

A Survey on Guaranteeing Availability in Smart Grid Communications

Mihui Kim

Department of Computer Engineering, Hankyong National University, Korea

mhkim@hknu.ac.kr

Abstract— Availability is the most important security objective in smart grid communications. In this paper, we present a review of the work related to guaranteeing availability in smart grid communications. The work reviewed is separated into three categories: defences against attacks, guarantee of critical real-time systems, and extension of communications availability. Because of significance of providing the seamless service from electrical power systems, defences against various attacks, i.e., false data injection attacks in smart grid have been researched. Moreover, the critical real-time systems in the smart grid require very short estimated maximum latency, i.e., 4 milliseconds. These systems continuously monitor the state of the electrical power grid, and a disruption in communications can cause a loss of power. Such delay-sensitive traffic should be guaranteed for the minimum latency. To increase availability of communications in smart grid, network architecture using cognitive radio technologies has been designed. Lastly, we suggest the open research issues for guaranteeing the availability in smart grid.

Keywords—Availability, Smart Grid, Survey, Defences, Critical real-time systems

I. INTRODUCTION

A modern power grid needs to become smarter in order to provide an affordable, reliable, and sustainable supply of electricity. Because of such reasons, the smart grid utilizes computer networks to manage generation and facilitate two-way communications between users and suppliers. However, we should address the opposite effect of the efficiency and reliability in smart grid, i.e., security vulnerabilities of cyber attacks by adversaries around the globe. Especially the electrical infrastructure can be a major target of adversaries in order to not only cause economic loss but also make the country in chaos. For example, it has already been widely reported that the United State electrical grid has been penetrated by cyber spies [1].

The security objectives of the smart grid cyber security are different from most of the other industries. It is important that any security countermeasure implemented in the Smart Grid do not impede power availability or safety. That is, *availability* is the most important security objective. The critical real-time systems in the Smart Grid have an estimated maximum latency of 4 milliseconds. These systems continuously monitor the state of the electrical power grid,

and a disruption in communications can cause a loss of power [2].

To guarantee the availability in smart grid networks, several researches have been done. We categorize the researches with three aspects: *defences against attacks*, *guarantee of critical real-time systems*, and *extension of communications availability*. First, both the discovery of novel attacks in smart grid (e.g., false data injection attack or load altering attacks) and general attacks (e.g., altering commands or signals) in IT systems are focused on by researchers [3-6]. The defence mechanisms against such attacks have begun to be proposed [7-10]. Second, the importance for guarantee of critical real-time systems (i.e., GOOSE in a link-layer multicast protocol designed in IEC61850 [11], or management traffic) is emphasized and the results have proposed in the perspective of QoS management or resource management [12,13]. Last, in order to extend communication availability, researches on utilizing cognitive radio technologies have been done [15-17].

The remainder of the paper is organized as follows. Section 2 clarifies network architecture of smart grid, and availability. Section 3 introduces the research trend for the defences against attacks in smart grid. Section 4 provides an analysis for recent research to guarantee critical real-time systems. Section 5 presents the effort for extending the communication availability in smart grid. Section 6 concludes this paper with future work.

II. NETWORK ARCHITECTURE OF SMART GRID AND AVAILABILITY

Network architecture of smart grid hierarchically consists of three components: home area network (HAN), neighbourhood area network (NAN), and wide area network (WAN), as shown in Fig. 1. The HAN provides access to in-home appliances while the NAN connects smart meters to local access points, and WAN provides communication links between the grid and core utility systems. Fig. 1 shows a basic illustration of the electrical power grid and the smart grid multitier communications network. As the characteristics of each tier network, different wireless communication techniques can be adapted, i.e., WiFi or Zigbee for HAN in indoor small area, WiMAX or WiFi for NAN with wireless mesh topology, and WiMAX, 4G or Cognitive Radio for WAN.

