Improving SCADA Security using IDS and MikroTIK

Albert Sagala and Rudy Pardosi
Del Institute of Technology, Toba Samosir, North Sumatera, Indonesia.
albert@del.ac.id

Abstract**—Industries have realized that SCADA System was built without considering the security aspect. It was believed that there are no attacks to the scada plant. Unfortunately, in this era, SCADA network needs to be connected to the Internet to increase its performance. In this case, the protection of Supervisory Control and Data Acquisition (SCADA) is needed against cyber-attacks. Much research has seen the big lost as cyber-attack happens at critical infrastructure. In this research, we simulated a test bed environment of SCADA system to monitor and mitigate the attack as well as give fast response report to the operator. We used Network Based Intrusion Detection System using SNORT rule, which is integrated with MikroTik for Deep Packet Inspection (DPI). This system inspects all traffic data going through the scada system. Results from the experiment show that the testbed environment was able to detect attacks effectively and efficiently.**

Index Terms**—DDoS Attack; MikroTik Router; SNORT, SCADA Security.**

I. Introduction

Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) is built in isolated system to secure the plant [1], [2], [8]. However, the system for the next generation of SCADA needs to be accessed from anywhere using the internet connection. This fact can be seen with the emerging of Internet of Things (IoT) technology. Things are connected to and communicate with each other to do the job as provided by the command. SCADA integrated with the office network makes it more susceptible to be attacked by a hacker [10], [14]. We know that the advanced hacking technique is evolving to crack the system and there is a need to anticipate this issue in the SCADA plant.

To enhance the SCADA security, while getting it connected to the Internet, we integrated the technology of MikroTik IDS (Intrusion Detection System) using CALEA Configuration, iptables firewall, and a SNORBY interface, which can be used as a new tool to monitor traffic data coming into the controller. For this purpose, we have made some changes to the previous SCADA topology. Researches that use IDS system to enhance the security have already been conducted by many researcher from many universities [4],[6][13].

Changes in the topology are needed to integrate Network Based IDS (NIDS) and MikroTik. These topology changes are based on the research that has already ben conducted to secure the scada system [9],[11],[12]. *Trafr* packet sniffing was installed on SNORT server. MikroTik helps the SNORT server, detects or monitors the network traffic passively. We installed SNORBY as a graphical user interface (GUI) for operator's easy usage.

Our contribution in this paper is to give a solution to improve scada security by integrating SNORT IDS Sensor and Packet Inspection using MikroTik.

The rest of the paper is organized as follows: Section II discusses the related work of our research and the experimental environment. Section III explains the network topology of our system in more detail. Section IV elaborates the result and an analysis, and we conclude in Section V.

II. Experimental

The SCADA security can be improved using many methods. Many researches were conducted to develop the design of a testbed environment to make an easy testing of the scada [9],[11]. In this research, the modbus protocol [15] used for communication between the HMI and the controller is excluded to enhance the security. Our previous research has already proposed a method to enhance the security using the modbus protocol.

On [5], Raspberry PI was used as a gateway to encryp and decrypt the communication from HMI to the controller. While, in [3], in order to improve cyber-security of SCADA networks, research presented a rule-based Intrusion Detection System (IDS) using a Deep Packet Inspection (DPI) method, which includes signature-based and model-based approaches tailored for SCADA systems. The proposed signature-based rules can accurately detect several known suspicious or malicious attacks.

In our research, the environment needs to be prepared well for anticipating internal or external attacker. These section will explore the environment proposed as a method to increase the SCADA security.

A. Testbed Environment SCADA Security

The experiment was conducted on a SCADA tesbed designed as shown in Figure 1. We extended the network using a MikroTik device to increase the plant. In the attack scenario, an adversary may compromise a system on the workstation network typically connected to the internet. From there, the attacker gains access to the MikroTik router, then infects the SCADA Operator, and finally performs reconnaissance, before continuing with the ethical-hacking steps.

