Experimental and Theoretical Modeling of DNP3 Attacks in Smart Grids

Ihab Darwish Obinna Igbe Tarek Saadawi
City University of New York, City College

Abstract —*Security challenges have emerged in recent years facing smart-grids in the energy sector. Threats are arising every day that could cause great scale of damages in critical infrastructure. Our paper will address internal security threats associated with smart grid in a simulated virtual environment involving DNP3 protocol. We will analyze vulnerabilities and perform penetration testing involving Man-in-the-middle (MITM) type of attacks. Ultimately, by utilizing theoretical modeling of smart-grid attacks using game theory, we will optimize our detection and mitigation procedures to reduce cyber threats in DNP3 environment. The use of intrusion detection system will be necessary to identify attackers targeting different part of the smart grid infrastructure. Mitigation techniques will ensure a healthy check of the network. Performing DNP3 security attacks, detections, preventions and counter measures will be our goals to achieve in this research paper*

Index Terms — Smart-Grid, SCADA, DNP3, IED, Malicious Attacks, MITM and Game Theory

I. INTRODUCTION

Security concerns in the energy sector will be our key driver and the smart-grid technologies will be our primary focus in this research paper. Physical and cyber security are using both physical and cyber components integrated with both legacy systems and new technologies running over TCP/IP platform. Legacy Supervisory Control and Data Acquisition (SCADA) [16] systems were initially designed to be isolated systems that had dedicated and separate communication links and therefore cyber or physical security was never considered to be a threat. Today's systems [1], [2] demand a much higher level of communication to be available in systems involving smart-grid automation components like Intelligent Electronic Devices ([1]IED's). IEDs are designed to automate protection, control, monitoring and metering for the smart grid system in both peer-to-peer and client server implementation.

SCADA [3] is using several standards and protocols developed over the years to provide communication including MODBUS, DNP3 [5] and latest IEC 61850. Distributed Network Protocol or DNP3 [6], 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 and it is considered to be the predominant SCADA protocol in the US energy sector.

DNP3 is a reliable and efficient protocol used in the delivery of measurement data from an outstation or slave located in the field to a utility master operating in the control center. Control requests are made from the master to outstations by an operator or using an automated process in addition to time synchronization, file transfer and other related tasks and therefore, it is very critical to study its behavior and application in real-time implementation. According to [7], many deficiencies and vulnerabilities have been identified in DNP3 including 28 generic attacks. Related SCADA attacks were also studied using techniques including fault trees, attack trees and risk analysis [11] that provide more theoretical approach as opposed to our method that is more specific to DNP3 and based on a combination of experimental and theoretical techniques to complement the conceptual analysis.

Our approach consists of performing three primary tasks starting with identification and testing of potential vulnerabilities associated with smart grid implementations involving DNP3. We will use smart-grid testbed experiments on virtualization environments to analyze vulnerabilities and performing penetration testing using man-in-the-middle (MITM) type of attacks to identify possible threats associated with smart grid. By utilizing theoretical modeling of smart-grid attacks using game theory, we can analyze the outcomes of MITM for DNP3 environment. Ultimately the use of intrusion detection system (IDS) will be necessary to identify attackers targeting different part of the smart grid infrastructure and mitigation strategies will ensure a healthy check of the network.

Our research paper will have three primary objectives as follows:

- Review security threats in DNP3 based smart-grid infrastructures and perform MITM attack experiments to show vulnerabilities in DNP3 implementation using Opendnp3 platform as a prototype environment.
- Use "Game Theory" to model man-in-the-middle (MITM) attack on DNP3 environment, analyze detection strategies, mitigations and perform Nash Equilibrium analysis.
- We introduce pass and drop mitigation technique to reduce the impact of MITM attacks along with the selection of retransmission timer.

Section two of this paper will discuss security threats and attacks facing DNP3 protocol in smart-grid implementations. Theoretical modeling using game theory will be presented in section three, detection and mitigation analysis will follow in section four along with our conclusion.

