韓國 컴퓨터情報學會 論文誌
第9卷 第4號, 2004. 12.

2004-9-4-3-5

ATM 망의 보안 패킷 지연에 관한 연구

임 청 규*

A Study on the Delays of Security Packet for ATM Network

Chung-Kyu, Lim*

요 약

개방형 통신망에서 CVR, VBR, UBR, ABR과 같은 다양한 트래픽 관리 및 지연에 관한 연구가 진행되고 있고 특히 ATM망에서는 대역폭 확장 및 트래픽 관리를 통한 망의 효율적이며 유연한 품질 서비스를 제공한다. 이러한 품질 서비스를 제공하기 위하여 트래픽에 보안서비스가 제공되어야 하며 이에 대한 연구가 진행되고 있다. 본 논문에서는 ATM 보안 그룹에 들어오는 패킷들을 안정성 기준으로 평가하고 등급으로 분류하여 안전한 패킷은 통과시키고 비안전한 패킷은 폐기 또는 마크 패킷으로 통과 시킨다. 본 논문은 스위치에서 마크 패킷을 통과 시킬때 발생하는 패킷 지연에 관한 연구 및 시뮬레이션 시나리오를 제공한다.

Abstract

A network of Asynchronous Transfer Mode (ATM) will be required to carry the traffics(CVR,VBR, UBR, ABR) generated by a wide range of services. ATM services the Quality-of-Service (QoS) management of traffice sources and bandwidth. Besides efficiency and throughput, the security services are achieved in the traffic sent in ATM network. In this paper, the scheduler evaluate and the packets sent in ATM security group. The scheduler transmits the safty packet, drop the unsafty packet and evaluate mark packet as the requirement of the delay. In this paper, we propose the scheduling algorithm of mark packet which evaluates the packet. The suggested model performance of the firewall switch is estimate simulation in terms of the delay by computer.

▸ Keyword : 트래픽(Traffic), 보안(security), 지연(Delay), 스케줄러(scheduler)

• 제1저자 : 임청규
• 접수일 : 2004.10.08, 심사완료일 : 2004.11.16
* 전북과학대학 인터넷 정보계열 조교수

Ⅰ. 서 론

초고속 정보화 사회의 기반은 ATM 기술에 기반을 둔 광대역 종합정보 통신망 (B-ISDN : Broadband Integrated Service Digital Network)이다. B-ISDN의 출현은 오디오, 데이터, 비디오와 같은 다양한 종류의 서비스들의 지원을 필요로 한다. 이러한 서비스들은 다른 트래픽 특성과 성능 요구사항을 가진 다양한 트래픽 형태를 가지고 있기 때문에 ATM 네트워크에서의 QoS 보장은 중요한 문제중의 하나가 되었다. 최고전송률, 평균전송률, 버스트니스 등의 트래픽 특성과 지연, 셀 손실률, 지터 등의 서비스 요구사항에 근거하여 ATM 네트워크는 각 응용에 필요한 자원을 할당한다.[1,7-13] 이러한 서비스를 제공하기 위하여 1988년 ITU-T는 B-ISDN을 구성하기 위한 기본 통신 방식으로 비동기식 전달 모드(ATM : Asynchrouse Transfer Mode)를 채택 하였다.

ATM 망에서는 전송하고자 하는 정보를 53 바이트 고정 길이인 셀을 분할 및 조립하여 여러 정보원으로부터 발생되는 셀을 보낼 필요가 있을 때에만 통계적 다중화하여 (Statistical Multiplexing) 하여 전송하며 패킷 헤더 부분에 목적지 정보를 부가하여 고정크기의 셀 형태로 전달된 후 원래의 정보로 복원하는 방식이다.

ATM 전송은 저속에서 고속까지 다양한 서비스를 제공하며 다음과 같은 장점을 가지고 있다. 첫째, 현존하는 서비스와 미래에 나타날 서비스를 지원하기 위한 융통성 확보가 용이하다. 둘째로는 셀 단위로 전송 할 수 있는 있기 때문에 동적인 대역폭 할당이 용이하다. 셋째로는 모든 정보 형태를 통합하여 전달 할 수 있다.

