Smart Grid DNP3 Vulnerability Analysis and Experimentation

Ihab Darwish Obinna Igbe Orhan Celebi Tarek Saadawi Joseph Soryal
Electrical Engineering Department
City University of New York, City College

Abstract* — *This paper highlights different security threats and vulnerabilities that is being challenged in smart-grid utilizing Distributed Network Protocol (DNP3) as a real time communication protocol. Experimentally, we will demonstrate two scenarios of attacks; unsolicited message attack and data set injection. The experiments were run on a computer virtual environment and then simulated in DETER testbed platform. The use of intrusion detection system will be necessary to identify attackers targeting different part of the smart grid infrastructure. Therefore, mitigation techniques will be used to ensure a healthy check of the network and we will propose the use of host-based intrusion detection agent at each Intelligent Electronic Device (IED) for the purpose of detecting the intrusion and mitigating it. Performing attacks, attack detection, prevention and counter measures will be our primary goal to achieve in this research paper.

Keywords—Smart-Grid, SCADA, DNP3, IED, Malicious Attacks and DETER

I. Introduction

Security, especially data integrity in communication protocols is one of the most challenging research area involving smart grids. Communication is not just about data transfer, it is about ensuring accuracy, integrity and confidentiality to critical data. Smart-grids are complex environments that facilitate an improved and an efficient two-way path of communication and power handling capabilities. This involves up to date technologies in areas such as power, communication, and renewable energy resources in order to achieve highly secure, reliable, economic, and environmentally friendly electric power system [2], [3]. With increased smart-grid complexity, experimental studies of large-scale grids are usually not economically feasible. Even for small micro-grid environment with limited number of distributed energy sources and intelligent loads, there are only a handful test platforms around the world [4], [5]. Therefore, simulation, virtualization and theoretical modeling become powerful and convenient tools in this research area.

Today's critical infrastructure involves both cyber and physical components integrated using both legacy systems and new technologies working together over TCP/IP platform. Legacy "Supervisory Control and Data Acquisition" (SCADA) [19] systems were initially designed to be isolated systems that had dedicated and separate communication links and therefore cyber and physical security threats were never considered to be an issue. High availability, controllability, and maintainability requirements of today's systems demand a much higher level of communication to exist among various smart-grid components like Intelligent Electronic Devices ([1]IED's). Specifically IED's are designed to automate protection, control, monitoring and metering of the smart grid system in both peer-to-peer and client server implementation within SCADA environment.

Several standards were developed over the years to provide communication within SCADA [24], such as MODBUS, DNP3, PROFIBUS, and the latest IEC 61850. Distributed Network Protocol or DNP3 [7], as our main focus in this research paper, is an IEEE-1815 standard and the primary protocol being deployed in smart-grids system and other utility providers. It is considered to be the predominant SCADA protocol in the US energy sector.

DNP3 is a reliable and an efficient protocol operating in critical infrastructure environments and it is used in the delivery of measurements data from an outstation or client located in the field to the master or server located at the control center. Therefore, it is very critical to study the protocol's behavior and its application in real-time implementation. According to [8], many deficiencies and vulnerabilities were identified in DNP3 including 28 generic attacks. In [1], we modeled smart grid technology experimentally and theoretically to evaluate specific cyber security threats on DNP3; Man in the Middle (MITM) attacks were explored and modeled using game theory analysis and techniques to provide understanding to detection and mitigation strategies. Related SCADA attacks were also studied using different techniques including fault trees, attack trees and risk analysis [13] that provide more theoretical approach as opposed to our method that is more specific to DNP3 and based on experimental results to complement the conceptual analysis.

Our research paper will attempt to achieve three primary goals as follows:

- Highlight security threats and vulnerabilities in DNP3-based smart-grid infrastructures.
- Perform two important attack scenarios experimentally and on [2]DETER to show vulnerabilities in DNP3 implementation using Opendnp3 [9] as a prototype library.
- Analyze strategies related to detection and mitigation using host-based internally developed intrusion detection agents.

Our paper is organized into five sections and our next section will address security threats and vulnerabilities in DNP3. Sections three will present two attack scenarios with the experimental results and analysis of the attacks, followed by attack's detection and mitigation approaches in section four. Then we will present our conclusion.