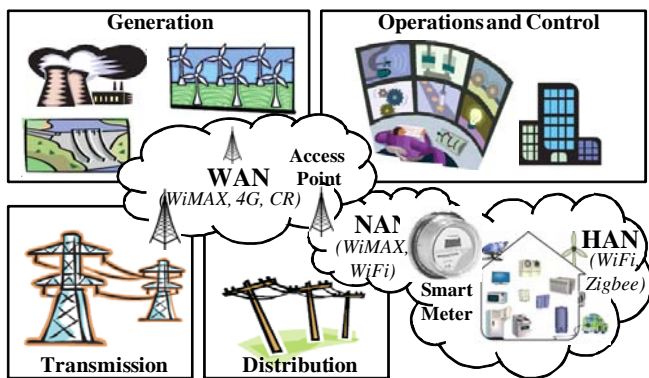


Figure 1. Network Architecture of Smart Grid

To protect the availability of machine-to-machine (M2M) communications in smart grid with multitier architecture, multilateral efforts should be made. In contrary, the adversaries could threaten each tier network, various type devices, communication networks and power systems. We should analyse the weaknesses in whole architecture, guarantee the characteristics of traffic, and provide the countermeasure of attacks as secondary choice. In this paper, we will analyse research trend classified with three perspectives as shown in Fig. 2 from Section 3 to Section 5 and exhibit the future work in Section 6.

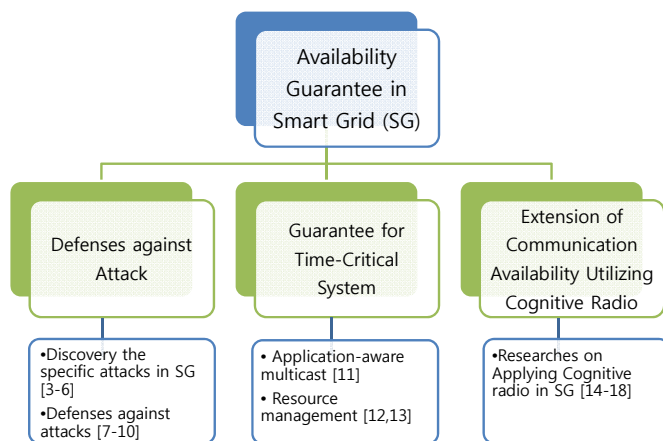


Figure 2. Research Trend for Availability Gaurantee in Smart Grid

III. DEFENCES AGAINST ATTACKS

We classify three different cyber-attack scenarios as [5], according to attack targets: *generation*, *distribution and control*, and *smart meters*. The defence or secure mechanisms against these attacks are shown in Fig. 2.

First attack targets power plants and aims in disrupting or taking over the operation of generators. Although such attacks are sophisticated and require significant resources to be successful, there are multiple reports indicating that such attacks have taken place in the past. For example, in January 2008, the Central Intelligence Agency reported knowledge of four disruptions by hackers of the power suppliers for four cities. As possible defence research direction against such type attacks, the author pointed out complex defence based on

threat and vulnerability assessment, R&D on prevention, mitigation, and restoration, because the spectrum of cyber attacks continue to evolve threatening multiple assets. It should include with risk-management frameworks, vulnerability-reduction tools, information-sharing programs, etc [19,20].

Second attack targets power distribution and control, i.e. supervisory control and data acquisition (SCADA) systems or process control system (PCS) which is the components responsible for monitoring and controlling physical properties of the electrical power grid. As a representative attack, *false data injection attack* to state estimation attempts to compromise measurement sensors or break into the routers that relay the measured data towards SCADA, in order to insert errors into certain state variable estimations [3,4]. This attack also is named as *malicious data attack* [7]. Such cyber attacks on SCADA systems operating power networks have been reported and major blackouts, as the August 2003 Northeast blackout, are worsened by the misuse of the SCADA system [6]. A successful attack can potentially cause grid instability and inability in the worst case. Defences against this attack have been researched. Y. Liu et al. introduced unobservable attack with false data injection to state estimator if the adversary controls enough meters to execute the attack [3,4]. This research firstly exposed an unknown vulnerability of existing bad measurement detection algorithms by presenting and analyzing a new class of attacks. As a defence against such attacks, adaptive CUSUM algorithm, which is recursive in nature, was proposed in [8]. Each recursion comprises two interleaved stages: Stage 1 introduces the linear unknown parameter solver technique, and Stage 2 applies the multi-thread CUSUM algorithm for quickest change detection.

