인터넷 상호연동망의 신뢰성 평가를 위한 위험관리 방법론의 응용

Development of Risk Management Model to Evaluate Reliability of Internet

김도훈

경희대학교 경영대학, dyohaan@khu.ac.kr

초 록

B2C, B2B와 같은 인터넷 상거래뿐만 아니라, 전자정부를 통한 G2C 등에서 보는 바와 같이, 공공 및 민간 IX(Internet eXchange)를 통한 인터넷 상호연동 인프라는 명실상부한 사회 신경망으로 기능한다. 따라서 전통적인 사회간접자본인 도로, 항만, 전력 등에서와 마찬가지로, 그 구축 및 운영에서의 안정성과 신뢰성에 대한 요구가 점차 강화되고 있다. 본 연구는 인터넷 상호연동망의 안정성과 신뢰성을 제고하기 위한 방안을 위험관리 관점에서 제안한다. 먼저, 인터넷 상호연동의 강건성(robustness)을 높이기 위한 방어기제와 더불어 상호연동 대안들을 개발한다. 이들 대안은 장애시에 작동하는 별도의 상호연동 비상망을 운영하는 방재형과, 지역적으로 분산된 상호연동 허브(IX)를 운영하여 장애에 따른 피해 확산을 방지하는 분산 허브형으로 구분된다. 본 논문에서는 또한 대안들의 위험효율성(risk efficiency)을 체계적으로 비교/평가하기 위하여 경영공학 방법론에 의한 위험평가 프레임워크를 개발하고, 이를 투자수준이 상이한 여러 대안들에 적용한다. 몬테카를로 시뮬레이션을 통한 ROI(Risk On Investment) 분석 결과, 방재형 대안이 비용대비 위험효율성 측면에서 최선의 후보로 평가되었다.

1. 서 론

인터넷은 애플리케이션을 담당하는 다양한 상위계층과 물리적 전송을 담당하는 하위계층으로 단순화된 개방형 프로토콜이므로, 이기종 망간의 효과적인 상호연동에 대한 논의는 인터넷 초기부터 끊임없이 제기되어 왔다. 특히 기간망 및 가입자망의 광대역화, QoS(Quality of Service) 및 SLA(Service Level Agreement)로 대변되는 품질보장, 보안 및 인증, 트래픽 관리 및 제어, IP주소 고갈문제 등의 이슈에 대응하기 위해서는, 인프라의 고도화에 못지않게, 인터넷이라는 틀내에서 다양한 종류의 인프라간 상호연동을 통한 끊임없는(seamless) 운영이 필수적이다.

다양한 인프라간 상호연동이 증가됨에 따라, 개별 네트워크의 피해가 인터넷에 연결된 전체 네트워크로의 확산될 위험성도 증가한다. 예를 들어, 사이버 공격에 취약한 지역 네트워크에서 발생된 위협이 인터넷 기간망(backbone network)을 통하여 빠른 속도로 전국으로 전파될 가능성이 높다. 특히 차세대 인터넷으로 거론되는 BcN(Broadband convergence Network)에서는 Open API 등과 같이 확대된 개방성을 전제로 하므로, 악의적 침투 및 피해 확산의 다양한 경로로 악용될 가능성 역시 그 만큼 높아진다.

21C 정보화 사회에서 인터넷에 대한 의존도가 점차 높아질 것은 자명하다. 인터넷 뱅킹 고객수는 이미 2004년 9월 기준으로도 약 2,581만 명에 이르며, 유선 인터넷을 이용한 은행업무 처리건수도 748만 건에 이르는 등, 인터넷 뱅킹의 이용률은 매년 20% 이상 증가하는 추세이다([7]). 또한 인터넷 전자상거래를 통한 B2C 거래 규모도 2006년에 연간 10조원에 육박하는 등, 인터넷이 유통시장의 핵심 매체로 부상한 지 오래 되었다([7]). 이는 인터넷망의 수 초 동안의 정체 및 서비스 중단이 초래할 경제적 손실 역시 천문학적인 금액에 이른다는 것을 의미한다. 따라서 인터넷 상호

연동체계의 안전성(security), 안정성(stability), 신뢰성(reliability)을 강화하기 위한 노력이 필요한 시점이다.

다양한 ISP의 인터넷망간 상호연동과 관련된 기술적 분석에 대해서는, 이미 많은 연구가 진행된 상태이다. 예를 들어, [2], [3], [9], [10], [11], [14], [18], [26] 등의 문헌에서는 인터넷 상호접속(interconnection) 및 연동에 관한 기술, 정책적 이슈를 자세히 소개하고 있다. 먼저 [9]는 인터넷 교환노드(IX, Internet eXchange)에 기반한 국내/외 상호연동의 사례와 정책들을 조사하여 비교하고 있다. [2]와 [3]에서는 BcN 환경에서 사업자간 원활하고 긴밀한 상호접속 및 연동의 중요성과 이를 지원하는 기술적 요구사항을 자세히 소개하고 있다. 특히 단대단(end-to-end) QoS를 보장하기 위한 IX 상호연동 플랫폼을 제안하고, 이에 대한 경제성 분석을 시도하고 있다. [14]와 [18]에서는 인터넷 상호연동의 경제적 의미와 중요성을 과거 철도산업 및 시내/외 전화망간 상호접속의 예와 비교하여 설명한다. [26]은 인터넷 상호접속 및 정산방식(settlement)을 자세히 소개한다. [10]은 인터넷의 진화에 따라 현행 인터넷 상호연동의 중심에 있는 IX의 바람직한 진화전략 및 제도적 요구사항에 대해 제안한다. 이들 문헌 모두가 효율적 상호접속과 연동이, 인터넷 상업화 이후, 원활하고 신뢰성 있는 인터넷 서비스 운영에 필수적임을 시사한다.

그러나, [2], [3], [14], [18], [29], [30] 등에서 지적하고 있는 바와 같이, 인터넷 상호접속과 연동은 비단 기술적 문제에만 국한되지는 않는다. 오히려 기술적 요구사항보다는 제도적, 정책적 지원이 현실적으로는 더 중요할 수 있다. 예를 들어, 단대단 QoS를 구현하기 위해서는 사업자마다 상이한 서비스 유형을 서로 연결시켜 주는 서비스 클래스 매핑(service class mapping)이 전제되어야 하는데, 미성숙한 정책 및 제도적 환경으로 인하여 이러한 전제가 실현되기 어려운 것이 현실이다. 이와 마찬가지로, 본 연구의 주제인 안정성과 신뢰성이 강화된 상호연동체계를 개발하기 위해서는 기술적 전제조건과 더불어 제도적, 정책적 뒷받침이 반드시 병행되어야 한다. 대표적인 예로, 상호연동 실패에 따른 위험(risk)을 추정하기 위해서는 기술적 이슈보다는 경영과학적 접근이 우선적으로 필요하다.

본 연구는 인터넷망간 상호연동의 경제적 가치와 위험도를 평가하는 시스템을 개발하고, 이를 바탕으로 상호연동 대안에 대한 위험-경제성 분석을 수행한다. 먼저 다음 장에서는 인터넷망간 상호연동체계를 소개하고 현행 방식의 문제점을 파악한다. 3장에서는 상호연동 장애 수준에 따른 피해 규모를 추정함으로써 상호연동 대안의 위험도를 평가할 수 있는 체계적인 프레임워크를 제안한다. 4장에서는 먼저 비상시에도 상호연동체계가 원활하게 작동하여 서비스의 안정성과 신뢰성을 높일 수 있는 상호연동 대안들을 제안한다. 또한 이들 대안에 대해 3장의 프레임워크를 적용하여, 장애와 같은 비상시 운영 성능을 비교/분석한다. 마지막으로 제안된 상호연동 위험평가 프레임워크를 정교화하고 확장할 수 있는 방안을 검토하면서 본 논문을 마무리한다.

2. 인터넷망간 상호연동체계

2.1 인터넷망간 상호연동과 IX

오늘날의 인터넷은 역설(paradox)로 가득하다는 주장이 있다([29]). 여기서 역설의 의미는, 현재 인터넷 기술을 고려할 때, 대규모 다자간 실시간 커뮤니케이션이 가능함에도 불구하고 이러한 서비스를 현실에서는 찾아 볼 수 없다는 것을 말한다. 즉, 기술적으로 가능한 일이 제도나 상업적 동기의 문제로 인하여 제공되지 못하는 현실이 첨단 분야에서 발생하고 있는 것이 마치 역설과도 같다는 의미이다. 이러한 현상의 원인은 글로벌 인터넷 연결과 관련된 사업구조와 정책에 있다. 인터넷이 네트워크의 네트워크라는 점에 비추어 볼 때, 이러한 산업구조의 특이성은 어느 정도 이해되기도 한다. 이러한 맥락에서 인터넷 서비스에서의 사업자간 상호접속과 연동의 문제를 점검해 볼 필요가 있다([2], [3], [14], [18], [26] 등).

둘 이상의 ISP가 서로 연결되는 지점을 일반적으로 IX라고 부른다. IX는 ISP간 자유롭고 안정된 상호연동을 보장함으로써 인터넷의 글로벌 연결성을 유지하는 연결고리로 정의될 수 있다. IX가 없다면, ISP간 peering 등, 개별적인 상호연동을 위하여 많은 수의 회선이 필요하거나, 타 ISP를 경유하는 transit의 경우에는 연결경로를 길게 하여 품질을 저하시킨다. 이러한 이유에서 IX의 설치 및 운영은 인터넷 자원의 효율적인 활용 측면에서도 중요하다.

