پنجمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران
انجمن رمز ایران
Iranian Society of Cryptology

پروتکل احراز اصالت در شبکه‌های حسگر سلسله‌مراتبی

هانی صالحی سیچانی
دانشگاه صنعتی اصفهان
hani_salehi@hotmail.com

علی فانیان
دانشگاه صنعتی اصفهان
alifanian@gmail.com

مهدی برنجکوب
دانشگاه صنعتی اصفهان
brnjkb@cc.iut.ac.ir

چکیده: احراز اصالت و مدیریت کلید یکی از مسائل مهم در طراحی و توسعه شبکه‌های حسگر امن می‌باشد. استفاده از شبکه‌های حسگری که در آن تمامی گره‌ها دارای سطح مدیریتی و توان پردازشی یکسانی هستند، باعث پایین آمدن کارایی شبکه می‌شود. با استفاده از شبکه‌های حسگر سلسله‌مراتبی می‌توان کارایی شبکه را چه در پروتکلهای مسیریابی و چه از لحاظ امنیتی افزایش داد. از آنجا که فرایند احراز اصالت و برقراری کلید به عنوان اساسی‌ترین رکن برقراری امنیت در شبکه است، این الگوریتمها بایستی به نحوی در شبکه طراحی و پیاده سازی شوند که کمترین بار محاسباتی و پردازشی را بر گره‌ها تحمیل نمایند. در این مقاله برای احراز اصالت گره‌های دارای توان بالا به گره‌های شبکه حسگر، نوعی گواهی بر مبنای الگوریتم رمزمتقارن و پروتکل تسلا پیشنهاد می‌گردد که در عین حالی که دارای کمترین بار محاسباتی بر روی گره‌ها است، پیامهای کنترلی کمی را نیز بر روی شبکه تحمیل می‌نماید.

واژه های کلیدی: ارتباطات بی‌سیم، شبکه‌های حسگر سلسله‌مراتبی، احراز اصالت، تسلا، امنیت شبکه.

۱- مقدمه

شبکه‌های اقتضایی[1] از اهمیت در حال رشدی در زندگی و صنعت بشر برخوردار شده‌اند و از آنها برای جمع‌آوری و تبادل اطلاعات در سطوح وسیع استفاده می‌گردد. شبکه‌های بی‌سیم حسگر که یک نمونه خاص از شبکه‌های اقتضایی هستند، عموماً شامل گره‌هایی می‌باشند که انرژی مورد نیاز خود را از طریق باطری تامین می‌کنند و در نتیجه از توان پردازشی و محاسباتی پایینی برخوردارند و لذا در پیاده‌سازی الگوریتمها و پروتکلهای رمزنگاری بایستی توان محدود این وسایل را مد نظر قرار داد.

علیرغم شیوع استفاده از شبکه‌های اقتضایی دارای اجزای هم‌سطح[2]، اینگونه شبکه‌ها با همبندی هم‌سطح، دارای محدودیتهای فراوانی در پیاده سازی شبکه و همچنین برقراری پروتکل‌های امنیتی می‌باشند. در [1] به برخی از محدودیت‌های شبکه‌های اقتضایی هم‌سطح اشاره شده است. در همین راستا، اخیراً شبکه‌های اقتضایی سلسله‌مراتبی جایگزین شبکه‌های اقتضایی مسطّح شده‌اند. در شبکه‌های حسگر نیز، استفاده از ساختار سلسله‌مراتبی باعث افزایش کارایی و ظرفیت شبکه می‌گردد و تأخیر ارسال بسته‌ها از لایه‌های پایین به لایه‌های بالا را در شبکه کاهش می‌دهد. دلیل اصلی اینگونه بهبودها در شبکه، کاهش تعداد عبور بسته‌ها از گره‌های میانی (تعداد جهش‌ها)، برای رسیدن به شبکه اینترنت و برنامه‌های کاربردی است؛ چرا که در بیشتر مواقع گره‌های انتهایی شبکه اقتضایی درخواست دسترسی به شبکه اینترنت را دارند، تا اینکه بخواهند با گره‌های هم‌سطح خود ارتباط برقرار نمایند (این فرایند عموماً در گره‌های حسگر روی می‌دهد). در ساختار سلسله‌مراتبی، در لایه‌ی

[1] *Adhoc*
[2] *Flat ad-hoc networks*

بالایی گره‌های حسگر، نقاط دسترسی[3] با توان پردازشی بالاتر قرار می‌گیرند و اطلاعات دریافتی از حسگرها را به برنامه‌های کاربردی می‌رسانند. بدین ترتیب با استفاده از ساختار سلسله-مراتبی، دسترسی گره‌ها به برنامه‌های کاربردی در شبکه اینترنت، با تعداد واسط حسگر کمتری امکان‌پذیر می‌شود [2].

برای برقراری امنیت در شبکه‌های حسگر سلسله‌مراتبی، روشهای گوناگونی پیشنهاد شده است. در [3] پروتکل *LEAP* برای مدیریت کلید در شبکه‌های حسگر سلسله‌مراتبی دو سطحی پیشنهاد شده است. در این پروتکل، برای نیازهای امنیتی مختلف از کلیدهای مختلفی استفاده شده است. برای این منظور، *LEAP* چهار نوع کلید مختلف را برای یک حسگر تعریف می‌کند که شامل: کلید خصوصی حسگر با *BS*[4] در سطح بالاتر، کلید گروهی که *BS* از آن برای ارسال پیام به اعضای گروه استفاده می‌کند، کلید دسته برای ارتباط حسگرهای محلی با یکدیگر و کلید مشترک هر حسگر با حسگر مجاور خود. مزیت اصلی این پروتکل آن است که هر حسگر حافظه کمی برای نگهداری کلیدها نیاز دارد.

