情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

트래픽 자기 유사성(Self-similarity)에 기반한 SCADA 시스템 환경에서의 침입탐지방법론

고 폴 린,[1†] 최 화 재,[1] 김 세 령,[2] 권 혁 민,[1] 김 휘 강[1‡]
[1]고려대학교 정보보호대학원, [2]한국인터넷진흥원

Intrusion Detection Methodology for SCADA system environment based on traffic self-similarity property

Pauline Koh,[1†] Hwa Jae Choi,[1] Se Ryoung Kim,[2] Hyukmin Kwon,[1] Huy Kang Kim[1‡]
[1]Graduate School of Information Security in Korea University
[2]Korea Internet & Security Agency

요 약

SCADA 시스템은 국가 산업의 주요기반 시설인 교통・상수도・전기・가스 등의 원격지 시설 장치를 감시 및 제어하는 시스템이다. SCADA 시스템은 보안상 여러 취약점을 내재하고 있지만 가용성이 극히 요구되는 특수한 환경에서 운영되고 있다는 점 때문에 보안 기술을 적용하기에 여러 제약을 받는다. 또한, 급속한 정보 통신의 발전과 함께 현대 사회의 많은 부분이 사이버 공간으로 확장되고, 스마트그리드의 필요성이 높아짐에 따라 폐쇄망에서 운영되던 SCADA 시스템이 인터넷과 연결된 개방된 망에서 운영되도록 발전하고 있다. 이로 인해 외부와 접촉할 수 있는 경로가 확장되면서 SCADA 시스템의 취약점이 해커에게 악용될 가능성이 높아졌다. SCADA 시스템에 대한 공격은 국가적 차원의 피해를 유발하므로 이를 예방하고 대응하기 위한 보안 방법이 연구되어야 한다. 일반적으로 정상적인 네트워크 트래픽에서는 자기 유사성의 특성이 나타나는 것으로 알려져 있다. 본 연구에서는 SCADA 시스템의 자기 유사성을 측정하여 이상증후를 탐지하는 침입탐지방법론을 제시하고자 한다.

ABSTRACT

SCADA system is a computer system that monitors and controls the national infrastructure or industrial process including transportation facilities, water treatment and distribution, electrical power transmission and distribution, and gas pipelines. The SCADA system has been operated in a closed network, but it changes to open network as information and communication technology is developed rapidly. As the way of connecting with outside user extends, the possibility of exploitation of vulnerability of SCADA system gets high. The methodology to protect the possible huge damage caused by malicious user should be developed. In this paper, we proposed anomaly detection based intrusion detection methodology by estimating self-similarity of SCADA system.

Keywords: Self-similarity, SCADA, Intrusion Detection

접수일(2011년 8월 18일), 수정일(2011년 10월 6일)
게재확정일(2011년 10월 31일)
* 본 연구는 환경부 "차세대 에코이노베이션사업(글로벌탑 환경기술개발사업)"으로 지원받은 과제임
† 주저자, hyper@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr

I. 서 론

현대 정보화 사회의 중요기반 시설들은 SCADA (Supervisory Control and Data Acquisition) 시스템에 의해 중앙 집중적으로 운영 및 관리되고 있다. SCADA 시스템은 최근까지도 폐쇄망에서 운영되고 있다는 점 때문에 보안상의 문제가 없을 것이라고 여겨져 왔다. 실제로 국내 전력회사의 내부 조사 보고서에서 대부분의 경영진이 SCADA 시스템이 다른 시스템과 연결되어 있지 않다고 인식하고 있음이 드러나기도 했다[1]. 그러나 대부분의 SCADA 시스템들은 ERP(Enterprise Resources Planning)와 같은 내부 시스템이나 VPN(Virtual Private Network)을 통한 외부 망과의 연결점을 가지고 있으며, 그간 SCADA 시스템은 보안성보다는 가용성(availability)에 중점을 두었기 때문에 SCADA 시스템에 발생할 수 있는 만에 하나의 오류를 예방하기 위해 적절한 보안조치를 취하지 못하고 있는 것 역시 사실이다. 최근 발생한 스턱스넷(stuxnet) 악성코드 사례에서 본 바와 같이, 악성코드가 제어망으로 유입되는 경우 그 피해는 헤아리기 어려울 만큼 막대한 규모로 나타난다. John D. Fernandez 등[2]에 따르면 사설 메인 프레임 기반 컴퓨터 제어 시스템에서 개방형 프로토콜과 표준을 사용한 분산 시스템으로의 변화를 이유로 SCADA 시스템의 보안 위협이 계속 증가할 것이라고 예상된다.

이 외에도 RipTech[3]에서 발표한 자료에 따르면 관리자에게 데이터를 제공하기 위해 회사 네트워크와 연결된 SCADA 네트워크에 누구나 접속하여 데이터를 변경할 수 있는 잠재성이 있고, 인증되지 않은 dial-up 모뎀이나 DMZ(DeMilitarized Zone), 내부 방화벽과 같은 안전하지 않은 네트워크 디자인의 존재 등이 SCADA 시스템을 취약하게 하는 요인이 되고 있다. Eric J. Byres 등[4]의 연구에서는 SCADA 시스템에서 사용하고 있는 프로토콜이 개발되는 과정에서 존재하게 된 근본적인 취약점이 위협요소가 된다고 주장한다. SCADA 시스템에 사용되는 여러 가지 프로토콜 중에서도 MODBUS 프로토콜의 취약점은 〔표 1〕과 같이 요약된다.

여기서는 최근 주목받고 있는 스마트그리드(smart grid) 기술의 등장으로 중앙 집중식의 SCADA 시스템이 분산화 및 웹 기반 SCADA 시스템으로 변화될 것으로 예상된다. 스마트그리드는 전력 공급자와 소비자 간에 양방향의 실시간 정보 교환이 가능하도록 기존 전력망에 정보기술(information technology)을 접목한 것으로 에너지 효율성 증가, 탄소 배출 감소 등의 효과를 가져다준다. 현재 기존 중앙 집중식의 SCADA 시스템이 스마트그리드로 발전함에 있어서, 스마트그리드 환경에서의 보안이 스마트그리드 활성화에 있어서 가장 선결되어야 할 과제로 떠올랐다. 외부자의 공격 가능성이 커지는 시스템의 변화와 시스템 내의 취약점이 실제 공격에 악용되는 사례가 증가하면서 최근의 연구들은 SCADA 시스템의 보안 유지를 위한 방법론에 관심을 보이고 있다.

〔표 1〕 MODBUS 프로토콜의 취약점

MODBUS 프로토콜의 취약점	
기밀성결여 (Lack of Confidentiality)	모든 MODBUS 메시지는 전송매체를 통해 암호화되지 않은 평문의 형태로 전송된다.
무결성 결여 (Lack of Integrity)	MODBUS 어플리케이션 프로토콜에 무결성 검사 과정이 없으므로 하위 계층(lower layer)프로토콜에 의존적이다.
인증상 결함 (Lack of Authentication)	몇몇 문서화되지 않은 프로그래밍 명령(programming command)을 제외한다면 MODBUS 프로토콜의 어느 계층에도 인증 과정이 없다.
극히 단순화된 프레임(Simplistic Framing)	MODBUS/TCP 프레임은 설정된 TCP 연결로 보내어지는 데, MODBUS 어플리케이션에 적용 시, TCP 연결은 레코드 경계(record boundaries)를 보호하지 않는다는 단점이 있다.
세션 체계상 결함(Lack of Session Structure)	TCP 연결과 마찬가지로 short-lived transactions으로 구성되는 세션 체계로, 인증상의 결함, ISN 생성 결함 등과 결합되면 해커가 기존 세션을 모르더라도 명령을 조작, 주입할 수 있다.

가장 쉽게 생각할 수 있는 보안 방법론은 침입탐지시스템(Intrusion Detection System, IDS)을 이용하는 것이다. 현재까지는 SCADA 네트워크에서 사용되는 MODBUS, DNP3와 같은 프로토콜을 탐지하기에 적합하지 않다는 단점을 가지고 있으나 관제를 용이하게 하고 알려진 공격에 대하여서는 높은 탐지율을 보인다는 장점이 있어 권고하고 있다[5]. 근본적으로는 프로토콜을 안전하게 재설계하거나 구조 변경 및 장비 교체 등을 수행해야 할 것이다. 그러나 SCADA 시스템은 쉽게 구조를 변경하거나 장비를 교체하기 어렵다는 특징을 가진다. 때문에 침입탐지시스템을 이용

한 보안은 현재의 SCADA 시스템 상황에 적합하다는 평가를 받고 있다. 특히, 이상증후 탐지(anomaly-based detection)를 기반으로 한 침입탐지시스템은 제로데이 공격(zero-day attack)과 같은 알려지지 않은 취약점을 이용한 공격이나 보안 장치를 우회하는 지능적인 공격까지도 탐지할 수 있다는 장점이 있다. 이상증후 탐지기법 중 네트워크 트래픽이 일반적으로 가지고 있는 통계적 특성인 자기 유사성을 이용하는 방법이 있다. 자기 유사성은 SCADA 시스템에서 더욱 뚜렷하게 나타나는 특징으로 볼 수 있고, 이를 측정하고 관측하여 전체 시스템과 네트워크의 상태를 볼 수 있고, 이상증후를 발견할 수 있다. 본 연구에서는 자기 유사성을 측정하여 이상증후를 탐지하는 침입탐지방법론을 제시하고 그 성능을 입증하고자 한다.