특히, 인터넷이 사회간접자본으로서 기능함에 따라 효율적일 뿐만 아니라 안정적이고 신뢰성 있는 상호연동은 더욱 중요해지고 있다. 이 과정에서 IX는 매우 유용한 상호연동방식을 제공한다.

인터넷이 상업화된 이후, MCI, AT&T 등의 ISP들에 의하여 미국 캘리포니아에 구축되었던 CIX(Commercial Internet eXchange), 미국 과학재단이 설립한 NAP(Network Access Point), MAE-E 등이 초기 IX의 예이다. 이후 비용공유(cost sharing) 차원에서 다수의 ISP들이 자발적으로 연동센터(상용 IX)를 운영하기 시작하였고 공공기관들도 사업자 중립적인 공공 IX를 제공하고 있다. 인터넷 상호연동과 관련된 역사적 배경과 기술적 이슈는 [26], [30] 등에 자세히 소개되어 있다.

2.2. 현행 국내 인터넷 상호연동체계의 신뢰성

상호연동체계의 피해 사례와 방어기제

인터넷 트래픽이 폭증하고 이에 따라 상호연동의 복잡성이 증가하면서, 상호연동체계의 취약점이 드러나기 시작하였다. 대표적인 예로, 2003년1월25일 Slammer Worm이 KT가 운영하는 DNS 서버를 다운시키면서 KT망을 중심으로 한 국내 인터넷망의 상당 부분이 작동하지 않는 사태가 발생하였다([12]). Slammer Worm에 감염된 MS-SQL 서버에 의해 대량의 불량 패킷이 발생하여 네트워크를 마비시키고, 이로 인하여 ISP내 DNS 서버와 Root DNS 서버 간의 교신장애를 유발하면서 결국에는 DNS 서버의 다운을 초래한 것이다.

국외의 경우, 9.11 테러로 인하여 미국 내 재난 지역의 인터넷을 비롯한 통신망이 상당기간 동안 작동하지 못하였다([31]). 최근에는 가장 인기가 높은 MySpace.com이 정전으로 인하여 약 12시간 동안 서비스가 중단되기도 하였다([17]). 미국의 경우 장애시 피해 규모가 시간당 수백만 달러로 추정된다([28]).

2003년 1.25 사태를 계기로 정부, ISP 등의 사업자와 기타 관련 단체들이 협력하여 정보통신기반보호를 위한 종합상황실을 구축하고, 해킹과 바이러스에 대한 조기 예/경보 시스템을 구축하는 등, 효율적인 대응체계를 갖추어 나가고 있다. 그러나 이는 서버나 호스트 중심의 보안체계일 뿐이며, 실질적으로 인터넷 트래픽을 전달하는 상호연동망에 대해서는 별다른 조치를 마련하지 않고 있다. 일반적으로 ISP 및 IDC와 같은 서비스공급자는 방화벽이나 침입탐지시스템을 구축하여 장애에 대비할 수 있으나, 대용량 트래픽이 빠르게 교환되어야 하는 IX에서 이러한 방어시스템을 구현하는 것은 쉽지 않다.

예를 들어, IX의 기능에 피해를 주는 가장 주요한 방법은 DoS(Denial of Service Attack) 공격이다([1], [5]). 다양한 인터넷 트래픽이 경유하는 IX의 경우, DoS 등과 같은 공격에 매우 쉽게 노출되며, 일단 이러한 공격이 발생하면 트래픽 폭증으로 인하여 IX 성능이 저하될 뿐만 아니라 IX간 트래픽 교환에도 장애가 발생한다. 특히 L3(Layer-3) 방식의 DIX(Dacom IX)와 KT-IX가 국내 인터넷 트래픽의 50% 이상을 처리하는 상황에서, 특정 IX에 장애가 발생할 경우, 이를 대체하거나 보완하는 메커니즘이 없다면 문제가 심각해질 가능성은 매우 높다.

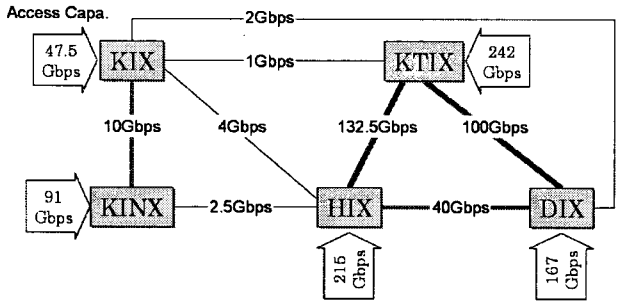
이와 같이, 장애에 취약한 상호연동체계의 개선을 위해 다음과 같은 방어기제(protection mechanism)를 생각해 볼 수 있다.

- IX 상호연동 자체의 생존성(survivability)을 강화하는 구조적 보완 : 상호연동망의 이중연결성(two-connectivity) 등을 높이는 토폴로지 재설계 등
- 네트워크 차단 및 격리와 같은 2차 방어 및 안전장치
- 우회경로(bypass route) 확보 의무조항 : 사업자의 의무사항으로, 복수의 IX 접속을 규정하여 비상시 우회경로를 확보하도록 함
- 트래픽 다중경로화(multi-path routing) : 기존의 Layer-3 방식은 DoS 공격이나 보안에 취약하므로, 트래픽 엔지니어링을 통하여 상호연동망 자체에서 이를 보완할 수 있도록 MPLS(Multi-Purpose Label Switching)과 같은 지능형 전달망(intelligent transport network)을 도입
- 기타 정책적 방안 : 인터넷 트래픽이 소수의 사업자에게만 집중되는 경향을 완화하고 트래픽을 분산시킬 수 있는 정책적 유인체계(분산에 대한 보상으로 법인세 감면 등) 제공

현행 국내 인터넷 상호연동체계

우리나라는 1995년 최초로 IX 서비스를 개시한 KIX(Korea Internet eXchange), 1996년

EIX(Expo Internet eXchange)를 모태로 탄생한 KT-IX, 1996년 KIX로부터 상용망을 이전받아 서비스를 개시한 DIX, 1999년 중소ISP 협의체인 한국인터넷연동협의회를 모태로 서비스를 시작한 KINX(Korea Internet Neutral eXchange), 그리고 2003년 부산/경남지역의 증가하는 트래픽 소통을 위해 구축된 BIX(Busan Internet eXchange) 등이 주요 IX 역할을 수행하고 있다. KIX와 BIX는 비영리를 목적으로 하는 한국정보사회진흥원이 운영을 담당하고, KT-IX와 DIX는 기간통신사업자인 ㈜케이티와 ㈜LG 데이콤이 각각 운영하는 상용 IX이다. KINX의 운영은 비영리 단체인 한국인터넷연동협의회 회원사 중 11개의 ISP가 공동출자한 ㈜케이아이엔엑스가 담당하고 있다.



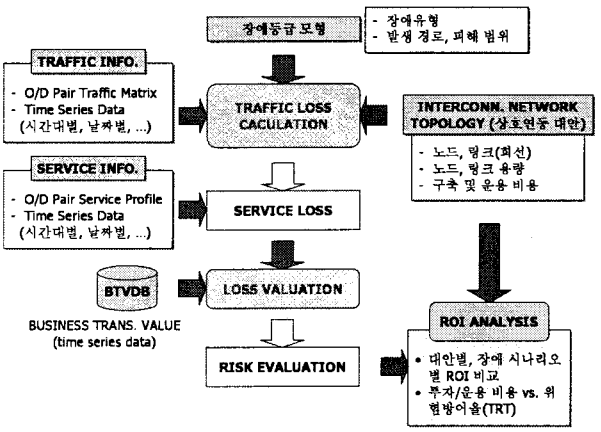
[그림 1] 현행 국내 인터넷 상호연동 네트워크

[그림 1]은 상기한 IX를 중심으로 한 국내 인터넷 상호연동망의 구조를 도식화한 것이다. 이러한 망토폴로지(network topology)적 특성은 과거 1.25 사태에서와 같이 침해사고(intrusion)에 취약한 구조를 보인다. 또한 허브 역할을 하는 IX에 문제가 발생하였을 경우, 전체 트래픽의 상당 부분이 차단되는 문제점도 안고 있다. 이는 1.25 사태가 가능하였던 원인을 암시한다. 즉, KT-IX에 대한 높은 구조적 의존성은, 한 사업자의 문제가 전체 인터넷의 상당 부분에 걸친 장애로 발전하는 것을 가능하게 한다.

또한 KIX가 다른 IX와의 연결성(degree)은 가장 높지만, 연결 용량(link capacity) 측면에서는 KT-IX와 다른 사업자와의 연결 수준이 더 높다는 사실에도 주목할 필요가 있다. 이는 상호연동망 설계에 있어서는 단순히 사업자간 연결성만으로 국한해서는 안되며, 사업자간 연결 용량도 고려해야 함을 의미한다. 현행 인터넷 상호연동방식이 대형 사업자 위주로 진행되면서, 이들로의 연결 수준 밀집으로 인한 불안정성은 더욱 가중된다. 따라서 장애 확산에 대한 차단장치나 망 및 설비의 이중화 등을 통하여 구조적 안정성을 제고할 필요가 있다. 상호연결망의 구조적 안정성을 강화하는 조치가 마련되지 않는 한, 1.25 사태와 같은 대형 사고로부터 안전할 수 없다.

