Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology

Yatin Wadhawan
University of Southern California
Los Angeles, California
ywadhawa@usc.edu

Dr. Clifford Neuman
ISI, University of Southern California
Los Angeles, California
bcn@isi.edu

ABSTRACT

In this research paper, we present a function-based methodology to evaluate the resilience of gas pipeline systems under two different cyber-physical attack scenarios. The first attack scenario is the pressure integrity attack on the natural gas high-pressure transmission pipeline. Through simulations, we have analyzed the cyber attacks that propagate from cyber to the gas pipeline physical domain, the time before which the SCADA system should respond to such attacks, and finally, an attack which prevents the response of the system. We have used the combined results of simulations of a wireless mesh network for remote terminal units and of a gas pipeline simulation to measure the shortest Time to Criticality (TTC) parameter; the time for an event to reach the failure state. The second attack scenario describes how a failure of a cyber node controlling power grid functionality propagates from cyber to power to gas pipeline systems. We formulate this problem using a graph-theoretic approach and quantify the resilience of the networks by percentage of connected nodes and the length of the shortest path between them. The results show that parameters such as TTC, power distribution capacity of the power grid nodes and percentage of the type of cyber nodes compromised, regulate the efficiency and resilience of the power and gas networks. The analysis of such attack scenarios helps the gas pipeline system administrators design attack remediation algorithms and improve the response of the system to an attack.

Keywords

Cyber Security; Cyber-Physical Threats; Gas Pipelines; Cyber-Physical Attacks; Supervisory Control and Data Acquisition

1. INTRODUCTION

Modern oil and gas cyber-physical systems (OGCPS) incorporates information and communication technologies for improving wide area control, maintaining situational awareness and controlling physical processes remotely. However, the dependency of the energy sector on information technology has opened the doors for various cyber-physical threats (CPT).

CPS-SPC'16, October 28 2016, Vienna, Austria

DOI: http://dx.doi.org/10.1145/2994487.2994488

According to the study conducted by Tripwire [18], 82% of oil and gas (OG) respondents reported that their organizations were subject to the cyber attacks in 2015 and 69% indicated that they were not sure that their system could detect cyber attacks. Recently, a cyber attack on Ukraine power grid [24] demonstrated the capability of cyber attackers to perform multi-level multi-site attacks on the cyber-physical infrastructures. Similarly, a cyber group launched an attack against Saudi Aramco [23], which is Saudi Arabia's largest exporter within Organization of Petroleum Exporting Countries (OPEC) companies, to stop oil and gas production. Such attacks on oil and gas CPS have raised the security fears of OPEC companies. Since OGCPS fuel various aspects of the economy, it has become a necessity to protect them from cyber-physical attacks (CPA).

The OG physical processes are controlled remotely from the cyber domain where operators use Supervisory Control and Data Acquisition (SCADA) system containing remote terminal units (RTUs) with sensors and meters are installed at remote locations to monitor the state of the physical processes. For instance, if a gas pressure in a pipeline is reduced below a threshold (which is a sign of a pipeline rupture or leakage), RTUs send this information to the SCADA system so that the system administrator can send control commands to the remote controlled valves (RCVs) to close. Imagine, if an adversary has control over the SCADA system, he sends malicious close commands to RCVs thereby closing a pipeline unnecessarily and affecting OG delivery. Thus, it is essential to characterize and understand such types of attacks such that the system administrators can design effective remediation plans. This research paper focuses on modeling and analyzing the CPAs on the OGCPS with the motive to evaluate the resilience of the system under sophisticated attack scenarios.

In this research paper, we present a function-based methodology to evaluate the resilience of OGCPS under two different attack scenarios. This research paper follows are qualitative work in [4]. The first attack scenario is the *pressure integrity* attack on high pressure natural gas transmission pipeline. We have analyzed:

1. the cyber attack on the end points which propagates from cyber to gas pipeline physical domain,
2. the time before which the SCADA system should respond to such attacks and
3. an attack which prevents the response of the system.

We have identified the shortest *Time to Criticality (TTC)*, which defines the time for an event to reach the failure state. We have used the combined result of the wireless network simulation and gas pipeline simulation to measure the parameter mentioned above. The second attack scenario is the *cyber-power-gas cascading* attack.

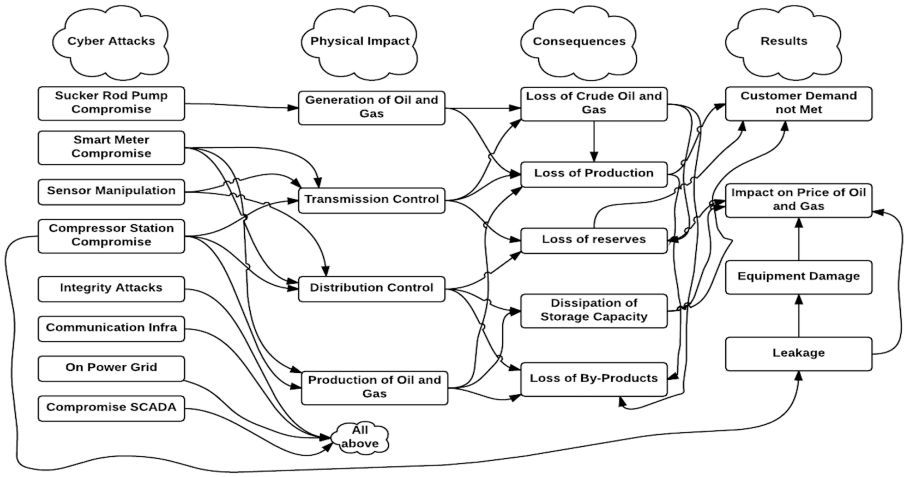

Fig. 1. Oil and Gas Cyber Physical System: Attack Graph.

It describes how a failure of a cyber node controlling a particular power grid functionality propagates from the cyber to power to gas pipeline system. This attack scenario quantifies the interaction between these systems using a graph-theoretic approach. For real networks such as a power grid or gas pipeline, the average shortest length [20] between nodes in the network is used as a metric to measure the efficiency of the network after an attack. The analysis of such attack scenarios will help the system engineers to understand the dynamics of gas pipelines and further assists them to design attack detection and remediation methods to improve the response of the system for an ongoing cyber attack. It also helps identify the failure paths in advance from one system to another so that they can deploy relevant resources effectively and efficiently.