As an variation of false data injection attack, stealthy or deception attacks are presented in [6,7]. If the adversary only possesses a perturbed model, i.e., a partial model of the true system, the stealthy deception attacks can be mounted. However, this attack has trade-off between model accuracy and possible attack impact. Oliver Kosut et al. presented a method to detect and localize such attacks using the generalized likelihood ratio test [7].

As a little different attack from false data injection attack, the possibility of *load altering attack* was shown in [5]. For example, the power load of a data center is highly elastic depends on the computation load of data center, and thus bogus computation tasks may result in extra power consumption at a data center. Moreover, it can cause major impact to the electric grid due to abrupt load fluctuations. As general defence mechanisms, the authors presented setting up passwords, firewalls, and identity authentication.

Last attack targets smart meters or advanced metering infrastructure (AMI). In [5], A.H. Mohsenian-Rad et al. showed the load altering attack to smart meter, i.e., modification of commands or price signals. As general defence mechanisms, the authors presented private key encryption and message authentication code for unicast command, and group key management for multicast price

signals. S. Kim et al. proposed a secure smart-metering protocol over power-line communication including: 1) key materials generation and provisioning to devices without exposure, 2) initialization to authenticate devices in the network and share keys between devices, 3) secure transmission, and 4) revocation management to handle discarded devices from the network [9]. For intrusion detection for AMI, R. Berthier et al. analysed the possible threats, i.e., curious eavesdroppers, motivated eavesdroppers, unethical customers, overly intrusive meter data management agencies, active attackers, and publicity seekers [10]. As defence mechanism, stateful specification-based monitoring (e.g., behavioural or finite state machine monitor), stateless specification-based monitoring (e.g., firewall log monitor or data validation), anomaly-based monitoring (e.g., threshold monitor) are suggested.

IV. GUARANTEE OF CRITICAL REAL-TIME SYSTEMS

In the smart grid networks, the noticeable characteristics of traffic is two types traffics are apparently divided: time controlled small data and massive metering traffic and delay sensitive management traffic. Especially, the delay sensitive traffic should be guaranteed for the delay time, because the delayed time can be directly related with power or cost loss [2].

To guarantee the delay of critical real-time system, (e.g., GOOSE messages are usually required to be delivered within 2 and 10 milliseconds), Z. Zhang et al. proposed an application-aware secure multicast for power grid communications; GOOSE is a link-layer multicast protocol designed in IEC61850 for transmitting timing-critical messages, such as substation events, commands and alarms, within power substation networks [11]. In 3GPP machine-to-machine communication networks, the research on massive access management for QoS guarantee can be another solution for delay sensitive traffic [12,13].

V. EXTENSION OF COMMUNICATIONS AVAILABILITY

To provide a reliable communications infrastructure which is a sophisticated, multi-layer network carrying different classes of data, researches with cognitive radio technologies have been presented in [14-16]. Cognitive radio technologies have been proposed to satisfy the increasing demand for wireless bandwidth and to increase the efficiency of channel utilization through sharing the resource between primary users (PUs) and secondary users (SUs) [17]. IEEE 802.22 is a representative standard designed to provide broadband access to rural areas using the white space in TV bands [18].

A. Ghassemi et al. applied cognitive radio (CR) based on the IEEE 802.22 to smart grid WANs as shown in Fig. 1, expecting the benefits of opportunistic access of TV bands, extended coverage, ease of upgradability, self-healing and fault-tolerant design. This standard offers extensive coverage area (33-100 km) due to the good propagation characteristics of TV bands.

