A Directive Antenna Based on Conducting Discs for Detecting Unintentional EM Emissions at Large Distances

Prateek Juyal, Sinan Adibelli, Nader Sehatbakhsh, and Alenka Zajic, *Senior Member, IEEE*

***Abstract*—This paper proposes a novel high gain planar antenna design that consists of conducting metallic discs suspended on air and operates at 1 GHz. The antenna is designed for receiving the unintentional EM emanations generated by one or multiple embedded, "smart" electronic systems. The antenna consists of two layers of slotted conducting metal discs suspended on air and placed above the ground plane using teflon screws. The circular discs are designed to operate in higher order TM_{12} mode. The screws location are the electric field nulls along the disc radius. The upper layer is 2×2 array of slotted circular discs electromagnetically coupled by lower identical disc which is fed directly by a single coaxial feed. The complete fabrication of antenna is done using aluminum metal sheets and involves no use of dielectric substrate. The antenna has a peak gain of 19 dBi with impedance bandwidth ($S_{11} \leq -6$ dB) of 6.7%. The simple and cost effective design can be easily scaled to higher frequencies.**

***Index Terms*— Circular discs, embedded systems security, side-channels, high antenna gain, planar antenna arrays, TM modes.**

I. Introduction

Electromagnetic (EM) side-channel attacks are a major concern for electronic security. They circumvent traditional security techniques by relying on observing confidential information via side-channels. The existence of EM side channel radiation and the potential risk it poses to computer security was reported in open literature [1]–[3]. Recently it was demonstrated that EM emanations produced by embedded devices carry information about program execution and can be received up to three meter away, even in the presence of significant counter measures [4]-[6].

One of the challenges in studying the side-channel EM emanations is how to improve signal reception, especially at a distance and in the presence of noise. The EM side-channel propagation model in [7] suggests that EM side-channel signal follows Friis formula once the signal is in far-field, and that the reception range can be extended by increasing antenna gain. Hence, the main objective of this paper is to design a high gain antenna that can improve the Signal to Noise Ratio (SNR) of the receiving EM signals.

Specifically, our goal is to design an antenna with peak broadside gain of 19 dBi, operating around 1GHz (which is where typically embedded devices are operating), which would allow for signal reception at >4 m distance. The bandwidth requirement is around 50 MHz. Secondly, the design should be planar in nature, which can be hang on the ceilings or walls and does not occupy more than 1x1 m area, so it can be used to receive EM signals form embedded devices in a room.

Among planar radiators, microstrip arrays are widely used for high gain planar antenna applications. The elements in those arrays are generally designed to operate in their fundamental mode. For instance, in case of rectangular patch, the mode is either TM_{10} or TM_{01}. Similarly for the circular patch, fundamental mode TM_{11} is used. For the single microstrip element, operating in the fundamental mode, the peak directivity is limited. For example, the peak directivity of circular disc in TM_{11} mode is 9.9 dBi [8]. The substrate permittivity between 2-3 is generally used in practice, which further reduces the single element directivity to 6-7 dBi for circular disc [9]. To achieve higher gain, planar microstrip array with the array dimensions of $N > 2$ are used. The array spacing is also limited and the optimum spacing for the maximum directivity, with no sidelobe, is between 0.7-0.9 λ_0 [10]. For a given physical area, say for 1×1 m, the microstrip array on the substrate permittivity of 1, has the least number of elements and the maximum directivity. Increasing substrate permittivity reduces the element size and hence will results in increased number of elements. In the lower L-band design frequency range, say for 1GHz, the printed element increases the cost, due to large physical area, as substrates are expensive. Also, feed lines are generally used to excite the array elements, which radiates on their own and are not preferable for the EM emissions detection.

Hence, we propose a 19 dBi gain, single feed planar circular disc antenna design that consists of conducting metallic discs suspended on air, operates at 1GHz and occupies 1.04×1.04 m area. The antenna consists of two layers of slotted conducting metal discs suspended on air and placed above the ground plane. The circular discs are designed to operate in higher order TM_{12} mode and are suspended on air, using teflon screws at the position of electric field nulls along the disc radius (shown in Section IV). The upper layer is 2×2 array of slotted circular discs electromagnetically coupled by lower identical slotted disc, which is fed directly by a single coaxial feed. The use of higher order TM_{12} mode permits the use of smaller number of

Manuscript submitted January 14, 2018
Authors are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: prateek.juyal@ece.gatech.edu, sinanadibelli2@gatech.edu, nader.sb@gatech.edu, alenka. zajic@ece.gatech.edu).

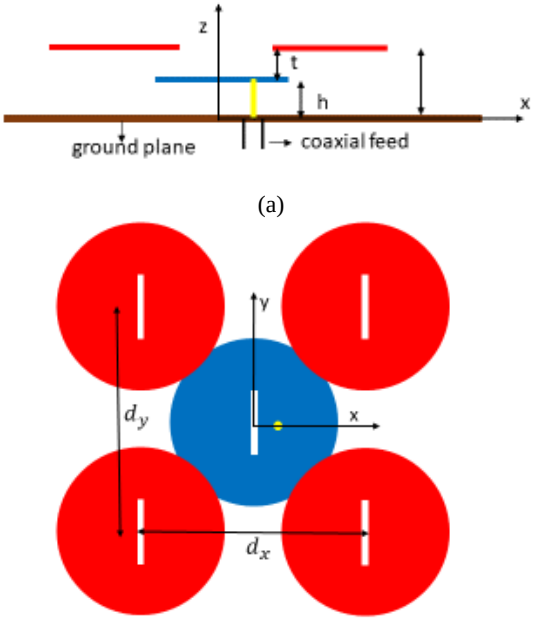
This work has been supported, in part, by DARPA LADS contract FA8650-16-C-7620. The views and findings in this paper are those of the authors and do not necessarily reflect the views of DARPA.

elements due to large electrical size than the fundamental TM_{11} mode. The complete fabrication of antenna is done using aluminum metal sheets and involves no use of dielectric substrate. Given the growing importance of embedded and smart systems, proposed antenna can be used to receive EM signals from a single or multiple of such embedded devices in a room. The receiving signal can then be used for software profiling [11] or security monitoring [12] which is illustrated at Section V. It is important to mention here that the similar antenna topology, using fundamental mode of rectangular patch, with conventional array spacing limited to $0.7\lambda_0$ has been used earlier in [13] for the directivity enhancement. The antenna was printed on dielectric substrate and directivity ~ 12 dBi was reported. In contrast, the antenna proposed in this paper has peak directivity ~ 19 dBi, uses air as the substrate medium and has larger ($1.75\lambda_0$) array spacings. This is due to the use of slotted TM_{12} mode discs as an array element, which is electrically large, has higher directivity compared to fundamental mode patch element [13] and can be easily suspended in the air, using four teflon screws on the position of the electric field nulls (as discussed in Section IV).

The rest of the paper is organized as follows. Section II describes antenna geometry and its design. Section III discusses element spacing, sidelobe and the impedance match. Section IV discusses the antenna fabrication, S_{11} and gain measurement. Section V illustrates the use of the proposed antenna by estimating SNR of received signal and demonstrating EM signal detection from an active board around processor clock frequency, at > 3 m distances. Finally Section VI concludes the paper.

II. Antenna Geometry & Design

This section describes the proposed antenna geometry. The antenna is a two layer stacked configuration as shown in Fig. 1(a).