2. RELATED WORK

Traditionally, researchers have focused on discussing resilience and reliability [5] [11] [12] [13] [15] [19], particularly of the power grid, under CPAs using qualitative and quantitative methods. Masera. M et. al. [16] employed a service-oriented approach to enhance the security assessment of a critical infrastructure. By correlating the security information from different domains, the authors have analyzed the dependencies within the infrastructure systems and relationships between the various security information sets. Laprie [15] described the qualitative model for modeling the interdependencies between the power network and information infrastructure. The authors have modeled the behavior of interdependent infrastructures by analyzing the impact of the cascading, escalating and malicious attacks. Huang and Cárdenas [14] demonstrated the effect of a cyber attack on the physical control system by taking an example of a chemical reactor. Such experiments clearly show how the physical components are affected by disturbing the cyber components but do not show how the system of systems are affected and how to quantify the response of the system to prevent damage that might follow from the attack on the end points. In reality, there is a need to describe a metric to quantify the impact of failures so that system engineers can take effective detection and remediation actions.

Neuman and Tan [11] described different ways that malicious attacks propagate from cyber to the physical domain and vice versa. AlMajali [5] demonstrated the consequences of the load drop attack on the smart grid by defining the resilience regarding end nodes compromised. Other researchers have used reliability metrics [13] such as Loss of Load Expectancy (LOLE) to quantify the interruptions of the electric supply caused by cyber attacks. Such metrics do not capture the dynamic behavior of cyber attacks and their impact on the operational resilience of the physical system.

Recently, researchers have focused on understanding the dynamics of the cyber attacks on OG infrastructure. Hasan [1] described the security of cross country OG pipelines using a qualitative approach by describing factors which affect its resilience but he does not argue how. In [4], we have described an approach to assess the resilience of OGCPS. This research paper follows are qualitative work in [4]. Zhang et. al. [2] described the security architecture model of oil and gas SCADA system but they have not described any process controls which are specific to the OG systems. Wu and Tang [3] demonstrated interdependence between the power grid and oil pipelines infrastructure by modeling the cascading failures. They used a graph theoretic approach to understand the correspondence between two graphs. Such methods failed to show how the dynamics of OGCPS are affected and up to what extent system nodes are resilient under attacks on different clusters of the network. Although cascading simulation is performed by researchers in [3] [19], our research is different from them in a way that we have modeled different clusters of the network with different functionality and evaluated the efficiency of the system due to a node failure of a particular feature. Before describing the attack scenarios in detail, the following section presents the attack graph applicable in the OGCPS context.

3. ATTACK GRAPH

Fig. 1 represents the attack graph showing how the cyber attacks propagate from cyber to the physical domain and their consequences. The attack graph is divided into four sections: cyber attacks, physical impact, consequences, and results. The cyber attacks column represents the compromised targets such as head ends, smart meters, compressor stations, etc. Once a cyber system is affected either due to malicious or non-malicious means, it has a physical impact on CPS. The physical impact column represents the functions that are affected due to cyber attacks such as loss of oil and gas transmission and distribution control.

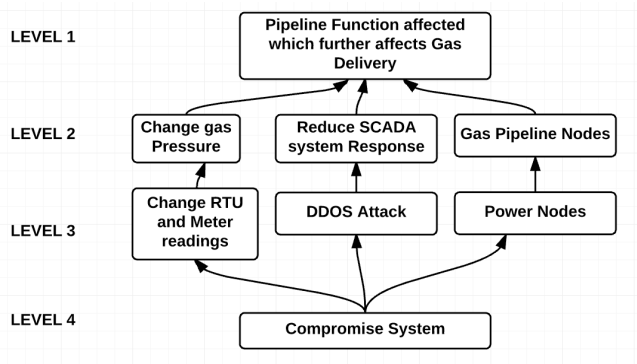

Fig. 2. Oil and Gas Cyber Physical System: Attack Tree

The disturbances in the physical functions have consequences on the system's functionality which results in to increase in gas prices, equipment damage or delay in gas delivery.

Consider a cyber-attack on the sucker rod pump system which affects OG generation; and leads to the loss of crude oil and gas production. The loss of production, in the long run, leads to dissipation of the OG storage capacity and ultimately unsatisfied customer demands. Alternatively, consider an attack on compressor stations which affects the transmission and distribution pipeline. Once such pipeline systems are affected, the gas is not delivered to the processing plants, industries and finally to customers. By understanding this attack graph, the system administrator can identify possible scenarios where the cyber attacks on different functions of OGCPS affect a targeted function and thus system's resilience.

4. FUNCTION-BASED APPROACH

The attack tree in fig. 2 represents the idea of the *function-based methodology* [4]. The motivation behind this approach is to narrow the focus to a particular function of the system. The function can be affected in malicious or non-malicious ways which are abstracted by this approach. We consider an important function of the OGCPS; gas delivery. We build an attack tree to see how gas delivery is affected. The first level of the attack tree represents the primary function of gas delivery, which an attacker wants to affect. The second level represents the impact on the physical system as a change in gas pressure or failure of gas pipeline nodes. The third level represents the cyber attack that affects the physical system in the second level. And finally the fourth level represents how cyber attacks are performed. We can extend the second, third and fourth level to further sub levels. For instance, the fourth level could describe a path from a system entry point (entry of an adversary) to the compromised system. The fourth level of the attack tree represents the cyber attack column in fig. 1.

We consider two attack scenarios in this work (see fig. 2.). The first one is the combination of a pressure integrity and a DDOS attack to affect the high-pressure natural gas pipeline system. An adversary compromises a system in the cyber domain from where he reprograms RTUs to show misleading system readings to the SCADA system and instructs a compressors station (CS) to change the pressure of the natural gas flowing through a pipeline. Simultaneously, he performs a DDOS attack on the communication network to reduce the response of the system. The second attack scenario is to compromise some set of cyber nodes that fail some set of the power nodes, and finally, failure propagates to the gas pipeline system affecting gas delivery. We now describe the first attack scenario.

5. PRESSURE INTEGRITY ATTACK

The sudden change in the pressure of gas flowing through a pipeline can affect the internal pipeline coating, and if pressure goes beyond the Maximum allowable operating pressure (MAOP) [22], pipeline segments are closed via RCVs [8] or may rupture. In this attack scenario, we describe how an adversary affects gas delivery by increasing the gas pressure maliciously through a pipeline. Similar to the Ukraine power grid attack [24], this attack scenario demonstrates multiple capabilities of the attackers such as RTU and SCADA system compromise, and DDOS attack, with the motive to affect the pipeline infrastructure and gas delivery.

