جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد
Archvie of SID

ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

ارائه گونه امن یک پروتکل همزمانی در شبکه‌های حسگر بی‌سیم

زهرا احمدی، مهدی برنجکوب

اصفهان، دانشگاه صنعتی اصفهان، دانشکده برق و کامپیوتر

z.ahmadi@ec.iut.ac.ir
brnjkb@cc.iut.ac.ir

چکیده

در شبکه‌های حسگر بی‌سیم، همزمانی بین گره‌ها اهمیت زیادی دارد. این اهمیت هم در مورد کاربردهایی که مستقیماً به زمان وابسته اند مانند برنامه ریزی برای TDMA و یا تعقیب شیء و هم برای کاربردهایی که از زمان به منظور سهولت انجام کار استفاده می‌کنند مانند برخی پروتکل‌های امنیتی مطرح است. در بیشتر پروتکل‌های موجود برای همزمانی در شبکه حسگر، محیط شبکه امن در نظر گرفته شده است؛ یعنی به خطر حملات بدخواهانه در محیطهای ناامن واقعی توجه نشده است. حملات مذکور می‌توانند مانع همزمانی صحیح شده و هر دو دسته از کاربردها را دچار مشکل نمایند. در دسته‌ای از حملات که حملات خارجی نامیده می‌شوند، دشمن گره‌ای را در اختیار ندارد. در دسته‌ای دیگر برخی گره‌ها توسط دشمن تسخیر می‌شوند که به آنها حملات داخلی اطلاق می‌گردد. در این مقاله ضمن معرفی یکی از پروتکلهای مطرح برای همزمانی شبکه‌های حسگر، پروتکل PBS، برای نخستین بار گونه‌ای امن از این پروتکل ارائه می‌شود. در ادامه ملاحظه می‌شود که پروتکل مذکور نسبت به هر دو نوع حمله داخلی و خارجی امن می‌باشد. همچنین این پروتکل در حالت امن با دو روش دیگر مطرح در همزمانی امن شبکه‌های حسگر مقایسه شده و نشان داده می‌شودکه به علت تعداد پیغام کمتر، عدم نیاز به پهنای باند زیاد و همچنین عدم نیاز به همزمانی اولیه نسبت به هر دو روش کارآمدتر است.

واژه‌های کلیدی

شبکه‌های حسگر بی‌سیم، همزمانی، همزمانی امن، پروتکل PBS.

۱- مقدمه

شبکه‌های حسگر بی سیم اخیراً مورد توجه زیادی قرار گرفته‌اند. به دلیل کاربرد گسترده آن‌ها در تعقیب هدف، مشاهده اتفاقات بویژه در محیطهای خطرناک و... نیاز به ساعت دقیق و هماهنگ بین گره‌ها ضروریست. مثلاً در تعقیب شیء، حسگرها به زمان و مکان شیء هنگام حس کردن آن نیاز دارند تا بتوانند به درستی سرعت و جهت حرکت آن را مشخص کنند ویا در مشاهده اتفاقات، وقتی چند حسگر واقعه ای را گزارش می‌کنند از روی زمان وقوعی که هر کدام گزارش داده‌اند می‌توان دریافت که آیا واقعه یکسانی را گزارش می‌کنند یا چندین واقعه مجزا اتفاق افتاده است. شاید یکی از راه حل‌های ممکن، همزمان شدن حسگرها با یک مرجع خارجی توسط سیستم GPS باشد. ولی GPS نیاز به دید مستقیم از آسمان دارد و در داخل ساختمان، زیر برگ درختان، زیر آب و... یا هنگامی که کانال GPS مسدود شود قابل استفاده نیست. ضمناً گیرنده GPS[۲۹۷] بزرگ، هزینه‌بر و مستلزم صرف انرژی است که در حسگرهای ارزان و کوچک کاربرد ندارد.

به دلیل محدودیت انرژی حسگرها، ماهیت پویای توپولوژی شبکه، محیط ناامن بی‌سیم و... پروتکل‌های قدیمی همزمانی مانند NTP[۲۹۸] که به راحتی در شبکه‌های غیر بی‌سیم قابل اجرا می‌باشند، نمی توانند مستقیماً در شبکه حسگر بی‌سیم استفاده شوند. چندین پروتکل برای همزمانی به صورت دوتایی یا به صورت گروهی در شبکه‌های بی‌سیم پیشنهاد شده است. برای همزمانی دوتایی نیز دو روش وجود دارد. روش فرستنده – گیرنده (SRS) و روش فقط گیرنده (ROS). در روش فرستنده – گیرنده که مثالی از آن TPSN [۱] است یک گیرنده با یک فرستنده ارتباط برقرار می‌کند تا اختلاف زمانی خود با آن

