2014 47th Hawaii International Conference on System Science

Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation

Robert K. Abercrombie, Bob G. Schlicher, and Frederick T. Sheldon
Computational Sciences and Engineering Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6085
abercrombier@ornl.gov, schlicherbg@ornl.gov, sheldon@ieee.org

Abstract

Information security analysis can be performed using game theory implemented in dynamic Agent Based Game Theoretic (ABGT) simulations. 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. We concentrated our analysis on the Advanced Metering Infrastructure (AMI) functional domain which the National Electric Sector Cyber security Organization Resource (NESCOR) working group has currently documented 29 failure scenarios. The strategy for the game was developed by analyzing five electric sector representative failure scenarios contained in the AMI functional domain. From these five selected scenarios, we characterize them into three specific threat categories affecting confidentiality, integrity and availability (CIA). The analysis using our ABGT simulation demonstrates how to model the AMI functional domain using a set of rationalized game theoretic rules decomposed from the failure scenarios in terms of how those scenarios might impact the AMI network with respect to CIA.

1. Introduction

Today's security, economic, and industrial systems depend irrevocably on the security of a myriad of devices and the networks that connect them together. These networks operate in an ever-changing threat environment. Adversaries are applying increasingly sophisticated methods to exploit flaws in software, telecommunication protocols, and operating systems; to infiltrate and exploit command, control, and communications capabilities, economic infrastructure, and vulnerable cyber-physical control systems; or exfiltrate sensitive data, and to obtain control of networked systems in order to prepare for and execute attacks. Information security continues to evolve in response to disruptive changes with a persistent focus on information-centric controls. A healthy debate is needed to address balancing endpoint and network protection, with a goal of improved enterprise / business risk management.

Traditional network security solutions, typically employing firewalls and intrusion detection devices do not have a quantitative decision framework [1]. To this end, a few groups of researchers have started advocating the utilization of game theoretic approaches [1]. Game Theory provides mathematical tools and models for investigating multi-player strategic decision making. Another technique that is promising is the application of simulations [2].

1.1. Definitions – Basis of Endeavor

Title 44 of the U.S. Code [3] 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.

1.2. Paper organization

In this paper, we first introduce the need for security in the introduction and define the key

The manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S Government retains a nonexclusive, royalty free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

978-1-4799-2504-9 2014

DOI 10.1109/HICSS.2014.255

IEEE computer society

components of security – confidentiality, integrity, and availability. In Section 2, we present our case for applying current known ABGT simulation approaches to the Smart Grid subject domain. In Section 3, we describe five selected failure scenarios concentrating on the Automated Metering Infrastructure (AMI) functional area within the electric sector. In Section 4, we describe our experimental setup within the context of allowable states, actions, and the corresponding parameter modeling set necessary to execute the game. In Section 5, we present our experimental results from the simulation within the AMI network via the model. We initially address what constitutes a successful attack and then address the confidentiality, integrity and availability of the AMI network. In the last section, we discuss conclusions and future work.

2. Problem Discussion

In September 2011, the DOE's Office of Electricity Delivery and Energy Reliability published the Roadmap to Secure Control Systems in the Energy Sector [4]. 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 (10 years): *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 [4].

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." The review 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" [5].

Table 1. Numeric State Labels (Sect. 4.1.1)

1	Normal operations
2	Communications bus monitored
2a	Detect communications bus monitoring
3	Secret key acquired
4	Secret key passed
5	Secret key compromised
5a	Detect secret key compromised
6	AMI usage data manipulated
6a	Detect AMI usage data manipulated
7	Duplicate APN for GSM cellular network on AMI network created
8	Meters within range associated with fake APN
8a	Detect meters associated with fake APN
9	Unauthorized devices create disruption of cellular based functions in AMI network
10	Meters do not receive messages from AMI network
10a	Detect meters not receiving DR messages detected
11	Customers pay more for power and/or experience loss of power
11a	Detect customers experiencing loss of power
11b	Detect customers AMI billing errors
12	Unauthorized devices gain access to HAN
12a	Detect unauthorized devices gain access to HAN detected
13	End customer devices do not receive DR messages
13a	Detect end customers devices not receiving DR messages
14	Customers pay more for power and/or customers suffer loss of usage of device requiring power
14a	Detect Customers experiencing loss of HAN device requiring power
14b	Detect customers HAN billing errors
15	Time stamping gets out of sync between meter and AMI head-end
15a	Detect time stamping out of sync conditions
16	Meters ignore legitimate commands
16a	Detect meters ignoring legitimate commands
17	Large scale outage due to utility inability implement DR
17a	Detect large scale outage due to utility inability implement DR messaging

