Hardware/Software Co-Design for Sensor Security

Anomadarshi Barua and **Mohammad Abdullah Al Faruque**, University of California, Irvine

Most sensors cannot differentiate between legitimate signals and spoofing signals. Therefore, a novel research focus is required using hardware/software co-design techniques in the sensor computation domain to detect, contain, and eradicate spoofing signals in sensors.

Sensors observe environments, measure physical quantities, and then convert the physical quantities into usable signals (such as electrical signals). Though there are different types of sensors, we want to bring the attention of the readers to the fact that all sensors share a common vulnerable physics. We explain the vulnerable physics first and then emphasize that a novel research focus is required using a hardware/software co-design technique, which involves a change of the sensor's transducer and the incorporation of lightweight algorithms in the sensor computation domain to filter out spoofing signals from the sensor.

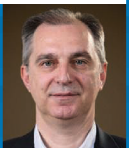
INTRODUCTION

The part of the sensor responsible for sensing the external stimulus signal from the environment and converting it into a usable signal is known as a *transducer*. The transducer is a unique part of a sensor that varies from one sensor to another. After converting the external signal into a usable signal, the transducer gives the usable signal to filters for denoising, and the denoised signal then propagates to the analog-to-digital-converter (ADC) for the digitization (see Figure 1).

The sensor pipeline from the transducer to the ADC has been technically improved in terms of accuracy and efficiency; however, to the best of our knowledge, much less attention has been paid to the security of the sensor before the ADC block of the sensor. Please note that there are many significant works in the literature that hold the sensor security after the ADC using secure cryptographic

Digital Object Identifier 10.1109/MC.2023.3248779
Date of current version: 3 May 2023

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on September 29,2023 at 23:44:21 UTC from IEEE Xplore. Restrictions apply.



operations through the digitization of the sensor data. However, they do not provide any security before the ADC in the physical layer of the sensor pipeline.

The absence of robust security before the ADC in the sensor pipeline makes the sensor vulnerable to a spoofing attack coming from an external attack source. For example, an adversary can inject a fake spoofing signal to the sensor (see Figure 1). As the sensor's transducer is naive, it cannot differentiate between the attacker's provided spoofing attack signal and the legitimate signal and, hence, cannot contain the attack signal inside of the sensor. As a result, the attack signal propagates with the legitimate signal inside the sensor and spoofs the sensor in its linear region or drives the sensor to its saturation region. As a result, the attack signal compromises the integrity and availability of the system controller connected with the sensor, resulting in a denial-of-service attack on the connected system. This may cause a catastrophic failure, a system shutdown, or a disruption of the system's normal behavior.[1,2] It is just a matter of time before more attacks on sensors will emerge from different attack surfaces as sensors are becoming more complex and sophisticated today without improvements to their security. This article highlights the existing vulnerability of the sensor physics that has been neglected so far while designing the sensor and provides a recommendation of how sensors can be redesigned using a hardware/software co-design approach to ensure their security without hampering their normal real-time operation.

Scope of our work

We consider the type of defense that provides security against fake signal injection into the sensor transducers before the ADC. An example is given here to clarify the scope of this work. A Hall current sensor can measure the current signal. If an attacker changes the current requirement by switching on/off any system load, the current reading changes. As a result, the Hall sensor measures a different current reading than the original one. We are not considering this type of attack on the Hall current sensor. Instead, we are considering the type of attack where the attacker directly injects fake signals (for example, magnetic fields) into the Hall transducer (that is, a p-type semiconductor) and changes the current reading from the original one.

> If a transducer can reject the attack signal, this approach would diminish the burden of using a complex encryption algorithm in the sensor hardware.

CURRENT PROGRESS

Throughout the last few decades, there has been a lot of work done to provide defense against sensor spoofing attacks. Almost all of the work is related to secure boot, secure firmware updates, and secure communication protocols, such as Transport Layer Security, to encrypt sensor data and prevent unauthorized access. All of these defenses are proposed to work after the ADC of the sensor pipeline. However, if the attacker injects fake signals into the transducer before the ADC, no amount of security after the fact can help. Therefore, almost all of these defenses don't work against a fake signal injection into the sensor's transducer.[3] Another set of defenses uses transduction shielding, adaptive filtering, lowpass filtering, and randomized phase sampling to filter out the injected spoofing signal from the original signal. However, these defenses do not work if the injected spoofing signal has the same bandwidth as the legitimate signal; they cannot filter out the injected spoofing signal if it has the same frequency as the legitimate signal.[3] Therefore, in summary, sensor security is still a *malnourished* domain; it requires more attention from security researchers to make the sensors robust against spoofing attacks on sensor transducers.

