RBR을 이용한 LAN 지연 장애 검출 및 진단알고리즘에 관한 연구

조 규 억† · 안 성 진†† · 정 진 욱†††

요 약

본 논문에서는 규칙 기반 추론 기법을 이용하여 LAN 상의 지연 장애 검출 알고리즘과 장애를 유발시킨 호스트에 대한 위치 확인 알고리즘 및 장애 원인 분석 알고리즘을 제시하고자 한다. 이를 위해 지연 장애 검출 모델과 RBR 기반 장애 검출 규칙 모델을 제시하고 있다. 또한 충돌율 검출 규칙과 이용률 검출 규칙을 적용하여 지연 장애 검출 알고리즘을 설계하였고, 최대 패킷 출력 호스트 파악 규칙을 적용하여 장애 위치 탐색 알고리즘을 설계하였다. 그리고 패킷 유형 분석 규칙과 장애 원인 파악 규칙을 적용하여 장애 원인 분석 알고리즘을 설계하였다. 이를 통하여 LAN 상의 지연 장애를 검출하고 진단하는 기법을 제시하고자 한다. 이와 같이 제시한 지연 장애 검출 및 진단 기법을 실제 네트워크 환경에 직접 적용시켜 봄으로써 본 논문에서 제시한 장애 검출 및 진단 기법의 정확성과 적용성을 확인하였다. 이러한 기법은 네트워크 관리자가 LAN 상의 장애를 진단하고 원인을 해결하는데 큰 도움을 줄 것으로 기대된다.

A Study on the Algorithms for Delay Fault Detection and Diagnosis on LAN based on RBR

Kyu-Oak Joe† · Seong-Jin Ahn†† · Jin-Wook Chung†††

ABSTRACT

This paper proposes algorithms for fault detection and diagnosis, and to find out from where the problem is issued on LAN by using RBR. Model for delay fault detection and RBR based rules are shown to take care of. Also, it has been designed a algorithm for delay fault detection by applying collision and utilization tracing rules, and a location algorithm against faulty host by analyzing maximum packet generating hosts. And fault analysis algorithm has been designed by rules for packet types and fault reason analysis. The proposed rules, which are the algorithms for delay fault detection and diagnosis, are experimented on real network environments. From this experiments, the correctness and applicability are confirmed. The proposed algorithms contribute to solve various problems on LAN, and are helpful to a network manager.

1. 서 론

최근 컴퓨터 통신 기술이 발달함에 따라 네트워크는 점차 방대하고 복잡해지게 되었고 이에 따라 네트워크 장애 발생에 대한 검출과 위치 확인이 어려워지고 있다. 그러나 신속한 장애 검출과 진단은 네트워크 장애로 인한 심각한 문제를 해결하고 네트워크의 신뢰성을 향상시키는데 중요한 요소가 될 수 있다[1].

특히 LAN 상의 응용 프로그램들의 사용 증가는 트래픽의 병목 현상을 보이는 WAN 뿐만 아니라, LAN 상의 트래픽 양을 크게 증가시키게 되었고, 네트워크 전체의 지연을 초래하게 된다. 따라서 LAN 상의 장애 원인의 신속한 검출 및 진단 없이 네트워크 장비에 대

† 준 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터공학부
†† 종신회원 : 성균관대학교 컴퓨터교육과 교수
††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터공학부 교수
논문접수 : 2000년 6월 23일, 심사완료 : 2000년 7월 26일

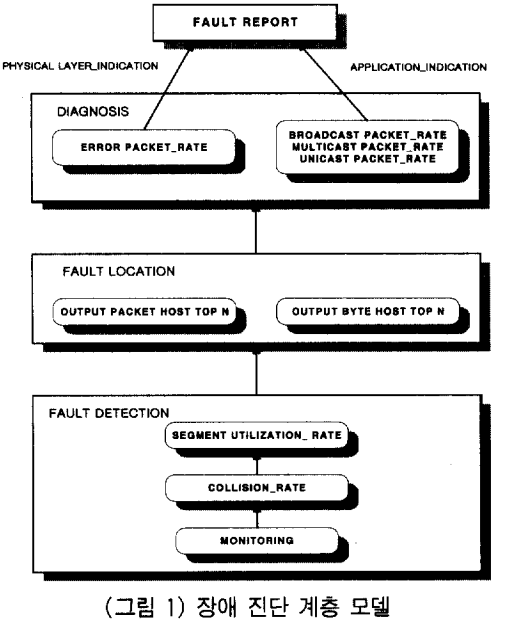
한 과다한 투자를 통하여 장애를 해결하려고 한다면 효율적인 네트워크 관리를 위한 해결책이 될 수 없다. LAN 상의 효율적인 장애 관리는 장비의 투자 및 유지 보수 비용을 낮추고 성능을 최대로 유지하는 것이기 때문이다[2, 3].

LAN 상의 장애 관리의 필요성이 증대됨에 따라 네트워크 장애 관리를 위해 현재 많은 연구가 진행 중이며 네트워크 장애에 효율적으로 대처하는 방안이 제안되고 있다[4, 5]. LAN 상의 장애에는 크게 하드웨어 장애와 소프트웨어 장애가 있다. 하드웨어 장애로는 전력 장애, 네트워크 케이블의 물리적인 단절, 라우터나 게이트웨이와 같은 주요 네트워크 구성 요소들의 장애 등이 있다. 이와 같은 하드웨어 장애는 많이 알려져 있어서 명확하게 정의되어 있고 또한 검출을 위한 HP OpenView, IBM Netview, NetLabs DiMONS 그리고 SunNet Manager와 같은 많은 NMS도구가 있다. 그러나 소프트웨어 장애는 장애에 대한 정의가 명확하지 않기 때문에 장애를 검출하고 진단하는데 어려움이 있다. 일반적으로 알려진 소프트웨어 장애로는 네트워크의 성능 저하나 네트워크 대역폭의 손실 등이 있다[6]. 이와 같이 장애에 대한 정의가 명확하지 않기 때문에 본 논문에서는 네트워크의 급격한 성능 저하를 장애로 간주하고 이에 대한 관점에서 장애를 검출/진단하고 통보하는 방법론을 제시한다. 따라서 네트워크의 급격한 성능 저하를 감지하고 이것이 장애인지를 파악하기 위해서는 규칙이나 사례 기반의 장애 진단 방법론이 필요하다[7, 8]. 그러나 사례 기반의 CBR을 이용한 네트워크 장애 진단 방법은 실시간으로 동작하는 네트워크 환경에서 규칙 기반의 RBR에 비해 관리 시스템에 부하를 줌으로써 이질적이고 급변하게 변화하는 환경에 빠른 대응을 하지 못한다[9].

