情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

물리적 부하 균형(Load-balancing) 기반의 침해방지를 위한 통신라인 다중화에 관한 연구

최 희 식[1†], 서 우 석[1‡], 전 문 석[2]
[1]숭실대학교 일반대학원, [2]숭실대학교

A Study on the Multiplexing of a Communication Line for the Physical Load Balancing-Based Prevention of Infringement

Hee-sik Choi,[1†] Woo-seok Seo,[1‡] Moon-seog Jun,[2]
[1]Soongsil Graduate School, [2]Soongsil University

요 약

2011년 현재 보안 침해를 목적으로 하는 많은 공격 도구들이 인터넷 상에 떠돌고 있으며, 이러한 도구들 중 대다수가 실제 침해 공격이 가능하다. 또한, 2010년 PS3의 취약점을 공격하는 프로그램 소스와 2011년에는 Stuxnet Source Code 등 다양한 공격 Agent와 공격 도구의 소스가 공개됨에 따라 방어를 목적으로 하는 부분에 있어서 가장 큰 부담이 되고 있으나, 방어하는 측의 입장에서는 공격 소스를 분석함으로써 동일하고 유사한 패턴의 공격을 방어할 수 있는 기법을 제안하고 개발할 수 있는 기회이기도 하다. 이와 같은 공격에 대비하기 위한 방법으로 공격의 대상이 되는 네트워크 영역을 로드밸런싱 기반 하에 공격 유형별 방어정책을 접근 게이트웨이 및 통신라인별로 구분하고 통신라인을 다중화 하는 방식의 방어기법을 제안한다. 본 연구 결과는 2010년을 기점으로 하드웨어 인프라의 가격 경쟁력 상승 등을 통한 높은 하드웨어 성능을 기반으로 방어정책 구현을 위한 현실적인 자료를 제공하고자 한다.

ABSTRACT

Presently in 2011, there are countless attacking tools oriented to invading security on the internet. And most of the tools are possible to conduct the actual invasion. Also, as the program sources attacking the weaknesses of PS3 were released in 2010 and also various sources for attacking agents and attacking tools such as Stuxnet Source Code were released in 2011, the part for defense has the greatest burden; however, it can be also a chance for the defensive part to suggest and develop methods to defense identical or similar patterned attacking by analyzing attacking sources. As a way to cope with such attacking, this study divides the network areas targeted for attack based on load balancing by the approach gateways and communication lines according to the defensive policies by attacking types and also suggests methods to multiply communication lines. The result of this paper will be provided as practical data to realize defensive policies based on high hardware performances through enhancing the price competitiveness of hardware infrastructure with 2010 as a start.

Keywords: PLB(Physical Load-Balancing), Dual Communication Line, Bandwidth, Infringement Prevention

I. 서 론

네트워크 보안 침해사고는 2009년 7.7 DDoS (Distributed Denial of Service attack, 분산 서비스 거부 공격) 대란이후 급격한 증가추세를 보이

접수일(2011년 8월 10일), 게재확정일(2011년 11월 9일)
† 주저자, dali3054@ssu.ac.kr
‡ 교신저자, ssws2003@yahoo.co.kr

고 있다. DDoS 공격으로 인한 파급효과로 새로운 공격 도구와 공격을 위한 제반정보 취합 등의 역할을 하는 악성 Agent들이 추가적으로 개발되어지고 다양한 환경 속에 깊숙이 침투하여 있는 실정이며, 치명적인 공격 도구의 소스 등이 공개되어 지고 있어 더 큰 사회적인 문제점과 장애를 유발하고 있다[1].

과거 또는 현 시점에도 다양한 보안장비인 Firewall, VPN(Virtual Private Network), IDS(Intrusion Detection System), IPS(Intrusion Prevention System), ESM(Enterprise Security Management) 등 침해공격에 대한 방어 목적으로 구축되고 운영되어지고 있으나, 통신라인을 통한 최초 불법적인 공격 접근 라인에 대한 사전보안이 아니며, 이미 네트워크에 침입을 하는 단계인 게이트웨이에 접근한 이후 이루어지는 보안기기 이므로 1차원적인 정보 흐름이 유지되는 통신라인 상에서 차단이 가능한 보안부문을 재조명 하고자 한다.

따라서 본 논문에서는 다양한 보안장비를 이용한 제반기기 상의 불법적인 공격을 차단하는 영역 이전에 최초 특정한 네트워크로 접근하는 물리적인 통신라인을 1차적인 방어 단계로 보고 이를 로드밸런싱 기법을 활용하여, 공격의 대상이 되는 네트워크 영역을 공격 유형별 방어정책을 적용함으로써 접근 게이트웨이 및 통신라인별로 구분하고 통신라인을 다중화 하는 방식의 방어기법을 제안한다.

본 논문의 구성은 2장에서는 심각한 침해사고 유형과 통신라인 운영현황, 국내외 주요 네트워크 장비 현황에 대해 분석하고, 3장에서는 침입 방어 기법에 대해서 3가지 기본방어방법과 제안기법을 순차적으로 비교 설명하며, 4장에서는 제안한 방어기법을 실험하고 결과를 도출한다. 마지막으로 5장에서는 논문의 결론과 향후 연구 과제를 제시한다.

