مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۳، پاییز ۱۳۹۵، ص ۱۰-۱

یک طرح احراز اصالت سبک وزن جدید برای شبکه‌های حسگر بی سیم

عبدالرسول میرقدری[1*]، رسول شیربانیان[2]، اکبر میرقدری[3]
۱- دانشیار، ۲- کارشناسی ارشد، دانشگاه جامع امام حسین(ع)
۳- کارشناس اداره هواشناسی اقلید
(دریافت: ۹۳/۰۴/۳۱، پذیرش: ۹۵/۰۵/۱۱)

چکیده

شبکه‌های حسگر بی‌سیم از نوع شبکه‌های اقتضایی هستند که می‌توانند در محیط‌های حساس و خطرناک به جمع‌آوری، پردازش و تبادل داده‌ها بپردازند. این شبکه‌ها متشکل از تعداد زیادی گره حسگر کم‌هزینه و کوچک می‌باشند که دارای محدودیت منابع مانند توان، حافظه و قدرت پردازش هستند و به صورت متراکم و تصادفی مستقر شده‌اند. شبکه‌های حسگر به دلیل ماهیت بی‌سیم با تهدیدات و آسیب‌پذیری‌های متعددی مانند حملات فیزیکی، حمله کشف کلید، حمله کاهش توان و غیره مواجه هستند. بنابراین هر طرح احراز اصالت برای این شبکه‌ها باید در برابر این حملات مقاوم باشد.

در این مقاله، با بررسی نقاط قوت و ضعف چند طرح احراز اصالت مناسب شبکه‌های حسگر بی‌سیم، یک طرح احراز اصالت جدید بر اساس یک رمز قالبی سبک‌وزن استاندارد برای امنیت این شبکه‌ها پیشنهاد می‌شود. طرح احراز اصالت پیشنهادی نقاط ضعف قبلی را پوشش داده و در مقایسه با سایر طرح‌ها از پیچیدگی محاسباتی کمتر، امنیت بیشتر و کارآمدی بهتر برخوردار است.

واژه‌های کلیدی: شبکه‌های حسگر بی‌سیم، طرح احراز اصالت، الگوریتم رمزنگاری سبک‌وزن، پیچیدگی محاسباتی

۱- مقدمه

در عصر اطلاعات و ارتباطات در هر ثانیه میلیاردها تراکنش و تبادل اطلاعات بر بسترهای ارتباطی انجام می‌شود. شبکه‌های حسگر بی‌سیم[1] یکی از این بسترهای ارتباطی است که شروع آنها به دوران جنگ سرد برمی‌گردد. این شبکه‌ها نوعی شبکه‌های اقتضایی بی‌سیم هستند. تا سال ۱۹۵۵ میلادی، توانایی این شبکه‌ها، محدود به جاسوسی‌ها و یا مراقبت‌های صوتی از محیط می‌شد. البته می‌توان سال ۱۹۹۹ را سال شکوفایی توسعه‌ی این شبکه‌ها در نظر گرفت. زیرا در این سال در کاربردهای غیرنظامی این شبکه‌ها مانند سلامت، کشاورزی، اقلیم شناسی و بخصوص فناوری اطلاعات نیز رشد قابل‌توجهی حاصل شد.

شبکه‌های حسگر بی‌سیم[1] به علت کاهش هزینه‌های تولید و کارآمدی آنها، به سرعت از طرفداران بسیار زیادی در سراسر دنیا برخوردار شدند. هزینه‌های کم این حسگرها باعث شده است تا در شرایط مختلف هم در زمینه‌های نظامی و هم در زمینه‌های غیرنظامی از قابلیت‌های بسیار بالایی برخوردار باشند. پیشرفت سریع این شبکه‌ها و کاربرد روزافزون آن‌ها در حوزه‌های مختلف به خصوص در تبادل اطلاعات باعث توجه جدی محققین به امنیت این شبکه‌ها شده است [۱].

با توجه به محدودیت‌های منابع انرژی، ذخیره اطلاعات و محاسبات در شبکه‌های حسگر بی‌سیم، این شبکه‌ها از پیچیدگی‌ها و تنگناهای خاصی برخوردار هستند. وجود این محدودیت‌ها در شبکه‌های حسگر بی‌سیم باعث شده تا تکنیک‌های امنیتی بیشتری برای این شبکه‌ها نسبت به دیگر شبکه‌های سنتی رایج پیاده‌سازی شود. همچنین کانال‌های ارتباطی ناامن و عملکرد غیرقابل اعتماد این شبکه‌ها، دست‌یابی به امنیت قابل قبول در این شبکه‌ها را دشوار کرده است. در دهه-های اخیر در بخش صنعتی، هزینه تولید این حسگرها، با حفظ توان محاسباتی و پردازشی مورد نیاز به‌طور قابل توجهی کاهش یافته است. با این حال بسیاری از محققان برای افزایش توانایی‌های پردازش و ذخیره انرژی بیشتر در این حسگرها و حفظ و حراست آن‌ها در برابر حملات نرم‌افزاری و سخت‌افزاری تلاش فراوانی نموده‌اند.

مسائل امنیتی و آن دسته از ملاحظاتی که برای ایجاد و حفظ امنیت شبکه‌های حسگر بی‌سیم، حائز اهمیت هستند باید رعایت شوند. رعایت تمام موارد فوق پرهزینه است لذا با توجه به نوع کاربرد و درجه حساسیت، در موارد خاصی از شبکه‌های

* رایانامه نویسنده مسئول: amrghdri@ihu.ac.ir
1-Wireless Sensor Networks (WSNs)

حسگر بی‌سیم با سطح امنیت مورد انتظار استفاده می‌کنند. با بررسی سه پروتکل احراز اصالت معروف مناسب شبکه‌های حسگر بی‌سیم و توجه به نقاط ضعف آنها، یک پروتکل احراز اصالت جدید بر اساس الگوریتم رمز قالبی سبک وزن پرزنت[1] پیشنهاد داده که نقاط ضعف پروتکل‌های قبلی را ندارد. در ادامه ساختار مقاله به این شرح است که ابتدا در بخش دوم ساختار شبکه‌های حسگر بی‌سیم را معرفی نموده و سپس چند پروتکل احراز اصالت مناسب این شبکه‌ها را در بخش سوم معرفی می‌نماییم. در بخش چهارم یک پروتکل جدید با سطح امنیت بالا و پیچیدگی کمتر برای این شبکه‌ها ارائه می‌دهیم. دلایل استفاده از رمز قالبی سبک‌وزن پرزنت در بخش پنجم بیان می‌شود. در بخش ششم تحلیل امنیتی و کارایی طرح پیشنهادی را بررسی می‌نماییم و در نهایت نتیجه‌گیری را در بخش هفتم بیان می‌کنیم.