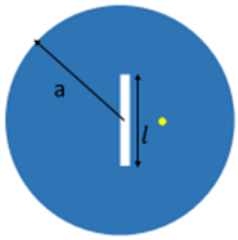
(a)

(b)

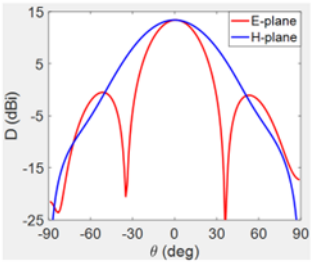
Fig. 1. Antenna Geometry (a) side view and (b) top view.

The upper layer is 2×2 array of slotted circular discs in TM_{12} mode, shown in Fig. 1(b), fed by an identical disc in the lower layer, which is directly fed by coaxial probe. A similar feeding technique was proposed in [13] where a 2×2 array of rectangular patches was excited by a microstrip fed and centrally located patch in the lower layer. This technique removes dependency on feed lines. Here, to avoid feed lines, we use coaxial feed to excite the lower disc. All circular discs have identical geometrical dimensions. The individual circular disc is loaded with narrow rectangular slot at the center. Slot loading is used to reduce the high sidelobes in the E-plane radiation pattern of TM_{12} mode, as explained and discussed in [14].

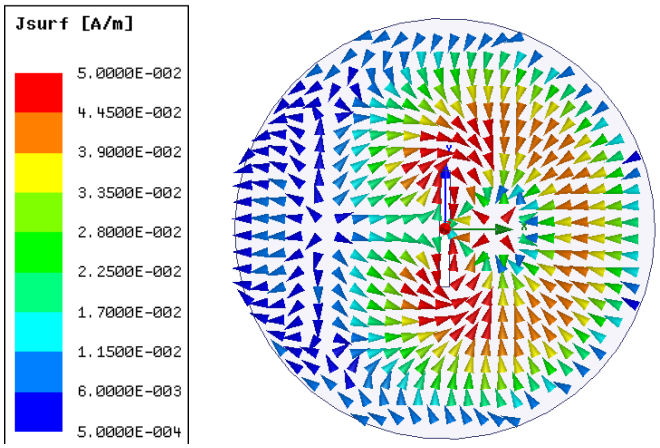
The design procedure is described as follows. Based on the peak directivity requirements, the single element is designed first as shown in Fig. 2(a). In the present case, the slot length is selected for maximum directivity, which is 13.4 dBi. The corresponding disc radius and slot length, *l*, are 20.5 and 11.3 cm respectively. Since it is a narrow slot, the slot width, *w*, is selected to be 1 cm. The thickness, *h*, is chosen to be 5 mm. Higher thickness values will result in increase in Side-Lobe Level (SLL) of the element as explained in [14]. The directivity pattern of the single element in the E and H-plane and its current distribution is shown in the Fig. 2(b) and Fig. 2(c) respectively. The current density is higher in the region adjacent to slots compared to the other parts of the patch as the narrow slot at the center intercepts the flow lines of current and gets excited. This produces the out of phase electric field at the slot aperture, which leads to sidelobe cancellation as explained in detail in [14]. The 2×2 array of identical elements is then placed at the height *t* above this layer as shown in Fig. 1(a). In this case, the *t* is selected to be 5 mm. The array spacing d_x and d_y is chosen to reduce E and H-plane sidelobe and to improve impedance match ($S_{11} \leq -6$ dB). Additionally, the parameters of the center disc in the lower level can also be adjusted to improve the impedance match which also results in the reduced H-plane sidelobe (see more details in Sec. III).



(a)



(b)



(c)

Fig. 2 Element design at 1.03GHz: (a) Slot loaded disc, (b) directivity pattern in E and H-plane, (c) the current distribution of the patch.

III. Element Spacing, SideLobe & Impedance

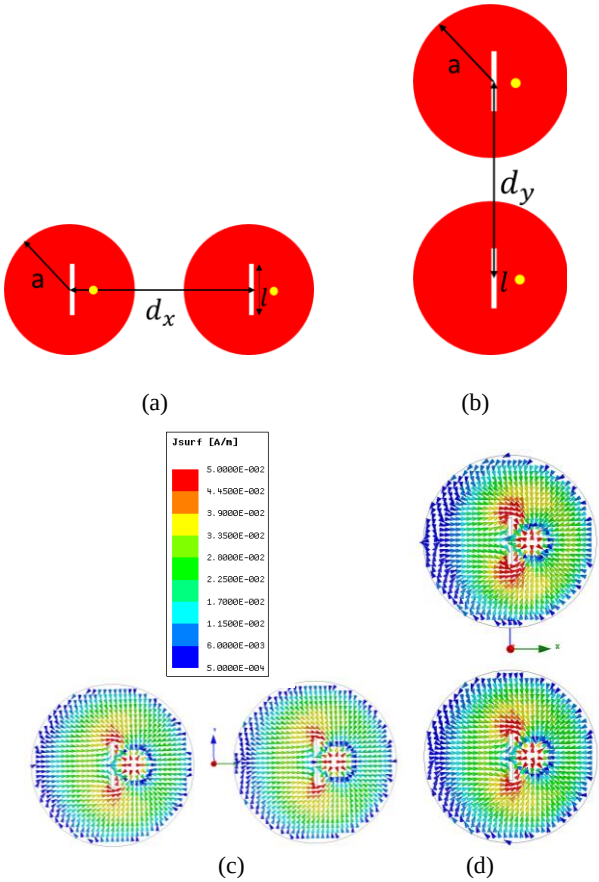
In this section, we investigate the effect of array spacing and positioning of the center disc on the sidelobes in the radiation pattern. This is required since the element radius is $\sim 0.7\lambda_0$ and hence the minimum array spacing will be greater than $1.4\lambda_0$. For the spacing greater than $1.4\lambda_0$, array theory predicts that the sidelobe will be high in the radiation pattern, which reduces the aperture efficiency and the directivity [15]. In antenna arrays, several methods have been used in the past for sidelobe suppression [16]-[19]. In this design, the side lobe in the E-plane is suppressed by the slot loaded in the disc. In the H-plane the sidelobe is suppressed by the center disc. This is explained in Section III-*A*. In addition to that, in Section III-*B*, we show the effect of lower disc parameters like slot length and disc radius on the impedance match of the antenna. The radiation patterns at the various frequencies in the band are also discussed in this section.

A. Element Spacing & SideLobe

To explain how element spacing impacts the sidelobe, we investigate E & H-plane radiation pattern of 2×1 array and 2×2 array of the element shown in Fig. 2(a), assuming infinite ground plane configuration. Fig. 3(a) & (b) shows the geometry of 2×1 and 1X2 array. Simulations were performed for the various spacing between array elements for both the geometries. Current distribution for both array geometries are shown in Fig. 3(c) & (d). For both elements, the excitation amplitudes are equal with zero phase difference. Current density scaling is the same as used in Fig. 2(c). It is observed that 2X1 array compared to 1X2 array has strong current density around the slot edges. The reason for this is the aperture field vector of the slot, which is in the direction of x-axis, as explained in [14], and hence can have possible coupling effects in the 2X1 configuration.

Fig. 4(a) & (b) shows the E & H-plane pattern for 2X1 array geometry with element spacing d_x as parameter. As d_x increases from 1.5 to $2\lambda_0$, the first sidelobe in the E-plane increases. For $1.5\lambda_0$, there is one lobe in the visible region while for 1.75 and $2\lambda_0$, there are two lobes. In all cases the minor lobes are 10 dB below the main beam. Fig. 4(b) shows that element spacing has negligible effect on the H-plane pattern.