II. 관련연구

2.1 통신 침해사고 유형

2009년 이후 후속적으로 발생하고 있는 침해기법은 과거처럼 공격자가 일부 특정 서버 또는 네트워크를 경유함으로써 자신을 숨기며, 공격하는 형태에서 이미 배포되어 숨겨져 있는 Agent를 가동하는 명령을 내림으로써 발생하는 침해가 증가하고 있다. 이러한 공격기법은 이미 우리가 사용하는 공중망뿐만 아니라 바이러스, 악성코드, 광고 선전을 위한 Agent 등에도 Backdoor 형태로 존재한다는 것이다. 따라서 공격을 막고 공격을 시행한 공격자를 역추적 하는 기술 또한 최초 Agent를 배포한 경로를 함께 확인하는 수준까지 이원화된 방어기법 및 역추적 기술이 함께 발전해야한다[2].

또한, 새로운 서비스를 위한 네트워크 최초 구성 시부터 공격과 방어를 위한 기술적 다면 성능 평가 등의 사전 평가가 이루어짐으로써 단순히 사회적인 문제가 되는 경우에 대한 제한적인 보안정책이 아닌 거시적인 면을 반영한 단계적, 순차적 보안기법 개발이 이루어져야 한다.

〔표 1〕은 2011년 상반기를 기준으로 한국인터넷진흥원에서 제공하는 해킹 사고 접수 및 처리 건수 현황으로 스팸릴레이를 비롯한 총 5가지의 공격 신고건수와 침해 증가 비율을 나타내며, 조사결과에서 확인할 수 있는 가장 큰 이슈는 지속적으로 공격이 증가함에 따라 사고접수 건수 역시 비례하게 증가되고 있다는 것을 의미하며, 통신라인을 논리적인 측면의 소프트웨어적인 부분과 물리적인 측면의 하드웨어적인 부분으로 구분하고 통신선로를 다중화 함으로써 접근하는 침해형태에 따른 안정적인 방어 인프라를 구축해야함을 나타낸다[3].

2.2 통신라인 운영 현황과 종류

논문에서 제안하고 실험하고자 하는 보안기법은 최초 네트워크상의 게이트웨이에 접근 이전에 통신라인을 물리적으로 로드밸런싱 함으로써 공격에 따른 라인

〔표 1〕 해킹 사고 접수 및 처리 건수 현황

구분	2011년						
	1월	2월	3월	4월	5월	6월	합계
스팸릴레이	174	256	408	443	448	453	2,182
피싱경유지	30	25	38	24	29	22	168
단순침입시도	322	231	272	243	257	214	1,539
기타해킹	358	239	155	179	121	222	1,274
홈페이지변조	141	103	129	110	206	46	735
총계	1,025	854	1,002	999	1,061	957	5,898

전환을 통한 방어를 나타내고 있다.

따라서 〔표 2〕와 같이 유선 통신 매체이자 서비스 라인 현황을 확인함으로써 소규모 네트워크에서 라인 이중화 및 다원화된 대규모 네트워크 규모까지 적용 가능한 환경 하에서 실험에 따른 객관적인 결과를 얻고자 하며, 다양한 통신선로 현황을 확인함으로써 작은 네트워크로부터 대규모 네트워크 인프라까지를 본 논문의 범주로 구성하고 실험하기 위한 유선 통신라인 매체 종류를 보이고 있다〔4〕〔5〕.

추가적으로 21세기에 접어들면서 유선시장은 다소 기술과 기능부분에서 많은 퇴보를 하고 있으며, 현재는 WiFi를 비롯한 많은 유무선 통신이 보편화되고 있는 시점에서 다양한 통신 매체를 기반으로 물리적인 보안 기법을 적용하기 위한 방안으로 〔표 3〕과 같이 무선통신 매체에 대한 종류 또한 분석이 필요하다.

다만, 통신 라인에 대한 다중화를 위한 본 논문에서는 유선을 기반으로 하는 각 통신 매체 서비스를 대상으로 공격에 따른 방어기법을 적용하고 최적의 통신 라인 조합을 구성한다.

2.3 국내외 통신 사업자 주요 네트워크 장비운영 현황

여러 종류의 통신 매체의 경우, 사용자의 요구에 따른 개발되고 구현되는 것이 아니며, 통신 사업자에 의

〔표 2〕 유선 통신라인 매체 종류

구분	Ethernet	Fast Ethernet	Giga Ethernet				ATM Lan	FDDI	Token Ring
			CX	LX	SX	TX			
전송속도	10Mbos	100Mbps	1Gbps				150~620 Mbps	200Mbps	4Mbps ~10Gbps
사용매체	UTP/STP	UTP/ STP/ Optical Fiber	UTP/Shieded Copper/Optical Fiber				UTP/STP/ Optical Fiber	Optical Fiber	UTP/STP/ Optical Fiber
표준화	IEEE802.3	IEEE802.3	IEEE802.3				-	X3T9.5	-
접근방법	CSMA/CD	CSMA/CD	CSMA/CD				CSMA/CD	CSMA/CD	-

* 각 통신사별 서비스 되고 있는 통신 서비스의 품질과 용어의 차이가 있어서 "통신 라인"은 거시적인 표현으로 "통신매체"는 미시적인 범주로 구성하고 의미를 부여한다.

