فصلنامه علوم و فنون نظامی/ سال یازدهم/ شماره ۳۲، تابستان ۱۳۹۴
صص ۹۸-۸۱

تاریخ دریافت:۱۳۹۴/۱۱/۰۳
تاریخ پذیرش: ۱۳۹۵/۰۳/۰۹

طراحی و ساخت سیستم ارتباط شناسایی فرکانس‌های رادیویی در مناطق نظامی

اسماعیل صفدریان*[۱]
جعفر خلیل پور[۲]

چکیده:

فناوری شناسایی از طریق امواج رادیویی(RFID)، یک فناوری جدید است که به هدف شناسایی و احراز هویت اشیاء و موجودات زنده به کار گرفته شده و به دلیل مزایای و اهداف گسترده دیگری همچون کاهش هزینه‌ها، افزایش سرعت و انجام احراز هویت در مقیاس وسیع، فناوری RFID مورد توجه سازمان‌ها، صنایع مختلف و به‌خصوص نیروهای نظامی قرارگرفته و روزبه‌روز بر دامنه کاربران آن افزوده می‌شود. ازاین‌رو بررسی جنبه‌های امنیتی این فناوری و میزان امنیت پروتکل‌های به‌کارگیری شده برای انجام احراز هویت، یک نیاز ضروری برای کاربران مختلف آن است. در این مقاله پس از یک آشنایی کوتاه با سامانه‌های RFID، این سامانه‌ها ابتدا مورد تحلیل امنیتی قرار خواهد گرفته و نتیجتاً در جهت افزایش امنیت و بومی کردن سخت‌افزار و نرم‌افزار سیستم‌های ارتباطی، یک مدار RF موجود در سیستم RFID طراحی و ساخته‌شده است.

واژگان کلیدی:

سیستم شناسایی از طریق فرکانس رادیویی (RFID)، شناسایی دوست یا دشمن (IFF)، شنود، مناطق نظامی

۱ - کارشناسی ارشد مخابرات رمز دانشگاه شهید ستاری
۲ - دکتری مخابرات، استادیار دانشگاه هوایی شهید ستاری
* نویسنده مسئول: Email: safdarian@gmail.com

مقدمه

این مقاله به بررسی سیستم‌های RFID[1]، تعیین اعتبار و امنیت در آن و درنهایت طراحی و ساخت سیستم ارتباطی RFID پرداخته است، در این مقاله سعی شده است جدیدترین مطالب در این زمینه جمع‌آوری شود و بهترین راه‌حل‌های ارائه‌شده، شرح داده شود.

امروزه ضرورت شناسایی خودکار عناصر و جمع‌آوری داده مرتبط با آن بدون نیاز به دخالت انسان جهت ورود اطلاعات در بسیاری از عرصه‌های صنعتی، علمی، خدماتی و اجتماعی و بالأخص نظامی احساس می‌شود. در پاسخ به این نیاز تاکنون فناوری‌های متعددی ازجمله کدهای میله‌ای، کارت‌های هوشمند، تشخیص صدا، برخی فناوری‌های بیومتریک و ... طراحی و پیاده‌سازی شده‌اند. در این مقاله نیز محققان به بررسی فناوری RFID پرداخته‌اند. امروزه RFID توسط فروشگاه‌های زنجیره‌ای بزرگی چون "وال‌مارت" و "مک‌دونالد" و نیز سازمان‌های مهمی چون "وزارت دفاع ایالات‌متحده آمریکا" استفاده‌شده و امتحان خود را به‌خوبی پس داده است.(ateriya & Sangeeta Sharma,2011 pp.115-119.) سیستم RFID براساس ذخیره‌سازی دیتا و بازیابی آن عمل کرده و با استفاده از تجهیزات، تگ‌ها و فرستنده‌ها و گیرنده‌های رادیویی یک تگ رادیویی می‌تواند امکان کنترل میسر شده و با الصاق تگ به‌صورت مستقیم به یک محصول، حیوان و یا انسان و یا جاسازی آن در ساختار موارد مذکور (مثل بدن انسان) برای شناسایی، از امواج رادیویی بهره برد.

(Wang Qinghua , Xiong Xiazhong , Tian Wenhao & D. He Liang,2011 pp.58-62)

مباحث نظری

سیستم‌های RFID:

مدار و قطعه برقرار کننده تبادل اطلاعات بین برچسب و خواننده می باشد.یکی از روشهایی که سیستمهای ارتباط برای شناسایی مورد استفاده قرار می گیرد فرکانسهای رادیویی RF می باشد که دامنه ای از نوسانات در بازه ۳ کیلوهرتز تا ۳۰۰ گیگاهرتز می باشد که معادل بسامد موج رادیویی و جریان متناوب حامل سیگنالهای رادیویی هستندبه‌طورکلی RFID یا سیستم شناسایی با استفاده از فرکانس رادیویی، سامانه شناسایی بی‌سیمی است که قادر به تبادل داده‌ها به‌وسیله برقراری اطلاعات بین یک برچسب که به یک کالا، شیء یا ... متصل شده است و یک خواننده می‌باشد.

