Chapter 8

DISTRIBUTED IP WATCHLIST GENERATION FOR INTRUSION DETECTION IN THE ELECTRICAL SMART GRID

Ray Klump and Matthew Kwiatkowski

Abstract The electric power infrastructure in the United States is undergoing a significant transformation. To enhance the ability of the grid to support the use of diverse and renewable energy resources and to respond to problems more quickly, the infrastructure is being redesigned to include greater options for automation, measurement and control. An enormous communications system will underlie the network of smart grid sensors and actuators. Devices will send messages to each other to coordinate control activity and formulate corrective strategies. The diversity and scale of this network will pose significant security challenges, especially since the number of entities charged with managing the grid will be large. A means for sharing information about cyber risks within the smart grid communications infrastructure is sorely needed. This paper proposes a strategy for sharing cyber security risks among smart grid stakeholders to enable them to identify attacks and mitigate their effects. The approach is inspired by the federated model, a cyber risk communications strategy employed by several U.S. national laboratories.

Keywords: Smart grid, federated model, intrusion detection

1. Introduction

The electric power grid is a complex interconnected control system of enormous scale and diversity. Disturbances in one part of the grid can profoundly impact conditions far away, despite control actions that are designed to isolate their impact. Different loads exhibit different dynamic response characteristics; different energy sources exhibit different availability profiles and rates of response to fluctuations in demand; and different units of protection equipment

respond at different rates to different signals. Furthermore, measurements of the system are reported at vastly different rates and are required by different applications running on varied computing platforms [14]. Reporting rates for synchrophasor measurement units, a key component for enhanced wide-area monitoring and control [17], now occur at 30 to 60 measurements per second. Moreover, because of its geographical expanse, the grid is operated by multiple entities. Despite a universal mandate to keep the system operationally reliable in the face of the loss of any one credible contingency [2, 13], these operating entities adhere to different policies and procedures to meet the reliability mandate.

The diverse enterprise that is the electric power grid operates in an increasingly threatened environment. The period from 2000 to 2004 saw a tenfold increase in successful cyber attacks on the supervisory control and data acquisition (SCADA) systems that comprise the bulk of its communications, monitoring and control infrastructure [4]. Furthermore, it is believed that many (if not most) SCADA systems are inadequately protected against cyber attack [24]. While SCADA systems monitor and control the bulk of the grid infrastructure, they increasingly operate alongside new devices that use standard networking protocols like IP to provide what is described as an "end-to-end smart grid communications architecture" [20]. In fact, the adoption of networking equipment in the emerging smart grid is expected to create a network that will eclipse the size of the Internet [8]. The deployment of various smart-grid-related enhancements is currently well underway.

Despite the challenges, the creation of the smart grid promises several benefits. Modernization of the electrical grid is central to the nation's push for greater energy efficiency, the incorporation of renewable and cleaner resources, and the creation of more energy-sector jobs. Although there is no single model for the smart grid, all the various visions call for the expanded use of computing and networking technologies to support the two-way communication and control of power system devices [12]. This complies with the Energy Independence and Security Act (EISA) of 2007, which calls for the increased use of information and control technology to improve efficiency, reliability and security [23]; implementing this will involve the integration of a vast number of smart devices [22]. However, meeting the EISA mandate will require the collaboration of all the grid stakeholders to keep the system secure in the face of growing threats.

One way to increase the effectiveness of the collaboration is to capitalize on the fact that cyber attackers often prey on similar organizations, so that an incident at one location can be a precursor to an attack at another similar location [1]. Indeed, at various levels of detail, the electric power grid can be considered to be a network of related organizations. If the cyber security experiences of one organization can be broadcast securely in real time to its peers, then the threat awareness of the entire system can be greatly enhanced. While threat awareness involves a variety of considerations, the analysis generally begins with the identification of the source and destination IP addresses and port numbers associated with communications in a monitored network.

