IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2022, No. 4, pp. 438–462. DOI:10.46586/tches.v2022.i4.438-462

PreMSat: Preventing Magnetic Saturation Attack on Hall Sensors

Anomadarshi Barua and Mohammad Abdullah Al Faruque

University of California, Irvine, Irvine, U.S.A. {anomadab,alfaruqu}@uci.edu

Abstract.
Spoofing a passive Hall sensor with fake magnetic fields can inject false data into the downstream of connected systems. Several works have tried to provide a defense against the intentional spoofing to different sensors over the last six years. However, they either only work on active sensors or against externally injected unwanted weak signals (e.g., EMIs, acoustics, ultrasound, etc.), which can only spoof sensor output in its *linear* region. However, they *do not* work against a strong magnetic spoofing attack that can drive the passive Hall sensor output in its *saturation* region. We name this as the saturation attack. In the saturation region, the output gets flattened, and no information can be retrieved, resulting in a denial-of-service attack on the sensor.

Our work begins to fill this gap by providing a defense named PreMSat against the saturation attack on passive Hall sensors. The core idea behind PreMSat is that it can generate an internal magnetic field having the *same* strength but in *opposite polarity* to external magnetic fields injected by an attacker. Therefore, the generated internal magnetic field by PreMSat can nullify the injected external field while preventing: (i) intentional spoofing in the sensor's *linear region*, and (ii) saturation attack in the *saturation region*. PreMSat integrates a low-resistance magnetic path to collect the injected external magnetic fields and utilizes a finely tuned PID controller to nullify the external fields in real-time. PreMSat can prevent the magnetic saturation attack having a strength up to ∼4200 A-t within a frequency range of 0 Hz–30 kHz with low cost (∼$14), whereas the existing works cannot prevent saturation attacks with any strength. Moreover, it works against saturation attacks originating from *any type*, such as constant, sinusoidal, and pulsating magnetic fields. We did over 300 experiments on ten different industry-used Hall sensors from four different manufacturers to prove the efficacy of PreMSat and found that the correlation coefficient between the signals before the attack and after the attack is greater than 0.94 in every test case. Moreover, we create a prototype of PreMSat and evaluate its performance in a practical system — a grid-tied solar inverter. We find that PreMSat can satisfactorily prevent the saturation attack on passive Hall sensors in real-time.

Keywords: Hall sensors · PID controller · Saturation region · Real-time defense

1 Introduction

A Hall sensor can measure magnetic fields from the surrounding environment and generates a proportional voltage at its output [Ram11]. Hall sensors are pervasive in many safety-critical systems, ranging from industrial controllers to power systems, computers to home automation, and automobiles to aircraft [TCC11, XPHL12, NLHL13, CCCS01, CLH+09, hal, CWAF17]. Over the last three decades, Hall sensors have been technically improved in terms of stability, accuracy, and linearity [Gil06]; however, to the best of our knowledge, designers still do not consider security as one of the important requirements while designing hall sensors. The vulnerability of Hall sensors has recently been exposed by few works [SMTS13, BAF20]. In these works, the attacker uses an external magnetic field to spoof

Received: 2022-04-15 Accepted: 2022-06-15 Published: 2022-08-31

Hall sensors located in a solar inverter and anti-lock braking system, resulting in a denial-of-service (DoS) attack on the connected power grids and automotive systems, respectively.

A Hall sensor has a Hall element [GN86], which outputs a voltage proportional to the sensed magnetic fields to a differential amplifier. The input-output characteristic of a differential amplifier is linear. If the output voltage from the Hall element is small, the differential amplifier typically works in its linear region. However, if the output voltage from the Hall element is large, the differential amplifier cannot work in its linear region and is driven to its saturation region [PP02]. In the saturation region, the input-output characteristic gets flattened; hence, no information can be recovered, causing a DoS attack on the Hall sensor. An attacker can use this knowledge to drive the differential amplifier to its saturation region by using a strong external magnetic field. We name this attack as the *saturation attack*. Please note that here, *sensor saturation* does not refer to *magnetic saturation* [HJBA20]. Moreover, Hall sensors are broadly two types: active and passive. Passive Hall sensors are naive devices; they send signals to the upper level without checking the integrity of the signals that makes them vulnerable to external fake magnetic fields.

Recent works [BAF22, TWX+17, CSWL14, Ale19, KBC+13, ZYJ+17, RSHC18] may prevent spoofing a sensor in its linear region to some extent. However, to the best of our knowledge, no work in literature can prevent a *saturation attack* on *passive* Hall sensors. Therefore, we provide a defense for passive Hall sensors against a saturation attack. We name it as PreMSat: Preventing Magnetic Saturation, which can prevent a saturation attack on passive Hall sensors[1] in real-time and also prevent spoofing in the linear region.

The core idea behind PreMSat is that it can generate an internal magnetic field having the *same* strength but in *opposite polarity* to the external magnetic field injected by an attacker. As a result, the internal magnetic fields generated by PreMSat can nullify the externally injected magnetic fields with two consequences: (i) it prevents magnetic spoofing in the linear region, and (ii) it prevents the saturation attack. Please note that only a portion of injected magnetic fields may contribute to the saturation attack on Hall sensors. Therefore, PreMSat introduces the following three techniques: (i) PreMSat provides a low-resistance magnetic path, made with ferrite core, to collect the contributing portion of the externally injected fields, (ii) PreMSat provides a *secondary sensor*, mounted in the ferrite core, to measure the strength and polarity of the contributing external field, and (iii) PreMSat uses a *proportional-integral-derivative (PID) controller* and a *primary coil* to generate an internal magnetic field equal to the contributing external field to nullify it. The PID controller is well-tuned so that it takes a settling time of 23 μs to generate the stable internal magnetic field. The low settling time of the PID controller fulfils the real-time requirement of PreMSat. We demonstrate the efficacy of PreMSat on a grid-tied inverter proving its real-time effectiveness against the saturation attack on practical systems. We present a prototype of PreMSat that nullifies external fields with a strength up to $\sim$ 4200 A-t. It seems that a strong attacker may overcome the defense prototype with a field higher than 4200 A-t. However, the strength of the prototype theoretically can be increased to any higher limit using stronger hardware that may prevent a stronger attacker.

Contributions: Our main technical contributions in this paper are listed below:

1. We propose PreMSat that can protect a passive Hall sensor against: (i) spoofing attacks on linear regions and (ii) saturation attacks on saturation regions. It works against any type, such as constant, sinusoidal, and pulsating magnetic fields, in real-time.

2. We create a prototype of PreMSat and show its effectiveness through experiments on ten different Hall sensors from four different manufacturers. We consider different types, namely unipolar, bipolar, open-loop, and closed-loop Hall sensors to prove that PreMSat is a general defense technique against the saturation attack on passive Hall sensors.

3. We evaluate the efficacy of PreMSat on a real-world practical system — a grid-tied inverter and demonstrate that PreMSat prevents the DoS attack on a practical system.

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

Demonstration: The demonstration of the proposed defense is shown in the following link: https://sites.google.com/view/preventingmagneticsaturation/home

2 Preliminaries

2.1 The physics of the Hall sensor

The physics of a typical Hall sensor is shown in Fig. 1 (left). The Hall sensor [Pau12] has a Hall element, which is a p-type semiconductor [OHN+08]. Let us denote the thickness of the Hall element by d. A DC voltage bias is applied across the Hall element that causes a bias current, I_{Bias} flowing through the Hall element along the +X axis. Let us assume a magnetic field/flux density, B is present along the +Z axis. The magnetic field, B exerts a Lorentz force, F [Hub09] on electrons and holes of the Hall element that deflects them to either side of the Hall element along the +Y axis [MVM09]. As electrons and holes move sidewards along the +Y axis, a voltage is generated between two sides of the Hall element along the +Y axis. The voltage is known as Hall voltage, V_H and is expressed as:

$$V_H = k(\frac{I_{Bias}}{d} \times B) \tag{1}$$

where k is the Hall coefficient. Typically I_{Bias}, d and k are held constant; therefore, V_H is proportional to the magnetic field density B. In this way, a Hall sensor can sense a magnetic field B and convert it to a useful electrical signal V_H.

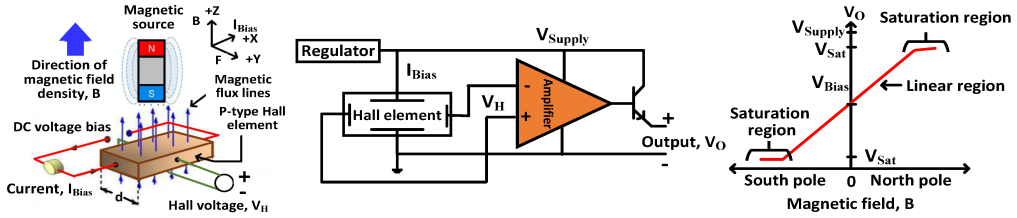

Figure 1: (left) The physics of a typical Hall sensor. (middle) Hall sensor electronics. (right) The linear and saturation regions of a typical Hall sensor.

2.2 Hall sensor electronics

Hall sensors have other electronics in addition to a Hall element that is shown in Fig. 1 (middle). The output of the Hall element is given to a signal conditioning block, which has a differential amplifier. A differential amplifier amplifies the output voltage of the Hall element (i.e., V_H) and also removes the common-mode noises from V_H. Common-mode noises are unwanted signals that are present at +ve and -ve input leads of the differential amplifier with respect to analog ground. Moreover, a voltage regulator is used to provide a stable bias current I_{Bias} to the Hall element. The stable I_{Bias} keeps the output V_H proportional to the input magnetic field B in Eqn. 1. It is clear from this discussion that Hall sensors don't have dedicated hardware to prevent a spoofing attack on them.

2.3 Linear and saturation regions of a Hall sensor

The sensed magnetic field B in Eqn. 1 can be either +ve or -ve depending upon its polarity (i.e., north/south pole). Therefore, the differential amplifier's output, denoted as V_O in Fig. 1 (middle), can go either +ve or -ve, thus requiring two (i.e., both +ve and -ve) power supplies. To avoid using two power supplies, a fixed bias voltage, V_{Bias} is added to the differential amplifier. Therefore, a +ve/-ve magnetic field B can drive the V_O to upper/lower position from the V_{Bias} and $V_O = V_{Bias}$ when B is zero. The term V_O works in the linear region, and the V_O cannot exceed the limit imposed by the power supply. In fact, the V_O will begin to flatten before the power supply limits are reached. This flattened region is known as the saturation region, denoted by V_{Sat}, which is illustrated in Fig. 1 (right). *Please note that the exact value of input field B cannot be recovered while the*

differential amplifier's output V_O is in the saturation region. Moreover, saturation occurs in the differential amplifier, not in the Hall element. Therefore, a strong spoofing magnetic field can drive the Hall sensor to saturation without damaging the Hall element.

A naive approach to prevent a saturation attack is to increase the saturation voltage of a differential amplifier. However, this is not a complete solution because the attacker can still spoof a Hall sensor in its linear region. We discuss the advantages of PreMSat over increasing the saturation voltage of a differential amplifier in Sections 4.3.2 and 5.10. In addition, the detection of the saturation attack can be done by checking the output V_O stuck to the +ve/-ve limits; however, this will not help to recover information from the saturation region and cannot prevent spoofing in the linear region of the amplifier.

