□ 研 究 論 文 □

情韓國國防經營分析學會誌
第33卷 第2號, 2007. 12. 31.

시뮬레이션 기반 육군전술지휘정보체계에 대한 웜 피해평가

(Simulation-based Worm Damage Assessment on ATCIS)

김 기 환(Gi-Hwan Kim)*, 김 완 주(Wan-Joo Kim)**, 이 수 진(Soo-Jin Lee)***

초 록

육군은 실시간으로 지휘통제 정보를 공유하는 전장정보체계의 구성을 위해 육군전술지휘정보체계(ATCIS : Army Tactical Command Information System)를 개발 하였다. 이러한 ATCIS 체계는 공개키 및 암호화 장비를 이용하여 무결성, 비밀성은 충분히 충족시키지만, zero day attack을 이용한 새로운 방법의 DDoS(Distributed Denial of Service)공격 등 가용성에 대해서는 무결성, 비밀성만큼의 안전성이 확보되지 못한 실정이다. 따라서 본 논문에서는 네트워크 시뮬레이터인 NS-2[3]에서 제공하는 DN-AN 모델을 이용하여 웜 피해평가를 위한 시뮬레이션를 구현하였다. 또한, 도출된 결과를 통해 ATCIS에서의 웜 취약점을 분석하고, 대응방안을 제안한다.

ABSTRACT

The army developed the ATCIS(Army Tactical Command Information System) for the battlefield information system with share the command control information through the realtime. The using the public key and the encryption equipment in the ATCIS is enough to the confidentiality, integrity. but, it is vulnerable about the availability with the zero day attack. In this paper, we implement the worm propagation simulation on the ATCIS infrastructure through the modelling on the ATCIS operation environment. We propose the countermeasures based on the results from the simulation.

Keywords : 웜 피해평가(Worm Damage Assessment), 육군전술지휘정보체계(ATCIS : Army Tactical Command Information System)

* 국방대학교 전산정보학과 석사과정

** 국방대학교 전산정보학과 석사과정

*** 국방대학교 전산정보학과 교수, 공학박사

1. 서 론

2003년 1월 25일 발생한 1·25대란은 인터넷 서비스 마비로 인터넷을 사용하는 국내의 모든 공공기관이나 기업뿐만 아니라 대다수 국민들이 불편을 겪으면서 해킹이나 바이러스에 대한 관심이 더욱 높아지는 계기가 되었다. 발생 10분만에 취약한 시스템의 90%를 감염 시켰으며 전 세계적으로 최소한 7만 5천대의 시스템이 피해를 입었다. 이 중 미국이 전체 42.87%로 1위, 한국이 그 다음으로 11.82%의 피해를 입었으며, 대량으로 발생된 트래픽을 그 주된 원인으로 보고 있다.[1]

현대 전장상황은 기반통신체계를 활용하여 정확한 전장정보의 전송 및 공유로 통합전투수행을 통한 효과적인 군사작전 수행이 핵심요소로 대두되고 있다. 따라서 육군은 실시간으로 지휘통제 정보를 공유하는 전장정보체계의 구성을 위해 육군전술지휘정보체계(ATCIS : Army Tactical Command Information System)를 개발완료 하였고, 현재는 각 부대로 전력화를 진행하고 있다. 이러한 ATCIS 체계는 공개키 및 암호화 장비를 이용하여 무결성, 비밀성은 충분히 충족시키지만, zero day attack을 이용한 새로운 방법의 DDoS 공격 등 가용성에 대해서는 무결성, 비밀성만큼의 안전성이 확보되지 못한 실정이다.[2] 또한 ATCIS 체계는 특수한 네트워크 형태로 대다수 동일한 사양의 PC가 운용된다. 이러한 특징은 ATCIS 체계에서 다양한 zero day attack 취약성을 발생시키지만 이에 대한 연구는 부족한 실정이다.

따라서 본 논문에서는 SI(Susceptible Infection) 웜 전파 모델 기반에서 네트워크 시뮬레이터인 NS-2[3]에서 제공하는 DN-AN(detailed network-abstract network) 모델을 이용하여 ATCIS 환경을 최대한 유사하게 묘사하여 웜 피해평가를 위한 시뮬레이션를 구현하고, 도출된 결과를 통해 ATCIS에서의 웜 취약점을 분석한다.

논문의 구성은 제 2장에서 웜 전파 모델에 대해 분석해 보고, 제 3장에서는 기존 DN-AN 모델의 문제점 도출, 시뮬레이션을 위한 ATCIS 환경 모델링을 통해 시뮬레이션을 구현한다. 4장에서는 도출된 결과를 이용하여 ATCIS에서의 웜 취약점을 분석하고, 5장에서 결론을 맺는다.

2. 관련연구

2.1 웜 및 웜 전파모델

웜은 자기복제 및 전파과정이 생물학적인 바이러스와 유사하여 기존의 전염병 모델을 적용할 수 있으며 이러한 전염병 모델을 기반으로 한 수학적 웜 전파 모델에 관한 연구가 활발히 진행 중에 있다.[4-6]

2.1.1 웜

웜은 1998년 MorrisWorm에서 시작하여 인터넷에 연결된 수많은 취약한 시스템을 공격하여 자기 자신을 복제하면서 전파되었다. Recent Worms : A Survey and Trends[7]에서는 "A worm is malicious code (standalone or file-infecting) that propagates over a network, with or without human assistance"로 정의하고 있으며 바이러스와의 차이점은 바이러스는 사용자가 자신을 의심하지 않고 실행하는데 중점을 두지만, 웜은 사용자의 도움 없이 시스템에서 다른 시스템으로 전파된다.