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 [6]. 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

Table 2. State transition names (CI) Sect. 4.1.2

Confidentiality	**Attacker**
1→2	Monitor communications bus
2→3	Acquire secret key
3→4	Pass secret key
4→5	Compromise secret key
5→2	Continue monitoring
5→6	AMI usage data (PII) manipulated/accessed
Confidentiality	**Defender**
2→2a	Detect communications bus monitoring
5→5a	Detect secret key compromised
6→6a	Detect AMI usage data manipulated
2a→1	Record monitoring activity and return to normal operations
5a→1	Replace Compromised Secret Key and Perform Mass Metering Rekeying
6a→1	Re-establish encryption and correct AMI network
Integrity	**Attacker**
1→7	Duplicate APN for GSM cellular network on AMI network created
7→8	Meters within range associate with fake APN
8→9	Create disruption of cellular based functions within AMI network
9→10	Cause DR messages to not reach end -customers devices
10→11	Cause customers pay more for power and/or customers suffer loss of usage of device requiring power
Integrity	**Defender**
8→8a	Detect meters associated with fake APN
10→10a	Detect meters not receiving DR messages
11→11a	Detect Customers experiencing loss of power
11→11b	Detect customers AMI billing errors
8a→1	Associate meters with true APN
10a→1	Ensure meters receiving DR messages
11a→1	Reconnect customers experiencing loss of power and ensure customers are propering connected
11b→1	Correct customers AMI billing errors

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 [7]: Demand response and consumer energy efficiency, Wide-area situational awareness, energy storage, electric transportation, network communications, advanced metering infrastructure (AMI), distribution grid management, and cybersecurity. From the Section 3 AMI failure scenarios [6], we extracted six specific 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 ABGT simulation.

Table 3. State transition names (A) Sect. 4.1.2

Availability	**Attacker**
1→12	Gain access to HAN via unauthorized devices and create DOS
12→13	Cause meters to not receive messages
13→14	Cause customers pay more for power and/or customers suffer loss of usage of device requiring power
1→15	Cause time stamping to get out of sync between meter and AMI head-end
15→16	Cause meters to ignore legitimate commands
16→17	Cause large scale outage due to utility -inability to implement DR messaging
Availability	**Defender**
12→12a	Detect unauthorized devices access to HAN
13→13a	Detect end customers devices not receiving DR messages
14→14a	Detect customers experiencing loss of HAN device requiring power
14→14b	Detect customers HAN billing errors
15→15a	Detect time stamping out of sync conditions
16→16a	Detect meters ignoring legitimate commands
17→17a	Detect large scale outage due to utility inability to implement DR messaging
12a→1	Remove unauthorized devices connected to HAN
13a→1	Ensure end customers devices receiving DR messages
14a→1	Reconnect customers experiencing loss of HAN device requiring power
14b→1	Correct customers HAN billing errors
15a→1	Provide periodic checks of time synchronization and resynchronize AMI Network
16a→1	Ensure meters receiving legitimate commands
17a→1	Check Integrity of DR and restart DR as needed

2.1. Known solutions and current approach

Researchers have recently advocated game theoretic approaches to making designed-in-security decisions [1]. Game theory provides mathematic tools and models for investigating multi-player strategic decision-making. Lye and Wing's work [8] presented a game theoretic method for analyzing the security of computer networks. The interactions between an attacker and the administrator were modeled as a two-player stochastic game for which best-response strategies (Nash Equilibriums) were computed. Mahimkar and Shmatikov [9] proposed a new protocol for preventing malicious bandwidth consumption and demonstrated how game based formal methods can be successfully used to verify availability-related security properties of network protocols. Liu et al. [10] presented a general incentive-based method to model attacker intent, objectives, and strategies (AIOS) and a

