View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Gyandhara International Academic Publication (GIAP): Journals

International Journal of Students' Research In Technology & Management
Vol 3(7), September - October 2015, ISSN 2321-2543, Pg 436-439

Synchrophasor Technology for Cyber Security in Smart Grid

[1]P. Thangarathinam, [2]N. Suganya, [3]T. Praddeep, [4]S.Vignesh

Department of Electrical and Electronics Engineering, Kongu Engineering College, Tamilnadu, India
[1]thangam102@gmail.com,[2]suganraj06@gmail.com,[3]praddeepsvp@gmail.com
[4]vicky900666@gmail.com

DoI: 10.18510/ijsrtm.2015.378
Article History: Received on 25th June 2015, Revised on 17th August 2015, Published on 28th October 2015

***Abstract*—Smart grid is controlled by an authority personnel who uses LAN or the internet to control it. By knowing this information any one from outside can control the smart grid using LAN or the internet. This process of hacking the smart grid control is known as aurora attack. The Aurora attack may pose a risk to rotating machinery operating under certain conditions on the electrical grid. The Aurora attack involves opening and closing one or more circuit breakers, resulting in an out-of-synchronism condition that may damage rotating equipment connected to the power grid. This paper focuses on the Aurora attack on a synchronous generator and the existing technology available to mitigate the attack. The root cause of the vulnerability is breakdown in security. The first level prevents the attack with sound security practices. The second level protects the equipment in the event that the security level is compromised. The equipment can be protected using wide-area synchronized phasor measurement and protection system and security considerations.**

***Keywords*—Aurora attack, Rotating Machinery, Out of synchronism, Synchronized Phasor Measurement Unit.**

I. INTRODUCTION

The intent of the Aurora attack is to intentionally open a breaker and close it out of synchronism to cause damage to the connected generators and motors. Good engineering practice includes synchronism-check relays installed in the power system to prevent out-of-synchronism closing. The Aurora attack assumes that these relays could be hacked to defeat their purpose. When an out-of-synchronism close is initiated, the high electrical torque translates into stress on the mechanical shaft of the rotating equipment. This stress reduces the life of the rotating equipment and can destroy it. The U.S. Department of Homeland Security worries that coordinated attacks could cause prolonged outages in large sections of the electrical grid. In order to initiate an Aurora attack, the attacker would need the following components:

- Power engineering knowledge
- Power system information
- Hacking skills

Now days, all the Circuit Breakers function using Intelligence Electronic Device (IED) based on Microprocessor (Fig. 1)

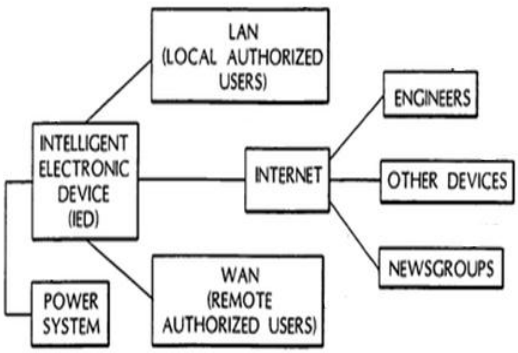

Fig .1 Intelligent Electronic Devices

II. BACKGROUND OVERVIEW

A. *Generator Protection in Existing System*

The Aurora attack seeks to exploit the opportunity to connect two electrical systems out of synchronism. This opportunity could arise from an unprotected system or a system not configured to recognize the threat of an Aurora attack. The Aurora attack seeks to take advantage of the time delay between a protective relay recognizing an out-of synchronism issue and the initiation of a protection action. Protective relays continuously sample the voltage and current of the power system and calculate other key protection information based on these samples. The relay must be able to separate a bad data sample from a sudden change in the measured variable. This process of sample verification and signal processing is referred to as filtering. One example of filtering is to average a number of inputs together and use the calculated average for protection decisions. This averaging process helps to smooth the signal, but it reduces the speed of the relay for recognizing sudden changes in the system. In order to keep the system connected and avoid separating based on variations in the power system; protection engineers also typically add time delays in the trip command sequence. These delays, either from signal processing or intentional design, open a window of opportunity for attack. As shown in

Fig. 2 [3], the Aurora attack is designed to open a circuit breaker, wait for the system and generator to slip out of synchronism, and reclose the breaker, all before the protection system recognizes and responds to the attack.