이 중 슬래머 웜은 2003년 1월 25일 인터넷 대란의 원인으로 인터넷데이터분석협력협회(Cooperative Association for Internet Data Analysis : CAIDA)에서 2003년 1월 27일 발표한 보고서에 따르면 마이크로소프트 SQL 2000 서버가 지닌 확인서비스(Resolution Service)의 취약점을 UDP 1434 port를 이용하여 버퍼 오버플로

우라는 해킹기법으로 시스템을 감염시킨 후 또 다른 시스템을 찾아서 전파한다. 작동원리는 다음과 같다.

① SQL 서버 1434/UDP로 접속
② SQL 서버의 확인서비스 취약점을 이용하여 버퍼 오버플로우 공격을 시도
③ 웜 코드를 메모리에 삽입 후 자동으로 실행
④ SQL 서버가 확인서비스에 대한 보안 패치가 적용되지 않은 경우, 혹은 서비스팩 3이 설치되지 않았을 경우에는 감염
⑤ 감염된 서버는 IP 주소를 무작위로 생성한 이후 ①~ ③과정을 자동 반복

2.1.2 웜 전파모델[8]

2.1.2.1 SI 모델

SI(Susceptible Infection)은 가장 일반적인 전염병 모델로써 고전적으로 사용하던 단순한 전염병 모델에 의거, 고정된 노드의 총 대수 N에 대하여 감염가능성이 높은 취약한 노드의 수 $S(t)$는 이미 감염된 노드의 수 $I(t)$에 대하여 $S(t) = N - I(t)$로 기술된다. 여기서 감염된 노드는 복구되지 않거나 폐기되는 것으로 가정한다. 이러한 고전적인 단순 전염병 모델에서 한정된 노드 수에 대하여 감염비율 β를 고려하면 감염 노드 수의 증분은 다음과 같이 기술될 수 있다.

$$\frac{dI(t)}{dt} = \beta I(t) S(t) \qquad (1)$$

즉, 식(1)은 시간에 따라 감염 노드의 증분은 감염비율 β, 시간 t에서 감염 노드 수 $I(t)$와 남아있는 감염 가능한 노드 수 $S(t)$에 비례하는 것을 의미한다.

2.1.2.2 SIR 모델

SIR(Susceptible Infectious Removed) 모델은 일반적인 SI모델을 확장하여 감염된 노드에 대한 보안패치 작업에 의해 복구되는 노드의 수를 고려하였다. 즉, 감염 가능성이 높은 취약한 노드의 수 $S(t)$, 감염된 노드의 수 $I(t)$, 여기에 복구된 노드의 수 $R(t)$와 복구비율 γ를 추가로 고려한다. 따라서 식(2)에서 보는 바와 같이 감염 노드 수의 증분은 SI모델에 비하여 복구되는 노드의 증분만큼 감소된다. 고정된 노드의 총 대수 N에 대하여 감염가능성이 높은 노드의 수 $S(t)$, 감염된 노드의 수 $I(t)$, 복구된 노드의 수 $R(t)$는 $S(t)+I(t)+R(t)=N$으로 기술된다.

$$\frac{dI(t)}{dt} = \beta I(t) S(t) - \frac{dR(t)}{dt} \qquad (2)$$

$$\frac{dR(t)}{dt} = \gamma I(t) \qquad (3)$$

2.1.2.3 IWMM

IWMM(Improved Worm Mitigation Model)에서는 SI 및 SIR모델에 비하여 실제 인터넷 환경에서는 추가적으로 다음 사항을 고려한다.

○ 인간의 대응에 의하여 감염되었거나 감염될 위험에 있는 취약한 노드를 동시에 복구 또는 예방한다.
○ 감염비율 β는 대용량 스캔 트래픽 발생에 따른 통신망 내부 라우터나 링크의 용량제한으로 인해 감속된다.

이러한 2가지 요소를 고려하여 제시된 새로운 모델에서는 기존의 고정된 감염비율 β 대신에 시간에 따른 변수값인 $\beta(t)$를 사용한다. 또한 시간 t에서 인간의 대응에 의하여 감염된 노드 $I(t)$를 복구한 수 $R(t)$뿐만 아니라 감염될 위험에 있는 취약한 노드 $S(t)$에 대하여 예방 조치한 노드 수 $U(t)$와 복구비율 μ 를 추가로 고려하며 고정된 노드의 총 대수 N에 대하여 $S(t)+I(t)+R(t)+U(t)=N$으로 기술된다.

$$\frac{dI(t)}{dt} = \beta(t)\, I(t)\, S(t) - \frac{dR(t)}{dt} - \frac{dU(t)}{dt} \quad (4)$$

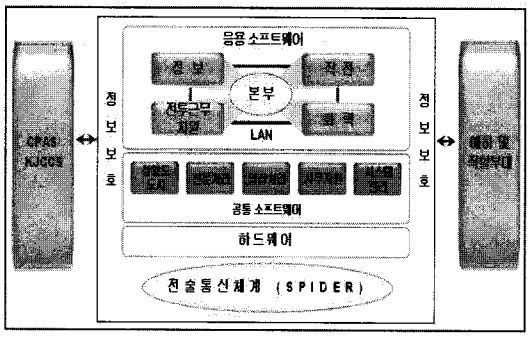
$$\frac{dR(t)}{dt} = \gamma I(t) \quad (5)$$

$$\frac{dU(t)}{dt} = \mu S(t) \quad (6)$$

2.2 ATCIS

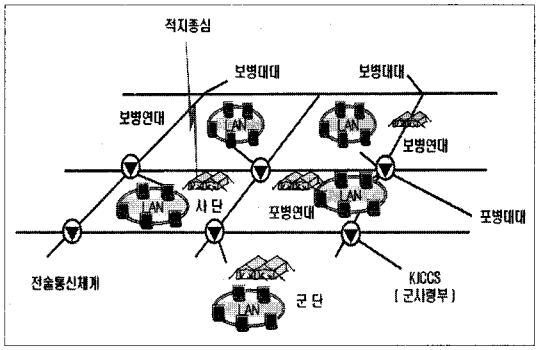
육군의 C4I체계는 지휘·통제·통신·컴퓨터의 유기적인 통합을 통해 효율적인 전장감시로부터 지휘결심, 효과적인 작전수행(타격)을 보장하는데 있으며 '96년 4월 개념연구를 시작으로 '05년 7월 국방부에서 전투용 사용 "가" 판정을 획득함으로써 현재 전방군단에 전력화가 진행되고 있다.