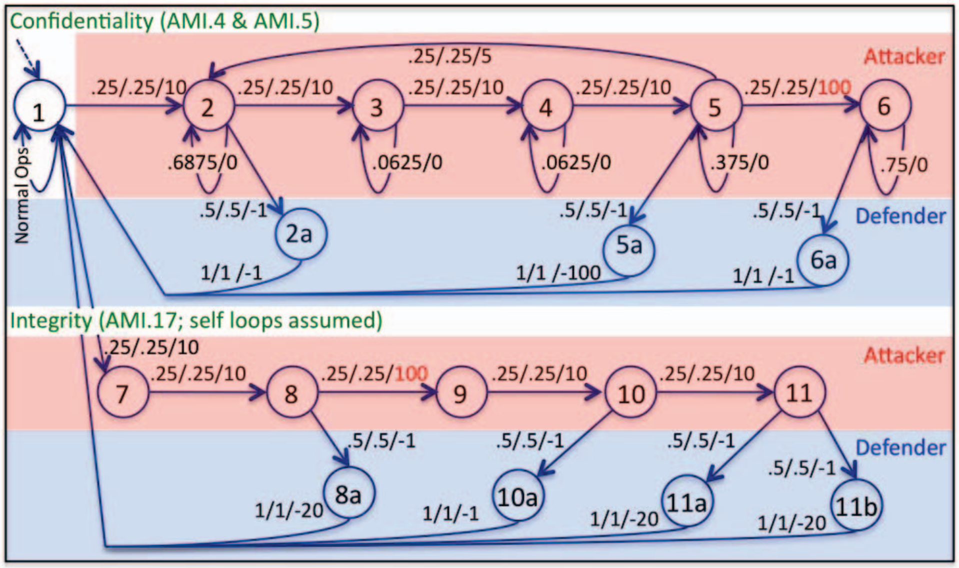

Figure 1. State transition diagram for confidentiality and integrity.

game theoretic approach to infer AIOS. The authors developed a game theoretic AIOS formalization that can capture the inherent interdependency between AIOS and defender's objectives and strategies in such a way that AIOS can be automatically inferred. Schlicher and Abercrombie [11] expanded on these works and presented a game theoretic generalized computational simulation engine using an agent based approach. The simulation incorporates agents which are active components of the model that represent and engage in the dynamics of interactions on a scenario-by-scenario basis among players (attackers and defenders).

Each ABGT simulation takes as input a model (i.e., rules of the game) of a specific failure scenario of interest (e.g., attack on integrity). Typically, these types of rule-based models are used to simulate evolutionary game theory involving multiple players in both cooperative and competitive or adversarial postures [12, 13]. The models bring significant benefits when: (1) interactions between the agents are complex, nonlinear, discontinuous or discrete; (2) space is crucial and the agents' positions are not fixed; (3) the population is heterogeneous; (4) the topology of the interactions are heterogeneous and complex; or (5) the agents exhibit complex behavior, including learning and adaptation [12, 13]. The agents in the simulation include the attacker and the defender (or administrator). The agents perform actions that can change the system state of the enterprise. For each state, agents are limited in the actions they can perform. Depending on the scenario, the attacker executes one of many actions with an associated probability of deciding to do the action and a probability that the action will be successful once the decision has been committed. Within each time unit, the simulator thread visits each agent giving them the opportunity to perform an action or not [11].

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 AMI 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

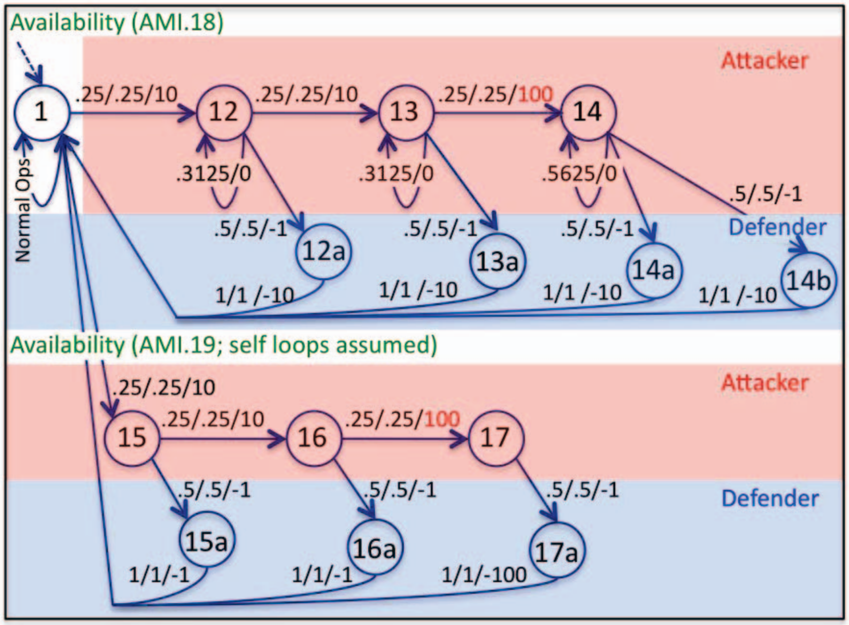

Figure 2. State transition diagram for Availability.

simulation spanning 250 simulated minutes, similar to [11]. Experimental results were aggregated into bins and averaged to arrive at the probabilities of attack success within a given time slot as in [11].

