European Journal of Scientific Research
ISSN 1450-216X / 1450-202X Vol. 134 No 1 August, 2015, pp.111-120
http://www.europeanjournalofscientificresearch.com

Cyber Attack Challenges and Resilience for Smart Grids

Sajid Nazir
University of Aberdeen, Aberdeen, UK
E-mail: sajid@erg.abdn.ac.uk

Hassan Hamdoun
University of Aberdeen, Aberdeen, UK
E-mail: hassan.hamdoun@abdn.ac.uk

Jafar A. Alzubi
Al-Balqa Applied University, Salt, Jordan
E-mail: j.zubi@bau.edu.jo

Omar A. Alzubi
Al-Balqa Applied University, Salt, Jordan
E-mail: o.zubi@bau.edu.jo

Abstract

A smart grid system supports intelligent metering and monitoring functions spanning the areas of power generation, transmission and distribution. It has enormous benefits for meeting the energy demands and billing requirements through controls at the supply side rather than at the demand side. This departure from the traditional perspective makes it a very attractive transformation for both developing and developed economies. However, a major drawback is the increased vulnerability of the highly connected system and knock-on ramifications on various related sub systems and networks. With the connectivity emerge the associated dangers of exposed system entry points through nodes located at various geographical locations; making an easy target for a motivated hacker. Starting at the compromised node, the inner system can be penetrated and its core functionality can be compromised. There is thus a need for having a system wide resilience in the design and architecture to meet these challenges. This paper reviews the vulnerabilities and resilience strategies for a smart grid and proposes the combined use of macro and micro management techniques as an evolutionary process to enhance system availability.

Index Terms: Computer Security, cyber security, Control systems, SCADA, critical infrastructures.

Introduction

Smart grid is the integration of digital technologies with power generation and transmission. It provides better control to consumers over their energy consumption, reduces expenses of the producers by matching supply to demand, and improves network visibility to infrastructure managers. It thus benefits the electricity consumers, local communities, environmental agenda and the country as a whole.

Smart grid transformation is a global issue and the key to meeting the demand on electricity generation and bettering manages the supply and demand [1]. This requires embedding [2] sensors and

actuators for process management and control. The decades old power generation and distribution system needs to be modernized in order to take advantage of the advancement in wireless, communications and sensing technologies. The basic structure for industrial control applications is based on Supervisory Control and Data Acquisition (SCADA) system. The industrial control systems (ICS) have been very efficient in providing timely information on system status, and fault localization but this was done in isolation to the energy consumers demands. The advent of digital technologies makes it possible for control systems to be interconnected through the Internet resulting in better control and timely exchange of information.

China's energy needs will double by 2020 and will be spending $96 billion [3] in smart grid technology. Similarly other developed nations have major programs for investment in smart grid architecture due to its enormous potential for return on investment. The benefits of transformed business processes apply equally to developing countries struggling with load-shedding and black-outs. Better controls for supply and demand through transformation of the smart grid can ease the burden of the growing energy demands at global scale. The electricity generation and distribution systems were not designed to be connected or accessed over the Internet and making these critical infrastructures accessible certainly has advantages but it can also make the system vulnerable [4]. The system thus gets exposed to potential cyber security risks inherent in any Internet connected system. The collapse or compromise of critical infrastructures like smart grid could result from malicious users, inadvertent mistakes, natural calamity, and disgruntled employees. Such failures of the system can have far reaching consequences on the economy and society creating public security issues.

Security concerns for smart grids have recently been raised and there are several standards and efforts under way to improve the security of ICS [5], [6], [7], [8]. Enhancing the cyber security of smart grid is a logical step but still it cannot prevent a breach of the system. The cyber security challenges and threats however can be met through designing a resilient system taking into account all the tiers of these complex interconnected sub-systems. Resilience ensures that the system contains the damage in case of an attack, degrades gracefully during attack and recovers to original operational state with minimum fallout. To be considered alongside is the fact that over the lifespan of the smart grid system, the security mechanisms and vulnerabilities will become widely known, necessitating the need for a continuous evolving security strategy including vulnerability assessment.