II. SECURITY THREATS IN DNP3

DNP3 [5], [6] is an open standard that can be deployed using several topologies including point-to-point (one master and one outstation or slave), multi-drop topology (one or multiple masters and multiple outstations) or using the

[1] IED is used to denote any station operating in the smart-grid including the DNP3 master and outstation or slave

978-1-4673-8042-3/15/$31.00 ©2015 IEEE

hierarchical layout where systems are arranged in a tree like setup and one outstation could act as both a slave to a DNP3 master or a master to other outstations. DNP3 messages can be mapped to the upper layers of the OSI model and are based on three layers including data link, transport and application layers.

The DNP3 data link frame consists of a fixed size 10 bytes long header block, block 0, followed by 282 byte long data portion divided into 16 bytes blocks and each block ends with two bytes as CRC code. The header 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 [9].

A. DNP3 Attack Model

In this section, we will simulate an experiment of smart grid environment involving one master and one outstation or slave (Fig. 1.) for the purpose of investigating important vulnerabilities and possible attack scenarios using MITM.

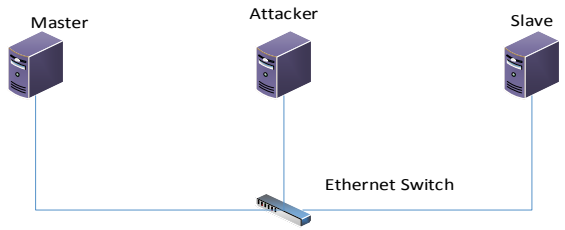

Fig. 1. A cyber-attack Model

To set up the infrastructure for performing MITM attack, , three Linux nodes are used to run in a virtualization environment and the following state transition diagram represents an attack scenario to stop unsolicited messages from the slave in the form of packet intercepting and packet injection.

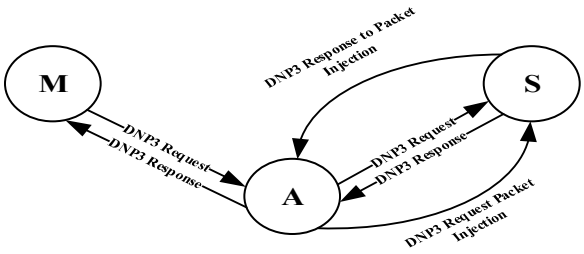

Fig. 2. MITM Attack State Diagram 1

The Master (M) and the Outstation or Slave (S) are both running Ubuntu [15] operating system with OpenDNP3 protocol [8] and exchanging dnp3 request and response packets. The attacker node (A) also is running Ubuntu with Ettercap [14] tools and it is configured to be in the middle of the communication between the master and the outstation. Now, to alter the exchanged packets between the master and the outstation, etterfilter was used to enable swift packet modification. The filter was able to capture only the dnp3 packets and Wireshark [13] was used to validate this process.

B. Attack Setup and Types

To intercept the DNP3 packets, our first step would be to poison the Slave and Master node's ARP cache by adding the target list for performing the ARP poisoning. Four possible attack scenarios are implemented as follows:

1) *Sniffing Slave and Master Generated Traffic:*

For sniffing or capturing the traffic passing between the master and the slave nodes by the attacker, Ettercap was used to perform the attack by adding both master and slave IP to the target list, and then ARP poisoning was initiated, and sniffing option was selected. Now in order to push all the traffic passing through the attacking node to our source code, we use the "nfqueue" python module in combination with Linux "iptables" utility that can be used to allow or to block incoming or outgoing traffic on specific ports.

2) *Selective DNP3 Packets Dropping Attack:*

Now, the Attacker node can view the DNP3 traffic of both victims and in order to drop the traffic generated by any of them, an Ettercap filter is created to specify the conditions to enable selective dnp3 dropping.

3) *DNP3 Packets Modification Attack:*

In order to modify the content of a specific DNP3 payload, the filter is modified and the payload is replaced with a new one. Here the attacker tries to manipulate DNP3 packets by imposing changes to the exchanged packets. Actually the attacker will capture one of the exchanged packets from the source to the destination and will apply modification to the DNP3 payload in order to portray different message to the destination while maintaining the proper sequence and acknowledgment numbering (SN) and (AN) and performing the new CRC and other packet adjustments, thus preventing the system from detecting such an attack.

4) *DNP3 Packet Injection Attack:*

To inject a new DNP3 packet into the traffic stream, the filter is modified and the attacker keeps track of the exchanged traffic between the dnp3 stations and monitors the sequence and the acknowledgement numbers and make the move to inject a totally new packet with newly predicted SN and AN. Also, the attacker will maintain a response to the injected packet and make sure it is dropped. Attacker, then will stop the MITM attack and the communication resumes between the master and the slave.