This paper proposes a distributed approach to generating watchlists and warning lists of IP addresses for intrusion detection and prevention. The concept is quite simple – it merely globalizes what local intrusion detection systems (IDSs) already do. This approach is based on the federated model, a technique used at a number of U.S. national laboratories [1, 11, 18]. Security and scale issues brought about as intrusion detection reports from increasing numbers stakeholders and devices contribute to the global watchlist are addressed using techniques implemented in the Worminator Project [21] and elsewhere [9, 10]. This paper also offers recommendations for sharing intrusion detection data in a variety of current and future grid architectures. Note that the framework for sharing IP address and port information from individual intrusion detection systems is just one component of a comprehensive cyber defense strategy for the power grid – one that formalizes the exchange of IDS data to strengthen the security vision of grid operators. It will be up to the individual entities to act on the shared data as they see fit.

2. Distributed Intrusion Detection

Several efforts have focused on techniques for sharing intrusion detection data among peers. Many of these efforts, including the popular online DShield tool [7], are cited in [9]. The federated model instituted at Argonne National Laboratory [1, 11, 18] is a recent implementation of distributed intrusion detection data sharing with centralized storage in a domain similar in scale and mission to the electric utility industry. The federated model grew from a "grass roots effort" to combat cyber security incidents at U.S. Department of Energy facilities [1]. The intent was to capitalize on the notion that attackers attempt to compromise related organizations and that, by working together, the related organizations can benefit from shared experiences as they combat attacks. By sharing potentially dangerous communication sources with each other, the organizations can contain the damage to just the first participant that received the communication.

Figure 1 illustrates the benefits of the model. Although Participant 1 is impacted by the attack, Participants 2, 3 and 4 benefit from the data reported via the federated repository and establish the appropriate defenses in a timely manner.

Argonne's implementation uses two mirrored repositories to store IP address and port combinations reported by the participating organizations. The additional repository provides a backup in case one goes down. The organizations report suspicious IP addresses identified by their intrusion detection systems to the repositories in an XML file based on the intrusion detection message exchange format (IDMEF) [6]. The organizations encrypt these files using their private PGP keys. The federated repositories collect this data and correlate it within a single IDMEF-formatted XML file, which is then passed to each organization encrypted under its public PGP key. All the organizations must register the IP addresses that are eligible to send and receive files.

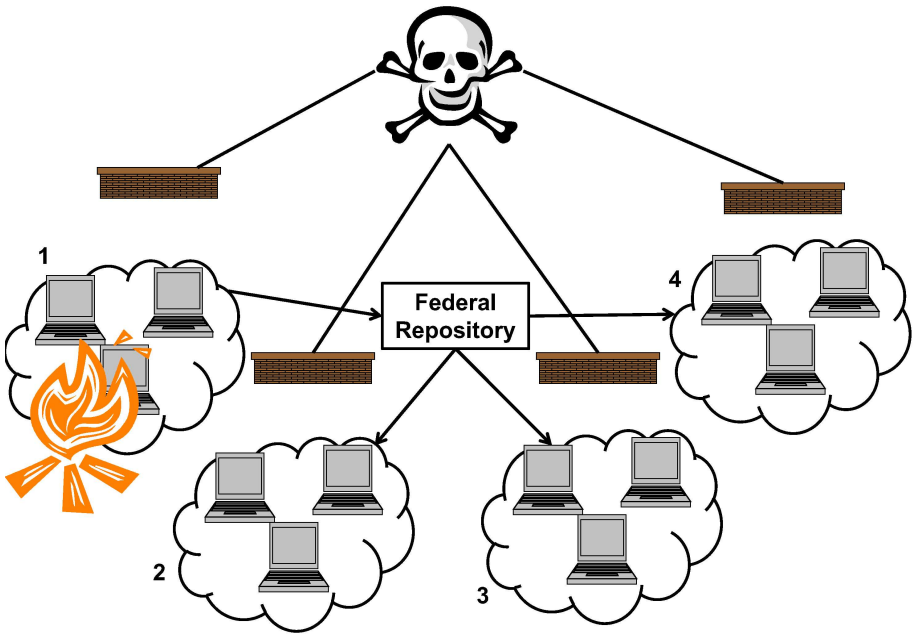

Figure 1. Attack limitation using the federated model.

