www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Improvement of the WAMS communication network against late attacks

D.Kalaivani, J.Gayathri

M.E. (Final year Student), Department of CSE, College of Gnanamani
Asst.Prof /CSE, College of Gnanamani.

ABSTRACT

Highly flexible, secured and bi-directional communication infrastructure for power system data exchange is the stepping stone for the success of smart grid vision. Traditionally, wired communication is the first choice for monitoring, protection and control systems. With advent in communication technologies, the wireless technologies have also emerged as potential contender for data communication in various industrial applications. Wireless technologies have distinct advantages over wired in terms of higher mobility, lower installation cost and faster deployment among others. The deployment of wireless technologies for monitoring and control systems of Smart Grid namely WAMS has been largely unexploited area. This paper devises a systematic approach that identifies the communication requirements of WAMS, defines the capability of various wireless technologies such as Wireless LAN (WLAN), Wi-Max, Wi-Fi, GSM, GPRS etc. based on performance criteria and selects the potential wireless communication technologies for WAMS based on closest match. The WAMS communication requirement specifications have been arrived based on Indian Smart Grid case studies. The paper also discusses the challenges and hence opportunities associated with implementation of wireless technologies for Smart Grid.

INTRODUCTION

Complex power exchange among regions, seasonal loads, effect of weather and critical events are leading to unwanted scenarios like congestion of corridor, fast changing power patterns, emergency loading, etc. All these complex operating scenarios combined with aging infrastructure have resulted in power systems being operated closer to their stability limits. Under such complexities, carrying out monitoring, protection on real time basis and responding to contingencies are critical for maintaining reliability and stability of the grid. Present power grid uses Supervisory Control And Data Acquisition (SCADA) system/Energy Management System (EMS) for situational awareness. The state estimation based on these values result in an inaccurate estimation and typically take few minutes to estimate the state and provide the knowledge of situation. However, the power system operation is highly dynamic and it changes the state at much higher rate than estimation.

Wide area measurement systems (WAMS) that measure state instead of estimation have come forward as a prominent technology option to improve the observability and situational awareness in both today's and the future electrical grids. WAMS obtains a lot of status data at high speed in many different forms and aggregates it to control centers for informed decision making. The control decisions are passed back in reverse directions to activate actuators like circuit breakers, relays etc. Thus highly flexible, scalable, seamless, bi-directional and secured communication infrastructure is vital for effective and efficient deployment of WAMS in Smart Grid.

WIDE AREA MEASUREMENT SYSTEM

The rapid deployment of synchrophasor measurements units (PMUs) supporting Wide Area Measurement System (WAMS) in the smart grid transmission system has opened opportunities to enhance the grid operations

Author for correspondence:
Department of CSE College of Gnanaman,

through the introduction of WAMS applications. However, the increased deployment of synchrophasor technologies increases the effective attack surface available to attackers and exposes WAMS applications. Such applications have strict and stringent delay requirements, e.g., end to end delay as well as delay variation between measurements from different PMUs.

PMU

The increased integration of PMUs introduces new vulnerabilities to cyber-attacks, which if exploited by attackers, may have damaging consequences ranging from local power outage to complete blackout. Recently, multiple PMU vulnerabilities have been reported by Arbiter [5]; these vulnerabilities can cause a Denial of Service (DoS) as identified in the Arbiter Systems Power Sentinel PMU. Moreover, some PMU vendors such as the National Instruments PMU (NI Grid Automation System) provide Linux-based PMUs that can be subject to linux worm/malware attacks (such as Moose and Darlloz.A). Many research efforts toward building a secure and reliable distributed WAMS architecture have been proposed recently.

PDC TIMER

The shared data network that forwards the phasor measurements to PDCs provides services to other sensors such as Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs), a video for surveillance purpose, and Voice over IP applications. Therefore, this shared network can contribute to larger network latency for a particular PDC. A WAMS with multiple PMUs communicating with different PDCs. In particular, for PDC (n), two PMUs are sending their measurements through a communication network. Each PMU might experience different network latency; thus, the packet arrival times of both PMUs at the PDC might vary.

