

**بررسی کلاسهای متفاوت پروتکل های تصدیق RFID**

**چکیده:**

**سامانه بازشناسی با امواج رادیویی** (RFID) تکنولوژی به روز و در حال پیشرفتی است. محدودیت های اصلی تکنولوژی RFID موارد امنیتی و حریم شخصی هستند. بسیاری از روش ها، از جمله رمزنگاری، تصدیق و تکنیکهای سخت افزاری، برای گذر از مشکلات امنیتی و حریم شخصی ارائه شده اند. این مقاله روی پروتکلهای تصدیق یا تایید متمرکز شده است. ترکیب محبوبیت تکنولوژِی RFID و نا امن بودن آن منجر به سیل پروتکلهای مشترک تصدیق شده است. پروتکلهای تصدیق به عنوان کامل، ساده، سبک و فوق سبک طبقه بندی می شوند. از سال 2002 تا به الان، تحقیقات مهمی انجام شده و پروتکلهای بسیاری نیز عرضه شده اند که برخی از این پروتکلها نیاز به ارتقا دارند. مقاله پیش رو پروتکلهای تصدیق مشترک RFID اخیرا ارائه شده را طبق کلاس تصدیق آن با جزئیات کامل بررسی می نماید. پروتکلهای که اکثرا بر اساس امنیت، تکنیک مقایسه شده اند مبتنی بر پروتکل هایی هستند که پروتکلهای ارائه شده با آنها و در نهایت، روش های تایید پروتکلها با یکدیگر مقایسه شده اند. نکات مهم این مقایسه در دو جدول تجمیع شده اند.

**کلمات کلیدی:** پروتکلهای تصدیق، **سامانه بازشناسی با امواج رادیویی ،** حمله های شناسایی فرکانس هایرادیویی، پروتکلهای تاییده شده **سامانه بازشناسی با امواج رادیویی**

**مقدمه:**

**سامانه بازشناسی با امواج رادیویی** **(RFID)**

برای شناسایی اشیا با برچسبی کوچک در حال ایجاد است. این تکنولوژی به عنوان یکی از ضروری ترین تکنولوژی های این چند دهه قلمداد می شود[[1]](#footnote-1). سیستمهای RFID از یک برچسب، یک برچسب خوان و یک سرور دیتابیس پشت خط تشکیل شده است. برچسب خوان شناساگر های نشگانگر های RFID را خوانده و هویت جستجو ها را برای سرور پشت خط می فرستند. اطلاعات بدست آمده از برچسب ورودی به پایگاه داده پشت خط خواهد بود.

برچسب ها در سه طبقه بسته به نوع تغذیه آنها دسته بندی میشوند: برچسب های فعال، نیمه فعال و غیر فعال. برچسب های RFID فعال نیازمند یک باتری داخلی برای تغذیه اجزای الکترونیکی خود و تولید سیگنال برای برچسب خوان هستند. برچسب های نیمه فعال و یا به عبارتی نیمه غیر فعال تنها از قدرت باتری برای روشن کردن مدار میکروچیپ استفاده می کنند و انرژی ساخت سیگنال پاسخ برای برچسب خوان را از سیگنال رادیویی برچسب خوان بدست می اورند. برچسب های غیر فعال تمام انرژی خود را از برچسب خوان بدست می آورند. علاوه بر این برچسب های RFID در سه بازه فرکانسی دسته بندی می شوند: فرکانس ضعیف(125-134KHz) فرکانس بالا(13.56KHz) و فرکانس فوق بالا(860-960KHz)]2[. برچسب های غیر فعال RFID (کم هزینه) که با پهنا های فرکانس فوق بالا کار می کنند امکان نو آوری را در حوزه های کاربرد روزانه، مثل ساخت اکسس کنترل، مدیریت زنجیره تجهیزات و موقعیت یابی کالا ها فراهم کرده اند. استاندارد کد الکترونیکی کالا(EPC) کلاس 1 (C1) نسل دوم(Gen2) مثالی از تکنولوژی های غیر فعال RFID است]3[.

برخی متخصصین بر این باورند که بارکد های دیداری با برچسب های RFID ارزان قیمت متصل به کالاهای مورد مصرف جایگزین می شوند]4[. با این حال، به خاطر طبیعت رابطه بی سیم بین برچسب و برچسب خوان، این تکنولوژی تهدیدات بزرگی در زمینه امنیت و حریم شخصی دارد. پروتکل های تایید شده مشترک معمولا برای غلبه به حمله های امنیتی بین برچسب و برچسب خوان استفاده می شوند. از سال 2002 تحقیقات بسیاری انجام شده و پروتکلهای بی شماری ارائه شده اند اما برخی از آنها همچنان نیاز به ارتقا دارند.

در بخش هایی که در ادامه خواهیم خواند بخش 2 در مورد پروتکل های تایید شده و اهدف آنها بحث و توضیح خواهد داد. بخش 3 پروتکل ها را با توجه به طبقه خود بررسی و مقایسه می کند. بخش 4 مقایسه را ارزیابی می کند. بخش 5 نتایج حاصل از بررسی پروتکل های احراز هویت را ارائه می دهد.

**2. پروتکل های تأیید شده**

لوپز و همکاران [5] راه حل های بسیاری برای غلبه بر مسائل امنیتی و خطرات مرتبط با سیستم های RFID را معرفی کردند.

در این مطالعه، ما قصد داریم تا پروتکل های تأیید شده را عمیق تر کنیم. تأییدیه اولین قدم در دفاع در مقابل حملات بی سیم به سیستم های RFID می باشد. هنگامی که سرور هویت برچسب RFID را تأیید می کند، اعتماد به برچسب آغاز می شود.

پس از تاییده، خواننده می تواند به محتویات برچسب های تأیید شده دسترسی پیدا کند.

**2.1 دسته های (کلاس های) پروتکل های تأیید شده**

چین [6] اظهار داشت که پروتکل های تاییدی به چهار دسته با توجه به هزینه محاسبات برچسب و عملیات پشتیبانی شده تقسیم می شوند.

•پروتکل های کاملا پیشرفته: پروتکل هایی که از رمزگذاری متقارن و نامتقارن و تابع یک طرفه پشتیبانی می کند. مثالها در [7، 8] هستند.

•پروتکل های ساده: پروتکل هایی که از تابع هش و مولد عدد تصادفی پشتیبانی می کند (RNG). نمونه هایی از این دسته در [9، 10] ارائه شده است.

• پروتکل های سبک: پروتکل هایی که از بررسی افزونگی چرخه ای (CRC) و RNG پشتیبانی می کند. مثالها در [11-14] ارائه شده است.

• پروتکل فوق العاده سبک: پروتکل هایی که به ویژه برای دستگاه های بسیار محدود طراحی شده اند. اینها پروتکل ها فقط شامل عملیات ساده بیتی (مانند AND، OR، XOR) در برچسب ها می باشند. مثالها در [15، 16] داده شده است.

**2.2 اهداف پروتکل های تأییدشده**

با توجه به انواع تهدیدات بالقوه، یک پروتکل تاییدی، در هر دسته ای، باید همه یا بیشتر تهدیدها و خدمات امنیتی زیر را بررسی کند.

**تهدیدات امنیتی**

• ردیابی حمله: مهاجم می تواند اطلاعات مرتبط با یک برچسب مشخص شده را ردیابی کند.  
• حمله عدم سرویس دهی (DoS): آن تلاشی برای تخریب تگ ها با داشتن خوانندگان مخرب که آنها را با اطلاعات بیشتر بجای کنترل آنها بارگذاری می کند.

• حمله غیرهمگامی: مهاجم خواننده و تگ را غیرهمگام می کند.

• حمله مرد میانی: این کنترل جریان پیام را می گیرد.

• حمله جعل هویت: مهاجم یک برچسب معتبر را جعل میکند و به عنوان یک برچسب معتبر عمل می کند.  
• حمله کلونینگ: مهاجم اعتقاد خواننده را فریب می دهد که داده ها را از برچسب قانونی دریافت می کند.  
• حمله افشاء کامل: مهاجم تمام اطلاعات مخفی تگ را به خطر می اندازد.

• استراق سمع: مهاجم در کانال های ارتباطاتی استراق سمع می کند.

• حمله بازپخش: مأمور یا مهاجم، احتمالا به عنوان بخشی از حمله تظاهرگونه توسط جایگزینی بسته، اطلاعات را قطع و دوباره انتقال می دهد.

