Security Analysis of Smart Grid Cyber Physical Infrastructures Using Game Theoretic Simulation

Robert K. Abercrombie*
Computational Sciences and Engineering Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6085 USA
abercrombier@ornl.gov

Frederick T. Sheldon
Computer Science Department
University of Idaho
Moscow, ID 83844-1010 USA
sheldon@uidaho.edu

Abstract—**Cyber physical computing infrastructures typically consist of a number of interconnected sites including both cyber and physical components. In this analysis we studied the various types and frequency of attacks that may be levied on smart grid cyber physical systems. Our information security analysis utilized a dynamic Agent Based Game Theoretic (ABGT) simulation. Such simulations can be verified using a closed form game theory analytic approach to explore larger scale, real world scenarios involving multiple attackers, defenders, and information assets. We concentrated our study on the electric sector failure scenarios from the NESCOR Working Group Study. We extracted four generic failure scenarios and grouped them into three specific threat categories (confidentiality, integrity, and availability) to the system. These specific failure scenarios serve as a demonstration of our simulation. The analysis using our ABGT simulation demonstrates how to model the electric sector functional domain using a set of rationalized game theoretic rules decomposed from the failure scenarios in terms of how those scenarios might impact the cyber physical infrastructure network with respect to CIA.**

I. Introduction

A nation's economic security rests upon a foundation of highly interdependent critical infrastructures. These infrastructures are those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [1] Infrastructures cover a large number of sectors, including the national electric power grid, oil and natural gas production, transportation, and distribution networks, telecommunications and information systems, water systems, transportation networks, the banking and finance industry, the chemical industry, agriculture and food systems, and public health networks. Understanding the operational characteristics of and providing a sufficient level of security for these infrastructures requires a "system-of-systems" perspective, given their interdependencies [2].

The operation of infrastructures that provide cyber services, such as network connectivity and computing capacity, requires the continued functioning of: (i) cyber components such as computers, routers, and switches, and (ii) physical components such as fiber routes, cooling, and power systems. While these infrastructures are built to provide cyber services, their operation is "cyber-physical" in nature due to its dependence on both cyber and physical components. For example, the components may be degraded by factors such as incidental (weather related) power failures and device fatigue failures as well as deliberate cyber-attacks on computers and physical attacks on fiber routes. While cyber-attacks on computing systems and networks seem to get more public media attention, in many occasions the infrastructure degradations have been due to physical factors such as power blackouts and backhoe incidents on fiber routes. Indeed, these cyber infrastructures can be compromised by attacks on physical components such as heating, ventilation, and air conditioning (HVAC) systems, power-supply lines, and physical fiber connections; in particular, the latter two are typically routed through long stretches of unprotected areas, making them vulnerable to physical attacks. Consequently, the design and operation of these infrastructures must strike a balance between the cost of such degradations based on estimates and empirical data, in particular attacks, and the benefits of infrastructure reinforcements on the overall performance.

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy (DOE). The United States Government (USG) retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for USG purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-publicaccess-plan).

* Robert K. Abercrombie is also an Adjunct Professor, Department of Computer Science, University of Memphis, Memphis, TN 38152 robert.abercrcombie@memphis.edu.

978-1-4799-7560-0/15 $31.00 © 2015 IEEE
DOI 10.1109/SSCI.2015.74

In this paper, we present game-theoretic models that capture the interactions between an attacker and a defender to support rigorous design and analysis of a class of cyber infrastructures that consists of network and computing components. These constitute a subclass of more general infrastructures such as monitoring and control networks for the energy grid, intelligent transportation systems, nuclear plants, and hydroelectric dams; in the latter, in particular, cyber-attacks can degrade physical capabilities, in addition to physical attacks degrading the cyber capabilities.

A. Definitions

A smart grid is a modernized electrical grid that uses analog or digital information and communications technology to gather and act on information in an automated fashion to improve the efficiency, reliability, economics and sustainability of the production and distribution of electricity [3, 4]. Smart grid policy is organized in Europe as Smart Grid European Technology Platform [5], and as policy in the United States described in Title 42 of the U.S. Code [6].

In the context of cyber security, Title 44 of the U.S. Code [7] defines Information security as a means of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- **Integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; and
- **Availability**, which means ensuring timely and reliable access to and use of information.

B. Paper Organization

In this paper, the need for security in the introduction and define the key components of security – confidentiality, integrity, and availability if first introduced. In Section II, the case for applying current known Agent Based Game Theoretic (ABGT) simulation approaches to the Smart Grid subject domain is presented. In Section III, we describe four selected generic failure scenarios that are concentrating on the general failure scenarios functional area within the electric sector.