II. 관련 연구

2.1 침입탐지시스템을 이용한 SCADA 시스템 보안 방법론

일반적으로 침입탐지시스템은 네트워크 기반의 침입탐지시스템과 호스트 기반의 침입탐지시스템으로 나눌 수 있으며, 탐지하는 방법에 따라 오용탐지(misuse detection)기반 방식과 이상증후 탐지(anomaly detection) 기반 방식이 있다. 오용탐지 방식은 알려진 공격 유형에 대하여서만 탐지가 가능하다는 단점 때문에 이상증후탐지 방식에 대한 연구가 상대적으로 활발하다. Dayu Yang등은 확률 및 통계 기반 방법과 auto-associative kernel regression model이라는 방법을 결합한 탐지 방법론을 SCADA 시스템 환경에서의 침입탐지에 적용하였다[6]. 가장 일반적인 이상증후 탐지 방법인 패턴 매칭(pattern matching)를 사용하였으며, 주어진 SCADA 시스템에 대하여 서비스거부공격 (denial of service attack) 시나리오를 실험하는 방법으로 성능을 입증하였다. 서비스거부공격을 수행하였을 때, 공격과 관련 없는 5가지 변수를 제외한 나머지 커널(kernel) 변수를 이용하여 공격이 수행 되었을 때 사용할 수 있는 5가지 지표(유휴시간, 평균 부하 등)를 선택하였다. SCADA 시스템이 반복적이고 일상적인 패턴(pattern)을 가지고 있으므로 이 지표들에 뚜렷한 변화가 발생하면 침입이 일어난 것으로 간주하였다. Rafael Ramos 등[7]은 SCADA 시스템 상에서 발생하는 패킷의 플로우(flow)를 이용하여 트래픽을 모델링하고 모델링 결과와 다른 트래픽 패턴이 나타나면 이상증후로 판단하여 탐지하는 방법론을 제안하였다. 이 역시 SCADA 시스템 상에서 나타나는 트래픽의 패턴이 일정하다는 것에 착안한 것으로 한정된 프로토콜이 사용되고 있고, 사용되는 네트워크 장비가 고정되어 있으며 일정한 통신 패턴을 가지고 있다는 것을 근거로 들었다. Andrea Carcano 등[8]은 시그너쳐(signature)기반의 침입탐지는 중요한 산업 기반 시설에 사용되는 SCADA 시스템에 적용하기에는 원시적이라고 보고 상태 기반의 침입탐지시스템 구조를 제안하였다. SVI(System Virtual Image)라는 정상 상태 모니터링을 위한 시스템이 있고 이것이 늘 정상적인 상태로 유지되는지 확인하는 SVAL(System Validation and Inspector)를 둔다. SCADA 시스템으로부터 들어오는 패킷들에 대한 rule을 별도로 관리하며, SPS(SCADA Protocol Sensor)가 저장된 rule을 기반으로 critical한 상태로의 전이가 있는지 여부를 확인한다.

지금까지 살펴본 연구들은 모두 나름의 독창적인 방법론을 적용하였으나 탐지의 과정이 복잡하거나 추가적인 장비를 갖춰야 하는 등의 단점을 가지고 있다. Dayu Yang 등[6]이 제안한 방법은 커널 변수를 모니터링 하고 지표가 될 만한 변수를 선택해야 하는 등의 복잡한 과정을 수행해야 한다. Rafael등이 제안한 방법의 경우는 트래픽의 패턴을 모델링하였으나 그 외에 일반적인 침입탐지시스템과의 두드러진 차이나 이점이 없다. Andrea Carcano등은 상태 전이에 의한 탐지 방법론을 제안하였으나 SVI, SVAL, SPS등의 복잡한 시스템 구조를 갖춰야 하므로 추가적인 비용이 발생하게 되고 탐지를 위해 지속적으로 상태에 대한 모니터링과 업데이트를 수행해야 한다.

이 연구들은 모두 한 가지 공통적인 가정에 기반하고 있는데 그것은 SCADA 시스템에서 발생하는 트래픽이 일정하고 반복적인 패턴을 갖는다는 것이다. 이것은 다시 말하면 시간 단위로 통계 특성치를 정의 할 수 있다는 것을 의미한다. 만약 통계 특성치가 프렉탈(fractal)구조처럼 반복되는 경우라면 이 데이터들은 자기 유사성(self-similarity)을 갖는다고 말할 수 있다. 본 연구에서는 이에 착안하여 SCADA 시스템에서 발생하는 네트워크 트래픽의 자기 유사성을 측정하여 침입탐지를 수행하였다.

본 연구에서 제시하는 자기 유사성 측정을 통한 침입탐지 방법론은 SCADA 시스템이라는 특수한 환경에 적용하기 유리하다. 중단 없는 운영이 이루어져야

하는 SCADA 시스템의 특성 상 보안 솔루션과 보안 장치의 설치가 어렵다. 대부분의 보안 도구 설정 과정과 운영체제의 업데이트에는 활성화를 시키기 위한 리부팅이 불가피하기 때문에 기반시설의 운영이 중단될 수도 있다. 보안 도구가 정상적인 상태를 침입 상황으로 잘못 판단할 경우에는 기반 시설의 운영 중단과 중요 데이터 손실 등 막대한 사회적 피해가 발생할 수 있다. 이러한 점들 때문에 SCADA 시스템 환경에서는 가용성과 장애유발 방지를 위해서 시스템 내에 에이전트(agent)를 설치하는 방식이 현실적으로 적용하기 어려운 것이다. 이는 현재 운영 중인 SCADA 시스템에 대한 직접적이고 적극적인 대응을 피해야 하는 주요 원인이다. 또한, 원활한 작동을 위해 시스템에 부하를 유발할 수 있는 방식은 지양해야 한다. 본 연구에서는 이와 같은 조건들을 만족시키기에 적합한 자기 유사성 측정을 통한 침입탐지 방법론을 제안한다.

2.2 자기 유사성(Self-similarity) 기반의 침입탐지

자기 유사성은 침입이 발생하지 않은 정상적인 네트워크 트래픽에서 발견되는 통계적 특성이라고 할 수 있다. World Wide Web traffic[9], Peer to Peer (P2P) traffic[10], Wide-area traffic[11] 등에서 자기 유사성이 존재한다는 것이 입증되었으며, SCADA 시스템의 경우 일정하고 규칙적인 네트워크 트래픽 형태를 갖기 때문에 자기 유사성이 일반적인 네트워크 트래픽에 비해 더욱 명확하게 나타나게 된다. 따라서 SCADA 시스템의 자기 유사성을 측정하고 관찰함으로써 침입을 탐지하는 것이 가능하다.

자기 유사성을 이용한 침입탐지 관련 연구들은 주로 실제 데이터나 시뮬레이션(simulation)한 데이터를 바탕으로 침입 상황을 연출해 침입 상황 전, 후의 허스트 파라미터(hurst parameter)를 각각 측정하여 값의 변화량을 기반으로 네트워크 및 시스템의 상태를 가늠하고, 이상증후를 판단한다.

C. M. Akujuobi 등[12]의 연구에서는 실험데이터로 2가지(MATLAB을 이용하여 파레토(pareto) 분포 형태의 트래픽을 발생시키는 코드를 구현한 것과 실제 트래픽 데이터)를 사용하였다. 발생시킨 트래픽의 허스트 파라미터는 0.75로 자기 유사성을 가지도록 하였다. 이 연구에서는 Multi-resolution technique을 적용한 새로운 방법론을 제시하였다. 결론적으로는 Multi-resolution technique을 이용한 새로운 방법론과 기존의 방법론은 효과 면에서 큰 차이를 보이지 않았다. 이 연구를 통해 자기 유사성의 변화 정도를 측정하여 네트워크나 시스템의 상태를 추측하고, 이상증후를 탐지할 수 있다는 것을 알 수 있다.

W. Schleifer 등[13]은 전통적인(conventional) 자기 유사성 분석 기법의 전형을 보여준다. 실제 대학에서 수집된 네트워크 트래픽 데이터를 대상으로, 에러를 삽입한 네트워크 트래픽을 임의로 구성하여 실험하였다. 전체적인 트래픽 패턴을 스케일 팩터(scale factor)에 따라 재설계(re-scale)하여 자기 유사성을 가지는지 확인한다.