Both scenarios, 3 and 4 can result in a major impact to the smart-grid network based on the intended message modification used by the attacker.

C. Manipulating DNP3 traffic

To manipulate the dnp3 traffic, we created a code to capture a packet instance and to check the length of the TCP before modification and replace the contents of the payload with the modified one and get the new length of the TCP packet, payload and compute the difference in length between the new and the old and set the new IP length field, delete both of the IP and TCP checksum fields so the scapy [18] would

recalculate this and finally accept and forward modified packet.

In order to send the modified packet, a new TCP session was initiated with the slave node listening at the dnp3 port 20000, and another hijacking technique was invoked to take over the existing TCP session. The test results showed that the attacker; by modifying the TCP/IP header and DNP3 messages, was able to manipulate, control and redirect the DNP3 traffic and even change the exchanged messages (DNP3 payload) between the master station and the outstation.

D. Unsolicited messages Attack Example

Unsolicited messages is considered to be a way the remote terminal unit (RTU), or 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 such penetration occurred in the smart grid network. Figure 3 shows an example of security penetration executed by the attacker to intercept the communication channel and to inject the malicious payload data without impacting the rest of the communication session.

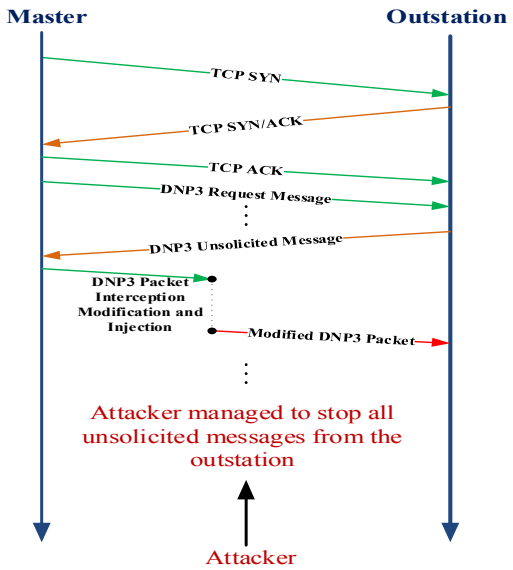

Fig. 3. A cyber-attack scenario – DNP3 Unsolicited Message Attack

III. THEORETICAL MODELING OF MITM ATTACK

In modeling the behavior of communication between the intruder and the legitimate IED devices, game theory principles [4] can be used to establish the attack scenarios as a competition game between the attacker and the IED defender, where each side's strategy is to maximize one's gains. The game will be a non-cooperative game between the Attacker (A) and the normal nodes, Master (M) or Slave (S).

We will model each exchange of DNP3 packets between the master and the slave as a single handshaking game where the master sends a request and the slave responds with a response packet. Fig. 4. displays an example of exchanged messages involving master (M), the slave (S) and the attacker node (A) while keeping track of the timing of each transaction. For simplicity, we are showing T_1, T_2 and T_3 as time stamps.

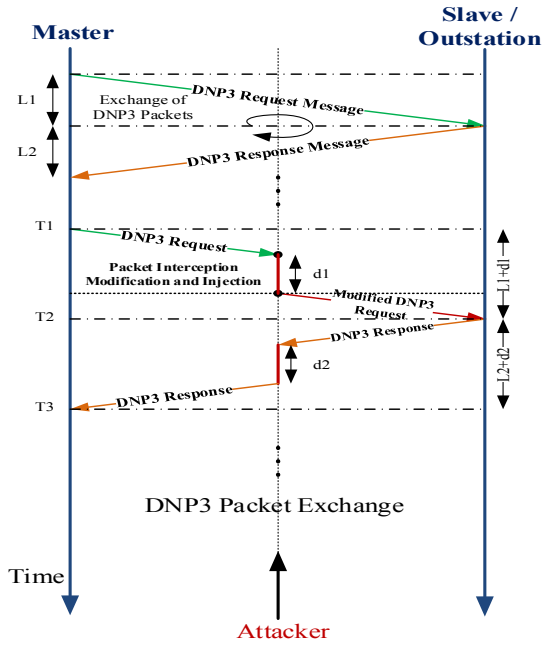

Fig. 4. DNP3 Packet Exchange

In our model, illustrated in Figure 5, we will demonstrate one type of MITM attacks, possible strategies for each node on the network and the possible outcome of the attack by analyzing Nash Equilibrium (NE).

