T

The Hall Sensor Security

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

Synonyms

Spoofing a hall sensor

Definitions

The state-of-the-art Hall sensors are vulnerable to an external magnetic spoofing attack. A smart attacker can use distinct types of external magnetic fields to inject malicious data into Hall sensors resulting in a denial-of-service (DoS) attack on the connected systems.

Background

Due to the continuous development in the Hall sensing technology, nowadays, the Hall sensor has excellent accuracy, high efficiency, and smaller form factor compared to other magnetic sensors. Therefore, the Hall sensor is a reliable choice over other magnetic/nonmagnetic sensors, and it is widely used for positioning, speed detection, proximity sensing, current sensing applications, power measurement, etc. Despite this growing market, Hall sensors are still not secured, and the integrity of the Hall sensor can be compromised by injecting external magnetic signals by an attacker (Barua and Al Faruque 2020).

Theory

Hall Sensor Basics

A Hall sensor has a p-type semiconductor material, which acts as the sensing structure. The p-type material generates an output Hall voltage, V_h, when it senses an input magnetic field B_i. Therefore, the output Hall voltage V_h can be expressed as,

$$V_h = k \times B_i \tag{1}$$

where k is a proportionality constant, which depends on the physical and electrical properties of the p-type semiconductor material. Let us assume an attacker injects a malicious external magnetic field, B_{atk} into the Hall sensor. As a result, Eq. 1 can be changed as follows:

$$V_h^f = k \times (B_i \times B_{\text{atk}}) \tag{2}$$

where V_h^f is the fake output Hall voltage. The injected attack component, B_{atk}, can be either positive or negative depending upon the types of the poles from where the magnetic fields are generated. Typically, magnetic fields from the

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1652-1

north pole are considered as $+B_{\text{atk}}$, and magnetic fields from the south pole are considered as $-B_{\text{atk}}$ or vice versa.

Distinct Types of B_{atk}

The attacker can generate mainly three types of malicious magnetic fields (B_{atk}), namely, constant, sinusoidal, and square pulsating fields. Mathematically, we can model the term B_{atk} for constant, sinusoidal, and square pulsating fields as follows:

$$B_{\text{atk}} = \begin{cases} C; & \text{constant field,} \\ B_a \sin(2\pi f t); & \text{sinusoidal field,} \\ sgn(B_a \sin(2\pi f t)); & \text{pulsating field.} \end{cases} \quad (3)$$

where C is a constant, f is the frequency and B_a is the magnitude of the injected B_{atk}, and sgn is the signum function.

Generation of B_{atk}

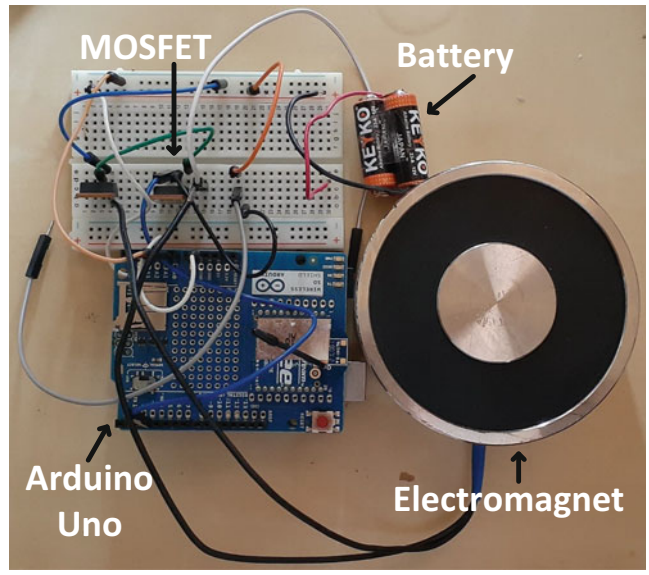
The different types of malicious magnetic fields (B_{atk}) can be generated by using an electromagnet. A constant voltage input to the electromagnet can generate a constant B_{atk}. Moreover, sinusoidal and pulsating B_{atk} can be generated by using the pulse width modulation (PWM) technique. Typically, the pulsating B_{atk} is a periodic switching of the constant B_{atk}. An electronic switch MOSFET with an Arduino board can be used to generate the PWM.

