Hybrid NIDS for Differential Protection Scheme in Power Transmission Lines

Vishak Muthukumar

Abstract

In the environment of physical system security, implementing security system with the knowledge of the physics of the system to be protected will perform better than existing security system which follows conventional computer security principles [e.g, attack signature].
The physical system under consideration is a transmission line, a Network Intrusion Detection System (NIDS) monitors the activity of the differential protection scheme of the transmission line and raises an alarm for activities which are not following its expected behavior.

Contents

1. Introduction

In the environment of physical system security, implementing security system with the knowledge of the physics of the system to be protected will perform better than existing security system which follows conventional computer security principles [e.g, attack signature].

The physical system may be spread geographically. The functioning of the physical system will include communication of the individual components spread across different geographic locations. So there is a requirement that network needs to be monitored at different locations and is reported to central location for analysis with a better view of the entire system.

To facilitate this, network monitoring programs written using a network based intrusion detection system, BRO IDS, which monitors the traffic between any two nodes of the network. Then these scripts raise alert if any vulnerability is found local to those nodes [any component of the physical system which communicates data to other parts of the system] where they are placed, they also send these monitored packet data to a central security system implemented using BROCCOLI [BRO Client Communication Library]. In Broccoli, the packet details are further analyzed collectively to identify higher level attacks [Like coordinated attacks, multistage attacks].

A prototype is implemented for ‘The differential protection scheme’ to protect an electrical power transmission line from faults/over currents. The details of the physical system are explained in section 2. Section 3 discuss about the various stages of the security system built. Section 5 is the screenshots of the results obtained after implementation.

2. Differential Protection scheme

The physical system to be protected is a transmission line.

A differential protection scheme compares the phase values at two points in the line and a difference in the phase values imply a fault in the line.

We used two relays connected to circuit breakers to measure the phase difference. A positive phase difference signifies an internal fault where the Circuit breakers isolate the transmission line from transmission system.

One of the relays is master [Relay 2] and the other relay is the slave. The master polls the slave for the phase value, then compares the phase values and if there is a phase difference, it then signifies an internal fault. The CB in the master will be turned ON and a signal is sent to slave to turn on its circuit breaker thus protecting the transmission line from fault.

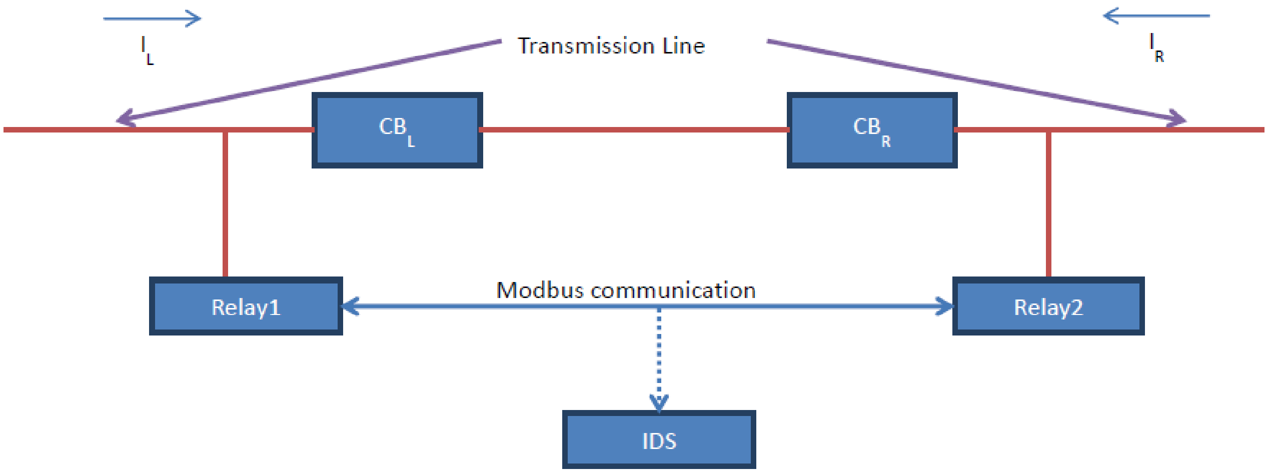


Figure 2 Automata of the security system for differential protection scheme

3 Security System

A security system is developed for a "differential protection scheme" discussed in the previous section.

The system has two stages-

1. The local BRO scripts monitoring the traffic between at relays analyze the packet for simple errors like protocol violation.
2. Broccoli has the knowledge of the physical process of the system, it understand what happens to the physical system for different commands being exchanged by the PLCs. So the broccoli, after getting the packet data from all the local BRO scripts, checks for vulnerabilities for the physical system level

The two stages are explained in detail below--

3.1. Local Analysis

The local BRO scripts monitoring the traffic between relays analyze the packet for simple vulnerabilities [e.g, a response without a request]. These scripts don't have the knowledge about the physical system. State of the system is not maintained for this analysis. Deeper analysis is always done in the broccoli with the knowledge of the packets from all other parts of the physical system.