1.Radio Frequency Identification

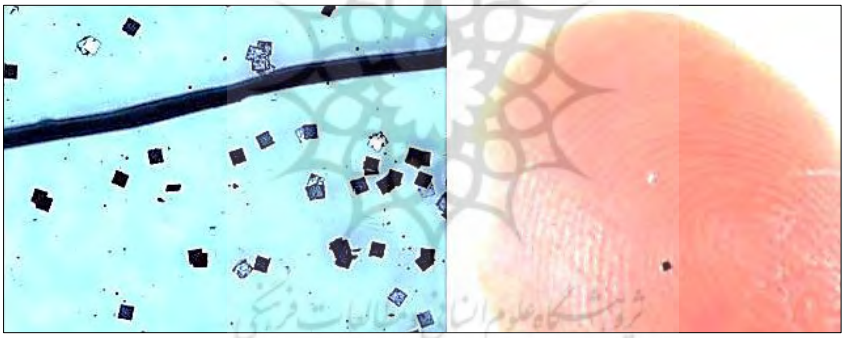
اصولاً سامانه‌های RFID از سیگنال‌های الکتریکی و الکترومغناطیسی برای خواندن و نوشتن داده‌ها بدون تماس بهره‌گیری می‌کنند. برچسب‌ها وسیله شناسایی متصل شده به کالایی است که می‌خواهیم آن را ردیابی کنیم و خواننده‌ها وسایلی هستند که حضور برچسب‌ها را در محیط تشخیص داده و اطلاعات ذخیره‌شده در آن‌ها را بازیابی می‌کنند. با توجه به اینکه این سیستم‌ها بر مبنای تغییرات امواج مغناطیسی و یا فرکانس‌های رادیویی کار می‌کنند، جهت تقویت سیگنال‌های موجود در محیط گاهی اوقات از تقویت‌کننده سیگنال نیز استفاده می‌شود.(A. Jianguo Hu,2010, pp.286-290, 17-19) به طور مثال وقتی نماینده یک یگان وارد یک انبار لجستیکی شده و اقلام موردنیاز خود را تحویل می گیرد، انباردار با استفاده از بارکد می‌بایستی تک‌تک اقلام تحویلی را برداشته و اطلاعات آن را توسط بارکد خوان یکی‌یکی داخل رایانه وارد کند تا قبض انبار اقلام واگذارشده به نماینده صادر گردد. بسیاری از اوقات به دلیل آن‌که تعداد کالاهای تحویل‌شده بسیار زیاد می‌باشند صف‌هایی طولانی مناطق و پایگاه‌ها در انبارها تشکیل می‌شود. گاهی اوقات نیز مخدوش شدن علائم بارکد از خواندن اطلاعات جلوگیری می‌کند که این خود موجب مشکلات بیشتری می‌شود. (A. Cristina Hurjui & B. Adrian Graur,2011, pp.315-320.) با این فناوری جدید یعنی RFID نماینده اجناس خود را برداشته و بدون این‌که مجبور به‌صرف زمان‌های طولانی شود و یا حتی بدون این‌که مجبور باشد اقلام را به انباردار یا نگهبان نشان دهد از درب خارج می‌شود.علت این است که برچسب روی جنس دیگر بارکد نیست بلکه از نوع RFID می‌باشد و خودش با فرستادن علائم رادیویی کلیه اطلاعات جاری خود از قبیل تعداد، کد یا امریه واگذاری، قیمت، وزن، ... را به کامپیوترهای موجود در درب‌های خروجی مخابره می‌کند.این برچسب‌ها دارای دو بخش تراشه و آنتن هستند و دارای عملکرد بسیار ساده‌ای می‌باشند، تراشه اطلاعات را از طریق آنتن منتشر می‌کند و حسگرهایی که در اطراف قرار دارند این اطلاعات را دریافت می‌کنند.

ازجمله مهم‌ترین محاسن آن افزایش سرعت در طی مراحل آمادی سازمان و کنترل آمار کالاهای موجود در انبار بدون نیاز به کمک نیروهای انسانی است. اما تنها اشکال این فناوری گران بودن آن است، اگرچه روزگاری می‌رسد که تمامی اشیاء و کالاها به‌جای بارکد، برچسب خواهند داشت. حتی در زمان جنگ نیز تکنولوژی RFID می‌توان در تصمیم‌گیری‌های صحیح و دقیق به‌کارگیری شود مثل: آخرین وضعیت نیروها، تلفات

جنگی، مهمات، رصد چتربازان، ادوات و ماشین‌آلات جنگی، آذوقه، جستجوی پهبادها، تجسس و... (A. Behzad Malek , B. Ali Miri & C. Luis Orozco-Barbosa,2011, pp.348-352)

امروزه با بهره‌گیری از یک فرایند و تکنولوژی ویژه که پیش‌ازاین در حوزه نظامی و توسط سازمان‌های اطلاعاتی و نظامی امریکا نظیر CIA، NSA و FBI را بکار گرفته‌شده است؛ میکروچیپهای RFID را به حوزه تجاری معرفی شده است. این میکروچیپ‌ها که به نام "غبار قدرت" نام دارد در اندازه میکرو بوده و پیش از این در سرویس‌های نظامی برای نشانگذاری افراد و اشیاء برای تعقیب نامحسوس استفاده می‌شده است. این میکروچیپ با داشتن یک آنتن و حافظه ۱۲۸ بیتی از نوع حافظه رام[1] و در اندازه ۰/۱۵ در ۰/۱۵ می‌باشد. سیگنال‌های ارسالی آن را به‌وسیله MEMS[2] دریافت می‌کنند. این میکروچیپ را در صنعت حمل‌ونقل، حوزه‌های امنیتی، امور تفریحی، رصد نمودن و پشتیبانی می‌توان به کار گرفت. (A. Yan Fang , B. Liu BingWu , C. Huo LingYu & D. Yang Xi,2010, pp.443-445.)

شکل ۱) میکروچیپ RFID



سیستم RFID:

شناسایی دوست یا دشمن (IFF)، همواره هدف جذاب نظامی بوده است. IFF خاص خرابکاری در طول جنگ جهانی دوم منجر به شکست در تمایز بین نیروهای دشمن و نیروهای دوست شد. نیروی هوایی ایالات‌متحده، رمزنگاران ماهری را برای تلاش در جنگ آماده کرد، مثل هورست فایستل، در طول سال‌های ۱۹۴۰ و ۱۹۵۰، سیستم IFF امن که حملات پخش آلمانی را کاهش می‌داد، توسعه داد. عملکرد سیستم این‌گونه بود که بازجویان IFF، سیگنال‌های رادیویی شامل یک چالش تصادفی به هواپیمای ناشناس ارسال

1. ROM: Read Only Memory
2. Micro-Electro-Mechanical Systems

می‌کنند. هواپیمای خودی چالش را رمزنگاری کرده و نتیجه را به بازجو بازگشت می‌دهد، هواپیمای دشمن قادر به پخش پاسخ‌های ضبط‌شده نیستند، زیرا در مواجه بعدی چالش مختلفی به کار می‌رود. پس از سال ۱۹۵۰، نمونه پاسخ چالش دو گذری فایستل مطرح شد و به این صورت بود که در زمان تست پایدار بود و همه انواع برنامه‌های کاربردی عملی و متعدد را در برداشت. این طرح هنوز هم در سیستم‌های امروزی MK XII IFF هواپیماهای خودی را از دشمن تشخیص می‌دهد.