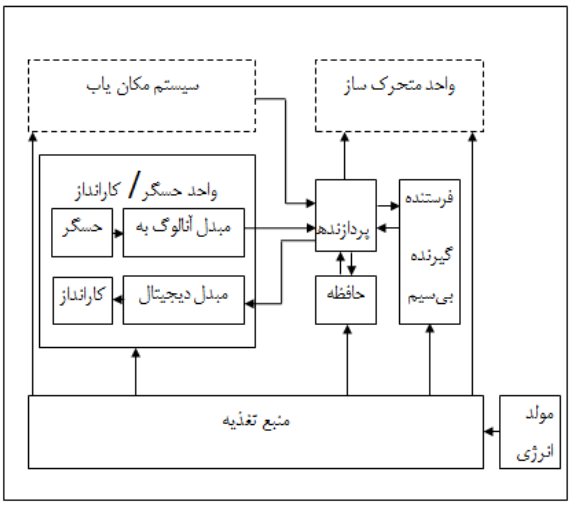
۲- ساختار شبکه‌های حسگر بی‌سیم

شبکه‌های حسگر بی‌سیم از نوع شبکه‌های اقتضایی هستند که می‌توانند در محیط‌های حساس و خطرناک به جمع‌آوری، پردازش و تبادل اطلاعات بپردازند. این شبکه‌ها از تعداد زیادی گره حسگری کم‌هزینه و کوچک تشکیل شده‌اند که دارای محدودیت منابع مانند توان، حافظه و قدرت پردازش هستند. هر گره شامل، واحد حسگر، واحد پردازش داده‌ها، فرستنده/گیرنده بی‌سیم و منبع تغذیه می‌باشد. بسته به نوع کاربرد ممکن است بخش‌های اضافی دیگری مثل واحد متحرک‌ساز، سامانه مکان‌یاب و واحد تولید توان نیز در گره‌ها وجود داشته باشند.

واحد پردازش داده‌ها، که شامل یک پردازنده‌ی کوچک و یک حافظه با ظرفیت محدود است، داده‌ها را از حسگرها گرفته و بنا به کاربرد، پردازش محدودی روی آن‌ها انجام داده و از طریق فرستنده ارسال می‌کند. همچنین واحد پردازش، مدیریت گره‌ها و هماهنگی و مشارکت گره‌ها با سایر گره‌های شبکه را برعهده دارد.

واحد فرستنده /گیرنده، ارتباط گره‌ها با یکدیگر و با شبکه را برقرار می‌کند. واحد حسگر، شامل یک سری حسگر و مبدل آنالوگ به دیجیتال است که اطلاعات آنالوگ را از حسگر گرفته و به صورت دیجیتال به پردازنده تحویل می‌دهد. واحد کارانداز، شامل کارانداز و یک مبدل دیجیتال به آنالوگ است که فرامین دیجیتال را از پردازنده گرفته و به کارانداز تحویل می‌دهد. واحد تأمین انرژی، توان مصرفی تمام بخش‌های گره را تأمین می‌کند که اغلب یک باطری با انرژی محدود است. محدودیت منبع انرژی یکی از چالش‌های اساسی طراحی شبکه‌های حسگر است که همه چیز را تحت تأثیر قرار می‌دهد. در کنار این بخش ممکن است واحدی برای تولید انرژی، مثل سلول‌های خورشیدی نیز وجود داشته باشد.

در گره‌های متحرک، علاوه بر قسمت‌های ذکر شده، واحدی برای متحرک‌سازی گره و واحد مکان‌یاب برای تشخیص موقعیت فیزیکی گره نیز وجود دارد. تکنیک‌های مسیریابی، جهت حسن انجام وظایف حسگری، به اطلاعات دقیق موقعیت مکانی نیاز دارند، یکی از مهم‌ترین مزایای شبکه‌های حسگر، توانایی در مدیریت ارتباط بین گره‌های متحرک می‌باشد. شکل (۱) ساختمان داخلی گره حسگر را نشان می‌دهد [۲].



شکل (۱). ساختار داخلی گره حسگر [۲]

۳- پروتکل‌های احراز اصالت

احراز اصالت رویه‌ای است که در آن یک نهاد، یک ادعای بیان شده توسط خود را برای نهاد دیگر به اثبات می‌رساند که این کار معمولاً با تبادل چند پیام بین آن‌ها انجام می‌شود. به عنوان مثال نهاد اول می‌تواند کاربری باشد که ادعای کاربر مجاز در یک شبکه را دارد و نهاد دوم نیز سرویس‌دهنده‌ای است که به کاربران مجاز این شبکه سرویس‌هایی را ارائه می‌دهد، که باید توسط رویه احراز اصالت، کاربر ادعای خود را به سرویس‌دهنده ثابت کرده و سپس از خدمات آن سرویس‌دهنده بهره ببرد. با همین شرح مختصر می‌توان فهمید که برای احراز اصالت حداقل به دو نهاد مجزا نیاز است که با یکدیگر در ارتباط باشند.

به طورکلی به الگوریتم‌های ارتباطی که بین دو یا چند نهاد مشترک به منظور اهداف امنیتی معین اجرا می‌شود، پروتکل گفته می‌شود. بنابراین به هر رویه احرازاصالت یک پروتکل احراز اصالت گفته می‌شود.

پروتکل‌های احراز اصالت می‌توانند بر حسب نوع کاربرد و هدف طراحی، از الگوریتم‌های رمز متقارن و نامتقارن استفاده کنند.

یک تراکنش بانکی را در نظر بگیرید که بین یک کاربر و یک بانک و از طریق اینترنت صورت می‌گیرد. در این تراکنش کاربر قصد انتقال مقداری پول از حساب بانکی خود به

1-PRESENT

حساب دیگری را دارد.