그러나 ATM의 이러한 장점에도 불구하고 컴퓨터 통신을 이용한 해커(Hacker)와 크래커(Cracker)에 의한 각종 정보 손실에 대한 위협이 커졌다. 특히 ATM망에서는 짧은 시간에 많은 자료를 해킹 및 크래킹 할 수 있어서 그에 대한 보안이 더욱 중요시 되었다. ATM 망에서는 이러한 보안의 중요성 때문에 1995년 ATM Forum에서 보안 문제에 대한 공식적인 연구가 있었으나 기존 서비스와 연관성으로 인해 1998년에 ATM Security Version 1.0이 완성되었고 2001년에는 ATM Security Specification Version 1.1 이 나오게 되었다.[2] ATM 망은 통신 매체 및 망의 성능이 향상되어 대량 및 초고속 버스트 트래픽을 전송하는데 보안 문제가 크게 대두 되었다.[8] ATM 망에서는 트래픽 관리를 위한 QoS를 제공하며 이는 트래픽 과대역 폭을 관리함을 의미하며 한정된 지원에서 대역폭을 효율적으로 관리하며 이를 통해 중요한 서비스에 대한 네트워크 품질을 보장한다.

이러한 배경하에서 ATM 망의 스위치 시스템을 통과하는 보안 패킷은 필터링 기능을 수행하는데 특정 패킷의 지연 값 분석을 하여 망에 미치는 영향에 대한 연구로 본 논문을 제시한다. 본 논문은 트랙픽 QoS 관리를 위해서 대역폭과 트래픽 문제를 유연하게 다루는 셀 스케쥴링 기능을 요구하며 이를 위한 패킷 필터링 과정을 거치면서 셀을 드롭 및 통과 시키는 기능을 수행한다. 2장에서는 ATM 망에서 요구하는 트래픽 관리와 보안에 관한 사항을 개략적으로 분석하였다. 3장에는 ATM 스위치 방화벽 처리과정과 보안 패킷 지연현상 설명하기 위한 마크 패킷 스케쥴링 처리과정을 구조 및 알고리즘으로 살펴본다. 4장에서는 제안된 알고리즘의 시뮬레이션 환경과 그 결과를 분석하고 5장에서는 본 논문의 추가연구 및 응용방향을 제시하며 결론을 맺는다.

Ⅱ. ATM 망의 트래픽 관리와 보안 서비스

초고속 멀티미디어 서비스를 수행할 수 있는 ATM 망에서의 트래피 관리 및 보안 요구 사항을 소개한다

2.1 트래픽 관리

ATM 망은 발생하는 모든 트래픽에 대해 트래픽의 중요도와 크기에 상관 없이 모든 서비스들이 경쟁적으로 대역폭 사용하며 패킷 손실 및 충돌이 발생하고 재전송에 의한 네트워크의 부하가 증가하여 네트워크 성능 저하의 원인이 되며 다음 사항을 관리한다..

① 우선순위와 대역폭 할당

사용하는 어플리케이션의 중요도에 따라서 서비스 수준을 차등화하여 대역폭과 트래픽을 정책적으로 관리한다.

② Quality of Service (QoS)

사용자 또는 어플리케이션에 대해 중요도에 따라 서비스 수준을 차등화하여 한정된 WAN 대역폭에서 트래픽과 대역폭을 정책적으로 관리하는 제반 기술 및 개념을 의미한다. 네트워크를 모니터링하고 분석하여 결과에 기반한 네트워크 관리 정책을 수립하며 한정된 자원에서 대역폭을 효율적으로 관리하며 이를 통해 중요한 서비스에 대한 네트워크 품질을 보장한다.

③ 정책 기반 QoS 스케줄링

정확한 트래픽 분류와 네트워크 분석을 토대로 요구되는 다양한 정책을 설정하고 사용자 환경에 따라 적합한 정책을 편리하게 적용 가능하다.

