Cybersecurity Analysis of an IEEE 802.15.4 Based Wireless Sensor Network for Smart Grid Power Monitoring on a Naval Vessel

Xaime Rivas Rey, Thomas J. Halpin, Shantanu Hadgekar, Karen Miu, Kapil R. Dandekar

Abstract

Most sensor networks on a naval vessel are wired directly to the control unit,[1, 16] and this includes the Power System. This paper demonstrates how an IEEE 802.15.4 based Wireless Sensor Network (WSN) could be used to have an easy to deploy, flexible and affordable Smart Grid Power System monitoring structure. In published literature, it has been qualitatively proven that a WSN can work on a ship, despite its more complex Radio Frequency (RF) environment. This work quantifies this, showing the achievable levels of Packet Error Rate under different levels of Signal to Interference and Noise Ratio, proving that it could be used instead of a wired channel. Another important aspect studied was the cybersecurity implications of using a wireless network versus a wired one. The effects of delayed, missing and faked power measurements were also studied, along with a discussion of what could be done to detect and mitigate them.

KEYWORDS: Wireless Sensor Network: IEEE 802.15.4; Wireless Cybersecurity; Ship; Power Smart Grid; Data monitoring

Introduction

The ability to actively monitor a power system using a supervisory control and data acquisition (SCADA) system along with state estimation is important in understanding power system performance and available capabilities.[5] Currently, most sensor networks on naval vessels are wired. In this work, we study the impact of using wireless sensors to reduce the cost and installation complexity of the smart grid power monitoring system while guaranteeing that the overall state estimation of the system is accurate. In addition to cost, Wireless Sensor Networks (WSN) provide other advantages over their wired counterparts such as adaptability, redundancy, and weight savings.[2] Even though not all wired communications can be replaced, since some wired networking is always needed to communicate data throughout the whole ship, the advantages of a wireless system are abundant. There is existing work, studying the feasibility of Wireless Sensor Networks on ships.[1] However, there is very little work connecting this wireless feasibility with the cybersecurity aspects associated with using such a network for smart grid power monitoring on a naval vessel. For example, understanding how delayed or corrupted measurements from the power system can impact a state estimator or prevent it from properly observing the system is important, particularly when operating near the end of a stable operating region. Various methods exist in state estimation to help determine bad measurements and nodes in the event of an attack, but understanding the impact of various attacks is important with respect to power system operation.[6-9] These state estimation methods often do not consider the wireless and cybersecurity issues that we consider in this paper.

IEEE 802.15.4 defines the operation of Low-Rate Wireless Personal Area Networks (LR-WPANs). It describes the Physical and Media Access Control (MAC) for LR-WPANs and it is one of the most popular options for Wireless Sensor Networks.[13]

In summary, this paper presents a novel Wireless Sensor Network for naval vessels based on the IEEE 802.15.4 standard

