [8]QoS를 제어하는 방법으로는, 트래픽에 대응하는 Token(제어권)을 통제하여 트래픽의 대역폭과 Burst양을 제어하는 Token Bucket 알고리즘과 실제 트래픽 자체를 제어하는 Leaky Bucket 알고리즘이 있다. 특히 TCP 트래픽의 혼잡제어기법은 WRED 와 UPC-RED가 있으며, 아래 그림은 실제 트래픽 사용량에 근거하여 Burst 값과 위반율을 제어하는 UPC-RED 알고리즘의 구조이다.



<그림 3> QoS UPC-RED의 트래픽 제어 구조

2.4 IPv4/IPv6 Security

IPv6로 네트워크가 전환되면서 주소의 확장이외에 근본적인 패킷 구조의 변화에 따라서, 다양한 기능이 추가로 구현된 만큼 관련된 보안 취약 요소들이 많아 졌다. 특히 IPv4/IPv6 듀얼스텍을 사용할 때는 IPv6 DNS 스니핑공격 및 멀티캐스트 서비스 중지 공격이 가능하며, IPv6 Hacking 툴도 아래의 예처럼 다양하다.

DoS Tool	6tunneldos imps6tools	IPv6 Sniffer	snorts netoeek , winpCap
Worms	Slapper	Packet forgers	Speak6 , Packetit

<표1> IPv6 Hacking Tool의 종류

보안 설정을 위하여, Router 및 S/W 등에서 각각 사용하는 IPv6 어플리케이션에 따른 공격유형을 차단할 수 있는 적당한, IPv6 ACL 등 보안 설정이 반드시 필요하다.

3. IPv6 멀티캐스트 네트워크에서의 개선책

IPv4 프로토클과 IPv6 프로토클은 각각 독립적으로 정의되어 있고, 각각이 별개로 동작할 때는 각각의 독립적인 동작에 대해서는 RFC 에서도 상세히 기록이 되어 있고, 해당 기능이 네트워크 장비 업체에서도 구현되어 있어서, 문제가 발생될 확률이 적다 그러나, 그렇지만 IPv6 프로토클이 아직까지는 상용화되어 실제 네트워크에서 운용되는 사례는 많지 않은 상황이며, 관련된 RFC에 부분에서 명시적으로 표시가 되어 있지 않은 부분에서는 문제가 발생할 수 있고 해당부분과 개선 대책을 살펴보겠다.

3.1 IPv6 라우팅 프로토클

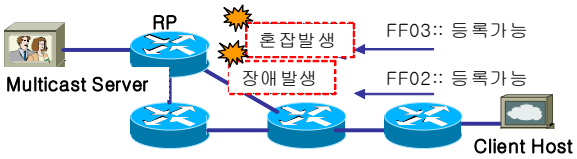
IPv6 프로토클인 RIPng(RFC2080)과 OSPFv3 (RFC 2740)가 각각 "독자적으로"로 동작할 때는 문제 발생이 가능성이 적지만, 각각의 라우팅 프로토클이 갖는 특성으로 인해서 상호 연동할때는 문제가 발생 하게될 가능성이 높아지며, IPv6 프로토클인 RIPng과 OSPFv3 를 예를들어서 상호연동시, 라우팅 프로토클간에 "재분배"할때 발생하는 아래의 문제점에 대해서 대응책을 제안한다.

문제점	IPv6 라우팅프로토클간의 Redistrabution 의 Metric 기준이 정의되지 않음
증 상	IPv6 RIPng 와 OSPFv3 간 재분배 할때 우회 경로 라우팅, 또는 루핑 현상등 장애가 발생
대응책	IPv6 라우팅간 Redistrabution 기준의 RFC 정립 및 특정 경로는 Route-Tag 지정을 통한 우선도 설정.

