Cost Modeling of Response Actions for Automated Response and Recovery in AMI

Ahmed Fawaz, Robin Berthier, and William H. Sanders
Electrical & Computer Engineering Dept., Information Trust Institute, and Coordinated Science Laboratory
University of Illinois at Urbana-Champaign. Emails: {afawaz2, rgb, whs}@illinois.edu

***Abstract*—The smart grid is creating new security vulnerabilities due to the deployment of networked devices into the traditional grid. A core component of the smart grid is the advanced metering infrastructures (AMIs), which increase the attack surface due to smart devices deployed at households. Manual management of security incidents in such a large and complex system is impractical, and the need for automated response and recovery to attacks is critical. This paper addresses that challenge through two main contributions. First, we introduce and classify an extended set of AMI-specific cyber incident response actions. Second, we define a cost model and an approach to translate security properties into monetary costs. The cost model is a key element in enabling an automated response engine to make optimal decisions and mitigate cyber incidents.**

***Index Terms*—AMI, CPS, Response action, Cyber security.**

I. Introduction

Advanced metering infrastructures (AMIs) are a core component of the smart grid effort. AMIs are the communication infrastructure for smart meters that transmit real-time meter readings to the administrative network and receive remote commands to control service. AMIs enable new applications, such as fine-grained measurements and instant detection of blackouts, and thus improve customer service and reliability.

However, AMIs also introduce significant security concerns, since the processing and communication capabilities of AMI devices allow for a larger attack surface. That attack surface includes 1) the corporate network, 2) the wireless mesh network, 3) the home area network, and 4) meters that are within the reach of customers. Possible threats can be classified according to attack scale, ranging from relatively small-scale activity targeting specific customers (e.g., to turn off service or specific appliances, such as alarm systems) or stealing energy (e.g., through the alteration of meter readings), up to major organized crimes that could target extended geographical regions. Moreover, attacks could target the control commands sent by a utility through the AMI. Additional security issues also rise from the use of wireless solutions for smart meter communication, in particular through the deployment of large mesh networks [1]–[3].

Researchers and organizations have made important efforts to promote security solutions for AMIs, such as VPNs, encryption [4], and remote attestation [5]. Those approaches are valuable, but they are not sufficient, mainly because vulnerabilities can always be found in the implementations of protocols and applications, or in human operators who can be tricked into providing access to restricted resources. Moreover, since meters may not have sufficient physical protection, tampering with devices may leak secret keys stored in internal memory and thus cause security breaches in the network. Thus, traditional attack prevention solutions must be supplemented with detection and mitigation approaches. While recent efforts have started to investigate the role of AMI intrusion detection (e.g., [6], [7]), response to incidents is still a manual procedure in the hands of security administrators.

The goal of this paper is to explore the concept of automated cyber incident response for AMIs. This concept is of critical importance due to 1) the potentially unmanageable volume of alerts and demands for decisions in such a large infrastructure, and 2) the stringent timing and availability requirements of certain power grid functions. In particular, utilities should be able to get the latest meter readings and send out control commands according to specific schedules. Additionally, disruption of services, such as outages, should be detected and addressed with minimum input from human operators. Automatic response to cyber incidents requires a solution that can process input sent by intrusion detection systems, assess the security state of the infrastructure, and select the best response action to mitigate issues in a timely manner. This paper addresses those challenges as follows:

- we review existing automated response frameworks and discuss their limitations,
- we introduce an extensive set of AMI-specific response actions through a taxonomy and the identification of key response characteristics, and
- we present a cost model to enable automated reasoning, and we introduce a set of approaches to computation of cost parameters.

II. Background

The goal of AMIs is to support two-way communications among smart meters, smart appliances, and utilities. Since AMIs can reach huge scales (sometimes more than a million meters) and have to accommodate a variety of environments (i.e., urban, suburban, and rural), several architectures have been proposed for deployment of flexible and cost-efficient communication infrastructure at scale.

A. Meter Communication

As shown in Figure 1, possible options for connecting meters to the utility include two hierarchical approaches and a direct approach.

