2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) | 979-8-3503-0062-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/HOST55118.2023.10133158

MagHop: Magnetic Spectrum Hopping for Securing Voltage and Current Magnetic Sensors

Anomadarshi Barua
Department of Electrical Engineering and Computer Science
University of California, Irvine
anomadab@uci.edu

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

***Abstract*—Voltage and current magnetic sensors (VCMSs) are pervasive in safety-critical systems. They use a magnetic field as a transduction medium to sense the input signal. Therefore, if an attacker manipulates the magnetic transduction medium of this sensor by using an intentional EMI or external magnetic fields, no amount of security mechanism after the fact can help. Fortunately, our work provides a defense against this form of physical attack. The core idea of our defense is to shift the frequency spectrum of the magnetic field, which is used as the transduction medium of the sensor, to another spectrum unknown to an attacker. In addition, the frequency spectrum, which carries the magnetic field in the transduction medium, is varied in a pseudo-random fashion so that the attacker will not be able to track it to inject any EMI into it. Even a sweeping attacker, who can vary the EMI's frequency, cannot bypass our defense because of *the check and select approach* of our defense. As the magnetic field's spectrum in the transduction medium of the sensor hops in a different spectrum, the defense is named as Magnetic Spectrum Hopping (MagHop). While prior works fail to prevent an EMI, which has the same frequency as the input signal, MagHop is equipped to handle this limitation of the prior works. Moreover, a low-power, real-time coherent prototype of MagHop is designed that is evaluated with a real-world application: a grid-tied inverter. Finally, we thoroughly evaluate MagHop on ten different sensors from six different manufacturers to prove its robustness against the EMI or external magnetic field injection attack on VCMSs.**

***Index Terms*—voltage and current magnetic sensor, EMI and magnetic field injection attack, magnetic transduction medium**

I. Introduction

A voltage or current signal is the most common signal in critical systems. Almost all analog signals from different modalities, such as electrical energy, acoustic, and vibration, are converted into voltage or current signals for further processing. Therefore, voltage and current sensors are abundant in safety-critical systems, ranging from computers to industrial controllers and automobiles to aircraft [1], [2], [3].

Among different voltage and current sensors present in the industry, Faraday's law and Hall effect based voltage and current sensors [4] are the widely used ones because of their galvanic isolation compared to the resistive drop/divider approach. Both sensors use a proportional magnetic field to sense the voltage and current signal and output a scaled-down signal. As these sensors use magnetic energy as a transduction medium, they are named voltage-current *magnetic* sensors (VCMSs) in our paper. Though researchers devote much of their efforts to improving their performance, their security is still neglected to date. And prior works [5], [6], [7], [8], [9] show that they are still not secured against attack signals, such as EMIs and magnetic fields. *The E-field and B-field of an EMI induces noise like voltage in VCMSs, and a pure magnetic field can perturb the magnetic transduction medium of VCMSs.*

Note that prior works [10], [11], [5], [12], [13] provide filtering and sampling-based defenses against unwanted attack signals. The main drawbacks of them are: *(i) they don't contain the injected EMIs/magnetic attack signals having the same frequency as the legitimate input voltage or current signal being measured, (ii) they cannot prevent an attacker, who can sweep the frequency of the injected EMIs, and (iii) they can't separate the injected magnetic field from the actual magnetic field, which is used as the transduction medium of VCMSs.*

Therefore, this paper proposes a novel defense to solve the above limitations. The core idea of the defense is that it shifts the frequency spectrum of the magnetic field, which is the transduction medium of VCMSs, to a different spectrum. The spectrum is varied in a pseudo-random fashion, so the attacker cannot inject EMIs into the unknown frequency spectrum. As the frequency spectrum of the magnetic field hops from one frequency to another within the sensor bandwidth, the defense is named as Magnetic Spectrum Hopping (MagHop).

As the magnetic field's frequency spectrum in the transduction medium of VCMSs is shifted to an unknown frequency, the proportional input signal and the corresponding output signal of the sensor are also shifted to the same spectrum, which is also unknown to the attacker. The pseudo-random variation of the spectrum is only known to VCMSs. Therefore, an attacker, who uses EMIs to inject E-field or B-field into VCMSs, cannot interfere with an unknown frequency spectrum of the magnetic field in the transduction stage. Moreover, an attacker, who also targets the conductors connected with the input and output of VCMSs, cannot inject any EMIs into the input and output signal, because the frequency spectrum of the input and output signal is also shifted to an unknown spectrum. Even a strong attacker, who can sweep the frequency of the EMIs, cannot interfere with the frequency spectrum of the magnetic field in the transduction stage. The reason behind this is that the defense always checks whether the spectrum is attacked by the EMIs before switching to that spectrum. Last but not least, the defense syncs up all the fragmented

979-8-3503-0062-8/23/$31.00 ©2023 IEEE

pseudo-random frequency spectrum at the output, so that the signal being measured is always coherent. *Hence, the defense never hampers the real-time behavior of the sensor.* We believe that our idea and implementation details will be beneficial to building the next generation of *secured* VCMSs having robust immunity to both EMIs and magnetic fields.

Contributions: Our main technical contributions are:

1. We introduce a methodology to pseudo-randomly vary the frequency spectrum of the magnetic field used as the transduction medium of voltage and current magnetic sensors.

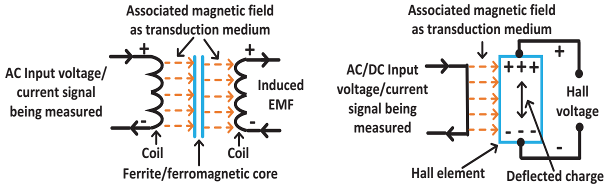
2. We show the effectiveness of MagHop against the injected EMIs or magnetic fields through experiments on ten different VCMSs from six different manufacturers. We experiment with both types, Faraday's law and Hall effect based VCMSs.

3. We do a low-power implementation of MagHop on an FPGA and Cortex-M processor and prove its real-time efficacy on a practical grid-tied solar inverter system.

II. Background

A. *Voltage & current magnetic sensor (VCMS)*

According to Ampere's law [14] of electromagnetism, a current signal has magnetic fields *associated* with it. VCMSs use the *associated magnetic field* to measure the voltage and current. Broadly speaking, the associated magnetic fields are used in two different techniques in VCMSs. The first one is related to Faraday's law and the second one is related to the Hall effect. These two techniques are briefly explained below.



Associated magnetic field as transduction medium
AC Input voltage/ current signal being measured
+
-
Induced EMF
+
-
Coil
Coil
Ferrite/ferromagnetic core
Associated magnetic field as transduction medium
AC/DC Input voltage/current signal being measured
+++

+
-
Hall voltage
Hall element
Deflected charge

Figure 1. (Left) Faraday's law and (Right) Hall effect based VCMS.

Faraday's law based VCMSs: A time-varying (i.e., AC) voltage or current signal has a time-varying magnetic field associated with it. Faraday's law of induction [15] states that a time-varying magnetic field can induce a proportional time-varying electromotive force (EMF) in a coil. Therefore, Faraday's law based VCMSs use the induced EMF to measure the time-varying voltage or current. A current transformer (CT), potential transformer (PT), audio transformer, and Rogowski coil are examples of this type (see Fig. 1 (Left)). This type uses a *ferrite/ferromagnetic* core [16] to host the coil, where the EMF is induced. As the ferrite core has high bandwidth (i.e., ∼ kHz), these sensors can measure high frequency signals. The high bandwidth of the ferrite/ferromagnetic core enables *magnetic spectrum hopping* technique in our defense.

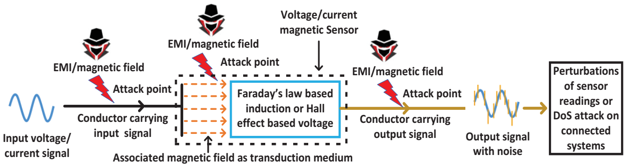
Hall effect based VCMSs: A Hall effect based VCMS has a Hall element (i.e., p-type semiconductor) (see Fig. 1 (Right)). When the Hall element is placed in the *magnetic field associated with a voltage or current signal*, the moving charge present inside of the Hall element gets deflected across it by obeying the Lorentz law [17]. This deflection across the Hall element generates a voltage known as Hall voltage, which is proportional to the magnetic fields associated with voltage or current signals. Either a constant or a time-varying associated magnetic field can deflect the moving charge of the Hall element. Therefore, Hall effect based VCMSs can measure both AC and DC signals. Similar to the ferrite/ferromagnetic core, the Hall element has high bandwidth (i.e., ∼ kHz) that enables *magnetic spectrum hopping* technique in our defense.

B. *Importance and security consequences*

VCMSs have good linearity, high accuracy, and faster response with galvanic isolation and are abundant in safety-critical systems. However, they are still not secured because these sensors cannot differentiate between the original associated magnetic field and the fake magnetic field injected by an attacker in the form of an EMI. The injected fake signal can be propagated to connected systems, resulting in a denial-of-service (DoS) attack on the system. A similar incident is found in the literature where an opportunistic attacker injects fake magnetic fields to current magnetic sensors in a microgrid, causing a blackout in the power system [18]. Therefore, a robust defense is much needed to make VCMSs secure against intentional EMI/magnetic field injection.