In Section IV, the experimental setup within the context of allowable states, actions, and the corresponding parameter modeling set necessary to execute the game is described. In Section V, experimental results from the simulation within the smart grid network via the model are presented. We initially address what constitutes a successful attack and then address the confidentiality, integrity and availability of the network. In the last section, we discuss conclusions and future work.

II. Problem Domain Discussion

The motivation for this work, is highlighted by existing and emerging technologies that complement The Roadmap for Cybersecurity Research in context of survivability of time-critical systems [8] and the President's Comprehensive National Cybersecurity Initiative [9] with respect to extending cyber security into critical infrastructure domains. The Roadmap synthesizes expert input from the control systems community, including owners and operators, commercial vendors, national laboratories, industry associations, and government agencies, to outline a coherent plan for improving cyber security in the energy sector. The plan provides a supporting framework of goals and milestones for protecting control systems for the foreseeable future: *By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions.* This is a bold vision that confronts the formidable technical, business, and institutional challenges that lie ahead in protecting critical energy control systems against increasingly sophisticated cyber-attacks [8]. The Cyberspace Policy Review, initiated by the White House, advised that "the Federal government should work with the private sector to define public private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources." Reference [10] recommended that as "the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks." The National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 (TWG1) consisting of industry experts, asset owners, and academia has developed a set of cyber security failure scenarios and impact analyses for the electric sector. Information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing [11]. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. The failure scenarios, impacts, and mitigations were developed from the "bottom-up," rather than a top-down assessment of potential cyber security events. The failure scenarios are organized in key functional categories, corresponding to the functional domains identified in the NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 [12]: demand response and consumer energy efficiency, wide-area situational awareness, energy storage, electric transportation, network communications, advanced metering infrastructure, distribution grid management, and cybersecurity.

The "Electric Sector Failure Scenarios and Impact Analyses" by the NESCOR Working Group Study [11], From the Section 5 electric sector representative failure scenarios [11], we extracted the four generic failure scenarios and grouped them into three specific threat categories (confidentiality, integrity, and availability) to the system. These specific failure scenarios serve as a demonstration of our simulation.

A. Known Solutions and Current Approach

The research and practicing community have been paying close attention to cyber security problems for more than two decades. However, Shiva et al. [13] state and it is generally agreed that the problem is far from being solved. In fact, some would argue that it is getting worse. As our dependence on the cyber infrastructure grows more complex and more distributed, the systems that compose it become more prone to failures and exploitation [14]. Failures in complex, tightly coupled systems can only be mitigated by collective decision making and organizational learning [15]. This is one way to view this game-theoretical approach.

The defender performs actions, which are governed by the probability of detecting that something is wrong or inconsistent with the normal state of operation within their enterprise (i.e., administrators may not actually recognize a zero day attack in progress). For our purposes, since the normal states are known, the simulation will try to limit the defender's actions, which is a counter action to the most current action performed by the attacker. Before the defender performs any counter action, a detection action is required to confirm the type of attack. In the simulation, our time unit represents one minute. One thousand (1,000) simulations were executed with each simulation spanning 250 simulated minutes, similar to [16, 17]. Experimental results were aggregated into bins and averaged to arrive at the probabilities of attack success within a given time slot as in [16, 17]. Information security analysis can thus be performed using game theory implemented in dynamic simulations using agent based models (ABMs). Such simulations can be verified with the results from game theory analysis and further used to explore larger scale, real world scenarios involving multiple attackers, defenders, and information assets. The major contributions of the work described in this paper include:

- A generalized approach to set up the rules of the game for our ABMs is flexible to accommodate arbitrary topologies and enterprise states.
- The ability to explore the range of feasible behaviors and incorporate imperfect information is facilitated simply by creating new rules that emulate new emergent behaviors. In this way, the analysis can evaluate the effect of a zero day. In such cases the defender is unprepared to deal with or defend against the scenario. Fig. 1 provides a State Transition Diagram (STD) that analyzes the case where defenders are unable to take defensive actions.
- The ability to assess the scalability of the defenders strategy addresses current limitations of stochastic game models. Such models only consider perfect information which assumes that: the defender is always able to detect attacks; the state transition probabilities are fixed before the game starts; the players' actions are always synchronous; most models are not scalable with respect to the size/complexity of the system under study.

