자동화 네트워크 침입 탐지 시스템

김태인, 황청환, 박재현
인하대학교 정보통신공학과
tikim@emcl.org, chhwang@emcl.org, jhyun@inha.ac.kr

Network Intrusion Detection System for Industrial Network

Tae-In Kim, CheongHwan Hwang, Jaehyun Park
School of Information and Communication Engineering, Inha University

Abstract - For the industrial network, various fieldbus protocols including Modbus/TCP are used to control the manufacturing system. To protect this idustrial network against malicious intrusion, it is important to use Network Intrusion Detection System(NIDS) because the protocol barely contains secure or cryptographic features. The commonly used NIDS are software-based and don't guarantee real-time detection since they are not for critical industrial system. In this paper, a FPGA-based automated NIDS is proposed which can detect suspicious network packet in real-time in order to be used in industrial system.

1. 서 론

산업용 자동화 시스템은 각종 센서 및 제어 장치들간의 통신망으로 필드버스(fieldbus) 프로토콜을 이용하고 있다. 최근 스마트 공장과 같은 다량의 다양한 정보를 요구하는 산업체의 수요에 대응하기 위하여 기존 필드버스들도 고속의 이더넷 통신을 활용하는 Fieldbus over Ethernet 형태로 발전되고 있다. 대표적인 예로서 Modbus/TCP는 기존 Modbus 프로토콜을 고속의 Ethernet TCP/IP 상에 구현한 것으로 기존 필드버스와의 호환성을 유지하면서 빠른 통신 속도를 제공한다. 하지만 이러한 규약에는 장치를 제어하는 기능을 위주로 정의가 되어있고 보안이나 암호화에 관한 부분은 존재하지 않기 때문에 네트워크 환경에서 이러한 프로토콜을 이용하는 시스템에 대한 침입을 방지할 방법이 필연적으로 요구된다.

일반적으로 해당 문제를 해결하기 위해 네트워크 침입 탐지 시스템(NIDS)를 도입하여 네트워크로부터 들어오는 패킷을 분석하고 공격이 의심될 때 이를 사용자에게 알려주는 방식을 이용하고 있다. 소프트웨어 NIDS인 SNORT[1]는 무료 오픈 소스에 제공하는 기능도 다양하여 널리 이용되고 있으나 호스트 PC가 패킷 탐지 및 분석을 수행하는 관계로 PC의 성능이나 네트워크의 속도, 패킷의 양 등 여러 가지 원인에 의해 패킷이 도착한 시점과 해당 패킷이 악의적인지를 판단하는 시점의 간격이 적당히 짧지 않아 시스템에 대한 공격을 유효한 시간 내에 막아내지 못할 수도 있다.[2] 해당 패킷이 소프트웨어 NIDS 자체를 공격하여 무력화할 가능성도 있다.

NIDS를 소프트웨어로 구현했을 때의 문제를 극복하기 위해 FPGA로 NIDS를 구현하면 공격자가 네트워크 패킷을 통해 NIDS를 공격하거나 악의적으로 변조할 수 없어 보안성을 높일 수 있고 호스트 PC를 이용하지 않아도 되며 빠른 속도로 패킷을 분석할 수 있다는 장점이 있다. FPGA로 이를 구현한 사례가 존재하는데, 일반적인 네트워크 환경에서의 공격과 침입을 탐지하기 위해 TCP 데이터를 직접 분석한다. [3]-[5] 하지만 산업 네트워크는 그 특성상 지정범위 내의 주소, 기기, 동작만 허용해도 충분히 침입을 막을 수 있으므로 이더넷, TCP, Modbus TCP 헤더 정보만 추출하여 분석을 진행할 것이다.

따라서 본 논문에서는 FPGA를 이용해 산업 네트워크에서도 충분히 사용할 수 있을 정도로 빠른 네트워크 탐지 시스템을 제시할 것이며, Modbus/TCP 프로토콜을 대상으로 하여 해당 프로토콜의 특징을 이용해 실시간으로 패킷을 검사하는 부분을 실제로 구현하고 그 결과를 설명할 것이다.

2. 본 론

2.1 전체 시스템 구조

본 논문이 제시하는 구조는 <그림 1>과 같다. Modbus/TCP 패킷을 이더넷 포트를 통해 받아들이고 비교기를 통해 비교할 패킷 정보를 추출하는 패킷 파서가 존재한다. 또한 SPI 통신을 통해 외부로부터 패킷에 대한 검사 규칙 조합을 받아 Block RAM에 저장하는 모듈이 있다. 규칙 조합을 수정한 직후엔 각 비교기의 순번에 대응하는 규칙 조합 정보를 갱신하게 된다.