Fig. 4(c) & (d) shows the E & H-plane pattern for 1X2 array geometry shown in Fig. 3(b). Compared to Fig. 4(a), H-plane pattern shown in Fig. 4(d), has higher sidelobes since the sidelobe cancellation effect of slot is less dominant in the H-plane configuration. The first sidelobe is reduced by ~ 3dB in the E-plane of 2X1 array, due to cancellation effect by slot loading, as compared to the H-plane pattern of the 1X2 array. Based on this study of how the array spacing impacts radiation pattern, we chose the value of $1.75\lambda_0$. We have also observed in simulations that the selected spacing has a good impedance match in the frequency band of interest. This is also shown in Fig. 6 (a).



(a) (b)

(c) (d)

Fig. 3 Array geometry (a) 2X1 array (b) 1X2 array (c) current distribution of 2X1 array, (d) 1X2 array.

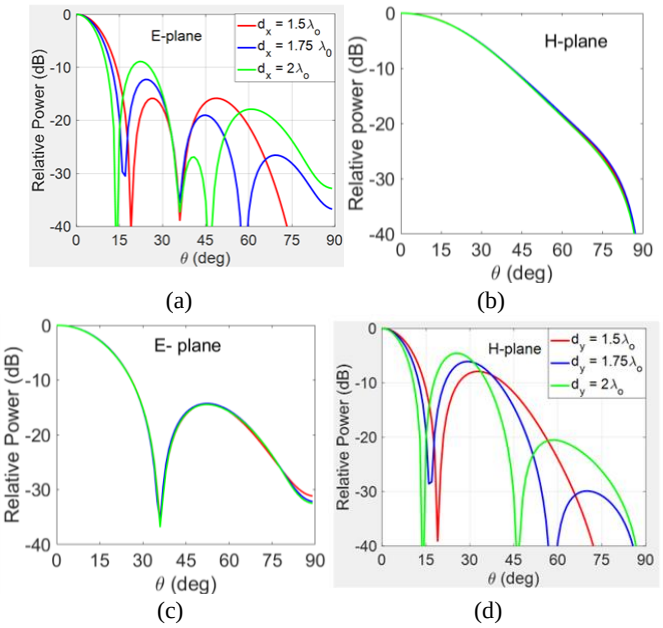
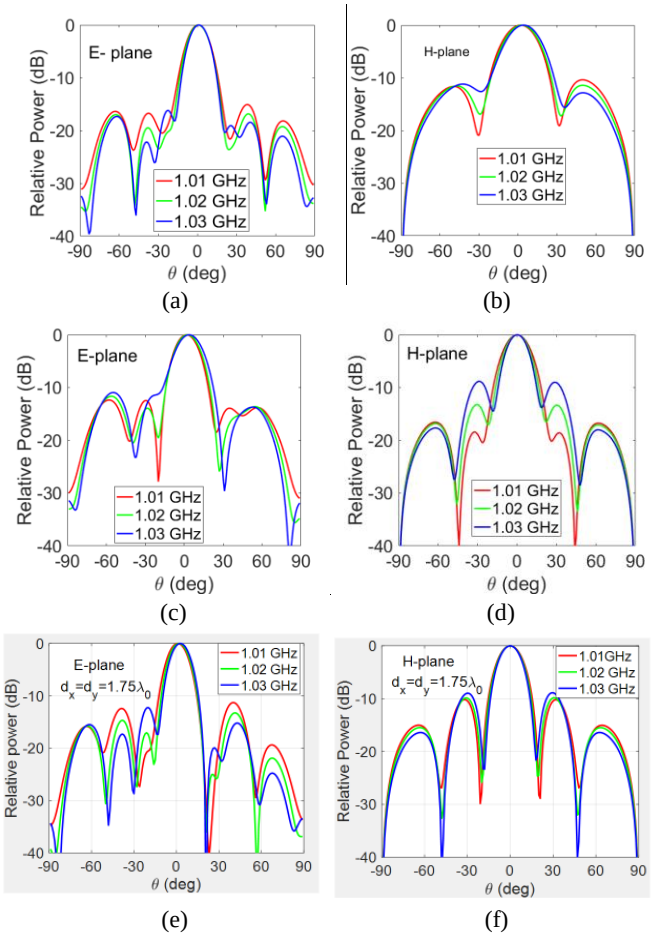


Fig. 4 Radiation pattern as a function of array spacing (a) & (b) E & H-plane pattern for geometry shown in Fig. 3(a), (c) & (d) for the geometry shown in Fig. 3(b)



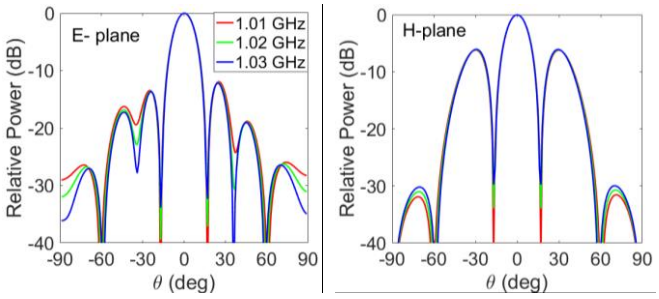


Fig. 5 Effect of the center disc on the radiation pattern in (a) 2X1 array E-plane, (b) 2X1 H-plane, (c) 1X2 E-plane, (d) 1X2 H-plane, (e) 2X2 E-plane, (f) 2X2 H-plane, (g) 2X2 array without lower center disc, E-plane, (h) 2X2 array without lower center disc, H-plane.

To excite the array, an identical disc is placed at the center of the ground plane, at smaller height than the upper four discs as shown in Fig. 1(a). Fig. 5 shows the effect of the lower layer center disc on the radiation pattern of the antenna. Effect of the center disc on the radiation pattern was studied in 2X1, 1X2 and 2X2 array configuration, for the selected element spacing of $1.75\lambda_0$. Figs. 5(a) & (b) show the effect in the 2X1 array geometry. Compared to Fig. 4, the sidelobes in the E-plane are reduced. In the H-plane, additional lobe is there in the visible region. Fig. 5 (c) & (d) shows the radiation pattern when the 1X2 array geometry is loaded with center disc. Compared to Figs. 4(c) & (d), it is observed that sidelobes are suppressed in the H-plane and in the E-plane additional lobes are introduced with the distorted pattern. Figs. 5 (e) & (f) show the radiation pattern of 2X2 array, with center disc loading. For the comparison, the radiation pattern of unloaded 2X2 array is shown in Figs. 5(g) & (h). Compared to the 2×2 array without center disc, the presence of the center disc reduces the sidelobe in the H-plane by ~ 3dB. In the E-plane, the pattern peak is off the boresight by 2°, but the sidelobes are still ~ 10dB below the main lobe.