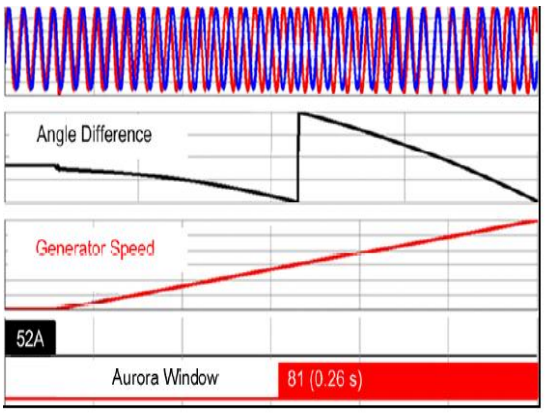

Fig. 2. Aurora Window of Opportunity

The window of opportunity can be narrowed by analyzing the response time of the generator and circuit breaker protection elements.

B. Drawbacks of Existing System

Traditional generator protection elements typically actuate and block reclosing within 15 cycles. Many variables affect this time, but the discussion in this paper uses this estimate for the Aurora window of opportunity Another contributing factor to why typical generator protection does not guard against an Aurora attack is shown in Fig.3 that the attack may not be initiated at the generator. By initiating the attack at a system tie point away from the generator, the synchronism-check element at the generator does not measure a difference between the two systems. This targeting of the tie-in breakers instead of the generator requires the protection engineer to expand the scope of typical generator protection to include the surrounding system tie points.

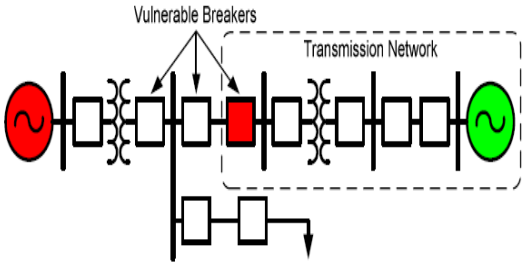

Fig. 3 The Target of the Aurora attack is the grid tie in the circuit breaker

III. THE PROPOSED SYSTEM

C. Phasor Measurement Technology

Synchronized Phasor measurements have become a mature technology with several international manufacturers offering commercial phasor measurement units (PMUs) which meet the prevailing industry standard for synchrophasors. With the occurrence of cyber security problems and major blackouts in many power systems around the world, the value of data provided by PMUs has been recognized, and installation of PMUs on power transmission networks of most major power systems has become an important activity. The occurrence of cyber security problem in many major power systems around the world has given a new impetus for large-scale implementation of wide-area measurement systems (WAMS) using PMUs and phasor data concentrators (PDCs) in a hierarchical structure.

D. Proposed System model block diagram

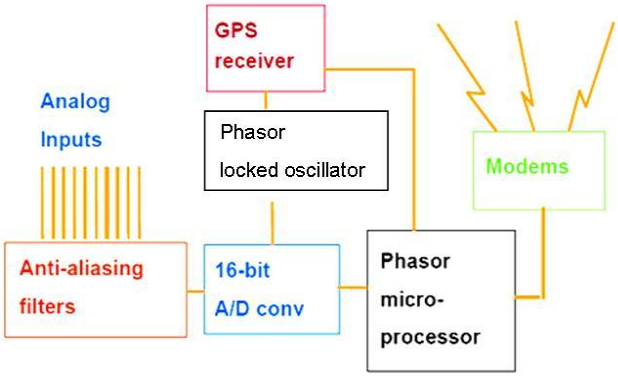

Fig. 4 Model Block Diagram of PMU

Data provided by the PMUs are very accurate and enable system analysts to determine the exact sequence of events which have led to the security crimes, and help analyse the sequence of events which helps to pinpoint the exact cause and malfunctions that may have contributed to the catastrophic failure of the power system. As experience with WAMS is gained, it is natural that other uses of phasor measurements will be found.

IV. VULNERABILITY IS SYSTEM DEPENDENT

The level of vulnerability to an Aurora attack is dependent on the configuration and operating characteristics of each system. For example, if the generator is on a backup system or only operates when disconnected from the main system, there is little Aurora risk to the generator. Generators connected to the grid through a single tie line are the most likely targets. These systems only need a single circuit breaker compromised for an attack to be initiated. In cases where the generating facility and utility are owned or controlled by separate parties, the mitigation protection becomes more difficult.[1] These installations typically lack the communications links that indicate the tie-breaker position. Without this indication, the generating facility must evaluate protection schemes that only require local data. Single-tie generating stations are the applications most likely to benefit from an Aurora hardware mitigation device.