2.4 Active and passive Hall sensor

An active Hall sensor [Wei01a] can measure signals transmitted by the sensor that were reflected, refracted, or scattered by the physical environment. A passive Hall sensor [Wei01b] can only measure natural emissions coming from the physical environment. PyCRA [SMY+15] works only for active sensors but not for passive Hall sensors. Therefore, we aim to provide a defense against the saturation attack on passive Hall sensors.

2.5 Proportional-integral-derivative (PID) controller

A PID controller [Pan12] is a closed-loop control system that generates a feedback signal to minimize an error. It continuously calculates an error, $e(t) = r(t)$ - $u(t)$, as the difference between a desired setpoint $r(t)$ and a feedback signal $u(t)$. It continuously updates $u(t)$ to minimize the error $e(t)$ so that $u(t)$ achieves a value closer to desired setpoint $r(t)$. It uses proportional, integral and derivative operations on $e(t)$ following Eqn. 2.

$$u(t) = K_p e(t) + K_i \int_0^t e(t)\,dt + K_d \frac{de(t)}{d(t)} \tag{2}$$

where K_p, K_i, and K_d are proportional, integral, and derivative gain, respectively. The values of K_p, K_i, and K_d should be tuned optimally so that the PID controller remains stable with a minimum overshoot of $u(t)$. Usually, tuning takes place in the s-domain for a continuous-time PID controller or in the z-domain for a discrete-time PID controller. The s-domain is used to solve the continuous-time differential equation, whereas the z-domain is used to solve a discrete-time equation with Z-transformation [FK77].

3 Saturation attack model and its consequences

The important four components of the saturation attack model are explained below:
1. Assumptions on attackers: The attacker can be a disgruntled employee or a guest, who is not allowed to modify the target Hall sensor like a lunch-time attack [GGK+16].
2. Attacker's goals: The attacker only uses high power magnetic energy from a distance to *noninvasively* spoof and inject malicious signals into the Hall sensor to drive it to its saturation region. Therefore, the attack can be seen as a *noninvasive physical attack*.
3. Attack tool and cost: The attacker can use an electromagnet [ama] to generate strong fields for a saturation attack. The electromagnet can be controlled with a MOSFET [pow] and an Arduino [ard] using pulse-width modulation (PWM) technique to generate different types, such as constant, sinusoidal, pulsating magnetic fields, with different frequencies. The total cost of attack tools is $<$ \$60, which will not be increased for higher strength or frequency of the magnetic fields. By changing the duty cycle and frequency of the PWM signal, it is possible to increase or decrease the strength or frequency of the magnetic fields at the same cost. Moreover, the attack tools are easily available on Amazon/Digikey. Therefore, the saturation attack is realistic by a strong attacker.
4. Sensor shield: A sensor shield may or may not be present around a Hall sensor. The saturation attack is strong enough to drive the Hall sensor to its saturation region even in the presence of a shield. We compare PreMSat with a shield in Section 5.9 in detail.

Consequences of the saturation attack: As Hall sensors are critical parts of safety-critical systems (i.e., autonomous vehicles, smart grids, etc.), the consequences of a saturation attack on a target Hall sensor can be catastrophic. A similar incident is found in the literature where an attacker injects fake magnetic fields into Hall current sensors located in a solar inverter and drives the hall sensor to its saturation. As a result, the solar inverter shuts down itself because the saturated Hall sensor cannot provide correct values from the micro-grid, causing a blackout in the micro-grid [BAF20]. Another incident demonstrates a *disruptive attack* on a Hall sensor located in an anti-lock braking system (ABS) of a vehicle, resulting in a possible brake failure [SMTS13]. An example of a saturation attack other than on a Hall sensor is demonstrated by Shin et al. [SKKK17] on lidars used in an autonomous vehicle. The outcome of this attack is the loss of control of the vehicle. Park et al. [PSS+16] saturate a drop sensor of a medical infusion pump using an IR laser. This attack makes the drop sensor insensitive to any fluid drops. *All these examples indicate that saturation attacks can cause a DoS attack on critical sensors and have catastrophic consequences in terms of loss of human life and monetary resources.* Therefore, a defense (i.e., like PreMSat) is necessary against a saturation attack on sensors.

4 The defense scheme - PreMSat

The core idea behind PreMSat is that it can generate an internal magnetic field having the *same* strength but in *opposite polarity* to the externally injected magnetic fields. *As a result, the internal magnetic fields can nullify the external magnetic fields.* Before designing PreMSat, it is required to discuss few important concepts related to electromagnetism that will be conceptualized in PreMSat.

4.1 Contributing direction of the magnetic fields on Hall sensors

The Hall element in the Hall sensor is not sensitive to all directions of a magnetic field. Rather, the Hall element is sensitive to a particular magnetic field direction that actually contributes to the generation of the Hall voltage V_H. We bring Proposition 1 below to state the contributing direction of magnetic fields on Hall sensors.

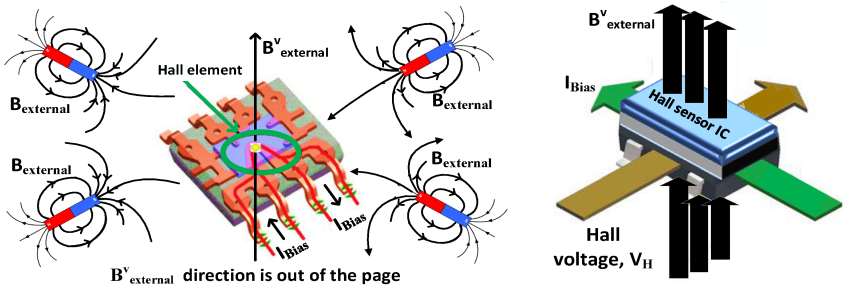

Figure 2: For multiple sources of $B_{external}$, the vector summation of vertical components of $B_{external}$, which is perpendicular to I_{Bias}, only contributes to the Hall voltage, V_H.

Proposition 1: The Hall element located in the Hall sensor is sensitive to only the vertical component of the magnetic fields that is perpendicular to the bias current I_{Bias}.

Explanation of Proposition 1: According to Lorentz Force [Hub09], the Hall voltage V_H in Eqn. 1 is only sensitive to magnetic fields B, which is perpendicular to bias current I_{Bias}. This phenomena is also illustrated in Fig. 1 (left), where magnetic fields B is in +Z axis and the bias current I_{Bias} is flowing along +X axis. Therefore, the Hall element is only sensitive to the vertical component of magnetic fields that is perpendicular to I_{Bias}.

Terminology: Let us denote the external magnetic fields injected by the attacker by $B_{external}$. If the attacker uses multiple magnetic sources to generate $B_{external}$, the vector summation of all the vertical components of the $B_{external}$ will contribute to the Hall voltage, V_H. Let us denote the magnitude of the summation of all vertical components of $B_{external}$

perpendicular to I_{Bias} by $B^v_{external}$. Fig. 2 depicts the presence of the $B^v_{external}$ in the case of multiple magnetic sources. As $B^v_{external}$ only contributes to the V_H, PreMSat should need to generate an internal magnetic field having the same magnitude of $B^v_{external}$ in opposite polarity to nullify the $B^v_{external}$. Let us denote the magnitude of the internal magnetic field generated by PreMSat by $B_{internal}$, where the $B_{internal}$ should be equal to the $B^v_{external}$ in opposite polarity to nullify the $B^v_{external}$.

4.2 Internal magneto-motive force (MMF) generated by PreMSat

The attacker needs a *magnetic source* (i.e., electromagnet, electromagnetic interference - EMI, etc.) to generate external magnetic fields $B_{external}$ to drive the target Hall sensor to its saturation region. The strength of the magnetic source is quantified by magneto-motive force (MMF) [Hub09]. For defense, PreMSat needs to use an internal magnetic source that can generate the exact MMF to provide an internal field $B_{internal}$ to nullify the $B^v_{external}$. Let us denote the internal MMF generated by PreMSat by $MMF_{internal}$.

Primary coil: PreMSat implements a circular *ferrite core* [KSG+99] with a coil winded in spiral direction to generate the $MMF_{internal}$. As the ferrite core has circular shape, it can also be called by a *toroid*. The term *toroid* is used interchangeably with *ferrite core* in this paper. Let us denote the winding coil, which generates the $MMF_{internal}$, by the *primary coil*. The construction of the toroid with the primary coil is shown in Fig. 3. The $MMF_{internal}$ generated by the primary coil is expressed in Eqn. 3.

$$MMF_{internal} = N_{primary} I_{primary} \tag{3}$$

where $N_{primary}$ is the total number of turns in the primary coil and $I_{primary}$ is the current flowing through the primary coil. The $MMF_{internal}$ generates the internal magnetic field $B_{internal}$, which can be expressed as follows for a toroid:

$$B_{internal} = \frac{\mu_r \mu_o N_{primary} I_{primary}}{2\pi r} = \frac{\mu_r \mu_o MMF_{internal}}{2\pi r} \tag{4}$$

where μ_o is the magnetic permeability of air, μ_r is the relative permeability of a ferrite core, and r is the radius of a toroid. The generated $B_{internal}$ should be equal to the $B^v_{external}$ but in opposite polarity to nullify the $B^v_{external}$. This will be discussed in the next section.

4.3 Primary coil nullifies the $B^v_{external}$

As discussed earlier, the primary coil generates a $B_{internal}$, which is equal to the $B^v_{external}$ but in opposite polarity to nullify the $B^v_{external}$. PreMSat generates the $B_{internal}$ by addressing the following two important questions:

Q1. How can PreMSat generate $B_{internal}$ having *equal magnitude* to the $B^v_{external}$?

Q2. How can PreMSat align the $B_{internal}$ in *opposite direction* to nullify the $B^v_{external}$?

These two questions are addressed below in Sections 4.3.1, 4.3.2, and 4.3.3.

4.3.1 Generating the $B_{internal}$ having equal magnitude to the $B^v_{external}$

At first, PreMSat needs a methodology to sense the *magnitude and direction* of the $B^v_{external}$ correctly to generate a correct $B_{internal}$. The steps to accomplish this is explained below.

■ ***1. Introducing a secondary sensor:*** As a Hall sensor under attack is a naive device, it cannot alone differentiate between the natural input magnetic fields and the attacker's provided external magnetic fields $B^v_{external}$. Let us denote the natural *input* magnetic field by B_{input} that actually needs to be measured by the Hall sensor. To differentiate the B_{input} from the $B^v_{external}$, PreMSat uses a *secondary sensor* placed in the toroid. Please note that the secondary sensor is used only to sense the external magnetic field $B^v_{external}$. The secondary sensor is placed close to the target Hall sensor so that it can sense the external magnetic fields injected into the target Hall sensor (see Fig. 3 and 4). The secondary sensor can be implemented using either a Hall sensor or a magnetic coil.

The next question is how the secondary sensor actually differentiates the natural input magnetic fields B_{input} from the externally injected magnetic fields $B^{v}_{external}$. Let us answer the above question by considering the following two scenarios.

First scenario: When the natural input field B_{input} is internal, the secondary sensor only senses the injected external magnetic field $B^{v}_{external}$ (Fig. 3). This happens for voltage/current Hall sensors, where the natural input magnetic field is generated internally from an internal voltage/current signal inside of the Hall sensor (sensors 1-6 in Table 2).