권혁민 등[14]은 클라우드 컴퓨팅(cloud computing)환경에 적용할 수 있는 경량화 된 호스트기반 침입탐지 방법론을 제시하였다. 윈도우 시스템의 이벤트 로그를 이용하여 자기 유사성을 측정하였다. 윈도우 시스템의 이벤트 로그가 보안에 관련된 많은 정보를 포함하고 있지 않음에도 불구하고 자기 유사성 측정을 통해 효율적인 침입탐지가 가능하다는 것을 보였다.

이제까지 자기 유사성과 관련된 연구는 일반적인 네트워크 트래픽을 대상으로 논의되었다. 본 연구에서는 SCADA 시스템이라는 특수한 용도의 네트워크 트래픽을 관측하고 자기 유사성을 이용한 새로운 이상증후 탐지기법을 제안하고자 한다.

III. Framework

3.1 자기 유사성

자기 유사성이란 서로 다른 스케일(범위 혹은 규모, scale)에서 보았을 때 동일하게 보이거나 동일하게 행동하는 것이 유사한 현상을 말한다. 자기 유사성은 주로 결정론적인 시계열(time series)에 의해 성립하게 되는데 상대적으로 짧은 시간 간격 안의 데이터 행태가 긴 시간 동안 관측된 데이터의 행태와 유사한 현상을 가진다. 즉, 짧은 시간 간격 동안의 데이터와 긴 시간 동안의 데이터가 자기상관(auto-correlation)이 있고, 아래와 (2)와 (3) 식이 성립할 때 자기 유사성이 있다고 한다.

각각의 m = 1, 2,…에 대해 다음과 같은 확률 정상 과정 $X(m)$을 정의한다.

$$X_k^{(m)} = \frac{1}{m}(X_{(k-1)m} + \cdots + X_{km-1}), k \geq 1 \quad (1)$$

확률 정상 과정이 모든 m 값에서 같은 통계 특성을 지닌다면, 자기 유사성이 있다고 한다. 통계적 특성은

다음과 같다. (단, 0 〈 β 〈 1)

$$Var[X^{(m)}] = \frac{Var[X]}{m^{\beta}} \quad (2)$$

$$\gamma_{X^m}[X] = \gamma[t', t'+k] = \gamma[k] \quad (3)$$

여기서 자기 상관이란 어떤 두 시점에서 취한 값의 상관관계를 의미하며, 자기 상관 함수는 아래의 식과 같다.

$$\gamma(t_1, t_1+\tau) = E(X(t_1) \times X(t_2)) \quad (4)$$

확률 과정 X(t)의 시간 차이가 τ인 두 시점을 각각 t_1, t_2라 할 때, 두 표본의 곱의 집합에 대한 기대값(평균)을 X(t)의 자기 상관 함수라 한다. 자기 상관 함수는 시간 차이에 대한 함수이다.

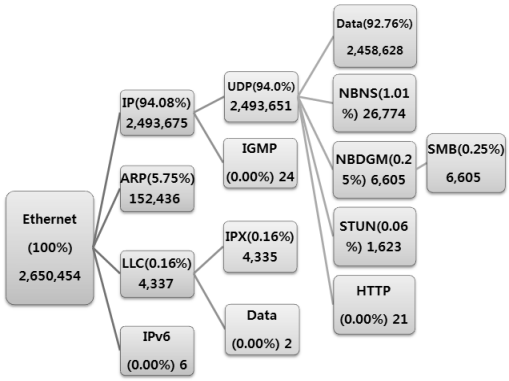
3.2 SCADA 시스템의 네트워크 구성

실험할 대상인 국내 모 SCADA 시스템의 네트워크 트래픽은 24시간의 관측을 통해 수행되었다. 분석한 데이터는 전체가 100% Ethernet 패킷으로 이루어져있으며, 그 중 대부분이 UDP 프로토콜(94.08%)로 구성되어 있었다. 〔표 2〕와 〔그림 1〕은 순서대로 분석한 시스템의 전체적인 데이터 요약 정보, 데이터를 구성하고 있는 프로토콜 분포, 그리고 프로토콜의 계층구조를 각각 나타낸다.

ARP는 IP주소와 MAC주소를 확인시키는 프로토콜이고, LLC는 데이터링크 층에서 MAC층과 상위의 IP층을 연결해주는 제어 프로토콜이므로 큰 의미를 가지지 못한다. 따라서 이 네트워크 상에서 의미를 가지는 프로토콜은 94.08%의 비율을 차지하는 UDP이다. 이 SCADA 네트워크의 전체 프로토콜 계층구조

〔표 2〕 실험 데이터 요약 정보

날짜 / 시간	2011/5/11 13:24:31 ~ 11/5/12 13:24:08 (총 23시간 59분 37초)
데이터 크기	228,752,001 Bytes (약 218MB)
총 패킷 개수	2,650,454개
초당 패킷 개수 (Packets / Second)	30.685 Packets / Sec
초당 바이트 (Bytes / Second)	2157.331 Bytes / Sec
평균 패킷 길이	70,307 Bytes



〔그림 1〕 SCADA 시스템의 프로토콜 분포와 구조

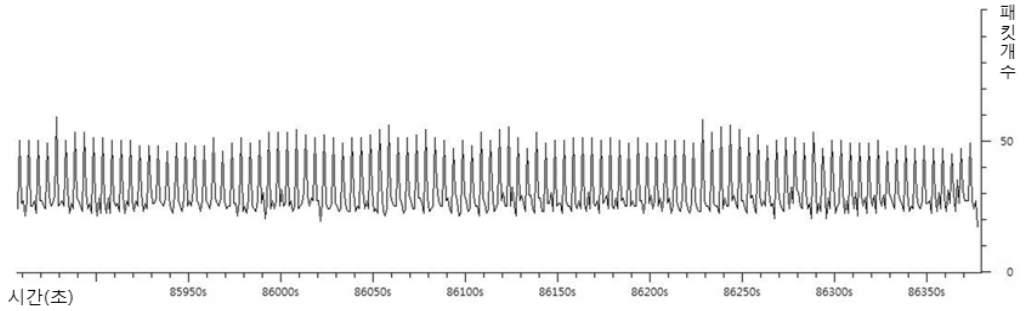
는 인터넷과 같은 일반적인 네트워크와 달리 단일 프로토콜이 대부분을 차지하였다. 〔그림 1〕에서 보듯이 UDP Data 가 전체의 92.76%를 차지하였고, NBNS(NetBIOS Name Service), NBDGM(NetBIOS Datagram), STUN(Session Traversal Utilities for NAT) 와 같은 프로토콜들은 모두 합쳐도 전체의 1% 정도만을 차지하였다. NBNS, NBDGM, STUN 같은 설정 및 제어 프로토콜들을 제외하면, 실질적으로 각 호스트들에게 의미 있는 메시지를 전달하는 것은 UDP Data 패킷들이다. 이 Data 안에는 시스템을 제어하는 메시지들이 포함되어 있다. 이러한 정상적인 경우의 전체적 데이터 수치들과 프로토콜의 분포율은 이 SCADA 시스템이 평소와 다름없는가에 대한 자기 유사성을 판단하는 근거의 지표를 제공해 줄 수 있다.

3.3 SCADA 네트워크 트래픽 특징

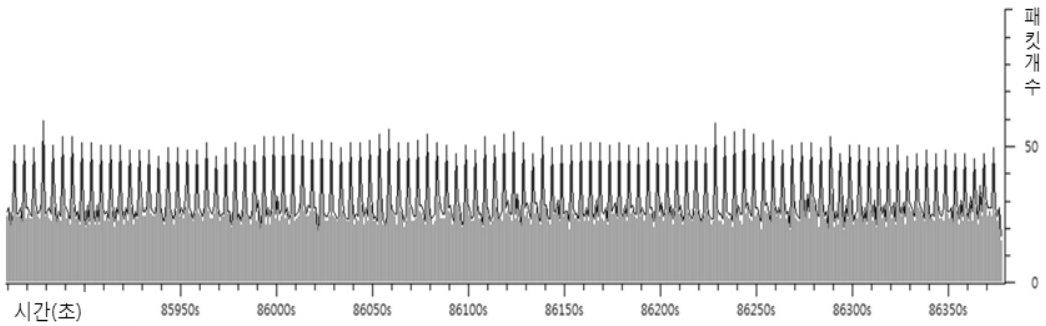
아래 〔그림 2〕는 전체 Ethernet 패킷을 1초 간격으로 관측하였을 때 패킷 개수를 나타낸다. 전체 트래픽은 일정한 주기성을 가지고 자기 유사성이 뚜렷하게 나타남을 알 수 있다. 공격으로 인한 또는 시스템 이상에 의한 트래픽 변화, 네트워크의 이상 현상, 트래픽의 폭주 등은 자기 유사성의 변화를 통해 탐지 할 수 있다. 자기 유사성의 실시간 모니터링을 통해 시스템 및 네트워크에서 일어나고 있는 전체적인 상황을 파악하기 쉬우며, 즉각적인 분석과 대응도 가능하다. 본 연구에서 사용한 SCADA 네트워크의 큰 특징은 거의 모든 트래픽이 브로드캐스트(broadcast)방식으로 이루어졌다는 것과 프로토콜의 비율이 UDP 프로토콜로 편중되어 있다는 것이다. UDP와 브로드캐

스트 트래픽 양상 또한 〔그림 3〕, 〔그림 4〕와 같이 일정하고 규칙적인 형태로 나타났다. 〔그림 3〕, 〔그림 4〕의 면적은 각각 〔그림 2〕의 전체 트래픽에서 UDP와 브로드캐스트의 초당 패킷수를 그렸을 때 차지하는 부분과 그 추이를 나타낸 것이다. 이를 통해 우리는 브로드캐스트의 경우 전체 트래픽과 거의 같은 양상을 가지며(즉, 전체네트워크는 브로드캐스트 통신을 통해 99% 이루어진다) UDP의 경우 94.08%를 차지하는데 이 역시 전체 트래픽의 거의 대부분을 차지하고 비슷한 양상을 따라감을 확인할 수 있다. 결국 이 SCADA 네트워크는 프로토콜 분포나 캐스팅 방식 등에 있어 매우 특징적인 면을 가지고 있으며, 규칙적으로 통신이 이루어지고 있다는 것을 의미한다.