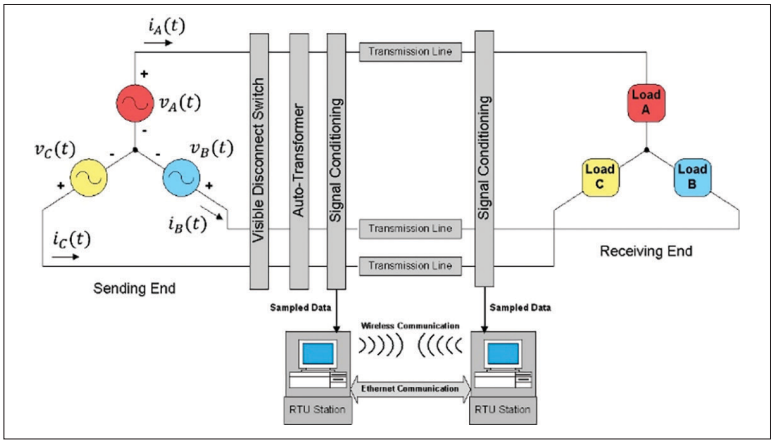

FIGURE 1. 3-Phase Power System

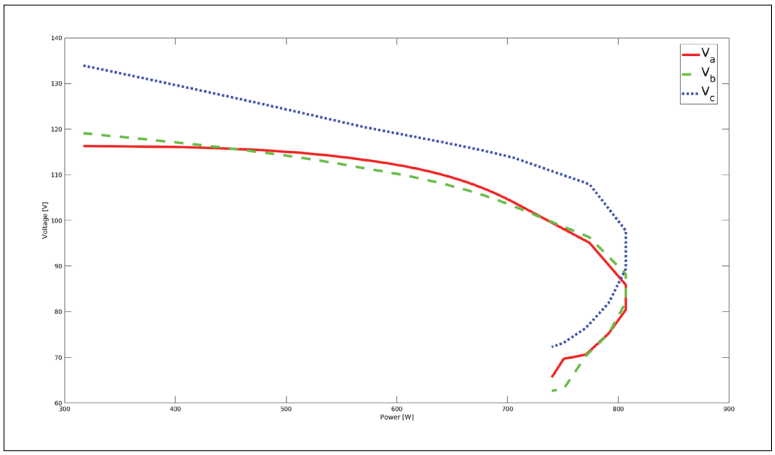

FIGURE 2. Power - Voltage curve for all phases.

for monitoring smart grid power systems under different levels of cyber-attack. Specifically, in our testbed driven approach, we leverage experimental data from both a power systems laboratory, and experimental wireless communications testbed, to consider the transmission, and potential corruption of smart grid monitoring data. We consider how this corrupted data can impact smart grid state estimation algorithms under various cybersecurity-related scenarios involving either defective or malicious nodes in the network.

Power System and Measurement Collection

To represent smart grid data on a naval vessel, data from a power system was collected using the Interconnected Power System Laboratory (IPSL) at Drexel University. The setup included a 3-Phase Power source, transmission lines, and a 3-Phase load as shown in Figure 1. Measurements were taken using signal conditioning boards connected to Remote Terminal Units (RTU) at different load levels to create a Power-Voltage curve of the system.[11]

Voltage and Current phasor measurements were taken at each load level, and used to create Power-Voltage curves. The individual measurements were then transmitted through a wireless network, subjected to different transmission scenarios as discussed in the Description of experiments section. Figure 2 shows the Power-Voltage curve for each one of the phases when the data is not jammed or modified:

Experimental setup

This experimental work sets the ground for a Wireless Sensor Network using IEEE 802.15.4 as the Physical and MAC foundation for a custom based communication protocol. There are multiple network topologies that could be used. However, due to the nature of the ship's geometry, the proposed topologies are two:[13]

- **Tree topology**: as shown on Figure 3, the network consists of a central node that acts as a coordinator at the root of the tree. This node is the monitoring unit for the power system. Connected to the root, we can have both end nodes and routers. The end nodes would be each of the sensors that measure the power levels on the smart grid. The routers collect data from either multiple sensors or other lower tier routers. All data flows from the bottom of the tree towards the coordinator of the network, which processes the data and predicts the state of the power system. The only disadvantage of this method is that there is no interconnection of devices in the same level of the tree, so if an upper level node is disconnected, everything below that node will disappear from the network.
- **Mesh topology**: as shown on Figure 4, the network consists of a central node that acts as a coordinator, routers and end nodes. The devices present in this topology are the same as in the previously shown tree structure, however the main difference is that routers are interconnected among themselves. This allows the network to send the data to the coordinator even if some routing nodes are damaged/disconnected. The drawback is that there is more data overhead, since more routing options are available and routing the data gets more complex.

Both topologies could be implemented with the same number of nodes. The trade-off between both options is the simplicity of the routing algorithm versus available routes for the

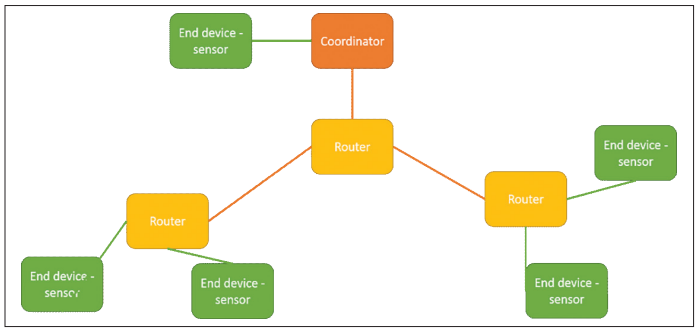

FIGURE 3. Example of a tree topology.

