OPAL-RT TECHNOLOGIES

Success Story

IOWA STATE UNIVERSITY

Cybersecurity/AI, & its Use in Grid Protection/Control, with Vivek-Kumar Singh, PhD Candidate, Iowa State University

Vivek-Kumar Singh is a PhD candidate at Iowa State University in the laboratory of Dr. Manimaran Govindarasu and a researcher on Cybersecurity/AI implementations on smart grids. He has two academic publications on the topics of AI/machine learning and power grid cybersecurity/protection and control:

V. K. Singh, M. Govindarasu, “Decision Tree Based Anomaly Detection for Remedial Action Scheme in Smart Grid using PMU Data,” IEEE Power and Energy Society 2018 General Meeting, August 5-9, 2018, Portland, Oregon, USA, 2018.

V. K. Singh, A. Ozen and M. Govindarasu, "A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid," 2018 Resilience Week (RWS), Denver, CO, 2018, pp. 63-69.

We recently sat down to speak with Mr. Singh to share some insights and perspectives, and to find out more about how OPAL-RT’s hardware platforms, communication protocols, and various solvers are instrumental to his research, which he uses in surprising ways for developing ground-breaking methodologies and research.

1. Introduction

Mr. Vivek-Kumar Singh's academic history originated in India, where, as an undergraduate student, he had already heard of the OPAL-RT brand of electrical/engineering real-time simulators. After finishing his undergraduate degree, he received a PhD offer at Iowa State University. His professor, Manimaran Govindarasu, was already working in cybersecurity for smart grids—and was eminent in the field. Dr. Govindarasu introduced Mr. Singh to this field, and it turned out that his lab had recently bought an OPAL-RT real-time simulation platform composed of hardware, software and toolbox (ePHASORSIM)--and were wondering what would be the next step with this new acquisition.

"Everyone who's doing or has done any sort of simulation in power systems and power electronics knows at the very least the name 'OPAL-RT'. I had heard about the simulator back in India when I was working as a project assistant at the Indian Institute of Technology, Delhi (IITD)," said Mr. Singh.

This all took place in the context of the Ukraine, in June 2017, where the citizenry had recently sustained serious cyberattacks. Mr. Singh attended summer courses and started attending conferences, which provided him strong motivation to join his Professor and to work in this field. Additionally, he started seeing ways to use Artificial Intelligence (AI) and machine learning to engage with this sort of problem, especially in power systems.

Mr. Singh found himself highly motivated by this kind of problem-solving thinking, in the case of cybersecurity for power grids, for example—and found that he liked being involved in solving real-world problems. So he and Dr. Govindarasu started exploring the outer limits of what they could do with the OPAL-RT real-time simulator—which turned out to be a great deal, because it had everything they needed to understand the attack surfaces in power systems by capturing their dynamic behavior.

2. Challenges

At this stage, Dr. Govindarasu and Mr. Singh still weren't sure how to use their OPAL-RT real-time simulator. The kind of really detailed, applied study they were conceiving of takes a lot of research and some really well-thought-out questions and areas of focus. Then, once researchers know their focus and methodology, they are able to get a much clearer idea on how to use the simulator to get the results they want.

Thus before they even started, they did a thorough survey of the extant academic literature, to find out what the areas of interest were and what had already been done. While getting into details, Mr. Singh learned that there was a field of study called Wide Area Monitoring, Protection & Control (WAMPAC), and he discovered that this area, specifically in the cybersecurity context, was a very current topic.

So he started doing power system modelling in OPAL-RT, and incidentally had the chance to interact with OPAL-RT's superb Customer Support Team:

"Your technical support organization is amazing. I must tell you, the Customer Support at OPAL-RT, they are really great! Every time I called them, they were always there. These guys were always helping me out, even in fixing minor issues," said Mr. Singh.

As Mr. Singh assembled his research experiment, he ran into several notable and significant challenges. Artificial Intelligence (AI) or machine learning referred, in his case, to training the machine learning model the difference between a normal controller command and a malicious attack. In order to teach the machines through example, they required a huge data-set to enable the machines to read and interpret the difference.

This was one of their biggest challenges to start with-- if one is working in machine vision, there are open source libraries of literally millions of images one can use. However, in their field, Singh and Govindarasu faced two

problems: First, the machines they were trying to teach are sometimes attached to private companies or institutions, and thus proprietary information, and there's little motivation for these companies to reveal to users either the security strengths or vulnerabilities of their hardware and software, and ii) there is no openly available source of this kind of information—large cybersecurity datasets--for cyberattack and security reasons. And this kind of machine teaching/learning requires large amounts of datasets or training materials.

3. Solution

"The generation of the datasets was one of the places where OPAL-RT saved our lives," said Mr. Singh.

