دومین کنفرانس ملی توسعه پژوهش های نوین در مهندسی برق و کامپیوتر
۸ و ۹ اسفند ۹۷
موسسه آموزش عالی وحدت، تربت جام، ایران
2nd National Conference of Innovative Research Developmentsin
Electrical and Computer Engineering
27 & 28 February 2019
Vahdat Higher Education Institute, Torbat-e Jam, Iran

مروری برامنیت و الگوریتمهای رمزنگاری در شبکههای حسگر بیسیم جهت احراز هویت

زهرا بیات*[1]

[1] فارغ التحصیل کارشناسی ارشد مهندسی نرم افزار دانشگاه آزاد واحد زنجان *Email:Zb_ec@yahoo.com*

چکیده

کاربرد شبکههای حسگر بیسیم یا گیرنده های بی سیم متنوع و زیاد است، آن‌ها برای استفاده در کاربردهای تجاری و صنعتی برای کنترل داده ها و جاهایی که گیرنده های سیمی مشکل و گران است به کار می روند. در واقع این شبکه ها خصوصیات منحصر به فرد ی دارند، مانند توانایی کار کردن در شرایط نامطلوب، توپولوژی شبکه پویا، خطاهای ارتباطی، توسعه در مقیاس بزرگ، افزایش ظرفیت نودها، تحرک نودها، عملیات بدون مراقبت همچون انرژی محدود و برخی دیگر ... اما چالش اصلی که در این شبکهها حاکم است این است که در معرض تهدیدات امنیتی مختلفیقرار دارند. بنابراین احرازهویت کاربر یکمسئله مهم در این شبکه‌ها با توجه به منابع محدود گره ها محسوب میشود و امنیت شبکه‌های حسگر بی‌سیم زمینه ای است که درسالیان گذشته بطور چشمگیری مورد تحقیق قرار گرفته است. از این رو در این تحقیق مروری بر امنیت شبکههای حسگر شده و در بخشی الگوریتم های رمزنگاری مناسب مختلفی امنیت شبکه های حسگر معرفی میشود و در بخش نهایی تکنیک هایی که جهت احراز هویت در شبکه های حسگر بیسیم مناسب است، معرفی شده است. امید است مطالعه این مقاله دید مناسب به کاربران جهت طراحی یک شبکه حسگر بیسیم را ارائه دهد.

کلمات کلیدی:شبکه حسگربیسیم، امنیت، الگوریتمهای رمزنگاری و احراز هویت.

۱ -مقدمه

شبکه حسگر شبکهای از تعداد زیادی گره کوچک تشکیل شده است. در هر گره تعدادی حسگر و یا کارانداز وجود دارد. شبکه حسگر بشدت با محیط فیزیکی تعامل دارد. از طریق حسگرها اطلاعات محیط را گرفته و از طریق کار انداز ها واکنش نشان می دهد. ارتباط بین گره ها بصورت بی سیم است. هرگره بطور مستقل و بدون دخالت انسان کار میکند و از لحاظ فیزیکی بسیار کوچک است و دارای محدودیت هایی در قدرت پردازش، ظرفیت حافظه،منبع تغذیه و... میباشد. این محدودیت ها مشکلاتی را بوجود می آورد که منشأ بسیاری از مباحث پژوهشی مطرح در این زمینه است[۳]. نام شبکه حسگربی سیم یک نام عمومی است برای انواع مختلف که به منظورهای خاص طراحی می شود و شبکه های حسگرنوعا تک منظوره هستند. در صورتی که گره ها توانایی حرکت داشته باشند شبکه می تواند گروهی از رباتهای کوچک در نظر گرفته شود که با هم بصورت تیمی کار می کنند و برای مقصد خاصی مثلا بازی فوتبال یا مبارزه با دشمن طراحی شوند. از دیدگاه دیگر اگر در شبکه تلفن همراه ایستگاههای پایه را حذف نماییم و هر گوشی را یک گره فرض کنیم ارتباط بین گره ها باید بطور مستقیم از طریق یک یا چند گره میانی برقرار شود. این خود نوعی شبکه حسگر بی سیم می باشد. این ایده توانسته در ذهن طراحان رباتهای متحرک مستقل یا حتی طراحان شبکه های بی سیم موبایل نیز شکل گیرد. به هر حال از آنجا که این فن نقطه تلاقی دیدگاه های مختلف است تحقق آن می تواند بستر پیاده سازی بسیاری از کاربردهای آینده باشد. [۲].این مقاله، مروری بر امنیت و الگوریتمهای رمزنگاری در شبکه - های حسگر بیسیم جهت احراز هویت میشود.

۲ -امنیت شبکهحسگربیسیم

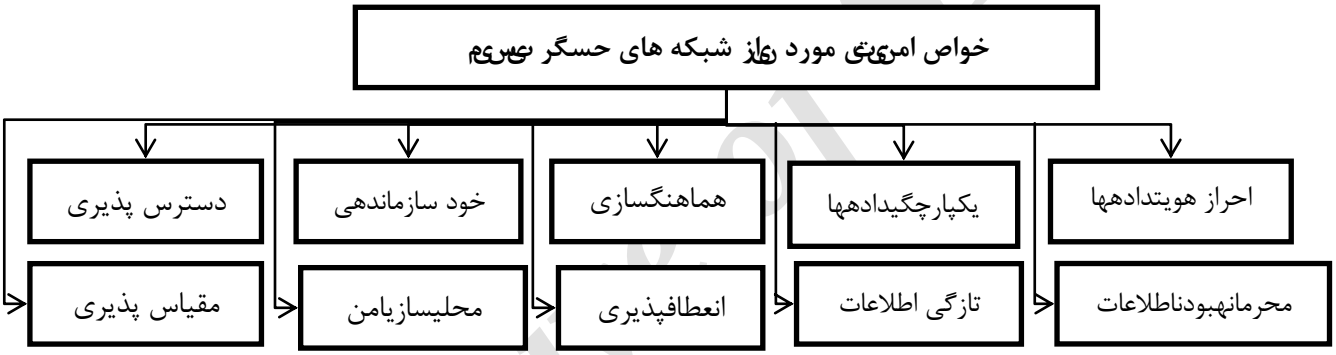
امنیتکامپیوترهموارهیکنگرانیبزرگبودوتمامانواعراه-حل هابهطورسنتیبرایبرخوردبا نقضامنیتیموجوددرزمینههایمختلفاستقرارماشینهایمحاسباتی دنبالشدهاست. اینینگرانیهاپسازمعرفیواستقرارفنآوریهایجدید تر، مانندشبکههای حسگربیسیم بیشتر و بیشتر شدهاست . باتوجهبهمحدودیتشدیدعناصرتشکیلدهندهاینشبکه،راهحل هایامنیتی کامپیوترهایسنتیدر اینجا قابلاجرانیست .