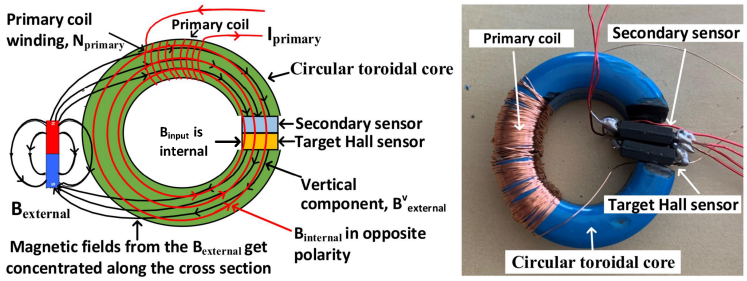

Figure 3: (left) The toroid hosts the target Hall sensor and the secondary sensor and provides a magnetic path to collect the injected $B_{external}$. Here, the natural input magnetic field B_{input} is internal. (right) The implementation of the toroid.

Second scenario: When the natural input field B_{input} and the injected external field $B^{v}_{external}$ both are external, there is a chance that the secondary sensor can sense both the natural and injected external fields (sensors 7-10 in Table 2). To prevent this from happening, a shield between the secondary sensor and the source of natural input field is used in PreMSat. This concept is illustrated in Fig. 4. We use a shield having six segments (i.e., i - vi in Fig. 4) made of a ferromagnetic material in such a way that it guides the external natural input field B_{input} not to go to the secondary sensor but only to go to the target Hall sensor. The segment (i) prevents the B_{input} to induce in the circular toroid. The segment (ii) guides the B_{input} to penetrate through the target Hall sensor for being measured. The segment (iii) provides a path to close the loop of the B_{input}. And the segments (iv), (v) and (vi) will be needed if the source of $B_{external}$ is placed at the same side of the source of B_{input}. Because in this scenario, the $B_{external}$ may influence the segments (i) and (iii) and may bypass the secondary sensor. To prevent this from happening, the segments (iv), (v), and (vi) are used to guide the $B_{external}$ to go to the circular toroid core without influencing the segments (i), (iii) and the B_{input}.

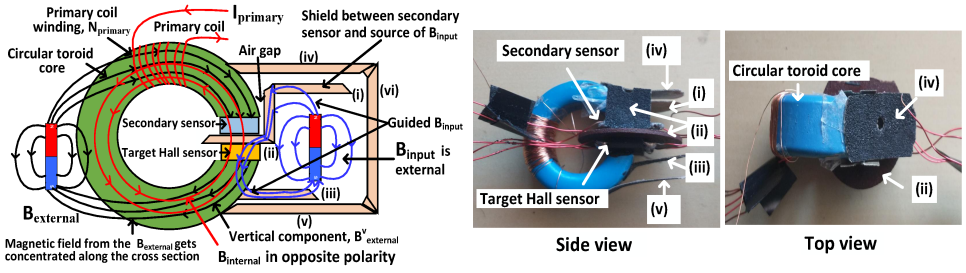

Figure 4: (left) The toroid hosts the target Hall sensor and the secondary sensor and provides a magnetic path to collect the injected $B_{external}$. Here, the natural input magnetic field B_{input} is external. (right) Side and top views of the implemented toroid.

Please note that the construction of the shield may vary for different requirements and locations of the B_{input} depending on its different use-cases. It is possible that more or fewer segments may be needed other than the above six segments. For example, the segment (vi) can be safely omitted if the attacker cannot access this side to place the source of $B_{external}$. The sizes of the shield's segments are not large compared to the toroid. Therefore, the structure shown in Fig. 4 (right) will work in most applications, such as

proximity sensing, and throttle angle sensing. However, few applications where moving parts are involved, such as brushless motors, may find it difficult to install the segments.

As the direction of the natural field B_{input} is known to the designer, he can always design a shield to prevent the natural field from going into the secondary sensor. Moreover, as the strength of the natural field is known to the designer, he can use a shield with proper ferromagnetic material to ensure that the natural field cannot penetrate the shield.

A further question may arise if the attacker can bypass the shield. 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 input magnetic fields (B_{input}) from going into the secondary sensor. Therefore, bypassing the shield with the $B_{external}$ by an attacker will not impact the defense because the secondary sensor and target Hall sensor can still sense the injected $B_{external}$. Moreover, if a strong injected $B_{external}$ penetrates the shield, that would not be a problem. Because in that case, the secondary sensor will still sense the injected $B_{external}$ by the attacker and won't sense the natural input field B_{input}.

■ ***2. Sensing $B^v_{external}$ from the $B_{external}$***: PreMSat uses a magnetic path to collect the vertical components $B^v_{external}$ from the $B_{external}$. The circular ferrite core in PreMSat provides that magnetic path. We bring Proposition 2 below to explain this concept.

Proposition 2: As the ferrite core in PreMSat has very low magnetic resistance compared to the air, practically speaking, most of the magnetic fields from $B_{external}$ will get concentrated along the cross-section of the ferrite core [Her91, Con19, Shi14].

Explanation of Proposition 2: The way how the circular ferrite core provides a magnetic path to collect the vertical components $B^v_{external}$ is shown in Fig. 3 and 4. When single/multiple sources of $B_{external}$ are present near the target Hall sensor, the $B_{external}$ needs to overcome the air gap present between the target Hall sensor and the source of $B_{external}$. As air has a very low magnetic permeability (e.g., $4\pi 10^{-7}$ Wb/A-t.m), the air gap present between the target Hall sensor and the $B_{external}$ works as a magnetic path having very high resistance. Therefore, the magnetic field lines coming from the $B_{external}$ change their normal path and try to find a new path having a low magnetic resistance. The circular ferrite core provides the very low resistive magnetic path to the $B_{external}$. In numbers, the relative magnetic permeability of ferrites can vary between 1150 to 25000 [fera]. In other words, the magnetic resistance of the ferrite core is 1150 - 25000 times less than air. As the ferrite core has very low magnetic resistance compared to air, practically speaking, most of the external magnetic fields from the $B_{external}$ get concentrated along the cross-section of the ferrite core, hence influencing the field pattern of the $B_{external}$.

Vertical projection of $B_{external}$ onto the Hall sensor: As the $B_{external}$ is concentrated along the cross-section of the ferrite core, if we could place the target Hall sensor in the cross-section of the ferrite core, the $B_{external}$ will be projected onto the target Hall sensor vertically. The reason behind this is that as the ferrite core has a circular shape, the concentrated fields $B_{external}$ along the circular core will be vertical to any *plane* placed in the cross-section of the circular core. The idea is illustrated in Fig. 3 and 4. A small gap is created to place the target Hall sensor in the cross-section of the ferrite core. Therefore, the concentrated $B_{external}$ will act as the $B^v_{external}$ to the target Hall sensor as the target Hall sensor is placed in the cross-section of the circular ferrite core.

The secondary sensor is also placed together with the target Hall sensor in the gap of the circular ferrite core. This is illustrated in Fig. 3 and 4. As the secondary sensor is placed together with the target Hall sensor, the same $B^v_{external}$ passes through the secondary sensor. Therefore, the secondary sensor sees the same amount of $B^v_{external}$, similar to the target Hall sensor. In this way, the secondary sensor placed in the ferrite core can sense the $B^v_{external}$ injected by the attacker.

■ ***3. Generating a voltage proportional to the $B^v_{external}$ by the secondary sensor***: PreMSat uses a Hall sensor as the secondary sensor for simplicity. A magnetic coil could also be used as the secondary sensor. As a Hall sensor is used as a secondary sensor, after

sensing the $B^v_{external}$, the secondary sensor generates a Hall voltage following Eqn. 1. Let us denote the generated Hall voltage in the secondary sensor by $V_{secondary}$.

Types of $B^v_{external}$***:*** We consider a strong attacker who can use constant, sinusoidal, and pulsating fields for a saturation attack because all other patterns can be derived from these three basic fields (i.e., Fourier transformation [BB86]). Therefore, we discuss how $V_{secondary}$ changes for the constant, sinusoidal, and pulsating magnetic fields. This information on $V_{secondary}$ is required to design algorithm 1, which can prevent the saturation attack generating from any type of $B^v_{external}$. Let us define the constant, sinusoidal and pulsating magnetic fields mathematically in Eqn. 5.

$$B^v_{external} = \begin{cases} C; & \text{constant field,} \\ B_{amplitude} \sin \omega t; & \text{sinusoidal field,} \\ B_{amplitude}\{sgn(\sin \omega t)\}; & \text{square pulsating field.} \end{cases} \tag{5}$$

where C is a constant, ω is the angular frequency and $B_{amplitude}$ is the magnitude of the injected magnetic field, and sgn is the signum function. If we use $B^v_{external}$ from Eqn. 5 in Eqn. 1, we can calculate the $V_{secondary}$, which is graphically illustrated in Fig. 5.

The $V_{secondary}$ ***is proportional to the*** $B^v_{external}$***:*** Eqn. 1 shows that the term V_H is proportional to the magnetic fields B present in the +Z direction. Therefore, the secondary sensor also generates the $V_{secondary}$, which is proportional to the vertical components of the externally injected magnetic fields, previously denoted by $B^v_{external}$. Hence, the $V_{secondary}$ has the shape and frequency equal to $B^v_{external}$ that is illustrated in Fig. 5.

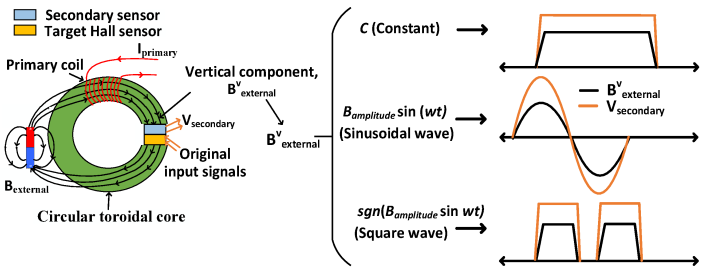

Figure 5: The $B^v_{external}$ can have constant, sinusoidal, or pulsating shapes. The generated voltage in the secondary sensor, $V_{secondary}$, has the same shape as the $B^v_{external}$.

■ ***4. Back calculating*** $B^v_{external}$ ***from the*** $V_{secondary}$***:*** PreMSat needs to back calculate the magnitude of the $B^v_{external}$ to use it in a defense algorithm 1 for generating the $B_{internal}$. It is evident from Eqn. 1 that if I_{Bias}, d, and V_H are known, B can be calculated. As the secondary sensor provides the $V_{secondary}$, it is possible to calculate the $B^v_{external}$ from the $V_{secondary}$ using Eqn. 6. The Eqn. 6 is derived by adjusting the terms of Eqn. 1.

$$B^v_{external} = K(\frac{d \times V_{secondary}}{I_{Bias}}) = K_c \times V_{secondary} \tag{6}$$

where K_c is the *sensitivity* of a Hall sensor that includes all constant terms for simplification. The term K_c is provided by the manufacturer of the Hall sensor in its datasheet.

In the next section, we discuss how the different blocks of PreMSat uses the $V_{secondary}$ to generate the internal magnetic fields $B_{internal}$ to nullify the $B^v_{external}$.

4.3.2 Blocks of PreMSat

In this section, we discuss all the blocks and algorithms used in PreMSat (see Fig. 6).