5.1 Attack Scenario Description

In the pressure integrity attack scenario, the cyber attacker performs two types of cyber attacks on pipeline infrastructure. First, he compromises a percentage of RTUs (including RCVs) present along the pipeline and CS to reduce the situational awareness of the pipeline segment maintained by the SCADA system. He then instructs the CS that pressure at which the natural gas should be delivered has increased. When most of the RTUs along a pipeline segment are compromised, the SCADA system cannot determine the actual pressure at which CS is pumping the natural gas into that pipeline segment. The CS will increase the pressure so that the natural gas can move through a pipeline and meet the delivery pressure at the sink node. Every pipeline has [22] MAOP below which gas flows normally without affecting the pipeline. Once the attack has started, SCADA system can determine that something is wrong with a particular pipeline segment after some delay. The CSs adjacent to the compromised CS will detect the change in the pressure of the gas delivered and notify the SCADA system. To reduce the pressure of the gas at the pipeline segment and to increase the situational awareness, the SCADA system starts sending control signals to RTUs and CS. Once RTUs are compromised, the attacker performs a DDOS attack on the wireless mesh network to reduce the response of the SCADA system. The questions we should ask at this stage are:

1) what is the percentage of RTUs compromised and for what time period?
2) what is the total amount of pressure increased between two end points given some percentage of compromised RTUs?
3) what is the percentage of compromised wireless nodes (meters) to perform a DDOS attack and how the packet delivery ratio gets affected?
4) time before which the SCADA system should react.

We need to model multiple systems in this attack scenario, therefore we have used separate simulations for the attacks on RTUs, network communication, and pipeline system. Finally, we have used the combined result of the wireless network simulation and gas pipeline simulation to measure the TTC parameter. In the following sections, we describe the system components for the experiment and finally simulation analysis with results.

5.2 Gas Pipeline Model

We chose Pipeflow software to model the behavior of a pipeline and to form a concept model for simulation. In fig. 3, the motive of the pipeline is to deliver natural gas at the sink placed at a distance of 160 miles from the source. CS has positioned at 96 miles from the origin and 64 miles from the sink and to maintain the consistent pressure of delivered gas. The diameter of the pipeline is 15.2 inches and made up of 16" steel material.

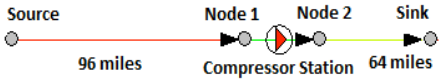

Fig. 3. Pipeline Model

The pressure to deliver the natural gas at the sink should be 900psig. MAOP of the pipeline is 1200psig (which is MAOP of high-pressure transmission pipeline [22]). These are the pressure values in the absence of the cyber attack. If the pressure is above MAOP, many unwanted scenarios may arise such as: pipeline internal coating damage due to pressure increase or immediate valves closure, leakage and the pipeline can explode. CS should pressurize the gas at 1196.61psig to deliver gas at 900psig at the sink node. CS can change the pressure according to the delivery requirements. The difference in pumping and delivery pressure is because of energy loss due to friction when gas flows through a pipeline.

5.3 Wireless Mesh Network (WMN)

We have modeled the WMNs (sensor network as in [25]) using network simulator (NS2) between compromised cyber system node & RTUs and SCADA system & RTUs. The RTUs present along the pipeline, are capable of communicating with the SCADA system over a WMN. Each RTU unit contains a meter which captures the physical properties and sends signals to the SCADA system. We have modeled each RTU as a meter in a WMN. The configuration [17] of meters operating over a radio network is:

1) Radio Frequency: 900MHz,
2) Data Rate: 10 Mb,
3) Transmitter Output: 30 dBm and
4) Receiver Sensitivity: -97 dBm.

The shadowed [6] propagation model is used to simulate outdoor communication because it predicts the mean received power and computes its variation at a certain distance. The configuration of the shadow propagation model is:

1) Path Loss exponent: 2.7,
2) Standard deviation: 4 and
3) Reference Distance: 4.0 m.

We have modeled 300 nodes distributed with uniform random distribution in a region of the pipeline and CS. There are 170 RTUs, a wireless router, a compromised node, a SCADA node and the wireless network nodes for communication. The wireless router is responsible for routing messages over the internet to the SCADA system. UDP/IP as transport layer protocol and Ad-hoc on-demand distance vector (AODV) as a wireless routing protocol are used to simulate the WMN. The compromised cyber system (in fig. 2.) is a node in the WMN that is used to control the functionality of the RTUs in the physical domain.

5.4 Analysis Methodology

In this attack scenario, we have assumed that the cyber attacker has already compromised a system that controls the RTU metering infrastructure. And using the same system, the attacker can modify the pressure set point of the CS (the pressure at which to deliver gas at the sink node). Although we can discuss different methods to compromise a specific ICS, such description is out of the scope of this research paper. The analysis methodology followed in this attack scenario is as follows:

1) We start the simulation by creating the background traffic where RTUs are sending data to the nearest CS and the SCADA system, about the status of a pipeline. Each command is assumed to have a size of 500 bytes.
2) We start the attack 45 secs after the simulation starts. The reason behind this is that we want the WMN to have steady state flow of data when we start the attack.
3) The adversary controlling the compromised node generates a series of commands targeting each RTU meter along the pipeline segment & CS. The time interval between consecutive commands is varied using uniform distribution (0, T) for different values of T.
4) We capture the time at which commands are received by each meter. The attacker sends re-program commands to the RTUs to show misleading pressure readings to the CS and SCADA and instructs CS to increase the pressure of the natural gas.
5) Once the attacker compromises RTUs, the correct information about the pipeline status is reduced and CS starts increasing the pressure to meet the pressure delivery rate at the sink. Since the natural gas is flowing through the pipeline, it is very hard for the attacker to hide the pressure increase from the SCADA for too long. In this scenario, the attack is performed on a particular pipeline segment and CS. (we have assumed that once RTUs are compromised, the SCADA system comes to know about the malicious pressure increase after a delay resulting from misinformation.)
6) The SCADA system sends signals to RTUs and CS to increase the information about the pipeline segment and to reduce the gas pressure.
7) Once RTUs are compromised, the attacker performs a DDOS attack by compromising particular nodes in the WMN. Each node in the WMN sends data at a time chosen from the uniform distribution (0, T), for different values of T.
8) We capture the cumulative number of RTUs received commands by varying the number of nodes compromised during the DDOS attack.
9) Finally, we combine the results of the WMN simulation and DDOS simulation to describe the time before which SCADA system should react (TTC) to avoid the increase in the pressure beyond MAOP.

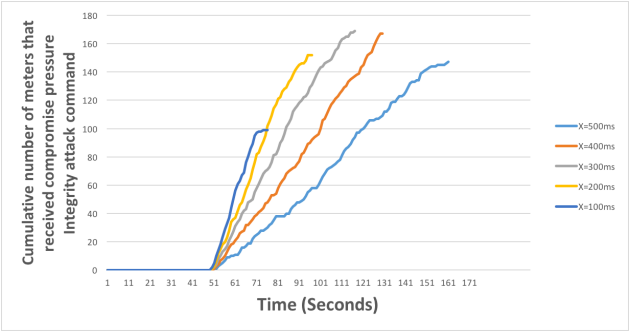

Fig. 4. Cumulative number of meters received command.