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. Figure 3 provides a 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.

3. Hypothesis Testing of Categories

We concentrated our analysis on 29 failure scenarios from the AMI [6]. The models presented here are based on the following five scenarios grouped into three threat categories. 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.

1) **Confidentiality**
   a) AMI.4 (overused key captured on meter bus enables usage data manipulation) and
   b) AMI.5 (mass meter rekeying required when common key compromised)
2) **Integrity**
   a) AMI.17 (malicious creation of duplicate APN prevents valid AMI messages)
3) **Availability**
   a) AMI.18 (unauthorized devices create DoS and prevent valid demand response [DR] messages), and
   b) AMI.19 (out of sync time-stamping causes discard of legitimate commands)

AMI.18 & 19 are special cases of the Failure Scenario: DR.1: Blocked DR messages result in increased prices or outages. The following six subsections detail the chosen scenarios directly from [6].

3.1. AMI.4: Overused key captured on meter bus enables usage data manipulation

Meters are deployed with the same symmetric cryptographic key on all meters in the AMI implementation. A threat agent is able to acquire the secret encryption key after monitoring communications on the internal bus of one of these meters. The secret key is passed in the clear on the bus. Usage data is then manipulated to overstate/understate energy usage or to under/overstate energy production from Distributed Energy Resources (DERs).

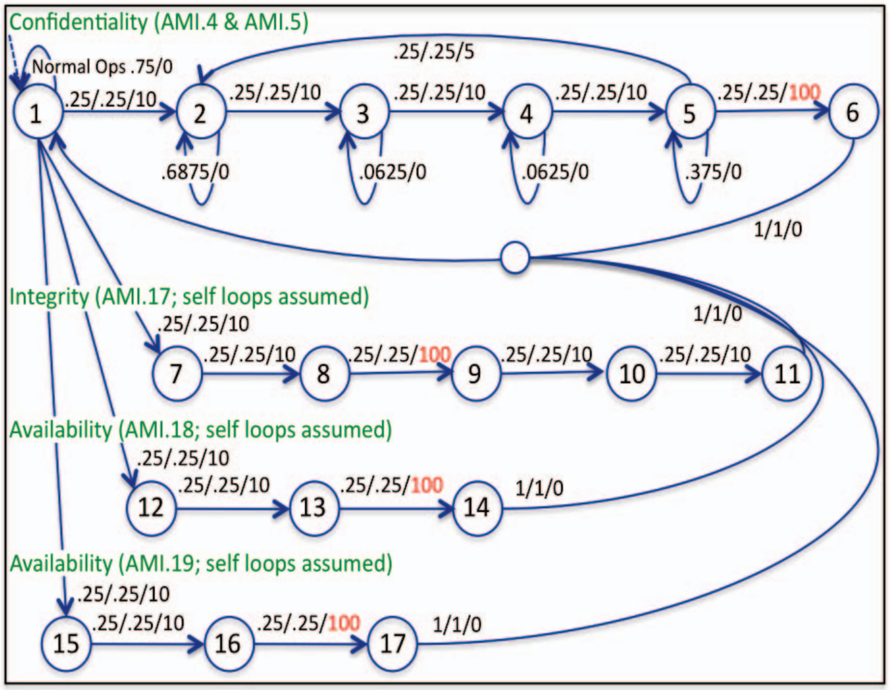

Figure 3. State Transition Diagram (STD): actions of the attacker only (no defender).

3.2. AMI.5: Mass meter rekeying required when common key compromised

Meters are deployed with the same symmetric cryptographic key on all meters in the AMI implementation. Key compromise occurs in the field due to the ability to extract the secret key when in physical possession of a meter, or during distribution of keys to meters. In this failure scenario, no known financial or energy usage information is actually compromised due to the compromised key, but all the meters still need to be rekeyed to mitigate the potential for future malicious activities.

3.3. AMI.17: Malicious creation of duplicate APN prevents valid AMI messages

A malicious individual creates a duplicate Access Point Name (APN) for the Group Special Mobile (GSM)-based cellular communications on an AMI network. The meters that are within the range then associate with the fake APN and do not receive messages from the AMI network.

3.4. AMI.18: Unauthorized devices create DoS and prevent valid DR messages)

Unauthorized devices gain access to a home area network (HAN). The devices can then be used to create a Denial-of-Service (DoS) condition so that DR messages cannot reach end customer devices. (Note: this is a special case of DR.1.)

