한국산학기술학회논문지
Vol. 11, No. 1, pp. 151-158, 2010

데이터 스푸핑 탐지를 위한 유휴 시간 측정 시스템 설계

정성모[1], 송재구[1], 김태훈[1], 소요환[1], 김석수[1*]
[1]한남대학교 멀티미디어학과

Design of Idle-time Measurement System for Data Spoofing Detection

Sungmo Jung[1], Jae-gu Song[1], Taihoon Kim[1], Yohwan So[1] and Seoksoo Kim[1*]
[1]**Department of Multimedia, Hannam University**

요 약 국내/외 산업기반시설들은 악의적인 사용자로부터 받은 공격으로 인해 큰 피해를 받고 있다. 특히, 전력, 댐, 철도, 원자력 등과 같은 국가 주요핵심기반시설이 피해를 입었을 경우 그 피해는 경제적인 문제뿐만 아니라, 국민의 생명과도 직결될 수 있다. 이러한 국가 주요핵심기반시설은 Modbus RS485통신을 사용하는 SCADA 시스템으로 구성되어 있는 것이 일반적이며, 이러한 특성상 SCADA 시스템에서 직접 명령을 전달하는 RTU Master와 Slave는 RJ11 케이블로 연결되어 있다. RJ11 케이블의 전송 범위는 1km정도로 대역이 넓기 때문에 케이블에 물리적인 접속을 통하여 데이터 스푸핑이 가능하다. 따라서 본 논문에서는 최근 보안 중요성이 대두되고 있는 국가 주요핵심기반시설 내의 SCADA 시스템 보안 향상을 위하여 데이터 스푸핑 탐지를 위한 유휴 시간 측정 시스템을 설계하였다.

Abstract The industrial foundation of the inside and outside of a country has brought significant damages due to attacks from hackers. Especially, if the national primary core infrastructures(like electric power, dam, railroad, atomic energy, etc.) has been significantly damaged, it can be directly linked not only to economic problems but also to people's lives. These national primary core infrastructures usually constitute SCADA system using Modbus RS486 communication. Because of this characteristic, SCADA system has RTU master and slave linked to RJ11 cables to directly pass commands. RJ11 is possible in data spoofing using physical connection because the transmission range of RJ11 has a wide bandwidth(almost 1km). Hence, this paper designed an idle-time measurement system for SCADA system for emerging security improvement in the national primary core infrastructures.

Key Words : Smart Grid, Spoofing, Measurement System, SCADA Security, Industrial Facilities Security

1. 서론

전력망, 철도, 댐 등 국가주요핵심기반시설은 대부분 SCADA(Supervisory Control and Data Acquisition) 시스템으로 관리와 운영이 이루어지고 있다[1]. 이러한 시스템의 특성으로 인해 국가 주요핵심기반시설은 사이버 테러 및 해킹, 바이러스 등의 표적이 되고 있다[2]. SCADA 시스템이 공격당하게 되면 조작 및 통제 권한이 상실하거나, 기기의 오작동이 일어날 수 있으므로 심각한 위험에 빠질 가능성이 크기 때문에 국가 주요핵심기반시설에 대한 보안의 중요성이 부각되고 있다.

SCADA 시스템을 이용하는 국가 주요핵심기반시설 보안의 중요성을 보여주는 두 가지 예로는 2003.1.25 인터넷 침해사고와 알카에다 교육 훈련소에서 발견된 SCADA 관련 정보가 있다. 먼저 2003.1.25 인터넷 침해사고는 슬래머 웜(Slammer Worm)에 의한 것으로 전 세계적으로 심각한 피해를 야기했다. 그 중 하나가 오하이호 Davis-Besse 원자력 발전소 안전 모니터링 시스템이 5

본 논문은 2009년도 산학협동재단 학술연구비 지원과제로 수행되었음.
*교신저자 : 김석수(sskim@hnu.kr)
접수일 09년 11월 01일 수정일 09년 12월 11일 게재확정일 10년 01월 20일

시간 동안이나 중단된 경우이다. 이 원자력 발전소와 같은 대규모 산업 플랜트를 운영하고 관리하는 시스템이 바로 SCADA 시스템이다[3]. 다른 하나는 9.11 테러를 주도한 것으로 알려진 알카에다의 교육 훈련소에서 발견된 컴퓨터에 댐에 관련된 SCADA 정보가 발견되었다[4]. 이처럼 최근 테러의 경향을 보면 점차 SCADA 시스템에 대한 공격으로 집중화되고 있는 것을 알 수 있다.