B. Impedance Match

To make the design practical, the simulations are performed with finite ground plane. We choose 1.04 m×1.04 m squared ground plane made of aluminum, which resembles the fabricated antenna in the next section. It was shown in [13] that stacked configuration has wideband characteristics and the impedance match depends on the overlapping area of the two layers. In the present design, the additional parameter that can affect the impedance is the lower disc slot length *l*. Fig. 6 shows the effect of the array spacing and the lower disc slot length on the S_{11} and the impedance over the frequency band. Each case displays two coupled resonances which corresponds to the upper and the lower layer. Fig. 6(a) shows that for the array spacing of $1.75\lambda_0$, the impedance match is obtained in the desired band. For closer spacing of $1.5\lambda_0$, due to resonance split around 1.045 GHz, there is a mismatch in the band. Hence the array spacing of $1.75\lambda_0$was selected for the design. Once the upper 2×2 layer geometry is fixed, the amount of coupling depends on the lower disc slot length. For l = 100 mm, the impedance is inductive as shown in the Smith chart in Fig. 6(c).

Increasing slot length to 110 mm results in impedance match for the whole band, shown in Fig. 6(b). Further increase to 120 mm reduces the input resistance which results in impedance mismatch.

Fig. 7(a) shows the reflection coefficient vs. frequency with lower disc radius, *a*, as parameter. With an increase in radius, the resonances shift to lower values. Furthermore, Fig. 7(b) shows less coupling between two resonances due to smaller loop sizes in the smith chart, which increases with the disc radius. When the disc radius is 205 mm, the impedance is matched for the band. Slot length, *l*, for this case is 113 mm, which is also the selected length for the fabrication.

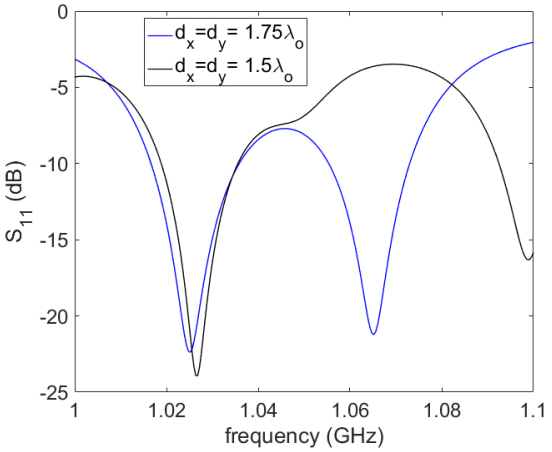


Fig. 6 (a) Reflection coefficient vs frequency with array spacing as parameters (b) Reflection coefficient vs. frequency and (c) Impedance loci variation with lower *slot length* as parameter.

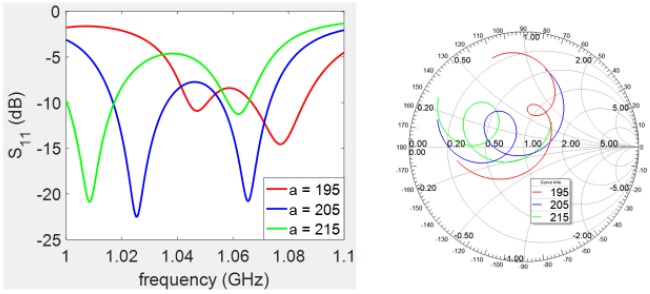


Fig. 7 (a) Reflection coefficient vs. frequency and (b) Impedance loci variation with lower *disc radius a* as parameter.

The simulated radiation patterns in the E & H-plane for four frequencies in the band of interest are shown in Fig. 8 (a) and (b). The peak gain is above 18 dBi in the whole frequency band with a maximum value of 19.1 dBi at 1.03 GHz. The maximum cross polarization level in H-plane is ~ 20 dB below the main lobe in the entire frequency band. We observe in the simulations that with the increase in frequency, the H-plane sidelobe increases from -10.2 dB at 1.01 GHz to -7.7 dB at 1.04 GHz. This is because at the higher frequencies of the band the array spacing becomes larger and hence results in increased SLL. In the E-plane, the beam is shifted 2° from the maximum at 1.03 GHz.

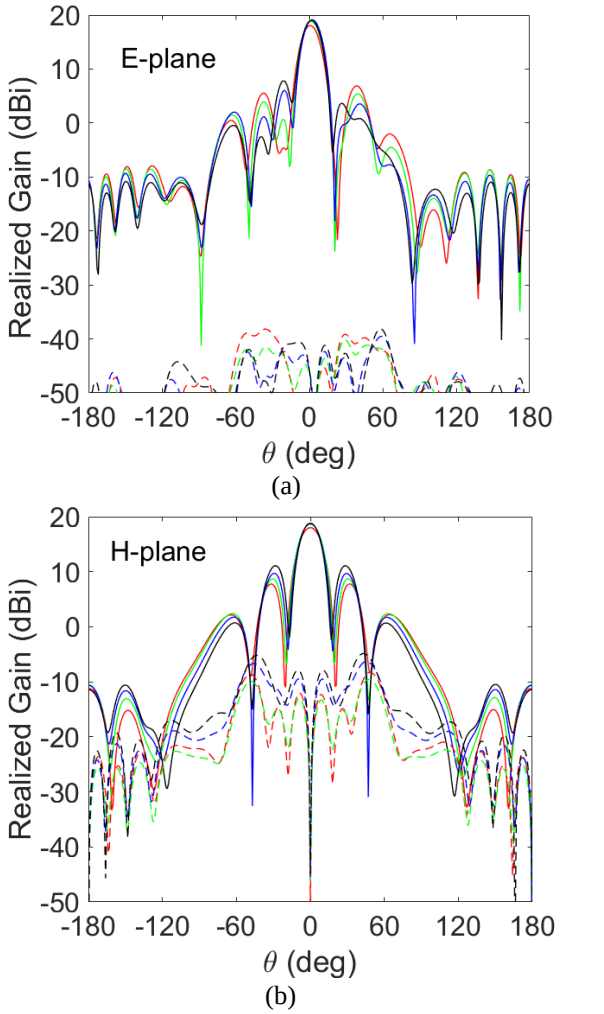


Fig. 8 Radiation pattern over the band for the antenna geometry shown in Fig. 1 at (a) E-plane, (b) H-plane.

IV. Antenna Fabrication & Measurements

The antenna geometry shown in the Fig. 1 was designed, fabricated and tested. The center frequency of the designed antenna is 1.03 GHz. A square aluminum sheet of dimension 1.04 m was used as a ground plane. The individual discs have the radius of 20.5 cm with the slot length and width of 11.3 cm and 1 cm respectively. Each of them are fabricated using aluminum sheet of thickness 2 mm. The center disc is suspended at 5 mm above the ground plane while the other four

are at 10 mm above the ground plane. The center disc is directly fed by a 50 Ohm coaxial probe, which is placed at 50 mm away from the center. The fabricated antenna picture is shown in Fig. 9.

(a) (b)

Fig. 9 Fabricated antenna (a) front view (b) side view.

Each disc is suspended using four Teflon screws. Modal electric field distribution of the TM_{12} mode is used to determine the position of screws. To explain this, Fig. 10 shows the simulated electric field $|E_z|$ inside the cavity vs. normalized radius, for a single unloaded and slot loaded disc. The $|E_z|$ of unloaded (UL) disc follows the first order Bessel function $J_1(k\rho)$ [10]. For UL case, the electric field null is at ~ 0.7a. We have observed that slot loading does not have significant effect on the position of electric field null as shown in Fig. 10. Compared to the fundamental mode, this property is an added advantage of TM_{12} mode since nulls in electric field allow us to suspend the patch on the air and hence eliminate the need for the substrate.