3. 상호연동 위험평가 프레임워크

위험관리는 위험을 측정하는 것으로부터 시작하여, 이를 (합리적인 수준에서) 수용하는 것으로 마무리된다. 또한 측정을 위한 적절하고 객관적인 모형이 마련되어야 한다. 상호연동의 경우, 해당 상호연동 대안의 구조적 특성(e.g., 토폴로지 구조 등)에 대하여 충분한 분석을 바탕으로, 기술적 하부구조 및 설계에 대한 이해와 서비스별 트래픽 등 관련 데이터베이스(DB)에 대해 명확한 규정이 필요하다. 아래 그림은 이러한 관점에서 인터넷망 상호연동 장애에 따른 위험을 평가하기 위한 프레임워크의 개요를 도시한다. 위험평가 프레임워크는, ① 인터넷 상호연동 트래픽 정보, ② 장애등급 모형, ③ 상호연동 대안 등을 주요 입력으로 하여, 대안별 및 장애등급별로 위험수준을 추정한다. 프레임워크의 구성과 자료 흐름에 대한 구체적인 설명은 다음과 같다.



[그림 2] 상호연동 위험평가 프레임워크 개요

1) 상호연동 장애유형과 장애등급 모형

첫 단계는 위험파악(risk detection)과 관련된다. 인터넷망 상호연동상의 장애는 크게 두 종류로 분리하여 살펴 볼 필요가 있다. 먼저

상호연동에 직접적으로 관련된 장애로서, 이는 주로 상호연동망에 부하되는 트래픽 관리가 핵심이 된다. 또한 ISP, IDC 및 CP 등 서비스 제공사업자의 네트워크 및 설비에 대한 장애로, 주로 네트워크 침해 및 H/W 혹은 S/W 오작동으로 인한 것이 대부분이다. 후자의 경우, 장비, 회선, 전기설비, 건물 내 배선 등과 같은 자산 관리와도 관련된다. [표 1]은 정보통신서비스에서 발생하는 대표적인 장애 사례를 바탕으로, 본 연구에서 고려하는 장애유형을 재정리한 것이다.

[표 1] 장애유형

통제	유형			예
통제 불가능	자연 재해			화재, 지진, 풍수해
	인적 재해			파업, 테러, 도난 등
통제 가능	인적장애		운영장애	시스템 운영 실수, 해킹, 바이러스 피해, 자료 관리 실수 등
	기술장애	시스템 장애		운영체제 결함, 프로그램 결함, H/W 손상 등
		기반구조 장애		정전, 단수, 온도조절 실패, 설비운영상의 장애, 건물 손상 등

[표 1]을 기준으로 장애유형별 시나리오에 의한 피해규모를 추정한다. 특히 시나리오에 따라 장애를 등급화하여 비교 및 분석의 편의성과 객관성을 도모한다. 장애등급을 나누는 기준에는 1) 장애의 유형과 특성, 2) 장애 발생 경로와 피해 확산의 범위, 3) 복구에 소요되는 시간 등을 들 수 있다. 예를 들어, 정보보호 전문기관인 ITIL(Information Technology Infrastructure Library)에서는 장애등급의 정의를 다음과 같이 내리고 있다.

장애등급 = 영향력(피해규모) * 긴급성(복구시간)

ITIL의 장애등급 모형을 따를 때, '영향력'은 장애유형, 발생경로와 파급 범위 등에 의해 결정될 수 있는데, 궁극적으로 예상되는 평균 피해 규모로 측정될 것이다. 특히, 분석의 편의성과 객관성을 위하여 손실되는 트래픽량을, 피해 규모를 평가하는 기준으로 삼는다. ITIL 모형에서의 긴급성 역시 장애등급을 결정하는 주요 요소가 될 수 있지만, 이번 연구의 일차적인 목적이 상호연동 위험평가 프레임워크의 프로토타입을 개발하는 것에 있으므로, 논의의 편의를 위하여 배제한다. 향후 보다 정교한 프레임워크를 구축할 기회가 있으면, 영향력과 긴급성에 대하여 보다 체계적인 조작적 정의(operationalization)를 내릴 필요가 있을 것이다.

2) 상호연동 대안

상호연동 대안의 특징을 구분하는 기준에는 상호연동망 토폴로지, 서버와 기타 장비간의 물리적 연결구조, 대안별 방어기제의 특징, 대안별 구축 및 운용비용 등의 속성이 포함된다. 상호연동 대안별로 장애등급에 따른 위험수준이 산출되면, 1) 구축/운용비용과 2) 안정성 및 신뢰성을 두 축으로 하는 ROI(Risk On Investment)[1] 분석을 시도한다. 이를 통하여 대안들 간의 정량적 비교가 가능하다.

3) 서비스 트래픽 정보

상호연동 대안에서 IX 노드쌍(node pair)을 하나의 o-d쌍(origin-destination pair)으로 보고, 날짜 및 시간대별로 전형적인 트래픽 포트폴리오 프로파일(portfolio profile)이 주어진다고 가정한다. 이 포트폴리오 프로파일은 IX 노드가 수용할 수 있는 부하(load)를 포함하여 o-d쌍간 서비스별 트래픽 정보를 담고 있다. 이러한 프로파일들을 바탕으로, 주어진 상호연동 대안에서 특정 장애등급의 장애가 발생하였을 때, o-d쌍별로 손실되는 서비스 트래픽이 계산될 수 있다.

4) 위험평가 모듈과 평가엔진

이 모듈은 장애등급에 따른 트래픽 손실량(traffic loss)과 설비 피해 규모(facility damage)를 계산하여 실질적으로 위험을 평가하는 시스템(risk evaluation system)을 의미한다. 본 연구에서는 논의를 명확하게 하고자 설비 피해 규모는 고려하지 않고 손실된 트래픽 규모에만 집중하기로 한다(그러나 전자까지 고려하는 것이 전체 프레임워크에 변화를 주는 것은 아니다).

손실된 트래픽량은 서비스 포트폴리오 피해(service portfolio loss)로 환산되어 그 경제적 가치를 추정한다. [그림 2]에서 보듯이, 이 과정은 BTVDB(Business Transaction Value DB)와의 연동에 의해 수행되도록 하여, 최신 정보에 의해 피해의 경제적 가치를 산정할 수 있도록

1) 경영학 용어로 ROI는 투자에 의한 수익을 의미하는 Return On Investment의 약자이나, 여기서의 R을 Risk를 의미한다.

한다.

손실된 트래픽 규모와 서비스별 손실 규모, 전체 피해의 경제적 가치를 추정하기 위하여 아래와 같은 평가엔진(evaluation engine)을 적용한다.

트래픽 손실 계산 알고리즘

이 알고리즘은 주어진 상호연동 대안의 토폴로지와 o-d쌍 트래픽 자료를 입력으로 하여, 특정 장애등급에 해당하는 노드와 링크가 기능을 상실(block or fail)하거나 저하(degraded)되었을 때, o-d쌍간 유실되는 트래픽량을 계산한다. o-d쌍을 하나의 상품(commodity)으로 본다면 이는 다상품 최대흐름(multi-commodity maximum flow) 문제([16], [19])로 규정된다. 상품의 종류가 두 개인 경우에는 Gomory-Hu Tree([21])를 다상품으로 확장한 알고리즘에 의해 o-d쌍별 최대 흐름을 계산할 수 있다([21], [22]). 그러나 상품의 종류가 3 이상일 경우에는 [19], [22]와 같이 선형계획법(LP, Linear Programming)에 의존할 수밖에 없다. 본 연구에서도 LP에 의해 다상품 최대흐름문제의 답을 구하여 o-d쌍간 유실된 트래픽 규모를 산출한다.

서비스 포트폴리오 피해 산정

트래픽 포트폴리오 프로파일과 IX 노드쌍에서의 손실된 트래픽 규모를 바탕으로 서비스별 손실 규모를 추정한다. 예를 들어, IX a와 IX b 사이에서 손실된 트래픽량이 100단위이고, 두 종류의 서비스 X와 Y가 각각 30%와 70%로 트래픽을 구성하고 있다고 한다면, IX a와 b 사이 서비스 손실은 X와 Y에서 각각 30 및 70단위이다. 현행 최선형(best-effort) 인터넷에서는 서비스별로 트래픽을 구별할 수 없기 때문에, 위와 같이 선형적으로 서비스 손실이 분배된다고 가정하는 것에 무리가 없다. 서비스별 총손실은 모든 o-d쌍에서의 서비스 손실의 합이다.

피해 규모의 경제적 가치 추정

이 모듈은 서비스별 손실 규모와 BTVDB를 참조하여 장애에 따른 피해의 경제적 가치를 추정한다. 서비스 손실의 경제적 가치는 여러 기준에서 바라 볼 수 있으나, 본 연구의 목적에서는 서비스 손실의 경제적 가치를 트랜잭션 중단이 야기하는 비즈니스 및 매출 기회의 상실로 정의한다. BTVDB는 시시각각으로 변하는 서비스별 경제적 가치를 추적하며, 서비스간 상관관계(correlation)도 추정한다. 따라서 전체 서비스 손실의 경제적 가치는 일종의 분포로 추정되는 것이 바람직하다.