[297] Global Positioning System

[298] Network Time Protocol

جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

Archive of SID

فرستنده را به دست آورد. TPSN مبتنی بر ساختار سلسله مراتبی است و شبکه را از طریق مبادله پیغام‌های همزمانی جفتی در هر یال درخت سلسله مراتبی، همزمان می‌کند. درروش فقط گیرنده که مثالی از آن RBS [۲] است، یک گره مرجع بسته ای را همه پخشی می‌کند و گره‌های دیگر زمان رسیدن این بسته بر حسب ساعت خود را به دست آورده و با هم مبادله می‌کنند. بدین ترتیب از اختلاف ساعت هنگام ورود بسته، میزان اختلاف زمان خود را با هم بدست می‌آورند.

پروتکل PBS[۲۹۹] [۳] با هدف کاهش تعداد پیغام‌های همزمانی لازم و در نتیجه کاهش مصرف انرژی در شبکه حسگر طراحی شده است.PBS مبتنی بر این ایده است که هنگامی که دو گره به روش فرستنده – گیرنده به مبادله پیغام‌های هم زمانی می‌پردازند، گره‌های دیگری که در نزدیکی آن دو گره واقع شده اند با شنیدن این پیغام‌ها، همزمان شوند. در واقع این روش ترکیبی از روشهای فرستنده- گیرنده و فقط گیرنده است که به طور قابل توجهی تعداد پیغام‌های مبادله شده را کاهش می‌دهد.

پروتکل‌های مورد استفاده برای همزمانی شبکه‌های حسگر دارای برخی ضعف‌های امنیتی می‌باشند که می‌تواند توسط دشمن برای ایجاد اخلال در همزمانی مورد سوء استفاده قرار بگیرد.

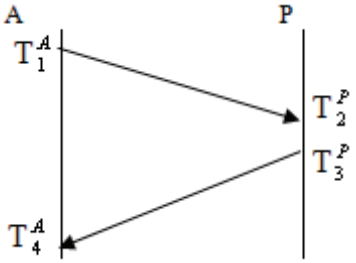
در روش همزمانی امن مبتنی بر سطح[۴] از هر پیغام توسط کلیدهای مشترک دوتایی میان گره‌ها، MAC گرفته می‌شود و به همراه پیام ارسال می‌گردد تا صحت پیام‌ها برای گیرنده محرز شود. در این روش به دلیل تک‌پخشی بودن، تعداد پیغام‌ها زیاد است. در روش Tinysersinc [۵] از روش تسلا[۳۰۰] [۶] برای احراز اصالت پیغام‌های همه پخشی همزمانی استفاده می‌شود که نیاز به همزمانی اولیه میان گره‌ها دارد.

هدف اصلی در این مقاله ارائه روشی مشابه تسلا برای احراز اصالت پیغامهای همه پخشی همزمانی است. در این روش از زنجیره کلید یک طرفه استفاده می‌شود بدون اینکه مانند تسلا نیاز به افشای کلید و یا نیاز به همزمانی اولیه داشته باشد.

ساختار این مقاله به این صورت است که در بخش دوم ابتدا پروتکل PBS معرفی می‌شود و حالت گسترش یافته آن برای همزمان کردن کل شبکه مطرح می‌گردد[۵] [۷]. در بخش سوم مخاطرات امنیتی این پروتکل بررسی شده و راه حلی برای امن کردن آن ارائه می‌شود. در بخش چهارم این پروتکل در حالت امن با دو پروتکل موجود دیگر برای همزمانی امن، مقایسه می‌گردد.

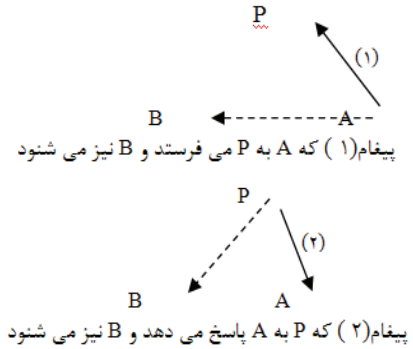
۲- پروتکل PBS

فرض کنید گره A می‌خواهد با گره P همزمان شود و سایر گره‌ها در محدوده ارسال این دو گره قرار دارند. طبق شکل ۱، A برای P پیغامی مبتنی بر درخواست زمان می‌فرستد. P زمان ورود درخواست به خودT$_2^P$ و زمان خروج پاسخ از خود T$_3^P$ را در جواب برای A می‌فرستد این پاسخ درزمان T$_4^A$ به A می‌رسد. T$_1^A$ و T$_4^A$ بر حسب زمان A و T$_2^P$ و T$_3^P$ بر حسب زمان P هستند.