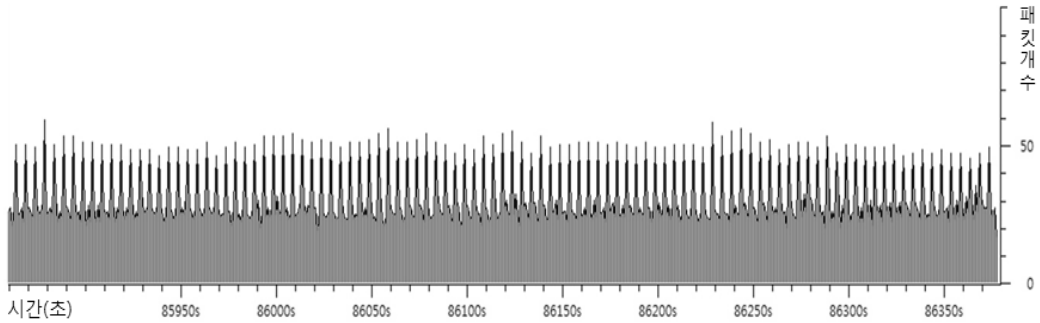
본 실험 대상 SCADA 시스템에서는 UDP가 주로 사용되었다. UDP는 특성 상, TCP에 비해 가볍고 빠르며 다자간의 통신 구현에 용이하다. 또한 단순히 짧게 제어메시지를 날리는 것에 TCP처럼 굳이 세션을 맺고 끊으면서 시스템의 자원을 낭비할 필요가 없다. 이러한 UDP만 주로 사용하는 특징은 UDP를 통한 공격 탐지에만 집중할 수 있다는 장점도 가지고 있다. 그리고 이 SCADA 망의 이런 특징 때문에 생기는 규칙적인 트래픽에 따른 탐지가 가능하다고 판단한다.



〔그림 2〕 실험 SCADA 시스템의 시간에 따른 전체 트래픽



〔그림 3〕 실험 SCADA 시스템의 시간에 따른 UDP 트래픽



〔그림 4〕 실험 SCADA 시스템의 시간에 따른 Ethernet 브로드캐스트 트래픽

IV. 자기 유사성을 이용한 이상증후탐지

4.1 자기 유사성 측정 방법

본 연구에서 제시하는 방법론은 네트워크 트래픽의 여러 요소를 활용할 수 있다. 시간 당 패킷의 개수(PPS, Packet Per Second), 시간 당 패킷의 크기(BPS, Byte Per Second) 등의 자기 유사성을 측정하여 서비스거부공격, 웜(worm) 발생 등을 탐지할 수 있고, 프로토콜별로 분석한 패킷의 자기 유사성을 측정하면 UDP, ARP 와 같은 특정 프로토콜을 이용한 공격을 탐지할 수 있다. 동일한 근원지 주소(source address), 목적지 주소(destination address), 포트 번호(port number), 평균 패킷 사이즈(average packet size) 등을 갖는 패킷의 집합인 플로우(flow)의 자기 유사성을 측정하면 서비스거부공격, 웜과 네트워크 스캐닝 등을 탐지하는 데 활용할 수 있다. 이러한 네트워크 트래픽의 여러 특징적인 요소를 분석하여, 해당 네트워크 환경의 특성을 잘 설명할 수 있는 측정 메트릭(metric)을 지정할 수 있고, 이를 통해 오경보(false alarm)를 줄이고, 다양한 공격을 정확히 탐지할 수 있다. 예를 들어, 시간 당 패킷의 개수를 관측하여 자기 유사성을 측정하는 데 사용한다고 할 경우 이를 이용한 자기 유사성 측정방식은 다음과 같다.

시점 t에 수집된 패킷 개수로 네트워크의 상태 벡터 $\overrightarrow{G_t}$를 정의한다. $\overrightarrow{E}$는 같은 차원의 단위 벡터이다. 자기 유사성을 측정하는 방법은 다양한데, 본 연구에서는 네트워크 상태 벡터와 단위 벡터 사이의 꼭지각의 코사인 거리(cosine distance) 값을 바탕으로, 코사인 값의 변화에 자기 유사성을 보이는 지를 측정하여 평가하는 방법을 제시하였다. 코사인 거리 값을 표본으로 하여 이들의 자기 유사성을 측정함으로써 방대한 데이터의 양을 압축하고 모집단의 특성을 효과적으로 나타낼 수 있다. 이러한 코사인 값의 자기 유사성인, 코사인 유사성 (cosine similarity) S_t를 다음과 같은 식으로 계산할 수 있다.

(6) 식으로부터 이상증후를 나타내는 이상점을 찾아낼 수 있다. S_t의 범위가 (6) 부등식의 조건을 만족시키지 못하면 이상점으로 판정한다. 코사인 유사성인 S_t는 1에 가까울수록 자기 유사성이 높은 것을 의미한다. 본 방법론은 SCADA 네트워크와 같이 자기 유사성이 높은 환경에서 트래픽 볼륨을 조금만 증가시키는 트래픽, 기존에 없던 프로토콜 요청, 패킷 길이,

g_t : t초에 발생한 패킷의 개수

$$\overrightarrow{G_t} = g_1, g_2, \cdots, g_m, t = 1, 2, \cdots m$$

$$\overrightarrow{E} = 1, 1, ..., 1$$

$$S_t(\text{코사인 유사성}) = \frac{\overrightarrow{G_t} \bullet \overrightarrow{E}}{\| \overrightarrow{G_t} \| \| \overrightarrow{E} \|}$$

$$where\ t = 1, 2..., k \qquad (5)$$

$$k = \frac{\text{패킷 수집 종결 시간} - \text{패킷 수집 시작 시간}}{\text{주어진 시간 간격}} \qquad (6)$$

$$\mu - c \bullet \sigma \le S_t \le \mu + c \bullet \sigma$$

$\mu = S_t$의 평균값

$\sigma = S_t$의 표준편차

source 및 target IP가 통신에 참여하게 되는 상황 등의 다양한 요인을 통해 네트워크 트래픽의 자기 유사성을 측정할 수 있다.

- 통신 source 에 참여한 IP 개수들의 변이
- 통신 destination 에 참여한 IP 개수들의 변이
- 특정 프로토콜 패킷의 비율
- flag가 RST로 세팅된 패킷의 비율
- IP option field에 값이 써져 있는 패킷의 비율

4.2 자기 유사성기반의 침입탐지 결과

본 실험에서는 SCADA 네트워크의 패킷데이터를 사용하여 SCADA 네트워크와 유사한 환경을 구축하였다. Colasoft의 패킷 리플레이어를 사용하였으며, 공격 PC에서 Tenable Nessus Scanner[15]를 사용하여 이 가상 SCADA 네트워크를 공격하였다. Tenable Nessus Scanner는 취약점 분석 도구로 약 40,000 개 이상의 다양한 공격 유형의 플러그인(plugin)을 갖추고 있다. 이 플러그인들 중 상당수는 실제 공격 상황을 재현하여 실제 익스플로잇(exploit)과 동일한 공격적인 기법을 이용하여 취약점을 발견해 낸다. 본 연구에서는 Tenable Nessus Scanner에서 제공하는 여러 가지 공격 상황을 이용하여 자기 유사성 기반의 침입탐지를 하였다. 본 실험에서 사용한 공격들은 크게 네 가지로 분류할 수 있다. 일반 네트워크에서 OS 및 어플리케이션(application)과 무관하게 일반적으로 발생할 수 있는 공격들인 General 플러그인을 사용한 공격, SCADA 시스템들 및 이를 관리하는 모니터링용 PC에서 상당수 사용되고 있는 Windows OS 의 취약점을 대상으로

한 Windows 플러그인을 사용한 공격, 분산서비스거부공격을 재현할 수 있는 DDoS 플러그인을 사용한 공격의 세 가지를 실험하였고, 마지막으로 SCADA 시스템의 취약점을 악용한 SCADA 관련 공격을 실험하였다. SCADA 환경에만 존재하는 공격패턴을 통한 실험 외에도, SCADA 네트워크 중 제어장비의 데이터를 계측하는 구간은 시리얼 통신이지만, 이 데이터의 연동 및 전송구간에서는 TCP/IP 프로토콜로 통신하기 때문에 일반적인 네트워크에서 일어날 수 있는 공격패턴에 대한 실험 역시 유효하다. SCADA 시스템에 인터넷이 연결되어 스마트그리드가 구성된다면 외부에서의 공격은 TCP/IP 프로토콜을 사용할 가능성이 높다. 더불어, SCADA 네트워크 내부에 침입하려면 원격 PC에 접속하여 공격하는 것이 일반적이며, SCADA 시스템의 OS에는 MS-DOS, Windows NT4.0, Windows 2000 등의 OS 들이 사용되고 있기 때문에 Windows 에 대한 공격패턴들 역시 여전히 유효하다. 일반 네트워크에서의 공격들이 SCADA 네트워크에서도 탐지가 되는지 여부를 확인하는 것 역시 중요하다고 할 수 있다.