따라서 본 논문에서는 규칙 기반의 RBR(Rule-Based Reasoning)을 이용하여 네트워크 성능 저하나 대역폭의 손실에 따른 LAN 상의 지연 장애를 검출하고 장애 발생 위치를 확인함으로써 LAN 상의 지연 장애 관리에 대해 보다 효율적으로 대처하고자 한다. 이를 위해 우선 LAN 상의 네트워크 성능 저하나 대역폭의 손실에 직접적인 영향을 미치는 충돌(Collision)율과 선로이용률을 파악한다. 충돌율과 선로이용률이 임계값을 넘을 경우 장애가 발생한 것으로 파악하고 장애 검출 규칙에 따라 장애를 검출하고 장애 발생 위치를 확인[10, 11]하여 관리자에게 통보하는 규칙 기반의 네트워크 지연 장애를 설계하였다. 그리고 이에 대한 실험을 통해 RBR기반의 네트워크 지연 장애 검출 기법에 대한 검증을 하였다.

2. 네트워크 지연 장애 검출 모델

LAN 상의 장애로 일반적으로 정의하고 검출할 수 있는 것으로는 전력 장애, LAN 케이블의 물리적인 단절, 라우터나 게이트웨이와 같은 주요 네트워크 구성 요소들의 장애 그리고 각 단말 시스템의 장애 등을 들 수 있다. 이러한 장애는 많이 알려져 있어서 명확하게 정의되어 있고 또한 검출을 위한 많은 NMS 도구가 있다. 그러나 실제적으로 LAN 장애 관리를 하는데 있어서 어려운 점은 성능 저하로 인한 장애라고 볼 수 있다. 이러한 장애는 사용자마다 관점의 차이가 있을 수 있고, 명확하게 장애 분석 항목에 대한 체계적인 정의가 되어 있지 않기 때문에 LAN 관리자가 능동적으로 대처하기가 힘들다. 따라서 본 논문에서는 먼저 네트워크의 급격한 성능 저하를 장애로 간주하고 이에 대한 관점에서 장애를 검출/진단하고 통보하는 장애 검출 모델을 제시한다. 이를 위해 우선, 장애 관리를 효과적으로 수행하기 위한 장애 분석 항목을 정의하고 이를 규칙 기반의 추론 과정을 바탕으로 유기적으로 연결하여 장애 검출을 위한 모델을 확립하였다.



(그림 1) 장애 진단 계층 모델

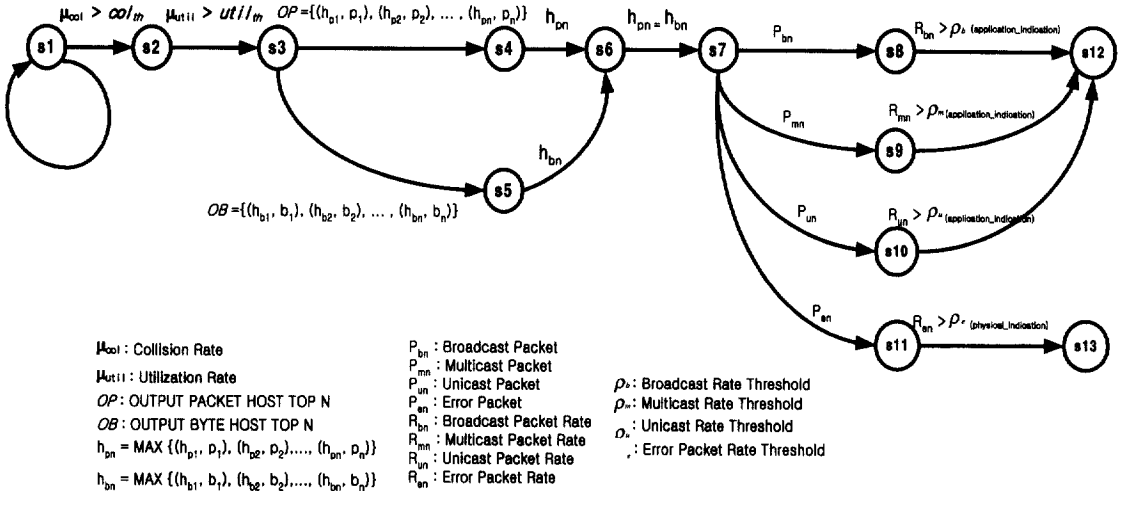
(그림 1)은 LAN 지연 장애 관리를 위해 적합한 장애 분석 항목을 기반으로 장애 검출과 장애 위치 확인 및 진단 그리고 장애 보고 과정을 체계적으로 수행할 수 있도록 확립된 장애 진단 계층 모델을 나타내고 있다. 그림에서 보는 바와 같이 LAN 상의 지연 장애 검출은 LAN 세그먼트 장애 검출에서부터 시작된다. LAN 세그먼트 장애 검출은 세그먼트 상의 충돌율과 이용률을 주기적으로 분석하여 허용치 이상이 되면 장애로 판단하고 장애를 유발시킨 호스트를 찾기 위한 장애 위치 확인 과정으로 전이한다. 장애 위치 확인 과정은 세그먼트 상의 각 호스트에 대한 출력 패킷과 출력 바이트를 모니터링하고 가장 많은 패킷을 발생시킨 호스트를 순위별로 분석한다. 순위별 분석을 통하여 세그먼트 상의 지연을 유발시킬 정도의 패킷을 출력하는 호스트를 찾아내고, 이 호스트에 대하여 장애 유발의 원인을 찾는다. 이 과정은 호스트 장애 진단 과정에서 진행된다. 즉, 지연의 원인이 된 패킷을 유형별로 분석한다. 호스트가 출력한 패킷이 브로드캐스트, 멀티캐스트, 에러 없는 유니캐스트 패킷이 다수를 차지한다면 이는 응용 서비스 상의 장애를 의미하고 이에 대한 처리는 응용 서비스 장애 진단 과정에서 수행한다. 만일 호스트가 많은 양의 에러 패킷을 출력한다면 이는 물리 계층의 인터페이스 카드나 선로 상의 장애를 의미하고 이에 대한 처리는 물리 계층 장애 진단 과정에서 수행한다. 그리고 응용 서비스 장애 진단 과정과 물리 계층 장애 진단 과정에서 검출된 장애를 관리자 계층에게 통보함으로써 LAN 상의 지연 장애를 검출하고 네트워크 관리자는 이에 대한 적절한 조치를 취하게 된다.