In this paper, we propose a holistic approach by grouping protective measures into macro and micro management techniques to provide resilience at various tiers of the system. Taking such an approach not only improves resilience but acts

Figure 1: Smart Grid Generation and Distribution System [9]

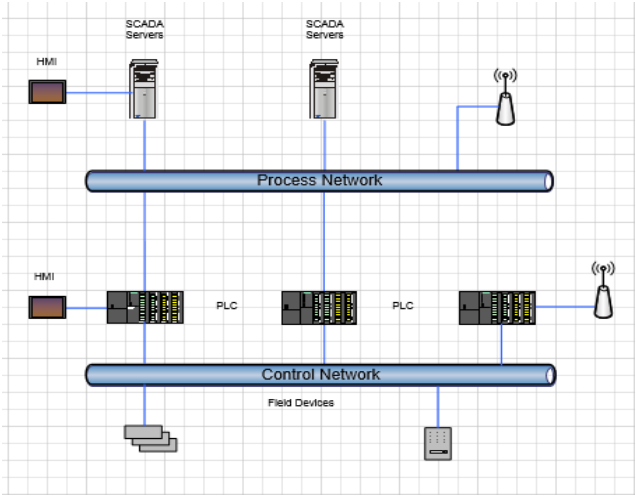
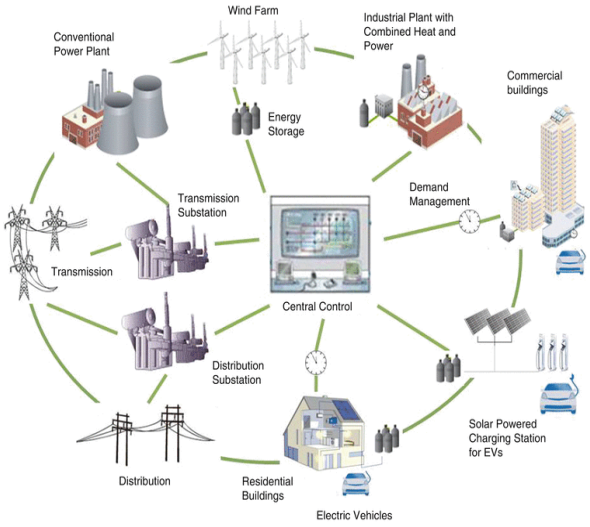


Figure 2: SCADA system. Adapted from [10]



as a safety net for the serious system breaches and possible ramification on other systems. The rest of the paper is structured as follows: The smart grid architecture is covered in Section II. The vulnerabilities, threats and recent attacks are described in Section III. Section IV covers the macro and micro resilience strategies. Finally Section V concludes the paper.

II. Smart Grid and Scada Systems

Smart grid is a system of systems interconnected through a communications network in order to interchange information for exercising better control on system resources. A simplified diagram is shown in Figure 1. It comprises of renewable power generation resources integrated into the electrical network. The demand management function is through the sensors, actuators and advanced metering infrastructure (AMI). Although a smart grid comprises of infrastructure and devices spread over a large geographical area, the central control is governed through the SCADA system. Data from smart meters and field devices such as those monitoring line voltages and current are fed into the central control room where the decisions are made for real time control. This real time control is based on algorithms controlling the generation and distribution processes.

A SCADA system is shown in Figure 2. It comprises of field devices (sensors and actuators) that measure the physical quantities and actuators to respond to commands. Remote Terminal Unit (RTU) is used to interface with the sensors for transmitting telemetry data. Programmable Logic Controller (PLC) provides data acquisition and control functions which is communicated through the network to the SCADA server. The interface presents the data to the operator, and permits generating commands for the process control [10].

SCADA interconnection to outside network [11] makes it vulnerable as the industrial communication protocols over TCP/IP become susceptible to generalized and targeted cyber attacks.