**خدمات امنیتی**

• تایید متقابل: ویژگی که هر دو برچسب و سرور به یکدیگر اعتبار می دهند.

• محرمانه بودن: املاک که تمام اطلاعات مخفی به طور ایمن منتقل می شود.

• در دسترس بودن: ویژگی که طرفین مورد تایید همیشه برای برقراری ارتباط در دسترس است.  
• امنیت جلو / عقب: ویژگی که مهاجم نمی تواند اطلاعات محرمانه قبلی / فعلی را به خطر بیاندازد حتی اگر اطلاعات محرمانه فعلی / قبلی را به دست آورد.

• مالکیت قابل انتقال: ویژگی که حریم خصوصی صاحبان فعلی و جدید نقض نمی شود زمانی که صاحب فعلی داده های لازم را به صاحب جدید منتقل می کند.

• ناشناس بودن برچسب: ویژگی که مهاجم نمیتواند از طریق گوش دادن به کانال، یک برچسب را پیدا کند.  
• قابل ردیابی: صاحب برچسب می تواند با استفاده از اطلاعات حریم خصوصی محل ذخیره شده در برچسب شناسایی شود.

• مکان خصوصی محل: ویژگی که مهاجم نمی تواند در مورد شیء ردیابی از اطلاعات یک برچسب قضاوت کند.  
• حریم خصوصی اطلاعات: ویژگی که تنها خواننده قانونی می تواند به اطلاعات ذخیره شده در برچسب دسترسی داشته باشد.

**3. بررسی و مقایسه پروتکل های تأییدی**

بر خلاف مطالعه و بررسی سو [17] که در آن پروتکل ها با توجه به خدمات ارائه شده و الگوریتم های استفاده شده طبقه بندی شده اند، این بخش، 22 پروتکل تایید شده پیشنهادی اخیرا RFID را با توجه به کلاس خود معرفی می کند؛ برخی از پروتکل ها به طور دقیق مورد بررسی و توضیح قرار می گیرند در حالی که سایر پروتوکل ها در جداول به دلیل فضای محدود ارائه شده اند

ستون اول جدول 1 ، 22 پروتکل را بر اساس کلاس خود فهرست می کند که از تمام پیشرفته شروع می شود و به پروتکل فوق العاده سبک ختم می شود. ستون دوم تابعی را ارائه می دهد كه پروتكل بر آن مبتنی است. ستون سوم ابزار تأییدیه مورد استفاده برای تصدیق را ارائه می دهد.

جدول1: تکنیکها، تایید و دسته ها پروتوکل تاییدی (پروتوکل، C دسته، F کاملا پیشرفته، S ساده، L سبک، وزن فوق العاده سبک UL )

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P | **تابع مبتنی بر** | **تایید شده توسط** | EPC | **مقایسه با** | **C** |
| [31] | ECC | **…..** | X | [27, 28, 30] | F |
| [37] | رمزنگاری کلید عمومی | منطق BAN | X | [38-42] | F |
| [32] | ECC | مدل پیشگو تصادفی | X | 25]، 28، 30، [43 | F |
| [33] | ECC & AES | تست و تحقق آن در دستگاه ها واقعی | X | [25, 28–30] | F |
| [44] | افزایش فضای کلیدی با استفاده از نانس ها | AVISPA | X | [45–47] | F |
| [48] | برچسب های NFC حمایت شده از نظر رمزنویسی در داروها | به صورت دستی در [49] | X | [49] | F |
| [50] | تابع هش یک طرفه و رمزگذاری نیمه تصادفی کلیدها | به صورت دستی در [51] | X | [9, 10, 36, 51, 52] | F |
| [53] | مبتنی بر هش | **.........** | X | [36, 51, 54] | S |
| [55] | مبتنی بر هش | **بصورت دستی** | X | [6, 56–61] | S |
| [62] | مبتنی بر هش و PRNG | منطق GNY[63] | √ | [64-66] | S |
| [67] | پیچیدگی زمان ثابت | **مدل رقابتی** بیزانتینی[52] | X | [68] | S |
| [69] | عملیات هش و RNG | منطق GNY[63] | X | [10, 70–75] | S |
| [76] | تابع هش یک طرفه | منطق GNY[63] | X | [10, 77, 78] | S |
| [79] | مبتنی بر XOR ، PRNG و CRC | بصورت دستی | √ | [42, 80] | L |
| [81 | مبتنی بر XOR ، PRNG | بصورت دستی همانند [82] | √ | [83–86] | L |
| [87] | شاخص برچسب سریع، PRNG و CRC | برنامه شبیه سازی شده | √ | [10, 73, 77, 88–91] | L |
| [92] | یادگیری یکسان با نویز | بصورت دستی همانند[93] | √ | [93–96] | L |
| [97] | یک ژنراتور شبه تصادفی بین خوانندگان و برچسب ها به اشتراک گذاشته شد | AVISPA | √ | [98-103] | L |
| [104] | **جایگزینی و** CRC | **مفسر ساده پروملا**(SPIN) | √ | [6, 38, 56, 105] | L |
| [106] | تبدیل یک بیتی فوق العاده سبک | به صورت دستی | √ | [6, 38, 57, 58, 64, 105, 107] | UL |
| [108] | **مبتنی بر چرخش بیتی XOR** | به صورت دستی | √ | [6, 38, 56–58, 105] | UL |
| [109] | توابع غیرقابل پنهان فیزیکی | **…….** PUF | √ | [110–112] | UL |

ستون EPC فهرست می کند که آیا پروتکل سازگار با EPC Gen2 است یا خیر. ستون "در مقایسه با" پروتکل های دیگر را فهرست می کند که پروتکل با آن مقایسه شده است. آخرین ستون دسته پروتکل تاییدی را ارائه می دهد. مقایسه پروتکل ها بر اساس تهدیدات امنیتی و خدمات امنیتی در جدول 2 ارائه شده است در حالی که جدول 3 نام های مقاله مورد بررسی و سال انتشار را همراه با منابع خود ارائه می دهد.

**3-1- پروتکل­های کاملا پیشرفته**

دسته کاملا تکامل­یافته (پیشرفته) [ی پروتکل­ها] شامل الگوریتم­های رمزنگاری است که عمدتا به دو گروه الگوریتم­های متقارن و نامتقارن تقسیم می­شوند. الگوریتم­های نامتقارن مبتنی بر رمزنگاری منحنی بیضی­شکل (ECC)، از جهت سرویس­ها و میزان امنیتی که ارائه می­کنند، قوی به حساب می­آیند. در مقایسه با سیستم شیوه‌ای رمزنگاری به روش کلید عمومی (RSA)، سیستم­های بر پایه­ی ECC، کوچکتر (کم حجم­تر)، سریع­تر و با مصرف انرژی پایین­تری هستند. از این رو برای سیستم­های با محدودیت منابع، الگوریتم­های مبتنی بر ECC انتخاب بهتری نسبت به الگوریتم RSA هستند. اشاره شده است که سیستم RSA، یک متغیّر مبتنی بر ECC دارد. به همین جهت بسیاری از پروتکل­های تاییده شده بر پایه­ی ECC، برای اجرای تگ­هایی یا برچسب هایی (کدهای برنامه­نویسی) دارای محدودیت شدید ارائه شده­اند.

در سال 2006، تویلز و همکاران با استفاده از پروتکل شناسایی Schnorr، یک پروتکل شناسایی RFID برپایه­ی ECC را ارائه کردند. آنها ادعا کردند که این پروتکل، در مقابل جعل­سازی تگ مقاوم است. با این حال در سال 2008، لی و همکاران نشان دادند که پروتکل تویلز و همکاران، در برابر ردیابی موقعیت مکانی بی­دفاع است، تایید متقابل و امنیت پیشرو را تضمین نمی­کند و در مقیاس­پذیری با نقصان روبه­رو است. در سال 2007، باتینا و همکاران، بر مبنای پروتکل احراز هویت اوکاماتو، یک پروتکل شناسایی RFID برپایه­ی ECC را ارائه و اشاره کردند که طرح پیشنهادی آنان (پروتکل ارائه شده­ی آنان) می­تواند در مقابل حملات فعال ایمن باشد. با این حال لی و همکاران اظهار داشتند که این پروتکل از منظر حمله­ی ردیابی موقعیت مکانی و امینت پیشرو آسیب­پذیر است و همچنین فاقد مقیاس­پذیری است. لی و همکاران ادعا کردند که سه مشکل یادشده را مرتفع ساخته­اند، اما مطالعات منتشرشده در سال 2008 نشان داد که طرح پیشنهادی لی و همکاران، در برابر حملات جعل اطلاعات و ردیابی بی­دفاع است و احراز تایید متقابل را نیز تأمین نمی­کند.

