Detecting Network Attack Vectors on SCADA Specific Network Operating On Modbus TCP/IP Protocol

[1]Neel H. Pathak, [2]Prof. H. B. Patel
[1]M.E. Research Student, [2]Assistant Professor
[1]Department of Computer Engineering
[1]Gujarat Technological University, PG School, Ahmedabad, India.
[1]neel.pathak@yahoo.com, [2]hasmukh.patel@lcit.org

***Abstract*—Supervisory Control and Data Acquisition (SCADA) systems, a part of Industrial Control Systems (ICS) are widely used for automation and control in many industry sectors, chemical plants, electric power grids, oil and gas plants etc. Traditionally these (i.e. SCADA) systems were operated in standalone manner, typically housed within the industries, chemical plants etc. However, due to the expansion of business and the need to centrally monitor and control these systems, they are now being connected to a completely alien world, the world of Internet. Naturally, as these systems are now being connected to the internet, they are prone to plethora of attacks prevailing on internet. Much research is being carried out to detect and mitigate the effect of network attacks on SCADA specific networks but, one must also consider the significance of attacks done inside the secured periphery of the controlled systems, called as "insider attacks". One can imagine the consequences if such critical infrastructure are tempered or illegally gained control of. If someone tries to gain control over some of the Servers or hacks into someone`s system through internet then the loss would be either financial and/or business function. However, when SCADA systems are compromised then the loss would not just be financial and/or business function but also THE LOSS OF LIFE.**

***Index Terms*—Internal and External Networks, SCADA Systems, SCADA network, Modbus TCP/IP Protocol, Network Intrusion Detection System**

I. INTRODUCTION

Let us first start with the brief introduction of SCADA Systems. Supervisory Control and Data Acquisition (SCADA) systems are considered as one of the types among various Industrial Control Systems (ICS). These systems refer to the combination of telemetry (i.e. communication) and data acquisition. Before moving further lets first understand the terms telemetry and data acquisition.

Telemetry [1]: As the name suggests, telemetry is used for the communications between RTU`s and MTU`s. The communication medium can be Ethernet, Radio Links or telephone etc. The information used in communication are actually control signals that are transmitted and received between RTU`s and MTU`s. These control signals can be measurements, such as speed, voltage or flow.

Data Acquisition [1]: This actually refers to the technique or method which is employed to access or poll data or information from the field devices being monitored and controlled. These data are then given to the telemetry system which is ready to transmit the data to various sites. Data can be either in analog or digital form. Some might get confused between DCS systems and SCADA systems. There is just a minor difference between these two. DCS`s are employed within more restricted or confined area and forms a closed loop for their operation. These uses high-speed communications medium like LAN. On the other hand SCADA systems have no such confined network boundaries and covers large geographical areas. Communication between such SCADA systems takes place by communications links such as radio and wireless networks.

Thus, we can say that these are basically control systems that are connected to the network. Such systems find their major applications in Power grid, chemical plants, oil and gas plants, public transports and utilities etc.

Now let's discuss underlying problem in SCADA system and/or Network. Unlike early SCADA systems, nowadays SCADA systems are connected to the network of networks i.e. the Internet. This is due to growing business needs and convenience in handling such systems from some central location. But as we know according to the security, functionalities and ease of use triangle, if we are near to the ease of use then we lack security and some of the functionalities. In fact SCADA systems were designed not focusing security in mind so there shall be some ways to keep it apart from emerging vulnerabilities and threats. As SCADA systems are considered as most critical control systems and an important asset to any Nation`s economy.

So, there is a rising concern to protect such systems both physically and logically. Such systems being connected to the Internet get exposed to the plethora of attacks already prevailing on the Internet. Despite of extensive research being carried out to detect such type of attacks and prevent/mitigate its effect there has always been security incidents taking place every now and then. The

main reason behind this is that we fail to remember the attacks that are done within the secured periphery of the controlled systems, called as "insider attacks". As these systems lack many security mechanisms such as authentication, non-repudiation, integrity etc. Thus any insider can easily cause damage to these controlled SCADA systems by sending malicious control messages to either MTU or RTU. An insider may also open the path for any external malicious person to attack such critical systems. We must consider this issue to be one of the many issues of the paramount importance. In this paper, we propose a mechanism to detect such security incidents happening both in an internal network and from an external network thereby, contributing to a safer society as whole.

The entire paper is divided into various sections in accordance with their relative content and their importance. **Section 2** sheds light on some background in the field of SCADA System/Network. **Section 3** briefly mentions the related work done in the field of Network Attacks detection on SCADA network. **Section 4** distinguishes between traditional I.T. network and SCADA network and also discusses why we chose Network Intrusion Detection System to mitigate the network attacks vectors on SCADA Network. In **section 5** we have explained the Modbus TCP/IP protocol as the entire research for detecting network attacks is based on the SCADA network operating on Modbus TCP/IP protocol. **Section 6** covers our proposed mechanism which detects network attack vectors both within Internal Network and External Network respectively. Comparison, Analysis and Results of our proposed mechanism are mentioned in **section 7**. And finally we conclude our research with a brief conclusion.

II. BACKGROUND

SCADA systems/networks, a vast topic in itself can`t be explored completely in this paper. So, we thought of touching the core security mechanisms in this section. Though our main focus is on Network Intrusion Detection Systems on SCADA Network.

SCADA systems being a critical infrastructure system for any Nation are of the prime target for cyber terrorists, hackers and state sponsored attacks done by security professionals. If we talk about the security incidents happened on such systems, then the first ever incident that took place was Siberian Pipeline Explosion in 1982 [2]. After this there were series of incidents that took place. All these caused a big financial loss but some of them even caused casualties and even loss of life. Some incidents that caused casualties and loss of life were Bellingham, WA Gas Pipeline in 1999 and Slammer worm on CSX Corporation in 2003. Recent incidents that took place includes Nuclear Iran`s power plant 2010 [2], project night dragon, duqu and flame.

These systems while connected to the internet get exposed to the same kind of attacks as business systems are exposed to. But unlike business systems these systems behaves differently when some sort of security is applied to them [2]. It is hard to believe that when some sort of blended attack is made on particular target then the database figures for SCADA systems can also be changed. There is a long debate carried out in InfoSec world about the manipulation of the figures of the stadium at Delhi during Common Wealth Games (CWG) that recently happened in India [3].