در اینجا لازم است که هویت کاربر برای بانک محرز شود تا بانک بتواند با اطمینان از عدم ایجاد خلل در حساب‌های مشتریان، این انتقال را انجام دهد و از طرف دیگر کاربر نیز باید از هویت بانک مطمئن شود تا اطلاعات شخصی خود را در اختیار عامل دیگری قرار ندهد. به منظور برقراری این تراکنش یک پروتکل احراز اصالت بین کاربر و بانک انجام می‌شود.

یکی دیگر از کاربردهای پروتکل‌های احراز اصالت، توزیع کلید احراز اصالت شده است. در این حالت از پروتکل‌های احراز اصالت به‌عنوان وسیله‌ای برای برقراری یک ارتباط امن استفاده می‌شود به طوری که یک کلید خصوصی مشترک احراز اصالت شده به کمک این پروتکل‌ها بین طرفین ایجاد و در نشست‌ها یا ارتباطات بعدی به‌کار گرفته می‌شود. به عبارت دیگر کلید به نحوی توزیع می‌شود که دریافت کنندگان آن از هویت یکدیگر و افرادی که کلید بین آنها توزیع شده است آگاه می‌شوند [۳].

مدل‌های مختلفی برای احراز اصالت وجود دارد. احراز اصالت در مدل‌های یک‌طرفه، متقابل، پخشی و غیره می‌تواند به کار گرفته شود [۴]. در ادامه چند پروتکل احراز اصالت که در شبکه‌های حسگر بی‌سیم استفاده می‌شوند را معرفی می‌نماییم.

۳-۱- پروتکل احراز اصالت لمپورت[1]

برای معرفی پروتکل‌های احرازهویت شبکه‌های حسگر بی سیم ابتدا پروتکل لمپورت را معرفی می‌کنیم [۵]. این پروتکل دارای کلمه عبور یک‌بار مصرف[2] بر اساس زنجیره چکیده‌ساز[3] است. در این پروتکل آلیس به‌طور تصادفی w را انتخاب می‌کند. یک تابع چکیده‌ساز برای تولید دنباله‌ای از کلیدها به صورت:

$$(w, H(w), H(H(w)), \dots, H^n(w)) \qquad (۱)$$

به‌کار می‌رود. $H^n(w)$ به این معنی است که تابع H، n بار تکرار شده است. $i-$ امین کلید احراز اصالت به صورت رابطه $w_i = H^{n-i}(w)$ تعریف می‌شود. آخرین عضو دنباله کلید که با n بار تکرار تابع چکیده‌ساز نتیجه می‌شود را w_0 می‌نامیم.

- مرحله اولیه: A مقدار w_0 را به روشی مطمئن برای B ارسال می‌نماید و نهاد B مقدار w_0 را ذخیره کرده و شمارنده j را با شروع از $j=1$ مقداردهی می‌نماید.
- برای احراز اصالت از $i = 1$ تا $i = n$ عملیات زیر انجام می‌شود.
- A مقدار w_i و i را برای کاربر B ارسال می‌نماید.
- B عبارت $i = j$ و $H(w_i) = w_{i-1}$ را بررسی می‌کند. اگر مقدار آن درست بود B مقدار w_i را ذخیره می‌کند و مقداردهی $j = j + 1$ را برای نشست بعدی انجام می‌دهد.

۳-۲- پروتکل احراز اصالت تسلا[4]

این پروتکل درسال ۲۰۰۲ توسط آدریان پرینگ[5] از دانشگاه برکلی ارائه شده است. نسخه دیگری از آن در سال ۲۰۰۴ به عنوان میوتسلا[6] که جزئی از پروتکل امنیتی SPINS[7] است، آمده است. این پروتکل معروفترین پروتکل احراز اصالت کارامد برای شبکه‌های حسگر بی‌سیم است[۶]. در این طرح از یک پروتکل پیش‌توزیع کلید، برای تأیید اولیه کلید K_0 استفاده شده است. این پروتکل برای احراز اصالت پخشی در شبکه‌های حسگر بی‌سیم به‌کار می‌رود [۷].

پروتکل احراز اصالت تسلا راه‌کار متفاوتی را با اضافه کردن برچسب زمان، ارائه می‌دهد. در این پروتکل فرستنده (آلیس) در ابتدا یک دنباله چکیده‌ساز از کلیدهای موقتی به صورت تولید می‌کند.

$$K_n, K_{n-1} = H(K_n), \dots., K_0 = H(K_1) \qquad (۲)$$

در ابتدا عضو انتهایی کلید K_0 را از طریق یک کانال امن برای همه کاربران انتشار می‌دهد. سپس آلیس پیام M_i تأیید شده توسط K_i را در فاصله زمانی t_i ارسال می‌کند. یعنی پیام‌ها فقط در فاصله زمانی t_i ارسال می‌شوند. در فاصله‌های زمانی بعدی آلیس کلید K_i را باز می‌کند و کاربران M_i را تأیید می‌کنند.

- در ابتدا A کلید K_0 را امضا نموده و عبارت $S = SIG(K_0, SK)$ را منتشر می‌کند. پس هر دریافت کننده، S که امضای K_0 توسط کلید خصوصی A می‌باشد را تایید می‌کند.
- برای پیام M_i در فاصله زمانی $t_i, i = 1, \dots, n$ حلقه زیر انجام می‌شود.
- A عبارت $X_i = MAC(M_i, X_i)$ را محاسبه نموده و مقادیر M_i و X_i را منتشر می‌کند.
- هر گیرنده بررسی می‌کند که آیا M_i و X_i را در فاصله زمانی t_i دریافت کرده است یا نه؟ و سپس این مقادیر را ذخیره می‌نماید.