3. 네트워크 지연 장애 검출 규칙

LAN 상의 응용 프로그램들의 사용 증가는 트래픽의 병목 현상을 보이는 WAN 뿐만 아니라, LAN 상의 트래픽 양을 크게 증가시키게 되었고, 이로 인한 대부분의 장애 요소는 LAN 내부에서 원인이 발생된다[12]. LAN 상의 트래픽 양의 증가로 인하여 패킷 충돌율이 높아지고 선로 이용률이 높아짐으로써 네트워크 지연이 발생할 가능성이 높아진다. 따라서 충돌율과 이용률이 높게 발생하는 원인을 찾아서 해결해야 한다. 이를 위해 장애 검출을 위한 장애 검출 규칙을 세우고, 장애 검출 규칙에 따라 장애를 검출하고 장애를 유발시킨 호스트를 찾는다. 그리고 장애를 진단함으로써 장애의 원인을 정확하게 규명하고자 한다.

본 논문에서는 네트워크 장애 검출을 위한 RBR 기반의 검출 모델을 세우고, 이를 바탕으로 한 규칙을 기반으로 상태 천이를 설명하고 있다.

(그림 2)은 이러한 RBR 기반의 장애 검출 규칙 모델을 나타내고 있다. 장애 검출 규칙 모델의 각 상태는 장애 검출의 분석 과정을 나타내고 있고, 13개의 상태로 나누어서 표현하였다. 각 호는 상태에서 분석된 결과를 나타내는 것으로 다음 상태에 필요한 요소



(그림 2) RBR에 의한 LAN 상의 트래픽 지연 장애 검출 규칙 모델

를 표현하고 있다. 또한 상태 천이를 위한 규칙도 포함하고 있다.

각 상태에 대한 정의와 천이는 <표 1>에서 설명하고 있다.

〈표 1〉 RBR 기반의 장애 검출 모델의 상태 및 천이

단계	상태 천이	상태 천이 원인	상태 정의
검 출 단계1	S1→S2	충돌율의 임계값 초과	S1 : 충돌율 분석 S2 : 이용률 분석
검 출 단계2	S2→S3	이용률의 임계값 초과	S3 : 호스트 패킷/바이트 출력량
검 출 단계3	S3→S4	호스트의 패킷 출력 순위별 분석	S4 : 순위별 호스트 패킷 출력 순위
	S3→S5	호스트의 바이트 출력 순위별 분석	S5 : 순위별 호스트 바이트 출력 순위
검 출 단계4	S4→S6	패킷 출력량이 가장 많은 호스트 도출	S6 : 순위별 호스트 바이트와 패킷 출력량 비교
	S5→S6	바이트 출력량이 가장 많은 호스트 도출	
검 출 단계5	S6→S7	패킷 출력량이 가장 많은 호스트와 바이트 출력량이 가장 많은 호스트가 같은 호스트	S7 : 출력 패킷 유형별 분석
검 출 단계6	S7→S8(S9, S10)	출력 패킷이 브로드캐스트, 멀티캐스트, 에러 없는유니캐스트	S8 : 브로드캐스트를 발생시킨 응용 서비스 분석 S9 : 멀티캐스트를 발생시킨 응용 서비스 분석 S10 : 에러 없는 유니캐스트를 발생시킨 응용 서비스 분석
검 출 단계6	S7→S11	출력 패킷이 에러 패킷	S11 : 에러 패킷을 발생시킨 물리 계층의 인터페이스 카드나 선로 상의 장애
검 출 단계7	S8(S9, S10)→S12	응용 서비스에 의한 장애로 진단	S12 : 장애 유발 응용 서비스 분석
	S11→S13	물리 계층의 장애로 인한 장애 진단	S13 : 물리 계층의 장애 분석

<표 1>에서 보는 바와 같이 검출 단계1은 S1에서 충돌율 분석을 통하여 장애 발생 여부를 진단하고 충돌율이 임계값 이상이 되었을 때 S2로 천이하는 단계이다. 검출 단계2는 S2에서 이용률을 분석하고 이용률이 임계값 이상이 되었을 때 S3로 천이한다. 검출 단계3은 세그먼트 상의 패킷 수를 많이 유발시킨 호스트의 패킷 및 바이트 출력을 순위별로 분석하는 단계이고, 검출 단계4는 검출 단계3에서의 순위별 분석을 통하여 패킷 및 바이트 출력량이 가장 많은 호스트를 도출하는 단계이다. 또한 검출 단계5는 패킷 출력량이 가장 많은 호스트와 바이트 출력량이 가장 많은 호스트를 비교 분석하여 가장 많은 패킷과 바이트를 출력한 호스트를 최종적으로 추출해낸다. 검출 단계6은 세그먼트 상의 지연 장애를 유발시킨 호스트가 어떤 종류의 패킷을 유발시키는 지를 파악하는 단계이다. 즉, 출력 패킷이 브로드캐스트, 멀티캐스트, 에러 없는 유니캐스트 패킷인지 아니면 에러 패킷인지를 구분하는 단계이다. 검출 단계7은 검출 단계6에서의 분석을 통하여 세그먼트 상의 지연을 유발시킨 원인이 응용 서비스에 의한 것인지, 물리 계층의 인터페이스 카드나 선로 상의 장애에 의한 것인지를 진단하고 이를 바탕으로 장애의 원인을 분석하는 단계이다.

3.1 충돌율 검출 규칙

LAN 상의 지연 장애를 발생시키는 중요한 원인 중의 하나가 충돌율이다. 따라서 충돌율을 산출함으로써 LAN 상의 네트워크 지연 장애 여부를 검출할 수 있다. 검출 단계1에서는 충돌율을 분석하고 이것을 임계값과 비교하여 임계값 이상이면 장애 발생으로 진단하고 세그먼트 이용률 분석 과정인 S2로 넘어간다. 임계값보다 낮으면 충돌율 분석 과정을 주기적으로 되풀이하면서 네트워크 장애 발생 여부를 진단한다.

(그림 3)은 이에 대한 검출 규칙을 나타내고 있다.