بنابراین،تحقیقاتزیادیدرچگونگیایمنسازی شبکهحسگربی سیممتمرکز است .

درآینده،هزارانومیلیونهاسنسورکوچک،شبکههای حسگر بی سیم خودسازماندهیشده را تشکیل میدهند . اینشبکه هایحسگرتوسطقدرتومنابع انرژیمحدود،پهنایباندکم،اندازهحافظهکوچک،ارتباطاتغیرقابلاعت ماد (بهعنوانمثال،انتقالغیرقابلاعتماد،برخوردوزمانتاخیر) وعملکردغیرقابل اعتمادمشخص می شوند . بنابراینتکنیک امنیتیسنتیدرشبکههایکامپیوتریبرایشبکههایحسگربیسیممفید و مناسبنمی باشد.محققانباتمرکزبرساختیکمدلاعتمادسنسوربرایحلمشکلاتفر اترازقابلیتهایامنیتیرمزنگاری شروع کردندوآنهاسعیکردندبهمقابلهباچالشها برایبهحداکثررساندنقابلیتپردازشوانرژیگرههایحسگر بیسیم بپردازنددرحالیکهدربرابرحملات ایمن باشند.

۲ ۱-خواص امنیتی مورد نیاز شبکه های حسگر بیسیم

دراینبخش،خواصامنیتیموردنیاز برایشبکهحسگر فرموله شده است ونشانداده می - شودکهچگونهآنهابهطورمستقیمدریکشبکهسنسورمعمولیقابلاجراه ستند[۴].



شکل ۲: نمایی از خواص امنیتی مورد نیاز شبکه های حسگر بیسیم

- **احراز هویتدادهها** :

احرازهویتبرایبسیاریازوظایفمدیران (بهعنوانمثالبرنامهریزیمجددشبکهیاکنترلچرخهجسگر) لازم می باشد . به طور همزمان،دشمنبهراحتیمیتواندپیامها راتزریق کند،بهطوریکهگیرندهنیازدارد تامطمئنشودکهداد هایموردااستفادهدرهرفرایندتصمیمگیری،ازمنبع درست سرچشمه گرفته است . اعتباردادههااجازهمیدهدتاگیرندهبررسی کند کهدادههاواقعاازفرستنده ایی که ادعا کرده ارسال شده است یا نه.

- **محرمانهبودناطلاعات:** در یکشبکهحسگر نبایدقرائتسنسوربهشبکههمسایه رخنه کند . روش هایاستانداردبرایمخفینگهداشتناطلاعاتحساس،بهرمزدرآو ردنداده ها بایککلیدمخفی استکهگیرندهاطلاعات ان را می داند.

- **یکپارچگیدادهها:** دشمنمی-تواندداده هاراتغییردهد،بهطوری کهارسال درشبکههایحسگربهبی نظمیمیخورد . بهعنوانمثال،گرهممکناستبرخیازقطعات رااضافه کندویا به دستکاریدادههادریکبسته بپردازد . اینبستهجدیدپسازآنمیتواندبهگیرندهاصلیارسالشود. از دست رفتنداده‌هایاآسیبحتیمیتواندبدونحضوریکگره بدخواهباتوجهبهارتباطاتسختمحیط رخدهد . بنابراین،تمامیتدادههاتضمینمیکندکههرداده‌دریافتشده درحملونقلتغییرنکند.

- **تازگی اطلاعات:** تازگی،یکفرایندکلیدیبرایشرکتکنندگان است که تضمینمی کندهرکلیدمشترکدر نشست

(جلسهکلید) تازهاست. به طور غیررسمی،تازگیداده هانشانمیدهدکهدادهها جدید هستند،وآنتضمینمیکندکههیچپیامقدیمیپخشنشدهاس ت. ایجادکلید،یکیازدوفرمتضمینتازگی را ایجادمیکند . فرمضعیفتر،کهسفارشپیامجزئی تر را فراهممیکند،اماحاملهیچاطلاعات تاخیری نیستوشکلقویتر،سفارشکلیدیکجفتدرخواستپاسخ را فراهممیکند وتخمینتاخیر رااجازهمیدهد . تازگیضعیفتوسطاندازهگیری سنسورموردنیازاست،درحالیکهتازگیقویبرایهماهنگ-سازیزماندرشبکههمفیدمیباشد.