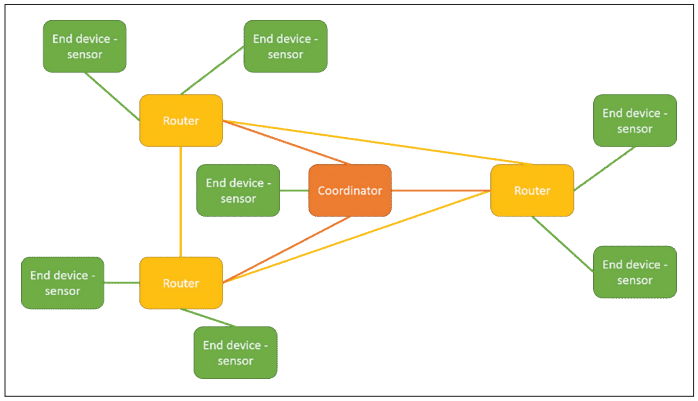

FIGURE 4. Example of a Mesh topology.

data to reach the coordinator. Since the ideal scenario is that the monitoring system gets data even if one or multiple nodes are damaged or compromised, the mesh topology is preferable to the tree topology.

A subset of the network was evaluated using an experimental approach based on software defined radio (SDR). The study was performed on a node to node link. This could represent a sensor—router link, a sensor—coordinator link or a router—coordinator link. Using the results obtained from this analysis of a wireless link between two nodes, one can gain some intuition regarding the behavior of the whole network and simulate it to predict its performance.

For the experiments in this work, three radios were used. A transmitter acting as a data source, a receiver acting as either a router or a coordinator and a third node, that depending on the experiment being run, played a different role. All experiments were performed using SDRs, in particular NI-USRP N210. IEEE 802.15.4 offers a different set of frequencies where the devices can operate. The protocol used is described and implemented in [14].

The transmitter and receiver are separated *15 ft* horizontally, whereas the transmitter and the interference source, reactive jammer or malicious node, depending on the experiment being

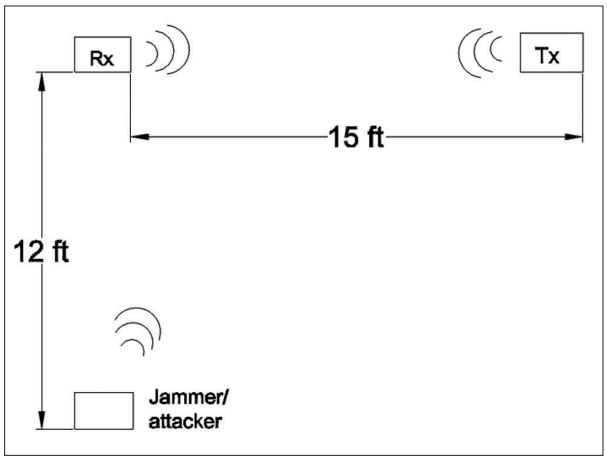

FIGURE 5. Experimental Setup of SDRs.

considered, are separated by *12 [ft]* vertically. Figure 5 and Figure 6 show the spatial arrangement of the radios.

Description of experiments

This section summarizes each one of the three different experiments that were run.

Experiment 1—Packet Error Rate vs SINR

For the first experiment, a set number of packets is sent through the wireless link. For different values of Signal to Interference and Noise Ratio (SINR) the Packet Error Rate (PER) or percentage of successfully received packets, is computed:

$$SINR_{dB} = 10\log_{10}\frac{P_s}{I+N} \quad (1)$$

Where P_s is the Power of the signal being received, I represents the interference level and N the noise level in [W].

$$PER = 100\frac{N_{Tx} - N_{Rx}}{N_{Tx}} \quad (2)$$

Where N_{Rx} is the total number of received packets and N_{Tx} is the number of transmitted packets.