Currently, more than twenty member organizations participate in the federated model. Nearly 1,000 events are communicated to the repository each day. Each organization has complete control over what it shares with other members through the central repository and the events to which it responds. Furthermore, each member is free to respond to the information it downloads from the repository as appropriate. This demonstrates respect for individual practices and an appreciation of the political pressures that may cause some organizations to be reluctant to share security-related data. Argonne personnel see this as a way to refine the organizations' observe-orient-decide-act (OODA) loop, because all but the directly-impacted organization will have more time and more intelligence to handle attacks. Martin [11] provides an example in which information conveyed via the federated model could have blocked a malicious site full two weeks before it was blocked manually. The federated model is germane to the electrical power grid because of its similarity in scale and mission, particularly when the grid is viewed from a regulatory framework.

3. Distributed IP Watchlist Generation

Whenever a hierarchical structure is to be controlled and monitored, it is necessary to determine the level at which most of the tasks will be performed. Only then can an appropriate strategy for sharing data and decisions be chosen. Deciding where to assign responsibilities requires the consideration of various operational models of the electrical grid. Details on how smart grid devices will

be integrated within the electrical and communications networks of the grid are still taking shape. Therefore, this section describes the electrical grid as it is currently managed and how it might be organized in the future. It is important to understand the models, because they affect the intrusion detection strategies that can be employed.

Like the Internet, the electric power grid can be viewed as a network of networks. Administratively, though, it can also be viewed as a hierarchy of managing entities. The organizational management perspective is most germane to how the grid operates today and reflects the current regulatory environment. For example, the North American grid has three interconnections: the Eastern Interconnection, the Western Interconnection and the Texas Interconnection. Each interconnection has one or more reliability councils, each of which monitors the operations of balancing authorities that usually deliver power to geographically contiguous areas. Within each balancing authority are generation sources, loads and transmission facilities that deliver power from generators to loads. Balancing authorities are responsible for ensuring that their generation matches their load and power exchange demands so that a constant system frequency can be maintained. The reliability councils help coordinate activities when their constituents are out of balance. The entire grid is monitored by the North American Electric Reliability Corporation (NERC).

At present, before the widespread adoption of smart grid technologies and the decentralized control strategies they may afford, the control of grid assets is centralized in the owning balancing authorities. Thus, the operation of the grid currently adheres to a regulatory model, which is shaped by the grid management and accountability structures.

Each balancing authority has its own information technology (IT) staff and each has a portion of the communications infrastructure for which it is responsible. The communications infrastructure for a balancing authority supports corporate systems as well as power monitoring and control systems. While a barrier typically exists between the two systems, it is not always secure (see, e.g., [5]).

Given this model, each balancing authority is required to monitor and respond to cyber attacks against the equipment within its jurisdiction. Viewed from a regulatory perspective, the structure that results is quite similar to the network of national laboratories that currently share intrusion detection data via the federated model. In this analogy, the grid's balancing authorities have jurisdictions similar to those of the national laboratories. The balancing authorities and national laboratories operate independently; both kinds of organizations answer to a supervisory body: reliability councils in the case of balancing authorities and federal agencies in the case of national laboratories. The balancing authorities share a common mission to operate their portions of the grid in accordance with the requirements set by the reliability councils, just as the national laboratories collaborate to achieve the larger research agendas.

To satisfy its own operating responsibilities and meet the requirements prescribed by its reliability council, each balancing authority has to share data

with the reliability council and with its neighbors. To increase the cyber security awareness of the reliability council, the data should include intrusion detection information. A reasonable data set consists of the IP addresses and ports of suspicious communications. Using the federated model as a template, each balancing authority within a reliability council could watch for possible intrusions on its network according to its IT department's policies and procedures. At a minimum, each balancing authority would have to maintain two lists of IP address and port combinations: a watchlist and a warning list [9]. The IP watchlist would contain potentially rogue address/port combinations encountered by the balancing authority during the monitoring period (set by the council to be a certain number of days). For example, a reliability council might require the watchlist to keep track of new IP address and port combinations for the past thirty days. IP address and port combinations that are deemed by the balancing authority to pose a particular threat, perhaps because they have appeared with a worrisome frequency during the monitoring period, would be transferred to the balancing authority's warning list, a permanent record of source or destination points that should be regarded as rogue or potentially dangerous by balancing authorities in the reliability council. How these lists are populated depends on the policies of the individual balancing authority. This approach would preserve local control over cyber security monitoring while enhancing cyber security awareness throughout the council.