III. Threat Model

We first explain the following four components of the threat model (see Fig. 2) against which our defense works.



Voltage/current magnetic Sensor
EMI/magnetic field
Attack point
EMI/magnetic field
Attack point
EMI/magnetic field
Attack point
Input voltage/ current signal
Conductor carrying input signal
Faraday's law based induction or Hall effect based voltage
Conductor carrying output signal
Output signal with noise
Perturbations of sensor readings or DoS attack on connected systems
Associated magnetic field as transduction medium

Figure 2. The threat model for the proposed defense.

1. Attacker's target: The attacker uses electromagnetic energy from a distance to *noninvasively* inject malicious signals into VCMSs. In this way, the attacker can inject false data into VCMSs that can eventually propagate to connected systems, resulting in an erroneous state or DoS attack on the system. The attacker may not get a long time to *modify or observe* the target VCMS like a lunch-time attack [19] or is not allowed to physically alter any parts of VCMSs. Attackers can target two attack points: (i) magnetic transduction medium of VCMSs and (ii) connected conductors which behave as antennas.

2. Attack signal's bandwidth: *The attacker can use EMIs with single or multiple tones to inject false data into VCMSs.* Moreover, the injected EMI can have the same bandwidth as the original signal, making it difficult to differentiate between injected EMIs and original signals. The attacker can vary the injected EMI's frequency in different ways. For example, a *static attacker* can inject EMIs with static frequency for a long time. A *sweeping attacker* can vary the EMI's frequency in a random or particular order. A *responsive attacker* at first can sense the frequency of the ongoing voltage or current signal and next use the same frequency EMI to attack the sensors.

3. Attack tool: The attacker can use an electromagnet to inject only B-field or an antenna connected with an oscillating signal to inject both E-field and B-field into VCMSs.

4. Penetrating the sensor shield: VCMSs may or may not be placed inside a shield [20] depending on their applications. In the presence of a shield, the injected EMI/magnetic field should be strong enough to penetrate the shield first.

IV. Modeling and Evaluating the Attack

Here, we mathematically model the consequences of our attack model and evaluate it through experiments.

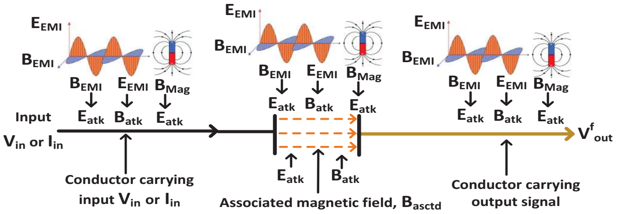

E_{EMI}
B_{EMI}
B_{EMI} E_{EMI} B_{Mag}
E_{atk} B_{atk} E_{atk}
Input
V_{in} or I_{in}
Conductor carrying input V_{in} or I_{in}
E_{atk}
B_{atk}
Associated magnetic field, B_{asctd}
Conductor carrying output signal
V^f_{out}

Figure 3. The surrounding electromagnetic field of the conductor and the associated magnetic field are perturbed by the injected EMI/magnetic field.

A. *Mathematical modeling*

Let us denote the input voltage and current signal being measured by the VCMS as V_{in} and I_{in}, respectively. The magnetic field density associated with the V_{in} or I_{in} is denoted by B_{asctd}. Ampere's law states that $B_{asctd} \propto \{V_{in} \text{ or } I_{in}\}$ (see Eqn. 1). The associated field B_{asctd} is induced in a ferrite/ferromagnetic core (i.e., Faraday's law) or sensed by the Hall element (i.e., Hall effect), resulting in a sensor output voltage. Let us denote the sensor output voltage *before an attack* by V_{out}, which is modeled by Eqn. 2.

$$B_{asctd} = k_1 V_{in} \;\text{ or }\; k_1 I_{in}; \quad \text{Ampere's law.} \tag{1}$$

$$V_{out} = \begin{cases} k_2 \frac{\delta B_{asctd}}{\delta t} = k_6\{V_{in} \,\text{or}\, I_{in}\}; & \text{Faraday's law,} \\ k_3 B_{asctd} = k_6\{V_{in} \,\text{or}\, I_{in}\}; & \text{Hall effect.} \end{cases} \tag{2}$$

where k_1, k_2, k_3, and k_6 are proportionality constants and depend on the properties of ferrite core and Hall element.

Fig. 3 illustrates that the B_{asctd} is the only medium for information transfer from the input stage (i.e., V_{in} or I_{in}) to the output stage (i.e., V_{out}) of VCMSs and there is no authentication or encryption in this magnetic medium. Therefore, an attacker can simply inject an external magnetic field into the magnetic medium to perturb the input signal V_{in} or I_{in}.

The attacker can use an EMI or electromagnet as the *attack-source*. Let us denote the electric and magnetic fields in EMIs by E_{EMI} and B_{EMI}, respectively. Let us denote the magnetic field from an electromagnet by B_{Mag}. The terms E_{EMI} and B_{EMI} from an EMI are always time-varying. The field B_{Mag} from an electromagnet, can be *static or time-varying* depending upon how the power is given to the electromagnet.

From Maxwell's equations [14], the attack electric field E_{EMI} generates a magnetic field B_{atk} (see Eqn. 3), and the attack magnetic field B_{EMI} or B_{Mag} generate an electric field E_{atk} (see Eqn. 4). The generated B_{atk} and E_{atk} are added to Eqn. 2, resulting in a false output voltage V^f_{out} (see Eqn. 5).

$$\Delta \times B_{atk} = \qquad k_4 \frac{\delta E_{EMI}}{\delta t}; \qquad \text{Maxwell's eqn.} \tag{3}$$

$$\Delta \times E_{atk} = -k_5 (\frac{\delta B_{EMI}}{\delta t} or \frac{\delta B_{Mag}}{\delta t}); \quad \text{Maxwell's eqn.} \tag{4}$$

$$V^f_{out} = \begin{cases} k_2 \frac{\delta(B_{asctd} + B_{atk})}{\delta t} - E_{atk}\, \delta s; & \text{Faraday's law,} \\ k_3 (B_{asctd} + B_{atk}) - E_{atk}\, \delta s; & \text{Hall effect.} \end{cases} \tag{5}$$

where k_4 and k_5 are proportionality constants, and δs is the direction along which δE_{atk} changes. The R.H.S of Eqn. 5 indicates that the fake output voltage V^f_{out} from the target sensor has the cumulative effect of the injected EMI or magnetic field by the attacker.

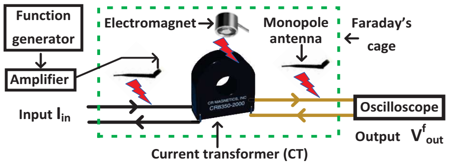


Figure 4. Experimental setup for the attack model evaluation.

B. *Evaluating the attack model*

We evaluate the attack model from Eqn. 5 with the experimental setup shown in Fig. 4. A Faraday's law based CT (part# CR8348-2000 [21]) is used as the target sensor. An off-the-shelf electromagnet (part # Grove [22]) having a strength of 1000 Gauss is used to inject a magnetic field into the sensor from a 1 cm distance. Moreover, an antenna is used to inject 1 kHz EMI into the conductor connected to the sensor from a 1 cm distance. The antenna has a 3 dB gain and 1 W input power from an amplifier and signal generator. The experimental setup is placed inside a Faraday's cage [23] to avoid external noise.

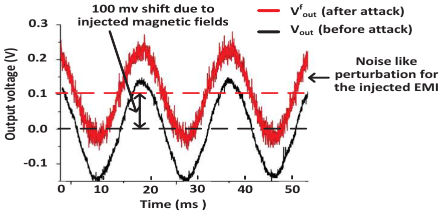


Figure 5. EMI/magnetic fields injected into the CT and connected conductor.

Results: A 60 Hz and 150 mV peak signal is given as input to the CT (see Fig. 5). The 1 kHz EMI signal injects noise-like perturbations into the sensor corrupting its measurement. The 1000 Gauss static magnetic field from the electromagnet adds a DC offset to the sensor's output. This shifts the V_{out} by 100 mV upward. The fake output voltage after an attack (i.e., V^f_{out}) has the accumulated impacts of B_{EMI}, E_{EMI}, and B_{Mag} on the CT, supporting our attack model.

V. Motivation and Defense Outline

A. *Motivation*

Let us first denote the input voltage or current signal (i.e., $V_{in}\, or\, I_{in}$) being measured has a bandwidth BW_{in}. If an injected EMI has a bandwidth BW_{atk}, Eqns. 3 and 4 indicate that the electric and magnetic field attack components E_{atk} and B_{atk} also have the same bandwidth BW_{atk}.