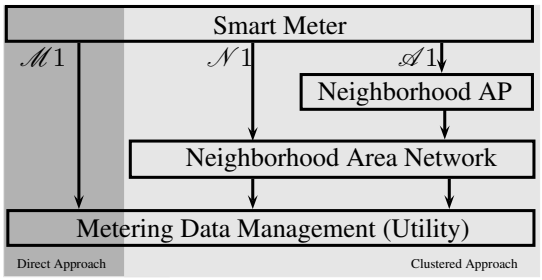

Fig. 1. Complete view of AMI architectures

1) Hierarchical Approaches: Hierarchical topologies enable the architecture to scale well with an increasing customer base. The goals are to cluster meters geographically and to use one or two aggregation levels to relay communication to and from the utility. Figure 1 presents both aggregation levels by showing that a meter can connect to the meter data management (MDM) system inside the utility network through either a collector in the neighborhood area network (NAN) or a second-level neighborhood access point (NAP). A NAP is added to increase scalability. A variety of technologies can be used to deploy the communication links labeled $\mathscr{N}1$ and $\mathscr{A}1$ in Figure 1:

- **Wireless mesh networks** allow for dynamic route generation and route healing. This scheme is the cheapest to implement, and it scales if an optimal placement of collector nodes is used. It is suitable for residential areas where interference between meters is minimal. However, it is prone to a wider class of attacks that can cause availability, integrity, and privacy issues. Examples are physical communication protocols like IEEE 802.15.4 and the proprietary RFLAN [8].
- **Power line communication (PLC)** carries information on power lines by modulating messages to a frequency other than 50Hz. This technology does not require new infrastructure. It is suitable when wireless solutions are not practical, such as in high rises. However, because of the varying impedance, noise, and high attenuation use of the power line as a channel increases the complexity of the modulator at the meter side [9]. Moreover, since the carrier is the electricity itself, losing a line means losing both power and communication.
- **Wireless Star** uses a collector node that directly connects to each meter. Such schemes include WiMax or cellular communication that incurs a communication fee per meter. It is suitable for low-density areas, such as rural areas.
- **Private wired networks** run by utilities, where a utility would deploy a private network infrastructure (e.g., cable or fiber optic) among meters. This approach is costly, but provides a higher level of security because of the closed nature of the network.

Those hierarchical approaches increase the attack surface by adding collectors, relays, and repeaters to the infrastructure. The attack surface varies depending on the choice of communication technology. For example, wireless communications can be vulnerable to a wide class of attacks, such as jamming, man-in-the-middle, and eavesdropping. That technology choice also impacts the set of response actions available. For instance, it may not be easy to quarantine a node in the case of a wireless mesh network.

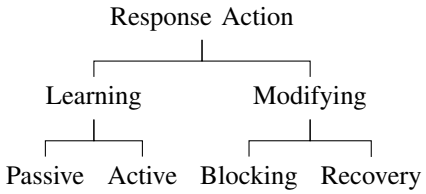

Fig. 2. Response action taxonomy

2) Direct Approach: In this scheme, meters directly communicate with the utility through $\mathscr{M}1$ [10]. This approach uses cellular communication (GSM, 3G), WiMax, or leased lines as the communication technology. Direct communication generally offers the security advantage of removing an attack vector by making the network hard to access. However, the scheme adds extra communication cost per meter for the utility and has a scalability issue, especially in dense areas.

B. HAN Connectivity

For the purpose of enabling demand-response and load shedding, utilities have to gain detailed measurements and control over some of the customer loads. With the advent of smart appliances, utilities have the ability to decrease demand for electricity during peak times by remotely sending price information and even control commands to appliances. Appliances that are most likely to be remotely controlled are high-power-consuming appliances (electric cars, washers, dryers, or HVAC). The communication technology for the home area network (HAN) that connects appliances to the AMI is usually ZigBee. This connectivity brings significant privacy and security issues, since it could enable an adversary to spy on appliance usage, or even to disable specific loads such as a security system. To balance the needs of demand-response applications and privacy and security concerns, several architectures have been proposed. The meter can be the gateway between the HAN and the utility. With a Zigbee radio integrated in the meter, it delivers load-shedding commands from the utility [10]. The HAN gateway can also be connected to the utility through a separate WAN [11], and even use the Internet to receive and send information and commands. The considered architecture leads to the worst case attack surface.