BEGIN S1 IF $\mu_{col} > col_{th}$ OR $\mu_{col} = col_{th}$ THEN GO S2 ELSE GO S1 END	
μ_{col} : Collision Rate	col_{th} : Collision Rate Threshold

(그림 3) 충돌율을 이용한 장애 검출 규칙

3.2 이용률 검출 규칙

검출 단계2에서는 충돌율을 통해 장애 발생을 감지하면, 이를 바탕으로 현재 세그먼트 상의 이용률을 파악한다. 이용률을 분석하고 이것을 임계값과 비교하여 이용률이 임계값 이상이면 충돌률과 이용률에 의해 네트워크 지연 장애가 발생했음을 파악하게 된다.

(그림 4)는 이에 대한 검출 규칙을 나타내고 있다.

BEGIN S2 IF $\mu_{util} > util_{th}$ OR $\mu_{util} = util_{th}$ THEN GO S3 ELSE GO S1 END	
μ_{col} : Collision Rate	$util_{th}$: Utilization Rate Threshold

(그림 4) 이용률을 이용한 장애 검출 규칙

3.3 최대 패킷 출력 호스트 파악 규칙

검출 단계3에서는 세그먼트 상의 각 호스트에 대한 출력 패킷 순위별 분석 및 출력 바이트 순위별 분석을 통하여 장애 유발 호스트를 분석한다. 검출 단계4에서

는 검출 단계3에서 파악한 출력 패킷 및 바이트 순위별 호스트들에 대하여 패킷을 가장 많이 발생시킨 호스트와 바이트를 가장 많이 발생시킨 호스트를 도출해 낸다. 일반적으로 패킷을 가장 많이 발생시킨 호스트와 바이트를 가장 많이 발생시킨 호스트는 같으므로 검출 단계5에서는 이를 확인한다. 즉, 패킷을 가장 많이 발생시킨 호스트와 바이트를 가장 많이 발생시킨 호스트를 비교 분석하고 두 호스트가 같은 호스트인지를 파악한다. 두 호스트가 같은 호스트이면 이 호스트가 세그먼트 상의 지연 장애를 유발시킨 호스트라고 판단하게 된다.

(그림 5)는 이에 대한 검출 규칙을 나타내고 있다.

BEGIN S3	
IF OP_c = OP_p THEN GO S4	
IF OP_c = OP_b THEN GO S5	
IF S4(MAX(h_{pn}) THEN GO S6	
IF S5(MAX(h_{bn}) THEN GO S6	
IF S6(h_{pn} = h_{bn}) THEN GO S7	
END	
OP_c : 현재 출력 유형	h_{pn} : 패킷 출력 호스트
OP_p : 패킷 출력	h_{bn} : 바이트 출력 호스트
OP_b : 바이트 출력	

(그림 5) 최대 패킷 출력 호스트 파악 규칙

3.4 호스트 출력 패킷에 대한 유형별 분석 규칙

검출 단계6에서는 지연 장애의 원인이 된 호스트가 발생시키는 패킷을 유형별로 분석하는 단계이다. 패킷 유형을 브로드캐스트, 멀티캐스트, 에러없는 유니캐스트 그리고 에러 발생 패킷으로 구분하여 브로드캐스트율, 멀티캐스트율, 유니캐스트율 그리고 에러 패킷율을 분석한다.

(그림 6)은 이에 대한 검출 규칙을 나타내고 있다.

BEGIN S7	
IF P_{cn} = P_{bn} THEN GO S8	
IF P_{cn} = P_{mn} THEN GO S9	
IF P_{cn} = P_{un} THEN GO S10	
IF P_{cn} = P_{en} THEN GO S11	
END	
P_{cn} : 출력 패킷	P_{un} : 유니캐스트 패킷
P_{bn} : 브로드캐스트 패킷	P_{en} : 에러 발생 패킷
P_{mn} : 멀티캐스트 패킷	

(그림 6) 호스트 출력 패킷에 대한 유형별 분석 규칙

3.5 출력 패킷 유형에 따른 장애 원인 파악 규칙

검출 단계7은 검출 단계6에서 분석한 패킷 유형을 바탕으로 브로드캐스트, 멀티캐스트, 에러없는 유니캐스트 패킷과 에러 발생 패킷에 대하여 임계값과의 비교를 통하여 장애의 원인을 분석한다. 즉, 각각의 유형에 대해 설정된 임계값과의 비교를 통하여 패킷 유형별 장애를 진단하게 된다. 따라서 브로드캐스트, 멀티캐스트, 에러없는 유니캐스트 패킷이 많이 검출되면 응용 서비스 상의 장애로 진단하고 이에 대한 결과를 관리자에게 통보하고, 에러 발생 패킷이 많이 검출되면 물리 계층의 인터페이스 카드나 선로 상의 이상으로 인한 장애로 진단하고 이에 대한 결과를 관리자에게 통보한다. (그림 7)은 이에 대한 규칙을 보여준다.

BEGIN	
IF S8(R_{bn} > ρ_b) THEN GO S12	
IF S9(R_{mn} > ρ_m) THEN GO S12	
IF S10(R_{un} > ρ_u) THEN GO S12	
IF S11(R_{en} > ρ_e) THEN GO S13	
S12(application_indication)	
S13(physical_indication)	
END	
R_{bn} : Broadcast Packet Rate	ρ_b : 브로드캐스트율에 대한 임계값
R_{mn} : Multicast Packet Rate	ρ_m : 멀티캐스트율에 대한 임계값
R_{un} : Unicast Packet Rate	ρ_u : 유니캐스트율에 대한 임계값
R_{en} : Error Packet Rate	ρ_e : 에러 패킷율에 대한 임계값

(그림 7) 출력 패킷 유형에 따른 장애 원인 파악 규칙

4. 네트워크 지연 장애 검출 및 통보 알고리즘

LAN 상의 지연 장애에 대한 규칙을 기반으로 네트워크 지연이 발생하는 원인을 찾아서 이를 해결하는 알고리즘을 설계한다. 알고리즘은 충돌율 및 이용률 계산 알고리즘($Å_{col}$), 장애 발생 위치 탐색 알고리즘($Å_{src}$), 장애 발생 원인분석 알고리즘($Å_{anal}$), 의 3단계로 나누어 설계한다.

$Å_{col}$은 RMON MIB변수를 읽어 들여 이를 분석 가공하여 충돌율과 이용률을 구하는 알고리즘이다. 이 알고리즘을 통하여 얻은 충돌율과 이용률이 모두 임계값을 초과할 때 트래픽 지연 장애가 발생한 것으로 진단하고 장애를 유발시킨 호스트와 원인의 검출을 시작한다.