결국 여기서 제안하는 위험평가 프레임워크의 목표는, 특정 장애등급에 대하여, 주어진 신뢰수준에서 해당 기간 동안 예상되는 경제적 피해의 분포를 추정하는 것이다. 이를 반대로 해석한다면, 목표 위험허용수준(혹은 목표 위험방어수준)이 주어질 때, 이를 만족시킬 확률을 계산할 수도 있다. 이를 위해 먼저 아래와 같이 용어와 기호를 정리한다.

- Q = o-d쌍(즉, commodity)의 집합
- W = 서비스 인덱스 집합(즉, $|W|$개의 서비스가 상호연동 트래픽 포트폴리오를 구성)
- K = 장애등급 인덱스 집합
- T_K = 장애등급 K에서 손실되는 트래픽량의 벡터(트래픽 손실 계산 알고리즘에 의해 산출). 즉, $T_K = (T_K^{p_1q_1}, \cdots, T_K^{p_{|Q|}q_{|Q|}})$, 여기서 p_iq_i는 집합 Q의 i번째 원소를 나타냄.
- S_{iK} = 장애등급 K의 손실 트래픽 프로파일 T_k에서 서비스 i가 차지하는 트래픽 규모 (Cf. $T_K=\sum_i S_{iK}$). 즉, S_{iK}는 전체 o-d쌍에 대한 서비스 손실의 합으로, $S_{iK} = \sum_{\{p,q\}\in Q} S_{iK}^{pq}$.
- $V(S_{iK})$ = S_{iK} 의 경제적 가치로, 시장가치의 변동을 반영하기 위하여 특정한 확률분포를 따르는 것으로 가정함. 즉, $V(S_{iK})$는 평균(mean)= μ_{iK}, 표준편차(standard deviation)= σ_{iK} 의 정규분포(normal distribution)를 따른다고 가정함.
- $H(T_K)$ = 장애등급 K에서의 손실의 경제적 가치로, $V(S_{iK})$의 함수. 즉, $H(T_K) = f(V(S_{1K}), \cdots, V(S_{|W|K}))$.

상기한 모형에서 함수 $f(\cdot)$의 구조는 일반적으로 $V(S_{ik})$들의 단순 합은 아닐 것이다. 즉, 서비스간 상관관계를 명확히 반영할 필요가 있기 때문에 공분산(covariance) $Cov(i,j) \equiv \sigma_{ij}$를 파악할 필요가 있다. 또한 서비스 포트폴리오 손실의 일반화된 형태에서, 평균은 $E[H(T_K)] = \sum \omega_{iK} \mu_{iK}$ 이고, 분산은 $Var[H(T_K)] = \sum_i \omega_{iK}^2 \mu_{iK}^2 + \sum_i \sum_j 2\omega_{iK}\omega_{jK}\sigma_{ijK}$ 와 같이 표현될 것이다.[2] 그러나 현실적으로 ω_{iK}에 대한 이론적

2) 이러한 표현방식은 VaR(Value at Risk) 모형에

도출은 물론 계량적 추정 또한 쉽지 않다. 본 연구에서는 몬테카를로(Monte Carlo) 시뮬레이션을 적용하여 $E[H(T_K)]$와 $V[H(T_K)]$를 추정할 것이다. 이를 위해서는 $V(S_{iK})$를 실시간으로 추적하고 관리하는 DB가 있어야 하는데, 다음의 BTVDB가 바로 이러한 역할을 한다.

BTVDB(Business Transaction Value DB)

이 DB는 B2C, B2B와 같이, 인터넷을 통한 e-비즈니스 트랜잭션의 경제적 가치를 지속적으로 추적하고 관리한다. 예를 들어, 2007년 9월 현재, 은행 38개, 증권사 41개, 신용카드사 22개 등, 금융권 웹사이트는 100개 이상이며, 이들이 유발하는 트래픽은 전체 웹 트래픽의 약 8%를 차지한다([7]). 1인당 금융 관련 웹사이트에 체류하는 시간은 14분 이상이며, 방문자당 페이지 검색(page view)도 월 166.6회에 이른다. 또한 2006년 1분기 동안 e-뱅킹을 통한 자금이체는 1,475조 원, 온라인 신용카드 이용금액은 16조7천억 원에 달하였다([7]).

그런데 실제로 e-뱅킹을 위한 트랜잭션의 상당 부분은 대형 포탈과 관련된 트랜잭션에도 포함될 것이다. 즉, 많은 금융서비스 트랜잭션이 대형 포탈을 통해 발생한다. 이 경우 서비스 손실량의 상당 부분은 서로 밀접한 관련을 가지게 될 것이고, 이러한 상관관계를 명시적으로 고려할 수 있어야 경제적 가치를 올바르게 추정해 낼 수 있다. BTVDB는 이러한 상관관계를 추적, 기록, 분석하여 서비스 i와 j 간의 공분산 σ_{ij}를 추정할 수 있다.

5) 아웃풋(Output): 위험 분포

위험평가 프레임워크는 아웃풋으로, 상호연동 대안별로 장애등급 혹은 시나리오에 따른 경제적 피해 규모의 추정치를 제공한다. 특히 추정치는 몬테카를로 시뮬레이션에 의해 위험분포(risk distribution)로 제시되는데, 이는 장애로 인한 손실의 경제적 가치(value-loss) H(T)의 확률분포로 해석된다. 이러한 위험 분포로부터, 장애등급 K에 의한 서비스 손실의 시장가치의 평균 $E[H(T_K)]$과 분산 $Var[H(T_K)]$ 등을 대안별로 비교할 수 있다.

따른 것이다. 이번 연구에서는 VaR 모형을 명시적으로 고려하고 있지는 않으나, 위험평가방식을 보다 정교하게 다듬어, VaR 모형을 수용하는 방향으로 확장될 수 있다.

6) 목표 위험방어수준(Target Risk Tolerance)과 ROI(Risk On Investment) 분석

[20]에 의하면 위험관리의 궁극적 목적은 위험-수익 프로파일(risk-return profile)을 최적화하는 것이라고 한다. 이 단계에서는 이러한 목적에 부응하여 정책적 의사결정을 지원한다. 즉, 장애등급별로, 특정 상호연동 대안이 주어진 목표 위험허용수준 혹은 위험방어수준(TRT, Target Risk Tolerance)을 만족할 확률을 산출한다. 예를 들어, (어떤 기준과 원칙 등에 의하여) TRT가 α원으로 주어졌다면, 특정 장애등급 K에서의 상호연동 대안 X의 위험 분포로부터 경제적 손실이 α원 이하일 확률($Pr_X[H(T_K) \leq \alpha]$)을 계산할 수 있다. 이러한 과정을 또한 역으로 이용한다면, 현재 고려중인 대안에서 합리적 수준의 TRT를 결정하거나, TRT를 달성할 확률을 높이기 위하여 대안을 개선하는 방법과 이에 소요되는 비용 등을 추산할 수 있다. 대안별로 이러한 과정을 반복하여 ROI(Risk On Investment) 분석을 수행한다.

4. 상호연동 대안의 위험평가

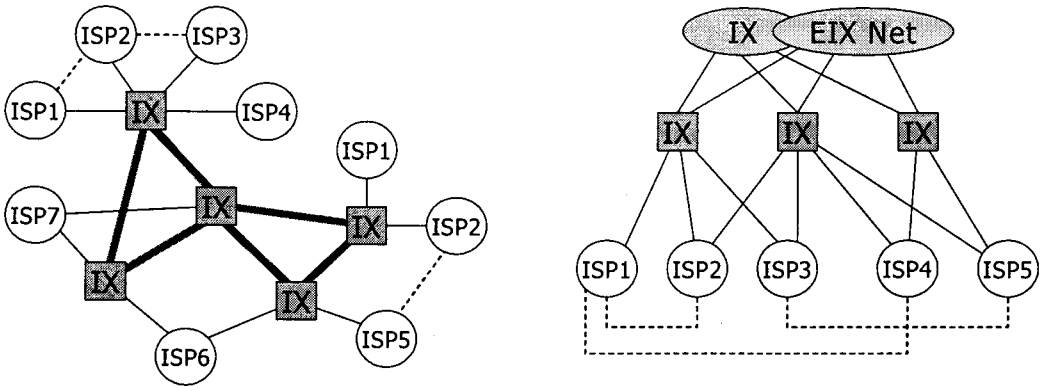
4.1 상호연동 대안의 개발

2절의 국내 인터넷 상호연동 현황에서 보면, KIX에 연결된 주요 상용망과의 대역폭은, KIX와 KT-IX, KIX와 DIX 등은 모두 2Gbps, KIX와 KINX는 11Gbps으로, 현재 각 IX별 처리능력이 최소 22Gbps에서 최대 100Gbps인 것을 감안 할 때, 대규모 인터넷 장애시 KIX의 중추적 역할을 기대하기는 어렵다. 이를 보완하기 위하여 다음 두 가지 방식의 상호연동 대안(기본형)을 제안한다.

먼저, ISP 및 상용 IX의 비상시 트래픽을 수용하는 비상용 IX(이하 방재형(emergency) IX로 부른다)를 구축하고, 국내 모든 ISP가 의무적으로 평균 트래픽의 특정 비율 이상을 방재형 IX로 전송할 수 있는 대역폭을 확보하는 방안을 생각해 볼 수 있다.

