HALC: A Real-time In-sensor Defense against the Magnetic Spoofing Attack on Hall Sensors

Anomadarshi Barua
Department of Electrical Engineering and Computer Science, University of California, Irvine

Mohammad Abdullah Al Faruque
Department of Electrical Engineering and Computer Science, University of California, Irvine

ABSTRACT

Several papers have been published over the last ten years to provide a defense against intentional spoofing to sensors. However, these defenses would only work against those spoofing signals, which have a separate frequency from the original signal being measured. These defenses would *not* work if the spoofing attack signal (i) has a frequency equal to the frequency of original signals, (ii) has zero frequency, and (iii) is *strong* enough to drive the sensor output close to its saturation region. More specifically, these defenses are not designed for a *magnetic* spoofing attack on *passive Hall sensors*.

Our work begins to fill this gap by providing a defense against the magnetic spoofing attack on passive Hall sensors. Our proposed defense HALC can detect and contain all types of strong and weak magnetic spoofing, such as constant, sinusoidal, and pulsating magnetic fields, in real-time. HALC works up to ~9000 G of external magnetic spoofing within a frequency range of 0 - 150 kHz, whereas existing defenses work only when the spoofing signals have a separate frequency from the original signal being measured. HALC utilizes the analog and digital cores to achieve a constant computational complexity O(1). Moreover, it is low-power (~1.9 mW), low-cost (~$12), and can be implemented in the sensor hardware. We have tested HALC on ten different industry-used Hall sensors from four different manufacturers to prove its efficacy and found that the correlation coefficient between the signals before and after the attack is greater than 0.91 in every test case. Moreover, we demonstrate its efficacy in two practical systems: a grid-tied solar inverter and a rotation-per-minute measurement system. We find through experiments that HALC is a robust real-time defense against a magnetic spoofing attack on passive Hall sensors.

CCS CONCEPTS

• **Security and privacy → Embedded systems security**.

KEYWORDS

hall sensors, noninvasive spoofing, real-time defense

ACM Reference Format:
Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2022. HALC: A Real-time In-sensor Defense against the Magnetic Spoofing Attack on Hall Sensors. In *25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022), October 26–28, 2022, Limassol, Cyprus.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3545948.3545964

RAID 2022, October 26–28, 2022, Limassol, Cyprus

ACM ISBN 978-1-4503-9704-9/22/10.
https://doi.org/10.1145/3545948.3545964

1 INTRODUCTION

Recent decades have observed the proliferation of smart sensors in embedded and cyber-physical systems (ECPSs). One widely used sensor is the Hall sensor, which can output analog voltage proportional to the magnetic field it senses in the environment. Due to the continuous development in Hall sensing technology, nowadays, the Hall sensor has excellent accuracy, high efficiency, and good linearity, and their markets are growing rapidly [18, 27, 33–35, 42, 46]. Despite this growth, they are still not secured, and recently, it has been proved that an attacker can compromise its integrity by injecting fake external magnetic fields [20, 38], causing an intentional spoofing and denial-of-service (DoS) in ECPSs. Therefore, a robust defense for Hall sensors is much needed to protect them from intentional magnetic spoofing attacks by an attacker.

The output voltage of the Hall sensor is linear to input magnetic fields [36]. Therefore, broadly speaking, the external magnetic field injected by an attacker can introduce two types of errors in the Hall sensor's output: the attacker can inject *strong magnetic field*, which can change the sensor's output on a large scale (i.e., volt range) and drive the output from its linear region to close to its saturation region, or can spoof with *weak magnetic fields*, which can change the sensor output in millivolt scale only in the linear region. We refer to the above definition of *strong* and *weak* magnetic fields when we mention these two terms in this paper. Moreover, Hall sensors are of two types: active and passive Hall sensors. As passive sensors [45] are naive devices, they blindly send signals to the upper level without proper authentication. Therefore, the security of passive Hall sensors is always challenging.

The state-of-the-art defenses [19, 23, 28, 37, 41, 47] target specific sensors other than passive Hall sensors, such as MEMS microphones, accelerometers, gyroscopes. However, these defenses have the following limitations: (i) They cannot contain strong spoofing signals, which can change the sensor output in volt scale, driving the output close to its saturation region. (ii) They cannot contain such spoofing signals, which have a frequency other than the resonant frequency of the target sensors. (iii) They don't work against DC/constant spoofing signals, which have a zero frequency. (iv) They cannot contain a spoofing signal if it has the same frequency as the original input signal being measured. Moreover, these defenses can handle spoofing signals having different modalities *other* than magnetic fields, such as acoustics, ultrasounds. Therefore, these defenses cannot be used for a *passive Hall sensor* [1]as it use magnetic fields.

[1]In this paper, Hall sensors mean unipolar/bipolar, open-loop/closed-loop ***passive*** Hall sensors, unless stated otherwise.

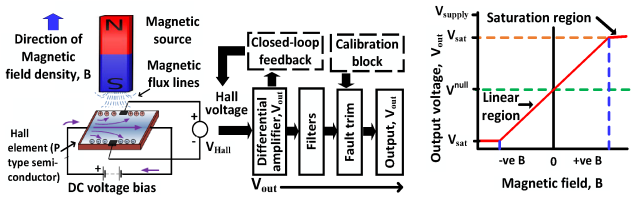

Figure 1: (Left) Hall *in-sensor* components of a typical Hall sensor. (Right) The transfer function of a typical Hall sensor.

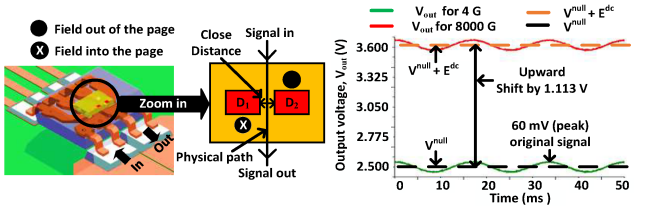

Figure 2: (Left) A differential Hall sensor. (Right) A differential Hall sensor may not work against a strong field.

Therefore, we propose ***HALC***[2]*: **Hal**l Spoofing **C**ontainer*, to provide a robust real-time defense against magnetic spoofing on passive Hall sensors by handling the above limitations that exist in the recent works [19, 23, 28, 37, 41, 47]. HALC can *detect and contain* all types of *weak and strong* magnetic spoofing, such as constant, sinusoidal, and pulsating fields up to ~9000 G and can prevent both *intentional spoofing and denial-of-service* of the system.

The core idea behind HALC is that it can separate the injected fake spoofing signal from the original signal using two different cores - analog and digital core. The analog core removes the fake AC (i.e., time-dependent) magnetic fields using inexpensive fast-order filters irrespective of their frequencies, and the digital core removes the fake DC (i.e., constant) fields using a DC feedback signal keeping the original signal intact. The analog core is implemented in such a way that it introduces two parallel paths to process inputs enabling faster signal processing. *The digital core runs a low-power algorithm with O(1) complexity that can even prevent attack signals having the same frequency/amplitude as the original input signals.* HALC is low-power and can be implemented in the sensor hardware domain. Therefore, we name this solution as *in-sensor defense* that is cheap and does not hamper the existing data-processing speed of connected systems. To the best of our knowledge, HALC is a robust real-time and in-sensor defense against the strong and weak magnetic spoofing attack on Hall sensors. We believe that the defense demonstrated here can be applied to a broad array of sensors beyond Hall sensors, including accelerometers and more.

Contributions: Our main technical contributions are:

1. We design HALC - a low-cost (~$12) and low-power (~1.9 mW) defense that can *detect and contain* the strong and weak magnetic spoofing in hard real-time with O(1) computational complexity.

2. We show the effectiveness of HALC through over 150 experiments on ten different Hall sensors from four different manufacturers. We experiment with different types, namely unipolar, bipolar, open-loop, closed-loop, and differential sensors to prove its efficacy.

3. We prove the efficacy of HALC in two critical systems: a grid-tied inverter in smart grids and a rotation-per-minute (RPM) system in industrial control systems (ICSs). The demonstration of HALC is shown in the following link: https://sites.google.com/view/hallspoofingcontainer/home

[2]Pronounced as Hulk, who is a mighty superhero in Marvel Comics.

2 BACKGROUND

2.1 Hall in-sensor components

The basic components of Hall sensors are shown in Fig. 1 (Left). A Hall sensor has a Hall element (i.e., p-type semiconductor), which generates a Hall voltage (V_{Hall}) proportional to an input magnetic field, B. A DC voltage bias is applied across the Hall element to energize it. The generated V_{Hall} is given as input to a differential amplifier with closed-loop feedback and a self-calibration block to reduce the measurement error. *It is clear from this discussion that state-of-the-art Hall sensors are still lacking hardware in the sensor domain to contain injected fake magnetic fields.*

Transfer function: The term V_{Hall} can be +ve or -ve because input magnetic field B can be +ve or -ve (i.e., north/south pole). Therefore, the output of the differential amplifier, denoted by V_{out}, can go either +ve or -ve from the *null-voltage* position. The null-voltage is denoted by V^{null}, which is the position of the V_{out} with no input magnetic field (i.e., B = 0). Therefore, the transfer function of a typical Hall sensor can be expressed as:

$$V_{out} = (K \times B) + V^{null} \quad (1)$$

where K is a coefficient. The graphical representation of Eqn. 1, which is shown in Fig. 1 (Right), indicates that V_{out} linearly varies with the input magnetic field B. As mentioned earlier, the existing defenses [19, 23, 28, 37, 41, 47] work against weak magnetic spoofing, which can vary the output in its linear region, but don't work against strong magnetic spoofing, which can change V_{out} in volt scale, driving close to the saturation voltage, V_{sat}.

2.2 Passive and active Hall sensor

A passive Hall sensor can simply detect magnetic fields coming from the environment, whereas an active Hall sensor [44] transmits a signal first and gathers data after the reflection of that transmitted signal from a target. PyCRA [39] works only with the active sensor but *does not* work with the passive one. State-of-the-art passive Hall sensors are largely blind that relay signals to the upper level without considering the signal integrity. *Therefore, our proposed defense targets passive hall sensors.*

2.3 Differential Hall sensor

The differential Hall sensor is the state-of-the-art sensor, which can reject common-mode spoofing signal [19]. It is an *in-sensor* defense. As our defense is also an in-sensor, the differential Hall sensor's limitations are important to understand the novelty of our work.