جدول2. مقایسه پروتکل های تایید از منظر تهدیدهای امنیتی و خدمات امنیتی (F تمام و کمال، S ساده، L خفیف، UL بسیار خفیف)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| پروتکل | 31 | 37 | 32 | 33 | 44 | 48 | 50 | 53 | 55 | 62 | 67 | 69 | 76 | 79 | 81 | 87 | 92 | 97 | 104 | 106 | 108 | 109 |
| تهدیدات امنیتی |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ردیابی حمله |  |  |  | √ |  |  | √ |  | √ |  | √ | √ |  | √ |  |  |  |  | √ | √ |  |  |
| DoS | √ | √ |  | √ | √ | √ | √ |  |  |  |  |  | √ | √ |  |  | √ |  | √ |  |  | √ |
| همگامسازی | √ | √ |  | √ | √ | √ | √ | √ | √ |  | √ | √ |  |  | √ | √ | √ |  |  | √ |  |  |
| مردمیانی | √ | √ | √ | √ | √ | √ | √ | √ |  |  |  |  |  |  | √ |  | √ |  |  |  | √ |  |
| حمله عدم پذیرش سرویس | √ |  | √ | √ | √ | √ |  | √ | √ |  | √ |  | √ | √ |  | √ |  |  |  |  |  | √ |
| حمله کلونسازی | √ |  |  | √ |  | √ |  |  | √ |  | √ | √ | √ |  |  |  |  |  |  |  |  |  |
| حمله افشای کامل |  |  |  | √ |  | √ |  |  | √ |  |  |  |  |  |  |  |  |  | √ | √ | √ |  |
| استراق سمع |  | √ |  | √ |  |  |  | √ |  |  |  |  |  |  |  |  | √ | √ |  |  |  |  |
| حمله بازپخش | √ | √ | √ | √ | √ | √ |  | √ |  | √ | √ | √ | √ | √ | √ | √ | √ |  | √ |  | √ | √ |
| سرویس امنیتی |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| احرازهویت متقابل | √ | √ | √ | √ | √ | √ | √ | √ |  |  | √ |  | √ | √ | √ |  |  | √ |  |  | √ | √ |
| محرمانه بودن | √ | √ |  | √ | √ | √ | √ |  |  | √ |  | √ |  |  |  | √ |  | √ |  |  | √ |  |
| در دسترس بودن | √ |  |  |  | √ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| امنیت رو به جلو | √ | √ | √ | √ |  | √ | √ |  | √ | √ | √ | √ |  | √ |  | √ |  | √ |  |  |  |  |
| امنیت رو به عقب |  |  | √ | √ |  |  |  |  |  | √ | √ |  |  |  |  | √ |  | √ |  |  |  | √ |
| مالکیت قابل انتقال |  |  |  |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |  |  |  |  |
| ناشناس بودن برچسب | √ |  |  | √ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | √ |  |
| قابلیت ردیابی | √ | √ | √ | √ |  | √ |  | √ |  | √ | √ | √ |  |  |  |  |  |  |  |  |  |  |
| اختفای موقعیت |  |  | √ | √ |  |  | √ |  |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |
| اختفای اطلاعات | √ |  |  | √ |  |  | √ |  |  |  |  |  |  |  |  | √ |  | √ |  |  |  |  |
| کلاس |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| کلاس | F | F | F | F | F | F | F | S | S | S | S | S | S | L | L | L | L | L | L | UL | UL | UL |

در سال 2009، با بازسازی سه مولفه لگاریتم مجزای دارای انحنای بیضی شکل بر اساس دسترسی کنترل شده تصادفی (EC-RAC) [18]؛ طرح های انتقالی شناسه و رمزعبور امن، و تایید هویت سرور با توجه به الزامات سیستم و ویژگی های امنیتی، لی و همکارانش [22] 6 پروتکل مختلف برای حداقل سازی حجم محاسبات مربوط به برچسب ها، ارائه نموده اند.

در سال 2010، لی و همکارانش [23] پروتکل مبنی بر ECC که به مشکلات ردیابی موجود در پروتکل های ارائه شده در [7، 19] اشاره نموده است را معرفی نموده اند. این طرح تنها برچسب مربوط برای شناسایی خواننده را درنظر گرفته و برچسب تایید اعتبار را نادیده گرفته است. در سال 2011، ژانگ و همکارانش [24] پروتکلی تصادفی و کلیدی مبنی بر ECC را معرفی نموده اند که در واقع شکل بهبود و اصلاح یافته از طرح های لی و همکارانش و تولس و همکارانش، می باشد. این پروتکل در برابر برخی از حملات مربوطه ایمن بوده اما همچنان قادر به ارائه تایید متقابل نمی باشد.

در سال 2014، به منظور دستیابی به تایید متقابل، لائو و همکارانش [25] پروتکل ایمن تایید مبنی بر توانایی ECC همراه با پروتکل انتقال شناسه بازبینی شده، را معرفی نموده اند. با این حال، مطالعات [26- 28] چنین نشان داده اند که پیشنهاد لائو و همکارانش دارای نقص های امنیتی و عملکردی ضعیف می باشد. بعدها در همان سال، با بهره گیری از ECC، چوو [29] پروتکلی برای تایید ارائه کرده و چنین اعلام داشته است که این پروتکل پیشنهادی در برابر حملات مختلف، دارای مقاومت می باشد. با این حال، ژانگ و چی [30] چنین نشان داده اند که پروتکل پیشنهادی توسط چوو از منظر ضمیمه نمودن اطلاعات حریم خصوصی و امکان ردیابی رو به عقب و رو به جلو دارای نقوص و مشکلاتی می باشد. سپس در سال 2015، جین و همکارانش [31] پروتکل تایید متقابل برای محیط های درمانی و بهداشتی مبنی بر ECC پیشنهاد نموده و چنین بیان نموده اند که این پروتکل پیشنهادی در برابر حملات مختلف مقاوم بوده و نسبت به طرح های ارائه شده در [27، 28، 30] عملکرد بهتری از خود ارائه می نماید.

در سال 2016، فاراش و همکارانش [32] چنین نشان داده اند که طرح پیشنهادی توسط ژانگ و همکارانش [30] محافظت پیش فرضی از خود ارائه نمی نماید. اخیرا در سال 2017، ابراهیم و همکارانش [33] پروتکل توانمند و قدرتمند از تایید متقابل بر اساس ECC ارائه و کارآیی این پروتکل با بهره گیری از آخرین نسخه بازبینی شده از تعیین هویت بی سیم و پلاتفورم حسگر (WISP5) ثابت شده است. در پروتکل پیشنهادی، تایید متقابل تنها در دو مرحله انجام گرفته و در برابر تمامی حملات معمول مقاومت نموده و تمامی الزامات سیستم های امنیتی RFID را برآورد می نماید.

به دلیل زمانبر بودن الگوریتم های نامتقارن، تنها گزینه برای سیستم های RFID این الگوریتم ها، نمی باشند. علاوه بر این، اجرا و پیاده سازی سیستم های RFID همچنان امری چالش برانگیز می باشد. از این رو، برخی از محققین توجه خود را بر طرح های متقارن که شامل دو گروه اصلی: متون رمزی بلوک شده و متون رمزی در جریان، می باشند، متمرکز نموده اند.