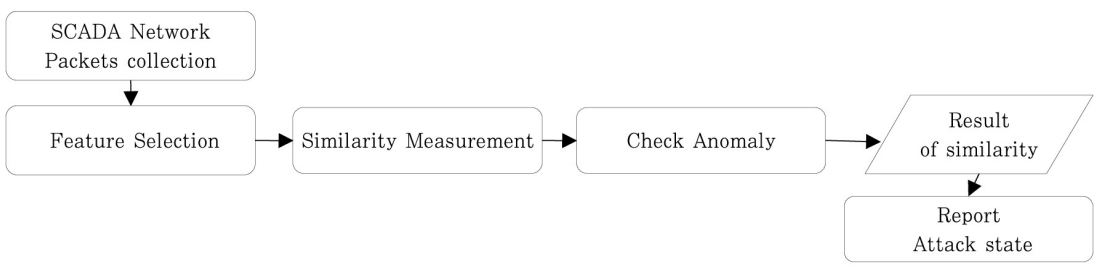
4.2.1 네트워크 트래픽 볼륨의 자기 유사성 측정을 통한 침입탐지 결과

본 연구에서는 SCADA 네트워크의 자기 유사성을 이용하여 대표적인 유형의 공격들을 탐지해낼 수 있는지를 실험하였다. 먼저, 정상 트래픽에 대하여 24시간 중 6시간 단위로 자기 유사성을 측정하였다. 결과는 아래의 〔표 3〕과 같다. 코사인 유사성은 평균적으로 0.9473에서 0.9501까지로 측정되었고 각 시간 단위별로 비교해 보았을 때 유사한 트래픽 형태와 자기 유사성을 가진다는 것을 알 수 있다. 여기에서 코사인 유사성의 표준 편차가 낮을수록 자기 유사성이 높다는 것을 의미한다.

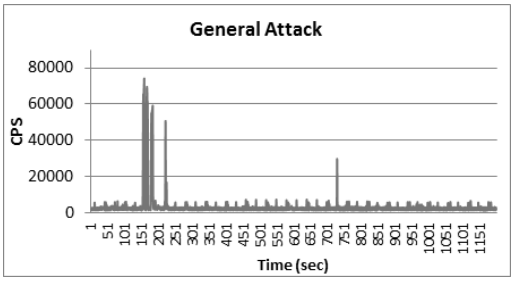
〔표 3〕 정상적인 트래픽 상황일 때 SCADA 시스템의 자기 유사성 측정 결과

시간(hour)		0-6	6-12	12-18	18-24
표본 개수		361	361	361	360
코사인 유사성 평균 (S_t)		0.947 592	0.947 389	0.947 317	0.950 112
코사인 유사성 표준편차(σ)		0.050 516	0.050 496	0.050 512	0.007 574
이상점의 개수	$\pm\sigma$	1	1	1	1
	$\pm 2\sigma$	1	1	1	1

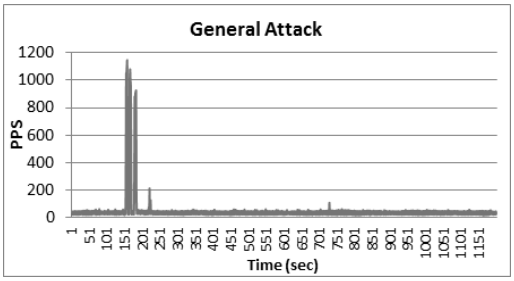
공격 실험에 적용한 Tenable Nessus Scanner의 플러그인들 중 실제 공격 시에 이루어지는 방식들을 분리하여 크게 세 가지의 공격 유형으로 분류하여 실험을 하였다. General 플러그인에서는 포트스캐닝, OS fingerprinting, Service enumeration, 패스워드 추측 등의 실제 공격과 동일한 스캐닝 방식을 선정하였으며, Windows 플러그인 역시 단순히 OS 와 서비스의 버전 유무만을 체크하는 것이 아닌, 공격을 수행하는 플러그인들을 포함하였으며, DDoS 플러그인 역시 실제 서비스거부를 유발시키는 실제 플러그인들을 이용하여 실험하였다. SCADA 시스템을 공격하는 SCADA 관련 공격은 SCADA 시스템 내의 어플리케이션 취약점을 이용하여 버퍼 오버플로우를 일으키는 것이다. 각 실험은 20분씩 지속되었고 공격 발생 시간은 약 2분이다. 모두 동일한 타이밍에 공격 PC로 가상 SCADA 네트워크에 공격을 시도하였으며, 와이어샤크(wireshark)프로그램으로 가상 SCADA 네트워크의 패킷을 캡쳐하여 CPS(Character Per Second)와 BPS를 분석하였다. 패킷데이터를 얻은 SCADA 네트워크와 동일한 환경을 구축하기 위하여 와이어샤크에서 수집된 패킷 중 관련이 없는 패킷은 모두 제거하였다. 20분 동안 각각 약 11만개정도의 패킷이 수집되었으며 리플레이(replay)



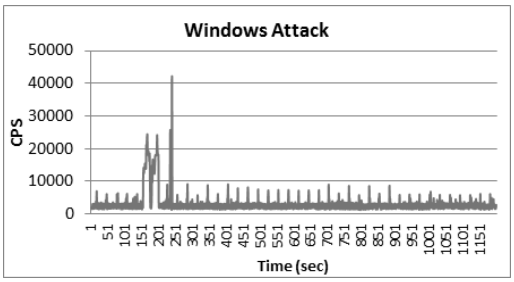
〔그림 5〕 SCADA 네트워크 트래픽 자기 유사성 측정 과정



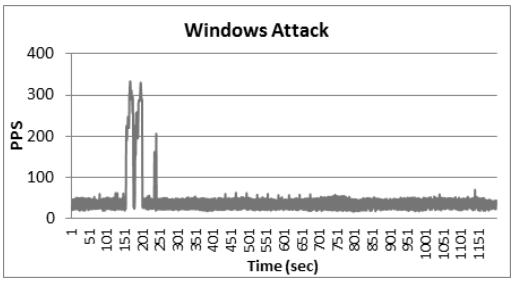
〔그림 6〕 General 공격에 따른 SCADA 시스템의 CPS 변화



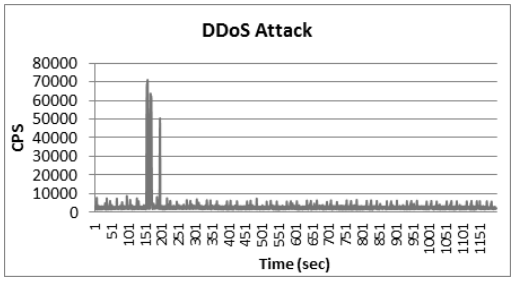
〔그림 7〕 General 공격에 따른 SCADA 시스템의 PPS 변화



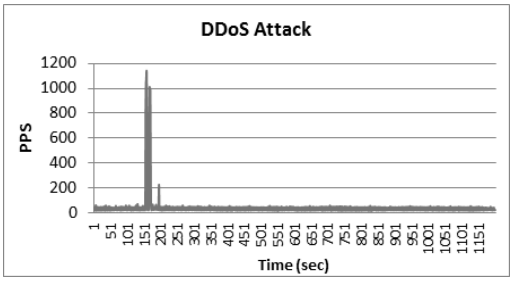
〔그림 8〕 Windows 공격에 따른 SCADA 시스템의 CPS 변화



〔그림 9〕 Windows 공격에 따른 SCADA 시스템의 PPS 변화



〔그림 10〕 DDoS 공격에 따른 SCADA 시스템의 CPS 변화



〔그림 11〕 DDoS 공격에 따른 SCADA 시스템의 PPS 변화

된 패킷과 공격 PC IP로부터 온 공격패킷만 남겨 약 4~5만 패킷정도가 수집되어 보다 정확한 SCADA 네트워크를 구축하였다. 아래 〔그림 6〕에서 〔그림 11〕은 각 공격에 대한 자기 유사성의 변화를 나타낸 그래프이다. X축은 시간(s)를, Y축은 CPS, PPS를 의미한다. General 플러그인은 공격 유형 중에서 어느 운영체제나 시스템이든 상관없이 시도해볼 수 있는 공격을 담고 있고, Windows 플러그인은 운영체제가 윈도우인 경우 시도해볼 수 있는 공격들을 포함한다.