1 -Lamport
2-One-time Password
3-Hash-chains

4-Timed Efficient Stream Loss-tolerant Authentication
5-Adrian Pering
6-Micro version of the timed Efficient Streaming, Loss-tolerant Authentication
7-Security Protocols for Sensor Networks

- A در فاصله زمانی $t_i + 1$ مقدار K_i را انتشار می‌دهد.
- هر گیرنده بررسی می‌کند که آیا $X_i = MAC(M_i, X_i)$ برقرار است یا نه؟

توجه کنید از کلیدی که در حافظه حسگرها ذخیره شده است فقط برای تایید کلید مرحله بعدی استفاده می‌شود و کلید هر مرحله فقط مختص همان مرحله است. چون پروتکل تسلا کلید اولیه را با امضای دیجیتال تأیید می‌کند لذا پاسخگوی همه نیازهای شبکه‌های حسگر بی‌سیم نمی‌باشد. زیرا این عملیات برای شبکه‌های حسگر بار محاسباتی خیلی زیادی دارد.

رمزگشایی یک کلید در هر بسته ارسالی نیازمند مصرف توان زیادی می‌باشد ذخیره یک کلید یک‌بار مصرف در یک گره حجم زیادی اشغال می‌کند.

این پروتکل از یک برچسب زمانی استفاده می‌کند که این باعث می‌شود از وقوع خیلی از حملات جلوگیری شود. تابع به‌کار رفته در ساختار چکیده‌ساز باید مقاوم در برابر تصادم[1] باشد مانند تابع چکیده‌ساز SHA-3 که در سال ۲۰۱۳ به عنوان استاندارد FIPS PUB 202 معرفی گردید [۸].

۳-۳- پروتکل احراز اصالت مهاتار[2]

این پروتکل از نوع سبک‌وزن است که توسط مهاتار و همکارش در سال ۲۰۱۱ برای احراز اصالت در شبکه‌های حسگر بی‌سیم ارایه شده است [۹]. یکی از مزایای این پروتکل این است که نسبت به سایر پروتکل‌ها پیچیدگی کمتری دارد.

در مقایسه با پروتکل SPINS [۶] این پروتکل می‌تواند مصرف انرژی را تا ۶۷ درصد کاهش دهد و به این خاطر است که مستقل از تعداد گره‌ها در شبکه تنها به یک پیام مبادله شده نیاز دارد. در پروتکل‌های قبلی هر گره باید با گره‌های دیگر به صورت جفت جفت کلید به اشتراک بگذارد و این نیازمند ذخیره‌سازی $n-1$ کلید در هر گره حسگر و $\frac{n(n-1)}{2}$ کلید در کل شبکه است و لذا موجب عملی نشدن پروتکل‌های قبلی برای شبکه‌های بزرگ می‌باشد. در پروتکل مهاتار کلید اصلی ابتدا برای همه گره‌های شبکه منتشر می‌شود. هر گره مقدار تصادفی خود یعنی R_i را برای مدت زمان کوتاهی انتشار می‌دهد. سپس مقادیر تصادفی از گره‌های مجاور خود دریافت کرده و با گره‌های مجاور خود کلید به اشتراک می‌گذارد.

این اشتراک‌گذاری باعث می‌شود که هر گره به جای اشتراک کلید با همه گره‌های شبکه فقط با گره‌های مجاور خود کلید به اشتراک بگذارد و این روش پروتکل توزیع کلید را برای شبکه‌های بزرگ عملی می‌کند.

مراحل پروتکل احراز هویت مهاتار را در زیر مشاهده می‌نمایید.

- A عدد تصادفی R_A را انتخاب نموده و آن را برای B ارسال می‌نماید.
- B یک عدد تصادفی R_B را انتخاب نموده و $E(K_{enc}^B, K_{auth}^j)$ و $H(R_A, K_{auth}^{j-1})$ و R_B را برای کاربر A ارسال می‌نماید که K_{enc}^B کلید رمزنگاری B و K_{auth}^j کلید احراز اصالت مرحله j-اُم است.
- A درستی تابع چکیده‌ساز را بررسی می‌کند و سپس مقادیر $E(K_{enc}^A, K_{auth}^j)$ و $H(R_B, K_{auth}^{j-1})$ را برای کاربر B ارسال می‌نماید.
- B درستی تابع چکیده‌ساز را بررسی می‌نماید.

این پروتکل با استفاده از توزیع کلید محلی و استفاده از رمزنگاری متقارن و توابع چکیده‌ساز باعث شده است تا بار محاسباتی آن به مقدار قابل توجهی نسبت به پروتکل‌های قبلی کاهش یافته و کارآمدتر باشد.

۴- دلایل استفاده از رمز پرزنت در طرح احراز اصالت پیشنهادی

در بررسی‌ها مشاهده شد که به دلیل محدودیت منابع انرژی و حافظه در شبکه‌های حسگر بی‌سیم نمی‌توان از پروتکل‌های احراز اصالت با بار محاسباتی سنگین و پیچیدگی محاسباتی زیاد برای این شبکه ها استفاده کرد. بنابراین بنا به دلایل فوق بایستی پروتکل احراز اصالت پیشنهادی سبک وزن باشد، لذا باید از الگوریتم رمزنگاری متقارن سبک وزن و تابع چکیده‌ساز سبک‌وزن در پروتکل احراز اصالت شبکه‌های حسگر بی‌سیم استفاده شود. اکنون با تجربه به‌دست آمده از تحلیل پروتکل‌های احراز اصالت می‌توان پروتکل احراز اصالتی را طراحی نمود که علاوه بر برخورداری از مزایای پروتکل‌های قبلی، معایب و نقاط ضعف آنها را نداشته باشد. به دلیل نیاز به داشتن پیچیدگی محاسباتی حداقلی، ما در طراحی پروتکل احراز اصالت پیشنهادی فقط از الگوریتم رمزنگاری متقارن سبک‌وزن و توابع چکیده‌ساز مناسب استفاده می‌کنیم. البته پروتکل‌های احراز اصالت قبلی برای رمزنگاری متقارن از الگوریتم‌هایی مثل AES و RC5 و DES استفاده می‌کردند که بار محاسباتی زیادی داشته و کارامدی را کاهش می‌دهند ولی در این پروتکل از الگوریتم رمز قالبی سبک‌وزن پرزنت استفاده می‌شود، این الگوریتم علاوه بر داشتن مزایای الگوریتم‌های قبلی از پیچیدگی محاسباتی بسیار کمتری برخوردار است و همچنین نسبت به حمله جبری و حمله تفاضلی مقاوم می‌باشد [۱۰].