국가 주요핵심기반시설은 한번 피해가 발생하면 대규모 인명피해 및 국가적 이미지를 손상하게 되는데, 해킹이 고지능화됨에 따라 사이버테러에 대한 대비가 무엇보다 중요하다. 예를 들어 Gartner사가 2004년 1월 발표한 보고서는 철도, 전력망, 발전소, 댐 등의 중요한 인프라 요소의 접속에 사용되고 있는 SCADA 시스템에 대하여 심각한 취약성을 지적하고 있다[5]. 즉, SCADA 시스템은 기술의 발전에 따라 취약성이 더욱 더 높아지고 있으며 앞으로 발생될 국가적인 사이버전의 주공격 대상이 될 것으로 예측하고 있다.

이처럼 국가 주요핵심기반시설은 Modbus RS485통신을 사용하는 SCADA 시스템으로 구성되어 있는 것이 일반적이며, 이러한 특성상 SCADA 시스템에서 직접 명령을 전달하는 RTU Master와 Slave는 RJ11 케이블로 연결되어 있다. RJ11 케이블의 전송 범위는 1km정도로 대역이 넓기 때문에 케이블에 물리적인 접속을 통하여 데이터 스푸핑이 가능하다.

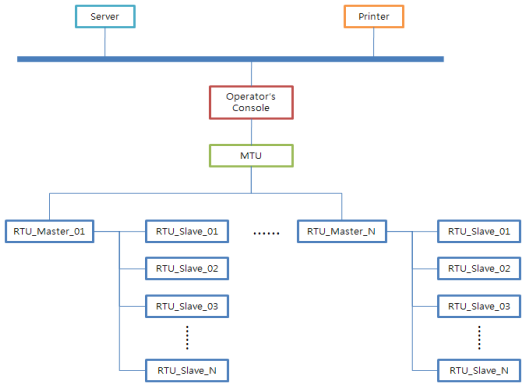
따라서 본 논문에서는 최근 보안 중요성이 대두되고 있는 국가 주요핵심기반시설 내의 SCADA 시스템 보안 향상을 위하여 데이터 스푸핑 탐지를 위한 유휴 시간 측정 시스템을 설계하였다.

2. 관련 연구

2.1 SCADA 시스템

SCADA 시스템은 대개 중앙호스트컴퓨터(Central Host Computers), RTUs (Remote Terminal Units), PLCs (Programmable Logic Controllers) 그리고 Operator Terminals 로 구성되며 Modbus 통신을 이용한다[6].

RTU 중심으로 설명된 전형적인 SCADA 시스템의 구조는 다음과 같다.



[그림 1] SCADA 시스템 구조

그림 1과 같이 현장에서 사용하는 전형적인 SCADA 시스템에서는 해커가 내부망에 접근했을 경우 RS485 멀티 터미널 유닛(MTU)과 RTU 간 Spoofing 공격에 대해 취약성을 보이게 된다.

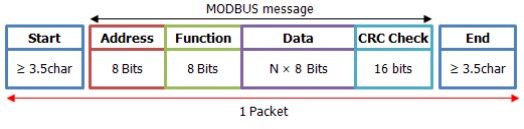
또한 현재 LAN 환경에서 주로 사용하는 TCP/IP 방식과는 다르게 SCADA 시스템에서 사용하는 Modbus 방식은 패킷을 평문으로 전송하고 있기 때문에 그 위험성이 크다.

2.2 Modbus 프로토콜

Modbus는 전 세계적으로 널리 보급되어 있는 자동화 프로토콜의 하나이며, 기존의 RS-232/422/ 485 디바이스를 지원한다. PLC, DCS, HMI, 계측기, 미터 등의 수많은 공업 기기는 Modbus를 통신표준으로 사용하고 있다. Modbus 통신의 종류는 Modbus serial, Modbus plus and Modbus TCP/IP이며, 전송방식은 ASCII 모드와 RTU 모드가 있다[7].