또 다른 대안으로, 별도의 방재형 IX를 설치하지 않고, 기존 상호연동체계를 존중하면서 상호연동망의 공공 IX를 분산시키는 토폴로지적 구조의 고도화를 통하여 장애에 대비하는 방안도 생각해 볼 수 있다. 이는 우리나라와 같이 특정 상용 IX가 전체 경로정보의 상당 부분을 운영하는 상황에 적합하다. 본 논문에

서는 전자와 같은 비상시 상호연동체계를 방재형 상호연동 대안으로, 후자를 분산 허브형(distributed hubs) 대안으로 부르기로 한다([그림 3] 참조).



(a) 분산 허브형 (b) 방재형

[그림 3] 상호연동 대안의 개념적 구분

[그림 3]은 각각 분산 허브형(a)과 방재형(b) 대안을 네트워크 모형 관점에서 개념적으로 도시한 것이다. (a)의 경우, 현재 수도권중심의 스타형 구조의 상호연동망으로부터 지역적 거점(허브) IX로 분산된 것이 특징이다. 이들 지역 IX를 별도의 망으로 연결하여 계층화시키고, ISP들로 하여금 최소한 두 곳 이상의 지역 IX와 이중으로 연결(bi-connected)되도록 한다. 이 경우, 계층화구조의 이점으로 인하여, 장애를 중간에 차단할 수 있다. 반면에 트래픽 로드의 분산을 위하여 상대적으로 많은 투자가 필요하다.

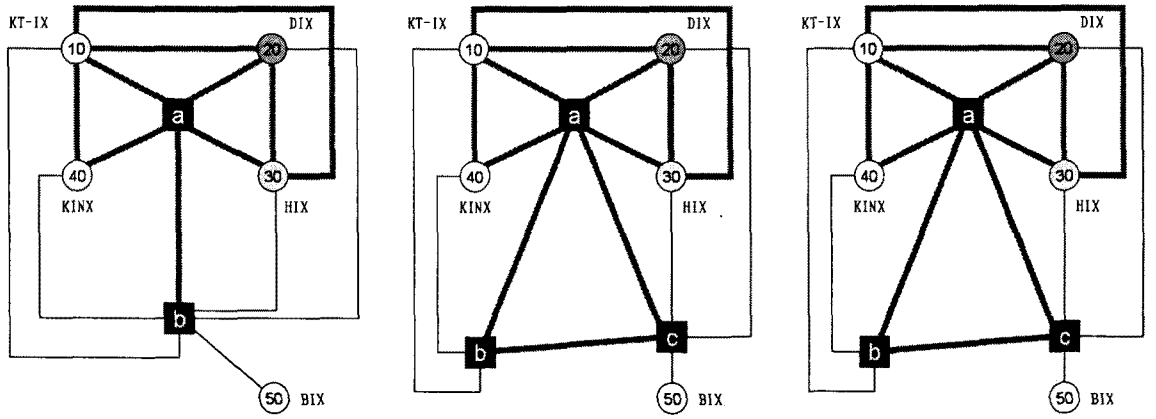
분산 허브형은 지역 거점 IX를 통하여 인터넷 활성화와 지역 발전의 촉매제가 될 수 있으므로, 지방자치단체의 적극적인 지원을 통해 재원을 조달할 수도 있을 것이다. 이를 바탕으로, 현재 국내의 인터넷 상호연동의 서울 및 수도권 집중을 완화할 수 있다. 현행 방식에서는 연동기반 자체가 서울과 수도권을 중심으로 형성되어 있어서, 수도권 이외의 지역 트래픽조차 서울을 경유하게 되어 단대단 경로가 길어지는 문제가 있다. 이에 따라 인터넷 품질이 저하되고, 장애발생 가능성도 증가되는 비효율성이 야기된다. 분산 허브형은 지역 인터넷 연동센터(거점 IX) 구축과 운영을 통해, 이러한 문제를 해결한다. 즉, 지역 허브는 비상시 트래픽 우회 및 문제가 발생된 지역 네트워크 분리 및 차단 등을 관리할 수 있다. 또한 상대적으로 트래픽이 밀집되는 특정 지역(수도권 등)에는 연동설비와 연결을 이중화하여 재난이 발생하여도 인터넷 트래픽을 분산처리할 수 있는 구조를 갖춘다.

이에 반하여 (b)의 방재형은 기존의 한국정보사회진흥원(舊 한국전산원)에서 운영하는 공공 IX(KIX)의 역할과 기능을 확대하는 방안을 제시한다. 즉, KIX가 공공기관 간의 연동뿐만 아니라 ISP 및 상용 IX 사이의 연동에도 관여하여, 비상시 끊임없는 상호연동이 유지되도록 한다. 방재형 IX는 최상위 인터넷 상호연동센터의 기능을 담당한다. 중립적이고 비영리기관에서 상호연동을 관장함으로써 상호접속을 공정하게 운영하고 중소형 ISP나 포탈의 인터넷 연동 비용을 낮추는 부수적인 효과도 기대할 수 있다.

이상에서 제안된 상호연동 대안들은 모두 지난 1.25 인터넷 사태를 비롯하여 수시로 발생하는 각종 해킹과 장애에 대비하기 위하여 국내 인터넷의 구조적인 취약성을 개선할 수 있을 것이다. 그러나 대안별로 장애유형에 효과적으로 대응하는 방식은 다를 것이다. 또한 투자 규모에 대하여 위험이 개선되는 효율성도 다를 것이다. 이와 같은 기술경제성을 종합적으로 고려하여 최선의 상호연동 대안을 선택하는 것이 바람직하다. 다음 절에서는 3장에서 제안된 위험평가 프레임워크를 적용하여 상호연동 대안별로 투자 규모에 따른 ROI를 산출하고 비교/분석한다.

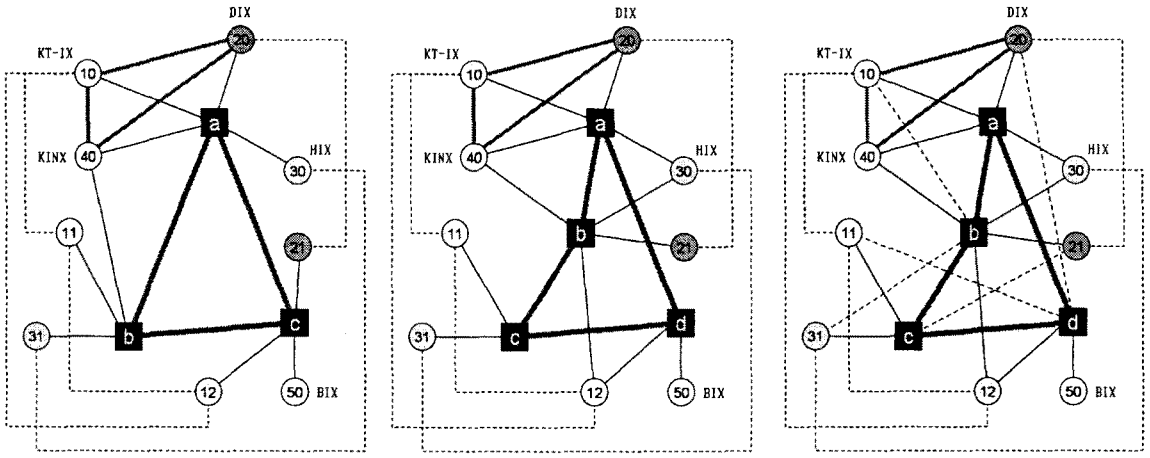
4.2 상호연동 대안별 위험평가

1) 실험 설계



방재형 1 방재형 2 방재형 3

(a) 방재형 상호연동 대안



분산 허브형 1 분산 허브형 2 분산 허브형 3

(b) 분산 허브형 상호연동 대안

[그림 4] 상호연동 대안

<u>상호연동 대안</u>

이번 실험에서는 분산 허브형과 방재형에 대해 각각 3가지 수준의 투자 단계(upgrade level)에 따른 상호연동망 토폴로지를 대안으로 한다. 이들 대안은 [그림 4]와 같으며, 대안별 노드 및 회선에 부속되는 비용과 트래픽 정보 등에 대한 자료는 지면제약상 생략한다.[3] 각 대안은, 예를 들어, '분산 허브형 x'와 같은 인덱스를 가지는데, 여기서 x는 해당 대안의 x단계 수준의 투자 규모에 의한 대안임을 나타낸다. x가 커질수록 보다 투자 규모가 증가하는 방향으로 하였다.

<u>장애등급 모형</u>

장애등급 모형에서는 총 6종류의 장애유형을 고려한다. 이 중에서 처음 3개는 경미한 수준의 장애가 서로 다른 위치에서 발생한 것으로 하며(Category 1-x), 나머지 3가지 유형은

3) IX 노드간 트래픽 및 대안별 구축/운영비용 등의 데이터는, KIX 및 KT-IX 등을 실제로 운영하는 전문가를 포함하여 관련 기관의 전문가들의 의견과 토의를 거쳐 본 실험에 적절한 수준에서 결정하였다.

순서에 따라 장애의 규모와 파급효과가 큰 중대형 장애(Category 2, 3, 4)를 나타낸다.