جدول 3 منبع شماره و اسامی پروتکل های بررسی شده

شماره مرجع اسم مقاله و سال انتشار

]31[ پروتکل بازشناسی مشترک RFID برای محیط های درمانی با استفاده از منحنی رمزگذاری بیضی (2015)

]37[ پروتکل بازشناسی مشترک RFID جدید با پیچیدگی پایین و امنیت بالا(2014)

]32[ پروتکل بازشناسی اثبات شده ایمن بر مبنای منحنی های بیضوی در محیط های درمانی(2016)

]33[ استاندارد رمزگذاری پیشرفته پروتکل بازشناسی مشترک بر مبنای رمزنگاری منحنی بیضوی برای RFID اثبات شده با WISP(2017)

]44[ افزایش فضای کلید ها با هزینه ای کم برای بازشناسی RFID

]48[ برچسب های NFC با پشتیبانی از رمزنگاری در دارو ها برای امنیت بیشتر در بیمار(2014)

]50[ HPAP طرح جدید بازشناسی برای سیستمهای RFID(2013)

]53[ پروتکل بازشناسی مشترک برچسب RFID بر مبنای هاش در سیستمهای اطلاعاتی دارو های مراقبت از راه دور (2015

]55[ پروتکل بازشناسی موثر ارائه دهنده امنیت و حریم خصوصی بالا(2016)

]62[ کشف رمزی پروتکل LMAP: یک پروتکل بازشناسی RFID ارزان قیمت(2017)

]67[ پروتکل بازشناسی RFID کاربردی و خصوصی با پشتیبانی از انتقال مالکیت (2013)

]69[ RSEL: طرح بازشناسایی RFID سبک، ایمن، کاربردی و ابطال پذیر(2014)

]76[ تابع یک سویه هاش بر مبنای پروتکل بازشناسی مشترک سبک RFID (2013

]79[ طرح جدیدی برای بازشناسی مشترک سیستم های RFID ارزان قیمت (2016)

]81[ پروتکل کاربردی بازشناسی RFID سبک با امنیت حریم خصوصی خط سیر (2017)

]87[ ایمن و کاربردی پروتکل بازشناسی RFID سبک بر مبنای فهرست بندی سریع برچسب (2014)

]92[ پیشرفتی در پروتکل های بازشناسی سبک خانواده HB برای استفاده کاربردی در سیستمهای RFID (2013)

]97[ KEDGEN2: پروتکل ثبت کلید و استخراج برای سیستم های EPC Gen2 RFID (2014)

]104[ پروتکل بازشناسی فوق سبک RFID با CRC و جایگشت (2014)

]106[ SLAP: پروتکل بازشناسی سبک و فشرده برای سیستمهای RFID ارزان قیمت

]108[ کشف رمز پروتکل جدید بازشناسی مشترک فوق سبک برای دستگاه های IoT با استفاده از برچسب های RFID (2017)

]109[ امنیت قوی K برای شناسایی پروتکلهای بازشناسی بر مبنای توابع غیر قابل جعل فیزیکی

رمز نگارهای جریان داده سری سریعتر هستند و اعمال آن ساده تر است ولی در مقایسه با رمز گذاری بلاکی ضعیف تر هستند. لذا رمز گذاری های بلاکی محبوب تر هستند و محبوب ترین رمزگذاری بلوکی استاندارد پیشرفته رمزگذاری(AES) است.

شایان ذکر است که فلدهوفر و همکارانش]8[ اعمال موفقی از AES را در سال 2004 معرفی کردند. با این حال در سال 2008 کاپس]34[ متوجه شد که استفاده از الگوریتم گسترده رمزگذاری ظریف(XTEA) قدرت و منابع کمتری نسبت به AES نیاز دارد. علاوه بر این تحقیقاتی که از AES استفاده می کنند بیشتر به تعداد درگاه ها اشاره می کنند نه اهداف امنیتی پروتکل های بازشناسی، که سوژه اصلی مقاله حاضر است.

**3.2 پروتکل های ساده**

کلاس پروتکل های ساده شامل پروتکل هایی است که از RNG و یک تابع هش یکسویه پشتیبانی می کنند. اکوبا و همکارانش]35[ در سال 2003 به پروتکل قدرتمندی به عنوان مثالی از پروتکل های بر پایه هش دست یافتند. با این حال هزینه جستجو برای برچسب توسط سرور برای این پروتکل بالا است. در همان سال این پروپوزال توسط ویز و همکارانش]10[ تحت عنوان پروتکل hash-lock ارتقا یافت و اگر چه پروتکل hash-lock در جایگذاری تگ و کاربردی بودن سرور خوب عمل کرده است، ولی در زمینه امنیت بسیار ضعیف عمل کرده اند. در سال 2006 سودیک مدعی شد که هنوز یک پروتکل بازشناسی RFID ناچیز(YA-TRAP) ]9[ در مقابل حملات موقعیت یابی مقاومت کرده است.

با این حال در سال 2007 سودیک متوجه نقایص پروتکل قبلی خود شد و پروتکل جدیدی]36[ را معرفی کرد، اگر چه پروتکل جدید وی هدف اصلی او را نشان نمی دهد و در مقابل حمله پاسخگویی نفوذ پذیر است. در سال 2011 شین و همکارانش]113[ طرحی را نشان دادند که در ]9[در مقابل حملات پاسخ گویی و DoS نفوذپذیر بوده ارائه شده و نسخه ای ایمن را معرفی کردند. در همان سال لوپز و همکارانش]114[ مدعی شدند که مطلب مطرح شده توسط شین و همکارانش]113[ در مقابل حملات جعل هویت و پاسخ گویی بی دفاع است و مفهوم جدیدی را تحت عنوان سیستم هایRFID امنیت ناشکیبا (IS-RFID) معرفی کردند.

در سال 2012، ین و همکارانش]115[ متوجه شدند که مدارک داروی تولید شده توسط IS-RFID به راحتی توسط بیمارستان قابل تغییر است. در سال 2012 شن و همکارانش]116[ پیشنهاد پروتکل مقاومت جعلی دادند که در مقابل حملات جعل هویت، عدم همگام سازی، و ردیابی پذیری مقاومت کند. در سال 2012 چو و همکارانش]65[ به پروتکل بازشناسی مشترک بر مبنای تابع هش دست پیدا کردند که از کار قبلی وی]54[ نشأت گرفته بود. در سال 2012 و 2013 طرح چو و همکارانش]65[ توسط کیم و همکارانش]117،118[ مورد آنالیز قرار گرفت و ضعف شدید آن در مقابل حملات عدم همگام سازی کشف شد.

در سال 2014 صف خانی و همکارانش]119[ نیز طرح چو و همکارانش]65[ را آنالیز کردند و نشان دادند که در مقابل عدم همگام سازی، جعل هویت برچسب و برچسب خوان نفوذ پذیر است. علاوه بر این، طرحی که در ]117،118[ بر مبنای فعالیت های انجام شده در ]65[ مطرح شد توسط ]119[ آنالیز شد و نیز همان نواقص را داشت. در سال 2015 پروتکل باز شناسی مشترک دیگری بر مبنای تابع هش توسط سیرواستاوا و همکارانش ]53[ معرفی شد و از نظر کیفی با پروتکل های معرفی شده در ]36،51،54[ مقایسه و برتر از آنها شناخته شد. در سال 2016 شن و همکارانش]55[ پروتکل بازشناسی RFID کاربردی(ERAP) را معرفی و ادعا کردند در مقایسه با تحقیقات پیشین، پروتکل آنها در مقابل انواع مختلف حملات با هزینه کم مقاومت می کند،که نیازهای برچسب های RFID با منابع اجباری بالا را برآورده می کند. در نهایت در سال 2017 ، لی و همکارانش]62[ که پروتکل بازشناسی مشترک سبک(LMAP) ]120[ در مقابل برخی حملات و تمامیت اطلاعات نفوذ پذیر است. برای بهبود وضعیت امنیت و حریم خصوصیLMAP، نسخه ارتقا یافته ای از LMAP را معرفی کرده و مدعی شدند که پروتکل آنها تمام نیاز های برنامه های RFID را برطرف کرده و در مقابل حملات رایج مقاومت می کند.

از دیگر پروتکل هاییی که ممکن است در این دسته قرار بگیرد و ارزش اشاره به آن را داشته باشد خانواده پروتکل هوپر و بلوم(HB) است. در سال 2001 هوپر و بلوم پروتکل سبک فوق العاده ای را مطرح کردند که تنها از اپرتور های AND و XOR در بردارهای بایناری و یک بیت نویز به نام بیت HB ]94[ استفاده می کند و می توان آن را از طریق یک رویداد فیزیکی تولید کرد. برای مقاومت در برابر حملات ضمنی، پروتکل وابسته به پیچیدگی محاسباتی یاددگیری پاریتی به همراه مشکل نویز است.