〔표 3〕 무선 통신라인 매체 종류

구분		WCDMA	WIBRO	Wi-Fi	LTE	HSPA+	WiMAX	HSDPA
최대 전송 속도	하향	14.4Mbps	10Mbps	300Mbps	300Mbps	14.4Mbps 〔가능 : 21~28Mbps〕	19.2Mbps	최대 1.8Mbps 또는 최대 3.6Mbps
	상향	5.7Mbps	10Mbps		150Mbps		4.95Mbps	
사용 대역폭		5MHz	10MHz	22MHz 이하	1.4M~20MHz	700MHz	2.3Ghz, 8.75/10Mhz	2~2.1GHz〕
다중접속 방식		CDMA	상향, 하양 : OFDM	CDMA	하향 : OFDMA 상향 : 단일 캐리어 FDMA	CDMA	하향 : OFDMA 상향 : OFDMA	CDMA
무선 접속	하향	CDMA	CDMA	-	OFDMA	HSDPA, HSUPA	-	HSDPA, CDMA 1X EV-DO
	상향	CDMA	CDMA	-	SCFDMA		-	
변조방식		QPSK/16QAM	하향(QPSK, 16QAM, 64QAM) 상향(QPSK, 16QAM)	OFDM	QPSK 16QAM/64QMA	16QAM에서 64QAM으로 전환	Subcarrier Allocation 〔채널코딩 및 H-ARQ〕	16QAM

〔표 4〕 주요 네트워크 장비구축 및 운영현황

구분	FTTH/BWA/x DSL/Cable	SDH/SONET/ MsPP/WDM	Router Switch	Traditional Switching	Voice Exchange/Control
2009년	6,141	13,376	9,873	1,495	5,104
2010년	6,373	13,820	12,086	1,278	5,077
전년대비 증가율	3.8%	3.3%	22.4%	-14.5%	-0.5%
2010년 비중치	7.7%	16.8%	14.7%	1.5%	6.2%

* 기준단위 : 백만 달러 / 현황기준 100%에서 제시현황을 제외한 사항은 기타 비율

해 개발되고 가장 최적의 서비스라고 홍보하고 또한, 통신 매체를 임대 사용하는데 있어서 경제성 논리를 반영한 도입이 가장 큰 비중을 차지한다.

따라서 〔표 4〕에서 통신 사업자들이 가장 중요시하고 구축 및 운영하는 통신 인프라에 대한 개발비용(구축비용 등)과 년도 별 확장 비율 등을 가시적으로 확인 가능하다〔6〕〔7〕.

통신사업자들이 선호하고 주요시 하는 통신 매체를 본 논문에서는 실험과 제안 시에 비교분석자료로 활용되어지며, 이외의 새로운 매체와 기술은 향후 연구에 과제로써 지속적인 관찰과 재실험이 요구된다〔8〕.

III. 침입 방어 기법과 물리적인 로드밸런싱을 이용한 통신매체 다중화 방어기법 제안

현재 통신 사업자들이 제공하고 지원 가능한 무선 또는 유선 통신매체를 확인하고 물리적인 로드밸런싱 기반을 이용해서 침해 발생 시 다중화 된 매체 중 무작위로 적정한 통신 매체를 선정, 운영함으로써 첫 번째 단계에서는 외부로부터 접근하는 경로를 변경하는 과정을 처리한다.

두 번째 단계에서는 통신매체의 변경에 따른 네트워크 IP 대역 역시 서비스를 제공하는 서버 또는 보안 제반기기가 일시에 변경되는 과정이 이루어져야 한다.

다만, 무선 통신매체에 대해서는 향후 논문의 확대 연구 시에 다룰 것이며, 유선의 경우 물리적인 전환 시에 얼마나 빠른 전환과 끊어짐이 없는 서비스가 지속되는가를 본 논문연구에서 실험하고 다중화 통신 매체의 구성을 연구해야 할 부분이다. 따라서 기존에 물리적으로 침해공격을 차단 가능했던 방어기법 3가지와 본 논문에서 제안하는 기법을 순차적으로 기술한다.

첫 번째. 제안하는 기법은 사설 IP 대역을 운영함으로써 집적적인 서비스 서버에 대한 정보유출 등에 대한 공격 차단, 두 번째. 제안하는 기법은 동일한 게이트웨이 또는 디폴트 게이트웨이를 하단의 네트워크를 사설 IP로 Sub-netting함으로써 공격 차단, 세 번째. 디폴트 게이트웨이를 이용한 차단, 마지막으로 순차적으로 제안하고 각 기법에서 발생하는 문제점을 최종 해결하는 기법 순으로 제안한다.

따라서 기존의 네트워크가 가진 문제점까지도 분석하고 방어기법을 적용함으로써 2차, 3차 발생 가능한 문제점을 사전에 제거했다.

3.1 동일 네트워크 내에서 사설 IP 대역 운영을 통한 공격 방어

현재 보안시장에서 보편적으로 공중망에서 일반인이 직접 운영하는 블로그(Blog) 등의 서비스에 사용가능한 장비로 공유기(IP Sharing)가 쓰이고 있다.

공유기의 경우는 과거 통신 매체의 대역폭을 동시에 여러 대의 시스템이 이용할 수 있도록 구성하는 네트워크 기기에서 향후 대역폭을 다수의 시스템이 로드밸런싱을 통해서 대역폭을 상호 균등 분할하여, 사용하는 장비로 거듭 개발되어 졌다.

하지만, 지금은 보안 정책과 다양한 방어 솔루션과 방어기법까지도 탑재하고 지원하는 장비로 부각되어 졌다.