As depicted in Figure 2, we put the sensor using Inline mode Sensor [7], where it must be placed in line with the firewall and other network security devices to monitor actual network traffic. Table 1 shows the hardware and software specification for our tesbed.

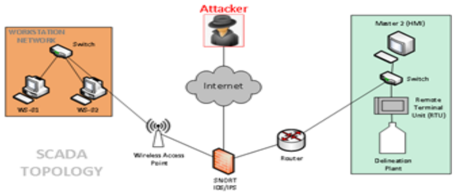


Figure 1: Testbed Environment of Secured SCADA Topology Using IDS-Mikrotik

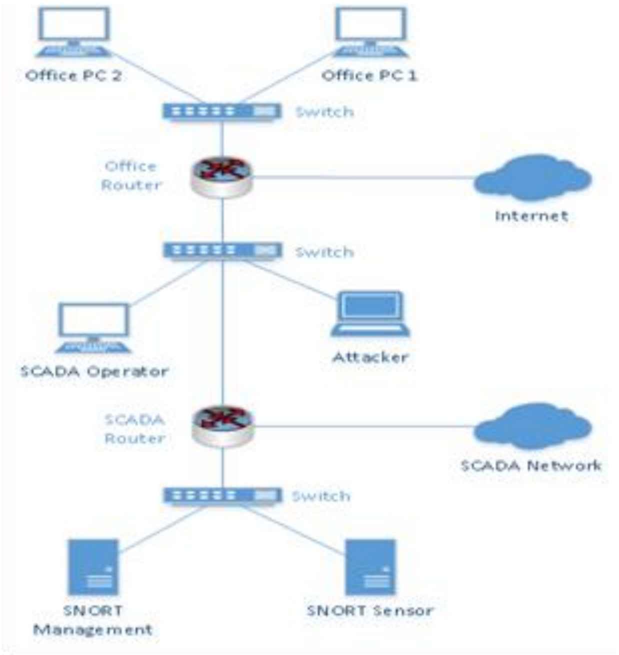


Figure 2: Inline Architecture of Sensor Mode

Table 1
Devices and IP Address

Device Name	IP Address	Operating System	Device Type
SCADA Operator	192.168.10.2	Windows XP	Client
Attacker	192.168.10.106	Kali Linux	Client
Snort Sensor	169.254.213.6	Ubuntu 10.04	Sensor
Database Snort Server	169.254.213.5	Security Onion	Server
Water Plant	169.254.213.2	PLC Controller	Plant
Router MikroTik	169.254.213.1	RouterOS RB951	Access Point

B. *Setting the MikroTIK Firewall and Packet Sniffing*

In the configuration of Mikrotik, we can access the setting via HTTP protocol on port 80. MikroTik Wireless Access Point (WAP) should be activated because it will connect to our SCADA plant. Packet sniffing mode in MikroTik should be activated to make it as sniffer mode, and then it will forward the packet to be analyzed by SNORT server.

C. *SNORT Rules*

In this part, we make a general DDOS rules of SNORT, which can detect TCP SYN flood attack from any port launched by the attacker. When the SNORT server detect the DDoS attack, it will send a trigger to the operator.

```
alert tcp any any → $HOME_NET any (msg: "TCP SYN
Flood Attack Detected !!"; flow:stateless; flags:S,12;
threshold:type threshold, track by_src, count 3, seconds
1; classtype: attempted-recon;sid:10002; rev:1;)
```

D. *Packet Filtering on Ubuntu*

Next, we set the IPTables packet filter so that it can accept the forwarding packet from MikroTIK on port 37008.

```
root@ubuntu:~# iptables –I INPUT 50 –p udp –
dport 37008 -j ACCEPT –n CONNECT comment
"Accept sniffed traffic from ROUTERBOARD"
```

E. *CALEA Client Configuration*

Communications Assistance for Law Enforcement Act (CALEA) requires the routers in the USA to have the ability to intercept and log the network traffic. Currently, RouterOS provides this facility by means of firewall rules. RouterOS can also function as a data retention server if the additional CALEA package is installed. The first step involves downloading the TRAFR archive file. The program will be used to encapsulate the packet sent by CALEA MikroTIK. After that, we extract the archive file and then, we start the trafr program to test the receiving packet from CALEA.

