امنیت در شبکه های حسگر بی سیم با رمز نگاری

پویان صالحی [۱]، اسماعیل ملک زاده سرایی[۲]،آزیتا رستمی[۳].فانوس پرنگ[۴]

۱و۴ گروه مهندسی کامپیوتر، موسسه آموزش عالی علوم و فناوری آریان، امیر کلا بابل

۲و۳ گروه مهندسی کامپیوتر، دانشکده علامه محدث نوری،نور

چکیده:

شبکه های حسگر بی سیم (WSN) شامل گره های کوچک است که با سنجش، محاسبات و قابلیت های ارتباط بی سیم در محیطی فیزیکی بر پا می شوند. سنسور ها با فاصله در محیط پخش شده اند و کاربرد های ویژه ای در زمینه های پزشکی ،نظامی، کشاورزی،محیط زیست و... دارند. این شبکه ها محیط های پویا را نظارت می کنند که در طول زمان به سرعت تغییر می کنند. انتظار میرود که نقشی اساسی در عصر آینده محاسبات فراگیررا بازی کرده و راه را برای بسیاری از زمینه ها باز کند. با توجه به محدودیت های سنسورها آنها در محاسبات، حافظه، منابع انرژی و امنیت ضعیف هستند. ارتباطات بی سیم این شبکه ها امنیت را به یک چالش تبدیل می کند در نتیجه امنیت باید عامل مهمی باشد که به آن پرداخته شود. دراین مقاله، ما در حال ارائه روشی برای حل مشکل امنیتی در این شبکه ها با استفاده از رمزنگاری به وسیله یک پروتکل جدید هستیم.

کلمات کلیدی: شبکه های حسگر بی سیم، امنیت، رمزنگاری

۱. مقدمه

امروزه زندگی بدون ارتباطات بی سیم قابل تصور نیست .پیشرفت تکنولوژی و ایجاد مدارهای کوچک و کوچکتر باعث شده است تا استفاده از مدارهای بی سیم در اغلب وسایل الکترونیکی امروز ممکن شود .این پیشرفت همچنین باعث توسعه حسگرها شده است. توسعه مداوم این شبکه های خاص منجر به ادغام و استفاده آن در مناطقی شده است که خیلی متفاوت است. شبکه حسگر بی سیم در مکان هایی که انسان در آنجا نمی تواند حضور مستمر داشته باشد استفاده بسیار پر کاربردی دارد. سنسورها برای برنامه های مختلف، از جمله نظامی، نظارت بر حیات وحش، ردیابی وسایل نقلیه و تشخیص مراقبت های بهداشتی و... کاربرد ویژه ای دارند[1]. یک مزیت عمده این شبکه ها توانایی بی سابقه آنها برای کشف و درک داده های دنیای واقعی و پدیده ها در یک سطح دقیق از تفکیک زمانی و مکانی در مقیاس های بزرگ می باشد. همانطور که حسگرهای مختلف ظهور می کنند و فناوری های مرتبط با آن پیش می روند، افزایش قابل ملاحظه ای برای امنیت این شبکه ها صورت گرفته است. ارائه سرویس کاربردی در این شبکه ها ، چالش های امنیتی قابل توجهی را برای طراحان این شبکه به ارمغان می آورد یک چالش مهم به دست آوردن ارتباطی امن و معتبر بین کاربران و سنسورها و جلوگیری از دسترسی غیرقانونی به اطلاعات حسگر و انتقال آنها توسط هکرها است.روش پیشنهادی ما برای حفظ داده های ارسالی در شبکه حسگر بی سیم استفاده از رمز نگاری می باشد.رمزنگاری شامل کدهای نوشته شده یا تولید شده

است که اجازه می دهد اطلاعات را مخفی نگه دارد. رمزنگاری داده ها را به یک فرمت غیر قابل خواندن برای یک کاربر غیر مجاز تبدیل کند و اجازه نمی دهد بدون هیچ گونه رمزگشایی آن به یک فرمت قابل خواندن تبدیل شود. امنیت اطلاعات از رمزنگاری در سطوح مختلف استفاده می شود. اطلاعات را نمی توان بدون کلید برای رمزگشایی آن خواند. اطلاعات در حین حمل و نقل ذخیره می شود و یکپارچگی آن را حفظ می کند. رمزنگاری همچنین اجازه می دهد تا فرستنده ها و گیرنده ها را با استفاده از جفت های کلیدی به یکدیگر اعتبار دهی کنند. الگوریتم های مختلفی برای رمزگذاری وجود دارد، برخی از الگوریتم های رایج عبارتند از:

رمزنگاری کلید مخفی[1](SKC) در اینجا فقط یک کلید برای رمزنگاری و رمزگشایی استفاده می شود. این نوع رمزگذاری همچنین به عنوان رمزنگاری متقارن نامیده می شود.[2]

رمزنگاری کلید عمومی[2](PKC) در اینجا دو کلید استفاده می شود. این نوع رمزگذاری نیز رمزگذاری نامتقارن نامیده می شود. این نوع رمز نگاری یک کلید عمومی است و هر کسی می تواند به آن دسترسی داشته باشد. کلید دیگر کلید خصوصی است و تنها مالک می تواند به آن دسترسی پیدا کند. فرستنده اطلاعات را با استفاده از کلید عمومی گیرنده رمزگذاری می شود. گیرنده پیام را با استفاده از کلید خصوصی خود رمزگشایی می کند. برای عدم لغو، فرستنده متن ساده را با استفاده از کلید خصوصی رمزگذاری می کند، در حالی که گیرنده از کلید عمومی فرستنده برای رمزگشایی آن استفاده می کند. بنابراین، گیرنده می داند که چه کسی آن را فرستاده است.[3]

باید در نظر داشت که معیار اصلی قدرتمند بودن یک الگوریتم رمزنگاری ربطی به وجود احتمال شکستن آن ندارد، زیرا در صورتی که مقدار کافی از جفت متن آشکار و متن رمزنگاری شده در اختیار باشد، هر الگوریتم رمزنگاری بالاخره شکسته خواهد شد .قدرت اصلی هر الگوریتم رمزنگاری امکان اجرای آن در یک زمان قابل قبول است .متنی که امکان شکسته شدن آن بعد از سالها، آن هم با شبکه ای از سوپرکامپیوترها وجود دارد، در حقیقت بسیار امن است. سیستم های رمزنگاری اولیه برای حفظ امنیت به محرمانه ماندن الگوریتم رمزنگاری بسیار وابسته بودند .به تدریج الگوریتمهای رمزنگاری بر مشکل وابستگی به طول کلید و محرمانگی آن غالب آمده اند .امروزه قابل اطمینان ترین الگوریتم های رمزنگاری ناچارند از پس چندین نوبت تحقیق موشکافانه و غیرمحرمانه به خوبی برآیند تا بتوانند اعتماد سازمان ها و مشتریان را جلب کنند .طبیعتاً بسیار سخت است که الگوریتم های رمزنگاری قابل اطمینان ایجاد کرد و آنها را به صورت عمومی و غیر محرمانه مورد آزمایش قرار داد. انتخاب کلید ضعیف یا محافظت نامناسب از آن راه را برای ورود نفوذگران باز می کند .در صورتی که یک نفوذگر به یک کلید رمزنگاری دسترسی پیدا کند، حتی قویترین الگوریتم های رمزنگاری نیز قادر به حفاظت از داده های مورد نظر نیستند.

۲. سرویس‌های امنیتی

در این قسمت فرضیات خود را براساس ساختار شبکه‌های بی‌سیم سنسوری ارائه خواهیم کرد و همینطور زیرمجموعه‌ای از ۴ سرویس امنیتی که از PKCبهره می‌برد را تعریف خواهیم کرد.

شبکه‌های سنسوری معمولا شامل تعدادی از نودها است که با استفاده از ایستگاه اصلی[3] با یکدیگر ارتباط برقرار می‌کند[4]. اسیتگاه اصلی اطلاعات را از نودها دریافت می‌کند و به دنیای خارج ارسال می‌کند. نودهای سنسوری دارای

[1] Symmetric Key Cryptography Algorithms
[2] public key cryptography
[3] Bus station

توان یا انرژی کمی هستند و تنها می‌توانند با نودهای نزدیک به خود ارتباط برقرار کنند. ایستگاه اصلی اینگونه فرض می‌شود که دارای توان کافی برای ارتباط با سایر نودها و ارتباط با دنیای خارج است.

۳. احراز هویت پخشی

در این سناریو، ایستگاه اصلی ابتدا پیامی را برای تمامی نودها ارسال خواهد کرد و هر نود باید اصالت خود را تایید کند. این سناریو کاربردی ساده از PKC است. تمامی نودها، باید کلید عمومی نود ایستگاه اصلی را داشته باشند. اطلاعاتی که توسط دشمن و از طریق آلوده کردن نودهای سنسوری بدست می‌آید نباید شامل اطلاعات مفیدی باشد. روش‌هایی که اخیرا به چاپ رسیده‌اند یا نیازمند مقدار زیادی اطلاعات برای ارسال هستند و یا دارای روش توزیع کلید متقارن پیچیده‌ای هستند[5].

