مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هفتم، شماره ۴، زمستان ۱۳۹۵؛ ص ۳۵۰-۳۳۹

طراحی و ساخت آنتن هوشمند برای بهبود امنیت لینک‌های ارتباطی

امیر حبیبی درونکلا[۱]، سمیه چمانی[۲*]، یعقوب قانع قره‌باغ[۳]
۱- کارشناسی ارشد، ۲- استادیار، دانشگاه صنعتی خواجه نصیرالدین طوسی، ۳- مربی، دانشگاه جامع امام حسین (ع)
(دریافت: ۹۴/۱۲/۲۵، پذیرش: ۹۵/۰۶/۲۰)

چکیده

در این مقاله یک سامانه آنتن هوشمند برای استفاده در سکوهای متحرک پیشنهاد شده است. سامانه طراحی‌شده می‌تواند به صورت هوشمند سمت سکوی متحرک دیگری را تشخیص داده و به صورت دید مستقیم با آن ارتباط برقرار کند. برقراری ارتباط با دقت بالا در جهت مورد نیاز نسبت به حالت همه‌جهته امنیت لینک و میزان سیگنال به نویز دریافتی در سامانه آنتن گیرنده را بالا می‌برد. سامانه آنتن هوشمند ساخته‌شده‌هساخته‌شده در این مقاله شامل شش قطاع است که عملکرد آن‌ها توسط یک برد کنترلی هوشمند کنترل می‌شود. عملکرد سامانه به این صورت است که برای شروع ارتباط، سکوی متحرک اولیه یک سیگنال به صورت همه‌جهته ارسال کرده و سکوی متحرک دوم بر اساس اینکه SNR از کدام قطاع قوی‌تر دریافت می‌شود، جهت سامانه اولیه را تشخیص می‌دهد، سپس عملیات هم‌راستاسازی انجام می‌شود. هر قطاع از آنتن هوشمند پیشنهادی دو باند فرکانسی C و UHF را پشتیبانی کرده و آرایه وفقی انتخاب‌شده‌هانتخاب‌شده از نوع بیم سوئیچ شده است. المان آنتنی انتخابی در باند C و UHF به ترتیب پچ و Rubber duck هستند. با به‌کارگیری آنتن هوشمند پیشنهادی در لینک ارتباطی امنیت لینک تا حدود ۴/۷ برابر افزایش خواهد یافت.

کلیدواژه‌ها: آنتن هوشمند، سطح امنیت، بیم سوئیچ شده

Design and Construction of Smart Antennas to Improve the Security of Communications Links

A. H. Daronkola, S. Chamani*, Y. Qane
K.N. Toosi University of Technology
(Received: 16/03/2016; Accepted: 10/09/2016)

Abstract

In this paper, a smart antenna system to be used in moving platforms is proposed. The designed system detects intelligently direction of the other moving platform and communicates with it in a poin to point manner. Compared to omnidirectional transmission, poin to point communication with a high accuracy in the required direction increases the link security and signal to noise ratio (SNR) in the receiver system. The fabricated smart antenna system consists of six sectors, the performance of which is controlled by an intelligent control board. First, the primary moving platform sends a signal to all directions and the second moving platform decides about direction of primary platform, considering the strongest SNR among sectors. In the next stage, aligning operation is performed. Each sector of the proposed smart antenna supports two frequency bands of UHF and C and the implementd adaptive array type is beam-switched. Antenna elements in C and UHF-band are Patch and Rubber duck, respectively. The results show that using the proposed smart antenna in the communication link, increases the security up to 4.7 times.

Keywords: Smart Antenna, Security Level, Switched-Beam

*Corresponding Author E-mail: chamaani@eetd.kntu.ac.ir

۱. مقدمه

با وجود اینکه علاقه به استفاده از سامانه‌های بی‌سیم روزبه‌روز در حال افزایش است، ولی هنوز مانعی در مسیر استفاده از سامانه‌های بی‌سیم وجود دارد و آن مانع ناامن بودن ذاتی شبکه‌های بی‌سیم است. با توجه به ماهیت بی‌سیم بودن لینک ارتباطی، یک شنودگر می‌تواند در یک مکان نامعلوم به صورت کاملاً نامحسوس به اطلاعات مهم دسترسی پیدا کند و علت این امر هم پخش همگانی[1] اطلاعات به سبب استفاده از آنتن همه‌جهته در لینک‌های ارتباطی است [۱].

سه حمله متداول شبکه‌های بی‌سیم را تهدید می‌کنند؛ استراق سمع، فریب و رد سرویس[2]. متخصصان به این مشکلات امنیتی پی بردند و راه‌حل‌هایی برای افزایش امنیت سامانه‌های ارتباطی ارائه دادند که عبارت‌اند از: استاندارد IEEE 802.1X، فیلتر کردن آدرس MAC[3] و الگوریتم‌های رمزنگاری WEP/IPSec[4] [۲-۴]. متأسفانه همه این روش‌ها بر پایه نرم‌افزار هستند و نیاز به روش‌های امن‌تری برای احراز هویت و یا الگوریتم‌های رمزنگاری مؤثرتری دارند. همان طورهمان طور که می‌دانید هر راه‌حل نرم-افزاری دارای مزایا و معایبی است. همچنین راه‌حل‌های نرم‌افزاری، منابع سامانه‌ای و پهنای باند بیشتری می‌طلبند، به همین دلیل، سهولت استفاده از آن‌ها کاهش می‌یابد. چندین مقاله در مجلات معتبر برای اثبات نفوذپذیری راه‌حل‌های نرم‌افزار محور به چاپ رسیده است. مسلماً ارائه یک بستر سخت‌افزاری امن راه‌حل بهتری نسبت به تحقق امنیت بر پایه نرم‌افزار خواهد بود. یکی از راه‌حل-های سخت‌افزاری، استفاده از آنتن هوشمند است [۵].

از طریق فناوری آنتن هوشمند می‌توان انواع طرح‌های روش دسترسی مالتی‌پلکس تقسیم فضایی[5] (SDMA) را اجرایی نمود. در روش SDMA یک فضای همه‌جهته به تعدادی زیرفضای پرتو باریک تقسیم می‌شود. هر زیرفضا به صورت جداگانه در حالت فرستندگی- گیرندگی کار می‌کند و بدون هیچ تداخلی با زیرفضای دیگر به ارسال اطلاعات می‌پردازد. در آنتن هوشمند زیرفضاهای روش SDMA از طریق قطاع‌بندی محقق می‌شوند [۶]. در دسته‌بندی آنتن‌های هوشمند رویکردهای مختلفی وجود دارد. از جمله می‌توان آن‌ها را به دو دسته کلی MIMO[6] و آرایه وفقی تقسیم‌بندی کرد. با به‌کارگیری فناوری MIMO، بازدهی طیفی افزایش می‌یابد و سامانه در برابر اثرات چند مسیرگی مقاوم خواهد بود. آنتن‌های آرایه وفقی نیز شامل: بیم سوئیچ شده، آرایه پارازیتیک، آرایه شکل‌دهی پرتو دیجیتال و آرایه فازی می‌شوند که از این بین آنتن بیم سوئیچ به علت هزینه پایین پیاده‌سازی، بیشتر مورد علاقه متخصصان بوده است [۷].