III. Vulnerabilities, Threats and Attacks

A. Vulnerabilities

(1) Industrial Protocols

The networking protocols used for industrial and wireless communications were not designed with the security concerns manifested in smart grids. For example, Modbus [12], a communication protocol used in industrial control systems has messages and responses sent in clear text. SCADA Distributed

Network Protocol 3.0 (DNP3) packets can also be analysed [1] through network sniffing tools to gain information and cause damage.

(2) Privacy Issues
Devices used in the field such as AMI increase the exposure to attacks [13]. The nature of the two-way flow of data raises potential privacy issues e.g. manipulation of billing information and injecting data into the network to degrade the system.

(3) Proliferation of Networked Devices
The connectivity of field devices through TCP/IP protocol brings many advantages but also brings vulnerability. The motivation of the hacker to gain access to a field device would generally be to penetrate deeper into the network. The biggest challenge is to protect the connected devices out in the field as corporate networks are generally well protected.

(4) Network Analysis Tools
Software tools like nmap [14] are freely available and can provide information about the network, which can be analysed further to gain more information about the network topology and exploit the vulnerabilities.

(5) Nature of Control Systems
The control systems' time sensitive data and control operations can be disrupted by denial of service (DoS) attacks [11]. Unexpected network traffic cannot only impact operations but can also result in the improper or detrimental functioning of physical devices.

(6) Dependence on Computing Technologies
The SCADA systems are based on commercial operating systems (OS) and available software packages and thus also inherit their vulnerabilities.

B. Threats

(1) Denial of Service (DoS)
The generation of unusually high traffic to a server can render it incapable of serving the normal requests and degrade its performance. This could cause delays in execution of the control by the system making the process unstable.

(2)Man in the Middle Attack
The interception of normal system traffic can provide an intruder with the means to generate and inject malicious traffic aimed at disrupting the system. Passive eavesdropping can compromise data confidentiality and privacy.

(3)Replay Attack
After the normal transmission has been captured [1], the same could be played at a later time which can offset the normal system operation.

(4)Malware Attack
The biggest threat is the malware, which could enter the system from many potential avenues. Malware can replicate and propagate through the system and can compromise security and privacy for a long time before being detected.

C. Recent Attacks and Disruptions

In the following we describe few of the recent attacks on critical infrastructures originating from different sources:

(1) Sewage System: Disgruntled Employee
The most well-known security incident in SCADA systems is the attack on sewage control system in Queensland, Australia [15]. In 2000, after the installation of control system for the sewage plant, it experienced numerous operational problems causing flooding at nearby hotel grounds, park, and a river with a million liters of sewage. The problem was tracked down to acts by a disgruntled employee.

(2) Generator Attack: Exploiting System Knowledge
Based on the knowledge of commands used in the normal system operation, invalid sequences of valid commands can be used to destroy physical components of the smart grid [16]. In an experiment at Idaho National Lab in 2007, a computer program was used to rapidly open and close the circuit breakers of a diesel generator which eventually caused the diesel generator to explode.

(3) Stuxnet: Malicious users
A sophisticated malware program, Stuxnet [17] targeting control system software was used in 2010 to exploit system vulnerabilities to attack a PLC in Iran's uranium enrichment program [11].

IV. Resilience

The intrusions and attacks cannot be eradicated by any degree of protective mechanism as the hackers always are on a look out to identify and exploit system vulnerabilities. However, a guarded system should be resilient such that compromising a portion of it does not result in a system wide collapse, and also that the system recovers sustaining the least downtime and damage. Effective intelligent and distributed control [3] enables parts of the networks to remain operational and possibly reconfigure in case of failures. There is a need for making the system adaptive and intelligent to make use of rule based logic and historical data to thwart potential breaches similar to other security aware institutions like financial institutions and military organizations.

Traditional protective measures at network level, which we term as micro resilience strategies are not sufficient in themselves to meet the challenge, but must be applied in conjunction with more broader system-wide macro strategies. The proposed techniques must also be analysed and evolved continuously to meet the new challenges as they emerge.