A differential Hall sensor has two [19] Hall elements, D_1 and D_2, placed *close* to each other (Fig. 2 (Left)). Let us assume D_1 sees

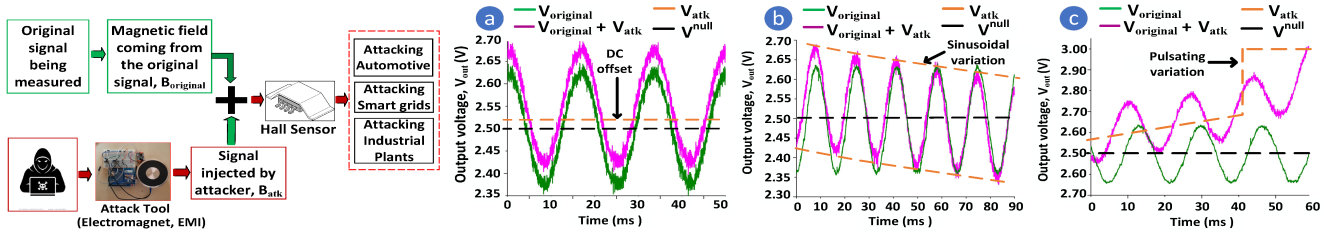

Figure 3: (Left) Noninvasive magnetic spoofing attack on Hall sensors. (Right) (a) The constant B_{atk} adds a DC offset. (b) The sinusoidal B_{atk} modulates the $V_{original}$ sinusoidally. (c) The square pulsating B_{atk} creates a pulsating variation in $V_{original}$.

magnetic field B_1, and D_2 sees magnetic field B_2. Therefore, the transfer function of a differential Hall sensor is:

$$V_{out} = K \times (B_1 - B_2) + V^{null} \tag{2}$$

where K is a proportionality coefficient. Let us assume an attacker injects an external magnetic field, B_{atk}. As D_1 and D_2 are placed close to each other, they may see the same magnetic field, B_{atk}. As a result, after the injection of B_{atk}, Eqn. 2 is changed as follows:

$$\begin{aligned} V_{out} &= K \times \{(B_1 + B_{atk}) - (B_2 + B_{atk})\} + V^{null} \\ &= K \times (B_1 - B_2) + V^{null} \end{aligned} \tag{3}$$

The B_{atk} can only be nullified in Eqn. 3 if and only if D_1 and D_2 can see the same (i.e., common-mode) B_{atk}. However, practically speaking, there is always a small physical distance between D_1 and D_2 as a physical signal path is present between D_1 and D_2. Therefore, they may not see the same B_{atk}. As a result, B_{atk} may not be exactly nullified in Eqn. 3. The mismatch gets worse if the injected magnetic field is strong. At a strong magnetic field, the magnetic reluctance of the material present in the tiny distance between D_1 and D_2 gets increased. The increase of reluctance increases the magnetic field gradient between Hall elements D_1 and D_2.

To prove this claim, an experiment is carried out on a differential Hall sensor (Part# ACS724) by injecting a weak 4G external magnetic field, and a strong 8000G magnetic field using an electromagnet and a permanent magnet (part# H33 [32], respectively (see Appendix 10.1) from 1 cm distance. The ACS724 typically has V^{null} = 2.5 V. Fig. 2 (Right) shows that 4 G shifts the V_{out} by 0.8 μV, which is negligible, whereas 8000 G adds a large DC offset, denoted by E^{dc}, with V^{null}. This shifts the V_{out} by 1.113 V upward causing a 44.52% change in V^{null}. This can corrupt the sensor data resulting in a DoS attack on the connected systems. It proves that industry-used Hall sensors are still vulnerable to strong magnetic spoofing.

3 ATTACK MODEL

The components of the attack model against which HALC works are explained below and also shown in Fig. 3 (Left).

a. Attacker's capability: The attacker can be a disgruntled employee or a guest, who may not get a long time to modify the target Hall sensor like a lunch-time attack [25]. The attacker just needs brief one-time access to *noninvasively* spoof Hall sensors from a *close* distance using external magnetic fields. The attacker is not allowed to physically alter any components of Hall sensors.

b. Attacker's strength: The attacker can inject any type of magnetic field. Here, we consider constant, sinusoidal, and square pulsating fields to cover the whole attack surface because all other patterns can be derived from these three basic fields (i.e., Fourier transformation [21]). Moreover, the attacker can use different intensities of magnetic fields inside or outside of the normal sensing range of the sensor. Let's denote the original magnetic field being measured by $B_{original}$ and magnetic fields injected by the attacker by B_{atk} (Fig. 3 (Left)). The term B_{atk} can be modeled as follows:

$$B_{atk} = \begin{cases} M; & \text{constant field,} \\ B_m \sin \omega t; & \text{sinusoidal field,} \\ sgn(B_m \sin \omega t); & \text{square pulsating field.} \end{cases} \tag{4}$$

where M is a constant, ω is the angular frequency and B_m is the magnitude of the injected magnetic field, and sgn is the signum function. Eqn. 1 can be written after an attack as:

$$\begin{aligned} V_{out} &= \{(K \times B_{original}) + V^{null}\} + (K \times B_{atk}) \\ &= V_{original} + V_{atk} \end{aligned} \tag{5}$$

Eqn. 5 shows that Hall sensor's output V_{out}, after an attack, has two components: an original component, $V_{original}$, coming from the $B_{original}$ and an attack component, V_{atk}, coming from the injected B_{atk}. An ideal defense should filter out the attack component V_{atk} originating from any type of attack magnetic field B_{atk}.

Demonstration: A demonstration of injecting a constant, sinusoidal, and square pulsating malicious magnetic fields B_{atk} into a Hall sensor is shown in Fig. 3 (Right). Before injecting the B_{atk}, the Hall sensor is giving a sinusoidal voltage $V_{original}$ (green line) at its output. A constant 300 G malicious B_{atk} adds a DC offset, shifting the $V_{original}$ by 0.02 V. A 2 Hz sinusoidal and pulsating 300 G malicious B_{atk} modulates the $V_{original}$ in a sinusoidal and pulsating fashion, respectively.

c. Attack tool and cost: The attacker can use a cheap electromagnet and an Arduino with pulse-width modulation to generate above distinct types of B_{atk} (see Appendix 10.1). For example, a simple electromagnet, such as Uxcell [17] can generate sufficient magnetic fields (i.e., ~ 8000 G) for a strong magnetic spoofing attack, and it is cheap (~$37) and easily available on eBay/Amazon.

d. Ineffective Shield: The Hall sensor may or may not be secured inside of a shield [26] depending on its application. In the presence of a shield, the injected B_{atk} is strong enough to penetrate a shield.

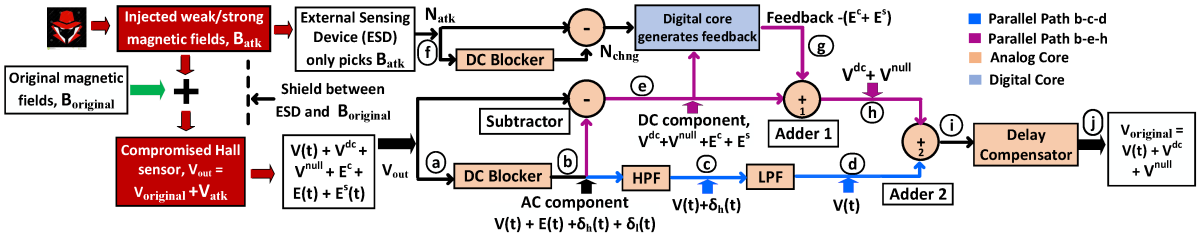

Figure 4: Basic blocks of the Hall Spoofing Container (HALC).

e. Target system: Hall sensors are used in many safety-critical applications, such as power grid monitoring, motor speed monitoring, proximity sensing in industrial plants, and braking in automotive. Therefore, the consequences of attacking Hall sensors can be catastrophic. For example, injecting fake magnetic fields into Hall sensors located in a micro-grid may cause a denial-of-service (DoS) attack on the power system [20]. Another notable attack happens on automotive systems where an attacker may cause a brake failure by spoofing Hall sensors located in anti-lock-braking systems (ABSs) of a vehicle [38]. The consequences of these attacks on Hall sensors are significant in terms of loss of human life and monetary resources. Moreover, an inaccurate Hall effect reading would cause immediate damage in the absence of a fail-safe, like an electric motor running at higher RPM than it is mechanically designed for. This may cause a complete shut-down of the compromised system. *Therefore, a defense (i.e., like HALC) is critical in the Hall sensor domain to prevent these catastrophic consequences.*

4 HALL SPOOFING CONTAINER (HALC)

In this section, we provide details on the design process of HALC by answering the following three questions.

Q1. How can HALC contain all types, such as DC/constant, sinusoidal, and pulsating attack magnetic fields?

Q2. How can HALC contain a strong magnetic spoofing attack?

Q3. How can HALC remove the injected fake magnetic field B_{atk} from the original magnetic field $B_{original}$ even if the frequencies of B_{atk} and $B_{original}$ are same?

We start by mathematically modeling the attack at first.

Attack modeling: A Hall sensor can measure AC (i.e., time-dependent) and DC (i.e., constant) magnetic fields. Therefore, the AC and DC magnetic fields will have a proportional AC and DC voltage components in the sensor output V_{out} in Eqn. 5. Let us define the AC and DC voltage components coming from the AC and DC components of original input magnetic field $B_{original}$ by $V(t)$ and V^{dc}, respectively. Therefore, we can write the original component, $V_{original} = V(t) + V^{dc} + V^{null}$ in Eqn. 5.

Let us assume that the attacker can cause a DC error voltage E^c by injecting a constant magnetic field, a sinusoidal error voltage $E(t)$ by injecting sinusoidal magnetic fields, and a square error voltage $E^s(t)$ by injecting square magnetic fields. *Here, we consider an extreme scenario when the attacker injects all three patterns at the same time.* Therefore, the attack component in the output voltage of the compromised Hall sensor can be written as, $V_{atk} = E^c + E(t) + E^s(t)$. Moreover, Fourier analysis [31] of the square error voltage $E^s(t)$ shows that it has a DC portion E^s and a low and high frequency portion $\delta_l(t)$ and $\delta_h(t)$, respectively (i.e., $E^s(t) = E^s + \delta_l(t) + \delta_h(t)$). Therefore, the output, V_{out}, of the compromised Hall sensor during an attack can be written from Eqn. 5 as:

$$\begin{aligned} V_{out} &= V_{original} + V_{atk} \\ &= (V(t) + V^{dc} + V^{null}) + (E^c + E(t) + E^s(t)) \\ &= V_{original} + (E^c + E(t) + E^s + \delta_l(t) + \delta_h(t)) \end{aligned} \tag{6}$$

From Eqn. 6, it is apparent that V_{out} under attack has two components, namely *AC (i.e., time-dependent)* component, $V(t) + E(t) + \delta_h(t) + \delta_l(t)$, and *DC (i.e. constant)* component, $V^{dc} + V^{null} + E^c + E^s$. Please note that inside of the AC component, the AC attack component is $E(t) + \delta_h(t) + \delta_l(t)$, and inside of the DC component, the DC attack component is $E^c + E^s$.

Parallelism: In an extreme scenario, if the attacker injects AC and DC attack components simultaneously, a proper defense should contain these attack components in real-time without hampering the existing speed of the connected systems. However, there is no defense exists that can contain the AC and DC attack components inside of existing sensors. Moreover, a naive solution, which may *sequentially* handle the AC and DC attack components, may make the defense slow, hampering the real-time requirement of the defense. To solve this problem, our proposed defense HALC introduces two different cores - analog and digital cores, to *parallelly* handle the AC and DC attack components in the following ways:

(i) Analog core: The analog core removes the high and low frequency AC attack components, $E(t) + \delta_h(t) + \delta_l(t)$, from the V_{out} using different filtering techniques.

(ii) Digital core: The digital core removes the DC attack components, $E^c + E^s$, from the V_{out} using a novel algorithm.

Fig. 4 shows all blocks of the two cores, and Fig. 5 shows the details of each block of the two cores. Fig. 4 shows two paths- paths b-c-d and b-e-h - that host the two cores. The parallel handling of the AC and DC attack components by two separate cores in two different paths makes HALC faster than the sequential handling of each attack component. We mathematically discuss each core in the following sections with implementation details.

4.1 Analog Core

At first, the analog core needs to separate the AC and DC components from V_{out} to parallelly process them in two different paths - paths b-c-d and b-e-h. To separate the AC and DC components from V_{out}, the analog core uses two blocks - DC blocker and subtractor, which are discussed below.