در یکی از طرح‌های مشابه به طراحی و ساخت آنتن هوشمند با ۱۲ المان آنتنی هورن در باند فرکانسی Ku پرداخته شده و روش‌های کاهش ابعاد و وزن ساختار کلی آنتن مورد بررسی قرار گرفته است. آنتن ساخته‌شدهساخته‌شده در این مقاله، شبکه تغذیه پیچیده‌ای دارد که جهت پیاده‌سازی به فناوری مواد و ابزارهای دقیق نیازمند است [۸]. در مقاله مشابه دیگری آنتن پهن‌باند چند پرتویی برای به‌کارگیری در سکوهای کوچک طراحی و ساخته‌شده است. ساختار کلی این آنتن شامل ۸ قطاع ۳۲ المانی است که المان در نظر گرفته‌شده جهت افزایش پهنای باند و کاهش وزن ساختار کلی، آنتن بال پروانه‌ای[7] است. آنتن ساخته‌شده در این مقاله قابلیت شکل‌دهی پرتو در هر قطاع را نیز دارد. باند فرکانسی آنتن ساخته‌شده در این مقاله GHz ۱۵-۶ است و هزینه پیاده‌سازی آن بالاست [۹]. همچنین در طرح مشابه دیگری نتایج ساخت آنتن بیم سوئیچ در باند فرکانسی GHz ۴۰-۳۷ بررسی شده است. این مقاله به ارائه راهکارهایی برای کاهش وزن ساختار کلی آنتن پرداخته و در نهایت تزریق پلاستیک در فرآیند ساخت المان آنتنی هورن را مد نظر قرار داده است. در این مقاله از ۱۲ المان آنتنی هورن برای تقسیم فضایی استفاده می‌شود [۱۰]. استفاده از آنتن هورن در فرکانس‌های پایین به علت افزایش ابعاد ساختار کلی، مورد علاقه طراحان نیست.

مقاله حاضر بر روی استفاده از آنتن هوشمند جهت بهبود امنیت شبکه‌های ارتباطی تمرکز کرده و یک نمونه آزمایشگاهی از آن را ساخته است. مقرون به صرفه بودن، کاهش ابعاد، جهتی کردن پرتو در فرکانس UHF با استفاده از آنتن همه‌جهته و استوانه فلزی و پشتیبانی از دو باند فرکانسی با اختلاف GHz ۳/۵، از وجوه تمایز آنتن پیشنهادی در این مقاله نسبت به کارهای گذشته است. سامانه آنتن هوشمند پیشنهادی توانایی ارسال و دریافت داده در هر دو باند فرکانسی مذکور را دارد، اما برای آزمایش عملکرد و کاهش هزینه‌ها، گیرندگی در باند C برای تشخیص جهت سیگنال و فرستندگی در باند UHF در آزمایشگاه مورد ارزیابی قرار گرفته است.

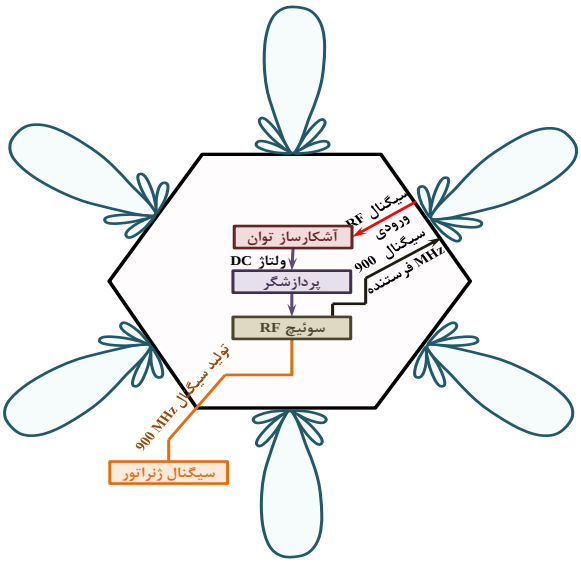
در ادامه معماری، آنتن هوشمند را بیان خواهد شد، سپس مدار کنترلی پیشنهادی معرفی و نتایج شبیه‌سازی ساخت آنتن‌های پچ[8] و Rubber duck را نشان داده خواهد شد. پس از بیان سطح امنیتی، نتایج شبیه‌سازی و آزمایش ارائه خواهد شد و در نهایت به نتیجه‌گیری کار پرداخت خواهد شد.

[1] Broadcast
[2] Deny of Service
[3] Medium Access Control
[4] Wired Equivalent Privacy
[5] Space Division Multiple Access
[6] Multiple Input Multiple Output
[7] Bowtie
[8] Patch

۲. معماری اجزای آنتن قطاعی با لحاظ کردن ابعاد واقعی

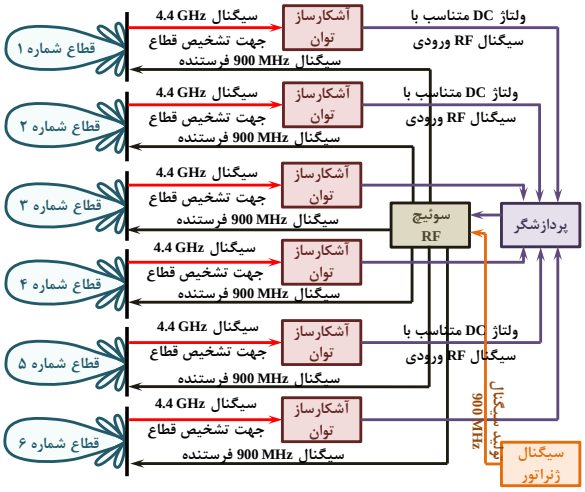
نمای مقطعی سامانه آنتن قطاعی در شکل (۱) نمایش داده شده است. در این شکل بلوک دیاگرام عملکرد یک قطاع ترسیم شده است که شامل بلوک آشکارساز توان[1]، پردازشگر، سوئیچ RF و واحدهای فرستنده و گیرنده است. همان طور که ملاحظه می‌شود؛ تعداد قطاع‌ها برابر ۶ در نظر گرفته شده است و این مقدار بر اساس قطر استوانه آنتن قطاعی تعیین شده است.

میزان قطر قابل‌قبول با توجه به محدودیت‌های وزن و ابعاد محموله برابر ۲۵ سانتی‌متر است. برای پوشش کل فضا در سمت، به وسیله آنتن قطاعی لازم است که هر آنتن کمینه ۶۰ درجه را پوشش دهد. نوع آنتن نیز بر اساس محاسبات بودجه لینک و بهره آنتن مورد نیاز تعیین می‌شود. در شکل (۲) بلوک دیاگرام طبقات مداری کل آنتن قطاعی نمایش داده شده است. همان طور که در این بلوک دیاگرام مشاهده می‌شود، پس از اینکه سیگنال توسط هر یک از قطاع‌ها دریافت شد، وارد طبقه آشکارساز توان می‌شود.

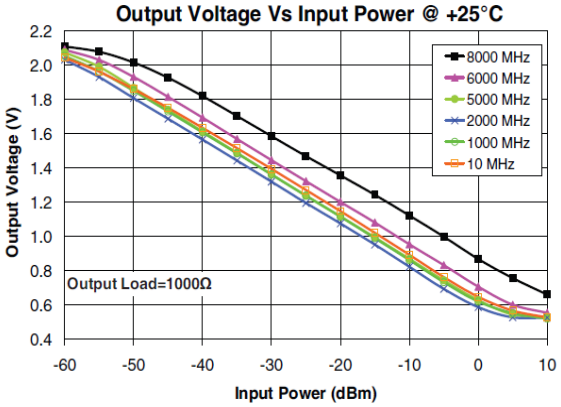


شکل ۱. نمای آنتن قطاعی با مشخص کردن مدارات مربوط به یک قطاع (از نمای بالا).