A *naive* defense could be to use adaptive or other different filters [10], [11], [5], [12], [13] to remove the attack bandwidth BW_{atk}. This strategy fails in the following two scenarios:

- First, if the attack frequency BW_{atk} overlaps with the input signal's frequency BW_{in}, a filter-based defense may filter out BW_{in} while filtering BW_{atk}, resulting in a distortion.
- Second, if a sweeping/responsive attacker sweeps the frequency of the injected EMI, the filter-based defenses may

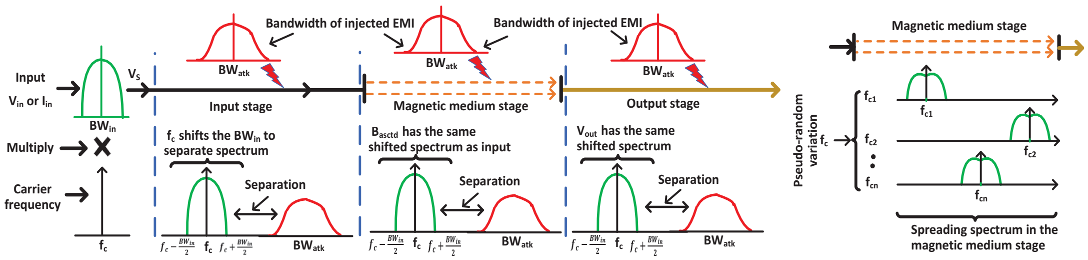


Figure 6. (Left) The bandwidth BW_{in} of an input signal is shifted to a separate spectrum so that it does not interfere with the BW_{atk} of injected EMIs. (Right) The pseudo-random hopping of B_{asctd} causes a spread spectrum in the magnetic medium stage.

not be able to track the *sweeping* frequency. Therefore, they may not be successful against a sweeping/responsive attacker.

In the next section, we discuss why our proposed defense is strong enough to solve the above two major limitations of the recent work [10], [11], [5], [12], [13].

B. Defense outline

To ease the explanation of the defense, we divide the pipeline of VCMS into the following three stages:

(i) **Input stage:** where the voltage or current signal (V_{in} or I_{in}) is given as input to measure the signal.

(ii) **Magnetic medium stage:** it is the transduction stage where input signal V_{in} or I_{in} is transferred to the output stage via an associated magnetic field B_{asctd}.

(iii) **Output stage:** where a scaled down output voltage V_{out} is generated proportional to the input V_{in} or I_{in}.

The attack model in Eqn. 5 holds for the injected EMI/magnetic fields in all stages of the sensor.

- **Attack modalities:** Attack components in Eqn. 5 have two different modalities: B_{atk} is the attack magnetic field and E_{atk} is the attack electric field. Our proposed defense adopts the following strategies to work against the E_{atk} and B_{atk} that are also illustrated in Fig. 6.

*1) **Defense against the attack electric field E_{atk}**:* To separate the E_{atk} from the input V_{in} or I_{in} signal being measured, our defense MagHop uses an unknown frequency to separate the input V_{in} or I_{in} signal from the E_{atk}. The unknown frequency is defined as the carrier frequency, f_c. When a carrier frequency carries a voltage or current signal, the bandwidth BW_{in} of the input signal is shifted to the carrier frequency f_c. If we consider a voltage or current signal, V_{in} or I_{in} = $A_{in}cos(2\pi BW_{in}t)$ with bandwidth BW_{in} and a carrier signal $c(t)$ = $A_c cos(2\pi f_c t)$, the frequency shifting process is expressed by multiplication as follows:

$$\begin{aligned} V_s &= A_{in}cos(2\pi BW_{in}t) \times A_c cos(2\pi f_c t) \\ &= A_{in} + A_c\{2\pi(f_c + BW_{in})t\} \end{aligned} \tag{6}$$

where A_{in} and A_c are the amplitudes of the voltage or current signal being measured and carrier signal, respectively, and V_s is the signal after the frequency shift to f_c + BW_{in}.

The shifting process shifts the BW_{in} in such a way that f_c ± $BW_{in}/2$ does not co-inside with BW_{atk}. Therefore, after frequency shifting, a filter can separate the attack frequency BW_{atk} from the input V_{in} or I_{in} signal. In this way, the E_{atk} can be removed from the input voltage or current signal.

*2) **Defense against the B_{atk}**:* Eqn. 1 implies that if V_{in} or I_{in} has a bandwidth BW_{in}, the B_{asctd} should also have the same bandwidth BW_{in}. Therefore, when a carrier frequency shifts the BW_{in} to $f_c \pm BW_{in}/2$, the frequency spectrum of the B_{asctd} is also shifted to $f_c \pm BW_{in}/2$. Because of this shifting, the attack magnetic field B_{atk} cannot interfere with the B_{asctd}. The frequency shifting of the B_{asctd} takes place in the *magnetic medium stage* of the sensor (Fig. 6 (Left)).

*3) **Mathematical intuition**:* Eqn. 5 can be written after an injection of EMI/magnetic fields to VCMSs as:

$$V_{out}^f = \begin{cases} V_{out} + k_2\frac{B_{atk}}{\delta t} - E_{atk}\,\delta s; & \text{Faraday's law,} \\ V_{out} + k_3 B_{atk} - E_{atk}\,\delta s; & \text{Hall effect.} \end{cases} \tag{7}$$

where V_{out} is the output voltage of VCMSs before an attack. MagHop uses a carrier frequency f_c to shift the frequency spectrum of V_{out}. Therefore, the V_{out} will have a different spectrum than the attack signal (i.e., E_{atk} and B_{atk}). Therefore, a filter can separate the V_{out} from the attack signals.

*4) **Choice of the carrier frequency**:* Please note that the success of MagHop relies on how we choose the carrier frequency f_c. After shifting the spectrum of the input voltage or current signal and its associated magnetic fields, we must ensure that it does not overlap with the bandwidth BW_{atk} of the injected EMIs. This technique has a few pitfalls.

Pitfall 1 - Sweeping and responsive attacker: One solution could be, at first, we need to calculate the bandwidth BW_{atk} and use BW_{atk} to calculate the correct carrier frequency f_c. This strategy could work against a static attacker, who keeps the bandwidth BW_{atk} static. However, it may not work against a sweeping/responsive attacker because the BW_{atk} must be calculated whenever the sweeping attacker changes it. The calculation of BW_{atk} requires Fast Fourier transformation (FFT) [24], which is computationally expensive, taking a finite amount of computation time. Therefore, if the sweeping/responsive attacker sweeps the bandwidth BW_{atk}, within the BW_{atk} computation time, the defense may not work.

Pitfall 2 - Hampering real-time sensor measurement: In addition, while waiting for the FFT computation, the input voltage or current signal cannot be transferred from the *input stage* to the *output stage* of VCMSs due to the lack of a correct carrier frequency f_c. Therefore, the sensor needs to wait, and this wait time may hamper the real-time measurement.

Solution: Pitfalls 1 and 2 imply that MagHop should avoid measuring the BW_{atk} of the injected EMI/magnetic fields to avoid FFT calculation. Therefore, we propose to pseudo-randomly vary the carrier frequency f_c to avoid these pitfalls.

Eqn. 6 indicates that if the carrier frequency varies in a pseudo-random fashion, the frequency spectrum BW_{in} of the input signal V_{in} or I_{in} also varies in the same pseudo-random fashion. Therefore, a static attacker cannot interfere with the input signal's frequency spectrum because it is not static anymore. Moreover, a sweeping/responsive attacker cannot also interfere because he/she does not know the pseudo-random sequence of the carrier frequency variation.

The probability of overlapping with the bandwidth BW_{atk} of injected EMIs/magnetic fields depends upon the number of frequency channels among which the carrier frequency hops from one another. For example, if there is n carrier frequencies: $\{f_{c1}, f_{c2}, .., f_{cn}\}$, the probability of overlapping is $1/n$. Therefore, for a large n, the probability of overlapping with the bandwidth BW_{atk} is reduced. In our design, we have used n = 255 channels, among which f_c can hop in a pseudo-random fashion. Therefore, it has only a 1/255 = 0.39% chance to overlap with the bandwidth BW_{atk} of injected EMIs.

Pseudo-random variation of f_c is not enough: Though the pseudo-random variation of the f_c gives a very low (i.e., 0.39%) chance of overlapping, however, the attacker still has this low chance to perturb the input signal's frequency. Specifically, a sweeping attacker, who can sweep the EMI's bandwidth BW_{atk}, may be lucky enough to overlap with the input signal's frequency spectrum after several attempts.

Solution - Check and select approach: MagHop ensures that the overlapping with the input signal's frequency does not happen even after several attempts in the following way. After selecting a carrier frequency f_c from n members, $\{f_{c1}, f_{c2}, ., f_{cn}\}$, MagHop first checks whether f_c has any interference with injected EMIs. If there is no interference, only then that carrier frequency will be selected. If there is an interference, that carrier frequency is skipped, and a new frequency is selected pseudo-randomly from n members. A check circuit, present in the sensor pipeline's output stage, is used to tune on the carrier frequency f_c to sense the presence of interference (see Section VI-D for details).