ATCIS의 주요기능은 정보·작전·화력·전투근무지원·공통분야로 나누어지며 구성품은 개발소프트웨어, 하드웨어, 보안장비 등을 포함하여 총 56종 7,000점이 있다. 구성은 <그림 1>과 같다.



〈그림 1〉 ATCIS 구성도

육군은 ATCIS를 군단에서 연대간 통합전투수행을 위한 지휘통제수단으로 활용하여 상·하제대 및 각 기능실별 주요정보를 실시간 공유함으로써 지휘관의 신속한 상황파악 및 판단, 결심에 주요한 역할을 수행 할 것으로 예상된다. 또한 핵심감시자산과 타격체계를 연동하여 실시간 타격 지원이 가능하며 전·평시 동일하게 중단 없이 체계의 활용이 가능하며, 전개 시 <그림 2>와 같이 근접노드의 지원을 통해 접속이 이루어진다.



〈그림 2〉 ATCIS 개념

2.3 웜 시뮬레이션 환경

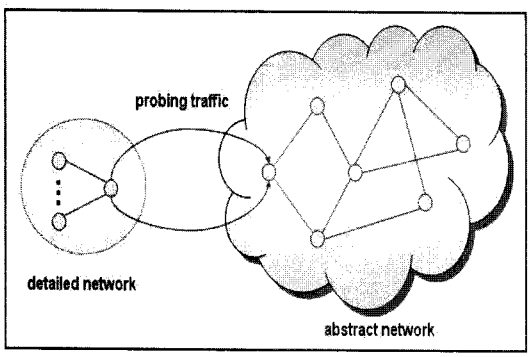
웜의 여러 가지 특성을 파악하는 것은 웜 연구에 있어서 매우 중요한 부분이다. 대규모 네트워크 환경에서의 공격 및 방어의 효과와 반응을 알아보기 위하여 방대한 규모의 인터넷을 실제로 구축하고, 구축된 환경에서 네트워크 공격을 실험하는 것보다 대규모 네트워크를 모델링한 후 다양한 환경에 대하여 시뮬레이션을 수행하는 것이 여러 측면에서 장점을 가지고 있다. 하지만 웜을 실제 환경에서 실험하는 방식은 매우 위험한 일임으로 이에 대한 대안으로 시뮬레이션 환경이 필요하다. 이에 많은 연구들이 제시한 웜에 대한 모델의 검증을 위해 많은 시뮬레이션 환경을 제시하고 이를 이용하고 있다.

2.3.1 NS-2

NS-2(Network Simulator version 2)는 콜롬비아 대학에서 개발한 시뮬레이션 테스트베드인 NEST를 기반으로 UC 버클리(Berkeley)에서 1988년에 개발한 리얼 네트워크 시뮬레이터이다. TCP, UDP, FTP, HTTP 등과 같은 TCP/IP 프로

토콜 패밀리와 라우팅 프로토콜(Routing Protocol), 그리고 멀티캐스팅 프로토콜, RTP, SRN 등과 같은 다양한 인터넷 프로토콜을 시뮬레이션할 수 있다. 그리고 Ad Hoc 네트워크, 이동 통신망의 기지국(Base Station) 모델, WLAN, Mobile-IP 관련 프로토콜, UMTS, 위성 네트워크(Satellite Notwork) 등과 같은 무선 네트워크까지 지원할 수 있는 매우 적용 범위가 넓은 네트워크 시뮬레이터로 웜 시뮬레이션 환경을 위해 DN-AN 모델을 2.27 버전부터 제공하고 있다.

DN-AN 모델은 연결된 노드 간 주고받는 패킷 흐름을 분석할 수 있는 정밀한 웜 시뮬레이션 모델로 <그림 3>에서 보는 바와 같이 크게 DN(detailed network)과 AN(abstract network) 두 가지로 구성된다.



〈그림 3〉 DN-AN 모델

DN은 인터넷서비스제공자에 의해 운영되는 LAN 환경으로 각 노드는 라우터에 연결되며 노드 간 패킷 흐름 분석이 가능하다. AN은 DN 이외의 전체 인터넷 영역을 의미하며 DN과 연결된 노드에서만 패킷을 발생하며 나머지 노드에서는 수학적인 계산에 의해 웜 전파 과정이 발생한다. 기존 DN-AN 모델은 DN에서 발생한 패킷을 필터링 없이 AN IP 대역으로 전송하여 AN의 급격한 감염률 증가로 부정확한 결과를 나타내는 문제점이 있다. 이러한 문제점 해결을 위해 프로그램 내 패킷 필터링 모듈을 추가하였고, <표 1>의 worm.cc, messpass.cc, worm.tcl 파일을 수정하여 시뮬레이션을 구현하였다. 시뮬레이션을 구현함에 있어서는 게이트웨이 역할을 하는 노드 단위로 운영되는 ATCIS의 특성을 고려하여 군단을 DN, 육군전체를 AN으로 모델링하였다.