HARDWARE/SOFTWARE CO-DESIGN

The next generation of sensor research should consider security, from

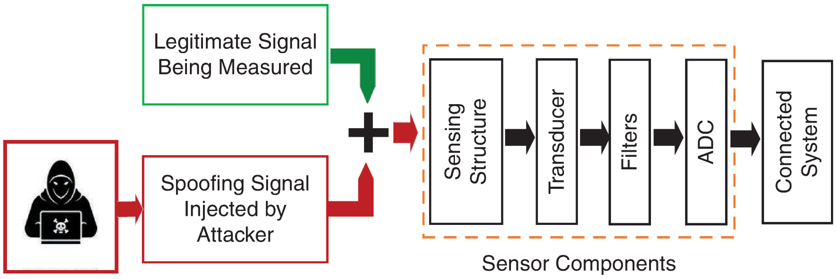


FIGURE 1. Noninvasive spoofing attack on sensor's transducers propagates from transducers to the connected system.

uthorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on September 29,2023 at 23:44:21 UTC from IEEE Xplore. Restrictions apply.

designing the new transducer to implementing lightweight algorithms in the sensor domain. We call it the *bottom-up approach*. In the bottom-up design, sensors may need computation blocks in between the transducer and the ADC, and lightweight algorithms should be implemented after the ADC to contain the attacks inside of the sensors. As sensors will have smart computations in the sensor domain, we propose this methodology as *in-sensor computation* for sensor security. Moreover, as our proposed method involves the integration of hardware and software components in the in-sensor computation block, we also name this methodology *hardware/software co-design* in the in-sensor computation for sensor security. This methodology has the following important components for in-sensor defense.

The sensor itself will act as a hardware/software co-designed firewall in the physical layer against the spoofing signal injected by an attacker.

Introducing smart transducers

The number and location of the transducers in the sensor should be revised to detect and differentiate between the injected attack signal and the legitimate signal. As a transducer is an entry point to the sensor, if a transducer can reject the attack signal, this approach would diminish the burden of using a complex encryption algorithm in the sensor hardware. One strategy is to use multiple transducers in specific geometric configurations to detect and reject external attack signals. For example, the differential configuration uses two transducers of the same type[4,5] placed in a line to nullify the common mode attack signal from the legitimate signal. This idea can be extended to other sensors as well. For the microelectromechanical system (MEMS) accelerometer, as our second example, a new idea to explore is to use three transducers in a triangular position to detect ultrasound frequency injected by an attacker. As the MEMS accelerometer is sensitive to a particular resonant frequency injected by an external attacker, there is a possibility that the triangular placement of transducers can nullify the injected resonant frequency while not perturbing its normal operation of measuring acceleration to a particular direction. A real-time lightweight algorithm will be implemented in the in-sensor computation block to contain the rest of the attack signals, which may slip through the transducer. Therefore, the sensor itself will act as a hardware/software co-designed firewall in the physical layer against the spoofing signal injected by an attacker. Though this strategy is quite novel, it has its own implementation challenge for all types of sensors. Research in this direction would be influential in the future.

Analog signal encryption

An active sensor can transmit a signal and obtain measurements after the reflection of the same transmitted signal from the environment. The main reason for the vulnerability of active sensors is that the signal transmitted by the transmitter of the active sensor is not encrypted. Therefore, an attacker can transmit a similar signal with corrupted information to spoof the sensor transmitter. If the legitimate transmitted signal can be encrypted with a key in the analog domain, the same signal can be decrypted with the same key after the reception of the same transmitted signal. The encryption of the analog signal can be achieved by transmitting the analog signal in a broad spectrum using the frequency hopping spread spectrum technique.

The encryption and decryption of analog signals in the in-sensor computation block is a robust solution against a spoofing attack on sensors. The main challenge of this approach is to ensure that the sensor-level encryption and decryption will not hamper the real-time measurement of the sensor. This requirement can be achieved by using robust cryptographic hardware using a hardware/software co-design technique in the transport layer of the sensor.

The main intention of this article is to make the readers aware of the existing vulnerability of the sensor physics that has been neglected so far while designing the sensor. We emphasize that the next generation of sensors should be redesigned from the transducer to the signal processing stage of the sensor pipeline to prevent sensor spoofing. Otherwise, no matter how efficiently the sensors are designed, their security will be compromised by an attacker using a simple external spoofing technique. We provide a research direction of how the sensors can be redesigned using a hardware/software co-design approach to ensure their security without hampering their normal real-time operation. C

ACKNOWLEDGMENT

This work was partially supported by the National Science Foundation under award ECCS-2028269. Any opinions, findings, conclusions, or recommendations expressed in this article are those of the authors and do not necessarily reflect the views of the funding agencies.