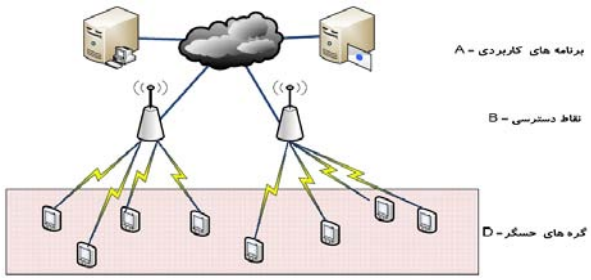
پروتکل پیشنهاد شده در [4] نیز مانند *LEAP* در دو سطح عمل می‌کند. در این پروتکل در زمان جابجایی گره حسگر میان دو ناحیه مختلف، کلید مشترکی میان او و *BS* برقرار می‌گردد. برای کم نمودن حجم محاسبات گره حسگر، این پروتکل از گواهی تسلا[5] که در [2] ارائه شده است، استفاده می‌کند. همچنین این پروتکل با استفاده از رمزنگاری خم بیضوی، حجم محاسبات اجزای شبکه را کاهش چشمگیری داده است.

هدف اصلی این مقاله، ارائه پروتکل احراز اصالت در شبکه-های حسگر سلسله‌مراتبی است که بار پردازشی بالایی را بر روی گره‌های حسگر تحمیل ننماید. در این روش برای احراز اصالت نقاط‌دسترسی به گره‌های حسگر، از گونه‌ی جدیدی از گواهی تسلا استفاده می‌کنیم که دارای زمان اعتبار طولانی‌تری در مقایسه با گواهی ارائه شده در [2] باشد و بدین طریق، با کاهش حجم پیامهای کنترلی لازم برای انجام پروتکل، کارایی پروتکل افزایش یابد.

در ادامه مقاله، ابتدا ساختار شبکه بی‌سیم استفاده شده در پروتکل شرح داده می‌شود. سپس، پروتکل تسلا و گواهی ارائه شده برای احراز اصالت مبتنی بر تسلا توضیح داده می‌شود. در ادامه، پروتکل اصلاح شده پیشنهادی به تفصیل معرفی می‌گردد و به دنبال آن پروتکل مذکور مورد ارزیابی قرار می‌گیرد.

۲- ساختار شبکه بی‌سیم سلسله مراتبی

در پروتکل احراز اصالت پیشنهادی از یک ساختار سه سطحی برای شبکه حسگر استفاده می‌شود. شکل ۱ ساختار سه سطحی مورد استفاده برای شبکه حسگر را نشان می‌دهد[5].



شکل ۱: شبکه حسگر سلسله مراتبی سه سطحی

این هم‌بندی از سه رده تجهیزات بی‌سیم تشکیل شده است:
کلاس D: این سطح، پایین‌ترین سطح شبکه است که در آن معمولاً تجهیزاتی با قدرت محاسباتی و ارتباطی پایین قرار دارد.
کلاس B: این سطح شامل تعدادی نقطه‌دسترسی است که واسط میان گره‌های *D* و برنامه‌های کاربردی هستند. این گره‌ها دارای توان پردازشی و ارتباطی بالایی در مقایسه با حسگرها هستند. نقاط دسترسی با استفاده از ارتباطات سیمی به شبکه اینترنت و برنامه‌های کاربردی (کلاس *A*) متصل می‌شوند.
با استفاده از ساختار سلسله‌مراتبی می‌توان به هر موجودیت متناسب با توان پردازشی آن، بخشی از الگوریتم لازم برای رمزنگاری یا احراز اصالت را محول کرد.

۳- احراز اصالت با استفاده از گواهی تسلا

امروزه استفاده ازگواهی‌های *PGP* و *X.509.V3* در شبکه‌های کامپیوتری متداول است. اینگونه گواهی‌ها بر اساس ساختار رمزنگاری کلید عمومی بنا شده‌اند و بنابراین برای استفاده در تجهیزات شبکه‌ای همانند حسگرها که دارای توان پردازشی و انرژی بالایی نیستند، مناسب نمی‌باشند. در [2] پروتکل احراز اصالتی مبتنی بر مکانیزم احراز اصالت همه پخشی تسلا که از رمز متقارن استفاده می‌کند، ارائه شده است. برای شرح این روش و پروتکل پیشنهادی، ابتدا به بررسی مکانیزم احرازاصالت تسلا می‌پردازیم.

[3] *Access Points (APs) - Base Station (BS)*
[4] *Base Station*
[5] *Time Efficient Stream Loss-tolerant Authentication Protocol (TESLA)*

۳-۱- معرفی مکانیزم احراز اصالت تسلا

در ارسال داده به صورت همه‌پخشی، در صورت نیاز به احراز اصالت مبدا ارسال داده، مناسب است از رمزنگاری کلیدعمومی استفاده شود. واضح است که استفاده از اینگونه رمزنگاری هزینه محاسباتی و پردازشی بالایی را هم بر روی گره ارسال کننده و هم بر روی گره دریافت کننده داده تحمیل می‌کند.