2.2 ATM보안 서비스

ATM Forum 의 보안 표준 1.1에 따르면 보안 요구사항을 다음과 같다.[6]

① 정보 기밀성(information Confidentiality)

정보 기밀성은 권한이 없는 사용자로부터 데이터의 보안을 위한 것으로 암호기술을 제공한다. ATM 망은 AAL레벨보다 셀 레벨에서의 기밀성 서비스를 제공하며 고정된 길이의 셀를 사용하므로 효율적인 암호화를 허용한다 . 더욱 이 셀의 Payload 만이 암호화가 되고 중간 Hop 노드에서는 복호화가 없이 망에 의해 전달 될수 있다. 이 서비스는 대칭형 암호화 알고리즘을 상요한다. 대칭형 알고리즘은 스피드, 블록 크기 및 보안 성질 등 때문에 ATM 셀 암호화를 위해서 사용한다.

② 정보 무결성 (Information integrity Service)

정보 무결성 서비스는 사용자들 간에 서로 정보를 주고받데 정보의 값 및 전송 순서 수정되지 않았음을 검증한다.

③ 정보인증(Information Authentication)

정보의 발신자와 수신자의 신분을 확인하는 보안 서비스다. 이 섭비스는 칩입 또는 스푸핑 위협으로부터의 방어를 제공한다. 이는 안전한 연결 제고, 키 교환 서비스 실현에 필수적이다 .인증 서비스는 통신하는 양자 간 또는 단 방향 등 형태로 진행된다.

④ 부인 방지 (Non-repudiation Services)

이 서비스는 사용자가 정보 서비스 와 자원에 대한 접근했음을 부인하는 것을 방지 하는 것이다.

III. 패킷 스케쥴링 과정

본 장에서는 기번적인 셀 스케쥴링 모델과 제안된 ATM 방화벽 처리 구조와 패킷 처리 지연 알고리즘을 제시한다.

3.1 기본적인 셀 스케쥴링 모델

다음 (그림 1)은 스케쥴링의 기본적인 구조를 표현하고 있다. 각각의 큐는 다른 여러 형태의 트래픽을 포함하며 이러한 큐들은 각기 하나의 출력 링크에 연결되어 있다. 스케쥴러는 출력링크 바로 앞에 노여 원하는 순서로 약간 정렬된 각각의 큐에 링크를 사용할 수 있는 권한을 부여한다. 각각의 셀 전송 슬롯에 하나의 큐만을 서비스 해야하는 것이 셀 스케쥴링의 기본적인 모델이다.[3]

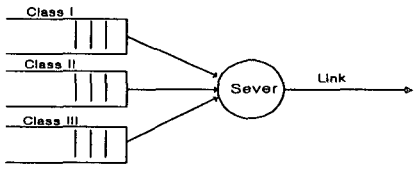

그림 1. 셀 스케쥴링의 기본적인 모델
Figure 1. Basic Model of Cell Scheduling

3.2 제안된 방화벽 스위치 모델

다음 (그림 2)는 제인된 방화벽 스위치 구조와 내부에 있는 스케쥴링 모델기법을 나타내는데 각각의 패킷은 스위치 내로 입력 되면서 스케쥴링 과정을 거친다.[4]

ATM망에서 요구하는 트래픽 관리 와 보안 서비스를 제공하며 이는 네트워크 자원을 효율적이며 유연하게 분배하여 중요한 사용자와 서비스에 대한 네트워크 품질 보장 요구를 신속하고 정확하게 반영할 수 있다. 이를 시뮬레이션 하기 위하여 스위치 개념을 일부 수정하여 모델을 제시한다. ATM 스위치 구성은 일반적으로 다음과 같은 기능으로 구성한다.