따라서 〔표 5〕와 같이 사설 IP를 구성하고 사용하면, 1차적으로 서비스를 제공하는 시스템에 불법적인 침해가 불가능하다는 논리를 정당한 방어 전략으로 기획하고 기법으로 구성하는 경우도 종종 발생한다. 그러나 사설 IP 대역을 운영하는 경우 역시 집적적인 서비스 서버에 대한 정보유출 등의 공격은 차단이 가능하지만, 단일 통신 매체를 이용한 대역폭 부하와 서비스 자원을 고갈시키는 공격이 가능하다.

서비스 자원과 대역폭 자원을 고갈시킴으로써 사설 IP 대역 방어기법 역시 통신 매체를 이용한 공격방어 기법으로는 적정하지 않다.

〔표 5〕 네트워크 사설 IP 대역 구성(사설 IP 대역에 대한 네트워크 분리를 위한 Sub-netting 구성도)

사설 IP 대역 Sub-netting 구성					
대상	192.168.60.0/24〔192.168.60.0/255.255.255.0〕				
Host 수	30				
Sub-netting 구성	11111111	11111111	11111111	111	00000
	255	255	255	Network Address	Host Address
세부 Sub-netting 주소(IP 영역) 구분	11000010	10101010	00111100	000	00000
	192.168.60.000 / 00000 =〉 192.168.60.0~192.168.60.31				
	11000010	10101010	00111100	001	00000
	192.168.60.001 / 00000 =〉 192.168.60.32~192.168.60.63				
	11000010	10101010	00111100	010	00000
	192.168.60.010 / 00000 =〉 192.168.60.64~192.168.60.95				
	11000010	10101010	00111100	011	00000
	192.168.60.011 / 00000 =〉 192.168.60.96~192.168.60.127				
	11000010	10101010	00111100	100	00000
	192.168.60.100 / 00000 =〉 192.168.60.128~192.168.60.159				
	11000010	10101010	00111100	101	00000
	192.168.60.101 / 00000 =〉 192.168.60.160~192.168.60.191				
	11000010	10101010	00111100	110	00000
	192.168.60.110 / 00000 =〉 192.168.60.192~192.168.60.223				
	11000010	10101010	00111100	111	00000
	192.168.60.111 / 00000 =〉 192.168.60.224~192.168.60.255				

3.2 동일 네트워크 내에서 Sub-netting을 통한 공격 방어

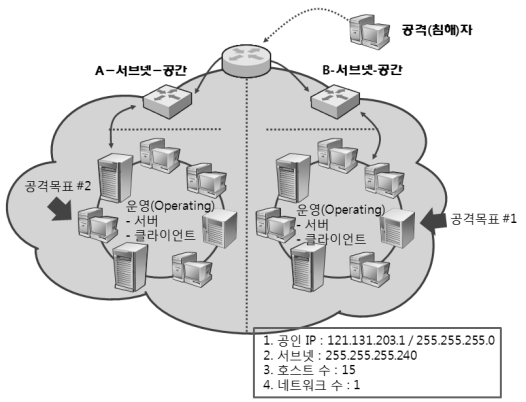
다소 네트워크 관리자가 외부로부터 접근하는 제 3자가 서비스 침해를 발생코자 불법 접근 하는 기법을 방어하는 기획과 기법 상에 손쉽게 실수하기 쉬운 방어기법이다.

이는 동일한 게이트웨이 또는 디폴트 게이트웨이를 상단 네트워크에 두고 하단의 네트워크만을 〔그림 1〕과 같이 네트워크를 2개로 Sub-netting한 네트워크 대역이 192.168.60.128로부터 192.168.60.159 까지 구성되어 있는 경우 동일한 네트워크 대역 상에 존재하는 192.168.60.130 시스템이 공격을 당하고 있다면, 해당 네트워크 IP 대역 이외의 Sub-netting 된 네트워크의 서비스 서버는 방어기법을 적용하지 않아도 된다는 실수를 한다.

하지만 동일한 게이트웨이 및 디폴트 게이트웨이를 망의 상단에 두고 외부로부터 접근 경로를 구성한다는 의미는 단일 통신 매체를 사용한다는 것으로 해당 네트워크 내의 한 대의 시스템이 집중적으로 공격을 당한다면, 전체 통신 매체의 대역폭을 전부 소비한다는 의미이다. 따라서 해당 네트워크 전체가 서비스 불가 상태에 빠진다.

** 국제 공인 IP 대역을 Sub-netting 하는 경우의 경우는 공인 IP가 이미 다수의 특정 회사 등에 배포 운영됨에 따라 사설 IP로 예를 들어 구성 및 기술했다.*

동일 네트워크 내에서 Sub-netting을 통한 공격 방어 역시 공격에 따른 침해 정도는 서비스 제공이 차단되는 수준이며, 특정 서비스의 정보를 침해당하는 치명적인 장애는 일부 차단이 가능하다.