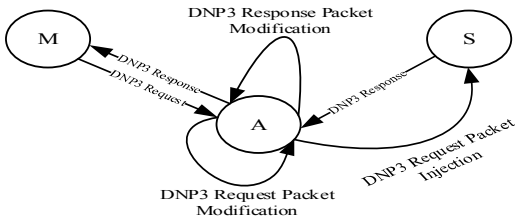

Fig. 5. MITM Attack State Diagram 2

A. Assumptions:

1. Each game is a single exchange of DNP3 packets between the master and the outstation.
2. Each player chooses a strategy and will receive a

payoff based on the selection.

3. Master station will initiate the transaction by sending a DNP3 packet.
4. Attacker node will intercept the packet and perform modification to the payload and sends the outstation the modified version of the original packet.

B. Game Setup

We will model the attack as a three node game involving non-cooperating strategies between the master and the attacker and with the communication channel (C) acting as the nature player imposing network delays that behaves stochastically.

In our analysis, we will use the master node that is generating the packet exchange and the attacker as the primary two rational non-cooperative players utilizing incomplete information but have common knowledge of the game setting including the payoffs. Our game is sequential and starts when attacker A, acting as MITM, chooses its actions, followed by the actions of the communication channel (C) and then by the initiating node M who chooses its actions based on the time stamps and based on the outcomes of A and C's actions. Figure 6 illustrates the game setup and actions in an extensive form with A as being the root of the tree.

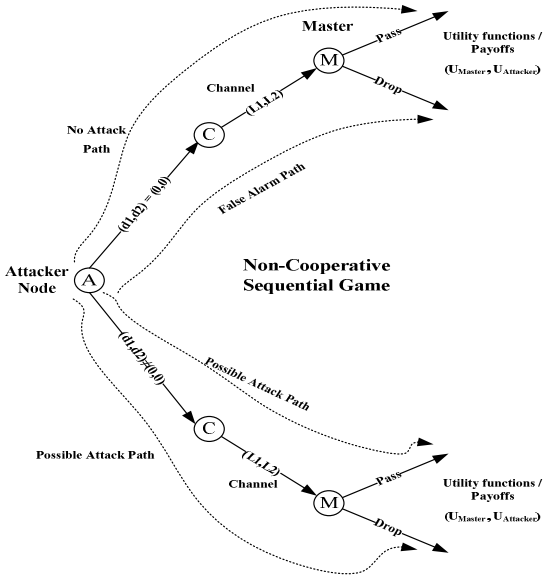

Fig. 6. Game Setup – Extensive Form

Attacker will be able to capture DNP3 traffic between the master and the slave and therefore can perform several type of attacks including Denial of Service (DoS), packet modification, packet injection and so on. In figure 4, we represented the time involved by the attacker in performing the interception and packet modification as d1 and d2 that both are real numbers and could take values between 0 and d_A.

The master node will generate the DNP3 request and will wait for the DNP3 response from the slave and can detect the attack based on the delay imposed by the attacker and will have two possible actions; either dropping the received packet or accepting it after checking the timestamps associated with this transaction (T_1 to T_3).

The communication channel C as the third player will have two possible decisions based on the delays in each direction of the packet exchange, L1 or L2 and are random real numbers and for simplicity we will assume that both are identical.

C. Pass/ Drop Algorithm

During packet exchange, we can compute the round trip time delay (RTTD) based on the actual timestamps (T_1 and T_3) as follows:

$$RTTD = (T_3 - T_1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Actually, each legitimate node on the smart-grid can be setup to calculate the round trip time delay for each DNP3 packet exchange and each node will be able to generate an average for RTTD as a baseline T_{rtrip}. We then have the following equation:

$$\Delta = (T_3 - T_2 - \tfrac{1}{2} T_{rtrip}) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

For symmetric exchange of packets between the master and the slave, $\frac{1}{2} T_{rtrip}$ will represent half the average round trip time delay for either request or response packets and Δ will represent the deviation from half of the average and if the deviation is between zero and a safety margin Δ_{SM} then master will accept the packet otherwise, it will be dropped. Therefore, the safety margin (Δ_{SM}) must be carefully chosen to prevent attacker from having the needed time to perform the attack.