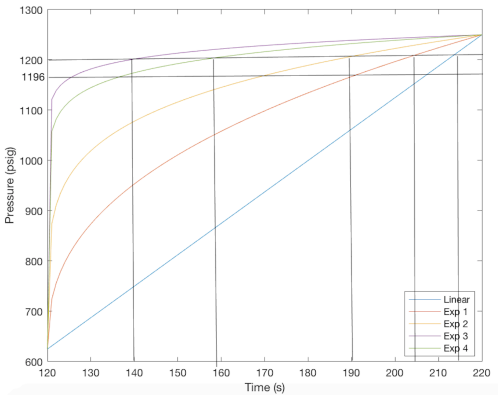

Fig. 5. Pressure Increase corresponding to each compromise command delivery rate to RTUs.

5.5 Simulation Analysis

In this section, we provide the analysis of simulations which demonstrate the above attack scenario. Fig. 4. shows the cumulative number of meters that received compromise commands to reduce the situational awareness about the pipeline and to mislead CS to increase the pressure. The SCADA system expects to receive a certain number of RTU reads within a limited time to maintain system status. If the SCADA system is not receiving correct data about the pipeline, the system administrator cannot take actions to avoid impending failures. X represents the frequency at which the attacker sends compromise commands. The high the frequency; the more quickly RTUs will receive the compromise commands, and the state information becomes less available. The delivery of the commands in the case of X=100ms is fast (see fig. 4), but the number of commands delivered is low because of congestion in the network caused by the short interval between commands. We consider the scenario when commands are delivered at X = 300ms which are stable and almost all meters (N=170) received commands till 115 secs. The CS also received a command to increase the pressure once all RTUs are compromised by the end of 115 secs. The pressure at which CS receive gas 621.624 psig (calculated from the Pipeflow software) and the pressure required at the sink is 900psig. To deliver gas at 900psig, CS has to pressurize gas at 1196.61psig. Therefore, CS starts increasing the pressure from 621.624 psig. Fig. 5. shows the pressure increase over the period starting from the timestamp around 115secs once all RTUs are compromised.

We consider different models of pressure increase to cover different scenarios from the software. The cases for increase in pressure are 1) instantly, 2) linearly and 3) logarithmic with various rates at which compromised commands are delivered to RTUs. When the natural gas is delivered to a sink node at a pressure higher than MAOP, the sink node will inform the SCADA system about the pressure increase. Now the SCADA system immediately launches a series of control commands to CS to reduce the pressure and RTUs to increase the amount of information received about the pipeline. At this stage, the attacker plays his second strategy. He performs a DDOS attack on the WMN connecting the SCADA router, CS and the pipeline network at 115secs, immediately after compromising all the RTUs. One can argue that the attacker can perform both attacks simultaneously, but in that case he cannot compromise all the RTUs because of the congestion in the network due to background and DDOS traffic.

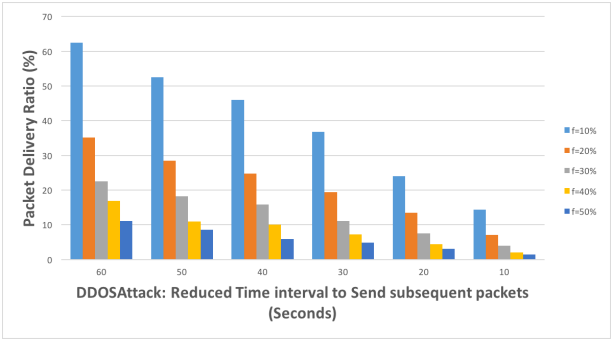

Fig. 6. Packet Delivery Ratio (%) during DDOS attack at different frequencies.

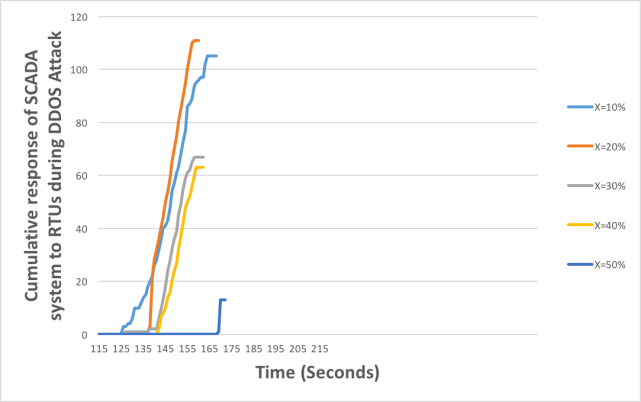

Fig. 7. SCADA Response delivered to RTUs during DDOS attack.

Fig. 6. represents the packet delivery ratio (PDR) when different percentage (f) of nodes are reprogrammed to send packets at various frequencies. If f=10% nodes are reprogrammed to send packets at the 40sec interval, the efficiency of the network goes below the 50%. And it further reduces, if we increase f and reduce the time interval of subsequent commands. In the wireless simulation, we see the effect of the DDOS attack on the command delivery of control signals from the SCADA system. Fig. 7. represents the cumulative response of the SCADA system to the RTUs under the DDOS attack when the different percentage of nodes (X) are compromised.

This graph represents the case when the attacker compromises nodes to reprogram them to send packets at the interval of 30secs (fig. 6.). The attacker can reduce the number of RTUs receiving control commands from the SCADA system quickly by increasing X. Now we need to consider the combine results of the wireless simulation of commands delivered to the RTUs and pipeline pressure simulation. Once the pressure is more than MAOP, many unwanted things can happen as discussed in section 5.2. Therefore, the SCADA system should detect the attacks as quickly as possible. In fig. 7., we consider the best scenario that is the SCADA system starts sending control commands at a time when all the RTUs across the pipeline are compromised. But in reality, it takes a time to determine the pressure change during such sophisticated attacks. Until the natural gas reaches the sink node with higher pressure, the SCADA system cannot find the irregularities because RTUs along the pipeline are compromised perfectly by the attacker. If we consider the delay, it will make the scenario worse. We are interested in time before which the SCADA system should react (that is TTC).