پروتکل HB برای FRID طراحی نشده بود و به عنوان سبک یا فوق سبک طبقه بندی نشده بود. بعد از آن خانواده پروتکل های سبک بر مبنای پروتکل HB معرفی شد. از آنجایی که پروتکل HB در مقابل حملات ضمنی مقاومت می کند، جولز و ویز در سال 2005 پروتکل تغییر یافته شده ای را تحت عنوان پروتکل HB+ ]93[ معرفی کردند که در مقابل حملات فعال مقاومت کند. آنها مدعی شدند که پروتکل آنها سبک ولی ممکن است نتوان بر روی برچسب های RFID اعمال کرد و استفاده از نسخه دو دوری آن ممکن است ایمن نباشد. همچنین در سال 2005، گیلبرت و همکارانش ]14[ اذعان داشتند که پروتکل HB+ در مقابل حملات فعال زمان خطی بی دفاع است.

در سال 2006، برینگر و همکارانش]11[ پروتکل HB+ را بهینه سازی کردند تا به پروتکل HB++ دست پیدا کنند که در مقابل حمله گیلبرت و همکارانش مقاومت کند. با این حال، برای شناسایی حملات، نیازمند توابع یونیورسال هش و محتوای کلید های امنیتی مضاعف هستند. در سال 2007 مونیلا و همکارانش]95[ ایده رند کردن را معرفی کرده و پروتکل جدیدی تحت عنوان HB-MP ارئه دادند که در مقابل نقایص پروتکل های HB و HB+ موثر است.

در سال 2008 گیلبرت و همکارانش]121[ کشف کردند که یک حمله غیر فعال ساده می تواند هویت یک برچسب واقعی را با استراق سمع یک مکالمه جعل کند. در سال 2008 پروتکل HB# به عنوان نسخه ارتقا یافته در زمینه پروتکل HB# تصادفی معرفی که در همان مقاله]122[ توضیح داده شد. پروتکل HB# در مقابل کلاس گسترده ای از حملات فعال شامل حمله فعال گیلبرت و همکارانش به پروتکلهای HB و HB-MP مقاومت است و بر خلاف پروتکل HB++، پروتکل HB# نیازمند سخت افزار اضافه که پیچیدگی پروتکل HB را افزایش دهد نیست. همچنین در سال 2008 لنگ و همکارانش]96[ پروتکل HB-MP را با معرفی پروتکل HB-MP+ ارتقا دادند. یون و همکارانش]123[ متوجه شدند که پروتکل HB-MP+ کارایی دفاعی واقعی در مقابل حملات فعال پیشرفته یا روش های قوی ای برای مقابله با مشکل ردیابی ندارد، و به دنبال آن پروتکل HB-MP++ را معرفی کردند. باز هم در سال 2008 کوافی و همکارانش]124[ یک حمله با حضور یک انسان در آن روی پروتکل HB# انجام دادند و یک راز به اشتراک گذاشته شده بین طرفین در حال کالمه را بدست آوردند.

در سال 2009 هالوی و همکارانش]125[ نشان دادند که پروتکل های PRF محور از جمله پروتکل های HB+ و HB# برای برچسب های ارزان قیمت کارایی ندارد و پروتکل های درختی HB+ و درختی HB# را معرفی کردند. در سال 2012 پروتکل GBH# ]126[ ایجاد و ادعا شد می تواند در مقابل حملات با حضور یک انسان مقاومت کند، حمله ای که یک حمله موثر برای پروتکل HB# بود. با این حال، با معرفی پروتکل درختی LSHB+ ]128[ در سال 2013 دنگ و همکارانش مدعی شدند که پروتکل های درختی و پروتکلهای HB معمولی تنها بازشناسی یک سویه دارند، تنها برچسب توسط برچسب خوان بازشناسی می شوند و آنها بازشناسی مشترک را اضافه کردند. در نهایت پروتکل LSHB+ درختی نمی تواند در مقابل حملات افشای اسرار، عدم همگامسازی، و قابل ردیابی بودن مقاومت کند]128[. در ]128[ نسخه بازبینی شده ای از LSHB+ درختی ارائه و ادعا شد نسبت به پروتکل LSHB+ درختی قبلی برتری دارد. تکامل خانواده پروتکل های HB در شکل یک نشان داده شده است. دیگر پروتکل های بررسی شده رد جدول 1 و2 نشان ارائه شده اند.

**3.3 پروتکل های سبک**

کلاس پروتکل های سبک شامل پروتکلهایی است که نیازمند توابع ساده ای از جمله کد CRC و یک RNG هستند و بیشتر شامل پروتکل های است که تایید کننده استاندارد های EPC C1 Gen 2 هستند. کارکردهایی که از EPC C1 Gen2 پشتیبانی می کنند ممکن است برای مسائل امنیتی زیاد کاربردی نباشد و از همین جهت ارتقای آنها از اهمیت بالایی برخوردار است. علاوه بر این برخورد با مشکلات جدید در زمان حل مشکلات مد نظر امری طبیعی به شمار می رود. در پروتکل های تایید شده با استاندارد EPC C1 Gen2 مشکل امنیتی اصلیCRC-16 است( که به موجب ضعف جبری CRC است

)

در سال 2005 جولز]129[ جز اولین افرادی بود که راه حل مورد تایید EPC C1 Gen2 را ارائه داد و مدعی شد که در مقابل شبیه سازی و کلاه برداری مقاوم است. در همان سال کارثیکیان و همکارانش]130[ پروتکلی معرفی و از XOR و توابع ماتریس استفاده کردند تا قابل ردیابی نباشند و از تایمر و بروزرسانی کلید برای دستیابی به بازشناسی مشترک استفاده کردند.



شکل 1 – تکامل خانواده HB

در سال 2006، دوک و همکاران]13[ نشان داد که طرح جولز]129[ دچار درز های اطلاعاتی و حریم خصوصی است. علاوه بر این پروتکل جدیدی را معرفی کردند که از CRC، XOR، و یک تولید کننده اعداد شبه تصادفی(PRNG) برای تضمین امنیت اطلاعات تعاملی استفاده می کند، تا به بازشناسی و همگام سازی بروز رسانی های کلید های امنیت دست پیدا کند. با این حال، پروتکل آنها در مورد حمله DoS و امنیت پیشرونده نفوذ پذیر است.

در سال 2007، شین و همکارانش]12[ هم تحقیقات کاثیکیان و همکاران]130[ و دوک و همکارانش]13[ دست خوش تغییر کردند تا پروتکل جدیدی به نام پروتکل شین و چن(CC) را معرفی کنند که مدعی هستند به امنیت پیشرونده و همچنین مقاومت در برابر حمله های DoS بدست آورده اند؛ با این حال اشتباه بودن اهداف امنیتی مورد نظر با استفاده از ویژگی خطی عمل CRC استفاده شده در پروتکل، ثابت شد. در همان سال، لو و همکارانش]131[ پروتکل CC در زمینه امنیت دیتا حریم خصوصی و کارایی بهبود بخشید ولی پروتکل CC همچنان نسبت به استراق سمع و ردیابی موقعیت جغرافیایی نفوذ پذیر است.

در سال 2009، لوپز و همکارانش]132[ متوجه شدند که پروتکل CC نمی تواند در مقابل جعل هویت برچسب و برچسب خوان، عدم همگام سازی و حملات ردیابی مقاومت کند. در سال 2010، یه و همکارانش]133[ پروتکل جدیدی را تحت عنوان پروتکل رمز ایمن از راه دور(SRP) ارائه دادند که پیاده سازی آن ساده و سریع بوده و ادعا کرده اند که نه تنها مشکلات پروتکل CC را رفع کرده است بلکه دقت عملکرد کلی را نیز افزایش داده است. با این حال حبیبی و همکارانش]83و134[ متوجه شدند که پروتکل SRP در مقابل حملات ردیابی و درز اطاعات بی دفاع است و اینکه پیچیدگی یک حمله موفق تنها 216 است و آنها SRP را بهبود بخشیده و نسخه جدیدی از آن را معرفی کرده اند.

در سال 2014، محمدی و همکارانش]120[ طرحی که در ]83[ معرفی شده بود را مطالعه و نشان دادند که در مقابل حمله ای که پارامترهای رمزی را نشان بدهد، حمله جعل هویت برچسب، حمله عدم همگام سازی دیتا، حمله ردیابی نفوذ پذیر است. به علاوه آنها طرحی که در ]83[ ارائه شده بود را ارتقا داده و طرحی را مطرح کردند که به آن پروتکل سبک بازشناسی مشترک ارتقا یافته(ILMAP) می گویند. بعدها در سال 2014 علوی و همکارانش]135[ پروتکل ILMAP را بررسی و نشان دادند که در مقابل حمله ای که پارامترهای مخفی آن را نشان دهد، حمله به یکپارچگی اطلاعات، حمله کشف اطلاعات پیشرونده برچسب خوان، حمله ردیابی و حمله های ردیابی رو به جلو و رو به عقب نفوذ پذیر است. علاوه بر آن در سال 2013 پنگ و همکارانش ]136[ با تغییر پروسه هایی در ILMAP از مبنای پروتکل SRP پروتکل بازشناسی ای به نام SRP+ معرفی کردند و ادعا کردند بر ضعف های پروتکل SRP غلبه کرده و پیچیدگی یک حمله موفق را به 223 افزایش داده اند.