- Category 1-1~1-3 (C1-1~C1-3) : KT, 데이콤, 하나로, KINX 등의 IX 사업자간의 장애로, 장애의 파급범위가 해당 o-d쌍의 직접적 연결에만 영향을 미치는 경우로 설정된다. 예를 들어, C1-1에서는 KT 루트서버에 대한 DoS 공격으로 인해 특정 사업자(e.g., 데이콤)와의 경로표(routing table)에 에러가 발생하고, 이로 인하여 KT-IX와 DIX간 Peering 연결이 마비되거나 기능이 저하되는 경우를 가정한다.
- C2 : C1 장애가 좀 더 파급되어, 특정 사업자의 문제가 다른 두 개 이상의 사업자에게 영향을 미치는 경우를 나타낸다. 예를 들어, KT 경로표 중 DIX 및 KINX로의 연결이 삭제되거나 왜곡되는 경우가 이에 해당된다.
- C3 : C1 장애보다 더 큰 규모의 장애가 특정 사업자에게 발생하여, 해당 사업자의 모든 기능이 마비되거나, 50% 이상의 성능 저하가 발생하는 시나리오를 가정한다. 특정 사업자에게 연결된 공공 IX로의 부분적인 파급효과도 가정된다.
- C4 : 전체 상호연동망에서 가장 큰 역할을 담당하는 IX(공공 IX일 수도 있고, 특정 상용 IX일 수도 있음)의 기능을 거의 마비시키는 치명적인 장애가 발생하는 경우를 나타낸다. 예를 들어, 방재형의 경우에는 핵심 공공 IX에 이상이 발생하여, 이에 연결된 사업자간 상호연동 트래픽 처리가 상당 부분 상실되는 경우를 들 수 있다.

o-d쌍간 트래픽 및 서비스

o-d쌍에서의 트래픽은 기존의 트래픽 패턴을 참조하여 임의로 생성하였다. 단, 상호연동 대안 간의 공정한 비교를 위하여 적절한 수준에서 고정하였다. 즉, 전체 총량이 모든 대안에 대해 일정하게 고정되어 있으므로, 장애에 따른 트래픽 손실 규모가 대안별 장애 취약성을 서로 비교하는 것이 가능하다.

또한 o-d쌍간 트래픽에서 서비스 포트폴리오 프로파일은 일정하다고 가정한다. [그림 2]의 프레임워크에서 볼 때, 이러한 가정은 자료수집의 어려움과 계산의 편의성을 위한 것일 뿐이며 일반성을 해치지는 않는다(즉, o-d쌍간 서비스 프로파일이 주어진다면 언제든지 적용 가능하다). 본 실험에서는 인터넷 상거래에서 높은 비중을 차지하는 인터넷 뱅킹, 주식 등의 금융거래, 온라인 쇼핑 등의 서비스를 선정하였는데(아래 참조), 이들이 한 단위의 트래픽에서 차지하는 비중을 60:30:10 으로 고정한다. 이 비율은 인터넷 이용에 따른 서비스별 비중이 실제 트래픽에 반영된다고 가정함으로써 도출된 것이다. 이 비율은 추후에 민감도분석(what-if analysis)에 의하여 보정될 수 있다.

o-d쌍별 손실된 트래픽은, [19]에서와 같이, 다상품 최대흐름문제를 LP로 정식화한 뒤 AMPL/Cplex(ver.7.0) 프로그램을 이용해 계산하였다. 상호연동망의 네트워크 크기가 크지 않은 편이기 때문에 계산시간은 길어야 몇 초 이내이다.

서비스 종류와 BTVDB

몬테카를로 시뮬레이션은 CPU 등 컴퓨팅 자원을 많이 사용하는 방법으로, 지나치게 복잡할 경우, 원하는 시간 내에 충분한 신뢰성을 담보하는 결과를 확보하기 어렵다. 따라서 본 실험에서도 서비스의 종류는, 상호연동 실패에 따른 사회/경제적 영향력이 가장 클 것으로 예상되는 다음 세 가지로 한정한다.

- A: 인터넷 뱅킹 ~ N(120, 82) (이하 단위는 1,000억 원임).
- B: 인터넷 주식거래 ~ N(110, 112)
- C: 포탈을 이용한 온라인 쇼핑 및 광고 ~ N(1, 0.22)

개별 서비스의 시장가치는 시간대별로, 그리고 사회/경제적 상황에 따라 동적으로 변화한다. 이러한 불확실성을 반영하기 위하여 VaR를 비롯한 위험관리 모형에서는 서비스의 시장가치 분포가 일종의 확률분포를 따르는 것으로 가정한다. 본 연구에서도 서비스의 시장가치가 정규분포를 따른다고 가정하는데, 이는 가격변화의 위험을 반영하기 위함이다.

서비스별 평균은 해당 서비스의 1일 거래규모를 근거로, [7] 등의 자료로부터 산출하였다. 그러나 서비스별 시장가치의 분포의 표준편차는 적절한 근거자료를 구하기 어려워서 전문가들과의 회의[4]를 통해 추정하였다. 예를

4) 인터넷 상호연동 연구반에 참여하는 NIA, ETRI, KISPA 등의 기관의 전문가들과 토론을 통하여 결정하였음.

들어, 포탈을 통한 거래규모의 경제적 가치는 그 자체가 또한 여러 서비스로 분해될 수 있기 때문에 가장 큰 변동계수(대략 20%)를 가지며, 반면에 인터넷 뱅킹의 시장가치는 상대적으로 안정된 변동계수(7%)를 가진다. 또한 주식거래의 경제적 가치는 그 중간의 변동계수(10%)를 가진다고 할 때, 이들 변동계수로부터 역으로 표준편차를 환산하였다.

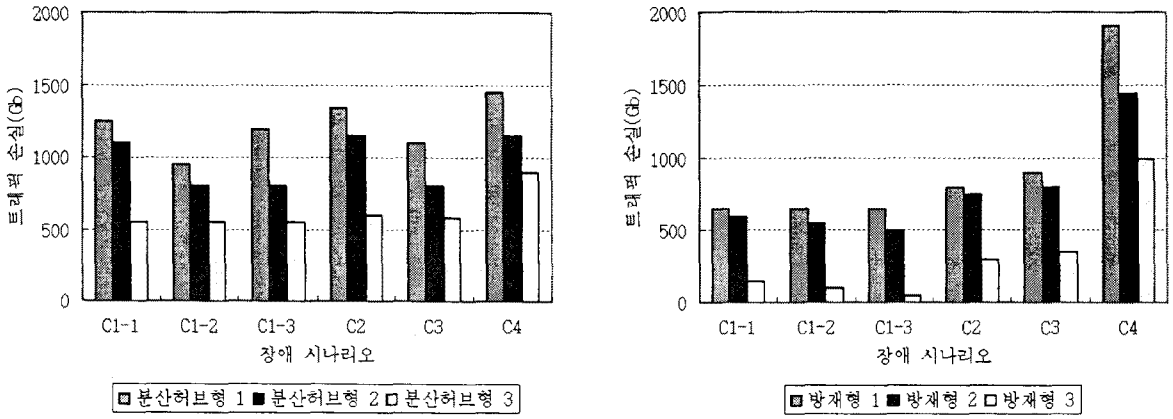
마지막으로, 피해 규모가 과대 추정되는 것을 막기 위하여 관련성이 높은 인터넷 서비스 거래의 경우 부(-)의 상관관계를 고려하여야 한다. 예를 들어, 온라인 쇼핑을 위해서는 인터넷 뱅킹과 같은 전자결제가 수반되므로, 이들을 별개로 추정하여 더한다면 피해 규모가 과대 계상된다. 이러한 오류를 막기 위하여 서비스간 상관관계를 다음과 같이 설정하였다: $\sigma_{AB} = 0.3$, $\sigma_{AC} = 0.6$, $\sigma_{BC} = 0.2$. 이 역시 기존의 문헌에서는 자료를 찾을 수가 없어서, [7] 등의 시계열 자료로부터 회귀분석을 통해 개략적인 상관관계를 추정하고, 이를 전문가 자문을 통해 보정하는 방식을 취했다. 본 연구의 위험평가 프레임워크를 본격적으로 적용한다면 이들 파라미터에 대한 보다 상세한 추정이 필요하다.

2) 실험 결과

<u>대안별 위험평가와 비교</u>

상호연동 대안별로 장애등급에 따른 트래픽 손실은 [그림 5]와 같다. 트래픽 손실량은 Gbps를 단위로 표현하였으며, 앞에서 소개한 6가지 장애 시나리오에 대해 손실되는 트래픽의 총량을 보여주고 있다. 그림에서 보듯이, 모든 대안에서, 그리고 모든 장애유형에 대해서, 방어기제 구축/운영비용이 증가함에 따라서 유실되는 트래픽 규모가 작아짐을 알 수 있다. 그러나 그 패턴에 있어서 차이를 보인다. 분산 허브형의 경우에는 손실 규모가 장애 시나리오 강도에 선형적으로 비례하는데 반하여, 방재형의 경우에는 장애등급이 강화됨에 따라서 트래픽 손실량이 급격히 증가한다.