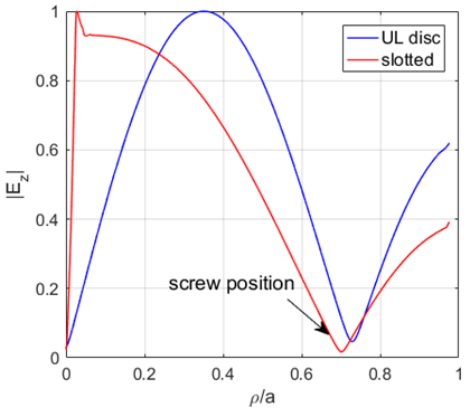


Fig. 10 Simulated cavity electric field vs normalized radius (ρ/a) for unloaded and slotted disc operating in TM_{12} mode.

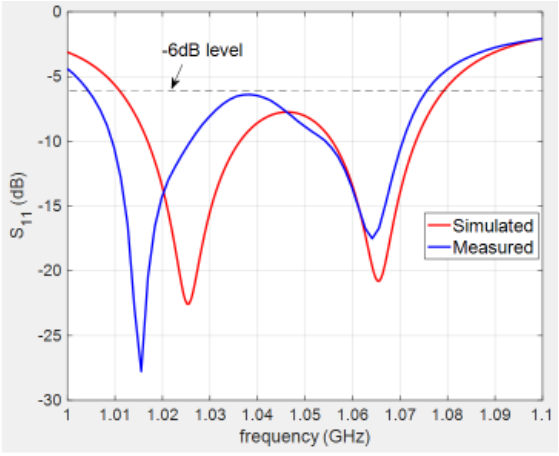
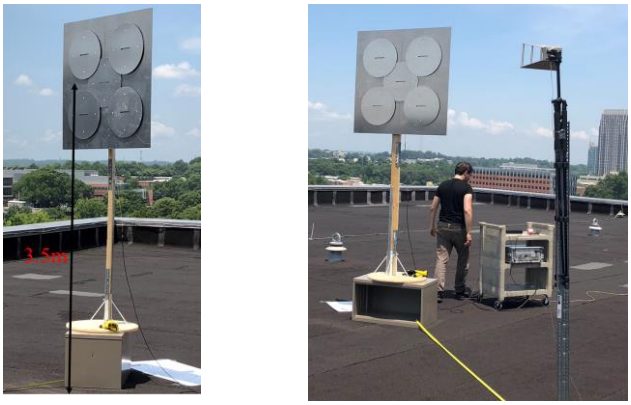


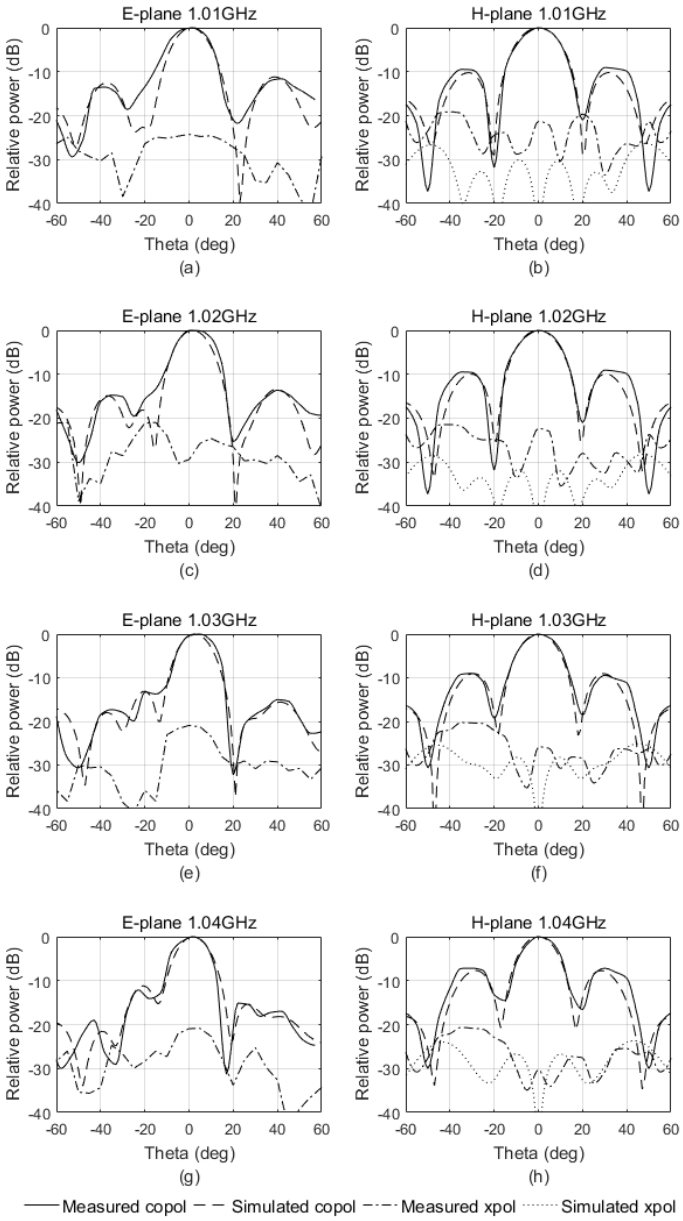
Fig. 11 Comparison of simulated and measured S_{11} as a function of frequency

Fig. 11 shows the simulated and measured reflection coefficient for the antenna shown in Fig. 9. The difference between the measured and the simulated resonant frequencies is less than 1%. The measured $S_{11} \leq -6$ dB bandwidth is 6.7% or 70 MHz. It covers the required bandwidth for the side-channel EM detection (shown later in Sec. V). Fig. 12 (a) & (b) shows the mounted antenna picture and the measurement set up to measure the near field and far field patterns of the proposed antenna. The proposed antenna is used as a receiving antenna while the transmitting antenna is a standard broadband double ridge waveguide horn shown in the Fig. 12(b). A digital protractor was used to measure the angle of rotation. The antenna patterns both near field and far field were measured at the roof top of Tech Square Research Building at Georgia Institute of Technology. The measurements were done for 3m, 5m (near field) and 15 m (far field) distance. The antennas were mounted at the height of 3.5 m above the ground. In the far field measurements, to reduce the specular ground reflections from the transmitting horn, the absorbers were used in the middle region of the measurement set up.



(a) (b)

Fig. 12 Pictures of antenna measurements (a) mounted antenna (b) measurement setup.



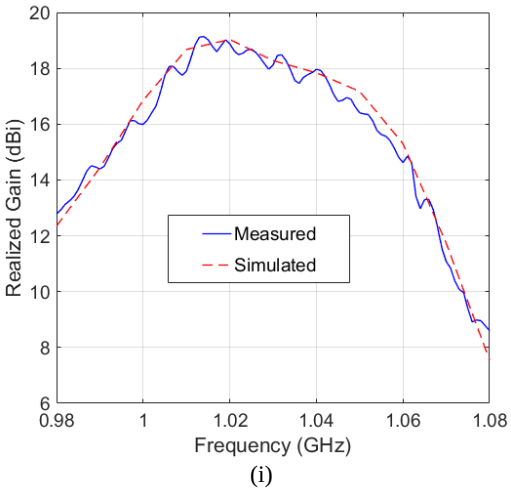


Fig. 13 Simulated and measured radiation patterns in E and H-plane (a) & (b) 1.01GHz, (c) & (d) 1.02GHz, (e) & (f) 1.03GHz, (g) & (h) 1.04GHz (i) Comparison of simulated and measured realized gain as a function of frequency.