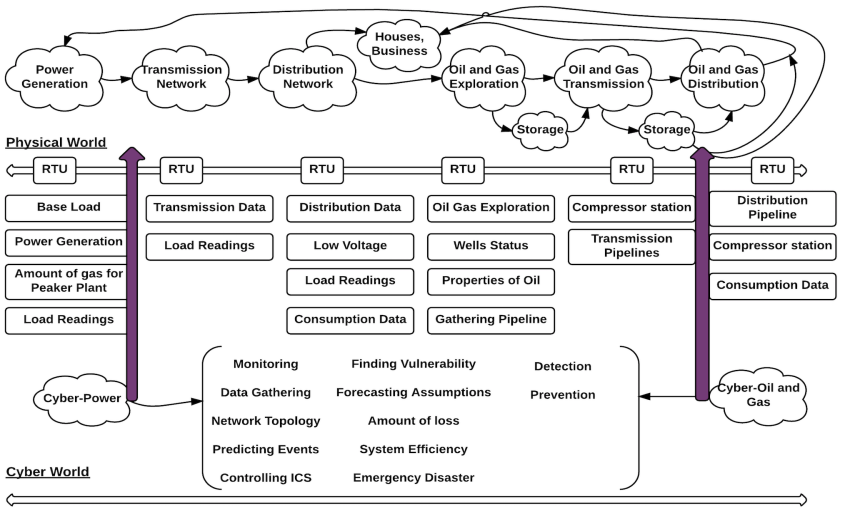

Fig. 8. Cyber-Power-Gas Cross Infrastructure Cyber Physical System

Finally consider fig. 5., if the gas pressure increases linearly with time, a time before which SCADA should act is 215 secs. If the pressure increases exponentially with the rate of change 0.5sec (500ms), 400ms, 300ms and 200ms, the time to react before 205sec, 190secs, 159secs and 140secs respectively. Since the SCADA system starts sending control commands around 115 secs, it takes more than 155 secs to deliver the control commands to just 110 RTUs (out of 170, including CS) when f=20% of nodes are compromised to perform a DDOS attack. Using fig. 5, it takes 159secs (Exp 3) to cross MAOP when the RTUs are compromised at X = 300ms in fig. 4. And if the attacker further increases the number of compromised nodes to reduce PDR, this becomes even worse as one can see in fig. 7. The time limit defined above are TTC in different scenarios when CS increases the pressure with different rates.

5.6 Results

The above analysis shows some of the interesting results about the pipeline system under such sophisticated attacks. The time before which the SCADA system should react depends on the percentage of RTUs and time up to which they are compromised. In both the attacks, by compromising some X% of nodes, the resilience of the pipeline is reduced by a certain level. And the response of the system to counter the attack depends on how quickly the attack is detected and actions are considered. It is important to implement attack detection algorithms, but it is also important to consider strategies to maintain and deliver response of the system under attacks. For instance, in an attack-defense tree: first you apply security controls to protect some system functionality, second an adversary attacks the system, third system detects the attack and respond, fourth the attacker reduces the response with some attack and finally one should have controls to counter the attacker's response to maintain the system' response. We have also demonstrated that if an attacker wants to reduce the resilience of the WMN along a pipeline, he should compromise a few nodes in a particular region. It is not only the communication infrastructure which is affected by such attacks, rather other network functions such as cyber security and system maintenance, are also get affected, which further reduce the response of the system and detection ability. This attack scenario is a glimpse of the real world situation [7] [4]. In reality, cyber attackers have enough resources and knowledge about the system to perform more sophisticated advanced persistent attacks on the OG ICS.

6. CYBER-POWER-GAS NETWORK CASCADING ATTACK

Many advanced technologies such as RCVs, leakage detection, AMIs, etc. have been integrated to develop large scale complex ICS. Fig. 8 represents the interdependence between the cyber, power and gas network. The cyber network monitors the power and gas network. The power network supplies electricity to customers, industries, gas network, etc. And finally gas networks provide gas to customers and power plants [21]. The power and gas system is divided into different subsystems: 1) generation (G), 2) transmission (T), 3) distribution (D) and 4) refinement (R) (specifically for the gas system). The RTUs are placed across the power and gas network that gather system information and feed into the cyber system. The cyber system uses this data to understand the topology, load distribution, predict demand patterns, use power and gas storage in case of emergency, predict attacks, find vulnerabilities and to control the physical processes. The interdependence between the cyber, power and gas networks increase the security concerns of such system of systems. The questions we should ask at this stage are:

1) how a cyber attack happens on a particular type of a cyber node?
2) how a physical change occurs in the power system due to a compromised cyber node?
3) how the failure of a power node causes cascading failure in the power network?
4) how power node failure propagates to the gas network?
5) how failure of gas nodes affects the power generation?

In this attack scenario, we address such questions by describing the interaction between these networks under a cyber attack using a graph-theoretic approach.

6.1 Network Generation

We now discuss the generation of cyber, power and gas networks. In this attack scenario, we want to evaluate the impact of the

failure of a cyber node on the power network which propagates to the gas network. We have considered the interaction between the cyber-power network and power-gas network. Although an adversary can attack the cyber system of the gas network to disrupt gas delivery, we have not considered this case. The focus is to quantify the interaction between cyber-power-gas cross infrastructures during a cyber attack.

We have generated three graphs: Cyber Gc (set of cyber nodes such as servers, RTUs, etc.), Power Gp (such as generators, substations, etc.) and Gas Gg (such as compressor stations, pipeline segments, etc.) similar to fig. 9. The number of nodes (N) in cyber network=100 (G-30, T-30, D-40), power network=100 (G-30, T-30, D-40) and gas network=120 (E-20, R-30, T-30, D-40) are fixed in each simulation. For each network, we generate (G), (T) and (D) nodes separately in the two dimensional space. These nodes are connected on the basis of the proximity (distance), separate clusters of each type of nodes are formed such that it forms the small world network [20].

In a small world network, there is no direct edge between many nodes, but there is a path between such nodes using a small number of hops. We interconnect (G), (T) and (D) clusters with some set of edges selected at uniform random distribution. The edges of the cyber network represent the interconnection between the cyber components over which they communicate. The power network edges represent the transmission lines between generators and substations. The edges in the gas network represent the pipelines through which gas flows sequentially. There are no weights on the edges. We now need to interconnect these networks once they are generated. According to Rinaldi et al. [10], interdependencies are classified into 1) physical, 2) cyber, 3) geographic and 4) logical. For an interdependent cyber-power network, we have used the cyber interdependencies and for power-gas network, we have used the geographic interdependencies. Since the cyber system controls different functions of the power system, the cyber nodes are connected to the power nodes. The edges from cyber network to the power network indicate the control from a cyber node to a particular power node.

Although there is a dependency from power to cyber network, we have not considered this here. We also connect power nodes to the gas nodes at different levels (see Fig. 9). The edges between them represent the path of power supplied to the gas nodes. The power (G) nodes do not provide power to the gas network directly that's why there are no links from power (G) to gas (E) and (R) nodes. The power nodes are connected to the gas nodes which are in the vicinity of the power nodes, according to the geographic interdependencies. One can argue whether such system represents the real world or not. If we consider the gas pipeline system or power grid system at the state level, we are abstracting the behavior of the subsystems. Instead, we should divide the system into different clusters to understand the effect of each group (different functionality) on the overall system. We have also included the closed loop from the gas to power system as compared to [3], so that we can understand the behavior network when gas delivery is affected.