Local Analysis covers the following alerts –

1. **Read Device Information** - A device can send a modbus packet with function code 43 to read slave device information. By this way an anonymous node with IP connectivity to the network can fabricate a modbus message to understand vendor product, version number.

2. **Read Server information** – A device can send a modbus packet with function code 17 to read server information.

3. **Slave Device Busy** – An attacker postpones any attack by fabricating a modbus packet with exception code 6 "Device Busy".

4. **Possible DOS** – If a packet of size greater than maximum size of a modbus message is observed, it means that the packet is not being sent by a PLC, this can be a possible DOS attack.

3.2. Security System by the master Broccoli

The master Broccoli system has the knowledge of the physical system based on stage-1. The master checks for the following vulnerabilities in the physical system –

1. **Intruder identification** – The broccoli looks up the network map built in stage 1 and checks whether the IP address of the sender and receiver is in the legitimate device list.
2. **Protocol recognition** – The protocol of the communication traffic is checked for modbus protocol.
3. **Anomalous modbus Request** – If there is any modbus request by a node other than master [data available in the map], there is a vulnerability since only modbus master can make a request.
4. **Malfunctioning over current LED -** If over Current Led 'On' When There Is No Over Current, an adversary could have tampered with the functioning of over current LED or the sensor values.
5. **Error in ordering of packets -**There is a specific order of modbus packets, if that order is not followed, there is a possible attacker trying for network Reconnaissance.
6. **Mismatch of Number of coils from read/write request** -- An attacker can possibly spoof the IP address of master and send modbus/TCP request, so the number and address of coils requested to read/write is checked with the physical system.
7. **Illegal data request** -- Only master can generate a read/write request. Since the IP address of the master is known beforehand, so a request from an IP other than master should raise an alert.