پروتکل تسلا، پروتکلی جهت احراز اصالت مبدأ ارسال داده مبتنی بر رمزنگاری متقارن است که به طور وسیعی از توابع درهم‌ساز یکطرفه استفاده می‌کند [6,7]. این پروتکل با استفاده از تأخیر زمانی، خاصیت نامتقارنی را که در رمزنگاری کلید عمومی وجود دارد، بدست می‌آورد. با استفاده از این روش، گره‌های دارای توان پردازشی پایین هم می‌توانند مبدا ارسال داده را احراز اصالت کنند. تسلا زمان را به بازه‌هایی با طول مساوی تقسیم می‌نماید و به هر بازه یک کلید اختصاص می‌دهد. به عنوان نمونه، به بازه‌زمانی n ام کلید tK_n اختصاص می‌یابد. برای هر بسته‌ای که در بازه n ام تولید و ارسال شود، فرستنده تابع درهمساز کلیددار (MAC) آن بسته را با استفاده از کلید tK_n محاسبه می‌کند و در کنار بسته ارسال می‌نماید. گیرنده‌ها بعد از دریافت بسته‌ها آنها را تا زمان آشکارسازی کلید MAC مربوطه، بافر می‌کنند. بعد از آشکار شدن کلید tK_n، هر گیرنده می‌تواند بسته‌های ذخیره شده را احراز اصالت کند. البته به دنبال اعلان کلید tK_n، هر موجودیتی می‌تواند بسته‌ای با MAC صحیح تولید کند و خود را به جای فرستنده جا بزند؛ اما تولید بسته‌هایی با کلید tK_n، تنها در بازه زمانی nام معتبر است و بازه‌های بعدی دارای کلیدهای تسلای مخصوص به خود هستند. در پروتکل تسلا هر کلید بعد از مدت زمان d که تحت عنوان "تأخیر آشکارسازی" شناخته می‌شود، اعلان می‌شود. در [6] مقدار کمینه d بدست آمده است.

tK_nها با استفاده از یک زنجیره تابع درهم یکطرفه به یکدیگر مربوط هستند. برای تولید این زنجیره، فرستنده ابتدا یک هسته اولیه tK_l انتخاب می‌کند و سپس با استفاده از تابع یکطرفه $Hash$، l بار از آن تابع درهم می‌گیرد. با هر بار تابع درهم گرفتن، هسته بعدی زنجیره به صورت زیر بدست می‌آید.

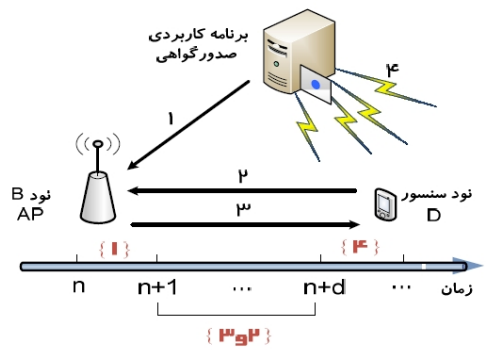
$$tK_{k-1} = Hash(tK_k) \qquad k = l,\ l-1,...,1 \qquad (۱)$$

فرستنده از مولفه‌های زنجیره فوق به صورت عکس روند تولید آنها یعنی از tK_0 به سمت tK_l استفاده می‌کند.

بعد از آشکار شدن هر کلید tK_n، گیرنده با استفاده از تابع $Hash$ و رسیدن به هسته قبلی احراز اصالت شده، به صحت tK_n پی می‌برد. نکته مهم در اجرای این پروتکل آن است که لازم است در ابتدا، فرستنده به صورتی یکی از کلیدها را برای گیرنده احراز اصالت کند که جزئیات آن در [6,7] آمده است.

۳-۲- پروتکل احراز اصالت مبتنی بر تسلا

همانطور که بیان شد، گره‌های اقتضاییِ دارای توان پردازشی پایین نمی‌توانند از گواهی‌های کلیدعمومی استفاده کنند و لازم است از گواهی‌های مبتنی بر رمزنگاری کلید متقارن استفاده نمایند. در [2] نوعی از ساختار گواهی برای برآورده شدن این هدف ارائه شده است. در این ساختار برای کم کردن حجم محاسباتی گره‌های حسگر، از الگوریتم تسلا استفاده می‌شود. در شکل ۲ موجودیت‌هایی که در ساخت و برقراری گواهی تسلا دخیل هستند و همچنین مراحل استفاده از این گواهی، نشان داده شده است.



شکل ۲ : مراحل برقراری و استفاده از گواهی تسلا

همانند ساختار گواهی کلید عمومی، در این ساختار هم موجودیتی تحت عنوان مرکز صدور گواهی وجود دارد. این موجود مسئول صدور گواهی برای موجودیت B است. هدف کلی از گواهی تسلا آن است که در صورتی که گره D با توان پردازشی پایین برای استفاده از سرویس با B تماس بگیرد، B بتواند با استفاده از گواهی تسلا، اصالت خود را به D احراز کند و در عین حال، D برای وارسی این گواهی و احراز اصالت B، توان بالایی را صرف ننماید. مراحل انجام کار بدین شرح است.

۱- مرکزصدورگواهی به صورت دوره‌ای برای B گواهی تسلا صادر می‌کند. این گواهی بدین شکل صادر می‌شود که در طول

بازه زمانی nام، مرکز صدورگواهی (CA) به جای استفاده از کلید خصوصی خود برای امضاء گواهی (همانند کاری که در صدور گواهی‌های کلید عمومی انجام می‌گیرد)، از کلید آشکار نشده تسلا tK_{CA_n} برای ساخت MAC درون گواهی، استفاده می‌کند. این کلید d بازه زمانی بعد توسط مرکز اعلان می‌شود. همچنین کلید عمومی گواهی $X.509$ مربوط به B، با کلید احراز اصالت موجودیت B (aK_{B_n})، جایگزین می‌گردد. این کلید با استفاده از کلید تسلای tK_{CA_n} و توسط مرکز رمز می‌شود. بدین ترتیب، ساختار گواهی تسلای صادر شده برای B در بازه زمانی nام، به صورت زیر می‌باشد:

$$Cert_{CA_n}(B) = \left\langle ID_B, \{aK_{B_n}\}_{tK_{CA_n}}, TS_A, MAC_{tK_{CA_n}}(...) \right\rangle$$

در این ساختار، TS_A یک مهر زمانی است که زمان اعتبار این گواهی را نشان می‌دهد. این گواهی به همراه کلید احرازاصالت B که با کلید مشترک میان مرکز و B، $K_{CA,B}$ ،رمز شده، در بازه زمانی nام برای B ارسال می‌گردد:

$$CA \rightarrow B: [\ Cert_{CA_n}(B), \{aK_{B_n}\}_{K_{CA,B}}, MAC_{K_{CA,B}}(...)\ ]$$