DDoS 플러그인에는, Ping of Death와 같은 공격처럼 네트워크 용량을 꽉 채우거나, 트래픽 볼륨에 의존한 공격이 아니더라도, 대상 시스템의 자원을 소비시켜 시스템을 마비시키는 공격들이 포함되어 있다. 이런 공격들은 SCADA 네트워크 환경에 악성코드가 유입되거나 해커가 침입하였을 때 충분히 발생 가능한 공격패턴들이다. 이 실험을 통해 각각의 공격 유형에 대한 자기 유사성 정도의 변화는 공격 시점 부근에서 급격한 코사인 유사성의 저하라는 비슷한 현상을 보였다. General 공격, Internet 공격, DDoS 공격에서 각각 150초에서 250초 부근에서 다량의 트래픽이 유입되면서 자기 유사성이 급격하게 변하였다. 〔표 4〕에서 나타나듯이, General 공격의 경우 정상 상태일

〔표 4〕 공격에 따른 코사인 유사성의 변화

공격 유형	메트릭	수집 시간(초)	상황	코사인 유사성	평균 유사도
General	CPS	0~300 미만	공격	0.403482	0.746075
		300~600 미만	정상	0.894459	
		600~900 미만	정상	0.780896	
		900~1200 미만	정상	0.905464	
	PPS	0~300 미만	공격	0.365549	0.795318
		300~600 미만	정상	0.941848	
		600~900 미만	정상	0.930035	
		900~1200 미만	정상	0.94384	
Windows	CPS	0~300 미만	공격	0.630341	0.831034
		300~600 미만	정상	0.887168	
		600~900 미만	정상	0.888499	
		900~1200 미만	정상	0.918129	
	PPS	0~300 미만	공격	0.611719	0.860649
		300~600 미만	정상	0.942555	
		600~900 미만	정상	0.940049	
		900~1200 미만	정상	0.948271	
DDoS	CPS	0~300 미만	공격	0.400391	0.778395
		300~600 미만	정상	0.903618	
		600~900 미만	정상	0.903894	
		900~1200 미만	정상	0.905676	
	PPS	0~300 미만	공격	0.36087	0.798111
		300~600 미만	정상	0.943922	
		600~900 미만	정상	0.940826	
		900~1200 미만	정상	0.946825	

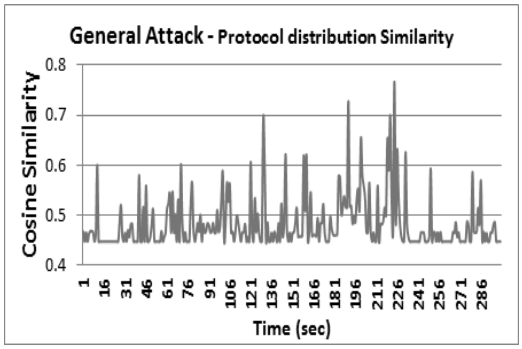
때 초당 패킷 개수(PPS)의 자기 유사성은 최소 0.9300으로 높았으나 공격의 발생했을 때는 0.3655으로까지 낮아졌고, 이러한 현상은 다른 공격 유형에서도 동일하게 나타난다. 이 특징을 이용하여, SCADA 네트워크의 높은 자기 유사성이 낮아지는 것을 관찰하여 공격의 발생 징후를 감지할 수 있다. 이는 평소와 다른 네트워크 트래픽의 변화에 따라 PPS, BPS 에의 자기 유사성 상에 변화가 생겼기 때문이다. 이는 알려지지 않은 공격이 발생한다 하더라도, 자기 유사성에 변화가 발생할 경우 공격이 잠재적으로 발생했음을 인지하고 분석 및 대응을 할 수 있다. 특히 제어망 환경과 같이 자기 유사성이 극히 높은 상태로 유지되는 네트워크에서는 자기 유사성의 변화가 공격의 증후를 감지하는 지표가 될 수 있다.

4.2.2 프로토콜별 비율에 대한 자기 유사성 측정

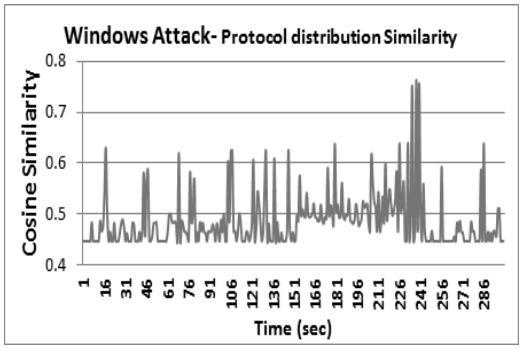
다음 실험은 본 방법론이 트래픽 볼륨의 특성을 직접적으로 나타내는 BPS, PPS 외에도 프로토콜의 분포 비율을 이용하여 네트워크 트래픽의 자기 유사성을 측정할 수 있음을 보여준다. 시간 t 일 때, 각 프로토콜의 비율을 선언한 vector 를 R 이라고 정의하고, UDP, TCP, NBNS, SSDP, 나머지 프로토콜 5개로 나눈다. 각 프로토콜의 분포 정도를 나타내는 벡터 R(UDP, TCP, NBNS, SSDP, etc)을 설정하여 t 초 일 때의 벡터 R_t = R(UDP_t, TCP_t, $NBNS_t$, $SSDP_t$, etc_t)로 표현할 수 있다. $UDP_t+TCP_t+NBNS_t+SSDP_t+etc_t=1$이고, 각 원소는 0보다 크고 1보다는 작은 값을 갖는다. 앞 실험에서 트래픽 볼륨 기반의 시간 별 자기 유사성을 코사인 유사성을 통해 측정했다면, 이번에는 프로토콜 비율로 코사인 유사성을 측정하여 자기 유사성을 분석하였다.

Tenable Nessus Scanner에서 제공하는 SCADA 시스템에 대한 Multiple Buffer Overflow 공격을 이용하여 실험을 하였다. 이는 원격에서 제어하는 PC의 윈도우 시스템이 버퍼 오버플로우(buffer overflow)에 취약한 어플리케이션을 가지고 있을 때에 실행할 수 있는 공격을 이용하였다. 〔그림 19〕와 같은 프로토콜 변화를 알 수 있었다. SCADA 시스템에 대한 외부의 공격 시, TCP 프로토콜을 사용하는 경향을 보였기 때문에 프로토콜 비율을 통한 자기 유사성을 측정함으로써 이상 증후를 파악할 수 있었다. 각 프로토콜의 비율은 공격 유형에 따라 〔그림 12〕부터 〔그림 19〕와 같이 나타나는데, 평소에는 UDP의

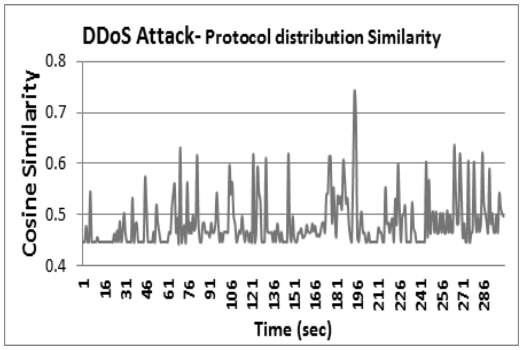
비율이 압도적으로 높다가, 공격이 발생하는 시점인 150초 부근에서 200초 이내에서 UDP의 비율이 낮아지고 대신 TCP의 비율이 급격하게 높아졌다. 동시에 자기 유사성이 대체적으로 낮아졌다가 높아졌다가를 반복하며 계속적으로 변화하였다. 대체로 자기 유사성은 0.4에서 0.6 사이를 오가는 형태를 보였고 공격 발생 시점에서 급격하게 증가하거나 자기 유사성의 변화폭이 커지는 형태를 보였다.