$Å_{src}$는 장애의 원인이 된 호스트를 찾아내어 이에 대한 정보를 $Å_{anal}$에 제공한다. $Å_{anal}$는 $Å_{src}$에서 제공한 정보를 기반으로 장애의 원인이 된 호스트가 발생시킨 프로토콜이 무엇인지를 파악하고 이에 따라 장애 발생 원인을 분석하고 관리자에게 통보한다.

(그림 8)은 이와 같은 4단계의 알고리즘 흐름도를 도식적으로 나타내고 있다.

(그림 8) 네트워크 지연 장애 검출 알고리즘 흐름도

이와 같은 세그먼트 상의 네트워크 지연 장애 검출 모델에 RBR(Rule Based Reasoning)을 적용하여 단계적으로 장애의 원인을 찾아내고 이에 대한 결과를 통보한다.

4.1 충돌율 및 이용률 계산 알고리즘(Åcal)

충돌율은 세그먼트 상의 전체 패킷 수에 대한 패킷 충돌 값을 백분율로 계산한 값으로 RMON probe에 의해 설정된 특정 인덱스 번호 I_{row}를 이용하여 폴링한 관리 MIB 변수 etherStatsCollision, etherStatsPkts을 누적하여 계산한다[12].

세그먼트 상의 전체 패킷량 누적

$$\sigma_p = \sum_{i=1}^{n_p} (etherStatsPkts_i - S_p)$$

충돌 패킷량 누적

$$\sigma_{col} = \sum_{i=1}^{n_p} (etherStatsCollision_i - S_{col})$$

최종 충돌율 계산

$$\mu_{col} = \frac{\sigma_{col}}{\sigma_p \sigma_{col}} \times 100$$

세그먼트 상의 이용률은 현재 사용되고 있는 세그먼트의 이용량을 백분율로 나타낸 값으로 RMON probe에 의해 설정된 I_{row}을 이용하여 폴링한 etherStats Octets, etherStatsPkts, ifSpeed, sysUpTime 등의 관리 변수를 누적하여 계산한다[12].

트래픽 변화량 누적

$$\sigma_p = \sum_{i=1}^{n_p} (etherStats\ Pkts - S_p)$$

$$\sigma_o = \sum_{i=1}^{n_p} (etherStats\ Octets - S_o)$$

$$\sigma_h = \sigma_p(96+64) + \sigma_o \times 8$$

시간 변화량 누적

$$\delta_t(i) = sysUpTime - S_t$$

$$\sigma_t = \sum_{i=1}^{n_p} \delta_t(i)$$

세그먼트 이용(μ_{su}) 계산

$$\mu_{util} = \frac{\sigma_h}{\sigma_t \mu_{spd}} \times 100$$

이와 같은 계산 알고리즘을 통하여 주기적으로 충돌율(μ_{col})과 이용률(μ_{util})을 구하고 LAN 관리 시스템이 이를 주기적으로 모니터링 한다.

4.2 장애 발생 위치 탐색 알고리즘(Å$_{str}$)

LAN 세그먼트 상에 임계값 이상의 충돌율과 이용률을 유발시킨 호스트를 찾아내기 위해 세그먼트 상의 호스트에 대한 출력 패킷와 출력 바이트를 분석한다.

호스트 출력 패킷 및 출력 바이트는 단위 시간 당 출력되는 패킷 및 바이트 수를 분석하는 것으로 RMON probe에 의해 설정된 I_{row}와 호스트의 MAC 주소인 h_{mac}을 이용하여 폴링한 hostOutPkts, hostOut Octets, sysUpTime 등의 관리 변수를 누적하여 계산한다[12].

분석 과정은 다음과 같다.

과정 1) RMON 설정 중 host 그룹 설정

과정 2) 초기 MIB 변수 폴링

관련 MIB 변수 집합 V{hostOutPkts, hostOctets, sysUpTime}를 I_{row}와 h_{mac}을 이용하여 폴링

과정 3) 비교 값 설정

h_{op}에 hostOutPkts, h_{oo}에 hostOutOctets, h_t에 sysUpTime 설정

과정 4) 다음 MIB 변수 폴링

다음 폴링 변수 집합 V{hostOutPkts, hostOutOctets, sysUpTime}를 I_{row}와 h_{mac}을 이용하여 t_p시간 간격으로 폴링하며, 폴링 회수인 n_p 증가

과정 5) 호스트에서 출력되는 패킷량 누적

$$\sigma_{op} = \sum_{i=1}^{n_p} (HostOutPkts_i - h_{op})$$

과정 6) 호스트에서 출력되는 바이트량 누적

$$\sigma_{op} = \sum_{i=1}^{n_p} (HostOutOctets_i - h_{oo})$$

과정 7) 시간 변화량 누적

$$\delta_t(i) = sysUpTime - S_t$$

$$\sigma_t = \sum_{i=1}^{n_t} \delta_t(i)$$

과정 8) 최종 호스트 출력 패킷 계산

$$\mu_{op} = \frac{\sigma_{op}}{\sigma_t}$$

과정 9) 최종 호스트 출력 바이트 계산

$$\mu_{oo} = \frac{\sigma_{oo}}{\sigma_t}$$

이와 같은 과정을 통하여 출력 패킷 호스트 TOP N과 출력 바이트 호스트 TOP N을 분석함으로써 LAN 세그먼트 상의 트래픽을 가장 많이 유발시킨 호스트를 찾아낼 수 있다.

4.3 장애 발생 원인분석 알고리즘(Å$_{anal}$)

주기적인 네트워크 트래픽에 대한 모니터링을 통하여 충돌율(μ_{col})을 계산하고 이를 임계값(col_{th})과 비교한다. 충돌율(μ_{col})이 임계값(col_{th})을 초과할 경우 그 때의 이용률(μ_{util})을 계산하고 이 값이 임계값($util_{th}$)을 초과할 경우 장애가 발생한 것으로 판단하고 장애를 유발시킨 호스트를 찾는다. 장애를 유발시키는 근본적인 원인인 호스트에 대하여 구체적으로 어떤 원인에 의해 장애가 발생하였는지를 분석한다.

네트워크 지연 장애를 유발시킨 가장 큰 원인은 특정 호스트에서 특정 어플리케이션이 트래픽을 과다하게 발생시키거나 물리 계층의 인터페이스 카드나 선로 상의 장애로 인한 에러 패킷이 과다하게 발생하는 경우이다. 따라서 장애를 유발시킨 호스트와 그 호스트가 세그먼트 상의 트래픽을 과다하게 발생시키는 패킷의 유형을 파악해야 한다.