III. Hypothesis Testing of Categories

Reference [11] organized the Smart Grid failure scenarios into six categories, which corresponds to the domains in [12] as 1) Advanced Metering Infrastructure (AMI), 2) Distributed Energy Resources (DER), 3) Wide Area Monitoring, Protection, and Control (WAMPAC), 4) Electric Transportation (ET), 5) Demand Response (DR), and 6) Distribution Grid Management (DGM). In addition, there are failure scenarios in a seventh cross-cutting category identified as "Generic," which includes failure scenarios that may impact the six original functional domains. We concentrated our analysis on the 4 failure scenarios which are generic [11].

The model presented here is based on the following four scenarios groups that address the collective three threat categories of confidentiality, integrity and availability. Our hypothesis claims that an ABGT simulation can represent the attacker/defender dynamics to ascertain the probability of successful attacks. Furthermore, in this experiment we believed the aforementioned scenarios could lend insight by accounting for likely offensive/defensive posturing. The following four subsections detail the chosen scenarios from the Electric Sector Failure Scenarios and Impact Analyses by the NESCOR Working Group Study [11].

A. *Generic.1 (G.1): Malicious and Non-malicious Insiders Pose Range of Threats*

Authorized personnel, who may be operators, engineering staff or administrators, become active threat agents with legitimate access to IT, field systems, and/or control networks.

B. *Generic.2 (G.2): Inadequate Network Segregation Enables Access for Threat Agents*

A threat agent compromises an asset that has access to the Internet via the "business" network. The asset on the business network also has access to a control system asset or network. The compromise of the business network asset provides a pivot point for the threat agent to gain control of a control system asset or network.

C. *Generic.3 (G.3): Portable Media Enables Access Despite Network Controls*

A threat agent introduces counterfeit firmware or software, a virus, or malware via removable media to obtain partial or total control of a device or networked system.

D. *Generic.4 (G.4): Supply Chain Attacks Weaken Trust in Equipment*

An adversary replaces a legitimate device with a maliciously altered device and introduces the device into the supply chain without directly compromising a manufacturing entity. This can be done by buying a legitimate device, buying or creating a malicious device and returning the malicious device in place of the legitimate device as an exchange. Alteration may be a modification or deletion of existing functions or addition of unexpected functions.

IV. Experimental Test Plan

Our ABGT models are based on previous works that have documented several attack scenarios [16-19]. The chosen case study was modeled from the failure scenarios identified as electric sector representative scenarios by domain [11].

A. *Baseline allowed states and actions*

Our distributed overall Smart Grid network is typical of the electric sector distribution configuration [15]. Our current model utilizes the following states adapted from [6], specifically addressing the Generic.1 (G.1), Generic.2 (G.2), Generic.3 (G.3), and Generic.4 (G.4) scenarios. The allowable states, actions and parameterization are provided in the following sections.

1) Allowable states

Table 1 assigns an integer to each state. The state transition diagrams enumerate each unique state. Note, that states 2a, 3a, 4.a, …, 13a represent the defenders actions.

2) Actions

An action is conducted by either an attacker or a defender, which causes the system to move from one state to another in a probabilistic manner with rewards (inaction is denoted Ø). All the allowable actions are provided in Table II and Table III.

3) Parameter modeling sets for STDs

The following section describes the intricacies of the STDs shown in Fig. 1. We label each transition with an action (see Tables II and Table III for the list of action labels), the probability of the transition, and the gain or cost in minutes of restorative effort incurred by the defender (or administrator). The X/Y/Z labels on the arcs indicate: X) Probability that the attacker chooses to attack, Y) Probability that the attack is successful and a Z) Reward for accomplishing that particular step (state transition). In a few cases (e.g., self-loop on state 2) we denote only the transition probability. For example, the self-loop of State 2 has P = 0.9375 = 1– (0.25*0.25) and the reward (R) is zero resulting in a label of ".9375/0". For State 3 the probability of staying in the current state is P=1-(0.25*0.25+0.25*0.25+0.25*0.25) = 0.8125.

In this scenario, the attacker gains no reward by remaining in state 2 (i.e., R=0). There are costs (negative values) and rewards (positive values) associated with the actions of the defender and attacker, respectively. The attacker's actions have mostly rewards and such rewards are in terms of the amount of damage he does to the network. Each attacker/defender game lasts 200 simulated minutes, and the values of the reward represent time in the game. Plus (+) means the game advances by that much time (in minutes) and negative (-) delays by that much time (in minutes). The attacker's actions gain (+) rewards and drive the game to completion to the attacker's advantage. Another way to think of rewards is in terms of the amount of damage he does to the network. Obviously some costs are difficult to quantify but others that decommission an asset for example are not. We utilize the following reward strategy: +10 for standard advance time reward, +100 for attacker success, -20 for routine restorative effort, and -100 for a significant restorative effort time to the defender. The time units represent minutes as in [18].