In real time, or at some interval defined by the reliability council, the balancing authorities would be required to communicate the updates to their watch and warning lists to the reliability council. The reliability council would consolidate the watchlist updates from the balancing authorities into a single council-wide watchlist containing unique IP address and port combinations along with the number of times that each combination was reported system-wide. Using criteria established by the reliability council, the global warning list would be augmented with the warning list updates provided by the member balancing authorities along with additions to the watchlist that exceeded the council's frequency threshold. For example, if the council's frequency threshold dictates that IP address and port combinations be moved from the watchlist to the warning list when the report count exceeds five, then a combination may be deemed dangerous if five different balancing authorities reported it recently, or if a single balancing authority reported the address more than five times during the monitoring period, or when some other combination of reporting parties and address detections arises. Updates to the global warning list would then be distributed to the balancing authorities to enable them to augment their firewall rules as appropriate.

Figure 2 illustrates the communications that would take place between the reliability council and its member balancing authorities. A similar set of communications could occur to manage global watch and warning lists for sets of reliability councils. In this case, each reliability council could publish its watch and warning list updates to a coordinating body, perhaps a NERC designee. This entity would be responsible for updating and disseminating global warning

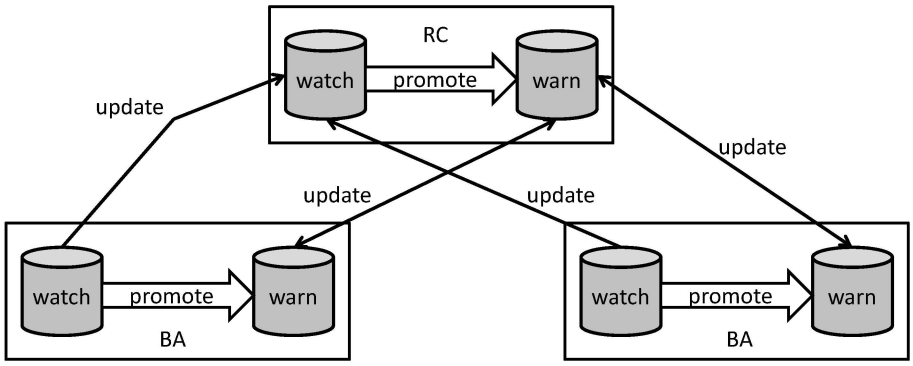

Figure 2. Distributed IP watch and warning list generation.

list updates to the member reliability councils, which in turn would pass these updates to their constituent balancing authorities.

An alternative to this approach is for each balancing authority to maintain a "white list" of IP addresses with which it may communicate. The proposed system could support this choice, since it merely provides a formal system for communicating events and threats and leaves it to the participants to decide how to use the data. Depending solely on a white list, however, may prove problematic for the balancing authority's operations and business centers. Because the facilities of balancing authorities host corporate and command and control systems, a comprehensive white list that supports both types of applications would be cumbersome to manage.

Based on the experiences of the national laboratories with the federated model, a collaboratively-generated black list that disallows communications based on data shared through the proposed system would be both proactive and flexible. Also, as individual devices evolve into smart components that can act autonomously, it is conceivable that a device that was within the safety zone defined by the white list could be compromised and become a bad actor. This requires the white list to be changed for the owning utility as well as for any other entity (e.g., an aggregator) allowed to communicate with it. In this case, the proposed system could be used to coordinate updates to either a white list or a black list database, depending on the policies in place at the participating entity.