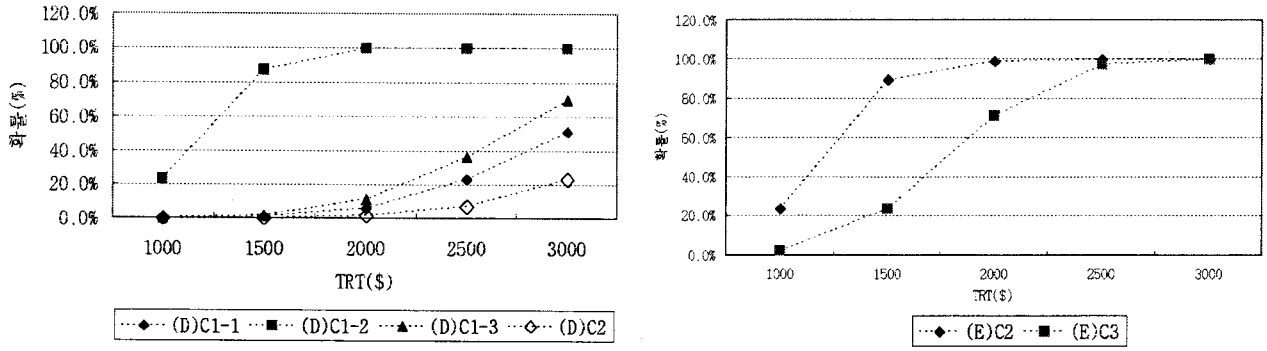
또한 투자에 따른 효과에 있어서도 두 대안 유형은 서로 다른 반응을 보인다. 방재형의 경우, 방어기제 투자에 따른 효과가 특정 단계 이후 급격히 증가하나, 분산 허브형에서는 투자에 따른 효과 역시 상대적으로 완만하게 증가하는 것으로 보인다.



[그림 5] 장애등급에 따른 트래픽 손실

장애등급에 따른 대안별 위험방어율은 아래 그림과 같다. [그림 6]에서 x-축은 5가지 TRT 수준을 나타내고 y-축은 방재형 2와 분산허브형 2 대안의 방어율을 나타낸다. 그림에서 보듯이, TRT 수준이 높아짐에 따라 모든 대안과 장애등급에서 방어율이 향상되는 것은 당연하나, 그 패턴은 대안별로 매우 상이하다. 예를 들어, 방재형에서 TRT 수준을 1,500으로 하였을 때, C2 장애등급에서는 90% 가까이 목표 TRT를 방어하였으나 C3 장애등급에 대해서는 그 확률이 20%대로 급속히 감소한다. 반면에 분산 허브형에서는 완만히 감소한다. 주어진 TRT 수준에서 방어율을 일종의 신뢰성으로도 해석할 수 있기 때문에, 이상의 결과로

부터 (C4 장애등급은 제외하고)전반적으로 방재형의 신뢰성이 분산 허브형에 비하여 높다고 말할 수도 있다.

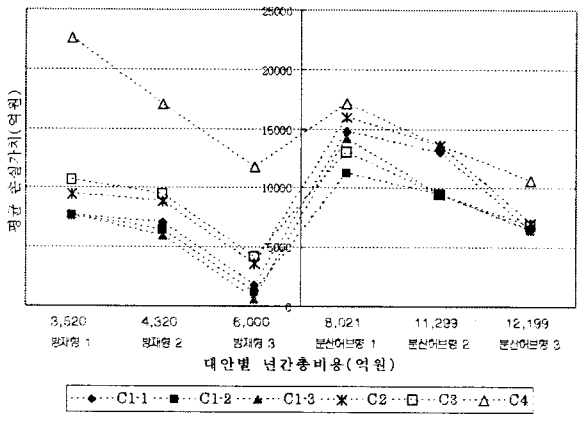


(a) 분산 허브형 2 (b) 방재형 2

[그림 6] TRT 수준에 따른 방어율 변화

반면에 C4 수준의 장애 시나리오에 대한 결과는 [그림 6]과는 정반대의 양상을 보인다 (도표는 생략함). 즉, TRT 방어율 측면에서 분산 허브형이 방재형을 지배한다. 이는 분산 허브형이 장애등급의 변화에는 매우 강건함(robust)을 보여주는 것으로, [그림 5]의 결과와도 일맥상통한다. 반면에 방재형은 장애의 수준이 특정 임계치를 넘게 되면 그 피해 규모가 급증할 수 있음을 의미한다.

ROI 분석과 최선의 상호연동 대안



[그림 7] 투자 규모 vs. 경제적 손실가치 평균

이 단계에서는 상호연동 대안들의 경제성과 신뢰성을 종합적으로 평가하여, 최선의 대안을 찾는다. 이하의 실험 결과에서 보듯이, ROI 분석은 (앞에서 시행한 것과 같이) 단순히 위험수준만을 평가해서는 올바른 대안을 찾을 수 없다는 점을 알려준다. 경제적 관점에서의 투자비용과 기술적 특성에 따른 위험수준을 동시에 고려할 수 있어야 정확한 판단을 내릴 수 있다.

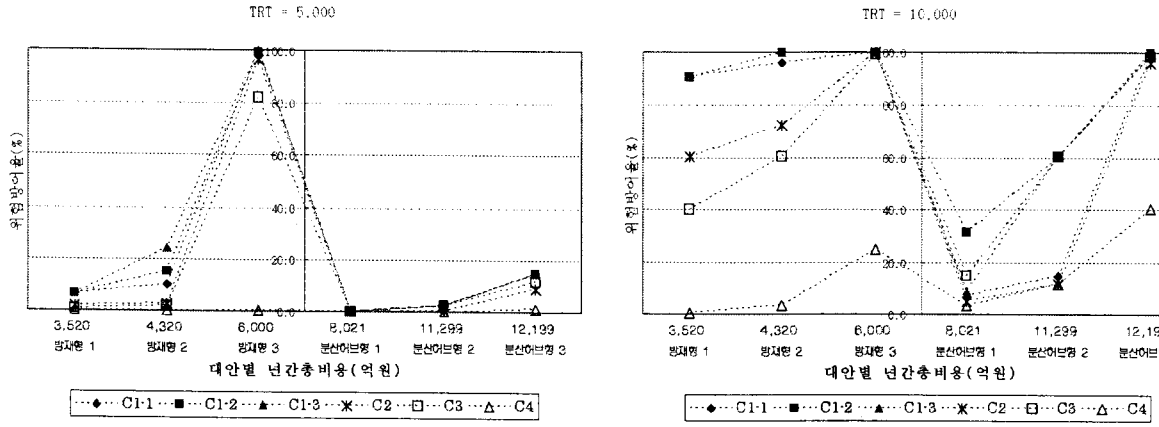
먼저, 대안별 투자 대비 장애 시나리오에 따른 위험도를 도시하면 [그림 7] 및 [그림 8]과 같다. 이들 그림은 대안별 구축/운영비용(x-축)에 대하여 평균적인 손실가치 혹은 주어진 TRT에서의 손실 방어율(y-축) 등을 보여준다.

그림들에서 보는 바와 같이, 모든 대안에 있어서 장애등급이 심화될수록 평균 손실도 증가한다. 그러나 방재형 대안 3의 경우, C4 장애에서도 손실가치의 평균이 분산 허브형 대안 1의 C2나 C3 (심지어 C1의 일부)에 대해서도 낮은 것으로 나타났다. 방재형 대안 3의 연간 구축/운영비용이 분산 허브형 대안 중에서는 가장 비용이 낮은 분산 허브형 1 보다도 낮다는 점을 고려할 때, 이러한 결과는 최소한 분산 허브형 대안 1은 후보에서 배제되어야 함을 의미한다.

주어진 TRT 수준에 따른 위험방어율 관점에서 대안들의 ROI를 비교한 것이 [그림 8]이다. 먼저 30분간의 장애에 대하여 TRT가 5,000억 원으로 비교적 엄격하게 주어진 경우에는, 방재형 대안 3을 제외하고서는 방어율이 20%에도 미치지 못하는 경우가 대부분이다. 방재형 대안 3의 경우에도 C3 장애에 대해서는 90% 이상의 가능성으로 방어할 수 없으며, C4 장애에 대해서는 급속히 취약해지는 (방어

율 0%에 근접) 취약점을 보인다.

TRT 수준을 10,000억 원으로 완화하였을 경우, (C4 장애를 제외한다면) 방재형의 방어율은 급속히 향상된다. 반면에 분산 허브형의 방어율은 방재형에 비하여 크게 개선되지 못한다.



[그림 8] TRT=5,000억 원 및 10,000억 원에서의 대안별 위험 방어율

이상의 실험 결과를 종합적으로 놓고 평가할 때, 분산 허브형 대안이 장애등급에 선형적으로 반응하는 강건함을 보이기는 하나, 그 구축/운영비용과 위험효율성 간의 ROI 측면에서 방재형에 비해 우수하지 못한 것으로 판단된다. 특히 분산 허브형 1은 가장 열등한 대안으로 고려 대상에서 배제하는 것이 바람직하며, 분산 허브형 3은 방재형과 비교가능한 위험효율성을 보이나 비용 측면에서 정당화되기 어렵다. 결론적으로, 방재형 대안이 투자비용에 대한 위험 개선 효과가 가장 좋을 것으로 판단된다. 다만, 방재형 대안들이 공통적으로 가지는 문제점, 즉, C4 장애처럼 공공 IX에 직접적인 피해를 유발하는 장애나, IX에 집중되는 공격에 대하여 급속히 성능이 저하되는 취약점을 보완하는 방안을 마련하여야 한다.