Each scenario was run a total number of 5 times, and for each run, a total of 1000 data packets were sent. The amount of successfully received packets was post-processed and the PER computed. Table 1 summarizes the obtained results.

Experiment 2—Reactive Jammer detection

When estimating the state at which the power system is in, it is key that we have a consistent stream of data. This experiment

FIGURE 6. SDR Testbed.

emulates a scenario where even though the SINR levels perceived by the receiver are at acceptable levels, the Packet Error Rate is higher than one would expect. There are multiple situations that could lead to such a scenario:

1. **Short-term path obstruction**: due to the nature of the ship and its metallic structure, we could have a wireless sensor in an isolated area, with a non-ideal connection to the receiver. If a big enough obstacle is placed between both transmitter and receiver there would be periods of time where the data from that wireless sensor would not be accessible. A metallic door being closed in between the wireless path connecting receiver and transmitter is a good example of how this could happen.[19]
2. **Reactive jammer**: a malicious node could be trying to prevent the data to get to the receiver by sending a short duration but high-power signal right when the transmitter is trying to send data.[4]

If faced against situation 1, there are multiple solutions. One option could be to move the wireless sensor closer to the receiver or if that is not an option due to the nature of the measurement that is being performed, say for example the angular speed of an electric motor, we could try to move the receiver closer to the sensor. The worst-case scenario solution would be to use a wired connection.

The scenario that has been simulated in this experiment was done using the third node as a jammer. The jammer would send short-duration high-powered signals, thus making it impossible for the receiver to successfully process all data points. In order to detect such a scenario, the concept of Time Between Consecutive Receptions (TBCR) is introduced. Due the nature of the challenge of power system state estimation, power measurements need to be sent periodically. Knowing this need, one can monitor that the time between consecutive receptions is indeed periodic and consistent with the rate at which the measurements are being sent by the transmitter. If the receiver has a PER above a certain threshold, compromising the state prediction of the power system, it should perform spectrum sensing and try to see if there are any unusual signals, by knowing when the transmitter is sending data it could also compute the SINR. Detection of a reactive jammer by simple spectrum analysis is difficult. If nothing is detected, yet the PER is high, the TBCR should be studied. If there is indeed a reactive jammer, we could see that some data is not going through in a consistent manner. To avoid this situation, IEEE 802.15.4 provides a channel hopping strategy, this could help the radios get away from the jammer.[10]

Experiment 3—Unreliable data

The last experiment that was carried out studies the effect of modified data when trying to estimate the state of the power system and also what the P - |V| data would look like if created using modified data. There are different scenarios where this could happen:

1. **Damaged sensor**: if one of the power sensors is damaged, its readings won't be reliable. If data from these sensors is used to estimate the state of the power system, it would lead to a wrong state prediction.
2. **Malicious node**: one or more nodes could be hacked, or replaced by a custom radio that is able to mimic the original sensor's behavior and disrupt the overlying power system through knowledge of how the devices are being used.

We will primarily focus on the second scenario. Measurement data packets will be modified and sent to appear as real measurements, but include falsified data that will give the false impression that the power system is reaching an unstable area (see Figure 7). To combat this cyber-attack on the state estimation side, detection methods exist that allow for bad measurements, whether being a bad sensor or maliciously

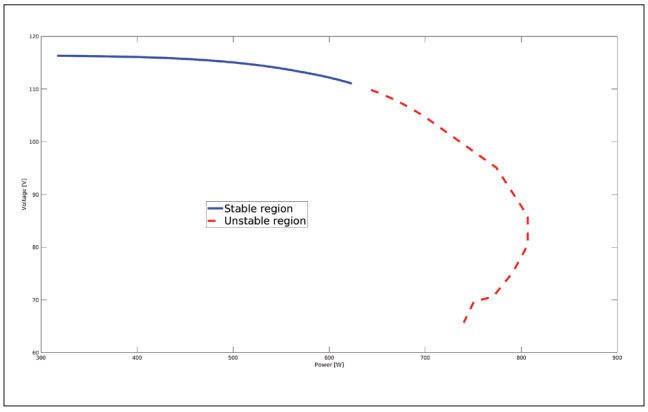

FIGURE 7. Stability region of the P - |V| curve

modified data, to be detected and ignored from the final estimation.[7-8] Although state estimation cannot determine the kind of scenario that might exist—whether it is modified data or a bad measurement node, it can still account for these measurements, and attempt to estimate the state of the power system without it.