III. Response Actions

In this section, we present an extensive set of response actions designed to actively mitigate cyber incidents. Our first effort towards defining those actions was to create a generic taxonomy of actions. Several taxonomies have already been proposed for response actions [12]–[14], but most are not suited for AMIs. Our taxonomy, presented in Figure 2 reflects the typical intrusion response process: collecting information, blocking or limiting attacks, recovering from attacks, and performing forensics. This taxonomy has been helpful for

TABLE I
ORGANIZED SET OF RESPONSE ACTIONS FOR AMIS

Learning	Passive	LP1	Log information
		LP2	Generate reports
		LP3	Generate alarm
		LP4	Profile customers' power usage
		LP5	Passive power book keeping
	Active	LA1	Start analysis tools
		LA2	Verify ARP caches
		LA3	Trace connections
		LA4	Enable dormant IDS sensors
		LA5	Detect duplicate nodes
		LA6	Locate routing attacks
		LA7	Request logs
		LA8	Add decoy nodes
Modifying	Blocking	MB1	Block meter
		MB2	Isolate neighborhood
		MB3	Revoke meter keys
		MB4	Restart meter
		MB5	Block connections
		MB6	Limit network access
		MB7	Limit system/service access
		MB8	Enable quarantine
		MB9	Jam Attacker
		MB10	Change IP addresses
	Recovery	MR1	Rollback previous responses
		MR2	Merge neighborhood network
		MR3	Distribute attack signature
		MR4	Renew keys of meters/utility
		MR5	Correct C12.22 routing tables
		MR6	Verify meter OS
		MR7	Apply patches
		MR8	Restart meter
		MR9	Replace meter
		MR10	Recover meter readings
		MR11	Recover service state

1) exploring the set of possible response actions following a structured approach, and 2) understanding the characteristics of the various actions that are primordial in the definition of cost models. We used the attack trees presented in [15] to map the set of actions to attack techniques and ensure a sufficient coverage of the threat model. The resulting set of actions is presented in Table I.

A. Learning Actions

Actions LP1, LP2, LP3, and LA1 involve log generation and collection. Those actions are applicable to all architectures. LP4-5 are related to power measurements and are also architecture-independent. Active learning actions are mainly used to deploy new sensors or to change sensor configurations in order to collect more activity. Those actions are more efficient when the same activity is visible to multiple sensors. Thus, they are suitable in the case of a shared medium (e.g., wireless or PLC) if meters can be used as sensors.

Actions LA1, LA2, LA5, and LA6 are related to verifying routes and detecting routing attacks. If wireless mesh communications are used, then cooperative behavior is needed to verify routes and detect routing attacks (e.g., man-in-the-middle, wormhole, and black hole attacks) [16], [17]. The responses typically consist of checking routing tables and caches on routers (e.g., cell relays), and sending probe packets to the mesh to verify that routing paths are correct. Action LA4 enables more IDS sensors using meters or utility trucks.

B. Modifying Actions

Modifying actions are mostly architecture-and technology-dependent, because the goal of those actions is to induce changes in the network. First, blocking actions aim to limit the access and privileges of a compromised entity in the network. Architectures and communication technologies provide a variety of control functions and granularity. For example, action MB1, "blocking a meter," can be performed by removing the meter from the utility registration list, which is a suitable action for all architectures but may still allow a compromised meter to attack other devices. In the case of a hierarchical topology, a more effective response is to update firewall rules at the level of the collector or the cell relay to block a compromised meter locally. In addition, if a wireless mesh network is used, quarantine of a meter can be performed through updating of routing information of neighboring meters.

Action MB6 includes rate limiting and is applicable to all architectures. The rate-limiting threshold can vary according to the level at which it is applied in the network topology. The scope of this action also depends on the granularity of the rate-limiting solution. For example, if individual flows for a specific device cannot be isolated, rate limiting at the level of a relay will impact a full neighborhood and will likely affect noncompromised devices. It is also possible to apply rate limiting the level of the head-end by delaying packet processing for compromised meters.