۲- در مدت زمان میان بازه n ام و $n+d$ ام، D برای استفاده از سرویس B با او تماس می‌گیرد و درخواست خود را ارسال می‌کند. $D \rightarrow B: [\ \text{Service Request}\ ]$

۳- در پی دریافت درخواست مرحله ۲، B بایستی اصالت خود را به D احراز نماید. بنابراین، B بسته احراز اصالت را که شامل گواهی تسلا و کد MAC گرفته شده بر روی درخواست D با استفاده از کلید aK_{B_n} می‌باشد، برای D می‌فرستد:

$$B \rightarrow D: [\ Cert_{CA_n}(B), MAC_{aK_{B_n}}(\text{D\_Request})\ ]$$

به محض دریافت این بسته، D با استفاده از مهر زمانی درون گواهی، از تازگی این پیام اطمینان حاصل می‌کند. در صورتی که این پیام تازه بود (قبل از زمان $n+d$ رسیده بود)، D تا زمان آشکار شدن کلید tK_{CA_n}، این پیام را بافر می‌نماید.

۴- در این مرحله و در زمان $n+d$، مرکزصدور گواهی، کلید تسلای tK_{CA_n} را آشکار می‌کند. بنابراین D می‌تواند درستی گواهی تسلای $Cert_{CA_n}(B)$ را با استفاده از $MAC_{tK_{CA_n}}(...)$ بررسی نماید و به کلید aK_{B_n} دست پیدا کند. سپس او می‌تواند $MAC_{aK_{B_n}}(\text{D\_Request})$ را بررسی کند و بدین طریق اصالت B برای D، احراز می‌گردد.

٤- احراز اصالت پیشنهادی مبتنی بر پروتکل تسلا

همانطور که مشاهده گردید، زمان اعتبار گواهی تسلا، TS_A، عموماً کوتاه و برابر با مدت زمان آشکار سازی کلیدهای تسلا می‌باشد. انتخاب زمان طولانی برای آشکارسازی کلید، باعث بروز تأخیر در فرایند احراز اصالت موجودیت B به گره حسگر D می‌گردد. از سوی دیگر زمان آشکارسازی کوتاه (البته نه کوتاهتر از بالاترین تأخیر RTT شبکه که باعث بروز مشکلات امنیتی گردد)، تأخیر احرازاصالت در گره D را کوتاه می‌کند اما باعث افزایش محاسبات در مرکز صدور گواهی و گره B و همچنین هدر رفتن پهنای باند شبکه (به دلیل بالا رفتن تعداد پیامهای ارسالی در شبکه)، می‌گردد. بنابراین بهتر است گواهی تسلا را به گونه‌ای اصلاح کنیم که در عین حالی که دارای زمان اعتبار طولانی‌تری است، موجود B بتواند در این زمان، خود را به گره‌های حسگر مختلف احراز اصالت نماید.

در این بخش، ابتدا مفهوم جلسات تسلای همزمان که از ایده‌ی آن در پروتکل احرازاصالت پیشنهادی استفاده شده است، شرح داده می‌شود. در ادامه نیز به بررسی پروتکل احراز اصالت پیشنهادی و تحلیل آن پرداخته می‌شود.

٤-١ جلسات تسلای همزمان

در شبکه‌های کامپیوتری حالاتی پیش می‌آید که گره‌های حسگر در احراز اصالت طرف مقابل خود، توانایی تحمل تأخیرهای متفاوتی را دارند؛ علاوه بر آن در بسیاری از شبکه‌ها، به دلیل مسافت‌های متفاوتی که گره‌های گیرنده نسبت به گره آشکارکننده کلیدهای تسلا دارند، لازم است جلسه‌های[٦] متفاوتی از تسلا با کلیدهایی با تأخیر آشکار سازی متفاوت ایجاد گردد. یک راه ساده برای اینکه چندین جلسه تسلای همزمان داشته باشیم آن است که با هر جلسه به طور مستقل رفتار کنیم و به عبارت دیگر برای هر جلسه یک زنجیره کلید تسلا در فرستنده و گیرنده‌ها داشته باشیم. مشکل اساسی این روش آن است که هر جلسه تسلای اضافی، باعث ایجاد بالاسری اضافی هم از لحاظ پهنای‌باند مصرفی پروتکل و هم از لحاظ فضای مورد نیاز در فرستنده و گیرنده می‌گردد. بنابراین

[٦] به هر ارتباط تسلا که در آن یک رشته کلید تسلا تولید می‌گردد و گره‌ی برقرار کننده‌ی ارتباط تسلا، از کلیدهای تسلا برای احرازاصالت خود به سایر گره‌ها استفاده می‌کند، یک جلسه تسلا گفته می‌شود.

بهتر است از روش دیگری برای برقراری جلسات همزمان استفاده شود.

در [8] روشی برای برقراری جلسه‌های تسلای همزمان پیشنهاد شده است که در آن با ایجاد جلسه‌های تسلای همزمان با تأخیر آشکار سازی کلید متفاوت، هر گیرنده می‌تواند تأخیر مناسب برای خود را انتخاب نماید و از جلسه تسلای مربوط به آن تأخیر استفاده کند. همچنین در آن روش، به جای استفاده از زنجیره‌های کلید مستقل برای هر جلسه تسلا، از یک زنجیره کلید اما با زمان‌بندی کلید متفاوت برای هر جلسه استفاده شده است. در ادامه به بررسی جزئیات این روش می‌پردازیم.