4.1.1 ***DC Blocker.*** The DC blocker blocks the DC component (i.e., $V^{dc} + V^{null} + E^c + E^s$) of V_{out} and outputs only the AC component (i.e., $V(t) + E(t) + \delta_h(t) + \delta_l(t)$) at node ⓑ to path b-c-d (Fig. 4). It

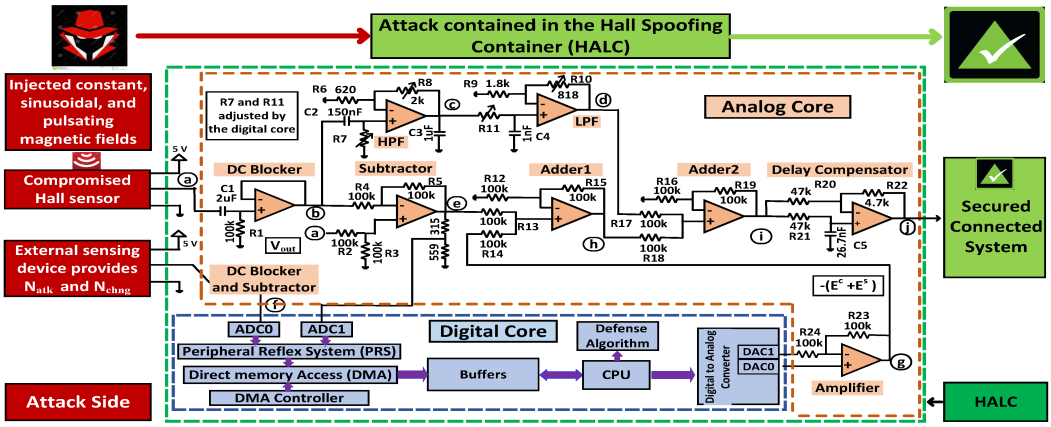

Figure 5: Implementation details of the analog and digital cores of the proposed Hall Spoofing Container (HALC).

uses a first-order high pass filter (Fig. 5) with R1 = 100 kΩ and C1 = 2 μF having a cut-off frequency, $f_c = 1/(2\pi R1C1) = 0.8$ Hz (i.e., it only blocks the DC signal).

4.1.2 ***Subtractor.*** The subtractor subtracts the AC component of V_{out} from V_{out} and outputs only the DC component of V_{out} (i.e., $V^{dc} + V^{null} + E^c + E^s$) at node ⓔ to path b-e-h (Fig. 4). The subtractor is implemented using a differential amplifier with a transfer function, V_+ - V_-, when R2=R3=R4=R5 (Fig. 5). Here, V_+ is the +ve input and V_- is -ve input of the amplifier.

Next, after separation, the AC component of V_{out} are processed by the high-pass and low-pass filters, and the DC component of V_{out} is processed by the digital core (see Section 4.2).

4.1.3 ***High-Pass Filter (HPF) & Low-Pass Filter (LPF).*** A first-order active HPF and a LPF are used to filter out the low-frequency (i.e., $E(t) + \delta_l(t)$) and high-frequency (i.e., $\delta_h(t)$) *attack components* from V_{out}, respectively, by keeping the original AC component $V(t)$ intact. The digital core, which works as an adjunct to the analog core (Section 4.2), can control the cut-off frequencies (i.e., f_c) of the HPF and LPF to filter out *only* low/high frequency *attack components*. In our implementation, the rheostats R7 and R11 (Fig. 5) are used to vary the cut-off frequencies of the HPF and LPF within 0 - 150 kHz (see Sections 4.3 and 7.1 for more details). Please note that the gain of the DC blocker, LPF, and HPF is ~1 (i.e., unity) and phase-shift is linear (i.e., constant) for all frequencies over f_c. *Therefore, path b-c-d does not add any non-linearity and unstability to the original AC component $V(t)$ in our design.*

4.1.4 ***Delay Compensator.*** The signal, V_{out} travels from node ⓐ to node ⓘ through different blocks. These blocks have capacitors and resistors with different values that introduce different *phase delays*. As a result, the signal at node ⓘ is a phase-delayed version of the signal from node ⓐ. For example, a 2.34 ms *leading* phase delay is present between node ⓐ and node ⓘ of our HALC. This could cause a 2.34 ms delay while taking a time-critical decision by the connected system. To compensate for the phase delay, a delay compensator is placed after node ⓘ. The delay compensator is an all-pass filter with a voltage gain, $A_v = 1$ at all frequencies and can create a specific phase shift. A *lagging* phase shift of 50.63° is implemented in our design that is equivalent to 2.34 ms of *lagging* delay. *As a result, the 2.34 ms of leading delay at node ⓘ is compensated to* ***zero*** *(See Fig. 8).* This ensures that HALC does not create any timing predictability issue to connected systems and preserves the hard real-time requirement of the overall system.

In summary, the analog core separates the AC component from the V_{out} and then contain the AC attack component (i.e., $E(t) + \delta_h(t) + \delta_l(t)$) by keeping the original AC component $V(t)$ intact.

4.2 Digital Core

The digital core uses a novel algorithm to generate a feedback signal $-(E^c + E^s)$, equal but opposite polarity to the injected DC attack component $E^c + E^s$. The digital core uses the generated feedback signal to nullify the injected DC attack component while keeping the original DC signal V^{dc} intact (see Eqn. 6). Moreover, it controls the cut-off frequencies of HPF/LPF of the analog core to remove AC attack components while keeping the original AC component $V(t)$ intact. To accomplish these two tasks, the digital core takes input from an external sensing device that is explained below.

External sensing device (ESD): As a Hall sensor under attack is a naive device, it cannot alone differentiate the original input magnetic fields ($B_{original}$) from the attacker's provided magnetic fields (B_{atk}). Therefore, the digital core uses an *external sensing device (ESD)*, which helps the compromised Hall sensor by *only* sensing the *presence* of the injected attack fields, B_{atk} (see Fig. 4 and 5). The ESD could be an external coil or another Hall sensor, which should be placed *side by side* with the compromised Hall sensor. *As the ESD can only sense the injected attack fields B_{atk}, the attacker cannot confuse the defense using multiple magnetic sources.*

Shield between ESD and $B_{original}$: *The next question is how to ensure that the ESD only picks the injected attack fields (B_{atk}), not the original fields ($B_{original}$).* Let's consider two scenarios. Firstly, suppose the original field is internal, such as for voltage/current Hall sensors (sensors 1-4, and 9-10 in Table 1). In that case the ESD only picks the injected external attack fields, not the original fields. Secondly, if the original fields and injected attack fields both are external to a sensor (sensors 5-8 in Table 1), there is a chance that the ESD can pick both the original and injected external fields. To prevent this happens, a shield is used between the ESD and the source of original magnetic fields, so that the ESD cannot pick up

the original fields but only can pick up the injected external fields. As the direction of the original fields is known to a designer, he can safely place a simple shield to prevent the original fields from going into the ESD (see Fig. 4 for the shield between ESD and $B_{original}$).

A question may arise if the shield can be bypassed by the attacker. Please note that the use of the shield is not to prevent attackers from influencing the target Hall sensor. However, the use of the shield is to prevent the original magnetic fields ($B_{original}$) from going into the ESD so that the ESD can only pick the injected attack fields (B_{atk}), not the original magnetic fields. Therefore, bypassing the shield with the B_{atk} by an attacker will not impact the defense because the ESD still can pick up the injected attack fields B_{atk}.

How the ESD is different from the recent works: Although the ESD is placed close to the compromised Hall sensor, there should always be a physical distance between the ESD and the compromised Hall sensor. Because of this physical distance, the ESD is unable to measure the exact *amplitude* of the external attack fields injected into the compromised Hall sensor. This is why we can not use the signal from the ESD to simply subtract the injected attack signals from the original signals to recover the original signal. Therefore, HALC uses the ESD differently compared to its use in the adaptive filtering technique found in recent work [28].

The ESD only provides the following two pieces of information to the digital core (see Fig. 4): (i) the attack notification signal, N_{atk}, which is only activated when the ESD senses the external attack field B_{atk}, and (ii) the notification signal, N_{chng}, when the ESD senses that the injected DC attack signal / component, $E^c + E^s$ changes. The N_{atk} and N_{chng} both do not consider any *absolute amplitude* of the attack signal, instead just only consider the *change/difference* in attack signal. Next, we discuss how the N_{atk} and N_{chng} are used by the digital core to generate the feedback signal -($E^c + E^s$) to nullify the injected DC attack signal ($E^c + E^s$).

Removing injected DC attack signal $E^c + E^s$: The digital core runs a novel algorithm 1 in a central processing unit (CPU) to remove the injected DC attack signal $E^c + E^s$. Let us summarize the algorithm first before introducing its technical implementation. When the ESD gives an attack notification signal (i.e., N_{atk}) that an attack happens at time t, the algorithm subtracts the DC component (see Eqn. 6) of *original signal* at time t from the previous DC component of *original signal* at time $t-1$ (i.e., data before the attack). The difference between the DC components during the attack and before the attack gives the amount of injected DC attack signal $E^c + E^s$ after the attack. The algorithm tracks this difference all the time and generates -($E^c + E^s$) to nullify the injected DC attack signal $E^c + E^s$. If the injected DC attack signal changes during an attack, the algorithm 1 can also track it from the previously calculated difference. It is noteworthy that algorithm 1 also tracks when the DC component of the original signal changes without any attack. This helps to correctly retrieve the original signal with and without attack. In summary, the continuous tracking of the DC component of the original signal before, after, and during the attack gives information of the injected DC attack signal, and this information is used to retrieve the DC component of original signal. *This idea and its implementation are absent in recent works [19, 23, 28, 37, 41, 47] that exist in the literature.* Next, we discuss the implementation (see Fig. 4 and 5) of algorithm 1 in detail.

4.2.1 ***ADC0 and ADC1.*** Two analog-to-digital converters - ADC0 and ADC1 provide data to the CPU (Fig. 5). ADC0 is connected with the ESD and provides the two information coming from the ESD, namely, notification signals N_{atk} and N_{chng} to the defense algorithm 1 running in CPU. Parallelly, ADC1 also provides the DC component (i.e., $V^{dc} + V^{null} + E^c + E^s$) of the V_{out} to algorithm 1 from node ⓔ. To reduce the power consumption, both ADCs use a low sampling frequency (35 kHz) at normal operating conditions (i.e., no attack), but start using a high sampling frequency (900 kHz) when an attack happens.

4.2.2 ***Peripheral Reflex System (PRS) and Direct Memory Access (DMA).*** To satisfy real-time requirement and reduce energy consumption, the workload of the CPU is shared with a peripheral reflex system (PRS) and direct memory access (DMA). The PRS and DMA handle the workload related to data movement from ADCs to CPU, whereas the CPU handles the workload related to running algorithm 1 and providing feedback signals to the analog core.

4.2.3 ***Central Processing Unit (CPU).*** The CPU runs the defense algorithm 1 and provides a feedback signal to nullify the DC attack signal (i.e., $E^c + E^s$) that is explained below.

Line 1-10: The CPU always checks the data coming from the ESD for the attack notification signal N_{atk} using the ADC0. Let's assume an attack happens at time t. Before any attack (at $t-1$ time), there is no presence of external spoofing magnetic fields. Therefore, the output of the ESD is zero, which indicates no attack happens (i.e., $N_{atk} = NO$). Moreover, when no attack happens, the data from ADC1 at $t-1$ is simply equal to $V^{dc}(t-1) + V^{null}(t-1)$ because no DC attack signals are present (i.e., $E^c + E^s = 0$) at node ⓔ. As no DC attack signals are present, the CPU does not need to nullify the DC attack signals $E^c + E^s$. That is why the CPU provides a NULL signal to digital-to-analog converters (DACs), and the DACs provide no feedback (0 V) at node ⓖ.