Figure 1 shows a prototype of a possible implementation to generate the distinct types of B_{atk}. We use a MOSFET (part # P7N20E) with an Arduino Uno to switch an electromagnet (part # WF-P80/38).

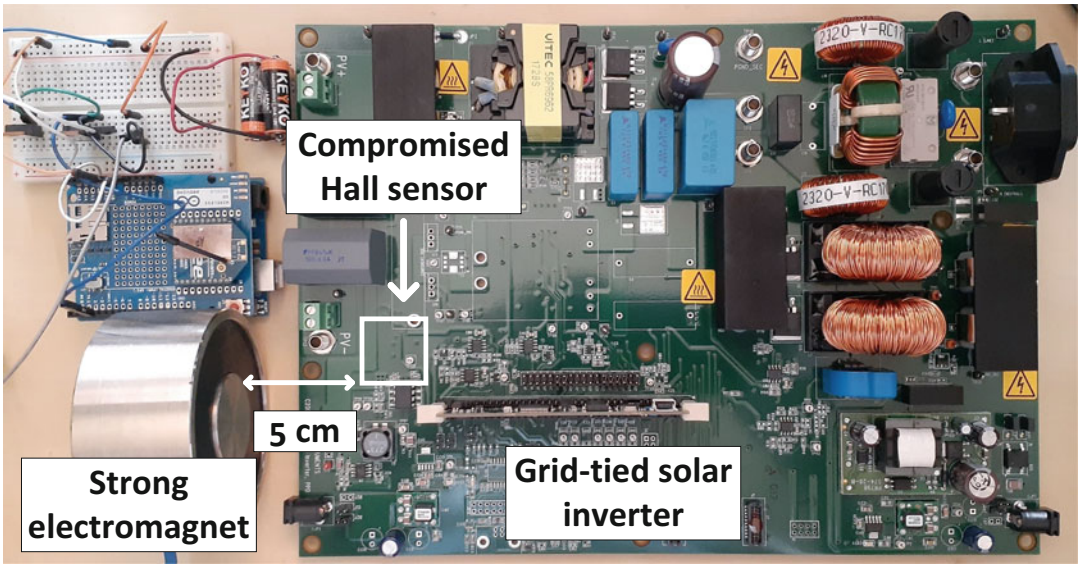
An Experimental Case Study

In this section, we demonstrate the vulnerability of a Hall sensor in a grid-tied solar inverter. A grid-tied solar inverter is an important component of today's smart grid, and Hall sensors are used to measure current in the grid-tied solar inverter.

Figure 2 shows the experimental setup. A 140 Watt inverter from Texas Instruments is used in our experiment. This inverter has a Hall effect current sensor with a part # ACS712ELCTR-20A-T. An electromagnet with the Arduino control is placed at 5 cm away from the target Hall sensor of the grid-tied solar inverter. The electromagnet injects constant, sinusoidal, and pulsating magnetic fields into the Hall sensor. In our experiment, the intensity of the injected B_{atk} by the electromagnet is 0.8 Tesla.



The Hall Sensor Security, Fig. 1 Generation of B_{atk} using an electromagnet with an Arduino control. A MOSFET is used to generate PWM for generating different types of B_{atk}



The Hall Sensor Security, Fig. 2 An experimental setup to demonstrate the vulnerability of a Hall sensor

Results

Figure 3 shows the results of injecting different types of magnetic fields to the Hall sensor of the grid-tied solar inverter.

The green curve in Fig. 3 indicates the inverter output voltage before any malicious magnetic field (B_{atk}) injection. A constant B_{atk} on the Hall sensor shifts the original inverter output voltage upward or downward (depending upon the polarity of the injected B_{atk}). The red curve in Fig. 3 indicates that the inverter output voltage shifts upward because of the injection of a constant B_{atk}. Here the polarity of B_{atk} is the north pole. As pulsating B_{atk} is a periodic switching of the constant B_{atk}, the injection of the pulsating B_{atk} causes periodic upward/downward shifting of the inverter output voltage similar to constant B_{atk}.