As SCADA network lacks many security features so, needless to say that there is much research being carried out to detect network attacks and prevent SCADA systems from such attacks. Majority of research is being conducted on improvement of SCADA protocols [4] [5]. This surely will improve the security posture of new SCADA systems as such protocols will be incorporated in their operation. But again what about the legacy SCADA systems that are already operating? This paper proposes the intrusion detection mechanism for SCADA systems operating on MODBUS/TCP protocol. Although there are many protocols that are used in SCADA network like DNP3 [6], IEC 60785 etc. but, MODBUS/TCP protocol is widely used in both legacy SCADA networks [7] as well as modern SCADA systems.

In [4] and [5] the security enhancement in the Modbus/TCP and DNP3 protocol is discussed, security in MODBUS/TCP protocol is provided using HASH based authentication and SCTP. In [5] a flexi-DNP3 protocol is proposed which uses DNPSec as primary protocol with a patent key exchange algorithm for preventing replay attacks.

Such method is of no use in an already operating SCADA network. In [8] author mentions L-V-C test-bed for SCADA networks which perfectly emulates the network to carry out experiments. However, author makes use of the Omron physical equipment in his work. Thus, it`s also not a perfectly simulated environment. [9] and [10] discusses about the assessment in SCADA networks, [9] mentions functional assessment whereas [10] makes use of Attack tress to assess the security of SCADA network. In [11] author mentions the optimization function which is used to reduce SCADA specific vulnerabilities. Security Challenges and some recommendations regarding safe SCADA networking is discussed in [12]. [13]- [17] discusses about NIDS to detect network attacks.

III. RELATED WORK

Unlike the concept of detecting network attack vectors on Business I.T. Systems or Traditional Networks, intrusion detection in the SCADA network is very recent phenomena. As we know that SCADA systems were not designed keeping security in mind. These systems were kept completely isolated during their operation. But with time these systems also got changed, they were connected to network for many reasons major among them were:

1. ***Connectivity:*** SCADA personnel can now issue commands from far away site and don`t need to be at the site every time.
2. ***Business Expansion***: The owners of SCADA system wanted to expand their business thereby, establishing remote sites at various locations.

So, the need to protect these networks by detecting network attacks and mitigate its effect has become an issue of paramount importance. This section mentions major research carried out in this field (i.e. intrusion detection on SCADA networks) along with its limitations. In [13] author proposes a novel way to detect cyber intrusions with the help of Distributed Intrusion Detection System (DIDS) which makes use of Neural Networks. Limitation: Fails to address the precision of the event co-relation. Author in [14] proposes an innovative approach of designing of filtering system based on the state analysis of the system being monitored.

Limitation: The proposed work only relies on the state of the system. What if the state of the system is found to be normal and malicious commands are fired? In [15] author have developed a set of command injection, data injection, DoS attacks and used such commands and attacks to design neural network for IDS. Limitation: Complex in design. [16] and [17] discusses the solution based on the fact that Modbus TCP/IP is highly periodic. Limitation: The model may fail if new components are added or removed from the system in [17] false +ve and false -ve are not shown. [18] proposes specific and more intelligent packet inspection mechanism, tailored traffic flow analysis and unique packet tempering detection. Limitation: It is considered as time consuming process.

IV. DISTINGUISHING BETWEEN SCADA SYSTEMS AND TRADITIONAL BUSINESS I.T. SYSTEMS AND SOME ISSUES TO CONSIDER

This section distinguishes SCADA Systems form Traditional Business I.T. Systems. In [19] authors have very briefly and accurately distinguished SCADA Systems from Traditional business I.T. Systems. Table below is adopted from the same.

Table 1 Difference between SCADA Systems and Traditional Business I.T. Systems

Business I.T. Systems	SCADA Systems
Not real-time	Real-time basis
Correctness of Information	Response time is critical
Delay Allowed	Big problems caused by delay
Planned Tasks	Sequential Tasks
Data integrity is important	User`s security is important
Task loss by data corruption	Economic loss and/or casualties
Restoration by re-booting	Continuous operation required.

As we can see from the table above that SCADA systems differs in many ways from traditional I.T. systems. So, special care has to be taken while operating or applying security mechanism on SCADA system/network. There are certain issues while applying security mechanism on SCADA system/network [20]. Major of them are as follows:

1. **How to audit SCADA systems and what to consider in audits?** Firstly, IT departments and SCADA/Process Automation departments have been managed differently. Former supports traditional business applications such as accounting and human resource system where as later systems are managed as part of plant operations and money is spent on them likewise. IT systems and their purpose are well understood by management, accounting and auditors. High level managers fail to understand this specialized technology and are also generally excluded from the scope of auditors.
2. **Patching SCADA systems is not so easy;** I.T. systems may have applied patches for some known vulnerability. This method of immediately patching the IT systems is considered a good practice. But when it comes to SCADA systems, they are rarely patched or updated. Engineers hesitate to put update or patch SCADA systems because of a concern that the patch itself could potentially negatively affect the operation of the system.
3. **Knowledge gap between SCADA personnel and IT system Engineers;** It is found that there is usually a huge knowledge gap between SCADA personnel and IT engineers. SCADA personnel fail to understand the network and IT engineers fails to understand SCADA operations.

We have discussed some of the issues to consider while applying security mechanisms, now it's time to discuss how we can improve security posture of these systems. There are various ways to improve security posture of SCADA systems/network major among them are listed below:

1. **Improvement in Protocol:** As mentioned in this report that earlier SCADA protocols were not designed considering security in mind. So, recently there has been certain improvement in SCADA protocols like ModbusSec and DNP3Sec protocol. These protocols have certain security features but with features there are limitations too. Work can be done in this field as it is proposed that 50% of security attacks can be prevented if a secure protocol is designed.
2. **Follow Defense in depth for securing SCADA network:** As we know that SCADA systems are very much prone to network attacks. Thus, one can implement defense in depth methodology to mitigate the effect of network attacks.
3. **Stable Standards:** Unlike other countries it is hard to believe that India has no fixed standard for implementing SCADA security till date [21]. Thus, using certain fixed standard can also help us in securing SCADA systems.
4. **Design a practical Intrusion Detection System to detect network attack vectors for SCADA specific networks:** This approach may be the most practical because of the several reasons. Firstly, one should remember that the normal operating life cycle of SCADA equipment is usually 20-30 years. Implementation of secure protocol will not prove beneficial as one has to completely stop the operating of SCADA network and systems, this may have adverse effects on ongoing operations. Secondly, as it is said that "there is no patch to a human stupidity" thus, even if we follow defense in depth very thoroughly and patch all the systems for the vulnerability, there will be usually some gaps left. Thirdly, an Intrusion Detection System can be used in the existing system with a minimum or no disruption which can give us alerts when any malicious activity happens in our SCADA network.