شکل ۱: مبادله پیامهای همزمانی در حالت فرستنده- گیرنده

این مبادله پیغام‌ها N بار تکرار می‌شود و اختلاف ساعت[۳۰۱] و اختلاف فرکانس[۳۰۲] بین A و P به روش فرستنده – گیرنده که در [۸] معرفی شده به دست می‌آید.



شکل ۲: گره شنونده

حال فرض کنید گره دیگری مانند B این پیغام‌ها را می‌شنود. طبق شکل ۲، B پیغام A را دریافت و زمان ورود آن به خود را ثبت می‌کند. همچنین پاسخی را که P به A داده است را نیز دریافت و زمان ورود آن را نیز ثبت می‌کند. زمان رسیدن پیغام A به P را نیز از این پیغام استخراج می‌کند. حال مسئله به مسئله فقط گیرنده تبدیل می‌شود. A نقش گره مرجعی را بازی کرده است که پیغام را همه‌پخشی می‌کند و B و P گیرندگان آن بوده‌اند. P زمان دریافت پیغام از A را برای B فرستاده است. حال B این زمان را با زمانی که خودش پیغام A را دریافت کرده مقایسه و از روی آن اختلاف ساعت خود با P را بدست می‌آورد. تکرار این پیغام‌ها باعث می‌شود B قادر باشد میزان اختلاف فرکانس خود با P را نیز به دست آورد. همچنین فرایند تکرار باعث حذف اثر تأخیرهای تصادفی در بین راه می‌شود. در مبادله پیغامها در شبکه حسگر چهار نوع تأخیر وجود دارد:

[299] Pairwise Broadcast Synchronization

[300] Timed Effcient Stream Loss-tolerant Authentication

[301] Offset

[302] Skew

جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

Archvie of SID

- تأخیر در ارسال که زمان مربوط به ساخته شدن پیام در فرستنده است.
- تأخیر دسترسی به کانال
- تأخیر انتشار پیغام
- تأخیر دریافت، یعنی فاصله زمانی که واسطه شبکه گیرنده پیغام را از کانال می‌گیرد و به میزبان خبر دهد که پیغام رسیده است.

وقتی از همه پخشی استفاده می‌شود دو تأخیر اول برای همه گیرندگان در مورد یک پیغام خاص، یکسان است. زمان انتشار نیز به دلیل سرعت بالای سیگنال که تقریباً نزدیک سرعت نور است و فواصل نه چندان زیاد حسگرها (حدود چند متر) در حد چند ده نانوثانیه است که قابل اغماض است. همچنین آنچه در روش فقط گیرنده مهم است تفاوت در زمان انتشار پیغام است که از مقدار مذکور نیز کمتر خواهد بود. تأخیر دریافت برای گیرندگان مختلف و به ازای پیغام‌های مختلف متفاوت است. تکرار پیغام‌ها باعث حذف اثر عدم قطعیت در زمان دریافت می‌شود.

در سایر روش‌های هم زمانی مانند TPSN و RBS تعداد پیغام‌های مبادله شده متناسب با تعداد گره‌هاست. در صورتیکه در PBS این مقدار ربطی به تعداد گره شنونده ندارد و همین مسئله باعث کاهش تعداد پیام لازم برای همزمانی در مقایسه با سایر روش‌ها می‌شود.

حال مسئله‌ای که وجود دارد این است که کدام دوگره انتخاب شوند تا به صورت دوتایی فرستنده – گیرنده همزمان شوند. دو شرط اساسی در اینجا وجود دارد.۱- دو گره‌ای انتخاب شوند که بیشترین تعداد گره دیگر را به طور مشترک در محدوده ارسال خود داشته باشند.۲- دو گره نباید متعلق به یک سطح باشند. به طور خلاصه برای همزمان‌سازی کل شبکه در PBS گام‌های زیر اجرا می‌شود :