*5) **Magnetic Spectrum Hopping (MagHop)**:* Here, we explain why we name the defense as magnetic spectrum hopping (MagHop). When the carrier frequency f_c is varied or *hopped* within a set of n members, the hopping of f_c also results in periodic shifting of input signal's (i.e., V_{in} or I_{in}) frequency spectrum. As the associated magnetic field B_{asctd} is proportional to V_{in} or i_{in}, the spectrum of B_{asctd} also hops within the same set of n members. As the B_{asctd} is the magnetic transduction medium, this frequency hopping technique is termed as magnetic spectrum hopping, shortly MagHop (see Fig. 6 (Right)). Because of the frequency hopping in the magnetic medium stage, the proportional sensor output voltage V_{out} has the same spread spectrum in the output stage of the sensor pipeline. Therefore, the V_{out} is also immune to injected EMI/magnetic fields in the output stage conductor.

VI. Implementation of MagHop

The blocks used in MagHop are shown in Fig. 7. MagHop has two blocks in the input stage of the sensor pipeline: (i) Pseudo-random frequency generator and (ii) Modulator.

*A. **Pseudo-Random Frequency Generator (PRFG)***

The PRFG generates a carrier frequency f_c, which hops within a set $S = \{f_{c1}, f_{c2}, f_{c3}, f_{c4}, ..., f_{cn}\}$ of n members, in a pseudo-random fashion. It has the following steps.

Maximal sequence pseudo-random code: An 8-bit linear feedback shift register (LFSR) with 4 tap positions is used to generate a maximal sequence pseudo-random code. A maximal code would be the ideal secured code [25] since it has the lowest possible auto-correlation and is easy to generate. The 8-bit LFSR can generate 2^8 - 1 = 255 (a value of zero is not possible) pseudo-codes. A pseudo-code corresponds to a carrier frequency. Therefore, n = 255 carrier frequencies are present in set S. A n = 255 carrier frequencies seemed reasonable because large values of n may reduce the separation between two adjacent carrier frequencies, resulting in a reliability issue. For example, if the separation between two adjacent carrier frequencies, say separation between f_{c1} and f_{c2} is low, there is a chance that both f_{c1} and f_{c2} can be within the same bandwidth BW_{atk} of the injected EMIs. As MagHop has the *check and select* approach, in this case, neither f_{c1} nor f_{c2} will be selected as the carrier frequency.

Code security: There are 12 different combinations of 4 tap positions that can generate maximal sequences in an 8-bit LFSR [26]. As we always keep one tap at position 8 and we don't use position 1 for tapping, there are only 8 possible tap combinations that can generate 255 maximal sequences. These 8 possible combinations of 4 tap positions are: (8,4,3,2), (8,5,3,2), (8,6,3,2), (8,6,5,2), (8,6,5,3), (8,6,5,4), (8,7,3,2), and (8,7,5,3). After every 255 cycles, the tap positions are dynamically changed to a random set of tap positions (i.e., (8,4,3,2) to (8,6,5,4)) so that attackers may not track the codes.

Largest carrier frequency: The generated carrier frequencies should support the sensor bandwidth. Therefore, the largest carrier frequency f_{cn} in the set S should always be less than the sensor bandwidth, denoted by BW_S, and the relationship can be expressed by Eqn. 8.

$$BW_S \geq f_{cn} + \frac{1}{2}BW_{in} \tag{8}$$

Look-up table: A faster approach to generate carrier frequencies is to take values from a look-up table. The look-up table must have values, at a minimum, twice the number of possible carrier frequencies because of the *Nyquist criteria*. Since there are n = 255 possible carrier frequencies, there must be a minimum of 510 values in the table. For an improved quality of the generated waveform, a total of v = 2048 values are used in the look-up table in our design. A digital-to-analog (DAC) converter takes v = 2048 values from the look-up table and generates the carrier sine wave. If the DAC takes values from the look-up table at a rate of f_{DAC} Hz, the minimum frequency of the generated sine wave is $\approx f_{DAC}$ / v. To change the frequency, DAC can skip some values from the look-up table. For example, if every other value is taken instead of every value from the table, the frequency gets doubled. If m is the output of the pseudo-random code generator (i.e., 1 to 255), then the carrier frequency can be calculated by Eqn. 9.

$$f_c = f_{DAC} \times \frac{m}{v} \tag{9}$$

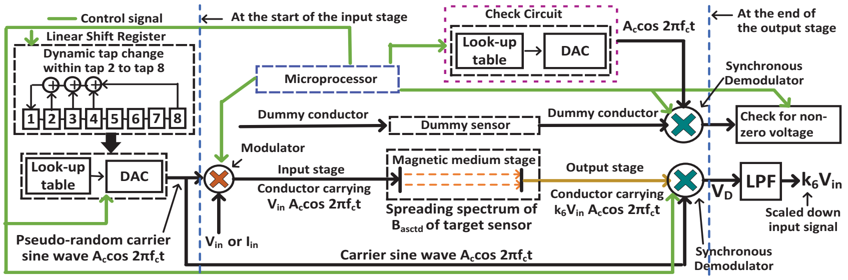

Control signal
At the start of the input stage
Check Circuit
Linear Shift Register
Dynamic tap change within tap 2 to tap 8
1
2
3
4
5
6
7
8
Microprocessor
Look-up table
DAC
$A_c$cos 2πf_ct
At the end of the output stage
Synchronous Demodulator
Dummy conductor
Dummy sensor
Dummy conductor
Check for non-zero voltage
Modulator
Look-up table
DAC
Input stage
Conductor carrying V_{in} $A_c$cos 2πf_ct
Magnetic medium stage
Spreading spectrum of B_{asctd} of target sensor
Output stage
Conductor carrying k_6V_{in} $A_c$cos 2πf_ct
V_D
LPF
k_6V_{in}
Scaled down input signal
Pseudo-random carrier sine wave $A_c$cos 2πf_ct
V_{in} or I_{in}
Carrier sine wave $A_c$cos 2πf_ct
Synchronous Demodulator

Figure 7. The implementation details of the proposed defense MagHop. There are 4 taps and the dynamic tap change happens within tap 2 to tap 8.

If m is not a factor of v, the generated wave is not sinusoidal. Interpolation [27] is used to solve this issue.

B. *Modulator*

The carrier wave $A_c cos(2\pi f_c t)$ from the PRFG is multiplied (see Fig. 7) by the input V_{in} or I_{in} (a proportional V_{in} is generated from I_{in}) by a modulator as below.

$$V_M = V_{in} \times A_c cos(2\pi f_c t) \tag{10}$$

The modulation takes place at the start of the input stage of the sensor pipeline. The carrier frequencies, which are *greater* than the bandwidth BW_{in} of the input V_{in} or I_{in}, are chosen for the modulation. As the $B_{asctd} \propto V_{in}$ or I_{in}, the frequency spectrum of the B_{asctd} is also spread in the *magnetic medium stage* and a scaled-down proportional voltage V_{out} is generated at senor's output, which can be written as,

$$V_{out} = k_6 \times V_{in} \times A_c cos(2\pi f_c t) \tag{11}$$

where k_6 is the scaling factor. *Because of the shifted frequency spectrum in the input and output stages of the sensor, the EMIs induced in the connecting conductors in the input and output stages cannot perturb the signal.*

C. *Synchronous demodulator*

A synchronous demodulator recovers the input V_{in} or I_{in} from the shifted spectrum *at the end of the output stage*. It multiplies the output V_{out} with the same carrier signal as:

$$\begin{aligned} V_D &= k_6 \times A_c cos(2\pi f_c t) \times V_{in} \times A_c cos(2\pi f_c t + \phi) \\ &= k_6(A_c^2/2)cos\phi \times V_{in} + k_6(A_c^2/2)cos(4\pi f_c t + \phi) \times V_{in} \end{aligned} \tag{12}$$

where ϕ is the phase difference present between the carrier signal from the modulator and the demodulator. A low-pass filter (LPF) can simply filter out the high frequency part $k_6(A_c^2/2)cos(4\pi f_c t + \phi) \times V_{in}$ from Eqn. 12 and gives output only the low frequency part $k_6(A_c^2/2)cos\phi \times V_{in}$.

As the same carrier signal generated in the PRFG is given to the modulator and demodulator, the phase difference ϕ is close to zero and constant. Therefore, the term $k_6 A_c^2$ /2 cosϕ is also constant in Eqn. 12, and a simple amplifier gives the correct $k_6 V_{in}$, which is a scaled-down version of V_{in}, at its output. The LPF does the amplification.