[1] IED: is any station operating in smart-grid including DNP3 master and outstation or slave, we use the terms "outstation" and "slave" interchangeably

[2] DETER or DeterLab [15] is the cyber DEfense Technology Experimental Research Laboratory primarily used by researchers and academics as a testing bed to perform critical security experiments by emulating real-world complex scenarios with high-level of scalability.

978-1-4673-9300-3/15 $31.00 © 2015 IEEE
DOI 10.1109/CSCloud.2015.86

II. Security Threats and Vulnerabilities in DNP3

A threat is anything that can cause an interruption to network operation or system's functionalities and can jeopardies its availability. There are different categories of threats including natural threats like floods, earthquakes, and storms, unintentional accident type of threats and also there are intentional threats caused by malicious intent. Each type of threats can be catastrophic to a network. A vulnerability on the other hand is an open hole or fault susceptible to a threat attributed to intrinsic weakness in the design, configuration, or implementation of a network or system. Most vulnerabilities can usually be traced back to one of three major sources; poor design, poor implementation or poor management.

In this section, we are considering security threats and vulnerabilities associated with DNP3 as an open standard protocol that can be deployed using several topologies including point-to-point (one master and one outstation or slave), multi-drop topology (using one or multiple masters and multiple outstations) or hierarchical layout topology where systems are arranged in a tree like setup and an outstation could act as both a slave to a DNP3 master and a master to other outstations.

A. The DNP3 Protocol Stack

DNP3 [6], [7] messages can be mapped to the upper layers of the OSI model and are based on three layers "Fig. 1" : data link, pseudo-transport and application layers where AH, TH and LH respectively denote Application Header, Transport Header and Data Link Header. If a DNP3 data stream will be sent over a LAN/WAN, it will be constructed from the three DNP3 layers and then encapsulated in the Transmission Control Protocol (TCP) by the transport layer, which in turn is encapsulated in the Internet Protocol (IP) layer.

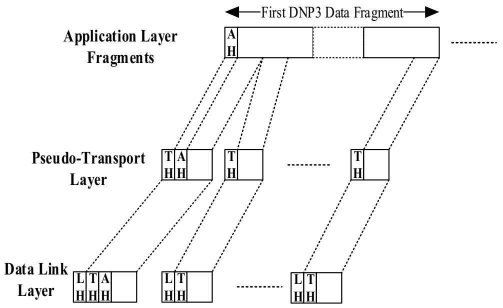


Fig. 1. DNP3 Protocol Stack

At the application layer, an application protocol data unit (APDU) or fragment is created by combining an application service data unit (ASDU), which is a packaged object, with application protocol control info (APCI) block referred to as AH in "Fig. 1". Then, pseudo-transport layer breaks the APDU fragment formed at the application layer into segments termed as transport protocol data units (TPDU) with a maximum size of 16 bytes and packages them with an 8-bit transport control header or TH. The maximum length of the TPDU segment is 250 bytes. Subsequently, the data link layer takes the TPDUs, and adds a link header (LH) to each of them and a Cyclic Redundancy Check (CRC) for error detection and correction. Each of these TPDUs modified at the data link layer is called the link layer protocol data unit (LPDU) or DNP3 packet with a maximum size of 292 bytes [10].

The DNP3 data link packet header (LH), "Fig. 2", consists of a fixed size 10 bytes long header block referred to as block 0, followed by 282 byte long data portion divided into 16 bytes blocks; block 1 to block 16, and each block ends with two bytes CRC code with a total of 32 bytes. The link header (LH) is split into a two bytes "sync" field for synchronizing the receiver and the transmitter, a one byte length field that specifies the number of bytes in the remaining fields (with the exception of the CRC length), a one byte control field, two bytes each for source and destination addressing, and finally a two bytes CRC field [11].