با توجه به شکل (۳) که نشان‌دهنده ولتاژ DC خروجی متناسب با توان RF ورودی است، آشکارساز توان در هر لحظه متناسب با توان RF ورودی یک ولتاژ DC تولید می‌کند که این ولتاژ توسط پردازشگر مرکزی قابل‌درک است. دقیقاً همین فرآیند به صورت هم‌زمان برای سایر قطاع‌ها اتفاق می‌افتد. بنابراین در هر لحظه درگاه‌های ورودی پردازشگر مرکزی، ولتاژ DC مربوط به قطاع منتسب به خود را ارسال کرده و با مقایسه این ولتاژها به بررسی وضعیت هر یک از قطاع‌ها در آن لحظه می‌پردازد. توجه شود که هرچه سطح سیگنال RF ورودی به قطاع بیشتر باشد، آن قطاع در وضعیت بهتری برای انتخاب برای حالت فرستندگی (یا گیرندگی) دارد. بنابراین پردازشگر، با توجه به الگوریتم پیش‌بینی‌شده، قطاع مورد نظر را انتخاب می‌کند و به سوئیچ RF دستور روشن کردن قطاع انتخاب‌شده‌انتخاب‌شده را می‌دهد. سوئیچ RF متناسب با دستور پردازشگر، مسیرسیگنال ۹۶۰MHz را از فرستنده تا قطاع مورد نظر برقرار می‌کند تا از طریق قطاع مورد نظر سیگنال ارسال شود.



شکل ۲. بلوک دیاگرام طبقات مداری آنتن قطاعی



شکل ۳. ولتاژ خروجی آشکارساز توان نسبت به توان ورودی در فرکانس‌های مختلف

۳. مدار کنترلی آنتن هوشمند پیشنهادی

پردازشگر مورد استفاده در مدار کنترلی آنتن هوشمند پیشنهادی جهت کاهش هزینه از خانواده AVR است. البته در سامانه‌های آنتن هوشمند جدید از پردازشگر FPGA نیز به علت سرعت بالای آن در پردازش استفاده می‌شود. در واقع مدار کنترلی آنتن هوشمند در این مقاله، ولتاژ DC تولید شده توسط آشکارساز توان

[1] Power Detector

را پردازش و بر روی آن عملیات انجام می‌دهد. در واقع وظیفه مدار کنترلی آنتن هوشمند این است که در هر لحظه، شش سیگنال DC متغیر با زمان تولید شده توسط آشکارساز توان‌ها را طی الگوریتمی توسط پردازشگر AVR، پردازش و متناسب با آن دستور برقراری لینک ارتباطی از قطاع انتخاب‌شده را صادر کند.

برد کنترلی پیشنهادی: برد کنترلی از پنج قسمت مداری تشکیل شده است که هر کدام از آن‌ها به طور جداگانه آزمایش‌شده و عملکردشان مورد بررسی قرار گرفته است. اولین و اساسی‌ترین قسمت یک مدار الکتریکی که باید تمامی محدودیت‌های آن اعم از بیشینه جریان، ولتاژ، توان اتلافی، نحوه عملکرد و کارایی مد نظر قرار گیرد؛ انتخاب صحیح و مناسب منبع تغذیه است.

برای تثبیت ولتاژ خروجی منابع تغذیه از رگولاتورهای ولتاژ استفاده می‌شود. یکی از ویژگی‌های مهم منبع تغذیه مقدار ولتاژ و جریانی است که می‌تواند برای بار خود تأمین کند. علاوه بر مسائل فوق، پایداری ولتاژ منبع تغذیه در شرایط مختلف باید مد نظر قرار گیرد.

قسمت دوم این سامانه، تقویت سیگنال کوچک ورودی‌های DC است. برای اینکه بتوان اثرات نویز را از بین برد، باید سیگنال‌ها تقویت شود تا در زمان نمونه‌برداری بهترین عملکرد را داشته باشند. یکی از مهم‌ترین و کلیدی‌ترین مسائلی که در مدار پیشنهادی مد نظر قرار گرفته، این است که همه تقویت‌کننده‌ها سیگنال‌های ورودی‌شان را به یک نسبت تقویت کنند و انحراف ولتاژ خروجی نزدیک به صفر باشد.

باید در نظر داشت که، تقویت‌کننده‌ها از نظر ساخت به طور کامل شبیه هم نیستند و تلرانس خود قطعات نیز باعث ایجاد خطا می‌شود. قسمت سوم سامانه، که هسته اصلی مدار است، میکروکنترلر Atmega16 است. قسمت چهارم سامانه، مسئول تقویت جریان با استفاده از ترانزیستورهاست. در این حالت ترانزیستور در ناحیه اشباع و قطع عمل می‌کند و کمترین تلفات را دارد. قسمت پنجم سامانه رله است، استفاده از رله موجب می‌شود که ولتاژها ایزوله شود و جریان مورد نیاز برای روشن کردن سوئیچ به راحتی تأمین شود.

۴. آنتن پچ

از مزایای مهم آنتن‌های پچ حجم کم، قابلیت تولید انبوه، قابلیت تطبیق با مدارات مجتمع و ... است. پس از بررسی انواع آنتن جهت پیاده‌سازی در آنتن هوشمند پیشنهادی، با توجه به مزایای ذکرشده، آنتن پچ جهت استفاده در باند فرکانسی C انتخاب شد.

اشکال اساسی این نوع آنتن‌ها، دایرکتیویتی و پهنای باند کم آن‌ها است. البته می‌توان با به‌کارگیری آن‌ها به صورت آرایه‌ای، دایرکتیویتی را افزایش داد.

از جمله عوامل مؤثر بر روی مشخصه و راندمان آنتن، ضریب دی‌الکتریک لایه عایقی، شکل و فرم عنصر تشعشع کننده، ضخامت لایه عایقی و شبکه، تغذیه این آنتن‌هاست. این عوامل بر روی فرکانس کار، امپدانس ورودی، پهنای باند، پرتو تشعشعی و پلاریزاسیون اثر می‌گذارد. پس از بررسی انواع ساختارهای آنتن پچ، پچ دایروی برای ساخت انتخاب شد.

آنتن پچ دایروی: پچ دایروی مشخصات مشابهی با پچ مستطیلی دارد؛ از جمله این مشخصات می‌توان به بهره، وضعیت پرتوهای تشعشعی و بازده اشاره کرد. اما به علت اختلاف در ساختار فیزیکی با پچ مستطیلی، پچ دایروی پهنای باند، پرتوها و الگوهای تشعشعی باریک‌تری نسبت به پچ مستطیلی ارائه می‌دهد. مهم‌ترین مزیت آنتن پچ نسبت به آنتن‌های دی‌الکتریکی تشدیدی سادگی ساخت و ارزان بودن است.

روش تغذیه: پچ دایروی به سادگی ساخته می‌شود و تغذیه آن به وسیله اتصال کابل کواکسیال به نقطه مناسبی از پچ انجام می‌شود. نقطه اتصال به طور اساسی به فرکانس مرکزی و امپدانس ورودی (معمولاً ۵۰ اهم) مرتبط است.