R.C. Qiu et al. built a real-time cognitive radio network testbed for smart grid in order to give security and reliability

enhancement to the network [14]. However, in this paper, they focused on the cognitive radio testbed system with narrowband and wideband platforms. They then presented the research plan based on the testbed as follows: scheduling in MAC layer, routing algorithm, key management algorithms, and attacks defence strategies, considering spectrum and situation.

N. Ghasemi et al. explained the cognitive radio as solutions for the problem of spectrum scarcity in smart grid [15]. They mentioned the techniques can enhance the requirements of smart grid, i.e., ability to heal itself, resist attacks or run more efficiently.

These researches are a beginning step, but all of them expected the cognitive radio to enhance the reliability or availability in smart grid [15]. Practical researches for how the cognitive radio technologies adapt to smart grid networks should be done.

TABLE 1. CHARACTERISTICS AND DEFENCES OF ATTACKS IN SMART GRID

Attack Targets	Characteristics	Defences
Generation	- Sophisticated and require significant resources - Spectrum of cyber attacks evolves threatening multiple assets	- Include with risk-management frameworks, vulnerability-reduction tools, information-sharing programs, etc. [19]
Distribution and control	- Threaten monitoring and controlling physical properties of the electrical power grid with false data injection - E.g., false data injection attack, stealthy deception attack, load altering attack	- Adaptive CUSUM algorithm against false data injection attack [8] - Algorithm using the generalized likelihood ratio test against stealthy attack [7] - Setting up passwords, firewalls, and identity authentication against load altering attack [5]
Smart meters	- Attack altering commands or price signals - Treats to smart meters, i.e., curious eavesdroppers, motivated eavesdroppers, unethical customers, overly intrusive meter data management agencies, active attackers, and publicity seekers	- Private key encryption or MAC for unicast, and group key management for multicast [5] - Secure key management and authentication protocol for smart metering over PLC [9] - Intrusion detection system (IDS) for AMI [10]

VI. CONCLUSIONS

In this paper, we discussed the availability importance in smart grid, and efforts to guarantee the availability in three perspectives: defences against attacks, guarantee of critical real-time systems, and extension of communications

availability. Most related work focused on introducing the attacks in smart grids and proposed the possible defence solutions. Some of researches presented the mechanisms to guarantee the transmission of delay sensitive traffic or provide the secondary communication using cognitive radio.

However, in the future, the more researches should be performed for the availability guarantee in smart grid. The open research issues are as following:

A. Analysis for Potential Attack Scenarios

Until now, several specific attacks in smart grid (e.g., false data injection attack or load altering attacks) have been presented. However, there would be the potential attacks in the future of smart grid. It is important to discover such future attack scenarios in order to design proper defence mechanisms. To perform this research issue, the collaboration of experts in IT security and experts in power systems are necessary.

B. Specification-based IDS or Converged IDSs

It is significant to design specification-based IDS considering specific protocols or standard specifications (i.e., IEC61850 or IEC62351-7 [21]) in power system, and moreover converged IDS to integrate IDSs in each network, i.e., HAN, NAN, and WAN.

C. Resource Management Understanding Traffic Characteristics

The distinct characteristic of traffic in smart grid is dis differentiation of traffic characteristics, i.e., massive metering traffic with small data and time controlled, and delay density traffic of managements or signals. Two traffic characteristics should be considered in design of most protocols in networks, i.e., scheduling, routing, resource management, etc.

D. Research on coexistence of cognitive radio networks and existing wireless networks

Research on coexistence of cognitive radio technologies and existing wireless technologies is an initial step. Practical issues on various operations on such environment should be researched, i.e., who does the role of spectrum sensing play in, how are the sensing results converged, how do the resource management of cognitive radios and primary wireless radios, etc.

E. Consideration for Renewable, Distributed Power Generation

In the future, it is essential that smart grid is integrated with new distributed generation resources such as wind turbines, photovoltaic arrays, micro turbines, and combined heat and power generators in buildings [20]. The history of security in complex networks implies that more vulnerabilities exist and are yet to be discovered. On such environments, the defence mechanisms to be available to respond quickly or load shedding or relocating schemes in attack cases should be researched.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2011-0014020).