- **خود سازماندهی:** شبکههحسگربیسیمنیازبهتعدادیگره سنسورمستقلو به اندازهکافیانعطاف - پذیر،برایخودسازماندهیوخوددرمانیباتوجهبهشرایط متفاوت دارد . هیچزیرساختیثابتی،برایمدیریتشبکههدریکشبکه سنسور در دسترسوجودندارد . اینویژگیذاتییکچالشبزرگبرایامنیتشبکههحسگر بیسیم رابهارمغانمیآورد . اگرخودسازماندهیدریکشبکههسنسور وجودنداشته باشد،آسیبناشیازیکحملهویاحتیمحیطزیستخطرناکممکنا ستمخرببباشد.
- **توانایی:**برایاطمیناناز توانایییحفاظتازپیام،شبکههحسگربایدا ز منابعخود (بهعنوانمثال،گرههایحسگر) ازپردازش-هایغیرضروریازمدیریت کلید بهمنظوربهحداقل رساندن مصرفانرژیوگسترشزندگیشبکههحفاظت کند . توابعمدیریتکلیدنبایدمحدودبهتواناییشبکههوایجادنقاطشک ست منفردمانندمدیریت گره کلیدمتمرکزبرایهمهمانیتشبکهباشد.
- **هماهنگسازی زمان:** اکثربرنامههایکاربردیشبکه-هایحسگرمتکی بر فرمهایی ازهماهنگسازیزمان می - باشند. بهمنظورحفظقدرت،رادیوسنسورممکناست برایدوره اییازمانخاموش شود . علاوهبراین،ممکناستسنسورهادوست داشته باشندتاخیرانتهابهانتهایکبستهرابهعنوانسفربیندوسنسورم حاسبه کنند. بیشترشبکههایحسگر مشارکتیممکناستبه هماهنگ-سازیگروهیبرایردیابیبرنامههایکاربردی،وغیرهنیاز داشته باشد[۱]،مجموعهایازپروتکل های هماهنگسازی امنیتیرابرایفرستندهوگیرنده (دوبهدو)،فرستندهگیرنده چندجهشی (برایاستفادهدرزمانیکههجفتگرههادرمحدودهتکهاپ نیستند)،وهماهنگسازیگروهی پیشنهاد شد.
- **محلیسازیامن:**دراغلبموارد،استفادهازیکشبکههحسگربرت وانایییدقیقوبهطورخودکارتعییننمحلهرسنسوردرشبکههمتک ی است . یک شبکههحسگربرای موقعیتیابیگسلها طراحی شدهاست که نیاز بهاطلاعاتدقیقمحلبه منظورمشخصکردنمحلیکگسلدارد. متاسفانه،یکمهاجمبهراحتیمیتواناطلاعات محلناامن راباگزارشنقاطقوتسیگنالهایدروغین،سیگنالهاپخش،وغیر ه دستکاری کندبرخیازتکنیکهادراینمنطقهوجوددارد . بهعنوانمثال(VM) چند جانبه قابل رسیدگیو(SeRLoc) محلیسازی امنمحدوده-مستقل که درچند جانبه،موقعیتدستگاهبهدقتدریکسریازنقاطشناختهشدهم رجع محاسبهمیشود . محدودهفاصله و تصدیقگرفتهبراياطمیناناز محلدقیقیکگره استفادهمی - شود. درSeRLoc،یکسنسورموقعیتخودراباگوشدادنبهاطلاعاتفان وسدریاییارسالشدهتوسطهرمحلیابمحاسبه میکند . چراغشامل موقعیتمحلیاباست . بااستفادهازتمامچراغ هاکهیکگرههحسگرتشخیص میدهد،یکگرههمکانتقریبی رابراساسمختصاتموضعگیری محاسبه میکند . همهچراغهایمنتقلشدهتوسط موقعیتیاب باکلیدمتقارن مشترکجهانیرمز می - شوندکهازقبلبهسنسورقبلازگسترش لود شدهاست . هرحسگرنیزکلیدمتقارن منحصربهفرد راباهرموقعیت یاب به اشتراک میگذارد . اینکلیدنیزبررویهرسنسور از قبللودشدهاست
- **مقیاسپذیری:**شبکههایحسگرتوزیع شدهاز ۱۰ تا۱۰۰۰۰گره دارند کهتعداد کوچکیازاینگرهها، گرهانرژیفوقالعادهغنییاگرههدروازه می باشند . شبکه-هایحسگرتوزیع شده هایبزرگنمیتوانندازیک

شمایکلیدزنیاستفاده کنندکهدارایخواصمقیاس گذاریضعیف (همازنظرهزینههایانرژیویازمانتاخیر) برایایجادوحفظیککلیدبرایشبکههایحسگرتوزیع شده بهعنوانیککلیابرایزیرمجموعهزیادیازگره می باشد.طرحهایکلیدزنی دارایبرخیازپارامترهای مربوطبه هزینه (تعدادعملیاترمزگذاری،تعدادبیتهایدریافتشده) می باشد کهبهسرعتباافزایشاندازهگروه، رشدمیکند . برایاستفادهدرگروه هاییکهدرآناعضااغلبپیام ها را در عوضانتقالان ها تغییر می دهند،اینکارآمدتر می باشدکه ازچندینزیرگروهکوچکتر (باگروههایمختلفکلید)، استفاده کنیموبهسادگیرمزگذاری مجددپیام کنیمزمانیکهآنها ازیکزیرگروهبه گروه دیگرفرستاده می شوند . اینروشبهخصوصزمانی جذاب استکههزینههای انتقالانرژیازهزینههای محاسباتیمهمتراست.

- **دسترس پذیری:** محرمانهبودن پایانبهپایاناطلاعاتحسگرنبایداجراشود،چونمانعازبرخورد داده سنسورتوسطگرههایمیانیدرحالوقوعمی شود . برای فراهمکردندسترسیگرههمیانی،یکطرح مدیریتکلیدبایدروابط کلید - زنیرا،یابهطورمستقیمیاTransitively،باتمامپتانسیلفراهم کند[۴].روابط کلیدزنیمستقیمبینهمهسنجشبالقوه،متوسط،وگرهمقصدم مکناستتوسطداشتنکلیدشبکهگستردهبرایتمامگره ها انجامشود. روابطمتعدیکلیدزنیاجازهمیدهدکه گره - هایمیانیدرامتدادمسیرارتباطیچندهاپرمزگشایی شوندودادههای دریافتیازطریقیککلید بررسی شودوازکلیددیگربرایرمزگذاری دوبارهوتصدیقدادهفرستادهمیشود . به جایایجادیکشبکهگسترده با تنهایککلید،روابط متعدداجازهمیدهدکه گروه های کوچکتری برای روابط کلیدزنی ایجاد شوند.