6.2 Modelling Attack Scenario

We assume that the failure in cyber-power-gas network originates from a cyber attack on some set of cyber nodes. When we start the simulation, each power node carries some initial load given by the shortest path from that node to other nodes in the network.

$$\text{Load}_i(0) = \Sigma_{k!=i}\, sd_{k,i} \quad \textbf{(1)}$$

where $sd_{k,i}$ is the number of shortest path from node i. Each power node has some maximum capacity of power it can carry. If the power it carries is more than its capacity, it fails. The maximum capacity [19] of the power node is given as follows:

$$C_i = (1 + \alpha)\, \text{Load}_i(0) \quad \textbf{(2)}$$

where α (>= 0) is called *capacity parameter*. It is impossible to make the capacity of any power node infinite due to resource constraints. When a power node fails, the amount of power it carries will be redistributed to its neighboring nodes. The neighboring nodes will receive this extra power on the basis of their fraction of power they can still consume as compared to their capacity.

$$\text{fraction}_i(t) = (C_i - \text{Load}_i(t)) \,/\, \Sigma_{k=f(i)} (C_k - \text{Load}_k(t)) \quad \textbf{(3)}$$

$$\text{Load}_i(t+1) = \text{Load}_i(t) + \Sigma_{k=x(i)} (\text{Load}_k(t) * \text{fraction}_i(t)) \quad \textbf{(4)}$$

where f(i) is the set of neighboring power nodes at time t and x(i) is neighboring power nodes failed at time t. The power node compares the load it gets from (4) with its capacity. If the load is more than its capacity, the power node fails. When a power node fails, the gas nodes to which it supplies power also fail. We have modelled direct relationship (no probability) between the power and gas nodes. Although there can be contingency plans for the situation when the power nodes do not supply power such as electricity storage, we have not modelled them here. Once a gas node fails, the neighboring gas nodes also fail because gas travels sequentially. For the real world networks such as power and gas, the flow between any two nodes in the network always follows shortest path between those nodes. Therefore, the metric to compute the consequences of the cyber node failure to the power and gas networks is the average reciprocal shortest path length [20]. The reciprocal is used to avoid the infinity path length.

$$E(G) = (1 / (N * (N-1))) * \Sigma_{i!=j}\, 1 / d_{ij} \quad \textbf{(5)}$$

where N is the total number of nodes in the graph G and d_{ij} is the shortest path from node i to j. The shortest path between the nodes have smaller values therefore flow between two nodes on an average will take less time and hence more efficient. This metric does not include the behavior of the power and oil/gas storage (which depends on the time and other variables) but it defines the network efficiency when certain nodes fail. We will incorporate the storage behavior in the future work.

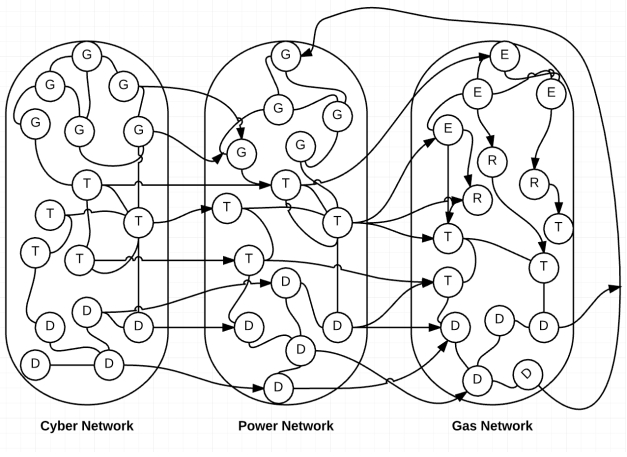

Fig. 9. Cyber to Power to Gas System of Systems.

6.3 Simulation Analysis

We analyze the behavior of the power and gas network when a fraction of the specific type of cyber nodes fail. The nomenclature we have followed: EP – Power Network Efficiency, EG – Gas Network Efficiency and f = percentage of the cyber nodes compromised. The initial value of the capacity parameter is 0.2 which acts as a base load in the power network because power lines always require a certain minimum load to maintain frequency through out the power grid. If the frequency goes beyond the range (under-frequency or over-frequency), the generators may trip causing the partial or whole system shutdown. We gradually increase the value of the capacity parameter in our experiments to see its impact on the efficiency of the network.

In the first case, we compromise the cyber nodes which monitor generation power nodes (see figure 10, 11). The EP and EG are zero in both cases when the capacity is below the base load. As we increase the capacity, EP also increases. Since it also depends on f, when f = 20%, EP = 0.25 stabilizes with $\alpha = 0.6$ and EG = 0.25 with $\alpha = 0.4$. With f = 40%, the EP = 0.24 (less than the previous case) stabilizes with $\alpha = 0.6$ and EG = 0.24 with $\alpha = 0.6$. When f = 40%, EP and EG stabilize with the same capacity and almost same value but if we further increase the percentage of generation node that fail, EG reduces quickly. It is because the failure of power generation nodes propagates to the transmission and distribution network which further affects the gas exploration and refinement nodes. If the gas network is affected in its top domain, the network efficiency reduces quickly as compared to power nodes because gas flows sequentially. If the gas transmission pipelines are affected, the distribution network will be affected too. But in the case of power network, power can be transferred via different transmission lines since it depends on the power capacity of the nodes. In fig. 12 and 13, some percentage of the cyber nodes controlling the power transmission network are compromised. The amount of capacity EP and EG require to stabilize is little higher than the previous case. This is because the transmission nodes failure directly affects all the zones of the power and gas network. When f = 20% the value of EG = 0.19 with $\alpha = 0.4$ (as compared to EG=0.25 with $\alpha = 0.4$ in previous case). When f = 80%, EG=0.12 with $\alpha = 0.6$ which is less than EG = 0.18 in the previous case. Similarly, in the case of power node when f=40%, EP=0.21 with $\alpha = 0.4$ (as compared to EP=0.25 with $\alpha = 0.4$ in previous case). In this case, the gas exploration and transmission network is affected which will affect the distribution network (since gas flows sequential). Therefore, the value of EG is least in this case.