A. Macro Resilience Strategies

A summary is given at Table I. This section discusses the various techniques for achieving macro resilience.

(1) Design and Architecture Principles
The system must be designed with security woven at each system tier. In [10] a novel network segmentation methodology is proposed for industrial processes, separating control hardware regulating input product flows from control hardware regulating output product flows. The proposed system comprises a graph-based representation of the physical process and a heuristic algorithm for generating network designs.

(2) Threat Awareness
The awareness of the potent dangers of a compromised system must be made clear to the operational staff. For instance, in systems, which do provide for password protection, many remain at their default values.

(3) Last Mile Protection
In the last mile the grid reaches the end users. The devices and networks close to user premises are more prone to attacks due to their exposed nature. The security measures should flow down to the communication end points in the field.

The concept of last mile vs. first mile protection comes from broadband networks and emerging perspective of first mile where broadband infrastructure development puts the needs of the consumers first before the communications service providers. The distinction comes from the difference in focus

(business case vs. digital divide) and priority (demand vs. supply); see [18] for other aspects and for a review. The same can be applied to smart grids in their early development where the notion of the priority of securing end equipments in the field should be established.

Table 1: Macro Resilience Strategies

Strategy	Affected Areas				
	Policy	***Standar-ds***	***Design***	***Software/Tools***	***Operati-ons***
Design and Architecture Principles	✓		✓		
Threat Awareness	✓				✓
Last Mile Protection		✓	✓		
Micro-grid	✓		✓		✓
Generation at point of use	✓		✓		
Open Source Systems		✓	✓	✓	
Physical security	✓				✓
Principle of Least Privilege			✓		
Risk Management and Contingency Planning	✓				
Threat Scenarios through Simulation				✓	
Network Attack Simulation Tools				✓	
Data Analytics	✓			✓	✓
System Modelling				✓	
Intrusion Detection and Prevention	✓			✓	
Honeypots	✓		✓		✓

(4) Micro Grids

Micro grids have their own localized power generation and storage capability. They provide the facility where the system can be served from multiple sources [3]. In case of a major shutdown across the network, critical services like hospitals and law enforcement can continue to operate through the facilities in their micro grids.

(5) Generation at Point of Use

The need for using greener energy sources like wind and solar makes it possible for traditional electricity consumers like home and small business owners to generate their own electricity and feed the surplus to the national grid. Tesla [19] has announced batteries for powering homes and with further advances in storage technologies, small consumers will be able to store electricity generated by them. This also enables users to continue with their normal usage in case of a blackout.

(6) Open Source Systems

The vulnerabilities of open systems can be relatively easily fixed due to the support of a large support community. This may seem counter-intuitive but consider how the potential security loopholes in proprietary systems can remain undetected even when exploited. Closed systems are also difficult to fix after the threat surfaces [20].

(7) Physical Security

The infrastructure may be target of a physical attack [3]. Additionally, network devices like switches and routers must be physically secured to limit access to critical entry points into the system. For wireless devices the intruder has to be in the vicinity to intercept and exploit the communication channel [2]. Autonomous video monitoring systems and access control can go a long way to deter the potential assailants.

(8) Principle of Least Privilege

The minimum access should be granted to a user group for achieving its interaction with the system. In [13] a technique, which covers the information accessible by a privilege class and models the flow of information to that class, is studied.

(9) Risk Management and Contingency Planning
The system should have detailed policies for what-if scenarios to enable a faster recovery cost shutdown. However, for a complex system like smart grid there could be a lot of contingencies to handle [1]. Tool such as machine learning and modeling approaches can help identify those contingencies and describe them in an easily accessible graphical format [13].

(10) Threat Scenarios through Simulation
The simulation models of the operational system can be used to check the vulnerabilities of the system and to fix them. A prototype for simulating computer network attacks is presented in [21] which can simulate large networks (thousands of hosts) realistically from attacker's point of view. The simulator is based on a model of computer intrusions, derived from the analysis of real world attacks [21]. A simulation study for the AMI infrastructure is provided in [13].