Thus, we have studied various possible ways that can improve the security posture of the SCADA network. Some of them like developing stable standards are out of the scope of our research as it needs the involvement of certain regulatory standards establishing authorities. Also if we carry out our research in the field of the SCADA protocols i.e. proposing secure mechanism for communication between HMI-PLC`s then the systems that are already operating would be left out from our proposed scheme. So, considering these issues we carried our research in the field of Intrusion Detection System. Such systems can be easily used in the existing SCADA infrastructure with minimum or no disruption of SCADA operations.

V. MODBUS TCP/IP PROTOCOL AND ITS STRUCTURE

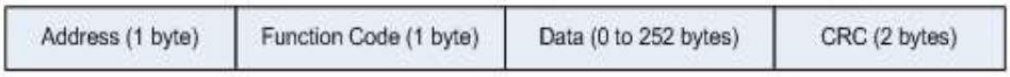
Our research is solely based on one of the most commonly used protocol in SCADA network, the Modbus TCP/IP protocol. So, it is very important to shed some light on the protocol basics and its structure. Please take a note that modbus is strictly an application layer protocol and modbus TCP/IP is the same protocol but wrapped in TCP interface (TCP payload). Basics about both of these protocols is mentioned below:

Modbus: The Modbus protocol suite, popular in the oil and gas sectors, is one of the oldest and most widely used SCADA protocols in North America [7]. The Modbus protocol suite can be broken into two main versions: Modbus Serial and Modbus TCP. Each protocol provides mechanisms for both unicast and multicast transmissions between one or more MTU`s and one or more RTU`s [4].

Modbus TCP [22]: Modbus TCP/IP is a simple the Modbus protocol with a TCP interface that runs on Ethernet. Modbus TCP/IP uses TCP/IP and Ethernet to carry the data of the Modbus message structure between compatible devices. That is, Modbus TCP/IP combines a physical network (Ethernet), with a networking standard (TCP/IP), and a standard method of representing data (Modbus as the application protocol). Essentially, the Modbus TCP/IP message is simply a Modbus communication encapsulated in an Ethernet TCP/IP wrapper. Modbus was originally used over serial communication channels. The protocol was extended to work over TCP communications and there are gateway products too that convert serial Modbus to Modbus TCP and vice versa.

Below given is the structure of Modbus protocol.

Figure 1 Basic Structure of Modbus Protocol [23]



Unlike DNP3, OPC, Ethernet/IP and other control system protocols, Modbus is a very simple protocol. Following are some points that are noteworthy [23]:

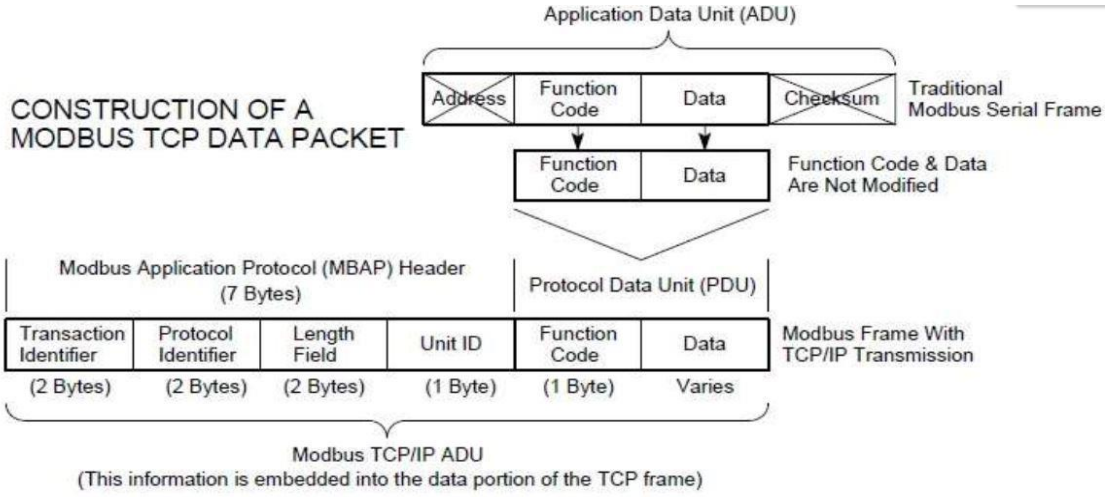
1. This protocol only specifies the application layer.
2. It's a strictly a request/response protocol and there is no support for report by exception or unsolicited response.
3. Modbus packets are small with maximum of 252 data bytes.

As shown in the figure above, the CRC field detects errors but does not prevent an attacker from modifying the packet and recalculating CRC. Request and response is identified by functional code. It ranges from 1 to 127. Some examples are as follows:

Function Code 1: Read Coils
Function Code 6: Write Single Register
Function Code 7: Read Exception Status
Function Code 17: Report Slave ID

Shown above was a simple Modbus protocol which is strictly an application layer protocol. Now, if one needs to have reply and response mechanism incorporated with Modbus protocol over the network then such protocol should be embedded within some transport layer protocol. Thus, to face such need Modbus TCP/IP (Modbus-TCP) was introduced. Below given is its protocol structure.

Figure 2 Construction of Modbus TCP/IP Protocol [22]



As we can see from the figure above that the fields Address and checksum (CRC) are removed and only the function code and data field are taken to form a Modbus TCP packet.

This is because the CRC field was not actually needed as TCP protocol has inherit capability to maintain the integrity and the address field is replaced by 7 byte MBAP header for communication. Below is the brief description of 7 byte MBAP header [22].