D. Players' Strategies

Root of the tree, Figure 6, represents the attacker node and each player will have a strategy set as follows:

1) S_{Master}: Strategy set for the master node is {Pass, Drop} and will depend on the round trip time delay according to the timestamps (Eq. 1)

2) $S_{Attacker}$: Strategy set for the attacker node, time delays (d1, d2) where: $0 \le d1 \le d_A$ and $0 \le d_2 \le d_A$

3) $S_{Channel}$: Strategy set for the communication channel, propagation delays {(L1, L2), where $L1 \ge 0$ and $L2 \ge 0$}

Therefore, the strategy space S will be (S_{Master} x $S_{Attacker}$ x $S_{Channel}$)

E. Payoff Utility Functions

In our game the attacker will try to maximize its gains and the defender or the master will try to minimize its losses and we will assume that the defender has no prior knowledge of the deviation Δ and for the attack to be successful Δ must be greater than Δ_{SM} . We introduce the following utility functions for a given strategy $s=\{s_{Attacker}, s_{Master}, s_{Channel}\}$:

$$U_{Attacker}(s) = \begin{cases} U_{g,}, \text{ if master selects pass and } \Delta > \Delta_{SM} \\ 0 \text{ , if master selects drop \& } s_{Attacker} \neq (0,0) \\ 0 \text{ , if master selects pass \& } \Delta \le \Delta_{SM} \\ U_f, \text{ if master selects drop \& } s_{Attacker} = (0,0) \end{cases} \quad (3)$$

$$U_{Master}(s) = \begin{cases} -U_{g,}, \text{ if master selects pass and } \Delta > \Delta_{SM} \\ 0, \text{ if master selects drop \& } s_{Attacker} \neq (0,0) \\ 0 \text{ , if master selects pass \& } \Delta \le \Delta_{SM} \\ -U_f, \text{ if master selects drop \& } s_{Attacker} = (0,0) \end{cases} \quad (4)$$

The attacker will receive a payoff of 0, if the defender will choose to play "drop" to the packet, or playing "pass" strategy

given that Δ, the deviation from half of the average round trip time delay (½ T_{rtrip}), is less than or equal to the deviation safety margin Δ_{SM}. Attacker will gain a positive payoff U_g if the master chooses "pass" and $\Delta > \Delta_{SM}$ and in this case the attack is successful. Also, the utility will pay U_f for having the master playing safe and drop the packet when there is no attack as being a false alarm case.

In our model, there is no positive gain for the master, and the maximum achieved payoff is zero for the case the attacker is choosing a strategy $s_{Attacker} \neq (0, 0)$, i.e. there is an attack and the master has managed to avoid the attack with "drop" strategy. In addition to second case where the master chooses to pass when $\Delta \leq \Delta_{SM}$. This a zero-sum game when we add the payoff utilities of both players, $U_{Attacker}(s)$ and $U_{Master}(s)$ and for all given cases, the sum will be zero.

F. Game Theory Analysis

In this section we will analyze the outcomes of the two-players game modeled for DNP3 packets exchange between the master and the slave where packets are being intercepted by the attacker acting as MITM.

According to the game settings and the strategy sets for each player, both the attacker and the defender had multiple strategies to choose from. For the attacker, he will observe the defender who chooses strategy $s1_{Master}$ from S_{Master} strategy set and then the attacker will choose strategy $s1_{Attacker}$ from $S_{Attacker}$ strategy set and we represent the strategy combination as $s=(s1_{Master}, s1_{Attacker}) \in S$, strategy space. Now, the attacker (A) can choose a strategy to either perform the attack successfully or having unsuccessful one. If A chooses the strategy $S_{Attacker}$ = (d1, d2) and $0 \leq d1 \leq d_A$ and $0 \leq d2 \leq d_A$, we will have the following possibilities illustrated in the following table:

TABLE I
GAME ANALYSIS – ATTACKER AND MASTER STRATEGY COMBINATIONS

$S_{Attacker}$	S_{Master}	Analysis
(d1,d2) = (0, 0)	Drop	Attacker chooses not to attack and Defender Drop the packet that will lead to a false alarm. Attacker in this case will gain $+U_f$ and defender will get $-U_f$
(d1,d2) = (0, 0)	Pass	Attacker chooses not to attack and Defender Pass the packet and the both receives a gain of 0 as payoff.
(d1, d2) $\neq$ (0, 0)	Pass and $\Delta > \Delta_{SM}$	Attacker chooses to attack from either direction and if either delays d1 or d2 is greater than safety margin Δ_{SM} and defender chooses to pass then the attack is successful. Attacker will gain Ug and defender will have a loss of the same value.
(d1, d2) $\neq$ (0, 0)	Pass and $\Delta \leq \Delta_{SM}$	Attacker chooses to attack similar to the previous case but Δ is less than the safety margin Δ_{SM} and the defender chooses to pass. In this case the attack is unsuccessful and both will a gain of 0.
(d1, d2) $\neq$ (0, 0)	Drop	There is an attack and the defender plays safe with a drop strategy payoff will be 0 for both the defender and the attacker.

The master node as being the defender will have one strategy $s1_{Master}$ conditioned according to the round trip time delay (RTTD) of eq. (1) and against the baseline average T_{rtrip}. Choosing a pass strategy if RTTD $\leq T_{rtrip}+\Delta_{SM}$ and a drop one if RTTD $> T_{rtrip}+\Delta_{SM}$. But due the nature of communication channel (C) and its stochastic nature, this strategy is not always safe as it can lead to have a false alarm to drop the packet even without having any attack.

G. Nash Equilibrium

Next, we will consider the evaluation of the Nash Equilibrium (NE) in reaching an equilibrium point(s) between the attacker and the defender that is the profile of strategies for each player in choosing the best strategy for the choices of the other player(s). Deviating from NE will not provide the best results to the players.

In our game we have two NE, the first one is reached when the defender always chooses to drop the packet irrespective of having an attack or not, this is the safe thing to do since this will lead to an equal payoff of zero and therefore both players have no interest of deviating from this equilibria. On the other hand, the attacker will not reach his goal of getting the attack done and the defender will not be able to complete the DNP3 packet exchange with the other party. Notice that if A decided to choose strategy (0,0) not to attack and defender chooses to drop the packet that will lead to false alarm and the attacker in this case will gain $+U_f$ and defender will get $-U_f$ and this will not provide the defender with the best possible payoff and hence it will tend to change its strategy.

Our second NE is using the drop threshold strategy discussed in part (F) and in this case the defender is choosing to pass the packet if $\Delta \leq \Delta_{SM}$ and hence RTTD $\leq T_{rtrip}+\Delta_{SM}$ and to drop it if $\Delta > \Delta_{SM}$ and RTTD $> T_{rtrip}+\Delta_{SM}$. In both cases, the attacker strategy is $s_{Attacker} \neq (0,0)$ and the attack will not be successful and results will lead to an equal payoff of zero for both the defender and the attacker reaching a NE. Therefore, for this NE, the defender will optimize its drop threshold value, ($T_{rtrip}+\Delta_{SM}$) to allow attack detection and to prevent from having false alarms possibly due to channel delays and hence this will yield an effective detection and mitigation strategy for the defenders. Our next section will support our analysis and results from game theory.

IV. DETECTION AND MITIGATION STRATEGIES

Intrusion Detection is the primary tool for protecting DNP3 environment from malicious behavior attempting to intercept the network, interrupting communication or manipulating data transmission. There are two types of intrusion detection, host based providing protection at the host level and network based that monitors traffic across the entire network. In our research we used the host based detection method, mitigations strategies and techniques as an attempt to prevent successful MITM attack on DNP3 environment.

In order to optimize our detection and mitigation procedures to eliminate cyber threats, we will utilize logs and machine-learning techniques such as statistical analysis to create and implement procedures for IED's to detect cyber threats independently and/or collaboratively. Also, we can prevent attacks by implementing pattern recognition based on traffic analysis between the legitimate devices and the attacker(s). Measuring the average round trip time delay T_{rtrip} between the legitimate communicating IED nodes for each request and response packet exchange and perform dynamic adjustments

to the maximum allowed timeout to be equivalent to T_{rtrip}+ Δ_{SM}, where Δ_{SM} is a safety marginal time for the round trip as discussed in section 3. This should prevent attackers from having enough time to initiate any attack by injecting traffic since their packets will be automatically dropped by the receiver.