1. Circular ferrite core: PreMSat uses a circular ferrite core to host the primary coil and secondary sensor (see Sections 4.2 and 4.3.1 for details).

2. Differential amplifier: The differential amplifier takes the $V_{secondary}$ as its input and removes the common-mode noises from it (see Section 2.2 for common-mode noise).

The differential amplifier is implemented using an operational amplifier shown in Fig. 6. It has four resistors R1, R2, R3, and R4. When resistors R1 = R2 and R3 = R4, the output of the differential amplifier, denoted by $V^{diff}_{secondary}$, can be simplified to Eqn. 7.

$$V^{diff}_{secondary} = \frac{R_3}{R_1} V_{secondary} \tag{7}$$

The ratio R_3/R_1 in Eqn. 7 is set to 1 in PreMSat. Therefore, the differential amplifier only rejects the common-mode noises from the $V_{secondary}$ with a gain 1.

3. Analog-to-digital converter (ADC): The ADC samples the $V^{diff}_{secondary}$, digitizes it, and provides the digitized value to the algorithm 1 running on a processor. To reduce the power consumption, the ADC is configured at a low sampling frequency (900 kHz) at normal operating conditions (i.e., when no attack happens). But the ADC uses a high sampling frequency when an attack happens (i.e., when there is a presence of $B^v_{external}$).

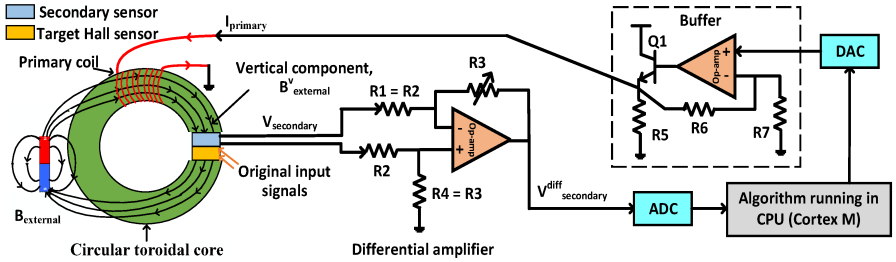

Figure 6: The different blocks of PreMSat.

4. PID controller: The output $V^{diff}_{secondary}$ from the ADC is given to a PID controller to generate a proper $B_{internal}$. The algorithm for the PID controller is designed in such a way that the generation of $B_{internal}$ should be fast enough so that it can nullify the $B^v_{external}$ in real-time. To meet the real-time requirement of PreMSat, the PID controller (see Section 2.5) is implemented in z-domain/discrete-time domain. There are three reasons behind implementing the PID controller in the z-domain instead of the s-domain/continuous-time domain. *First*, the z-domain takes ADC's sampling time in consideration that makes the PID controller more stable in the z-domain compared to the s-domain. *Second*, the PID controller in z-domain is highly deterministic. *Third*, most importantly, the PID controller in the z-domain has a much faster response time than the s-domain implementation. These properties are critical for real-time defense against the saturation attack.

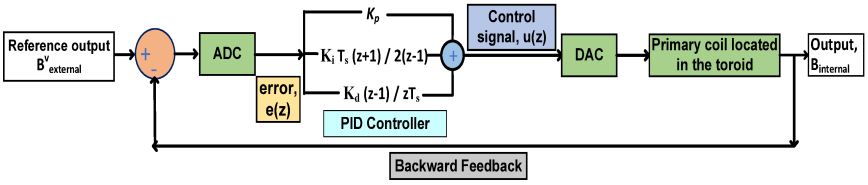

Figure 7: The PID controller tries to minimize the error between $B_{internal}$ and $B^v_{external}$.

The functional diagram of the PID controller is shown in Fig. 7. The variable $e(z)$ represents the error, which is the difference between the desired output $B^v_{external}$ and the actual output $B_{internal}$. Here, the $B^v_{external}$ is defined as the desired output because the PID controller should generate the $B_{internal}$ equal to the $B^v_{external}$. The $B^v_{external}$ is also known as the reference output. The error signal $e(z)$ is fed to the PID controller, and the controller computes both the derivative and the integral of this error signal.

The control signal $u(z)$ is fed to the primary coil, and the new output $B_{internal}$ is obtained. To obtain a continuous-time signal $B_{internal}$ from a discrete-time signal $u(z)$, a digital-to-analog converter (DAC) is used before the primary coil. The new output $B_{internal}$ is then fed back and compared to the reference $B^v_{external}$ to find the new error

signal $e(z)$. The controller takes this new error and computes an update of the control signal $u(z)$ again. This process continues until the error $e(z)$ settles to a minimum value.

The transfer function of the PID controller in the z-domain is expressed in Eqn. 8.

$$\begin{aligned} \frac{u(z)}{e(z)} &= K_p + K_i \frac{T_s(z+1)}{2(z-1)} + K_d \frac{z-1}{zT_s} \\ \Rightarrow u(z) &= z^{-1}u(z) + ae(z) + bz^{-1}e(z) + cz^{-2}e(z) \end{aligned} \tag{8}$$

where $a = K_p + K_i\frac{T_s}{2} + \frac{K_d}{T_s}$, $b = -K_p + K_i\frac{T_s}{2} - \frac{2K_d}{T_s}$, $c = \frac{K_d}{T_s}$, and T_s is the sampling period of the ADC. Eqn. 8 can be expressed as a difference equation shown in Eqn. 9.

$$u(k) = u(k-1) + ae(k) + be(k-1) + ce(k-2) \tag{9}$$

where $u(k)$ and $e(k)$ are discrete-time domain equivalent of z-domain terms $u(z)$ and $e(z)$, respectively. Eqn. 9 is a recursive equation and has a second-order infinite-impulse-response (IIR) filter format. Therefore, the PID controller, used in PreMSat, is a second-order IIR filter that requires less memory space and computational time compared to the finite-impulse-response (FIR) filters. This supports the idea that PreMSat provides real-time defense against the saturation attack on Hall sensors.

Please note that the secondary sensor only measures $B^v_{external}$ before generating $B_{internal}$. When PreMSat generates $B_{internal}$, the secondary sensor correlates more with the error $e(z)$ than $B^v_{external}$. Therefore, the PID controller minimizes $e(z)$ between $B^v_{external}$ and $B_{internal}$. Once $e(z)$ is close to zero, the secondary sensor starts to measure $B^v_{external}$ again.

■ ***Parameters of the PID controller:*** As the PID controller is a critical component of the real-time machine of PreMSat, few parameters that control the real-time properties of the PID controller are discussed here. These parameters are rise time, overshoot, settling time, and steady-state error. The values of K_p, K_i, K_d are tuned using MATLAB for a sampling frequency of 900 kHz to result in the lowest rise time, overshoot, settling time, and steady-state error. The values of these parameters are tabulated in Table 1.

Table 1: Parameters of the PID controller used in PreMSat

Response	Rise time	Overshoot	Settling time	Steady-state error
$K_p = 350$; $K_i = 300$; $K_d = 50$	8 μs	$< 1\%$	23 μs	$< 1\%$

Table 1 indicates that the settling time is 23 μs. In other words, it takes 23 μs to generate the $B_{internal}$ equal to the $B^v_{external}$ with less than 1% steady-state error. The less than 1% steady-state error is negligible compared to the large values of the $B^v_{external}$ required for the saturation attack (see Section 7.3).

■ ***Prevents strong or weak multiple signal shapes at the same time:*** The PID controller minimizes the error $e(z)$ while generating the $B_{internal}$ equal to the $B^v_{external}$, irrespective of the *strength* and *shapes* of the injected $B^v_{external}$. Even when multiple shapes, such as constant, sinusoidal, and pulsating fields, are injected at the same time, the vector summation of these fields will have a vertical component $B^v_{external}$ influencing the target Hall sensor (see Section 4.1, Fig. 2 and 5). The PID controller will nullify this $B^v_{external}$ in exactly the same way using the $B_{internal}$.

Moreover, a weak $B^v_{external}$, which can spoof the differential amplifier in its *linear region* (see Fig. 1), can also be nullified by the $B_{internal}$. Because a weak injected $B^v_{external}$ will also be picked up by the ferrite core, and PreMSat can nullify it using the $B_{internal}$.

In addition, PreMSat can nullify a injected $B^v_{external}$ even if the $B^v_{external}$ has the *same frequency* as the natural input signal B_{input}. Because the generated $B_{internal}$ by PreMSat can nullify the $B^v_{external}$ irrespective of its frequency, which is equal to the B_{input} or not.

5. Algorithm: The Algorithm 1, which handles the PID controller and controls the generation process of $B_{internal}$, is explained below.

Line 1-4: The ADC is configured initially to a low sampling frequency of 35 kHZ to ensure low power consumption by PreMSat. The ADC samples the $V^{diff}_{secondary}$ and

algorithm 1 continuously tracks the $V^{diff}_{secondary}$ to check whether any attack happens.

Line 5-8: As $V^{diff}_{secondary}$ is coming from the secondary sensor, any change of $V^{diff}_{secondary}$ from a reference voltage indicates the presence of the $B^{v}_{external}$. The ADC changes its sampling frequency (i.e., $1/T_s$) to a higher value (i.e., 900 kHz) to provide the optimum a, b, and c in Eqns. 8 and 9. Then the $B^{v}_{external}$ is calculated using Eqn. 6 and the calculated $B^{v}_{external}$ is used to calculate the term $e(z)$.

Line 9-18: The PID controller is implemented using the difference equation from Eqn. 9. The PID controller generates $u(k)$, which is the discrete-time representation of $u(z)$, and converts the term $u(k)$ to an equivalent analog signal $I_{primary}$ using a DAC. The $I_{primary}$ is used to generate $B_{internal}$ using Eqns. 3, and 4. The error signal $e(z)$ is calculated and this process repeats until the term $e(z)$ settles within the 1% of the reference $B^{v}_{external}$. If the $e(z)$ does not settle down to 1% of $B^{v}_{external}$ within a certain time x, there is a possibility that $B_{internal}$ is not strong enough to nullify the $B^{v}_{external}$. This may cause the $V^{diff}_{secondary}$ to stuck in +ve/-ve saturation voltage. If this happens, PreMSat notifies the authority to fail-safe the system. The value of x is user defined. We use $x = 50$ μs.

Line 19-20: If no attack happens, the algorithm does not generate any $B_{internal}$ and keeps the Hall sensor running as it is.

Algorithm 1: Algorithm running on PreMSat.

```
   Input: Data from ADC: V^diff_secondary
   Output: Current signals to the primary coil: I_primary
 1 Setup ADC ← (12 bits, sampling freq. = 35 kHz)
 2 B_internal ← 0
 3 for t ← 1 to ∞ do
 4     Track V^diff_secondary
 5     if V^diff_secondary changes then
 6         Setup ADC ← (12 bits, sampling freq. = 900 kHz)
 7         Calculate B^v_external from V^diff_secondary using Eqn. 6
 8         Calculate e(z) ← B^v_external - B_internal
 9         for Continue until e(z) is within 1% of the B^v_external do
10             Generate u(z) and u(k) using Eqns. 8, and 9
11             Convert u(k) to I_primary, where I_primary is an analog version of u(k), using DAC
12             Generate B_internal from I_primary using Eqns. 3, and 4
13             Calculate e(z) ← B^v_external - B_internal
14             if e(z) does not settle down to 1% of the B^v_external within x time then
15                 Possibility that B_internal cannot nullify the B^v_external
16                 Possibility that V^diff_secondary is stuck in +ve/-ve saturation voltage
17                 Notify authority to fail-safe the system and break from the loops
18         Output = I_primary
19     else
20         Do not generate B_internal from I_primary using Eqns. 3, and 4
```

6. Buffer: A digital-to-analog converter (DAC) converts the digital signal $u(k)$, which is the output of the PID controller, to an analog signal $I_{primary}$. As the DAC does not have the capability to provide high values of $I_{primary}$ to the primary coil, a buffer is used after the DAC to support high current to the primary coil (see Section 5.1). The primary coil, next, generates the $B_{internal}$ that is already explained in Section 4.2.