1. ***Transaction/invocation Identifier (2 Bytes):*** This identification field is used for transaction pairing when multiple messages are sent along the same TCP connection by a client without waiting for a prior response.
2. ***Protocol Identifier (2 bytes):*** This field is always 0 for Modbus services and other values are reserved for future extensions.
3. ***Length (2 bytes):*** This field is a byte count of the remaining fields and includes the unit identifier byte, function code byte, and the data fields.
4. ***Unit Identifier (1 byte):*** This field is used to identify a remote server located on a non TCP/IP network (for serial bridging). In a typical Modbus TCP/IP server application, the unit ID is set to 00 or FF, ignored by the server, and simply echoed back in the response.

The Function Code and Data fields have the same meaning that it had in the simple Modbus protocol shown above. Function Code stores the specific code related to the PLC and the Data field stores the sub-function code and other related data.

As Modbus TCP protocol relies on TCP/IP stack for its communication and this protocol has no inherit security mechanism like authentication, integrity, non-repudiation. So, it is relatively easy for someone to perform MITM, Denial of service and replay attack. Although Modbus provides robust legacy hardware support, security was not kept in mind during the development phase of the protocol. Any attacker that reach a Modbus slave or server will be able to read and write device as well as reboot the device and may run diagnostic commands [23].

VI. PROBLEM FORMULATION AND PROPOSED MECHANISM

As discussed above, we have carried our research work on Network Intrusion Detection System for SCADA network operating on Modbus TCP/IP protocol. Main reason to use NIDS instead of Host Based Intrusion Detection System (HIDS) is that if we use HIDS then we need to install a software agent to all the host systems in SCADA network and installing such may disrupt ongoing operations in network or may also cause adverse effect. In NIDS we are not taking any risk by installing agent on any system in SCADA network instead we are just placing our equipment in the SCADA network to detect network attacks.

We also don`t deny the fact that by introducing NIDS into the SCADA network there would be no disruption. But there would be significantly less disruption then HIDS which even can`t be noticed sometimes.

When SCADA systems are concerned, the **CIA** triad of typical Business/Enterprise network is not sequenced as **C-I-A** but it is sequenced as **I-A-C** i.e. in such systems (SCADA) **I Integrity** is of paramount importance followed by **A Availability** and that in turn is followed by **C Confidentiality** paradigm. The attacks that hamper the integrity property is Man In The Middle (MITM) attack, replay attack, buffer overflow attack etc. and attacks that hamper the availability property is mainly Denial of Service attack and/or Distributed Denial Of Service attack.

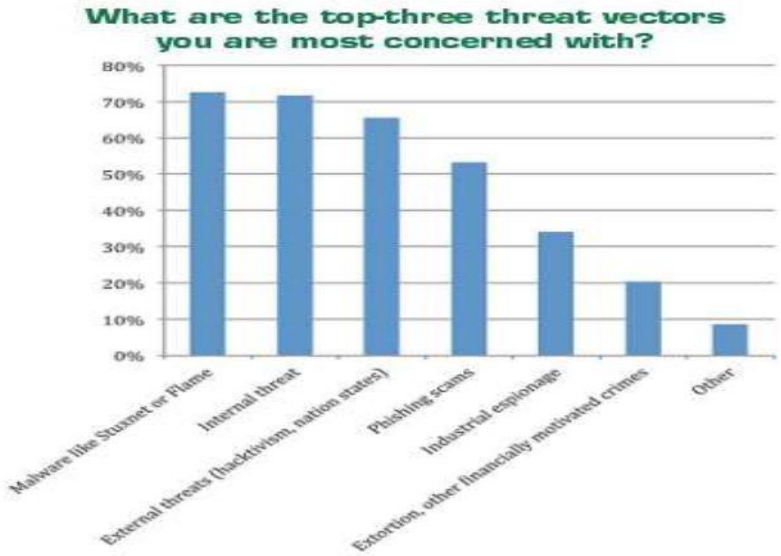
We have successfully performed such attacks such as Man-in-the-middle, replay and Denial of Service attacks using several tools and validated our proposed scheme. It is also important to understand that Modbus is strictly an application layer protocol working at layer 7 which is wrapped within TCP frame. This is shown in the figure below.

Figure 3 Modbus TCP/IP Communication Stack [22]

MODBUS TCP/IP COMMUNICATION STACK			
#	MODEL	IMPORTANT PROTOCOLS	Reference
7	Application	Modbus	
6	Presentation		
5	Session		
4	Transport	TCP	
3	Network	IP, ARP, RARP	
2	Data Link	Ethernet, CSMA/CD, MAC	IEEE 802.3 Ethernet
1	Physical	Ethernet Physical Layer	

If we look at the survey conducted by SANS institute [27], we can notice that the majority of the attack vectors are internal network attacks and external network attacks. Such attacks are mainly from advanced zero-day malware such as stuxnet or flame, internal agents/employees, and external threats from hacktivists, terrorists or governments. The graph for the same is shown below.

Figure 4 SANS Survey Statistics [24]



The protocol structure of Modbus/TCP not being so difficult to understand we have considered three layers of attacks happening on the SCADA specific networks viz. Application layer (protocol payload analysis), Transport layer (TCP flags analysis) and Network layer (Source And Destination IP analysis).

Attack Scenario (1) MITM attack: We used an application that works on Modbus/TCP and created an attack scenario. The Modbus master application for HMI (Modbus Poll) working on Host machine, the slave application for PLC (Modbus Slave) working on the Virtual Machine 1. The attacker machine is on the same network on Virtual Machine 2 equipped with all the tools needed to perform an attack. While Modbus master application was giving instructions to Modbus slave application running on VM 1, we passively gathered traffic from VM 2 using wireshark and changed the contents of the packets and again transmitted to Modbus slave application on VM 1 changing our IP address of Master and amazingly the slave application accepted all illegitimate data from a fake master.

This is one of the classic scenarios of unauthorized master on Modbus/TCP operated SCADA network. Such attack works because Modbus/TCP has no inherit authentication scheme. Diagram is shown below.