Although it can be claimed that each balancing authority has a competitive impetus to act in an adversarial manner toward its peers, there is considerable motivation to act cooperatively because of the dire public consequences of a grid security failure. Furthermore, each participant has the freedom to choose the entities with which it will share intrusion detection data and on whose data it will act. If trust in particular entities is compromised, the participants of the federation can decide how to respond to mend the relationships. The flexibility comes about because of the voluntary nature of the federation.

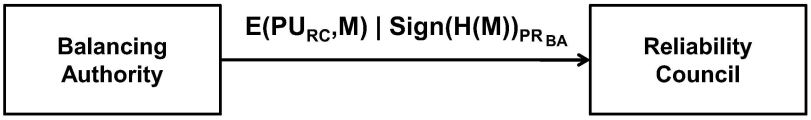

Figure 3. Public key approach for confidentiality, authenticity and integrity

4. Security and Scalability

This section discusses the security of the update messages passed between entities and the scalability of the architecture.

The update messages passed between balancing authorities must be confidential and authentic, and have integrity. The messages must be confidential because one balancing authority may not wish its peers to know the parties with which it is communicating. This is true even if the parties are adversarial – unwanted contact may cause the cyber security readiness of one of the parties to come under the scrutiny of its peers. The messages must be authentic in terms of source and destination, because the recipient, whether it is the reliability council receiving an update from a balancing authority or a balancing authority receiving an update from the reliability council, must be confident that the sender is identified correctly. Finally, update messages must be received as sent. It should not be possible to modify the contents of updates via a man-in-the-middle attack.

There are several ways to achieve the requirements of confidentiality, authenticity and integrity. For example, a public key infrastructure could be used to provide public and private keys to each balancing authority and reliability council. A balancing authority would encrypt a watchlist or warning list update to the reliability council using the reliability council's public key. The update would also be signed by the balancing authority by computing and encrypting the hash of the update using its private key. The encrypted update and the signature are then communicated to the reliability council. Upon receipt, the reliability council can decrypt the update using its private key. It then deciphers the signature by decrypting the hash with the sender's public key. Next, it computes the hash of the decrypted update and compares it with the decrypted signature; if the two match, the sender is authenticated and the received update matches what was sent.

Figure 3 illustrates the public key approach. M denotes a watch or warning list update message sent from the balancing authority to the associated reliability council. To prevent replay, it may also be necessary to send a timestamp that the recipient can check against a list of previously received timestamps. The public key approach works in a similar (albeit reverse) manner for messages sent from the reliability council to a balancing authority. The reliability council could send each balancing authority an update encrypted with the balancing authority's public key. Alternatively, it could send multiple balancing authorities within its jurisdiction the same update encrypted using a public

key shared by the group. Key distribution would be manageable in both cases because the number of communicating entities would be small.

In determining how well this approach scales, it is necessary to consider the number of participants and the sizes of the watch and warning lists and the update messages. In the regulatory model, the number of communicating entities would be small as the number of balancing authorities, which generally coincide with electric utilities, is unlikely to grow much beyond the hundred or so that exist today. Therefore, the number of participants engaged in communications between the reliability council and balancing authority would not contribute to a problem of scale; in fact, the number would be approximately the same as the number of entities participating in the federated model.

However, the sizes of the updates and the watch and warning lists may be a concern. Individual balancing authorities control how much detail they provide to the reliability council. The filter used by a balancing authority for the set of IP addresses and ports it collects and passes to the reliability council may be more stringent than the criteria it uses internally to add the address-port combinations to its watchlist. Also, it may make the reasonable choice to omit attempts to access non-existent services in its reports to the repository. However, if balancing authorities choose not to be as selective in what they report, additional steps would have to be taken to maintain system performance at acceptable levels.

One approach for managing message volume is to use a Bloom Filter to represent messages more compactly [9]. In this approach, the watch and warning lists could each be represented as a large array of bits initialized to zero. When a new IP address and port combination is reported to the reliability council, authenticated and integrity-checked, it is stored as sent and it is also hashed. Portions of that hash are used to calculate the indices of entries in the bit array that should be set to one. Thus, whenever an IP address and port combination is sent in an update, the indices in the Bloom Filter array are checked to see if they are all already turned on. If all the bits are not equal to one, then the combination has been reported for the first time. If all the bits are set to one, then the combination may be a repeat of a earlier combination, in which case the list of hashes recorded as sent have to be checked to determine if it is indeed a duplicate. If it is a duplicate, then its occurrence count is increased, possibly making it a candidate for promotion to the warning list.