۴. رمزنگاری اطلاعات:

رمزنگاری اطلاعات با استفاده از PKC بسیار گرانتر از رمزنگاری با کلید مخفی است. با این حال در مواردی که کلید پنهان(منظور استفاده از رمزنگاری متقارن) تولید نشده است استفاده از PKC کارآمد است. که یکی از این موارد، توزیع کلید نود به نود است که در ادامه توضیح داده می‌شود.

۴-۱ توزیع کلید نود به نود:

کاربرد ساده‌ی PKC ،توزیع کلید و توافق کلید است. توافق کلید به پروتکلی گفته می‌شود که دو طرف، باهم کلیدی را تولید می‌کنند در حالی که توزیع کلید پروتکلی است که در آن یک طرف کلیدها را به صورت امن به طرف‌های دیگر ارسال می‌کند. اینجا فرض می‌کنیم که هر نودی کلید عمومی نود همسایه‌ی خود را می‌داند. کلید خصوصی، می‌تواند در فاز راه‌اندازی و یا با درخواست از ایستگاه اصلی توزیع شود. اگر دو نود بخواهند که کلید نشستی را ایجاد کنند، یک نود می‌تواند اینکار را با استفاده از کلید عمومی نود همسایه رمز کرده و به او ارسال کند. برخلاف روش‌های دیگر، ایستگاه اصلی دیگر درگیر این تراکنش نمی‌شود که موجب کاهش اتلاف توان می‌شود.

۴-۲افزودن نود جدید:

در هر زمانی ممکن است که نودهای قانونی جدیدی به هر قسمت از شبکه افزوده شود. در این وضعیت استفاده از PKC دوباره کارآمد است. هر نود دارای جفت کلید عمومی و خصوصی خود و کلید عمومی ایستگاه اصلی است. کلید عمومی نود جدید را می‌توان با استفاده از ارتباطات خارجی به ایستگاه اصلی فرستاد و سپس ایستگاه اصلی با استفاده از کلید عمومی نود جدید می‌تواند کلید نشستی را برای نود جدید اختصاص داده رمز کرده و ارسال کند. یا نود می‌تواند حضور خود در شبکه را با استفاده از ارسال پیامی امضا شده به ایستگاه اصلی خبر دهد.

۵ روش پیشنهادی

روش‌های مختلف رمزنگاری کلید عمومی برای فراهم کردن سرویس‌های امنیتی فوق مورد استفاده قرار گیرد. در این پژوهش سه روش RABIN, NTRUENCCRYPT, ELLIPTIC CURVE بعنوان روش‌هایی که دارای مصرف توان کمی هستند مورد بررسی قرار گرفته است. معماری ما برای توابع رمزنگاری‌های RABI و NTRUENCRYPT و ECC در [6] گزارش شده است. برای مقایسه‌ی کیفی این الگوریتم‌ها و میزان کارآمدی آنها برای استفاده در شبکه‌های با مصرف توان بسیار پایین، مجموعه پارامترهای خاص الگوریتم را انتخاب کرده‌ایم که تقریبا دارای سطح امنیتی مشابه‌ای است. در این قسمت، از دلیل این انتخاب سخن می‌گوییم و مختصری درمورد پیده‌سازی آن‌ها سخن می‌گوییم.

روش‌های مختلف رمزنگاری کلید عمومی برای فراهم کردن سرویس‌های امنیتی فوق مورد استفاده قرار گیرد. در این پژوهش سه روش RABIN, NTRUENCCRYPT, ELLIPTIC CURVE بعنوان روش‌هایی که دارای مصرف توان کمی هستند مورد بررسی قرار گرفته است. معماری ما برای توابع رمزنگاری‌های RABIN و NTRUENCRYPT و ECC در [7] گزارش شده است.

برای مقایسه‌ی کیفی این الگوریتم‌ها و میزان کارآمدی آنها برای استفاده در شبکه‌های با مصرف توان بسیار پایین، مجموعه پارامترهای خاص الگوریتم را انتخاب کرده‌ایم که تقریبا دارای سطح امنیتی مشابه‌ای است. در این قسمت، از دلیل این انتخاب سخن می‌گوییم و مختصری درمورد پیده‌سازی آن‌ها سخن می‌گوییم.

