Special Session: Noninvasive Sensor-Spoofing Attacks on Embedded and Cyber-Physical Systems

Anomadarshi Barua and Mohammad Abdullah Al Faruque
Department of Electrical Engineering and Computer Science
University of California, Irvine
{anomadab, alfaruqu}@uci.edu

***Abstract*—Recent decades have observed the proliferation of sensors in embedded and cyber-physical systems (ECPSs). Sensors are an essential part of embedded and CPSs and serve as a bridge between physical quantities and connected systems. The tight coupling between sensors and systems enables many critical applications where decisions are taken by using the information from various sensors at different time-scales. This tight coupling opens the "Pandora's Box" of unknown threats that could come from very unconventional ways. An unconventional attack model could be to noninvasively attack sensors using forged spoofing signals and trigger unwanted behavior in connected systems. This paper introduces this type of new, strong, and unorthodox attack model and elaborates how important this will be in the near future when sensors will pervade our lives. Moreover, this paper presents a motivational example of a sensor-spoofing attack on Hall sensors in the context of smart grids to demonstrate the harmful consequences of this type of attack in ECPSs.**

***Index Terms*—embedded and cyber-physical systems, noninvasive sensor-spoofing, Hall sensor, sensor-level defense, system-level defense**

I. Introduction

Sensors are one of the most sophisticated and integral components of ECPSs. However, from a security point of view, most of them are still unsafe and prone to intelligent attacks by a smart attacker. One type of unconventional attack could come by noninvasively attacking sensors using external spoofing signals. This paper explains different aspects of sensor-spoofing attacks on ECPSs with an appropriate demonstration.

Sensors observe environments and measure physical quantities, such as motion, ultrasound, acoustics, magnetic fields. The physical quantities are then converted into a usable signal (e.g., an electrical signal). We show a typical signal path from sensors to connected systems in Fig. 1. The converted electrical signal passes through a signal conditioning block to downstream of the signal path. The signal conditioning block consists of different types of filters and amplifiers to remove noises originating from environmental interferences. Next, this filtered signal is converted to digital format and fed into connected systems. Nowadays, connected systems deploy sophisticated hardware as the *system controller*, which reacts

This work was partially supported by the University of California, Office of the President under Grant No. LFR-18-548175, NSF under award ECCS-2028269 and CMMI-1739503, and the Broadcom Fellowship. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of funding agencies.

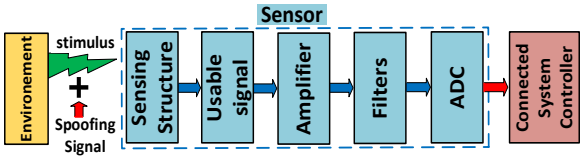

Fig. 1. A typical signal path from sensors to systems.

to sensor data in real-time. The underlying system controller inherently trust signals coming from sensors. As there is no hardware/software firewall present between the sensor and the system interface, this could be an entry point of an attacker. A smart attacker can *noninvasively* inject fake signals into sensors by using a suitable spoofing technique [1]–[3]. The injected fake signals can eventually propagate from sensors to the underlying system controller. As the underlying system controller cannot authenticate the truthfulness of received signals from sensors, the smart attacker can use this vulnerability to control the connected system by carefully injecting intelligent signals into sensors [4]–[8]. This could disrupt the normal behavior of the underlying hardware and result in adversarial control over the connected system [9]–[11]. This may compromise the system availability and integrity [12] and cause system failure resulting in denial-of-service (DoS) attacks on connected systems. All these moderate to severe consequences may happen just by spoofing a single sensor; therefore, this type of noninvasive sensor-spoofing attack is already a concern in the community. This paper deals with this type of new attack by first introducing a generalized attack model with a proper demonstration and provides research challenges along this direction.

II. Attack Model

To facilitate the understanding of sensor-spoofing attacks on ECPSs, the components of the sensor-spoofing attack model are introduced below (Fig. 2).