(11) Network Attack Simulation Tools
Snort [22] is a free tool available for intrusion detection and prevention. It could also be used to analyze traffic in real time, perform packet logging, protocol analysis and much more. It can detect a wide variety of attacks, like buffer overflows, and port scans etc. Another tool for host-based intrusion detection is OSSEC [23]. Network Attacks (NETA) [24] is based on OMNet++ and provides a framework for simulating attacks in heterogeneous networks.

(12) Data Analytics
The large data generated [25] in a smart system can be used to extract information through data analytics for effective management. The machine learning techniques investigated in [26] can be very helpful for implementing such a strategy.

(13) System Modelling
The structural vulnerabilities have been studied through complex network theory [27]. Randomized time delay countermeasures, as in [28], for smart meter remote connection or disconnection (RCD) attacks are proposed and their effectiveness demonstrated under different attack scenarios.

Table 2: Micro Resilience Strategies

Strategy	Affected Areas				
	Policy	**Standards**	**Design**	**Software/Tools**	**Operations**
Vulnerability Assessment and Scanning	✓			✓	
Cryptography		✓		✓	✓
Firewalls			✓	✓	
VPNs			✓		✓
Authorization and Accounting	✓				✓

Linear dynamical models, in [29], are used to model the behavior of control systems. A model for a web robot network (botnet) is proposed, in [30], which can be used to attack the system in different ways. The resiliency of the communication architecture under cyber attack is simulated in [19] for metering, and demand response.

(14) Intrusion Detection and Prevention
The Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS) work on rule based logic [29] to detect and prevent attacks against the system by recognizing abnormal events. Rule-based IDS for IEC 60870-5-104 protocol for SCADA networks is proposed using protocol analysis and a Deep Packet Inspection (DPI) [31]. Time-bounds checking techniques are proposed to detect intrusions in cyber-physical control systems [32]. A semi-supervised anomaly detection model is proposed in [11]. The lack of adequate intrusion detection and their limitations for the smart grid are discussed in

[33]. Domain-specific anomaly detection algorithms are needed which can classify both measurements and commands as valid/anomalous, as investigated in [34].

(15) Honeypots
A honeypot consists of a computer, data, or a network site that is actually isolated and monitored, but appears exposed as a resource of value to attackers. It can be used to detect, and counteract attempts of unauthorized use [35]. The actual system remains hidden and protected.

B. Micro Resilience Techniques

All the conventional approaches to providing the network and communications infrastructure are still relevant but the safeguards now must be placed more stringently and be widely deployed. This section discusses the various techniques and tools that facilitate for achieving micro resilience.

(1) Vulnerability Assessment and Scanning
New vulnerabilities affect computer systems and present security challenges and unknown system impact [13]. The vulnerability assessment of the system through some agency other than the implementers can help determine and uncover the weaknesses in the system. Scanning for open ports can also help isolate and overcome potential problems.

(2) Cryptography
The cryptographic algorithms can make it infeasible for an intruder to decipher the information and deny the opportunity to inject malicious traffic [2]. Cryptography and key management techniques can offer some protection [36].

(3) Firewalls
The standard practices are helpful to segregate the corporate network from malicious traffic. Firewalls can provide an effective protection layer for connected embedded computers such as smart grid devices [37].

(4) Virtual Private Network (VPN)
VPNs can allow secure access to the networked corporate resources over geographically separate locations ensuring the implementation of the network management policies.

(5) Authorization and Accounting
The Access control lists (ACL) can be used to filter unwanted traffic in a network based on IP headers in the source or destination packet. The intrusion attempts or anomalous traffic can be easily discovered if all the user and system activity is being logged and analyzed at various tiers.

Conclusion

The integration of computing and communications technologies to make the electricity infrastructure smart provides benefits to all the stakeholders, that is, consumers, distributors and generation companies. However, it makes the grid vulnerable to cyber attacks by exposing a large attack surface to hackers through diverse system entry points, potentially compromising the whole system. The smart grid attacks can render the infrastructure inoperable with consequences for public security and safety.