روابط آنتن پچ دایروی: فرکانس رزونانس آنتن پچ دایروی ۴/۴GHz، ثابت دی‌الکتریک ۳/۳۸ و ارتفاع فیبر را ۰/۸ mm در نظر گرفته می‌شود و با توجه به روابط زیر شعاع پچ را به دست می‌آید [۱۱]:

$$a=\frac{F}{\left\{1+\frac{2h}{\pi\varepsilon_r F}\left[ln\left(\frac{\pi F}{2h}\right)+1.7726\right]\right\}^{\frac{1}{2}}} \qquad (۱)$$

در رابطه بالا، h بیانگر ضخامت زیرلایه است و a همان شعاع پچ دایروی است. F در رابطه (۱) از رابطه زیر به دست می‌آید [۴].

$$F=\frac{8.791\times10^9}{f_r\sqrt{\varepsilon_r}}=\frac{8.791\times10^9}{4.4\times10^9\sqrt{3.38}}=1.0867 \qquad (۲)$$

با جایگذاری مقادیر $F=1.0867$، $\varepsilon_r=3.38$ و $h=0.8mm$ در رابطه (۱) شعاع پچ دایروی $a=10.4mm$ خواهد شد. شعاع مؤثر پچ دایروی از رابطه (۳) به دست می‌آید [۱۱].

$$a_e=a\left\{1+\frac{2h}{\pi\varepsilon_r a}\left[ln\left(\frac{\pi a}{2h}\right)+1.7726\right]\right\}^{\frac{1}{2}} \qquad (۳)$$

با جایگذاری مقادیر در رابطه بالا شعاع موثر پچ دایروی نیز $a_e = 10.8mm$ خواهد شد.امپدانس ورودی در هر فاصله شعاعی $\rho' = \rho_0$ از مرکز پچ از رابطه زیر به دست می‌آید [۱۱]:

$$R_{in}\left(\rho' = \rho_0\right) = \frac{1}{G_t}\frac{J_m^2(kp_0)}{J_m^2(ka_e)} \qquad (۴)$$

در رابطه بالا، $\rho = 2(2a)/\lambda$ فاصله شعاعی است. با توجه به رابطه (۴) جهت تطبیق امپدانس ۵۰ Ω، فاصله نقطه تغذیه از مرکز پچ می‌بایست ۲/۸ mm باشد.

۵. آنتن Rubber duck

آنتن‌های Rubber Duck، آنتن‌هایی با طول الکتریکی کم هستند. به طور خلاصه زمانی به یک آنتن از لحاظ الکتریکی کوچک گفته می‌شود که طول آنتن از $\lambda/10$ بزرگ‌تر نباشد. آنتن‌هایی که از لحاظ الکتریکی کوتاه‌تر هستند، باید راکتانس خازنی بالایی داشته باشند. راکتانس خازنی با فرکانس سیگنال رابطه عکس دارد، بنابراین هر چه فرکانس افزایش یابد؛ راکتانس خازنی کم می‌شود. راکتانس خازنی کم، مطلوب نیست؛ پس باید راکتانس خازنی را به نحوی خنثی کرد. این کار با اضافه کردن سلف تحقق می‌یابد. مقدار سلف باید طوری انتخاب شود که راکتانس‌های سلفی و خازنی یک دیگر را خنثی کنند. برای این منظور سلف با آنتن سری می‌شود. به این نوع از آنتن‌ها که در آن‌ها سیم‌پیچ با آنتن سری بوده و در پایه آنتن قرار می‌گیرد، آنتن‌های Base Loaded گفته می‌شود [۱۲].

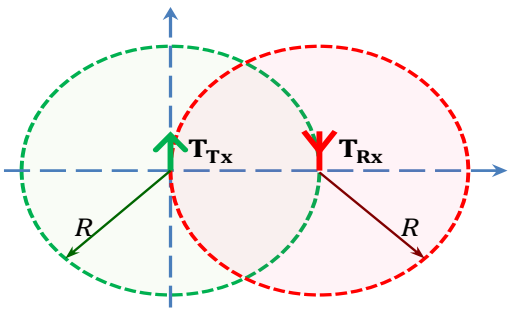
در آنتن Rubber Duck سلف (سیم‌پیچ) به جای اینکه در پایه آنتن باشد، داخل خود آنتن ساخته‌شده است. یعنی در واقع آنتن تماماً از یک فنر فلزی که کارکردی مشابه همان سیم‌پیچ دارد ساخته‌شده است. این آنتن‌ها برای پشتیبانی از باند UHF تهیه و به کمک ساختار فلزی کلی آنتن هوشمند، پرتو همه‌جهته آن جهتی شده است [۱۲].

۶. تعیین سطح امنیتی

با توجه به آزمایش‌های انجام‌شده برای هک کردن پروتکل امنیتی WEP و به دست آوردن داده‌های بسته، زمانی شنودگر می‌تواند به شنود و اخلال در یک لینک ارتباطی بپردازد که او یا تجهیزاتش درون محیطی باشند که هر دو سیگنال نقطه دسترسی (AP[1]) و پایانه، با کیفیت مطلوبی دریافت شوند [۱۳]. محدوده‌ای که بتوان هر دو سیگنال را به خوبی دریافت کرد همان محدوده فصل مشترک دو سیگنال است. اگر یکی از این دو سیگنال معیوب دریافت شود، اطلاعاتی که شنودگر به دست می‌آورد، ناقص و حتی غیرقابل آشکارسازی است. البته اطلاعات AP برای شنودگر نسبت به پایانه از اهمیت بیشتری برخوردار است؛ چون می‌تواند از بسته‌های داده مدیریتی، اطلاعات مهمی به دست آورد. این مسئله به معنی بی‌اهمیتی اطلاعات پایانه نیست. این محدوده را محدوده امنیتی نامیده می‌شود و یک سطح امنیتی متناظر با آن تعریف می‌شود که با ابعاد محدوده سیگنال و ابعاد محدوده امنیتی رابطه دارد.

به دلیل اینکه اکثر تجهیزات شبکه‌های ارتباطی موجود، مجهز به آنتن همه‌جهته هستند، معمولاً محدوده سطح امنیتی با محدوده سیگنال برابر است. اگر آنتن هوشمند در ارتباطات بی‌سیم به کار گرفته شود، وضعیت امنیتی متفاوت خواهد بود. محدوده امنیتی باید کوچک‌تر از محدوده سیگنال باشد. از منظر ارتباطات بی‌سیم هر چه این محدوده کوچک‌تر باشد؛ ارتباط امن‌تر خواهد بود. با فرض شرایط LOS[2] (آنتن‌ها روبه‌روی هم قرار گرفته‌اند و مانعی در مسیر وجود ندارد)، فاصله بین AP تا پایانه را به عنوان شعاع یک دایره در نظر گرفته می‌شود. تمرکز این مقاله بر سیگنال درون این محدوده است. ابعاد محدوده سیگنال را S_1 و ابعاد محدوده امنیتی را S_2 نامیده می‌شود. همچنین، پهنای بیم آنتن جهتی استفاده‌شده در AP و پایانه را به ترتیب θ و α نامیده می‌شود. جهت تعیین سطح امنیتی از لگاریتم نسبت مساحت‌ها استفاده می‌شود. بر اساس اینکه AP و پایانه هر کدام از آنتن هوشمند جهتی استفاده می‌کنند یا خیر، چهار سناریو امکان‌پذیر است:

سناریو اول: نقطه دسترسی و پایانه مجهز به آنتن همه‌جهته هستند. این سناریو بسیار متداول است. سطح امنیتی در این حالت برابر است با [۱۳]:



شکل ۴. نحوه پوشش آنتن‌ها در سناریو اول

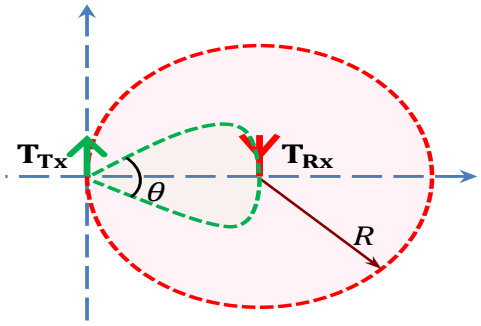
$$\eta = \log\left(\frac{10\times S_1}{S_2}\right) = \log(10) = 1 \qquad (۵)$$

سناریو دوم: نقطه دسترسی مجهز به آنتن جهتی و پایانه مجهز به آنتن همه‌جهته است (شکل (۵)). شکل بیم آنتن جهتی به صورت بیضی است ولی محاسبه سطح امنیتی با شکل بیم بیضوی مشکل

[1] Access Point

[2] Line of Sight

است، به همین دلیل جهت ساده‌سازی محاسبات به جای بیضی از قطاعی که مرزهای آن نقاط ۳ dB و پهنای بیم θ است؛ استفاده می‌شود. با توجه به شکل (۵) در می‌یابیم که محدوده امنیتی از سطح دایره کامل در سناریو ۱ به سطح قطاع تقلیل پیدا می‌کند.



شکل ۵. نحوه پوشش آنتن‌ها در سناریو دوم

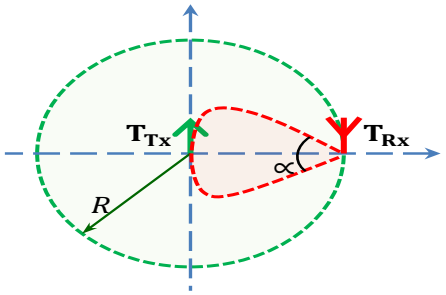
$$S_1 = \pi R^2$$

$$S_2 = \pi R^2 \frac{\theta}{360}$$

سطح امنیتی در سناریوی دوم از طریق رابطه (۶) محاسبه می‌شود.[۱۳].

$$\eta = \log\left(\frac{10\times S_1}{S_2}\right) = \log\left(\frac{3600}{\theta}\right) \qquad (۶)$$

سناریو سوم: نقطه دسترسی مجهز به آنتن همه‌جهته و پایانه مجهز به آنتن جهتی است. این سناریو پیچیده‌تر از سناریو ۱ و ۲ است. محدوده امنیتی از شکل یک قطاع ساده خارج می‌شود. محدوده امنیتی را می‌توان با توجه به شکل (۶) به دست آورد.



شکل ۶. نحوه پوشش آنتن‌ها در سناریو سوم

$$S_1 = \pi R^2$$

$$S_{sector} = \pi R^2 \frac{2\alpha}{360} = \pi R^2 \frac{\alpha}{180}$$

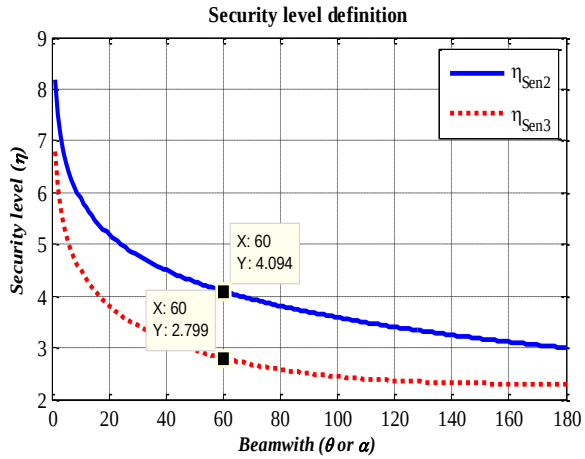
$$S_{triangle} = 2\times\frac{1}{2}\times R\times R\times\sin\left(\frac{360-2\alpha}{2}\right) = R^2\sin(180-\alpha)$$

$$S_2 = S_{triangle} + S_{sector} = R^2\sin(180-\alpha) + \pi R^2\frac{\alpha}{180}$$

سطح امنیتی در سناریوی سوم از طریق رابطه (۷) محاسبه می‌شود [۱۳].

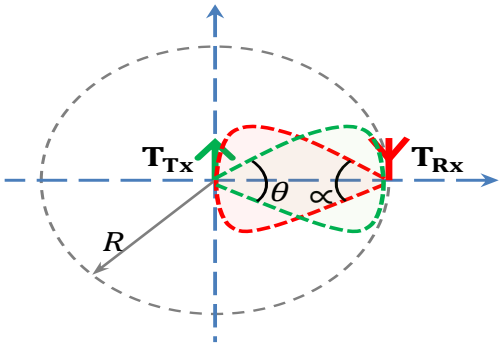
$$\eta = \log\left(\frac{10\times S_1}{S_2}\right) = \log\left(\frac{10\pi}{\sin(180-\alpha)+\pi\alpha/180}\right) \qquad (۷)$$

شکل (۷) نشان‌دهنده نمودار سطح امنیتی رسم شده است.



شکل ۷. نمودار تعیین سطح امنیتی سناریو دوم و سوم

سناریو چهارم: نقطه دسترسی مجهز به آنتن جهتی و پایانه مجهز به آنتن جهتی است (شکل ۸). این سناریو بسیار امن است. در این سناریو، محدوده امنیتی به شکل یک چهارضلعی منتظم خواهد شد.



شکل ۸. نحوه پوشش آنتن‌ها در سناریو چهارم

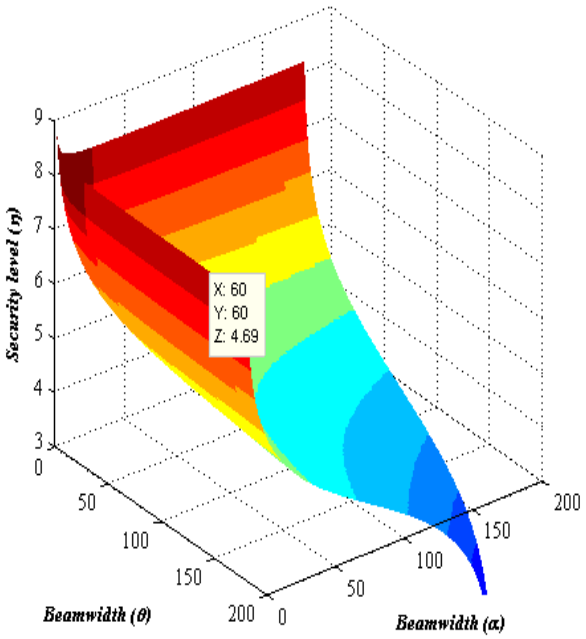
$$S_1 = \pi R^2$$

$$S_2 = \frac{\left(\tan\frac{\theta}{2}\times\tan\frac{\alpha}{2}\right)10R^2}{\left(\tan\frac{\theta}{2}+\tan\frac{\alpha}{2}\right)}$$

در سناریوی چهارم سطح امنیتی از طریق رابطه (۸) محاسبه می‌شود [۱۳].

$$\eta = \log\left(\frac{10\times S_1}{S_2}\right) = \log\left(\frac{\left(\tan\frac{\theta}{2}+\tan\frac{\alpha}{2}\right)10\pi}{\tan\frac{\theta}{2}\times\tan\frac{\alpha}{2}}\right) \qquad (۸)$$

در صورت افـزایش زوایـای θ و α، دو گوشـه چهارضـلعی کـه ناشی از تقاطع امتداد خطوط آن‌هاست، مطابق شکل (۸) در بیرون از دایره خواهد بود. همان طور که قبلاً ذکر شد تمرکز ما بر سـطح داخل دایره است. در این مـورد ابعـاد محـدوده امنیتـی بـه جمـع مساحت دو قطاع و دو مثلث تغییر می‌کند. شکل (۹) بیـانگر خـط سیر سطح امنیتی است.