To activate TRAFR with SNORT, this command is entered:

```
root@ubuntu:~# ./trafr -s | snort -r -
root@ubuntu:~#./trafr -s | tcpdump -r - -n
root@ubuntu:~#./trafr -s | snort -c /etc/snort/snort.conf
root@ubuntu:~# –l /var/log/snort/ -r -
```

If the output messages that confirm the settings and rules are loaded successfully, the operator needs to wait few minutes before stopping the process with Control + C. If the statistics show a number different from 0, it means that Snort works well with Trafr. Snort must start as a process that cannot be demonized because of Trafr data injection. This means that the operator needs to run it directly on a console or use a tool like "screen" and then run Snort with Trafr. The last line instructs Snort to use a specified configuration and log path. All of the traffic that go through the router for a specified source/destination addresses was intercepted and sent to CALEA Server (sniff-target).

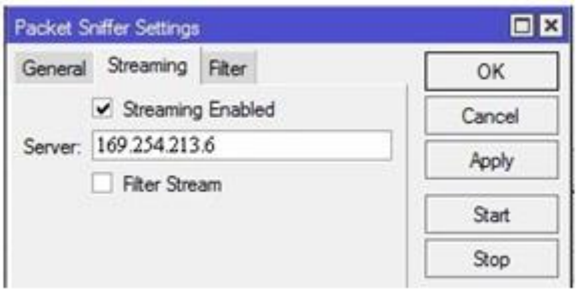
```
[admin@MikroTik] > ip firewall calea print
Flags: X – disabled , I – invalid , D – dynamic
```

```
[admin@MikroTik] > ip firewall calea add
action=sniff chain=forward sniff-target=169.254.213.6
sniff-target-port=37008 sniff-id=100.
```

Set up the Streaming Configuration for MikroTik to accept the entire data stream on Packet Sniffer Settings.

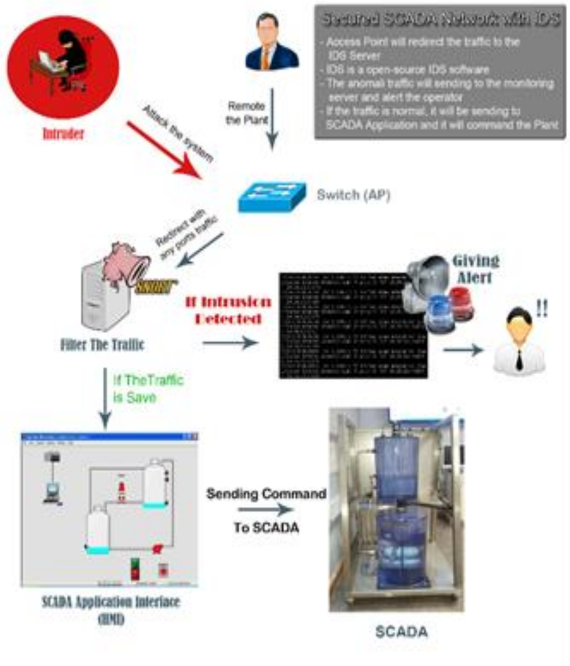
III. Results And Discussion

We conducted testing on the environment that we prepared. The HMI can monitor and control the plant. We added the Intruder to assess the topology proposed.