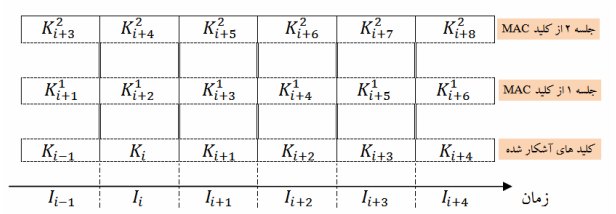
برای تمامی جلسات تسلا، یک زنجیره کلید وجود دارد که زمان آشکار سازی هر کدام از کلیدهای این زنجیره با شاخص مربوط به هر بازه زمانی یکسان است. به عبارت دیگر کلید K_i از زنجیره کلید، به بازه زمانی T_i متعلق است و در آن بازه آشکار می‌گردد (این زمان‌بندی کلید با زمان‌بندی کلید پروتکل تسلا که در آن کلید K_i جهت محاسبه MAC در بازه زمانی T_{i+d} آشکار می‌گردد، متفاوت است).

تصور شود که ارسال کننده بسته‌های تسلا، تمایل داشته باشد w جلسه از تسلا را ایجاد نماید. این جلسه‌ها را با $\tau_1,\tau_2,...,\tau_w$ نشان می‌دهیم. هر جلسه τ_u دارای تأخیر آشکار سازی کلید متفاوت d_u می‌باشد. برای بدست آوردن کلید MAC مربوط به این جلسه، لازم است که کلید آشکارشده به اندازه d_u بازه زمانی شیفت پیدا کند تا زمان‌بندی مناسب برای این جلسه برقرار گردد. در صورتی که $K^u_{i+d_u}$ کلید MACی باشد که توسط جلسه uام در بازه زمانی T_i مورد استفاده قرار می‌گیرد، این کلید به صورت زیر تولید می‌شود:

$$K^u_{i+d_u} = HMAC(K_{i+d_u}, u) \qquad (۲)$$

برای محاسبه مقدار MAC بسته P_j در زمان T_i و در صورتی که مقدار تأخیر جلسه‌ای که بسته P_j در آن ارسال می‌شود به اندازه d_u بازه زمانی باشد، فرستنده MAC پیام M_j را با استفاده از کلید $K^u_{i+d_u}$ محاسبه می‌کند و آنرا در کنار پیام M_j برای گیرنده ارسال می‌نماید.

در شکل ۳ زمان‌بندی استفاده از کلیدها در جلسات مختلف با یک مثال نشان داده شده است. در این مثال دو جلسه از تسلا برقرار شده است. جلسه اول دارای تأخیر آشکار سازی کلید به اندازه دو بازه زمانی و جلسه دوم دارای تأخیر آشکارسازی کلید به اندازه چهار بازه زمانی است. سطر "کلیدهای آشکار شده" زمان بندی آشکار کردن کلیدها را نشان می‌دهد. با توجه به این زمان‌بندی واضح است که هر کلید در بازه زمانی هم‌اندیس خود، آشکار می‌گردد. سطرهای اول و دوم نیز زمانبندی استفاده از کلیدها برای تولید کد MAC را در هر بازه زمانی نشان می‌دهد. در بازه زمانی I_{i+1} ام، فرستنده برای ارسال بسته‌ای از جلسه اول از MAC با کلید K^1_{i+3} استفاده می‌کند.



شکل ۳ : نمونه ای از جلسات تسلای همزمان

با استفاده از این تکنیک، فرستنده تنها لازم است که برای تمامی جلسه‌ها، تنها یک زنجیره کلید (کلیدهای سطر سوم) را آشکار نماید. این امر در کاهش استفاده از پهنای باند شبکه، کمک زیادی می‌کند.

۲-۴ اصلاح گواهی صادر شده برای نقاط‌دسترسی

زمان اعتبار گواهی ارائه شده در بخش ۳-۲، توسط TS_A مشخص شده است. این زمان در واقع همان تأخیر آشکار سازی کلید (tK_{a_n}) می باشد که برابر d است. اکنون گواهی احراز اصالتی پیشنهاد می‌شود که دارای زمان اعتبار طولانی‌تری نسبت به گواهی فوق الذکر باشد و در عین حال در طول این مدت زمان بتوان با استفاده از آن گواهی، گره‌های AP را به گره‌های حسگر احراز اصالت نمود.

مدل احراز اصالت در نظر گرفته شده بدین صورت است که در آن گره AP با m دسته گره حسگر در ارتباط است و می‌خواهد خود را به آنها احرازاصالت نماید (این دسته‌ها مجازی می‌باشد و هر گره می‌تواند پیوسته دسته خود را عوض نماید). این دسته‌ها را با شاخص‌های 1 تا m نشان می‌دهیم. در ضمن فرض می‌شود که مرکز صدور گواهی (CA) در لایه A، گواهی AP را در بازه زمانی I_n برای او صادر کرده است.

در این مدل، دسته حسگر ۱ تا قبل از بازه زمانی I_{n+d_1} (یعنی تا d_1 بازه زمانی بعد از بازه nام) درخواست خود را به AP ارسال می‌کنند و در این بازه می‌خواهند AP برای آنها احرازاصالت شود. دسته حسگر iام از بازه زمانی $I_{n+d_{i-1}}$ ام تا بازه زمانی I_{n+d_i} ام نیاز به احراز اصالت کردن AP دارند و به همین ترتیب دسته حسگر mام از بازه زمانی $I_{n+d_{m-1}}$ تا بازه زمانی I_{n+d_m} ام فرایند احراز اصالت را انجام می‌دهند. در این صورت تصور می‌شود پروتکل تسلا برای آشکار شدن کلیدها، دارای m جلسه می‌باشد. بدین ترتیب کلیدهای تسلای استفاده شده برای m جلسه، (K^x_{n+dx}) (که در حالت یک جلسه تسلا، با tK_{A_n} نشان داده می‌شد)، و کلید احرازاصالت B مربوط به آن جلسات ($aK^x_{B_n}$)، به صورت زیر نمادگذاری می‌شود.