Experimental Results

This section summarizes the results obtained for the previously described experiments. To avoid interference from 802.11 signals, the center frequency used was 1.68 [*GHz*]. Along with the results, a discussion is done and solutions are proposed for each scenario. For experiments 2 and 3, the proposed solutions come from both the power system point of view as well as from the perspective of wireless networks.

Experiment 1—Packet Error Rate vs SINR

SINR [dB]	PER [%]
1	100.00
2	95.50
5	80.20
7	51.80
10	0.01

TABLE 1. PER vs SINR

As expected, the trend is that as SINR increases, the number of packets that are successfully received does too, and the Packet Error Rate decreases. These results are consistent with published literature, validating our testbed.[15] We can see that if the SINR is above *10 [dB]*, the packet rate is almost 0 %. These results confirm that IEEE 802.15.4 is a great candidate for a Wireless Sensor Network on a naval environment, where due to the high multipath components and metallic elements the SINR levels will be low.

Experiment 2—Reactive Jammer detection

In this case, since some measurements are not delivered to the estimator, they cannot be used when the state estimation is attempted. For the power system used here, the state can still be determined by using the source measurements and known transmission line parameters, but if those are not available, the state cannot be observed at that moment in time. In the case of a naval vessel, losing information from a small subset of sensors could be acceptable for a short period of time since the total number of sensors is in the order of thousands.[1,3]

If the state cannot be observed, then operators may not know the real-time conditions of the system, and will have to make decisions based off older data. It is important that there is a redundancy in case of jamming, so operators can still make appropriate decisions. If there are more states to be estimated than measurements available, the system cannot be properly estimated. To combat this, it is important to have enough wired sensors to allow for the system state to be observable without the wireless measurements in the case of wireless jamming. This allows for the system state to still be estimated, although the estimate may not be as accurate.

The following figure shows what the TBCR looks like for a legitimate communication in the absence of a jammer and what it would look like if a periodic jammer where to be present:

If a periodic jammer is transmitting, there are spikes on the Time Between Consecutive Receptions, when they should be periodic within a margin. Thus, the TBCR offers a simple yet effective way of detecting a jammer.

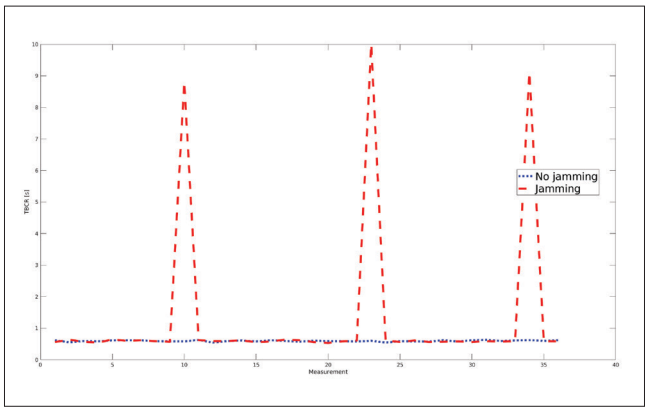

FIGURE 8. TBCR in the absence of a jammer (blue) and with a periodic jammer (red).