■ ***Security of PreMSat itself:*** An important question may arise what will happen if the attacker attacks the different components of the defense itself, such as the secondary sensor and differential amplifier. As the secondary sensor is placed in the ferrite core, the generated $B_{internal}$ will also nullify the injected $B^{v}_{external}$ to the secondary sensor in the same way it prevents the saturation attack on the target Hall sensor. Therefore, the differential amplifier connected with the secondary sensor will not be saturated.

4.3.3 Generating the $B_{internal}$ in opposite direction to the $B^{v}_{external}$

As the $B^{v}_{external}$ is concentrated along the cross-section of the toroid, the $B_{internal}$ should also be provided along the same cross-section but in the opposite direction to nullify the $B^{v}_{external}$. *To provide the $B_{internal}$ in opposite polarity, the primary coil is connected in reverse polarity with the buffer chip.* Therefore, the PID controller does not need to spend any extra time to make the polarity of the $B_{internal}$ reverse to nullify the $B^{v}_{external}$.

5 Evaluation of PreMSat

5.1 A prototype

A prototype of the proposed PreMSat is implemented using different discrete components, which is shown in Fig. 8 (left). A Hall sensor (part #ACS718) is used as the secondary sensor. The differential amplifier uses a low-power op-amp (i.e., part # TL084CN) with a high slew rate, low input bias and offset currents with a rise time of 0.05 μs and a unity-gain bandwidth of 3 MHz. The buffer uses an op-amp (part # TL084CN) in voltage-follower configuration with a high-power transistor $Q1$ (part # TO-220 [TO2]) connected at op-amp's output (see Fig. 6). The CPU of PreMSat is an EFM-32 Giant Gecko development board from Silicon Labs [EFM] having a Cortex M-3 based 32-bit CPU with built-in ADCs and DACs. The EFM-32 has an ultra-low-power CPU with a 48 MHz clock. A low-cost soft ferrite, such as Mn-Zn ferrite is used as the material of the circular toroidal core [ferb]. Mn-Zn ferrite [OWL03] has a high relative permeability (~25000), and can support high frequency and low eddy current loss. Therefore, Mn-Zn ferrite can provide a low-resistive magnetic path to collect the externally injected field $B_{external}$ for PreMSat.

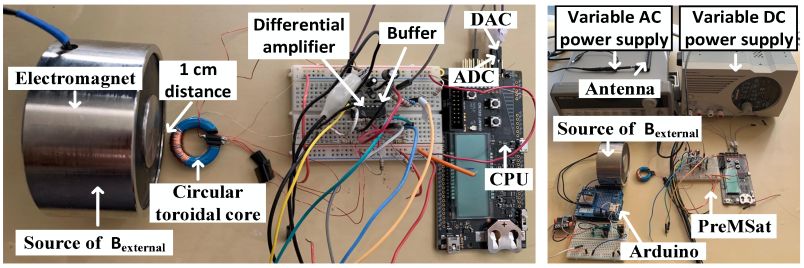

Figure 8: (left) The prototype. (right) The different instruments used in the testbed.

5.2 Testbed

We test ten different Hall sensors (Table 2 (a)) of all types, such as open/close loop, bipolar/unipolar sensors from four different manufacturers. As different Hall sensors measure different types of input signals, we use different sources to supply input signals to these different Hall sensors. We use a variable AC and DC source to supply current/voltage as original input signals to Hall sensors with serial no. 1-6 and use a magnet [Lit] to supply magnetic fields as input signals to Hall sensors with serial no. 7-10 in Table 2. The external fields $B_{external}$ are generated in two ways: an electromagnet (uxcell [ama]) with a MOSFET (part #STP4NK80Z [pow]) connected with an Arduino is used to generate constant, sinusoidal, and pulsating fields, and a function generator connected with a monopole antenna [mon] is used to radiate high and low frequency electromagnetic interference (EMI) signals to attack Hall sensors. The testbed is shown in Fig. 8 (right).

5.3 PreMSat prevents the saturation attack

Here, we justify how PreMSat prevents the saturation attack on Hall sensors. We randomly pick ACS710KLATR-10BB from Table 2 as the target Hall sensor. A 7.5 A peak-to-peak AC current of 60 Hz frequency is given as an input signal to ACS710KLATR-10BB. Before any injection of external magnetic fields, the output of the target Hall sensor is shown

in Fig. 9 (i), which shows an undistorted sinusoidal signal. An electromagnet with an MMF of $\sim$ 3600 A-t is used to inject different types of external magnetic fields $B_{external}$, such as constant, sinusoidal, and square pulsating fields, to the target Hall sensor from 1 cm. We use 2 Hz as the frequency of injected sinusoidal and square pulsating fields as an example. Fig. 9 (ii) shows that the output of the target Hall sensor is driven to its saturation voltage (4.8 V) after the saturation attack resulting in a flattened output signal. As the output signal is flattened, any critical information cannot be recovered from the output signal in its saturation region. After integrating PreMSat with the target Hall sensor, the external magnetic fields $B_{external}$ cannot drive the output of the target Hall sensor to its saturation region. We can see from Fig. 9 (iii) that the output of the target Hall sensor remains unperturbed during the saturation attack.

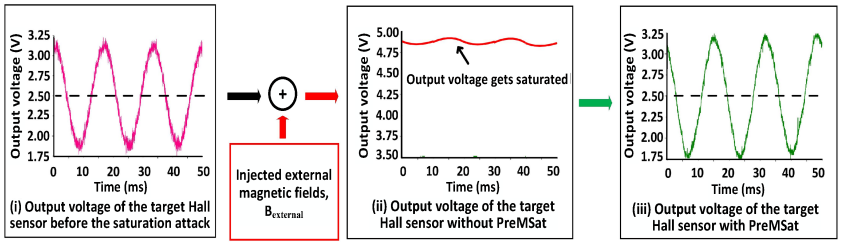

Figure 9: (i) The output signal of the target Hall sensor before the saturation attack. (ii) The output signal of the target Hall sensor gets saturated if PreMSat is not used. (iii) The output signal of the target Hall sensor does not change if PreMSat is used.

Performance metric: If we can prove that the output voltage of the target Hall sensor before the saturation attack is similar to the output voltage of the target Hall sensor after the saturation attack *with* PreMSat, we can claim that PreMSat is effective to prevent the saturation attack. To quantify the similarity, we calculate the *correlation coefficient (C)* [KDRB68] between signals in Fig. 9 (i) (i.e., before the saturation attack) and Fig. 9 (iii) (i.e., after the saturation attack with PreMSat). The value of correlation coefficient (C) is 0.97 for this case that is very close to unity. This indicates that the signal in Fig. 9 (i) (i.e., before the saturation attack) is *statistically the same* as the signal in Fig. 9 (iii) (i.e., after the saturation attack with PreMSat) in a point-by-point fashion. This proves that PreMSat can successfully prevent the saturation attack on a Hall sensor.

Table 2: Testing different Hall sensors in testbed for different amplitudes of input signals.

Sl.	Manufac. (a)	Part # (a)	Polarity/Loop (a)	Amplitude of input signal (b)	Avg. C (c)
1	Allegro	ACS718MATR-20B[datc]	Bipolar/Open	1A, 5A, 10A, 15A, 20A	0.94
2	Allegro	ACS710KLATR-10BB [data]	Bipolar/Open	2A, 4A, 6A, 8A, 10A	0.95
3	Allegro	ACS715ELCTR-20A [datb]	Unipolar/Open	1A, 5A, 10A, 15A, 20A	0.95
4	Allegro	ACS724LLCTR-10AU [datd]	Unipolar/Open	2A, 4A, 6A, 8A, 10A	0.96
5	LEM	LTSR 6-NP [datf]	Bipolar/Closed	1A, 2A, 3A, 4A, 5A	0.95
6	LEM	LV 25 P [datg]	Bipolar/Closed	30V, 50V, 70V, 90V, 110V	0.96
7	Texas Ins	DRV5053OA [date]	Bipolar/Open	100G,200G,300G,400G,500G	0.97
8	Honeywell	SS49/SS19 [datj]	Bipolar/Open	100G,200G,300G,400G,500G	0.97
9	Honeywell	SS39ET [dath]	Bipolar/Open	100G,200G,300G,400G,500G	0.96
10	Honeywell	SS494B [dati]	Bipolar/Open	100G,200G,300G,400G,500G	0.96

5.4 Testing PreMSat for different amplitudes of input signals

Table 2 (c) shows the average correlation coefficient C for different amplitude of input signals to ten different Hall sensors for a $B_{external}$ having an MMF of 3000 A-t. We vary the amplitude of the input signals within the entire input range (Table 2 (b)) of Hall sensors and calculate C for every input value and do an average of C for every sensor. The average of C is *greater* than 0.94 for every sensor when PreMSat is used (Table 2 (c)) compared to 0.1 when PreMSat is not used. This indicates that PreMSat works within

the entire input range of every Hall sensor. We use 60 Hz as the frequency of input signals to Hall sensors with serial 1-6 and 10 Hz to Hall sensors with serial 7-10.

5.5 Testing PreMSat for different frequencies of input signals

Section 5.4 shows the performance of PreMSat for different amplitudes of the input signals. In this section, we vary the frequency of the input signals to different Hall sensors within their entire input range (Table 3 (a)) and calculate the correlation coefficient (C) for every case. We keep the amplitude of input signals fixed at 1 A/100 G/110 V. We find that the average value of C is greater than 0.94 for every sensor when PreMSat is used compared to 0.1 when PreMSat is not used (see Table 3 (b)). This indicates that PreMSat works within the entire input frequency range of every Hall sensor.

Table 3: Testing different Hall sensors for different frequencies of input signals and different strengths of injected $B_{external}$.

Sl.	Part #	Frequency range of input signal (a)	Avg. C (b)	Strength of $B_{external}$ (c)	Avg. C (d)
1	ACS718MATR-20B	0 Hz–40 kHz	0.94	0 A-t–4200 A-t	0.95
2	ACS710KLATR-10BB	0 Hz–120 kHz	0.94	0 A-t–4200 A-t	0.94
3	ACS715ELCTR-20A	0 Hz–80 kHz	0.96	0 A-t–4200 A-t	0.97
4	ACS724LLCTR-10AU	0 Hz–120 kHz	0.96	0 A-t–4200 A-t	0.95
5	LTSR 6-NP	0 Hz–100 kHz	0.94	0 A-t–4200 A-t	0.94
6	LV 25 P	0 Hz–25 kHz	0.95	0 A-t–4200 A-t	0.95
7	DRV5053OA	0 Hz–20 Hz	0.96	0 A-t–4200 A-t	0.96
8	SS49/SS19	0 Hz–30 Hz	0.97	0 A-t–4200 A-t	0.97
9	SS39ET	0 Hz–40 Hz	0.95	0 A-t–4200 A-t	0.96
10	SS494B	0 Hz–30 Hz	0.96	0 A-t–4200 A-t	0.94

5.6 Testing PreMSat for different strength of injected $B_{external}$

At first, we find the strength of the external magnetic fields $B_{external}$ required to drive the Hall sensors to their saturation region (i.e., saturation attack) experimentally in our testbed. It is already mentioned in Section 4.2 that the strength of the magnetic field is quantified by the magneto-motive force (MMF). At first, we vary the MMF of the $B_{external}$ using an electromagnet and find that an MMF $>$ 3600 A-t can cause the saturation attack from 1 cm distance for all of the ten different Hall sensors. If the distance is $<$ 1 cm, an MMF less than 3600 A-t is required for the saturation attack.