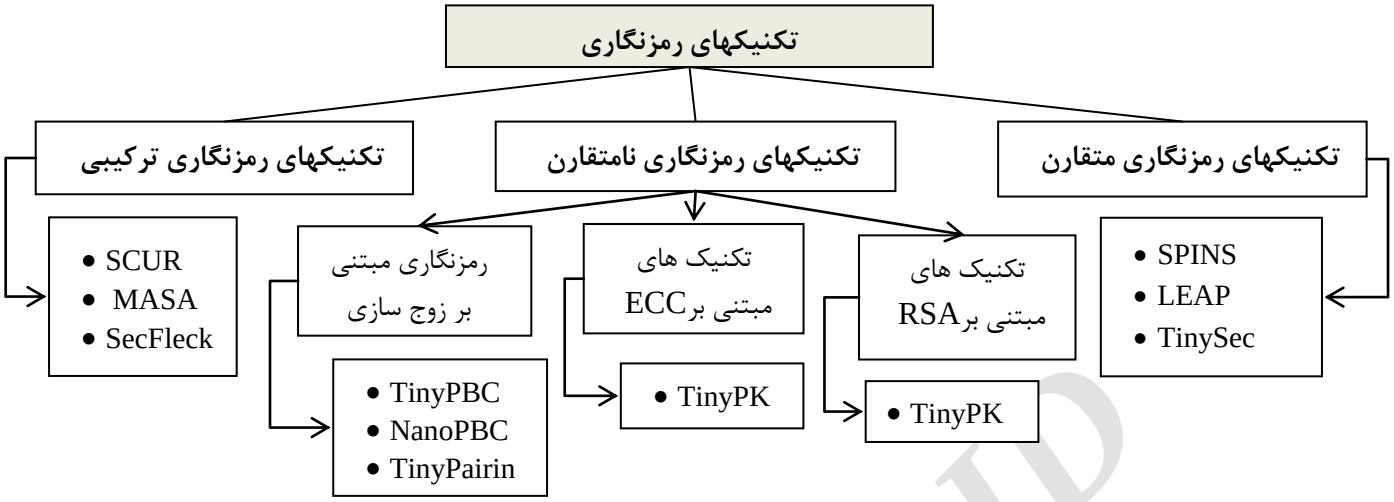
- **انعطافپذیری:**شبکه- هایحسگردرحالاتمیدانپویااستفادهمیشوندکهدرآنشرایطزیس تمحیطی،تهدید،وماموریتممکناستبهسرعتدرحالتغییرباشن د. تغییراهدافماموریتممکناست نیازبه حذف سنسوربایکگرهحسگرباشد.

علاوهبراین،دوشبکهحسگریابیشترممکناستدر یک شبکهترکیب شوند،ویایکشبکهواحدممکناستبهدو شبکهتقسیم شود.پروتکل های ایجاد کلیدبایدبهاندازهکافیبرایارائهکلیدزنیبرایتمامحالاتبالقوهی کسنسورشبکهکه ممکناست با انروبرومیشود انعطافپذیر باشد.

پروتکلهانیازبهآگاهیازگرههایدیگردارند،درحالیکهپروتکلهابا حداقلتصوراتتشویقمیشوند .

۳ - مروری بر تکنیک‌های رمزنگاریدرشبکه‌هایحسگربیسیم جهت امنیت بالا

ازآنجا که اهمیت WSN برای محدوده وسیعی از کاربردها شامل تغییرآبوهوا،نظارتبرمحیطزیست،نظارتبرترافیکواتوماسیونخ انگی افزایش پیدا کرده است امن نگاه داشتن WSN یک موضوع چالشی بسیار مهم است. رمزنگاری یک روش جهت تأمین امنیت است. این مورد می‌تواند توسط روش‌های رمزنگای متقارن، نامتقارن و تابعِهش انجام شود. ازآنجا که WSN از نظر محاسبات، مخابرات و توان باتری محدودیت‌های زیادی دارد، این مورد نیازمندی یک الگوریتم رمزنگاری با وزن سبک است. به سبب محدودیت‌های گره‌های سنسوری، انتخاب روش رمزنگاری در WSN حیاتی است. رمزنگاری در WSN می‌تواند در سه جنبه زیر توصیف شود: متقارن، نامتقارن و تابع هِش(ترکیبی)[۵].



شکل ۲: تکنیک های رمزنگاری در شبکه های حسگر بیسیم

۳ ـ۱ روش‌های رمزنگاری متقارن

در روش‌های رمزنگاری متقارن، یک کلید مشترک اساسی که بین دو گره ارتباطی هم برای رمزنگاری و هم برای رمزگشایی وجود دارد. این کلید باید در شبکه به صورت امن باقی بماند که این کار می‌تواند در محیط‌های آزاد بسیار دشوار باشد. اغلب روش‌های امن برای WSN تنها از پیاده - سازی متقارن به سبب آسانی آن در پیادهسازی با توجه به نیاز به انرژی اندک و محدودیت‌های سخت افزاری، علی الخصوص اگر پیادهسازی در سخت افزار جهت حداقل کردن تلفات عملکرد باشد، استفاده می‌کنند. دو نوع از رمزهایی که استفاده می‌شوند، رمزهای بلوکی که در بلوک‌های با طول مشخص کار می‌کنند و رمزهای رشته‌ای که برروی‌داده‌ها فرمان‌هایبیتپردازکارمی‌کنند، می‌باشند. یک رمز رشته‌ای می‌تواند به صورت یک رمز بلوکی با یک طول بلوک برابر با ۱، درنظر گرفته شود. در رمزنگاری متقارن، یک کلید خصوصی می‌تواند به منظور کدگشایی داده علامت استفاده شود درحالیکه یک کلید عمومی می‌تواند به منظور رمزنگاری و داده تأیید نیز به کار برود. کلید خصوصی نیازمند امن بودن باقی می‌ماند درحالیکه کلید عمومی می‌تواند به صورت آزاد منتشر شود. در این زیربخش، چارچوب‌های رمزنگاری‌ای که مبتنی بر تک کلید مشترک در هر دو حالت رمزگذاری و رمزگشایی می‌باشد بحث شده است. چنین ساختاری به صورت SPINS، رمزنگاری موضعی و پروتکل تشخیص(LEAP) و TinySec می‌باشد[۵].