1-Collision Resistance
2 -Mohatar

در سال ۲۰۰۷ رمز قالبی سبک وزن پرزنت توسط دکتر آندره بوگدانف و همکارانش ارایه گردید. پرزنت یک رمز قالبی سبک‌وزن با ساختار فیستلی بوده و دارای طول قالب ۶۴ بیتی و طول کلید ۱۲۸ بیت می‌باشد و در ۳۱ دور اجرا می‌شود. این رمز برای کاربرد در محیط‌های سبک‌وزن طراحی شده و طبق ادعای طراحان می‌تواند امنیت لازم در برابر حملات شناخته‌شده از قبیل تحلیل تفاضلی، تحلیل خطی، تحلیل تفاضلی ناممکن و حملاتی از این دست را فراهم آورد [۱۰]. همچنین سازمان بین المللی استاندارد و کمسیون علوم الکترونیکی بین المللی این رمز سبک‌وزن را به عنوان استاندارد ISO/IEC 29192-2 در سال ۲۰۱۲ برای محیط‌های سبک‌وزن کم‌هزینه اعلام نموده و به صنعت توصیه کرده که برای امنیت محصولات آینده خود از این رمز استفاده نمایند [۱۱].

این رمز ۲/۵ برابر کوچکتر از رمز استاندارد پیشرفته AES بوده و هزینه پیاده‌سازی آن به صورت تراشه ۲/۵ برابر کمتر بوده و مقرون به صرفه است [۱۲]. رمز پرزنت در هر دو پیاده‌سازی نرم‌افزاری و سخت‌افزاری کارایی بالایی داشته و در هر دو حالت یک رمز سبک‌وزن به شمار می‌آید. اما در اصل به‌صورت سخت‌افزاری طراحی شده و در فناوری $0.18\mu m$ با ۱۵۷۰ گیت قابل پیاده‌سازی است که در پردازنده ۱۰۰کیلوهرتز دارای کارایی ۲۰۰ کیلوبیت بر ثانیه می‌باشد. چون بر اساس توصیه NIST حداقل طول کلید برای ایجاد امنیت ۸۰ می‌باشد [۱۳] و بر اساس تحلیل‌های انجام شده روی رمزهای سبک‌وزن و مزایای الگوریتم‌های رمزنگاری سبک‌وزن پرزنت، مناسب‌ترین گزینه برای پروتکل احراز اصالت مدنظر ما رمز پرزنت می‌باشد. امنیت الگوریتم رمز سبک وزن پرزنت توسط افراد مختلف در برابر حملات مختلف مورد تحلیل و ارزیابی قرار گرفت [۱۷-۱۴]، ولی در عمل هنوز امنیت آن خدشه‌دار نشده است.

برای امنیت بیشتر نیز ترجیح می‌دهیم که از دنباله کلید یک‌بار مصرف و تابع چکیده‌ساز استفاده نماییم. چون برای احراز اصالت، کلید رمزنگاری با الگوریتم رمز قالبی سبک‌وزن پرزنت با طول کلید ۱۲۸ بیت و طول قالب ۶۴ بیت ارسال می‌شود بنابراین کلید را به دو قسمت تقسیم کرده و هر قسمت را با الگوریتم پرزنت رمز می‌نماییم. ساختار پروتکل پیشنهادی در ذیل شرح داده می‌شود.

۵- پروتکل احراز اصالت پیشنهادی

پروتکل احراز اصالت پیشنهادی از دو بخش توزیع کلید و احراز اصالت تشکیل شده است. این پروتکل در کلاس سبک‌وزن طراحی شده و برای شبکه‌های با حافظه و قدرت محاسباتی کم مناسب است. در ابتدای بکارگیری شبکه، طرح پیش‌توزیع کلید اجرا و سپس طرح احراز اصالت بین گره‌های شبکه انجام می‌شود.

برای افزایش کارایی و امنیت گره‌ها طرح توزیع کلید به صورت محلی اجرا می‌شود، یعنی هر گره با گره‌های مجاور خود کلید به اشتراک گذاشته که این امر باعث صرفه‌جویی در انرژی شده و از طرفی در صورت افشای کلید یک گره، کل شبکه آسیب نمی بیند.

نمادهای مورد استفاده به شرح ذیل می‌باشند.

عدد تصادفی انتخابی توسط A،	R_A
عدد تصادفی انتخابی توسط B،	R_B
کلید رمز گره i–ام	K_i
کلید رمز A	K_{enc}^{A}
کلید رمز B	K_{enc}^{B}
کلید احراز اصالت مرحله iام	K_{auth}^{i}
چکیده کلید مرحله قبلی با کلید K،	
	$K_i = \mathrm{Hash}(K_{i-1})_K$
رمزگذاری توسط الگوریتم رمز پرزنت	$Prsent(K_{enc}^{j})_{K_{auth}^{i}}$

۵-۱- طرح پیش‌توزیع کلید

در این مرحله ابتدا یک کلید رمزنگاری متقارن K_i در گره‌ها به روشی امن ذخیره می‌شود. که این فرآیند می‌تواند به دو صورت انجام شود یکی این که در مرحله ساخت گره‌ها، این کلید در حافظه هر گره ذخیره شود یا این کلید توسط کلید خصوصی مرکز کنترل شبکه رمزشده و برای کل شبکه ارسال شود. بهتر است که این کلید در مرحله ساخت گره در آن ذخیره شود و انرژی شبکه صرف بازگشایی این کلید نشود. این کلید باید حداقل طول لازم برای مقاوم بودن در برابر حملات خطی و تفاضلی را داشته باشد که آن را ۱۲۸ بیتی در نظر گرفته‌ایم.

سپس هر گره j یک عدد تصادفی X_j انتخاب و کلید رمزنگاری $K_j = \mathrm{Hash}(K_i, X_j)$ را محاسبه نماید. چون مهاجم از مقدار K_j اطلاعی ندارد لذا نمی‌تواند به محتوای اطلاعات ارسالی بین گره‌ها دسترسی یابد. برای افزایش امنیت در هر مرحله احراز اصالت، هر گره از تابع چکیده‌ساز کلید اولیه، یعنی از $K_i = \mathrm{Hash}(K_{i-1})_{kj}$ به عنوان کلید احراز اصالت استفاده می‌نماید. سپس کلید اولیه از حافظه حسگرها حذف می‌شود.