۵-۱ انتخاب پارامتر:

زمانی‌که از تطابق سطوح امنیتی سخن می‌گوییم، فرضیات خود را بر اساس آنالیزهای لنسترا و ورهول[۶] پایه‌گذاری می‌کنیم. که این آنالیزها مربوط به انتخاب اندازه‌ی کلید انواع مختلف سیستم‌های رمزنگاری و میزان اتلاف آنها است. با این حال آنها رمزنگاری‌های مبتنی بر مشبکه مانند NTRUENCCRYPTرا مورد آنالیز قرار نداده‌اند. برای انتخاب پارامتر NTRUENCCRYPT به آنالیزهای هافشتن و سیلورمن و وایت[8] مراجعه کرده‌ایم.

با توجه به اینکه در عمل، کلاس‌های خاصی از کاربردها نیازمند سطح امنیتی بالاتری نسبت به دیگر کاربردها است با این حال ما طراحی خود را به اندازه‌ای ساده در نظر می‌گیریم که بتوانیم کارایی مورد نظر را داشته باشیم پس آنها را به صورتی پیاده‌سازی می‌کنیم که بتوانند حداقل نیازهای امنیتی را برآورده کنند. که با استفاده از آنالیزی که در پایان این مقاله انجام می‌دهیم تخمینی صحیح از پیاده‌سازی با سطوح امنیتی بالا به دست آوریم. برای روش RABIN ماژول ۵۱۲ بیتی انتخاب کرده‌ایم که با توجه به [9] سطح امنیتی ۶۰بیتی را به همراه داشته باشد. معماری ECC[4] دارای عملیات ریاضی در میدان اول با اندازه‌ی ۱۰۰ بیت است که سطح امنیتی مابین ۵۶ تا ۶۰ بیتی را فراهم می‌کند. در مورد NTRUENCCRYPT پارامترهای سیستم را (N,p,q) = (167,3,128) انتخاب کرده‌ایم که این انتخاب براساس یافته‌های [۵] است که سطح امنیتی از مرتبه‌ی ۵۷ بیت را فراهم می‌کند.

۵-۲ روش RABIN:

روش رابین در سال ۱۹۷۹ در [10] ارائه شد که این روش مبتنی بر مسئله‌ی تجزیه‌ی اعداد بزرگ است امنیتی مشابه با RSA دارد. روش رابین دارای هزینه‌ی محاسباتی همانند رمزنگاری نامتقارن است. عملیات رمزنگاری سریعتر از عملیات رمزگشایی است. نامتقارن بود این روش موجب می‌شود که برای استفاده در سناریوی شبکه‌های سنسوری که

[4] ELLIPTIVE CURVE CRYPTOGRAPHY

نودها و استگاه اصلی دارای توان محاسباتی متفاوتی هستند یکی از بهترین گزینه ها باشد. جزئیات روش رابین در [۷و۱۰] آمده است.

تابع رمزنگاری روش رابین $E_{n,b}(x)=x(x+b) \bmod n$ است اگر $b=0$ تنظیم شود این تابع تبدیل به یک تابع مربع ساده می‌شود $E_n(x)=x^2 \bmod n = y$. روش رابین برای رمزنگاری، تنها نیازمند یک مربع کردن است. رمزگشایی نیازمند پیدا کردن ریشه‌ی y است. تابع رمزگشایی $D_n= \sqrt{y} \bmod n$ که ۴ نتیجه را به همراه دارد.

جزئیات بیشتری از پیاده‌سازی توابع رمزنگاری در [11] آمده است. ما توان دوم کننده‌ای را مانند یک ضرب‌کننده‌ی بیتی سریال ساخته‌ایم که بر روی تمامی ۵۱۲ بیت ضرب‌شده و یک بیت از ضرب‌کننده در یک زمان عمل می‌کند. این رویکرد دارای مزایایی است که این واحد می‌تواند برای انجام عملیات توان رساندن که برای قسمت رمزگشایی روش رابین مورد نیاز است نیز بکاربرده‌شود. مدار ضرب‌کننده نیازمند چیپی با محدوده‌ی ۱۷۰۰۰گیت است که دارای میانگین اتلاف توان ۱۴۸,۱۸ میکرو وات است.

۳-۵ NtruEncrypt , NtruSign :

این دو روش امضا سیستم‌های رمزنگاری مبتنی بر مسئله‌ی سخت کوتاهترین بردارSVPو مسئله‌ی سخت نزدیکترین بردار CVPدر مشبکه‌های با ابعاد N=167...503است.