이러한 결론은 신뢰성과 안정성이 강화된 상호연동체계로의 진화와 관련하여 다음과 같은 방향성을 제시한다. 먼저, 현행 상호연동체계로부터의 진화를 고려해야 한다는 현실적 제약을 감안할 때, 기존의 구조와 가장 유사한 방재형 대안이 첫 번째 후보가 되는 것이 바람직하다. 실제로 지역별로 복수의 IX를 설치하고 IX간 네트워크를 다시 탑재(overlay)해야 하는 분산 허브형에 비하여, 방재형 대안은 현행 상호연동체계의 확장을 통하여 상대적으로 쉽게 구현된다. 또한 방재형 대안(특히 방재형 3)의 비용 대비 위험효율성은, 최소한 중간 단계 해결책으로서 이 대안을 매력적으로 보이게 한다. 이러한 로드맵을 바탕으로 모든 장애유형에 대해 강건함으로 보이는 상호연동망으로 단계적으로 발전시켜 나가는 것이 바람직할 것이다.

5. 결론

본 논문에서는 기존의 최선형(best-effort) 인터넷에서의 상호연동의 신뢰성과 안정성을 높이기 위한 상호연동 대안들을 고찰하였다. 특히, 이들 대안의 성능을 비교/평가하기 위하여 위험평가 프레임워크를 개발하여 적용하였다. 프레임워크는 대안별로 장애로 인해 손실된 트래픽과 서비스의 경제적 가치의 분포(위험분포)를 제공한다. 또한 몬테카를로 시뮬레이션을 통하여 다양한 상호연동 대안의 ROI 분석도 시도하였다.

실험 결과는 방재형 대안이 투자 대비 위험효율성 측면에서 다른 대안들에 비해 우위에 있음을 보여준다. 방재형 대안은 기존의 상호연동체계로부터의 확장과 이전(migration)에 있어서도 보다 용이하므로, 향후 방재형 대안을 중심으로 상호연동망을 진화시키는 로드맵이 바람직할 것으로 보인다. 단, 방재형 대안의 경우 C4와 같은 대형 장애에 대해서는 급격히 취약해지는 단점을 보이기 때문에, 이를

보완하는 메커니즘을 개발할 필요가 있다.

본 연구의 한계와 이를 보완하기 위한 향후 연구방향은 다음과 같다. 첫째, 현실 데이터를 수집/가공하는 데에는 한계가 있었기 때문에 프레임워크 적용에 필요한 각종 파라미터가 다소 주관적으로 결정된 경향이 있다. 따라서 위 실험 결과에서의 수치에는 큰 의미를 부여하지 않는 편이 나을 것이다. 단지 실험 결과의 질적인 측면(예를 들어, 방재형이 분산 허브형에 비해 비용 대비 효과 측면에서 유의한 수준으로 우월하다는 결과 등)에만 관심을 가지면 된다. 향후 연구에서 파라미터들에 대한 보다 신뢰성 있는 추정치가 제공된다면, 실험 결과의 값 자체도 시사하는 바가 있을 것이다.

또한 이번 연구에서는 현행 최선형 인터넷 방식에서의 상호연동망을 대상으로 하지만, 향후 BcN과 같은 차세대 인터넷에서의 상호연동방식에는 변화가 있을 것이기 때문에, 새로운 특성이 반영되도록 위험평가 프레임워크를 확장할 필요도 있다. 대표적으로, BcN에서는 서비스별 차별화에 따른 QoS 보장 메커니즘이 제공된다. 이 경우 유실된 트래픽에 대응되는 정확한 서비스 손실량을 추정하는 것은 매우 복잡해진다. 특히 서비스별로 차별화된 우선순위 경로설정(priority routing)이 적용된다면, o-d쌍별로 손실된 트래픽을 서비스 프로파일의 비율에 따라 선형적으로 분배할 수는 없을 것이다. 이를 추정하기 위해서는 공개가 어려운 사업자의 망운영 정보에 의존해야 하는 현실적으로 어려운 문제에 직면한다. 그럼에도 불구하고, 본 연구에서 제안한 프레임워크의 일반적인 틀은 차세대 인터넷 상호연동에서도 그대로 유지될 것이다.

참고문헌

[1] 김대원, 최양서, 김익균, 오진태, 장종수 (2006) 네트워크 보안을 위한 공격 분류법, 주간기술동향 통권 제1249호, 2006.6.7.

[2] 김도훈 (2006) All-IP 컨버전스에서 End-to-End QoS의 효과적 구현을 위한 ISP 상호접속, Telecom. Review, 제16권 제1호.

[3] 김도훈 (2004) SLA 제약하에서 ISP간 상호접속 모형에 대한 개관 및 기술/정책적 문제에 대한 고찰, 정보통신정책학회 2004 학술대회 발표논문집, pp.37-58.

[4] 문호건, 최진기, 김형순 (2004) ISP(Internet Service Provider) 네트워크의 정량적인 위험분석을 위한 시스템 설계 및 구현, 정보보호학회논문지, 제14권 제2호, 2004.4.

[5] 서동일, 김기영, 장종수 (2006) 유비쿼터스 사회의 사이버 공격 기술 동향, 주간기술동향 통권 제1259호, 2006.8.16.

[6] 하나로텔레콤 (2007) 네트워크 장애유형 분류와 대응방안 사례, 인터뷰 메모, 2007.1.

[7] 한국정보사회진흥원 (2007) 인터넷 백서, 한국인터넷진흥원.

[8] 한국정보사회진흥원 (2006) 최근 주요 인터넷 서비스 장애와 이용자, Issue Tagging.

[9] 한국전산원 (2005) 인터넷 교환노드(IX) 법제도화를 위한 연구, NCA 보고서(II-RER-02115).

[10] 한국전산원 (2005) IP기반의 통합서비스 제공 및 상호연동체계 수립을 위한 연구, NCA 보고서(II-RER-05032).

[11] 한국전산원 (2002) 차세대인터넷 기반구축에 관한 연구, NCA 보고서(II-RIR-02115).

[12] "1·25 인터넷대란 후 1년, 이제 안전한가?," 좌담회 자료, 2004.1.

[13] KISA, 월간 침해사고 통계.

[14] Bailey, J. and L. McKnight (1997) Scalable Internet Interconnection Agreements and Integrated Services, in Coordinating the Internet (Eds: Brian Kahin and James H. Keller), MIT Press, pp.309-324.

[15] Berman, D.K. (2003) Wire Transfer: Telecom Investors See Big Potential In Failed Networks, Wall Street Journal (Eastern edition), New York, Aug 14, 2003.

[16] Boldyreff, A.W. (1995) Determination of the Maximal Steady State Flow of Traffic through a Railroad Network, Journal of the Operations Research Society of America, Vol.3, No.4., pp.443-465.

[17] CNET (2006) MySpace Feels the Heat, http://www.cnet.com (2006.7.24 접속).

[18] Dewan, R., M. Friemer and P. Gundepudi (1999) Evolution of Internet Infrastructure in the 21st Century: the Role of Private Interconnection Agreements, Proceedings of ICIS, pp.144-154.

[19] Ford, N.R. and D.R. Fulkerson (1958) A Suggested Computation for Maximal Multicommodity Network Flows, Management Science, Vol.5, pp.97-101.

[20] Froot, K.A., D.S. Scharfstein and J.C. Stein (1994) A New Approach to Risk Management, Harvard Business Review, Nov./Dec. Issue, pp.91-102.

[21] Gomory, R.E. and T.C. Hu (1961) Multi-terminal Network Flows, SIAM Journal, Vol.9, pp.551-570.

[22] Gomory, R.E. and T.C. Hu (1962) An

Application of Generalized Linear Programming to Network Flows, SIAM Journal, Vol.10, pp.260-283.
[23] Grubesic, T.H. and A.T. Murray (2005) Spatial-historical Landscapes of Telecommunication Network Survivability, Telecom Policy, Vol.29, pp.801-820.
[24] Heckmann, O., J. Schmitt and R. Steinmetz (2004) Optimizing Interconnection Policies, Computer Networks, Vol.46, pp.19-39.
[25] Hu, T.C. (1963) Multi-commodity Network Flows, Operations Research, Vol.11, pp.344-360.
[26] Huston, G. (1999) ISP Survival Guide: Strategy for Running a Competitive ISP, Wiley.
[27] Kolesar, M. and L.L. Stanford (2004) Rationalizing Interconnection Agreements in Competitive Markets, in Global Economy and Digital Society (Eds: Erik Bohlin, et. al.), Elsevier.
[28] Mavrakis, N. (2003) Vulnerabilities of ISPs, IEEE Potentials, Oct/Nov Issue, pp.9-15.
[29] Metz, C. (2001) Interconnecting ISP Networks, IEEE Internet Computing, March/April Issue, pp.74-80.
[30] Pongpaibool, P. and H.S. Kim (2004) Providing End-to-end Service Level Agreements across Multiple ISP Networks, Computer Networks, Vol.46, pp.3-18.
[31] Reuters (2001) U.S.A. Terror: Sever Damages on Telecom Infrastructure in NYC, 2001.9.14.