REFERENCES

- [1] J. Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN*, Sep. 2007.
- [2] T. Baumeister, "Literature Review on Smart Grid Cyber Security," *Technical Report of University of Hawaii*, 2010.
- [3] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. on Computer and Communications Security*, New York, NY, USA, pp. 21–32, 2009.
- [4] Y. Liu, P. Ning, and M. K. Reiter, "Generalized False Data Injection Attacks against State Estimation in Electric Power Grids," *ACM Transactions on Information and System Security (TISSEC)*. Vol. 14, Issue 1, May 2011.
- [5] A.H. Mohsenian-Rad, and A. Leon-Garcia, "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," *Smart Grid, IEEE Trans. on*, vol. 2, pp. 667–674, Aug. 2011.
- [6] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, and S.S. Sastry, "Cyber Security Analysis of State Estimators in Electric Power Systems," in *proc. IEEE Conf. on Decision and Control*, 2010.
- [7] O. Kosut, L. Jia, R.J. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," in *Proc. SmartGridComm*, 2010.
- [8] Y. Huang, H. Li, K.A. Campbell, and Z. Han, "Defending False Data Injection Attack On Smart Grid Network Using Adaptive CUSUM Test," in *Proc. CISS*, 2011.
- [9] S. Kim, E. Kwon, M. Kim, J. Cheon, S. Ju, Y. Lim, and M. Choi, "A Secure Smart-Metering Protocol Over Power-Line Communication," *IEEE Trans. on Power Delivery*, Vol. 26, No. 4, Oct. 2011.
- [10] R. Berthier, William H. Sanders, and Himanshu Khur, "Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions," in *Proc. SmartGridComm*, 2010.
- [11] Z. Zhang, and C.A. Gunter, "Application-Aware Secure Multicast for Power Grid Communications," *Int. J. Security and Networks*, Vol. 6, No. 1, 2011.
- [12] S. Lien, and K.C. Chen, "Massive Access Management for QoS Guarantees in 3GPP Machine-to-Machine Communications," *IEEE Comm. Letter*, Vol.15, No. 3, pp.311-313, Mar. 2011.
- [13] S. Zhang, C. Zhu, J. K. O. Sin, and P.K.T. Mok, "Latency for Real-Time Machine-to-Machine Communication in LTE-Based System Architecture," in *Proc. European Wireless Conference*, 2011.
- [14] A. Ghassemi, S. Bavarian, and L. Lampe, "Cognitive Radio for Smart Grid Communications," in *Proc. SmartGridComm*, 2010.
- [15] R.C. Qiu, Z. Chen, N. Guo, Y. Song, P. Zhang, H. Li and L. Lai, "Towards A Real-time Cognitive Radio Network Testbed: Architecture, Hardware Platform, and Application to Smart Grid," in *Proc. IEEE Workshop on Networking Technologies for Software Defined Radio (SDR) Networks*, 2010.
- [16] N. Ghasemi, and S. M. Hosseini, "Comparison of Smart Grid with Cognitive Radio: Solutions to Spectrum Scarcity," in *Proc. ICACT*, 2010.
- [17] S. Haykin, "Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications* vol. 23, no.2, pp. 201–220, Nov. 2005.
- [18] IEEE P802.22 Working Group on Wireless RANs, <http://www.ieee802.org/22/>.
- [19] S. M. Amin, "Securing the electricity grid," *Bridge*, Vol. 40, No. 1, pp.13–20, Mar. 2010.
- [20] W. F. Boyer, and S. A. McBride, "Study of security attributes of smart grid systems current cyber security issues," *Idaho Natl. Lab. Tech. Rep.*, Apr. 2009.
- [21] IEC 62351-7 TS Ed.1: Power systems management and associated information exchange –Data and communication security – Part 7: Network and system management (NSM) data object models, 2009.