The cyber security challenges cannot be met through only considering a conventional network view as the security mandates protecting not only the corporate network but also the widespread system nodes. A holistic approach to tackling the challenges through a mix of resilience techniques at the micro and micro level is proposed which can help to identify, isolate, contain and overcome the cyber security challenges. It is an ongoing process rather than a one-shot operation, and must continually evolve to meet the new challenges as they surface.

References

[1] Yilin Mo; Kim, T.H.-H.; Brancik, K.; Dickinson, D.; Heejo Lee; Perrig, A.; Sinopoli, B., "Cyber–Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE , vol.100, no.1, pp.195,209, Jan. 2012. doi10.1109/JPROC.2011.2161428

[2] Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk. 2015. Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security (CPSS '15). ACM, New York, NY, USA, 61-68.DOI=10.1145/2732198.2732203

[3] Amin, S. M. (2011), 'Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control.', Eur. J. Control 17 (5-6) , 547-567.

[4] Zubair A. Baig and Abdul-Raoof Amoudi, "An Analysis of Smart Grid Attacks and Countermeasures" Journal of Communications, vol. 8, no. 8, pp. 473-479, 2013. doi: 10.12720/jcm.8.8.473-479

[5] NEMA Report, Modernizing America's Electric Grid Solutions for Transmission, Storage, Distribution & Resilience For Consideration during the 2014 Quadrennial Energy Review, Available online: http://www.nema.org/Policy/Documents/QER_Recommendations-for-Modernizing-Americas-Electrical-Grid.pdf.

[6] Alejandro PINTO, 'Cyber security of SMART GRIDS Commission Policy initiatives-State of play', Presentation to the European Commission. Available online: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/eu-us-open-workshop/2nd-presentation

[7] IEEE Guide for Electric Power Substation Physical and Electronic Security," IEEE Std 1402-2000 , vol., no., pp.i,, 2000 doi: 10.1109/IEEESTD.2000.91305 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=836296&isnumber=18048

[8] The North American Electric Reliability Corporation (NERC). http://www.nerc.com/comm/CIPC/Pages/default.aspx

[9] Image source: Google Images.

[10] Béla Genge and Christos Siaterlis. 2014. Physical process resilience-aware network design for SCADA systems. Comput. Electr. Eng. 40, 1 (January 2014), 142-157. DOI=10.1016/j.compeleceng.2013.11.018 http://dx.doi.org/10.1016/j.compeleceng.2013.11.018

[11] Á. MacDermott, Q. Shi, M. Merabti, and K. Kifayat, "Intrusion Detection for Critical Infrastructure Protection," in 13th Annual Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting (PGNet 2012), 2012

[12] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, B, "Attack taxonomies for the Modbus protocols", Int. J. Critical Infrastructure Protection, vol. 1, pp. 37–44, Dec. 2008.

[13] A. Hahn, and M. Govindarasu, "Cyber Attack Exposure Evaluation Framework for the Smart Grid", IEEE Trans. on Smart Grid, Vol. 2, No. 4, Dec 2011.

[14] nmap: https://nmap.org/

[15] Slay, J., and Miller, M. "Lessons learned from the maroochy water breach" in Critical Infrastructure Protection (November 2007), vol. 253/2007, Springer Boston, pp. 73–82.

[16] Case Study 10 [ICS]: The Aurora attack. http://www.secmatters.com/casestudy10

[17] J. Vijayan, B, "Stuxnet renews power grid security concerns," Computerworld, Jul. 26, 2010. Available online: http://www.computerworld.com/article/2519574/security0/stuxnet-renews-power-grid-security-concerns.html

[18] Mcmahon, R., Philpot, D., O'donnell, S., Beaton, B., Whiteduck, T., Burton, K., Gurstein, M. The First Mile of Broadband Connectivity in Communities:. *The Journal of Community Informatics*, North America, 10, Mar. 2014. http://cijournal.net/index.php/ciej/article/view/1123.