Line 11-16: However, when the attacker injects magnetic fields at time t, the ESD senses this injection that generates an attack notification signal, $N_{atk} = YES$. The ADC0 and ADC1 increase the sampling frequency from 35 kHz to 900 kHz to capture tiny changes of injected signals. During attack at time t, the data from ADC1 is equal to $V^{dc}(t) + V^{null}(t) + E^c(t) + E^s(t)$. As the DC component of the $V_{original}$ does not change, $V^{dc}(t) + V^{null}(t)$ at time t is equal to the previous value of $V^{dc}(t-1) + V^{null}(t-1)$ at time $t-1$. As $V^{dc}(t-1) + V^{null}(t-1)$ is known, the injected DC attack signal $E^c(t) + E^s(t)$ can be calculated as shown in line 16.

Line 17-20: After calculating the value of the injected DC attack signal $E^c(t) + E^s(t)$, the DACs (Fig. 5) generate a analog signal which is equal to the $E^c(t) + E^s(t)$. If the injected DC attack signal $E^c(t) + E^s(t)$ is positive, the amplifier in Fig. 5 is configured as inverting amplifier with a gain of -1 and outputs a feedback signal -($E^c(t) + E^s(t)$) at node ⓖ with the help of DACs. If $E^c(t) + E^s(t)$ is non-positive, the amplifier is configured as non-inverting amplifier with a gain of +1 and outputs a feedback signal +($E^c(t) + E^s(t)$) at node ⓖ with the help of DACs. The adder1 adds signals at node ⓖ with signals at node ⓔ and nullifies the injected DC attack signal $E^c(t) + E^s(t)$ from the V_{out} (see Fig. 4).

Line 21-29: After an attack happens at time t, the DC component of V_{out} sampled by ADC1 may change anytime after time t.

Algorithm 1: Proposed Defense Algorithm.

Input: Data from ADC0 and ADC1
Output: Feedback signal at node ⓖ to nullify the $E^c(t) + E^s(t)$

1 $t \leftarrow$ *attack happens*
2 Setup ADC0, and ADC1 $\leftarrow$ (12 bits, sampling freq. = 35kHz)
3 $V^{dc}(t-1) + V^{null}(t-1) \leftarrow$ *ADC1(t-1)*
4 **for** $t \leftarrow 1$ ***to*** ∞ **do**
5 $N_{atk} \leftarrow$ *ADC0(t-1)*
6 **if** $N_{atk} = NO$ **then**
7 $V^{dc}(t-1) + V^{null}(t-1) \leftarrow$ *ADC1(t-1)*
8 func_Notifies_system (no_attack_happens)
9 ADC0, ADC1 $\leftarrow$ sampling frequency 35 kHz
10 **Output** = *no feedback signal (i.e., 0V at node ⓖ)*
11 **else**
12 func_Notifies_system (attack_happens)
13 ADC0, ADC1 $\leftarrow$ sampling frequency 900 kHz
14 $V^{dc}(t) + V^{null}(t) + E^c(t) + E^s(t) \leftarrow$ *ADC1(t)*
15 $V^{dc}(t) + V^{null}(t) = V^{dc}(t-1) + V^{null}(t-1)$
16 $E^c(t) + E^s(t) \leftarrow$ *ADC1(t)* $-V^{dc}(t) - V^{null}(t)$
17 **if** $E^c(t) + E^s(t) > 0$ **then**
18 **Output** = *feedback signal -($E^c(t) + E^s(t)$) at node ⓖ to nullify the $E^c(t) + E^s(t)$*
19 **else**
20 **Output** = *feedback signal +($E^c(t) + E^s(t)$) at node ⓖ to nullify the -($E^c(t) + E^s(t)$)*
21 **if** *The data from ADC1 changes after t at t+n time* **then**
22 $N_{chng} \leftarrow$ *ADC0*(t+n)
23 **if** $N_{chng} = YES$ **then**
24 $V^{dc}(t+n) + V^{null}(t+n) = V^{dc}(t) + V^{null}(t)$
25 $E^c(t+n) + E^s(t+n) \leftarrow$ *ADC1(t+n)* $-V^{dc}(t+n) - V^{null}(t+n)$
26 **if** $E^c(t+n) + E^s(t+n) > 0$ **then**
27 **Output** = *feedback signal -($E^c(t+n) + E^s(t+n)$) at node ⓖ to nullify the $E^c(t+n) + E^s(t+n)$*
28 **else**
29 **Output** = *feedback signal +($E^c(t+n) + E^s(t+n)$) at node ⓖ to nullify the -($E^c(t+n) + E^s(t+n)$)*
30 **else**
31 $E^c(t+n) + E^s(t+n) \leftarrow E^c(t) + E^s(t)$
32 $V^{dc}(t) + V^{null}(t) =$ *ADC1(t+n)*$+E^c(t+n) + E^s(t+n)$
33 **if** $E^c(t+n) + E^s(t+n) > 0$ **then**
34 **Output** = *feedback signal -($E^c(t+n) + E^s(t+n)$) at node ⓖ to nullify the $E^c(t+n) + E^s(t+n)$*
35 **else**
36 **Output** = *feedback signal +($E^c(t+n) + E^s(t+n)$) at node ⓖ to nullify the -($E^c(t+n) + E^s(t+n)$)*
37 $V^{dc}(t-1) + V^{null}(t-1) = V^{dc}(t) + V^{null}(t)$

Let us assume the data from ADC1 changes at time $t+n$ where $n\epsilon\{1, 2, 3, .., \infty\}$. The change can happen under *two scenarios*: either the attacker changes the DC attack signal ($E^c + E^s$), or the DC component ($V^{dc} + V^{null}$) of the $V_{original}$ may change naturally. Under the *first scenario*, when the attacker changes the DC attack signal at time $t+n$, the ESD outputs a notification signal $N_{chng} = YES$, which is extracted from the ADC0 at $t+n$. As the DC component of the $V_{original}$ do not change under the first scenario, the previously saved DC component ($V^{dc}(t) + V^{null}(t)$) of the $V_{original}$ at time t must be equal to the most recent DC component ($V^{dc}(t+n) + V^{null}(t+n)$) of the $V_{original}$ at time $t+n$. Therefore, the injected DC attack signal ($E^c(t+n) + E^s(t+n)$) can be calculated using the data from ADC1 at time $t+n$ shown in line 25. The $E^c(t+n) + E^s(t+n)$ can be similarly used to generate feedback signals explained in line 17-20.

Line 30-37: Under the *second scenario*, when the DC component ($V^{dc} + V^{null}$) of the $V_{original}$ changes naturally at time $t+n$, the ESD outputs a notification signal $N_{chng} = NO$, which is extracted from the ADC0 at $t+n$. As the injected DC attack signal does not change under the second scenario, the previously saved DC attack signal ($E^c(t) + E^s(t)$) at time t must be equal to the most recent DC attack signal ($E^c(t+n)+E^s(t+n)$) at time $t+n$. The calculated $E^c(t+n)+E^s(t+n)$ is similarly utilized to generate feedback signals, which is explained in line 17-20. The DC component ($V^{dc}(t)+V^{null}(t)$) of the $V_{original}$ at time t are updated in line 32 that is used in line 37 to update $V^{dc}(t-1)+V^{null}(t-1)$. The updated $V^{dc}(t-1)+V^{null}(t-1)$ will be used in the next iteration at line 15.

In lines 21-29, two scenarios are considered, change due to attack and change naturally. A question might arise what will happen if a persistent attack coincides with a natural change. The answer lies in the execution time of lines 21-23. Let us denote the time required to execute lines 21-23 as p. Therefore, if the time difference between change due to attack and change naturally is greater than p, HALC can successfully detect both changes. For example, the time required to execute lines 21-23 is ~3 μs for our prototype. The time difference can be reduced to a lower value using a faster CPU resulting in a more robust defense against the error.

4.3 Controlling HPF & LPF of the analog core

The digital core decides the appropriate cut-off frequencies of the HPF and LPF after sensing the frequency of the injected attack magnetic fields (B_{atk}) using the *ESD*. If the injected attack magnetic field has a single frequency (i.e., single tone), the digital core configures the HPF and LPF in such a way that the HPF and LPF jointly act as a *band-stop* filter, which stops the injected single tone attack signals $E(t) + \delta_h(t) + \delta_l(t)$. If the injected attack magnetic field has multiple frequencies (i.e., multiple tones), the digital core configures the HPF and LPF in such a way that the HPF and LPF jointly act as a *band-pass* filter, which only passes the original input signal ($V_{original}$), removing the injected attack signals behind. In this way, with the help of the digital core, the HPF and LPF jointly eliminate the AC attack components ($E(t) + \delta_h(t) + \delta_l(t)$) of the injected V_{atk} from the V_{out} by keeping the $V_{original}$ intact.

4.4 Removing equal frequency attack signals

A concern may arise what will happen if the amplitude and frequency of the injected V_{atk} are same as the $V_{original}$. To handle this concern, a Hall sensor should be used in the differential configuration [19]. Referring to Section 2.3, let us assume two Hall elements D_1 and D_2 are placed close to each other in a differential configuration. During an attack, let us assume the two Hall elements D_1 and D_2 sense $B_{original1}$, B_{atk1} and $B_{original2}$, B_{atk2}, respectively, while measuring an original signal $B_{original}$. As $V_{original} \propto B_{original}$ and $V_{atk} \propto B_{atk}$, we can write the transfer function of the differential sensor during an attack from Eqn. 3 as,

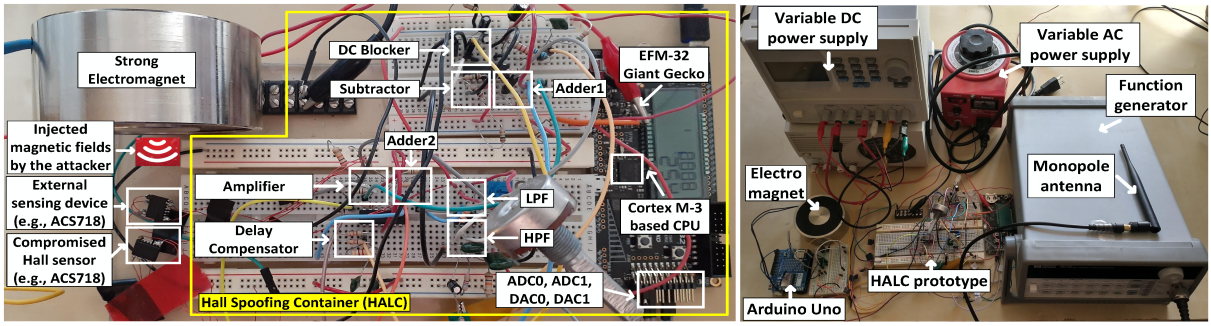

Figure 6: (Left) A prototype of our proposed HALC implemented in the lab. (Right) Different types of tools used in the testbed.

$$\begin{aligned} V_{out} &= k[B_{original1} + B_{atk1} - B_{original2} - B_{atk2}] + V^{null} \\ &= V_{original1} + V_{atk1} - V_{original2} - V_{atk2} + V^{null} \\ &= (V_{original1} - V_{original2}) + V^{null} + (V_{atk1} - V_{atk2}) \\ &= 2V_{original1} + V^{null} + E^c \end{aligned} \quad (7)$$

where $V_{original1} \approx$ - $V_{original2}$ (i.e., differential input). The B_{atk1} and B_{atk2} both have the same frequency because they are coming from the same attack signal. But they have different amplitudes because there is a small gap present between the two Hall elements D_1 and D_2 (refer to Section 2.3 for explanation). Therefore, the V_{atk1} and V_{atk2} have the *same* frequency, but they have *different* amplitudes (i.e., $B_{atk1} \neq B_{atk2}$). Therefore, the $(V_{atk1} - V_{atk2})$ results in a *constant* error E^c, which acts as a DC attack signal. Therefore, the defense algorithm 1 can remove the DC attack signal E^c from V_{out} in the same way that is already described in Section 4.2.3.