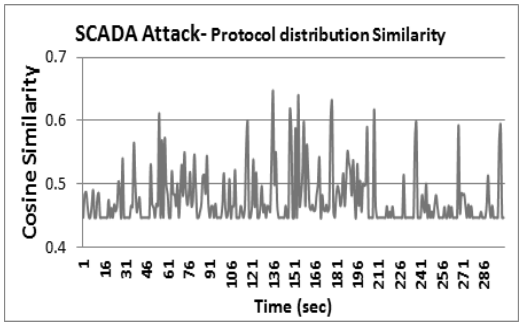
〔그림 12〕 General공격에 따른 프로토콜 분포 자기 유사성



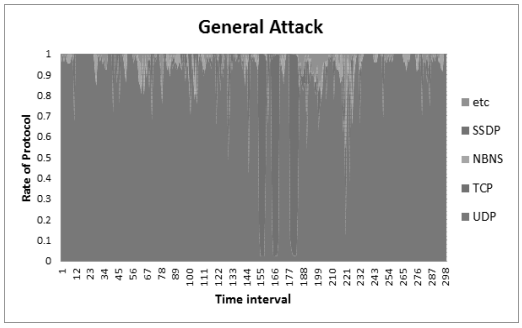
〔그림 13〕 Windows공격에 따른 프로토콜 분포 자기 유사성



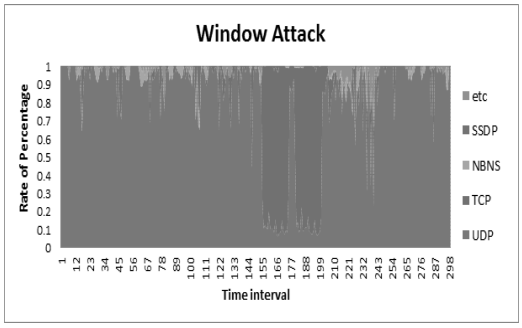
〔그림 14〕 DDoS공격에 따른 프로토콜 분포 자기 유사성



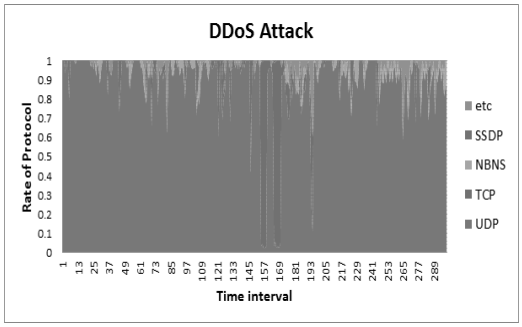
〔그림 15〕 SCADA공격에 따른 프로토콜 분포 자기 유사성



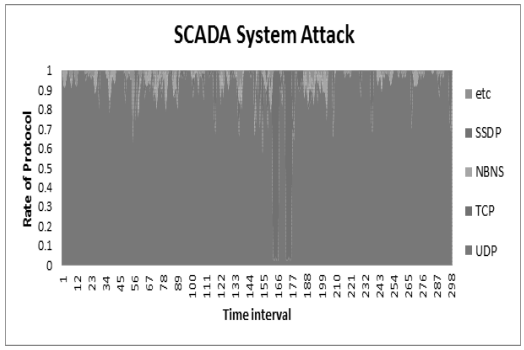
〔그림 16〕 General공격 발생 시, 프로토콜 분포도



〔그림 17〕 Window공격 발생 시, 프로토콜 분포도



〔그림 18〕 DDoS공격 발생 시, 프로토콜 분포도



〔그림 19〕 SCADA 공격 후 프로토콜 분포도

4.3 자기 유사성 기반 이상증후 탐지기법의 효과

본 연구에서 제시하는 이상증후 탐지기법은 〔표 5〕와 같이 기존의 방법들과 달리 SCADA 시스템에 적용할 수 있고, 정확한 탐지도 가능한 여러 이점을 가지고 있다. 기존의 rule 기반의 방법론은 SCADA 시스템의 취약점을 이용한 알려지지 않은 공격들을 탐지할 수 없었다. 보안 장치나 보안 프로그램을 우회하는 새로운 유형의 공격, 인가된 내부자의 지능적인 공격 등은 예측할 수 없었다. 그러나 본 방법론은 이상증후를 탐지하기 때문에 정상적인 상태와 다른 후를 통계적 방법으로 분류함으로써 제로데이 공격과 같은 새로운 공격을 탐지할 수 있다는 장점이 있다. 또한, 기존의 SCADA 시스템에 대한 침입탐지 기법은 추가적인 장비와 복잡한 시스템 구조로 구성되어야 했다. 이는 탐지 과정의 효율성을 저하시킨다. 본 방법론은 간단한 통계적 방법을 이용하며 복잡한 장치나 시스템 구조의 설정을 필요로 하지 않는다. 무엇보다 기존의 방법들은 SCADA 시스템에 부하를 유발하여 가용성을 저하시킬 우려가 있는 등 여러 한계가 있다. 운영 상 작동 중단의 위험이 없어야 했기에 기존의 침입탐지시스템이나 보안 도구를 적용하기 어려운 점이 있었다. 본 방법론은 SCADA 네트워크 단에서 탐지하므로 SCADA 시스템 작동 중단의 위험이 없다. 보안 도구의 오진으로 인한 불필요한 피해의 가능성이 없기 때문에 SCADA 시스템에 적용하기에 무리가 없다. 본 연구에서는 자기 유사성을 이용한 이상증후 탐지기법을 〔표 5〕와 같이 여러 문제점을 개선하였다.

4.4 자기 유사성 기반 이상증후 탐지기법을 응용한 하이브리드 침입탐지시스템

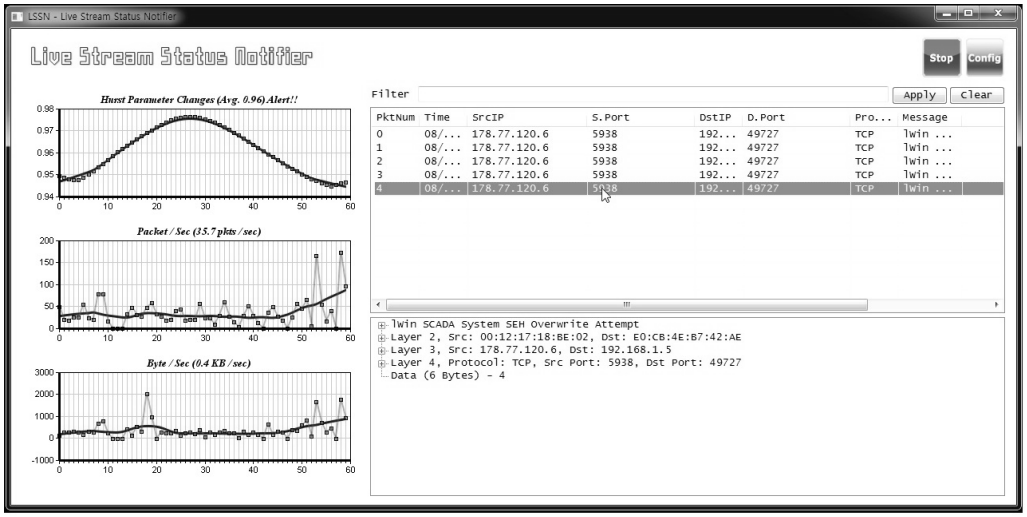
트래픽 분석을 기반으로 자기 유사성을 측정하는 방법은 여러 알려지지 않은 공격을 탐지하는 데에 유용하지만, 자기 유사성의 변화를 주지 않는 익스플로잇과 같은 공격을 탐지하는 데에는 한계가 있다. 하지만 이러한 익스플로잇과 같은 공격은 대부분 알려진 취약점을 이용하여 이루어지는 경우가 많기 때문에 이에 대해서는 시그너쳐 기반의 오용 탐지(misuse detection)로 대응할 수 있다. 이를 이용하여 트래픽 분석 기반의 이상증후 탐지(anomaly detection)과 시그너쳐 기반의 오용탐지를 결합한 하이브리드(hybrid) 침입탐지시스템을 제작하였다. 〔그림 20〕은 아키텍처와 해당 프로그램의 스크린 샷이다.

V. 결 론

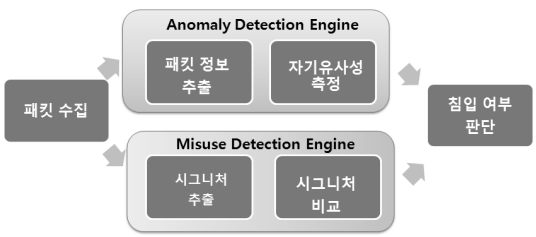
본 연구에서는 SCADA 시스템이 일정하고 규칙적인 트래픽 패턴을 가지고 있음에 착안하여 자기 유사성 기반의 침입탐지 방법론을 제안하였다. 실제 현장에서 수집된 패킷 데이터를 이용하여 SCADA 네트워크가

〔표 5〕 기존의 방법론과 자기 유사성을 이용한 방법론 비교

	기존의 방법론	자기 유사성을 이용한 방법론
공격 탐지	rule 기반의 방법론은 알려지지 않은 공격을 탐지할 수 없고, 지속적인 업데이트를 해야 한다.	알려지지 않은 공격과 우회하는 공격을 탐지할 수 있다.
복잡성	추가적인 장비를 필요로 하거나 복잡한 탐지 과정을 필요로 한다.	추가적인 장비가 필요 없고 비교적 간단한 탐지 과정이다.
안전성	알려지지 않은 공격이 유입되는 경우 SCADA 네트워크 상에 존재하는 침입탐지시스템 에이전트가 탐지하지 못하게 되므로 그대로 공격에 노출된다.	SCADA 네트워크 단에서 탐지하므로 시스템 작동 중단의 위험이 없다.
가용성	DDoS와 같이 다량의 트래픽이 유입되는 경우 SCADA네트워크에 부하가 발생하고 시스템의 오류를 유발할 수 있다.	추가 장비가 필요 없고, 모델링도 간단하여 SCADA 시스템에 부하를 주지 않는다.