برای دسته حسگر ۱ : $K^1_{n+d_1}$, $aK^1_{B_n}$

برای دسته حسگر ۲ : $K^2_{n+d_2}$, $aK^2_{B_n}$

.....

برای دسته حسگر m : $K^m_{n+d_m}$, $aK^m_{B_n}$

ارتباط کلیدهای احرازاصالت B با یکدیگر به صورت زیر می‌باشد:

$$aK^2_{B_n} = MAC_{K^2_{n+d2}}(aK^1_{B_n}) \quad (۳)$$
$$aK^3_{B_n} = MAC_{K^3_{n+d3}}(aK^2_{B_n})$$
.....
$$aK^m_{B_n} = MAC_{K^m_{n+dm}}(aK^{m-1}_{B_n})$$

در واقع اگر مرحله i ام را فاصله زمانی میان بازه $I_{n+d_{i-1}}$ ام تا بازه زمانی I_{n+d_i} ام در نظر بگیریم، کلید احراز اصالت B برای هر مرحله (کلید $aK^i_{B_n}$ برای مرحله i)، با استفاده از MACی بدست می‌آید که بر روی کلید احراز اصالت B در مرحله قبلی ($aK_{B_n^{i-1}}$) و با استفاده از کلید آشکار شده این مرحله ($K^i_{n+d_i}$) گرفته شده است. حال گواهی صادر شده برای B در بازه زمانی n ام به صورت زیر معرفی می‌شود:

$$Cert_{CA_n}(B) = \left\langle ID_B, \{aK_{B_n^1}\}_{K^1_{n+d1}}, TS_A, MAC_{K^1_{n+d1}}(...) \right\rangle$$

در این گواهی فرض شده است که بازه‌های زمانی مختلف که برای احراز اصالت AP به دسته حسگرهای ۱ تا m استفاده می‌شوند، دارای طول مساوی هستند. در صورتی که در شبکه‌ای بنا به دلایلی لازم باشد که از بازه‌های با طولهای مختلف استفاده گردد، این گواهی را می‌توان به صورت زیر اصلاح نمود:

$$Cert_{CA_n}(B) =$$
$$\left\langle ID_B, \{aK_{B_n^1}\}_{K^1_{n+d1}}, TS_{A1}, TS_{A2}, ..., TS_{Am}, MAC_{K^1_{n+d1}}(...) \right\rangle$$

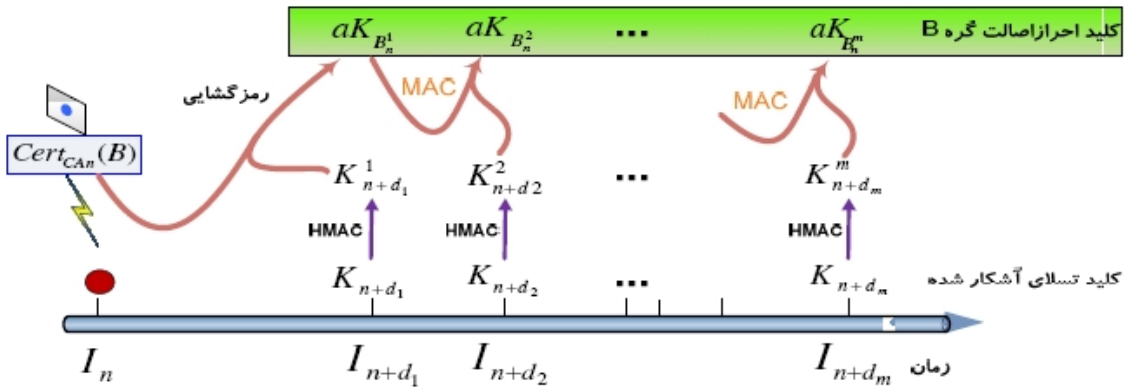
که در این گواهی $aK^1_{B_n}$ کلید احراز اصالت B مربوط به مرحله اول است که با کلید تسلای آن مرحله و به صورت متقارن رمز شده است. زمان TS_{Ai}، زمان آشکار سازی کلید تسلای مرحله iام را مشخص می‌کند. به عنوان مثال در زمان TS_{A1}، کلید تسلای مرحله اول(K_{n+d_1})، آشکار می‌گردد و کاربران می‌توانند کلید $K^1_{n+d_1}$ را از روی آن تولید کنند.

$$TS_{Ai} = n + d_i \quad (٤)$$

در شکل ۴ ارتباط میان کلیدهای مختلف و بازه‌های زمانی آنها در پروتکل پیشنهادی، مشاهده می‌شود.

CA برای برقراری سرویس صحت بر روی گواهی صادر شده، MAC گواهی را با استفاده از کلید $K^1_{n+d_1}$ می‌گیرد و آنرا به گواهی اضافه می‌نماید.

در نهایت، پیام صادر شده از سوی مرکز CA در بازه زمانی I_n برای نقطه‌دسترسی B، به صورت معادله (۵) اصلاح می‌گردد.



شکل ٤: ارتباط میان کلیدهای مختلف در پروتکل پیشنهادی

$$CA \rightarrow B: \quad [\,Cert_{CA_n}(B), \{aK_{B_n^1}, aK_{B_n^2}, ..., aK_{B_n^m}\}_{K_{CAB}}, MAC_{K_{CAB}}(...)\,] \qquad (۵)$$

مرکز صدور گواهی (CA) ناچار است که تمامی کلیدهای احراز اصالت مربوط به m مرحله را با استفاده از کلید مشترک میان خود و B رمز کند و در این پیام برای B ارسال نماید. البته این پیام تنها یک بار و در بازه زمانی n ام برای AP ارسال می‌گردد. در ادامه فرایند احراز اصالت در پروتکل پیشنهادی، مورد بررسی قرار می‌گیرد.