To test PreMSat, we vary the MMF from 0 A-t to 4200 A-t (i.e., $\sim$ 1.2x of 3600 A-t) at frequency zero with a step size of 200 A-t (see Table 3 (c)) and calculate C for every case for ten different Hall sensors. We do a total of $\sim$200 experiments in our testbed and find that the average value of C is greater than 0.94 for every sensor when PreMSat is used compared to 0.1 when PreMSat is not used (see Table 3 (d)). This proves that the prototype PreMSat can prevent the external magnetic fields $B_{external}$ having an MMF within 0 - 4200 A-t. *This indicates that PreMSat can prevent a weak MMF that can cause spoofing in the linear region as well as a strong MMF that can cause a saturation attack.*

5.7 Testing PreMSat for different frequencies of injected $B_{external}$

In Section 5.6, we vary the MMF of the $B_{external}$ from 0 A-t to 4200 A-t by keeping the frequency of the $B_{external}$ at zero. In this section, we vary the frequency of the $B_{external}$. As mentioned in Section 5.2, we use an electromagnet and a function generator connected with a mono-pole antenna to radiate high and low frequency $B_{external}$. We vary the frequency of the $B_{external}$ from 0 Hz to 30 kHz with a step size of 1 kHz (see Table 4 (a)) and calculate C for every case for ten different Hall sensors. We do an average of C for every Hall sensor in our testbed and find that the average value of C is greater than 0.94 for every sensor when PreMSat is used compared to 0.1 when PreMSat is not used (see Table 4 (b)). *This proves that the prototype PreMSat can prevent both low and high frequency external magnetic spoofing within a range of 0–30 kHz.*

5.8 Testing PreMSat for different distances of the magnetic source

In Sections 5.4, 5.5, 5.6, and 5.7, we place the source of $B_{external}$ 1 cm away from the target Hall sensor. In this section, we vary the distance of the magnetic-source (i.e., $B_{external}$) from the Hall sensor. We use an MMF of ∼3600 A-t for the $B_{external}$ and keep the frequency and amplitude of the input signals fixed at 60 Hz/10 Hz 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 (Table 4 (c)) and calculate the average of C for every Hall sensor. The average value of C is greater than 0.94 for every case when PreMSat is used compared to 0.1 when PreMSat is not used (Table 4 (d)). This proves that PreMSat can prevent the saturation attack from a very close distance.

Table 4: Testing different Hall sensors for different frequencies and distances of $B_{external}$.

Sl.	Part #	Different frequencies of $B_{external}$ (a)	Avg. C (b)	Different distances of $B_{external}$ (c)	Avg. C (d)
1	ACS718MATR-20B	0 Hz - 30 kHz	0.94	0 cm - 7 cm	0.94
2	ACS710KLATR-10BB	0 Hz - 30 kHz	0.95	0 cm - 7 cm	0.97
3	ACS715ELCTR-20A	0 Hz - 30 kHz	0.96	0 cm - 7 cm	0.95
4	ACS724LLCTR-10AU	0 Hz - 30 kHz	0.97	0 cm - 7 cm	0.96
5	LTSR 6-NP	0 Hz - 30 kHz	0.94	0 cm - 7 cm	0.97
6	LV 25 P	0 Hz - 30 kHz	0.96	0 cm - 7 cm	0.94
7	DRV5053OA	0 Hz - 30 kHz	0.96	0 cm - 7 cm	0.95
8	SS49/SS19	0 Hz - 30 kHz	0.97	0 cm - 7 cm	0.96
9	SS39ET	0 Hz - 30 kHz	0.94	0 cm - 7 cm	0.94
10	SS494B	0 Hz - 30 kHz	0.96	0 cm - 7 cm	0.95

5.9 Comparing PreMSat with a ferromagnetic shield

We compare PreMSat with a ferromagnetic shield to prove PreMSat's effectiveness over a shield. There are specialized materials for magnetic shielding. The foremost of these is MuMetal [mum], which has high magnetic permeability and is used in industry. We use a strong electromagnet as a source of $B^{v}_{external}$ with an MMF of ∼ 3600 A-t. We use a box made of MuMetal as a shield and enclose the target Hall sensors with it. We keep the source of MMF 1 cm away outside of the shield and keep the Hall sensor 1 cm away inside of the shield. We vary the thickness of the shield and measure C for every thickness. We find that even an 1 inch thick shield cannot prevent a strong MMF of 3600 A-t (i.e, low value of C in Table 5 (c)). The reason behind this is that at strong magnetic fields, MuMetal gets saturated [mum]. In saturation, the shielding property of the MuMetal is diminished [CHFP97], and sensors become vulnerable to external magnetic fields. Next, we only use PreMSat without a shield and find that PreMSat can maintain C close to unity (see Table 5 (d)). This proves the efficacy of PreMSat over a shield.

Table 5: Comparing PreMSat with a ferromagnetic shield and a high supply voltage.

Sl.	Part #	C (0.3 in. thick) (a)	C (0.5 in. thick) (b)	C (1 in. thick) (c)	C (PreMSat only)(d)	V_{Supply} range (e)	Max. MMF range (f)
1	ACS718...	0.20	0.26	0.37	0.94	4.5-5.5 V	1300-1900 A-t
2	ACS710...	0.14	0.21	0.31	0.96	3-5.5 V	1000-2200 A-t
3	ACS715...	0.19	0.27	0.36	0.97	4.5-5.5 V	1200-2000 A-t
4	ACS724...	0.27	0.35	0.39	0.95	4.5-5.5 V	1500-2700 A-t
5	LTSR 6-NP	0.28	0.39	0.41	0.97	4.7-5V	1700-1900 A-t
6	LV 25 P	0.13	0.28	0.38	0.94	12-15 V	1600-2000 A-t
7	DRV5053OA	0.33	0.39	0.42	0.96	2.5-38 V	1200-1400 A-t
8	SS49/SS19	0.10	0.21	0.32	0.96	4-10 V	1100-3600 A-t
9	SS39ET	0.15	0.29	0.35	0.95	2.7-6.5 V	1300-2800 A-t
10	SS494B	0.25	0.32	0.37	0.94	4.5-10.5V	1400-3400 A-t

5.10 Comparing PreMSat with a high supply voltage

It may appear that increasing the supply voltage, denoted by V_{Supply}, of the differential amplifier located in a Hall sensor (see Fig. 1 and Section 2.3) may prevent the saturation

attack because increasing the V_{Supply} will also increase the saturation voltage of a differential amplifier. To verify this claim, we vary the V_{Supply} of 10 Hall sensors within their acceptable ranges (see Table 5 (e)) and measure the maximum MMF, up to which every sensor can tolerate within their supply voltage ranges. We find that increasing the V_{Supply} may increase the maximum MMF up to which Hall sensors can tolerate before going to saturation (see Table 5 (f)). *However, the maximum MMF, up to which they can tolerate, is still much smaller compared to PreMSat's capability of preventing an MMF of* $\sim$ *4200 A-t.* Please note that the output of DRV5053OA gets saturated at $\sim$ 2 V irrespective of the V_{Supply} variation within 2.5–38 V (see [date]). Therefore, DRV5053OA's maximum MMF spans within a small range of 1200 - 1400 A-t.

5.11 Real-time defense against the saturation attack

Broadly speaking, PreMSat spends most of its time executing the following five tasks: (i) to remove common mode noise by the differential amplifier, (ii) to sample the $V_{secondary}^{diff}$ by the ADC, (iii) to generate the $B_{internal}$ and settle it (i.e., PID controller), (iv) to convert the $u(k)$ to $I_{primary}$ by the DAC, and (v) to provide the $B_{internal}$ in opposite polarity. In Table 6, we provide the amount of time required to execute each of these tasks along with the name of the block responsible for each task.

From Table 6, it is important to note that PreMSat can provide the $B_{internal}$ within 28.79 μs. This execution time is deterministic, and no additional latency/delay is involved in this process. Therefore, PreMSat can prevent the saturation attack within 28.79 μs that can be termed as a real-time defense against the saturation attack.

Table 6: Timing analysis of PreMSat.

Task name	Block name	Clock freq.	Time
Remove common-mode noise	Differential amplifier	NA	0.25 μs
Sample the $V_{secondary}^{diff}$	ADC	11 MHz	1.2 μs
Generate the $B_{internal}$ (PID controller)	CPU	48 MHz	23 μs
Convert the $u(k)$ to $I_{primary}$	DAC	500 kHz	4 μs
provide the $B_{internal}$ in opposite polarity	Buffer	NA	0.34 μs
			28.79 μs (total)

5.12 Feasible structure, and maintenance

To integrate the Hall and secondary sensors in a toroid, a small gap needs to be created in the cross-section of a toroid. *Industries are already using a similar structure where creating a small gap and winding a primary coil is similar to creating a transformer (Fig. 5-22 in [Hon19]). Therefore, the structure is feasible in today's technology.* Moreover, regular maintenance is sufficient as PreMSat does not have parts that may be easily damaged.

5.13 Cost

The total cost of our prototype is $\sim$\$14, comparable with the sensor cost ($\sim$\$2–\$70). *However, the actual cost will be much less than* $\sim$*\$14 in mass level production.*

5.14 Power consumption

The CPU runs at a low power, ADCs work at a low sampling frequency (i.e., 35 kHz), and the buffer, primary coil, and ferrite core consume low power when no attack happens. The overall power consumption when no attack happens is $\sim$ 5 mW. However, when an attack happens, the CPU and ADCs start working with high frequencies, and the primary coil generates fields $B_{internal}$. The primary coil is the main source of power consumption during an attack as it needs to generate a counter MMF. We use Mn-Zn soft-ferrite as the toroid, which has high relative permeability and magnetization. Therefore, the primary coil can generate strong counter MMF (i.e., 0–4200 A-t), consuming power within 0–3 W. Moreover, Mn-Zn soft-ferrite has low resistance resulting in a low eddy-current loss. The overall power consumption when an attack happens is $\sim$ 5 mW–3 W.