NtruEncrypt به طور خاص در کاربردهایی مانند کارتهای هوشمند و یا تگ‌های RFID کاربرد کارآمدی دارد با این حال دارای امنیتی قابل مقایسه با روش‌های دیگر است.

ریاضیات هردو روش مبتنی بر کانولوشن دوری در حلقه‌ی چندجمله‌ای $R=Z(x)/(x^N-1)$ است. سطوح امنیتی مختلفی را با انتخاب پارامترهای (N,p,q) می‌توان بدست آورد.

ما عملکرد NtruSign را با استفاده از اطلاعات بدست آمده از پیاده‌سازی معماری مقیاس‌پذیر NtruEncrypt خود که در [12] توضیح داده‌ایم تخمین می‌زنیم. کوچکترین پیاده‌سازی NtruEncryptبا استفاده از یک واحد ریاضیاتی نیازمند چیپی با ۳۰۰۰ گیت است که کمتر از ۲۰ میکروات توان اتلاف می‌کند در حالی که سیستمی با ۸۴ واحد ریاضیاتی موازی که از ۱۶۲۰۰ گیت استفاده می‌کند تقریبا ۱۲۰ میکرووات در ۵۰۰ کیلوهرتز توان مصرف می‌کند.

۶.معماری خم بیضوی:

رمزنگاری خم بیضوی به گروهی بزرگ از تبادل کلیدرمزنگاری‌های نامتقارن و پروتکل‌های توافق کلید اتلاق می‌شود برای مثال ECDH, ECDSA, ECMV . ضرب نقطه‌ای اسکالر اصلی‌ترین بلوک سازنده‌ی این نوع رمزنگاری است و همچنین این نوع رمزنگاری بسیار گرانبها است.

ما از ECDSA بعنوان پروتکلی برای تولید و تایید امضا و ECMV بعنوان پروتکلی برای انتقال کلید استفاده کرده‌ایم. با توجه به استفاده از ضرب نقطه‌ای اسکالر در این پروتکل‌ها و با توجه به اطلاعاتی که از معماری ECC خود به دست آورده‌ایم، عملکرد و پیچیدگی محاسباتی آنها را تخمین می‌زنیم.

میدان‌های محدود مختلفی برای ایجاد گروه‌های خم بیضوی مورد استفاده قرار می‌گیرد. مشهورترین این میدان‌ها، میدان گالوا با ویژگی‌های اول یعنی $GF(p)$ است.

در معماری ضرب نقطه‌ای اسکالر ECC که ما پیاده‌سازی کرده‌ایم[۸] عملیات بر روی نقاط خم بیضوی با رابطه‌ی $y^2=x^3+aX+x$ انجام می‌شود که این نقاط در میدان $GF(p)$ می‌باشند که $p=(2^{101}+1)/3$ است. ما از ماژول مقیاس

خاصی با $m= 2^{101}+1$ با ضریب مقیاس $s=3$ استفاده کرده‌ایم که موجب افزایش کارآمدی در کاهش مدولار می‌شود. تمامی محاسبات ریاضی اولیه مانند جمع، تفریق، ضرب و تقسیم بصورت سریال بیتی پیاده‌سازی شده است. این معماری، چیپی با ۱۸۷۲۰ گیت را نیازمند است که کمتر از ۴۰۰ میکروواط در فرکانس ساعت ۵۰۰کیلوهرتز را اتلاف می‌کند.

۷.تجزیه و تحلیل:

جدول ۱ نشانگر مقایسه‌ای از پارامترهای مختلفی است که برای معماری رمزنگاری در روش رابیت و دو نوع NtruEncrypt و همینطور ضرب نقطه‌ای اسکالر در ECC مورد استفاده شده است. NtruEncryptدارای کوچکترین اندازه‌ی مدار است و به همین دلیل کمترین مقدار انرژی را تلف می‌کند اما دارای بدترین فاکتور در گسترش پیام[5]است. مدل موازی‌شده‌ی NtruEncrypt توانی در حدود روش رابین اتلاف می‌کند اما با این حال از لحاظ مصرف توان، بسیار مقرون به صرفه است.

معماری ECC از لحاظ مصرف توان با روش‌های دیگر قابل مقایسه نیست که بخاطر محاسبات ریاضیاتی آن است.

در ادامه با استفاده از اطلاعاتی که از این پیاده‌سازی‌ها بدست آمده است توان مورد نیاز برای رمزگشایی، امضا و تایید امضا برای هر روش PKC را تحت فرضیاتی، بدست می‌آوریم.