در طول جنگ، هر دو طرف برای مکان‌یابی رادارهای دشمن و دستگاه‌های متراکم تلاش می‌کردند به‌طوری‌که آن‌ها می‌توانستند اقدام تلافی‌جویانه و یا گریز را انجام دهند. در جنگ جهانی دوم هواپیمای متفقین از دستگاه پیش‌بینی رادار استفاده می‌کردند RPD که دارای نقشه‌های برجسته قلمرو دشمن بود و موقعیت رادار مشکوک را نشان می‌داد. RPD ها نقاط ضعف و یا نقاط کور در پرتو رادار دشمن را نشان می‌دادند که به هواپیماهای متفقین برای فرار از تشخیص کمک می‌کرد.

خلبانان بمب‌افکن RAF در جنگ جهانی دوم، راه قوی که هواپیما به‌وسیله پاسخگرهای IFF شان تعیین محل می‌شوند را یاد گرفتند. اما راه‌حل این مشکل ساده بود و متفقین از تعدادی روش‌های دیگر برای محافظت از دستگاه IFF در برابر حملات استفاده کردند. پخش فرکانس طیف گسترده FHSS یک روش ابداعی برای مبارزه با استراق سمع و پارازیت سیگنال بود که در سال ۱۹۴۲ توسط هدی لامار (بازیگر) و جورج آنتیل (آهنگساز) اختراع شد، FHSS روش انتقال سیگنال به‌وسیله سوئیچینگ سریع در میان چندین کانال حاوی فرکانس، با استفاده از یک دنباله شبه تصادفی شناخته‌شده بین هر فرستنده و گیرنده است. علاوه بر این روش، جنگیدن به‌وسیله تهیه کردن پاسخگرهای IFF با یک کد مخفی بود، بنابراین تجهیزات بازجویی IFF به سرقت رفته نمی‌توانست توسط نیروهای دشمن بدون ورود به دوره این کد استفاده شود.

در مقایسه سیستم‌های IFF، RFID مدرن تمایل به تحمیل محدودیت‌های فیزیکی برای مکانیسم‌های امنیتی در برچسب دارد. برای مقابله با این محدودیت‌ها محققان، رمزنگاری فوق‌العاده سبک و راه‌حل‌های رویه‌ای ابداع کردند که به دسته‌بندی‌های مشابه راه‌حل‌های مبتنی بر IFF گروه‌بندی‌شده است. (A. N.W.Lo & B. Kuo-Hui Yeh,2010, pp.566-570.)

محققان نسخه‌های بسیار سبک‌وزنی از کلید متقارن[1] و کلید عمومی رمزنگاری را توسعه داده‌اند. رمزنگاری RFID مخصوص احراز هویت طرح‌های روبه رشد هستند، برخی از آن‌ها مانند تکنولوژی‌های "رمزنگاری مینیمالیستی" و "احراز هویت انسان و کامپیوتر" بسیار سبک‌وزن هستند. دیگر طرح‌های پیچیده آف‌لود[2] در پایگاه داده، شبیه قفل‌های هش و EPCglobal سرورهای تشخیص هویت پیشنهاد می‌شوند. یکی از اولین طرح‌های تأیید هویت RFID خاص که به‌طور گسترده بر اساس کلید متقارن می‌باشد، سیستم کنترل دسترسی درحال‌توسعه برای گذرنامه‌های دیجیتال است. همچنین یک طرح توسعه برای کتابخانه RFID وجود دارد.(A. A.Ahmadpour , B. A.Ahadpour Shal & C. M.Ziabari,2009, pp.808-811.) مصرف‌کنندگان قادر به تشخیص فعالیت RFID دشمن هستند و همچنین می‌توانند مانور گریز خود را ببینند. ردیاب RFID و شخصی‌سازی داده Foe-BUD'S به کاربران در شناسایی نزدیک‌ترین فعالیت RFID کمک می‌کند. دستگاه‌های دیگر مفاهیمی از اسکن‌های RFID را مانند محافظ RFID تفسیر و ثبت می‌کنند. کاربران می‌توانند همچنین بیشتر حیله RFID فعال را به‌وسیله مسدود کردن RFID در هر دو مد توزیع‌شده و یا متمرکز انجام دهند.

همان‌طور که خلبان جنگنده برای فرار از تشخیص، دستگاه IFF خود را غیرفعال می‌کند، مصرف‌کنندگان هم می‌توانند گاهی برچسب‌های RFID خود را برای فرار از مدرن‌ترین تهدیدهای روز غیرفعال کنند. یکی از روش‌های غیرفعال شدن موقت برچسب استفاده از یک جعبه فارادی است، مانند جلد فلزی منحرف‌کننده امواج رادیویی که با گذرنامه‌های دیجیتال صادر خواهد شد. برای غیرفعال‌شدن دائمی برچسب، کارجوت و موسکوویتز برچسب‌های بریده‌بریده ایجاد کردند که می‌توانست به‌طور فیزیکی با پارگی و قطع آنتن برچسب را از کار بیاندازد. محققان همین‌طور مکانیسم‌هایی برای بی‌اثرسازی برچسب آغازین SW ایجاد کردند. با ورود به برچسب‌های EPCglobal نیاز به کلمه عبور است. برچسب‌های EPCglobal با رمزهای حفاظت‌شده همراه است که کارکرد برچسب‌های غیرفعال را برای همیشه از بین می‌برد و برخی از برچسب‌های گران‌تر ممکن است برای تابع خواب/ بیداری محافظت پسورد ارائه دهند که کدام برچسب RFID به‌طور موقت غیرفعال و سپس مجدداً فعال شود.