در برآیند این مرحله هر گره دو کلید دارد یکی K_j کلید رمزنگاری ارتباط بین گره‌ها و دیگری K_i کلیدی که برای احراز اصالت استفاده می‌شود. حافظه‌ای که در این مرحله برای حسگر نیاز است مربوط به ذخیره کلید رمزنگاری خودش و کلید احراز اصالت می‌باشد. البته در عمل می‌توان از توابع چکیده‌ساز سبک وزن با خروجی ۱۲۸ بیت مانند HAVAL ، PHOTON،

GLUON SPN-HASH, و DM-PREZENT-128 استفاده نمود [۱۸].

۵-۲- طرح احراز اصالت

طرح احراز اصالت وقتی اجرا می‌شود که یک گره بخواهد هویت خود را به گره مجاور اثبات نماید و یا هنگامی که گرهی جدید به شبکه اضافه می‌شود بایستی اصالت و هویت آن در شبکه تایید شود. پس از انجام مرحله پیش توزیع کلید، گره‌ها ارتباطات خود را با کلید K_j رمز می‌کنند. هنگامی که یک گره جدید به شبکه اضافه شود پروتکل احراز اصالت اجرا می‌شود.

فرض کنید که گره A می‌خواهد هویت خود را به گره B اثبات نماید. مراحل انجام پروتکل احراز اصالت به صورت زیر است. برای احراز اصالت در هر مرحله، از تابع چکیده‌ساز کلید مرحله قبلی استفاده می‌شود. به این ترتیب کلیدها یک‌بار مصرف است و مهاجم نمی‌تواند از کلیدهای مراحل قبلی برای احراز اصالت خود استفاده نماید. یادآوری می‌شود که $K_j = \mathrm{Hash}(K_i, X_j)$ کلید رمزنگاری بوده و $K_i = \mathrm{Hash}(K_{i-1})_{K_{j-1}}$ کلید احراز اصالت می‌باشد.

برای احراز اصالت در مرحله iام به شرح ذیل عمل می‌شود:

- کاربر A عدد تصادفی R_A را انتخاب کرده و سپس مقدار آن را برای B ارسال می‌نماید.
- کاربر B یک عدد تصادفی R_B را انتخاب نموده و با محاسبه $P_B = Prsent(K_{enc}^B)_{K_{auth}^i}$ و $H_B = \mathrm{Hash}(R_A \| ID_A \| t)_{K_{enc}^B}$ مقادیر P_B، H_B و R_B را برای کاربر A ارسال می‌نماید.

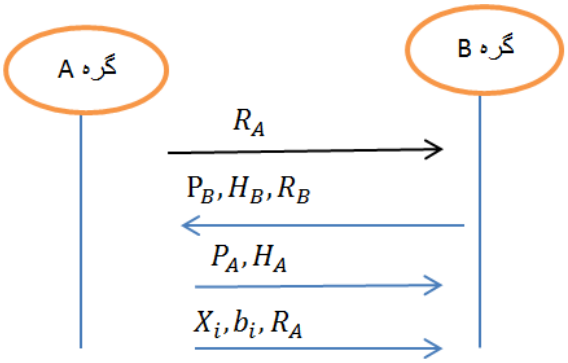
  توجه کنید که K_{enc}^B کلید رمزنگاری B و K_{auth}^i کلید احراز اصالت مرحله iام است.
- A با مقادیر زمان t، شناسه خود و R_A درستی تابع چکیده‌ساز را بررسی می‌کند و در صورت تایید اصالت B، مقادیر $P_A = Prsent(K_{enc}^A)_{K_{auth}^i}$ و $H_A = Hash(R_B \| ID_B \| t)_{K_{enc}^A}$ را برای کاربر B ارسال می‌نماید.
- B با بررسی تابع چکیده‌ساز و اثبات درستی آن، هویت A را تایید می‌کند.

پس از احراز اصالت گره‌ها می‌توانند برای مبادله پیام M از متن رمزشده $Prsent(M)_{K_{enc}^A}$ استفاده نمایند.

در این پروتکل ابتدا K_i توسط کانالی امن بین همه کاربران منتشر می‌شود.

سپس A یک عدد تصادفی R_A را انتخاب نموده و مقادیر $X_i = Hash(R_A \| ID_B \| t)_{K_{enc}^B}$ و $b_i = Prsent(K_{enc}^{jB})_{K_{auth}^i}$ را محاسبه می‌نماید. در مرحله بعدی مقادیر R_A و X_i و b_i را برای گیرنده (کاربر B) ارسال می‌نماید. هر گیرنده ابتدا اعتبار t و $K_i = H(K_{i-1})$ را بررسی می‌نماید، سپس با رمزگشایی b_i و دستیابی به کلید در صورت درستی و صحت عبارت $X_i = Hash(R_A \| ID_B \| t)_{K_{enc}^B}$ اصالت A را تصدیق می‌نماید.

نمای کلی پروتکل در شکل (۲) نمایش داده شده است.



شکل (۲). نمای کلی پروتکل احراز اصالت پیشنهادی

۶- تحلیل امنیتی و کارایی پروتکل

در ساختار پروتکل پیشنهادی از الگوریتم‌های رمزنگاری امن و مقاوم در برابر حملات استفاده نموده و نیز با به‌کارگیری برچسب زمانی و زنجیره کلید یک‌بار مصرف باعث جلوگیری از بروز حملات مختلفی مانند حمله منع خدمت، حمله ملاقات در میانه، حمله تکرار و غیره خواهد شد. امنیت و کارایی پروتکل پیشنهادی را در ادامه مورد بحث قرار می‌گیرد.

۶-۱- امنیت

محرمانگی، جامعیت داده‌ها، تازگی داده‌ها و حملات فیزیکی مانند حملات تکرار، جعل پیام، منع خدمت و فردی در میان بحث می‌شود.