شکل ۹. تعیین سطح امنیتی سناریو چهارم

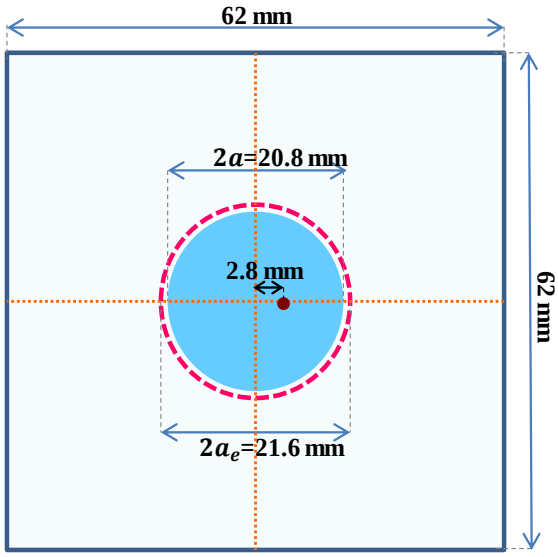
با توجه به نتایج شبیه‌سازی درصورتی‌که هم AP و پایانه هردو مجهز به آنتن هوشمند باشند، لینک ارتباطی برقرارشده از بالاترین سطح امنیتی برخوردار خواهد بود که بـا توجـه بـه سـاختار آنـتن هوشمند پیشنهادی در این مقاله و پهنای بیم ۶۰ درجه این مقدار برابر ۴/۶۹ است.

۷. نتایج شبیه‌سازی و ساخت

در این بخـش نتـایج شـبیه‌سـازی، سـاخت و انـدازه‌گیـری آنـتن هوشمند پیشنهادی آورده شده است.

۷-۱. نتایج شبیه‌سازی و ساخت آنتن پچ

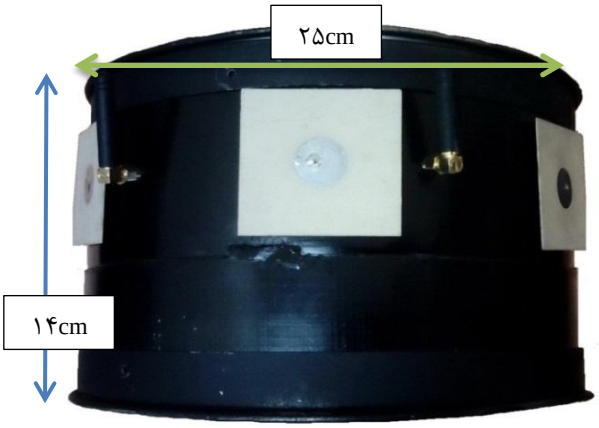
در مراحل شبیه‌سازی با نرم‌افزار CST و ساخت بـه بررسـی تـأثیر ساختار آنتن به تنهایی و بـا وجـود سـاختار کلـی آنـتن هوشـمند (استوانه فلزی) پرداخته شـده اسـت (شـکل‌هـای ۱۳-۱۰). فیبـر به‌کاررفتـه در سـاخت آنـتن پـچ از نـوع Rogers RO4003 اسـت. مشخصات فیبر عبارت‌اند از $\varepsilon = 3.38$ و $h = 0.8mm$.



شکل ۱۰. ابعاد آنتن پچ تک المان در فرکانس مرکزی ۴/۴ GHz

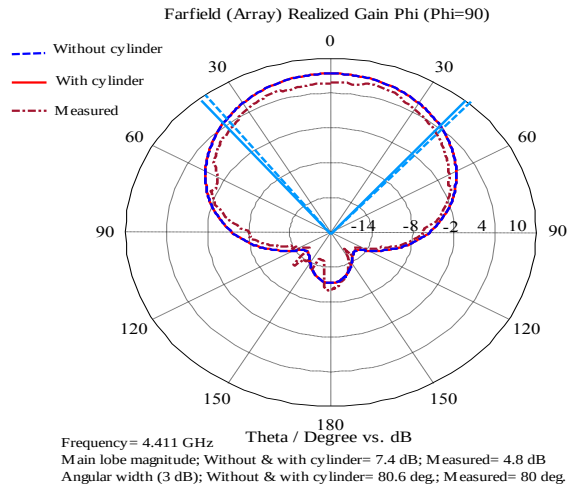
شکل ۱۱. نمای روبه‌رو آنتن پچ ساخته‌شده

شکل ۱۲. نمای وجه کناری آنتن پچ به همراه نحوه اتصال کانکتور

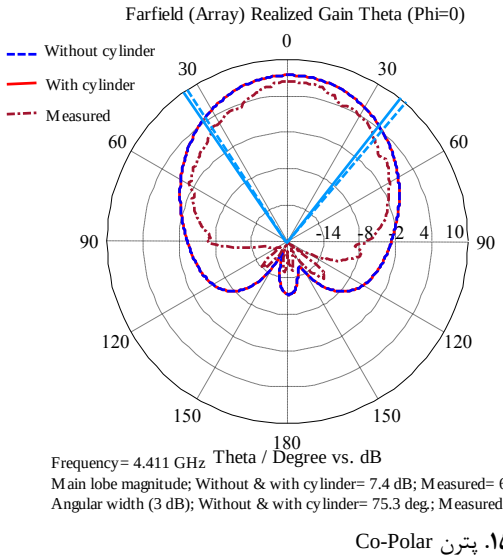


شکل ۱۳. آنتن پچ به همراه ساختار کلی آنتن هوشمند

نمودار پترن آنتن در صفحه H-Plane در شکل (۱۴) و نمودار پترن آنتن در صفحه E-PLANE در شکل (۱۵) آورده شده است.



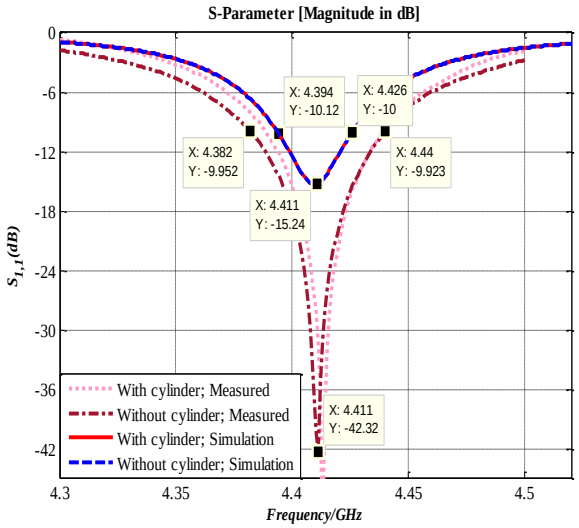
شکل ۱۴. پترن Co-Polar



شکل ۱۵. پترن Co-Polar

پس از شبیه‌سازی و طی مراحل ساخت، S_{11} آنتن‌ها با دستگاه تحلیل‌گر شبکه[1] مدل HP8510C اندازه‌گیری و نتایج آن در شکل (۱۶) آورده شده است. با توجه به شکل (۱۵) می‌توان نتیجه گرفت که انتظار ورود سیگنال مطلوب با سیگنال به نویز مناسب تا زاویه کمینه ۶۰ درجه محقق شده است.