1. Symmetric-key
2. Off Load

برخی روش‌های دیگر همانند FHSS برای محافظت از دستگاه‌های RFID در برابر حملات وجود دارد. اصلاح دوره‌ای ظاهر شناسه‌های برچسب RFID و یا داده می‌تواند از دسترسی غیرمجاز به برچسب جلوگیری کند. نام‌های مستعار در برچسب‌های RFID شامل یک لیست از نام‌ها هستند که به‌صورت دوره‌ای توسط خوانندگان RFID مطمئن یا با مولد عدد شبه تصادفی بر روی برچسب تازه‌سازی می‌شوند. برچسب داده همچنین به‌صورت دوره‌ای به‌وسیله یک "mixnet" از خوانندگان RFID دوباره رمزگذاری می‌شود.

تجزیه و تحلیل

سیاست‌ها و قوانین امنیتی

گسترش RFID باید در سطح بالای سیاست‌های امنیتی RFID/IT، سیاست‌های امنیتی درون‌سازمانی (یعنی EPC global) و سیاست‌های حریم خصوصی، برای جمع‌آوری داده‌های RFID باشد. همچنین توسعه‌دهندگان متعهدند به‌منظور بالا بردن آگاهی عمومی در مورد خطرات ذاتی ناشی از سیستم‌های RFID شان، به‌واسطه جلوگیری از استثمار به کاربران کمک کنند.

علاوه بر این توسعه‌دهندگانRFID نیاز به کمک انواع دیگر کنترل‌های امنیتی در تکمیل و ارائه به‌وسیله RFID دارند. برای مثال کنترل دسترسی فیزیکی اندازه‌گیری‌های امنیتی بحرانی برای بسیاری از برنامه‌های کاربردی پرمخاطره است، بازرسی تصادفی می‌تواند به تضمین آن‌که برچسب‌های RFID متعلق به اشیاء فیزیکی متناظر با آن‌ها هستند، کمک کند. این روش، به‌سرعت می‌تواند در زمینه حفاظت اشیاء از حمل‌ونقل ظروف گرفته تا داروهای ژنوئولوژی الکترونیکی کمک کند.

حسابرسی دیگر ابزاری است که اپراتور سیستم RFID به‌منظور بررسی سیستم‌های خود می‌تواند استفاده کند. همچنین معماران سیستم RFID باید در تهیه دوره‌های آموزشی جهت آگاهی برای اپراتورهای RFID توجه و رسیدگی داشته باشند و به‌صراحت طرز کار برچسب را در دسترس کاربران قرار دهند. برای نمونه‌های بیشتر در مورد چگونگی ایمن‌سازی سیستم‌های RFID در مؤسسه ملی استاندارد و فناوری (NIST) راهنمای امنیت (NIST SP 800-98) پیش‌بینی‌شده است.

مرتب کردن وضع قانونی امنیت و حریم خصوصی، نیاز مردم در محیط‌های فعال RFID است. به‌طور مثال مردم آمریکا "کدهای رفتاری" غیررسمی را با الهام از منابعی مانند قانون اساسی و ده فرمان ایجاد کرده‌اند. در این موضوع همچنین تلاش‌های رسمی برای ایجاد قانون حریم خصوصی RFID در مکان‌هایی از ایالات‌متحده آمریکا (کالیفرنیا/ مکزیکو/ یوتا/ ماسوچوست)، ژاپن و اتحادیه اروپا شده است. نمونه اخیر این قانون پیشنهادی در اتحادیه اروپا، توسط بدنه مشورتی (گروهی که رایزنی و نظریه را آماده می‌کنند) به‌نام حزب کار حفاظت از اطلاعات، قانون"سند همکاری در مورد مسائل حفاظت از داده‌های مربوط به فناوری RFID" تصویب شد. حتی قانون‌گزارن تأکید می‌کنند که راه‌حل‌های تکنولوژیکی در حمایت از حقوق حریم خصوصی RFID مردم ضروری است. همان‌طور که گفتیم در اتحادیه اروپا "سند همکاری در مورد مسائل حفاظت از داده‌های مربوط به فناوری RFID" دولت موجود است.

راه‌حل دیگر، جلوگیری از نفوذ و تزریق بد افزارها (ویروس‌ها، کرم‌ها و ...) به تجهیزات نرم افزاری و سخت افزاری RFID می‌باشد.(A. R.K.Pateriya & B. Sangeeta Sharma,2011, (pp.115-119

یافته‌های پژوهش

طراحی وساخت سیستم ارتباط RFID:

یکی از روش‌های ایجاد و حفظ امنیت بیشتر در سیستم‌های ارتباطی، بومی‌سازی سخت‌افزار و نرم‌افزار آن سیستم‌ها می‌باشد. در این راستایک شبکه کنترل تردد RFID به‌صورت اکتیو در نیروی دریایی ارتش جمهوری اسلامی ایران اجرا گردیده است.این شبکه در فاز اول بمنظور کنترل تردد افراد (کارکنان، مأمورین، میهمانان و ...)، و در فازهای آتی در شبکه لجستیکی (انبارها، اقلام، خودرو و...) مورد بهره‌برداری قرار گرفته است. به صورتی که با نصب برچسب فعال در قالب یک کارت به اشخاص، اموال و یا تجهیزات و خودرو وثبت کد برچسب در ورودی اولیه، قابلیت جستجو ودنبال کردن هدف مورد نظر بر روی نقشه الکترونیکی وصدور مجوز تردد تنها به گیت‌های موردنظر در ورودی ساختمانها ودرب‌ها فراهم می‌گردد.

بدین صورت که در ورودی هر ساختمان دو آنتن با فاصله نصب بوده و طبق قراردادی زمانی که آنتن اول عبوری را ثبت و سپس آنتن دوم همان عبور را نشان دهد به‌منزله ورود و زمانی که برعکس تردد را احساس کنند خروج محسوب می‌شود. ارتباط بین مدار RF

خواننده و کارت توسط نرم‌افزارهایی بومی در شبکه RFID نداجا به‌طور عملی طراحی و اجرا گردیده است.این مدار RF به‌صورت یک ماژول کوچک بر روی برد اصلی طراحی شده و در صورت معیوب شدن به سهولت قابل تعویض و جایگزینی است.