- **محرمانگی**[1]: هر پیام در پروتکل پیشنهادی در مقابل حملات استراق سمع حفاظت شده است. چون برای تمام ارتباطات از توابع چکیده‌ساز و الگوریتم رمز متقارن استفاده شده و هیچ گونه اطلاعات مفیدی از پیام‌ها در اختیار مهاجم قرار نمی‌گیرد. بنابراین پروتکل پیشنهادی حالت محرمانه بودن را حفظ می‌نماید.
- **جامعیت داده‌ها**[2]: برای حفظ جامعیت داده نباید پیام‌های تبادلی بین حسگرها توسط مهاجمان تخریب شوند. در صورت وقوع خرابی، دریافت‌کننده پیام باید از تخریب داده‌ها مطلع شود. اگر درستی عبارت $X_i = H(R_A \| ID_B \| t)_{K_{enc}^B}$ برقرار باشد؛ دریافت‌کننده می‌تواند مطمئن باشد که داده‌ها صحیح هستند در غیر

1- Confidentiality
2- Data Integrity

این‌صورت دریافت‌کننده می‌تواند پیام را نادیده گرفته یا حذف کند.

- **تازگی داده‌ها**[1]: در هر زمانی که داده‌ها دریافت شدند، گیرنده باید مطمئن شود که داده‌ها تازه رسیده‌اند و مربوط به نشست قبلی نیستند. در این پروتکل به دلیل وجود برچسب زمانی و این‌که کلید هر مرحله با کلید مرحله قبلی در ارتباط است لذا تازگی داده و پیوستگی ارتباطات حفظ می‌شود.
- **حمله فیزیکی**[2]: چون پس از ایجاد و گسترش شبکه، کلید اصلی از حافظه حسگرها پاک شده و در هر مرحله کلید جدیدی جایگزین آن می‌شود، لذا پروتکل پیشنهادی در مقابل حملات فیزیکی مقاوم می‌باشد.
- **حمله تکرار**[3]: در هر زمانی که پیام‌های جدیدی ایجاد و ارسال می‌شوند، مهاجم نمی‌تواند با پیام‌های قدیمی درخواست احراز اصالت دهد، زیرا پیام‌های قبلی با پیام‌های جدید تفاوت دارند، کلید هر مرحله منحصر به فرد است و مدت زمان t برای تایید اصالت هر پیام محدود می‌باشد.
- **حمله جعل پیام**[4]: چون هر گره یک کلید رمزنگاری منحصر به فرد با گره دیگر به اشتراک گذاشته است که مهاجم آن را نمی‌داند، بنابراین مهاجم نمی‌تواند پیام جعلی را ارسال نماید و در نتیجه حمله جعل پیام امکان‌پذیر نخواهد بود.
- **حمله منع خدمت**[5]: چون در این پروتکل از مکانیزم برچسب زمانی استفاده کرده‌ایم، مهاجم نمی‌تواند از پیام‌های استفاده شده در نشست‌های قبلی برای برقراری نشستی جدید استفاده کند، به علاوه کلید رمزنگاری در هر نشست به روز می‌شود.
- **حمله ملاقات در میانه**[6]: در پروتکل پیشنهادی حمله استراق سمع غیرممکن است، زیرا مهاجم کلید رمز منحصربه‌فرد را نمی‌داند، بنابراین او نمی‌تواند با استفاده از اعداد تصادفی، تابع چکیده‌ساز را مشخص و ایجاد کند. با توجه به مباحث فوق وضع امنیت پروتکل‌ها در شکل (۳)، مقایسه و خلاصه شده است.

پروتکل / امنیت	لمپورت	تسلا	مهاتار	پیشنهادی
حمله تکرار	•	✓	•	✓
استراق سمع	•	•	•	•
حمله DOS	✓	✓	✓	✓
حمله فرد در میان	✓	✓	✓	✓
حمله فیزیکی	✓	✓	✓	✓

شکل (۳). مقایسه امنیت پروتکل‌های احراز اصالت

✓ مقاوم در برابر حمله

• آسیب‌پذیر در برابر حمله

۶-۲- کارایی

در این مقاله چند پروتکل مختلف احراز اصالت در شبکه‌های حسگر بی‌سیم مطرح شدند. همان طور که از قبل هم مشاهده شد برقراری تعادل بین امنیت و منابع کاری مشکل و دشوار است. زیرا هر اندازه که به امنیت یک گره افزوده شود از کارایی آن کاسته خواهد شد. هر پروتکل احراز اصالت باید ابتدا شرایط لازم برای امنیت مانند محرمانگی داده‌ها، جامعیت داده‌ها و تازگی داده‌ها را داشته و سپس در مقابل حملات مختلف مقاوم باشد. اگر پروتکل احراز اصالت دارای شرایط بالا باشد و نیز دارای پیچیدگی محاسباتی کمتر بوده و از حافظه کمتری برای ذخیره اطلاعات استفاده کند لذا کارایی بهتری خواهد داشت. از مزیت‌های طرح احراز اصالت پیشنهادی این است که قابلیت تبدیل شدن به طرح احراز اصالت پخشی را دارد. به دلیل مهر زمانی برای تصدیق هویت و استفاده از تابع چکیده‌ساز و الگوریتم رمزنگاری قالبی با کلید ۱۲۸ بیتی لذا پیچیدگی محاسباتی پروتکل پیشنهادی حداقل 2^{128} بوده که امنیت بالایی دارد و از

1- Data Freshness
2- Physical Attack
3- Replay Attack
4- Spoofing attack
5- Denial of Service attacks
6- Man in the middle attack

طرفی انرژی مصرفی آن تا حدود ۶۰ درصد کاهش می‌یابد که این امر به دلیل استفاده از الگوریتم رمز سبک وزن و حافظه مصرفی کم می باشد زیرا در پروتکل پیشنهادی حافظه مصرفی مربوط به کلیدهای K_i ، K_j ، اعداد تصادفی، ID، نتایج حاصل از الگوریتم‌های رمزنگاری و توابع چکیده‌ساز است که با توجه به ۱۲۸ بیت طول کلیدها و خروجی تابع چکیده ساز، در کل حدود ۵۴۰ بیت حافظه لازم دارد که نسبت به الگوریتم‌های تسلا (۶۴۰ بیت) و مهاتار (۵۸۰ بیت) کمتر است.