DELAY ATTACK

The constructed trees before and after the attack. We notice that attacking a communication link will change the constructed trees and a new path has been constructed. Figure (6) shows the number of invalid measurements as we vary the amount of injected delays. Clearly, the larger the delay value, the more invalid measurements and hence more dropped packets at PDCs. In the case of IEEE 30-bus system, the model was always able to avoid the attacked link and construct forwarding trees that will meet the delay constraints. Moreover, we simulate an attack on a communication link in the network; such attack causes link disconnection.

MULTICAST TREE

The authors construct QoS multicast tree to deliver control massages from controller to a set of remote devices while minimizing the end-to-end delay. In, an analysis of the communication network for WAMS applications with focus on end-to-end delay is presented. The aim of such analysis is to quantify the end-to-end delay given a specific communication network (envisioned design for the Swedish transmission grid). In, the authors proposed a flocking based multicast routing for the smart grid with efficient situational-awareness for network traffic. The aim is to balance the end-to-end delay and bandwidth for WAMS communication. However, considering the time variation between the arrivals of synchrophasor measurements; hence, the PDC timer in the tree construction has not been addressed.

DELAY ATTACK IMPACT ANALYSIS

In this subsection, we analyze the impact of delays attacks (due to cyber-attacks) on the constructed trees. Even though WAMS communication network tends to be a dedicated Intranet, this does not mean that such networks are immune to cyber-attacks. For instance, removable media such as USB drives can be used to carry malware and hack computers to be used as sources of other attacks such as denial of service (DoS). Moreover, increasing the number of mobile devices can be used as a malicious medium and we cannot rule out the possibility that utility employees directly inject attacks into the network. A delay attack may be caused by flooding the network with a huge amount of redundant data traffic to consume the target (communication link) resources such as network bandwidth; this means that a very limited

bandwidth is left for the useful data. In this case, the measurements data will experience longer communication delays and as a result may be dropped by the PDC.

VALIDATION ON REAL-TIME CO-SIMULATOR

In this subsection, we validate the performance of the proposed model in comparison with shortest path tree using a real-time co-simulation testbed. In this testbed, a hardware in- the-loop approach to simulate the power grid real-time dynamics is used. Our hardware-in-the-loop (HIL) testbed is enabled with four PMUs from different manufacturers. Those PMUs receive the analog output from Hypersim, and sample the measurements in the form of C37.118 traffic. The traffic generated by the PMUs is routed to two physical PDCs, one considered as local and the other as regional. The local PDC aggregates the measurements, and forwards them to the regional PDC. The regional PDC sends the received measurement to the control center.

EXISTING SYSTEM

Present power grid uses Supervisory Control and Data Acquisition (SCADA) system/Energy Management System (EMS) for situational awareness. The state estimation based on these values result in an inaccurate estimation and typically take few minutes to estimate the state and provide the knowledge of situation. However, the power system operation is highly dynamic and it changes the state at much higher rate than estimation.

Wide area measurement systems (WAMS) that measure state instead of estimation have come forward as a prominent technology option to improve the observability and situational awareness in both today's and the future electrical grids. WAMS obtains a lot of status data at high speed in many different forms and aggregates it to control centers for informed decision making. The control decisions are passed back in reverse directions to activate actuators like circuit breakers, relays etc. Thus highly flexible, scalable, seamless, bi-directional and secured communication infrastructure is vital for effective and efficient deployment of WAMS in Smart Grid.

PROPOSED SYSTEM

Research paper presents the framework of smart grid and challenges related to wireless communication infrastructure of the smart gird. The potential smart grid applications for wireless LAN, WiMAX, ZigBee, 3G/4G cellular, MobileFi, digital microwave, Bluetooth have been discussed in the paper. Research paper has come up with a systematic approach to provide guidelines for smart grid wireless communications.