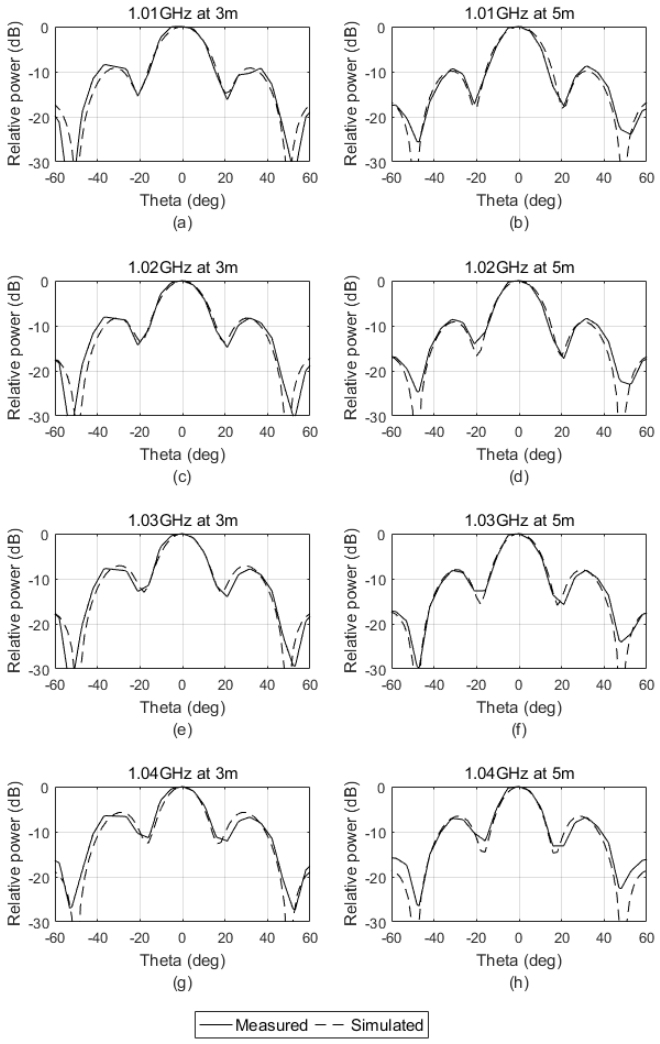


Fig. 14 Near field relative power patterns at 3m and 5m distances from the antenna aperture, (a) & (b) 1.01GHz, (c) & (d) 1.02GHz, (e) & (f) 1.03GHz, (g) & (h) 1.04GHz

Fig. 13 (a) - (h) shows the measured E & H-plane radiation patterns of the antenna, for the various frequencies in the band. The measured radiation patterns matches well with the simulated ones. In the measured E-plane pattern at 1.03 GHz, the beam is shifted by 3° as compared to 2° in the simulations, also observed earlier in Fig. 8. The measured cross-polarization is less than -21 dB and -19 dB, for the entire band in the E and H-plane respectively. In Fig. 13, the simulated crosspolarization in the E-plane are less than -40dB also shown in Fig. 8. Fig. 11 (i) shows the simulated and measured realized gain as a function of frequency for the fabricated antenna. For planar directive antennas, the peak gain and gain pattern measurements are conveniently conducted in the antenna measurement ranges. However, since we do not have access to antenna measurement ranges, we have verified the peak gain of the antenna by using the conventional gain transfer method [20], using standard horn. The measured gain matches well with the simulated one. Peak measured value is 19.2 dBi as

compared to 19.1dBi in the simulations. The measured value is higher due to the ripples in the gain measurements, which are ~ 1.2 dB and are caused by the standing wave patterns in front of the aperture due to reflections.

Fig. 14 shows the near field patterns of the antenna at 3 and 5m distances from the antenna aperture. Both the distances are in the radiating near field region of the antenna. The measured power pattern matches well with the simulated patterns. The measured maximum sidelobe level at 3 and 5m are -6.1dB and -6.6 dB respectively. It is observed that between 1.01 to 1.04 GHz, the maximum sidelobe level changes by ~ 3 dB, for both 3m and 5m distances. The antenna is used to receive the fields from the board processor at those distances as presented in the next section.

V. SNR Measurements & Malware Detection

The proposed antenna was used to measure the radiated emissions from the various embedded systems and Internet-of-Things (IoT) boards, at various distances under two conditions: direct Line of Sight (LoS) and Non-Line of Sight. These IoT boards typically consist of an ARM processor, a Flash memory, and a set of peripherals (e.g. WiFi modules, etc.). IoT boards are typically used for controlling a variety of tasks in factory lines, hospitals, critical infrastructures, etc. Recently, there have been a growing interest in attacking these devices since both the number and importance of them are growing rapidly. Monitoring these devices using the EM side-channel signals generated by them is one of the ways to improve the security of IoTs against cyber-attacks. Collecting stronger EM signals will improve the accuracy of the malware detector and that is the main goal of designing our proposed antenna.

A. Line of Sight (LoS) Measurements

Here, we will first describe the direct LoS measurements for the IoT board shown in Fig. 15 in detail. Figure 15 (a) shows a diagram of the measurement setup and Fig. 15 (b) shows the photo of the measurement setup where the proposed antenna is measuring the EM signal from an IoT device named Olimex [21] which has an ARM processor and runs a Linux operating system. The signal power measurements, using a spectrum analyzer (Agilent N9020A), were conducted at various distances between 1-5 m from the device. For each distance, two measurements were collected and the corresponding Signal to Noise Ratio (SNR) was calculated. Since it is not straightforward to estimate SNR for emanations from the electronic devices, we have conducted additional experiments to estimate SNR as described below.

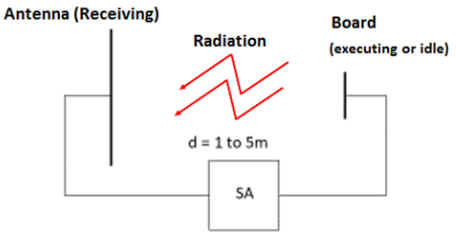
In the first set of measurements the objective is to estimate total emanated power, S, received when the board is on and running the program activity of interest.

In the second set of measurements, the objective is to estimate the noise spectral power, N, received when the board is on but there is no application running (idle mode). The noise power here includes thermal ($N_{thermal}$) noise as well as emanations coming from the board itself (N_{board}) that are not related to the program activity. SNR is then calculated as:

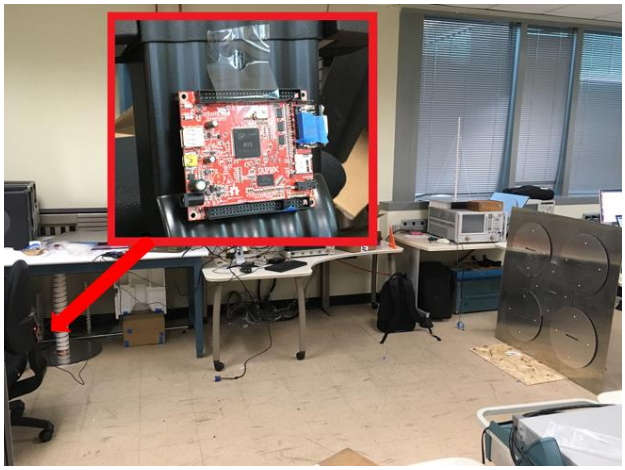
$$SNR\ (dB)\ =\ S\ (dB) - N\ (dB) \quad (1)$$

$$\text{SNR} = \frac{P_{r_{executing}}}{P_{r_{idle}} + N_{thermal}} \quad (2)$$

where, $P_{r_{executing}} \propto \frac{P_t}{r^2}$ is the power received when the processor is executing the code, while P_t is the power at the input. $P_{r_{idle}}$ is the power received when the processor is turned on but not executing a code. This part carries no useful information, and acts as a source of noise. $N_{thermal}$ is the thermal noise, independent of distance.