6 Demonstration of preventing the saturation attack

In this section, we demonstrate PreMSat's capability on a practical system — a grid-tied solar inverter. Grid-tied solar inverters are critical components in smart grids and are typically used as a power source in solar plants. Solar inverters have Hall sensors, which are typically used to measure AC and DC current or voltage [SWXL18]. Therefore, an attacker can target Hall sensors located in grid-tied inverters and inject external magnetic fields to drive Hall sensors to their saturation regions. This type of attack can shut down the inverter, and for a weak grid scenario, it can also cause a blackout in the region. To demonstrate that PreMSat can prevent the saturation attack, we use a 140 Watt inverter from Texas Instruments [tex] in the testbed. This inverter has a Hall effect current sensor with a part # ACS712ELCTR-20A-T. At first, we inject constant, sinusoidal, and pulsating magnetic fields into the inverter with an MMF = 3600 A-t from a 1 cm distance. This causes a saturation attack on the Hall sensor located inside of the inverter. As a result, the inverter shuts down itself, causing a DoS attack on the inverter. To evaluate PreMSat, we integrate PreMSat with the Hall sensor and repeat the same experiment (Fig. 10). We notice that the inverter continues working without any shutdown at this time. This proves that PreMSat can prevent the saturation attack on a practical system.

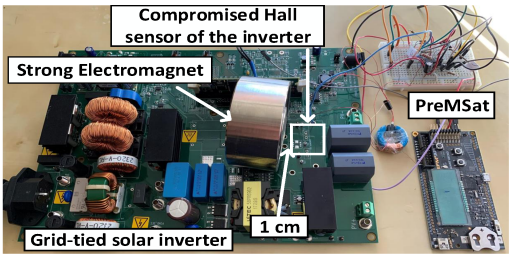

Figure 10: PreMSat prevents the saturation attack on the grid-tied solar inverter.

7 Limitations of PreMSat

7.1 Power consumption and usability of PreMSat

PreMSat consumes 0 - 3 W power while generating a strong internal field. The power consumption may be small for some applications, such as solar inverters and automotives, but may be substantial for few applications, such as proximity detection and position sensing. Moreover, the toroid has a 1.3 cm outer radius which is accommodable if designers would plan ahead to provide the space so that it would not affect the common use cases. However, few applications, such as Hall sensors in brush-less motors, may not fit the toroid. Moreover, the current prototype cannot be directly applicable to multiple axis Hall sensors. However, the idea of generating an internal magnetic field to nullify the external field would be applicable to a multiple-axis sensor with a change in the ferrite core's structure.

7.2 Non-zero settling time of the PID controller

It is already described in Section 4.3.2 that the PID controller has a non-zero settling time (i.e., 23 μs), which is also the main contributing factor to the total time (see Table 6) required to generate the $B_{internal}$. Therefore, if the attacker changes the injected magnetic fields $B_{external}$ within 23 μs, the timeliness of the defense will not be guaranteed. We have already finely tuned the values of K_p, K_i, K_d to obtain the lowest possible rise-time and settling time for the PID controller.

7.3 Non-zero steady-state error of the PID controller

The PID controller is tuned in such a way to have the lowest amount of steady-state error (i.e., <1%) possible for the problem at hand. In spite of the fine-tuning, the PID controller has a non-zero steady-state error, which may add error to the $B_{internal}$ while

nullifying the $B^v_{external}$. However, <1% error is negligible compared to the large values of the $B^v_{external}$ required for the saturation attack. For example, 3600 A-t is required for the saturation attack from a 1 cm distance, and 1% of 3600 A-t is only 36 A-t, which results in a negligible noise at the output of the Hall sensor.

7.4 Upper limit strength of the injected $B_{external}$

Our prototype can prevent an external magnetic field $B_{external}$ up to an MMF of 4200 A-t. The reason behind this is that our prototype cannot generate a $B_{internal}$ having an MMF more than 4200 A-t. The upper limit 4200 A-t is limited by the amount of power that the buffer can provide. The idea is supported by Eqn. 4, which says $B_{internal}$ depends on the $I_{primary}$. The $I_{primary}$ is provided by the buffer to the primary coil. The buffer used in the prototype has its maximum capacity that can support a $I_{primary}$, which can generate an MMF up to 4200 A-t. However, the limit can be theoretically increased from 4200 A-t to any higher value using a stronger buffer, causing a trade-off between cost and strength.

7.5 Upper limit frequency of the injected $B_{external}$

Our prototype can prevent the $B_{external}$ up to a frequency of ∼30 kHz. The upper limit 30 kHz results from the total time 28.79 μs required to generate the $B_{internal}$ (see Table 6). The reciprocal of 28.79 μs is 1/ 28.79 μs = ∼35 kHz. The prototype supports up to ∼30 kHz instead of 35 kHz because an additional time is spent to overcome the parasitic inductance/capacitance present in the primary coil. Note that the total time of 28.79 μs is obtained for our prototype using a clock frequency of 48 MHz. This time can be reduced further using a faster CPU having a clock frequency higher than 48 MHz.

8 Related work

To the best of our knowledge, no state-of-the-art work can prevent a saturation attack on Hall sensors. However, there is related work exists for other sensors that cannot be used to prevent a saturation attack on Hall sensors for the following reasons.

Barua et al. [BAF22] proposed an in-sensor defense for Hall sensors. However, it does not work for a saturation attack. Trippel et al. [TWX+17] proposed randomized and 180^0 out-of-phase sampling to provide defenses against an acoustic signal injection into MEMS accelerometers. They sample at random times with 180^0 out-of-phase within the resonant frequency period to nullify the spoofing signals. They are not suitable for saturation attacks because: (i) They can only filter out a forged signal, which has a frequency equal to the resonant frequency of the MEMS sensor. Therefore, they do not work other than a specific resonant frequency, for example, any attack frequency. (ii) They do not work against a DC/constant forged signal because randomized sampling cannot filter out a DC signal. (iii) They do not work when the sensor output is flattened.

Cheng et al. [CSWL14] and Alexander [Ale19] from Allegro Microsys. used differential sensing by using two sensing elements to cancel out common-mode attack signals. However, it does not prevent a sensor output from getting flattened during a saturation attack.

Kune et al. [KBC+13] used an adaptive filter to mitigate EMIs in microphones. An adaptive filter estimates EMIs first and then subtracts the estimated EMIs from the original signal to recover the original signal. This technique cannot estimate any attack signal if the sensor output is flattened because of the saturation attack.

Zhang et al. [ZYJ+17] used a Support Vector Machine (SVM), and Roy et al. [RSHC18] used a non-linearity tracing classifier to filter inaudible ultrasonic voice commands from MEMS microphones. They have the 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 don't work if the sensor output is flattened because of the saturation attack.

Shoukry et al. [SMY+15] proposed PyCRA to detect spoofing attempts by turning off the active sensor's transmitter at random instants such that the attacker cannot react to the sudden changes. However, PyCRA only works for active sensors; it is not applicable for passive sensors. Moreover, PyCRA only detects intentional spoofing but cannot prevent it.

Wang et al. [WXZ+14] designed a state graph-based approach to detect state corruption due to intentional spoofing. Again, Shoukry et al. [SNB+15] used the satisfiability modulo theory (SMT) to recover from corrupted states. The main drawback of the above-mentioned state recovery techniques as a defense is that they do not work against time-varying spoofing signals, which may create oscillations between corrupted and recovered states of the system controller. The oscillations between corrupted and recovered states may eventually compromise the integrity and availability [CAS+09, W+16] of the system under attack. Moreover, they cannot prevent saturation attacks on any sensor.

In contrast, PreMSat uses a PID controller to generate an internal magnetic field to nullify the injected external field. The PID controller can nullify the injected external field even if the injected external field (i) is constant, sinusoidal or square magnetic fields, (ii) has zero/DC frequency, (iii) has the same frequency as the natural signal being measured, and (iv) can cause a saturation attack. Moreover, PreMSat can work against $\sim$ 4200 A-t and within 0–30 kHz. However, PreMSat achieves these advantages with high power and physical overhead compared to recent works (see Table 7 for a summary).

Table 7: Comparing PreMSat with other defenses.

Properties	Recent works [TWX+17, CSWL14, Ale19, KBC+13, ZYJ+17, RSHC18]	PreMSat
Saturation attack	✗	✓
Spoofing in linear region	few work for a specific resonant frequency or a frequency other than the natural signal's frequency	works for any frequency within 0 - 30 kHz
0 A-t $\leq$ MMF $\leq$ 4200 A-t	✗	✓
Constant/DC, sinusoidal, and square magnetic spoofing	✗	✓
0 $\leq$ frequency $\leq$ 30 kHz	✗	✓
External signal has the same frequency as the natural input signal	✗	✓
Power consumption	mW range	5mW - 3 W
Overhead	extra parts for adaptive filter, etc.	ferrite core

9 Conclusion

PreMSat is the first of its kind in literature and industry that can prevent the saturation attack satisfactorily on passive Hall sensors. PreMSat can prevent the saturation attack originating from different types, such as constant, sinusoidal, and pulsating magnetic fields, in hard real-time. Moreover, PreMSat can also prevent weak magnetic spoofing in the linear region of the differential amplifier. PreMSat integrates a low resistive magnetic path to collect the external magnetic fields injected by the attacker and utilizes a finely tuned PID controller to nullify the external fields. The PID controller is tuned in such a way that it has minimum settling time and steady-state error. This helps to keep the existing data processing speed of the connected system undisturbed. We have presented a prototype of PreMSat, which can nullify external fields up to $\sim$ 4200 A-t. We have done an extensive analysis of PreMSat through more than 300 experiments on ten different Hall sensors from four different manufacturers and proved its efficacy against the saturation attack. However, PreMSat has high power cost and overhead that might not be suitable for all applications. Moreover, we have demonstrated the efficacy of PreMSat on a practical system — a grid-tied solar inverter. The demonstration proves that PreMSat can prevent the DoS attack on a practical system by nullifying the saturation attack on a Hall sensor. *Finally, we believe that the necessity of developing a similar defense like ours is going to be increased in the near future for other sensors when sensors will pervade our lives.*

Thanks

The authors would like to thank the anonymous reviewers and shepherd 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

[Ale19] Latham Alexander. Common Mode Field Rejection in Coreless Hall-Effect Current Sensor ICs, 2019. https://www.allegromicro.com/-/media/files/application-notes/an269123-common-mode-field-rejection-in-coreless-current-sensor-ics.pdf. (Accessed: 03-22-2022).

[ama] uxcell DC24V 80KG Force Electric Lifting Magnet Electromagnet Solenoid Lift Holding 65mm x 30mm. https://www.amazon.com/uxcell-Solenoid-Electric-Holding-Electromagnet/dp/B07FKKYT22/ref=sr_1_4?dchild=1&keywords=electromagnet+80kg&qid=1594966282&sr=8-4. (Accessed: 03-22-2022).

[ard] Arduino Uno. https://store-usa.arduino.cc/products/arduino-uno-rev3/. (Accessed: 03-23-2022).

[BAF20] Anomadarshi Barua and Mohammad Abdullah Al Faruque. Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1273–1290. USENIX Association, August 2020.

[BAF22] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 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.

[BB86] Ronald Newbold Bracewell and Ronald N Bracewell. *The Fourier transform and its applications*, volume 31999. McGraw-Hill New York, 1986.

[CAS+09] Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry, et al. Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security*, volume 5. Citeseer, 2009.

[CCCS01] F Caricchi, F Giulii Capponi, F Crescimbini, and L Solero. Sinusoidal brushless drive with low-cost linear hall effect position sensors. In *2001 IEEE 32nd Annual Power Electronics Specialists Conference (IEEE Cat. No. 01CH37230)*, volume 2, pages 799–804. IEEE, 2001.