It is based on the framework of cyber-physical system (CPS). Research paper reviews methods for joint transmission over the powerline and wireless channels to improve reliability of smart grid communication. The paper explores design trade-offs in communication performance vs. implementation complexity for joint transmission. Research paper gives a detailed comparative study of communication protocols that can be implemented in this domain. It focuses on various aspects such as network spanning, data rates, power consumption, data security and encryption standards, data access and spread spectrum techniques, modulation and duplexing schemes for all the communication standards in Smart Grid. However it does not explore the communication requirements to be met for smart grid.

PROPOSED APPROACH

Presents the framework of smart grid and challenges related to wireless communication infrastructure of the smart gird. The potential smart grid applications for wireless LAN, WiMAX, ZigBee, 3G/4G cellular, MobileFi, digital microwave, Bluetooth have been discussed in the paper. Research paper has come up with a systematic approach to provide guidelines for smart grid wireless communications. It is based on the framework of cyber-physical system (CPS). Research paper reviews methods for joint transmission over the powerline and wireless channels to improve reliability of smart grid communication. The paper explores design trade-offs in

communication performance vs. implementation complexity for joint transmission.

Research paper gives a detailed comparative study of communication protocols that can be implemented in this domain. It focuses on various aspects such as network spanning, data rates, power consumption, data security and encryption standards, data access and spread spectrum techniques, modulation and duplexing schemes for all the communication standards in Smart Grid. However it does not explore the communication requirements to be met for smart grid. This paper mainly focuses on WAMS deployment in smart grids and wireless communication technologies for information flow for monitoring, protection and control functions of WAMS. The contribution of this paper is the systematic approach to select wireless communication technologies for WAMS infrastructure in the smart grid. The devised approach identifies the communication requirements specifications of typical hierarchical WAMS architecture based on number of monitoring devices; classifies various wireless communication technologies based on performance parameters; matches both based on criterion and provide with recommendations in terms of suitable wireless communication technologies for each of hierarchy of particular WAMS deployment in smart Grid.

HIERARCHICAL WAMS ARCHITECTURE

Hierarchical WAMS architecture logically divides the grid monitoring and control into two or more levels based on deployment of PMUs and PDCs in wide area network. Hierarchical WAMS architecture, outlines typical levels namely substation, regional and national or central control centers. PDCs are classified as Substation or Local PDC, Regional PDC and Super or Master PDC based on their placement into particular hierarchical level. The roles and responsibilities of each of the PDCs in power grid varies according to particular hierarchical level it belongs to.

Local/Substation PDC

Local PDCs are installed at substations and they typically cater to maximum of few tens of PMUs. They aggregate and time-align synchrophasor data from multiple substation level PMUs and feed the data to upper level PDCs namely regional PDCs. Optionally the time aligned and aggregated data could be sent to third party clients for analysis.

Regional PDC

Intermediate regional PDCs are installed at regional control center and cater to maximum of few hundreds of direct or indirect PMUs. They collect synchrophasor data from multiple substation level PDCs, further aggregate, time align and feed the data to higher level PDC namely master PDC. Many of the times, it hosts data analytics applications and data visualization.

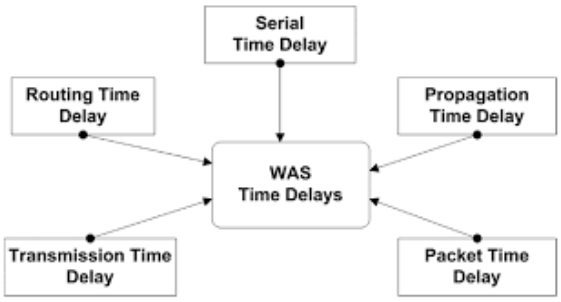
Master/Super PDC

Master PDC is installed at main or national control center and caters to maximum of few thousands of direct or indirect PMUs. It aggregates and time aligns synchrophasor data from multiple regional PDCs. It hosts Wide Area Monitoring, Protection and Control (WAMPAC) applications that run on synchrophasor data. The protection and control commands are sent back to respective primary equipment such as relays or circuit breaker via communication network. It also provides data visualization and storage facility.