۱- ابتدا با استفاده از الگوریتم‌های انتخاب گره سردسته، یک گره مرجع انتخاب می‌شود و سطح آن صفر قرار می‌گیرد.
۲- یک پیغام کشف سطح توسط گره مرجع همه پخشی می‌شود. این پیغام شامل ID گره پخش‌کننده و شماره سطح آن است.
۳- همه گره‌هایی که پیغام کشف سطح را گرفتند سطح خود را یکی بالاتر قرار می‌دهند و خود یک پیغام کشف سطح جدید را به همه گره‌های همسایه جز گره‌ای که از آن این پیغام رادریافت کرده و پذیرفته اند (یعنی گره پدر) می‌فرستند. در هر گره پس از تعیین سطح، پیغام‌های کشف سطح بعدی رد خواهند شد.
۴- مرحله سوم تکرار می‌شود تا همه گره‌ها در شبکه دارای سطح شوند.
۵- پس از اینکه درخت سلسله مراتبی در شبکه شکل گرفت هر گره فرزند پیغام کشف اتصال را همه پخشی می‌کند و به پیغام‌های کشف اتصال سایر فرزندان هم گروه خود (یعنی فرزندانی که پدر مشترک با او دارند) پاسخ می‌دهد. گره پدر این پیغام‌های همه پخشی فرزندان و بعضاً پاسخ سایر فرزندان خود را می‌شنود و در ماتریس همسایگی خود درایه مربوط به همسایگی فرزند j (که پیغامی را همه پخشی کرده) و فرزند k (که پاسخ داده است) را یک می‌کند (Mjk=1).توجه کنید که Mjk در صورتی صفر می‌شود که پدر پیغام همه پخشی فرزند j را شنیده باشد ولی پاسخ فرزند k را نشنود. چون فرزند k ممکن است پیغام همه پخشی j را دریافت نکرده باشد. بنابراین k همسایه فرزند j محسوب نمی‌شود و در ماتریس همسایگی Mjk=0 قرار می‌گیرد.
۶- در هر گروه یک یا چند فرزند انتخاب و با پدر به صورت جفتی و به روش گیرنده – فرستنده همزمان می‌شوند. سایر فرزندان با شنیدن پیغام‌های مبادله شده‌ی پدر و فرزند خود را با پدر همزمان می‌کنند.

فرایند انتخاب فرزند برای همزمانی فرستنده – گیرنده توسط پدر به صورت زیر انجام می‌شود. فرض کنید گره i پدر گروه i ام باشد. برای هر گره j و k که عضو گروه i باشند (فرزند گره i باشند) $N_{ROS}^{i,j}$ یا تعداد همسایگان مشترک گره‌های i و j به صورت زیر محاسبه می‌شود :

$$N_{ROS}^{i,j} = \sum_{j \neq k} Mjk \qquad (۱)$$

$j \in$ گروه i

و گره $\hat{j}$ به صورت زیر انتخاب می‌شود :

$$\hat{j} = \arg\max N_{ROS}^{i,j} \qquad (۲)$$

یعنی گره‌ای که بیشترین همسایه مشترک را با گره پدر دارد. سپس پدر طی یک پیغام همه پخشی، گره $\hat{j}$ را به همه اعلام می‌کند بدین ترتیب گره $\hat{j}$ با گره پدر گروه به روش گیرنده – فرستنده همزمان می‌شوند و سایر گره‌ها که شنونده خواهند بود خود را با پدر همزمان می‌کنند. اگر پس از این مرحله هنوز گره‌ای وجود داشته باشند که همزمان نشده است فرزند دیگری برای i انتخاب و عملیات تکرار می‌شود.

۳- پیشنهاد پروتکل امن

در این قسمت ابتدا پروتکل PBS را از نظر نقاط ضعف امنیتی موجود در آن بررسی می‌نماییم. آنگاه به ارائه راه حل خود برای امن‌سازی آن خواهیم پرداخت. سپس تغییرات ایجاد شده برای امن نمودن این پروتکل را بررسی می‌نماییم.

Archive of SID

۳-۱ ضعفهای امنیتی PBS

همانطور که اشاره شد همزمانی درPBS از طریق پیغام‌های (۱)و(۲) انجام می‌شود. پیغام (۱) را فرزندA به پدر می‌فرستد که شامل برچسب زمانی T_1^A است. فرزندان دیگر مثلB نیز این پیغام را می‌شنوند. پدر در پیغام (۲) زمان دریافت پیغام (۱) و زمان خروج پاسخ از خود را برای A می‌فرستد وB نیز می‌شنود. این پیغام برچسب‌های زمانی T_2^P و T_3^P را خواهند داشت. فرض کنید B پیغام A را در ساعت ۳ به وقت خود دریافت کرده است، P نیز اعلام می‌کند که پیغام A را در ساعت ۳:۵ دریافت کرده و این پیغام را برای B می‌فرستد. B اختلاف ساعت خود تا P را برابر پنج دقیقه اندازه‌گیری می‌کند. البته این کارN بارتکرار می‌شود تا علاوه بر امکان محاسبه اختلاف فرکانس، اثر تأخیرات تصادفی نیز تعدیل شود.