3.5. AMI.19: Out of sync time-stamping causes discard of legitimate commands

Time-stamping, sometimes used to detect replay attacks, gets out of sync between a meter and its respective AMI head-end system, causing the meter to ignore legitimate commands it interprets as a potential replay attack. This causes loss of advanced metering functionality such as two-way communications, remote connect/disconnect, and metrology. (Note: this is a special case of DR.1.)

3.6. DR.1: Blocked DR messages result in increased prices or outages

A threat agent blocks communications between a demand response automation server (DRAS) and a customer system (smart meters or customer devices). This could be accomplished by flooding the communications channel with other messages, or by tampering with the communications channel. These actions could prevent legitimate DR messages from being received and transmitted. This can occur at the wired or the wireless portion of the communications channel.

4. Experimental test plan

Our ABGT models are based on previous works that have documented several attack scenarios [8, 11, 14]. The chosen case study was modeled from the failure scenarios identified in sub-sections [6]. Our enterprise network topology illustrated in Figure 1 provides a generic basis to apply the selected failure scenarios.

4.1. Baseline allowed states and actions

Our distributed overall AMI network is typical of the electric sector distribution configuration [15]. Our current model utilizes the following states adapted from [6], specifically addressing the AMI.4, AMI.5, AMI.17, AMI.18, and AMI.19 scenarios with supporting information from DR.1. The allowable states, actions and parameterization are provided in the following sections.

4.1.1. Allowable states

Table 1 assigns an integer to each state. The state transition diagrams enumerate each unique state. Note, that states like 5a represent the defenders actions.

4.1.2. 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 Tables 2 – 3.

4.1.3. Parameter modeling sets for STDs

The following section describes the intricacies of the state transition diagrams (STDs) of Figures 1-3. We label each transition with an action (see Tables 2-3 for the list of action labels for all the transitions), 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 = 0.6875 = 1– (0.25*0.25 + 0.5*0.5) and the reward (R) is zero resulting in a label of ".6875/0". For State 3 and 4 the probability of staying in the current state is P=1-(.25*.25) = 0.0625; for State 5 the probability of staying in the current state is P=1-(.25*.25+.25*.25+.5*.5) = .375. For State 6, the probability of staying in the current state is P=1-(.5*.5) = 0.75.

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 250 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 [8].

Confidentiality AMI.4 & AMI.5 combined: From State 1 (normal operations) to State 2 represents the case where an attacker is monitoring the communication bus. State 2 to 3 occurs when a secret key is acquired. State 3 to 4 occurs when the secret key is passed. State 4 to 5 occurs when the key is compromised via decryption. State 5 to 2 enables continued monitoring of the communication bus. State 5 to 6 results when AMI usage data is manipulated. The defender (State 2 to 2a) detects the communication bus is being monitored. For State 5 to 5a, the defender detects that a secret key has been compromised. The State transitions from State 6 to 6a represent the detection that AMI usage data has been compromised (exposed) by the attacker. State 2a to 1 (normal operation) detects/records monitoring activity and returns to normal operation. State 5a to 1 replaces the compromised secret key by performing (up to mass) rekeying. State 6a to 1 reestablishes encryption (confidentiality of data) on the AMI network to mitigate future malicious activity such as exfiltration of PII.

Integrity AMI.17: From State 1 (normal operations) to State 7 represents the case where a duplicate APN (Access Point) is created by an attacker on the GSM Cellular AMI network. State 7 to 8 occurs when meters within range associate with the duplicate APN. State 8 to 9 the attacker has gained the advantage by disrupting the cellular base functions within the AMI network. State 9 to 10 results in loss of DR messages between the head-end and the various customers meter (or associated devices). State 10 to 11 is the effect of customers having to pay more for their power (i.e., the payment system integrity is altered as a result). The defender (State 8 to 8a) detects meters associated with duplicate (spoofed) APN. For State 10 to 10a, the defender detects end customer meters not receiving DR (demand/response) messages. The State transitions from State 11 to 11a and 11b represent the detection of customers experiencing loss of power and detection of customers experiencing AMI billing errors respectively. State 8a to 1 (normal operation) associates the meters with the correctly authenticated (true) APN. State 10a to 1 ensures meters are correctly receiving DR messages once again. State 11a to 1 and 11b to 1 ensures that customers are properly reconnected and billing errors are corrected respectively.