Conventionally, the communication within and beyond substations is dominantly wired. The wired communication has always struggled with higher complexity, frequent maintenance and longer down times. Over the last few years, wireless technology has taken a huge leap in terms of gaining acceptance as communication choice for many industrial applications. Advanced wireless systems bring the benefits of inexpensive products, rapid installation, low maintenance and less number of down times with widespread access, and mobile communications which wired technologies and even the older wireless technologies often cannot offer. Some of the significant advantages of wireless technologies over wired communication are listed below:

- Wireless can be deployed anywhere and anytime so there is widespread access to information.
- Wireless deployment removes or reduces complexity introduced by wires.
- Wireless enables higher flexibility and scalability in network deployment.

- Wireless communication network results in lower installation, maintenance and service cost.
- Hierarchical WAMS architecture can utilize different wireless technologies at different levels owing to different requirements and availability of variety of wireless technologies.



METHODOLOGY

Communication bandwidth

Channel capacity defines amount of data that can be carried by a communication network. Essentially, the chosen communication infrastructure should satisfy the bandwidth requirement in a reliable way. To understand the typical communication bandwidth requirement of the WAMS deployment, Indian grid is considered as a case study. There are five major regions in this grid, i.e., Northern Region (NR), Eastern Region (ER), North Eastern Region (NER), Western Region (WR) and Southern Region (SR). Presently, all five regions are synchronized and is addressed as the All India Synchronized Grid.

LATENCY

Latency is defined as the time delay between the time that data is generated and it's availability for applications. The latency in WAMS architecture is characterized by communication latency and PMU, PDC latency. Communication latency on the network is comprised of transmission delays, propagation delays, processing delays, and queuing delays. PDC latency comprises of PDC device latency and PDC wait time.

POWER CONSUMPTION

Wireless technologies use special devices like power amplifiers to transmit data and hence use significant amount of power. Many power scavenging applications require the entire communication infrastructure including transmitters, receivers, data transmission modes to be designed for low power consumption.

CYBER SECURITY

With increase in "internet of things" systems, the cyber attacks such as piggybacking, cloning, hijacking, and cracking are on the rise. WAMS or smart grid is no exception to this. There is always a need to improve device and communication level security in WAMS. This has led to inception of newer wireless communication technologies with latest security standards implemented.

CONCLUSION

Wireless technologies are significant contenders to meet WAMS communication requirements with many advantages over already established wired communication. However, different wireless technologies have different characteristics such as varied data rates, latency, availability, complexity, security standards etc. On the other hand, there are specific requirements attached to different WAMS level applications. Therefore appropriate wireless technologies must be used with knowledge of their capabilities and weaknesses in all levels of WAMS.

The paper established a systematic approach to select wireless communication technologies for varying levels of WAMS in smart grid by studying the communication requirements in the

grid for both monitoring and control purposes. These requirements are then compared with the performance of various available wireless technologies to evaluate the suitability of the suggested technology. The paper also discussed the challenges with deployment of wireless communication in WAMS and opportunities posed by them. By addressing the key aspects related to wireless technology adoption in WAMS communication, this paper provides a contemporary look in the still not much explored research areas in Smart Grid Communication.

FUTURE WORK

The devised framework and study was primarily for transmission corridors of smart grid. The same framework can be applied to distribution automation with few changes as the communication requirements change at distribution level. The study considered few selected communication requirements and performance parameters to establish a systematic method to identify potential wireless communication technologies. The same study can be extended to include number of other requirements such as. cyber security and performance parameters such as reliability.

REFERENCES

[1]. P. P. Parikh, M. G. Kanabar, T. S. Sidhu, ”Opportunities and challenges of wireless communication technologies for smart grid applications”, *IEEE Power and Energy Society General Meeting,* 2010, 1-7.

[2]. Y Pi, Y Zhang, X Wang et al., ”A cyber-physical system framework for smart grid wireless communications[C]”, *ICT Convergence (ICTC) 2013 International Conference on,* 2013, 179-184.

[3]. G. Sebaali, B. L. Evans, ”Design tradeoffs in joint powerline and wireless transmission for smart grid communications”, *Proc. Int. Symp. Power Line Commun. Appl.,* 2015, 83-88.