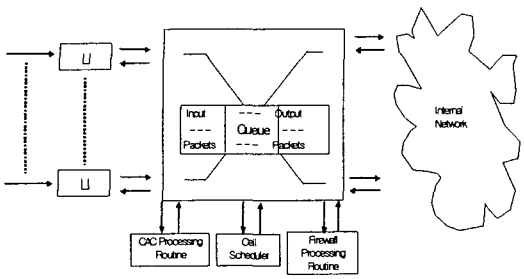

그림 2. ATM 스위치 구성
Figure 2. ATM Switch Configuration

① LI

SDH 프래임 형태의 페이로드로부터 셀을 축출하여 각 셀을 목적 포트를 결정하고 ATM망의 스위치로 보내고 셀에 부착된 내부 태그에 기록한다. 입력된 셀들은 라우팅 과정, CAC처리 루틴 및 방화벽 처리 루틴등을 수행한다.

② CAC

호 접수 및 시그널링 메시지를 처리하며 신호 메시지에 따라 망 자원을 안전한 관리를 위한 호 설정 및 대역폭 할당등의 Call 서비스 구현을 위한 향상된 기능을 제공한다.

③ 설프 라우팅 스위치

스위치 네트워크에서는 입력단에서 들어온 패킷들의 정보에 따라 셀들을 라우팅하거나 셀 헤더에 부착된 방화벽 관련 정보에 따라 셀을 방화벽 처리 루틴으로 보내어 보안을 위한 안전성 검사를 거친후에 스위치 출력단으로 보낸다.

④ 방화벽 처리 루틴

제안된 각 셀에 부착된 내부 방화벽 관련 정보를 처리하는데 안전한 셀은 스위치 출력단으로 보내게 되고 그렇지 않으면 셀을 제거한다. 이 방화벽 처리 과정은 셀 필터링 서비스 기능을 제공한다. 이 방화벽 처리 루틴은 IP 레벨 보안 기법을 제공하며 ATM 스위치의 하드웨어 요소로 합병한다. 대부분 셀 필터링서비스는 병렬적으로 정상적인 셀 처리로 수행되며 대부분 비용이 ATM 스위치의 기본비용에 포함된다.

⑤ 스케쥴러 구조

다음 (그림 3)은 방화벽 스위치 구조에서 내부로 들어오는 패킷들을 셀 스케쥴러가 일반 패킷과 마크 패킷을 전송하는 경우을 그림으로 나타낸 것 이다. 패킷 처리 알고리즘에 자세히 소개하고 있다. (그림 2)과 같이 외부 망으로부터 패킷 들이 어떻게 들어오는지를 알 수 있다. 외부 망에서 내부 망으로 들어오는 패킷들을 처리한다.

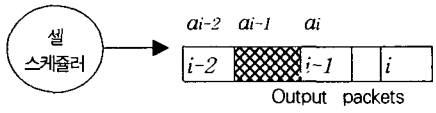

그림 3. 패킷 처리 구조
Figure 3. Packet Processing Structure

각 패킷 획득과 일련의 패킷 처리 과정을 통해서 패킷의 안전성 여부를 판단한다. 방화벽 처리과정을 통한 검사과정을 거치며 안전한 패킷은 셀 스케쥴링과정에 보낸다. 셀 스케쥴러가 안전한 패킷과 비안전성 패킷을 구분한다. 비안전성 패킷중에 공격용 패킷은 폐기하며 비공격용 폐킷을 마크 패킷 으로 분류하여 셀 스케쥴링 과정을 거치며 지연 평가 요인으로 활용한다.

3.3 패킷 처리 알고리즘

스케쥴링 알고리즘은 외부 망으로부터 들어오는 일반 패킷 처리과정과 비안전성 패킷인 마크 패킷 처리하는 과정을 Pseodo-code 로 알고리즘을 묘사한다. 스케쥴링는 큐 속에 마크 패킷을 전송함으로써 지연 값을 측정 할 수 있다. 즉 마크패킷이 전송되는 경우에 카운터 값을 증가 시킨다. 스케쥴러는 그림 1과 같이 일반 패킷의 시작 헤드 부분과 끝 부분을 QueueFront 와 QueueRear으로 설정한다. 도착하는 패킷을 도착순서로 1, 2, ... 와 같이 정한다.패킷 i 는 패킷 i-1 전송전에 도착한다. 마크 패킷으로 인한 축 지연은 다음 식을 만족 한다.[5]

for $a_i \leq t \leq$ di-1
EDi(t)-EDi(ai)=EDi-1(t)-EDi-1(ai)
따라서
EDi(t)=EDi-1(t)-{EDi-1(ai)-EDi(ai)}