<표 2> IPv6 라우팅 프로토클 연동시 문제 대응책

3.2. IPv6 멀티캐스트 프로토클

IPv6 멀티캐스트는 IPv4 멀티캐스트와 가장 큰 차이점은 다양한 그룹 주소를 활용할 수 있는 IPv6 address 구조를 갖고 있는 것이며, 때로는 이것이 장애요인이 된다. 특히 Group 주소 관리 부분에서는 IPv6 RFC(3513)에서는 해당 Group 주소의 명칭은 기록이 되어 있지만, 각각의 Group 주소의 상세한 구현 및 적용시 필요한 용도와 제약 사항은 명시적으로 표현되어 있지 않다. 또한 KT,하나로 텔레콤등 ISP 사업자의 IP-TV공식 파트너 업체로 공급되는 벤더업체 들의 장비 매뉴얼 에서도 Group 주소는 RFC기준이 요약 기록되어 있어서, 실제 구현 시 문제가 발생할 수 있다.

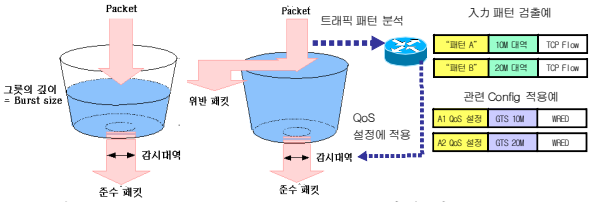


<그림 4> IPv6 Multicast에서 이슈 사항

상기와 같은 혼잡 및 장애를 방지하기 위해서는 가입자 단말이 Dynamic 하게 그룹주소를 등록하고자 할때, 단말에서 지정하여 쓸 수 없는 FF02::및 FF03::등 reserved 되어야하는 Group 주소는 사용자가 등록이 불가능하도록 RFC 에 명시되어야하며, IPv6 멀티캐스트를 구현하는 관리자는 Group 주소체계를 별도 설계를 통한 효율적인 네트워크를 구현하도록 제안한다.

3.3. IPv6 QoS

기존의 IPv4 QoS 에서 단점은 패킷헤더 길이의 가변성으로 인해서, 스트림의 변화에 따른 QoS 설정을 다이내믹하게 변경하는 것이 어렵다는 것이다. 이를 개선하여, IPv6 QoS 에서는 IPv6 패킷 구조상의 장점인 고정길이 기본헤더에 포함된, 플로우 라벨을 이용하여, 빠른 룩업이 가능하도록 스트림 Flow 패턴별로 source가 지정한 값을 [9]sFlow 등 모니터링 기능을 이용하여 적절한 QoS 정책을 트래픽에 따라서 적용하는 것이 가능하다. 즉 flow 별로 스트림 패턴에 따라서 QoS 정책을 자동으로 바꾸어 주는 Flow pattern Adaptive QoS 알고리즘을 제안한다. 아래 그림은 QoS적용시 입력 FLOW 에 따라서 트래픽을 제어하는 것을 “Leaky Bucket 알고리즘”을 예를 들었다.



<그림 5> IPv6 Adaptive QoS를 적용한 Leaky Bucket

트래픽의 패턴에 따라서 설정을 자동으로 바꾸는 것을 시뮬레이션 하기위한, 트래픽 패턴을 A,B 두개를 각각 가정하여 트래픽 패턴 A 에 적합한 QoS config를 A1, 패턴 B 에 적합한 QoS config를 B1 으로 가정하여, 입력 트래픽이 패턴 A에서 B 로 변경될 때, 설정 내역 A1을 지속 적용할 때 와 A1에서 B1으로 변경 적용할 때 각각의 특성을 비교 검증하여 검증 결과를 분석 하겠다.