ارتباط بین آنتن و کارت به‌صورت شبکه Zigbee (که در ادامه توضیح داده می‌شود) در فرکانس کاری 2.45GH و طبق استاندارد 802.11 مربوط به شبکه‌های وایرلس استفاده‌شده است. شبکه مذکور به‌صورت Full mesh و ادهاک بوده ودارای ۱۶ کانال ارتباطی می‌باشد.

کارت با آنتنبه‌صورت LOS[1] و در حالت ارسال همه جهته می‌تواند بین فواصل ۳۰۰ تا ۱۰۰۰ متر (با افزایش توان) ارتباط برقرار کند.

کارت در هر ثانیه ۲ مرتبه ID خود را ارسال می‌کند. خواننده نیز اولین پکت ارسالی از کارت را ذخیره کرده و بقیه را فیلتر می‌کند تا ۱۰ دقیقه، سپس مجدد اگر ID ارسال شد بررسی کرده و در صورت نیاز (مثلاً تغییر موقعیت کارت) دوباره ثبت می‌کند.

سیستم‌های Zigbee:

زیگبی مشخصه‌ای برای مجموعه‌ای از پروتکل‌های ارتباطی سطح بالا بوده که از رادیوهای دیجیتال کوچک و با توان پایین بر مبنای استاندارد IEEE 802_(موسسه مهندسین الکتریسیته و الکترونیک) برای شبکه‌های بخش خصوصی استفاده می‌کند. کاربردهای آن شامل سوییچ‌های الکتریکی بی‌سیم، کنتورهای الکتریکی با صفحه نمایش خانگی، و تجهیزات صنعتی و مصرفی دیگری می‌باشد که نیازمند انتقال داده بی سیم با برد کوتاه در میزان نسبتاً پایین است، می‌باشد. فناوری که توسط خصوصیات زیگبی تعریف می‌گرددبه‌نظر می‌رسد که ساده‌تر و کم هزینه‌تر از WPAN (شبکه‌های بی سیم شخصی) بوده و همانند بلوتوث می‌باشد. هدف زیگبی کاربردهای فرکانس رادیویی (RF)می‌باشد که نیاز به میزان داده‌های پایین، عمر باتری بالاو شبکه بندیامن دارد. زیگبی دارای استاندارد تعریف شده مارک تچ (MarkTech) بوده که متناسب با داده‌های متناوب یا دوره‌ای یا انتقال سیگنال مجزا از یک حسگر یا دستگاه ورودی می‌باشد. سیستم مدیریت ترافیک بر مبنای زیگبی نیز اجرایی می‌باشد. این نام اشاره‌ای به رقص زنبور عسل بعد از برگشت به کندو دارد.

---

[1]. Line of sight

ارتباط یکطرفه و دوطرفه آنتن و کارت

ارتباط آنتن و کارت می‌تواند به‌صورت یک‌طرفه و دوطرفه برقرار باشد. زمانی‌که ارتباط به‌صورت دوطرفه باشد، کارت از آنتن تنظیماتی دریافت می‌کند که شامل (فعال یا غیر فعال کردن، توان ارسالی و...) می‌باشد. در این حالت آنتن می‌تواند کارت خاصی را فراخوان کند و در این حالت LED موجود بر روی کارت چشمک می‌زند.

عیب ارتباط دوطرفه مصرف بیش از حد باتری در کارت می‌باشد. چراکه کارت در حالت گیرندگی توان بیشتری مصرف می‌کند. به‌طور متوسط باتری ظرف دو ماه تخلیه می‌گردد. لذا در این مقاله از ارتباط یکطرفه آنتن و کارت استفاده‌شده است.

محاسبات توان باتری کارت ACTIVE:

با زدن کلید موجود بر روی کارت یک وقفه فعال شده و LED قرمز رنگی روی کارت به مدت ده میلی ثانیه روشن می‌گردد. از این عملیات برای تشخیص سالم بودن باتری، کارت ونیز جهت اطمینان از ارسال شدن ID به آنتن استفاده می‌شود. لازم به ذکر است با هر بار زدن کلید یک مرتبه ID کارت ارسال می‌گردد. تعداد بسته‌هایی که یک کارت با میکروی PIC و فقط با استفاده از انرژی خازن ۲۲۰ میکرو فاراد خود که با ولتاژ ۲ ولت شارژ شده است ارسال می‌کند حدود ۳۰ بسته است که در ۱۵ ثانیه ارسال می‌شوند.

توان مصرفی میکرو از این آزمایش اینطور به‌دست می‌آید:

(1) $\Rightarrow (1/2)CV^2 = (1/2)220_{\mu F} \times 2^2 = 440_{\mu W}$ توان ذخیره‌شده در خازن

که این توان در ۱۵ ثانیه مصرف می‌شود پس:

(2) $440_{\mu W} / 15 \approx 29_{\mu WSec}$

جریان باتری از روی دیتاشیت ۲۲۰ میلی آمپر ساعت می‌باشد که از تبدیل آن به ثانیه به‌دست می‌آید:

(3) $\Rightarrow 220_{\mu A} \times 3600_{Sec} = 792_{ASec}$ توان باتری برحسب جریان ساعت

(4) $\Rightarrow W = VI \Rightarrow 29_{\mu WSec} = 2I \Rightarrow I \approx 15_{\mu ASec}$ توان مصرفی برحسب جریان ساعت

در نهایت:

(5) $\Rightarrow (729/15_{\mu}) = 5280000 \Rightarrow 5280000/(3600 \times 24 \times 365) \approx 1.6_{year}$ برای یک باتری

اگر دو باتری در نظر بگیریم دو برابر می‌شود اما اگر ۳ ولت در نظر بگیریم باز هم ۲ برابر می‌شود:

(6) $1.6 \times 2 \times 2 = 6.4_{year}$

تراشه nRF24L01:

تراشه به کار رفته در این مقاله با نام nRF24L01 محصول شرکت Nordic Semiconductor می‌باشد.

تراشه‌ها دسته بندی متفاوت دارند:

DIP: تراشه‌هایی که دارای پایه‌های باز واز طریق رد شدن از سوراخ برد به آسانی لحیم‌کاری می‌شوند.