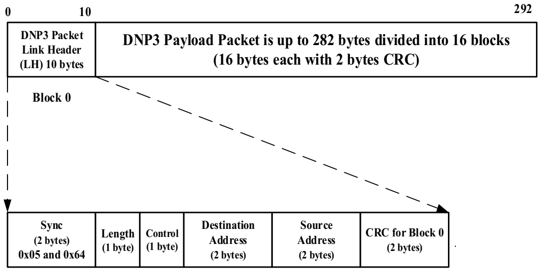

0
10
292
DNP3 Packet Link Header (LH) 10 bytes
DNP3 Payload Packet is up to 282 bytes divided into 16 blocks (16 bytes each with 2 bytes CRC)
Block 0
Sync (2 bytes) 0x05 and 0x64
Length (1 byte)
Control (1 byte)
Destination Address (2 bytes)
Source Address (2 bytes)
CRC for Block 0 (2 bytes)

Fig. 2. DNP3 Packet Blocks

B. DNP3 Threats and Vulnerabilities

28 security threats and vulnerabilities were identified in [8] and classified according to the target and the threat categories. Additional examples of possible threats and vulnerabilities are highlighted here as follows:

- DNP3 operates as an open standard communication protocol. It allows IED's to communicate using many different protocols like TCP, UDP, HTTP etc. [12]. This will lead to having more threats and vulnerabilities in the smart grid environment.
- DNP3 promotes an architecture which supports remote network access for all types of data within the IED. The system depends on remote access point, which is a logical location to implement security function (i.e. authentication, encryption.) [20]. This means that communication within IED's are clear text and vulnerable.
- Current deployments of DNP3 are with or without the secure authentication (DNP3-SA) which can still lead to having a system with mixed protocols, thus increasing the risk and potential for penetration due to having devices running DNP3 without the authentication.
- DNP3 does not define any security mechanism for IED's, and the only security measure for remote access authentication is username and password available only to DNP3 version with Secure Authentication. Due to system limitations, most IED's come with factory defined usernames and passwords. This means that any adversary (an insider or outsider) who can infiltrate the network access point, can easily attack the smart grid system by using dictionary attacks on IED's to gain access [21].

- The protocol allows remote client to IED's to download IED Configuration Definition files which allows interoperability, and it also allows transfer of other files, remote control of IED, reconfiguration of IED, restarting the IED, logging etc [20]. So, any adversary who successfully infiltrates an IED, is able to reconfigure the IED for malicious purposes, render IED inaccessible, or worse, use the IED as a stepping stone to discover connectivity graph, pinpoint other IED's that might possibly have bigger impact on the overall system by downloading Configuration Definition file which contains all necessary information about substation network such as network diagram, IED composition, etc. [13] and cause expensive and irreversible damage to the power grid.

III. Attack Models under DNP3

As a result of the Internet and technology paradigm, security incidents are rising at a very high rate demanding security polices and measures to protect networks. It seems that every other day there is a story in the news about a computer network being compromised by hackers. In fact, in the previous few years, hundreds of hacking incidents at energy companies that were reported and investigated by the Computer Emergency Readiness Team (CERT) [25], a division of the Department of Homeland Security (DHS). These attacks illustrate how extensive the threat from outside hackers has become. At the same time, every organization that uses computers faces the threat of hacking from individuals within the organization. Employees or former employees with malicious intent are also a threat to an organization's computers and networks.

In this section, we are considering internal security threats and we will simulate and experiment small-scale smart grid environment by establishing one master and one outstation for the purpose of investigating two important possible attack scenarios; DNP3 unsolicited messages attack and DNP3 data set manipulation attack.

A. Scenario I - DNP3 Unsolicited Messages Attack

Unsolicited messages is considered to be a way the remote terminal unit (RTU); the outstation, can communicate certain activities or events data to the master station without being polled. Messages can be in the form of specific readings, warnings, or errors detected by the outstation that need to be sent to the master station for further and immediate actions. It is a way to ensure that current status is understood by the master station, for example unsolicited message from the RTU in a smart-grid environment can be sent to the master to indicate that the load's requirement has decreased and it needs to be changed by the master station to a different value and the outstation will be expecting to receive the control message from the master.

In virtualization environment while normal communication is occurring between the master station and the outstation exchanging DNP3 messages encapsulated in TCP/IP packets, an attack is successfully performed to intercept the communication by stopping the outstation from sending unsolicited messages without impacting the normal communication behavior. Such an attack can lead to very disastrous situation if penetration occurred in real smart grid networks. "Fig. 3", shows an example of security penetration executed by the attacker to intercept the communication channel and then inject the malicious payload data without impacting the rest of the communication session between the master and the outstation.