D. *Check circuit*

The *check and select* approach checks if the carrier frequency interferes with the EMI's bandwidth BW_{atk}. A check circuit, made with a look-up table and a DAC, executes the *check and select* approach. The check circuit is connected with a dummy conductor and a dummy sensor, which have the same physical properties as the input signal carrying conductor and target magnetic sensor, respectively. The dummy sensor and conductor are placed close to the input signal carrying conductor and target sensor. Therefore, they can sense the same EMIs injected into the target sensor/conductor and provide this signal to a synchronous demodulator (Fig. 7).

The check circuit generates the same f_c *before* the modulator uses the f_c to modulate the input V_{in} or I_{in} (see Section VI-E), and provides the carrier signal to a synchronous demodulator. The check circuit also varies the carrier frequency within $f_c - BW_{in}/2$ to $f_c + BW_{in}/2$. If the EMI's bandwidth BW_{atk} interferes within $f_c - BW_{in}/2$ to $f_c + BW_{in}/2$, Eqn. 12 indicates that a non-zero voltage will be generated at the output of the synchronous demodulator. The presence of a non-zero voltage indicates that the EMI interferes with the carrier frequency. Therefore, the current carrier frequency is discarded, and a new carrier frequency will be chosen next.

E. *Coherency, real-time measurement, and overhead*

An important question is how MagHop keeps a real-time and coherent measurement of the voltage or current signals. As different carrier frequencies carry the bandwidth BW_{in} of the input V_{in} or I_{in}, the signal gets fragmented. The reassembly of the fragmented signal after the demodulation is challenging because the coherency among fragments should be maintained. Here, a critical parameter is how long MagHop takes to generate a carrier signal. Let us denote it by generation time, t_{gen}. Another important parameter is how long a carrier frequency operates before hopping to another carrier frequency. Let's denote it by operating time, t_{op} (Fig. 8).

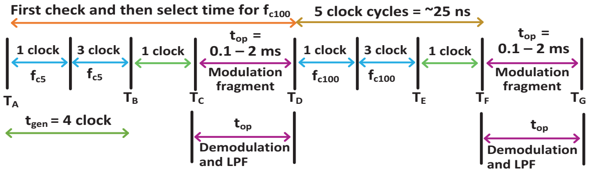


Figure 8. Timing information of MagHop for keeping real-time coherency.

It takes one clock cycle to generate a pseudo-random code by the LFSR. It takes another 3 clock cycles to calculate how the look-up table will be sampled by DAC to generate the carrier wave. Therefore, the carrier wave is generated after t_{gen} = 4 clock cycles. The operating time t_{op} is chosen by the designer. It is kept short so that the attacker cannot anticipate the carrier frequency. We choose t_{op} within 0.1 ms - 2 ms.

Let's say, within time $T_A \rightarrow T_B$ (4 clocks), a pseudo-random carrier frequency, say f_{c5} is generated. The time $T_B \rightarrow T_C$ (1 clock) is used to prepare for modulation. The carrier frequency f_{c5} operates for t_{op} = $T_C \rightarrow T_D$, where the modulation takes place. During $T_C \rightarrow T_D$, parallelly, a demodulation takes place in the synchronous demodulator.

Again, within $T_D \rightarrow T_F$ (5 clocks), a new carrier frequency, say f_{c100} is prepared, and within $T_F \rightarrow T_G$ both the modulation and demodulation take place by f_{c100}. The check circuit finishes the interference checking for carrier frequency f_{c100} within $T_A \rightarrow T_D$ before the f_{c100} is generated. Therefore, no extra time is used for the *check and select* approach. It is apparent that there is a 5 clock cycles gap (i.e., $T_D \rightarrow T_F$) between one modulation fragment $T_C \rightarrow T_D$ to the next modulation fragment $T_F \rightarrow T_G$. As the PRFG has a high-speed clock with a period 5ns, the 5 clock cycles is only 25 ns. As the bandwidth of VCMSs is typically 0 - 200 kHz (i.e., $\sim$ 5 μs), the 25 ns is 200x times smaller than the smallest rate of change of the input voltage or current signal. Therefore, a 5-clock delay does not hamper the coherency and real-time behavior of any of the existing sensors. Moreover, as the check circuit works ahead of the next carrier frequency being generated, the *check and select* approach does not overload the defense. In addition, The LPF parallelly works within the demodulation time $T_C \rightarrow T_D$. Therefore, the LPF does not hamper the coherency of VCMSs.

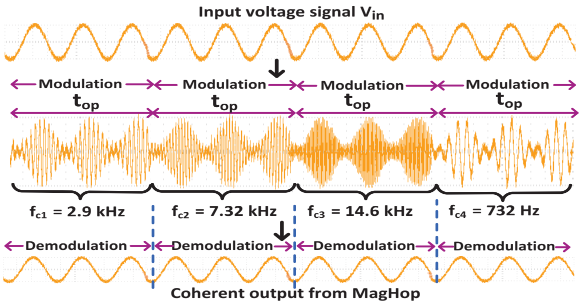


Figure 9. The output of MagHop is coherent.

Justification: To justify the coherency, a voltage sensor LV25P is connected with MagHop. A 10 V and 100 Hz signal is given as an input V_{in} to the sensor. The bandwidth 0-25 kHz of the LV25P is divided into 255 carrier frequencies. As the input signal is 100 Hz, the carrier frequencies are selected within 100 Hz $< f_c <$ 25 kHz in a pseudo-random fashion. Fig. 9 shows four such carrier frequencies. which are selected pseudo-randomly to modulate the input V_{in}. Each carrier frequency modulates the V_{in} for t_{op} before switching to the next carrier frequency. A simultaneous demodulation takes place within each t_{op}. Fig. 9 indicates that the output signal is coherent and real-time after the demodulation.

F. *Defense algorithm and control signals*

The algorithm 1, which binds together all the components of MagHop, runs on a microprocessor. The microprocessor generates control signals to the PRFG to start and stop the shift register and sampling from the look-up table. The control signal also syncs the operation of the check circuit with the PRFG and controls their execution order following Fig. 8. Another control signal controls the start and stop of the operating time, t_{op}. Lines 1-14 in algorithm 1 are self-explanatory and already discussed in detail in previous sections.

G. *Security of the defense itself*

A question may arise what will happen if the attacker attacks the defense itself? The defense does not have any magnetic medium stage; therefore, it could not be directly impacted by the attack. However, in an extreme case, the attacker can cause a random bit flip in the LFSR/look-up table using EMI. It may result in a new carrier frequency. However, this will not create any problem as the carrier frequency is still unknown to the attacker. As the *same* carrier frequency is used in the modulator and synchronous demodulator, any change/perturbation in this will not hamper the normal processing of the defense.

Algorithm 1: Defense algorithm.

```
   Input: Voltage/current signal $V_{in}$ or $I_{in}$ being measured
   Output: Scaled down voltage: $k_6 V_{in}$
1  POINT A:
2  Generate pseudo-random code $m$ & configure DAC to sample
     look-up table
3  Sample the look-up table and generate the carrier wave, $f_c$
4  Check circuit checks if $f_c$ has interference with $BW_{atk}$
5  while $f_c$ has interference do
6      Generate the next pseudo-random code $m$
7      Generate another carrier wave, $f_c$
8      Check circuit checks if $f_c$ has interference with $BW_{atk}$
9  Start the modulator
10 Shift the bandwidth $BW_{in}$ of the $V_{in}$ or $I_{in}$ to $f_c \pm BW_{in}/2$
11 Continue transmission for one operating time, $t_{op}$
12 Parallel demodulation by the synchronous demodulator
13 The LPF outputs $k_6 V_{in}$
14 If operating time, $t_{op}$ is over, JUMP to POINT A and iterate over
```

H. *A prototype*

A prototype of MagHop is shown in Fig. 10 (Left). The LFSR and the look-up table are implemented on a Zynq-7000 SoC with a 200 MHz clock on a Zedboard [37]. The inbuilt SPI flash of the Zedboard is utilized to hold the look-up table. As mentioned earlier, the size of the look-up table is v = 2048. A *Perl* script is used to automate the process of making this look-up table which came with the System Verilog code. An 8-bit DAC (part# ADV7125V [38]) is used to sample the v = 2048 data from the look-up table. As the DAC is 8 bits, the memory needed to store the look-up table is 2048 $\times$ 8 = 16384 bits. The DAC accesses the look-up table with a rate of f_{DAC} = 1.5 MHz. For m = 1 to 255, Eqn. 9 indicates that the carrier frequency will be between 732 Hz and 186 kHz. By increasing the f_{DAC}, we can generate greater than 186 kHz carrier wave. If a carrier frequency is higher than the sensor's bandwidth, that frequency will not be used to modulate.

The modulator and the synchronous demodulator are implemented [39] using a high frequency power MOSFET (part# R6012JNX C7G) with a modulation index $<$ 1. The check circuit uses a MOSFET of the same type as the demodulator and the same Zedboard for the look-up table. A second-order LPF is implemented using a low-power op-amp (part # TL084CN). The defense algorithm runs on an ARM Cortex-M3 (part #EFM32GG990F1024 [40]) with a 48 MHz clock.