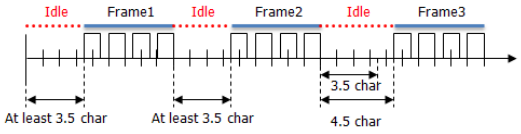
전송방식은 네트워크에 따라 전송된 메시지의 비트 바이트의 내용을 정의하며, 메시지를 스트림으로 패키지화하는 방법 및 메시지 정보를 해독한다. 표준 Modbus 네트워크는 ASCII나 RTU 모드 전송방식 중에서 한 가지를 사용하며, 본 연구에서는 RTU 모드 기반의 탐지 시스템을 설계하였다.

Modbus serial의 종류는 RS232(EIA/TIA-232), RS422, RS485(EIA/TIA-485)가 있으며, Start/End 비트를 포함하는 패킷 구조와 Modbus 메시지 구조는 다음 그림과 같다.



[그림 2] Modbus 메시지와 패킷 구조

Modbus는 RJ11 케이블에 위와 같은 구조의 패킷을 전송하여 데이터를 송/수신한다. 다수 패킷을 송/수신하기 위해서는 3.5~4.5 Char의 유휴 시간(Idle-time)이 필요하며, 그 구조는 다음과 같다.



[그림 3] 패킷 송/수신 구조

만약 패킷 송/수신시 이러한 유휴 시간이 침해를 당하게 되면 전송중인 데이터는 깨지게 된다. 따라서 케이블에 직접적인 외부 공격을 실행할 때, 이러한 문제점을 해결하기 위해서 Man-in-the-Middle 공격을 실행하는데, 그 구조는 다음과 같다.

[그림 4] 물리적 연결을 통한 데이터 변조 구조

Modbus RS485통신을 사용하는 SCADA 시스템의 특성상 RTU Master와 Slave는 RJ11 케이블을 통해 1km까지도 연결될 수 있기 때문에 이러한 케이블에 물리적인 접속을 통하여 데이터를 Sniffing[8]하고 Spoofing하는 것이 가능하다.

이처럼 데이터 스푸핑은 RTU Master와 Slave가 연결된 케이블에 T자형으로 단일 결선을 이루지 않고, RTU Master와 Slave의 송/수신 데이터를 처리할 수 있도록 스레드를 구성한다. 그리고 CRC 처리와 내부 스레드의 데이터 변조가 이루어지는 Man-in-the-Middle 결선 구조에서 주로 이루어지며, 탐지를 위한 기존의 기법에 대해서는 2.3에서 자세히 설명한다.

2.3 기존 탐지 기법

기존의 데이터 스푸핑을 탐지하기 위한 연구로는 Ack-Only 패킷 비율 변화[9]를 측정하는 방법과 MAC 주소를 이용하여 스푸핑 공격을 탐지[10]하는 방법이 있다.

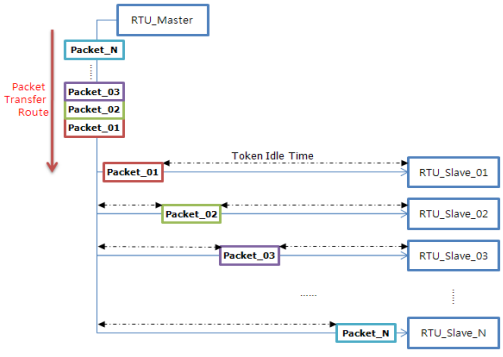
Ack-Only 패킷 비율 변화를 측정하는 방법은 공격 시 크고 급격한 변화를 측정하기 위해 설계되었고, MAC 주소 스푸핑 공격 탐지 방법은 고유한 MAC 주소를 통해 스푸핑 공격을 탐지한다.

본 논문에서는 위 두 가지 기존 탐지 기법과 비교 분석을 통해 효율성을 검증하였다.