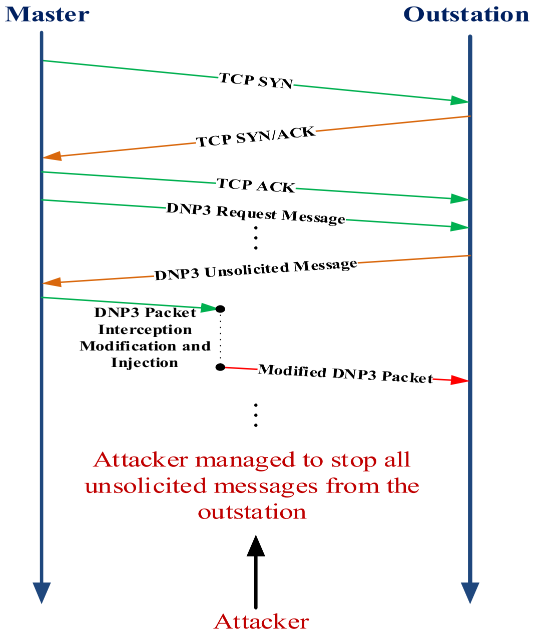

Master
Outstation
TCP SYN
TCP SYN/ACK
TCP ACK
DNP3 Request Message
DNP3 Unsolicited Message
DNP3 Packet Interception Modification and Injection
Modified DNP3 Packet
Attacker managed to stop all unsolicited messages from the outstation
Attacker

Fig. 3. A cyber-attack scenario 1 – DNP3 Unsolicited Message Attack

B. Scenario II - DNP3 Data Set Manipulation Attack

The DNP3 data set manipulation attack includes all forms of attacks against the contents of the DNP3 packet. This type of attacks exploits the non-secured nature of any DNP3 over TCP/IP which does not use any form of transport layer encryption.

In this scenario, the attacker can modify the content of the TCP payload or replace the entire payload with a new one and by modifying the TCP/IP header and DNP3 messages, the attacker can manipulate, control and redirect the DNP3 traffic and even modify the exchanged messages (DNP3 payload) between the master and the outstation. One of the most common data set attack involves the attacker altering the destination address of the DNP3 packet coming from a master node to point to a rogue DNP3 outstation node. This enables the attacker to collect more information about the master node.

C. Experimental Setup

To set up the infrastructure for performing the experiments, three Linux nodes were used to run in a virtual environment and in order to allow for scalability and further testing of complex attack scenarios we have emulated similar setup utilizing DETER [15] network testbed.

Virtual Environment Setup

The virtual nodes used for this experiment consist of a Master station, an Outstation or Slave and an Attacker node. All of these nodes are running Ubuntu [18] operating system. "Fig. 4", shows a diagram of the setup.

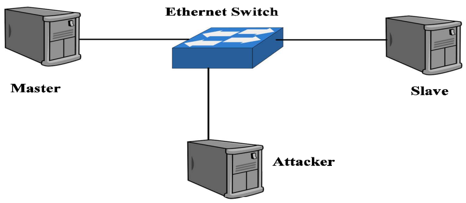


Fig. 4. Virtual Environment Network

In our experiments, an insider attack is assumed and hence, the three virtual nodes are placed on the same network which exposes the Master and Salve nodes to a MITM attack. Both of the Master and the Slave nodes are running OpenDNP3 [9] application and constantly are exchanging dnp3 requests and responses messages. The attacker node is equipped with the capability of sniffing packets using TCPdump and Ettercap [17]. Also, Wireshark [16] is used to analyze the sniffed packets.

DeterLab testbed Setup

Similarly, four nodes are utilized in setting up DeterLab testbed for the experiment. A Master and an Outstation nodes; both running the OpenDNP3 on Ubuntu, and the Attacker node with the same capability as that used in the virtualized environment in addition to a control node for collecting network traffic statistics and remote management across two routers, "Fig. 5" shows network diagram of this setup.