۳-۴ چگونگی احراز اصالت AP به حسگر D

بعد از اینکه AP در بازه زمانی nام پیام مربوط به صدور گواهی جدید برای خود را از سوی برنامه‌کاربردی A (CA) دریافت نمود، تا بازه زمانی I_{n+d_1} می‌تواند از گواهی صادر شده و کلید احراز اصالت اول ($aK_{B_n^1}$)، برای احرازاصالت خود به دسته حسگر ۱ استفاده کند. بدین ترتیب در صورتی که در طول این بازه، D درخواست خود را به B ارسال کند، B می‌تواند با پیام زیر خود را به D احراز اصالت کند:

$$B \rightarrow D: [\,Cert_{CA_n}(B), MAC_{aK_{B_n^1}}(\text{D\_Request})\,]$$

از سوی دیگر، اگر در بازه nام، مرکز صدور گواهی، گواهی صادره برای B را همه‌پخشی نماید، حسگرها در صورت حضور در شبکه، می‌توانند این گواهی را ذخیره کنند و بنابراین گره حسگر می‌تواند در هنگام ارسال درخواست خود، با تنظیم پرچمی به AP اعلام نماید که گواهی مربوطه را در اختیار دارد و نیازی به ارسال مجدد آن توسط AP نیست. در این صورت، پیام ارسالی B به D به صورت زیر، ساده می‌گردد:

$$B \rightarrow D: [\,MAC_{aK_{B_n^1}}(\text{D\_Request})\,]$$

در هر حال، در بازه زمانی I_{n+d_1} که کلید تسلای K_{n+d_1} توسط A آشکار می‌گردد، دسته حسگر ۱ می‌توانند با استفاده از رابطه (۶)، کلید MAC مربوطه را بدست آورند:

$$K^1_{n+d_1} = HMAC\,(K_{n+d_1}, 1) \qquad (۶)$$

حال او می‌تواند با استفاده از این کلید، صحت گواهی صادر شده برای B را با وارسی $MAC_{K^1_{n+d1}}(...)$ درون گواهی $Cert_{CA_n}(B)$، احراز نماید. بدین طریق او می‌تواند با رمزگشایی $\{aK_{B_n^1}\}_{K^1_{n+d1}}$، کلید احراز اصالت B یا همان $aK_{B_n^1}$ را بدست آورد و با استفاده از آن، B را احرازاصالت نماید. چرا که B در فاصله زمانی بازه I_n تا بازه I_{n+d_1}، پیامی را به صورت $MAC_{aK_{B_n^1}}(*)$ (* می‌تواند عبارت مشخصی باشد) برای حسگر D ارسال نموده است.

در پایان بازه I_{n+d_1}، گواهی $Cert_{CA_n}(B)$ هنوز دارای اعتبار است. به بیان دیگر این گواهی تا بازه I_{n+d_m} از اعتبار کافی برخوردار می‌باشد.

برای فاصله زمانی بعدی، یعنی بازه زمانی I_{n+d_1} تا بازه زمانی I_{n+d_2} که دسته حسگر ۲ از B تقاضای ارتباط می‌کنند، نقطه دسترسی B از کلید $aK_{B_n^2}$ برای احراز اصالت خود استفاده می‌کند. در انتهای این فاصله و در بازه I_{n+d_2} که کلید K_{n+d_2} توسط A آشکار می‌گردد، حسگرهای دسته ۲ می‌توانند با استفاده از آن کلید، به کلید $K^2_{n+d_2}$ دست یابد. بعد از دستیابی به کلید $K^2_{n+d_2}$، حسگرها با استفاده از معادله (۷) می‌توانند به کلید احراز اصالت B در آن بازه دست پیدا کنند.

$$aK_{B_n^2} = MAC_{K^2_{n+d2}}(aK_{B_n^1}) \qquad (۷)$$

سپس با استفاده از $aK_{B_n^2}$، آنها می‌توانند B را احرازاصالت کنند. توجه شود که درون گواهی B، $Cert_{CA_n}(B)$، پارامترهای $\{TS_{A1}, TS_{A2}, ..., TS_{Am}\}$ موجود می‌باشند و بنابراین حسگرهای دسته دوم علاوه بر آنکه TS_{A1} (یا همان $TS_{A1} = n + d_1$) را می‌دانند، TS_{A2} (یا همان $TS_{A2} = n + d_2$) را هم می‌دانند و بنابراین آنها می‌توانند بر طبق معادله زیر و به دلیل آنکه کلیدهای K_{n+d_x}، کلیدهای تسلا هستند، از K_{n+d_2} به K_{n+d_1} برسند:

$$K_{n+d_1} = Hash^{d_2-d_1}(K_{n+d_2}) \qquad (۸)$$

که در رابطه ۸ منظور از $Hash^{d_2-d_1}$، اخذ تابع درهم به تعداد $d_2 - d_1$ بار از K_{n+d_2} می‌باشد.

در مرحله بعدی دسته حسگر ۲ می‌توانند از روی K_{n+d_1} به $K^1_{n+d_1}$ دست پیدا کنند. آنها با استفاده از $K^1_{n+d_1}$ و گواهی رسیده از B می‌توانند از درون گواهی، $aK_{B_n^1}$ را رمزگشایی کنند و آنرا بدست آورند و با استفاده از روش ذکر شده به کلید $aK_{B_n^2}$ برسند. از سوی دیگر $K^1_{n+d_1}$ در احراز اصالت گواهی صادر شده برای B هم به حسگرها کمک می‌کند.

برای سایر دسته حسگرها و بازه‌های زمانی متناظر نیز روند مشابهی برای احراز اصالت B برقرار است.