(a)



(b)

Fig.15 SNR Measurements for an IoT (Olimex) board: (a) Block diagram of set up (b) Set up picture that shows the antenna (on the right side) and the board (on the left side).

The proposed antenna is used to receive electromagnetic radiation coming from the board's processor. The objective is to find the possible malicious activities by analyzing the program execution through EM emanations. The main idea behind the malware detection method is that since there is a correlation between the program activities and the generated EM signals, executing a certain application will generate a unique and distinguishable signatures in the EM signal. Thus by collecting these EM signals for each application and extracting the signatures, a reference model for each application can be built. Then during monitoring, if an attacker changes the application's code, this will result in generating different EM signals that no longer match with the model and hence can be detected. Further details can be found in [11, 12].

The signature extraction is based on the premise that a program spends most of its time executing some repetitive code

(e.g. loops) which results in prominent peaks appearing in the spectrum separated by $\Delta f = {}^{1}/_{T}$, where T is the duration of a single loop iteration. In addition of base-band signal where these loops can be observed, they can also be observed as a modulated signal around the processor clock frequency (in our case 1 GHz), which is the signal we are observing. Measured power spectrum at the distances of 3 m and 5 m are shown in Fig. 16 (a) and (b) respectively. From Fig. 16 (a), we can observe that the strong spectral lines are amplitude modulated by a clock frequency (which acts as a carrier) of 1.008 GHz, which is significantly stronger than everything else. Each of the labeled harmonics are approximately 1.95 MHz apart from one another, which indicates that each iteration of the loop in the code takes about 514 ns. Since the board has many activities going on at once, it creates some other signals that are not related to the code that is being run on the processor. An example of this is marked as undesired signal in Fig. 16 (a).

Fig. 17 shows the measured SNR for various distances in comparison with the SNR obtained by a theoretical model defined in (2). The theoretical fit agrees well with the measured SNR.

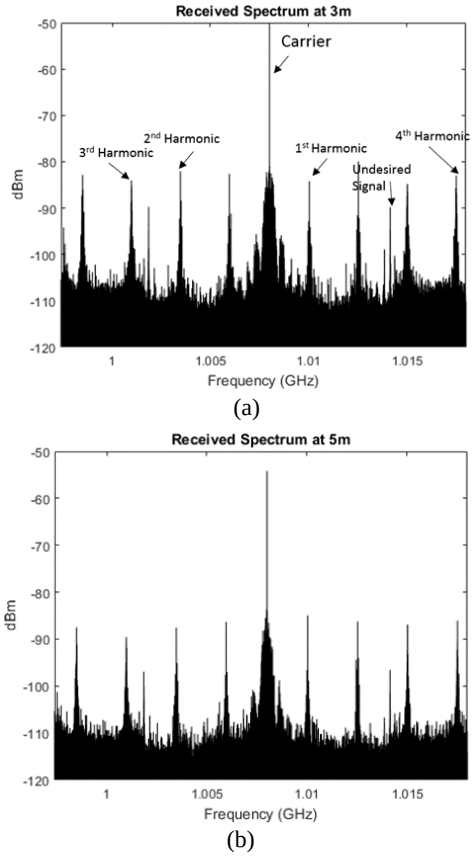


Fig. 16 Measured signal power while code is executing at various distances (a) 3 m and (b) 5 m.

To explain the measured SNR, with the theoretical model, the noise observed in the measurements is assumed to be created by two sources: thermal noise and the noise generated by the board itself. Since the processor is not intended to function as a transmitter, only a part of the total radiation coming out of the board carries meaningful information. This undesired part of the radiation lowers the quality of the signal. Since this part of the signal is radiated from the board, it gets weaker by a factor of r^2 , whereas the thermal noise is constant, as pointed out in (2). For this reason; at smaller distances $P_{r_{idle}}$ is more significant, at larger distances $N_{thermal}$ is more significant, and at intermediate distances the SNR trend is neither constant nor r^2. SNR fit is given as:

$$SNR_{fit} = \frac{\frac{a}{r^2}}{\frac{b}{r^2}+c} \tag{3}$$

$$SNR_{fit}^{-1} = \frac{b}{a} + \frac{c}{a}r^2 \tag{4}$$

It can be seen that SNR_{fit}^{-1} is a linear function of r^2 and the data points were fitted using linear least squares method. The multiplicative inverse was taken of the resulting line, which fitted the data very well.

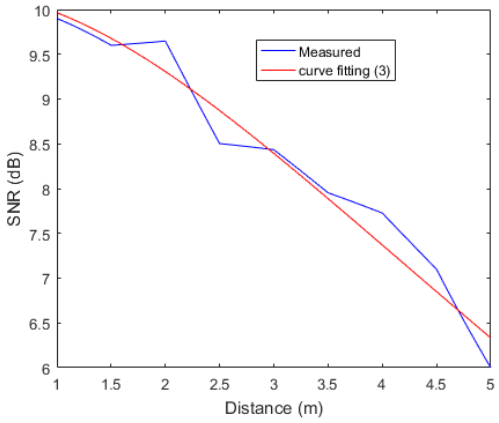


Fig. 17 Measured SNR vs. distance in comparison with the theoretical model fit.

B. Non-LoS Measurements

As mentioned earlier, the proposed antenna is designed so that it can be hanged on the wall and received the EM signals from electronic devices that are active in a room. In this scenario, not all the monitored devices would be in the LoS but the antenna should still be able to monitor them. In order to use the EM signals for malware detection, the spectral peaks (as shown in Fig. 16) should at least be 1dB higher than the noise floor. In other words, in order to be able to monitor non-LoS devices, the receiving signal should have peaks with at least 1dB higher than the noise floor.

To evaluate the effectiveness of our design, we repeat the measurement in Sec. V-A, this time with moving the board toward up-down and/or left-right directions from the center of the antenna with the step of 10 cm. All measurements are done while the center of the board is 3 m away from the center of the antenna. For each step (i.e. different distances from the center of antenna while being 3m away from it), we measure the SNR for the receiving EM signal. Fig. 18 shows the results for the weakest peak in the test application.

As shown in the Fig. 18, the antenna can receive EM signals with only 30% decrease in SNR while being 1 m away from the center of the antenna. However, our measurements show that beyond 1m, the SNR decreases dramatically. This is due to directive beam in both E and H-plane.

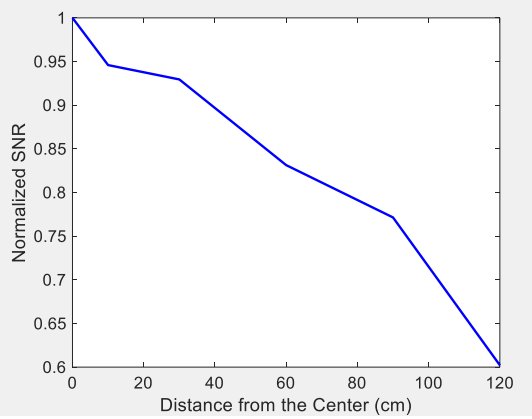


Fig. 18 Measured normalized SNR vs offset distance from the LoS (SNR = 1 corresponds to LoS).