VII. Evaluation of the Defense MagHop

A. *Testbed*

A testbed (see Fig. 10 (Right)) is used to evaluate MagHop. Ten different VCMSs of all types, such as open-loop, closed-loop, and differential sensors from six different manufacturers,

Table I
EVALUATION OF MAGHOP. HERE, H = HALL EFFECT; F = FARADAY'S LAW; CURR = CURRENT; VOL = VOLTAGE; D = DIFFERENTIAL

Manuf.	Part #	Type/Modality /Loop	EMI power/freq. (a)	Avg. R (fixed interval) (b)	EMI power/freq. (c)	Avg. R (rand. interval) (d)
Allegro	ACS710 [28]	H/Curr./Open	0-10W / 0-120kHz	0.99	10W / 0-120kHz	0.99
Allegro	ACS724 [29]	D/H/Curr./Open	0-10W / 0-120kHz	0.98	10W / 0-120kHz	0.98
Honeywell	CSNS300M [30]	F/Curr./Closed	0-10W / 0-150kHz	0.97	10W / 0-150kHz	0.98
Acu AMP	CTF-5RL [31]	F/Curr./Open	0-10W / 50-400Hz	0.97	10W / 50-400Hz	0.99
CR Mag.	CR8410 [32]	F/Curr./Open	0-10W / 50-50kHz	0.99	10W / 50-50kHz	0.99
CR Mag.	CR8320 [21]	F/Curr./Open	0-10W / 50-50kHz	0.98	10W / 50-50kHz	0.97
LEM	LTSR 6-NP [33]	H/Curr./Closed	0-10W / 0-100kHz	0.98	10W / 0-100kHz	0.98
LEM	LV 25 P [34]	H/Vol./Closed	0-10W / 0-25kHz	0.99	10W / 0-25kHz	0.99
Triad Mag.	MET-28-T [35]	F/Vol./Open	0-10W / 300-100kHz	0.98	10W / 300-100kHz	0.98
Triad Mag.	MET-42-T [36]	F/Vol./Open	0-10W / 300-100kHz	0.97	10W / 300-100kHz	0.98

are used to evaluate MagHop (see Table I). The defense is tested against two sources: (i) a pseudo-random frequency generator, which is implemented in the Zedboard with logic circuits, connected with signal amplifiers (0-200 kHz) and a monopole antenna is used as a source of EMI, and (ii) a Grove electromagnet [22] is used as the source of static magnetic fields. *The monopole antenna and the electromagnet are placed within 1 cm of the conductors and also near the sensors.* Moreover, variable DC and AC power supplies are used to provide input voltage or current signals to sensors.

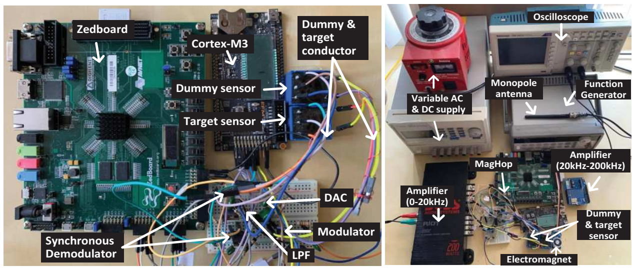


Figure 10. (Left) The prototype. (Right) The testbed.

Performance metric: If the sensor output before the attack is *similar* to the sensor output after the attack with MagHop, we can claim that MagHop works. The similarity between the sensor output before and after the attack is quantified by calculating the correlation coefficient [41], R between both signals. If the correlation coefficient is $\sim$1, the output voltage before the attack and after the attack with MagHop are similar, indicating the effectiveness of MagHop under an attack.

B. *Evaluating sweeping & responsive attacker*

1) ***Varying EMI power/frequency in fixed interval:*** To evaluate the efficacy of MagHop, at first, we vary the power of the injected EMI from 0 to 10 W with a 0.1 W increment. For every power increment, the frequency of EMI is varied within the *entire bandwidth* of the sensor with a 100 Hz increment and with a fixed 2 ms interval. For example, say for LV25P sensor, we use a 0.1 W and 100 Hz EMI at the beginning. After 2 ms, we increase the EMI frequency to 200 Hz. In this fashion, we vary the EMI frequency within the entire sensor bandwidth (25 kHz). Next, we repeat the same process for a 0.2 W EMI, and so forth. We calculate the correlation coefficient R for every combination of the power and frequency of the EMI and do an average of R for every sensor. The experimental data is logged and analyzed, and the average R is calculated using a *Python* script. The average R for every sensor in hand is less than 0.7 before MagHop is used compared to close to $\sim$1 after MagHop is used (see Table I(a, b)). This indicates that MagHop works against a sweeping or responsive attacker, who can vary the frequency and power of the EMI signal within a *fixed* time interval.

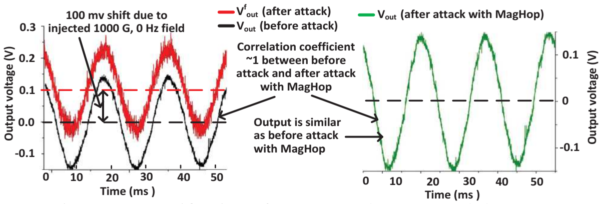


Figure 11. Justification of MagHop when an attack happens.

Justification: Fig. 11 shows a justification for using MagHop during an attack as an example. We consider a strong attacker who can inject 3W and 1 kHz EMI, and 0 Hz and 100 G static magnetic field together into a target VCMS. The 1 kHz EMI signal causes noise-like perturbations, and 1000 G static magnetic fields add a DC offset to the sensor's output. Now, after using MagHop, all the injected attack fields are contained. Therefore, the sensor output during an attack with MagHop is exactly similar to before the attack, with a correlation coefficient of 0.99. This justifies that MagHop can provide an unperturbed output signal during an attack.

2) ***Varying EMI frequency in random interval:*** We keep the EMI power fixed at 10 W but randomly vary its frequency in a *random* time interval within 0.1 s to 3 s. For example, a 10 W EMI has a 100 Hz frequency at the beginning. After a random time interval, we increase the EMI frequency to a random value and repeat the same process for the entire sensor bandwidth. We calculate the R for every reading and do an average of R for every sensor. The average R for every sensor in hand is < 0.5 before MagHop is used compared to $\sim$1 after MagHop is used (see Table I(c, d)). This indicates that MagHop works against a sweeping/responsive attacker, who can randomly vary the frequency in a *random* interval.

3) ***Varying operating time t_{op} in incremental interval:*** In Sections VII-B1 to VII-B2, we keep the t_{op} fixed at 0.3 ms. Here, we vary the t_{op} within 0.1 ms to 4 ms with an increment of 0.1 ms. For each t_{op}, we keep the EMI power fixed at 10 W and vary the EMI frequency with a 100 Hz interval with an *increment* of 0.1 ms time interval. We see that when the defense has $t_{op} > 2.2$ ms, the average of R is dropped below $\sim$0.94. The reason behind the drop of R is that the probability of having interference gets increased for a long modulation fragment (i.e., large t_{op}). Therefore, the t_{op} should be kept short (i.e., 0.1 - 2 ms) to be effective against a sweeping attacker. In addition, if the $t_{op} < 0.1$ ms, MagHop faces reliability issues because of the fast switching between small modulation fragments. A $t_{op} < 0.1$ ms can be achieved by increasing the hardware speed with a trade-off in the cost.

*4) **Varying the EMI's bandwidth BW_{atk}:*** A question may arise what will happen if the attacker jams the entire sensor bandwidth BW_S using an EMI, which has the same bandwidth BW_{atk} equal to BW_S. If this happens, MagHop will not work as the carrier frequency f_c will not find any unoccupied channel within BW_S. For this case, MagHop will do a *fail-safe shutdown* and notify the system about the possible reason.

However, if the attacker partially jams the sensor bandwidth BW_S, MagHop still works, and its performance varies depending upon what percentage of sensor bandwidth is jammed. Because, if BW_S is partially jammed, MagHop should hop multiple carrier frequencies to find an unjammed channel and check circuit kicks in before every hopping. As the check circuit requires a certain time (i.e., 115 ns) to check a carrier frequency whether its jammed or not, if the check circuit needs to do multiple frequency checks to find an unjammed bandwidth, the latency before every operating time t_{op} increases, hampering the real-time measurement of sensors. Fig. 12 (Left) shows how latency is related to the percentage of sensor bandwidth BW_S jammed by the attacker. It shows that latency is less impacted until 37% of the jammed BW_S. However, latency keeps increasing exponentially after 37% until a fail-safe shutdown occurs at 100%.

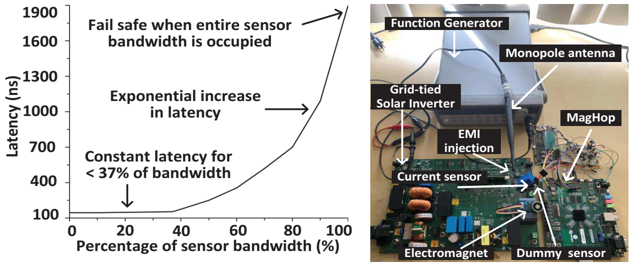


Figure 12. (Left) Latency for different attack bandwidth. (Right) Evaluating MagHop on a practical system: a grid-tied solar inverter.