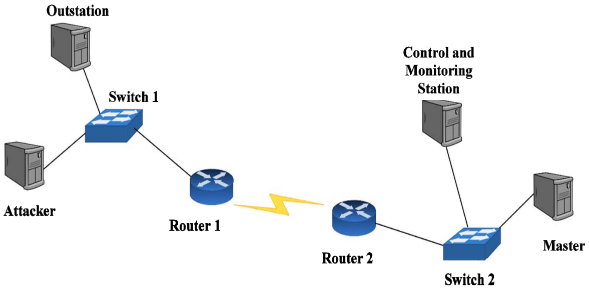


Fig. 5. DETER Lab Testbed Network

D. *Attack Implementation*

Both attack scenarios that will be implemented require the attacker to be in the middle of the communication between the master and the outstation. To perform this step, the ARP cache of both victims (master and outstation nodes) were poisoned by adding their IP addresses (192.168.1.10 for master and 192.168.1.51 for outstation) to Ettercap's target list. In ARP poisoning, the attacker node sends an ARP response packet to the master node saying "I'm 192.168.1.51" i.e., the outstation node. And then sends "I'm 192.168.1.10" to the outstation. Now, all traffic between the master and the outstation is passing through the attacker node as an indication of a successful MITM attack, then we proceed to perform the two attack scenarios.

1) DNP3 Unsolicited messages attack

As mentioned in section A, this attack involves sending a disable unsolicited messages command to the outstation. The "Disable Unsolicited Messages" command is using function code 21 (0x15) that will cause the target outstation to stop sending unsolicited messages to the master. To perform this attack, a Python script was written following an algorithm illustrated in "Fig. 6". Based on the flowchart, the script initially sniffs packets from the interface that connects the Attacker node to the Master-Outstation network. The script searches for an "Operate" command packet (other dnp3 commands could be used as well) which has the function code 04. If an "Operate" packet is observed, then the script copies the packet details including the acknowledgment number and other TCP info. The copied packet is then used to create a "Disable Unsolicited Messages" packet. The script moves on to sniff the packets in the interface and compares their sequence numbers to the previously recorded acknowledgment number. If there is a match, then it is for a response to the initial operate request. Our script immediately updates the sequence number in the crafted packet, along with IP length field, and recalculates its DNP3 Cyclic Redundancy Check (CRC).

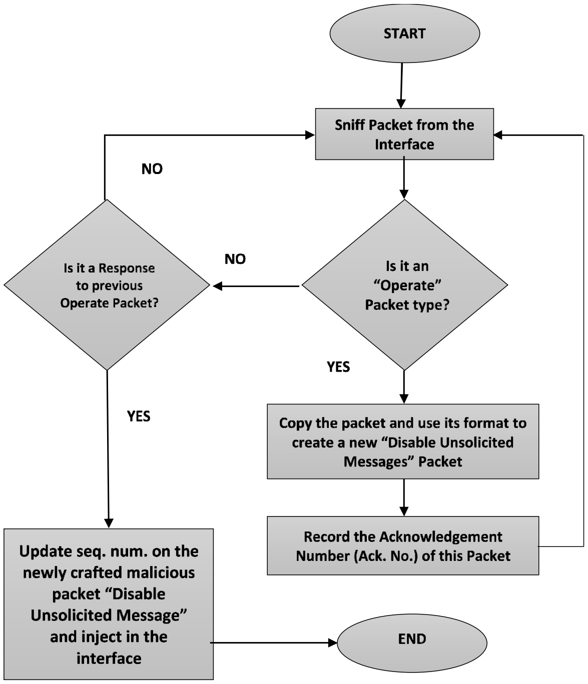
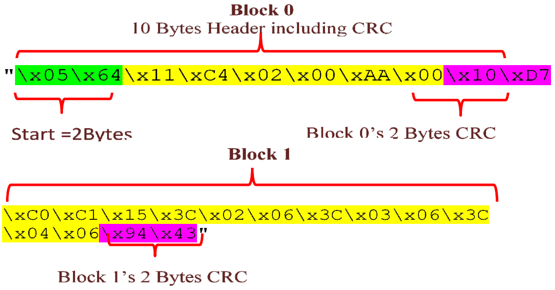

START
Sniff Packet from the Interface
NO
Is it a Response to previous Operate Packet?
NO
Is it an "Operate" Packet type?
YES
YES
Copy the packet and use its format to create a new "Disable Unsolicited Messages" Packet
Record the Acknowledgement Number (Ack. No.) of this Packet
Update seq. num. on the newly crafted malicious packet "Disable Unsolicited Message" and inject in the interface
END