مخاطرات امنیتی موجود در این پروتکل به صورت زیر است :

- ایجاد تأخیر در پیغام‌ها : این تأخیر می‌تواند در رسیدن پیغام (۱) بهP یا B یا هر دو باشد. همچنین در رسیدن پاسخ نیز می‌تواند تأخیر ایجاد شود.
- تسخیر گره‌ها : دشمن با تسخیر یک گره قادر خواهد بود پیغام‌های غلط بفرستد. اگر گره A تسخیر شود دشمن قادر خواهد بود پیغام (۱) را در زمانهای متفاوت برای P و B بفرستد و باعث بر هم زدن همزمانی در قسمت فقط گیرنده شود و چنانچه گره پدر تسخیر شود می‌تواند در پیغام (۲) به گره‌های A و B زمان اشتباهی را در مورد T_2^P یا زمان دریافت پیغام ازA، اطلاع داده و همزمانی را در هر دو قسمت فرستنده – گیرنده و فقط گیرنده دچار مشکل نماید.
- تغییر پیغام‌ها : دشمن می‌تواند برچسب‌های زمانی که درهر دو پیغام (۱) و (۲) وجود دارند را در بین راه تغییر دهد.

۳-۲ ارائه راه حل

در ابتدا گفتیم که حملات به دو دسته خارجی (تأخیر و تغییر پیغام‌ها) و داخلی (تسخیر گره‌ها) تقسیم می‌شوند. در مورد تأخیر اگر دشمن در رسیدن پیغام (۱) تأخیر ایجاد کندN بار تکرار این پیغام‌ها، اثر تأخیرات عمدی را نیز محدود می‌کند. در مورد ایجاد تأخیر در پیغام (۲)، گره A باید از روش محاسبه تأخیر که در[۴] پیشنهاد شده است استفاده کند. در این روش پارامتر تأخیر انتها به انتها در گرهA به صورت زیر محاسبه می‌شود :

$$d = \frac{(T2 - T1) + (T4 - T3)}{2} \qquad (۳)$$

اگر این مقدار از مقدار*d بیشتر باشد از این اختلاف محاسبه شده صرفنظر می‌گردد. *d بیشینه تاخیر انتها به انتها است. در[۹] نشان داده شده تاخیر انتها به انتها دارای توزیع نرمال با متوسط d_{ave} و انحراف معیار σ است و با احتمال زیاد مقدار بیشینه تأخیر از$3+ \sigma$ d_{ave} تجاوز نمی کند. با اندازه گیری (روی گره‌های Mica2) مقدار*d حدود ۷۷۱ میکروثانیه به دست آمده است. همچنین چون بزرگترین علت عدم قطعیت در محاسبه تأخیر، تأخیر دسترسی به کانال است، به منظور حذف اثر این عدم قطعیت، الصاق برچسب‌های زمانی در زیر لایه MAC انجام می‌شود.

اگر دشمن پیغام (۱) را تأخیر دهد، باعث خطا در برچسب‌های زمانی می‌شود. این حالت را می‌توان مشابه حالتی دانست که گرهP تسخیر شده باشد و برچسب زمانی غلط اعلام کند. پس می‌توان برای هر دو مسئله راه حل یکسانی ارائه داد.

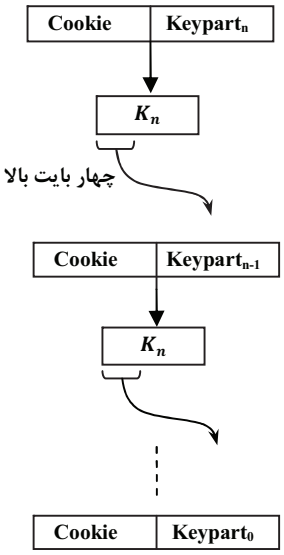
راه حل ارائه شده این است که در فاز جستجوی سطح هر فرزند به جای عضویت در یک گروه در3t+1 گروه عضو شود تا در صورت تسخیرt پدر، فرزند همچنان قادر باشد با میانه گیری روی مقادیر به دست آمده از 3t+1 پدر، زمان صحیح را به دست آورد.[۴] دلیل این امر این است که حتی اگر مقدار میانه به دست آمده مربوط به گره پدر تسخیر شده‌ای باشد، این مقدار در میانه دو مقداری که توسط گره‌های پدر تسخیر نشده اعلام شده قرار دارد و بنابر این مقدار خطای آن کم است.