5. Decentralized IP Watchlist Generation

Section 3 described the implementation of a distributed scheme for identifying problematic IP addresses that was centralized at the balancing authority. As more smart grid devices capable of two-way communication are deployed in the future, it may become necessary to adopt a more decentralized scheme in which localized clusters of devices share information.

Consider the more device-focused architecture shown in Figure 4. In this model, the end loads L_i at the lowest level of the architecture are controlled to achieve the operating objectives. For example, in [19], the end loads are

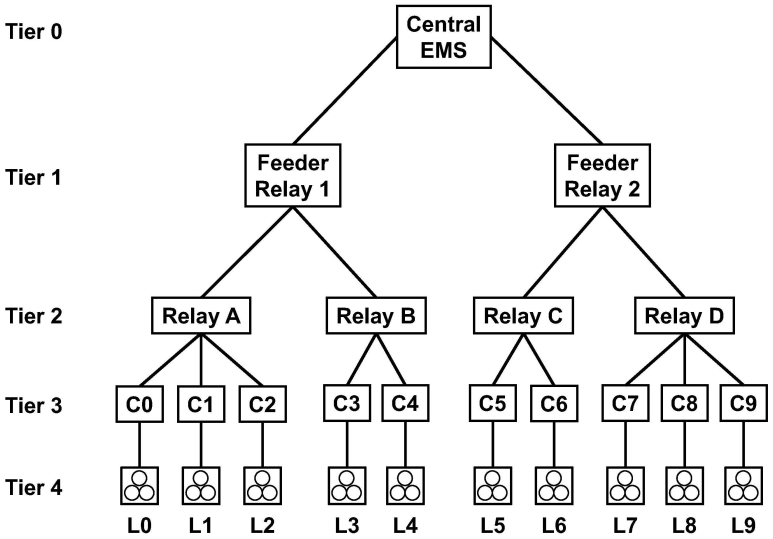

Figure 4. Delegation model for smart grid communications and control.

regulated to provide more reactive power support to regions experiencing depressed voltage. Given the proper equipment, the problem may be detected and addressed locally instead of by the central energy management system (EMS) housed at the balancing authority. If this is possible, then the load L_i is regulated by its corresponding controller C_i to address the problem. If the problem cannot be handled locally, but requires the assistance of peer devices in nearby regions, then the responsibility for the problem may be assigned to the next higher tier. Again, if properly equipped, the device at the next higher tier can formulate a response to mitigate the problem that calls for support from a broader pool of devices than just those in the affected region. Messages passed among tiers of this model must be authenticated and checked for integrity, and the devices in each tier must be "smart" in that they have the processing power to assess the electrical characteristics and formulate a control response.

This architecture manages the grid through delegation: each tier can communicate only with the tier directly above it or directly below it. For example, if a problem at load L_1 in Tier 4 cannot be handled by the controller C_1, Relay A or Feeder Relay 1 in the intervening lower tiers, then the Central EMS in Tier 0 will formulate a strategy that calls for supportive action and communicate it to its two children in Tier 1, Feeder Relay 1 and Feeder Relay 2. These, in turn, will pass instructions contained in the just-received directive from the Central EMS to the appropriate relays in Tier 2, the next lower tier. The relays repeat the parse-and-pass procedure to forward required instructions to the appropriate load controllers C_i in Tier 3.