4.5 Novelty of HALC

The novelty of HALC compared to recent work [19, 23, 28, 37, 41, 47] is discussed here by answering the three questions from Section 4.

Q1. How can HALC contain all types, such as DC/constant, sinusoidal, and pulsating attack magnetic fields?

Answer: The Eqn. 6 models the constant, sinusoidal, and pulsating attack++ magnetic fields using the AC attack component $E(t)$ + $\delta_h(t)$ + $\delta_l(t)$ and DC attack component E^c + E^s. The AC attack component is contained by HPF and LPF of the analog core with the help of the digital core (see Sections 4.1 and 4.3). The DC attack component is contained by the digital core with a feedback signal E^c + E^s (see Section 4.2). In this way, HALC can contain constant, sinusoidal, and pulsating injected attack magnetic fields.

Q2. How can HALC contain strong magnetic spoofing attack?

Answer: Fig. 1 (Right) indicates that the attacker can spoof the output of the Hall sensor within its linear region close to its saturation voltage using a strong magnetic field. Please note that the digital core of HALC can generate the DC feedback signal E^c + E^s within the entire linear region of the Hall sensor close to the supply voltage (i.e., greater than the saturation voltage) to nullify the injected DC attack component. Moreover, the analog core can filter out the AC attack component within the entire operating region of the HPF and LPF. As the operating region of the HPF and LPF is greater than the linear region of the Hall sensor (i.e., the supply voltage of HPF/LPF is greater than the Hall sensor), the analog core can also contain the AC attack components within the entire linear region of the hall sensor close to the saturation voltage. In this way, HALC can contain strong magnetic spoofing attack.

Q3. How can HALC remove the injected fake magnetic field B_{atk} from the original magnetic field $B_{original}$ even if the frequencies of B_{atk} and $B_{original}$ are same?

Answer: The answer is already given in Section 4.4.

Another important point to note is that HALC only nullifies injected attack component V_{atk} in the sensor output V_{out} by keeping the original component $V_{original}$ intact. It is possible that original signals may contain anomalous data. HALC does not alter any anomalous data present in original signals as HALC only works on the injected attack component. The ESD is used to differentiate between original and attack components (refer to Section 4.2).

5 PERFORMANCE ANALYSIS

5.1 A prototype of the proposed HALC

A prototype of the proposed HALC is implemented in a lab setup as a proof-of-concept and is shown in Fig. 6 (Left). The DC blocker, subtractor, adder1, adder2, delay compensator, HPF, and LPF of the analog core are implemented using a low-power op-amp (part # TL084CN from Texas Ins.). The TL084CN has a JFET input stage that provides high slew rates, low input bias, and low offset currents. The values of discrete resistors and capacitors of the analog core are shown in Fig. 5. The digital core is implemented in an EFM-32 Giant Gecko board from Silicon Labs [6] that has Cortex M-3 based 32-bit CPU with PRS, ADCs, DACs, and DMA. It has an ultra low-power CPU with a 48 MHz clock.

5.2 Testbed

Different tools used in the testbed are shown in Fig. 6 (Right). We use a Hall sensor (part #ACS718) as the external sensing device (Fig. 6 (Left)). We test 10 different Hall sensors (see Table 1) of all types, such as unipolar, bipolar, open-loop, and closed-loop Hall sensors, from four different manufacturers in the testbed. As these sensors require different types of inputs (S_{in}), we use different sources to supply input signals to these Hall sensors. We use a variable AC/DC power supply to supply current/voltage as original input signals to the Hall sensors with serial no. 1-4, and 9-10 of Table 1. We use a permanent magnet [32] to supply magnetic fields as input signals to the Hall sensors with serial no. 5-8 of Table 1. We use an electromagnet [17] with an Arduino Uno as an attack

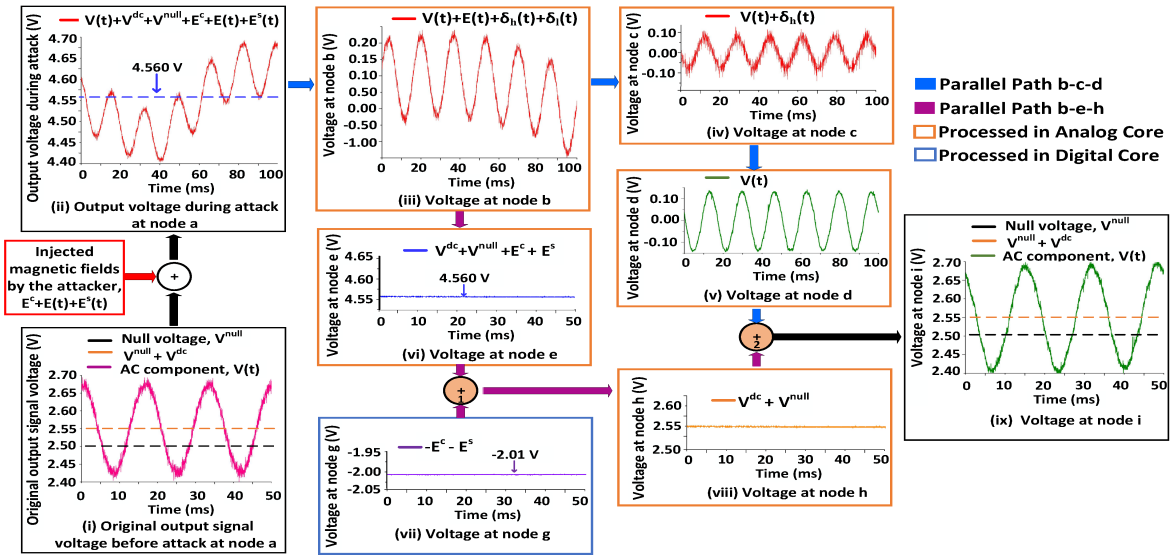

Figure 7: Signal analysis at all nodes of HALC. The signal at node ⓘ is a phase-delayed form of the input signal at node ⓐ.

tool to generate constant, sinusoidal, and pulsating attack fields using a pulse-width-modulation (PWM) technique. In addition, we use a function generator connected with a monopole antenna [16], which is also used as an attack tool, to radiate high and low frequency EMI signals. We can change the power and frequency of the electromagnet and EMI to generate weak and strong magnetic fields with different frequencies within a range of 0 - 9000 G in our testbed. The demonstration of the testbed is shown in the following link: https://sites.google.com/view/hallspoofingcontainer/home

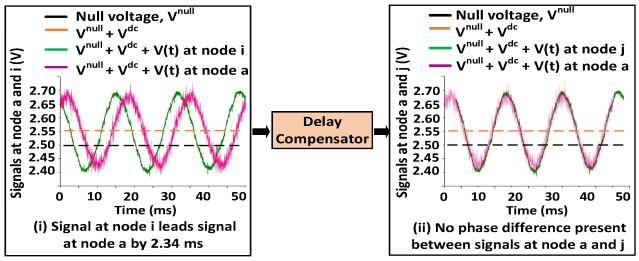

Figure 8: The delay between nodes ⓐ and ⓙ is compensated.

5.3 Justification of HALC

Now, we justify how HALC can contain the injected magnetic fields by analyzing signals at all of its nodes. We arbitrarily choose ACS718 from Table 1 as the target Hall sensor and connect it to HALC to analyze signals at all of its nodes. A 3 A peak-to-peak AC current of 60 Hz and a 0.5 A DC current are given as input signals (S_{in}) to the target sensor. Before any attack, the Hall sensor outputs the $V_{original}$ at node ⓐ (Fig. 7 (i)). A $V(t)$ = 300 mV peak-to-peak, V^{null} = 2.5 V, and V^{dc} = 50 mV are present in the $V_{original}$ before any attack. An electromagnet with a magnetic field density of 5600 G is used to inject constant (E^c), sinusoidal ($E(t)$) and pulsating ($E^s(t)$) external magnetic fields from 1 cm distance. We use 2 Hz as the frequency of injected $E(t)$ and $E^s(t)$ as an example. Fig 7 (ii) shows that the output of the Hall sensor at node ⓐ is shifted close to its saturation voltage (4.7 V) after the attack. The injection of the AC attack signal, $E(t) + E^s(t)$ distorts the $V_{original}$, and the injection of the DC attack signal, $E^c + E^s$ shifts the $V^{null} + V^{dc}$ of the $V_{original}$ from 2.55 V to 4.56 V. The DC blocker blocks only the DC components, $V^{dc} + V^{null} + E^c + E^s$ and outputs only the AC components, $V(t) + E(t) + \delta_h(t) + \delta_l(t)$ at node ⓑ (Fig. 7 (iii)).

The signals from node ⓑ propagate forward using two paths - path b-c-d and path b-e-h. Let us discuss the path b-c-d first. The HPF filters out the injected low-frequency error, $E(t) + \delta_l(t)$ and outputs $V(t) + \delta_h(t)$ at node ⓒ (Fig. 7 (iv)). The LPF filters out the injected high-frequency errors ($\delta_h(t)$) and outputs the AC component of the original input signal $V(t)$ at node ⓓ (Fig. 7 (v)).

Now, we discuss the path b-e-h. The subtractor outputs the overall DC components, $V^{dc} + V^{null} + E^c + E^s$, at node ⓔ (Fig. 7 (vi)). The value of $V^{dc} + V^{null} + E^c + E^s$ is 4.56 V. As the $V^{null} + V^{dc}$ of the original input signal is shifted from 2.55 V to 4.56 V, a DC error ($E^c + E^s$) of 2.01 V is injected by the attacker. Therefore, our proposed defense algorithm running in the digital core gives a feedback signal ($-E^c - E^s$) of -2.01 V at node ⓖ (Fig. 7 (vii)). The adder1 adds signals from node ⓔ and node ⓖ, and outputs only $V^{dc} + V^{null}$ with a value of 2.55 V at node ⓗ (see Fig. 7 (viii)).

The adder2 adds signals from nodes ⓓ and ⓗ and outputs a delayed version of the $V_{original}$ at node ⓘ (Fig. 7 (ix)). A 2.34 ms of leading delay is present between signals at node ⓐ and node ⓘ (Fig. 8 (i)). A delay compensator compensates for the delay and outputs the $V_{original}$ at node ⓙ (Fig. 8 (ii)).

Performance metric: If we can prove that the output of the target Hall sensor before an attack is *same* to the output of the target Hall sensor after an attack with HALC in a *point-by-point* fashion, we can claim that HALC is effective to prevent the spoofing attack. To quantify the similarity between signals before and after an attack, we calculate *correlation coefficient (C)* [29] between signals of node

ⓐ (i.e., before an attack) and node ⓙ (i.e., after an attack). If the correlation coefficient is close to unity, it indicates that the output of the target Hall sensor before and after an attack is same in a *point-by-point* fashion.