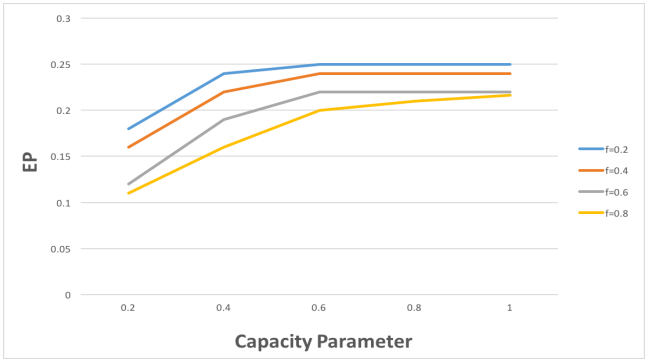

Fig. 10. Effect on Power Network when cyber nodes controlling power generation fail.

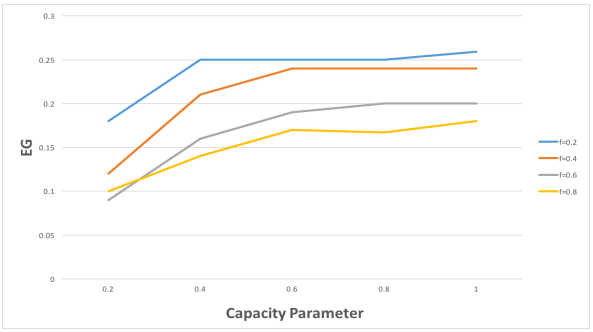

Fig. 11. Effect on Gas Network when cyber nodes controlling power generation fail.

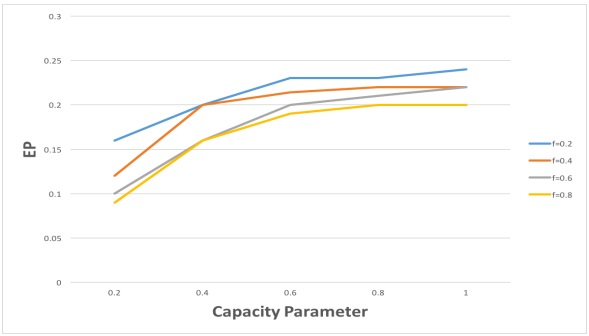

Fig. 12. Effect on Power Network when cyber nodes controlling power transmission nodes fail.

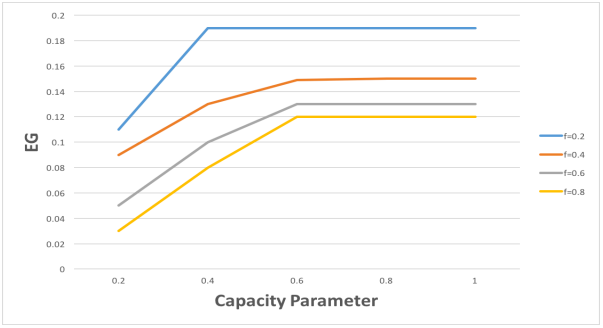

Fig. 13. Effect on Gas Network when cyber nodes controlling power transmission nodes fail.

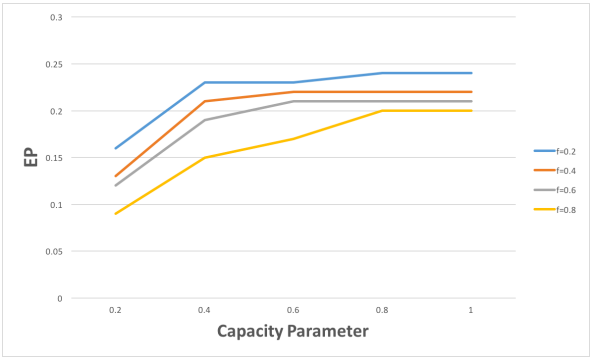

Fig. 14. Effect on Power Network when cyber nodes controlling power distribution nodes fail.

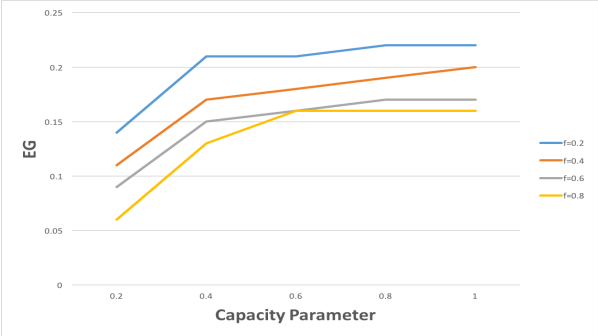

Fig. 15. Effect on Gas Network when cyber nodes controlling power distribution nodes fail.

When some of the cyber nodes controlling the power distribution network fail, the pipeline distribution nodes will also fail (see fig. 14 and 15). EG is little higher than the previous case because if the distribution network is affected, it does not affect the pipeline generation and transmission network. Therefore, EG = 0.22 when f = 20% with $\alpha = 0.8$. The same argument is valid for other cases when we increase f. In the case of power distribution network, intuitively EP should be greater than EP when transmission nodes fail. But in fig. 14. EP stabilizes with equivalent values as compared to EP in fig. 12. This behavior is seen because the gas distribution network is affected which further affects the power generation network.

6.4 Results

The result of the simulation indicates that transmission network should be given greater importance to maintain the overall resilience of the network. The reason is: it connects both the generation and distribution networks. Therefore, a failure in the transmission network affects both the networks. In the real systems, the storage facility at the generation and distribution networks are connected to the transmission network. So if the transmission network is compromised, the oil/gas is not delivered on time and power is not delivered to the distribution network. It is important to understand the interconnection between different types of nodes and their connection with the different networks. If the power generation nodes are compromised beyond a certain level, the storage capacity will not be able to serve and transmission and distribution network will be affected. If the gas distribution network is affected, the power generation will be affected too. The second contribution is that the capacity parameter plays an important role in the resilience of the networks. If we increase the capacity of the power nodes, they become more resilient. It is also advisable to have some power nodes with very high capacity in each of the clusters (specifically in transmission network) so that they can handle load when their neighboring nodes collapse. Such high capacity nodes should be monitored and protected from within the cyber domain. By creating different clusters for different functionality we have created a more realistic model. The difference is the number of nodes in the network and its degree distribution as compared to the real system. In our case if we increase the number of nodes in the network, the results will be unchanged.

7. CONCLUSTION AND FUTURE WORK

Critical industrial control systems are becoming more dependent on information and communication technology. Technologies like advance metering infrastructure have changed the way such infrastructure communicates. In this research paper, we have demonstrated two attack scenarios on the gas pipeline infrastructure which ultimately disrupt gas delivery.