So2n: تراشه‌هایی که به‌صورت المان‌های SMD می‌باشند. (2n تعداد پایه‌هامی‌باشد) که به دو دسته تقسیم می‌شوند:

- ✓ Melf: در این تراشه‌ها پایه‌های آن در بغل و یا زیر بدنه تراشه بوده و لذا لحیم کاری آن بسیار سخت و مشکل می‌باشد. بدین صورت که ابتدا با شابلون خمیر لحیم بر روی مدار ریخته شده و با شابلون دیگر که خاصیت چسبندگی دارد تراشه روی خمیر لحیم گذاشته شده حال یا فرو می‌رود و یا به‌صورت آلتراسونیک لحیم کاری انجام می‌شود. در این مقاله از این نوع تراشه استفاده‌شده است.
- ✓ QFP: پایه‌ها در کنار آن و لحیم کاری آن ساده‌تر از Melf انجام می‌گردد.

تراشه nRF24L01 به‌طور پیش فرض در ۱۲۵ کانال قابلیت ارسال و دریافت دارد. که به‌طور خودکار رمزنگاری نیز بر روی آن انجام می‌شود.

تراشه‌ها توسط یک پورت عمومی سریال تحت عنوان SPI[1]به میکروکنترلرها جهت برنامه ریزی متصل می‌شوند. این پورت سریال به‌صورت یک خط رفت، یک خط برگشت و خط کلاک می‌باشد. یعنی با هر کلاک یک بیت رفت و یک بیت برگشت انجام می‌شود.

طراحی PCB[2]مدار

از نرم‌افزار Altium Designer جهت تهیه PCB مدار استفاده‌شده است. در این نرم‌افزار ۴ قسمت زیر انجام می‌شود:

- طراحی فیزیکی (PCB)
- طراحی منطقی (schematic)
- - کتابخانه المان‌های فیزیکی طراحی شده (PCB Lib)

---

1. Serial Peripheral Interface
2. Printed Circuit Board

- - کتابخانه المان‌های نکات کار با نرم‌افزار:

-در این نرم‌افزار بعد از هر تغییرات در طراحی شماتیک برای انتقال به PCB باید از مسیر زیر در منوی ابزار عمل نمود:

Design/Import changes

برای جابجایی قطعات از X و Y در طراحی شماتیک استفاده می‌شود و برای PCB از L برای جابجایی استفاده می‌شود.

برای اتصال در طرح شماتیک باید از Place Net Lable استفاده شود و یا از Place Port در منوی ابزار کمک گرفته شود.

درساخت مدارRF :

- ✓ جهت رفع خاصیت القایی خطوط به‌صورت ۴۵ درجه ترسیم شود.
- ✓ عرض (TRACK) برای Power باید زیاد وبرای فرکانس‌های بالا کم باشد چون فاصله بیشتر، از ایجاد خاصیت القایی جلوگیری می‌کند.
- ✓ می‌توان از کریستال داخلی تراشه استفاده کرد که باعث کاهش هزینه شده و جای کمتری اشغال می‌کند ولی زمان آماده به کار آن بالا رفته و توان نیز بیشتر مصرف می‌شود. لذا در این مقاله از کریستال خارجی به‌صورت SMD و در فرکانس 16GH کار می‌کند.

نرم‌افزار برنامه‌ریزی تراشه

ابتدا در مدار فرستنده گیرنده از تراشه AVR استفاده‌شده بود که به علت مصرف زیاد توان با تراشه PIC جایگزین شد. از نرم‌افزار MPLAB IDE و کمپایلر Hi-Tech جهت تولید برنامه PIC استفاده گردید. همچنین از برنامه PIC Kit2 برای برنامه ریزی تراشه PIC استفاده شد.

IDE[1] محیط ویژوالی برای برنامه نویسی است. در داخل این IDE کمپایلرهای مختلفی پشتیبانی می‌شود که در اینجا شرکت میکروچیپ نرم‌افزار MPLAB را به عنوان IDE جهت محصولاتش ارائه کرده است. به دلیل نداشتن کمپایلر در نرم‌افزار MPLAB از نرم‌افزار Hi-Tech استفاده‌شده است. در نرم‌افزار Hi-Tech برنامه به زبان C نوشته وکمپایل شده و با PIC Kit2 به PIC انتقال می‌یابد.

1. Integrated Development Environment

شرح تابع Main در PIC

مراحل زیر در تابع Main برنامه اصلی در کارت اجرا می‌شود:

-ابتدا میکرو کنترلر خودش را راه‌اندازی می‌کند.

-سپس چیپ را راه‌اندازی می‌کند.

- یک پکت چند خطی به‌صورت یک آرایه راه‌اندازی می‌کند تا وقتی پکت به آنتن ارسال گردید، آنتن از وجود کارت با خبر شود.

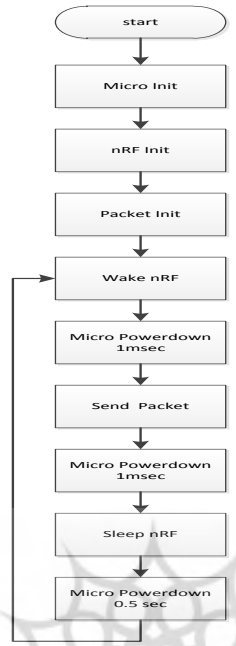
برنامه عملیات بالا به فرم صفحه بعدمی‌باشد:

```
void main(void)
{
//----Initialize
microInit();
RF_TXRX_Init();
RF_TX_Init();
//initiating_timer();
// Disable CE
RC_RF_PORT_CE &= ~RC_RF_PIN_CE;
```

شرح حلقه اصلی برنامه:(While)

- ابتدا میکروکنترولر nRF را بیدار می‌کند. یعنی دستور Wake up را صادر می‌کند.
- حال میکرو به حالت Down Power می‌رود تا چیپ کاملاً Wake up شود.
- میکرو بسته را به تراشه منتقل می‌کند.
- میکرو دستور ارسال را صادر می‌کند.
- میکرو خودش را به حالت Down Power برده تا ارسال چیپ تمام شود.
- پس از ارسال توسط چیپ، میکرو بیدار می‌شود.
- حال میکرو، چیپ را به حالت Down Power می‌برد.
- میکرو نیز به حالت Down Power می‌رود.
- تا فاصله ۱ ثانیه‌ای صبر کرده و دوباره از اول (تکرار حلقه) مراحل تکرار طی می‌شود.
- این روند ادامه دارد تا باتری کارت تمام شود!