با توجه به شکل‌های (۱۴) تا (۱۶)مشاهده می‌شود که وجود یا عدم وجود ساختار کلی تأثیری در نتایج مربوط به آنتن پچ ندارد و میزان انحراف نمودارهای شبیه‌سازی و ساخت نیز ناشی از خطای ساخت است.



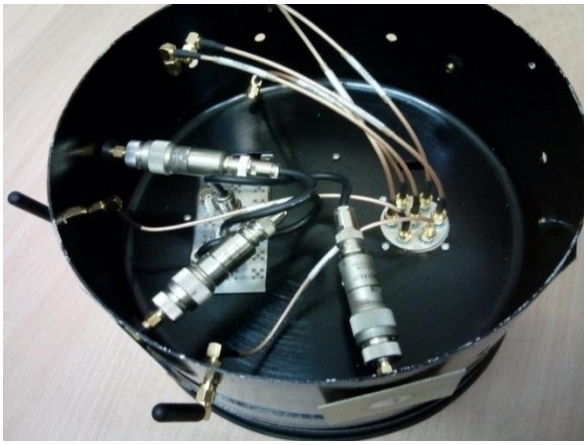
شکل ۱۶. نمودار S_{11} مربوط به آنتن پچ شبیه‌سازی شده در نرم‌افزار CST

۷-۲. نتایج شبیه‌سازی(FEKO) و ساخت آنتن Rubber duck

شکل‌های (۱۷) و (۱۸) به ترتیب نمایی از آنتن Rubber duck به تنهایی و با وجود کل ساختار و همچنین نحوه اتصال آنتن Rubber duck به سوئیچ را نشان می‌دهند.

شکل ۱۷. آنتن Rubber duck به تنهایی

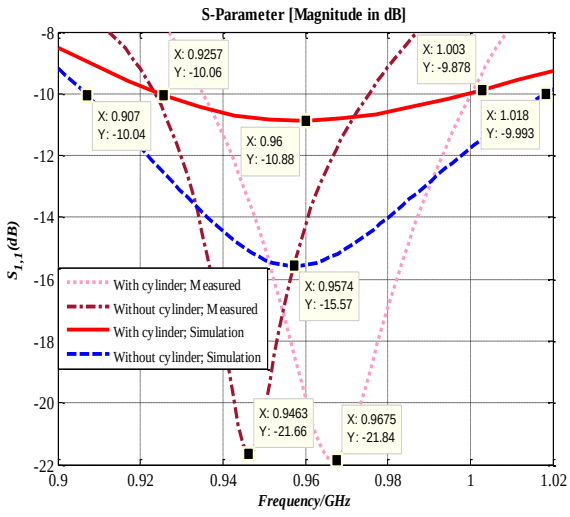
[1] Network Analyzer



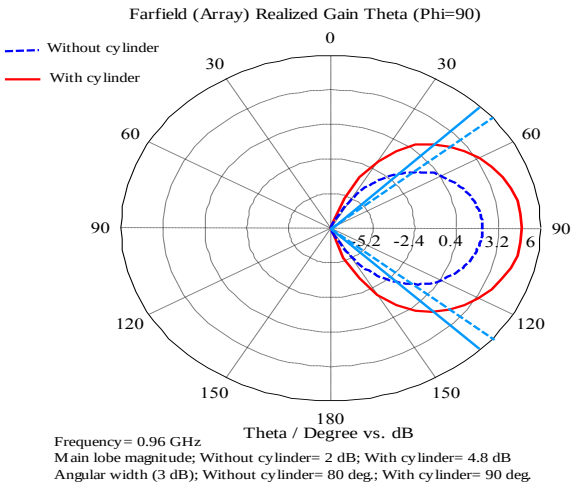
شکل ۱۸. نمایی از جانمایی آنتن Rubber duck به همراه کل ساختار

میزان انحراف نمودار S_{11} مشاهده‌شده در شکل (۱۹) ناشی از تأثیر بدنه فلزی ساختار و همچنین فرکانس کاری به نسبت پایین آنتن Rubber Duck بر میزان موج برگشتی است، ولی چون شکل پترن آنتن هم تحت مصالحه‌ای در این سامانه مورد اهمیت است از این میزان انحراف نیز می‌توان چشم‌پوشی کرد. با توجه به شکل (۲۰) انتظار قبلی وجود استوانه فلزی سبب افزایش گین آنتن در راستای عمودی شده است ولی رفتار پترن تغییر محسوسی نکرده است.

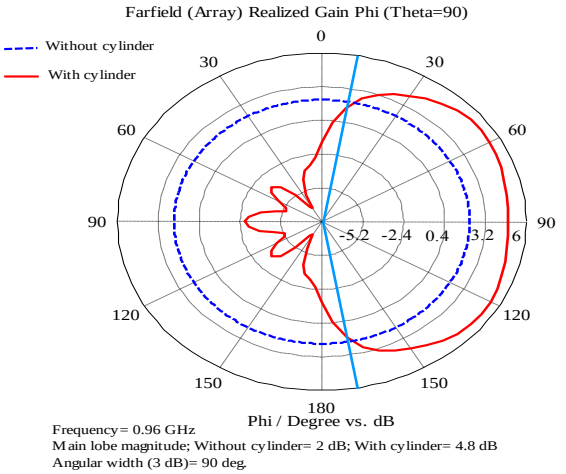
با توجه به شکل (۲۱) می‌توان دریافت که وجود استوانه فلزی ساختار با توجه به انتظار قبلی سبب جهتی کردن پترن آنتن همه‌جهته Rubber Duck شده است و با توجه به پهنای بیم ۹۰ درجه‌ای می‌توان نتیجه گرفت که انتظار ورود سیگنال مطلوب با سیگنال به نویز مناسب تا زاویه کمینه ۶۰ درجه محقق شده است. از جمله مزایای اساسی این روش عدم افزایش ابعاد آنتن اصلی در فرکانس پایین و کمک گرفتن از بدنه فلزی جهت برآورده کردن انتظارات مورد نیاز سامانه است.



شکل ۱۹. S11 آنتن Rubber duck



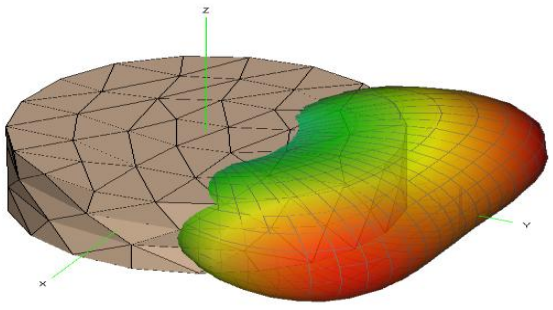
شکل ۲۰. پترن Elevation



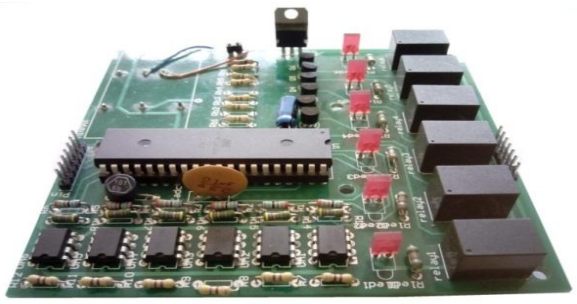
شکل ۲۱. پترن Azimuth

۷-۳. نتایج ساخت مدار کنترلی

پس از شبیه‌سازی عملکرد مدار کنترلی در نرم‌افزار Proteus و انجام مراحل ساخت، در نهایت مدار کنترلی آنتن هوشمند به صورت شکل‌های (۲۲) و (۲۳) جهت جانمایی درون ساختار آنتن هوشمند ساخته شد.