3.4. IPv6 Security

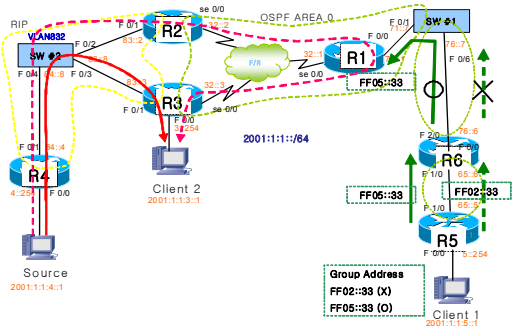
IPv6 에서의 보안 취약성을 분석하면, 기존의 IPv4 에서의 공격유형이 되는 Smurf Attack, spoof된 주소 이용 공격 등이 IPv6 에서도 똑같은 형태로 발생할 수 있고, 추가로 IPv6 에서만 발생이 되는 공격유형들이 다수 존재한다. 예를 들면 IPv6 멀티캐스트 ALL라우터 공격, DHCPv6서버 공격 후 응답정보를 이용한 simple flooding direct attack, 확장 헤더 hop by hop 옵션값 변경을 이용한 서비스 중지 공격 등이 발생할 수 있다. 이를 대응하여, Multicast에 대한 IPv6 공격 패킷으로부터 내부 자원의 공격을 방어하도록, 각각에 대한 공격유형에 맞는 IPv6 ACL 과 uRPF(Unicast Reverse Path Forwarding) 설정을 제안한다.

4. 실험 및 검증

본 장에서는 IPv6 네트워크 개선책을 적용하여, 실제 환경과 유사한 네트워크를 구현하여 개선결과 및 서비스 품질을 확인하는 것을 목적으로 검증하였다.

4.1. IPv6 라우팅 및 멀티캐스트 검증

하단 구성도에서 좌측 점선 화살표는 최적화 이전의 유니케스트 라우팅 경로이며, 실선 화살표는 최적화 설정을 적용한 이후의 경로이다.

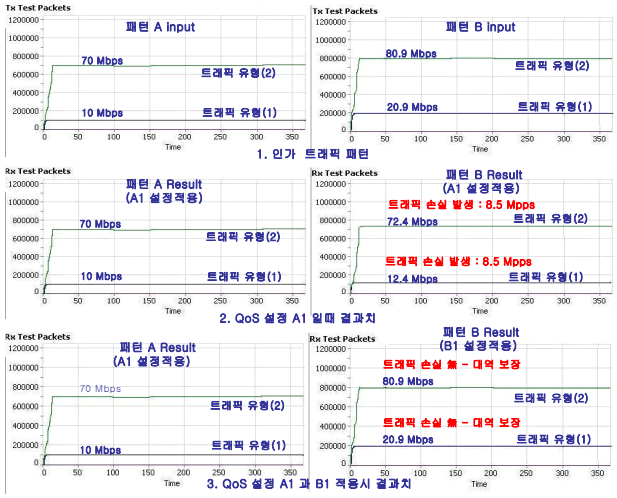


<그림6> IPv6 라우팅 및 멀티캐스트 개선결과

적용방법은 R2와 R3에 각각 상대방의 라우터에 대한

OSPF의 AD값을 RIP보다 큰 130으로 줌으로써 경로우회의 문제를 방지 한다. 이를 통해서 R2/R3 각각 RIP 정보를 우선하여 테이블에 등록하여 최적의 경로를 선택한것이 실선의 경로이다. 또한 사용자가 사용하는 것이 부적합한 Group 주소인 FF02:: 등은 설정하지 않도록 정의하고, 멀티캐스트 그룹 주소로 Scope Organization local 주소를 지정하여 최적화 하였다.