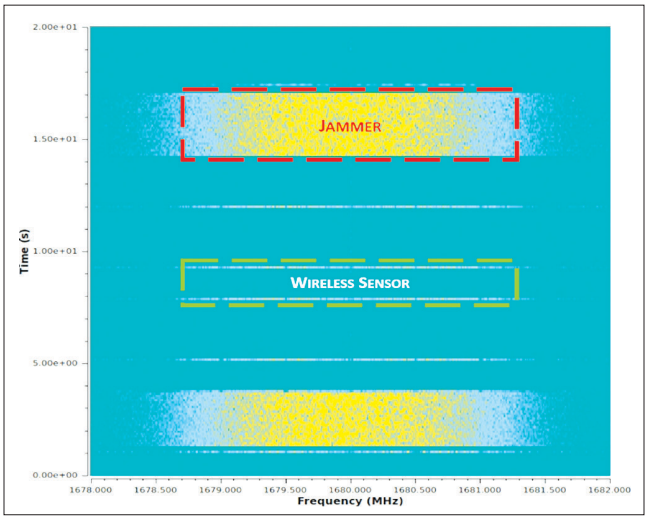

FIGURE 9. Spectrum waterfall plot for jammer experiment

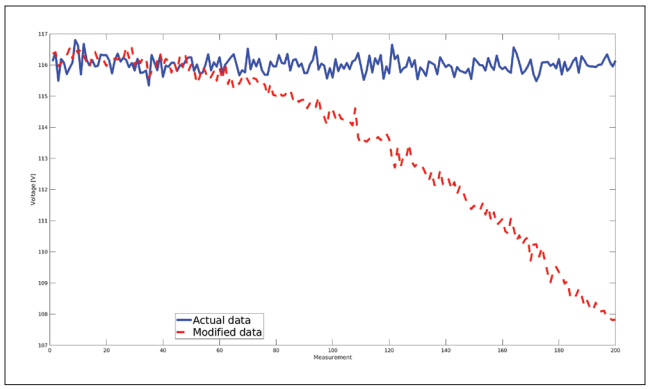

FIGURE 10. Voltage evolution (real-blue, transmitted-red)

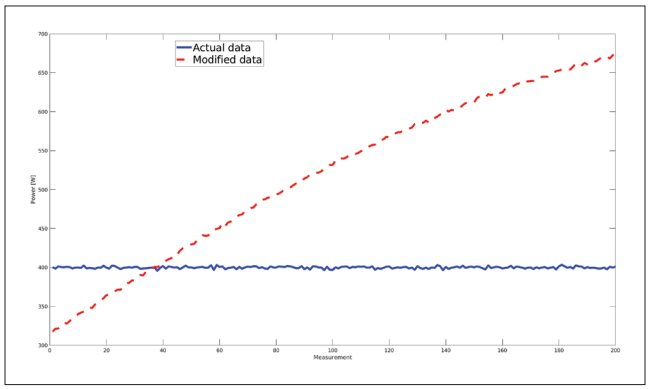

FIGURE 11. Power evolution (real-blue, transmitted-red)

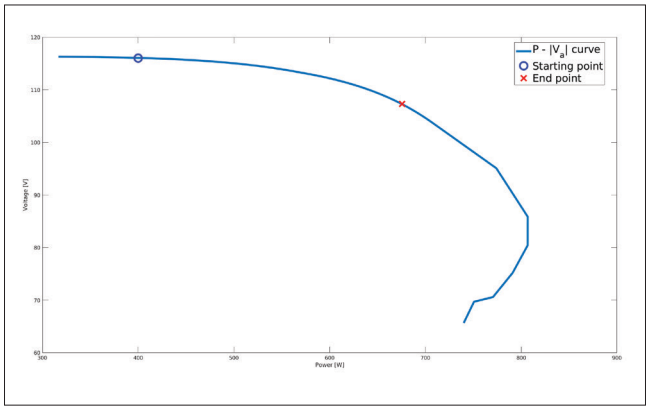

FIGURE 12. Received P - |V| curve for one phase.

From a wireless point of view, the options to combat this jammer are various:

- **Frequency hopping**: if the number of packets being dropped is above a certain threshold, both transmitter and receiver start transmitting on a different channel. This should be done until they both see each other in the same channel and the number of packets being dropped decreases to acceptable levels. The method presented in [17,18] is a good example of this approach. Detection of the hopping pattern would presumably be difficult by a malicious node.
- **Rendezvous channel**: if the communication channel is being jammed, the radios go to a set center frequency, sense the whole spectrum for a while and exchange that information. The idea here is to reach an agreement regarding available channels and which one to use. This approach would not be effective against an adaptive reactive jammer.