〈표 1〉 DN-AN 프로그램 구성 모듈

구 분	설 명
worm.cc	웜 어플리케이션 모듈
messpass.cc	패킷 전파 모듈
worm.tcl	웜 시뮬레이션 환경 설정

2.3.2 SSFNet

SSFNet(Scalable Simulation Framework Net)는 프로세스 기반 이산 사건 중심 시뮬레이션 커널(Process-based Discrete Event- oriented Simulation Kernel)이다. 시뮬레이션 커널인 SSF의 소스는 공개되지는 않았으나 그 중에서 네트워크의 시뮬레이션을 지원하는 SSFNet은 라우터, 링크, 네트워크 인터페이스 카드 등 대부분의 인터넷 서브시스템들을 시뮬레이션 하는데 필요한 다양한 객체들이 Java로 구현되어 있어 시뮬레이션 특성에 맞추어 그들의 특성을 변경할 수 있다는 장점이 있다. 또한 SSFNet은 이를 기반으로 상위단계의 10만개 이상의 노드로 구성된 대규모 네트워크까지도 표현하도록 허용하고 있으며, 네트워크상의 실존하는 특정 행동을 따라 구현이 가능하다. 그러나 SSFNet은 네트워크 시뮬레이션의 scalability만을 강조하여 다양한 네트워크 프로토콜이나 시뮬레이션 프로세스간의 데이터의 교환이 어려운 단점이 있다.

2.3.3 NWS

NWS(Network Worm Simulation)웜 코드를 가

상으로 실행 할 수 있는 환경을 제공해 준다. NWS에서 제공해 주는 오브젝트를 기반으로 perl을 사용하며, 웜만을 위한 시뮬레이터이다. 현실 세계에 존재하는 다양한 종류의 웜을 시뮬레이션 할 수 있고, 오브젝트를 이용하여 실세계의 네트워크를 묘사할 수 있다. 또한, perl을 사용함으로써 프로그래밍에 초보자라 할지라도 다른 언어에 비해 다소 쉽게 접할 수 있는 장점이 있는 반면, 프로그래밍 용량이 크며, 디버깅이 어렵다는 단점이 있다.

3. 시뮬레이션을 위한 네트워크 모델

본 장에서는 ATCIS 기반 하 웜 전파 시뮬레이션을 위한 기반체계 구조를 모델링한다. 이를 위해 NS-2에서 제공하는 DN-AN 모델을 수정 후 활용하였으며, 실제 운영 중인 ATCIS 환경을 최대한 DN-AN 모델에 반영하였다.

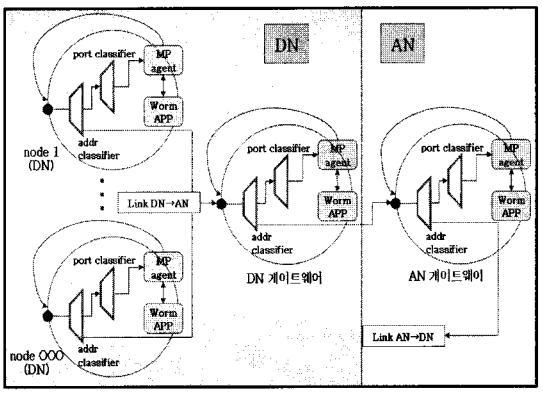
3.1 ATCIS 모델링

네트워크 모델링을 위해서는 노드, 네트워크 구성 등에 대한 정확한 데이터가 필요하며, 이를 위해 실제 운영 중인 ATCIS 환경을 면밀히 분석하였다. 이러한 분석을 통해 도출된 모델링 데이터는 <표 2>과 같다.

〈표 2〉 시뮬레이션 모델링 데이터

구 분		내 용	비 고
전체 IP		4,294,967,296	2^{32}
노드 수	내부(LAN)	OOO대	군단
	외부(WAN)	O,OOO대	육군
노드 분류	서버	O,OOO대	4%
	클라이언트	O,OOO대	96%
대역폭	내부(LAN)	100Mbps	
	외부(WAN)	1Mbps	
지연시간		1ms	

<표 2>에서 도출된 모델링 데이터를 이용하여 구현한 ATCIS 기반 웜 전파 시뮬레이션 구성은 <그림 4>과 같으며, 전술한 바와 같이 DN은 군단 네트워크를, AN은 육군 전체 네트워크를 의미한다.



〈그림 4〉 DN-AN 구성도

3.2 시뮬레이션 환경

시뮬레이션 환경은 가상머신 VMware를 기반으로 Fedora 5.0환경에서 NS-2 2.31 버전을 이용하여 수행하였다.

3.2.1 가정

본 논문에서는 ATCIS 기반 하에서 zero day attack이 가능한 공격용 웜의 출현 시, 그 피해상황을 시뮬레이션 한다.

첫째, 슬래머 웜을 zero day attack이 가능한 공격용 웜으로 가정한다. 따라서 ATCIS에서 운용되는 모든 클라이언트는 공격용 웜에 대한 취약성을 갖고 있으며, 사용되는 백신은 공격용 웜을 차단하지 못하고, 단시간 내 웜을 막을 수 있는 백신을 만들어 치료할 수 없다.

둘째, 배치된 클라이언트는 정보, 작전, 전투근무지원, 화력, 본부의 각 기능별 동일한 사양과 종류의 PC로 구성된다.