REFERENCES

1. A. Barua and M. A. A. Faruque, "Hall spoofing: A non-invasive DoS attack on grid-tied solar inverter," in

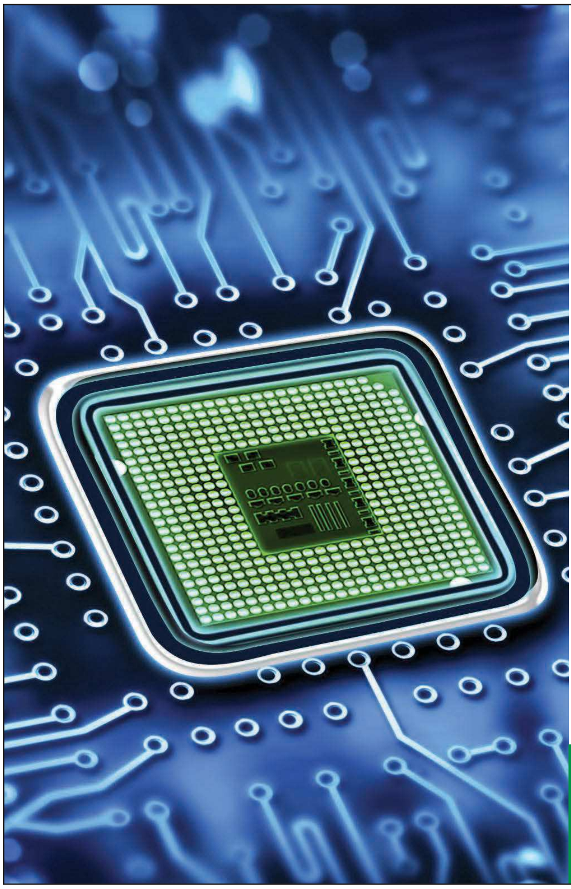
uthorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on September 29,2023 at 23:44:21 UTC from IEEE Xplore. Restrictions apply.

Proc. 29th USENIX Secur. Symp., 2020, pp. 1273–1290.

2. A. Barua, Y. Gizachew Achamyeleh, and M. A. A. Faruque, "A wolf in sheep's clothing: Spreading deadly pathogens under the disguise of popular music," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2022, pp. 277–291, doi: 10.1145/3548606.3560643.
3. A. Barua and M. A. A. Faruque, "Sensor security: Current progress, research challenges, and future roadmap," in *Proc. 41st IEEE/ACM Int. Conf. Comput.-Aided Des.*, 2022, pp. 1–7, doi: 10.1145/3508352.3561100.
4. A. Barua and M. A. A. Faruque, "HALC: A real-time in-sensor defense against the magnetic spoofing attack on hall sensors," in *Proc. 25th Int. Symp. Res. Attacks, Intrusions Defenses*, 2022, pp. 185–199, doi: 10.1145/3545948.3545964.
5. A. Barua and M. A. A. Faruque, "PreMSat: Preventing magnetic saturation attack on hall sensors," in *Proc. IACR Trans. Cryptogr. Hardware Embedded Syst.*, 2022, pp. 438–462, doi: 10.46586/tches.v2022.i4.438-462.

ANOMADARSHI BARUA is a Ph.D. candidate studying computer engineering at the University of California, Irvine, Irvine, CA 92697 USA. Contact him at anomadab@uci.edu.

MOHAMMAD ABDULLAH AL FARUQUE is a professor at the University of California, Irvine, Irvine, CA 92697 USA, and director of its Embedded and Cyber-Physical Systems Lab. Contact him at alfaruqu@uci.edu.



IEEE TRANSACTIONS ON

COMPUTERS

Call for Papers: *IEEE Transactions on Computers*

Publish your work in the IEEE Computer Society's flagship journal, *IEEE Transactions on Computers*. The journal seeks papers on everything from computer architecture and software systems to machine learning and quantum computing.

Learn about calls for papers and submission details at **www.computer.org/tc.**

IEEE COMPUTER SOCIETY IEEE

Digital Object Identifier 10.1109/MC.2023.3263979

uthorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on September 29,2023 at 23:44:21 UTC from IEEE Xplore. Restrictions apply.