[4]. Mulla, A.; Baviskar, S.; Khare, N.; Kazi, F. ”The Wireless Technologies for Smart Grid Communication: A Review” *In proceedings of IEEE International Conference on Communication Systems and Network Technologies (CSNT),* Gwalior, 2015, 442-447.

[5]. A.G.Phadke, J.S. Thorp, Synchronized Phasor Measurements and Their Applications, New York: Springer, 2008.

[6]. *Electricity sector in India*, https://en.wikipedia.org/wiki/Electricity sector in India.

[7]. V. K. Agrawal and P. K. Agarwal, *Challenges faced and Lessons Learnt in Implementation of First Synchrophasor Project in the Northern India*, http://www.nrldc.org/docs/documents/Papers/Challenges Final AsSubmitted.pdf

[8]. *Technical Specifications for WAMS Packages-I & II of "Unified Real Time Dynamic State Measurement (URTDSM)" Project*, Vol.II, Part-B, Appendix - A.

[9]. Rahul Gore, Simi P. Valsan, ”Big Data challenges in smart Grid IoT (WAMS) deployment,” *8th International Conference on Communication Systems and Networks (COMSNETS),*, Bangalore, 5-10 2016.

[10]. Prashant Kansal, Anjan Bose, ”Bandwidth and Latency Requirements for Smart Transmission Grid Applications,” *IEEE Transactions On Smart Grid*, 3(3), 2012.

[11]. Stefan Svensson, ”Challenges of Wireless Communication in Industrial Systems”, Keynote, *SIES 2011 - 6th IEEE International Symposium on Industrial Embedded Systems, Conference Proceedings,* Vasteras, Sweden, 15-17, 2011.

[12]. H. Lim and C. Kim, “Multicast tree construction and flooding in wireless ad hoc networks,” in Proceedings of the 3rd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems. ACM, 2000, 61–68.

[13]. S. Ramanathan, “Multicast tree generation in networks with asymmetric links,” IEEE/ACM transactions on Networking, 4(4), 1996, 558– 568.

[14]. G. N. Rouskas and I. Baldine, “Multicast routing with end-to-end delay and delay variation constraints,” IEEE Journal on Selected Areas in communications, 15(3), 1997, 346–356.

[15]. Q. Zhu, M. Parsa, and J. Garcia-Luna-Aceves, “A source-based algorithm for delay-constrained minimum-cost multicasting,” in INFOCOM’ 95. Fourteenth Annual Joint Conference of the IEEE

Computer and Communications Societies. Bringing Information to People. Proceedings. IEEE, 1, 1995, 377–385.

[16]. H. F. Salama, D. S. Reeves, and Y. Viniotis, "Evaluation of multicast routing algorithms for real-time communication on high-speed networks," IEEE Journal on Selected Areas in Communications, 15(3), 1997, 332–345.

[17]. H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," IEEE Journal on Selected Areas in Communications, 30(6), 2012, 1097–1107,

[18]. Q. Zhu, D. Wei, and T. Basar, "Secure routing in smart grids," in Workshop on Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS), 2011, 55–59.

[19]. R. Hou, C. Wang, Q. Zhu, and J. Li, "Interference-aware qos multicast routing for smart grid," Ad Hoc Networks, 22, 2014, 13–26.

[20]. J. Wei and D. Kundur, "Goalie: goal-seeking obstacle and collision evasion for resilient multicast routing in smart grid," IEEE Transactions on Smart Grid, 7(2), 2016, 567–579.

[21]. M. Chenine and L. Nordstr¨om, "Investigation of communication delays and data incompleteness in multi-pmu wide area monitoring and control systems," in Electric Power and Energy Conversion Systems, 2009. EPECS'09. International Conference on. IEEE, 2009, 1–6.

[22]. M. Chenine and L. Nordstrom, "Modeling and simulation of widearea communication for centralized pmu-based applications," IEEE Transactions on Power Delivery, 26(3), 2011, 1372–1380.

[23]. S. Wang, W. Gao, J. Wang, and J. Lin, "Synchronized sampling technology-based compensation for network effects in wams communication communication," IEEE Transactions on Smart Grid, 3(2), 2012, 837–845.