C. Varying the frequency of the input signal V_{in} or I_{in}

In Sections VII-B1 to VII-B3, we keep V_{in} or I_{in} fixed at 1 A/110 V with 60 Hz. Here, we vary the frequency of V_{in} or I_{in} within the *entire sensor bandwidth* while keeping t_{op} = 0.3 ms. We also vary the 10 W EMI's frequency with a 1 ms interval. The avg. R for every sensor is less than 0.6 before MagHop is used compared to ∼1 after MagHop is used, indicating that MagHop does not hamper the sensor bandwidth.

D. Varying the magnetic field strength

To test the strength of MagHop, we vary the magnetic field density of injected magnetic fields upto 12000 G with a 100 G interval using an electromagnet. Please note that an 8000 G can penetrate a ferromagnetic shield [42], [43]. Therefore, the 12000 G is indeed a high amount for a shield to defend. Without MagHop, the high magnetic flux of the injected field gives an average R = 0.2. After using MagHop, the average R is ∼1. It indicates that MagHop also works against a strong magnetic field, which can even penetrate a shield.

E. Low cost, low-power and easy to integrate

The shift registers and look-up tables are implemented in an FPGA with power gating [44] for low-power design. Low-power discrete ICs are used for modulators, demodulators, LPF, and DAC for rapid prototyping. The total power consumed by the prototype is 1.5 mW, which is compatible with ∼10 mW [45] consumed by VCMSs itself. MagHop can be connected with the target VCMS in a plug-&-play manner.

As we use a Zedboard for rapid prototyping, the size and cost of the prototype are high. However, the shift register and look-up table can be implemented in discrete cheap registers instead of a Zedboard. For this, we estimate the total cost is < $20 for bulk orders, excluding the dummy sensor. A complete SoC design would reduce the size and cost even more.

VIII. Evaluating on a Practical System

The effectiveness of MagHop is evaluated with a practical system: a grid-tied solar inverter that uses VCMSs to calculate power. An attacker can target these VCMSs and inject EMIs/magnetic fields to mislead the inverter's controller with wrong data, leading to a wrong operating state (e.g., disconnecting the grid-tied inverter from the power grid).

We integrate MagHop with a scaled-down 140 W grid-tied solar inverter [46] kit (part# = TMDSOLARUINVKIT) from Texas Instruments (Fig. 12 (Right)). Before the EMI attack, the inverter generates 94 W. This inverter has a Hall effect current sensor with a part # ACS712ELCTR-20A-T. Now, we inject a 100 G magnetic field from an electromagnet into this current sensor from a 1 cm distance. The power reading goes up to 129 W because of the perturbation in the sensor reading. Next, we connect MagHop with the Hall effect current sensor and repeat the same experiment. At this time, the power is not changed from 94 W. This proves the efficacy of MagHop against a magnetic field injection into a VCMS.

IX. Limitations

Skin effect: As MagHop uses high-frequency carrier waves, the skin effect [47] can occur in the conductor present in the input/output stage of the sensor. However, as the conductor length is small, the resistance increase from the skin effect is negligible and does not impact the overall measurement.

High-speed hardware: To maintain coherency among different fragments, the microprocessor should be comparatively faster than the input voltage or current signal; otherwise, a time lag will be introduced while shifting the carrier frequency. Empirically, the microprocessor clock should be at least 100× faster than the sensor's bandwidth. Moreover, the time required for carrier frequency generation and switching to a new carrier frequency also should be low. Therefore, hardware speed is a critical requirement. We use a 200 MHz clock for the FPGA and a 48 MHz clock for the microprocessor in our prototype.

Jamming the entire sensor bandwidth: As mentioned before, if the entire sensor bandwidth is jammed, MagHop will fail safely. However, if there is a free spectrum to use, MagHop will *slip though* using the free spectrum.

Exploitation by a strategic attacker: There are 12 different combinations of 4 tap positions that can generate maximal sequences in an 8-bit LFSR [26]. As we keep one tap at position 8 and we have not used position 1 for tapping, there are 8 possible tap combinations that can generate *8 sets* of LFSR sequences (see Section VI). A strategic attacker who can observe the frequency for a long time (i.e., contradictory to the threat model) can theoretically calculate all 8 possible next-states for the current state and jam those 8 frequencies. However, practically speaking, this could be *complicated* as the attacker needs to know the timing information, such as t_{gen} and t_{op} of MagHop, and needs to be very fast to be always one step ahead of the defense; otherwise, the *check circuit* can sense the channel as jammed, and MagHop will find another unjammed channel to slip through using the free spectrum. If this process continues to happen, a situation similar to Section VII-B4 will happen, and MagHop will do a fail-safe shutdown notifying the system about the possible reason.

X. Related Work

EMI shielding: Bora et al. [48] and Merizgui et al. [49] proposed new shielding material to prevent EMIs. The main limitation of the shielding approach is that it may work against time-varying EMIs, but not against a static magnetic field. Moreover, an attacker can saturate the shield using a strong magnetic field to diminish its shielding property [43].

Filtering: Zhang et al. [13] provided ways for only EMI detection but did not provide any defense against it.

Kune et al. [5] proposed an adaptive filtering technique to estimate the attack signal first and then subtract it from the input signal to filter out attack signals from analog acoustic sensors. This technique may fail for the following two reasons: (i) Because of the physical distance between the adaptive filter and the compromised sensor, the adaptive filter cannot measure the exact amplitude of the external attack fields injected into the sensor. (ii) This will also fail if the attack signals and the original signals have identical frequencies.

Zhang et al. [11] proposed low-pass filters to filter out the injected ultrasound from baseband voice commands. This approach only worked because the ultrasonic signal and the baseband voice signal have two different spectra, which are separable by filters. This approach will also fail if the attack signal and the original signals have identical frequencies.

Trippel et al. [10] proposed randomized and 180^0 out-of-phase sampling to prevent acoustic injection on inertial sensors. They take two samples with 180^0 out-of-phase from input signals at random intervals to cancel attack signals. They will fail for the following two scenarios: (i) If the attack and original input signals have identical frequencies, they will filter out original signals while filtering the attack signals. (ii) They cannot work against static magnetic fields as randomized sampling cannot filter out a DC signal.

Tu et al. [12] proposed a transduction shield (TS) to estimate attack signals first and then subtract attack signals from the original one. The main limitation is that it assumes the TS and the target sensor are identical and TS sees the same attack signals as the target sensor. However, there is always a mismatch and physical distance between the TS and the sensor. Therefore, the attack signals cannot be exactly nullified. The defenses proposed by Barua et al. [50], [51] have upper limits for frequency and power of EMIs up to which these defenses could work, whereas MagHop does not have these limits.

State machine: The state machine based defenses by Cardenas et al. [52], [53], Urbina et al. [54], and Shoukry et al. [55] do not directly prevent EMI injection. Instead, they use state information to recover the controller from an attack.

Summary: MagHop is novel in the sense that it encrypts the information within the magnetic medium stage using pseudo-random channel. Therefore, there is no practical limit to the attack signal's strength up to which MagHop can tolerate. MagHop can handle attack signals of any strength as long as the entire sensor bandwidth is not jammed. Moreover, MagHop can contain attack signals having the same bandwidth as the input signal being measured. A comparison between MagHop and recent works is provided below:

Table II
Comparison between MagHop and recent work.

Comparison	Recent works [10], [11], [5], [12], [13]	MagHop
strength of injected B_{atk}	support up to a limit	no limit if free bandwidth exists
frequencies of injected B_{atk}	does not support entire sensor bandwidth	support entire sensor bandwidth
injected B_{atk} power	low power ($\sim 4W$)	no theoretical limit
power consumption	unknown	$\sim$1.5 mW

XI. Conclusion

We present MagHop to design a secure VCMS against an intentional EMI/magnetic field. MagHop shifts the frequency spectrum of the transduction medium to another spectrum, which is unknown to an attacker. Therefore, the attacker cannot inject any perturbations in the form of an EMI/magnetic field into the magnetic medium stage. Even a strong sweeping/responsive attacker cannot interfere with the magnetic transduction stage because of the *check and select* approach of MagHop. We implement a low-power design of MagHop on an FPGA and Cortex-M processor for rapid prototyping. We thoroughly evaluate MagHop on ten different VCMSs from six different manufacturers. Our results from these experiments show a promising efficacy against intentional EMI/magnetic field injection while keeping the sensor output coherent and real-time. *As designing secure sensors is important for critical infrastructures, finally, we believe that the idea presented in this paper will be beneficial to other sensor types to build the next generation of trustworthy sensors.*

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments. This work was partially supported by the National Science Foundation (NSF) under award ECCS-2028269. Any opinions, findings, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] A. A. Makky, H. Abo-Zied, F. Abdelbar, and P. Mutschler, "Design of the instrument current transformer for high frequency high power applications," in *2008 12th International Middle-East Power System Conference*. IEEE, 2008, pp. 230–233.