3.2.2 시뮬레이션을 위한 웜 전파 모델

웜의 자기복제 및 전파 특성에 따라 전염병 모델의 웜 전파 모델을 적용할 수 있으며, zero day attack이 가능한 웜이 발생했을 경우 단기간에 전파되므로 복구율을 고려하지 않은 SI 모델의 적용이 타당하다. 또한 ATCIS 체계는 특수한 네트워크 형태로 대다수 동일한 사양의 PC와 바이러스 방역체계가 운용되고 있어, 이러한 특징은 특정 취약점에 대해 공통적으로 노출되어 단기간 웜 감염률은 더욱 높아질 것이다. ATCIS는 전시에 운영되는 체계로 실제 전시 사황에서 zero day attak의 공격을 받을 경우

3.2.3 시뮬레이션을 위한 파라메터 설정

ATCIS 환경에 적합한 시뮬레이션을 위한 내부 파라메터 값은 <표 3>와 같다. β[9]는 감염률로 슬래머 웜의 초당 발생 패킷 수 4,000과 전체 IP 대역 대비 취약한 노드 수의 비율의 곱이며, AN 취약 노드 수를 $S_{\max}$ 에 적용하여 계산하였다.

$$\beta = 4{,}000 \times \frac{S_{\max}}{2^{32}} \tag{7}$$

v_percent는 AN에서의 취약 노드비율이며, 404바이트 크기의 패킷을 초당 4,000개 발생시켜 1434번 포트를 이용하여 공격하는 슬래머 웜의 특징에 따라 ScanRate, ScanPort, ScanPacketSize 값을 설정했다.

〈표 3〉 시뮬레이션을 위한 파라메터 값

구 분	값	비 고
β	0.006	AN 감염률
v_percent	0.96	AN 취약 노드 비율
ScanRate	4,000	스캔 횟수
ScanProt	1,434	스캔 포트
ScanPacketSize	404	패킷 크기(byte)

3.2.4 Notation

시뮬레이션 내부 웜 전파를 계산하기 위해 본 논문에 사용된 Notation은 <표 4>과 같다.

〈표 4〉 Notation

구 분	설 명
N	AN 노드 수
$S(t)$	시간에 따른 AN 취약 노드 수
$S_{\max}$	AN 전체 취약 노드 수($N \times 0.96$)
$I(t)$	시간에 따른 AN 감염 노드 수
β	AN 감염률
$I_O(t)$	시간에 따른 외부망으로부터 감염 노드 수

$I(t)$의 첫 번째 항은 이전 시간까지의 감염된 노드 수, 두 번째 항은 감염률과 이전 시간까지의 감염된 노드 수, 취약한 노드 비율의 곱으로 이루어지며, 세 번째 항은 DN으로부터 전파된 감염 패킷의 합이다.

$$I(t) = I(t-1) + \beta I(t-1)\frac{S(t-1)}{S_{\max}} + Probe In_{AN} \tag{8}$$

$S(t)$는 AN의 취약한 노드 수로 전체 노드에서 감염된 노드 수를 제외한 값이다. $I_O(t-1)$는 외부망으로부터 감염된 노드 수다. $Probe In_{AN}$는 DN로부터 AN_{IP} 대역으로 전파된 감염 패킷의 합이며, $Probe Out_{AN}$은 AN에서 DN으로 전파된 감염 패킷 의 합이다.

$$S(t) = S_{\max} - I(t-1) \tag{9}$$

$$I_O(t-1) = Probe In_{AN} \times \frac{S(t-1)}{N} \tag{10}$$

$$Probe In_{AN} = \text{DN으로부터 받은 감염 패킷 수} \tag{11}$$

$$Probe Out_{AN} = 4{,}000 \times I(t-1)\frac{IP_{DN}}{2^{32}} \tag{12}$$

DN에서는 수학적 계산 없이 실제 주고받는 패킷 단위 분석을 통해 $Probe In_{DN}$, $Probe Out_{DN}$ 값을 구하고, 실제 DN으로부터 발생되는 대부분의 패킷은 AN, DN 범위를 넘는 IP로 전송되며, 소수의 감염 패킷만이 DN 또는 AN으로 들어오게 된다.

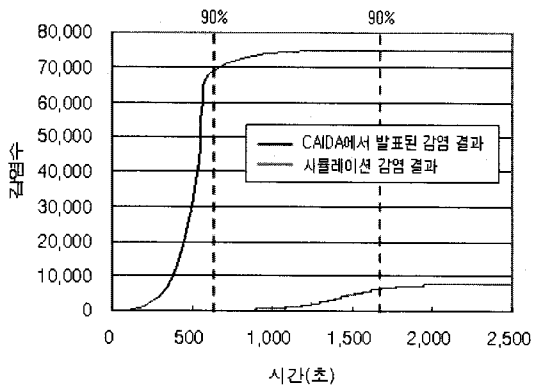
$$Probe In_{DN} = \text{AN으로부터 받은 감염 패킷 수} + \text{DN으로부터 전파된 감염 패킷 수} \quad (13)$$

$$Probe Out_{DN} = AN_{IP} + DN_{IP} + Out_{IP} \quad (14)$$

4. 시뮬레이션 결과분석

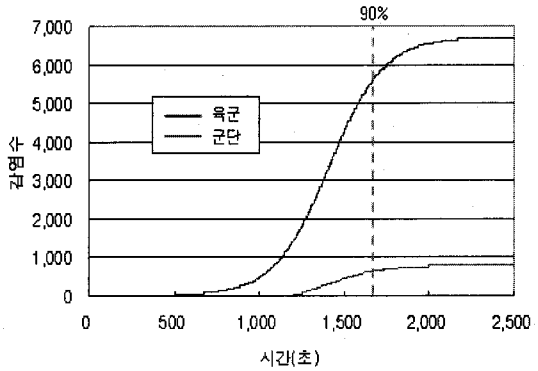
4.1 시뮬레이션 결과와 실제 감염률과의 비교

전체적인 시뮬레이션 결과는 <그림 5>에서와 같이 1.25 대란 당시 실제 감염양상과 동일한 일반적인 RCS(random constant spread) 모델 형태의 그래프로 나타났다. <그림 5>를 세부적으로 표현한 <그림 6>을 통해 더욱 자세히 확인 할 수 있다. 그러나 ATCIS의 구성 노드 수와 대역폭이 실제 인터넷 환경과 다르기 때문에 실제 감염률과는 차이가 발생함을 확인하였다.