패킷의 분석 유형으로는 브로드캐스트 패킷, 멀티캐스트 패킷, 에러없는 유니캐스트 패킷 그리고 에러 발생 패킷으로 분류할 수 있다. 따라서 장애 유발의 원인이 된 호스트가 발생하는 패킷을 위의 유형별로 구분하여 분석하고 이를 바탕으로 그 호스트가 발생시킨 패킷의 유형이 무엇인지를 파악한다.

우선 세그먼트 상의 패킷 유형 중, 브로드캐스트, 멀티캐스트, 에러 없는 유니캐스트 그리고 에러 발생 패킷에 대한 패킷 수를 구한다. 그런 다음 각 패킷에 대하여 가장 많이 발생된 패킷의 유형을 구한다. 이를 위해 특정 샘플링 시간 동안 장애의 원인이 된 호스트가 가장 많이 발생시킨 패킷 유형을 찾아서 발생된 트래픽의 비율을 분석한다.

분석 과정은 다음과 같다.

과정 1) 초기 RMON MIB 변수 폴링

관련 RMON MIB 변수 집합

V{hostOutBroadcastPkts, hostOutMulticastPkts, hostOutPkts, hostOutErrors}를 I_{row}와 호스트 MAC 주소인 h_{mac}을 이용하여 폴링

h_{bp} = hostOutBroadcastPkts

h_{mp} = hostOutMulticastPkts

h_{up} = hostOutPkts-hostOutBroadcastPkts-hostOutMulticastPkts-hostOutErrors

h_{ep} = hostOutErrors

로 설정

과정 2) 브로드캐스트 출력 패킷량 분석

$$b_p = \sum_{i=1}^{n_t} (hostOutBroadcastPkts_i - h_{bp})$$

과정 3) 멀티캐스트 출력 패킷량 분석

$$m_p = \sum_{i=1}^{n_t} (hostOutMulticastPkts_i - h_{mp})$$

과정 4) 에러없는 유니캐스트 출력 패킷량 분석

$$u_p = \sum_{i=1}^{n_t} (hostOutPkts_i - h_{up})$$

과정 5) 에러 발생 출력 패킷량 분석

$$e_p = \sum_{i=1}^{n_t} (hostOutErrors_i - h_{ep})$$

이와 같이 브로드캐스트, 멀티캐스트, 에러없는 유니캐스트 패킷 및 에러발생 패킷에 대한 출력량 분석[5]을 통하여 장애 유발의 원인이 되는 패킷 유형을 분석한다. 즉, 출력 패킷 유형 중 브로드캐스트 패킷, 멀티캐스트 패킷, 에러없는 유니캐스트 패킷이 많이 발생하면 응용 서비스 상의 장애로 진단하고, 에러발생 패킷이 많이 발생하면 물리 계층의 인터페이스 카드나 선로 상의 이상으로 인한 장애로 진단한다.

이와 같은 과정을 통하여 특정 호스트의 특정 응용 서비스나 물리 계층에 장애가 발생하였음을 보고한다.

5. 실험 및 고찰

이번 장에서는 본 논문에서 제시한 RBR 기반의 장

애 진단 알고리즘 모델을 실제 네트워크에 적용시켜 제시된 장애 검출 및 진단 기법이 제대로 동작하고 그 원인을 분석하는지 실험을 통하여 알아보았다.

5.1 실험 환경

네트워크 지연 장애를 진단하기 위한 실험을 성균관 대학교 내부 망인 203.252.53.0에 연결되어 있는 시스템을 실험 대상으로 하여 실시하였다. 203.252.53.0 네트워크에는 약 160여 개의 호스트가 연결되어 있으며 100Mbps Ethernet LAN이다. 네트워크 장애 진단 시스템의 관리 시스템과 디폴트 게이트웨이에 대한 설명은 <표 2>에 있다.

〈표 2〉 실험 환경 시스템

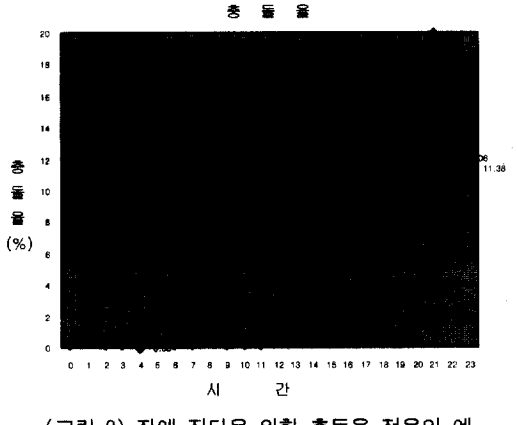
종 류	IP 주소	시스템	운영체제
디폴트 게이트웨이	203.252.53.1	CiscoRouter	ROM
관리 시스템	203.252.53.42	Sun Ultra SPARC 1	SunOS release 5.5.1

5.2 실험 결과 및 고찰

<표 3> 규칙 기반의 네트워크 장애 검출 및 진단에 대한 실험 결과를 나타내고 있다.

제시한 규칙이 <표 3>에서 보는 바와 같이 적용되고 이를 바탕으로 충돌율과 이용률을 통하여 장애를 검출하고 장애발생 원인 호스트를 찾아내어 그 호스트가 유발한 장애의 종류를 파악할 수 있었다.

(그림 9)은 네트워크 장애 진단을 위한 충돌율을 성균관 대학교 내부 망인 203.252.53.0의 각 시간대별로 트래픽의 유형을 모니터링 한 실험 결과를 나타내고 있다.