A. Setting up the Round Trip Time Measurement

Steps for setting up the average round trip time measurement at the master or the outstation using Round Trip Timing Agent tool (RTTA developed internally):

1. Establish the dnp3 session between master and the slave.
2. Compute the average dnp3 round trip time delay for dnp3 packets (T_{rtrip}) by running the RTTA at the master and the slave.
3. An output text file is generated for the duration of the runtime that contains round trip time (RTTD) for each dnp3 packet exchange.
4. An Average Round Trip Time Delay (T_{rtrip}) is calculated.

B. Pass/ Drop Algorithm

During packet exchange between master and outstation, we will compute the round trip time delay (RTTD) for each DNP3 packet exchange and will be able to generate an average as a baseline T_{rtrip}. We have the following equation similar to Eq.2:

$$\Delta = (T_{arrival} - T_{transmitted} - \tfrac{1}{2} T_{rtrip}) \quad (5)$$

$T_{arrival}$ and $T_{transmitted}$ are actual time stamps for the returning packet and for symmetric exchange of packets between the master and the slave, $\frac{1}{2} T_{rtrip}$ will represent half the average round trip time delay for either request or response packets and Δ will represent the deviation from the average and 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}, must be carefully chosen to prevent attacker from having the needed time to perform the attack. The following scenario steps show the algorithm sequence in more details:

1) Each node will measure its average round trip time delay T_{rtrip} for each exchange of DNP3 packets.

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

3) Outstation will send DNP3 response to master 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 Techniques

Mitigation techniques will follow the retransmission strategy. In [12], two events have been defined to require this strategy, damaged TCP segments in transit is the first possible event and the segment fails to arrive as the more common one. In both cases, if segment does not arrive successfully, there is a timer associated with each segment and a retransmission will occur if the timer expire before acknowledging the segment. Therefore, it is a key design issue to evaluate the timer in TCP that encapsulate DNP3 packets, timer should not be too small to cause many unnecessary retransmissions or too large to cause response delay for lost segments. The timer is variable and it should be set larger than the round trip time delay.

Now, if we consider the DNP3 packet exchanges between the master and the outstation, they will follow the same analogy and if the timer is carefully set close to the round trip delay, MITM attacks could be prevented. Hence, any delays caused by the attacker exceeding the safety margin Δ_{SM} will trigger a retransmission to the original packet by the sender. Both, master and the outstation will use the average round trip delay calculated in part A to adjust its retransmission timer.

V. CONCLUSION

In this paper we have managed to model Smart Grid technology using a testing environment in order to evaluate specific cyber security threats on DNP3 operating in SCADA based implementation. MITM attacks were explored and modeled using game theory analysis and techniques. Nash equilibria was utilized to highlight possible outcomes of MITM attacks and to prove the pass and drop strategy effectively used to detect attacks and to provide understanding to mitigation. We could expand the theoretical model to detect additional types of attacks involving availability, confidentiality and integrity of the data using multiple-players game running DNP3 in larger environment with mixed strategies and complex topologies. Our future work, will expand this area further by implementing real-time smart-grid network and perform more penetration testing.

REFERENCES

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

[2] 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.

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

[4] Noam Nisan, Tim Roughgarden, Eva Tardos and Vijay V. Vazirani “Algorithmic Game Theory” Cambridge (Sep 24, 2007)

[5] 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

[6] www.DNP3.org

[7] 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.

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

[9] Gordon Clarke, Deon Reynders, “Practical Modern SCADA protocols”, 2004, Newnes, ISBN 978-0-7506-5799-0

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

[11] 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, pp. 865–873, Dec. 2011.

[12] William Stallings, “HIGH-SPEED NETWORK AND INTERNETS”, 2/e, 2001, William Stallings, ISBN 0-13-032221-0

[13] www.wireshark.org

[14] github.com/Ettercap/ettercap/issues/23

[15] www.ubuntu.com

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

[17] 1815-2012 - IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)

[18] SCAPY- www.secdev.org/projects/scapy