State 1 (normal operations) to State 2 (G.1 scenario) represents the case where an authorized person becomes an active threat agent. State 2 to 3 occurs when a threat agent inflicts significant damage on system either intentionally or by mistake. The defender (State 2 to State 2a) detects the threat agent. For State 3 to 3a, the defender detects significant damage. State 2a to State 1 (normal operation) detects/records threat agent presence and returns to normal operation. From State 3a to State 1, the defender records threat agent damage activity and returns to State 1 (normal operation).

From State 1 (normal operations) to State 4 (G.2 scenario) represents the case where a threat agent compromises an asset that has access to the Internet via the "business" network. State 4 to State 5 occurs when a threat agent gains control of a control system asset or network. The defender (State 4 to 4a) detects a compromised asset. For State 5 to State 5a, the defender detects the threat agent has gained access. State 4a to State 1 (normal operation) detects/records the compromised asset and returns to normal operation. State 5a to State 1, the defender records the threat agent has gained access and returns to State 1 (normal operation).

State 1 (normal operations) to State 6 (G.3 scenario) represents the case where a threat agent gains physical access to the system. State 6 to State 7 occurs where a threat agent introduces a threat via removable media. The defender (State 6 to State 6a) detects the threat agent's physical access. For State 7 to 7a, the defender detects threat agent's removable media activity. From State 6a to State 1 (normal operation) records threat agent activity and returns to normal operation. State 7a to 1, the defender records defender records the threat agent's removable media activity and returns to State 1 (normal operation).

State 1 (normal operations) to State 8 (G.4 scenario) represents the case where an adversary gains access with the intent to affect the Supply Chain. State 8 to State 9 occurs with an adversary replaces legitimate device. State 9 to State 10 occurs when an adversary introduces a malicious device into supply chain.

The defender (State 8 to 8a) detects the threat adversary. From State 9 to State 9a, the defender detects the threat adversary device replacement. From State 10 to State 10a, the defender detects that a malicious device has been introduced into the supply chain by the attacker. From State 8a to State 1 (normal operation), the defender records the threat agent activity and returns to State 1 (normal operation). From State 9a to State 1, the defender records the threat adversary device replacement and returns to State 1 (normal operation). From State 10a to State 1, the defender records the threat adversary malicious device in the supply chain and returns to State 1 (normal operation).

From States 3, 5, 7 and 10 to State 11, the threat agent exposes PII. From States 3, 5, 7 and 10 to State 12, the threat agent corrupts data. From States 3, 5, 7 and 10 to State 13, the threat agent causes large scale outages. From State 11 to State 11a, the defender detects and repairs PII and from State 11a to State 1, the defender returns to normal operations monitoring. From State 12 to State 12a, the defender detects and repairs corrupted data and from State 12a to State 1, the defender returns to normal operations monitoring. From State 13 to State 13a, the defender detects and repairs the larger scale outage and from State 13a to State 1, the defender returns to normal operations monitoring.

TABLE I. STATES

State	State Label
1	Normal Operations
2	G.1 Active threat agents
2a	Threat agents detected
3	G.1 Significant damage on system inflicted either intentionally or by mistake
3a	Significant damage detected
4	G.2 Threat agent compromised an asset that has access to the Internet via the "business" network
4a	Compromised asset detected
5	G.2 Threat agent in control of a control system asset or network.
5a	Threat agent access detected
6	G.3 Physical access gained
6a	Physical access detected
7	G.3 Threat introduced via removable media by threat agent
7a	Threat agent activity detected
8	G.4 Adversary threat agent access gained
8a	Adversary access detected
9	G.4 Legitimate device replaced
9a	Adversary replacement detected
10	G.4 Malicious device introduced into supply chain by adversary
10a	Adversary introduction into supply chain detected
11	PII exposed
11a	Exposed PII detected and repaired
12	Data corrupted
12a	Corrupted data detected and repaired
13	Large scale outage
13a	Large scale outage detected and repaired