〔그림 1〕 동일한 네트워크에서 Sub-netting을 통한 공격 방어

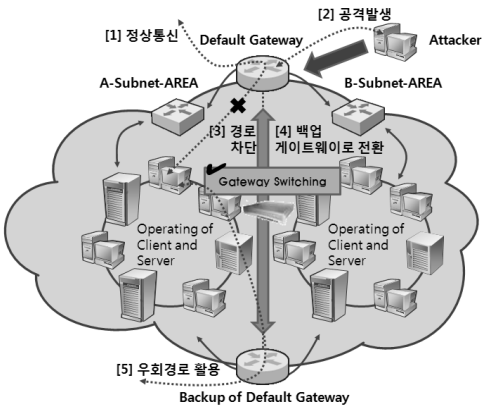
* *동일 네트워크 내에서의 사설 IP 대역운영시의 침해 종류*
  - *단일 게이트웨이에 대한 Ping of Death 공격*
  - *디폴트 게이트웨이에 대한 Redirect of Broadcast 공격*
  - *동일 게이트웨이 하단에 존재하는 시스템을 이용한 서비스 서버 접근시의 TCP/IP Protocol의 3-way Hand sharking 기법을 이용한 Land 공격*
  - *이외의 TCP/IP Protocol 기반의 대역폭과 자원 고갈 공격*

3.3 동일한 디폴트 게이트웨이를 이용한 공격 방어

사설 IP 대역을 이용한 방어와 IP 대역을 Subnetting으로 네트워크를 분리해서 방어하는 기법은 서비스 자원과 통신 매체의 자원 고갈을 목적으로 하는 공격에 대한 방어기법으로는 적정하지 않음을 확인했다. 따라서 앞선 방어기법의 문제점을 보완한 동일한 디폴트 게이트웨이를 이용한 방어와 공격을 〔그림 2〕와 같이 확인한다.

디폴트 게이트웨이를 통신 트래픽 량과 접근 공격의 성격 및 성향, 서비스 서버별로 상호 다른 네트워크 IP 대역과 상호 로드밸런싱이 가능한 별개의 통신사를 두고 2개로 네트워크를 구성함으로써 상호 유기적인 접근 정보에 따라 네트워크 영역과 IP 대역을 교차할 수 있는 형태로 구성한다.

2개의 디폴트 게이트웨이를 구성함으로써 이루어지는 운영절차를 별도로 표기한다.



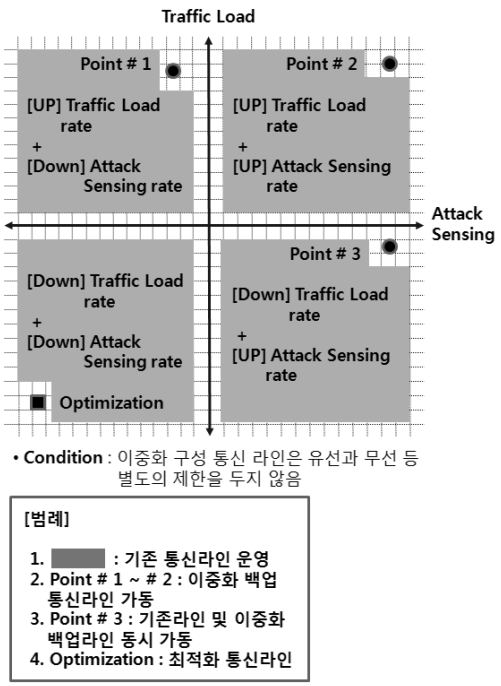
〔그림 2〕 이원화 게이트웨이를 이용한 공격방어

* *Default Gateway 운영절차*
  〔1〕 정상통신 - Default Gateway〔ON〕 / Backup Default Gateway〔OFF〕
  〔2〕 공격발생 - Default Gateway〔ON〕 / Backup Default Gateway〔OFF〕
  〔3〕 경로차단 - Default Gateway〔OFF〕
  〔4〕 백업 게이트웨이로 전환 - Backup Default Gateway〔ON〕
  〔5〕 우회경로 활용 - Backup Default Gateway〔ON〕

3.4 물리적 로드밸런싱 Agent를 이용한 통신라인 다중화 기반의 공격 방어

다양한 물리적 통신 매체를 이용한 공격에 대한 방어기법을 살펴보았으며, 본 논문에서 제안하는 로드밸런싱 Agent를 이용한 방어기법은 〔그림 3〕과 같은 Traffic과 Attack 감지 비율에 따른 다중화 통신라인 로드밸런싱 프로세서를 통한 방어를 기준으로 한다.

4가지 영역을 두고 Traffic Load 및 Attack Sensing의 두 가지 평가지표를 운영함으로써 공격에 따른 통신라인의 전환을 위한 기준척도로 활용함으로



〔그림 3〕 Traffic과 Attack 감지 비율에 따른 다중화 통신라인 로드밸런싱 프로세서를 통한 방어

써 최적의 다중화 통신 매체를 선정하고 상호 부하 량을 최소화하는 비율을 구한다.

본 논문에서 물리적인 통신 매체를 로드밸런싱 하는 부분에 대한 알고리즘을 구성하고 해당 알고리즘에 의한 빠르고 신속한 라인 전환과 공격성 접근임을 확인하는 과정이 이루어진다. 각 실험을 통한 세부 영역을 4개로 구성하고 최종 통신 매체 전환과 IP 대역 재구성 효율성을 확인한다.