- **SPINS**: این مورد مبتنی بر دو بولک ساختمانی امن است، SNEP (پروتکل رمزنگاری شبکه امن) و TESLA (ورژن کوچک پروتکل تشخیص هویت زمانی، کارا، رشته ا و مقاوم در برابر خطا). SNEP داده را به صورت محرمانه،دوحزبیاعتبارداده‌ها،وداده‌تازه باهزینه‌هایمخابراتیکمتر فراهم می‌کند. درحالیکه میکروتسلا پخش را برای محیط‌های با محدودیت منابع بسیار اندک فراهم می‌کند. این روش جهت جذب گره انعطافپذیر بوده و قادر به ابطال کلید است. اما مقیاس - پذیر نیست و ایستگاه پایه در اینجا هدف حمله قرار می‌گیرد. این روش، زمانی که گره مخرب شروع به ارسال درخواست جهت ارتباط با کلید جاری می‌کند، یک جواب برای حملات DOS(رد سرویس) فراهم نمی‌کند زیرا یک دشمن می‌تواند به آسانی یک حمله پاسخ را فعال سازی کرده و انرژی در گره‌های سنسور را از بین ببرد[۸].
- **LEAP**: طراحی پروتکل مبتنی بر مبانی است که انواع مختلف پیام‌های تبادل شده بیان گره‌های سنسور دارای نیازمندی‌های امنیتی مختلفی می‌باشند. یک مکانیزم کلید اساسی برای برآورده کردن این نیازمندی‌های امنیتی مختلف مناسب نیستند. ارزیابی کد در روش Mica۲ انجام می‌شود. این مورد شامل موضوعات تلفات بسته و انفجاربازخورد نمی‌باشد. LEAP تحت مدلهای حمله مختلف تحلیل شده‌اند و در دفاع دربرابر بسیاری

از حملات مخرب مانند حمله سیل HELLO، حمله Sybil و حمله Wormhole بسیار مؤثر عمل می‌کند. این مورد مبتنی بر برخی فرض‌ها است که یک کلید ازپیش توزیع شده در میان تمامی گره‌ها در مدت زمان آغازین t در عملیات شبکه فاشنخواهدشد و زمانی که این کلید حذف شد، نمی‌تواند از حافظه بازیابی شود[۹].

- **TinySec:** این اولین پروتکل پیادهسازی شده به صور کامل برای رمزنگاری لایه اتصال در شبکه‌های حسگر است. پیاده سازی TinySec در نسخه TinyOS نیز ثبت شدهاست. این روش شامل برخی از بده-بستانها بین عملکرد، شفافیت و امنیت رمزنگاری بوده و یک طراحی مبتنی بر نیازهای کاربردی در فضا شبکه حسگر می‌باشد. پهنای باند، تأخیر و هزینه های انرژی در TinyOS برای کاربردهای شبکه حسگر بسیار ناچیراست. TinySec به سادگی قابل توسعه بوده و در پروتکل‌های سطح بالا نیز مورد استفاده قرار می‌گیرد[۵].

۳ ۲ روش‌های رمزنگاری نامتقارن

رمزنگاری غیرمتقارن نیز به عنوان رمزنگاری کلید عمومی شناخته می‌شود. رمزنگاری کلید عمومی تمایل دارد که به صورت منبع فشرده باشد زیرا اغلب سیستم‌ها براساسحسابعددصحیحبزرگ می‌باشند. برای سالهای متمادی، بسیاری از محققان از رمزنگاری کلید عمومی به صورت نشدنی در سخت افزار محدود استفاده شده در WSN نام می‌بردند. سایز کد، اندازه کد، زمان پردازش و مصرف توان این روش رابرایتکنیکالگوریتمکلیدعمومی مانندپرتکلتوافقیکلیدی-Diffie HellmanیاامضاRSA،درWSNهابهکارگرفتهشود،نامطلوب می‌سازد. الگوریتم‌های کلید عمومی مختلفی شامل روش رابین، رمز-نترو، RSA، رمزنگاری منحنی بیضوی (ECC) رمزنگاری مبتنی بر زوجیت (PBC)، و رمزنگاری مبتنی بر تشخیص می‌باشد[۵].

۳-۲-۱ ساختارهای رمزنگاری مبتنی بر RSA

در این زیربخش از ساختارهای رمزنگاری، ساختارهای رمزنگاری‌ای را که از الگوریتم RSA برای اندازه گیری امنیت استفاده می‌کنند، مورد بحث قرار گرفته است. RSA از نظر محاسباتی سنگین بوده و عموماً هزاران یا حتی میلیون‌ها عملیات ضرب جهت انجام یک عملیات تک-امنیتی در آن انجام می‌شود. تعداد چرخه‌های کلاک مورد نیاز جهت انجام یک عملیات ضرب ابتداعاً بازده الگوریتم کلید عمومی میکروپروسسور را تعیین می‌کند. کارمن و همکاران ۲۰۰۰ یافتند که این مورد عموماً هزاران نانوژول جهت انجام یک عملیات ضرب با نتایج ۱۲۸ بیتی لازم دارد[۵].

- **TinyPK:** TinyPK استفاده از TinySec را ترکیب کرده و عملکرد مورد نیاز برای یک جزء و یک شخصثالثجهت تشخیص هویت آنها توسط یکدیگر و مخابره امن را فراهم می‌کند. TinyPK مبتنی بر رمزنگاری RSA معروف است[۱۰].

۳-۲-۲ ساختارهای رمزنگاری مبتنی بر ECC

در این زیربخش از ساختارهای رمزنگاری نامتقارن، ساختارهای رمزنگاری‌ای را که از الگوریتم ECC برای معیارهای امنیتی استفاده می‌کنند بررسی شده است. امنیت ECC مبتنی بر مسئله لگاریتمی گسسته منحنی بیضوی است که در آن جامعهرمزنگاریبه صورت بسیار دشوارتر از مسئله فاکتورصحیحولگاریتمگسسته‌ای که بیان کننده الگوریتم‌های RSA و کلید عمومی DiffieHellman می‌باشد، تلقی می‌شود. ECC دارای دو مزیت اصلی است: (۱) کلیدهای عمومی ECC برای سطح یکسانی از امنیت در جواب‌های مبتنی بر Diffic Hellman یا RSA کوچک‌تر است که درنتیجه تعداد بیت‌هایی که لازم به تبادل هستند را کاهش می‌دهد و (۲) عملیات کلید عمومی ECC نیازمند محاسبات کمتری نسبت به روش‌های کلید عمومی متعارف هستند. مزیت کلید کوچکتر این است که نیازمند حافظه کنتر، پهنای باند کمتر و درنتیجه انرژی کمتری هستند و لذا سربار مخابراتی و پردازشی را کاهش می‌دهد که برای گره‌های سنسور با انرژی محدود، ایدهآل است[۵].