The blue curve in Fig. 3 indicates that an injection of the sinusoidal B_{atk} creates a sinusoidal variation in the inverter output voltage. Here the frequency of the injected sinusoidal B_{atk} is 2 Hz.

Defense

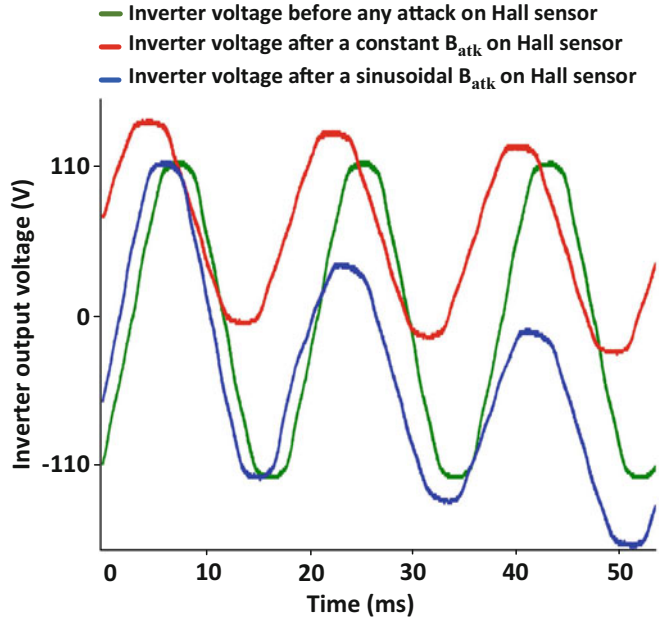
The following defense techniques should be adopted to protect Hall sensors from the external magnetic spoofing. It is important to note that these defense techniques may lessen the external magnetic spoofing impacts on Hall sensors but may not completely prevent it. It is still open research to make the hall sensors secured from this type of intentional external magnetic field injection.

Shielding

By providing shielding around the Hall sensor, the impacts of the external magnetic fields can be reduced. Shields can redirect magnetic fields from hall sensors. It is recommended to use multiple lamination layers in the shield instead of a single layer. High saturation magnetic flux density materials can be combined with amorphous alloy material to provide multiple lamination layers in shields. However, we must remember that having only a good shield is not enough, as any shield can be compromised with a stronger magnetic field.

Robust Sensors

Differential Hall sensors should be used instead of non-differential Hall sensors because differential Hall sensors are robust against common mode magnetic fields. The symmetric placement of the two similar Hall materials can cancel out common-mode magnetic fields in the differen-



The Hall Sensor Security, Fig. 3 Inverter output voltage after injecting different types of malicious magnetic fields (B_{atk}) into the Hall sensor

tial Hall sensor. Moreover, a field concentrator can be introduced to the Hall sensor to make it more insensitive to external malicious magnetic fields. However, it is important to note that these techniques can also be compromised by using stronger magnetic fields.

Open Problems and Future Directions

To provide complete defense against the external magnetic spoofing on the Hall sensor, the defense techniques should not only detect the presence of the external magnetic fields but also should contain the magnetic fields inside of the Hall sensors, so that the injected malicious fields cannot propagate farther to connected systems. Security aspects should be considered from the very beginning while designing Hall sensors. New hardware-software architectures (Yan et al. 2020) should be introduced in the Hall sensor design that may act as firewalls in the sensor-system interface. Moreover, the introduction of low-power, real-time, and unsupervised algorithms (Barua et al. 2020) in the Hall sensor could add new values to tackle the external magnetic spoofing.

References

Barua A, Al Faruque MA (2020) Hall spoofing: a non-invasive DoS attack on grid-tied solar inverter. In: 29th USENIX Security Symposium (USENIX Security 20). USENIX Association, pp 1273–1290. https://www.usenix.org/conference/usenixsecurity20/presentation/barua

Barua A, Muthirayan D, Khargonekar PP, Al Faruque MA (2020) 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, pp 188–189

Yan C, Shin H, Bolton C, Xu W, Kim Y, Fu K (2020) SoK: a minimalist approach to formalizing analog sensor security. In: 2020 IEEE Symposium on Security and Privacy (SP), pp 480–495