TABLE II. STATE TRANSITIONS FOR GENERAL ATTACKS/DEFENSES

General	**Attacker**
1→2	Authorized personnel become active threat agent
2→3	Threat agent inflicts significant damage on system either intentionally or by mistake
1→4	Threat agent compromises an asset that has access to the Internet via the "business" network
4→5	Threat agent gains control of a control system asset or network
1→6	Threat agent gains physical access
6→7	Threat agent introduces threat via removable media
1→8	Adversary gains access
8→9	Adversary replaces legitimate device
9→10	Adversary introduces malicious device into supply chain
General	**Defender**
2→2a	Detect threat agent
3→3a	Detect significant damage
4→4a	Detect compromised asset
5→5a	Detect threat agent access
6→6a	Detect physical access
7→7a	Detect threat agent's removable media
8→8a	Detect adversary
9→9a	Detect replaced device
10→10a	Detect malicious device in supply chain
2a, 3a, 4a, 5a, 6a, 7a, 8a, 9a, 10a →1	Return to normal operations monitoring

TABLE III. STATE TRANSITIONS FOR CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

Confidentiality	**Attacker**
3, 5, 7, 10 →11	Threat agent exposes PII
Confidentiality	**Defender**
11→11a	Detect and repair exposed PII
11a→1	Return to Normal Operations monitoring
Integrity	**Attacker**
3, 5, 7, 10 →12	Threat agent corrupts data
Integrity	**Defender**
12→12a	Detect and repair corrupted data
12a→1	Return to Normal Operations monitoring
Availability	**Attacker**
3, 5, 7, 10 →13	Threat agent causes large scale outage
Availability	**Defender**
13→13a	Detect and repair large scale outage
13a→1	Return to Normal Operations monitoring

V. EXPERIMENTAL RESULTS

In this section we simulate the security of the enterprise network via the above model. We initially address what constitutes a successful attack and then address the confidentiality, integrity and availability of the enterprise network.

A. *Security Analysis – Probablity of a Successful Attack*

The probability of a successful attack is determined by the parameter modeling set as defined in Fig. 1. Fig. 2 illustrates the successful attacks in the enterprise network at each time interval (minutes), which is not cumulative. Fig. 3 shows the same data as a cumulative distribution indicating when the probability of successful attacks reaches 1 for the arrival rates

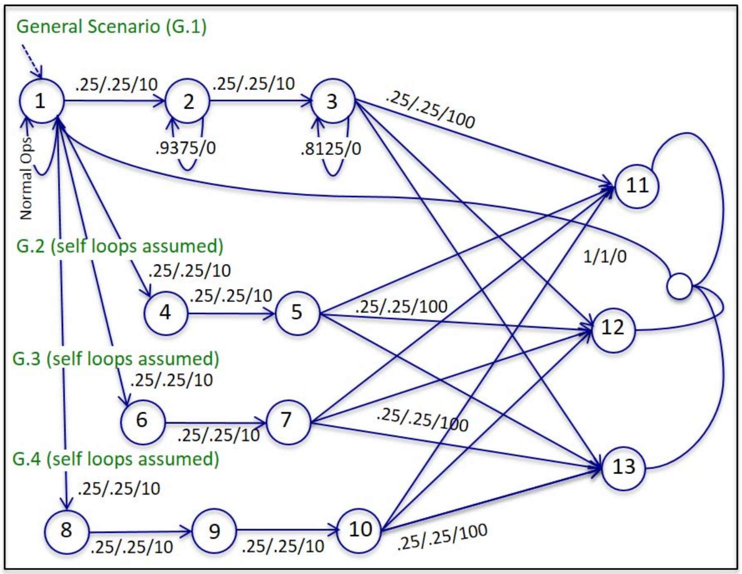

Fig. 1. State Transition Diagram (STD): actions of the attacker only (no defender). Note: Outing arcs from States 3, 5, 7 and 10 to States 11, 12 and 13 are .25/.25/100.

(0.12, 0.37, 0.63 and 0.88) respectively. This particular model illustrates that the attacker has a distinct advantage as the arrival rates of the attack increases.

B. Confidentiality

We define confidentiality as the absence of unauthorized disclosure of information (e.g., Personally Identifiable Information [PII]) [16, 17]. A measure of confidentiality is the probability that important data and information are not stolen or tampered. Confidentiality can be described as:

$$C = 1 - P_{PII\_exposed} \tag{1}$$

where $P_{PII\_exposed}$ is the probability that the attacker succeeds in reaching the "PII_exposed" State 11 in Table 1. Figure 4 (top panel) illustrates the confidentiality variation over the period of time for "PII_exposed."