The value of C is 0.93 for this case, that is very close to unity (i.e., due to the presence of noise, C is slightly less than unity). This indicates that the signal at node ⓙ (i.e., after an attack) is *same* as the original signal at node ⓐ (i.e., before an attack) in a point-by-point fashion. This proves that HALC can separate V_{atk} from $V_{original}$ and successfully contain the spoofing attack inside of it.

5.4 Varying the amplitude of the input signals

We vary the amplitude of the input signals (S_{in}) to 10 different Hall sensors within their entire input range (Table 1(a)). We keep the frequency of the S_{in} fixed at 15/60 Hz (Table 1(b)). We calculate C for every different amplitudes and do an average of C for every sensor. The avg. of C is *greater than 0.93* when HALC is used compared to 0.2 when HALC is not used (Table 1(c)). This indicates that HALC works within the entire input range of every Hall sensor.

5.5 Varying the frequency of the input signals

We vary the frequency of input signals (S_{in}) to 10 different Hall sensors within their entire input frequency range (Table 1(d)). We keep the amplitude of the S_{in} fixed at 1 A/100 G/110 V (Table 1(e)). We calculate C for every different frequency and do an average of C for every sensor. The avg. of C is *greater than 0.93* for every sensor when HALC is used compared to 0.2 when HALC is not used (see Table 1(f)). This indicates that HALC works within the entire input frequency range of every Hall sensor.

5.6 Varying the magnetic field density of B_{atk}

In Sections 5.4 and 5.5, we keep the magnetic field density (i.e., ~5600 G) and distance (i.e., 1 cm) of the source of B_{atk} (i.e., electromagnet) fixed. In this section, we vary the magnetic field density of the source of B_{atk} from a fixed distance (1 cm) and keep the frequency and amplitude of the input signals (S_{in}) fixed at 60 Hz/15Hz and 1 A/100 G/110 V, respectively. We vary the magnetic field density from 0 G to 9000 G at frequency zero and calculate C for every case for 10 different Hall sensors. The C is *less than 0.2* before HALC is used. However, the C is *greater than 0.93* for every sensor (Fig. 9 (Left)) when HALC is used. This proves that HALC can satisfactorily contain *both the weak and strong (i.e., 0 - ~9000 G)* magnetic fields injected by the attacker.

5.7 Varying the frequency of the B_{atk}

We keep the magnetic field density of B_{atk} at 300 G and very the frequency of the B_{atk} within 0 to 150 kHz. We keep the frequency and amplitude of the input signals (S_{in}) fixed at 60 Hz/15Hz and 1 A/100 G/110 V, respectively. The C is *within 0.3 to 0.71* before HALC is used. However, the C is *greater than 0.92* for every sensor (Fig. 9 (Right)) when HALC is used. This proves that HALC can satisfactorily contain both the low and high frequency magnetic spoofing within 0 - 150 kHz. It is important to note that the range 0 - 150 kHz covers the entire input frequency range (see Table 1 (d)) supported by 10 different Hall sensors from 4 different manufacturers. The range also includes the same frequency as the input signals.

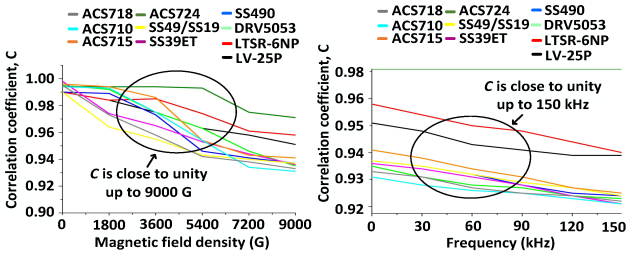

Figure 9: (Left) C with varying the magnetic field density of the B_{atk}. (Right) C with varying the frequency of the B_{atk}.

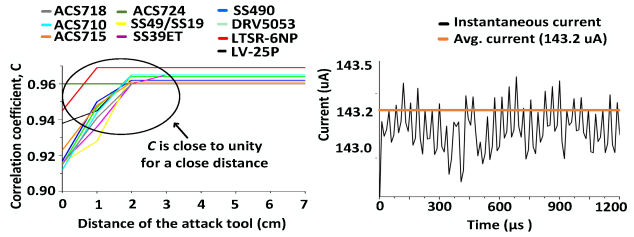

Figure 10: (Left) C with distance variation of the attack tool. (Right) The average and instantaneous current of digital core.

5.8 Varying the distance of the attack tool

We vary the distance of the attack tool (i.e., electromagnet, EMI) from the Hall sensor. We use a magnetic field density of 9000 G for B_{atk} and keep the frequency and amplitude of the input signals (S_{in}) fixed at 60 Hz/15Hz and 1 A/100 G/110 V, respectively. We vary the distance from 0 cm (very close) to 7 cm with an increment of 1 cm and calculate C for every case for all Hall sensors listed in Table 1. The value of C is greater than 0.91 for every case (Fig. 10 (Left)) when HALC is used. This proves that HALC can contain a magnetic spoofing attack from a very close distance.

5.9 Comparing HALC with a shield

We compare HALC with a MuMetal shield [12], which is a foremost industry-used specialized material for magnetic shielding. We keep the source of B_{atk} = 9000 G 1 cm away outside of the shield and keep Hall sensors 1 cm away inside of the shield. We vary the thickness of the shield and find that even a 0.9 inch thick shield cannot prevent the B_{atk} = 9000 G (i.e., low C in Table 1 (g), (h)). Because strong magnetic fields can saturate the MuMetal and diminish its shielding property, making it vulnerable to strong fields [24]. Next, we use HALC without the shield and find that C is close to unity (Table 1 (i)). This proves the efficacy of HALC over a shield.

5.10 Timing analysis of the analog core

The analog core is typically implemented by using a high-speed op-amp (Section 5.1) with very high slew rate, low rise-time, and high bandwidth. Therefore, the delay associated with the DC blocker, subtractor, adder1, and adder2 is typically less than 20 μs. The path b-c-d of the analog core comprises HPF and LPF. They introduce a delay in the form of phase shifts at nodes ⓒ, and ⓓ. The HPF creates a leading phase shift of +72.43°, and the LPF creates a lagging phase shift of -21.68°. The total phase shift occurs in path

Table 1: Testing Hall sensors with HALC for different amplitudes and frequencies of input signals, and with a MuMetal shield.

Sl.	Manufacturers	Part #	Polarity/Loop	Different amplitudes (a)	Frequency (b)	Avg. C (c)	Different frequencies (d)	Amplitude (e)	Avg. C (f)	C (0.4 in thick) (g)	C (0.9 in thick) (h)	Avg. C (i)
1	Allegro	ACS718 [3]	Bipolar/Open	1A, 5A, 10A, 15A, 20A	60 Hz	0.93	0 - 40kHz	1 A	0.93	0.43	0.55	0.95
2	Allegro	ACS710 [1]	Bipolar/Open	2A, 4A, 6A, 8A, 10A	60 Hz	0.93	0 - 120kHz	1 A	0.93	0.39	0.47	0.94
3	Allegro	ACS715 [2]	Unipolar/Open	1A, 5A, 10A, 15A, 20A	60 Hz	0.94	0 - 80kHz	1 A	0.93	0.43	0.51	0.93
4	Allegro	ACS724 [4]	Unipolar/Open	2A, 4A, 6A, 8A, 10A	60 Hz	0.97	0 - 120kHz	1 A	0.97	0.49	0.56	0.95
5	Honeywell	SS49/SS19 [15]	Bipolar/Open	100G,200G,300G,400G,500G	15 Hz	0.94	0 - 30Hz	100 G	0.93	0.36	0.46	0.96
6	Honeywell	SS39ET [13]	Bipolar/Open	100G,200G,300G,400G,500G	15 Hz	0.94	0 - 40Hz	100 G	0.94	0.39	0.49	0.95
7	Honeywell	SS494B [14]	Bipolar/Open	100G,200G,300G,400G,500G	15 Hz	0.94	0 - 30Hz	100 G	0.94	0.48	0.56	0.94
8	Texas Ins.	DRV5053 [7]	Bipolar/Open	100G,200G,300G,400G,500G	15 Hz	0.94	0 - 20Hz	100 G	0.94	0.54	0.59	0.95
9	LEM	LTSR6-NP [9]	Bipolar/Closed	1A, 2A, 3A, 4A, 5A	60 Hz	0.96	0 - 100kHz	1 A	0.96	0.33	0.43	0.96
10	LEM	LV 25 P [10]	Bipolar/Closed	30V, 50V, 70V, 90V, 110V	60 Hz	0.96	0 - 25kHz	110 V	0.96	0.37	0.51	0.94

b-c-d is +72.43° + (-21.68°) = +50.74° leading. The +50.74° phase shift is equivalent to 2.36 ms of delay between signals at node ⓐ and node ⓓ. *This 2.34 ms of delay is compensated to **zero** by using a delay compensator (see Section 4.1.4). This preserves the hard real-time requirement of the overall system.*

5.11 Constant computational complexity

We implement the necessary filters in the analog core using first-order circuits. If these filters were implemented in the digital core using *higher-order* FIR or IIR filters, the CPU would require higher-order operations with high computational complexity. *HALC utilizes the analog and digital cores in such a way that the CPU does not need to handle higher-order arithmetic operations.* Instead, it handles first-order tasks that ensure a constant computational complexity of O(1). Moreover, the complexity of the defense algorithm 1 does not grow with the input data, and it remains constant independent of the different input signals/magnetic fields.

5.12 Timing analysis of the digital core

Broadly speaking, the digital core of HALC handles the following four tasks: (i) It samples signals using ADCs, (ii) It transfers sampled data to internal variables using DMAs, (iii) It processes the sampled signals by using an algorithm 1, and (iv) It generates DC feedback signals ($-E^s$-E^c) at node ⓖ using DACs. In this section, we calculate the time required to execute each of these tasks by considering the clock cycles required for each of these tasks. Four different clocks are used for the ADCs, DMAs, CPU, and DACs in the digital core. The frequencies of these clocks and the execution time required for each task are tabulated in Table 2.

The minimum and maximum execution time of tasks 1, 2, and 4 are constant as they don't involve the CPU. Task 3 involves the CPU and requires a minimum execution time of 31 μs and a maximum execution time of 43 μs. The CPU requires minimum and maximum execution time when a minimum and maximum number of cache miss occurs, respectively. The digital core requires a maximum of 105 μs or a minimum of 93 μs in total to generate the DC feedback signals -(E^s+E^c) to contain the DC attack component.

Table 2: Timing analysis of the digital core

Task #	Clock name	Clock freq.	Min. time	Max. time
Task 1	ADC clock	11 MHz	16 μs	16 μs
Task 2	DMA clock	48 MHz	19 μs	19 μs
Task 3	CPU clock	48 MHz	31 μs	43 μs
Task 4	DAC clock	500 kHz	27 μs	27 μs
			93 μs (total)	105 μs (total)

5.13 Attack containment in hard real-time

It is guaranteed that the digital core will provide feedback signals within a maximum of 105 μs of delay after signal changes at node ⓔ. The digital core executes the four tasks sequentially, and there is no task-scheduling involved in the process. Therefore, the delay associated with the digital core is always deterministic. Moreover, the digital core typically handles the low-frequency DC signals, which vary less slowly than the introduced delay/latency by the digital core. Therefore, a 105 μs of delay is negligible compared to the rate of signal change in path b-e-h. *In addition, the phase-shift introduced by the analog core is taken care of by the delay compensator.* Therefore, the attack is contained in hard real-time.