〈그림 5〉 시뮬레이션 결과와 실제 감염률 비교

시뮬레이션 세부 결과는 <그림 6>와 같다. AN은 1초에 최초감염을 시작으로 1,762초에, DN은 1,181초를 시작으로 1,784초에 취약 노드의 90%가 모두 감염되었다. CAIDA의 발표에 따르면 슬래머 웜은 발생 10분(600초)만에 취약한 시스템의 90%이상을 감염시켰지만, 본 시뮬레이션에서는 약 29분(1,765초)의 시간이 소요되어 약 20분(1,165초)의 차이가 있었다.



〈그림 6〉 시뮬레이션 세부 결과

이러한 차이의 원인은 두 가지가 있다. 첫째, 슬래머 웜이 공격대상으로 하는 전체 노드 수의 차이다. 실제 슬래머 웜의 공격 대상은 세계에서 인터넷에 연결되어 사용된 노드 중 슬래머 웜에 취약한 약 75,000여대로 ATCIS에서의 취약한 노드 수의 10배에 달한다. 두 번째로는 대역폭의 차이다. 국가 간 차이가 있겠지만 한국을 예로 들었을 경우 국제 인터넷 대역폭은 2001년 9.5Gbps에서 2005년 말 48.6Gbps로 약 5배 이상 증가하였다.[10] 하지만 SPIDER를 기반 인프라로 사용하는 ATCIS에서는 1Mbps의 낮은 대역폭으로 실제 외부 인터넷과는 큰 차이가 있다.

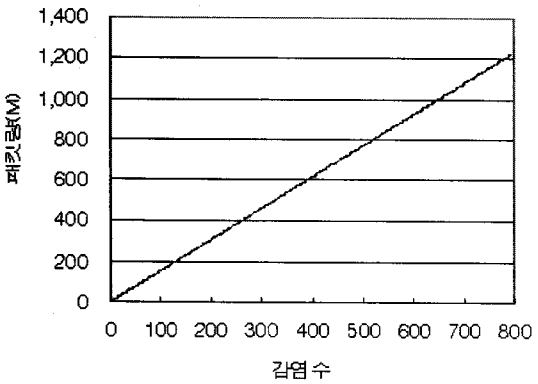
위의 두 가지 원인은 감염된 노드 수를 구하는 식(8)을 통해서도 확인 할 수 있다. 노드 수가 많으면 각 노드에서 임의 IP로 발생하는, 초당 4,000개의 감염 패킷에 감염될 확률이 그만큼 높아지고, 대역폭이 크게 되면 $Probe In_{AN}$값이 커지게 되어 감염 수가 늘어나기 때문에 감염시간은 그만큼 빨라지게 된다.

시뮬레이션 결과에서 DN의 감염이 1,181초에

서 시작하는 것은 DN의 노드 수가 적어 AN에서 발생된 감염 패킷이 DN으로 넘어 오는데 시간이 소요되기 때문으로 이는 식(13)으로 확인할 수 있다.

4.2 감염 수에 따른 패킷 발생량

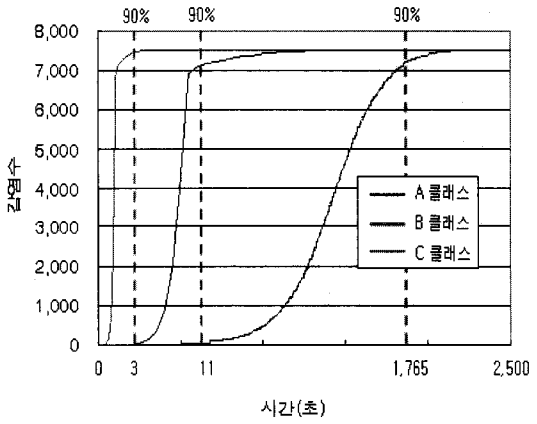
<그림 7>은 DN 감염에 따른 감염 패킷 발생량을 나타낸다. DN-AN 모델에서 발생된 패킷의 대부분은 DN에서 발생시키므로 최초 DN이 감염된 후 1초 안에 발생시킨 패킷량이 증가하면서 ATCIS의 대역폭인 1M를 모두 사용하게 되어 네트워크 병목현상이 발생한다. 즉 패킷크기(404Byte) × 패킷량(4,000) = 1,616,000로 전체 대역폭인 1Mbps를 넘게된다.



〈그림 7〉 감염 수에 따른 패킷 발생량

4.3 공격 IP대역 범위에 따른 감염률

전술통신망의 IP 대역 구성은 특정 IP 대역으로 국한되어 있어 국지적 공격에 더욱 취약할 수 있다. 따라서 고정되어 있는 특정 IP 대역에 대한 국지적 공격을 위하여 슬래머 웜 공격대상을 2^{32}의 A 클래스 IP영역에서 2^{24}의 B 클래스, 2^{16}의 C 클래스 영역으로 축소하여 실험을 하였으며, 결과는 <그림 8>와 같다.

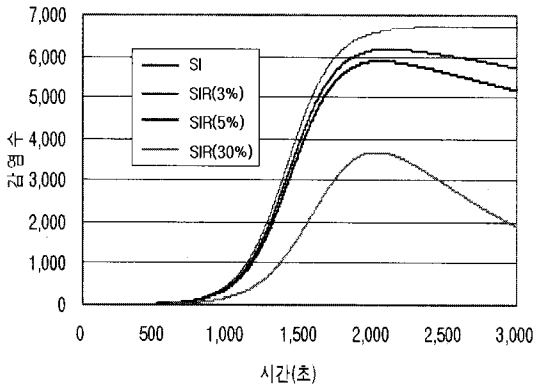


〈그림 8〉 공격 IP대역 범위에 따른 감염률

A 클래스에서는 1초를 시작으로 1,762초에, B 클래스에서는 1초를 시작으로 11초, C 클래스에서는 1초를 시작으로 3초에 취약노드의 90%가 모두 감염되었다. IP 범위가 약 256배 축소되면서 취약노드의 90%가 감염되는 시간 또한 11초, 3초로 각 160배, 588배가 축소되었다. 이러한 결과를 통해 특정 취약점에 대한 제한된 범위의 공격 시 짧은 시간에 치명적인 피해가 가능함을 확인 할 수 있었다.