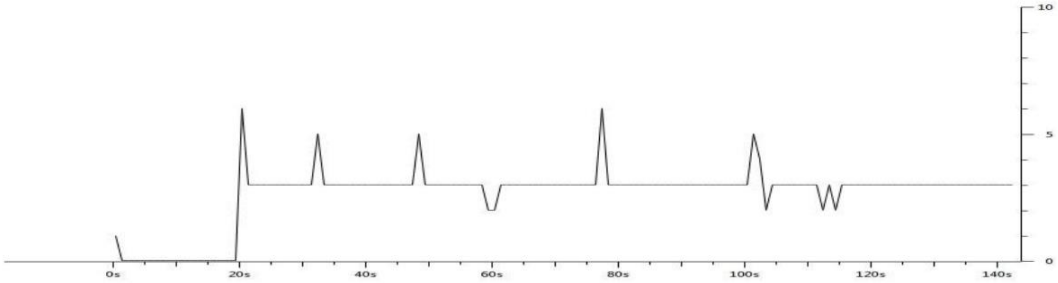
Figure 5 MITM Attack Scenario

Attack Scenario (2) DoS Attack: Here we crafted a legitimate Modbus packet to continuously made illicit response to Master application as a result the slave application couldn`t give true response to the master. And similarly the replay attack scenario was also created. So, as per our study and experiments carried out so far we can say that due to the inherit nature of Modbus/TCP protocol, network attacks such as MITM, DoS, and replay attacks are easily done on SCADA networks operating on such protocol.

IV. PROPOSED MECHANISM

The concept of Intrusion Detection System in SCADA network has been very recent. Although there are various mechanisms to detect the malicious activity in SCADA specific networks which have some advantages and some limitations. So, here we have taken an innovative approach based on Sequencing and direction of packets, Deep Packet Analysis with whitelisting approach along with measuring critical state of detected event. Modbus/TCP traffic is highly predictable. This is shown in the diagram below.

Figure 6 Modbus TCP/IP Traffic



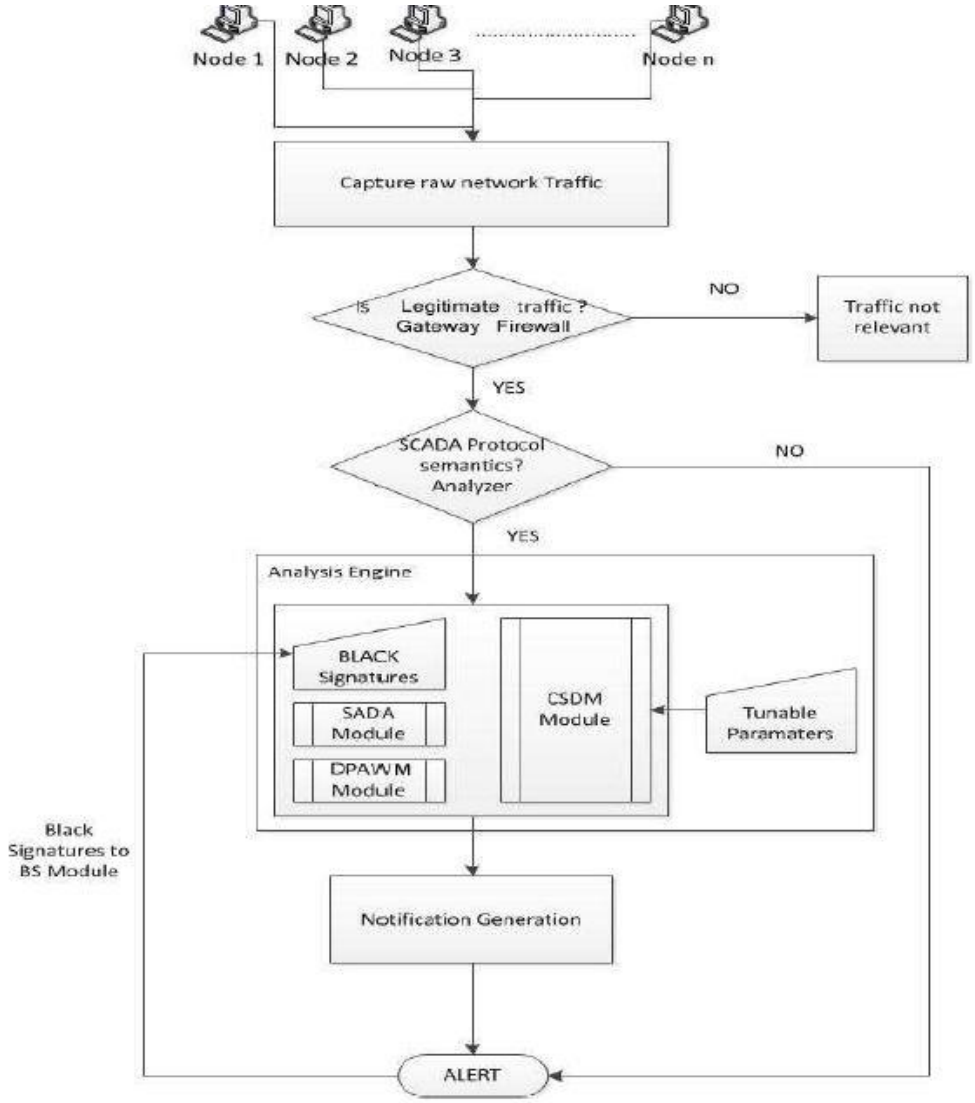
It`s interesting to know that not only the protocol traffic is highly predictable but, the sequence of the packets and direction is also highly predictable (based on our experiments). Adopting the work of [14], we have determined critical state distance of the generated event using the Critical State Language (CSL) so proposed.

It is always considered better to divide any complex task and proceed further. Here also our proposed NIDS mechanism is divided into 5 phases described below.

1. Capture raw Network Traffic.
2. Filtering legitimate traffic.
3. SCADA Protocol Analyzer.
4. Analysis of captured traffic (three modules SADA, DPAWM and CSDM)
5. Notification generation and Alerting.

PROPOSED FLOW DIAGRAM:

Figure 7 Proposed Flow Diagram of Our Mechanism



FUNCTIONAL DESCRIPTION OF FLOW DIAGRAM

To demonstrate a particular SCADA network, our proposed scheme will be having two networks viz. External Network and Internal SCADA Network. The external network is same like some corporate network having internet connectivity and other services. While the Internal network is isolated network used for SCADA operations.