"We did a sort of fault injection in the simulator; we mimicked or 'staged' all types of attacks and observed the system dynamics, and we collected the data from the system dynamics. So through this process, we were able to generate our own good and bad teaching datasets. Then this data was used to train the machines by example, and then, in turn, to teach the machines to monitor for good and bad signals in real time."

Ingeniously, they had generated their own AI learning libraries of both good and malicious examples! Without question, Singh and Govindarasu had reverse-engineered a required element for their study in an unexpected way. They grew to appreciate the flexibility and many options of the OPAL-RT simulators. For

example, they could connect physical relays and PMUs (synchrophasors) if desired, and do Hardware in the Loop (HIL) testing. When they implemented the staged 'cyberattacks' in a realistic way for the teaching/learning datasets, they could inject dynamics into the system—a sort of fault injection--which could then be recorded again and played back for reference. From the perspective of a relay and PMU, they don't know if this is a cyber attack or normal operation since they are embedded devices, so their dataset-generation methodology was near-identical to collecting and observing real-world behaviors. It may have been SCADA or synchrophasor data, but then they got to use these good and bad sources for training and testing their applied machine learnng methodologies.

In terms of the communications system network, they didn't resort to a communications system emulator. OPAL-RT provides an extensive list of communications protocol supports. Various types of communications exist, for example, if they were using SCADA, OPAL-RT simulators had the GOOSE (IEC 61850) support for relays. For DNP3, there were OPC drivers that facilate DNP3 master-slave configuration. To allow synchrophasor communications, there are PMU communications as well. This is another facet of the OPAL-RT simulator that made it invaluable for Singh and Govindarasu--they had the whole toolset of communications in one place--that allowed them to perform wide-area monitoring, protection, and control.

Singh reflects on how much he has come to enjoy making discoveries in his milieu, and enjoys working with the OPAL-RT simulators:

"Well, I've got a year left at Iowa State on my PhD, and then I am looking for possible opportunities to continue working in the field, may be at the research Labs like INL, PNNL or NREL, and doing the same level of work, keeping on using OPAL-RT simulators, in all likelihood!"

4. Results

So how did Singh and Govindarasu feel, finally, that the fruits of their research could be deployed on power systems—specifically AI and cyber-physical systems simulation?

There's always a way in industry or utility that this knowledge can be put into action. They're currently also working with the US Army Research Laboratory in Maryland. At this stage, they're connecting two OPAL-RT simulators remotely—one in Iowa and another one in Maryland, where one is working as the control center gathering data and the other is simulating multiple substations for the IEEE 39 bus system. They are developing a cyber federation based testbed with the aim of understanding the real-time, real-world latency (the communications delay--which is about 26.7 milli-seconds for synchrophasor data packets), and testing their machine learning based algorithm for bad signal detection with that latency. The entire networks are complex to the nth degree, and they're modeling a lot in the OPAL-RT simulators at a reduced scale.

"We're getting to the place where we can propose a valid solution to people," Singh says, "and we can tell them there's little latency, there's no packets lost—and this is exciting for us in terms of industry as well. People are happy to deploy under these circumstances commercially."

They are also involved in providing SCADA-oriented cyber security training at utilities and industries like Cedar Falls Utilities (CFU), Central Iowa Power Cooperative (CIPCO), MidAmerican Energy, Idaho Power Company, and Corn Belt Power Cooperative (CBPC) in order to better understand some industry concerns. Their next stage training is to use OPAL-RT simulators to provide cyber physical training where they can model big, complex grid topologies in a hardware-in-the-loop context, with possible attack surfaces.

While focusing on research, their next stage of work is doing research into cyberphysical networks, again using OPAL-RT simulators. They are looking at releasing some of their developing datasets which capture attack signatures, like PMU information, to help other people do research with the datasets that they had such a hard time finding—but nothing proprietary or potentially damaging from the datasets related to hardware devices can be released for obvious reasons.

This has exciting implications for advancing the Wide Area Protection and Control field; and OPAL-RT would like to thank Singh and Govindarasu for speaking with us.

Interviewee Biography: Vivek-Kumar Singh

Vivek Kumar Singh received a B.Eng. in electrical engineering from the National Institute of Technology Durgapur, West Bengal, India. He is a Ph.D. candidate with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA, USA. He has received a Journeymen Fellowship award at US Army National Research Laboratory, MD, USA. His research interests are in the areas of cyber physical systems, cyber security, smart grids, machine learning, data mining and artificial intelligence.

About OPAL-RT TECHNOLOGIES

OPAL-RT is the world leader in the development of PC/FPGA Based Real-Time Digital Simulator, Hardware-In-the-Loop (HIL) testing equipment and Rapid Control Prototyping (RCP) systems to design, test and optimize control and protection systems used in power grids, power electronics, motor drives, automotive industry, trains, aircrafts and various industries, as well as R&D centers and universities

1751 Richardson, Suite 2525, Montreal, Quebec, Canada H3K 1G6| Tel.: +1 514-935-2323 | www.opal-rt.com