- **TinyECC:** هدف اولیه از TinyECC، تأمین یک بسته نرمافزاری دردسترس عمومی و آماده استفاده برای عملیات PKC مبتنی بر ECC است که می‌تواند به صورت قابل انعطافی پیکرندی شده و با کاربردهای شبکه حسگر بیسیم تلفیق شود. TinyECC تعدادی از سوئیچ‌های بهینه سازی را فراهم می‌کند که می‌تواند بهینهسازیهای

مشخصی را مبتنی بر نیازهای توسعه دهنده فراهم کنند. ترکیب‌های مختلفی از بهینه سازی دارای زمان اجرا و مصرف منابع متفاوتی می‌باشند که برای توسعه دهندگان قابلیت انعطاف زیادی در جهت تلفیق TinyECC با کاربردهای شبکه حسگر بیسیم را فراهم می‌کند[۱۱].

۳-۲-۳ ساختارها رمزنگاری مبتنی بر زوج سازی

دراینبخشازچارچوبرمزنگارینامتقارن،یکچارچوبرمزنگاریکهبااستفادهازرمزنگاریبراساسجفتشدنبرایاقداماتامنیتیمورد بحثقرار گرفته است. رمزنگاریبااستفادهازدسته (PBC) یکحوزهدرحالظهورمربوطبهECCاستکهموردتوجهجامعهبینالملل رمزنگاریاست.طراحیطرحهایرمزنگاریاصلی را مقدور ساختهوباعثمی‌شودپروتکل‌هایرمزنگاریشناختهشدهکارآمدتر باشند[۵].

- **TinyPBC:** TinyPBC مبتنی بر کتابخانه C/C++ ریاضیاتی صحیح و گویا چند-دقتی است که یک کتابخانه منبع باز قابل دسترس نوشته شده در C است. نویسندگان نشان دادند که چگونه گرههای سنسور می‌توانند کلیدها را در یک روش تصدیقیوغیرتعاملی مبادله کنند. آن‌ها همچنین سریعترین محاسبات زوجسازی در یک بستر ۸ بیتی را ارائه کردند که بیانگر بهترین شکل برای ضرب حوزه باینری در یک بستر ۸ بیتی می‌باشد. نتایج نشان می‌دهد که TinyPBC تنها ۵.۴۵ ثانیه جهت محاسبه زوج سازی در ATmega۱۲۸L. زمان می‌برد. TinyPBC نیازمند نیمی از زمان لازم برای انجام NanoECC است که درآن روش ۱۰.۹۶ ثانیه جهت محاسبه زوج سازی زمان لازم بود[۱۲].
- **NanoPBC:** این مورد برایبهحداقلرساندنعملیاتدسترسیبهحافظه،کهبررویپلتفرمه دفماگرانهستند، بهینه سازی شده است. نویسندگانتوضیحاتعمیقیدرموردچگونگیپیادهسازیزوج سازیمؤثردردستگاه‌هایبامنابعمحدود ارائه دادندوسریع‌ترینشکل‌هابرایجفتشدنمحاسباتبررویکپلتفرم ۸ بیتیبیانشدهاست[۱۳].
- **TinyPairing:** این روش یکراهبهتربرایمحاسبهسرعت رافراهممی‌کند چون این روشحافظهکمیبرایهردوRAMوROMتوسط انتخاب برخی از منحنی‌های بیضوی فوق یکتا به صورت گروه‌های زوج و برخی از حوزه‌های محدود مشخص که بیانگر گروه منحنی بیضوی می‌باشند را مصرف می‌کند[۱۴].

۳ ۳ روش‌های رمزنگاری ترکیبی

رمزنگاری متقارن و غیرمقتارن می‌توانند جهت دستیابی به مزایای هر دو روش با یکدیگر ترکیب شوند و یک روش رمزنگاری ترکیبی را برای تولید ساختار شبکه دوبهدو بر اساس کلیدهای تشخیص هویت در WSN معرفی کرد که مبتنی بر جبر خطی در GF(q) است. روش متقارن برای رمزگذاری و تشخیص هویت استفاده می‌شود در حالیکه روش غیرمتقارن برای تولید کلید استفاده می‌شود. در این زیربخش، ساختارهای رمزنگاری بحث می شود که مبتنی بر ترکیب دور روش رمزنگاری متقارن و رمزنگاری نامتقارن هستند[۵].

- **SCUR**: این مورد الزاماتامنیتیوهمچنینبهرهوریانرژی را برآورده می‌کند. هدفاز SCUR بهحداقلرساندنهزینهبوده درحالیکه سه سطح مورد نیاز در امینت را نیز حفظ کند: (۱) سربار مخابراتی در حالت مخابره بسته‌های رمزنگاری شده. (۲) سربار محاسباتی در امن کردن شبکه به منظور حفظ طول عمر سنسور. (۳) فضایکلیداستفاده شده[۱۵].
- **MASA**: ماسا ترکیب روش‌های متقارن و نامتقارن را جهت تأمین امنیت داده پشتسرهم برای شبکه‌ها حسگر میباشد. این مورد مبتنی بر مفهوم شبکه جغرافیایی مجازی است که درآن کل محدوده به نواحی کوچکتری که به آن سلول گفته می‌شود، شکسته می‌شود. هر سنسور دو نوع از کلیدها را که شامل متقارن و نامتقارن است را حمل می‌کند. MASA از کلید خصوصی جهت امضا یک اطلاعرسانیرویدادهش شدهجهت فراهم کردنمحرمانه بودن،اصالت،وتمامیتداده‌ها استفاده می‌کند. کلید متقارن به منظور تعیین هویت اطلاعرسانیرویداد در سلول خود، استفاده می‌شود[۱۶].