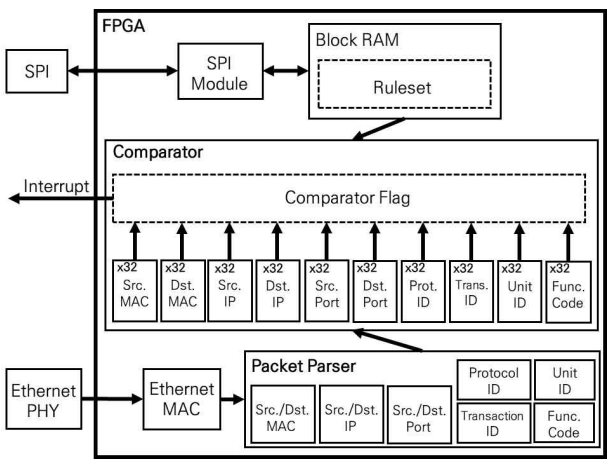
2.1.1 Modbus/TCP 패킷 수집기

Modbus/TCP 패킷은 RGMII 인터페이스에 기반을 둔 이더넷 매체 접근 제어(MAC)와 물리 계층 기기(PHY)를 통해 수집한다. 패킷을 수신하는 중에 본 시스템이 분석할 규칙에 대응하는 정보가 들어오면 즉시 버퍼에 저장하여 비교기를 통한 분석을 수행하게 한다. 예를 들면 Modbus/TCP 패킷에서 가장 먼저 들어오는 정보는 출발지의 MAC 주소인데, 이것에 해당하는 6바이트만큼의 정보가 모두 들어온 직후에 출발지의 MAC 주소에 대한 규칙을 비교하는 비교기들이 동작하게 된다.

2.1.2 비교기

본 논문에서 이용할 규칙 조합은 10가지의 세부 규칙으로 이루어져 있다. 따라서 하나의 비교기는 내부적으로 10가지 규칙을 비교하는 세부 비교기들이 있어 패킷 추출기를 통해 들어온 정보를 분석하게 된다. 세부 규칙 비교기는 하나의 특정 패킷 정보에 대한 8개의 세부 규칙을 가지고 비교를 수행하게 된다.

본 논문에서는 화이트리스트에 기반을 둔 비교를 하므로 특정



<그림 1> 시스템 블록 다이어그램

패킷 정보와 그에 대응하는 세부 규칙을 XOR 연산한 결과를 OR 연산으로 모아 해당 패킷이 하나의 세부 규칙이라도 만족하는지에 대한 정보를 상위 비교기에 전달한다.

상위 비교기에서는 10개의 세부 비교기들의 비교 결과를 다시 AND 연산하여 패킷이 10가지 세부 규칙을 모두 만족하는지를 상위 모듈에 전달한다. 따라서 수신된 패킷이 하나의 규칙 조합이라도 만족할 때를 알아내어 조처할 수 있다.

2.1.3 화이트리스트 기반 규칙 조합

이더넷 프레임에 있는 MAC 주소는 통신기기별로 고유한 식별자이기 때문에 규칙으로 이용하기 좋다. 또한, 대부분의 NIDS 프로그램은 IP 주소와 포트 번호를 규칙으로 이용하므로 호환을 위해 규칙 조합에 포함하였다. Modbus/TCP 프레임에선 Length 정보를 제외한 모든 헤더 정보와 Function Code를 규칙 조합에 포함하였다. 이러한 규칙 조합을 <그림 2>와 같은 구조로 BRAM에 저장하고 불러오게 된다.

2.2 구현 및 실험 결과

본 논문에서 제시한 시스템을 구현하기 위해 AVNET社 의 PicoZed 7030 SOM을 이용하였다. 이더넷은 RGMII 100Mbps 규격을 이용했으며 256개의 규칙 조합을 미리 저장한 상태에서 Modbus TCP 패킷을 FPGA에 보내 실험을 진행했다.

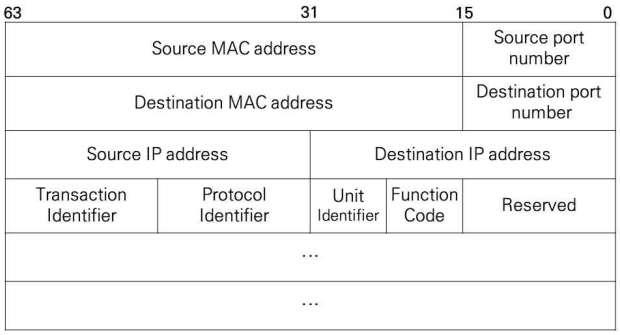
RGMII_CTL 신호가 0에서 1로 바뀌면 Modbus TCP 패킷이 들어오며 패킷 검사에 필요한 정보들을 패킷 수집기에서 추출해 비교를 수행하고 결과를 출력하게 된다.