Load-Balancing Processor Flow
Define=Traffic_Load_Value, Attack_Sensing_Value

Traffic_Load_Value_Routine={UP} .and. {DOWN} Ejection
{ rate={UP}
Branch=Area_01_module .and. Area_02_module
else brance=Area_03_module .and. Area_04_module
Select Area_01_module .or. Area_02_module
Processing Load-Balancing Processor
~ }

Attack_Sensing_Value_Routine={UP} .and. {DOWN} Ejection
{ rate={UP}
Branch=Area_02_module .and. Area_04_module
else brance=Area_01_module .and. Area_03_module
Select Area_02_module .or. Area_04_module
Processing Load-Balancing Processor
~ }

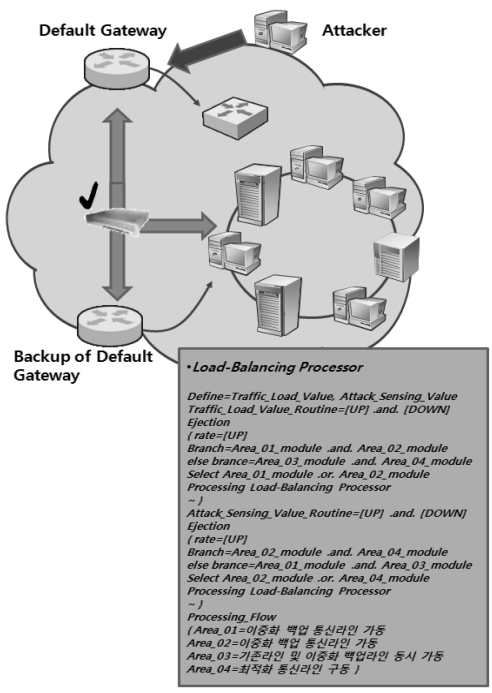
Processing_Flow
{ Area_01=다중화 백업 통신라인 가동
Area_02=다중화 백업 통신라인 가동
Area_03=기존라인 및 다중화 백업라인 동시 가동
Area_04=최적화 통신라인 구동 }

최종적으로 제안하는 방어기법에서 제안하는 부분은 다양한 유무선 통신 매체를 통신사별 운영하고 구현하는 통신방식에 따라 공격성 접근 시 난수에 의한 통신 매체 전환을 1차적으로 구성하고 2차적으로는 전환된 네트워크에서 운영하는 네트워크 IP 대역으로 변환이 필요하다.

IV. 공격에 대한 방어 실험

4.1. 제안환경 및 실험

공격을 시행하는 Attack 시스템은 동일 네트워크에 존재하지 않는 시스템을 구현한다. 공격 시스템의 운영체제는 Ping of Death와 서비스 접근 부하 량을 확인하기 위한 접속 Session 모듈을 이용한 개발 도구 탑재가 용이한 Cent-OS로 구성한다. 또한 공격 도구는 첫 번째로 Ping of Death 공격을 Ethernet에서 운영하는 Packet 최대 크기의 MTU(Maximum Transfer Unit) 사이즈인 1,500Byte 크기로 실시간 지속적인 단일 서비스 하에서 공격 또는 다양한 서비스 하에서 공격을 〔그림 4〕와 같이 시행한다. 두 번째로는 TCP 기반 하에서 서비스에 접속하는 Session 부하 량을 측정한다. 단순 트래픽 부하를 발생시킴으로써 공격에 따른 방어기법의 적정성 확인보다는 물리적인 로드밸런싱에 의한 통신 매체의 효율적인 전환이 이루어지고 트래픽 부하가 조정되어 빠른 전환이 이루어짐을 확인한다. 추가적으로 단일 통신 매체와 다수의 통신 매체를 접목함으로써 트래픽 부하량을 측정하는 부분까지 확인함으로써 기본 통신 매체



〔그림 4〕 제안 및 실험환경

〔표 6〕 집중화 공격 가능 비율에 따른 단일 통신라인과 다중화 통신라인의 추론성능 비교

구분	단계	Traffic Load Rate 〔unit : session〕	Attack Sensing Rate 〔unit : Sniffer Detection / tool : Ping, ARP, DNS, Decoy, ARP Watch〕	Prediction
단일 통신라인	1	1,500,000~1,700,000	5~45%	〔추론〕 접속 session 1,900,000 이상 및 86% 이상의 2단계 공격 시 치명적인 서비스 장애 발생
	2	1,800,000~1,900,000	46~86%	
	3	over 2,000,000	over 87%	
이중화 통신라인	1	1,500,000~1,700,000	5~45%	〔추론〕 접속 session 2,000,000 이상 및 87% 이상의 3단계 공격 시 지속적인 서비스 지원 가능
	2	1,800,000~1,900,000	46~86%	
	3	over 2,000,000	over 87%	

를 이용할 때 제안된 기법과의 객관적인 비교평가를 확인한다.

4.2. 트래픽 부하 량에 대한 집중화 공격

특정 실험을 위한 서비스 지원함에 있어서 불법적인 접근 방법을 통한 트래픽 부하 량을 session 접속 단위로 구성한다.

또한, 추측이론을 통해서 단일 통신라인의 경우는 가상의 추론을 접속 session 1,900,000 이상 및 86% 이상의 2단계 공격으로 구성하고 이중화 통신라인의 경우는 접속 session 2,000,000 이상 및 87% 이상의 3단계 공격으로 구성해서 실험을 측정한다. 이때 유의해야 하는 부분은 TCP 기반으로 실험 범위를 제한하고 측정함으로써 실험의 범위가 축소되는 반면, 정확한 트래픽 부하 량에 따른 〔표 6〕과 같은 추론성능 비교표가 도출된다.