4. Implementation [Screenshots]

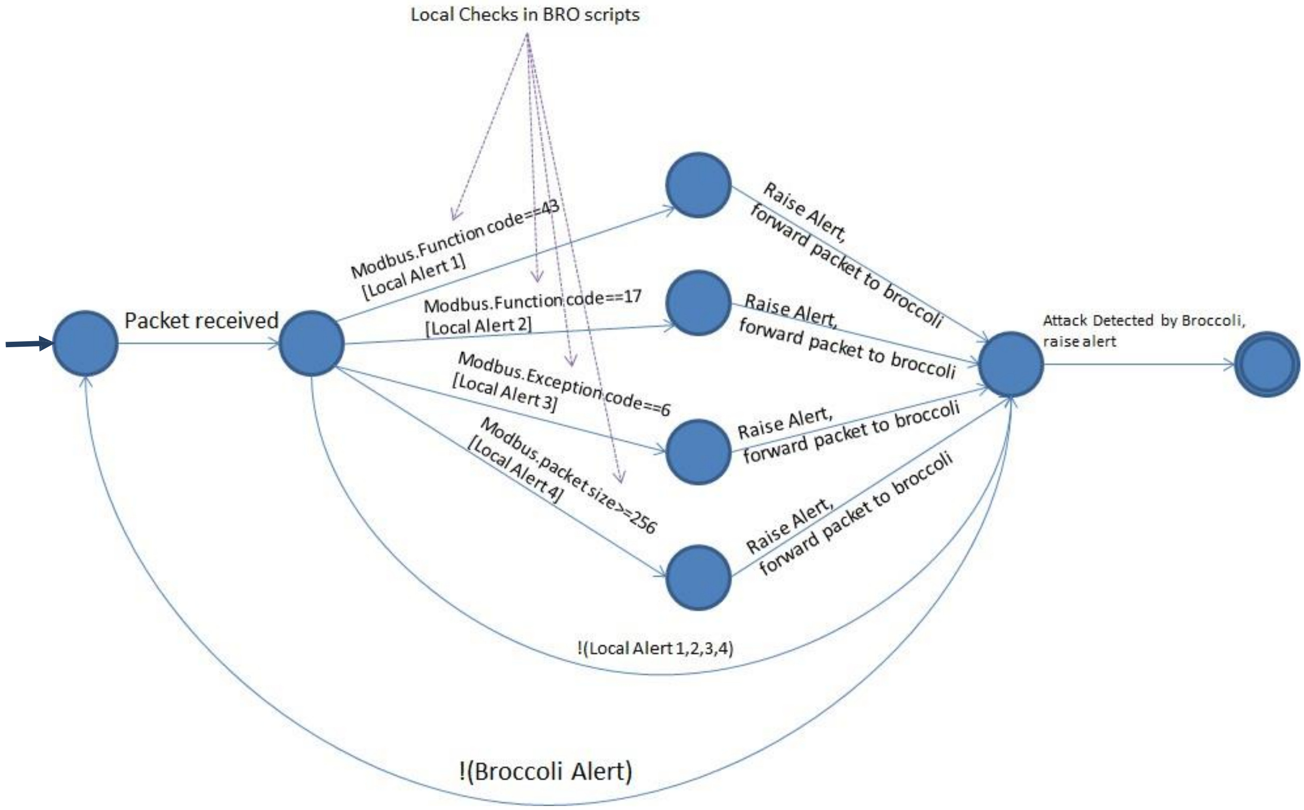
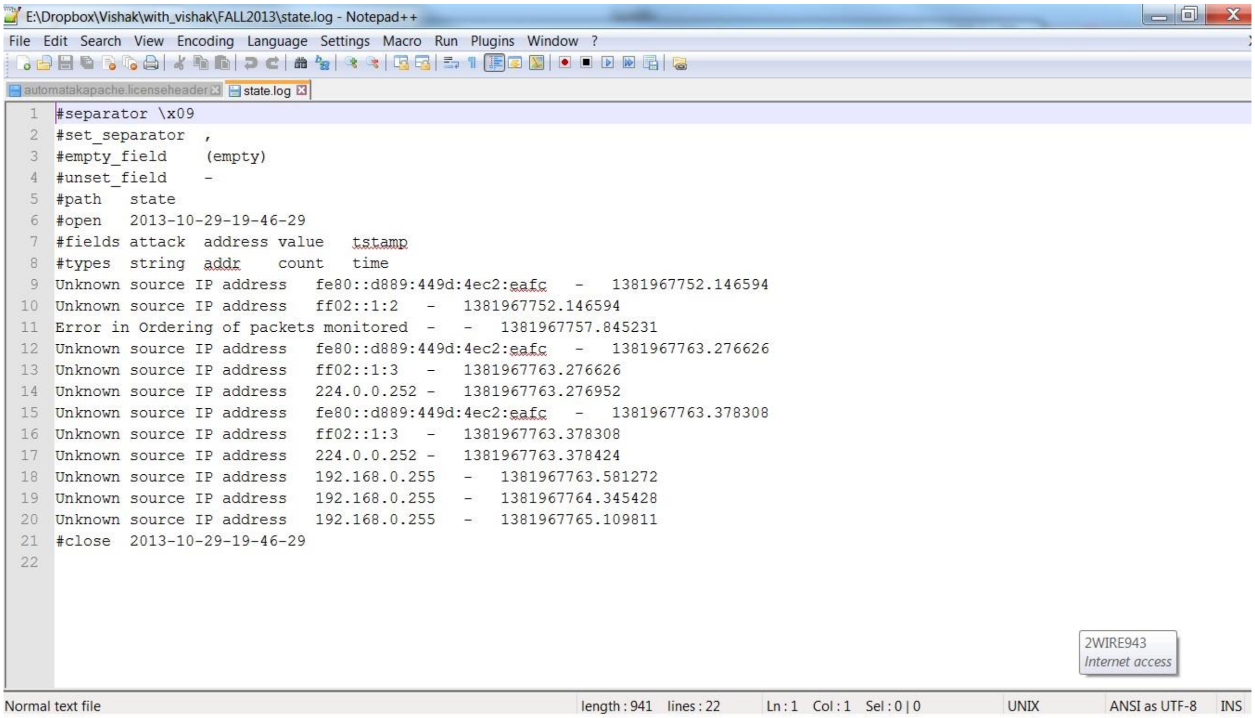


Figure 2 Automata of the security system for differential protection scheme



```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   state
#open   2013-10-29-19-46-29
#fields attack  address value   tstamp
#types  string  addr    count   time
Unknown source IP address   fe80::d889:449d:4ec2:eafc   -   1381967752.146594
Unknown source IP address   ff02::1:2   -   1381967752.146594
Error in Ordering of packets monitored  -   -   1381967757.845231
Unknown source IP address   fe80::d889:449d:4ec2:eafc   -   1381967763.276626
Unknown source IP address   ff02::1:3   -   1381967763.276626
Unknown source IP address   224.0.0.252 -   1381967763.276952
Unknown source IP address   fe80::d889:449d:4ec2:eafc   -   1381967763.378308
Unknown source IP address   ff02::1:3   -   1381967763.378308
Unknown source IP address   224.0.0.252 -   1381967763.378424
Unknown source IP address   192.168.0.255   -   1381967763.581272
Unknown source IP address   192.168.0.255   -   1381967764.345428
Unknown source IP address   192.168.0.255   -   1381967765.109811
#close  2013-10-29-19-46-29
```

Figure 3 Log of alerts recorded by BRO scripts