(그림 4), (그림 5)와 (그림 6)는 큐내에서 패킷 처리과정을 보여준다.

```
Initially
QueueFront=0;
QueueRear =0;
AddQueue:
  if(Current Packet is Ordianry Packet)
    AddQueue()
  else
    if (AddQueue is not empty) then
       Change QueueRear Value
  end
  end
```

그림 4. 스케줄러 초기화 및 AddQueue 과정
Figure 4. Scheduler Initialization and AddQueue Processing

```
DeleteQueue:
While (Queue is not empty)
  CurrentPacket=Packet of QueueFront
  if(CurrentPacket is Ordinary Packet) then
    Transmit Ordinary Packet(P)
  else
    if(AddQueue is not Empty) then
      if(QueueFront + TransmitTime(P)
       <= C) then
      QueueFront=QueueFront+
                  TransmitTime(P)
      QueueRear=QueueRear+
                  TransmitTime(P)
      TransmitPacket(P)
      else
       Drop and TransmitOrdinary Packet(P)
      end
    else
      TransmitPacket(P)
    end
  end
end
```

그림 5. 스케줄러 DeleteQueue 과정
Figure 5. Scheduler DeleteQueue Processing

```
TransmitPacket:
if(AddQueue_length >= 2)
  Delete AddFront from AddQueue
Front=Current Position of AddQueue
  If(Front.Add < QueueFront) then
    QueueFront=QueueFront-Front.Add;
  else QueueFront=QueueFront-Front.Add
  end
  TransmitPacket(P)
else
  TransmitPacket(P)
  Delete QueueFront from AddQueue
  Front=Current Position AddQueue
  if(Front is not Null)
    and Add.Queue(QueueFront) then
    QueueFront=QueueFront-Front.ADD;
  else
     QueueFront=0;QueueRear=0;
  end
end
```

그림 6. 스케줄러 패킷 전송과정
Figure 6. Scheduler PacketTransmit Processing

Ⅳ. 시뮬레이션 및 성능분석

(그림 2)와 (그림 3)과 같이 시뮬레이션 환경을 설정하고 결과를 분석하였다. 시뮬레이션 환경에서 출력 링크 용량은 그림과 같고 각 입력 부하 량에 따른 패킷 지연 현상을 보여준다. 그리고 ATM 망의 셀 발생은 아래 식과 같이 Poisson 분포를 따르도록 하였다.

$$\Pr(\text{T시간동안에 k개 도착}) = \frac{(\lambda T)^k}{k!} e^{-\lambda T} \quad \lambda: \text{입력 부하}$$

아래의 (그림 7)은 주어진 시간안에 나타나는 밀도 값을 보여준다. 각 할당된 대역별로 시뮬레이션 결 값에 의하면 입력 부하 값인 시간에 따라 지연 값이 현격하게 낮아지고 있어서 ATM 망 트래픽의 유연성을 제공할 수 있다.

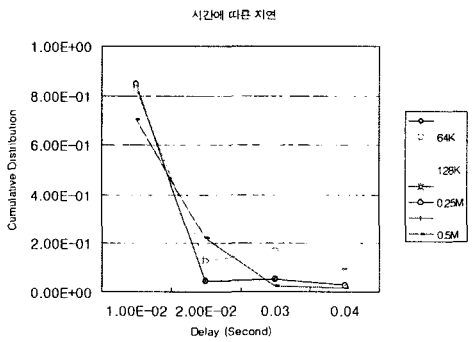

그림 7. 시간에 따른 지연
Figure 7. The Delay to second

Ⅴ. 결 론

본 논문은 ATM 망에서 다양한 사용자와 트랙픽 요구에 맞는 안정적이며 유연한 서비스를 제공할 수 있도록 마크 패킷 서비스에 대한 대역폭 별 지연 현상을 제시 하였다.