- **SecFleck**: این مورد مبتنی بر یک چیپ ماژول بستر مورد اعتماد است که قابلیت یک گره استاندارد را توسعه می‌دهد. SecFleck از روش رمزنگاری کلید متقارن XTEA به سبب اثرات اندک آن بر روی رم استفاده می‌کند که این روش را تبدیل به یک گزینه مناسب برای تجهیزات سنسوری کوچک می‌کند که به صورت نوعی دارای رَم کنتری از ۱۰ کیلوبایتی می‌باشد. XTEA می‌تواند در یک حالت فیدبک خروجی جهت رمزنگاری یا رمزگشایی رشته‌های طول متغیر استفاده کند. نویسندگان عملکرد بستر secFleck را براساس زمان محاسبات، مصرف انرژی و هزینه مالی مورد بحث قرار داده‌اند[۱۷].

۴ امنیت شبکه های حسگر بی سیم با استفاده از تکنیک های احراز هویت

شبکه‌های حسگر بی سیم به صورت گسترده ای در سالیان اخیر در کاربردهای گوناگون مانند صنعت نفت، صنعت گاز، پزشکی و ... مورد استفاده قرار گرفته است. همچنین شبکه های حسگر بی سیم توانایی جمع آوری داده ها از محیط های گوناگون برای پردازش را دارد. در شبکه ای حسگر بی سیم به دلیل حساس بودن اطلاعات، امنیت نقش مهمی دارد و لازم است اطلاعات به صورت محرمانه نگهداری شود.در برخی کاربردها مثل رهگیری هدف، ردیابی کاربران مشکوک شبکه های حسگر بی سیم اغلب به هماهنگی محیط های عمومی و دشمن می پردازد. بنابراین یک تهدید امنیتی فرصتی برای استخراج کل اطلاعات از حافظه است. برای برخی برنامه های کاربردی ویژه WSNمانند صنایع نفت و گاز، پزشکی و نظامی اطلاعات جمع آوری شده حساس است و باید محرمانه نگهداری شود. بنابراین در چنین برنامه های کاربردی، امنیت و لزوم بررسی احراز هویت شرط لازم برای دستیابی به تمام پتانسیل های موجود در شبکه های حسگر بی سیم است. در این بخش تهدیدات امنیتی و پیشنهادات مکانیزم امنیتی برای شبکه های حسگر بی سیم و تعدادی از تکنیک های احراز هویت کاربر که یکی از مکانیزم های مربوط به امنیت است مورد بررسی قرار گرفته است[۶،۷].

۴ ۱معرفی تکنیک های احراز هویت در شبکه های حسگر بیسیم

در این بخش به معرفی تکنیک های احراز هویت در شبکه های حسگر بیسیم معرفی شده است[۶،۷].

- پروتکلBenenson یک پروتکل تصدیق کاربر است که برای حملات گره مورد استفاده قرار می‌گیرد. این پروتکل چون نیاز به محاسبات نمایی دارد. طبق نتایج زمان محاسباتی پروتکل پیشنهادی Benensonبالاست. در نتیجه محاسبات نهایی پروتکل بیننسون گران است. همچنین این پروتکل تکیه بر وجود شخص ثالث مورد اطمینان دارد[۷].
- Wongیک طرح تاییدی WSN پویا و مبنی بر پسورد قوی پیشنهاد داد. این طرح شامل ۳ فاز ثبت نام، داخل شدن به سیستم و تایید می باشد که دارای سه مزیت اصلی نسبت به طرح قبلی دارد که این مزیت این است که کاهش هزینه محاسباتدر مقابل برخی حملات جعل اسناد امنیت دارد و به کاربرانی که تایید شده اند اجازه دستیابی به داده در هر گره حسگر را می دهد. همچنین دارای معایی می باشد یک اینکه کلمه عبور را می تواند توسط هریک از گره های حسگر نشان دهد. دوم اینکه در مقابل حملات جعل اسناد نقطه ضعف هایی از نظر امنیتی دارد. سوم اینکه اجازه تغییر پسورد را به صورت آزادانه به کاربر نمی دهد و آخرین مورد همچنین نسبت به تهدید دزدیده شدن آسیب پذیر است[۷].
- T-seng با ثابت کردن ضعف امنیتی در طرح Wong به بهبود این طرح پرداخت. این بهبود با افزودن یک فاز اضافی در طرح ونگ صورت گرفت که دارای ۴ فاز ثبت نام، قطع ارتباط، تایید کاربر و تغییر پسورد می باشد[۷].
- Novelty نشان داد که فرآیند تاییدی نشان داده شده در طرح T-seng هنوز غیر ایمن بوده و به یک تایید دوطرفه که برای بعضی کاربردها مهم است دست پیدا نمی کند[۶].
- Vaidya یکی دیگر از تکنیک‌های احراز هویت کاربر است. در این طرح به بررسی نقاط ضعف طرح های تسنگ، ونگ و نولتی پرداخت. ویدیا همچنین عنوان کرد که طرح ها در مقابل برخی حملات مثل

پاسخ به قطع ارتباط و حملات افراد نیز قوی نیست.این طرح به بررسی امنیت توسط پیشنهاد دو طرح تصدیق WSN پرداخته‌است که بستگی به طرح‌های تصدیق پسورد متداول دارد[۶].