رمز نگاری / رمز گشای		Rabin	الگوریتم رمزنگاری	الگوریتم رمزنگاری موازی	ENCV
- ظرفیت پیام - متن رمز (بسته ۳۰ بایت)		< 512 bits 512 bits (3)	< 256 bits 1,169 bits (5)	< 256 bits 1,169 bits (5)	< 200 bits 400 bits (2)
رمز نگاری	زمان در هر پیام متوسط قدرت انرژی در هر پیام	2.88 ms 148.18 µW 426.769 nJ	58.45 ms 19.13 µW 1.118.15 nJ	0.87 ms 118.7 µW 102.79 nJ	817.7 ms 394.4 µW 322.5 nJ
رمز گشای	زمان در هر پیام متوسط قدرت انرژی در هر پیام	1.089 s 191.5 µW 208.64 nJ	116.9 s 58.73 µW 6,865.54 nJ	1.732 s 158.3 µW 274.18 nJ	411.54 s 394.4 µW 162.31 nJ

[5] Message expansion

امضا کردن / تأیید		Rabin	الگوریتم رمزنگاری	الگوریتم رمزنگاری موازی	ENCV
- طول امضاء (بسته ۳۰ بایت)		512 bits (3)	1,169 bits (5)	1,169 bits (5)	200 bits(1)
رمز نگاری	زمان در هر پیام متوسط قدرت انرژی در هر پیام	1.89 s 191.5 µW 208.64 µJ	233.8 ms 58.73 µW 13.73 µJ	3.464 ms 158.3 µW 548.35 nJ	410.45 ms 394.4 µW 161.88 µJ
رمز گشای	زمان در هر پیام متوسط قدرت انرژی در هر پیام	2.88 ms 148.18 µW 426.76 nJ	58.45 ms 19.13 µW 1,118.15 nJ	0.87 ms 118.7 µW 102.79 nJ	822.5 ms 394.4 µW 324.39 nJ

جدول ۱: مقایسه عملکرد توابع PKC

۸.امکان سنجی:

در قسمت ۲ چهار سوریس امنیتی که می‌توند از پیاده‌سازی مقرون به صرفه‌ی PKC سود ببرد سخن گفتیم. در اینجا مشخص می‌کنیم که کدام تابع PKC برای هریک از این سرویس‌ها مورد نیاز است. احرازهویت پخشی از تایید امضا در نودی که از کلید عمومی ایستگاه اصلی استفاده می‌کند کاربرد دارد. برای اینکه اطلاعات در حین ارسال به ایستگاه اصلی رمزنگاری شوند نود باید اطلاعات را با استفاده از کلید عمومی اسیتگاه اصلی رمز کند. توزیع کلید نود به نود نیازمند رمزنگاری و رمزگشایی است. افزودن نود جدید مبتنی بر این است که یک نود باید دارای کلید مخفی باشد. یک نود ممکن است پیامی را امضا کند و به ایستگاه اصلی ارسال کند و یا ممکن است پیامی را که از ایستگاه اصلی دریافت کرده است را از رمز خارج کند. جدول ۱ مروری بر این توابع در سه سیستم PKC که ما در نظر گرفته‌ایم را ارائه می‌کند.

۹.روش‌های کلید عمومی:

حال نشان می‌دهیم که کدامین روش PKC از سرویس‌های امنیتی که در بالا اشاره شد را فراهم می‌کند و تخمینی از توان مصرفی آنها را ارائه می‌کنیم. روش رابین همان‌گونه که در [9] آمده است برای هر ۴ سرویس می‌تواند مورد استفاده قرار گیرد. قسمت ۳ نشان می‌دهد که این روش چگونه برای رمزنگاری اطلاعات به کار گرفته می‌شود که این عملیات همان عملیات موردنیاز برای تایید امضا نیز هست. رمزگشایی اطلاعات همانند تولید امضا نیازمند حل معادله‌ی $D_n= \sqrt{y} \bmod n$ است. اگر $p=q=3$ به سنج ۴ تنظیم شود سپس ریشه‌ی دوم با استفاده از محک اویلر و الگوریتم گارنر محاسبه می‌شود که در ادامه آمده است. $Y^{(p+1)/4}=c1 \bmod p$ و $Y^{(q+1)/4}=c2 \bmod q$ را محاسبه می‌کنیم. با استفاده از الگوریتم گارنر نتایج را بصورت $x= +\text{-}c1 + [(+\text{-}c2+\text{-}c1).p(p^{-1} \bmod q)] \bmod n$ بدست می‌اوریم. توان‌های $(p+1)/4$و $(q+1)/4$ و همچنین $p(p^{-1} \bmod q)$ را می‌توان قبلا محاسبه کرد و همانند کلیدها توزیع کرد. عمل