C. Integrity

We define integrity as the absence of improper system alterations and/or data manipulation (i.e., preventing improper or unauthorized change) [16, 17]. Furthermore, integrity can be measured as the probability that network services are not affected, altered or damaged. Integrity can therefore be described as:

$$I = 1 - P_{Data\ Corrupted} \tag{2}$$

where $P_{Data\ Corrupted}$ denotes the probability that the attacker succeeds in corrupting data by reaching the "Data corrupted" State 12 in Table 1. Figure 4 (middle panel) illustrates the integrity variation over the period of time for "Data_corrupted." Again the arrival rate (or attack intensity) has an effect on the dynamics of the probability of the data being corrupted.

D. Availability

We define availability as a system or infrastructure being available when needed; associated computing resources can be accessed by authorized users [16, 17]. Moreover, availability is the ability by authorized users or systems to access information resources as necessary. The lack of availability is demonstrated by increased probability of disturbance when, for example, smart grid services are degraded/impeded. We express availability as:

$$A = 1 - P_{Large\_scale\_otuage} \tag{3}$$

where $P_{Large\_scale\_otuage}$ denotes the probability the attacker succeeds in causing disruptions leading to large scale outages in the worst case (State 13). Figure 4 (bottom panel) illustrates the availability dynamics in terms of large scale outages over time.

Comparing and contrasting Fig. 1 with the results in Figure 2-4, with respect to

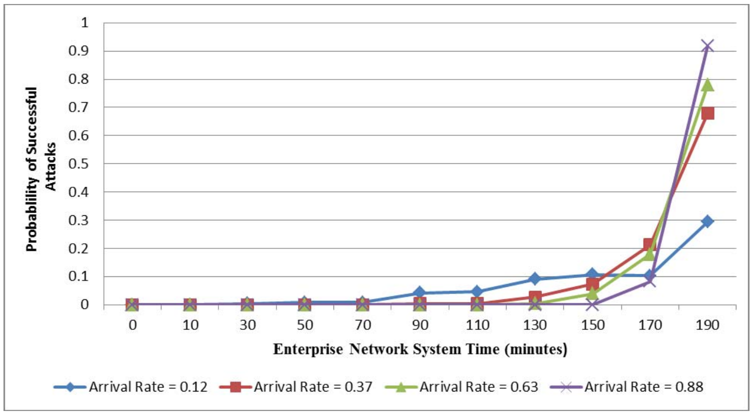

Fig. 2. The probability of successful attacks in the enterprise network per system time.

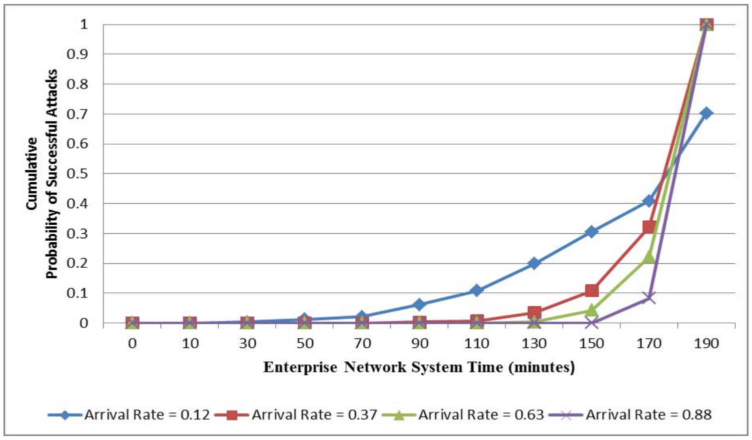

Fig. 3. The probability of successful attacks cumulatively in the enterprise network per system time.

confidentiality, integrity, and availability yields some interesting results. The variability of data in Fig. 4 shows similar results as a nearly 40% decrease in all three models security entities. This can be explained as all four generic failure scenarios converge on State 11, 12, 13 (Confidentiality, Integrity and Availability).