4.3. 공격에 대한 방어 솔루션과 제안 알고리즘

본 논문에서 제안하는 물리적 로드밸런싱 Agent를 이용한 통신라인 다중화 기반에서 공격에 대한 방어기법의 원활한 처리결과를 위해 첫 번째 각 영역별 트래픽 부하 량과 공격감지 센서를 통한 최적화 통신 매체 구성 부분을 확인한다. 또한 Area_01과 Area_02, Wireless module 알고리즘을 생성하고 적용한다.

```
* Area_01, 02=이중화 백업 통신라인 가동
  START
     RUN=community_line_select
     Line= {wire, wireless }
     Detail_line_= {ethernet(general, fast,
     giga), FDD I, Token ring)}
      Select= {line || detail_line }
      Operation_line="select"
      Breakup=traffic_rate .and. attack_rate
   END

* Wireless module
  START
     RUN=community_line_select
     Line= {wire, wireless }
     Detail_line_= {WCDMA, WIBRO, WiFi,
     LTE, HSPA+, WiMAX, HSDPA}
     Select= {line || detail_line }
     Operation_line="select"
     Breakup=traffic_rate .and. attack_rate
    END
```

다음으로는 Area_03의 기존라인 및 이중화 또는 다중화 백업 통신 매체를 동시 가동할 경우와 Area_04의 최적화 통신라인 비율을 보인 알고리즘을 기술했다.

〔표 7〕 제안 및 실험결과에 따른 Traffic load rate와 Attack sensing rate 분류 기준 표

구분	Traffic Load Rate 〔unit : session〕		Attack Sensing Rate 〔unit : Sniffer Detection / tool : Ping, ARP, DNS, Decoy, ARP Watch〕	
1	A	1,500,000~1,700,000	A′	5~45%
2	B	1,800,000~1,900,000	B′	46~86%
3	C	over 2,000,000	C′	over 87%

〔표 8〕 제안 및 실험결과에 따른 최종 통신라인 선정 분석결과

구분		Ethernet	Fast Ethernet	Giga Ethernet				ATM Lan	FDDI	Token Ring
				CX	LX	SX	TX			
Ethernet		A/A',B'	A/A',B'	A/A',B',C'				A/A',B',C'	A/A',B',C'	A/A',B'
Fast Ethernet		B/A',B'	B/A',B'	C/A',B',C'				C/A',B',C'	C/A',B',C'	B/A',B'
Giga Ethernet	CX	B/A',B',C'	B/A',B',C'	C/A',B',C'				B/A',B',C'	C/A',B',C'	B/A',B',C'
	LX									
	SX									
	TX									
ATM Lan		A/A',B',C'	C/A',B',C'	C/A',B',C'				C/A',B',C'	C/A',B',C'	B/A',B',C'
FDDI		A/A',B',C'	B/A',B',C'	C/A',B',C'				C/A',B',C'	C/A',B',C'	B/A',B',C'
Token Ring		A/A',B'	B/A',B',C	B/A',B',C				B/A',B',C	B/A',B',C	B/A',B',C'

** Area_03=기존라인 및 이중화 백업라인 동시 가동*
START
RUN=community_line_select .and. present_line
Line= {wire, wireless }
Detail_line_= {ethernet(general, fast, giga), FDD I, Token ring}
Select= {line || detail_line }
Operation_line="select"
Breakup=traffic_rate .and. attack_rate
END

** Area_04=최적화 통신라인 구동*
START
RUN=Optimization_line
Line= {wire, wireless }
Detail_line_= {ethernet(general, fast, giga), FDD I, Token ring}
Select= {line || detail_line }
Operation_line="select"
Breakup=traffic_rate .and. attack_rate
END

각각의 영역별 트래픽 부하 량과 불법접근 센서를 가동한 비율을 확인한 결과 Area_03 영역이 가장 최적의 통신 매체 전환과 네트워크 영역 변환을 통한 방어기법을 적용하기 가장 좋은 비율을 보였다.

4.4. 공격에 대한 결과 분석

최종 실험결과에 따른 공격분석을 확인함에 있어서 〔표 7〕과 같은 제안 및 실험결과에 따른 Traffic load rate와 Attack sensing rate 분류 기준 표에 의한 비율을 확인하고 각 비율을 Area_01, 02, 03, 04에 접목함으로써 다중화를 위한 가장 신속하고 차단비율이 높은 통신 매체의 조합이 가능하다.

통신 매체별 다중화 구현을 통한 물리적인 1차 방어기법과 로드밸런싱 기법을 동시적용 하는 경우의 최적화 통신 매체 조합구성을 위한 결과가 〔표 8〕과 같이 도출됐다.

해당 표에 기반 한 예를 분석해보면, 이중화 통신 매체를 Ethernet과 Giga Ethernet으로 구성 시에는 B/A',B',C'라는 결과가 나오며, B는 분류 기준표에 의해 Traffic Load 비율에 있어서는 1,800,000~1,900,000개의 접속 session에 대한 접근 시에 장애를 감안하고 전환에 따른 방어기법을 적용 시 서비스가 지속적으로 지원 가능하며, 또한 Attack Sensing 비율은 5에서 87% 이상까지도 접목이 가능함을 의미한다.