[2] T. et al., "Design of a hall effect current microsensor for power networks," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 421–427, 2011.

[3] "Hall-Effect Current Sensor Market," 2020, https://www.marketsandmarkets.com/Market-Reports/hall-effect-current-sensor-market-201606539.html.

[4] H. Kirkham, "Current measurement methods for the smart grid," in *2009 IEEE Power & Energy Society General Meeting*. IEEE, 2009, pp. 1–7.

[5] K. et al., "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159.

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

[7] S. Dhia, A. Boyer, B. Vrignon, M. Deobarro, and T. V. Dinh, "On-chip noise sensor for integrated circuit susceptibility investigations," *IEEE transactions on instrumentation and measurement*, vol. 61, no. 3, pp. 696–707, 2011.

[8] F. Fiori, "A sensor signal amplifier resilient to emi," *IEEE Sensors Journal*, vol. 16, no. 18, pp. 7008–7015, 2016.

[9] O. Aiello, P. Crovetti, and F. Fiori, "Investigation on the susceptibility of hall-effect current sensors to emi," in *10th International Symposium on Electromagnetic Compatibility*. IEEE, 2011, pp. 368–372.

[10] T. et al., "Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks," in *2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 2017, pp. 3–18.

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

[12] Y. Tu, V. S. Tida, Z. Pan, and X. Hei, "Transduction shield: A low-complexity method to detect and correct the effects of emi injection attacks on sensors," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 901–915.

[13] Y. Zhang and K. Rasmussen, "Detection of electromagnetic interference attacks on sensor systems," in *IEEE Symposium on Security and Privacy*, 2020.

[14] W. H. Hayt Jr, J. A. Buck, and M. J. Akhtar, *Engineering Electromagnetics— (SIE)*. McGraw-Hill Education, 2020.

[15] C. I. Hubert, *Electric Machines: Theory, Operation, Applications, Adjustment & Control*, 2nd ed. Pearson Education, 2009.

[16] B. Cogiore, J. P. Keradec, and J. Barbaroux, "The two winding ferrite core transformer: An experimental method to obtain a wide frequency range equivalent circuit," in *1993 IEEE Instrumentation and Measurement Technology Conference*. IEEE, 1993, pp. 558–562.

[17] C. Chien, *The Hall effect and its applications*. Springer Science & Business Media, 2013.

[18] A. Barua and M. A. Al Faruque, "Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 1273–1290.

[19] G. et al., "Dancing on the lip of the volcano: Chosen ciphertext attacks on apple imessage," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016, pp. 655–672.

[20] ——, "EMI shielding: Methods and materials—A review," *Journal of applied polymer science*, vol. 112, no. 4, pp. 2073–2086, 2009.

[21] "CR8320 datasheet," 2022, https://www.crmagnetics.com/Assets/ProductPDFs/CR8300\%20Series\%20Specification\%20Page.pdf. (Accessed: 03-18-2023).

[22] "Grove datasheet," 2022, https://www.mouser.com/datasheet/2/744/Seeed_101020073-1217554.pdf. (Accessed: 03-18-2023).

[23] J. H. Wu, J. Scholvin, J. A. del Alamo, and K. A. Jenkins, "A faraday cage isolation structure for substrate crosstalk suppression," *IEEE Microwave and Wireless Components Letters*, vol. 11, no. 10, pp. 410–412, 2001.

[24] E. O. Brigham, *The fast Fourier transform and its applications*. Prentice-Hall, Inc., 1988.

[25] S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005.

[26] "Maximal Length LFSR Feedback Terms," http://users.ece.cmu.edu/~koopman/lfsr/. (Accessed: 03-18-2023).

[27] A. Salazar, G. Bahubalindruno, G. Locharla, H. Mendonça, J. Alves, and J. Da Silva, "A study on look-up table based sine wave generation," *Proceedings of the Regional Echomail Coordinator, Porto, Portugal*, pp. 3–4, 2011.

[28] "Acs710 datasheet," 2020, https://www.allegromicro.com/~/media/Files/Datasheets/ACS710-Datasheet.ashx. (Accessed: 03-18-2023).

[29] "Acs724 datasheet," 2020, https://www.allegromicro.com/~/media/Files/Datasheets/ACS724-Datasheet.ashx. (Accessed: 03-18-2023).

[30] "CSNS300 datasheet," 2022, https://datasheet.octopart.com/CSNS300M-Honeywell-datasheet-68416259.pdf. (Accessed: 03-18-2023).

[31] "CTF-5RL-0050 datasheet," 2022, https://cdn.automationdirect.com/static/specs/acuampsolidcore.pdf. (Accessed: 03-18-2023).

[32] "CR8410 datasheet," 2022, https://www.crmagnetics.com/Assets/ProductPDFs/CR8400\%20Series\%20Specification\%20Page.pdf. (Accessed: 03-18-2023).

[33] "LTSR 6-NP datasheet," 2022, https://www.lem.com/sites/default/files/products_datasheets/ltsr_6-np.pdf. (Accessed: 03-18-2023).

[34] "LV 25-P datasheet," 2022, https://fastron.com.au/products/lv25p-sp5.

[35] "MET-28-T datasheet," 2022, http://catalog.triadmagnetics.com/Asset/MET-28-T.pdf. (Accessed: 03-18-2023).

[36] "MET-42-T datasheet," 2022, http://catalog.triadmagnetics.com/Asset/MET-42-T.pdf. (Accessed: 03-18-2023).

[37] "Zedboard datasheet," 2022, https://digilent.com/reference/_media/zedboard:zedboard_ug.pdf. (Accessed: 03-18-2023).

[38] "ADV7125V datasheet," 2022, https://www.analog.com/media/en/technical-documentation/data-sheets/ADV7125.pdf. (Accessed: 03-18-2023).

[39] "Circuit Design: How to make an amplitude modulated wave," 2022, https://www.engineersgarage.com/circuit-design-how-to-make-an-amplitude-modulated-wave/. (Accessed: 03-18-2023).

[40] "EFM32 Giant Gecko datasheet," 2022, https://www.silabs.com/documents/public/data-sheets/efm32gg-datasheet.pdf. (Accessed: 03-18-2023).

[41] R. Taylor, "Interpretation of the correlation coefficient: a basic review," *Journal of diagnostic medical sonography*, vol. 6, no. 1, pp. 35–39, 1990.

[42] C. Steinmetz, *Theory and Calculation of Electric Circuits*, 1st ed. The McGraw-Hill Companies, 1917.

[43] L. Chiesi, K. Haroud, J. A. Flanagan, and R. S. Popovic, "Chopping of a weak magnetic field by a saturable magnetic shield," *Sensors and Actuators A: Physical*, vol. 60, no. 1-3, pp. 5–9, 1997.

[44] J. et al., "Benefits and costs of power-gating technique," in *2005 International conference on computer design*. IEEE, 2005, pp. 559–566.

[45] "Allegro MicroSystems : Hall-effect sensors consume very little power," 2020, https://www.eetimes.com/allegro-microsystems-hall-effect-sensors-consume-very-little-power/. (Accessed: 03-18-2023).

[46] "Grid-tied Solar Micro Inverter with MPPT," https://www.ti.com/tool/TIDM-SOLARUINV. (Accessed: 03-18-2023).

[47] O. Gatous and J. Pissolato, "Frequency-dependent skin-effect formulation for resistance and internal inductance of a solid cylindrical conductor," *IEE Proceedings-Microwaves, Antennas and Propagation*, vol. 151, no. 3, pp. 212–216, 2004.

[48] B. et al., "Outstanding absolute electromagnetic interference shielding effectiveness of cross-linked pedot: Pss film," *Advanced Materials Interfaces*, vol. 6, no. 22, p. 1901353, 2019.

[49] T. Merizgui, B. Gaoui, T. A. Sebaey, and V. A. Prakash, "High content silver/zinc oxide nanoparticle and cobalt nanowire in caryota urens fibre-epoxy composites for enhanced microwave shielding," *Journal of Magnetism and Magnetic Materials*, vol. 536, p. 168118, 2021.

[50] A. Barua and M. A. Al Faruque, "Premsat: Preventing magnetic saturation attack on hall sensors," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 438–462, 2022.

[51] A. Barua and M. A. A. Faruque, "Halc: A real-time in-sensor defense against the magnetic spoofing attack on hall sensors," in *Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses*, ser. RAID '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 185–199. [Online]. Available: https://doi.org/10.1145/3545948.3545964

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

[53] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry *et al.*, “Challenges for securing cyber physical systems,” in *Workshop on future directions in cyber-physical systems security*, vol. 5, no. 1. Citeseer, 2009.

[54] U. et al., “Limiting the impact of stealthy attacks on industrial control systems,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1092–1105.

[55] S. et al., “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, 2015, pp. 3804–3809.