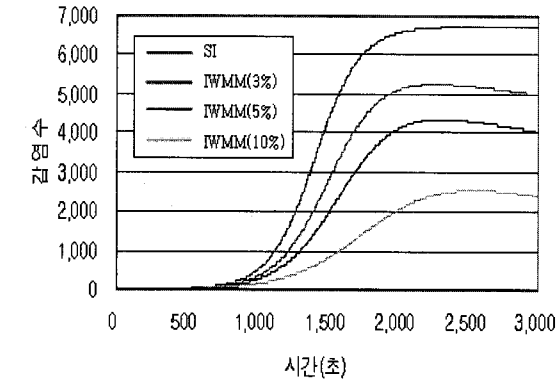
4.4 SI, SIR, IWMM 모델 결과 비교

<그림 9>는 감염된 노드에 패치를 통한 복구율을 적용한 결과를 나타낸다. 복구율은 5분 내에 3%, 5%, 30%까지 복구되는 비율을 적용했다. 복구율에 따라 감염 노드 수가 점차 감소하였고, 최대 30%를 적용했을 경우 3,680대로 복구율을 미적용 한 경우보다 3,072대 감소하였다. 또한, 3,000초에서의 감염 수는 1,891대로 최대 감염 수 3,680대의 49% 복구율을 보였다. 이러한 결과를 통해 웜 발생 이후 즉각적인 대응조치의 중요성을 확인 할 수 있었다.



〈그림 9〉 SI 모델과 SIR 모델의 결과 비교

<그림 10>은 취약한 노드에 대한 예방조치와 감염된 노드에 패치를 통한 복구율을 적용한 결과로 5분 내에 3%, 5%, 10%까지 예방조치 및 복구되는 비율을 적용했다. 시뮬레이션 결과 취약한 노드에 대한 사전 예방조치를 적용하여 SIR 모델에 비해 최대감염 수가 현저히 줄어들었다.



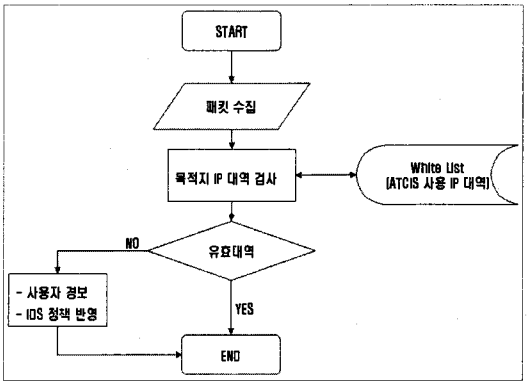
〈그림 10〉 SI모델과 IWMM 모델의 결과 비교

4.5 대응방안

실험을 통해 웜의 위험성과 피해의 심각성에 대해 알아보았으며 이러한 웜 피해 예방을 위해 본 논문에서는 다음 세 가지 대응방안을 제안한다.

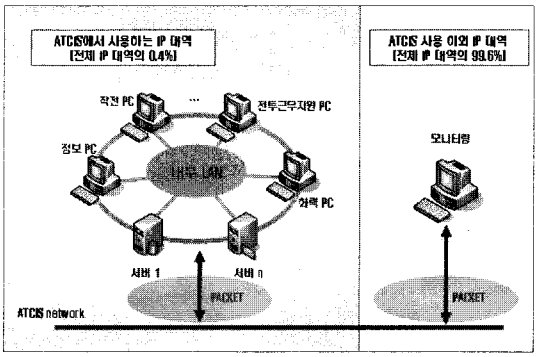
첫째, 조기경보체계의 구축이다. 대부분 웜이 불특정 IP를 공격하는 특성을 고려하여 다음 알고리즘을 제안한다. 흐름도는 <그림 11>과 같다.

① 패킷 수집
② 목적지 IP 대역과 ATCIS 사용 IP대역을 비교
③ ATCIS 사용 IP 대역을 벗어나는 경우 웜으로 판단하여 관리자 경보 및 IDS 정책 반영
④ ATCIS 사용 IP 대역을 벗어나지 않을 경우 정상 패킷으로 판단



〈그림 11〉 패킷 분석 흐름도

ATCIS에서 사용하는 IP대역은 전체 IP대역의 0.4%이므로 사용 IP 대역에 대한 정보를 White List로 저장하고 수집되는 패킷의 목적 IP를 비교한다. 제안 아키텍처는 <그림 12>와 같다.



〈그림 12〉 패킷 분석 아키텍처

조기대응체계를 위해 현재까지 다양한 연구가 진행되고 있으며, 대표적으로 네트워크 트래픽의 분석을 통해 연속 수신된 동일한 패킷이 특정 횟수를 넘을 경우 웜으로 판단하여 내부 시스템을 보호하는 EarlyBrid[11]가 있다. 이러한 다양한

체계를 ATCIS 도메인 특성에 맞는 도입을 통해 웜 피해를 예방할 수 있을 것이다.

둘째, 내부자에 의한 정보유출 방지를 위한 교육 강화다. 공격 IP대역 범위에 따른 감염률 비교 실험에서 볼 수 있듯이 ATCIS에서 사용하고 있는 IP 대역과 같은 민감한 데이터가 유출 될 경우 막대한 피해가 예상되기 때문이다.