[CHFP97] Laurent Chiesi, Karim Haroud, John A Flanagan, and Rade S Popovic. Chopping of a weak magnetic field by a saturable magnetic shield. *Sensors and Actuators A: Physical*, 60(1-3):5–9, 1997.

[CLH+09] Baoping Chen, Guoqing Lu, Ronghua Hao, Liqiang Hu, and Xiushu Tian. Intelligent speed and mileage measurement system for vehicles based on hall sensor. In *2009 First International Workshop on Education Technology and Computer Science*, volume 2, pages 272–274. IEEE, 2009.

[Con19] Vibration Engineering Consultant. EMI Interference: Understanding and Mitigating AC and DC Magnetic Fields. 2019. https://www.vibeng.com/blog/emi-interference-understanding-and-mitigate-the-ac-and-dc-emi-interference. (Accessed: 03-23-2022).

[CSWL14] Xingguo Cheng, Zhenjun Sun, Xiaoyan Wang, and Sheng Liu. Open-loop linear differential current sensor based on dual-mode hall effect. *Measurement*, 50:29–33, 2014.

[CWAF17] Sujit Rokka Chhetri, Jiang Wan, and Mohammad Abdullah Al Faruque. Cross-domain security of cyber-physical systems. In *2017 22nd Asia and South Pacific design automation conference (ASP-DAC)*, pages 200–205. IEEE, 2017.

[data] ACS710 datasheet. https://www.allegromicro.com/~/media/Files/Datasheets/ACS710-Datasheet.ashx. (Accessed: 03-22-2022).

[datb] ACS715 datasheet. https://www.allegromicro.com/~/media/Files/Datasheets/ACS715-Datasheet.ashx. (Accessed: 03-22-2022).

[datc] ACS718 datasheet. https://www.allegromicro.com/~/media/Files/Datasheets/ACS718-Datasheet.ashx. (Accessed: 03-22-2022).

[datd] ACS724 datasheet. https://www.allegromicro.com/~/media/Files/Datasheets/ACS724-Datasheet.ashx. (Accessed: 03-22-2022).

[date] DRV5053 datasheet. https://www.ti.com/lit/ds/symlink/drv5053.pdf?HQS=TI-null-null-mousermode-df-pf-null-wwe&ts=1594782613247&ref_url=https%253A%252F%252Fwww.mouser.com%252F. (Accessed: 03-22-2022).

[datf] LTSR 6-NP datasheet. https://www.lem.com/sites/default/files/products_datasheets/ltsr_6-np.pdf. (Accessed: 03-22-2022).

[datg] LV 25-P datasheet. http://www.farnell.com/datasheets/51633.pdf. (Accessed: 03-22-2022).

[dath] SS39ET datasheet. https://www.digikey.com/htmldatasheets/production/43186/0/0/1/SS39ET-49E-59ET-Series-Datasheet.pdf. (Accessed: 03-22-2022).

[dati] 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).

[datj] SS49/SS19 datasheet. https://www.digikey.com/htmldatasheets/production/809995/0/0/1/SS49-SS19-Series-Install-Instr.pdf. (Accessed: 03-22-2022).

[EFM] Cortex-M3 Reference Manual: EFM32 Microcontroller Family. https://www.silabs.com/documents/public/reference-manuals/EFM32-Cortex-M3-RM.pdf. (Accessed: 03-22-2022).

[fera] According to Ferroxcube (formerly Philips) Soft Ferrites data. https://www.ferroxcube.com/zh-CN/download/download/21. (Accessed: 03-22-2022).

[ferb] Mn-Zn Toroid. https://content.kemet.com/datasheets/KEM_E5003_ESD-R-H.pdf. (Accessed: 03-23-2022).

[FK77] Otto Föllinger and Mathias Kluwe. *Laplace-und Fourier-Transformation*. Elitera Berlin, 1977.

[GGK+16] Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. Dancing on the lip of the volcano: Chosen ciphertext attacks on apple imessage. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pages 655–672, 2016.

[Gil06] Joe Gilbert. Technical advances in hall-effect sensing. *Allegro MicroSystems technical paper STP 00-1. http://www. allegromicro. com/techpub2/stp/stp00-1. pdf*, 2006.

[GN86] MC Gold and DA Nelson. Variable magnetic field hall effect measurements and analyses of high purity, hg vacancy (p-type) hgcdte. *Journal of Vacuum Science & Technology A: Vacuum, Surfaces, and Films*, 4(4):2040–2046, 1986.

[hal] Hall-Effect Current Sensor Market by Type, Technology, Output (Linear and Threshold), Industry (Industrial Automation, Automotive, Consumer Electronics, Telecommunication, Utilities, Medical, Railways), and Region - Global Forecast to 2023. https://www.marketsandmarkets.com/Market-Reports/hall-effect-current-sensor-market-201606539.html. (Accessed: 03-22-2022).

[Her91] F Herrmann. Teaching the magnetostatic field: Problems to avoid. *American Journal of Physics*, 59(5):447–452, 1991.

[HJBA20] William H Hayt Jr, John A Buck, and M Jaleel Akhtar. *Engineering Electromagnetics/ (SIE)*. McGraw-Hill Education, 2020.

[Hon19] Honeywell. HALL EFFECT SENSING AND APPLICATION. 2019. http://www.rsp-italy.it/Electronics/Databooks/Honeywell/_contents/Honeywell%20-%20Hall%20Effect%20Sensing%20and%20Application%201998.pdf. (Accessed: 03-23-2022).

[Hub09] Charles I Hubert. *Electric Machines: Theory, Operation, Applications, Adjustment & Control*. Pearson Education, 2.00 edition, 2009.

[KBC+13] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost talk: Mitigating emi signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159. IEEE, 2013.

[KDRB68] Werner Kutzelnigg, Giuseppe Del Re, and Gaston Berthier. Correlation coefficients for electronic wave functions. *Physical Review*, 172(1):49, 1968.

[KSG+99] Marian K Kazimierczuk, Giuseppe Sancineto, Gabriele Grandi, Ugo Reggiani, and Antonio Massarini. High-frequency small-signal model of ferrite core inductors. *IEEE Transactions on Magnetics*, 35(5):4185–4191, 1999.

[Lit] Littelfuse. Magnets and Actuators. https://www.littelfuse.com/~/media/electronics/datasheets/magnetic_actuators/littelfuse_magnetic_actuators_datasheet.pdf.pdf. (Accessed: 03-22-2022).

[mon] *Tektronix 119-6609-00*. https://www.testequipmentdepot.com/tektronix/accessories/cables-hardware/attachments/flexible-monopole-antenna-119660900.htm?ref=gbase. (Accessed: 03-22-2022).

[mum] *MU METAL SPECIFICATIONS*. http://mumetal.co.uk/?p=100#more-100. (Accessed: 03-22-2022).

[MVM09] F.P. Miller, A.F. Vandome, and J. McBrewster. *Lorentz Force*. Alphascript Publishing, 2009.

[NLHL13] Dong-Hyun Nam, Woo-Beom Lee, You-Sik Hong, and Sang-Suk Lee. Measurement of spatial pulse wave velocity by using a clip-type pulsimeter equipped with a hall sensor and photoplethysmography. *Sensors*, 13(4):4714–4723, 2013.

[OHN+08] Yoichi Ogo, Hidenori Hiramatsu, Kenji Nomura, Hiroshi Yanagi, Toshio Kamiya, Masahiro Hirano, and Hideo Hosono. p-channel thin-film transistor using p-type oxide semiconductor, sno. *Applied Physics Letters*, 93(3):032113, 2008.

[OWL03] G Ott, J Wrba, and R Lucke. Recent developments of mn–zn ferrites for high permeability applications. *Journal of Magnetism and Magnetic Materials*, 254:535–537, 2003.

[Pan12] Rames C Panda. *Introduction to PID controllers: theory, tuning and application to frontier areas*. BoD–Books on Demand, 2012.

[Pau12] Paul Peter Urone, Roger Hinrichs. College Physics. 2012. https://openstax.org/books/college-physics/pages/22-6-the-hall-effect. (Accessed: 03-22-2022).

[pow] STP4NK80Z. https://media.digikey.com/pdf/Data%20Sheets/ST%20Microelectronics%20PDFS/ST(D,P)4NK80Z(-1,FP).pdf. (Accessed: 03-23-2022).

[PP02] Gaetano Palumbo and Salvatore Pennisi. *Feedback amplifiers: theory and design*. Springer Science & Business Media, 2002.

[PSS+16] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. This ain't your dose: Sensor spoofing attack on medical infusion pump. In *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016.

[Ram11] Edward Ramsden. *Hall-effect sensors: theory and application*. Elsevier, 2011.

[RSHC18] Nirupam Roy, Sheng Shen, Haitham Hassanieh, and Romit Roy Choudhury. Inaudible voice commands: The long-range attack and defense. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, pages 547–560, Renton, WA, April 2018. USENIX Association.

[Shi14] Y. Shibuya. Magnetic Shielding Effect of a Spherical Shell. 2014. https://demonstrations.wolfram.com/MagneticShieldingEffectOfASphericalShell/. (Accessed: 03-23-2022).

[SKKK17] Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 445–467. Springer, 2017.

[SMTS13] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 55–72. Springer, 2013.

[SMY+15] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1004–1015, 2015.

[SNB+15] Yasser Shoukry, Pierluigi Nuzzo, Nicola Bezzo, Alberto L Sangiovanni-Vincentelli, Sanjit A Seshia, and Paulo Tabuada. 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)*, pages 3804–3809. IEEE, 2015.

[SWXL18] Yanjun Shi, Lu Wang, Ren Xie, and Hui Li. Design and implementation of a 100 kW SiC filter-less PV inverter with 5 kW/kg power density and 99.2% CEC efficiency. In *2018 IEEE Applied Power Electronics Conference and Exposition (APEC)*, pages 393–398. IEEE, 2018.

[TCC11] Yuan-Pin Tsai, Kun-Long Chen, and Nanming Chen. Design of a hall effect current microsensor for power networks. *IEEE Transactions on Smart Grid*, 2(3):421–427, 2011.

[tex] Grid-tied Solar Micro Inverter with MPPT. https://www.ti.com/tool/TIDM-SOLARUINV. (Accessed: 03-22-2022).

[TO2] *TO-220*. https://www.jameco.com/z/MJE8502-Motorola-TO-220-NPN-Power-Transistor-700V-5A_2281319.html. (Accessed: 03-22-2022).

[TWX+17] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In *2017 IEEE European symposium on security and privacy (EuroS&P)*, pages 3–18. IEEE, 2017.

[W+16] Guangyu Wu et al. A survey on the security of cyber-physical systems. *Control Theory and Technology*, 14(1):2–10, 2016.

[Wei01a] Martin H. Weik. *active sensor*, pages 21–21. Springer US, Boston, MA, 2001.

[Wei01b] Martin H. Weik. *passive sensor*, pages 1235–1235. Springer US, Boston, MA, 2001.

[WXZ+14] Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, and Guofei Gu. Srid: State relation based intrusion detection for false data injection attacks in scada. In *European Symposium on Research in Computer Security*, pages 401–418. Springer, 2014.

[XPHL12] Yue Xu, Hong-Bin Pan, Shu-Zhuan He, and Li Li. A highly sensitive cmos digital hall sensor for low magnetic field applications. *Sensors*, 12(2):2162–2174, 2012.

[ZYJ+17] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–117, 2017.