۵- ارزیابی پروتکل پیشنهادی

اصلاح پروتکل احرازاصالت، بهبود مناسبی در استفاده از پهنای-باند شبکه ایجاد می‌کند. در شرایطی که AP با m دسته حسگر که هر کدام بازه‌های احراز اصالت متفاوتی دارند (برای احراز اصالت AP)، روبرو باشد، در پروتکل اولیه، AP نیاز به m گواهی مجزا از هم دارد که این گواهی ها بایستی از سوی مرکز صدور گواهی برای او صادر و ارسال شوند. این در حالی است که گواهی صادر شده در پروتکل اصلاح شده، در عین حالی که دارای طول برابری با طول گواهی صادر شده در پروتکل اولیه است، برای انجام m روند احراز اصالت، تنها یک بار ارسال می‌گردد (با فرض آنکه در پیام CA در بازه nام، گواهی B برای تمامی حسگرها همه‌پخشی گردد). برای تحلیل دقیق‌تر، در صورتی که طول شناسه هر AP را L_{ID}، طول کلیدهای احرازاصالت را L_{aK}، طول مهرزمانی را L_{TS} و طول خروجی تابع MAC را L_{MAC} فرض نمائیم، در کل با تفاضل پهنای باند مصرفی دو پروتکل، روش پیشنهادی به مقدار قابل توجهی از هدر رفتن پهنای باند شبکه جلوگیری می‌کند که این مقدار در جدول ۱ مشخص شده است.

جدول ۱: مقایسه پروتکل پیشنهادی و پروتکل ارائه شده در [2]، از نظر پهنای باند مصرفی

	پهنای باند مصرفی پیام اول	پهنای باند مصرفی پیام سوم	پهنای باند مصرفی برای m مرحله احراز اصالت
پروتکل اصلی	$L_{ID}+2L_{aK}+L_{TS}+2L_{MAC}$	$L_{ID}+L_{aK}+L_{TS}+2L_{MAC}$	$m(2L_{ID}+3L_{aK}+2L_{TS}+4L_{MAC})$
پروتکل پیشنهادی	$L_{ID}+(m+1)L_{aK}+L_{TS}+2L_{MAC}$	L_{MAC}	$L_{ID}+(m+1)L_{aK}+L_{TS}+(m+2)L_{MAC}$
بهبود پروتکل پیشنهادی			$(2m-1)[L_{ID}+L_{aK}+L_{TS}]+(3m-2)L_{MAC}$

البته باید متذکر شد که در صورت افزایش m، مقدار پردازش هر حسگر برای احراز اصالت AP به دلیل افزایش تعداد دفعاتی که یک حسگر ناچار است تابع یکطرفه کلید دار را محاسبه کند، افزایش می‌یابد. اما از آنجایی که در گره‌های حسگر، مصرف توان در اثر تبادلات رادیوئی بسیار قابل توجه است و از سوی دیگر پروتکل پیشنهادی در قبال افزایش کمی در پردازش هر حسگر، پهنای باند مصرفی حسگر از شبکه را به میزان قابل توجهی کاهش می‌دهد، این پروتکل باعث کاهش چشمگیری در مصرف انرژی گره‌های حسگر می‌شود. در عین حال پروتکل پیشنهادی این امکان را نیز به گره‌ها می‌دهد که با حضور مداوم در شبکه بتواند در هر بازه زمانی کلیدهای احراز اصالت $aK_{B_n^x}$ را محاسبه و ذخیره نماید و بدین صورت پردازش حسگر در طول زمان توزیع شود و پردازش زیادی در هنگام احراز اصالت، بر گره حسگر تحمیل نگردد.

۶- نتیجه‌گیری

در این مقاله، پروتکل جدیدی جهت احراز اصالت نقاط دسترسی به گره‌های اقتضایی در شبکه‌های سلسله‌مراتبی، پیشنهاد شد. جهت انجام فرایند احراز اصالت، از پروتکل تسلا و گواهی مبتنی بر آن استفاده گردید و با استفاده از ایده‌ی جلسات تسلای همزمان، این گواهی به گونه‌ای اصلاح شد که دارای زمان انقضاء طولانی‌تر از گواهی تسلای پیشنهاد شده در [2] باشد.

در نهایت مشاهده شد که پروتکل پیشنهادی به اندازه مقدار $(2m-1)L_{ID}+(2m-1)*L_{aK}+(2m-1)L_{TS}+(3m-2)*L_{MAC}$ بایت در پهنای باند شبکه صرفه‌جویی می‌کند. که این صرفه‌جویی در پهنای باند، به دلیل کاهش مصرف توان رادیوئی گره حسگر باعث کاهش مصرف انرژی گره حسگر به میزان قابل توجهی می‌شود. علاوه بر این، پروتکل پیشنهادی امکان توزیع محاسبات را نیز به گره‌های حسگر می‌دهد.

۷- مراجع

[1] Gupta, P. and Kumar, P. "The capacity of wireless networks". 2000, Vols. IT-46(2), pp. 388–404.
[2] Bohge, M. and Trappe, W. "An Authentication Framework for Hierarchical Ad Hoc sensor networks" 2003.
[3] S. Zhu, S. Setia, S. Jajodia ,"LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks",June 14, 2004
[4] Q. Huang, H. Kobayashi, B. Liu, "An Unbalanced Key Establishment Scheme for Heterogeneous Wireless Networks",IEEE Communications Society, Globecom 2004
[5] S. Zhao, K. Tepe, I. Seskar, and D. Raychaudhuri, "Routing protocols for self-organizing hierarchical ad-hoc wireless networks," in *IEEE Sarnoff 2003 Symposium.*
[6] A. Perrig, R. Canetti, J.D. Tygar, D. Song,"The TESLA Broadcast Authentication Protocol",UC Berkeley and IBM Research
[7] A. Perrig, R. Canetti, J.D. Tygar, D. Song,"Timed Efficient Stream Loss-Tolerant Authentication (TESLA):Multicast Source Authentication Transform Introduction" , RFC 4082
[8] Perrig, A., et al. "Efficient and Secure Source Authentication for Multicast", 2000