برای مقابله با تغییر پیغام‌ها باید از کدهای احراز اصالت پیام (MAC) استفاده شود. واضح است که این احراز اصالت در حالت همه پخشی باید انجام گیرد تا همه گیرندگان قادر به احراز اصالت پیام‌ها باشند. در این مورد چنانچه بخواهیم از روش تسلا [۶] استفاده نمائیم نیاز به همزمانی اولیه خواهیم داشت که در اینجا ممکن نیست. زیرا مسئله اصلی رسیدن به همزمانی است.

راه حل پیشنهادی استفاده از زنجیره کلید یک طرفه‌ی شکل۳، مشابه تسلا، توسط پدر هر گروه است.در این زنجیره در فرستنده، هر کلید با استفاده از کلید قبلی ساخته می‌شود و در موقع استفاده، کلیدهای زنجیره از آخر به اول استفاده می‌شوند. تفاوت این روش با تسلا این است که کلید فاش نمی شود بلکه هر کلید از دو بخش cookie(ثابت)+keypart (متغیر) تشکیل شده است. بخش متغیر چهار بایت با وزن بالای کلید قبلی در زنجیره کلید یک طرفه است و بخش ثابت یک عدد با طول مورد نیاز مثلاً ۹۶ بیت است که توسط پدر گروه انتخاب می‌شود و قبل از مبادله پیغام‌های همزمانی توسط کلیدهای مشترک دوتایی که بین پدر و هر یک از فرزندان وجود دارد، رمز شده و به صورت تک پخشی برای هر فرزند ارسال می‌شود. به همراهcookie, $keypart_0$ و تعداد کلیدهای ساخته شده با استفاده از این cookie نیز به صورت رمز شده فرستاده می‌شود. پس از استفاده از همه کلیدهای ساخته شده، cookie جدیدی توسط پدر اعلام می‌شود. حال همه فرزندان cookie و $keypart_0$ را دارند. پدر برای ارسال هر پیغام، MAC آن پیغام را با استفاده از کلیدk_i (کلید مربوط به پیام‌iام) محاسبه و همراه پیغام ارسال می‌کند. ضمناً$keypart_i$ هم ارسال خواهد شد. هر فرزند

Archvie of SID

با دریافت پیغام (۲) ابتدا با استفاده از $keypart_i$ موجود درپیغام و cookie موجود در نزد خود، این دو را در کنار هم قرار داده و مقدار درهم آن را حساب می‌کند. اگر چهار بایت بالای کلید به دست آمده با $keypart_{i-1}$ که در پیغام قبلی فرستاده شده بود یکسان باشد کلید صحیح است.



شکل ۳: زنجیره کلید یک طرفه

آنگاه فرزند از پیغام دریافتی با استفاده از کلید محاسبه شده MAC می‌گیرد و باMAC دریافتی مقایسه می‌کند. در صورت تطابق صحت پیغام محرز می‌شود. واضح است کس دیگری جز پدر گروه که زنجیره کلید را تولید کرده است نمی‌تواندkeypart صحیحی بفرستد که پس از ساختن کلید با استفاده از آن، چهار بایت بالای کلید همان keypart قبلی شود.

گفتیم که پیغام (۱) که توسط یکی از فرزندان برای پدر ارسال می‌شود نیز دارای برچسب زمانی است و بنابراین امکان تغییر آن توسط دشمن وجود دارد. فرزندی که می‌خواهد پیغام (۱) را بفرستد از آن با کلید حاصل از $cookie+keypart_o$, MAC گرفته و ارسال می‌نماید. بدین‌ترتیب سایر فرزندان شنونده و پدر گروه قادر خواهند بود صحت این پیغام را بررسی نمایند.

فرزندان تعداد کلیدهای ساخته شده با این cookie توسط پدر را می‌دانند. پس از استفاده از همه کلیدهای ساخته شده، cookie جدیدی توسط پدر اعلام می‌شود.

۳-۳ مقایسه باPBS

درPBS امن در مقایسه باPBS تغییرات زیر ایجاد شده است:

- فازهای کشف سطح و کشف اتصالات و انتخاب فرزند مناسب مانندPBS است. تنها نیاز است که پدرcookie و$keypart_o$ را برای تک تک فرزندان توسط کلید دوبه‌دو مشترک، رمزگذاری نموده و برای آن‌ها ارسال کند.
- به همراه هر پیغام یکMAC ۱۲۸ یا۱۶۰ بیتی فرستاده می‌شود.
- در گیرنده ابتدا کلید ساخته می‌شود و اعتبار آن بررسی می‌گردد. آنگاه با استفاده ازآن، مقدار MAC پیغام محاسبه می‌شود و با MAC دریافت شده مقایسه می‌شود.