1) Physical attack: The attacker injects a seemingly legitimate but malicious stimulus signals into sensors. As the injected signal is an analog signal generated in the physical environment, the sensor-spoofing attack can be termed as a physical attack. This attack comes from a *physical domain* and impacts the *cyber domain* of the connected system [13].

2) Noninvasiveness of the attack: Though the attack is coming from the physical domain, the attacker is not allowed to invasively access and modify any hardware or firmware of

2576-6996/20/$31.00 ©2020 IEEE
DOI 10.1109/ICCD50377.2020.00024

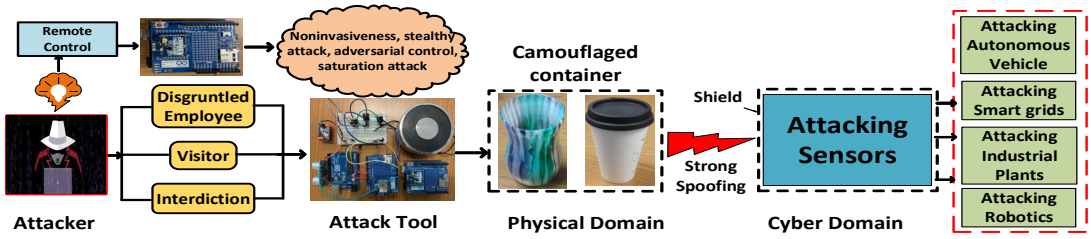

Fig. 2. A generalized attack model of the noninvasive sensor-spoofing attack.

the target sensor. The attacker could be a disgruntled employee [14], visitor or the attack could be an interdiction [15]. The attacker only uses a specific form of stimulus energy from a distance to inject malicious data into sensors. In this sense, the attack model is noninvasive, which makes it harder to be detected and contained.

Physical tampering with sensor hardware and software can be eliminated by using secured infrastructure and smart detection methods. Therefore, this type of physical invasive attack is not considered here. For example, a physical tempering with a Hall current sensor of the smart meter can be easily detected and eliminated by smartly placing extra sensors with the live and neutral wires inside of the smart meter [16].

3) Stealthy or non-stealthy attack: The attacker can attack the target sensor in a stealthy or non-stealthy manner. In a simple attack scenario, the attacker can leave his *attack tool* near the sensor to disrupt its normal operation. This type of simple attack is an example of a non-stealthy attack as the attack tool may be identified easily, and then can be removed from the attack-scene. In contrast, the attacker can camouflage the attack tool with a remote controller within a small container. This camouflaged attack tool is hard to detect. The attacker can remotely control the camouflaged attack tool and wisely choose the timing of the attack to remain unidentified and to maximize the impact. This makes the attack model strong and stealthy.

4) Adversarial control and the saturation attack: Broadly speaking, two types of attacks can be possible by sensor-spoofing, namely adversarial control and the saturation attack. Sensors, typically, have two operating regions [17]: (i) The linear region, where the input-output relationship of a sensor is linear, and (ii) The saturation region, where the input-output linear relationship of a sensor is diminished. The adversarial control typically occurs in the linear region of a sensor and hampers the system integrity. By injecting seemingly legitimate but malicious low power signals to sensors, the attacker can force the target sensor to work at a particular operating point in its linear region. In doing so, the attacker can control the operating point of the sensor and intentionally cause a false triggering in the connected actuation system. For example, an attacker can use an ultrasound signal to adversarially control the operating point of a gyroscope in its linear region and can intentionally move a mega-wheel scooter to the attacker's provided directions [10].

On the other hand, the attacker can inject a strong malicious signal to drive the sensor to its saturation region. We define this type of strong attack as the saturation attack. In the saturation region, the input-output linear relationship of sensors is subsided; as a result, sensors go completely blind to any variation of the input. This causes a failure in connected systems, compromises the system availability, and results in DoS attack on connected systems.

5) Types of the injected spoofing-signal: A strong attacker can inject distinct types of stimulus signals into sensors. In a simple attack model, the attacker can inject a constant stimulus signal into sensors. In a sophisticated attack model, a smart attacker could use a time-varying stimulus signal to modulate the original input signal being measured. For example, [11] shows that the original input signal to a Hall sensor can be intelligently modulated by injecting a sinusoidal and square magnetic pulses into a Hall sensor.