فلوچارت عملیات بالا (ارتباط یکطرفه کارت به آنتن) در ادامه آمده است:

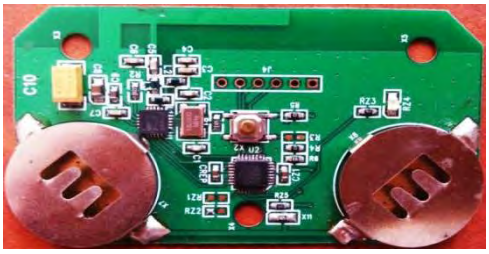


برنامه عملیات صفحه قبل در زیر آمده است:

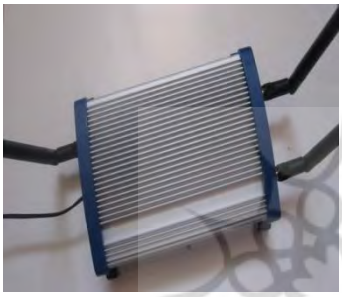
```
while(1)
{
wake_nRF();
WDTCON = 0b000000000;//1msec
SWDTEN = 1;
asm("sleep");
asm("nop");
SWDTEN = 0;
sendCardID(currentLocator);
// Clear IRQ flags in STATUS
//NRF24L01P_CLEAR_IRQ(NRF24L01P_MASK_IRQ_FLAGS);
WDTCON = 0b000000000;//1msec
SWDTEN = 1;
asm("sleep");
asm("nop");
SWDTEN = 0;
sleep_nRF();
WDTCON = 0b000010010;//0.5sec
SWDTEN = 1;
asm("sleep");
asm("nop");
SWDTEN = 0;
```

تصاویر سخت‌افزار پژوهش

شکل ۲) نمایی از مدار کارت اکتیو وپوشش آن



شکل ۳) مدار خواننده به همراه مدارهای RF و Zigbee و تصویر پوشش آن



نتیجه‌گیری

سیستم‌های شناسایی از طریق فرکانس رادیویی امروزه به عنوان جایگزین مناسبی برای سیستم‌های بارکد و دستی، تبدیل به یکی از پرکاربردترین فناوری‌های امنیتی شده است. این سیستم‌ها با وجود کاربرد وسیع در مسائل امنیتی، هنوز نسبت به بسیاری از تهدیدات امنیتی، حملات و مسائل حریم خصوصی آسیب‌پذیر هستند. در این راستا در سال‌های اخیر پروتکل‌های امنیتی مختلفی به منظور برقراری تعادل بین سطح امنیتی موردنیاز و توانایی‌های محاسباتی محدود دستگاه‌های RFID مطرح شده‌اند.

یکی از موارد موردبحث در این سیستم‌ها پروتکل‌های تعیین اعتبار می‌باشند. تاکنون پروتکل‌های بسیاری در زمینه‌ی تعیین اعتبار در سیستم‌های RFID مطرح گشته‌اند، اما هنوز بحث آسیب‌پذیری در آن‌ها مطرح می‌باشد.در این مقاله پس از شناخت سیستم‌های RFID، کاربردها و مشخصات آن، نمونه عملی یک سیستم RFID ارائه گردید. با توجه به به‌کارگیری این سامانه‌ها در سازمان‌های نظامی و اهمیت امنیت آن، بومی بودن سخت افزار و نرم افزارهای سیستمهای ارتباطی از اولویت‌ها و مهمترین روش در ارتقاء امنیت، تعیین اعتبار وکاهش آسیب پذیری ونفوذ می باشدکه در این مقاله سعی بر تحقق این امر بوده

است.از سوی دیگر با بومی سازی سیستمهای یاد شده گامهای موثری در پیشبرد اهداف عالیه‌ای همچون حمایت از تولید داخل، اصلاح الگوی مصرف و صرفه جویی منابع ارزی و انسانی، اقتصاد مقاومتی و در نهایت خودکفایی عینی، خواهد بود.

جدول شماره۱) کلید واژه علائم و اختصارات پژوهش

Abbreviation	English	معادل فارسی
CIA	Central Intelligence Agency	آژانس اطلاعات مرکزی آمریکا
C'T	Creative Talent Magazine	مجله خلاقیت واستعداد
DIP	dual in-line package	تراشه دو جهته
EPC	Electronic Product Code	تولید کننده تگ وکد الکترونیکی
FBI	Federal Bureau of Investigation	اداره پلیس فدرال آمریکا
FHSS	Frequency Hopping Spread Spectrum	سیستم طیف گسترده پرش فرکانسی
ID	Identification	شناسه
IDE	Integrated Development Environment	محیط ویژوالی برنامه نویسی
IEEE	Institute of Electrical and Electronics Engineers	مؤسسه مهندسان برق و الکترونیک
IFF	Identification Friend or Foe	سامانه تشخیص دوست از دشمن
LED	Light-Emitting Diode	دیود نورافشان
MELF	Metal Electrode Leadless Face	قطعات استوانه ای بدون پایه فلزی
MEMS	Micro-Electro-Mechanical Systems	سامانه میکرو الکترومکانیکی
Mix Net	Mix Network	شبکه مختلط
NIST	National Institute of Standards and Technology	موسسه ملی استاندارد و فناوری
NSA	National Security Agency	آژانس امنیت ملی ایالات متحده آمریکا
PCB	Printed Circuit Board	برد مدار چاپی الکترونیکی
PIC	Programmable Interface Controllers	کنترل کننده های ارتباطی برنامه پذیر
QFP	Quad Flat Package	تراشه چهار سطحی
RAF	Royal Air Force	نیروی هوایی سلطنتی
RF	Radio Frequency	فرکانس رادیویی
RFID	Radio Frequency Identification	سامانه شناسایی امواج رادیویی
RPD	Radar Probability of Detection	دستگاه پیش‌بینی رادار
SMD	surface-mount device	قطعات نصب شده روی سطح
SPI	Serial Peripheral Interface	گذرگاه ارتباط جانبی سریال
WPAN	wireless personal area network	شبکه شخصی بی‌سیم

منابع

- Jianguo Hu and B. Deming Wang and C. Yanyu Ding and D. Jun Zhang and E. Hongzhou Tan,(2010) Design and Implementation of Intelligent RFID Security Authentication System, IEEE International Conference on RFID-Technology and Applications, Guangzhou, China, pp.286-290, 17-19 June.