Power flow is an important variable when assessing the Aurora vulnerability. For protection purposes, the risk should

be evaluated based on the power flow at the connection point. Systems can be broken into three groups as follows:

Systems with own generation that also receive power from the grid. Systems like this may include industrial plants that create their own generation but still need to purchase power from the grid.

Systems that approximately balance the power they generate with the power they need. The result is that little power is imported or exported.

Systems that export power to the grid. The variations in power flow affect the ability and type of protection needed to detect an undesired disconnection. Each of these groups provides a different system and vulnerability window. System evaluation should analyze an attack under each operating condition.

V. Vulnerability Test on Relay Characteristics

The transmission system protection relays plays important role in determining the network. If a fault on line persists for long duration without being detected and isolated then it may cause severe damage to the network security. Hence the settings of protection relays are made sensitive to detect even the weakest fault. These settings some time make relay vulnerable to false operation during remote fault or when the system is highly stressed. So the relay that was set properly for one network condition may become vulnerable to undesired tripping when network condition changes.

VI. System Protection with Synchrophasor Technology

Synchronized phase or measurements offer solutions to a number of complex protection problems. In general, phasor measurements are particularly effective in improving protection functions, which have relatively slow response times. For such protection functions, the latency of communicating information from remote sites is not a significant issue. Adaptive Out-Of-Step Protection is recognized that a group of generators going out of step with the rest of the power system is often a precursor of a complete system collapse. Whether an electromechanical transient will lead to stable or unstable condition has to be determined reliably before appropriate control action could be taken to bring the power system to a viable steady state. Out-of-step relays are designed to perform this detection and also to take appropriate tripping and blocking decisions. Traditional out-of-step relays use impedance relay zones to determine whether or not an electromechanical swing will lead to instability. In order to determine the settings of these relays, it is necessary to run a large number of transient stability simulations for various loading conditions and credible contingencies. Using the apparent impedance trajectories observed at locations near the electrical centre of the system during these simulation studies, two zones of an impedance relay are set, so that the inner zone is not penetrated by any stable swing.

Security-Dependability should be recognized that a relay has two failure modes. It can trip when it should not trip (a false trip) or it can fail to trip when it should trip. The two types of reliability have been designated as "security" and "dependability "by protection engineers. The existing protection systems with their multiple zones of protection and redundant systems are biased toward dependability, i.e., a fault is always cleared by some relay. [2] The result is a system that virtually always clears the fault but as a consequence permits larger numbers of false trips. High dependability is recognized as being a desirable protection principle when the power system is in a normal "healthy" state, and high-speed fault clearing is highly desirable in order to avoid instabilities in the network. The consequent price paid in occasional false trip is an acceptable risk under "system normal" conditions. However, when the system is highly stressed false trips exacerbate disturbances and lead to cascading events. An attractive solution is to "adapt" the security—dependability balance in response to changing system conditions as determined by real-time phasor measurements. With three primary digital protection systems it is possible to implement an adaptive security–dependability scheme by using voting logic (see Fig.5). The conventional arrangement is that if any of the three relays sees a fault, then the breaker is tripped. More secure decision would be made by requiring that two of the three relays see a fault before the trip signal is sent to the breaker. The advantage of the adaptive voting scheme is that the actual relays are not modified but only the tripping logic responds to system conditions.

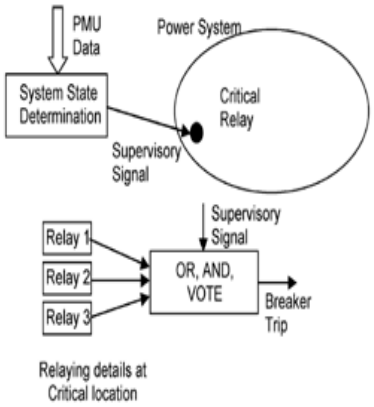

Fig. 5 Adjustment of Dependability- Security balance under stressed system condition

VII. Security Considerations to Mitigate An Aurora Attack

The Aurora attack can easily target systems that have little or no security. Take proper security precautions should be taken to protect the system from both physical attacks and cyber-attacks. Many technical papers are available to show proper methods of securing substations or communications networks. An electric utility communications system is typically isolated from the public Internet system. [1] This isolation provides one level of protection but is insufficient by

itself to prevent a cyber-attack. Any assessment of protection against the Aurora Vulnerability must start with a review of security measures. Proper security for any system must be

viewed as layers of protection with security in depth. In order to execute a successful Aurora attack, the perpetrator must have knowledge of the local power system, know and understand the power system interconnections, initiate the attack under vulnerable system load and impedance conditions, and select a breaker capable of opening and closing quickly enough to operate within the vulnerability.