(그림 9) 장애 진단을 위한 충돌율 적용의 예

〈표 3〉 규칙 기반의 네트워크 장애 검출 및 진단 과정 결과 예

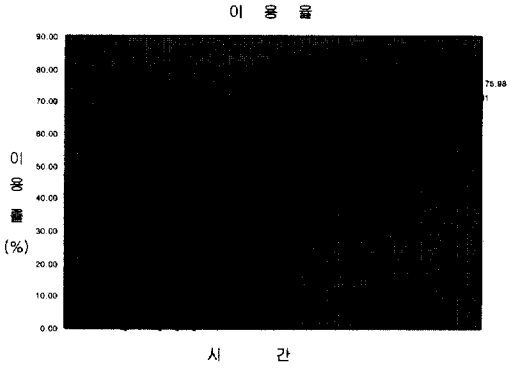
검출 과정	상태 천이	천이 조건 (실험값)
충돌율 검출 규칙	S1→S2	μ_{col} : 15.34%, col_{th} : 5% $\mu_{col} > col_{th}$
이용률 검출 규칙	S2→S3	μ_{util} : 85.64%, $util_{th}$: 70% $\mu_{util} > util_{th}$
최대 패킷 출력 호스트 파악 규칙	S3→S4	상위 3개 호스트의 출력 패킷율 00 00 A2 CB 29 41 (40.5%) 08 00 20 80 57 5D (37.8%) 00 00 00 00 00 00 (14.6%)
	S3→S5	상위 3개 호스트의 출력 바이트율 00 00 A2 CB 29 41 (39.1%) 08 00 20 80 57 5D (38.8%) 00 00 00 00 00 00 (15.3%)
	S4→S6	출력 패킷을 가장 많이 발생시킨 호스트→00 00 A2 CB 29 41
	S5→S6	출력 바이트를 가장 많이 발생시킨 호스트→00 00 A2 CB 29 41
	S6→S7	장애 유발 원인 호스트 →00 00 A2 CB 29 41
호스트 출력 패킷에 대한 유형별 분석 규칙	S7→S8	총 출력 패킷에 대한 브로드캐스트율→5.29%
	S7→S9	총 출력 패킷에 대한 멀티캐스트율→2.21%
	S7→S10	총 출력 패킷에 대한 에러없는 유니캐스트율→92.17%
	S7→S11	총 출력 패킷에 대한 에러 패킷율 →0.32%
출력 패킷 유형에 따른 장애 원인 파악 규칙	S10→S12	IP주소가 203.252.53.57 (00 00 A2 CB 29 41)인 호스트의 출력 응용 프로토콜 분석 결과 SMTP→70.8%, ftp-data→11.2% ftp→10.1%, telnet→7.9% 따라서 관리자에게 장애 호스트 IP주소와 SMTP 프로토콜이 장애 원인임을 통보

(그림 9)에서 보는 바와 같이 15시에서 23시까지 충돌율이 이전 시간대의 충돌율에 비해 월등히 높아짐을 알 수 있다. 이는 일반적인 LAN상의 허용 가능한 충돌율의 임계값을 훨씬 넘어선 수치임을 알 수 있다. 이러한 상황이 발생하면 LAN 상의 트래픽이 굉장히 많이 증가했다는 것을 알 수 있다.

(그림 10)은 네트워크 장애 진단을 위한 이용률을 성균관 대학교 내부 망인 203.252.53.0의 각 시간대별로 트래픽의 유형을 모니터링 한 실험 결과를 나타내고 있다.

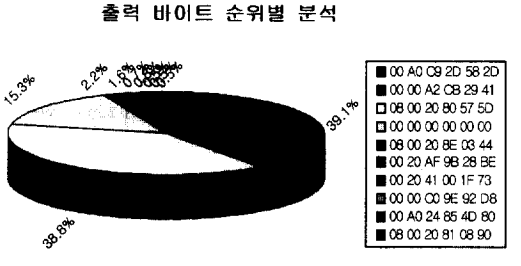
(그림 10)에서 보는 바와 같이 (그림 10)처럼 15시에서 23시까지 LAN이용률이 이전 시간대의 이용률에 비해 월등히 높음을 알 수 있다. 즉, 충돌율이 높아짐에 따라 이용률도 같이 높아짐을 볼 수 있다. 따라서 충돌율과 이용률이 LAN 세그먼트가 허용하는 임계값을

훨씬 초과했을 경우 LAN상의 트래픽이 굉장히 많이 증가하고 네트워크 지연 장애를 유발하는 원인이 될 수 있다.



(그림 10) 장애 진단을 위한 LAN 이용률 적용의 예

(그림 11)은 장애 발생 위치 탐색 규칙을 통해 203.252.53.0 세그먼트에서 충돌율과 LAN이용률이 임계값을 초과하여 장애라고 진단한 시점에서 트래픽을 가장 많이 발생시킨 호스트들의 상위 10개를 분석한 결과이다.

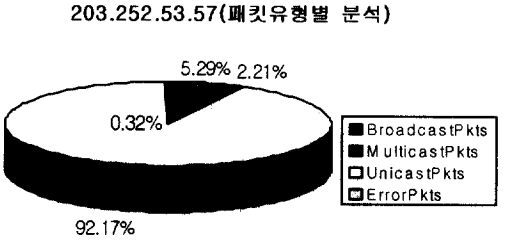


(그림 11) 장애 발생 위치 탐색 적용의 예

(그림 11)에서 보는 바와 같이 2개의 호스트가 전체 트래픽의 약 80%를 차지하고 있음을 알 수 있다. 실제로 세그먼트 상의 두 호스트는 각각 메일 및 ftp 서버와 라우터로 동작하고 있었다. 라우터는 일반적으로 외부 네트워크에서 로컬 네트워크로 사용자의 요구에 따라 많은 트래픽을 발생시키고 있기 때문에 메일 및 ftp 서버의 장애 여부를 의심할 수 있다.

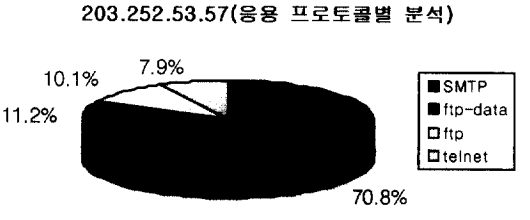
이를 바탕으로 가장 많은 바이트를 출력한 호스트인 203.252.53.57(00 00 A2 CB 29 41)에 대해 (그림 12)와 같이 출력 패킷 유형별로 분석하였다.

(그림 12)에서와 같이 호스트(203.252.53.57)이 발생한 패킷 중 에러없는 유니캐스트가 가장 많은 발생율을 보이고 있다. 이를 통하여 응용계층의 응용 프로토콜(서비스) 상의 장애가 있음을 판단할 수 있다.



(그림 12) 장애 발생 패킷 유형별 분석의 예

따라서 (그림 13)와 같이 호스트(203.252.53.57)에 대하여 응용 프로토콜별 분석을 하였다.