- طرح Khan and Alghathbar برای برطرف کردن ضعف طرح Dosپیشنهادی مبنی بر افزودن فاز تغییر پسورد و فراهم کردن فاز تاییدی دو طرفه حسگر داد.با این حال طرح پیشنهادی به دلیل محدودیت در ایجاد جلسات کلیدی بین گره حسگر و کاربرد در WSN هنوز ضعیف است[۷].
- Yeh نیز یک طرح تصدیقی کاربر جدید وابسته به سیستم رمز منحنی بیضی و روش تصدیقی کارت هوشمند است. این تایید هنوز در سه مورد ضعف دارد، اول اینکه هزینه ارتباطی در مقایسه با طرح های موجود گران است. مورد دوم کارکردن بدون تایید دو طرفه گره کاربر/حسگر می باشد و در نهایت کارکردن بدون مشارکت کلیدی بین کاربر و گره حسگر می باشد[۶].
- Yuan یک طرح تصدیق کاربر مبنی بر زیست سنجی که باعث فراهم کردن امنیت بیشتر در مقایسه با طرح داس است. اگرچه آنها بهبود امنیتی پروتکل یوآن را تایید کردند اما هنوز برخی موانع در پروتکل آنها وجود دارد.به عنوان مثال هیچ جلسه کلیدی پس از تایید بین گره حسگر و کاربر وجود ندارد. و همچنین هیچ پیام محرمانه ای مورد بررسی قرار نمی گیرد.همچنین پروتکل آنها نیاز به برخی تجهیزات پیچیده دارد. و هنوز نسبت به انواع حملات مثل حملات تکذیب خدمات آسیب پذیر است[۷].
- آلتوبایتی نیز یک طرح تصدیق کاربر مبنی بر زیست سنجی کارآمد برای Wsn ارائه داد. با بررسی های به عمل آمده مشخص شد که این طرح دارای چندین تله امنیتی است و طبق نتایج این طرح خیلی جهت استفاده برای کاربردهای عملی WSN مناسب نیست و همچنین در مقابل چندین حمله شناخته نشده در این طرح ایمن نیست[۶].

۵ - نتیجهگیری

شبکه‌های حسگر متشکل از گره های حسگر و یک ایستگاه مرکزی به نامسینک بوده که در این شبکه هاگرههای حسگر وظیفه‌ی حس کردن محیط و ارسال این اطلاعات به سینک را دارا میباشند . گره های حسگر به دلیل اندازه ی کوچکی که دارند، دارای محدودیت‌هایی نظیر؛ ظرفیت حافظه، قدرت پردازش و منبع تغذیه را دارا بوده که این محدودیت‌ها از چالش‌های این شبکه هامحسوبمیگردند . ساختار شبکه های حسگر بهگونه‌ای است که در آنها گره های حسگر معمولا در منطقه‌ی ناامن و به‌اصطلاحدرمحیط‌های دشمن‌خیز مستقر می باشند و گره‌ی سینک در مکانی امن جای دارد. از این‌روی این شبکه‌هادرمعرضتهدیدات امنیتی فراوانی قرار میگیرند. یکی از دلایل آن را میتوان در محدودیت منابع آنان دانست. به همین‌دلیل مسأله ی احراز هویت در این شبکه هابهیکی از مسائل مهم و مورد توجه تبدیل شده است.از این رو در این مقاله به امنیت شبکه های حسگر پرداخته شد و در بخشی دیگر از مقاله الگوریتمهای مناسب رمزنگاری شبکه های حسگر بیسیم معرفی شد همچنین در بخش آخر تکنیکها و روشهایی که در جهت احراز هویت در شبکه های حسگر بیسیم انجام شده بود، معرفی شد.

منابع

[1] Wong, K. H., Zheng, Y., Cao, J., & Wang, S.2006. A Dynamic User Authentication Scheme for Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, p. 244–251.

[2] Kumar Sh and Jangra S.(2014)." *A Review: Data Aggregation in Wireless Sensor Network by using Mobile Agent*" International Journal of Advance Research in Computer Science and Management Studies © *2014, IJARCSMS All Rights Reserved* ISSN: 2321-7782

[3] Gungor V, and Hancke G.(2009)." *Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches*". IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 56, NO. 10, OCTOBER 2009

ACM Workshop on Security of ad hoc and 04).

[۱۱]Liu, A., Ning TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks 2008,Washington, DC, USA, IEEE Computer Society.

[۱۲]Oliveira, TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks 5th International Conference on Networked Sensing Systems.

[۱۳]Aranha, D., Lopez, J., Oliveira, L., Dahab, R. NanoPBC: Implementing Cryptographic Pairings on an 8-bit Platform Conference on Hyperelliptic curves, discrete Logarithms, Encryption, etc. (CHiLE 2009), Frutillar, Chile.

[۱۴]Xiong, X., Wong, D., Deng TinyPairing: A Fast and Lightweight Pairing-based Cryptographic Library for Wireless Sensor Networks WCNC 2010, IEEE Communications Society.

[۱۵]Tahir, R., Javed, M., Ahmad, A., Iqbal SCUR: Secure Communications in Wireless Sensor Networks Using Rabbit World Congress on Engineering 2008, I, London, U.K.

[۱۶]Alzaid, H., Alfaraj MASA: End-to-End Data Security in Sensor Networks Using a Mix of Asymmetric and Symmetric Approaches 2nd IEEE International Conference on New Technologies, Mobility and Security.

[۱۷]Hu, W., C ecFleck: A Public Key Technology Platform For Wireless Sensor Networks 6th European Conference on Wireless Sensor Networks, Cork, Ireland.

[4] Mona Sharifnejad, Mohsen Sharifi.” A Survey on Wireless Sensor Networks Security”. SETIT 2007 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications.

[5] Gaurav Sharmaa* Suman Balaa, Anil K. Vermaa.(2012).”Security Frameworks for Wireless Sensor Networks-Review”. 2nd International Conference on Communication, Computing & Security [ICCCS-2012].

[6] Kui Ren.(2007).”Communication Security in Wireless Sensor Networks”. WORCESTER POLYTECHNIC INSTITUTE In partial fulfillment of the requirements for the Degree of Doctor of Philosophy in Electrical and Computer Engineerin.

[۷] Muhammad Khurram Khan , and Khaled Alghathbar.(2010).” Cryptanalysis and Security Improvements of ‘Two-Factor User Authentication in Wireless Sensor Networks’”. ISSN 1424-8220 www.mdpi.com/journal/sensor

[۸]Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar Spins: Security Protocols for Sensor Networks 7th annual ACM/IEEE international conference on mobile computing and networking.

[۹]Zhu, S., Setia, S., Jajodia, S., 2003. LEAP: Effcient Security Mechanisms For Large-Scale Distributed Sensor Networks ACM Conference on Computing and Communicati

[10]Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., Kruus TinyPK: securing sensor networks with public key technology 2nd