Moreover, a smart attacker can use a stimulus signal from different modalities to spoof a sensor operating in another modality. For example, typically, a MEMS microphone is sensitive to an acoustic signal. However, a smart attacker can use a stimulus other than acoustic, such as light to spoof the MEMS microphone from a long-distance [18].

6) Presence of a sensor shield: Depending on applications, sensors may or may not be placed inside of a shield. For example, a Hall proximity sensor in the antilock braking system is typically exposed to the outside world and is not placed inside of a shield. In contrast, a Hall sensor in a smart meter is typically located inside of a metallic shield. In this case, it is possible to generate a strong stimulus signal to penetrate the shield first and then spoof the target sensor [11].

III. A Case Study of Sensor-spoofing Attack on a Hall Sensor

A Hall sensor is used to sense the presence of magnetic fields and widely used in different ECPSs, such as industrial control systems (ICSs) [19], automotive systems [20], smart grids [21]. In this section, we give a motivational example of a noninvasive sensor-spoofing attack using a Hall sensor of a grid-tied solar inverter in the context of smart grids. Here, we use *inverter* interchangeably with *grid-tied solar inverter*. Grid-tied inverters are typically used as central inverters in solar/industrial plants or shopping malls. They widely use Hall effect current sensors instead of traditional sensors because Hall sensors have excellent accuracy, high bandwidth, high efficiency, and very good linearity. They are used in inverters to simultaneously measure AC/DC current, increase efficiency, reduce power loss, stop the injection of DC and circulating current into smart grids.

A. Hall effect current sensor basics

A Hall effect current sensor has a p-type semiconductor material, which generates an output voltage (V_{Hall}) proportional to input magnetic fields (B_{input}). The B_{input} is again proportional to the input current (I_{input}) being measured. So, the transfer function of a Hall effect current sensor is:

$$V_{Hall} = k \times B_{input} = K \times I_{input} \quad (1)$$

where K is the Hall coefficient. Eqn. 1 indicates that an attacker can perturb the original output voltage (V_{Hall}) by injecting a forged external magnetic field, B_f.

B. Spoofing attack on a Hall effect current sensor

The intention of attacking a Hall sensor of an inverter is to hamper the normal operation of the inverter. This will eventually cause grid instability and grid failures in a weak grid scenario [22]. The attacker can inject constant, sinusoidal, and pulsating magnetic fields into a Hall effect current sensor of an inverter by using an attack tool (approx. $50 of cost). The attack tool comprises an electromagnet, an Arduino, RF modules and battery packs (Fig. 3). A spoofing algorithm, running on the Arduino, intelligently controls the electromagnet to exert a strong magneto-motive force (MMF) towards the inverter. The exerted MMF should be strong enough to penetrate the inverter shield first and then impact the Hall sensor inside [11].

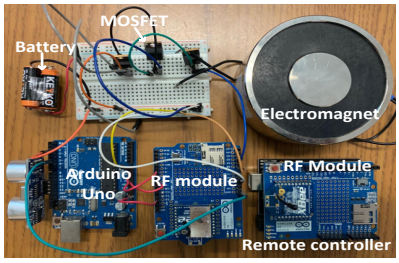

Fig. 3. Attacker's attack tool to spoof Hall sensors of an inverter.

The attacker could be a disgruntled employee or visitor and can camouflage the attack tool within a small container, such as flower vase, coffee cup. To place the camouflaged attack tool near the inverter, the attacker needs a brief one-time access near the inverter and it may not be difficult in an isolated solar plant. The attacker can remotely control the timing of the attack by using an RF module and can pick a vulnerable time (e.g., peak hour) to make the attack more severe.