Availability AMI.18: From State 1 (normal operations) to State 12 represents the case where an attacker has gained access to home area network (HAN) via unauthorized devices which ultimately cause a denial-of-service and consequently DR

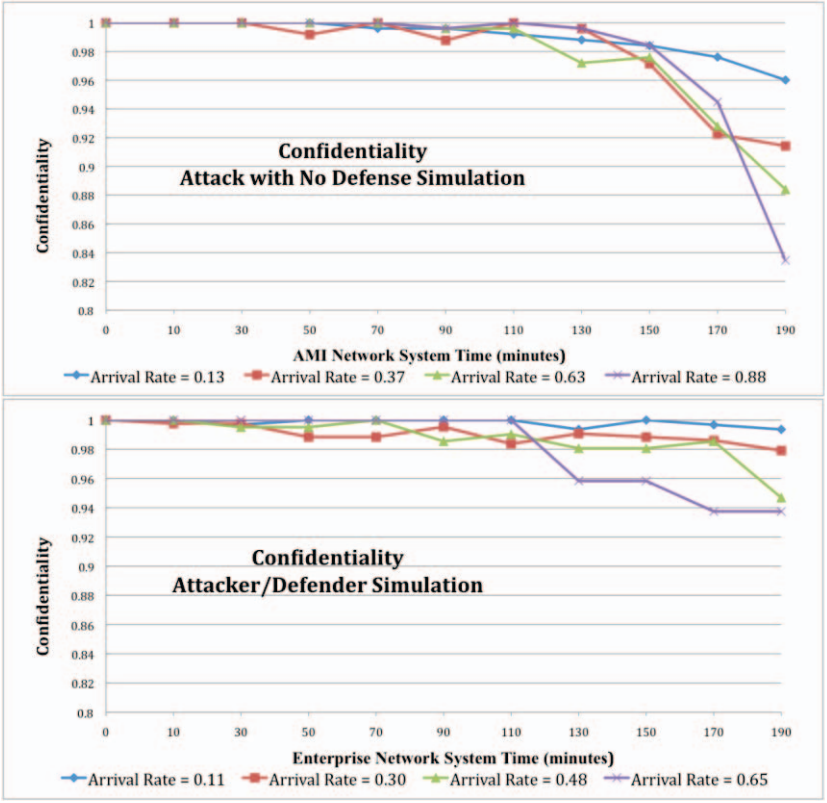

Figure 4. Confidentiality: (1) attacker only (no defense), (2) attacker/defender interplay.

messages can not reach the end customer devices. The transition from State 12 to 13 occurs when the unauthorized devices cause meters to not receive messages. The transition from State 13 to 14 causes customers to pay more for power and/or for customers to suffer the loss of usage of devices requiring power. The defender (from State 12 to 12a) detects unauthorized devices have gained unauthorized access to the customers HAN. The transition from State 13 to 13a represents the defender detecting end customer devices that are not receiving valid DR messages. The transitions from 14 to 14a or to 14b detects that a customer has lost HAN devices requiring power or detects HAN billing errors respectively. The state transition from State 12a to 1 removes unauthorized devices connected to the HAN. The state transition from 13a to 1 ensures that end user devices are receiving proper DR messages. The state transition from State 14a/14b to 1 reconnects experiencing loss of HAN devices requiring power and corrects customer HAN billing errors respectively.

Availability AMI.19: From State 1 (normal operations) to State 15 represents the case when an attacker causes time stamping to become out of synchronization between the meters and the head-end. This causes meters to ignore legitimate commands (State 15 to 16). Transitioning from State 16 to 17 results in large scale outages due to the utility's inability to implement DR messaging between the meter and the AMI head-end. The defender (from State 15 to 15a) detects time stamping out of synchronization conditions. The transition from State 16 to 16a detects meters ignoring legitimate commands (e.g., the meter enters a state where it believes that it is subject to a replay attack). The transition from State 17 to 17a detects large scale outages due to the utility's inability to implement DR messages. State 15a to 1 (normal operation) provides periodic checks of time synchronization, and integrity and availability protections for the time synchronization protocol and resynchronizes the AMI network. State 16a to 1 (normal operation) ensures that meters are receiving legitimate commands. State 17a to 1 provides DR message integrity checks and restarts the demand response automation server (DRAS) as needed.

5. Experimental results

In this section we describe the results (probability of successful attack) from the simulations of the five failure scenario models. In Figure 4 (top panel) we initially address what constitutes a successful attack (states 1 through 6) with no defender response (only monitoring the communications bus) to baseline the effect of no defense. We repeated this logic as shown in Figure 3 (1 to 7-11, 1 to 12-14, 1 to 15-17) obtaining similar results to Figure 4 top panel. In the next series of experimental runs we allow the defender to apply his complete complement of detection and recovering mechanisms and addressing the confidentiality, integrity and availability categories as shown in Figure 4 (bottom panel) and Figure 5 (top and bottom).