The Internal network is made isolated by a Gateway Firewall and only certain operations are allowed to perform from a single external node. This single external node is only permitted to Activate, Deactivate the firewall and is used for Debugging Purposes. In the Internal Network then it comes SCADA protocol analyzer. This module will check for the semantics of SCADA protocol (checking buffer-overflow conditions etc). Next comes very interesting phase, the heart of the overall process the analysis phase. As shown in the figure above this analysis engine will contain three modules. Their description is given as below:

1. **Sequencing and Directional Analysis (SADA) Module:** This module will search for the particular sequence and direction of the SCADA related packets. As we checked in our experiments that the sequence of the SCADA packets and its direction (from or to PLC-HMI) is highly predictable. If any anomaly is found outside its accepted bounds then alert is raised.
2. **Deep Packet Analysis and Whitelisting Module (DPAWM):** We know that the blacklisting based NIDS is more preferred then anomaly based. This is because in blacklisting based NIDS we get less FLASE POSITIVE rate, each and every attack vector (if signature is present) is detected. But, what if some attacker make use of blended attack? What if some other vulnerability is found as the time passes? Naturally, as the signature of such newly found attack/blended attack is not present in our blacklist database so there is a possibility of the attack vector going un-noticed by NIDS. So, to overcome this situation we make use of whitelisting based approach. In DPAWM module we will model the actual behavior of MASTER-SLAVE and the behavior of the channel (in our case there are two channels MASTER - SLAVE1 and MASTER - SLAVE2) and is put it in this module. Each and every packet will be deeply examined here based on our whitelisting parameters. We have gathered more than 20 (22 to be precise) whitelisting parameters among those Modbus DATA, Slave ID, TCP Flags(PSH/URG), Transaction ID, Length of Modbus Packet, Function Codes, Word and Byte Count are important parameters to check for any SCADA packet. Thus, even if some attacker uses blended type of attack, those attacks can be identified as the attack vectors will not match with what is expected by our NIDS. We shall note that if

any anomaly is found in SADA module then this module will not be processed. This is will relieve the un-necessary burden on our NIDS.

3. **Critical State Distance Measuring (CSDM) Module:** The work done in [14] is adopted to calculate the critical state distance. Here outer file is also given as an input for changing various parameters due to environment conditions.

If the SADA module is evaluating the traffic and found any anomaly then the DPAWM module will not be used for analysis. Whenever any anomaly is found, alert is raised and its critical distance is also computed for that alert within pre-defined critical range. The notification generator generates appropriate notifications and alert is given as a final output. Alerting condition is given as an input to the Black Signature Component such that when it has reasonable amount of conditions, it will check only that database first for signature matching.

Thus, if any signature is found an alert is raised and critical distance is calculated and given as output. We have to take care that duplicate black signature doesn`t get feed in Black Signature database. This is done to reduce false positive ratio.

V. HOW OUR APPROACH IS DIFFERENT FROM EXISTING MECHANISMS?

As per our experiments we have found that not only the frequency of the traffic is highly predictable but, the sequencing of the packets and the direction to and from PLC-HMI is also highly predictable. However, there is an inherit problem if one depends upon the periodicity analysis, what if there is some sort of congestion in the SCADA network? The periodicity approach proposed by the author in such condition will totally fail.

Secondly, for more accurate results we have whitelisted all the possible communication between HMI-PLC, thus if the data packet does not belongs with this whitelisted signatures then again an alert is raised. We will accomplish this by doing Deep Packet Analysis on incoming packets.

Thirdly, in order to reduce false positive rate, we have thought of placing a Black Signature Database which will be very first checked (after it is reasonably filled with Black Signature conditions) to match the signatures.

Fourthly, we have used layered system approach such that there is no additional burden on the entire SCADA network. If any anomaly is found at the first level itself then our proposed mechanism will not allow it to go it further and will flag it as anomaly thereby raising an alert.

Fifthly, we have extended the work proposed in [21] to calculate the critical distance for early detection of changing a state from "Normal" to "Critical".

The proposed scheme being quite innovative and simple in design is complex to implement as it demands much analysis for various datasets.

VII. COMPARISON, ANALYSIS AND RESULTS

In order to test the effectiveness of our proposed system, we have tried possible comparison with nearly existing system. The term "nearly" is used because till now no such system have been proposed which deeply looks for the Modbus TCP/IP protocol packets with Whitelist database signatures. We have taken one of the most popular Network Intrusion Detection System Snort and followed 50 blacklist SNORT rules (signatures) [25] for our comparison. In order to make our comparison more effective, we have also added some additional blacklist signatures for SNORT from digital bond website [23]. Here comparison is based on various parameters and is not limited to just detection capabilities only. Below are various parameters.

Performance: When we talk about Network Intrusion Detection System (NIDS) then we can`t forget to discuss one of the most important factor, the performance of NIDS. Here we have compared the performance of SNORT NIDS with our proposed NIDS from CPU`s resource utilization perspective. We have found that our IDS consumes less resources then SNORT.

The reason behind that is in SNORT many modules and preprocessors gets activated when we start SNORT detection engine where as in our NIDS unlike SNORT only single daemon runs in background thus, utilizes less resources. We have made use of atop utility which checks the CPU`s resource utilization every ten seconds and gnuplot for plotting graph of the same. We have found that our NIDS consumes almost 3 times less CPU`s resources. We can see this from the snapshot below.