با این حال در سال 2015 ونگ و همکارانش]137[ پروتکل SRP+ را آنالیز کرده و نشان دادند که به خاطر نقص معروف عملکرد CFC در مقابل حمله های عدم همگام سازی و در مقابل حمله ی افشای منفعل با ضریب پیچیدگی O (216) نفوذ پذیر است. علاوه بر آن، نسخه بروز رسانی شده SRP+ به نام SRP++ معرفی شد و ادعا شد می تواند د مقابل حملات افشا کننده با ضریب پیچیدگی O(223) مقاومت کند و این به معنی ارائه امنیتی بالاتر از نسخه اسبق خود را داراست.

در سال 2016 معروف و همکارانش]79[ طرح بازشناسی مشترک جدیدی را مطرح کردند که مطابق با استاندارد EPC C1 Gen2 بود. آنها اینطور می گفتند که طرح آنها در زمینه حملات امنیتی مقاوم است، از طرح های قبلی بهتر بوده و به علت استفاده از اپراتور های ساده (XOR، CRC و PRNG) به راحتی می توان در سیستمهای RFID اعمال کرد. در نهایت در سال 2017 ژانگ و همکارانش]81[ پروتکل بازشناسی RFID سبکی را با مسیر امنیت حریم شخصی قوی(LAP-STP) معرفی کردند. آنها اینطور اطلاع رسانی کردند که پروتکل آنها می تواند حملات متفاوتی را تحمل کرده و ضامن مسیر حریم شخصی قوی باشد. دیگر پروتکل های بررسی شده در جداول 1و 2 ارائه شده اند.

**3.4 پروتکل های فوق سبک**

پروتکل های فوق سبک مخصوصا برای دستگاه های بسیار ضروری ساخته شده اند که تنها از اپراتور های بیتی ( مثلXOR، AND، OR)در آنها استفاده شد. بعد از عرضه Gen2 در سال 2006، لوپز و همکارانش پروتکل های RFID سبکی را تحت عنوان پروتکل های بازشناسی مشترک فوق سبک (UMAPها) را معرفی کردند و پروتکل بازشناسی مشترک ساده گرا(M^2AP)،]56[ پروتکل بازشناسی مشترک سبک(LMAP) ]57[ و پروتکل بازشناسی مشترک موثر(EMAP) ]58[ که فقط از توابع مثلثاتی(∨،∧،⊕) و جمع استفاده می کند را در بر گرفتند.این خانواده از نظر هزینه محاسباتی و هزینه نگهداری مناسب برچسب های RFID ارزان قیمت هستند.

با این حال در سال 2007 لی و همکارانش]15،16[ حملات متعددی را به M^2AP، LMAP و EMAP ارائه دادند. در همان سال شین]6[ گفت UMAP ها در مقابل حملات بسیاری نفوذ پذیر هستند، عملیات چرخش را معرفی کرد و بازشناسی قوی و یکپارچگی قوی(SASI) را معرفی کرد. با این حال به خاطر استفاده از توابع مثلثاتی(⊕،∨)، و تعداد محدود چرخش ها و جمع بستن ها، پروتکل SASI در مقابل حملات متعددی نفوذپذیر است و این امر توسط ]138،139[ نشان داده شده است. بعد ها در سال 2009 لوپز و همکارانش]105[ از XOR که در توابع و جمع های تو در تو نگه داری شده استفاده و پروتکل تار عنکبوت را معرفی کردند که نشأت گرفته از پروتکل SASI بود.

با این حال در سال 2010 تاگرا و همکارانش حمله ی عدم همگام سازی را برروی تار عنکبوت انجام دادند. بعد از تار عنکبوت، لوپز و همکارانش]141[ قدری LMAP را ارتقا داده و پروتکل بازشناسی فوق سبکی (ULAP) را معرفی کردند که برای غلبه بر حملات ضمنی تنها از جمع و توابع مثلثاتی استفاده می کند. در همین حال ريال در سال 2010 حمله ای ضمنی بروس ULAP توسط ونگ و همکارانش]142[ انجام شد.

در سال 2012 تیان و همکارانش]38[ پروتکل بازشناسی RFID فوق سبک جالبی را تحت عنوان پروتکل بازشناسی RFID با جایگشت(RAPP) را معرفی کردند که فقط سه عملیات شامل XOR بیتی، چرخش به چپ و جایگشت است. با این حال وزن همینگ چرخش و جاگشت تغییر ناپذیر است( یعنی وزن همینگ خروجی دو عملیات با وزن همینگ اولین پارامتر برابر است) به خاطر ویژگی های جایگشت، ژوانگ و همکارانش]143[ در سال 2013 دو حمله به RAPP داشت که باعث می شود برچسب علاوه بر حملات عدم همگام سازی و پاسخگویی به حالت DoS در بیاید.

علاوه بر این در سال 2013 ژوان و همکارانش]144[ با استفاده از عملیات های تجمیع( تجمیع دو رشته بیتی) و تفکیک(عکس تجمیع) پروتکل بازشناسی جدید را تحت عنوان پروتکل بازشناسی RFID فوق سبک کاربردی(EURFID) معرفی کنند. با این حال، در همان سال همان نویسنده]66[ کشف کرد که پروتکل EURFID درشرایط تداخل برچسب ها به خوبی عمل نمی کند و پروتکل بازشناسی RFID را برای برچسب های ارزان قیمت(RAPLT) معرفی کرد که عملیات تجمیع و تفکیک جدیدی بر مبنای پروتکل فوق سبک است. با این وجود،طبق گفته های ژوانگ و همکارانش]145[ RAPLT در مقابل حملات پاسخگویی و عدم همگام سازی، و محافظت از یکپارچگی اطلاعات و حریم خصوصی کاربر نفوذ پذیر است. در سال 2015 ونگ و همکارانش]137[ حمله افشا سازی را بر روی RAPLT ]66[ با استفاده از ویژگی خطی عملیات تجمیع و حمله عدم همگام سازی را روی SRP+ ]136[ را با استفاده از ویژگی خطی عملیات CRC انجام دادند. آنها نسخه ای بهینه شده و کاربردی از پروتکل SRP+ را که با استاندارد EPC C1 Gen2 همخوانی دارد و توسط SRP++ را معرفی کردند. آنها مدعی شدند که این پروتکل می تواند در مقابل حمله کامل جستجو مقاومت کند.

در سال 2016ريال لوو و همکارانش]106[ پروتکل بازشناسی مشترک فوق سبک جدیدی را بر مبنای تبدیل ایمن بیتی فوق سبک ارائه دادند. هدف از این کار ارتقای بازشناسی فوق سبک در مقابل مقاومت امنیتی ضعیف در پروتکل های اخیر که بود که در منابع ]107[ و ]64[ ذکر شده است. پروتکل آنها تنها از 3 عملکرد بیتی استفاده می کند: XOR، چرخش به چپ و تبدیل. آنها ادعا می کنند پروتکل آنها امن تر از دیگر پروتکلهای مورد مقایسه است، میتواند در مقابل حملات موجود مقاومت کند و نسبت به پروتکل های مورد مقایسه برای سیستمهای RFID ارزان قیمت مناسب تر است. در نهایت در سال 2017 تواری و همکارانش]108[ پروتکل بازشناسی مشترک فوق سبکی را ارائه دادند که از XOR بیتی و چرخش به چپ استفاده می کند. آنها اذعان داشتند که پروتکل آنها از تمامیت اطلاعات، یکپارچگی اطلاعات، بی نامی برچسب ها اطمینان حاصل می کند و در مقابل حملات ردیابی و حملات دیگر مقاومت می کند. دیگر پروتکل های ارزیابی شده در این کلاس در جداول 1 و 2 ارائه شده اند.