Experiment 3—Unreliable data

For this experiment, the system is working in the stable region. However, the data being transmitted has been modified, simulating what an attacker could do in order to prevent the state estimation from being accurate. The following plots show the state at which the system actually is and what the wireless sensor is actually transmitting.

Placing this on the measured P - |V| curve for one of the phases, it can be inferred that the system is moving towards the unstable area:

When an attacker attempts to make the power system appear in a state that it actually is not in, the decisions, if any, made to keep the system within the parameters based on the operator's observations can be impacted. For example, if the attacker makes a system performing normally and within parameters appear like it is collapsing, as seen in Figure 11, the operator may take control actions based off the false appearance of the system to try and prevent the collapse. In reality, these control actions are unnecessary since the system is operating normally.

To successfully implement such a cyber-attack, an attacker may need to access multiple sensors and modify enough critical measurements, as discussed in [9], to make the estimate wrong. This can result in the bad data detection methods to mistake the good measurements as bad.

To combat this attack, a similar method to the one presented for Experiment 2 can be used, where enough wired measurements can be installed to allow the system to remain observable, and reduce the impact of maliciously modified measurements. Although there will still exist some vulnerabilities, the redundancy allows for multiple means of acquiring data in the case of an attack.

When trying to identify and ignore individual malicious nodes, bad data analysis can be used to detect and ignore these. As shown in [7,8], one can ignore measurements that do not align with the estimated system state based on the residuals between measurements and the estimated state. This can be used to determine nodes sending bad data.

By giving each measurement an error range, and using the given measurements and known system parameters, the unknown measurements can be estimated. Using the same estimation, the actual measurements can be compared to what the estimator calculates those values to be. The residuals can be determined from that, and the measurements with high residuals can be ignored to help improve the state. With this method, malicious measurements can be detected and ignored in individual cases. The state can then be re-estimated using the ignored data, in attempt to get a better estimation.

By using a combination of a hybrid network and bad data detection, the malicious measurements can be identified and ignored.

Future work

A single wireless link has been tested under different scenarios. What happens in the presence of a jammer or if data is manipulated has been studied. The next step would be to, using this single link knowledge, simulate a bigger and more representative network and try to detect, as presented in [6,9] malicious or missing data and still successfully estimate the state of the Power System.

The same experiments could be carried out on a channel emulator, where the actual multipath channel from a ship could be simulated. This would allow for a more accurate PER vs SINR curve.

Conclusion

This paper has shown that an IEEE 802.15.4 based Wireless Sensor Network can be successfully implemented for monitoring a Smart Grid Power System on a Naval vessel.

First, the Packet Error Rate was computed for different levels of SINR, showing promising results consistent with up-to date literature. Secondly, a cybersecurity analysis from both a power point of view and a wireless point of view was made. A discussion on how to deal with missing data in the presence of a wireless jammer was done. From a power point of view, to prevent missing wireless measurements from doing a proper state estimation of the power system, it was determined that some strategic sensors should also be wired, providing some redundancy and helping the system not only to deal with missing data. From a wireless point of view, in order to deal with a jammer, different approaches were discussed.

Lastly, the third experiment shows what would happened if a node is compromised by an attacker, and started sending wrong readings trying to mislead the state estimator. The proposed solution for this also relies on having some redundancy of data by wiring some of the sensors. NEJ

Acknowledgements

This research was supported by the Department of the Navy Office of Naval Research (Proposal No. N00014-16-1-2037). This material is also based upon work supported by the National Science Foundation under Grant No. 1730140.

AUTHOR BIOGRAPHIES

XAIME RIVAS REY is the principal author and is currently pursuing a PhD in Electrical Engineering at Drexel University. His main interests are related to cognitive radios, artificial intelligence and deep reinforcement learning.

THOMAS J. HALPIN is currently pursuing a M.S. degree in the Department of Electrical and Computer engineering at Drexel University.

SHANTANU HADGEKAR got his M.S. in Electrical Engineering at Drexel University in 2018.

KAREN MIU, PHD is a Professor in the Department of Electrical and Computer Engineering. She obtained a PhD degree from Cornell University.