به دلیل استفاده شدن از برچسب زمانی در طرح جدید لذا امنیت آن بیشتر از امنیت پروتکل مهاتار است و چون برای احراز اصالت از کلیدهای یک‌بار مصرف استفاده شده است و کلید به صورت رمزشده ارسال می‌شود لذا نسبت به الگوریتم تسلا و لمپورت نیز دارای امنیت بهتری می‌باشد. از طرفی چون در پروتکل تسلا از امضا استفاده شده لذا پیچیدگی محاسباتی را به شدت افزایش می‌دهد. پیچیدگی حمله به الگوریتم پیشنهادی از مرتبه 2^{128} بوده که در مقیاس سبک وزن مقدار بسیار مناسبی است.

۷- نتیجه‌گیری

در این مقاله ابتدا چند پروتکل احراز اصالت برای شبکه‌های حسگر بی‌سیم معرفی شد و سپس پروتکل احراز اصالت سبک‌وزن را تشریح گردید. مزیت این پروتکل‌ها استفاده از الگوریتم‌های متقارن و کاهش پیچیدگی محاسباتی می‌باشد اما به دلیل استفاده نکردن از برچسب زمانی در برابر برخی از حملات مقاوم نمی‌باشد. در انتها یک پروتکل احراز اصالت جدید سبک وزن مناسب شبکه‌های حسگر بی‌سیم ارائه داده شد. در این پروتکل از طرفی برای برقراری امنیت از مهر زمانی و زنجیره کلید یک‌بار مصرف استفاده شد و از طرف دیگر برای کاهش پیچیدگی محاسباتی از الگوریتم سبک‌وزن رمز قالبی پرزنت استفاده شد که این امر باعث افزایش امنیت و کارایی این پروتکل نسبت به سایر پروتکل‌های احراز اصالت شده است. پیچیدگی حمله به پروتکل پیشنهادی از مرتبه 2^{128} است که نشان می‌دهد در برابر حملات معروف مقاوم است. کل حافظه مصرفی پروتکل پیشنهادی حدود ۵۴۰ بیت است که مربوط به کلیدهای رمزنگاری، اعداد تصادفی، شناسه کاربر، نتایج حاصل از الگوریتم‌های رمزنگاری و توابع چکیده‌ساز می‌باشد که نسبت به الگوریتم‌های تسلا (۶۴۰ بیت) و مهاتار (۵۸۰ بیت) کمتر است.

۸- مراجع

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, August 2002.

[2] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita, "A line in the sand: A wireless sensor network for target detection, classification, and tracking," Computer Networks Journal, Oct. 2004.

[3] G. Merret and Y. Kheng Tan, "Wireless Sensor Networks: Application Centric Design," Janeza Trdine 9, 5100 Rijeka, Croatia, 2010.

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, Florida, USA, 1997.

[5] M. Abadi and R. Needham, "Prudent Engineering Practice for Cryptographic Protocol," Tech. Report, DEC SRC 125, Digital Equeipment Corporation, November 1995.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," In Proceedings of MOBICOM, 2001.

[7] A. Perring, R. Canetti, D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," Technical Report 2, RSA Laboratories, 2002.

[8] Charles H. Romine, "SHA-3 Standard," Federal Information Processing Standards Publication 202, 2014, available at http://csrc.nist.gov/publication/.

[9] O. Mohatar, A. Fster-Sabater, and M. Sierra, "A light-weight authentication scheme for wireless sensor networks," Ad Hoc Network Journal, Elsevier, 2011.

[10] A. Bogdanov, L. R. Knudsen, G. Leander, C. Parr, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," In: P. Paillier, I. Verbauwhede, (eds.) CHES 2007. LNCS, vol. 4727, pp. 450-466. Springer, Heidelberg, 2007.

[11] W. Fumy, "Information technology-Security techniques-Lightweights Part 2: Block Ciphers," 2012., http://webstore.iec.ch/info-isiiec 29192-2

[12] ISO, ISO/IEC 29192-2, 2012., http://www.iso.org

[13] NIST, "Recommendation for Key Management, Part 1: General Guideline," Special Publication 800-57, p. 63, 2007.

[14] S. Bulygin, "More on Linear Hulls of Prezent-like Ciphers and a Cryptanalysis of Full-round EPCBC-96," 2013.

[15] G.-Q. liu and C.-H. Jin, "Differential Cryptanalysis of Prezentilike Cipher, DES. Codes Crypto, vol. 76, pp. 385-408, 2015.

[16] F. Abed, C. Forler, E. List, S. Lucks, and J. Wenzel, "Biclique Cryptanalysis of PREZENT," LED and KLEIN, eprint, iacr, 2014.

[17] M. H. Faghihi Serashgi, M. Dakhilalian, and M. Shakiba, "Biclique Cryptanalysis of MIBS-80 and

PREZENT-80 Block Ciphers," Security and Communication Networks, vol. 9, pp. 27-33, 2016.

[18] A. Biryukov, "Crypto LUX Wiki," Lightweight Hash Functions, 2014.
Available at https://www.cryptolux.org/index.php/

A New Lightweight Authentication Scheme for Wireless Sensor Networks

A. B. Mirghadri*, R. Shirbanian and A. Mirghadri

*Imam Hossein University

(Received: 22/07/2014, Accepted: 01/08/2016)

ABSTRACT

Wireless Sensor Networks (WSNs) are the type of Ad Hoc networks that can be used in critical and dangerous environments to collect, process and exchange their data. WSNs consist of a large number of low-cost sensor nodes that are small and have limited resources like power, memory and processing power, that have been deployed as dense and random. Due to the nature of WSNs are faced with multiple threats and vulnerabilities such as physical attacks, the recovery key attacks, reducing power attack, and etc. Therefore, any authentication scheme for these networks should be resistant against these attacks.
In this article, we examine the strengths and weaknesses of the proper WSNs authentication schemes and a new authentication scheme based on block cipher lightweight PRESENT for the security of these networks is suggested. The proposed authentication scheme covering the previous weaknesses compared with other schemes of less computational complexity, increased security and better efficiency.

Keywords: Wireless Sensor Networks (WSNs), Authentication Scheme, Lightweight Protocol, Attacks and Threats.

* Corresponding Author Email: amrghdri@ihu.ac.ir