3. 실험 환경 구성과 유휴시간 측정 시스템 설계

3.1 취약성 분석

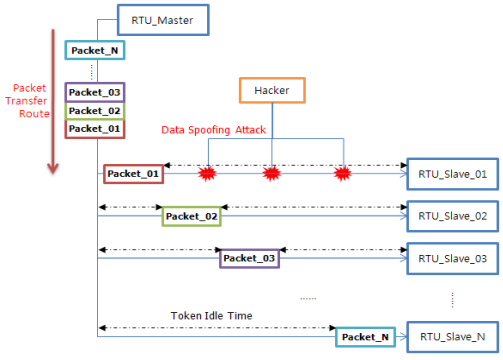
RTU Master는 토큰을 이용하여 각 Slave에 데이터를 전송한다. 이때 패킷이 순차적으로 전송이 되면서 패킷이 전송되지 않을 때에 유휴시간이 발생하게 된다. 이러한 유휴시간은 패킷 내의 데이터에 속해 있는 유휴시간과는 다른 것으로 하나의 간격(Interval)이며, 패킷을 전송하는 과정은 다음 그림과 같다.



[그림 5] 토큰으로 인한 유휴시간 발생

RTU Master와 연결되어 있는 각 Slave들은 모두 동일한 간격의 유휴시간을 갖게 되며, 이 유휴시간을 타깃으로 하여 특정 Slave에 데이터 스푸핑 공격을 시도하게 되면 Slave의 데이터는 변조된다.

유휴시간 데이터 스푸핑 공격 구조는 다음 그림과 같다.



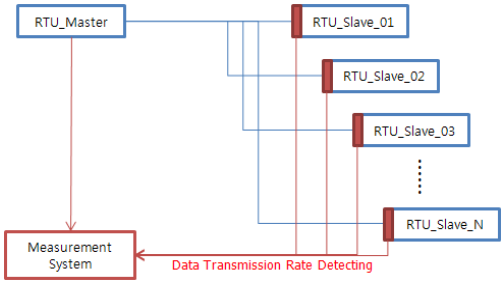
[그림 6] 유휴시간에 데이터 스푸핑 공격

다수의 Slave를 운용할 경우, 이러한 유휴시간은 더 길어지게 되기 때문에 데이터 스푸핑 공격이 가능한 시간 또한 늘어난다.

본 논문에서는 각 Slave에 일정한 유휴시간을 고정 값으로 입력하고, 유휴시간에 데이터 스푸핑 공격이 탐지되었을 때의 유휴시간을 실시간으로 측정할 수 있는 시스템을 구현하였다.

3.2 시스템 구조

유휴시간 측정 시스템의 구조는 RTU Master와 Slave들 간에 연결되어 있는 RJ11에 직접 케이블을 연결하여 패킷이 이동되는 속도를 확인한다. 이때 케이블은 RTU Slave의 전면에 연결하여 최종적으로 패킷이 이동될 때의 시간을 확인하여 측정 시스템과 Slave 사이에 데이터 스푸핑 공격이 일어날 수 없도록 하였다.



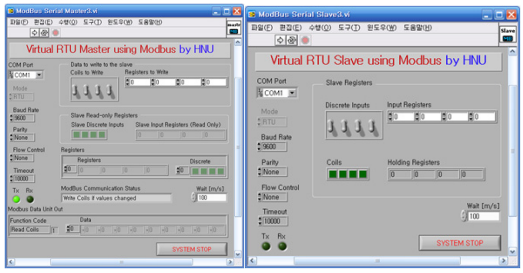
[그림 7] 유휴시간 측정 시스템 구조

3.3 일반적인 RTU 환경 구성

본 연구와 같은 실험 환경에서 H/W 요소를 모두 구비할 수는 없다. 따라서 LabVIEW로 구현된 S/W RTU Master/Slave로 대체하여 구성을 하였다.

실험을 위한 RTU Master와 Slave는 가상 환경 구현 프로그램으로 각 RTU들은 정상적으로 데이터를 송/수신하고 있는 것을 확인할 수 있다. 가상 RTU 환경 구현 프로그램은 Modbus 프로토콜을 사용하여 Function code 01, 02, 03, 04, 15, 16번에 대한 데이터를 송수신한다. 이는 현재 운용되고 있는 국가주요핵심기반시설의 SCADA 시스템에 연결된 RTU와 기능이 같다고 할 수 있다.