Figure 8 Comparing CPU Performance 1) SNORT 2) Our Mechanism

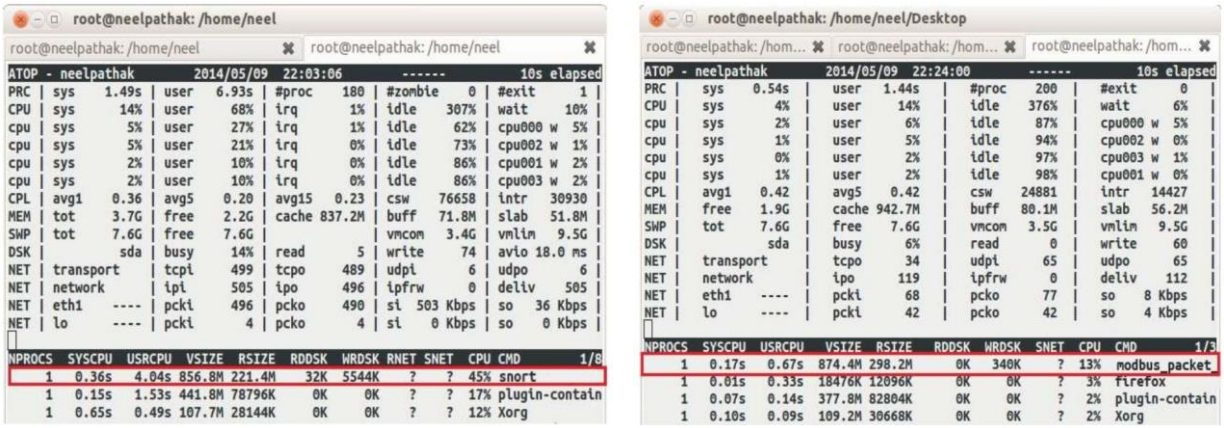
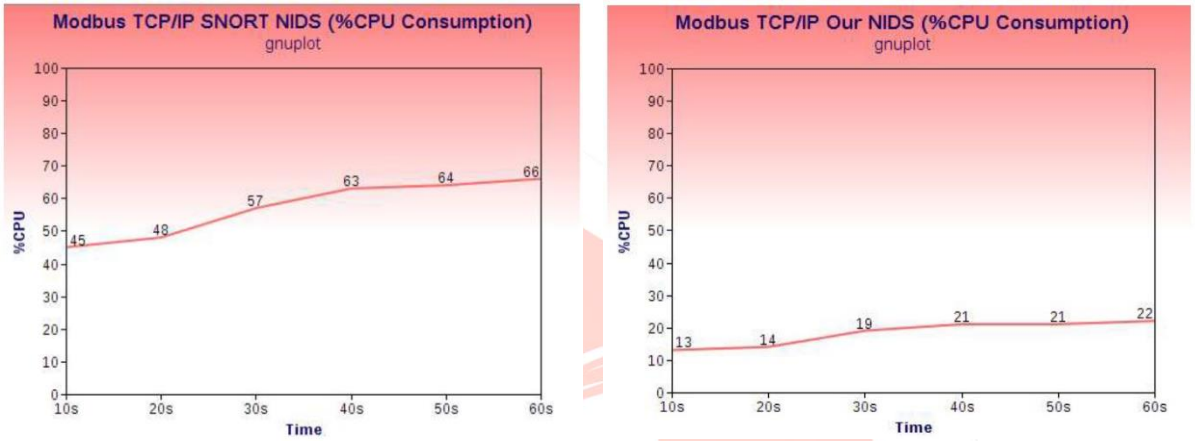


Figure 9 Graphically Comparing CPU Performance with gnuplot 1) SNORT 2) Our Mechanism



0-Day attack Detection: Our proposed system is based on whitelist signatures. What we try to say is, we have already defined fixed set of whitelist signatures that is only possible between HMI and PLC and modelled our communication channel accurately. Any other communication packet other than our defined one is considered as illegitimate and alert is raised. Thus, any new attack vector is easily detected. Here SNORT NIDS fails completely as it is based on blacklist signatures. It is very tedious and clumsy task to update blacklist signatures every now and then for latest vulnerabilities and 0-day attacks. If SNORT is not updated with the latest signatures then all the 0-day attacks will go undetected.

TCP Veto Detection: In [26] author have mentioned a new type of attack and its application to SCADA system. If the attack is done successfully then it leads to desynchronized state between HMI and PLC. SNORT and other NIDS (if operating as statistical mode) doesn`t detect such attacks as it produces 600 times less traffic. As our NIDS is not entirely based on statistical or pattern matching detection, proposed system is very likely to detect such attacks.

Deep Packet analysis check: SNORT NIDS works on Network Layer (IP), Transport Layer (TCP/UDP) and Application Layer where as our proposed NIDS system adds one more layer for its effective detection, the Ethernet layer (Physical + Data-link layer). The Ethernet layer effectively identifies the MAC address of SENDING and RECIEVING hosts and prevent MAC Spoofing attacks inside the SCADA network periphery.

False Positives and False Negatives: False positives w.r.t NIDS are those in which false alerts are raised by detection engine for legitimate packets whereas False Negatives w.r.t NIDS are those in which illegitimate or malformed packets goes undetected pretending that everything is working perfectly fine. The balance between both is very difficult task, if we reduce false negative rate then false positive will increase and vice versa. We have tested both SNORT and our proposed system with 5000 normal traffic packets and then 5000 Modbus TCP/IP attack packets. The results we have obtained were as follows:

Testing Machine: Ubuntu 12.04 LTS 32 bit OS, 3.7 GB RAM and Intel Core i3 CPU M 380 @ 2.53GHz × 4.

Table 2 False +ve and False –ve

	Modbus TCP/IP SNORT NIDS	**MODBUS TCP/IP Our Proposed Mechanism**
Data Packets	5000	5000
Actual Attack	950	950

Packets		
Alerts	2033	977
False +ve	1084	84
False –ve	19	13
Packets Loss	302	549

Please note that 5000 packets which we have used to measure the effectiveness are sniffed from normal operation of SCADA system then we have malformed about 950 packets through Colosoft Packet Generator [27] and again gave those packets to our NIDS such that it can flag that packets as malformed or illegitimate packets.

Early Detection Capability: In our proposed system we have also measured the probability of SCADA system to get into CRITICAL state, thus giving us early alerts before reaching the critical state. SNORT does not provide any such functionality.

Bump-in-the-wire for existing SCADA systems: The proposed system uses BITW technique such that in SCADA Network the ongoing operation does not gets disturbed.

Why BITW? Usually, some NIDS when being introduced in some network sends becon packets/frames to introduce themselves in the network to gateway but, in our case the NIDS is completely operating in stealth mode.

Table 3 Various Parameter Comparison

	SNORT	**Proposed NIDS**
Installation/Deployment	Medium	Very Easy
New Attacks Detection	No (until sig. updates)	Yes
Configuration level	Medium	Easy (Just one XML file)
Packet Loss	302	549
Crafted Packet Detection	No	Yes
Integration level with other H/W	Medium (Requires good processing power)	Easy

We have compared SNORT with our proposed NIDS below in a tabular form. One can come to know from the table that our NIDS is more efficient then SNORT for our particular scenario regarding Modbus TCP/IP traffic.