☑ Streaming Enabled
Server: 169.254.213.6
□ Filter Stream

Figure 3: MikroTik Settings for Packet Sniffer



Secured SCADA Network with IDS
- Access Point will redirect the traffic to the IDS Server
- IDS is a open-source IDS software
- The anomali traffic will sending to the monitoring server and alert the operator
- If the traffic is normal, it will be sending to SCADA Application and it will command the Plant

Figure 4: IDS Phase Snort on SCADA System

The steps taken for the implementation are in the configuration of SNORT and MikroTIK configuration, and setting the Network Topology. We used TRAFR for tcpdump translate from the MikroTIK to SNORT server. Installation and configuration were done using Ubuntu 12.04 TLS operating system server. DDoS attack was trained using HPING3 tools, in which the traffic was sniffed by SNORT server to forward to MikroTIK.

A. Testing DDoS Attack on SCADA

The attack was conducted by sending a TCP SYN flood packet with a header size with 120 bytes of data on its protocol_header. Data will be sent up to 10000 of data in windows 64 bit ID. Protocol attacked is an active port of SCADA controller, in this case is the port 80. If the intrusion that goes across the MikroTik is detected, then it will send the message to the server monitoring which gives alert message to the operator.

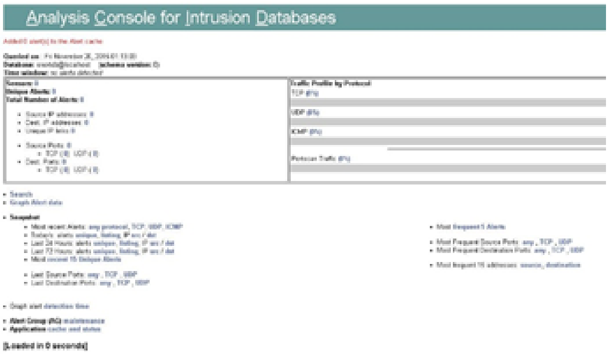
B. Graphical User Interface BASE and ACID

Analyzing the traffic that comes from another system is used by BASE (Basic Analysis and Security Engine) and ACID (Analysis Console for Intrusion Databases). They have a web interface to see the graphical statistic of the traffic. We can set and install the application on the sensor server in Ubuntu 10.04 Lucid environment. The interface is as shown in Figure 5 and 6.

Basic Analysis and Security Engine (BASE)

Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)
Portscan Traffic (0%)

Figure 5: BASE Interface that access from the browser



Analysis Console for Intrusion Databases

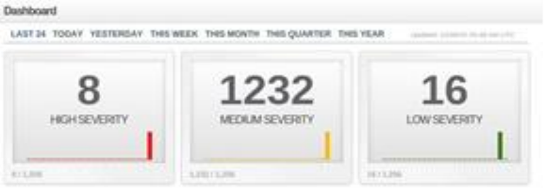
Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)
Portscan Traffic (0%)

[Loaded in 0 seconds]

Figure 6: BASE Interface that access from the browser

C. Alert to Operator From SNORBY

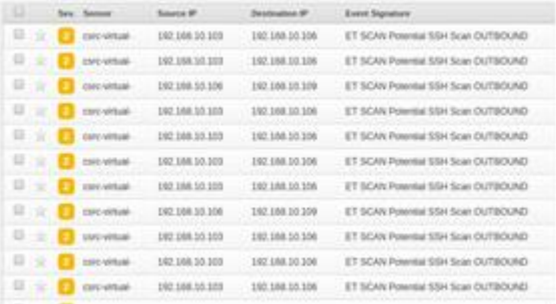
SNORBY has event report and history for the traffic analyzer. SNORBY can separate three severity events of the event data traffic on the network. The report will be shown on the dashboard as can be seen in Figure 7.



8 HIGH SEVERITY
1232 MEDIUM SEVERITY
16 LOW SEVERITY

Figure 7: Graphical User Interface (GUI) On Attack Detection Using SNORBY

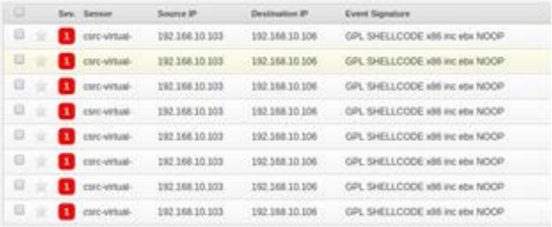
If we want to see the detail of the event, we click the Severity Interface, and the detail of the event will be shown as presented in Figure 8.