Recovery actions attempt to return the system to a secure state. They deconstruct operations performed by attackers and require a detailed understanding of the AMI security state. For example, action MR6 checks the integrity of a meter's operating system. Actions MR7-8 can then be used to put the meter back into a secure and working state. MR9 would be used if a recovery is not possible (e.g., the meter has been physically damaged). An important action is MR1, which enables utilities to reverse the effect of one or several response actions. If an action is performed based on incorrect information, or if an attacker is able to take advantage of it, then canceling the action may be necessary. Note that different actions have different rollback levels, ranging from fully reversible (e.g., adding decoy nodes), to irreversible but with removable effects (e.g., blocking a connection), to fully irreversible (e.g., alerting an intruder).

The rollback capability is an important characteristic to take into consideration when calculating a cost model for

each action, since irreversible actions are likely more expensive for utilities than reversible actions are. We defined the following set of characteristics to help us understand cost parameters and to guide the response engine: 1) rollback level, 2) applicability to specific architectures and communication technologies, 3) system-level involvement (i.e., whether an action can be performed locally by a single device, or requires multiple devices to cooperate on a wider scale), 4) flexibility (e.g., the rate-limiting threshold can be tuned dynamically), 5) the system layer impacted (e.g., physical, network, or application layer), and 6) manual involvement, ranging from none (fully automated action) to some (input required from an operator). That last characteristic is critical if an action can have potentially unsafe effects.

IV. Towards a Cost Model

Automated response and recovery systems have to make decisions after assessing the security state of the system. Those decisions require predicting the positive and negative effects of different combinations of attack steps and responses. That element of needing to predict the behavior of multiple entities explains why game theory has often been used in implementing automated reasoning systems for security [18]. To obtain accurate predictions, it is necessary to have a cost model. Automated response systems cannot decide on optimal actions without a cost model. "Optimization" usually means minimization of the cost for the organization, either locally or globally [19]. Moreover, the performance of any recovery algorithm depends on the quality of the cost model. A cost model that does not reflect the complete and real cost of an action might lead to suboptimal or counterproductive actions.

A survey of the literature indicates that availability of services is used as a main metric in computing costs for traditional IT systems. For example, e-commerce systems require high availability to keep customers, and loss of availability is proportional to loss of revenue. However, an AMI is a large cyber-physical system in which the cost of an action is linked to the physical system controlled by the AMI. Using availability as the cost metric doesn't represent the actual cost for a utility. Additionally, customers play an important role in the system, since they are directly affected by outages, price updates, and energy delivery services. As a result, we propose a cost model that goes beyond service availability and considers three entities: utilities, customers, and attackers.

A. Related Work

We can divide past research on cost models into three categories: models based on static costs, models based on parameterized costs with static parameters, and models based on dependency graphs. In the first category, the approach consists of generating a taxonomy of response actions for general IT systems and then tagging each action with a static cost value [12], [13], [20]–[23]. Those costs have to be assigned by system administrators based on their subjective knowledge of the system. The issue with this approach is that it does not capture the system dynamics (i.e., an action that induces changes in a system may affect the costs of subsequent actions). Moreover, requiring administrators to assign cost values is often impractical, and results in inaccuracies.

In the second category, [24], [25] decompose the cost of actions into several parameters to better capture how actions may impact the system. [26] assigns static costs for each parameter and uses an analytical hierarchy process to compute impact factors. [27] proposes to use static costs that would linearly increase over time. The advantage of these approaches is that the cost model captures more aspects of the actual cost for the utility. However, use of static parameters still does not capture system dynamics.