- R.K.Pateriya and B. Sangeeta Sharma, (2011) The Evolution of RFID Security and Privacy: A Research Survey, IEEE International Conference on Communication Systems and Network Technologies, pp.115-119,.
- Jack Yu and B. Gul Khan and C. Fei Yuan,(2011) XTEA ENCRYPTION BASED NOVEL SECURITY PROTOCOL, IEEE Electrical and Computer Engineering, , Canada.
- Wang Qinghua and B. Xiong Xiazhong and C. Tian Wenhao and D. He Liang,(2011) Low-cost RFID: Security problems and solutions, IEEE, pp.58-62.
- Cristina Hurjui and B. Adrian Graur(2011) Analysis of RFID security and privacy by means of identification and authentication protocols, IEEE, pp.315-320,.
- Behzad Malek and B. Ali Miri and C. Luis Orozco-Barbosa(2011) Backward Link Authentication For RFID Tags, IEEE International Conference on FID-Technologies and Applications, pp.348-352,.
- A. Yan Fang and B. Liu BingWu and C. Huo LingYu and D. Yang Xi(2010) Research and Design of a security Framework For RFID system, IEEE International Forum on Information and Applications, pp.443-445,.
- A. N.W.Lo and B. Kuo-Hui Yeh(2010)De-synchronization Attack on RFID Authentication Protocols, IEEE, pp.566-570, Octobr 17-20,.
- A. A.Ahmadpour and B. A.Ahadpour Shal and C. M.Ziabari(2009) A Novel formulation of Hamming Code, IEEE, pp.808-811,.
- A. Hyun-Seok Kim and B. Jung-Hyun oh and C. Jin-Young Choi, Analysis of the RFID Security Protocol for Secure Smart Home Network, IEEE International Conference on Hybrid Information Technology, vol. 2, pp.356-363, 2006.
- A. Chunuhui Piao and B. Zhenjiang Fan and C. Chunyan Yang and D. Xufang Han, (2010)Research on RFID Security Protocol Based On Grouped Tags and Re-encryption Scheme, IEEE, pp.568-572,.
- A.Syeda Iffat Naqvi and B. Adeel Akram(2011) Pesudo-random Key Generation for Secure HMAC-MD5, IEEE, pp.573-577.
- A.Zhao Li Ping and B. Shu Qi Liang and C.Lai Xiao Liang(2011) RSA Encryption and Digital Signature, IEEE International Conference on Computational and Information Sciences, pp.369-372.
- Ohkubo, M., Suzuki, K., Kinoshita, S.(2003) "A cryptographic approach to a ‘privacy-friendly’ tag", RFID PrivacyWorkshop, MIT.
- Piramuthu, S.(2007)"Protocols for RFID tag/reader authentication", Decision Support System, University of Florida,.
- Yang, J., Park, J., Lee, H., Ren, K., Kim, K.(2005) "Mutual authentication Protocol for low-cost RFID", Proceedings of the Workshop on RFID and Light Weight Cryptography.

- Piramuthu, S(2010)"RFID mutual authentication Protocols", Decision Support System, University of Florida.
- Weis,S. A., Sarma, S. E., Rivest, R., Engels, D. W.(2004) "Security and Privacy aspects of low-cost radio frequency identification systems", 1st Security in pervasive computing LNCS,.
- Lee, S., Asano, T., Kim, K.(2006) "RFID Mutual Authentication Scheme based on Synchronized Secret Information", Symposium on Cryptography and Information Security, Hiroshima, Japan.
- Luo, Z., Chan, T., Li, J.S.(2005) "A light weight mutual authentication protocol for RFID networks", Proceedings ofthe IEEE International Conference on e-Business Engineering,.
- Piramuthu, S.(2010) "RFID mutual authentication Protocols", Decision Support System, University of Florida.
- Piramuthu, S.(2010) "RFID mutual authentication Protocols", Decision Support System, University of Florida.
- Lee, S., Asano, T., Kim, K.(2006) "RFID Mutual Authentication Scheme based on Synchronized Secret Information", Symposium on Cryptography and Information Security, Hiroshima, Japan,.
- Piramuthu, S.(2007) "Protocols for RFID tag/reader authentication", Decision Support System, University of Florid.,
- Yang, J., Park, J., Lee, H., Ren, K., Kim, K.(2005) "Mutual authentication Protocol for low-cost RFID", Proceedings of the Workshop on RFID and Light Weight Cryptography.
- Han, S., Potgar, V., Chang, E.(2007) "Mutual authentication protocol for RFID tags based on Synchronized secret information with monitor", Proceedings of ICCSA, LNCS.
- Piramuthu, S.(2010) "RFID mutual authentication Protocols", Decision Support System, University of Florida,.
- Deursen, T. V., Radomirovic, S.(2009) "Security of RFID Protocols-A case study", Electronic Notes in Theoretical Computer Science.
- Pietro, R.D., Molva, R.(2010) "An optimal probabilistic solution for information confinement, privacy, and security in RFID systems", Journal of Network and Computer Applications.
- S. Garfinkel, and B (2005)Rosenberg, "RFID: Applications, Security, and Privacy", 1st edition, Addison-Wesley Professional.
- M. Nilsson, J. Hallberg(2002) "Positioning with Bluetooth, IrDA and RFID", Master's Thesis of Luleå University of Technology, Sweden.
- T. Haver(2006)"Security and Privacy in RFID Applications", Master's Thesis of Norwegian University of Science and Technology, Norway