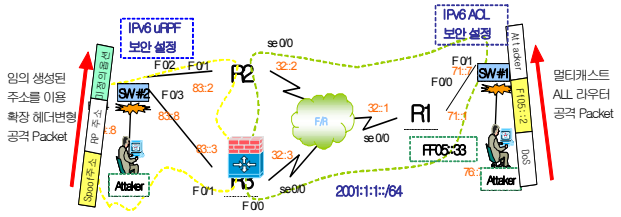
4-2. IPv6 Adaptive QoS 적용 결과



<그림7> QoS 적용 결과 검증

IPv6 트래픽을 시뮬레이션 하여 검증하기 위하여 WRED 방법과 명시적으로 대역폭 지정이 가능한 트래픽 제어방법인 Generic Traffic Shaping (GTS)을 적용하였다. 트래픽 패턴이 A->B 로 갈 때, 기존의 일반적인 QoS 방식처럼 트래픽의 패턴에 연동되지 않고, 설정이 고정적으로 적용되어 있을 때는 입력되는 트래픽 패턴과 대역폭이 바뀌어 지는 것을 검출하지 못하고, 고정적인 QoS 설정으로 인해서 인가된 트래픽에 대한 패킷 손실이 발생할 뿐 아니라, 가용 대용폭 용량도 줄어드는 현상을 확인할 수 있다. 그러나 개선된 방식에서는 A1 에서 B1 설정으로 Adaptive 하게 QoS 설정이 변경 적용 되었을 때는, (1)트래픽은 20.9M가 전송되고, 전체 가용 대역폭 용량도 약 80.9Mbps 로 증가하여, TCP 세션이 효율적으로 처리되어, IPv6 Adaptive QoS를 통해서 우수한 성능과 가용대역폭 용량이 보장되는 것을 확인 할 수 있다.

4-3. IPv6 Multicast Security 대응책 적용결과



<그림 8> IPv6 Attack 트래픽의 대응결과

IPv6 Multicast Link Local 주소를 이용하여 외부의 고의적인 IPv6 DoS Attack 트래픽이 IPv6 ACL을 통해서 Border 라우터에서 차단하였으며, IPv6 Multicast Rendezvous Point를 목적지로 하여 공격하는 Craft 된 패킷 역시도 uRPF 를 통해서 원천적으로 차단하여 내부의 자원인 Multicast라우터 및 스위치 등에 불필요한 multiple response 가 발생하여 내부 자원 소진으로 서비스 불가능 상태가 되는 것을 차단하여 안정적인 서비스를 구현하였다.

5. 결론

IPv4/IPv6 멀티캐스트 네트워크를 구현하여 IPv4 환경에서 IPv6 로 전환되는데 필수적인 고려요소인 Routing, Multicast, QoS, Security 각각에 대해서 최적화 방안을 통해서 안정성과 서비스 품질이 보장된 결과를 확인하였다. 이제 몇 년 안에는 현실에서 상용화된 IPv6 네트워크의 구축이 확산될 것으로 예상되며, 향후 Internet 트래픽 용량이 폭증하게 될 것으로, 예상됨에 따라서 네트워크 기반인프라 확장은 비용과 직결되므로, QoS의 적절한 적용을 통해서 투자규모절감(Cost Saving)이 가능하며, Green Computing 효과도 생길 것 이다. 이러한 추세에 따라 KT 에서는 기존의 CISCO 장비 외에도 2006년이후 QoS 성능과 안정성이 우수한 HITACHI 장비를 선정하여 1500대 이상을 도입하여 설치하는 이유도 납득할 수 있다. 또한 IPv6 Internet 을 통한, 유무형 재산에 관련된 개인정보가 포함된, 중요 어플리케이션이 더욱 많이 도출될 것으로 예상되므로, 응용 기능의 확장에 따라서 보안 침해 요소는 더욱 많이 발생하므로 Security 보장을 위한 선행 연구가 반드시 필요할 것이다. IPv6는 다양한 분야의 응용을 위한 무한 가능성이 있는, Flexible한 패킷 구조를 갖고 있으므로, 잘 활용할 수 있는 알고리즘이 많이 개발되어, 인류 행복을 위한 여러 가지 가치가 생성되고, 특히 국내에서, IPv6 관련 국제 표준 기술들이, 많이 도출되어 국가의 기술 경쟁력이 강화되기를 기대 한다.

참고문헌

[1] Ken, Wieland, IP TV nightmare (2007.03.28) Telecommunication Magazine
[2] 한국정보진흥원, 인터넷 침해 사고 동향및 월보 (2008.02)
[3] 정보통신 연구 진흥원, 주간 기술 동향 (1090호)2003.4
[4] 정보통신 국제 협력진흥원,IP-TV 동향 조사 보고. (2008.02.12)
[5] ietf.org,RIPng(Routing Information Protocol next generation) RFC2080
[6] Cisco Systems, IPv6 Multicast White Paper,2006
[7] ietf.org, IPv6 Flow Label Specification (RFC 3697)
[8] Radbond University, QoS and Network Layer, 2006
[9] ietf.org sFlow specification (RFC 3176)