**3.5 روش های بازشناسایی جدید تر**

ذکر این موضوع که از روش های بروز تری از جمله استفاده از جستجوی جامع برای فعال کردن حفاظت امنیتی نیز استفاده می شود خالی از لطف نیست. مانیسم تصادفی کردن شناسه گر های برچسب ها برای محافظ از حریم شخصی آنها اولین بار در سال 2003 توسط ویز و همکارانش ]10[ مطرح شد. با استفاده از یک نانس که توسط یک برچسب و مقدار مخفی، شناسه گر را شناسایی می کنند. در همان سال اکوبا و همکارانش ]35[ در سال 2005 آویون و همکارانش]146[ این ایده را با روشی متفاوت بهبود بخشیدند؛ که در آن کلید جدید پیغامی بود که در پیام قبل ارسال شده بود.

در سال 2008، هنریکی و همکارانش]147[ روش اکوبا و همکارانش]35[ و آویون و همکارانش]146[ را استفاده کردند ولی کلید جدید با استفاده از زنجیره های هش قبلی تولید می شد. مشکل اصلی شناسه گر های تصادفی برچسب ها در قسمت سرور است که شناسه گر باید در بین حجم بزرگی از دیتا جستجو شود. راه حلی برای این مشکل روش ساختار جستجوی درختی است که توسط مولنار و همکارانش]70[، مولنار و همکارانش]148[ و دیمیتریو]149[ استفاده شده است. در این مقاله، شاخه ها کلید های مشخصی دارند و هر برچسبی مجموعه از کلید ها را دارد. برای شناسایی برچسب، کلید هر قسمت و بر روی شاخه خاصی استفاده می شود.

با این حال در سال 2010، آویون و همکارانش]150[ اینطور ذکر کردند که پروتکل هایی که از جستجوی جامع استفاده می کنند در معرض حمله تمام وقت هستند. در سال 2014، فیگویردو و همکارانش]151[ پروتکلی را معرفی کردند که برچسب های RFID در خودرو ها استفاده شده بودند. برچسب از کلیدی که در آن قرار داده شده استفاده و دو مقدار تصادفی تولید شده توسط برچسب خوان و برچسب استفاده می کند تا شناساگر تصادفی بدلی تولید کند. نرم افزار های شناسایی جستجوی جامعی انجام می دهند تا برچسبی که شناساگر را تولید کرده کشف کنند.

فیگویردو و همکارانش]151[ اینطور گفتند که روش های]35، 146،147[ مشکلات همگام سازی شدیدی نرم افزار های شناسایی و برچسب ها بوجود می آورد. آنها همچنین اذعان کردند که روشهای ساختاری استفاده شده در ]70،148،149[ محاسبات درون برچسب را زیاد می کند و میزان جواب برچسب را طولانی می کند. در نهایت، اینطور بیان کردند که مشکلات فوق را رفع کرده، و اطلاع دادند که هدف آنها از این پروپوزال ایجاد بهترین امنیت برای صاحبان برچسب ها نیست بلکه نشان دادن امکان جستجوی جامع کلید بدون استفاده مستقیم یا مشخص از شناساگر ها در زمان بازشناسی برچسب است.

**جدول شماره 4 بررسی کلی محصولات MIFARE**



**ارزیابی قیاسی**

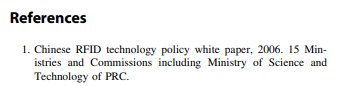
در جدول 2، پروتکل ها با یکدیکر در زمینه تهدیدات امنیتی و خدمات با یکدیگر مقایسه شده اند. هر کدام از پروتکل های مورد مقایسه قابلیت ویژه ای در حل مشکلات امنیتی و حریم خصوصی دارد. بعد از اینکه تعداد تیک ها از جدول شمرده شد، کلاسی که بر بیشتر تهدیدات فایق آمده و بیشترین خدمات را ارائه دهد به تکامل رسیده است و کلاسی که بر کمترین تهدیدات فایق آمده و کمترین خدمات را ارائه می دهد کلاس فوق سبک است. پروتکلی که در ]33[ ارائه شده است که که بهترین امنیت را ارائه می دهد کامل است و بر 9 مورد از تهدیدات غلبه کرده و 9 خدمت را ارائه می دهد. پروتکلی که در ]106[ ارائه شده است، که کمترین امنیت را به همراه دارد فوق سبک بوده و بر 3 تهدید غلب کرده و تعداد 0 خدمت را ارائه می دهد. انتظار می رود که تعریفات کلاس های بازشناسی را مد نظر قرار دهید. به عبارت دیگر، کمترین دست آورد را زمانی از یک پروتکل بازشناسی خواهیم داشت که قدرت سخت افزاری برچسب ضعیف است. جای تعجب ندارد که بیشتر برنامه های RFID محور از جمله دسترسی کنترل ساختمان]152[، پاسپورت هی الکترونیک]153[، عوارضی الکترونیکی]154[ و جریمه الکترونیک]155[ از کلاس به تکامل رسیده استفاده می کنند. علاوه بر این تکنولوژی هایی که در حجم گسترده در این حوزه استفاده می شوند، مثل کالیپسو]156[ و بیشتر نسلهای MIFARE ]157[ از کلاس به تکامل رسیده استفاده می کنند. وقتی که مسئله زندگی یک شخص و حریم خصوصی است، اینگونه انتظار می رود. با این حال، هزینه ها باید کاهش داشته باشد و نیاز برای پروتکلهای سبک و فوق سبک بیشتر و قوی تری بر همگام واضح است. برای خوانندگانی که نیاز به تعمق در مورد ویژگی های خاصی هستند، لطفا ]158[ را بررسی نمایید.

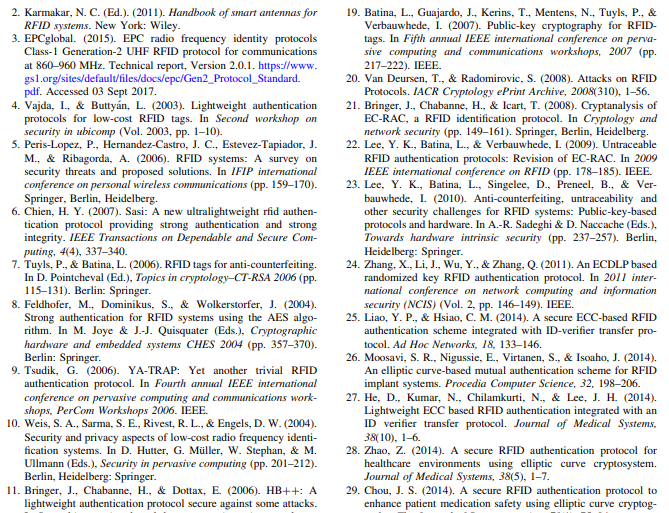
**5 نتیجه گیری**

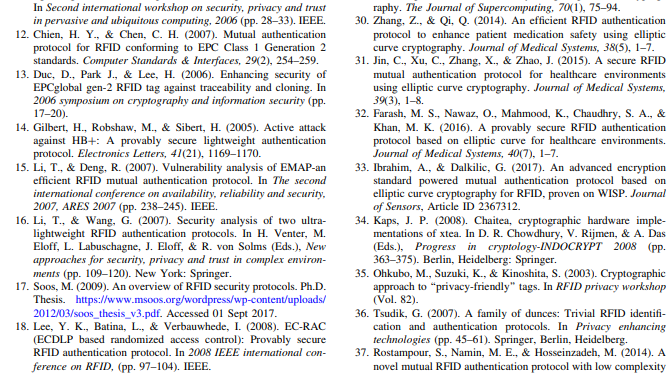
استفاده از پروتکل های بازشناسی اولین مرحله در در مقابله با حملات بیسیم به سیستمهای RFID است. مقاله پیش رو برخی از پروتکل های بازشناسی RFID اخیر را بررسی و مقایسه کرده است. نکات اصلی این مقایسه در جداول 1 و 2 ارائه شده است. جدول 1 نشان می دهد که برای مقابله با با این حملات و حصول اطمینان از امنیت و حریم شخصی، پروتکل های بازشناسی بررسی شده روش های متفاوتی را پیش گرفته اند ، مثل ECC، توابع هاش، تولید کنندگان اعداد تصادفی و تلفیق، تفکیک، بیت ترکیبی و عملیات های چرخش؛ و متد های تایید متفاوتی برای تایید پروتکل های معرفی شده استفاده شده اند. با اینکه برچسب های RFID ارزان قیمت به شدت محدود به سخت افزار خود هستند، در زمینه های ذخیره سازی و ظرفیت پردازش، ولی اکثر پروپوزال های بررسی شده در کلاس تکامل یافته قرار دارند و تعداد کمی از آنها در کلاس فوق سبک قرار می گیرند.