또한 마크 패킷을 서비스 할 수 있도록 스케쥴링 과정을 제안 하였다. 이런 제안들은 ATM 망에서는 트랙픽 문제와 대역폭에 유연한 네트워크 관리 정책을 서비스함으로써 네트워크 자원에 대한 효율적 분배와 네트워크 신속성 있는 서비스를 제공 할 수 있다.

이 제안은 ATM 스위치 망과 방화벽을 통과하는 패킷을 트래픽 우선 순위와 보안 우선 순위에 따른 분류 정책을 기준으로 적용 할 수 있다. 우선순위를 고려한 차등 정책을 적용하여 스케쥴링하는 패킷 필터링 기능을 반영함으로써 이에 대한 보안이 필요하다. 마크 패킷에 대한 분류와 다양한 버퍼 조건을 설정함으로써 시간당 지연 현상을 분석 비교 할 필요가 있다.

참고문헌

[1] S. Sathaye, "ATM Forum Traffic Management Specification, Version 4.0," ATM Forum Technical Committee, Mar. 1996.

[2] The ATM forum "ATM Security Specfication version 1.1".

[3] L. Zhang, "Virtual clock: a new traffic control algorithm for packet switching," ACM Trans. Computer Systems, 9(2):101-124, May 1991.

[4] 임청규, "ATM 방화벽 스위치 기반의 패킷 보안에 관한 연구", 한국컴퓨터정보학회 논문지, 8권 3호 2003년 9월.

[5] Hongyuan Shi, Harish Sethu "On scheduling Real-Time under Controlled Load Service in an Integrated Services Internet," Journal of Communications, and Networks, Vol, 5, NO, 1 March. 2003..

[6] 임청규, "ATM 망에서의 보안과 인증", 한국컴퓨터정보학회 논문지, 3권 3호 1998년 10월.

[7] Katevenis, M., Sidiropoulos, S., and Courcoubetis, C, "Weighted round-robin cell multiplexing in a general purpose ATM switch chip," IEEE J. Sel Areas Commun., SAC-9, pp. 1265-1279, 1991.

[8] Biao Chen, Gopal Agrawal, and Wei Zhao. Optimal synchronous capacity allocation for hard real-time communications with the timed token protocol. In Proc. of the 13th Real-Time Systems Symposium, pages 198-207, Phoenix, Arizona, December 1992.

[9] Abhay K, Parekh and Robert G. Gallager, "A generalized processor sharing approach to flow control in integrated services networks: The single-node case," IEEE/ACM Trans. on Networking, 1(3):344-357, June 1993.

[10] S. Jamaloddin Golestani, "A self-clocked fair queueing scheme for broadband applications," In Proc. IEEE INFOCOM'94, pages 636-646. IEEE, 1994.

[11] T. Wang, T. Lin, and K. Gan, "An Improved Scheduling Algorithm for Weighted Round-Robin Cell Multiplexing in an ATM Switch," Proc. ICC'94, Vol. 2, pp. 1032-1037, 1994.

[12] S. Archambault and J. Yan, "Performance Analysis of Per-VC Queueing," Proc. IEEE GLOBCOM'96, Vol. 3, pp. 1721-1725, November 1996.

[13] Shimonishi H, Suzuki H, "Performance Analysis of Weighted round robin Cell Scheduling and its Improvement in ATM Networks," IEICE Transactions on Communications, V.E81-B no. 5, May. 1998.

저 자 소 개

임 청 규

1986년 한남대학교 전자 계산공학과 졸업

1990년 自 由中國 (臺灣) 國立交通大學校 資訊情報工學科 工學碩士

1998년 국립 전북대학교 전자공학과 박사과정 수료

1995년 현재

전북과학대학 인터넷 정보 계열 교수