셋째, 최신동향 / 기술 연구개발 및 대응조직 활성화다. SIR, IWMM 모델을 적용하여 복구율 및 예방조치율을 3%, 5%, 30%로 점차 증가한 실험에서 볼 수 있듯이 웜 발생 이후 조기 대응을 통해 웜 피해를 줄일 수 있을 것이다.

5. 결 론

본 논문에서는 NS-2를 이용하여 ATCIS 환경하에서의 웜 전파 시뮬레이션을 구현했다.

정확한 ATCIS 모델링을 위해 실제 ATCIS 운용환경을 면밀히 분석하여 NS-2에서 제공하는 DN-AN 모델에 적용했다. 또한, 기존 DN-AN 모델에서 필터링 없이 DN에서 발생한 감염 패킷을 AN으로 전송하여 급격한 감염률 증가로 부정확한 결과를 나타내는 문제점을 도출하고, 프로그램 내 패킷필터링 모듈을 추가하였다. 시뮬레이션을 통해 웜 피해에 대한 위험성을 확인 하였으며, 이러한 웜 피해를 사전에 예방하기 위해 조기경보체계 구축, 내부자에 의한 정보유출 방지, 최신동향 / 기술 연구개발 및 대응조직 활성화를 제안했다. 시뮬레이션 결과 ATCIS에서 사용하는 노드 중 취약노드의 90%가 1,762초에 모두 감염되었다. 또한 전술망 IP 대역 특성을 감안하여 국지적인 IP 대역에 대한 웜 공격 시뮬레이션 결과 B 클래스의 경우 11초, C 클래스에서는 3초에 취약노드의 90%가 감염되어 zero day attack에 대한 위험성이 증가함을 확인할 수 있었으며, 이러한 연구결과는 향후 전술망의 보안성을 강화시키는 기초자료로 활용할 수 있을 것이다. 현재 ATCIS 체계는 대역폭을 1Mbps에서 3Mbps로 개량 중에 있으며, 본 논문에서는 1Mbps를 기준으로 시뮬레이션을 구현했다. 차후 TICN으로의 발전은 더욱 큰 대역폭과 많은 노드의 운용으로 웜 피해에 대한 위험성이 더욱 커질 것이다.

향후 연구로는 슬래머 웜 이외 다양한 웜 시나리오에 대한 실험과 육·해·공 전술 C4I체계가 연동된 국방 전술망에 대한 웜 전파 시뮬레이션을 구현하고자 한다.

참고문헌

[1] David Moore, et al., "The Spread of the Sapphire / Slammer Worm" available at http://www.caida.org/publications/papers/2003/sapphire/sapphire.html

[2] 방사청, "육군전술지휘정보체계(ATCIS) 체계소개 및 운용가이드", 2006. 11. 30.

[3] Kevin Fall, Kannan Varadhan, "The ns Manual", 2007.

[4] S. Staniford, V. Paxson and N. Weaver, "How to 0wn the Internet in Your Spare Time," Proceedings of the 11th USENIX Security Symposium, 2002.

[5] C. C. Zou, W. Gong and D. Towsley, "Code Red Worm Propagation Modeling and Analysis," In Proceedings of the 9th ACM conference on Computer and communications security, 2002.

[6] J.O. Kephart and S.R. White, "Measuring and Modeling Computer Virus Prevalence," Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, Oakland, CA,May 1993.

[7] Darrell M. Kienzle, Matthew C. Elder, "Recent worms : a survey and trends", Proceedings of the 2003 ACM workshop

on Rapid malcode, 2003.

[8] 임재명, 윤종호, "슬래머 웜 전파과정 분석을 위한 네트워크 모델링 및 시뮬레이터 구현", 한국통신학회논문지, 2007.

[9] D. Moore, C. Shannon, G. M. Voelker and S. Savage, "Internet Quarantine : Requirements for Containing Self-Propagating Code", INFOCOM, 2003.

[10] 한국 전산원, "2006 국가 정보화 백서", p.247, 2006.

[11] S. Singh, C. Estan, G. Varghese, S. Savage, "The EarlyBird System for Real-time Detection of Unknown Worms", Technical Report CS2003-0761, UCSD, 2003.

저자소개

김 기 환 (E-mail: akkh1128@google.com)

2002 육군3사관학교 졸업(학사)
현재 국방대학교 전산정보학과 석사 과정 재학 중, 육군 대위
관심분야 웹 보안, 웜, 바이러스

김 완 주 (E-mail: sizipus1@google.com)

1998 서울산업대학교 졸업(학사)
현재 국방대학교 전산정보학과 석사 과정 재학 중, 육군 대위
관심분야 암호, 네트워크 보안

이 수 진 (E-mail: cyberkma@kndu.ac.kr)

1992 육군사관학교 졸업(학사)
1998 연세대학교 졸업(석사)
2006 한국과학기술연구원 졸업(박사)
현재 국방대학교 국방과학부 교수
관심분야 침입탐지시스템, MANET&USN Security, 암호학, 정보보호관리

<주요저서 / 논문>

- Real-Time Analysis of Intrusion Detection Alerts Via Correlation」, (Computers & Security, 2006)
- 「Threshold Password-based Authenticated Key Exchange using Matrix」,(CCCT'05, 2005)
- 「최적확장체 위에서 정의되는 타원곡선에서의 고속상수배 알고리즘」, (한국정보보호학회 논문지, 2005)
- 「Security Enhancement in Ad hoc Network with ID-based Cryptosystem」,(ICACT, 2005)
- 「연관성을 이용한 침입탐지정보 분석 시스템의 설계 및 구현」,(정보과학회 논문지, 2004)