رمزگشایی نیازمند دو عملیات به توان رسانی با پایه‌ی حداکثر ۲۵۵ بیتی و یک ضرب به سنج n است. هزینه‌های مربوط به جمع در مقابل هزینه‌های ضرب قابل چشم پوشی است. عمل رمزگشایی نیازمند ۷۶۲ ضرب با میانگین ضریب همبستگی ۲۵۵ بیتی و یک ضرب ۵۱۲ بیتی است. اگر ما همان مداری که برای رمزنگاری استفاده کردیم را به کار گیریم، یک عملیات رمزگشایی بطور میانگین ۵۴۴ و ۷۵۳ سیکل زمان را نیازمند خواهد بود یعنی عملیات رمزگشایی و یا امضا ۱,۰۹ ثانیه زمان خواهد گرفت. این مدار جدید ممکن است نیازمند حافظه‌ی بیشتری برای c1 و c2، ضرب‌کننده‌های اضافی برای ثابت‌های از پیش محاسبه شده و کنترل منطقی بیشتری باشد. مشاهدات نشانگر توان اتلاف کل در حدود ۱۹۱,۵میکرو وات می‌باشد. NtruEncrypt و NtruSign نشانگر اطلاعاتی خوب برای استخراج توان و انرژی موردنیاز برای رمزگشایی و تولید امضا و تایید امضا هستند. در معماری اصلی، کلید عمومی را بعنوان مقادیر ثابتی در یک جدول ذخیره کرده‌ایم. برای تخمین مناسب، سرباری به میزان ۴۰میکروات از توان ثابت را به نتایج شبیه‌سازی اضافه کرده‌ایم که این عملیات به دلیل حافظه‌ی اضافی موردنیاز است. اساس تخمین‌های ما، تعداد کانولوشن‌های دوری مورد نیاز است چرا که این عملیات اصلی‌ترین عملیات در روش NTRU است. بر اساس تعداد عملیات‌های کانولوشن مورد نیاز باید ۱ و ۲ و ۴ و ۱ به ترتیب برای رمزنگاری، رمزگشایی، امضا و تولید امضا باشد. کانولوشن، پیچیده‌ترین عملیاتی است که برای NtruEncrypt و NtruSign مورد استفاده قرار می‌گیرد و به همین دلیل، منطقی است که انرژی و زمان به تعداد کانولشن بستگی داشته‌باشد.

ECMV و ECSDA الگوریتم‌های رمزنگاری و امضایی که ما انتخاب کرده‌ایم مبتنی بر خم بیضوی و ضرب نقطه‌ای اسکالر هستند. با توجه به تعریف این الگوریتم‌ها در بسیاری از استانداردها و مولفات، رمزنگاری و تایید امضا در ECMV و ECDSA نیازمند دو ضرب نقطه‌ای اسکالر هستند در حالی که رمزگشایی و تولید امضا نیازمند یک ضرب نقطه‌ای اسکالر هستند. اساس تخمین ما نیز بر اساس همین یافته‌ها است.

۱۰.مقایسه:

جدول ۱ توابع PKC را با توجه به سرعت، توان، انرژی و طول پیام مقایسه می‌کند. توان انتقالی برای پیام‌ها با توجه به اینکه جز فرضیات ما نیست در نظر گرفته نشده است. با این حال طول متن رمز شده و امضا می‌تواند برای برخی از فرستنده‌ها مورد استفاده قرار گیرد. برای رمزنگاری و رمزگشایی، نرخ طول سربار به طول متن رمز شده مهم است. امضا به همراه پیام اصلی ارسال می‌شود.

اندازه‌ی پاکت معمولی در WSN ها ۳۰بایت و ۵۶ بایت است [13]. با توجه به نامتقارن بودن، روش رابین در صورت نیاز به رمزنگاری و تایید امضا در نودها، روشی مناسب است. در غیراینصورت این روش با ECC قابل قیاس است. Ntruدارای کمترین میانگین توان است اما دارای بزرگترین طول پیام به اندازه‌ی ۵ پاکت است. در محیط‌هایی که اتلاف توان اهمیت زیادی ندارد Ntru دارای مزایای است. ECC دارای گسترش پیام کوچک برای رمزنگاری و اتلاف توان بالا است اما نیازمند کمترین تعداد پیام است. با توجه به اینکه معمولا محتوی پیام(کلید) معمولا بیشتر از ۲۰۰ بیت است. در بسیاری از نودهای WSN ، انتقال یک بیت به اندازه‌ی انجام ۱۰۰۰ دستورالعمل توان مصرف می‌کند. اندازه‌ی پیام کوچک و سربار کمتر مهمترین مزیت استفاده از ECC است.