۴- تحلیل مقایسه‌ای امنیت و کارآمدی پروتکل پیشنهادی

برای مقایسه PBS امن با سایر روش‌های همزمانی امن موجود، فاکتورهای متفاوتی را باید در نظر بگیریم و هم جنبه امنیتی و هم جنبه کارایی را مد نظر قرار دهیم. دیگر روش‌های امن موجود، همزمانی مبتنی بر سطح[۴] وTinysersync [۵] هستند.

۴-۱ تحلیل امنیتی

حملات خارجی دسته‌ای از حملات ممکن به پروتکل‌های همزمانی هستند. در این حملات دشمن گره مجازی را در اختیار ندارد. تنها پیغام‌های گره‌ها را در بین راه می‌شنود و می‌تواند آنها را تغییر دهد یا در رسیدن آنها به مقصد تأخیر ایجاد نماید. پروتکل امن پیشنهادی در مقابل تأخیر مقاوم است. در قسمتی از پروتکل که روش فرستنده-گیرنده اجرا می‌شود با مقایسه تأخیر محاسبه شده با *d یا مقدار بیشینه تأخیر مجاز و با صرف نظر از مقادیر خارج از این محدوده، اثر تأخیرات عمدی به حداقل می‌رسد. در بخش فقط گیرنده نیز N بار تکرار پیام، موجب حذف اثر تأخیرات عمدی یا تصادفی می‌شود. زیرا دشمن به آسانی نمی‌تواند همه N پیام را تأخیر دهد. حتی در این صورت نیز به علت استفاده از مکانیزم افزونگی و تغییر مرجع همزمانی(گره‌های در حال همزمانی به صورت فرستنده-گیرنده) و با میانه‌گیری روی مقادیر به دست آمده از مراجع مختلف، پروتکل نسبت به تأخیر عمدی امن خواهد شد.

دسته دوم حملات ممکن به پروتکل‌های همزمانی، حملات داخلی هستند. یعنی حملاتی که دشمن با تسخیر تعدادی از گره‌ها، با استفاده از هویت آنها و یا کلیدهای مربوط به آنها، پیغام‌هایی به ظاهر مشروع ولی حاوی برچسبهای زمانی غلط می‌فرستد. افزونگی پیشنهاد شده باعث می‌شود همانند روش روش همزمانی امن مبتنی برسطح در صورت تسخیر یک سوم گره‌ها توسط دشمن، فرآیند همزمانی همچنان به درستی ادامه یابد.

برای انجام حمله جستجوی کامل به روش پیشنهادی، اگر طول کلید (t) برابر با طول cookie+keypart باشد فضای جستجو به اندازه cookie یعنی2^{t-32} عمل خواهد بود. اینکه دشمن دچار آژیر غلط بشود نیز مشکلی را حل نمی‌کند! چون دشمن می‌تواند در مراحل مختلف شکل ۳، عمل بررسی آژیر غلط (cookie اشتباه) را بررسی کند. یعنی با به دست آوردن یک مقدار تصادفی صحیح برای کلید در یک مرحله، صحت cookie به دست آمده را در مرحله بعد بررسی نماید.

Archive of SID

اگر چه روش پیشنهادی نسبت به روش تسلا با طول کلید t و فضای جستجوی 2^t، دارای فضای جستجوی کمتری است ولی نیاز به پهنای باند کمتر نسبت به تسلا برای انتقال کلید بیشتر مشهود است. یعنی در اینجا نوعی مصالحه میان امنیت کلید و طول پیام وجود دارد. ضمن اینکه برای افزایش فضای جستجو می‌توان طول cookie را افزایش داد و چون cookie یکبار ارسال می‌شود این کار پهنای باند مصرفی را افزایش نمی‌دهد.
نیاز به کلیدهای مشترک دوتایی میان گره‌ها که در این پروتکل برای رمز کردن بخش ثابت کلید استفاده شده است در دو روش دیگر مورد مقایسه نیز وجود دارد و از این جنبه هر سه پروتکل مشابه هستند.