VI. Conclusions and Future Work

The use of game theory is a natural way to organize this investigation and the simulation results present an enormous amount of important and interesting data for analyses. Game theory has been used in many other problem analyses involving attacker-defender interaction. This smart grid subject domain is similar because a hacker on the Internet may wish to attack a smart grid network and the administrator of the smart grid network has to defend against the various actions of the attacker. Attack and defense actions cause the smart grid network to probabilistically change state. The attacker can gain rewards that represent different levels of importance. A small reward can be gained for example from reducing the cost of electricity. The smaller disruptions can be (often are) used as a stepping-stone to larger much more significant compromises (e.g., data corruption, compromise of PII, large scale outages). Meanwhile, on the other side of the game, an administrator can suffer damages that result in system downtime, theft or alteration of customer data, or impact to the supply chain, that may takes much longer to repair. The attacker's gain may or may not be of the same magnitude as the administrator's cost. Our current ABGT simulation is ideal for capturing the dynamics of these interactions. When compared to data in our previous works [16, 17], it is evident that the approach can be expanded to incorporate all of the steps that are involved in describing realistic failure scenarios [11] (i.e., the 4 selected generic failure scenarios from the 113 total scenarios: 32 AMI, 26 DER, 12 WAMPAC, 16 ET, 7 DR, and 16 DGM). Naturally, there can be more than one attacker per network and more than one administrator managing the network at the same time, which our model accommodates. It would appear that a multiplayer game model is more apt than the two player game model described here. Further, the current game makes no distinction as to the uniqueness in capability or identity of an attacker or for that matter a defender (administrator). In this model, we expanded our previous model to accommodate a team of attackers at different locations, and similarly for the defenders. In this way the two-player game model more closely reflect the real work and extend our analysis base of the AMI network security problem. We plan to incorporate the current findings as validated probability inputs to the econometric model described in [20-22]. In this way, we will be able to more realistically determine how much security is needed in the smart grid from both the utility's and customer's perspective. This is an important endeavor because in classical risk assessment approaches, the probabilities are usually guessed and not much guidance is provided on how to make the

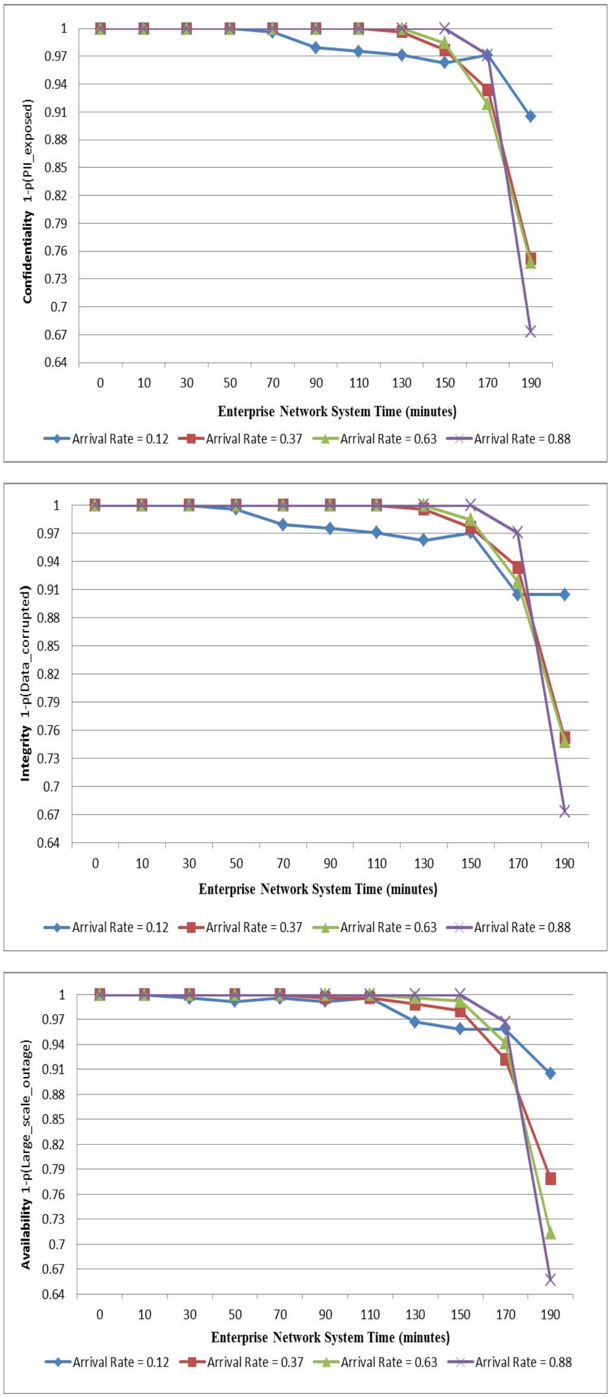

Fig. 4. Confidentiality ((PII_exposed), Integrity (Data_corrupted), and Availability (Large_scale_outage) attack impact on the Smart Grid enterprise network per system time.

probabilities accurate [23]. When coming up with probabilities, people are generally not well calibrated. Even though, this has been well documented for some time, we still need to better understand how sensitive these analyses are to changes in the modeling sets and to minor changes in the threat scenarios. Nonetheless, our ABGT simulations continue to addresses this very question because of its emphasis on collecting representative data to assist stakeholders in assessing the values of the outcomes of incidents rather than just collecting the likelihood or probability of various future incident scenarios that may not be stochastic.