The probability of complete and secure CIA is shown in Figure 4 and 5 over time. The interesting aspect is to see the effect on CIA over time for the different attack arrival rates. Further, we benchmark the curve/slope of each attack arrival rate and as a reference point the probability dynamics over the course of the simulation periods.

5.1 Confidentiality

We define confidentiality as the absence of unauthorized disclosure of information (e.g., Personally Identifiable Information [PII]) [11]. A measure of confidentiality is the probability that important data and information are not stolen or tampered. Confidentiality can be described as:

$$C = 1 - P_{AMI\_usage\_data\_manipulated} \quad (1)$$

Where $P_{AMI\_usage\_data\_manipulated}$ is the probability that the attacker succeeds in reaching the "data manipulated" State 6. Figure 4 (top panel) illustrates the confidentiality variation over the period of time for $P_{AMI\_usage\_data\_manipulated}$ with no defense. Figure 4 (bottom panel) shows the attacker/defender interplay over time (up to 190 minutes). The attacker with the highest arrival rate produces the greatest gains (i.e., decrease in confidentiality).

5.2 Integrity

We define integrity as the absence of improper system alterations and/or data manipulation (i.e., preventing improper or unauthorized change) [11]. Furthermore, integrity can be measured as the probability that network services are not affected, altered or damaged. Integrity can therefore be described as:

$$I = 1 - P_{DR\_messages\_to\_not\_reach\_end\_customers\_devices} \quad (2)$$

where $P_{DR\_messages\_to\_not\_reach\_end\_customers\_devices}$ denotes the probability that the attacker succeeds in preventing DR messages from reaching end customer's devices (States 9 through 10: the effect causes customers to pay more for their power and that the payment system integrity is altered as a result). Figure 5 (top panel) illustrates the dynamics of integrity in terms of $P_{DR\_messages\_to\_not\_reach\_end\_customers\_devices}$ over time. Again the arrival rate (or attack intensity) has an effect on the dynamics of the probability of the DR messages reaching end customers' devices.

5.3 Availability

We define availability as a system or infrastructure being available when needed; associated computing resources can be accessed by authorized users [11]. 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 meter infrastructure (i.e., AMI) services are degraded/impeded. We express availability as:

$$A = 1 - P_{Cause\_meters\_to\_not\_receive\_messages} \qquad (3)$$

Here $P_{Cause\_meters\_to\_not\_receive\_messages}$. denotes the probability the attacker succeeds in causing meters to not receive DR messages, which in turn causes *out_of_sync_time_stamping* to occur, which may lead to *large_scale_outages* (State 17). Figure 5 (bottom panel) illustrates the availability dynamics in terms of $P_{Cause\_meters\_to\_not\_receive\_messages}$ over time.

Comparing and contrasting Figures 1-3 with the results in Figure 4 and 5, with respect to confidentiality, integrity, and availability yields some interesting results. The variability of data in Figure 4 (top panel) shows nearly a 20% range in variability. The variability of data in Figure 4 (bottom panel) and Figure 5 (both panels) show only a 4-5% range. These variabilities reflect the interplay of the attacker and the defender and the defensive poster as it is accounted for in the state transitions: State X → State Xa → State 1.

6. Conclusions and future work

The use of game theory is a natural way to organize this investigation and the simulation results present lots of interesting data for analyses. Game theory has been used in many other problem analyses involving attacker-defender interaction. This AMI subject domain is similar because a hacker on the Internet may wish to attack an AMI network and the administrator of the AMI network has to defend against the various actions of the attacker. Attack and defense actions cause the AMI 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 compromises (e.g., mass rekeying, compromise of PII, large scale outages). Meanwhile, on the other side of the game, an administrator can suffer damages that result in system downtime or theft of customer data. 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 [11], it is evident that the approach can be expanded to incorporate all of the steps that are involved in describing realistic failure scenarios [6] (i.e., 5 selected