In order to access a protective relay, the attacker needs physical or electronic access to the relay. Assuming the attack is initiated via remote electronic access, the perpetrator needs to understand and violate the electronic media, find a communications link that is not encrypted or is unknown to the operator, ensure no access alarm is sent to the operators, know all passwords, or enter a system that has no authentication. If a protective relay is used for the attack, the perpetrator also needs to be able to communicate with the relay to control the appropriate circuit breaker, understand the engineering needed to initiate a fast trip and close, and disable any logic and protection elements preventing fast open/close operations.

Some basic security considerations include:

- Know and secure all communications paths to your system assets. These paths include SCADA, energy management system (EMS), engineering access, report collection, maintenance, telephone lines, wireless, Internet, and interconnections and bridges between systems.
- Use strong passwords. Make sure your equipment uses strong length and character passwords (e.g., weak: Webster, strong: M$i4fp&r).
- Manage passwords. Do not use default passwords, change them periodically, change them when someone leaves the company, control them, and use different ones in different areas.
- Practice "need-to-know." Keep your designs safe and secure. Limit access to system details to those who really need to know them in order to do their jobs.
- Compartmentalize knowledge. Keep security information localized. Do not use the same security and passwords throughout the system or on multiple systems.
- Review alarms and access activity. Know which users are on your system and why.
- Guard your access tools. Keep laptop computers locked and encrypted. Keep system drawings in a secure location with restricted access. Know who has keys, and set up multiple
- Levels of access. By initiating proper and prudent security measures, the Aurora vulnerability can be mitigated.

VIII. CONCLUSION

System owners must contend with not only accidental faults to the system but also targeted attacks seeking to damage equipment. Proper security must become a standard operating policy. Implementing proper security, including system, information, access, passwords, and encryption, produces an effective barrier to the Aurora attack. Protective relay schemes were modeled using a real-time phasor measurement unit, and the results compared. While no silver bullet exists for perfect protection, this testing clearly shows existing digital relays with proper protection schemes offer protection against Aurora attacks. While the standard generator protection did operate well under most conditions, it did not operate in a timely manner under near balanced load conditions. Wide-area synchronized phasor measurement is the best one to mitigate aurora attack.

IX. ACKNOWLEDGEMENT

At this moment of accomplishment, first of all we have to specially thank our guide, Dr. R.Meenakumari, Professor, Dept. of EEE, Kongu Engineering College, Erode, Tamilnadu, India. This work would not have been possible without her guidance, support and encouragement. Under her guidance we are successfully overcame many difficulties and learned a lot. We can't forget her hard times. Despite of her heavy work schedule, she used to review our thesis progress, give her valuable suggestions and made corrections. Her unflinching courage and conviction will always inspire us .It is to her that we dedicate this work.

REFERENCES

[1] D. Salmon, M. Zeller, A. Guzmán, V. Mynam, and M. Donolo, "Mitigating the Aurora Vulnerability With Existing Technology" proceedings of the 36th Annual Western Protective Relay Conference, Spokane, WA, October 2009.

[2] Synchronized Phasor Measurement Applications in Power Systems Jaime De La Ree, Senior Member, IEEE, Virgilio Centeno, Senior Member, IEEE, James S. Thorp, Life Fellow, IEEE, and A. G. Phadke, Life Fellow, IEEE, IEEE TRANSACTIONS ON SMART GRID, VOL. 1, NO. 1, JUNE 2010

[3] Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator? Mark Zeller, *Schweitzer Engineering Laboratories, Inc.* Protective Relay Engineers, 2011 64th Annual Conference

[4] Unified Real Time Dynamic State Measurement by Power Grid Corporation of India and Central Electrical Authority of India.

[5] www.phasor-rtdms.com

[6] www.cea.nic.in