〔그림 20〕 자기 유사성 기반의 하이브리드 침입탐지시스템 스크린 샷



〔그림 21〕 하이브리드 침입탐지 시스템 동작 프로시져

일정한 패턴을 가지고 있음을 직접 확인해 보았으며, 이를 이용하여 침입 상황을 시뮬레이션 하였을 때, 뚜렷하게 자기 유사성이 무너지는 것을 증명하였다.

본 연구에서 제안하는 자기 유사성을 이용한 침입탐지 방법론은 SCADA 시스템이라는 특수한 환경에 적용할 수 있다. 본 방법론의 성능과 효과는 다음과 같다. 첫째, SCADA 네트워크 트래픽을 감시하고 침입 상황을 실시간 모니터링 할 수 있다. 네트워크 트래픽의 통계적 특성인 자기 유사성을 관측함으로써 현 네트워크 상황을 간단한 수치와 그래프로 파악할 수 있다. 침입 발생 시, 신속한 보고를 통해 보안 담당자가 합리적인 판단을 할 수 있도록 돕고, 네트워크의 형태를 통해 앞으로의 상황도 예측할 수 있다. 둘째, SCADA 시스템의 작동 중단과 부하를 유발하지 않는다. 기존의 보안시스템들은 SCADA 시스템의 독자적인 프로토콜 체계와 특성을 반영하지 않아 침입탐지에 한계가 있었다. 직접적인 대응 방식의 보안 기술은 작동의 중단이 허용되지 않는 SCADA 시스템 환경에는 부적합하다. 본 연구에서는 네트워크 단에서 트래픽 모니터링을 통해 전체 시스템의 자기 유사성 변화를 감시하므로 시스템의 작동 중단, 부하 유발 등의 위험요소가 존재하지 않는다. 셋째, 추가적인 장비나 복잡한 모델링 등의 설정을 필요로 하지 않는다. 기존의 방법론은 보통 추가적인 장비와 복잡한 시스템 구조 등을 요구한다. 이는 추가적인 비용과 관리, 가용성에 대한 부담을 주므로 효과적이지 않다. 넷째, 알려지지 않은 공격이나 보안 도구를 우회하는 고도의 해킹 기술도 탐지할 수 있다. 기존의 방법들 중 알려진 공격을 시그너쳐로 하여 침입탐지를 하는 경우, 알려지지 않은 공격 및 우회하는 공격 등은 탐지할 방법이 없다. SCADA 시스템은 여러 취약점을 내포하고 있기 때문에 다양한 공격 가능성이 있다. 본 연구에서는 자기 유사성 측정을 통해 통계적인 정상 행위를 기반으로 이상증후를 탐지함으로써 알려지지 않은 공격과 우회하는 공격도 탐지하고자 설계하였다. 다섯 째, 새로운 메트릭을 지정하여 다양한 분석을 할 수 있다. 전체 네트워크 트래픽의 자기 유사성뿐만 아니라, 프로토콜별 자기 유사성, 근원지 주소, 목적지 주소, 패킷의 크기 등 여러 가지 지표를 분석하여 자기 유사성을 측정 할 수 있다. 분석할 수 있는 데이터에 크게 제약받지 않아, 다양한 경우를 분석하여 연구할 수 있다. 본 연구에서는 일반 네트워크에서의 공격 유형과 SCADA 시스템에 관련된 공격 유형을 모두 포함하여 실험하였고, 이를 통해 자기 유사성 기반의 침입탐지 기법을 통해 공격발생을 용이하게 탐지함을 보였다.

특히, 제어망 및 SCADA 시스템을 대상으로 한 공격들은 아직 알려지지 않은 경우가 많은데, 자기 유사성을 이용한 침입탐지 방법론은 어떠한 공격이 발생하였는가를 뚜렷하게 알기는 어려우나 침입 상황이 발생하였다는 사실을 알아낼 수 있으며 실시간으로 침입 상황을 보고한다는 점에서 매우 효율적이다. 자기 유사성이 변화하는 과정을 쉽게 파악할 수 있도록 시각화 기법이나 통계적 기법 등을 결합하여 연구한다면 발전된 보안 관제 시스템 기술을 개발할 수 있을 것이다.

참고문헌

〔1〕 이철원, "주요 제어시설의 사이버 보안 동향," 국가보안기술연구소, 2007년.

〔2〕 Riptech, "Understanding SCADA system security vulnerabilities," http://www.iwar.org.uk/cip/resources/utilities/SCADA Whitepaperfinal1.pdf, Dec. 2004.

〔3〕 J.D. Frenandez and A.E. Fernandez, "SCADA systems: vulnerabilities and remediation," Journal of Computing Sciences in Colleges, vol. 20, no. 4, pp. 160-168, Apr. 2005.

〔4〕 J.B, Eric, M. Franz, and D. Miller, "The use of attack trees in assessing vulnerabilities in SCADA systems," International Infrastructure Survivability Workshop, Dec. 2004.

〔5〕 K. Stouffer, J. Falco, and K. Kent, "Guide to supervisory control and data acquisition (SCADA) and industrial control systems security," Recommendations of the National Institute of Standards and Technology, Sep. 2006.

〔6〕 D. Yang, A. Usynin, and J. Hines, "Anomaly-based intrusion detection for SCADA systems," 5th International Topical Meeting on Nuclear Plant Instrumentation Controls and Human Machine Interface Technology, Nov. 2006.

〔7〕 R. Ramos, R. Barbosa, and A. Pras, "Intrusion detection in SCADA networks," Mechanisms for Autonomous Management of Networks and Services, LNCS 6155, pp. 163-166, 2010.

〔8〕 A. Carcano, I.N. Fovino, M. Masera, and Alberto Trombetta, "State-based network intrusion detection systems for SCADA protocols: a proof of concept," Critical Information Infrastructures Security, LNCS 6027, pp. 138-150, 2010.

〔9〕 M. Crovella and A. Bestavros, "Explaining world wide web traffic self-similarity," Computer Science Department, Boston University, Ott Technical Report, TR-95-015, 1995.

〔10〕 Li, R, H.L Zhu, Y. Xin. C. Wang, and Y.X. Yang, "Study on the self-similarity of P2P traffic behavior based on fractal method," Journal of Beijing University of Posts and Telecommunications, vol. 33, no. 4, pp. 35-38, 58. Jul. 2010.

〔11〕 V. Paxson and S. Floyd, "Wide-area traffic: the failure of poisson modeling," IEEE/ACM Transactions on Networking (TON), vol. 3, no. 3, pp. 226 - 244, June 1995.

〔12〕 C.M. Akujuobi, N.K. Ampah, N.O. Matthew, and Sadiku, "Application of wavelet and self-similarity to enterprise network intrusion detection and prevention systems," IEEE International Symposium on Consumer Electronics, pp. 1-6, June 2007.

〔13〕 W. Schleifer and M. Mannle, "Online error detection through observation of traffic self-similarity," Communications, IEE Proceedings, vol. 148, no. 1, pp. 38-42, Feb. 2001.

〔14〕 H. Kwon, T. Kim, S.J. Yu, and H.K Kim, "Self-similarity based lightweight intrusion detection method for cloud computing," Intelligent Information and Database Systems, LNCS 6592, pp. 353-362, Apr. 2011.

〔15〕 Tenable Network Security, Nessus, http://www.nessus.org/plugins

〈著者紹介〉

고 폴 린 (Pauline Koh) 정회원
2008년 2월: 고려대학교 산업시스템정보공학과 학사
2011년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 침입 탐지, 스마트그리드 보안, 악성코드 탐지

최 화 재 (Hwa Jae Choi) 정회원
2011년 2월: 고려대학교 컴퓨터 공학과 학사
2011년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 침입 탐지, 온라인게임 보안, 역공학, 악성코드 탐지

김 세 령 (Se Ryoung Kim) 정회원
2005년 2월: 서울여자대학교 컴퓨터 공학과 학사
2012년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2011년 12월~현재: 한국인터넷진흥원 주임 연구원
〈관심분야〉 정보보호, 침입 탐지, 전문가 시스템, 역공학

권 혁 민 (Hyukmin Kwon) 정회원
2009년 2월: 광운대학교 컴퓨터 공학과 학사
2010년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 침입 탐지, 온라인게임 보안, 네트워크 보안

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직