C. *Malware Detection*

Finally, to illustrate how well the proposed antenna works in the system for malware detection, we use the antenna to receive EM signals while we are running several standard embedded systems applications such SHA, Djikstra's path-finding algorithm, QSort, CRC32, and FFT from a standard benchmark called *MiBench*. We also implement two real attacks: one a Distributed Denial-of-Service (DDoS) attack, and the other a Ransomware attack. We run the applications first 25 times without having any attack on them (benign), and 25 times with the DDoS attack, and 25 times with the Ransomware attack. We then used an algorithm proposed in [12] to analyze the receiving EM signals and label each run as either "benign" or "malicious". We then calculate False Positive Rate as the number of runs that were incorrectly labeled as "malicious" divided by the total number of runs. Similarly, True Positive is defined as the number of runs that are correctly labeled as "malicious".

Our results show that for all the applications while measuring from 3m, 4m, and 5m distances, we can perfectly find all the instances of the malware while achieving 0% false positive rate which confirms that our designed antenna is suitable for receiving EM signals from such devices from >3m distance.

Note that the results in [12] were reported while measuring from 5cm distance from the board and collected by a probe.

VI. Conclusions

In this paper a high gain planar slotted circular disc antenna, designed for receiving EM emanations modulated around processor clock was presented. The antenna was designed around 1 GHz for a 70 MHz bandwidth, using higher order mode TM_{12} mode, which had a larger electrical size than the fundamental mode. This was done to reduce the number of elements. The antenna was designed in stacked configuration which permits the use of EM coupling as an excitation and hence feed lines were avoided. The antenna was fabricated using aluminum circular slotted discs, which are suspended in air using Teflon screws. It was shown that the electric field null property of TM_{12} mode allows the use of screws to suspend the discs above the ground plane. The signal detection at the distances greater than 3 m were demonstrated by direct LoS SNR measurements from an IoT board. For each distance, SNR was calculated by subtracting the detectable signal power, when board activity is on, with the noise power when there is no activity. Finally, the antenna was used to collect EM signals from an IoT board while being >3m away from the board. The results show that using this antenna, an IoT board can be monitored from >3m with excellent accuracy. Furthermore, the antenna is cost effective and can be treated as a sub array for larger array for going further distances in EM emanations measurements.

References

[1] M. G. Kuhn, "Compromising emanations of lcd tv sets," *IEEE Trans. On Electromagnetic Compatibility*, vol. 55, no. 3, pp. 564–570, June 2013.

[2] Y. I. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J. L. Danger, "Analysis of electromagnetic information leakage from cryptographic devices with different physical structures," *IEEE Trans. On Electromagnetic Compatibility*, vol. 55, no. 3, pp. 571–580, June 2013.

[3] H. Sekiguchi and S. Seto, "Study on maximum receivable distance for radiated emission of information technology equipment causing information leakage," *IEEE Trans. on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 547–554, June 2013.

[4] A. Zajić and M. Prvulovic,"Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 4, pp. 885-893, August 2014.

[5] N. Sehatbakshsh, R. Callan, M. Alam, M. Prvulovic, and A. Zajic, "Leveraging Electromagnetic Emanations for IoT Security," Hardware Demo at *IEEE International Symposium on Hardware Oriented Security and Trust* (HOST) May 1-5, 2017.

[6] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, and M. Prvulovic, "EDDIE: EM-Based Detection of Deviations in Program Execution," *Proceedings of the 44th International Symposium on Computer Architecture (ISCA)*, June2017.

[7] A. Zajic, Milos Prvulovic, and Derrick Chu, "Path loss prediction for electromagnetic side-channel signals," *Proceedings of the 11th European Conference on Antennas and Propagation*, pp.1-5, Paris, France, April 2017

[8] A. Derneryd, "Analysis of the microstrip disc element," IEEE Trans. Antennas Propagation, vol. 27, no. 5, pp. 660–664, Sep. 1979.

[9] P. Juyal and L. Shafai, "A novel high-gain printed antenna configuration based on TM_{12} mode of circular disc," IEEE Trans. Antennas Propagation, vol. 64, no. 2, pp. 790–796, Feb. 2016.

[10] J. R. James and P. S. Hall, Eds., Handbook of Microstrip Antennas. London, U.K.: Peregrinus, 1989.

[11] N. Sehatbakhsh, A. Nazari, A. Zajic, and M. Prvulovic, "Spectral profiling: Observer-effect-free profiling by monitoring em emanations," in Microarchitecture (MICRO), 2016 49th Annual IEEE/ACM International Symposium on, 2016, pp. 1–11

[12] Nazari, Alireza, et al. "EDDIE: EM-Based Detection of Deviations in Program Execution." Proceedings of the 44th

Annual International Symposium on Computer Architecture. ACM, 2017.

[13] H. Legay and L. Shafai, “New stacked microstrip antenna with large bandwidth and high gain,” Inst. Elect. Eng. Proc. Microw. Antennas Propagation, vol. 141, no. 3, pp. 199–204, Jun. 1994.

[14] P. Juyal, L. Shafai, "Sidelobe Reduction of TM_{12} Mode of Circular Patch via Non-resonant Narrow Slot", IEEE Trans. Antennas Propagation, vol. 64, pp. 3361-3369, 2016,

[15] A. Vosoogh and P.-S. Kildal, “Simple formula for aperture efficiency reduction due to grating lobes in planar phased arrays,” IEEE Trans. Antennas Propagation, vol. 64, no. 6, pp. 2263–2269, Jun. 2016.

[16] K. C. Kerby and J. T. Bernhard, “Sidelobe level and wideband behavior of arrays of random subarrays,” IEEE Trans. Antennas Propagation, vol. 54, no. 8, pp. 2253–2262, Aug. 2006.

[17] S. A. Razavi, P.-S. Kildal, L. Xiang, and E. Alfonso, “2 × 2-slot element for 60 GHz planar array antenna realized on two doubled-sided PCBs using SIW cavity and EBG-type soft surface fed by microstrip-ridge gap waveguide,” IEEE Trans. Antennas Propagation, vol. 62, no. 9, pp. 4564– 4573, Sep. 2014.

[18] T. J. Brockett and Y. Rahmat-Samii, “Subarray design diagnostics for the suppression of undesirable grating lobes,” IEEE Trans. Antennas Propagation, vol. 60, no. 3, pp. 1373–1380, Mar. 2012.

[19] D. Blanco, N. Llombart, and E. Rajo-Iglesias, “On the use of leaky wave phased arrays for the reduction of the grating lobe level,” IEEE Trans. Antennas Propagation, vol. 62, no. 4, pp. 1789–1795, Apr. 2014.

[20] G. Mayhew-Ridgers, J. W. Odendaal and J. Joubert, "Accuracy of the gain-transfer method for a standard gain antenna and a test antenna with equal aperture dimensions," *Communications and Signal Processing, 1998. COMSIG '98. Proceedings of the 1998 South African Symposium on*, Rondebosch, 1998, pp. 313-314.

[21] Olimex, “A13-olinuxino-micro user manual.” https://www.olimex. com/Products/OLinuXino/A13/A13-OLinuXino-MICRO/open-sourcehardware, accessed April 3, 2016.