احرازهویت پخشی می‌تواند از PKC بهره‌های فراوانی را کسب کند. با استفاده از ECC یک پاکت اضافی باید برای احراز اصالت پیام به ایستگاه ارسال شود. پروتکل‌هایی مانند µTESLA [14] نیازمند روش پیچیده‌ی تاخیر در افشای کلید است که این روش، نیازمند به‌روزرسانی ثابت کلید، ذخیره‌ی کلید توسط نودها و همزمانی است. فعالسازی یک نود جدید در این روش بسیار سخت است. حال می‌توان توزیع کلید نود به نود را با دو پاکت ECC و یا سه پاکت RABIN انجام

داد. چنانچه نودهای ارتباطی تعداد بیشتری باشند استفاده از ایستگاه اصلی در این روش بسیار هزینه‌بر است. روشی که در ارائه شده است حداقل نیازمند ۴ پیام است که سه تای آنها شامل ایستگاه اصلی است. جزئیات اینکه رمزنگاری اطلاعات چه زمانی دارای مزیت است و چگونه عملیات افزودن نود جدید مدیریت می‌شود به پروتکل مورد نظر بستگی دارد.. با این حال، نتایج ما نشانگر اسن است که پاکت‌های کمی در صورت استفاده از PKC مورد نیاز است.

۱۱.نتیجه‌گیری:

در این مقاله، مقایسه‌ی عمیقی از سه روش PKC پیاده‌سازی شده در شبکه‌های حسگر بی‌سیم صورت گرفت. نشان دادیم که استفاده از PKC نسبت به استفاده از مدیریت کلید در شبکه‌های حسگر بی‌سیم بسیار کارآمدتر است که موجب کاهش مقدار سربار ترافیکی می‌شود و همچنین هزینه‌های محاسباتی در حد مطلوبی است و به اندازه‌ی کافی سریع است.

مراجع

1. Daemen, Joan, Rijmen, Vincent. (March 9,),AES Proposal: Rijndael. *National Institute of Standards and Technology* 2003; p. 1. Retrieved 21
February 2013.
2. Jawahar Thakur, Nagesh Kumar. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis.
International Journal of Emerging Technology and Advanced Engineering December 2011; vol 1(2), p.6-12.
3. R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*Communications of the*
ACM 1977; p. 120-126.
4. D. Boneh. Twenty Years of Attacks on the RSA. *Notices of the American Mathematical Society* 1999; vol 46(2),p.203–213.
5. O. Acıi cmez, C. Kaya Ko and J.P. Seifert, On the power of simple branch prediction analysis. *IACR Cryptology* 2006; ePrint Archive.
6. G. Gaubatz, J.-P. Kaps, and B. Sunar. Public key cryptographyin sensor networks—revisited. In *1st European Workshopon Security in Ad-Hoc and Sensor Networks (ESAS2004)*, 2004.
7. N.Koblitz, Elliptic Curve Cryptosystems. *Mathematics of Computation* 1987; volA8, p.203 -209.
8. S.M.Celestin ,V.K.Muneeswaran, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography. *IEEE International*
Conference on Advanced Computing Dec 2009; p. 82-85.
9. Hafid Mammass and Fattehallah Ghadi, Implementation of Smartcard Personalization Software.
International Journal of Future Generation
Communication and Networking 2012; vol 5(4).p.39-54.
10. F. Amounas and E.H. El Kinani, A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin ½ Matrices.
International Journal of Information & Network Security (IJINS) 2013; vol 2(3),p. 190-196.
11. Md.Zaheer Abbas, Dr.JVR Murthy,Authenticated And Policy - Compliant Source Routing. *International Journal of Engineering Research*
and Applications (IJERA) 2012;vol 2(3),p.1347-1352.
12.A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E.Culler. SPINS: security protocols for sensor networks. *WirelessNetworks*, 8(5):521–534, 2002
13.J. Hoffstein, J. Silverman, and W. Whyte. NTRU report 012,version 2. estimated breaking times for NTRU lattices. Technical Report 12, NTRU Cryptosystems, Inc., 2003
14. J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman,and W. Whyte. NTRUSign: Digital signatures using the
NTRU lattice. In *Topics in Cryptology–CT-RSA 2003*, volume2612 of *LNCS*, pages 122–140. Springer Verlag, 2003.