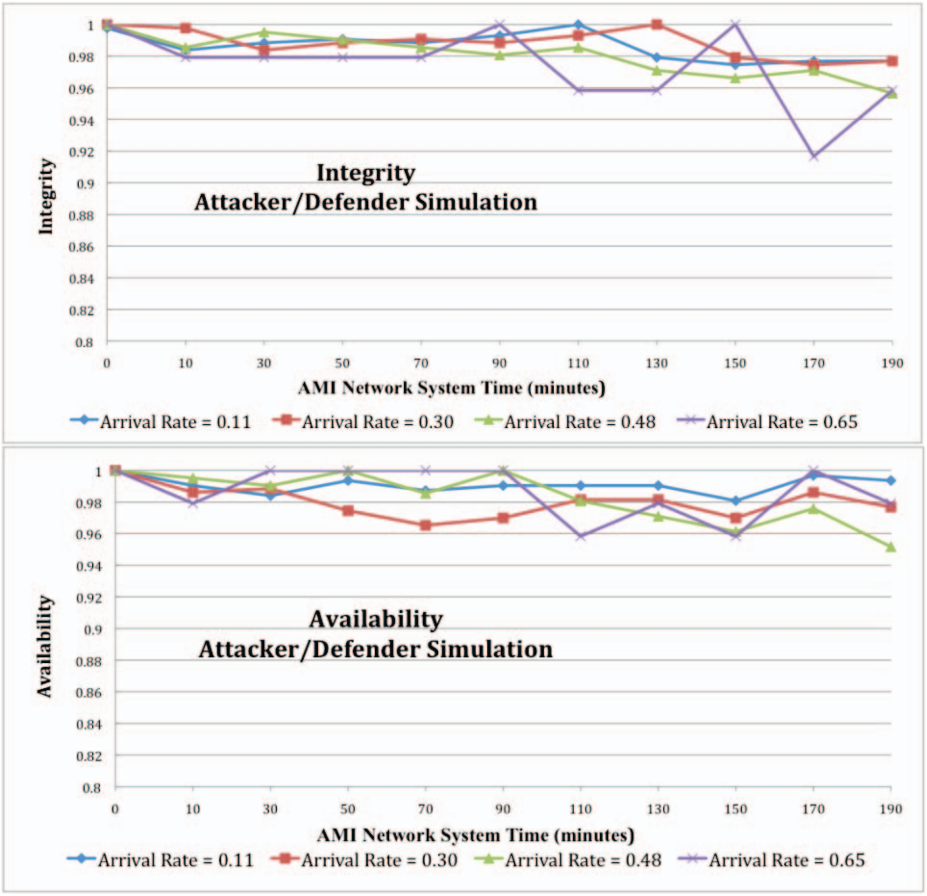

Figure 5. Integrity (1) and Availability (2): attacker/defender interplay.

scenarios from the 29 total AMI scenarios).

Naturally, there can be more than one attacker per network and more than one administrator managing the network at the same time. 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 the future, we plan to expand the model to accommodate a team of attackers at different locations, and similarly for the defenders. In this way the two-player game model will 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 [16, 17]. In this way, we will be able to more realistically determine how much security is needed in the AMI 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 probabilities accurate [18]. When coming up with probabilities, people are generally not well calibrated. We 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 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.

7. References

[1] 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.

[2] H. Gintis, *The Bounds of Reason: Game Theory and the Unification of the Behavioral Sciences*: Princeton University Press, 2009.

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

[4] "Roadmap to Achieve Energy Delivery Systems Cybersecurity," Energy Sector Control Systems Working Group, September 2011.

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

[6] A. Lee, "Electric Sector Failure Scenarios and Impact Analyses - Draft," in *National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1* vol. Version 0.9, ed. Washington, D.C., 2013.

[7] "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, 2012.

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

[9] A. Mahimkar and V. Shmatikov, "Game-based analysis of denial-of-service prevention protocols," in *Computer Security Foundations, 2005. CSFW-18 2005. 18th IEEE Workshop*, 2005, pp. 287-301.

[10] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," *ACM Trans. Inf. Syst. Secur.,* vol. 8, pp. 78-118, 2005.

[11] 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.

[12] E. Bonabeau, "Agent-Based Modeling: Methods and Techniques for Simulating Human Systems," *Proceedings of National Academy of Sciences,* vol. 99 Suppl 3, pp. 7280-7287, 2002.

[13] A. Nowak, "On Stochastic Games in Economics," *Mathematical Methods of Operations Research,* vol. 66, pp. 513-530, 2007.

[14] 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.

[15] "Roadmap to Secure Energy Delivery Systems - Draft Update," Energy Sector Control Systems Working Group, January 11, 2011.

[16] 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.

[17] 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.

[18] L. Rajbhandari and E. Snekkenes, "Mapping between Classical Risk Management and Game Theoretical Approaches," in *Communications and Multimedia Security*. vol. 7025, B. Decker*, et al.*, Eds., ed: Springer Berlin Heidelberg, 2011, pp. 147-154.