5.14 Low-power HALC

The digital core consumes 0.5 mW and 0.3 mW average power when an attack happens and does not happen, respectively. When there is no attack, the digital core runs in energy-saving mode. The power is measured using an energy profiler app of the Simplicity Studio IDE [30]. The average and instantaneous current are shown in Fig. 10 (Right). The spike of the instantaneous current occurs during the ADC conversion. Moreover, the analog core consumes 1.4 mW of average power with or without an attack. Therefore, the total power consumed by HALC is ~1.7-1.9 mW, which is compatible with power ~ 10 mW [5] consumed by the Hall sensor itself.

5.15 Low-cost HALC and easy to integrate

HALC uses a cheap (~$2) Hall sensor as the ESD. The total cost of our prototype is ~$12, which is comparable with the sensor cost (~$2 - $70). *However, as ~$12 is the cost of the prototype, the actual cost will be much less in mass level production using SoC fabrication.* HALC can be connected with the target Hall sensor in a plug-&-play manner after fabricating HALC in a chip.

6 EVALUATION OF HALC

We evaluate HALC in two practical systems: a grid-tied solar inverter and a rotation-per-minute (RPM) system.

6.1 Grid-tied solar inverter

Grid-tied solar inverters are typically used as central inverters in solar/industrial plants or shopping malls. They widely use Hall sensors to measure AC and DC current. A 140 Watt inverter from Texas Ins. [8], which is a miniature version of a practical inverter, is used in the testbed to evaluate HALC. This inverter has a Hall effect current sensor with a part # ACS712ELCTR-20A-T with a *magnetic*

shield around it. At first, we use our attack tool to inject constant, sinusoidal, and pulsating magnetic fields with a magnetic field density of 7000 G into the Hall sensor from a 1 cm distance. This drives the Hall sensor close to saturation and forces the inverter to shut down, causing a denial-of-service (DoS) attack even with a shield. Next, we connect HALC with the Hall sensor and repeat the same experiment (Fig. 11). At this time, nothing happens to the inverter, and it continues working without any disruption.

6.2 Rotation-per-minute (RPM) system

The RPM system is used in ICSs to measure the rotational speed of any rotating structure, such as a motor shaft, wheel. We use a motor shaft in our testbed with a Hall sensor having part # SS490. A small permanent magnet (part # HE510-ND) is mounted on the motor shaft. When the motor shaft rotates, the permanent magnet also rotates. The Hall sensor can sense the change of magnetic fields coming from the motor shaft (i.e., permanent magnet) and use this information to count motor shaft rotations. At first, we provide a 100 RPM speed to the motor shaft. Then we inject magnetic fields with a magnetic field density of 5000 G from a 1 cm distance into the Hall sensor. As a result, the Hall sensor cannot measure the number of rotations correctly. Next, we connect HALC with the Hall sensor and repeat the same experiment. Now, the Hall sensor starts measuring the RPM correctly without any error (Fig. 12).

We find that if the C is < 0.8, a DoS attack happens in both the solar inverter and the RPM system. As HALC can keep the C close to unity, it can prevent the DoS and spoofing attack on Hall sensors.

7 LIMITATIONS

There are a few limitations of HALC. These limitations exist because of the limitations of the practical hardware.

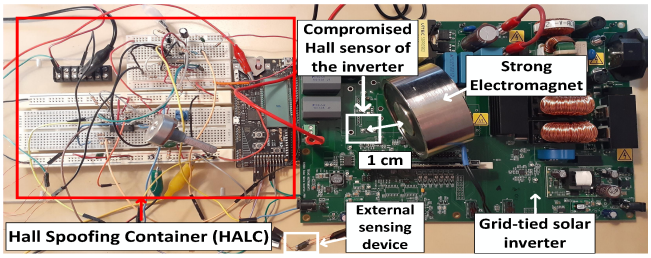

Figure 11: HALC can prevent the magnetic spoofing attack on the grid-tied solar inverter.

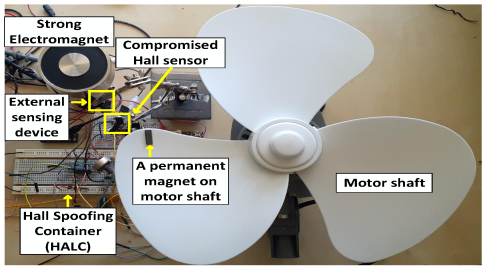

Figure 12: HALC is connected with the Hall sensor of the RPM system to prevent magnetic spoofing.

7.1 Non-zero settling time of rheostat

The digital rheostats R7 and R11 used in the design have a non-zero settling time. We use MCP4252 [11] to implement rheostats R7 and R11 in our prototype (see Section 4.1.3). MCP4252 has an SPI interface that supports a 10 MHz clock. The total time required to calculate R7 and R11 and write these values to the MCP4252 chip using a 10 MHz SPI port is ~3.5 μs. The time required to settle down the wiper of the digital rheostat is ~240 μs. Therefore, the total settling time of the rheostat is 240 + 3.5 = 243.5 μs in our prototype. If the attacker changes the injected magnetic fields within 243 μs, the timeliness of the defense will not be guaranteed. The settling time of the rheostat results from its parasitic capacitance. Therefore, the settling time can be reduced from 243 μs to a lower value using a rheostat having lower parasitic capacitance, which can be achieved using JFETs instead of traditional MOSFETs in a rheostat.

7.2 Upper limit magnetic field density of B_{atk}

HALC can work up to a magnetic field density of ~9000 G. The upper limit ~9000 G originates from the amplifier in Fig. 5, which cannot provide the feedback signal -($E^c + E^s$) more than the supply voltage (i.e., 5 V). By increasing the supply voltage from 5 V to a higher value, the upper limit of the B_{atk} can be increased.

7.3 Upper limit frequency of B_{atk}

The prototype of HALC can prevent a B_{atk} with frequencies of 0 Hz to 150 kHz. The upper limit of 150 kHz can be increased beyond 150 kHz by increasing the maximum upper limits of rheostats R7 and R11. To increase the maximum upper limits of rheostats, multiple digital rheostats can be connected in series. However, it may increase the settling time of the rheostats.

7.4 Multiple co-located Hall sensors

In the present state of the design, if multiple sensors are co-located, HALC should be used with each co-located sensor separately.

8 RELATED WORK AND LIMITATIONS

To the best of our knowledge, no state-of-the-art work provides a defense against a strong magnetic spoofing attack on Hall sensors. However, few related works exist for other sensors that can not be applicable to Hall sensors for the following reasons.

Trippel et al. [41] proposed randomized and 180^0 out-of-phase sampling to nullify acoustic spoofing signals injected into MEMS accelerometers. Randomized sampling samples at random times and 180^0 out-of-phase sampling takes 2 samples with 180^0 out of phase within the resonant frequency period to nullify the spoofing signals. These defenses will fail in two scenarios: (i) When the spoofing signal has the same frequency as the original signal being measured because randomized sampling will nullify both the spoofing and original signals. (ii) When the spoofing signal is a DC/constant signal because randomized sampling cannot filter out a DC signal.

Cheng et al. [23] and Alexander [19] from Allegro Microsystems proposed differential Hall sensors to nullify common-mode spoofing signals. This technique would work for weak magnetic spoofing but does not work against strong magnetic spoofing. The reasons behind this limitation are already explained in Section 2.3 in detail.

Table 3: Summary of the strength of HALC.

Strength	Values
values of injected B_{atk}	up to ~ 9000 G
frequencies of injected B_{atk}	0 - 150 kHz
proximity of the attack tool	< 1 cm
power consumption	~ 1.7 - 1.9 mW
cost	~ $12
latency	93 μs - 105 μs
constant, sinusoidal, pulsating B_{atk}	✓
spoofing signal having same frequency as original signal	✓
Works within entire input signal (S_{in}) range	✓

Kune et al. [28] proposed adaptive filtering to estimate the spoofing attack signal first and then subtract the estimated attack signal from the original signal to clean up the original signal. This technique will fail in two scenarios: (i) Because of the physical distance between the adaptive filter and the compromised Hall sensor, the adaptive filter cannot measure the exact amplitude of the external attack fields. This is why we can not simply subtract the estimated attack signals from the original signals to recover the original signal. (ii) This technique uses higher order FIR filters for adaptive filtering that is computationally expensive and may hamper the real-time requirement of the defense (refer to Section 5.11 for details).

Zhang et al. [47] used a Support Vector Machine (SVM), and Roy et al. [37] proposed a non-linearity tracing classifier to contain the inaudible voice commands injected into MEMS microphones in ultrasonic range. These defenses have following limitations: (i) They will work only for spoofing signals located in ultrasonic frequency band (> 20kHz), which has a clear separation from the audible voice signals (< 20 kHz). As the spoofing signal may share the same band as the original signal in Hall sensors, these defenses don't work for Hall sensors. (ii) They will not work for DC spoofing signals.

The works in [19, 23, 28, 41] are sensor-level and [37, 47] are system-level defenses. There are other system-level defenses. Shoukry et al. [39] proposed PyCRA that only can detect an attack but cannot prevent it. Cardenas et al. [22] and Urbina et al. [43] incorporated the knowledge of the physical system under control to detect an attack on ICSs. But their approaches cannot contain the attack. Again, Shoukry et al. [40] proposed to reconstruct the state to recover from a sensor spoofing attack using the satisfiability modulo theory (SMT) that can not be implemented in the *in-sensor* hardware.

Moreover, machine learning techniques and other system-level defenses require complex computations to converge for attack detection and recovery, requiring powerful hardware resources. Therefore, they are not suitable for low-power real-time sensor systems with constrained resources. *In addition, they may not work against a time-varying magnetic spoofing as a time-varying signal may create oscillations between two safe states of the controller, and they are incapable of handling these oscillations in real-time.*

HALC is novel in the sense that it can *detect and contain* a strong magnetic spoofing up to ~9000 G of any type, such as constant/DC, sinusoidal, and pulsating magnetic fields, in real-time and can keep the connected system running during the attack. A summary of the strength of HALC is given in Table 3.

9 CONCLUSION

We have presented HALC, a defense against a weak and strong magnetic spoofing attack on Hall sensors. HALC can not only detect but also contain the weak and strong magnetic spoofing of different types, such as constant, sinusoidal, and pulsating fields, in hard real-time. HALC utilizes the analog and digital cores to achieve a constant computational complexity O(1) and keep the existing data processing speed of the connected system undisturbed. We have done extensive analysis of HALC on 10 different Hall sensors from 4 different manufacturers and proved its efficacy against the magnetic spoofing attack. We have demonstrated that our proposed defense is low-power and low-cost and can be implemented in the sensor hardware domain. Moreover, we have evaluated the effectiveness of HALC in two practical systems. Our results from these experiments prove that HALC can accurately and reliably detect and mitigate the magnetic spoofing attack in hard real-time. To the best of our knowledge, HALC is the first of its kind that can provide defense against a weak/strong magnetic spoofing on the Hall sensor. Finally, we believe that HALC has the potential to be adopted for other passive sensors in general to protect them from a spoofing attack.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and our shepherd Prof. Aaron Schulman for their valuable comments that greatly helped to improve this paper. This work was partially supported by the National Science Foundation (NSF) under awards CMMI-1739503 and ECCS-2028269. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding agencies.