Fig. 6. Unsolicited Messages Attack Flowchart

"Fig. 7", below shows an example of a modified DNP3 packet structure including newly computed CRCs:



```
"\x05\x64\x11\xC4\x02\x00\xAA\x00\x10\xD7
\xC0\xC1\x15\x3C\x02\x06\x3C\x03\x06\x3C
\x04\x06\x94\x43"
```

Fig. 7. DNP3 Modified Message Request Packet

SCAPY [22] is used to recalculate the TCP and IP CRCs, then this modified packet is sent to the Outstation node. Upon receiving the “Disable Unsolicited Messages” command sent by the attacker, the outstation is under the impression that the received request was initiated by the legitimate master and it will stop sending unsolicited messages to the master. The Attacker immediately sends out ARP response packets to master and outstation reverting the poisoning and restoring the communication to its initial state just before the attack. Once this is done, the Python script running on the Attacker node ends.

2) DNP3 Data Set Manipulation Attack

Similar techniques were used to perform the data set manipulation attack, but instead of injecting a crafted packet, the attacker captured a packet in transit, modified its content and allowed this modified packet to proceed to its previous destination. To alter the contents of a packet transmitted from the Master node to the Outstation, the Python script will check for the IP address of the Master node in the traffic that passes through the Attacker according to the following script:

```
if (ip.src=='192.168.1.10'):
  if (search(DATA.data, "\x05\x64\")):
    print "dnp3 header seen\n"
    DATA.data="\x05\x64\x05\xc0\x64\x00\x00\x01”
    Print “master packet replaced\n"
```

After matching the IP address to that of the Master node, then the script will check for DNP3 over TCP packets. And if the packet passes both checks, then alteration is made and the altered packet is then allowed to continue in its path. Otherwise, the packet is forwarded unaltered to the destination.

Another form of data set attacks that we have successfully implemented involved altering the destination of the intercepted packet. Using this type, the attacker can alter the destination IP address field of a packet moving from the master node to the outstation or from the outstation to the master causing the packet to be redirected to another node specified by the attacker. Results and impacts can be disastrous in a real smart-grid network.

IV. Attack Detection and Mitigation Strategies

The primary tool for protecting DNP3 based implementations from malicious attacks is by using the Intrusion Detection (ID). Malicious intents include the attempt to intercept the network, interrupt communication or manipulating DNP3 traffic. Two types of intrusion detection are usually deployed in organizations; host based to provide protection at the host level and network based that monitors all traffic on the network. In our research we developed a host based detection and mitigation tools as an attempt to prevent successful MITM attack on DNP3 environment.

Usually the attacker will send a discovery message to the legitimate node in order to sense the security level and if there is no positive alarm in response to this attempt, it will be an indication of an attack that could be successful. Otherwise, if the intrusion was detected then the malicious packet will be dropped by the legitimate nodes as the first step in mitigating the attack, and furthermore, an alert could be sent to administrator to react against attacker who ultimately could be blocked or isolated.

To optimize our detection and mitigation strategies to minimize cyber threats, we can utilize logs and machine-learning techniques such as statistical analysis. Also, we can implement pattern recognition based on traffic analysis between the legitimate devices and the attacker(s). Our method in preventing attacks was conducted by measuring the average round trip time delay (Trtrip) between the legitimate communicating DNP3 nodes for each request and response and perform dynamic adjustments to the maximum allowed timeout to be equivalent to (Trtrip+ΔT), where ΔT is a safety marginal time. This will allow request packets to be received by the slave preventing attackers from having enough time to initiate any attack by injecting traffic and if they do so, then their malicious packets will be automatically dropped by the receiver.

A. Round Trip Time Measurement

To perform the average round trip time delay measurement at any DNP3 node; master or slave, we will use the Round Trip Timing Agent (RTTA), an internally developed tool in C++ according to the following steps:

1) Initiate the dnp3 session between master and slave.

2) Run the RTTA tool at the master or slave to compute the average round trip time delay for dnp3 packets.

3) An output text file is generated that contains round trip time for each dnp3 packet exchange.