Sev.	Sensor	Source IP	Destination IP	Event Signature
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.106	192.168.10.109	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.106	192.168.10.109	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND
2	csrc-virtual	192.168.10.103	192.168.10.106	ET SCAN Potential SSH Scan OUTBOUND

Figure 8: Medium Thread for Alert on Event Log

The most important event was High Severity event, As shown in Figure 9, these categories must be highly concerned because it is categorized for a high risk attack.



Sev.	Sensor	Source IP	Destination IP	Event Signature
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP
1	csrc-virtual-	192.168.10.103	192.168.10.106	GPL SHELLCODE x86 inc ebx NOOP

Figure 9: High Thread for Alert on Event Log

For every detail event, it has more specific information as shown in Figure 10.

Figure 10: Event Detail on SNORBY Detection Log

The proposed integrated method will give rich information to the operator, so the anomaly traffic can be detected early and the data have more detailed information from the MikroTik or SNORT Server. In MikroTik, MRTG was activated to see live traffic.

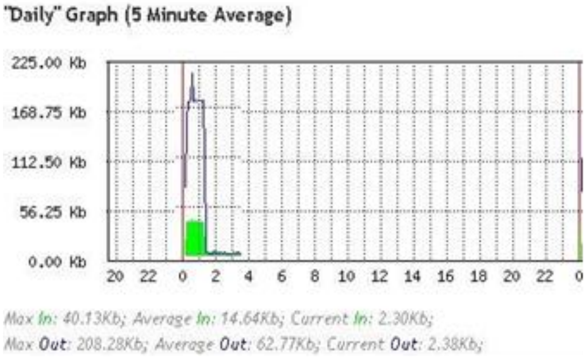
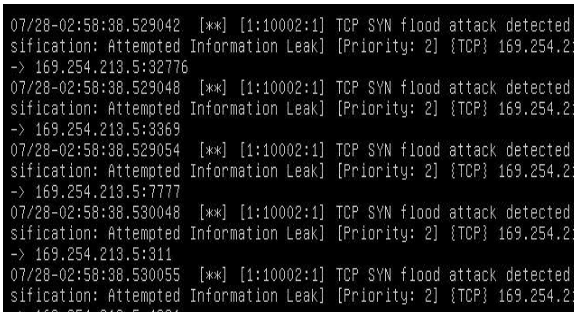


Figure 11: MikroTik Graph For Data Traffic in SCADA Network

Figure 11 shows the graphic when DDoS attack was executed. In a short period of time, the traffic increased very fast and slower after the DDoS stopped. The attack was used by hping3 tools. As shown in Figure 12, the alert was sent to the operator.



```
07/28-02:58:38.529042  [**] [1:10002:1] TCP SYN flood attack detected
sification: Attempted Information Leak] [Priority: 2] {TCP} 169.254.2
-> 169.254.213.5:32776
07/28-02:58:38.529048  [**] [1:10002:1] TCP SYN flood attack detected
sification: Attempted Information Leak] [Priority: 2] {TCP} 169.254.2
-> 169.254.213.5:3369
07/28-02:58:38.529054  [**] [1:10002:1] TCP SYN flood attack detected
sification: Attempted Information Leak] [Priority: 2] {TCP} 169.254.2
-> 169.254.213.5:7777
07/28-02:58:38.530048  [**] [1:10002:1] TCP SYN flood attack detected
sification: Attempted Information Leak] [Priority: 2] {TCP} 169.254.2
-> 169.254.213.5:311
07/28-02:58:38.530055  [**] [1:10002:1] TCP SYN flood attack detected
sification: Attempted Information Leak] [Priority: 2] {TCP} 169.254.2
```