REFERENCES

[1] [n.d.]. *ACS710 datasheet.* https://www.allegromicro.com/~/media/Files/Datasheets/ACS710-Datasheet.ashx. (Accessed: 03-22-2022).
[2] [n.d.]. *ACS715 datasheet.* https://www.allegromicro.com/~/media/Files/Datasheets/ACS715-Datasheet.ashx. (Accessed: 03-22-2022).
[3] [n.d.]. *ACS718 datasheet.* https://www.allegromicro.com/~/media/Files/Datasheets/ACS718-Datasheet.ashx. (Accessed: 03-22-2022).
[4] [n.d.]. *ACS724 datasheet.* https://www.allegromicro.com/~/media/Files/Datasheets/ACS724-Datasheet.ashx. (Accessed: 03-22-2022).
[5] [n.d.]. *Allegro MicroSystems : Hall-effect sensors consume very little power.* https://www.eetimes.com/allegro-microsystems-hall-effect-sensors-consume-very-little-power/. (Accessed: 03-22-2022).
[6] [n.d.]. *Cortex-M3 Reference Manual: EFM32 Microcontroller Family.* https://www.silabs.com/documents/public/reference-manuals/EFM32-Cortex-M3-RM.pdf. (Accessed: 03-22-2022).
[7] [n.d.]. *DRV5053 datasheet.* https://www.ti.com/document-viewer/DRV5053/datasheet. (Accessed: 03-22-2022).
[8] [n.d.]. *Grid-tied Solar Micro Inverter with MPPT.* https://www.ti.com/tool/TIDM-SOLARUINV. (Accessed: 03-22-2022).
[9] [n.d.]. *LTSR 6-NP datasheet.* https://www.lem.com/sites/default/files/products_datasheets/ltsr_6-np.pdf. (Accessed: 03-22-2022).
[10] [n.d.]. *LV 25-P datasheet.* http://www.farnell.com/datasheets/51633.pdf. (Accessed: 03-22-2022).
[11] [n.d.]. *MCP4252 datasheet.* https://ww1.microchip.com/downloads/en/DeviceDoc/22060b.pdf. (Accessed: 03-22-2022).
[12] [n.d.]. *MU METAL SPECIFICATIONS.* http://www.mu-metal.com/technical-data.html. (Accessed: 03-22-2022).
[13] [n.d.]. *SS39ET datasheet.* https://www.digikey.com/htmldatasheets/production/43186/0/0/1/SS39ET-49E-59ET-Series-Datasheet.pdf. (Accessed: 03-22-2022).
[14] [n.d.]. *SS490 datasheet.* https://prod-edam.honeywell.com/content/dam/honeywell-edam/sps/siot/en-us/products/sensors/magnetic-sensors/linear-and-angle-sensor-ics/ss490-series-linear-sensor-ics/documents/sps-siot-sensors-linear-hall-effect-ics-ss490-series-datasheet-005843-2-en-ciid-50358.pdf. (Accessed: 03-22-2022).

[15] [n.d.]. SS49/SS19 datasheet. https://www.digikey.com/htmldatasheets/production/809995/0/0/1/SS49-SS19-Series-Install-Instr.pdf. (Accessed: 03-22-2022).
[16] [n.d.]. *Tektronix 119-6609-00.* https://www.testequipmentdepot.com/tektronix/accessories/cables-hardware/attachments/flexible-monopole-antenna-119660900.htm?ref=gbase. (Accessed: 03-22-2022).
[17] [n.d.]. *uxcell DC12V 100KG Force Electric Lifting Magnet Electromagnet Solenoid Lift Holding.* https://www.amazon.ca/uxcell%C2%AE-Solenoid-Electric-Holding-Electromagnet/dp/B07FKNJ7CZ?th=1. (Accessed: 03-22-2022).
[18] Andrea Ajbl, Marc Pastre, and Maher Kayal. 2013. A fully integrated Hall sensor microsystem for contactless current measurement. *IEEE Sensors Journal* 13, 6 (2013), 2271–2278.
[19] Latham Alexander. 2019. *Common Mode Field Rejection in Coreless Hall-Effect Current Sensor ICs.* https://www.allegromicro.com/-/media/files/application-notes/an269123-common-mode-field-rejection-in-coreless-current-sensor-ics.pdf. (Accessed: 03-22-2022).
[20] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2020. Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter. In *29th USENIX Security Symposium (USENIX Security 20).* USENIX Association, 1273–1290. https://www.usenix.org/conference/usenixsecurity20/presentation/barua
[21] Ronald Newbold Bracewell and Ronald N Bracewell. 1986. *The Fourier transform and its applications.* Vol. 31999. McGraw-Hill New York.
[22] Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. 2011. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security.* 355–366.
[23] Xingguo Cheng, Zhenjun Sun, Xiaoyan Wang, and Sheng Liu. 2014. Open-loop linear differential current sensor based on dual-mode Hall effect. *Measurement* 50 (2014), 29–33.
[24] Laurent Chiesi, Karim Haroud, John A Flanagan, and Rade S Popovic. 1997. Chopping of a weak magnetic field by a saturable magnetic shield. *Sensors and Actuators A: Physical* 60, 1-3 (1997), 5–9.
[25] Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. 2016. Dancing on the lip of the volcano: Chosen ciphertext attacks on apple imessage. In *25th {USENIX} Security Symposium ({USENIX} Security 16).* 655–672.
[26] S Geetha, KK Satheesh Kumar, Chepuri RK Rao, M Vijayan, and DC Trivedi. 2009. EMI shielding: Methods and materials—A review. *Journal of applied polymer science* 112, 4 (2009), 2073–2086.
[27] Ersan Kabalci and Yasin Kabalci. 2018. A wireless metering and monitoring system for solar string inverters. *International Journal of Electrical Power & Energy Systems* 96 (2018), 282–295.
[28] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. 2013. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy.* IEEE, 145–159.
[29] Werner Kutzelnigg, Giuseppe Del Re, and Gaston Berthier. 1968. Correlation coefficients for electronic wave functions. *Physical Review* 172, 1 (1968), 49.
[30] Silicon Labs. [n.d.]. *Energy Profiler.* https://docs.silabs.com/simplicity-studio-5-users-guide/1.0/using-the-tools/energy-profiler/. (Accessed: 12-10-2021).
[31] BP Lathi and Zhi Ding. 1998. Modern analog and digital communication systems. *Third generation OXFORD University Press, NEW YORK* (1998), 50–51.
[32] Littelfuse. [n.d.]. *Magnets and Actuators.* https://www.littelfuse.com/~/media/electronics/datasheets/magnetic_actuators/littelfuse_magnetic_actuators_datasheet.pdf.pdf. (Accessed: 03-22-2022).
[33] Hrishikesh Mehta, Ujjwala Thakar, Vrunda Joshi, Kirti Rathod, and Pradeep Kurulkar. 2015. Hall sensor fault detection and fault tolerant control of PMSM drive system. In *2015 International Conference on Industrial Instrumentation and Control (ICIC).* IEEE, 624–629.
[34] Dong-Hyun Nam, Woo-Beom Lee, You-Sik Hong, and Sang-Suk Lee. 2013. Measurement of spatial pulse wave velocity by using a clip-type pulsimeter equipped with a Hall sensor and photoplethysmography. *Sensors* 13, 4 (2013), 4714–4723.
[35] Radivoje Popovic and Christian Schott. 2007. Sensor for detecting the direction of a magnetic field in a plane. US Patent 7,235,968.
[36] Edward Ramsden. 2011. *Hall-effect sensors: theory and application.* Elsevier.
[37] Nirupam Roy, Sheng Shen, Haitham Hassanieh, and Romit Roy Choudhury. 2018. Inaudible Voice Commands: The Long-Range Attack and Defense. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18).* USENIX Association, Renton, WA, 547–560.
[38] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. 2013. Non-invasive spoofing attacks for anti-lock braking systems. In *International Conference on Cryptographic Hardware and Embedded Systems.* Springer, 55–72.
[39] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. 2015. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.* 1004–1015.
[40] Yasser Shoukry, Pierluigi Nuzzo, Nicola Bezzo, Alberto L Sangiovanni-Vincentelli, Sanjit A Seshia, and Paulo Tabuada. 2015. Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving. In *2015 54th IEEE Conference on Decision and Control (CDC).* IEEE, 3804–3809.
[41] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. 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, 3–18.
[42] Yuan-Pin Tsai, Kun-Long Chen, and Nanming Chen. 2011. Design of a Hall effect current microsensor for power networks. *IEEE Transactions on Smart Grid* 2, 3 (2011), 421–427.
[43] David I Urbina, Jairo A Giraldo, Alvaro A Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. 2016. Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.* 1092–1105.
[44] Martin H. Weik. 2001. *active sensor.* Springer US, Boston, MA, 21–21. https://doi.org/10.1007/1-4020-0613-6_258
[45] Martin H. Weik. 2001. *passive sensor.* Springer US, Boston, MA, 1235–1235. https://doi.org/10.1007/1-4020-0613-6_13692
[46] Yue Xu, Hong-Bin Pan, Shu-Zhuan He, and Li Li. 2012. A highly sensitive CMOS digital Hall sensor for low magnetic field applications. *Sensors* 12, 2 (2012), 2162–2174.
[47] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.* 103–117.

10 APPENDIX

10.1 Generation of magnetic fields

Generation of a constant magnetic field: We use a permanent magnet (part # H33 [32]) having 10900 G of B and a solenoid having 100 turns and 3 cm radius with variable DC power supply to generate a constant magnetic field.

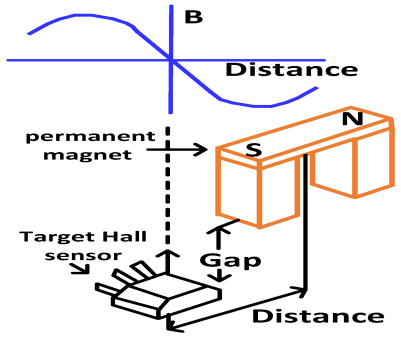

Figure 13: A specially crafted structure to generate sinusoisal magnetic field using two permanent magnets.

Generation of a sinusoidal magnetic field: A sinusoidal magnetic field variation ($B_m \sin \omega t$) can be created by two ways. The first way is to use two magnets crafted in a particular way that is shown in Fig. 13. In our experiment, this magnet pair is crafted using two permanent magnets (part # H33 [32]) having 10900 G magnetic field density. We slide this magnet pair from left to right from 3 cm distance periodically to generate a sinusoidal magnetic field. The angular frequency (ω) of this sinusoidal magnetic field is equal to the sliding rate of the magnet pair moving from left to right.

The second way is to use an electromagnet or solenoid. We sinusoidally vary the input voltage to the electromagnet by using the pulse-width-modulation technique. We use an electronic switch MOSFET (part # P7N20E) with an Arduino control to switch an electromagnet (part # WF-P80/38 [17]) (Fig. 14).

Generation of a square pulsating magnetic field: A square pulsating magnetic field variation ($sgn(B_m \sin \omega t)$ can be created by

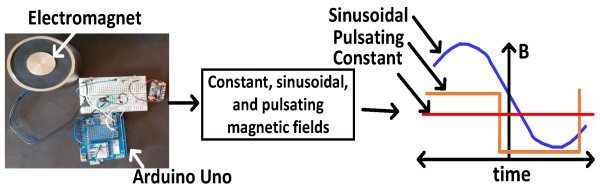

Figure 14: An electromagnet with Arduino control can generate constant, sinusoidal, and pulsating magnetic fields.

switching an electromagnet/solenoid on/off periodically. In our experiment, we use an electronic switch MOSFET (part # P7N20E) to switch an electromagnet (part # WF-P80/38 [17]) on/off to generate a square pulsating magnetic field Fig. 13 (Right). The angular frequency (ω) of the injected square pulsating magnetic field is calculated from the switching rate of the electromagnet.