[19] Tesla: http://www.bbc.co.uk/news/technology-32545081

[20] R. Clarke, and D. Dorwin, “Is Open Source Software More Secure?”, Project Report, University of Washington, http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf
[21] C. Sarraute, F. Miranda, and J. I. Orlicki, "Simulation of Computer Network Attacks",Cornell University library, Available online: http://arxiv.org/abs/1006.2407
[22] Snort: https://www.snort.org/ (Date accessed:25 May 2015).
[23] OSSEC: http://www.ossec.net/ Date accessed:25 May 2015.
[24] NETA: www.omnetpp.org/component/content/article?id=3712:neta-release
[25] Technical report, “Ten Leading Practices for Smart Grid Analytics”. Accenture, 2011. http://www.accenture.com/SiteCollectionDocuments/PDF/WSS101_SmartGridAnalytics_A4.pdf
[26] Rudin, C.; Waltz, D.; Anderson, R.N.; Boulanger, A.; Salleb-Aouissi, A.; Chow, M.; Dutta, H.; Gross, P.N.; Huang, B.; Ierome, S.; Isaac, D.F.; Kressner, A.; Passonneau, R.J.; Radeva, A.; Wu, L., "Machine Learning for the New York City Power Grid," Pattern Analysis and Machine Intelligence, IEEE Transactions on , vol.34, no.2, pp.328,345, Feb. 2012 doi: 10.1109/TPAMI.2011.108.
[27] Ettore Bompard, Roberto Napoli, Fei Xue, Analysis of structural vulnerabilities in power transmission grids, International Journal of Critical Infrastructure Protection, Volume 2, Issues 1–2, May 2009, Pages 5-12, ISSN 1874-5482, http://dx.doi.org/10.1016/j.ijcip.2009.02.002.
[28] Temple, W.G.; Binbin Chen; Tippenhauer, N.O., "Delay makes a difference: Smart grid resilience under remote meter disconnect attack,", 2013 IEEE International Conference on , vol., no., pp.462,467, 21-24 Oct. 2013.
[29] Jafar A. Alzubi, Omar A. Alzubi, and Thomas M. Chen. *Forward Error Correction Based on Algebraic-Geometric Theory*. Springer Publishing Company, Incorporated, 2014.
[30] M. Brand, C. Valli, and A. Woodward, "A Threat to Cyber Resilience: A Malware Rebirthing Botnet", International Cyber Resilience conference Security Research, 2011.
[31] Yang, Y.; McLaughlin, K.; Littler, T.; Sezer, S.; Wang, H.F., "Rule-based intrusion detection system for SCADA networks," Renewable Power Generation Conference (RPG 2013), 2nd IET, vol., no., pp.1,4, 9-11 Sept. 2013.
[32] F. Mueller, S. Bhattacharya and C. Zimmer, "Cyber Security for Power Grids", 2009. http://cimic.rutgers.edu/positionPapers/paper-FrankMueller.pdf
[33] N. Kush, E. Foo, E. Ahmed, I. Ahmed, and A. Clark,”Gap analysis of intrusion detection in smart grids" , Proceedings of the 2nd International Cyber Resilience Conference. Duxton Hotel, Perth, 2011.
[34] Sridhar, S.; Hahn, A.; Govindarasu, M., "Cyber attack-resilient control for smart grid,"Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, vol., no., pp.1,3, 16-20 Jan. 2012.
[35] Honeyspot computing, Wikipedia, http://en.wikipedia.org/wiki/Honeypot_(computing)
[36] Swapna Iyer, “Cyber Security for Smart Grid, Cryptography, and Privacy,” International Journal of Digital Multimedia Broadcasting, vol. 2011, Article ID 372020, 8 pages, 2011.
[37] Firewall: Smart Grid Security: Blocking Cyber-attacks with an Embedded Firewall (EE Catalog Oct 2012). Available online: http://www.iconlabs.com/prod/smart-grid-security-blocking-cyber-attacks-embedded-firewall-ee-catalog-oct-2012.