C. Experimental Setup

A scaled-down version of a power grid is created as a testbed to demonstrate the spoofing attack on Hall sensors (Fig 4). A 140 Watt inverter from Texas Inst., which is a miniature version of a practical inverter, has Hall effect current sensors inside and is used in the testbed. The inverter is connected with an emulated weak grid, which is created by using another power inverter with a 300 Watt load. The attack tool is placed close to the inverter. Our attack tool can spoof Hall sensors from at most 10 cm distance. It is possible to spoof from 10+ cm distance by investing more money (>$50) on buying rare earth material to use as a magnetic core of the electromagnet.

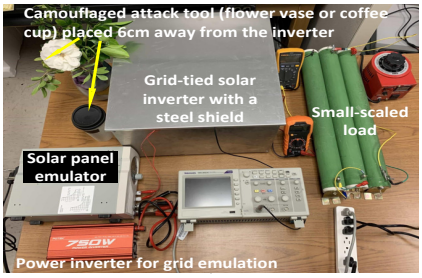

Fig. 4. A scaled-down testbed of a power grid.

D. Impacts of the spoofing attack

The injected forged magnetic field (B_f) propagates from the sensor hardware domain to the inverter controller. The reason behind this is that the low-pass filter and the DSP unit of the inverter cannot filter out the injected forged signal. This eventually changes the operating-point of the proportional-integral (PI) controller of the inverter. This change in operating-point drives the phase-locked loop (PLL) and space vector pulse width modulation (SVPWM) blocks of the inverter to an erroneous state. This results in a drastic change in inverter output voltage and frequency. Fig. 5 shows that an injection of constant magnetic fields into Hall effect current sensors adds a DC component to the inverter output voltage; whereas, an injection of sinusoidal magnetic fields adds harmonics to the inverter output voltage. Both results indicate that inverter voltage and frequency are severely distorted. This forces the inverter to shut down causing a DoS attack on our testbed.

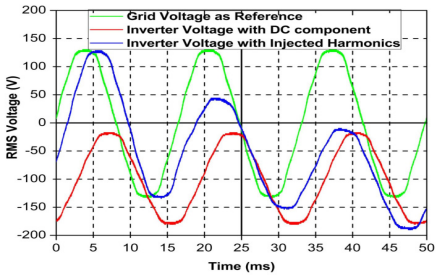

Fig. 5. Impacts of Hall sensor-spoofing on inverter output voltage.

IV. Research Challenges

Any defense methodology, which has an intention to work against a sensor-spoofing attack, must consider the components of the attack model explained in Section II. It has been always a challenging task to provide a defense that works against a strong, noninvasive, physical spoofing attack on sensors with adversarial control. There are few works in the literature that provide defense considering all the components of the attack model.

Any defense against the sensor-spoofing attack should fall either of the following two categories: sensor-level defense and system-level defense. Existing sensor-level defense methodologies [2], [4], [9], [23], [24] do not work against all the components (e.g., saturation attack) of the attack model. They work mostly against low power spoofing signals but fails against

strong malicious signals. On the other hand, existing system-level defense methodologies [25]–[28] are not suitable for low-power, hard real-time systems with constrained resources.

The next-generation defense method should not only detect the sensor-spoofing attack but also should contain the attack inside of sensors; so that the attack cannot propagate farther to connected systems. Sensors cannot remain naive anymore and they should be smarter while handling stimulus physical entities from environments. Novel hardware-software architecture should be introduced in the sensor-level design that may act as a *firewall* in the sensor-system interface. The time-sensitive components of the firewall should be implemented in FPGA to increase the processing efficiency and reduce the deterministic latency. In addition, the inclusion of parallelism using analog and digital domain in the sensor-level design could add a new dimension in the next-generation defense. This will help to keep the bandwidth, or other normal system performances intact. Moreover, the introduction of low-power, real-time, and unsupervised algorithms [29] in the system-level could add new values to tackle existing research challenges.

V. Conclusion

With the exponential growth of sensors in ECPSs, new security challenges have emerged. Various threats, vulnerabilities, and attacks may come just by attacking sensors using intelligent spoofing signals in the new generation of ECPSs. This paper introduces a generalized attack model on noninvasive sensor-spoofing with a proper demonstration and provides research challenges along this direction. Defenses against noninvasive sensor-spoofing attacks will be more critical in the near future when sensors will pervade our lives.