In the third category, [28] proposes to model the system using a dependency graph. The graph is used to compute the availability by propagating the impact of nodes becoming unavailable due to a response action. This work was later extended in [29] to cover all security properties (CIA) by proposing to use three separate graphs (one for each property) and adding links between the graphs when dependencies among the properties are found. Finally, [30] combines the three graphs into one by labeling the nodes with a vector and used a matrix to model the relation among the different security properties. The importance of this approach is that it enables the modeling of system dynamics to capture the effect of an action on the system. However, the problem is that it still requires considerable work from system administrators to define parameter values in the graph. Moreover, the resulting output vector represents the total effect on the CIA properties and would require additional processing to be used by an automated reasoning system.

B. Approach

The objective of a cost model is to evaluate the real cost of an action for utilities and customers. The notion of cost can be divided into a managerial cost (i.e., operational cost, recovery cost, and labor cost), an attack cost, and a cost due to the impact of an action on the system. Consequently, the cost of an action is computed using the following equation:

$$C_{Action} = C_{Impact} + C_{Operation} + C_{Attack}, \qquad (1)$$

where $C_{Operation}$ is the operation cost, which includes the cost of labor to initiate the action and the resources required to run the action. The latter will likely increase over time, which means that the duration of a response action has to be evaluated. That evaluation can be done based on experience or computed using a simulation of the system. C_{Impact} is the cost of the impact of the action on the system. We characterize that impact by measuring the changes to the system that positively or negatively affect confidentiality, integrity, and availability (CIA). Those changes are captured through a dependency graph model of an AMI that include devices (e.g., meters) and entities (e.g., customers and utilities). Prediction of the effects of a response action is achieved through updating of the dependency graph and computation of a vector that characterizes the impact of actions on each security property. The impact must be converted into financial values in order to

TABLE II
COST BREAKDOWN FOR EACH SECURITY PROPERTY AND SERVICE

	Integrity	Availability	Confidentiality
Real-time Pricing	Electricity Market		N/A
Usage Readings	Market	SLA	Empirical Data
Service Commands	SLA	SLA	

be combined with the managerial cost and to be evaluated across different configurations. This conversion requires a financial understanding of the repercussions of AMI actions on the grid. We rely on the electricity market, service-level agreements (SLAs), the cost of outages, customer revenues, and customer retention factors to assess the costs of impacts, such as unavailable services or power outages. (We illustrate our approach to conversion of response impact into financial values in Section IV-D.) Finally, C_{Attack} is the cost of the consequences of an attack on the system and is discussed in the next subsection.

C. Cost Effectiveness

Evaluation of the cost of a response represents half of the information needed by the decision algorithm to choose an optimal response strategy. One also has to evaluate how effective a response is in mitigating attacks. We propose to use the cost of an attack as a measure of effectiveness. A response $R1$ is defined as more effective than a response $R2$ if the cost of the attack for $R1$ is less than that for $R2$. To compute the cost of an attack, we make the following differentiation based on the taxonomy of response actions. *Learning actions* allow the attack to keep running while being monitored, so their costs include both the cost of the running attack and the cost of the running action. *Limiting actions* are intended to stop or reduce the impact of attacks. Their costs are mostly represented by the resources required for their implementation.

The cost of an attack often has high uncertainty, because we cannot predict the next attack steps planned by attackers. We are currently investigating using a simulation framework such as ADVISE [31] to simulate adversaries. The stochastic model defined in ADVISE allows for subjective evaluation of several threat models, offering results on attack likelihood, system weaknesses, attack duration, and attacker strategy based on attacker preferences and system configuration.

D. Converting Impact into Financial Values

In this section, we explore how to compute the cost of the deterioration of security properties of AMI services due to a response action or an attack. We illustrate our approach through a case study that includes 3 AMI services. Those services are 1) real-time pricing information sent by utilities to meters, 2) usage readings sent by meters to collection engines, and 3) control commands sent by utilities to meters. Table II shows the information source used to evaluate the impact on integrity, availability, and confidentiality of those 3 services.