KAPIL R. DANDEKAR, PHD is a Professor in the Department of Electrical and Computer Engineering at Drexel University as well as Associate Dean for Research and Graduate Studies for the College of Engineering. He obtained a PhD degree from the University of Texas at Austin.

REFERENCES

[1] H. Kdouh, G. Zaharia, C. Brousseau, G. Grunfelder, H. Farhat and G. El Zein, "Wireless Sensor Network on board vessels", 2012 19th International Conference on Telecommunications (ICT), Jounieh, 2012, pp. 1-6. Doi: 10.1109/ICTEL.2012.6221242.

[2] Zacot, Chimi I. "Shipboard wireless sensor networks utilizing Zigbee technology". September 2006, Dissertation thesis.

[3] Swartz, R. A. et al. "Hybrid Wireless Hull Monitoring System for Naval Combat Vessels". Department of Civil and Environmental Engineering University of Michigan.

[4] Danh Nguyen, Cem Sahin et al. (2014). "A real-time and protocol-aware reactive jamming framework built on software-defined radios". Doi: 10.1145/2627788.2627798.

[5] A. Monticelli, "Electric power system state estimation," in *Proceedings of the IEEE*, vol. 88, no. 2, pp. 262-282, Feb. 2000.

[6] C. W. Ten, C. C. Liu and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," in *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[7] H. M. Merrill and F. C. Schweppe, "Bad Data Suppression in Power System Static State Estimation," in IEEE Transactions on Power Apparatus and Systems, vol. PAS-90, no. 6, pp. 2718-2725, Nov. 1971.

[8] F. F. Wu, W. H. E. Liu and S. M. Lun, "Observability analysis and bad data processing for state estimation with equality constraints," in IEEE Transactions on Power Systems, vol. 3, no. 2, pp. 541-548, May 1988.

[9] M. Göl and A. Abur, "Identifying vulnerabilities of state estimators against cyber-attacks," 2013 IEEE Grenoble Conference, Grenoble, 2013, pp. 1-4.

[10] IEEE Standards Association 802.15.4: Standard for information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks-- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs).

[11] C. Nwankpa, K. Miu, D. Niebur, Xiaoguang Yang and S. P. Carullo, "Power transmission and distribution system laboratories at Drexel University," IEEE Power Engineering Society General Meeting, 2005, 2005, pp. 1198-1205 Vol. 2.

[12] F. Wunsch, H. Jakel and F. K. Jondral, "Performance Evaluation of IEEE 802.15.4 OQPSK and CSS PHY in the Presence of Interference," 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, 2015, pp. 1-5. doi: 10.1109/VTCFall.2015.7391078

[13] Kazem Sohraby et al. "Wireless Sensor Networks: Technology, Protocols, and Applications", published by John Wiley & Sons, Inc., Hoboken New Jersey, 2007.

[14] Bastian Bloessl et al. (2013). "A GNU Radio-based IEEE 802.15.4 Testbed".

[15] IEEE 802.19 Wireless Coexistence Working Group (WG)—"Coexistence analysis of IEEE Std 802.15.4 with other IEEE standards and proposed standards".

[16] J. P. Lynch and K. J. Loh, "A summary review of wireless sensors and sensor networks for structural health monitoring", The Shock and Vibration Digest, 38 (2), 2006, pp. 91-128.

[17] M. Rahmanil, "Frequency hopping in Cognitive Radio Networks: A survey," *2015 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, Orlando, FL, 2015, pp. 1-6. doi: 10.1109/WiSEE.2015.7393102

[18] P. R and B. Amrutur, "Cognitive radio implementation for a frequency hopping primary signal," *2013 National Conference on Communications (NCC)*, New Delhi, India, 2013, pp. 1-5. doi: 10.1109/NCC.2013.6487929.

[19] M. Bielinski, K. Wanuga, G. Sosa, R. Primerano, M. Kam, and K. R. Dandekar, "Transceiver design for high data rate through-metal communication in naval applications," *Naval Engineers Journal*, vol. 125, no. 1, pp. 121–126, 2013.