<그림 3>은 규칙 조합 중 하나 이상의 조합과 일치하는 Modbus/TCP 패킷이 들어왔을 때 각 신호의 변화를 보여준다. 규칙과 일치하는 정보면 비교 결과 신호가 1에서 0으로 바뀌게 되는데, 모든 규칙이 패킷의 각 부분과 모두 일치하게 되면 MATCH 신호가 1에서 0으로 바뀌어 규칙을 만족하는 패킷이 들어왔다는 것을 알려준다.

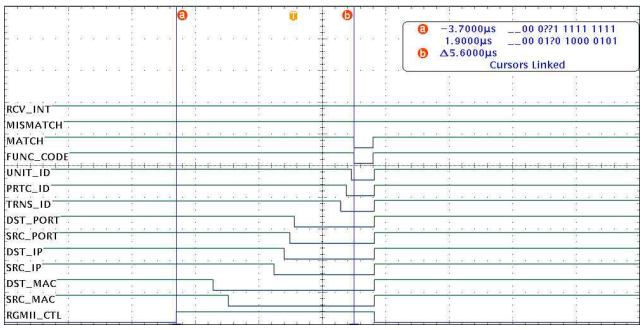
반대로 <그림 4>는 어떤 규칙 조합도 만족하지 않는 패킷이 들어왔을 때를 보여준다. 규칙에 정의되어 있지 않은 Modbus Function Code가 들어 온 경우를 캡처한 것인데, 다른 규칙들이 일치하더라도 해당 규칙이 불일치하므로 MISMATCH 신호가 0으로 바뀌고 인터럽트 신호에 해당하는 RCV_INT 신호가 나오게 된다. Modbus TCP 프레임 구조상 Function Code 이후 Data 부분이 모두 들어오기 전에 패킷에 대한 검사를 완료하고 비정상적인 패킷이 들어왔다는 사실을 인터럽트 신호를 보내 알리므로 실시간 탐지 능력을 갖추고 있음을 알 수 있다.

3. 결 론

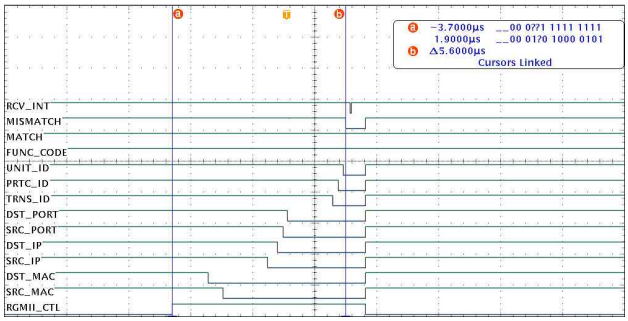
본 논문은 산업 네트워크를 위한 자동화된 네트워크 침입 탐지 시스템을 제안하였다. 제안한 시스템은 패킷 수신부, 비교기, 규칙 조합 저장부로 구성되어 있다. 실시간으로 침입을 탐지하기 위해 MAC 주소, IP 주소, Modbus Function Code 등을 기반으로 화이트리스트 룰셋을 수립하고 이를 만족하는 Modbus



<그림 2> Block RAM에 저장된 규칙 조합



<그림 3> 수신된 패킷이 규칙과 일치



<그림 4> 수신된 패킷이 규칙과 불일치

TCP 패킷만 통과할 수 있게 구현하였다. 따라서 제시한 시스템을 이용하면 산업용 네트워크의 보안성을 높일 수 있을 것으로 기대한다.

감사의 글

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. 지원에 감사드립니다. (No. 20171510102110)

[참 고 문 헌]

[1] Cisco, “Snort Users Manual”, https://snort.org/documents/snort-users-manual, [Online; accessed May 9, 2019]

[2] A.Mitra, W.A.Najjar, and L.N.Bhuyan, “Compiling PCRE to FPGA for accelerating SNORT IDS”, *ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, pp. 127-136, December 2007

[3] H. Chen, Y. Chen, and D.H.Summerville, “A survey on the Application of FPGAs for Network Infrastructure Security”, *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 13, pp. 541-561, Fourth Quarter 2011

[4] A. Das, D. Nguyen, J. Zambreno, G. Memik and A. Choudhary, "An FPGA-Based Network Intrusion Detection Architecture," in *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 118-132, March 2008.

[5] B. L. Hutchings, R. Franklin and D. Carver, "Assisting network intrusion detection with reconfigurable hardware," *Proceedings. 10th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, Napa, CA, USA*, pp. 111-120., 2002

[6] 오성록, 신상호, 박재현,“이더넷 환경 상에서의 FPGA 기반 네트워크 침입 탐지”, 제어로봇시스템학회 국내학술대회 논문집,413-414. May 2017