Acknowledgment

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the University of Idaho, University of Memphis, Oak Ridge National Laboratory, the Department of Energy, or the U.S. Government.

References

[1] "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," The White House, Washington, D.C., Feburary 2003.

[2] S. H. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies"," in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS-37)*, HI, 2004, p. 20054a.

[3] (2015). *Smart Grid, US Department of Energy*. Available: http://energy.gov/oe/services/technology-development/smart-grid

[4] (2015). *Smartgrid.gov - Initiatives that Catalyze the Industry to Modernize the Grid*. Available: https://www.smartgrid.gov/the_smart_grid/

[5] (2013). *Smart Grids European Technology Platform*. Available: http://www.smartgrids.eu/

[6] "Public Printing and Documents," in *42 USC 152 Subchapter IX, Smart Grid*, ed. USA, 2007, pp. 17381-17386.

[7] "Public Printing and Documents," in *44 USC 3502*, ed. USA, 2009, p. 3542.

[8] "Roadmap to Secure Energy Delivery Systems," Energy Sector Control Systems Working Group, September 2011.

[9] "The Comprehensive National Cybersecurity Initiative (CNCI)," The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), January 2008.

[10] "Cyberspace Policy RevIew - Assuring a Trusted and Resilient Information and Communications Infrastructure," ed: The White House, 2009, pp. 1-76.

[11] "Electric Sector Failure Scenarios and Impact Analyses (Version 2.0)," in *National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1*, ed: Electric Power Research Institute (EPRI), 2014.

[12] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0," National Institute of Standards and Technology (NIST), Gaithersburg, MD NIST Special Publication 1108R2, February 2012.

[13] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. S. Wu, "A Survey of Game Theory as Applied to Network Security," in *43rd Hawaii International Conference on Systems Sciences Vols 1-5*, ed, 2010, pp. 880-889.

[14] C. Perrow, *Normal Accidents: Living with High-risk Technology*. Princeton: Princeton University Press, 1999.

[15] W. Sun, X. Kong, D. He, and X. You, "Information Security Problem Research Based on Game Theory," in *2008 International Symposium on Electronic Commerce and Security*, Guangzhou City, 2008, pp. 554-557.

[16] B. G. Schlicher and R. K. Abercrombie, "Information Security Analysis Using Game Theory and Simulation," in *WORLDCOMP'12 - The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing; SAM'12 - 2012 International Conference on Security and Management*, Las Vegas, NV, 2012, pp. 540-546.

[17] R. K. Abercrombie, B. G. Schlicher, and F. T. Sheldon, "Security analysis of selected AMI failure scenarios using agent based game theoretic simulation," in *47th Hawaii International Conference on System Sciences (HICSS)*, Big Island, HI, 2014, pp. 2015-2024.

[18] K.-w. Lye and J. M. Wing, "Game strategies in network security," *International Journal of Information Security,* vol. 4, pp. 71-86, 2005.

[19] Y. Wang, M. Yu, J. Li, K. Meng, C. Lin, and X. Cheng, "Stochastic game net and applications in security analysis for enterprise network," *International Journal of Information Security,* vol. 11, pp. 41-52, 2012.

[20] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Failure impact analysis of key management in AMI using cybernomic situational assessment (CSA)," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, Oak Ridge, Tennessee, 2013, pp. 1-4.

[21] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Risk Assessment Methodology Based on the NISTIR 7628 Guidelines," in *2013 46th Hawaii International Conference on System Sciences (HICSS)*, Wailea, Maui, HI USA, 2013, pp. 1802-1811.

[22] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Quantifying the impact of unavailability in cyber-physical environments," in *2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, 2014, pp. 1-8.

[23] L. Rajbhandari and E. Snekkenes, "Mapping between Classical Risk Management and Game Theoretical Approaches," in *Communications and Multimedia Security*. vol. 7025, B. Decker, J. Lapon, V. Naessens, and A. Uhl, Eds., ed: Springer Berlin Heidelberg, 2011, pp. 147-154.