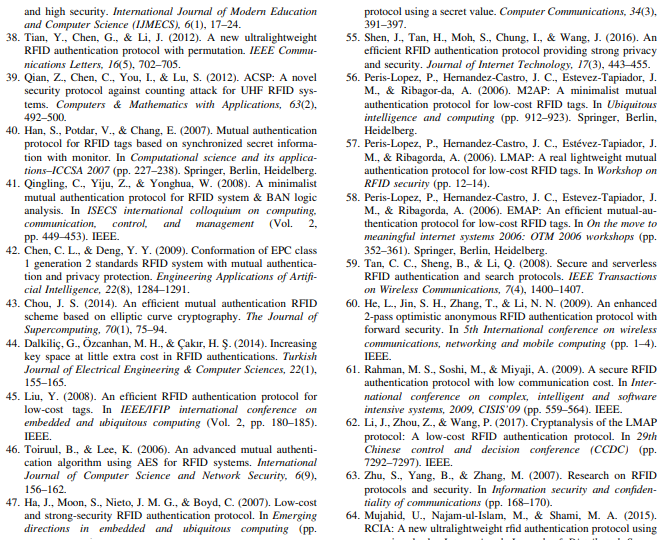
جدول 2 نشان داده که هرکدام از پروتکلهای بررسی شده قابلیت خاصی برای مواجهه با مسائل امنیتی و حریم خصوصی است. پروتکل های تکامل یافته بسیاری از تهدیدات را پشت سر می گذارند خدمات بسیاری نسبت به دیگر پروتکل ها ارائه میدهند. با در نظر گرفتن تعاریف کلاس های بازشناسی و هدفی که پروتکلهای بازشناسی باید به آن دست پیدا کنند، چنین نتیجه ای انتظار میرود.

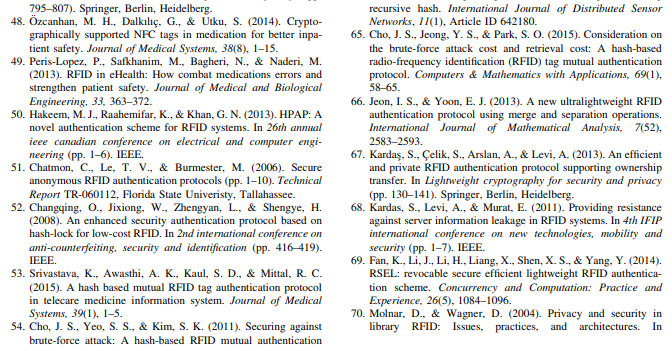
مقاله حاضر اینچنین نتیجه می گیرد که نیاز برای پروتکل های بازشناسی قوی تر وجود دارد، علی الخصوص در زمینه پروتکل های بازشناسی فوق سبک. لذا ضروریست پروتکل بازشناسی قوی تری ارائه شود که روش یکپارچه ای برای مواجهه با همه یا حداقل بیشتر تهدیدات را نسبت به پروتکل های ارائه شده در این مقاله را در کارآتی خود داشته باشد.

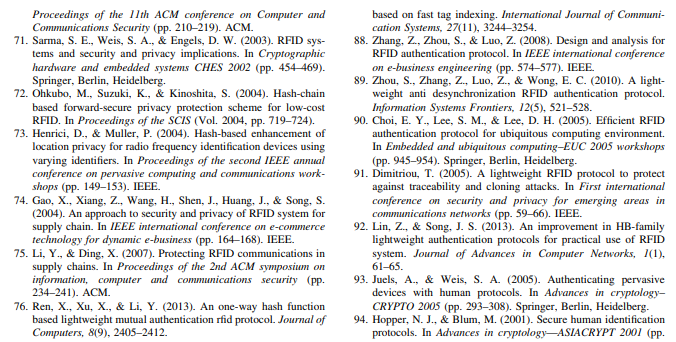
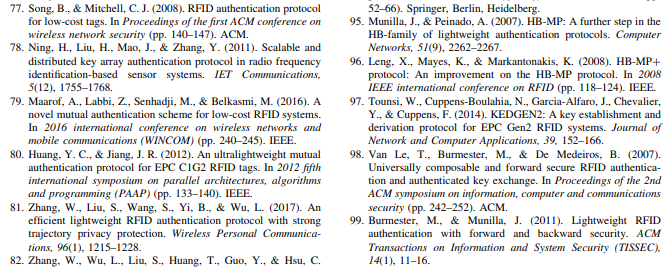


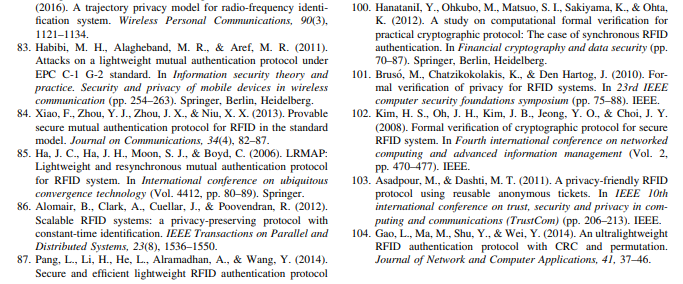


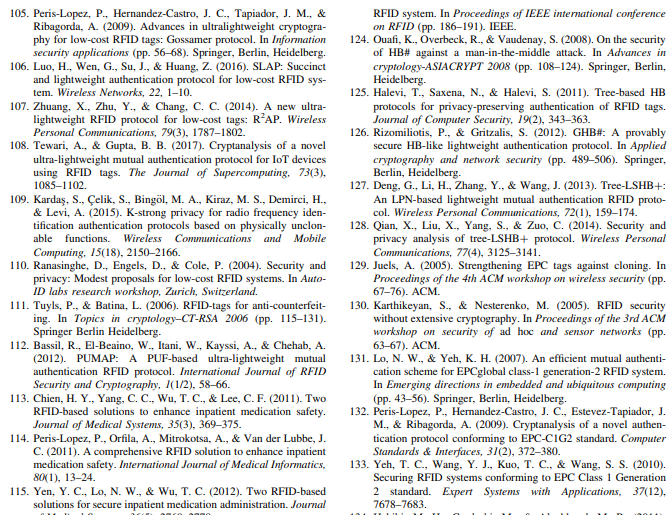


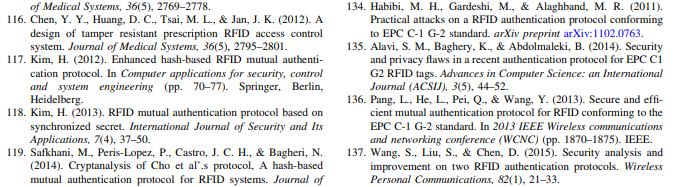


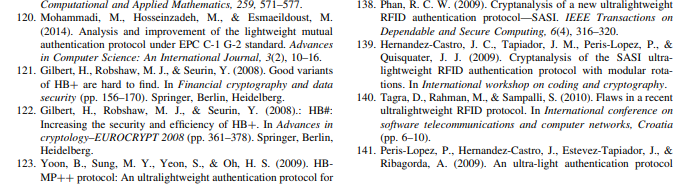


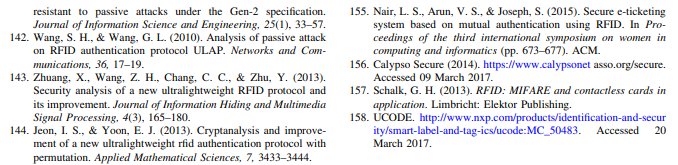
 

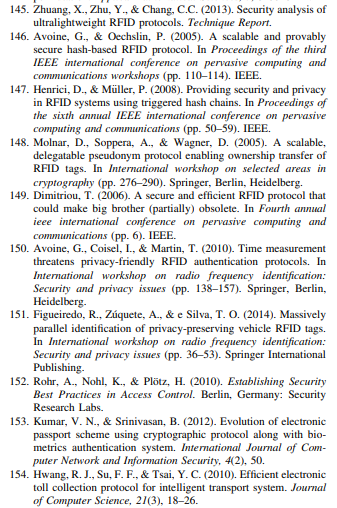












1. دپارتمان مهندسی کامپیوتر، دانشگاه دوکوز ایلل، ازمیر 35160، ترکیه [↑](#footnote-ref-1)