A distributed approach to collecting and correlating intrusion detection data in this case might involve establishing a separate repository for each tier. The

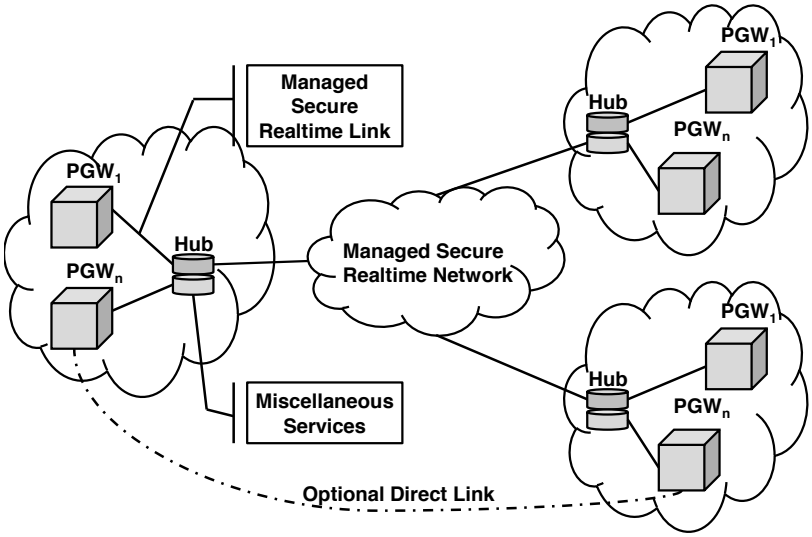

Figure 5. Hub-based NASPInet architecture (from [3]).

repository at Tier n would maintain the watch and warning lists for the devices in Tier $n + 1$. Since control requests never pass beyond the immediately next tier, such a short-range approach to compiling the watch and warning lists would support the needs of the smart grid architecture. By defining the repositories by tier, the scaling problem that would otherwise be encountered if the entire system communicated with a single repository is avoided. Furthermore, in the event of a multi-tier attack, the suspicious activities recorded in each tier could provide the data necessary to interfere with the progress of the attack.

Bobba, *et al.* [3] describe another example of a tiered architecture, motivated by a specific application, that exhibits elements of the regulatory and delegation models. One of the aims of the emerging smart grid is to increase wide-area situational awareness. A tool for achieving this is the synchrophasor measurement unit (PMU), a GPS-time-synchronized meter capable of measuring voltage and current magnitudes, phase angles and frequencies between 30 to 60 times per second. The North American Synchrophasor Initiative (NASPI) is planning the deployment of PMUs throughout the grid. The current plan, documented in [15, 16], assigns monitoring and control of each PMU to its owning utility through devices called phasor gateways (PGWs).

An alternative NASPInet architecture is proposed in [3] to address a potential bottleneck in reporting large quantities of data to the owning authority. In this design, which is illustrated in Figure 5, the phasor gateways report to hubs that share information with each other using a secure realtime network. The hubs manage requests for data as well as the collection and correlation of phasor measurement data. They could also serve as hosts for the distributed intrusion detection effort. Each hub could maintain watch and warning lists

for its constituent phasor gateways and share the lists with its peer hubs. This approach should scale well because the number of hubs is much more than the number of individual PMUs and PGWs. Regardless of whether the hub communications are regulated by a white-list-based or black-list-based approach, by sharing intrusion detection intelligence with each other, the hubs can achieve a more comprehensive view of security threats.

6. Conclusions

The distributed intrusion detection architecture presented in this paper gathers threat data from multiple sources and disseminates consolidated updates to participating entities, helping improve the wide-area security awareness of the electrical power grid. The architecture is applicable to the current grid that operates according to a regulatory model as well as various future smart grid designs that operate in a distributed, device-oriented manner. Also, the architecture supports secure messaging and is scalable.

Acknowledgements

This research was partially supported by the National Science Foundation under Grant No. CNS-0524695 and by the Department of Energy under Award No. DE-OE0000097. This article was created by UChicago Argonne, LLC, Operator of Argonne National Laboratory, a U.S. Department of Energy Office of Science Laboratory, which is operated under Contract No. DE-AC02-06CH11357. Note that the U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license to reproduce this article, prepare derivative works, distribute copies to the public, perform publicly and display publicly by or on behalf of the U.S. Government.

References

[1] Argonne National Laboratory, Federated model for cyber security: Collaborative effort to combat Internet attackers, Argonne, Illinois (webapps .anl.gov/federated), 2009.