정상적으로 연결되어 데이터 송/수신을 하는 화면은 다음과 같다.



[그림 8] S/W RTU_Master(좌)/Slave(우)

3.4 스푸핑 공격 시스템 구현

3대의 PC에 Master, Slave, Intruder를 구성하여 스푸핑 공격 시스템을 구성하였으며, S/W RTU Master/Slave를 현장의 상황에 맞게 구현하기 위해 다음과 같은 요소를 구성하였다.

1. LCS-485 컨버터 4대
2. RJ-11 케이블
3. USB to RS232 케이블 4대

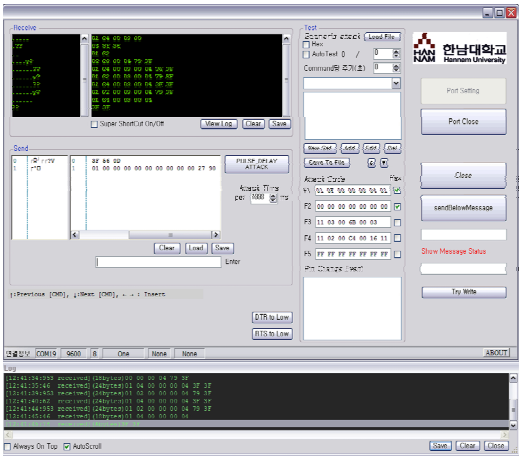
스푸핑 공격 시스템은 Windows XP를 기반으로 하여 C언어로 구성되었으며 핵심 코드는 다음과 같다.

[표 1] 스푸핑 공격 시스템 코드

```
if(gModulateType==MODULATE_ID) {
 Mod_ID = rand()%10+1;
 memcpy(Mod_Buff, Org_Buff, Org_Buff_Len);
 Mod_Buff[0] = (unsigned char)Mod_ID;
}

else if(gModulateType==MODULATE_DATA) {
memcpy(Mod_Buff, Org_Buff, Org_Buff_Len);

if(Org_Buff[1]==0x01 || Org_Buff[1]==0x02) {
 Byte_Cnt = Org_Buff[2];
  for(Loop=0; Loop<Byte_Cnt; Loop++) {
   Mod_Buff[3+Loop] = rand()%255+1;
  }
}

else if(Org_Buff[1]==0x03 || Org_Buff[1]==0x04) {
 Byte_Cnt = Org_Buff[2];
 for(Loop=0; Loop<(Byte_Cnt/2); Loop++) {
  memcpy(&Org_Data, &Org_Buff[3+Loop*2], 2);
  Org_Data=User_htons(Org_Data);
  Mod_Data = rand()%65534+1;
  Mod_Data = User_htons(Mod_Data);
  memcpy(&Mod_Buff[3+Loop*2], &Mod_Data, 2);
 }
}
```

본 시스템의 구성은 크게 모듈레이터 타입을 정의해서 Port Open/Close, Attack, Stop으로 구분되며, 송/수신 데이터 확인을 할 수 있는 Log Print로 가 있다.

화면 구성은 다음과 같다.