1) **Pricing Information:** After deregulation of the energy sector, distribution companies began buying energy from the electricity market. The price of electricity in the market is dictated by the rules of supply and demand. Utilities will sell electricity to the customer at market rate. Thus, the utility will send real-time pricing information to customers. Customers will use the pricing information to determine their level of power consumption. Loss of availability and integrity of such information leads to costs for both the utility and customers.

a) Availability: If pricing information is unavailable or delayed, we assume that the customer will be sold electricity at an incorrect flat rate, causing losses for either the customer or the utility. If the current rate is greater than the flat rate, then the utility will be losing revenue by paying more for power than the price at which it is selling it. In the opposite case, the customer will be overbilled, paying a higher price for electricity. That can lead to customer dissatisfaction and long-term revenue losses for the utility.

b) Integrity: Integrity loss for pricing information would lead to inaccurate information delivered to meters. If the received information shows a value higher than the real market price, then no losses are incurred but customer dissatisfaction is possible. However, if the received information shows a value lower than the real market price, then customers will be billed for the original price, which also leads to loss of confidence in the utility. It may result in increased demand due to the low price, potentially causing generation perturbations.

2) **Meter Readings:** The primary goal of AMIs is to automate meter readings. Readings are sent periodically by meters to the collection engine in the back-end. Usage information is used to bill customers for the electricity used and also to gain detailed information about load profiles so that usage can be better forecasted.

a) Availability: Availability of the information is crucial for billing. If information is lost, the utility has to estimate usage. Moreover, the metering company may pay a penalty for the loss of availability, as defined in the SLA.

b) Integrity: Inaccurate usage information leads to inaccurate billing information. If the information leads to a decrease in the actual usage (e.g., due to energy theft attempts), then the utility would lose revenue.

3) **Utility Commands:** Utility commands are used to control the AMI network, e.g., by turning service on or off, or by controlling smart appliances. Availability and integrity of those commands are important to ensuring that the energy delivery system works properly.

a) Availability: The metering company pays a penalty for loss of availability, as defined in their SLA. In addition, unavailability of utility commands would reduce the ability to diagnose problems and outages in the power grid. Moreover, unavailability of commands would delay critical services, such as remote connect or remote disconnect of customers.

b) Integrity: Integrity loss in utility commands may lead to faulty control over the grid. If a control command is altered, it might lead to overcharging of customers, or even disconnection of customers from the grid.

4) **Confidentiality:** Some of the services provide public information, such as pricing information. Thus, loss of confidentiality has no financial impact for either the customer or

the utility. However, access to control commands and usage information might lead to privacy violations for the customer (e.g., loads could be identified, and usage profiled). The cost of privacy violation is difficult to assess. We are investigating techniques that use empirical metrics, such as historical court records, to evaluate the violation of privacy policies.

V. Conclusion

This paper presented an approach to understanding the role of automated responses for AMIs. We introduced a set of cyber incident response actions that are suitable for AMIs. The definition of those actions followed a rigorous process that included a review of the possible AMI architectures and communication technologies, the definition of a response taxonomy, and the identification of key response characteristics. We then proceeded to define an attack/response cost model that, unlike traditional cost models, takes into account the cyber physical nature of an AMI by integrating system dynamics to capture the potentially significant consequences for the power grid. As future work, we plan to formalize the cost model using power models. We are also working on implementing the actual automated response system for AMIs over the TCIPG AMI testbed, which contains a hybrid network of real and emulated meters.

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000097. The authors would like to thank Jenny Applequist for her editorial assistance.

References

[1] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," in *Proceedings of the 42nd Annual Southeast Regional Conference*.

[2] L. Buttyán and J. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2007.

[3] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–380, Feb. 2006.

[4] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011.

[5] M. LeMay and C. Gunter, "Cumulative attestation kernels for embedded systems," in *Computer Security ESORICS 2009*.

[6] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *In Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 350–355.

[7] Y. Zhang, L. Wang, W. Sun, I. Green, M. Alam *et al.*, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.

[8] G. Picard, H. Van Wyk, F. Monier, J. Bartier, and A. I. Clave, "Metering rflan protocol and cell/node utilization and management," Patent WO2 008 033 514, 2008.

[9] N. Pavlidou, A. Han Vinck, J. Yazdani, and B. Honary, "Power line communications: State of the art and future trends," *IEEE Communications Magazine*, vol. 41, no. 4, pp. 34–40, April 2003.