또한 네트워크 보안 및 접근 통신선로의 다중화 또는 이원화 기법과 솔루션을 실무에서 운영 가능하지만, 다소 선정되어지는 통신선로의 실험 대상에 대한 범주가 폭넓지 못하다. 하지만, 상호 서로 다른 ISP(Internet Service Provider)가 지원하는 일반적인 고유 통신선로를 대상으로 한 간단한 실험 결과 또한 본 결과분석과 비례한 현상과 결과를 도출함으로써 결과에 대한 객관성을 증명했다.

물론 가장 중요한 통신사에서 제공하는 통신 매체에 대한 최고의 성능을 두고 실험한 사항이 아니므로 오차가 발생 가능하다. 이 부분은 향후 논문 연구에서 각 통신사간의 정보공유를 통한 기술점목이 요구되어진다.

V. 결론

본 논문에서는 다양한 통신사업자가 제공하는 통신 매체를 물리적으로 다중화 라인으로 구성하고 제공하는 서비스의 대역폭 부하 량을 로드밸런싱을 통해서 분할하고 전환함으로써 지속적인 서비스 제공이 이루어지도록 하는 방어기법을 제안하고 있다.

첫 번째 제안하고 실험한 결과로는 다중화 통신 매체를 공격과 동시에 물리적인 매체의 전환이 어느 정도 빠르게 전환되느냐에 대한 내용이며, 둘째는 전환됨과 동시에 전환된 통신 매체에 부여되어진 네트워크 IP 대역으로 공격을 당하고 있는 네트워크 하단의 시스템들이 가진 네트워크 정보가 어느 정도 빠르게 변환되느냐를 확인하는 것이다. 마지막으로 앞선 2가지 조건이 만족함과 동시에 가장 최적의 로드밸런싱이 가능한 통신 매체의 조합을 확인하는 것이다. 최종 실험하고 제안되어진 방어기법 상에서는 최적의 전환과 변환 통신 매체의 조합을 제시하였다.

향후 연구방향으로는 각각의 통신 사업자들이 자신만의 통신 매체를 활용하고 있으며, 전환의 원활한 핵심 기술에 대해서는 상호 정보를 제공하지 않고 있기 때문에 지속적인 상호 정보공유와 논의가 필요한 사회적인 문제점이 존재한다. 또한 물리적인 1차 방어기법의 경우는 통신 매체를 이중화 또는 다중화 함으로써 통신비용의 증가가 예상되어진다. 따라서 지속적인 제안기법의 연구뿐만 아니라 통신사업자간의 상호 정보교류에 대한 정보의 확장성이 요구되어진다.

참고문헌

〔1〕 문화일보, http://www.munhwa.com/news/view.html?no=2011050401070427128002, "檢, 기관망 파괴 악성코드 '스턱스넷' 경계령", 김백기 기자, 2011년 5월 4일.

〔2〕 곽미숙, 김아빈, 김윤희, 한국정보기술학회, "통합적인 악성코드 수집 및 모니터링 시스템의 설계 및 구현", v.8 no.2, pp.117-125, 2010년 2월.

〔3〕 인터넷침해대응센터, "인터넷 침해사고 동향 및 분석 월보", 2011년 06월호, pp.6, 2011년 06월.

〔4〕 하현태, 이해동, 백현철, 김상복, 한국해양정보통신학회논문지, "엔터프라이즈 네트워크에서 DDoS 공격의 부하 개선을 위한 큐잉 모델",v.15 no.1, pp.107-114, 2011년 1월.

〔5〕 전정훈, 한국통신학회논문지, "내부 네트워크의 성능저하요인에 관한 연구",v.36 no.1, pp.43-50, 2011년 1월.

〔6〕 오정숙, 정보통신정책연구원, "국내외 네트워크 장비 시장 현황 및 시사점", 방속통신정책 제23권 9호 통권 508호, pp.35-52, 2011년 5월 16일.

〔7〕 오남석, 한영순, 엄찬왕, 오경석, 이봉규, 한국전자거래학회지, "정보보호 수준평가 방법 개선에 관한 연구", v.16 no.2, pp.159-169, 2011년 5월.

〔8〕 고웅, 이동범, 곽진, 정보보호학회논문지, "국내 정보보호 제품 평가 서비스 간소화 방안", v.19 no.2, pp.141-153, 2009년 4월.

〈著者紹介〉

최 희 식 (Hee-sik Choi) 정회원
2006년 2월: 숭실대학교 컴퓨터공학(공학석사)
2007년 3월: 숭실대학교 전자계산원 출강
2007년 3월: 삼육대학교 출강
2008년 3월: 경원대학교 출강
2006년 3월 ~ 현재: 숭실대학교 일반대학원 컴퓨터학과 박사과정
〈관심분야〉 DRM, 유비쿼터스, RFID & VoIP, SNS보안, 인터넷 보안

서 우 석 (Woo-seok Seo) 종신회원
2006년: 숭실대학교 정보과학대학원 정보통신융합학과 석사
2009년 9월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 방화벽, Router & Network Design

전 문 석 (Moon-seog Jun) 종신회원
1981년 2월: 숭실대학교 전자계산학과 졸업
1986년 2월: University of Maryland Computer Science 석사
1989년 2월: University of Maryland Computer Science 박사
1986년 9월~1989년 12월: University of Mary 강사
1989년 3월~7월: Morgan State University 조교수
1989년 9월~1991년 2월: New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재: 숭실대학교 정교수
〈관심분야〉 정보보호, 네트워크 보안, 전자여권, 암호학