In the first attack scenario, we have analyzed the behavior of the high pressure natural gas pipeline and compressor station in the presence of a cyber attack. The attacker first compromises the RTUs to reduce the situational awareness and then perform DDOS attack on the metering infrastructure to reduce the response of the system. Through this, we have identified and analyzed the metric Time to Criticality which depends on the percentage of end nodes and time up to which they are compromised. In fig.5, we presented the minimum TTC. The time before which the pressure of the compressor station should be controlled before it reaches the MAOP. Metrics like TTC identified in this analysis will be used by the system administrator to determine the time before their system should act. Accordingly, they should design attack remediation algorithms for an ongoing attack. Ultimately, it will improve the response of the system to the cyber attacks. Future work will be to extend this attack scenario to see the effect of the cyber attack on the natural gas storage capacity which ultimately affects the peaker power plant.

In the second attack scenario, we have shown that if a node in the cyber network is vulnerable, we can see the impact of its failure on power and gas systems. In this scenario, we generated a cyber, power and gas network based on the functions interdependencies between them. We have demonstrated through numerical simulations how the efficiency of these networks fluctuates by compromising a certain percentage of cyber nodes and increasing the power nodes capacity parameter. The results show that cascading affect can be avoided when the capacity parameter is above a certain threshold given that a certain percentage of nodes are compromised or failed. If we increase the value of the capacity parameter, the efficiency increases. However, the system administrators cannot increase the capacity of the power nodes since they have cost constraints and having infinite capacity is impractical. If the interdependency between these cross infrastructure nodes increases, the cascading affect accelerates. To improve the resilience of the system against cascading attacks, the system engineers should understand the structure of the cyber, power and gas networks and interdependency between them. There is a need to build a system which will capture the interdependency between them in real time. Administrators should also understand the failure paths in advance from one system to another so that if a node fails in one system (especially cyber where attacks are frequent), immediately they can apply the security controls to the specific components in different systems which are present on the failure path. Future work will improve our understanding of the behavior of the storage areas in the power and gas network with different degree distributions of the network.

8. ACKNOWLEDGMENT

This work was conducted with partial funding by Northrop Grumman Information Systems through the Northrop Grumman Cyber Security Research Consortium.

9. REFERENCES

[1] Hasan, A.: Security of Cross-Country Oil and Gas Pipelines: A Risk-Based Model. Journal of Pipeline Systems Engineering and Practice, 04016006. (2016)

[2] Jian Zhang, Li Yang, and Haode Liao.: A Security Architecture Model of Oil and Gas SCADA Network

Based on Multi-Agent. International Journal of Security and Its Applications, Vol. 10, No. 1, pp.449-46. (2016)

[3] Wu, B., Tang, A., and Wu, J.: Modeling cascading failures in interdependent infrastructures under terrorist attacks. Reliability Engineering & System Safety, 147, 1-8. (2016)

[4] Wadhawan, Y., and Neuman, C.: Evaluating Resilience of Oil and Gas Cyber Physical Systems: A Roadmap. Annual Computer Security Application Conference (ACSAC) Industrial Control System Security (ICSS) Workshop. (2015)

[5] AlMajali, A., Rice, E., Viswanathan, A., Tan, K., and Neuman, C.: A systems approach to analyzing cyber-physical threats in the Smart Grid. In Smart Grid Communications (SmartGridComm), IEEE International Conference on pp. 456-461. (2013)

[6] Radio Propagation Model used in Ns-2 http://kom.aau.dk/group/05gr1120/ref/Channel.pdf

[7] How Hackers take down a Natural gas pipeline. (2009) http://www.popularmechanics.com/military/a12303/4307528/

[8] Pipeline Control Valves, Southern California Gas Company. https://www.socalgas.com/documents/news-room/fact-sheets/PipelineValves.pdf

[9] Zhu, Q., Rieger, C., and Başar, T.: A hierarchical security architecture for cyber-physical systems. (ISRCS), 4th IEEE International Symposium on In Resilient Control Systems (pp. 15-20). (2011)

[10] Rinaldi, S., Peerenboom, J. & Kelly, T.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6): 11-25. (2001).

[11] Neuman, C., and Tan, K.: Mediating cyber and physical threat propagation in secure smart grid architectures. In Smart Grid Communications (SmartGridComm), IEEE International Conference on (pp. 238-243). (2011)

[12] Yan, Y., Qian, Y., Sharif, H., & Tipper, D.: A survey on cyber security for smart grid communications. Communications Surveys & Tutorials, IEEE,14(4), 998-1010. (2012).

[13] J. Stamp, A. McIntyre and B. Ricardson.: Reliability Impacts from Cyber attack on Electric Power Systems. Power Systems Conference and Exposition. IEEE/PES. (2009)

[14] Huang, Y. L., Cárdenas, A. A., Amin, S., Lin, Z. S., Tsai, H. Y., & Sastry, S.: Understanding the physical and economic consequences of attacks on control systems. International Journal of Critical Infrastructure Protection, 2(3), 73-83. (2009)

[15] Laprie, J. C., Kanoun, K., and Kaâniche, M.: Modelling interdependencies between the electricity and information infrastructures. In Computer Safety, Reliability, and Security, pp. 54-67. Springer Berlin Heidelberg. (2007)

[16] Masera, M., & Fovino, I. N.: A service-oriented approach for assessing infrastructure security. In Critical Infrastructure Protection (pp. 367-379). Springer 2007, US.

[17] Communications Module for Electricity Meters. (2013) http://www.silverspringnet.com/pdfs/SilverSpring-Datasheet-Communications-Modules.pdf

[18] Tripwire Study: Cyber Attackers Successfully Targeting Oil and Gas Industry, (2016) http://www.tripwire.com/company/news/press-release/tripwire-study-cyber-attackers-successfully-targeting-oil-and-gas-industry/

[19] Lan, Q., Zou, Y., & Feng, C.: Cascading Failure of Power Grids Under Three Attack Strategies. Chinese Journal of Computational Physics, 29(6), 943-948 (2012)

[20] Latora, V. & Marchiori, M.: Efficient behavior of small-world networks. Physical Review Letters, 87(19): 198701. (2001).

[21] Here's how the Porter Ranch gas leak could lead to power outages. (2015) http://www.scpr.org/news/2016/03/24/58622/here-s-how-the-porter-ranch-gas-leak-could-lead-to/

[22] Pipeline Pressure Limits. http://www.hse.gov.uk/pipelines/resources/pipelinepressure.htm

[23] Report: Oil and Gas cyber security risks continue in 2015. http://www.rigzone.com/news/oil_gas/a/136434/Report_Oil_Gas_Cybersecurity_Risks_to_Continue_in_2015

[24] Analysis of the Cyber Attack on the Ukrainian Power Grid, March 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[25] Jawhar, I., Mohamed, N. and Shuaib, K. A framework for pipeline infrastructure monitoring using wireless sensor networks. In *Wireless Telecommunications Symposium, (2007). WTS 2007* (pp. 1-7). IEEE.