[2] N. Balu, T. Bertram, A. Bose, V. Brandwajn, G. Cauley, D. Curtice, A. Fouad, L. Fink, M. Lauby, B. Wollenberg and J. Wrubel, On-line power system security analysis, *Proceedings of the IEEE*, vol. 80(2), pp. 262–282, 1992.

[3] R. Bobba, E. Heine, H. Khurana and T. Yardley, Exploring a tiered architecture for NASPInet, presented at the *First IEEE PES Conference on Innovative Smart Grid Technologies*, 2010.

[4] E. Byres and D. Hoffman, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, Technical Report, Department of Computer Science, University of Victoria, Victoria, Canada, 2004.

[5] E. Byres, A. Paller and B. Geraldo, Special webcast: Cyber attacks against SCADA and control systems, SANS Institute, Bethesda, Maryland, 2009.

[6] H. Debar, D. Curry and B. Feinstein, The Intrusion Detection Message Exchange Format (IDMEF) (www.ietf.org/rfc/rfc4765.txt), 2007.

[7] DShield, DShield Cooperative Network Security Community (www.dshield .org).

[8] M. LaMonica, Smart grid will eclipse size of Internet, CNET News (news .cnet.com/8301-11128_3-10241102-54.html), May, 18, 2009.

[9] M. Locasto, J. Parekh, A. Keromytis and S. Stolfo, Towards collaborative security and P2P intrusion detection, *Proceedings of the IEEE Workshop on Information Assurance and Security*, pp. 30–36, 2005.

[10] M. Locasto, J. Parekh, S. Stolfo, A. Keromytis, T. Malkin and V. Misra, Collaborative Distributed Intrusion Detection, Technical Report CUCS-012-04, Department of Computer Science, Columbia University, New York, 2004.

[11] T. Martin, Federated model for cyber security: Sharing intrusion detection results, Argonne National Laboratory, Argonne, Illinois (webapps.anl.gov /federated/site_media/docs/Presentations/DOETechSummit.pdf), 2008.

[12] National Institute for Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, Gaithersburg, Maryland, 2010.

[13] North American Electric Reliability Corporation, Reliability Standards for the Bulk Electric Power Systems of North America, Princeton, New Jersey, 2010.

[14] North American Synchrophasor Initiative, Phasor Applications Taxonomy, Pacific Northwest National Laboratory, Richland, Washington, 2007.

[15] North American Synchrophasor Initiative, Data Bus Technical Specifications for North American Synchrophasor Initiative Network, Pacific Northwest National Laboratory, Richland, Washington, 2009.

[16] North American Synchrophasor Initiative, Phasor Gateway Technical Specifications for North American Synchrophasor Initiative Network, Pacific Northwest National Laboratory, Richland, Washington, 2009.

[17] North American Synchrophasor Initiative, Synchrophasor Technology Roadmap, Pacific Northwest National Laboratory, Richland, Washington, 2009.

[18] S. Pinkerton, A federated model for cyber security, presented at the *Cyberspace Research Workshop*, 2007.

[19] K. Rogers, R. Klump, H. Khurana and T. Overbye, Smart-grid-enabled load and distributed generation as a reactive resource, presented at the *First IEEE PES Conference on Innovative Smart Grid Technologies*, 2010.

[20] J. St. John, Duke Energy enlists Cisco in smart grid efforts, Greentech Media, Cambridge, Massachusetts (www.greentechmedia.com/articles/read /duke-energy-enlists-cisco-in-smart-grid-efforts), June 9, 2009.

[21] S. Stolfo, Worm and attack early warning, *IEEE Security and Privacy*, vol. 2(3), pp. 73–75, 2004.

[22] U.S. Department of Energy, Recovery Act – Smart Grid Investment Grant Program, DE-FOA-0000058, Washington, DC, 2009.

[23] U.S. Government, Energy Independence and Security Act of 2007, Public Law 110–140, *United States Statutes at Large*, vol. 121, pp. 1492–1801, 2007.

[24] C. Wilson, Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, RL32114, Congressional Research Service, Washington, DC (www.fas.org/irp/crs/RL32114.pdf), 2003.