4) An Average Round Trip Time Delay (RTTD) is then calculated.

“Fig. 8” below shows the flowchart depicting the steps involved in calculating the RTTD as measured by RTTA tool.

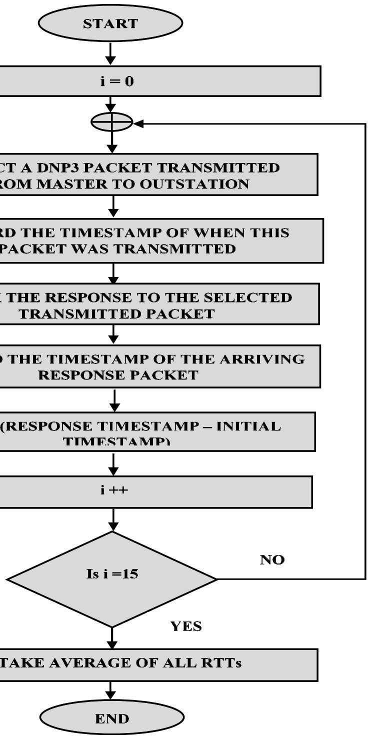

START
i = 0
SELECT A DNP3 PACKET TRANSMITTED FROM MASTER TO OUTSTATION
RECORD THE TIMESTAMP OF WHEN THIS PACKET WAS TRANSMITTED
CHECK THE RESPONSE TO THE SELECTED TRANSMITTED PACKET
RECORD THE TIMESTAMP OF THE ARRIVING RESPONSE PACKET
RTT= (RESPONSE TIMESTAMP – INITIAL TIMESTAMP)
i ++
Is i =15
NO
YES
TAKE AVERAGE OF ALL RTTs
END

Fig. 8. RTTD Measurement Flowchart

B. Pass and Drop Algorithm

Round trip time delay (RTTD) is measured for each packet exchange between the master and the outstation, and actually, each legitimate node on the smart-grid could be setup to calculate the round trip time delay for each DNP3 packet exchange and will be able to generate an average as a baseline (T_{rtrip}). We have the following equation:

$$\Delta = (T_{arrival} - T_{transmitted} - ½ T_{rtrip}) \quad (1)$$

The actual time stamps, $T_{arrival}$ and $T_{transmitted}$ are used for each symmetric DNP3 packet exchange between the master and the slave, ½ T_{rtrip} represents half the average round trip time delay for either request or response packets and Δ will represent the deviation from the average in each direction. If the deviation is between zero and a safety margin Δ_{SM} then the master will accept the packet otherwise, the packet will be dropped. The safety margin Δ_{SM}, is carefully chosen to prevent attacker from having the needed time to perform the attack. The algorithm sequence is as follows:

1) Each DNP3 node will measure the average round trip time delay T_{rtrip} for each exchange of DNP3 packets (Request & Response).

2) The Master sends a DNP3 packet to the outstation encapsulated in a TCP segment with Sequence Number (SN) and Acknowledgement Number (AN).

3) The Outstation will send back a DNP3 response to the master DNP3 request.

4) The master will monitor the round trip time for the received response packet and perform a comparison against T_{rtrip} and if the deviation exceeds the safety margin, then the packet will be dropped and a retransmission will occur.

C. Mitigation – Retransmission Strategy

In [14], two events have been described to require the retransmission strategy, a damaged TCP segment in transit is the first possible event and the second event is related to a segment's failure to arrive as the most common event. In either cases, if a segment does not arrive successfully, there is a timer associated with each segment and a retransmission will occur if the timer expires before acknowledging the segment. Therefore, it is a key design issue to evaluate the timer in TCP that encapsulate the DNP3 packets. The timer is variable and it should be set larger than the round trip time delay to prevent from unnecessary retransmissions.

DNP3 packet exchange between the master and the outstation will follow similar strategy and if the timer is carefully set close to the round trip time delay, MITM attacks could be minimized or prevented. Hence, any delays caused by the attacker exceeding the safety margin Δ_{SM} in either direction will trigger a retransmission to the original packet by the sender. Both, the master and the outstation will use the average round trip delay calculated in section A to adjust its retransmission timer.