As we can see from the table above that our proposed NIDS works efficiently for Modbus TCP/IP protocol except one factor, the packet loss factor. We assume that such might have occurred because we have not opted for Multi-threading in our NIDS.

VII. CONCLUSION

Super visionary control and data acquisition (SCADA) systems being most critical infrastructure systems of any Nation and its economy must be in an adequate security posture. The concern about such system rises because unlike earlier SCADA systems which were operating in a stand-alone manner nowadays are connected to the Internet. One shall think about the security of such systems in a pro-active manner rather than reactive manner. Besides considering the network attacks from external network, one must also consider attacks within the secured periphery of these controlled systems as such system lacks many security features.

Considering such issues on SCADA network, we have proposed an innovative and hybrid approach to detect network attacks thereby designing a Network Intrusion Detection System capable of detecting both types of network attacks within secured periphery and attacks from external network. The approach is based on identifying the intrusion based on Sequencing and directional analysis of SCADA network traffic which also adds profiling/whitelisting model and BS signature database to reduce false positives. We have successfully validated our approach by implementing certain attack vectors to detect the odds in SCADA system.

We have tested our proposed mechanism in specific scenario (i.e. One Master or HMI and Two Slaves or PLC`s) and are satisfied with the results as there were accurate and as expected. However, we have not tested our proposed mechanism in real environment and is left for future work.

REFERENCES

[1] "SCADA Primer" [online] Available: (http://www.micrologic.ph/primers/scada.htm) [Dt. 16/09/2013]

[2] Robles, R. J., & Choi, M. K. (2009). Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems. Assessment, 2(2).

[3] Zia Saquib (2013, October). Internal Security- Technologies to Pre-empt and Protect. IEEE SCADA Conference, Mumbai Section.

[4] Hayes, G., & El-Khatib, K. (2013, June). Securing modbus transactions using hashbased message authentication codes and stream transmission control protocol. In Communications and Information Technology (ICCIT), 2013 Third International Conference on (pp. 179-184). IEEE.

[5] Bagaria, S., Prabhakar, S. B., & Saquib, Z. (2011, December). Flexi-DNP3: Flexible distributed network protocol version 3 (DNP3) for SCADA security. In Recent Trends in Information Systems (ReTIS), 2011 International Conference on (pp. 293-296). IEEE.

[6] DNP3 Users Group. A DNP3 Protocol Primer, (March), 1–8. 2005

[7] Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498-506.

[8] Urias, V., Van Leeuwen, B., & Richardson, B. (2012, October). Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. In MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012 (pp. 1-8). IEEE.

[9] Gao-Wang, L., Wen-Yun, J., & Dong-Yuan, S. (2012, March). Functional Vulnerability Assessment of SCADA Network. In Power and Energy Engineering Conference (APPEEC), 2012 Asia-Pacific (pp. 1-4). IEEE.

[10] Byres, E., Franz, M., & Miller, D. (2004, December). The use of attack trees in assessing vulnerabilities in SCADA systems. In Proceedings of the International Infrastructure Survivability Workshop.

[11] Kim, S. H., Eom, J. H., & Chung, T. M. (2012, June). A study on optimization of security function for reducing vulnerabilities in SCADA. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on (pp. 65-69). IEEE.

[12] Rautmare, S. (2012, December). SCADA system security: Challenges and recommendations. In India Conference (INDICON), 2012 Annual IEEE (pp. 1-4). IEEE.

[13] Shosha, A. F., Gladyshev, P., Wu, S. S., & Liu, C. C. (2011, September). Detecting cyber intrusions in SCADA networks using multi-agent collaboration. In Intelligent System Application to Power Systems (ISAP), 2011 16th International Conference on (pp. 1-7). IEEE.

[14] Carcano, A., Fovino, I. N., & Masera, M. (2010, July). Modbus/DNP3 state-based filtering system. In Industrial Electronics (ISIE), 2010 IEEE International Symposium on (pp. 231-236). IEEE.

[15] Gao, W., Morris, T., Reaves, B., & Richey, D. (2010, October). On SCADA control system command and response injection and intrusion detection. In eCrime Researchers Summit (eCrime), 2010 (pp. 1-9). IEEE.

[16] Goldenberg, N., & Wool, A. (2013). Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. International Journal of Critical Infrastructure Protection, 6(2), 63-75.

[17] Barbosa, R. R. R., Sadre, R., & Pras, A. (2012, September). Towards periodicity based anomaly detection in SCADA networks. In Emerging Technologies & Factory Automation (ETFA), 2012 IEEE 17th Conference on (pp. 1-4). IEEE.

[18] Verba, J., & Milvich, M. (2012, May). Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS). In Technologies for Homeland Security, 2012 IEEE Conference on (pp. 469-473). IEEE.

[19] Pathak N. & Prof. Patel H. B. (2014, May). Modern SCADA Systems, "A review on Modern SCADA systems and security considerations of individual system components". In International Journal of Engineering Development and Research (IJEDR).

[20] Johnson, R. E. (2010, November). Survey of SCADA security challenges and potential attack vectors. In Internet Technology and Secured Transactions (ICITST), 2010 International Conference for (pp. 1-5). IEEE.

[21] Bureau Of Indian Standards [online] Available: (http://www.bis.org.in) [Dt. 16/09/2013]

[22] Mi, U. S. A. (2005). INTRODUCTION TO MODBUS TCP / IP, (248).

[23] Digital Bond [online] Available:https://www.digitalbond.com/scadapedia/protocols/modbus-2/ [Dt. 22/12/2013]

[24] SANS Institute [online] Available: https://www.sans.org/reading-room/analystsprogram/sans-survey-scada-2013 [Dt. 22/12/2013]

[25] Morris, T. H., Jones, B. A., Vaughn, R. B., & Dandass, Y. S. (2013, January). Deterministic Intrusion Detection Rules for MODBUS Protocols. In System Sciences (HICSS), 2013 46th Hawaii International Conference on (pp. 1773-1781). IEEE.

[26] Hagen, J. T., & Mullins, B. E. (2013, February). TCP veto: A novel network attack and its Application to SCADA protocols. In Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES (pp. 1-6). IEEE.

[27] Colasoft Packet Builder [online] Available: http://www.colasoft.com/packet_builder/ [Dt. 17/02/2014]