[10] CEN and CENELEC, "Functional reference architecture for communications in smart metering systems," European Committee for Electrotechnical Standardizations, Tech. Rep. CEN/CLC/ETSI/TR50572, December 2011.

[11] S. Ravens, "Great britain smart meter infrastructure: Analysis of potential architectures," Dec 2010, White Paper. [Online]. Available: http://www.datamonitor.cloud.ipdgroup.com/detail/OI00034-006

[12] W. Lee, W. Fan, M. Miller, S. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response," *Journal of Computer Security*, vol. 10, no. 1-2, pp. 5–22, 2002.

[13] S. Tanachaiwiwat, K. Hwang, and Y. Chen, "Adaptive intrusion response to minimize risk over multiple network attacks," *ACM Trans on Information and System Security*, vol. 19, pp. 1–30, 2002.

[14] N. Stakhanova, S. Basu, and J. Wong, "A taxonomy of intrusion response systems," *International Journal of Information and Computer Security*, vol. 1, no. 1, pp. 169–184, Jan. 2007.

[15] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in *SmartGridComm 2012*. IEEE, 2012, p. To Appear.

[16] S. Marti, T. Giuli, K. Lai, M. Baker *et al.*, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, 2000, pp. 255–265.

[17] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *In Proceedings of the IEEE Symposium on Security and Privacy*, May 2005, pp. 49–63.

[18] S. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A game-theoretic intrusion response and recovery engine," in *In Proceedings of the IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*. IEEE, 2009, pp. 439–448.

[19] K. J. Qian, Tipper, *Intrusion Response Systems: A Survey*, 1st ed. Morgan Kaufmann, 2007, ch. 13, pp. 377–412.

[20] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, and S. Dubus, "Risk-aware framework for activating and deactivating policy-based response," in *In Proceedings of the 4th International Conference on Network and System Security (NSS)*, Sept. 2010, pp. 207–215.

[21] Y. Wu and S. Liu, in *In Proceedings of the 12th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*.

[22] Z. Zhang, X. Lin, and P.-H. Ho, "Measuring intrusion impacts for rational response: A state-based approach," in *In Proceedings of the Second International Conference on Communications and Networking in China (CHINACOM)*, Aug. 2007, pp. 317–321.

[23] B. Foo, Y.-S. Wu, Y.-C. Mao, S. Bagchi, and E. Spafford, "Adepts: Adaptive intrusion response using attack graphs in an e-commerce environment," in *In Proceedings of the International Conference on Dependable Systems and Networks (DSN)*, 2005.

[24] Z. Zhang, P.-H. Ho, and L. He, "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach," *Computer Security*, vol. 28, no. 7, pp. 605–614, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404809000273

[25] C. Strasburg, N. Stakhanova, S. Basu, and J. Wong, "The methodology for evaluating response cost for intrusion response systems," Technical Report 08-12, Iowa State University, Tech. Rep., 2008.

[26] N. Anuar, S. Furnell, M. Papadaki, and N. Clarke, "A risk index model for security incident prioritisation," pp. 25–39, 2011.

[27] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, "A game theory based risk and impact analysis method for intrusion defense systems," in *In Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications (AICCSA)*, May 2009, pp. 975–982.

[28] T. Toth and C. Kruegel, "Evaluating the impact of automated intrusion response mechanisms," in *In Proceedings of the 18th Annual Computer Security Applications Conference*, 2002, pp. 301–310.

[29] M. Jahnke, C. Thul, and P. Martini, "Graph based metrics for intrusion response measures in computer networks," in *In Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN)*, Oct. 2007, pp. 1035–1042.

[30] N. Kheir, H. Debar, N. Cuppens-Boulahia, F. Cuppens, and J. Viinikka, "Cost evaluation for intrusion response using dependency graphs," in *In Proceedings of the International Conference on Network and Service Security (N2S)*, June 2009, pp. 1–6.

[31] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using adversary view security evaluation (advise)," in *In Proceedings of the 8th International Conference on Quantitative Evaluation of Systems (QEST)*, Sept. 2011, pp. 191–200.