Figure 11: SNORT Alert on Console Interface When Attack Has Been Detected

IV. CONCLUSION

A DDoS-like attack was simulated on SCADA system and the effects of attacks were observed by implementing the IDS and MikroTik. While the effects of the total communication disruption might have been estimated and mitigated by using IDS SNORT. DDoS attack can be detected if the router in sniffing mode and SNORT can classify the packet that came in. In such a case, a simulation is the best way to estimate the detection of these IDS. The difference of this method with another method is that the IDS is combined with MikroTik. The iptables only allows the traffic from MikroTik, and IDS effectively detects the traffic to SCADA system.

In our simulation, we used a general rule attack, which is DDoS. Hacker can modify the technique and attack to avoid the firewall or Intrusion Detection System; hence it still needs further research to enrich the rule tested.

ACKNOWLEDGMENT

We are grateful for the support from Lab Cyber Security Research Centre of Del Institute of Technology for using SCADA plant to make this experiment feasible.

REFERENCES

[1] Keith Stouffer, Joe Falco, Karent Kent., "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security", *National Institute of Standards and Technology (NIST*), 2006.

[2] Patel C., Ganesh Bhatt D., James Graham H., "Improving the Cyber Security of SCADA Communication Networks", *Communication*, vol.52, no.7, 2009, pp.139-142.

[3] Yang Y., Power and Energy Society General Meeting (PES), IEEE. Intrusion Detection System for IEC 60870-5-104 based SCADA networks, Queen's University, 2013

[4] Zouheir Trabelsi, Walid Ibrahim., "A Hands-on Approach for Teaching Denial of Service Attacks: A Case Study", *College of Information Technology*, 2013.

[5] Albert Sagala, Deni Lumbantoruan, Epelin Manurung, Iroma Situmorang, Adi Gunawan., IAES, "Secured Communication Among HMI and Controller Using RC-4 Algorithm and Raspberry Pi", *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol.15, no.3, 2015.

[6] Rohan Chabukswar, Bruno Sinopoli, "Simulation of Network Attacks on SCADA Systems", *University of California Berkeley*, 2012.

[7] Miguel A.Calvo Moya, "Analysis and Evaluation of the Snort and Bro Network Intrusion Detection Systems", *Universidad Pontificia Comillas*, 2006.

[8] Eric D.Knap, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", *Syngress Elsevier*, 2011.

[9] Hahn.A., Ashok.A., and Sridhar S., "Cyber-Physical Security Sandboxs:Architecture, Application, and Evaluation for Smart Grid", *IEEE Transaction on Smart Grid*, vol.4, no.2, 2013.

[10] Falco J., Gilsinn J., and Stouffer K., "IT Security for Industrial Control Systems: Requirements Specification and Performance Testing", *2004 NDIA Homeland Security Symposium & Exhibition*, Crystal City, VA, 2004.

[11] Lemay. A, Fernandez. J, Knight. S, "An isolated virtual cluster for SCADA network security research", *Proceeding of the 1st International Symposium for ICS &SCADA Cyber Security Research*, 2013.

[12] RBarbosa R.R., Sadre R., and Pras A., "A First Look into SCADA Network Traffic", in *IEEE/IFIP Network Operations and Management Symposium (NOMS 2012)*,Springer, 17: 6, 2012.

[13] Steven Cheung, et al, "Using Model-based Intrusion Detection for SCADA Networks", *SRI International, Computer Science Laboratory*, 2006.

[14] Giani. A, Sastry. S, Karl H. J., and Sandberd H., "The VIKING Project: An Initiative on Resilent Control of Power Networks", *KTH University*, Sweden, 2012.

[15] Dutertre B., "Formal modeling and analysis of the Modbus protocol", Technical report*, Computer Science Laboratory, SRI International*, 2006.