شکل ۲۲. نمای سه‌بعدی پترن آنتن Rubber Duck با در نظر گرفتن ساختار کلی



شکل ۲۳. نمای جلوی مدار کنترلی آنتن هوشمند

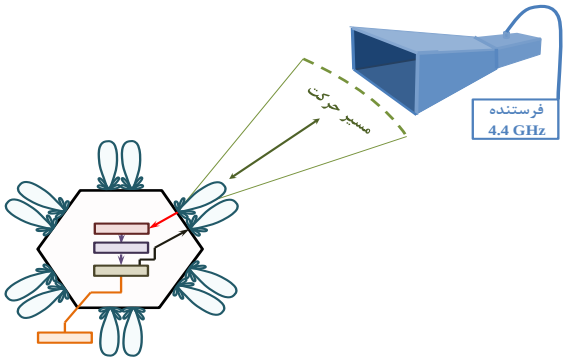
به علت اینکه کانکتور خروجی‌های آشکارساز توان از نوع BNC است، با طراحی و ساخت یک طبقه دیگر بر روی مدار کنترلی، مدار واسطی بین خروجی‌های آشکارساز توان و مدار کنترلی اصلی ایجاد شد که مدار نهایی در برابر فشار و نویز محیطی مقاوم باشد. در شکل (۲۴) نحوه اتصال کانکتورهای BNC به مدار کنترلی اصلی توسط مدار واسط نشان داده شده است.

شکل ۲۴. نحوه اتصال کانکتورها به مدار اصلی توسط مدار طبقه دوم

شکل ۲۵. نمای پایین آنتن هوشمند و نحوه جانمایی مدار کنترلی در آنتن هوشمند

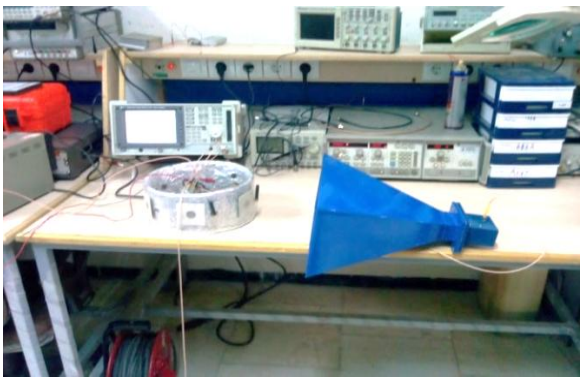
۸. سناریو آزمایش عملکرد آنتن هوشمند پیشنهادی

با توجه به بلوک دیاگرام کلی سامانه، آنتن هوشمند ساخته‌شده مورد ارزیابی و آزمایش قرار گرفت. سناریوی آزمایش در شکل (۲۶) مشخص شده است.



شکل ۲۶. سناریو آزمایش آنتن هوشمند

آنتن مورد استفاده برای آزمایش عملکرد تشخیص قطاع آنتن هوشمند، آنتن هورن است. با چرخش آنتن هورن در مسیر حرکت به دور آنتن هوشمند، به محض اینکه آنتن هورن در زاویه دید هر قطاع قرار گرفت، قطاع مورد نظر انتخاب و در همان زمان سیگنال ۹۰۰ مگاهرتز تولیدشده توسط سیگنال ژنراتور از همان قطاع ارسال می‌شد و به این ترتیب عملکرد تشخیص قطاع مورد ارزیابی قرار گرفت. شکل (۲۷) مراحل انجام آزمایش آزمایشگاهی عملکرد آنتن هوشمند را نشان می‌دهند.



شکل ۲۷. آزمایش عملکرد آنتن هوشمند از نمای روبه‌رو

۹. نتیجه‌گیری

در این مقاله به بررسی میزان افزایش امنیت لینک‌های ارتباطی با وجود سناریوهای مختلف به‌کارگیری آنتن هوشمند پرداخته شده و پس از بررسی و شبیه‌سازی طرح‌های مختلف، آنتن هوشمند پیشنهادی ساخته‌شده و در آزمایشگاه مورد ارزیابی قرار گرفته است. نتایج شبیه‌سازی و ساخت اجزای مختلف سامانه حاکی از برآورده شدن انتظارات از سامانه آنتن هوشمند پیشنهادی است. مقرون به صرفه بودن، حجم کم و وزن پایین کل سامانه می‌تواند از وجوه تمایز آن نسبت به سامانه‌های با عملکرد مشابه باشد. میزان افزایش نرخ امنیتی یک لینک مجهز به آنتن هوشمند پیشنهادی بدون در نظر گرفتن راهکارهای نرم‌افزاری امنیتی کمینه ۴/۶۹ برابر یک لینک مجهز به آنتن همه‌جهته است.

۱۰. مراجع

[1] Jeon, H.; Hwang, D.; Choi, J.; Lee, H.; Ha, J. "Secure Type-Based Multiple Access"; IEEE Trans. Inf. Forensics Secur. 2011, 6, 763–774.

[2] Trappe, W.; Cheng, J. "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks"; IEEE Trans. Parallel Distrib. Syst. 2013, 24, 1, 44–58.

[3] Yajun W.; Tongqing, L.; Chuanan W. "An Anti-Eavesdrop Transmission Scheduling Scheme Based on Maximizing Secrecy Outage Probability in Ad Hoc Networks"; China Commun. 2016, 13, 176–184.

[4] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J. "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks"; IEEE Commun. Lett. 2014, 18, 110–113.

[5] Lakshmanan, S.; Tsao, C.; Sivakumar, R. "Aegis: Physical Space Security for Wireless Networks With Smart Antennas"; IEEE/ACM Trans. Netw. 2010, 18, 1105–1118.

[6] Okamoto, G. T. "Smart Antenna Systems and Wireless Lans"; Kluwer Academic Publication, Santa Clara, 2002.

[7] Kaiser, T.; Bourdoux, A.; Fonollosa, J.; Andersen, J.; Utschick, W.; Boche, H. "Smart Antennas: State of the Art"; Hindawi Publication, New York, 2005.

[8] Williams, W. L.; Anderson, L. A.; Kroening, A. M. "Lightweight Agile Beam Antennas for UAVS Using Advanced Injection-Molded Materials"; Proc. IEEE Antennas and Propagation Int. Symposium, 2007, 21–24.

[9] Ouacha, A.; Gunnarsson, R.; Pattersson, L.; Huss, L. "Wideband Multibeam Antenna for Integration in Small Platforms"; Antennas and Propagation (EuCAP), 2010, 1-5.

[10] Kroening, A. M.; Covert, L. N. "RF Performance of Lightweight Multi Horn Switched Beam Antennas Made of Injection Molded Plastics for Unmanned Systems"; Proc. IEEE Int. Conf. Wireless Inf. Tech. Syst., 2010, 1–4.

[11] Kwaha, B. J.; Inyang, O. N. ; Amalu, P. "The Circular Microstrip Patch Design and Implementation"; Int. J. Res. Reviews Appl. Sci. 2011, 8, 86-95.

[12] Johnson, R. B. "Rubber Ducky Antenna, Invented by Richard B. Johnson, Abominable Firebug Author"; http://www.abominablefirebug.com/rduckey.html, 2016.

[13] Zhaohui, S.; Junwei, L.; Ireland, D. "Increased Security Level Using Space-Division Approach in Wireless Computing Network"; Proc. Asia-Pacific Microwave Conf. (APMC), 2005, 3.