[그림 9] 스푸핑 공격 프로그램 UI

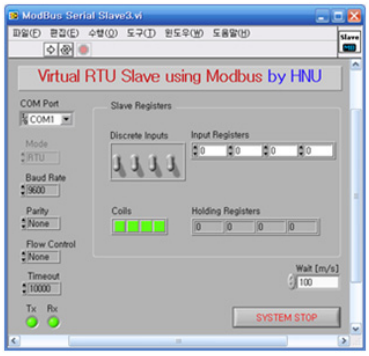
```
[12:58:02:234 port    ]     COM19(9600bps / using None) Opened
[12:58:04:796 received]     (21bytes)01 02 00 00 00 04 79
[12:58:04:812 received]     (3bytes)3F
[12:58:04:843 received]     (24bytes)01 04 00 00 00 04 3F 3F
[12:58:09:734 received]     (24bytes)01 02 00 00 00 04 79 3F
[12:58:09:828 received]     (18bytes)01 04 00 00 00 04
[12:58:09:859 received]     (6bytes)3F 3F
[12:58:14:718 received]     (9bytes)01 02 00
[12:58:14:750 received]     (15bytes)00 00 04 79 3F
[12:58:14:828 received]     (24bytes)01 04 00 00 00 04 3F 3F
[12:58:21:265 received]     (6bytes)01 02
[12:58:21:281 received]     (18bytes)00 00 00 04 79 3F
[12:58:21:375 received]     (6bytes)01 04
[12:58:21:390 received]     (18bytes)00 00 00 04 3F 3F
[12:58:21:718 received]     (21bytes)01 02 00 00 00 04 79
[12:58:21:750 received]     (3bytes)3F
[12:58:21:828 received]     (24bytes)01 04 00 00 00 04 3F 3F
[12:58:22:218 received]     (9bytes)01 02 00
[12:58:22:234 received]     (15bytes)00 00 04 79 3F
[12:58:22:328 received]     (24bytes)01 04 00 00 00 04 3F 3F
[12:58:22:734 received]     (24bytes)01 02 00 00 00 04 79 3F
[12:58:22:812 received]     (3bytes)01
[12:58:22:875 received]     (21bytes)04 00 00 00 04 3F 3F
[12:58:23:218 received]     (24bytes)01 02 00 00 00 04 79 3F
[12:58:23:328 received]     (12bytes)01 04 00 00
[12:58:23:343 received]     (12bytes)00 04 3F 3F
[12:58:23:718 received]     (18bytes)01 02 00 00 00 04
[12:58:23:750 received]     (6bytes)79 3F
```

[그림 10] 송/수신 데이터 확인(Log Print)

이와 같은 데이터 형식은 16진수 Hex코드로 Modbus Function Code를 기준으로 데이터를 분류한다.

정상적으로 동작하는 RTU Master와 Slave 사이에 임의의 실수 값이 입력되도록 데이터 스푸핑 공격을 시도할 경우, RTU는 정상적으로 입력 받던 데이터 값을 표기할 수 없으며 공격된 임의의 값으로 불린(Boolean)이 랜덤하게 출력되게 된다.

공격을 받은 RTU Slave 화면은 다음과 같다.

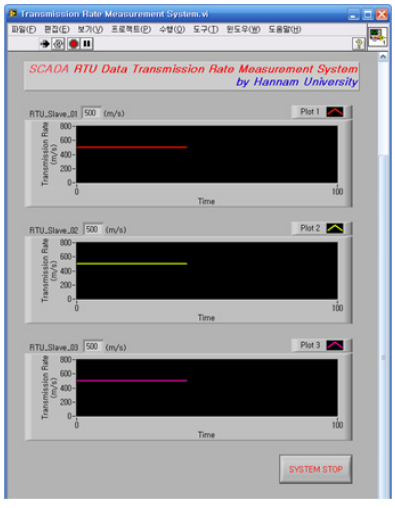


[그림 11] 스푸핑 공격 시 데이터 변화

3.5 유휴시간 측정 시스템

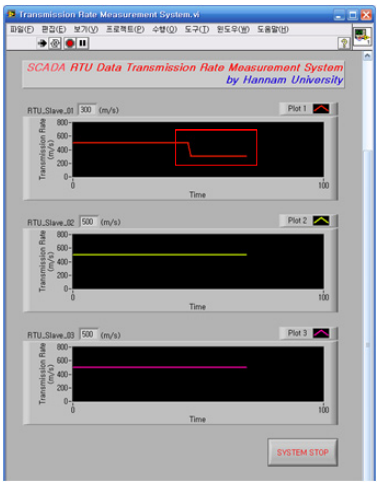
실험 규모는 RTU Master 1대와 RTU Slave 3대를 연결하여 구성하였다. 각 RTU들은 실험속도 관찰을 위해 500m/s의 속도로 데이터를 전송하도록 고정 값을 설정하였다.

구현된 측정 시스템은 다음과 같다.