References

[1] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON*, vol. 24, no. 8, p. 109, 2016.

[2] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 103–117.

[3] Z. Wang *et al.*, "Sonic gun to smart devices: Your devices lose control under ultrasound/sound," *BlackHat USA*, 2017.

[4] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159.

[5] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2013, pp. 55–72.

[6] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, 2015, pp. 881–896.

[7] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, "This ain't your dose: Sensor spoofing attack on medical infusion pump," in *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016.

[8] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling UAVs with sensor input spoofing attacks," in *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016.

[9] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2017, pp. 3–18.

[10] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 1545–1562.

[11] A. Barua and M. A. Al Faruque, "Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 1273–1290. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/barua

[12] G. Wu *et al.*, "A survey on the security of cyber-physical systems," *Control Theory and Technology*, vol. 14, no. 1, pp. 2–10, 2016.

[13] S. R. Chhetri, J. Wan, and M. A. Al Faruque, "Cross-domain security of cyber-physical systems," in *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2017, pp. 200–205.

[14] S. Faezi, S. R. Chhetri, A. V. Malawade, J. C. Chaput, W. H. Grover, P. Brisk, and M. A. Al Faruque, "Oligo-snoop: A non-invasive side channel attack against dna synthesis machines." in *NDSS*, 2019.

[15] S. R. Chhetri, A. Barua, S. Faezi, F. Regazzoni, A. Canedo, and M. A. Al Faruque, "Tool of spies: Leaking your ip by altering the 3d printer compiler," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[16] N. Mohammad, A. Barua, and M. A. Arafat, "A smart prepaid energy metering system to control electricity theft," in *2013 International Conference on Power, Energy and Control (ICPEC)*. IEEE, 2013, pp. 562–565.

[17] G. Garcia, S. Tarbouriech, and J. M. G. da Silva, "Dynamic output controller design for linear systems with actuator and sensor saturation," in *2007 American Control Conference*. IEEE, 2007, pp. 5834–5839.

[18] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: laser-based audio injection attacks on voice-controllable systems," *arXiv preprint arXiv:2006.11946*, 2020.

[19] H. Mehta, U. Thakar, V. Joshi, K. Rathod, and P. Kurulkar, "Hall sensor fault detection and fault tolerant control of PMSM drive system," in *2015 International Conference on Industrial Instrumentation and Control (ICIC)*. IEEE, 2015, pp. 624–629.

[20] A. Ajbl, M. Pastre, and M. Kayal, "A fully integrated Hall sensor microsystem for contactless current measurement," *IEEE Sensors Journal*, vol. 13, no. 6, pp. 2271–2278, 2013.

[21] E. Kabalci and Y. Kabalci, "A wireless metering and monitoring system for solar string inverters," *International Journal of Electrical Power & Energy Systems*, vol. 96, pp. 282–295, 2018.

[22] E. Muljadi, C. Butterfield, B. Parsons, and A. Ellis, "Effect of variable speed wind turbine generator on stability of a weak grid," *IEEE Transactions on Energy Conversion*, vol. 22, no. 1, pp. 29–36, 2007.

[23] B. Razavi, *Design of analog CMOS integrated circuits*. Tata McGraw-Hill Education, 2002.

[24] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 445–467.

[25] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1004–1015.

[26] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[27] Y. Wang, Z. Xu, J. Zhang, L. Xu, H. Wang, and G. Gu, "Srid: State relation based intrusion detection for false data injection attacks in scada," in *European Symposium on Research in Computer Security*. Springer, 2014, pp. 401–418.

[28] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM symposium on information, computer and communications security*, 2011, pp. 355–366.

[29] A. Barua, D. Muthirayan, P. P. Khargonekar, and M. A. Al Faruque, "Hierarchical Temporal Memory Based Machine Learning for Real-Time, Unsupervised Anomaly Detection in Smart Grid: WiP Abstract," in *2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2020, pp. 188–189.