۴-۲ تحلیل کارآمدی

در اولین روش از روشهای مورد مقایسه یعنی روش همزمانی مبتنی بر سطح، پس از ساخت درخت سلسله مراتبی در شبکه، هر گره فرزند با گره پدر به صورت تک پخشی ارتباط برقرار کرده و به مبادله برچسب‌های زمانی می‌پردازند. همراه هر پیغام نیزMAC آن با استفاده از کلیدهای مشترک دوتایی فرستاده می‌شود. سربار زیاد حاصل از ارتباط تک‌پخشی هر فرزند با پدر که با افزایش تعداد فرزندان به طور خطی افزایش می‌یابد از معایب این روش است. در حالی که در PBS امن از ماهیت همه‌پخشی پیام‌ها استفاده می‌شود و افزایش تعداد گره شنونده باعث افزایش پیغام‌های همزمانی نمی‌گردد.

در روش دوم از روش تسلا برای احراز اصالت برچسب‌های زمانی استفاده می‌شود که نیاز به یک همزمانی اولیه بین گیرندگان و فرستندگان دارد و عیب بزرگ این روش نیز همین است. همچنین در روش تسلا به همراه هرMAC (یا به ازای چندین MAC) یک کلید ۱۲۸ یا ۱۶۰ بیتی ارسال می‌شود و در روش PBS امن تنها بخش متغیر کلید که چهار بایت است ارسال خواهد شد. بنابر این پهنای باند مصرفی در روش PBS امن به مراتب کمتر از روش دوم است. ضمناً در این روش نیز مانندPBS امن، مقدار کلید اولیه باید توسط کلیدهای مشترک دوتایی رمز شود و برای گیرندگان به صورت تک‌پخشی فرستاده شود. در جدول ۱ ویژگی‌های این سه روش با هم مقایسه شده‌اند.

جدول ۳: مقایسه کارآمدی چند پروتکل همزمانی امن

روش همزمانی	پهنای باند مصرفی به ازای هر پیام	تعداد پیامها	نیاز به همزمانی اولیه	نیاز به ارسال مقدار اولیه
همزمانی مبتنی بر سطح	کم	زیاد	-	-
Tinysersinc	زیاد	کم	×	×
PBS امن	متوسط	کم	-	×

۵- نتیجه‌گیری

در این مقاله گونه امنی از پروتکل PBS برای برقراری همزمانی در شبکه‌های حسگر پیشنهاد شد و این پروتکل با سایر روش‌های همزمانی امن موجود مقایسه گردید. در PBS امن، تعدادی از حسگرها می‌توانند تنها با شنیدن پیغام‌های همزمانی که بین جفت‌هایی از گره‌های دیگر مبادله می‌شود و بررسی صحت این پیغام‌ها، همزمان شوند. مزیت این روش نسبت به سایر روش‌های موجود، تعداد پیغام کمتر، عدم مصرف پهنای باند زیاد به ازای هر پیام و عدم نیاز به همزمانی اولیه می‌باشد.

مراجع

[1] Ganeriwal S., Kumar R., and Srivastava M. B., "Timing-sync protocol for sensor networks", in Proceedings of the1stInternational Conference on mbeddedNetworked Sensor Systems (SenSys '03), pp. 138–149, ACM Press, Los Angeles, Calif, USA, November 2003.

[2] Elson J., Girod L., and Estrin D., "Fine-grained network time synchronization using reference broadcasts", in Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI '02), pp. 147–163, Boston, Mass, USA, December 2002.

[3] Noh K.-L. and Serpedin E., "Pairwise broadcast clock synchronization for wireless sensor networks", in Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '07), pp. 1–6, Helsinki, Finland, June 2007.

[4] SUN K., NING P., AND WANGC, "Secure and resilient clock synchronization in wireless sensor networks", In IEEE Journal on Selected Areas in Communications, Vol. 24, NO. 2, pp. 395- 408, February2006.

[5] SUN K., NING P., AND WANG C, "Tinysersync: secure and resilient time synchronization in wireless sensor networks", In Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06), ACM Press, Pages: 264 – 277, Alexandria, Virginia, USA,2006.

[6] Perrig A, "The TESLA broadcast authentication protocol," RSA CryptoBytes, vol. 5, no. 2, pp. 2–13, 2002.

[7] Noh K.-L., Wu Y.-C., Qaraqe K AND Suter BW, "Extension of pairwise broadcast clock synchronization for multicluster sensor networks", EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 286168, 10 pages,2008.

[8] Noh K.-L., Wu Y.-C., Qaraqe K., and Serpedin E., "Time synchronization for wireless sensor networks", in Adaptive Signal Processing for Wireless Communications, M.Ibnkahla, Ed., CRC Press, 2008.

[9] GANERIWAL S., POPPER C., CAPKUN S.AND SRIVASTAVA M., "Secure time synchronization in sensor networks", ACM Transactions on Information and System Security (TISSEC), Vol.11, Issue 4, New York, NY, USA, July 2008.