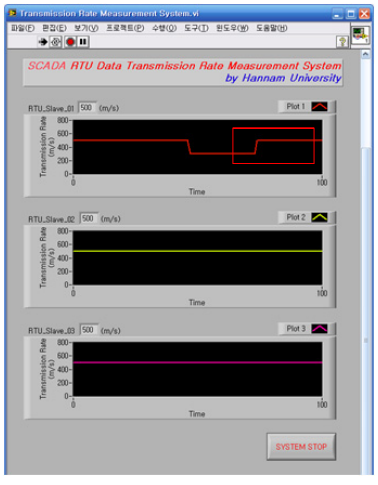
[그림 12] 패킷 전송 속도 측정

500m/s의 정상 속도로 측정될 때, 300m/s의 속도로 데이터 스푸핑 공격을 가하면 다음과 같이 그래프의 출력 값이 변화되는 것을 알 수 있다.



[그림 13] RTU_Slave_01에 스푸핑 공격

스푸핑 공격이 탐지되는 동안에는 실시간으로 측정된 값을 통하여 이를 탐지할 수 있으며, 공격이 정지될 경우 다음과 같이 원래 속도의 500m/s로 복구되는 것을 확인할 수 있다.



[그림 14] RTU_Slave_01에 스푸핑 공격 중지

이처럼 특정 선로에 스푸핑 공격이 탐지 되면 경보 또는 특정 방식으로 모니터링을 담당하는 관리자에 알리고, 관리자는 이를 물리적으로 정지시켜 공격을 차단할 수 있다.

3.6 성능 평가

기존의 데이터 스푸핑을 탐지하기 위한 연구로 Ack-Only 패킷 비율 변화를 측정하는 방법과 MAC 주소를 이용하여 스푸핑 공격을 탐지하는 방법이 있지만, 각 탐지 기법에는 단점이 있는데, 먼저 Ack-Only 패킷 비율 변화를 측정하는 방법은 공격 시 크고 급격한 변화가 아니면 탐지하기 힘들다. 다음으로 MAC 주소 스푸핑 공격 탐지 방법은 MAC 주소가 바뀔 경우 실시간 탐지를 할 수 없다.

[표 2] 탐지 기법 비교

구분 \ 종속성	특정 성향 종속	실시간 탐지
Ack-Only	변화가 작을 경우, 탐지 불가능	가능
MAC Addr	MAC 주소 종속	불가능
Idle-time Measurement	없음	가능

4. 결론

정보통신 기술이 발달함에 따라 해킹 기술도 더불어 발달해오면서 보편화된 공개 프로그램을 이용하여 누구나 해킹 시도를 할 수 있게 되었으며, 이로 인해 보안의 중요성이 높은 국가 주요핵심기반시설에도 피해를 입힐 수 있는 환경이 되었다. 국외의 피해사례에서도 보이듯이 국가 주요핵심기반시설에 피해가 발생하게 되면 피해대상은 해당 시설에 그치는 것이 아니라, 국민의 생명까지도 위협할 수 있을 정도로 범위가 넓다.

이러한 환경에 영향을 받아 국가 주요핵심기반시설의 위협 요소 분석 및 보안관리가 이슈화되고 있으며, 많은 연구가 진행되고 있다.

본 논문에서는 이러한 연구의 일환으로 국가 주요핵심기반시설에서 발생할 수 있는 데이터 스푸핑 탐지를 위한 유휴 시간 측정 시스템을 개발하였다.

본 논문에서 설계한 유휴시간 측정 시스템은 작은 시간 변화에도 공격을 탐지할 수 있으며, MAC 주소에 종속되지 않는 탐지 기법을 제공하여 효율성이 향상되었다. 하지만 본 시스템은 실제 도입하기 위해서는 각 케이블에 측정 케이블을 설치해야 하기 때문에 시간적/비용적인 부분을 고려해야 할 것이다.

향후 연구에서는 케이블을 추가로 설치해야 하는 문제 때문에 실제로 산업에서 활용할 수 있도록 하는 방법을 연구할 것이다. 또한 다수의 RTU의 데이터 속도를 측정할 수 있는 시스템을 구성하여 보다 확장성 있는 시스템을 구현할 것이다.