(그림 13) 장애 발생 응용 프로토콜 분석의 예

(그림 13)은 장애 발생 위치 탐색 규칙을 통해 찾아낸 메일 및 ftp 서버로 동작하고 있는 호스트(203.252.53.57)에 대한 패킷 분석 결과를 나타내고 있다. (그림 13)에서 보는 바와 같이 SMTP가 전체 패킷 트래픽의 70%이상을 차지하고 있는 것을 볼 수 있다. 이는 정상적인 SMTP 트래픽을 훨씬 초과하는 수치이다. 이를 통해 203.252.53.0 세그먼트 상의 호스트(203.252.53.57)의 SMTP 프로토콜이 전체 네트워크 지연 장애의 원인임을 추측할 수 있고, 실제 조사 결과, 해당 서버의 sendmail 설정이 잘못되어 이상 패킷을 계속 발생하고 있는 것을 확인했다.

장애 지연 검출 및 진단 알고리즘을 실제 네트워크에 적용시켜봄으로써 LAN상의 지연 장애 발생시 체계적인 규칙을 기반으로 장애 원인 및 장애 위치를 신속하게 검출할 수 있음을 확인했다.

6. 결 론

본 논문에서는 LAN 상의 지연 장애 관리를 효율적으로 하기 위한 RBR(Rule-Based Reasoning) 기반의 네트워크 지연 장애 검출 및 진단 알고리즘 모델을 설계하였다. 네트워크 지연 장애 검출을 위해 RMON MIB을 이용하여 충돌율과 이용률을 구하고, 이를 이용하여 장애를 검출하고 호스트의 패킷 및 바이트 출력을 순위별로 분석하여 장애 유발의 원인이 된 호스트의 위치를 확인하였다. 그리고 브로드캐스트, 멀티캐스트, 유니캐스트 그리고 에러 패킷 발생율을 비교 분석하여 장애 유발 호스트가 발생시키는 장애의 원인이 무엇인지를 파악하여 관리자에게 통보하는 전체 알고리즘을 설계하였다. 이러한 알고리즘에 RBR 기반의 네트워크 장애 검출 규칙을 적용시켜 보다 체계적이고 지능적인 네트워크 지연 장애 관리 모델을 설계하였다. 이를 기반으로 실험을 통하여 본 논문에서 제시한 규칙 및 알고리즘이 제대로 적용됨을 확인하였다.

이러한 RBR 기반의 네트워크 지연 장애 검출 알고리즘은 기존의 LAN분석 시스템이 가진 성능 위주의 분석 방식에서 벗어나, 최근의 복잡하고 방대해진 네트워크에서 발생할 수 있는 장애에 대하여 능동적으로 대처할 수 있도록 네트워크 정보 수집에서 장애 판단 및 원인 해결까지 체계적인 과정을 나타내었다. 따라서 이러한 RBR기반의 네트워크 지연 장애 검출 알고리즘은 LAN 상의 지연 장애 발생시 효율적으로 대처할 수 있는 충분한 해결책을 제시해 줄 것으로 기대된다.

참 고 문 헌

[1] I. Rouvellou and G. W. Hart. "Automatic alarm correlation for fault identification," In *Proc. IEEE INFOCOM*, pp.553-561, 1995.

[2] Allan Leinwand, "Accomplishing Performance Management with SNMP," INET'93, pp.CEA-1-CEA-5, 1993.

[3] William Stallings, "SNMP, SNMPv2, SNMPv3 and RMON 1 and 2," Addison-Wesley, 1999.

[4] Cynthia S. Hood, Chuanyi Ji, "Intelligent Agents for Proactive Fault Detection," IEEE Internet Computing, Vol.2, No.2, 1998.

[5] 안성진, 정진욱, "SNMP MIB-II를 이용한 인터네트 분석 파라미터 계산 알고리즘에 관한 연구", 정보처리학회, 제5권 제8호, pp.2102-2116, 1998.

[6] R. Maxion. "A case study of Ethernet anomalies in a distributed computing environment," IEEE transactions on Reliability, 39(4), Oct. 1990.

[7] Sun, R. "Neural network models for rule-based reasoning," IEEE International Joint Conference on, Vol.1, pp.503-508, 1991.

[8] Egri, P. A., Underwood, P. F., "HILDA : Knowledge extraction from neural networks in legal rule based and case based reasoning," IEEE International Conference on, Vol.4, pp.1800-1805, 1995.

[9] Cronk, R. N., Callahan, P. H., Bernstein, L., "Rule-based expert systems for network management and operations : an introduction," IEEE Network Vol.23, pp.7-21, Sept. 1988.

[10] A. Lazar, W. Wang, and R. Deng. "Models and algorithms for network fault detection and identification," A review. In Proc. IEEE ICC, 1992.

[11] Irene Katzela, Mischa Schwartz, "Schemes for Fault Identification in Communication Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, Vol.3, No.6, DECEMBER, 1995.

[12] 조강홍, 안성진, 정진욱, "RMON MIB을 이용한 LAN 성능 파라미터 계산 알고리즘", 한국통신학회 논문지, 제24권 제4B호, pp.670-679, 1999.

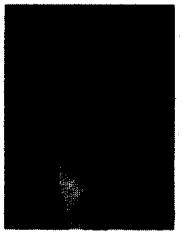
조 규 억

e-mail : kojoe@songgang.skku.ac.kr

1999년 성균관대학교 정보공학과 졸업(학사)

1999년~현재 성균관대학교 전기전자 및 컴퓨터 공학부 대학원 석사과정

관심분야 : 네트워크 관리, 트래픽 분석



안 성 진

e-mail : sjahn@comedu.skku.ac.kr

1988년 성균관대학교 정보공학과 졸업(학사)

1990년 성균관대학교 대학원 정보공학과 졸업(석사)

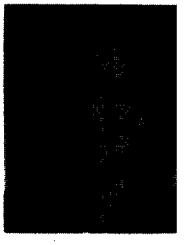
1990년~1995년 한국전자통신 연구원 연구 전산망 개발실 연구원

1996년 정보통신 기술사 자격 취득

1998년 성균관대학교 대학원 정보공학과 졸업 (박사)

1999년~현재 성균관대학교 컴퓨터교육과 전임강사

관심분야 : 네트워크 관리, 트래픽 분석, Unix 네트워킹



정 진 욱

e-mail : jwchung@songgang.skku.ac.kr

1974년 성균관대학교 전기공학과 학사

1979년 성균관대학교 대학원 전자공학과 석사

1991년 서울대학교 대학원 계산통계학과 박사

1982년~1985년 한국과학기술 연구소 실장

1981년~1982년 Racal Milgo Co. 객원연구원

1985년~현재 성균관대학교 전기전자 및 컴퓨터공학부 교수

관심분야 : 컴퓨터 네트워크, 네트워크 관리, 네트워크 보안