V. Conclusion

In this paper we modeled Smart-Grid technology using several testing platforms including virtual lab environment and DETER in order to evaluate specific cyber security threats and vulnerabilities on DNP3 operating in SCADA based implementation. We used various techniques in our analysis to setup different attack scenarios, attack detection and mitigation strategies. Our contribution involved understanding DNP3 vulnerabilities in smart-grids, simulation using different platforms in addition to establishing attack detection and mitigation strategies. More achievements were gained in setting up the Round Trip Time Measurement, Pass and Drop Algorithm and Mitigation Techniques based on timer retransmission. Future work, will expand the detection mechanism in addition to modeling complex real-time smart-grid network scenarios to allow for deep penetration testing along with mathematical modeling and formulation using statistical techniques and game theory.

Acknowledgements

We acknowledge the support of various team members that assisted in scripting and program coding efforts, including Armando Hernandez and Shalini Choudhury; both are graduate students in the Electrical Engineering Department at City College of New York.

References

[1] Darwish, I.; Obinna, I.; Saadawi, T., "Experimental and Theoretical Modeling of DNP3 Attacks in Smart Grids," in Sarnoff, 2015 36th IEEE Sarnoff Symposium on , vol., no., pp.155-160, 20-22 September 2015

[2] R. Brown, "Impact of smart grid on distribution system design," in Proc. IEEE Power Energy Soc. Gen. Meeting, 2008, pp. 1–4.

[3] P. Parikh, M. Kanabar, and T. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in Proc. CCECS Power Energy Soc. Gen. Meeting, 2010, pp. 1–7.

[4] R. H. Lasseter, J. H. Eto, B. Schenkman, J. Stevens, H. Vollkommer, D. Klapp, E. Linton, H. Hurtado, and J. Roy, "CERTS Microgrid laboratory test bed," IEEE Trans. Power Del., vol. 26, no. 1, pp. 325–332, Jan. 2011.

[5] M. Mao, M. Ding, J. Su, L. Chang, M. Sun, and G. Zhang, "Testbed for microgrid with multi-energy generators," in Proc. IEEE Can. Conf. Elect. Comput. Eng., 2008, pp. 637–640.

[6] IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3) - " IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010) -, vol., no., pp.1,821, Oct. 10 2012

[7] www.DNP3.org

[8] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," Critical Infrastructure Pretection III, Springer Berlin Heidelberg, 2009.67-68.

[9] https://github.com/automatak/dnp3

[10] Gordon Clarke, Deon Reynders, "Practical Modern SCADA protocols", 2004, Newnes, ISBN 978-0-7506-5799-0

[11] DNP USers Group, "DNP3 Protocol Primer", http://www.dnp.org/aboutus/dnp3%20primer%20rev%20a.pdf, Accessed: October 6, 2014

[12] U.-K. Premaratne, J. Samarabandu, T.-S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC 61850 automated substations," IEEE Trans. Power Del., vol. 25, no. 4, pp. 2376–2383, Oct. 2010.

[13] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cyber security of the substations," IEEE Trans. Smart Grid, vol. 2, no. 4, Dec. 2011.

[14] William Stallings, "HIGH-SPEED NETWORK AND INTERNETS", 2/e, 2001, William Stallings, ISBN 0-13-032221-0

[15] http://www.deter-project.org/

[16] https://www.wireshark.org/

[17] https://github.com/Ettercap/ettercap/issues/23

[18] http://www.ubuntu.com/

[19] Cyber security risk assessment for SCADA and DCS networks, ISA Trans. 2007 Oct ;46(4):583-94. pub 2007 Jul 10 .

[20] 1815-2012 - IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3) Description: The DNP3 protocol structure, functions, and interoperable application options (subset levels) are specified.

[21] DNP3 Users Group, "DNP3 Secure Authentication Version 5 Overview,"

http://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf, Accessed: May 16th, 2015

[22] SCAPY- http://www.secdev.org/projects/scapy/

[23] 2014 NITRD Cyber Physical Systems Vision Statement; http://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdfR. Brown, “Impact of smart grid on distribution system design,” in Proc. IEEE Power Energy Soc. Gen. Meeting, 2008, pp. 1–4.

[24] J. Wiles, "Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure", Elsevier, 2008.

[25] https://ics-cert.us-cert.gov/advisories