참고문헌

[1] McClanahan, R.H., “The Benefits of Networked SCADA Systems Utilizing IP-Enabled Networks”, Rural Electric Power Conference, 2002. 2002 IEEE, 5-7 May 2002 Pages: C5 - C5_7.

[2] National Intelligence Service, “2004 The White Paper of National Information Security”, http://www.nis.go.kr, 2004.

[3] Ron Derynck, “Cyber-Security and System Integrity for Transportation Networks, Verono White paper”, 2004.

[4] GAO, “Critical Infrastructure Protection: Challenge and Efforts to Secure Control System”, http://www.gao.gov, Mar. 2004.

[5] David L, Fraley, “Cyberwarfare: VoIP and Convergence Increase Vulnerability”, Gartner Report, http://www.gertnder.com, Jan. 2004.

[6] Technical Information Bulletin 04-1, “Supervisory Control and Data Acquisition (SCADA) Systems”, NCS TIB 04-1, Oct. 2004.

[7] Introduction to MODBUS, Technical Tutorial, Dec. 2002.

[8] What is a packet sniffer?.tech-faq.com.RetrievedonMar.2008.

[9] 서우일, 박현민, 최병석, 박재현, “TCP Connection ARP Spoofing/Hijacking에 대한 탐지 및 추적에 대한 연구”, 정보통신연구진흥원 학술기사, 2000.

[10] 조제경, 이형우, “Access Point 기반 무선 네트워크 환경에서의 MAC Address Spoofing 공격 탐지 및 차단 기법”, 인터넷정보학회논문지 제9권 제4호, 2008.

정 성 모(Sungmo Jung) **[준회원]**

- 2008년 2월 : 한남대학교 멀티미디어학과 (공학사)
- 2008년 3월 ~ 현재 : 한남대학교 멀티미디어공학과 석사과정

<관심분야>
USN, 정보보안, 상황인식, u-Healthcare

송 재 구(Jae-gu Song) **[준회원]**

- 2006년 2월 : 한남대학교 멀티미디어학과 (공학사)
- 2008년 2월 : 한남대학교 멀티미디어학과 (공학석사)
- 2008년 3월 ~ 현재 : 한남대학교 멀티미디어공학과 박사과정

<관심분야>
상황인식, uHealthcare, SCADA, 정보보안, USN

김 태 훈(Taihoon Kim) **[정회원]**

- 1995년 2월 : 성균관 대학교 전기공학과(공학사)
- 1997년 2월 : 성균관 대학교 전기공학과(공학석사)
- 2002년 2월 : 성균관 대학교 전기전자컴퓨터학과(공학박사)
- 2007년 3월 ~ 현재 : 한남대학교 멀티미디어학부 조교수

<관심분야>
대형시스템보안, 정보보증, 보안성평가

소 요 환(Yohwan So) **[정회원]**

- 1992년 2월 : 홍익대학교 회화과 (학사)
- 1995년 2월 : 홍익대학교 서양화과 (석사)
- 1998년 2월 : New York Institute of Technology (석사)
- 2009년 2월 : 홍익대학교 영상학과 (박사수료)
- 2003년 3월 ~ 현재 : 한남대학교 멀티미디어학과 교수

<관심분야>
USN, 영상 클러스터 구축, 영상 특수효과, 렌더링

김 석 수(Seoksoo Kim) **[종신회원]**

- 1989년 2월 : 경남대학교 계산통계학 (이학사)
- 1991년 2월 : 성균관대학교 대학원 (공학석사)
- 1991년 3월 : 정풍물산(주)중앙연구소 주임연구원
- 1997년 3월 : 한국 탑웨어 책임연구원
- 1998년 3월 : 경남 도립 거창전문대학교 교수
- 2000년 3월 : 동양대학교 컴퓨터공학부 교수
- 2002년 2월 : 성균관대학교 대학원 (공학박사)
- 2003년 3월 ~ 현재 : 한남대학교 멀티미디어공학과 교수

<관심분야>
USN, 원격교육 및 교육용 콘텐츠, 의료정보 및 원격진료 솔루션, 웹 시스템 구축 및 전자상거래, 유비쿼터스 보안 및 상황인식, 네트워크 및 보안솔루션, 데이터베이스